OpenLearn

The Open University

Introduction to cyber security

This item contains selected online content. It is for use alongside, not as a replacement for the module website, which is the primary study format and contains activities and resources that cannot be replicated in the printed versions.

Contents

Introduction and guidance 7
Introduction and guidance 7
What is a badged course? 7
How to get a badge 8
Week 1: Threat landscape 11
Introduction 11
1 Online, the new frontline 13
1.1 Talking security: the basics 14
1.2 Obtaining Sophos Threatsaurus 17
1.3 Cyber security attacks and phishing 18
1.4 Examples of high profile cyber security breaches 19
1.5 Taking stock of your information assets 23
1.6 What are your own safeguards? 24
2 Understanding current threats 26
2.1 Identifying vulnerable systems 27
2.2 How to keep up to date 28
2.3 Staying informed 32
3 Securing my digital information 33
3.1 Threats to your assets 34
4 Week 1 quiz 36
5 Summary of Week 1 37
Further reading 38
Week 2: Authentication 40
Introduction 40
1 Passwords: what are they for? 41
1.1 What happens when you enter a password? 41
1.2 Attacking passwords 43
1.3 Salt to protect 45
2 Improving password security 47
2.1 How to pick a proper password 47
2.2 Checking the strength of a password 50
2.3 Password managers 51
2.4 Installing and using a password manager 52
2.5 Alternatives to using password managers 54
3 Two-factor authentication 56
3.1 Setting up two-factor authentication 58
3.2 Other services supporting two-factor authentication 59
4 Week 2 quiz 61
5 Summary of Week 2 62

Further reading 63

Week 3: Malware 65

Introduction 65

1 Viruses 66

1.1 Worms 67

1.2 Trojans 68

1.3 Defining terms 69

2 How malware gets into your computer 70

2.1 What is malware for? 71

2.2 Phishing 72

2.3 Trapping phishing emails 74

2.4 Spotting a phishing email 76

2.5 Emails are not the only phish 78

2.6 The role of malware in click fraud 79

2.7 Botnets 80

2.8 Confessional 81

3 Keeping yourself protected 82

3.1 Antivirus software 83

3.2 Installing antivirus software 85

3.3 Keeping your software up to date 86

3.4 End-of-life software 87

3.5 Sandboxes and code signing 88

4 Week 3 quiz 90

5 Summary of Week 3 91

Further reading 92

Week 4: Networking and communications 94

Introduction 94

1 What is the internet? 95

1.1 How data moves around the internet 96

1.2 Introducing the datagram 97

1.3 Datagrams on the move 98

1.4 Wireless networks 99

2 Is your private information really private? 101

2.1 Network security challenges 102

2.2 Encryption in wireless networking 103

2.3 Using wireless networking securely 105

3 Why we need standards on the internet 106

3.1 Introducing the TCP/IP protocols 107

3.2 The internet protocol and IP addresses 109

3.3 From numbers to names 111

3.4 The internet is not the world wide web 112

4 Week 4 quiz 114

5 Summary of Week 4 115

Week 5: Cryptography 117

Introduction 117

1 The secret of keeping secrets 118

- 1.1 Plaintext and ciphertext 119
- 1.2 Encryption keys 120
- 1.3 The key distribution problem 121
- 1.4 Asymmetric or public key cryptography 122
- 1.5 Why isn't the internet encrypted? 123

2 Putting cryptography to use 125

- 2.1 Setting up a PGP email client 127
- 2.2 Sending signed and encrypted email 128

3 Comparing different cryptographic techniques 129

- 3.1 Using cryptography to prove identity 131
- 3.2 Digital signatures and certificates 132
- 3.3 Encrypted network connections 136
- 3.4 How secure is your browsing? 138

4 Week 5 quiz 140

5 Summary of Week 5 141

Week 6: Network security 143

Introduction 143

1 Firewall basics 144

- 1.1 Personal firewalls 145
- 1.2 Configuring your own firewall 146

2 VPN basics 149

- 2.1 Securing the tunnels 151
- 2.2 Security risks of VPN 153
- 2.3 Putting VPN to work 155

3 Intrusion detection system (IDS) 157

- 3.1 IDS techniques 158
- 3.2 Honeypots 159

4 Week 6 quiz 161

5 Summary of Week 6 162

Further reading 163

Week 7: When your defences fail 165

Introduction 165

1 Identity theft 166

- 1.1 Loss of data 167
- 1.2 Risks of data loss 170

2 Laws and computers 172

- 2.1 Data Protection 174
- 2.2 The Investigatory Powers Act 2016 (IPA) 176
- 2.3 The Computer Misuse Act 1990 (CMA) 178
- 2.4 The Fraud Act 2006 180
- 2.5 Lawful Business Practice Regulations 181

2.6 Cyber security and the law 182
2.7 Cyber security in the EU 183
2.8 What laws apply in your country? 184
3 Who should you contact? 186
3.1 Getting your computer working again 188
3.2 Making your information less vulnerable 190
3.3 Protecting your data for the future 192
3.4 Backup media 193
3.5 Remote backups 196
3.6 Do you backup your data? 198
3.7 Archiving data 199
4 Week 7 quiz 200
5 Summary of Week 7 201
Further reading 203
Week 8: Managing security risks 205
Introduction 205
1 Information as an asset 206
1.1 Your own information assets 208
1.2 Risk analysis 209
1.3 Risk analysis in practice 210
2 Staying safe online 213
2.1 Fix your browser 215
2.2 Risk management in practice 218
2.3 Protecting your information assets 219
2.4 What should I do next? 220
2.5 Tracking a moving target 221
3 What do you do now? 223
3.1 Confessional 223
4 End-of-course quiz 225
5 End-of-course guide and round-up 226
6 Next steps 227
Tell us what you think 228
References 228
Acknowledgements 229

Introduction and guidance

Introduction and guidance

Introduction to cyber security: stay safe online is an informal, introductory course for people who want to feel more confident about their online safety. This free online course will help you to understand online security and start to protect your 'digital life', whether at home or work. You will learn how to recognise the threats that could harm you online and the steps you can take to reduce the chances that they will happen to you.

Part of this practice will be the weekly interactive quizzes, of which Weeks 4 and 8 will provide you an opportunity to earn a badge to demonstrate your new skills. You can read more on how to study the course and about badges in the next sections.

Like most courses these days, *Introduction to cyber security: stay safe online* has learning outcomes. These are not as complicated as they sound, but are simply what we hope you will achieve by the end of the course. After completing this course, we hope that you will have a better understanding of:

- implementing a plan to protect your digital life
- recognising threats to online safety
- taking steps to reduce the risk of online threats
- concepts including malware, viruses and Trojans
- network security, cryptography and identity theft.

Moving around the course

The easiest way to navigate around the course is through the 'My course progress' page. You can get back there at any time by clicking on 'Back to course' in the menu bar.

It's also good practice, if you access a link from within a course page (including links to the quizzes), to open it in a new window or tab. That way you can easily return to where you've come from without having to use the back button on your browser.

Get careers guidance

This course has been included in the National Careers Service to help you develop new skills.

What is a badged course?

While studying *Introduction to cyber security: stay safe online* you have the option to work towards gaining a digital badge.

Badged courses are a key part of The Open University's mission *to promote the educational well-being of the community*. The courses also provide another way of helping you to progress from informal to formal learning.

To complete a course you need to be able to find about 24 hours of study time, over a period of about 8 weeks. However, it is possible to study them at any time, and at a pace to suit you.

Badged courses are all available on The Open University's OpenLearn website and do not cost anything to study. They differ from Open University courses because you do not receive support from a tutor. But you do get useful feedback from the interactive quizzes.

What is a badge?

Digital badges are a new way of demonstrating online that you have gained a skill. Schools, colleges and universities are working with employers and other organisations to develop open badges that help learners gain recognition for their skills, and support employers to identify the right candidate for a job.

Badges demonstrate your work and achievement on the course. You can share your achievement with friends, family and employers, and on social media. Badges are a great motivation, helping you to reach the end of the course. Gaining a badge often boosts confidence in the skills and abilities that underpin successful study. So, completing this course should encourage you to think about taking other courses.

How to get a badge

Getting a badge is straightforward! Here's what you have to do:

- read each week of the course
- score 50% or more in the two badge quizzes in Week 4 and Week 8.

For all the quizzes, you can have three attempts at most of the questions (for true or false type questions you usually only get one attempt). If you get the answer right first time you will get more marks than for a correct answer the second or third time. Therefore, please be aware that for the two badge quizzes it is possible to get all the questions right but not score 50% and be eligible for the badge on that attempt. If one of your answers is incorrect you will often receive helpful feedback and suggestions about how to work out the correct answer.

For the badge quizzes, if you're not successful in getting 50% the first time, after 24 hours you can attempt the whole quiz, and come back as many times as you like.

We hope that as many people as possible will gain an Open University badge – so you should see getting a badge as an opportunity to reflect on what you have learned rather than as a test.

If you need more guidance on getting a badge and what you can do with it, take a look at the OpenLearn FAQs. When you gain your badge you will receive an email to notify you and you will be able to view and manage all your badges in My OpenLearn within 24 hours of completing the criteria to gain a badge.

Get started with Week 1.

Week 1: Threat landscape

Introduction

Video content is not available in this format.

Welcome to this free course, *Introduction to cyber security: stay safe online*.

Cory Doctorow is your guide through this course. He is a visiting professor at The Open University. He'll meet you at the start of each week to let you know what's coming up and remind you of what you've learned so far to help you make the most of your learning.

About the course

Your journey into the world of cyber security and protecting your digital life has been organised into eight weeks of study. The first three weeks focus on understanding the basics of cyber security. This includes an exploration of the security threat landscape, together with some of the basic techniques for protecting your computers and your online information.

You'll then look 'under the hood', exploring some of the technologies that underpin the internet and cyber security. This will include gaining an understanding of how computers are connected in a network and how the data transmitted across that network is kept secure.

In the final two weeks of the course, you'll look at what can be done if you suffer a successful cyber security attack and how to develop an action plan. As part of this, you'll learn about both the legal and technical aspects of recovering from an attack.

This course will not only help you take steps to protect yourself online, such as how to create a strong password, but also provide an overview of cyber security from the security threat landscape to how the internet works. It will also provide a foundation for further study of this important discipline.

To test your knowledge you can try the end-of-week practice and end-of-course compulsory badge quizzes.

The Open University would really appreciate a few minutes of your time to tell us about yourself and your expectations for the course before you begin, in our optional start-of-course survey. Participation will be completely confidential and we will not pass on your details to others.

1 Online, the new frontline

Video content is not available in this format.

We shop online. We work online. We play online. We live online. More and more, our lives depend on online, digital services. Almost everything can be done online – from shopping and banking to socialising and card making – and all of this makes the internet, also known as cyberspace, an attractive target for criminals.

Large-scale cyber security breaches often make the headlines but about 70% of organisations are keeping their worst security incidents under wraps, so what makes the news is just a small proportion of the breaches that are actually taking place. Computers and their users in Britain are being targeted by many thousands of cyber attacks every hour.

We all have a responsibility to protect services from being maliciously disrupted or misused, through our vigilance, through our own security measures and through reporting events when they arise.

The knowledge, tools and best practices relating to protecting the computers, communications networks, programs and data that make our digital lives possible are collectively referred to as cyber security, or information security. For the purposes of this course, we use the two terms interchangeably.

Behind the numbers

Cyber security is definitely one of those areas where you need to evaluate the validity of any information you find online before accepting it. The UK government regularly publishes surveys of cyber security breaches. In 2019, 32% of businesses identified cyber security breaches or attacks in the previous 12 months. Medium (over 50 employees) and large businesses (over 250 employees) were particularly at risk with 60% reporting attacks. The report also notes that attacks may be under reported and the true cost and impact of cyber security breaches may be undervalued. It also notes that some businesses may not be aware that they have been attacked (Department for Digital, Culture, Media and Sport, 2019).

By far the largest number of attacks reported are fraudulent emails, or fraudulent websites. Phishing attacks have resulted in the most disruptive and expensive breaches in the past 12 months. Specialist security firms also publish regular reports on the current cyber security situation. TrendMicro reports blocking 26,804,076,261 threats in the first half of 2019 (TrendMicro, 2019). Again, the largest proportion contained in emails. Sophos also reports spam emails as the biggest source of attacks and warns that ransomware is increasing and can be the most destructive (Sophos, 2019).

Statista is a business that focuses on collecting and presenting statistics on a huge variety of subjects. Some of these reports are free of charge. For example, it reports that over 446.5 million records were exposed by data breaches in the United States in 2018 (Statista, 2018).

Let's get started by learning some of the basic terminology used when discussing cyber security.

1.1 Talking security: the basics

Figure 1

In any discussion of security, there are some basic terms that will be used a lot. This section will introduce you to the basic terminology of information security.

CIA

The guiding principles behind information security are summed up in the acronym CIA (and we're pretty sure there's a joke in there somewhere), standing for confidentiality, integrity and availability.

We want our information to:

- be read by only the right people (confidentiality)
- only be changed by authorised people or processes (integrity)
- be available to read and use whenever we want (availability).

It is important to be able to distinguish between these three aspects of security. So let's look at an example.

Case study: Equifax, credit reporting company

In September 2017, Equifax reported a data breach in which the records of 147 million people had been exposed. This mostly affected people in the US, but 693,665 people in the UK also had their data exposed. Equifax UK later wrote letters to each of these people explaining the situation.

The exposed data contained millions of names and dates of birth, Social Security numbers, physical addresses, and other personal information that could lead to identity theft and fraud. Equifax had a system to monitor network traffic, but it hadn't worked for the previous 19 months because a security certificate hadn't been renewed.

Equifax stored its data in a database called ACIS, and was alerted in March 2017 to a critical security vulnerability in an Apache Struts web server that provided access to this database. A patch had been issued but Equifax failed to ensure that the patch was installed. Hackers exploited this vulnerability until the missing certificate was installed at the end of July 2017.

In May 2019, the data breach was thought to have cost Equifax $1,400,000,000.

In July 2019, Equifax agreed a settlement with The Federal Trade Commission (US) of over $575,000,000 (perhaps up to $700,000,000) with a free monitoring and identity theft service for up to 10 years.

So how do the principles of CIA apply to the Equifax case? Quite obviously, confidentiality was violated: unauthorised people could read the data. However, authorised users still had full access to the data, so it remained available; and the data was not changed, so its integrity was preserved.

Information assets

Time for another definition. When talking about valuable data we use the term ‘information assets’. In the Equifax case, the information assets were the data about people and their financial records collected by Equifax.

When we consider security of online communications and services, we also need two additional concepts: ‘authentication’ and ‘non-repudiation’.

When we receive a message, we want to be confident that it really came from the person we think it came from. Similarly, before an online service allows a user to access their data, it is necessary to verify the identity of the user. This is known as authentication.

Non-repudiation is about ensuring that users cannot deny knowledge of sending a message or performing some online activity at some later point in time. For example, in an online banking system the user cannot be allowed to claim that they didn’t send a payment to a recipient after the bank has transferred the funds to the recipient’s account.

Malware

Finally, there are a number of terms associated with software that attempts to harm computers in different ways. Collectively these are known as ‘malware’ (a contraction of malicious software).

Depending on what the malware does, different terms are used to in relation to malware. For example:

- **ransomware** is malware that demands payment in order to refrain from doing some harmful action or to undo the effects of the harmful action
- **spyware** records the activities of the user, such as the passwords they type into the computer, and transmits this information to the person who wrote the malware
- **botnets** are created using malware that allows an attacker to control a group of computers and use them to gather personal information or launch attacks against others, such as for sending spam emails or flooding a website with so many requests for content that the server cannot cope, called a denial-of-service attack.

You’ll learn more about malware in Week 3.

Now that you understand some of the basic concepts and terminology, you’ll use this knowledge to study real examples of cyber security breaches.

1.2 Obtaining Sophos Threatsaurus

Figure 2

There are lots of technical terms relating to cyber security and it can be difficult to keep track of what's what.

Sophos is one of the major players in the anti-malware business. They publish a Threatsaurus to help you remember and define the terms relating to malware. The Threatsaurus is a plain-English guide, to help IT managers and end users understand the threats posed by malicious software. The Threatsaurus includes:

- an A–Z glossary on computer and data security threats
- practical tips to stay safe from email scams, identity theft, malware and other threats
- a guide to Sophos's security software and hardware.

Download the Sophos Threatsaurus PDF from https://ugc.futurelearn.com/uploads/files/3f/d3/3fd36a66-d941-4595-b587-1a7b41998ae9/Week_3_Sophos_Threatsaurus_AZ.pdf.

We have provided the complete web address for this file, so that you can easily check that the link points to a trustworthy site – in this case futurelearn.com. In general, before clicking on any link you should develop the habit of checking the address that it points to. This can be done by hovering your mouse pointer over the link and checking the status bar of your browser. On a mobile or tablet device, touching and holding the link will usually bring up a dialog box showing the complete link and some options of how to open it.

Save it so that you can refer to it throughout the course. You'll use it again in Week 3.

1.3 Cyber security attacks and phishing

Video content is not available in this format.

Britain is being targeted by many thousands of cyber attacks every hour. For small organisations the worst breaches cost between £65,000 and £115,000 on average and for large organisations may run to many millions of pounds. These costs can occur as direct financial losses due to fraud or theft; the loss of productivity due to time spent recovering from the effects of a successful attack; or the lost of trust and reputation.

Phishing

It may be surprising that many cyber security breaches do not result from technical failures. In fact, it is commonplace for attackers to exploit the goodwill and trust of people to gain access to systems, using a form of attack that is known as ‘social engineering’. Pretending to be technical support personnel or crafting emails that ask for usernames and passwords are common forms of social engineering attacks. You may have heard the term ‘**phishing**’ used to describe these kinds of emails. Phishing is a form of social engineering. In the video, course guide Cory explains how it happened to him.

Phishing emails can use your real details and passwords to make you think that the attacker is a real contact that you already know, or to make you think that they have more information than they actually do to panic you into clicking on a message. The criminals get your email address and password data etc. from breaches of many online databases.

In October 2019, over 30,000 aggressive phishing emails an hour were being sent out to email addresses where a password was known:
https://www.bbc.co.uk/news/technology-50065713

In January 2019, Troy Hunt, a security professional, published details of a database being used by criminals that contained 773 million records and over 21 million unique passwords.

To check if your account has been part of a data breach that included your email address visit https://haveibeenpwned.com. To check if a password that you use has also been found in a data breach visit https://haveibeenpwned.com/Passwords. Don't type in a complete password to start with. Type in the first few characters and click 'pwned?' If it doesn't come up, your password is safe. If it does get a match, add the next character and check again. If you have typed in the complete password and get a match it is time to change your password!

Of interest, check the password 123456789. How many times has that been seen?!

In a later week in the course you'll study how to create secure passwords.

In the next section you'll find out about three high profile cyber security breaches.

1.4 Examples of high profile cyber security breaches

Figure 3

Cyber security attacks take many forms from obtaining users' personal information, to attacking critical national infrastructure and obtaining companies' proprietary data. Here we describe four high profile cyber security breaches which caused major financial losses and damaged the reputations of the organisations concerned.

Attacking online identities

Adobe Systems is one of the more important companies in the digital economy. Its software is used to produce, publish and present an enormous amount of material – chances are your favourite magazines and books were laid out with Adobe software.

Over the years, Adobe had stored the names, addresses and credit card information of tens of millions of users on its servers. Then, in October 2013, Adobe admitted that data

from 2.9 million accounts had been stolen. Later, that number was revised to 38 million accounts, but when the data file was found on the internet it contained no less than 153 million user accounts. Much of this data could be read and soon copies of the stolen accounts were in wide circulation. It also became clear that the people who had stolen user data had also gained access to Adobe's development servers – program code, potentially worth billions of dollars, had also been stolen.

Adobe was forced to change the log in details of every one of its users and to greatly improve its own security. And, of course, users sued Adobe for not protecting their information.

You can check to see if your email address was included in this information that was stolen by visiting: https://haveibeenpwned.com/ and entering your email address into the email input box.

Is Adobe alone, or are other companies holding valuable data but not protecting it properly?

Fast forward to 2019

- A huge database of 49 million Instagram accounts was exposed online without any password protection (TechCrunch, 2019a).
- A database containing hundreds of millions of phone numbers linked to Facebook accounts was left exposed online (TechCrunch, 2019b).
- Personal data of the entire population of Ecuador was available online – 20.8 million records, some including bank balance (ZDNet, 2019).

Attacking industrial systems

Not many people want a uranium centrifuge, but those that do, really want a uranium centrifuge. The centrifuge was developed after the Second World War for enriching uranium so that it can be used either for generating nuclear power, or, as the heart of a nuclear weapon.

Under international treaty it is not illegal for countries to slightly enrich uranium for nuclear energy, but high levels of enrichment are forbidden to all but a handful of countries. As a consequence, centrifuge technology is tightly controlled, but still, centrifuges have gradually spread around the world. Most recently they have been developed by Iran, ostensibly for that country's legal civil nuclear programme; but it is sometimes suspected it might possibly be for the development of an Iranian nuclear bomb.

In the summer of 2010, a new piece of malicious software for the Microsoft Windows operating system was discovered by an antivirus company in Belarus. The software was dissected and found to attack a very specific set of computer-controlled high-speed motors manufactured by Siemens. Left unchecked, the software, dubbed 'Stuxnet', would rapidly increase and decrease the speed of the motors causing irreparable damage to whatever was connected to them – among other things, uranium centrifuges.

The very specific nature of the systems targeted by Stuxnet make many believe that it was developed specifically to disrupt the Iranian uranium enrichment programme. By the autumn of 2010, reports were appearing that the Iranian centrifuge programme was in trouble. The Israeli paper Haaretz reported that Iran's centrifuges had not only produced less uranium than the previous year, but that the entire programme had been forced to

stop and start several times because of technical problems. Other sources reported that Iran had been forced to remove large numbers of damaged centrifuges from its enrichment plant.

In 2016, there was a serious cyber attack on the Ukrainian power grid (Ars Technica, 2019). Recent analysis has provided much more detail about how it was carried out. It would appear that the intention was to disable safety monitoring equipment in such a way that the operators would not be aware that important safety equipment had also been turned off. This could have caused catastrophic damage when operators attempted to restore power. The target was a known vulnerability in a piece of Siemens equipment known as a Siprotec protective relay. A security patch was available but may not have been installed.

In 2017, there was an incident at a Saudi oil refinery, Petro Rabigh, when malware shut down the plant. A report by Dragos, updated in 2019, suggested that the malware was probing the plant's industrial control systems when it accidentally triggered the shutdown. In 2019, Dragos reports that the same group behind this malware was probing industrial control systems within the electrical transmission networks in the US and Europe-wide. They have named this threat XENOTIME (Dragos, 2019).

In 2019, a week after suffering a crippling ransomware infection by LockerGoga, Norwegian aluminum producer Norsk Hydro estimates that total losses from the incident had already reached $40 million. It is not clear whether Norsk Hydro was specifically targeted, or whether this was the result of a random infection, but it illustrates the risk to industrial operations from attacks on the IT infrastructure.

Attacking specific targets

In December 2013, the American retailer Target announced that hackers had stolen data belonging to 40 million customers. The attack had begun in late November and continued for several weeks before it was detected. By then it had compromised more than 110 million accounts, including unencrypted credit and debit card information as well as encrypted PIN data. By February 2014, American banks had replaced more than 17 million credit and debit cards at a cost of more than $172 million. The amount of fraud linked to the attack is unknown, as is the damage to Target's reputation.

Target was not the first major retailer to be hit by hackers, but this attack was different from most; the weakness that allowed the attackers into the Target computers lay outside of the company. The hackers had gained access through computers belonging to one of Target's heating, ventilation and air conditioning services (HVAC) contractors. Like many large organisations, Target allows other companies to access its internal networks, to submit bills and exchange contracts.

The hack appears to have begun when an employee of the HVAC company received an email from one of their trusted partners. In fact, the email was fake and contained malicious software. Unlike traditional spam email, this message had been targeted at a very specific audience – the HVAC company. It was what is known as 'spear phishing'.

Once the email had been opened, the hidden software went to work and retrieved the HVAC company's Target network authorisations, allowing them to log on to their real objective. In an ideal system, the HVAC company's authorisations should have restricted them to a network responsible solely for billing and contracts, but, like a lot of big organisations, Target used a single network for all of its data, allowing the attackers to eventually locate, and steal, customer data.

The Target attack is an example of an advanced persistent threat. Rather than attempting to attack the retailer directly, the hackers had chosen an external company which was much less likely to have the resources to detect and defend against an attack. Their spear phishing email was directly targeted at the contractor, lulling them into a false sense of security and allowing the malware to retrieve the logon credentials needed to attack Target itself.

In 2017, Target had to pay a settlement of $18,500,000 and agree to make the following changes to significantly improve its security.

- Develop and maintain a comprehensive information security program
- Maintain software and encryption programs to safeguard people's personal information
- Separate its cardholder data from the rest of its computer network
- Rigorously control who has access to the network
- Regularly bring in an independent and well-qualified third party to conduct regular, comprehensive security assessments of its security measures.
- Hire an executive officer to run its new security program and serve as a security advisor to the CEO and the board of directors.

You don't need to be a huge company to be specifically targeted by criminal hackers

An employee responsible for handling the company finances knew that a meeting to finalise the acquisition of another company was in progress. He received the email: 'Hey, the deal is done. Please wire $8m to this account to finalise the acquisition ASAP. Needs to be done before the end of the day. Thanks.' The employee thought nothing of it and sent the funds over, ticking it off his list of jobs before heading home. But alarm bells started to ring when the company that was being acquired called to ask why it had not received the money. An investigation began - $8m was most definitely sent, but where to?

The criminal hacker clearly new of the meeting in progress. Most likely by intercepting emails over several days or weeks to look for an opportunity for an attack. For the rest of the report see https://www.bbc.co.uk/news/technology-49857948

Even private individuals have been attacked in this way – again the most likely method of attack is by intercepting emails. Perhaps by sitting in a car outside the victims house and snooping on the data transmitted through home router wireless networks (WiFi) that have not been password protected, or perhaps by snooping the WiFi traffic of a local tradesman or estate agent, waiting for emails that show that an invoice is about to be sent. The hacker then sends an identical invoice, but with a different account to receive the payment.

Activity 1 Describing cyber security breaches

Allow about 10 minutes

Choose one of the three example attacks outlined above. You can choose Adobe, Stuxnet or Target.

Using the terminology you've learned so far, try writing a brief description of the attack which might explain it to other learners, and write it in the space below.

Examples of things you might put into your description are:

- the CIA concepts that are relevant to the example you have chosen
- whether malware was involved in the attack, and what type of malware it was
- the asset that was affected by the attack.

Provide your answer...

1.5 Taking stock of your information assets

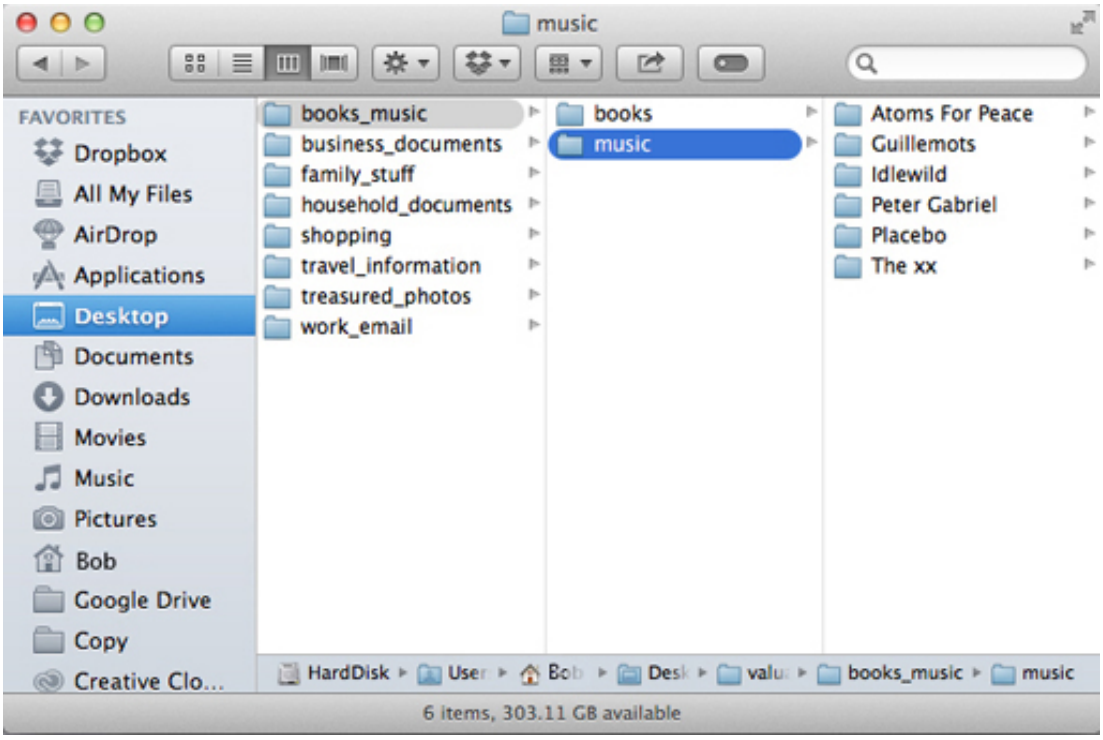


Figure 5

Before you can take steps to protect your corner of cyberspace, you need to know what information you have that needs protection: your information assets.

Activity 2 Your information assets

Allow about 15 minutes

Compile a list, perhaps in a spreadsheet or using one of our templates, of the different types of information you store on your computer or online. For example, you may have personal correspondence, photographs, work documents or personal details such as your National Insurance number, insurance policy details and passwords for online services.

- Information assets list template (PDF)

For each type of information, think of its value to you. Label the most valuable types of information as ‘High’, the least valuable as ‘Low’ and those that are in between as ‘Medium’.

The value could be the cost to replace the information, in time or money, or the impact of its loss on your reputation, for example, all your emails or photographs could all be published online.

Do the same exercise for the online activities you engage in. For example, you might use online banking, shopping or social networking services. This time, label each one with a value based on the potential cost of an unauthorised person gaining access to it.

In the next section, you will use this information as part of a survey that will help you get a picture of your exposure to information security threats but you won’t be asked to share the details of your list. You’ll use this list later in the course, too.

1.6 What are your own safeguards?

Figure 6

It’s time for you to take stock of your own safeguards against data loss, unwarranted access or malicious software. We’d also like to know a bit more about the frequency of computer crime to the average user.

This survey is a series of multiple-choice questions based on your current habits. There are no right or wrong answers so you should choose the answer that most closely matches the way you use your computer.

The data collected is anonymous and cannot be linked to your OpenLearn profile or email address. However, filling in online surveys is not something to be done without considering the risk. Many surveys are often designed to capture saleable information, or

information to use in a phishing attack, or for identity theft. Often a small prize is offered as well. Remember, your online security is worth far more than any possible prize.

2 Understanding current threats

Figure 7

Now you know what information assets you have, you'll look at how those assets can be compromised.

You will learn about some different kinds of threat, the vulnerabilities that they exploit and some countermeasures that can be put in place to guard against them. When we use those terms we mean:

- **vulnerability** – a point at which there is potential for a security breach
- **threat** – some danger that can exploit a vulnerability
- **countermeasure** – action you take to protect your information against threats and vulnerabilities.

Threats can take many different forms, including unauthorised access to data with the intent of committing fraud against individuals or businesses. At its most extreme, there is the potential for the systematic disruption of computer networks and services, putting cyber security threats on a par with those associated with terrorism. The UK government set up the National Cyber Security Centre to act as the UK government's single authority on cyber security – improving our understanding of the threat, reducing the harm from cyber attacks and providing a unified source of advice and support.

In a 2018 report, the UK government's National Cyber Security Centre highlighted that cyber security threats to UK businesses continue to grow, with particular emphasis on ransomware and distributed denial of service (DDoS) attacks.

New threats are being discovered all the time and they can affect any and every operating system, including Windows, Mac OS, Linux, Android and iOS. Additionally, there are growing threats due to potential vulnerabilities in the growing number of Internet of Things

devices being connected to our networks. To protect ourselves it is important to keep ourselves up to date with the latest cyber security news.

Next, you will explore how vulnerable systems can be identified using the Shodan search engine.

2.1 Identifying vulnerable systems

The first step in protecting systems from attack is to identify if there are any vulnerabilities.

Video content is not available in this format.

The proliferation of networked computing devices that are embedded in everyday things (often called the “Internet of Things” or “IoT”) is going to pose a significant challenge for cyber security in the future. Already we are seeing examples of security vulnerabilities in home entertainment devices like Smart TVs and internet connected home security cameras. Sources of these security vulnerabilities range from devices that use out of date operating systems or software applications, to devices that do not use any cryptography to protect their communications.

The video describes how different types of system vulnerabilities can be identified by using the Shodan search engine. This is a tool that catalogues millions of devices connected to the Internet, collecting information about the operating systems they use, their configurations and even in some cases default user names and passwords for accessing them.

Using Shodan to find computers connected to the Internet is legal. However, please note that it is an offence under the Computer Misuse Act 1990 to try and gain access to a computer without authorization. And even if you failed to get in, you could well be found guilty of a crime. It is incredibly easy to break the law if you misuse information from Shodan, so don't do it!

Addressing the security challenges of IoT systems is a multi-pronged effort, with researchers in academia and industry working on developing new technology solutions

for improving their security. It is also critical that engineers are trained to ensure that security and privacy is considered as a core part of the design and development of all computer systems, including the Internet of Things.

2.2 How to keep up to date

Figure 8

Attackers are constantly finding new vulnerabilities and ways of attacking computer systems. Therefore, it is important to keep yourself informed and up to date with threats that are relevant to your situation.

There are many sources of news about cyber security. Many of them are extremely technical and are designed for security specialists to communicate their findings with one another, for software developers to improve their programs or academic publications. There are also plenty of free resources, written by journalists, security professionals and enthusiastic amateurs, where you can learn more even if you are new to the field.

The links provided below are a selection from those that are available. You are not expected to look at all of them in detail.

Government sites

- National Cyber Security Centre

News sites

The best places to get started are the major media outlets, most of whom employ technology journalists. These sites will give you readable information intended for as wide an audience as possible. Many of them are updated several times a day, but they will only consider 'newsworthy' events such as a major hack or virus outbreak, and some will only cover news in a particular country – so you may need to look at a variety of sites:

- BBC News Technology
- Guardian Online Technology
- The Telegraph Internet security
- Bloomberg Cyber security

Technology sites

Many sites devoted to technology will cover aspects of security on a regular basis. Most of the sites below cover other topics, so you might need to use their search functions to find relevant information.

- Wired – Threat level
- Computer Weekly
- The Hacker News
- Info-Security magazine

Information security companies

There are a large number of companies selling security software to home users and to businesses. Almost all of them maintain regularly updated websites explaining new and emerging security threats and how they can be overcome.

Much of this information is technical and aimed at administrators responsible for large computer systems, but the introductory material is often quite easily understood. These sites can be the best to use when a new security issue is identified.

- Sophos labs
- Microsoft
- Apple

Blogs

- Krebs On Security Brian Krebs is an American journalist and investigative reporter. He is best known for his coverage of profit-seeking cybercriminals. His interest grew after a computer worm locked him out of his own computer in 2001.
- Graham Cluley is an award-winning security blogger, researcher and public speaker. He has been working in the computer security industry since the early 1990s, having been employed by companies such as Sophos, McAfee and Dr Solomon's.

- Bruce Schneier is an internationally renowned security technologist who writes a monthly newsletter, called ‘Crypt-o-gram’. He provides commentary and insights into critical security issues of the day. The content of this blog can be accessed in multiple forms, including a podcast and an email newsletter.
- Troy Hunt provides analyses of different system breaches and useful hints on how to avoid being attacked.

Before you can identify your enemies you need to know who you can trust. First you need to think about, and constantly evaluate who and what you trust, and to what degree you trust them. You cannot rigorously check every possible contact or item of software yourself, so you build up a network of trusted contacts or sources of information. For each of your trusted contacts or sources you need to evaluate the degree to which you trust them. What is their level of expertise? And to what degree do you trust them? If you compare sources of information, to what degree is one simply copying from the other? You need sources that have the expertise and independently evaulate the information you are interested in.

For example, you build trust in a bank because it has branches on many high streets, it is recognised and regulated by The Financial Conduct Authority in the UK and your money is protected by laws in the UK and the EU up to EUR100,000 when in a regulated bank. Based on this trust you may use the bank's website, or an app provided by that bank.

You may share information about yourself with people and organisations that you trust - but even so you need to evaluate what information they might need to have and what they might do with that information.

You throw away that security if you post information about yourself to any stranger who might come across it. So think carefully before placing any information online that may be passed on by a friend, who then passes it on to someone else and so on. Also think carefully about information that might be included in web pages, photos or videos posted online and available to many strangers.

Here are a couple of examples of information you shouldn’t trust:

- **Profiles on dating websites:** there may be a genuine person behind that profile, but on the other hand it might be a criminal or scammer. Scammers may continue to exchange information for a year or more, drawing you in, using fake information and images from someone else's blog, even exchanging intimate pictures, until there is a very plausible request for money for the plane fare to visit you, or blackmail you over your intimate pictures. You have no basis for trust! Only what they have told you.
- **An advert for anti-malware software at a bargain price:** the link takes you to a website that claims it is totally brilliant, with lots of reviews on that site saying how good it is. It may also claim that it has been ranked number 1 by various other sites. But note that you have no basis for trust. A criminal can easily create such a website with that information, a shopping cart payment system to take your money and provide software for you to download. At best the software may be useless. At worst it will install malware on your computer and attempt to take repeated payments from your account.

When searching for information on how to keep yourself secure you need to evaluate your trust in the sources of information, and you should start from our highly trusted sources.

Activity 3 Knowing your enemies

Allow about 20 minutes

Carry out some research about different cyber security threats and the types of groups who pose the threat.

Using the information sources above find out about:

- a threat to your information, computers and other devices that arise from malware
- a threat to your communications (such as spam and denial of service (DoS) or distributed denial of service (DDoS) attacks, often launched using botnets).

For each threat, try to identify the type of individuals or organisations that are posing the threat. Which of the following types would best describe them?

- **Cybercriminal:** those carrying out cyber attacks for personal financial gain.
- **Spies:** those engaged in espionage activities on behalf of either commercial organisations or national governments.
- **Hacktivists:** those who carry out cyber attacks as a form of protest against organisations or governments.
- **Insider attacker:** disgruntled or dishonest staff who attack their organisation's computer systems.

If you identify a different type of attacker, how would you describe it?

Spend 10–15 minutes researching, then spend five minutes noting down your findings in the space below.

Provide your answer...

2.3 Staying informed

Figure 9

Hopefully, you now have some ideas of how to stay up to date with the latest developments in cyber security.

Before continuing to the final part of the week, take some time to plan some concrete steps you will take to keep yourself more informed.

For example, you could subscribe to a blog via email or Feedly, or follow updates via Twitter or Facebook.

3 Securing my digital information

Figure 10

What issues arise in doing everyday activities online? As we've already discussed, most of us rely on the internet for everyday tasks such as shopping, working, banking or social networking. We often do this without stopping to think about the security issues that might be involved.

Activity 4 Securing your information

Allow about 15 minutes

Choose one of the following activities and think about the main security issues that might threaten your chosen activity.

- **Online banking** – for example, to check the balance in your account or make a payment.
- **Online shopping** – think particularly about buying something from a new store that you don't recognise and haven't shopped from before.
- **Social networking** – think about whether you would add someone as a 'friend' if you hadn't met them in person.
- **Working from home** – consider the need to transfer documents that contain confidential information between members of your team.

Answer

The following case study provides an example for the fourth option above, working from home.

Case study: working from home

When working from home you may need to share a confidential file with a colleague in another location. You could email it to them, but this is not a secure method of transmitting information – email is easily intercepted en route to its destination and there is always the risk that you send it to the wrong person!

You could use an online cloud service such as Dropbox, Google Drive or Microsoft OneDrive to store the file, but you will have to make sure that your colleague can access the uploaded file. You might also be worried about the security of the cloud services against hackers.

You could put the file on a USB flash memory drive and post it to your colleague. But the drive could be lost, stolen or intercepted by an attacker who adds malware to the drive as a way of infecting your organisation's computers.

Or, you could use encryption to lock the file against intruders. You could email the encrypted file safe in the knowledge that no one else could read the document. However, you would have to be sure that your colleague knows how to use encryption software so that they can decrypt the document when it arrives.

Questions to consider

Remember that earlier this week we classified security issues under three headings. We want our information to:

- be read by only the right people (confidentiality)
- only be changed by authorised people or processes (integrity)
- be available to read and use whenever we want (availability).

3.1 Threats to your assets

As you have already seen, for many the threats are most likely to arrive as emails or attached to emails. Another significant threat comes from apps for mobile devices that are not what they seem. In 2019, Sophos reported apps that hide their icons and use other tricks to prevent the user uninstalling them while aggressively displaying advertising.

Other examples reported include:

- Many utility apps don't initially contain malware but include the code to download and install malware from elsewhere. This extra code installed may be designed to collect your banking details, or lock you out of your phone until you pay the criminals.
- A VPN client that installs a trojan designed to capture banking details.

- Fleeceware – apps that pretend to offer a free trial for some simple function and ask you to provide banking details first. Even after uninstalling the app, users still get charged a large amount unless they explicitly cancel the trial.

You can find up to date Sophos reports at:
https://news.sophos.com/en-us/tag/android-malware/

For the final activity this week you'll update your own list of cyber threats.

Activity 5 Your threats

Allow about 5 minutes

Update the list of information assets and online activities you compiled in Taking stock of your information assets. Add any threats that are relevant to your assets.

Save this list to use later in the course.

Next, you have a chance to review your learning in the end-of-week practice test.

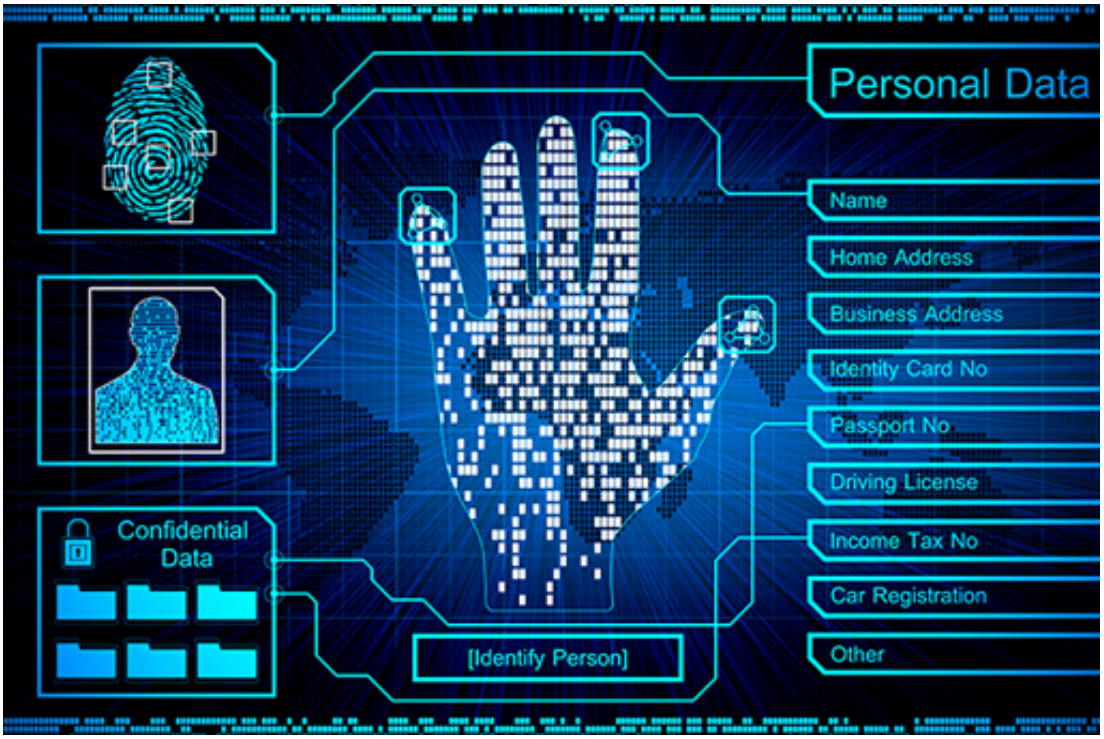


Figure 11

4 Week 1 quiz

This quiz allows you to test and apply your knowledge of the material in Week 1.

Complete the Week 1 practice quiz now.

Open the quiz in a new window or tab then come back here when you're done.

5 Summary of Week 1

Figure 12

This week you explored the security threats that could affect your digital information and use of online services.

You also learned how to keep your knowledge of these threats up to date and started looking at how these threats relate to your own information assets and online activities. In the coming weeks you will explore the different ways in which these threats can become attacks.

You have also learned about the wider world of cyber security and how attacks can affect a variety of systems. As we enter into an age where most everyday devices are connected to the internet – the 'Internet of Things' – we will have to deal with a growing range of threats and cyber security will be increasingly important.

There is some optional further reading relating to cyber security in a business setting in the further reading section.

You can now go to Week 2: Authentication.

Further reading

Microsoft Security Response Centre

Microsoft – Turning automatic updates on or off

Apple Product Security

Cyber Governance Health Check: the annual FTSE 350 Cyber Governance Health Check assesses and reports on cyber security risk management in the UK's 350 largest firms (the "FTSE 350".)

National Cyber Security Centre – Threat Listing

National Cyber Security Centre – The cyber threat to UK business 2017-2018 report

Week 2: Authentication

Introduction

Video content is not available in this format.

Cory introduces you to Week 2 of the course.

Last week you explored the security threats that could affect your ability to stay secure online. You also learned how to keep your knowledge of these threats up to date.

This week you'll learn about the purpose of passwords and the different situations in which they are used, the ways in which attackers try to learn your password so they can impersonate you online and ways of improving the security of your passwords and online identification methods.

Important warning: This week, you will be asked to discuss different aspects of password security. It is critical that you never share your actual passwords and only discuss the general principles. If you need an example, please make one up rather than give an actual password!

1 Passwords: what are they for?

Figure 1

Millions of people use online services every day, and it is crucial that these systems prevent users from accessing each other's information. To do this, they need a way of uniquely identifying each user that prevents users from impersonating each other. This is called identification and authentication.

Passwords and passcodes are the most common way of authenticating users. Examples of their use includes the PIN (Personal Identifier Number) you use with your credit and debit card as well as the many passwords you are expected to remember when logging in to computer-based services.

An ideal password must satisfy two conflicting aims. It should be:

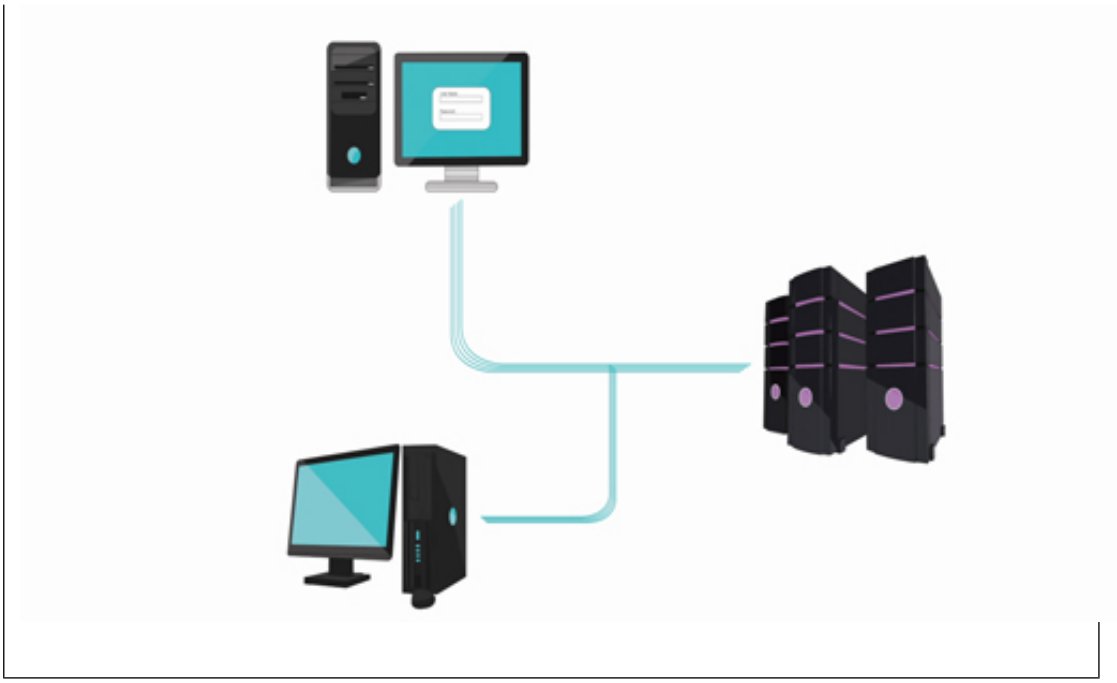
1. memorable enough that the user can recall it without writing it down
2. long enough and unique enough that no one else can guess it.

As you've almost certainly found out, remembering passwords is hard and it can be even harder to think of one that is secure. For these reasons many services are thinking about replacing passwords – we will return to this later.

First, let's think about how passwords are used and the different ways attackers try to learn our password.

1.1 What happens when you enter a password?

Video content is not available in this format.



If the password is *transmitted* from the user to the server as **plaintext** (what you see is exactly what you get; it isn't hidden in any way) – it could be intercepted as it travels across the network.

This is usually overcome by encrypting the communication between the user and the server. The most common form of encryption is the Transport Layer Security (TLS) standard or the older SSL standard (Secure Socket Layer). You'll recognise that TLS or **SSL** is being used when you see 'https' at the beginning of a web page address instead of 'http', and by a padlock symbol in your browser. (You'll look at encryption and TLS and SSL more fully in Week 4.)

Another problem occurs if a password is stored on a server as plaintext. In this case a successful attack on the server would not only reveal the user's password, but all the passwords for all the users of the system. However, when a user enters a password the server needs to be able to confirm that this is the correct password for that user before it grants access.

This second problem can also be solved using a technique called hashing. A hash with salt is the result of processing plaintext to create a unique, fixed length identifier – you'll find out more in Week 5. It cannot be used to reconstruct the original data – even if the hash falls into hostile hands. In this scheme, a hashing function is used to create a hash of a password, which is stored on the server – the password itself is discarded. When the user enters a password, this is sent over the network and hashed on the server using a copy of the same hashing function. The resulting hash is compared to the hash stored on the password server. Only if they match will the user be granted access. Some implementations of this scheme will hash the user's password before sending it across the network to be compared with the hash stored on the server.

Almost all online services and computer systems store passwords as hashes – but surprisingly, errors still happen. The problems described in the following case study could have been avoided if hashing had been used.

Case study: RockYou

The game and advertising company RockYou suffered a major security breach in 2009 when 32 million user accounts were compromised, revealing that not only did the company store passwords in plaintext, it encouraged insecure passwords by only requiring them to be five alphanumeric characters long.

RockYou's problems were made worse when it became clear that they had known that their database was vulnerable to an attack for more than ten years. The company had previously been criticised on privacy grounds for sending emails containing complete lists of their advertising partners, and for poor security in issuing passwords through insecure email.

Over the years many billions of accounts have been breached and the data collected by criminals. These criminals then try the same user name and password on other accounts. If you have reused the same password then they may take over your account.

In 2016, a list of 593 million unique email addresses together with multiple passwords for each address was being circulated by criminals. This list was known as 'Exploit.In'

You can check to see if your own email has been part of a data breach by visiting https://haveibeenpwned.com/. Later this week you will look at how to improve your password security.

Even when hashing and encrypted communications are used, there are still ways in which attackers can successfully learn your password.

1.2 Attacking passwords

Figure 2

The obvious ways that attackers can find or steal passwords, such as looking over your shoulder when you're using an ATM or credit card machine or trying obvious passwords such as 'abc123' and 'password', are familiar to us.

Almost as long as there have been passwords there have been people attempting to break passwords. One of the oldest methods of automatically breaking into computers is to perform a **dictionary attack**. As its name suggests, a computer will attempt to log into an account by working its way through one or more dictionaries – each entry in the dictionary is one possible password and if it doesn't work, the computer moves on to the next.

Dictionaries need not be the familiar A–Z references that we are familiar with: a concerted dictionary attack will also include more specialised reference works such as atlases, lists of astronomical bodies and characters from literature, as well as lists of the most commonly used passwords and lists of stolen passwords that are in widespread circulation.

Dictionary attacks can also be performed on the hashed values of words; they may take a little longer, but they will work. Some system administrators might set up dictionary attacks on their own users' passwords to try to identify weak passwords that should be changed.

An alternative, simple attack is a **brute force attack** where a computer will methodically work through all possible passwords (so beginning with 'A', then 'AA', 'AB' and so on …) trying each in turn until it stumbles upon an actual password.

Dictionary and brute force attacks can be foiled by having computers watch for unsuccessful attempts to log in to accounts. Almost all computer systems restrict the number of unsuccessful logins after which the account is locked and can only be accessed after the intervention of an administrator.

Another type of attack on passwords is based on the incorrect configuration of the hashing technique used to store the passwords on the server, which is discussed in the next section.

1.3 Salt to protect

Figure 3

The security of stored passwords can be increased by a process known as salting – in which a random value (called the salt) is added to the plaintext password before the hashing process.

This greatly increases the number of possible hash values for the password and means that even if two people choose identical passwords, their hashed passwords have completely different values.

The hashed password and the relevant salt are stored by the password server. When the user attempts to log in to the computer, their password and the salt are added together, hashed and compared to the stored, hashed value.

Salting is only effective if:

- truly random salts are used for each password (some systems have either used a single salt for all passwords, or have only changed the salt when the computer is restarted)
- the salt is long enough that, when added to a password, it will create enough possible hashed values that an attacker cannot generate a table containing all possible hashes from a salted dictionary. For instance, the passwords used by UNIX in the early 1970s were restricted to eight characters and used a 12-bit salt. When released this was secure enough – it was not feasible to generate the hashes for every possible password each of which had been salted with all 4,096 possible salts. However, the rapid advance in computer power and storage capacity meant that longer salts are required. A typical piece of advice is that the salt should be the same length as the output of the hashing function – so if your hashing function generates 256-bit hashes, a different 256-bit unique salt should be used for each password.

Case study: LinkedIn

In the middle of 2012, the hugely successful social networking site LinkedIn was attacked by Russian hackers. The passwords to some 6.5 million accounts were stolen, but although they were stored as hashed values, the passwords had not been salted.

The hashing had been performed using the relatively old SHA-1 hashing algorithm which can be performed at very high speed (a desktop computer can calculate several tens of millions of SHA-1 hashes per second).

It was therefore not surprising that within a day, decrypted passwords were being published on the internet and LinkedIn was forced to ask all users to change their passwords.

Preventing the attacks described above depends on the online service taking steps to encrypt the transmission and storage of passwords. As users, we can help in this protection by choosing passwords that are difficult to attack.

2 Improving password security

Figure 4

Just about every website you sign up to requires a password. What strategies do you use when choosing passwords?

If your passwords are easily guessable, you are effectively giving attackers easy access to your accounts. If your passwords are along the lines of ‘password’, ‘123’ or ‘letmein’, they won’t even need to use their automatic password-breaking tools. This is especially true when people don’t change the default passwords that are used to control access to the settings of certain pieces of equipment such as broadband routers.

Think about your strategies for picking memorable passwords. Consider these questions:

- How many passwords do you use?
- How long are the passwords you use?
- Do you use upper and lower case letters, numbers, other symbols in them?

2.1 How to pick a proper password

Video content is not available in this format.

Using your pet's name, your street's name or a random word can be easy to remember, but can also be easy to guess.

Even if the website uses hash functions, if the passwords are single dictionary words, the attacker can generate lots of possible passwords, hash them and see whether any of them match a stored one. Attackers always start with dictionary words and variations thereof, as most passwords are normal words.

So your accounts will be more secure using long passwords made up of a collection of numbers, letters and symbols that don't resemble a dictionary word. One way of coming up with such passwords is first to choose a memorable phrase and convert it in the way described in the video above.

Strong passwords – long strings of characters that don't appear in any dictionary, or at least five separate non-related words that are not easily guessable – are vital. The other thing to remember is to use a different password for every account.

The majority of cases in which someone's password has been compromised have occurred when an attacker has cracked someone's password on a low-value, low-security site, and that user used the same password for another, higher-value site. The attacker either knows or guesses the target's username on the higher-value site and then tries the cracked password on it.

For more advice about how to choose strong passwords read the Good password checklist. It might be useful to print off and keep this.

Good password checklist

- Don't use simple, short, easy to guess passwords such as names of friends, family and pets. Don't use words from the dictionary or commonly used passwords such as 12345 or QWERTY.
- Don't use substitute characters such as pa22w0rd
- Don't use the same password on more than one website

- Do use long passwords that are a random mix of upper case, lower case, numbers and other characters, such as giYT%$54vcD3W
- For memorable passwords do use a string of at least five unrelated disctionary words such as bamboo glasses book engine red
- Don’t share passwords with other people. If they need access to data they should be given their own login.
- Don’t leave passwords lying around in notebooks, or on sticky notes close to your computer, or in files on your computer where they can easily be read.
- Before you enter a password into a website, make sure it is using a secure connection beginning with https:// (it might also show a small padlock close to the address) this means the site is using a secure link that cannot be intercepted by attackers.
- When you register with some online services they will send you a password so that you can log in. Many sites force you to change the password when you first log in, if they don’t, change it when you first visit the site.
- If possible, change the default password on devices such as your internet router. This is programmed at the factory and some companies have a single password for all their devices. An attacker only needs to know the make of your router to gain access.
- If you have trouble remembering passwords try a password manager program that not only stores passwords, but can generate new, highly complex passwords for you.
- Two-factor authentication gives you additional protection as it requires two pieces of information (such as a password and a random number sent by SMS) to provide access to your data. If a company offers two-factor authentication, you should use it.

In the next section you’ll get to test the strength of your passwords.

2.2 Checking the strength of a password

Figure 5

So you've learned to pick strong passwords that are easier to remember, to use different passwords for different organisations and to change them periodically.

When you create a new password you will sometimes see an indication of how weak or strong a password is. There are also apps that can help us to create and manage our passwords. We will look at these a little bit later, but let us start by getting some understanding of how to measure the strength of a password.

Construct an example password using the place name of the city, town or village where you live using only lower case letters – no capitals, spaces, dashes, and so on.

Test it using the password strength checker on the OpenLearn site and make a note of the score. Open the link in a new window so that you can refer back to it as you continue with this section. If you live in a place with a short name such as Ayr, just repeat the name a few times until you have met the minimum length requirement for the password checker.

Modify it into a very strong password using the technique for converting a phrase into a password that you learned earlier.

Think about why the security of the two passwords was different and what makes a very strong password. Things to consider include:

- password length
- the range of characters you used
- whether any personal information is recognisable in your passwords (and could be guessed)
- how easy or difficult it is for you to remember the new password.

2.3 Password managers

Figure 6

While it is possible to create your own strong passwords, it can sometimes be difficult to remember each one, especially if you use a number of online services.

A password manager is an application running on your computer that stores passwords for you. Very simple password managers allow stored passwords to be copied and pasted into login boxes. More sophisticated managers let users launch and log in to an application or website by clicking on their entry in the manager itself, while some password managers include browser 'plug-ins' so that you can complete a login on a web page simply by pressing a button.

The majority of password managers also offer password generation facilities. Since computers can remember arbitrarily long pieces of nonsense text, say MHpKQCvpYoouTAaPiiWuFKjpNe7qnsbwkrvq3s3cX, password managers have no problems with creating passwords that are highly resistant to both brute force and dictionary attacks. Since a password manager contains a great deal of extremely valuable information it represents an attractive target for an attacker. Before choosing a manager you should check that:

- The password manager itself requires a password to use it. This prevents an attacker simply starting the password manager and accessing your passwords.
- The password manager should lock itself after a period of inactivity. This stops an attacker accessing the passwords if you have previously used the password manager and then left your machine unattended.
- The passwords themselves should be encrypted on your computer. This prevents an attacker reading your passwords without needing to open the password manager.

Most modern web browsers offer to remember passwords when you enter them into web forms, providing password management for websites you visit using the browser. This can be very convenient for frequently visited sites where you regularly have to enter details. The security of this password storage is strong and your data will not be visible to casual inspection, but you should be **extremely** careful using them on any computer that you do not own or have sole control of, since your data will be stored on the machine and could be misused by another user or an administrator.

You should only consider using a browser's password storage on a machine that you are the sole user of, or one where you entirely trust the other users. Under no circumstances should you store passwords in the browsers of public machines in places such as cafes, libraries and workplaces.

When using a password manager check that the password manager's security functionality has been evaluated by a reputable independent organisation that has the ability to understand and test how such software works. For example, https://www.av-test.org/en/news/secure-passwords-its-a-snap/. Additionally, make sure you select a very strong password for controlling access to the password store. This will minimise the risk of attackers having access to your passwords, even if they do manage to steal the encrypted password store, either from your machine or from online storage provided by the password manager software.

Password managers are a prime target for hackers, and occasionally hackers have managed to find ways of attacking them. It is important that such software is always kept up to date.

2.4 Installing and using a password manager

Figure 7

Alternatives to a browser's password management are dedicated password management applications.

Before choosing any product to manage your passwords, you should make sure that it meets your requirements – in particular:

- Is the software available for your computer?
- Does it manage passwords on one machine or more than one computer?
- Can it synchronise passwords between multiple machines?
- Does it have a good reputation?

Check that the password manager software has a good reputation by making sure that it has been evaluated by a reputable organisation such as av-test.org : https://www.av-test.org/en/news/secure-passwords-its-a-snap/. Don't depend on anecdotal evidence.

When you evaluate using a password manager consider the balance of risk. A password manager only requires you to memorise a single secure password. All the other passwords it looks after can be long, unique strings of random characters, for example, dyet%eb5YT%^ahyrp)(nd. This is much more secure than using a paper notebook – thieves breaking into a house or office look for password notebooks. Notebooks also get dropped or left on the train!

Some examples of password manager applications are:

- LastPass is available for a range of operating systems, including mobile devices. It can generate and store passwords, and manage them across multiple devices.
- 1Password is available for Windows and Mac computers as well as mobile devices running iOS, Android and Windows Phone. As well as generating and storing passwords, 1Password can be used to hold other confidential documents. It offers password synchronisation through the free Dropbox cloud service where encrypted copies of all 1Password data are shared between your machines.
- KeePass is available for Windows, Mac and Linux operating systems. It is an open source password manager, which makes it easier for security experts to check its program code and identify potential security problems.

The protection offered by a password manager is only as good as the password you select to control access to it – the 'master password'. Therefore, make sure to select a long, hard to guess password – ideally a phrase or combination of random words. This will prevent attackers from getting access to all of your passwords, even if they steal the password store from your machine or an online password system. For example, in June 2015 attackers were able to steal a large number of password stores from LastPass, putting those users with very weak master passwords at risk of having all their passwords used by hackers.

In September 2019, another vulnerability was discovered in LastPass by a Google Project Zero researcher. This was fixed almost immediately by LastPass in an update.

2.5 Alternatives to using password managers

Figure 8

Using a password manager makes your life much simpler because, rather than having to remember a multitude of passwords, you only need to remember a single password and the computer does the rest.

But what if you forget that password? All of a sudden all of your passwords are unavailable. And what if your password manager's data file falls into the wrong hands? You'd better hope your password is strong, otherwise all of your passwords are accessible to an attacker. But, what are the alternatives?

For an increasing number of websites it is possible to use your existing online accounts, such those provided by Google or Facebook, to register and log in. This approach for managing users' account details depends on an authentication mechanism called OAuth (i.e. Open Authentication).

This method of checking a user's identity requires the website to ask the user's computer for some proof that the user's identity has been authenticated by the OAuth provider (e.g., Google). This requires the user's computer to first contact the OAuth provider where the user can input their username and password. The OAuth provider provides a digitally signed token that confirms the user's identity.

You will learn more about digital signatures in Week 5 of the course, but for now it is sufficient to understand that in this case the digitally signed token cannot be created or modified by anyone other than the OAuth provider. Once it receives the token all the website needs to do is to check that the signature on this token is valid to confirm the identify of the user.

So using OAuth can simplify your password management because all you need to remember is the username and password for your account with the OAuth provider. However, just as with password managers, if you forget this password you will no longer

have access to any of the accounts. Additionally, if an attacker gets access to this password, they will be able to access all the online systems you are able to access using your OAuth account details.

So while password managers and online authentication services like OAuth can simplify the management of your online accounts, they are not complete solutions.

Often an account will ask you for other information such as date of birth, or for memorable information or answers to security questions. For official websites such as government sites, banking, or airline sites the date of birth needs to be accurate. But for most other sites you can make up your memorable security information so that these cannot be worked out from your social media pages, and the answers could be unique for each website, e.g. Mothers name, first school, favourite pet would be different every time. To keep track of all this information you could use a spreadsheet. To keep this spreadsheet secure the spreadsheet should be stored inside an encrypted folder . For this you could use VeraCrypt: https://www.veracrypt.fr/en/Home.html. Then, you only need to remember a single very strong password for the secure folder.

Next, you will look at another way of improving the security of the authentication mechanisms you use.

3 Two-factor authentication

Figure 9

So, if a password isn't secure enough, perhaps having two pieces of information is more secure? This is known as two-factor authentication and you've almost certainly used it without realising.

When you take money out of an ATM you have to give the bank two pieces of information – the first is the data stored on your bank card, the second is the PIN. Individually, neither can access your account, but when brought together they allow you to withdraw money.

Some banks have given similar two-factor authentication to online banking customers – in this case accounts need to be unlocked with the combination of a password and a four or six digit number generated on a hardware banking card reader. If you use online banking and don't have a card reader device it will be well worth finding out if your bank offers them to customers, and if they do not, consider switching to a more secure banking service.

Banking card reader

The banking card reader reads the account details from your bank debit card, which includes your account number and a hash of your pin. It will also require you to enter a pin to log in, and if the pin matches the hashed pin this reader can generate passcodes that can be used on the banks website to authorise log in and for certain transactions. The banking card reader confirms that you both have the card and know the pin, without the need to enter a pin on a web page.

Two-factor authentication on the web

A number of companies, including Apple, eBay, Google and Microsoft support two-factor authentication (2fa) to improve the security for their web users. Rather than a single password, two-factor authentication requires the user to enter two pieces of information – their password and a changing value which is either sent by the website to their mobile phone, or generated by a companion application on the user's own computer.

Depending on the site, it might be necessary to enter the two values every time (which is inconvenient), or after a period of inactivity, or it may be possible to tell the site that the computer which has already been authenticated should be trusted in future and a single password will be sufficient to allow you to use the site (although this raises a security weakness if the machine should be stolen).

This method of two-factor authentication works well as protection against random attacks. However, if you are being specifically targeted by the attacker, the attackers have found it quite easy to take over the user's phone number and then intercept authentication messages. They don't need to steal the phone to do this. Criminals can locate the telephone number and date of birth on social media, and then ask for the number to be transferred to a new sim with a new provider.

One way to greatly reduce this risk is to use a dual sim phone with a number on a pay-as-you-go tariff where the balance remains indefinitely – you usually have to make one call every 6 months to keep the sim working. Only use that number for two-factor authentication, not for anything else and never publish that number.

Alternatively, use a separate very basic phone or an old phone with a new pay-as-you-go sim purely for authentication. Switch it on only when you want to get an authentication. Don't used the phone for making phone calls. Don't publish the number anywhere.

If your phone number stops working contact your phone provider immediately to check why. It might have been diverted.

A much more secure method of two-factor authentication is to use a special hardware security key on the computer instead of the phone. This restricts authentication to the computer with a unique hardware security key.

Another place where you might have come across two-factor authentication is if you've ever connected to a virtual private network (VPN), which is a type of encrypted network connection. (You will cover VPNs in more detail in Week 5.)

The organisation that owns the network you are connecting to will give you a card or device, often called a VPN token, that can be used to generate a sequence of random characters. When you try to connect to the VPN, you will first be asked for your password (the secret based on something you know) and then will be challenged to provide some information from the VPN token (the secret based on something you have).

3.1 Setting up two-factor authentication

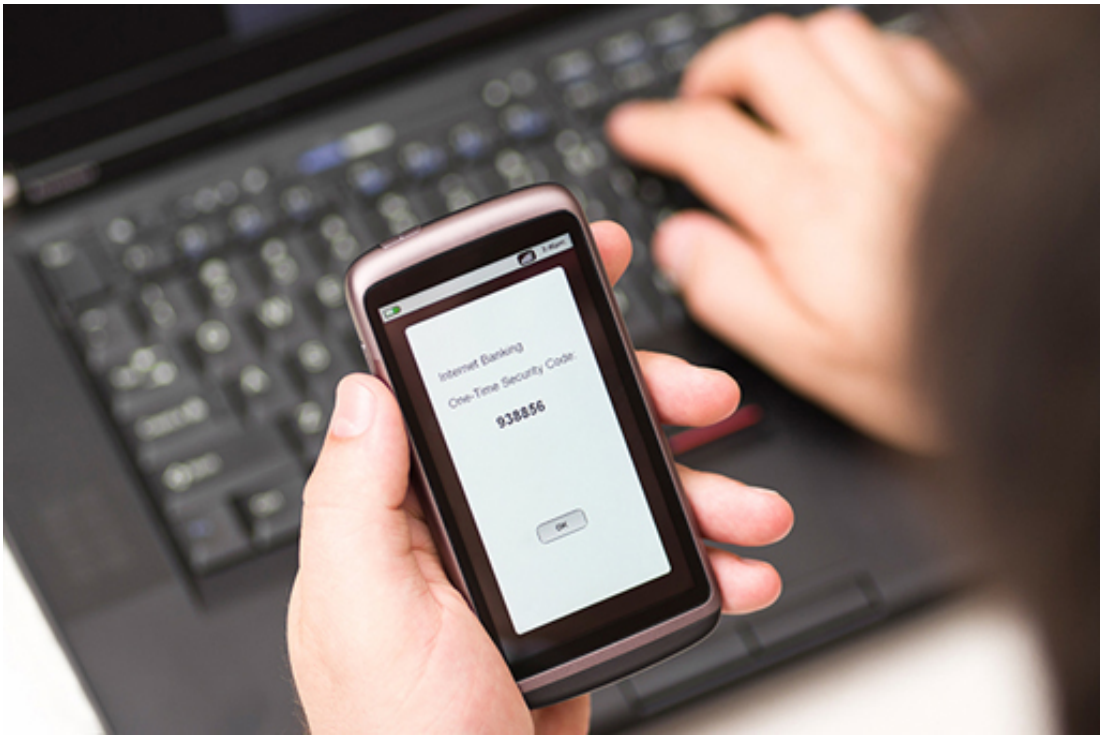


Figure 10

Two-factor authentication is available on many websites such as Google and Facebook and it's very easy to set up. Follow the instructions below to add two-factor authentication to your accounts.

You should make sure that you check how you would log in if you didn't have access to your phone or phone signal, or you lost your phone or had it stolen.

Two-factor authentication on Google

If you have a Google account it is a good idea to set up two-factor authentication.

Google's two-factor authentication sends authentication codes to your mobile phone. You will need a phone that only you have access to, as otherwise someone who has stolen your details could use it to gain access to your Google account.

You can find out more at Google's 2-Step page and follow the instructions there to set it up.

Two-factor authentication on Facebook

Facebook also supports two-factor authentication (which it calls Log in Approvals). Facebook's two-factor authentication process is activated whenever you log in from a new computer. An SMS is sent to your phone containing a unique security code, which you will need to enter into Facebook before you can log in.

Set it up using following the instructions on
https://www.facebook.com/help/148233965247823/

Other two-factor authentication services

As well as many online banking systems, other websites support two-factor authentication, most of which rely on SMS messages. Services include:

- **Apple**
- **Dropbox** – a cloud file sharing service
- **Evernote** – a cloud-based document and note taking service
- **Microsoft Accounts** – used by the Microsoft App Store and its OneDrive cloud storage service
- **PayPal** – online payments used by many small web retailers and eBay
- **Steam** – online game delivery
- **Twitter**

Look out for two-factor authentication on other websites. Set it up to better secure access to your data.

3.2 Other services supporting two-factor authentication

Figure 11

You may be surprised at the range of services and products that provide two-factor authentication. You'll consider these in the next activity.

Activity 1 Two-factor authentication

Allow about 15 minutes

Consider the questions below and see what you can find out.

- Does your bank or credit card company use two-factor authentication, either online or via telephone banking? If so, what form does it take?
- What kind of two-factor authentication is used by shops that you use, either online or in the high street?
- Can you find examples connected with your work, for example to access the company VPN or different areas of the building?

Write a short comment about the type of methods and devices you came across that offer two-factor authentication in the space below. Then discuss the questions with colleagues and add to your notes any other methods and devices you have learned about.

Provide your answer...

Next, you will have an opportunity to review your learning in the end-of-week practice test.

4 Week 2 quiz

This quiz allows you to test and apply your knowledge of the material in Week 2.

Complete the Week 2 practice quiz now.

Open the quiz in a new window or tab then come back here when you're done.

5 Summary of Week 2

Figure 12

This week you explored how authentication works and the role of passwords in the operation of authentication mechanisms.

You learned how weak passwords could threaten the security of digital information and your online identity. You also learned about different ways of improving your password security, including techniques for coming up with strong passwords, using password managers and two-factor authentication.

Of course attacking passwords are not the only way that attackers can gain access to systems. They can also exploit vulnerabilities in software, making it important that you keep systems up to date with the latest security fixes/patches. Attackers might also try to execute malicious software, 'malware', on your systems. These topics will be covered in the week ahead.

You can now go to Week 3: Malware.

Further reading

An article by The Verge on hardware security keys:
https://www.theverge.com/2019/2/22/18235173/the-best-hardware-security-keys-yubico-titan-key-u2f

Fido Alliance administers and develops standards for hardware security keys:
https://fidoalliance.org/

Week 3: Malware

Introduction

Video content is not available in this format.

The two biggest threats to consumers online are malware and phishing. Cory introduces you to malware, which is the focus of this week.

Malware is the collective name for software that has been designed to disrupt or damage data, software or hardware. There are several types of malware, such as viruses, worms and Trojans, which you'll learn more about in the next few sections.

However, as malware has evolved from its beginnings as demonstrations of prowess by individual programmers to sophisticated technologies developed by organised crime, the boundaries between the different categories are beginning to blur.

1 Viruses

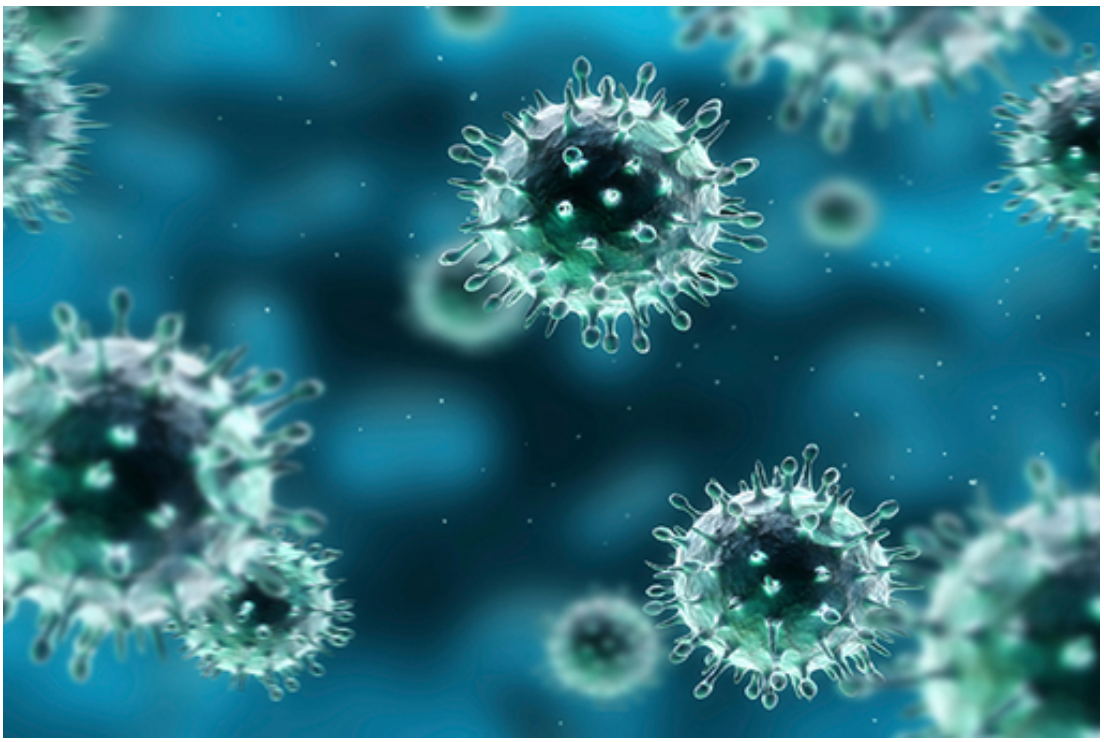


Figure 1

The best-known type of malware is probably the virus; although many pieces of malware are called viruses, they are nothing of the sort.

A virus is a piece of software that has been written to insert copies of itself into applications and data and onto crucial parts of a computer's data storage systems (e.g. hard disks, memory sticks, etc.). Viruses are said to be self-replicating programs and date back as far as the early 1970s, but they only became well known with the advent of microcomputers and later, the internet.

Viruses attach themselves to specific applications on a computer and are activated when the program is first run. At that point, the virus may make a copy of itself on the hard disk and continue to run, or it may only run each time the application is used. Early viruses, relying on floppy disks for transmission, spread quickly as infected data disks were shared around an office, or pirated software was passed around a playground. Nowadays, viruses rely on devices such as flash memory cards or are transmitted through internet connections.

Although some viruses are not intended to cause harm, the majority of these programs are designed to harm users, by corrupting their data or attacking the operating system itself or providing an exploitable 'back door', giving attackers access to the computer. Even where no harm is intended, viruses consume memory, disk space and processing power.

1.1 Worms

Figure 2

Another type of self-replicating malware is the worm; like a virus it is designed to make copies of itself, but unlike a virus, a worm is a standalone application.

Worms spread through network connections, accessing uninfected machines and then hijacking their resources to transmit yet more copies across the network.

There are four stages in a worm attack:

1. The first stage is when the worm probes other machines looking for a vulnerability that can be exploited to copy itself to.
2. The second stage is to penetrate the vulnerable machine by performing the operations for exploiting the vulnerability. For example, the worm might detect an open network connection, through which it can get the remote machine to execute arbitrary instructions.
3. In the third stage, the worm will download itself to the remote machine, and store itself there. This is often called the ‘persist’ stage.
4. In the final stage, the worm will propagate itself by picking new machines to attempt to probe.

Worms were invented as a curiosity and have even been suggested as ways of testing networks or distributing software patches across a network; however their drawbacks far outweigh their benefits. Even the most ‘benign’ worm consumes resources and can affect the performance of a computer system.

1.2 Trojans

Figure 3

The final major type of malware is the Trojan (or Trojan horse) – named after the wooden horse that supposedly smuggled Greek soldiers into the ancient city of Troy.

A Trojan disguises itself as an entirely legitimate program (such as a screensaver), but behind the scenes it is causing damage – perhaps allowing someone else to gain control of the computer, copying personal information, deleting information, monitoring key-strokes, or using email software to pass itself on to other computers. Unlike viruses and worms, Trojans are not self-replicating − they rely on their apparent usefulness to spread between computers.

Some Trojans work in isolation. Some, however, rely on networks, either to transmit stolen information – such as passwords, bank account details or credit card numbers – or to act as back doors to compromised computers. They allow attackers to bypass the operating system's security features and gain access to data or even control the machine over a network.

Trojans have become a serious problem with Android apps.

1.3 Defining terms

Figure 4

In addition to the types of malware described in the previous sections, ‘Adware’, that forces users to view advertising, and ‘Spyware’, malware that attempts to access personal information and user passwords, are other examples you may have heard about.

From the Sophos Threatsaurus PDF downloaded in Week 1 (https://ugc.futurelearn.com/uploads/files/3f/d3/3fd36a66-d941-4595-b587-1a7b41998ae9/Week_3_Sophos_Threatsaurus_AZ.pdf) , look for a term that you have not come across before.

Try to think of a way to define the term in your own words.

You could also look at examples or information from the sources recommended in Week 1, Section 2.2, How to keep up to date.

2 How malware gets into your computer

Figure 5

Malware can get into a computer through a variety of mechanisms, most of which involve exploiting a combination of human and technical factors.

For example, a malware creator might get you to download their malware by putting a link in an email, or attaching the malware to an email. Alternatively, malware might be packaged with illegal copies of standard software so that it can get into the machines of people who choose to use these illegal copies rather than pay for the genuine versions.

However, before looking in detail at how malware gets into your computer, it's worth thinking about why it does. What is malware for?

2.1 What is malware for?

Figure 6

There are many reasons why malware is created including intellectual curiosity, financial gain or corporate espionage.

Many programmers thrive on the challenge of seeing what is possible, and set out to create a malware program even if they do not intend to do harm. Perhaps the most famous of these experiments was the 1988 Morris Worm – the first worm to spread over the internet. The supposed intent of this worm was to gauge the number of machines connected to the network. However, the result was to slow down the operation of infected machines to the point of being unusable.

Worms continue to represent a major threat, as shown by the case of the Conficker Worm of 2008.

Case study: Conficker

In 2008, Microsoft Windows computers began being infected by an advanced worm called Conficker, which spread when users shared files, either over networks or via USB flash memory drives. The malware disabled important security features, such as antivirus software and automated update systems and blocked users from down-loading fixes. At the same time, Conficker would exploit a weakness in Microsoft's server software to infect computers on the same network.

Conficker became the fastest-spreading malware known then, eventually being found in almost every country. Conficker outbreaks were reported from (among others) the armed forces of the UK, France and Germany, as well as the British House of Commons and UK police forces. In the US, Conficker's impact was sufficiently serious that the Department of Homeland Security set up a Conficker Working Group of

security experts tasked with creating strategies that could be used against similar outbreaks in the future.

Conficker's authors were clearly not amateurs. They released new variants of Conficker on a regular basis to overcome weaknesses in the original malware and took steps, (including using digital signatures), to ensure that no one else could hijack their program.

Although Conficker caused a great deal of nuisance, it did not appear to do any actual harm to data, however, the program could have delivered other malware that would have attacked users. In many ways, Conficker was a harbinger of the advanced criminal malware – such as Cryptolocker – that is a major threat to today's users.

A detailed analysis of the development of Conficker and how the source was identified was published by Mark Bowden in the *New York Times* in June 2019: https://www.nytimes.com/2019/06/29/opinion/sunday/conficker-worm-ukraine.html

2.2 Phishing

Figure 7

Phishing is any attempt by attackers to steal valuable information by pretending to be a trustworthy party – a form of social engineering attack.

So, an attacker might impersonate a bank to obtain credit card numbers or bank account details. It gets its name from 'fishing' – as in 'fishing for information', the process of luring people to disclose confidential information.

Phishing relies on people trusting official looking messages, or conversations with apparently authoritative individuals, as being genuine. It is widespread and it can be

enormously costly to people who find their bank accounts emptied, credit references destroyed or lose personal or sensitive information.

Email phishing

The use of electronic technologies to perform phishing attacks was described in the late 1980s, but the term did not become commonplace until the mid 1990s when a program called AOHell allowed AOL users to impersonate other people (including the founder of AOL itself).

Phishing became increasingly common as more and more people connected for the first time and began receiving official looking messages that looked very much like those sent out by genuine organisations such as banks, stores and government departments. What most of these users did not realise was that not only could email addresses be faked, but that electronic data can be easily copied – just because an email claims to come from your bank and has your bank's logo doesn't mean that it is genuine.

Phishing emails may be indiscriminate. A phisher will create an email asking the user to get in touch with a bank or credit card company claiming that there is a problem with the account or that the bank may have lost some money. These sorts of messages make people justifiably worried and more likely to follow the instruction. The phisher will then include some plausible looking details such as the bank's logo and address and then send it to millions of individuals. Among all the recipients, a few people will have accounts with that bank and will click the link in the message, or telephone a number, which will begin the process of eliciting further personal information.

What to do

If you do receive an email that worries you from an organisation such as a bank or shop that you use, do not click on or follow the links in the message. Get in touch with their customer services department, or log in to your account through their website. Type in their web address or use the address in your list of favourite sites, or use their published phone number. Most organisations will have a published policy of not asking for sensitive information such as your password through email or over the phone so you should be suspicious of anything that contravenes this policy.

Social media phishing

Although email still accounts for the majority of phishing attacks, the technique is also used in social media sites as well as in text messages. The same rules apply – if in doubt, go to the official site and make contact with the company through their published links.

As we saw in the first week of the course, phishing can sometimes be targeted at individuals or specific parts of an organisation. These attacks, commonly called a 'spear phishing attack', will depend on detailed information about the target. For example, an attacker might use information gleaned from recent emails to craft a plausible reply that appears to come from colleagues of the targeted user.

Attackers may also include links to malware-infected software in personal messages posted in social media. This is especially common after major disasters or during fast-

breaking news when people are likely to click on interesting looking links without thinking carefully.

2.3 Trapping phishing emails

Figure 8

Phishing is just one type of spam email which clutters our mailboxes and often delivers unsuitable or even illegal content to individuals.

Spam

Spam is yet another consequence of the early internet being developed by people who trusted one another. Just as we have had to protect computer networks against hackers – which you'll cover in Week 6 – as more and more people have accessed the internet, email has become a tool that anyone can use for good or bad.

Most internet email is moved around the world using the Simple Mail Transfer Protocol (SMTP) which defines a standard template of commands and formatting that allow different mail programs, on a huge range of computers, to understand one another. Protocols are used to specify a set of special messages that should be exchanged between computers to achieve a particular functionality, in this case the delivery of email.

SMTP was defined when the internet had only a tiny number of users, so the original specification did not include any way for computers to authenticate one another, i.e. there was no way of knowing if the message claiming to come from TrustedBank actually came from TrustedBank's computers. This weakness was addressed in a later extension to SMTP called SMTP-AUTH, but crucially it was not required, and so almost all mail servers still accept unauthenticated messages.

Spoofing

Spammers can attack a mail system by changing the information stored in email 'envelopes' which enclose the messages themselves. This is known as 'spoofing' and allows a spammer to disguise their actual address by writing new addresses for the sender (such as replacing their own address with that of TrustedBank) and the destination for receipts. Since SMTP servers do not perform any authentication, they simply pass on the email without checking that it was sent out by TrustedBank.

Simple spoofing is now being challenged by technologies that allow genuine senders to authenticate messages which can be checked by the recipient's mail server, however only about half of all mailboxes have any protection against spoofing.

Provided a spammer has access to a fast network (or increasingly to a botnet), spam costs the sender almost nothing and although only a tiny fraction of users will respond to a spam message, sufficiently vast numbers of emails are sent that the rewards far outweigh the costs. It has been estimated that seven TRILLION spam messages, making up more than 85% of all email, were sent during 2011 alone. In 2018, spam was estimated to be down to 55% of all messages. Such is the torrent of spam that internet service providers and companies have to buy far more bandwidth and storage than they will ever need for legitimate purposes.

2.4 Spotting a phishing email

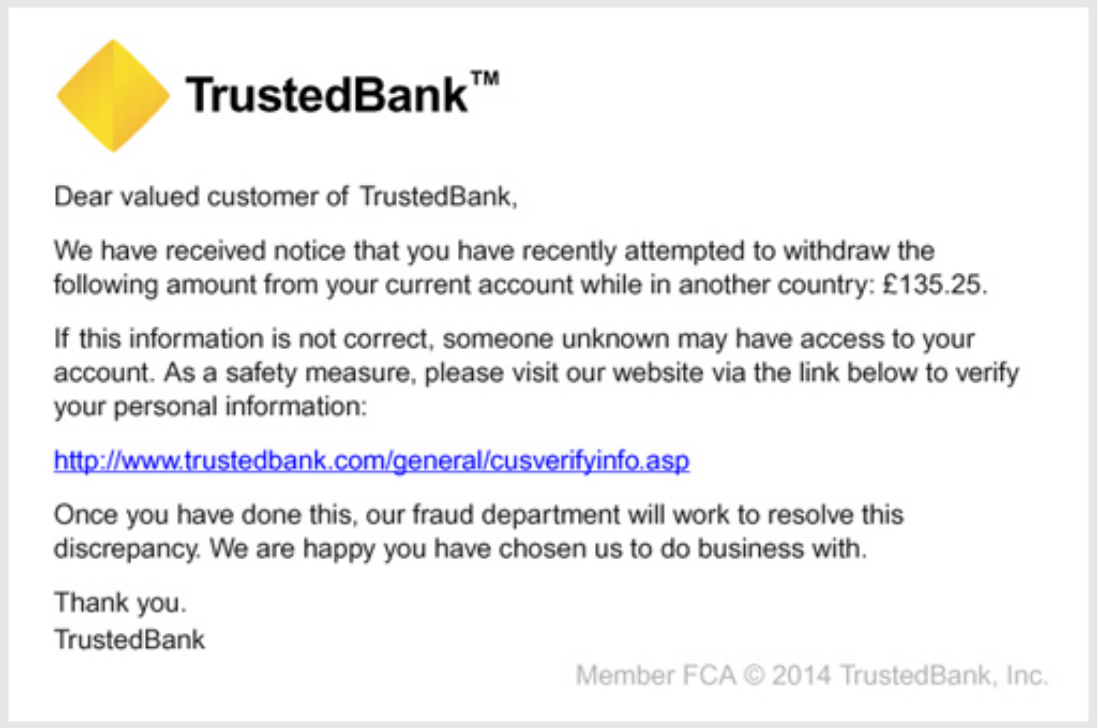


Figure 9

Although a phishing attack may appear plausible at first glance, there are some tell-tale signs that should make you very cautious about clicking on any links or giving any personal information to the supposed sender.

Read through the points below to find out what to look out for.

- **Spelling mistakes**: Most English-language phishing expeditions are sent from countries where English is not the primary language. Attackers often give themselves away by imprecise use of English, even with quite common phrases, and including spelling errors. So read the message carefully. However, there are many phishing emails that use excellent English.
- **Who is it to?** Many, but not all phishing attacks do not use your name in the introduction – preferring 'Dear valued customer,' or 'Dear user,'. This is because they cannot personalise the emails sufficiently. Your bank or online store can do this and should address you as 'Dear Bob,' or 'Dear Mrs Jones,' (or whatever your name is). However, note that because so many millions of user details have been revealed by data breaches it is quite possible for a phishing email to use your personal details.
- **Poor quality images**: Sometimes, the images used in the emails are fuzzy, or your information may appear as an image rather than type. These images have been copied from screens and would not be used by original companies. It is easy to obtain images every bit as good as the originals though, so a high quality image should not persuade you the message is genuine.
- **Content of the email**: In almost all countries, banks and other financial bodies will not email you to tell you about problems with your account. They recognise that email is fundamentally insecure and that personal information should not be sent by email. So, even the method of communication will give you a clue about whether it's

genuine. The email may give a false sense of urgency, claiming that your account is at risk if you do not act quickly. This is not the case.

- **Links**: The text of a web link is not the same as the destination of the link itself – the link might say it is taking you to, for example http://www.trustedbank.com, but in fact it can take you anywhere on the web – including to a phisher's computer impersonating that of a reputable company. You can spot some fake links by hovering your mouse pointer over the link – but do not click the button. The actual destination of the link will appear at the bottom of the window or in a small floating window next to the link. In a phishing email, the link will probably be to an address you aren't familiar with. Other fake links may display a genuine destination when you hover over them, but still take you to a fake website because code in the page intercepts the link and sends your click elsewhere.

The example message below claims to come from a fictional site called ePay and is about unauthorised activity on the account. The link says it goes to ePay's site, but the address is slightly different and is unlikely to be owned by ePay.

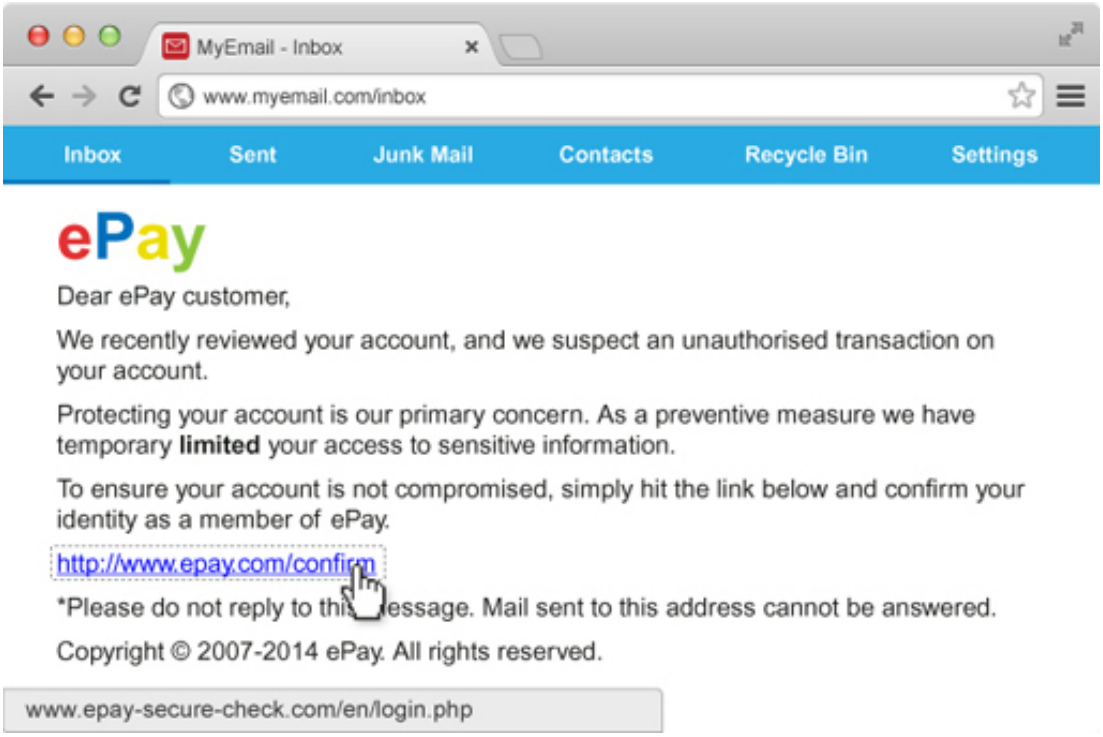


Figure 10 A phishing email claiming to come from the fictional ePay site

So the rules are to be suspicious and to look at the details of the message, the language, the quality of the images and where the links actually take you. Banks and shops will always prefer you to call them and check rather than risking your security.

If you have not already done so recently, check you email address on https://haveibeenpwned.com/. Email addresses that are on a breached list are much more likely to receive spam than those that are not listed. If your email address is on the list you need to assess what related data may have been revealed. You may need to change passwords that use that email address, especially if you have reused the same passwords in the past, or even stop using that email address

2.5 Emails are not the only phish

Figure 11

Please don't think that malware is spread solely through email. Malware will be spread through any means possible.

Malware can be distributed by including it with pirated material such as illegal copies of software, video games and movies. Malware can also be installed on your computer by clicking links on websites – especially sites that distribute illegal copies of software, videos and pornography – or by annoying pop-up windows that claim to have identified problems with your computer (quick tip – they probably haven't! But it's a great prompt to run your antivirus software and remind yourself what a genuine alert looks like on your computer).

A recent trend is for malware to be spread through social networking services, like Cory's experience of the direct message on Twitter that you heard about in Week 1. Once it is on a machine running social networking software, the malware masquerades as the real user and posts messages containing links to sites that distribute yet more malware.

Once again, this type of malware relies on social engineering to multiply – users of social networks are highly likely to click on links they think have come from friends and spread the infection. Most of these social networking infections have exploited weaknesses in client software rather than the web versions of the networks, so it is important to keep social networking client software, such as the Facebook App for mobile devices, up to date.

2.6 The role of malware in click fraud

Figure 12

The majority of modern malware has been designed with malicious intent; to cause damage to a computer's operating system or its data, or to steal information from a user, or increasingly, from online advertisers.

As you will have seen, many large websites rely on advertising for their revenue. The amount of money spent on online advertising is growing rapidly with more than £16 billion spent in the UK alone during 2011. This is expected to exceed £26 billion in 2020. Advertisers like online advertising because it can be relatively cheap compared to a printed advertisement and because software allows for individuals to be targeted with specific adverts for products they are likely to buy.

The most common type of advertising is 'pay per click' where advertisers only pay the owners of a site when a user clicks on an advert. This system can be subverted by either generating clicks that don't come from genuine customers, or by hijacking a click intended for a genuine advertiser. This is known as click fraud, it accounts for more than 20% of all clicks and it can be aided by malware. Computers all around the world, operating as a botnet, can generate false clicks, siphoning money from advertisers through multiple layers of publishers and redistributors to hide its eventual destination.

There are two frequently used modes of click fraud – both can use botnets to generate the clicks.

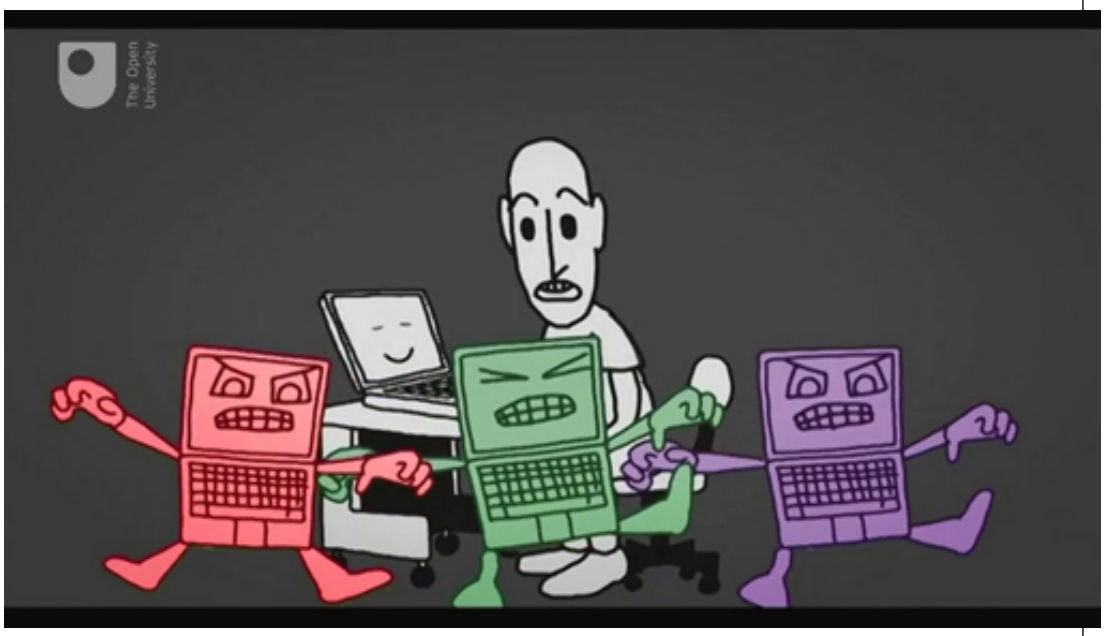
1. Clicking on targeted company ads on genuine sites to waste their advertising revenue. The perpetrator doesn't collect any income.
2. The criminal sets up many hundreds or thousands of websites, often just copying other website content. They sign up for advertising e.g. adsense with google. Then they commission a bot network to click on the ads on their own pages and collect their share of the ad revenue.

While an individual click will only raise a tiny amount of money, done millions of times, click fraud can raise serious amounts of money. In 2011, the FBI broke a click fraud operation based in Estonia that had infected more than four million computers in 100 countries and stolen in excess of $14 million from advertisers.

In 2016, a Russian criminal group created 6,000 websites with over 250,000 pages containing video advertising. Their bot network 'watched' over 300 million video ads each day. They were defrauding the advertisers of close to four million dollars a day.

2.7 Botnets

Video content is not available in this format.



You heard about botnets briefly in Week 1, when we said that botnets are created using malware that give an attacker control over a group of computers and commonly use them to gather information from the computers (e.g., usernames and passwords), launch attacks against others. These attacks might be sending spam emails, or flooding a website with so many requests for content that the server cannot cope, which is known as a denial-of-service attack.

A single piece of malware can cause enormous damage, but when thousands, or even millions of computers run the same program, their effects can be devastating. So a botnet is a group of computers that coordinate their activity over the internet. There are a number of harmless botnets used for such purposes as the Internet Relay Chat (IRC) text messaging program, but the vast majority are created by malware.

Botnets spread through viruses and worms and once installed on the victim's computer they use the internet to make contact with a control computer. At this point, the infected computer (often called a zombie) will do nothing more except periodically check for instructions from the control computer. Over time, more and more computers are recruited to the incipient botnet until it may contain tens of thousands of zombies, but they don't raise suspicion as they appear to be doing nothing.

At some point in the future, the control computer will issue a command for the botnet to wake up and begin doing something. Often the people who created the botnet itself have either sold or rented the botnet to another group who want to use its capabilities.

Botnets have been used to flood the internet with spam messages, to commit fraud against advertisers and to perform so-called distributed denial-of-service attacks on companies and governments. Botnets are so large, and so widely distributed across the internet that they can be very hard to tackle and the effects of a coordinated attack on critical parts of the network can mean even very large websites struggle to remain online while the botnet targets their computers.

2.8 Confessional

Figure 13

It's time to confess! Think about the following:

- Has your computer ever been infected with malware?
- Do you know the name of the malware that was involved?
- Was it a virus, worm or Trojan?
- What happened, and what were the consequences?

If you discuss this with others, remember not to share any personal information including the name of the company you work for.

3 Keeping yourself protected

Figure 14

The growth in malware has been accompanied by an explosive growth in software designed to prevent it spreading.

So-called antivirus software (which actually targets a range of malware) is a multi-billion pound business with a large number of commercial and free packages available for all computer users ranging from individuals to large corporations.

At the same time, the developers of computer operating systems are incorporating a wider range of security features that try to stop malware running at all.

And there is a lot you can do yourself to keep yourself protected such as installing antivirus software, keeping your software up to date, looking out for the signs of phishing emails and implementing new security developments.

Before you install or change anti-malware software you should check the reviews from a number of reputable and independent organisations. Look at how they rate the free packages as well as the paid for packages.

- https://www.av-test.org/en/
- https://selabs.uk/
- https://www.av-comparatives.org/

3.1 Antivirus software

Figure 15

Antivirus software aims to detect, isolate and if necessary, delete malware on a computer before it can harm data. Antivirus software uses several techniques to identify malware – the two most common are known as signatures and heuristics.

Signatures

A malware's signature is a distinctive pattern of data either in memory or in a file. An antivirus program may contain thousands of signatures, but it can only detect malware for which a signature has been identified and published by the antivirus program's authors. As a result there is a period between a new piece of malware being released 'into the wild' and when its signature can be incorporated into antivirus products. During this period, the malware can propagate and attack unprotected systems, exploiting the so-called 'zero day' vulnerabilities that exist until the systems are fixed and antivirus signatures are updated. It is not uncommon for several variants of a malware program to be published at intervals, each sufficiently different that they possess different signatures.

A second weakness of signatures is that more sophisticated malware has the ability to change its program (it is said to be polymorphic or metamorphic), disguising itself without affecting its operation.

Heuristics

Complementing signatures, heuristics use rules to identify viruses based on previous experience of the behaviour of known viruses. Heuristic detection may execute suspicious programs in a virtual machine (a software recreation of a physical computer) and analyse

the program for operations typical of known malware (such as replicating itself or attempting to overwrite key operating system files); or it might revert the program back to its original source code and look for malware-like instructions. If the heuristic analysis considers that the file acts in a malware-like manner, it is flagged as potentially dangerous.

Unlike signatures, heuristics do not require specific knowledge about individual types of malware – they can detect new malware, for which signatures do not exist, simply by their behaviour. The drawback of heuristics is that they can only draw conclusions based on past experience; radically new malware (which appears all too regularly) can pass unnoticed.

Issues with antivirus software

Although antivirus software is an essential part of protecting your computer, it is not a complete solution to malware problems.

Despite the best endeavours of its makers, antivirus software has occasionally proved to contain bugs with consequences like being inaccurate, failing to update itself or simply consuming huge amounts of computer power. Fortunately, these problems are rare, easily fixed and much less serious than the risk from a malware attack.

Note that not all anti-malware software is equally good. There is even fake anti-malware offered for sale, especially for mobile devices.

Check the reviews of anti-malware software by reputable organisations:

- https://www.av-test.org/en/
- https://selabs.uk/
- https://www.av-comparatives.org/

In October 2019, the BBC reported that a combined operation by British Police, Indian police and Microsoft had shut down two Indian call centres using web pages and phone calls to sell fake computer security services. Victims were conned out of thousands of pounds. The City of London Police say it is one of the most common online scams, with over 2,000 cases reported to Action Fraud every month.

The police offered these tips to avoid being scammed:

- Always check out callers, especially cold callers who claim to be Microsoft, your telephony provider or internet service provider.
- Legitimate organisations will encourage you to call back via a number you've obtained from a trustworthy source.
- Do not assume that the number displayed on your phone is accurate, these can be spoofed, leading you to believe that the caller is in the UK or from a trusted organisation.
- Don't call phone numbers on pop-up messages which indicate there is a problem with your computer.

(BBC, 2019)

3.2 Installing antivirus software

Figure 16

If you don't already have antivirus software on your computer, it should be a high priority to install some. Windows 10 has Windows Defender built into the OS and got a top rating in June 2019: https://www.av-test.org/en/antivirus/home-windows/.

There are a number of good, free packages available but you should always check that it meets your needs before installing it. Some important features to consider are:

- **Is it compatible with your computer?** You will have to make sure the antivirus software is appropriate for the operating system and computer that you have.
- **Does it come from a reputable source?** For example, it may have been developed by one of the major computer security companies, such as Norton, Kaspersky, Sophos or AVG. Alternatively, it may have been provided or recommended by your bank or internet service provider.
- **Does it provide updates that allow it to protect you against the latest malware?** New malware is being developed all the time, and it is important that you use an anti-malware application that will update itself.
- **Have you checked the reviews?** Use: https://www.av-test.org/en/, https://selabs.uk/ or https://www.av-comparatives.org/.

Use the above criteria to research antivirus products available so that you can choose the one that is best for you. If you already have an antivirus application, answer the questions for the program you have.

3.3 Keeping your software up to date

Figure 17

Computer operating systems and application programs are so large that they inevitably contain bugs, some of which could compromise your security.

The majority of companies issue regular updates to their programs to fix known problems. Major operating systems and some application packages (such as Microsoft Office and the Adobe productivity suite) automate most of the process of updating software by automatically checking for updates, prompting the user to install them and then actually performing the update itself. This process is sometimes called ‘patching’.

Activity 1 Keeping your software up to date

Allow about 15 minutes

How do you go about keeping one of the software applications on your computer or device up to date? Reseach the application online to find out if there is any additional information about keeping it up to date.

3.4 End-of-life software

Figure 18

Software is continually being developed and replaced by a new version. The lifespan of software begins when it is released and ends when it's no longer supported and updated.

Software doesn't become completely unsafe as soon as it reaches the end of its lifespan; in many cases you can continue to use it, but you should be aware that security risks may not be addressed by its authors. If you work for an employer, you may be required to move to an updated version of the software as part of their security management process.

The first effect you will feel from end-of-life software is that companies will cease telephone and internet support for queries. So if you have problems using a product you won't get any help. The manufacturer may also withdraw bug reporting, so you won't be able to tell them about problems. At the same time you might also find that cheap upgrades to later versions of paid software are no longer available.

Most large software companies will continue to offer critical software support to obsolete products for a period of time. However, they will not prioritise these programs, instead they will concentrate on fixing problems in up to date software and releasing patches; only then testing older products to see if they are affected and if they can be fixed. This means that users of older products might be exposed to vulnerabilities for longer than those using more modern software. Developers of malicious software, who know about unpatched bugs in older products, are likely to attack these older, weaker programs in preference to more secure programs.

In 2019, Windows 10 was used by 55.77% of Windows OS computers. Windows 7 was still used by 33.42% and Windows 8 and XP and older by 10%. Windows 7 loses extended support on 14 January 2020. Windows 8.1 loses extended support on 10 January 2023.

For example, Windows XP is now no longer supported by Microsoft (since April 2014), despite being widely used. Windows XP and Windows Vista, the two oldest operating systems, have much higher incidences of infection than the newer operating systems that feature much greater levels of security.

If you are using end-of-life software, security applications such as up-to-date firewalls and antivirus software are essential as well as keeping up to date with key applications, such as web browsers and email programs which are used to send and receive personal data. Good information security will help keep you safe. Even if you take these precautions, you should begin planning for a transition to more modern applications. Upgrades are relatively cheap from one version to another (or even free), and any expense should be considered in the light of what you stand to lose if you do not use more secure software.

Finally, don't forget that even supported software can be vulnerable if it is not updated regularly. In 2017, the WannaCry ransomware infected thousands of computers globally and it was later determined that most infected systems were running Windows 7, an operating system that was still supported by Microsoft. Indeed, months before the global infection of systems, an update to fix the vulnerability exploited by WannaCry had been released, but many systems had not been updated.

3.5 Sandboxes and code signing

Figure 19

In addition to keeping software up to date and using antivirus products, there are other technological innovations that can help mitigate the threats of malware.

Sandboxes and code signing are examples of some of the technologies that developers are integrating into the software we commonly use to help protect our computers.

Sandboxes

A software sandbox is a way for computers to run programs in a controlled environment. The sandbox offers a constrained amount of memory and only allows very limited access to resources such as operating system files, disks and the network. In theory, the software cannot break out of the sandbox and affect other parts of the computer, so even if malicious software attempts to overwrite parts of the disk, the sandbox will prevent it from doing so.

Sandboxing is widely used in modern web browsers, such as Internet Explorer 10 onwards, and Chrome, to prevent internet content causing damage to files on the computer. Similar sandboxes exist for most browser plugins and the Adobe Acrobat PDF viewer.

Code signing

Code signing is a use of cryptography where software companies issue digitally signed copies of their programs that can be checked by recipients for its authenticity. You'll discover more about digital signatures in Week 4.

Code signing is used by the designers of all three major operating systems (Microsoft Windows, Mac OS and Linux) to guarantee that operating system updates are genuine even if they are distributed using flash memory cards rather than directly from the publisher.

Microsoft Windows uses code signing on operating systems components, such as hardware drivers, which have direct access to the heart of the operating system. Apple has taken code signing even further. Versions of Mac OS from 10.8 onwards can restrict users to only running programs that have been certified by the Apple App Store. While this does offer greater security against malware, it may also restrict choice and prevent users from running certain unsigned apps from third parties.

Next, you have an opportunity to review what you've learned in the end-of-week practice test.

4 Week 3 quiz

This quiz allows you to test and apply your knowledge of the material in Week 3.

Complete the Week 3 practice quiz now.

Open the quiz in a new window or tab then come back here when you're done.

5 Summary of Week 3

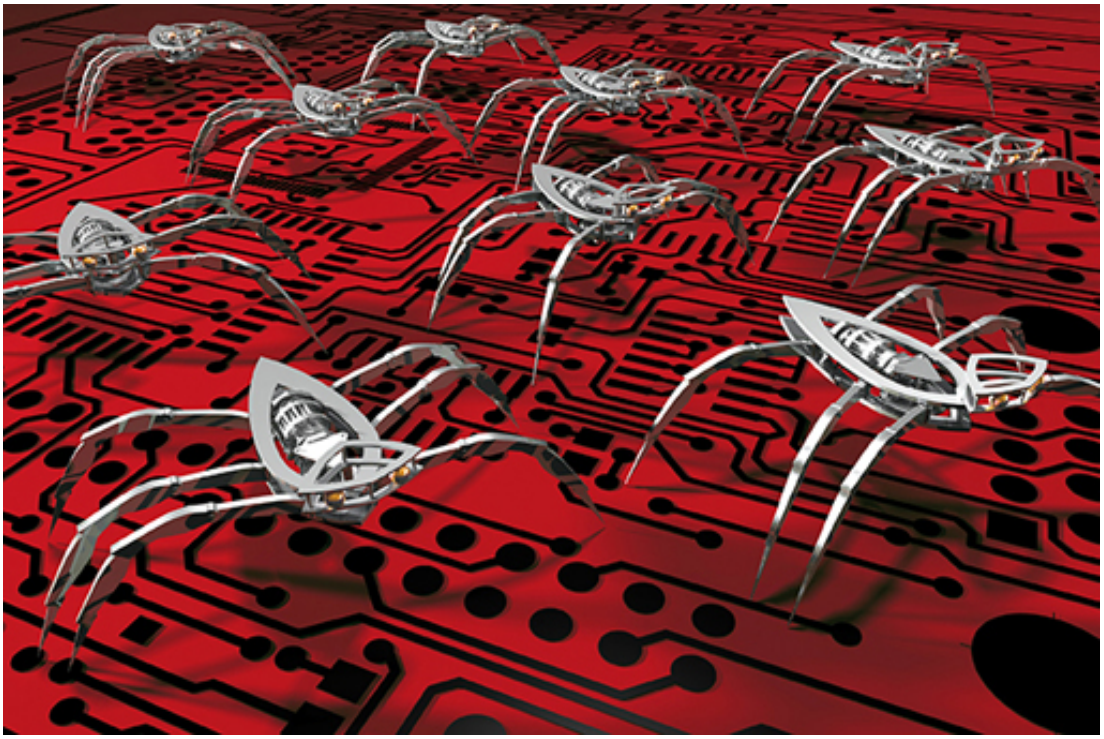


Figure 20

You have also taken a closer look at ways of keeping attackers from impersonating you online or infecting your devices with malware.

In the next part of the course, you will delve a little deeper into the technologies that underpin information security, first focusing on how to protect the networks that we depend on for transmitting our digital information and accessing online services.

There is some optional further reading in the next section relating to some basic precautions you should take before you go online.

You can now go to Week 4: Networking and communications.

Further reading

Keep a clean machine Basic precautions to take before you go online.

Week 4: Networking and communications

Introduction

Video content is not available in this format.

Cory introduces the networking and communications topic.

You'll learn how data is transmitted across the networks, including wireless networks and understand the difference between the internet and the world wide web.

1 What is the internet?

Figure 1

The internet is not a single entity with a single owner; instead it comprises a hierarchy of individual networks that have been connected to one another. These networks range from local area networks (LANs) that can be found in many businesses and universities to the telephone and data networks that link cities and countries by fibre optic cables and satellite links.

A definition often used is that the internet is a network of networks. Before looking at the design of the internet in more detail, let's hear from Vinton Cerf, one of the engineers who was involved in the creation of one of the earliest computer networks:

Audio content is not available in this format.

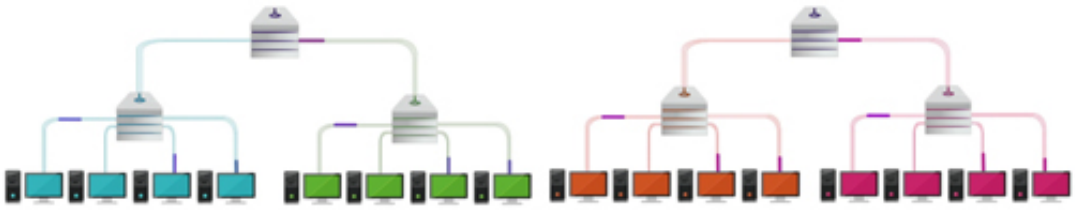
Two key factors in the design of the internet were:

1. The network would not have a central controlling computer. Each computer on the network would be assumed to have the same authority as every other computer.
2. The network should be able to deliver information between any two computers on the network even if some of the machines in the network had failed (or given its Cold War origins, been blown to pieces). There would be a large number of alternative routes through the network, so it was not necessary for information to travel by the most direct route, instead it could travel in a roundabout route, avoiding the damaged parts of the network.

In the next section, you'll see how this works.

1.1 How data moves around the internet

Video content is not available in this format.



The video explains how data is routed across a network of computers and how the internet is resilient to failures of individual computers, known as nodes of the network, or connections between computers, known as the links.

Instead of using a dedicated circuit for all of the information, internet traffic is split up and may take any number of routes through the network moving from its origin to the destination by a series of hops.

Note: Early in the above the video [2:05], an example packet is shown with destination address 6.7.8.104. However, there are subsequently two separate examples of different packets being routed. In the first example, the packet is being sent to a host on the local network, 1.2.3.104 and in the second example it is being sent to a remote host, 6.7.8.101.

1.2 Introducing the datagram

Figure 2

When data, such as a picture, movie or a document is sent over the internet, it is not sent as a single chunk. Instead it is split up into small, uniformly sized blocks called ‘datagrams’, also sometimes called ‘packets’.

Imagine that you have a large book that you want to post to a friend, but you only have small envelopes. One way to post the book is to tear it into a number of pieces, placing each piece in a different envelope. Each envelope is addressed to the recipient. It makes sense to label each envelope with a number to tell your friend where the pages belong in the whole book. When the envelopes are put in the postal system they may all travel through the same sorting offices and arrive on the same day, or they might take different routes and arrive on different days. However, your friend should be able to recreate the book when they receive all the envelopes.

A number of different datagrams are used by data travelling over the internet, but they all have a similar structure. One envelope and its contents correspond to a single datagram. The envelope (which is called the ‘header’) contains the sender and recipient’s addresses, a unique number, a date stamp and some error correction information, while the contents (called the ‘payload’) contains the actual information being delivered.

The address is an IP number that you will look at later in Week 4. You can look up the details of an address by using a ‘whois’ service. For example, you could use the site https://whois.domaintools.com/ and type open.ac.uk into the whois search box.

In the details returned you can see:

IP Address 137.108.200.90

Other details show that the domain belongs to The Open University. The IP location is in Milton Keynes, England, and is hosted on an Apache server.

1.3 Datagrams on the move

We have seen how, in theory, datagrams of information move around the internet. It's actually possible to see this in action, often with surprising results.

Each datagram is sent through a series of computer nodes that form the backbone of the Internet. There are many thousands of these nodes and often many different routes between them. Each of these nodes has an IP address. If you look up the IP address of the node using 'whois', some will provide a geographical location for the node. Some will provide only the country of that node, and some provide no location information.

On most computer systems you can run software that will follow the route from your computer to a destination IP address, and it will return a list of the nodes that it passes through. These are usually known as 'Traceroute' apps. See the wikihow page for information on how to run this Traceroute tool on your computer: https://www.wikihow.com/Traceroute.

Instead of looking up the 'whois' for each node to see where it is located, you can use an online utility that does this looking up for you and plots the results on a map. Open https://peter-thomson.com/leaflet-map-tutorial/traceroute-mapper.html in your browser and paste in the output from running 'Traceroute' on your computer.

Activity 1 Datagrams

Allow about 15 minutes

Spend about 10 minutes exploring the routes to some of the following Australian organisations:

- the University of Sydney
- the Sydney Morning Herald newspaper.

Be warned! You might be surprised at what you find – information is not necessarily coming from where you might expect it to. Also, bear in mind that things change frequently when it comes to the internet; not only might the route be different if you look at the same destination at different times, but even the location where the information comes from might be different.

Nodes increasingly don't provide information – a security precaution. Nodes only identify a country – or the wrong country as they are using factory defaults. The destination might also not be the original server as sites may be cached or served from multiple locations.

Now use the site https://whois.domaintools.com/ to locate the Sydney Morning Herald.

Not where you expected?

The information for usyd.edu.au is less informative, but shows:

IP Location - New South Wales - Sydney - University Of Sydney

Discussion

You will have discovered that the route to the Sydney Morning Herald website did not terminate in Australia.

A URL ending in '.au' is an Australian domain, but that doesn't mean that the computer hosting the site has to be in Australia.

The Australian Domain Name Administrator (auDa) is responsible for licensing users of '.au' names, and it has rules that require the licensees to have some connection with

Australia (that is not the case with all countries; some authorities allow anyone to license their names). However, where the website is hosted – which computer the website is stored on – is a different question from who is using the URL. For example, Google (based in the USA) offers a service hosting websites (Google Sites). It's possible to use a service with a '.eu' (European) domain name, with the result that the '.eu' site is in the USA.

You can look up the details of an address by using a 'whois' service. For example, you could use the site https://whois.domaintools.com/ and type innovations.ac.uk into the whois search box. Note that this domain is also associated with The Open University.

In addition, websites that receive heavy usage from a particular location might be cached locally – that is to say, copies of the website's data might be temporarily stored on a computer closer to the location from which the information is being accessed. This saves making heavy use of long-distance connections.

How many stages did your information take? Did anything surprise you about the route your information took?

Use Trace Route and 'whois' to look up the location of other website domains that you use.

1.4 Wireless networks

Figure 4

Early computer networks depended on wires to move their data around the world, but engineers quickly realised that it would be useful to be able to use wireless (radio) connections to create a local wireless network.

Nowadays, wireless local area networks are commonplace. These wireless local networks have become known as Wi-Fi after the trademark of the Wi-Fi Alliance that certifies compatible products. If you have a laptop, tablet or smartphone, it probably has wi-fi access. Wi-fi is also being incorporated into an ever wider range of consumer goods including eBook readers, smart televisions, burglar and smoke alarms.

Wi-fi enables devices such as computers and printers to be connected together wirelessly to form a local area network (LAN). Instead of the signals going through cables and wires, they are sent through the air instead as radio waves.

The name ‘wi-fi’ refers in particular to wireless local area networking technology that is compliant with a particular family of standards maintained by the Institute of Electrical and Electronics Engineers (IEEE) and called the 802.11 family. You will see different variants of this standard on wireless routers, for example 802.11b, 802.11g and 802.11n.

In wireless LANs, the individual laptops, mobile phones and other devices, or nodes, are usually referred to as stations, acknowledging the fact that each communicating device acts as a radio station with a transmitter and a receiver.

In order to connect to a wi-fi network, a station needs to know the name of the network. This is also known as the service set identifier (or SSID) of the wireless LAN. The ‘service set’ referred to here is the set of wireless devices to be served by a particular wireless LAN.

The SSID allows the nodes on a wireless LAN to distinguish themselves from nodes on other wireless LANs that may be operating in the same physical space. For example, in many airports mobile phone companies provide free wireless LAN services to their customers and use the SSID to ensure that customers connect to the appropriate wi-fi network.

When you are trying to connect to an available network, you will see a list of SSIDs that are reachable from your device, some of these will have padlocks against them – more about what that means later.

2 Is your private information really private?

Video content is not available in this format.

We all hope that the information we send wirelessly is private, but is that always the case?

Channel 4 News was able to learn personal information about unsuspecting people by intercepting their, supposedly private, but in reality completely public, wireless internet signals.

The attack shown in the video was possible because the hackers had set up their own wi-fi hotspot that either advertised the name of a common wireless hotspot provider, or the users chose to connect to a ‘free’ wi-fi network. The lesson here is to be careful about the public wi-fi networks you connect to, and the types of information you access using these networks.

2.1 Network security challenges

Figure 5

Internet routers are designed to move datagrams to their destination but how secure are they?

They have been programmed with strategies to overcome problems such as congestion or the failure of a part of the network. These strategies involve re-routing datagrams via any alternative path, as you saw from using Trace Route. Therefore, it is impossible to state with any assurance which route will be taken by a datagram travelling outside a local network.

The datagram may travel directly, or, more probably, travel through several routers located anywhere in the world. These routers will most probably not belong to either the sender or the recipient, but a third party. In most cases this will not matter, but datagrams can be copied, and their security compromised, as they pass through a router without alerting either the sender or receiver.

The process is known as packet sniffing and it has many legitimate purposes including analysing network performance and for law enforcement, but packet sniffing software is readily available to anyone who chooses to use it. In the past, packet sniffing required a computer that was wired to the network, but wireless networking means this is no longer the case.

2.2 Encryption in wireless networking

Figure 6

Since wireless networks transmit data over a medium that is shared by everyone, anyone with a compatible receiver or transceiver is able to eavesdrop on the radio signals being sent.

Ensuring that the eavesdropper is not able to convert these signals into the original message is a desirable security property of any wireless network, referred to as ensuring *confidentiality*. (This was one of the three security essentials we mentioned earlier, along with integrity and availability.)

Another security problem with using a shared medium for transmission is that malicious users could interpose themselves between a sender and a receiver and modify the messages being exchanged or even destroy them entirely. This is sometimes called a 'man-in-the-middle attack', and it compromises the *integrity* of the data being transmitted across the network.

Finally, an attacker could transmit lots of random data on the frequency being used by the wireless network, congesting the network and thus preventing other users from sending data. As we saw earlier in the course, this is called a 'denial-of-service' (DoS) attack and is an example of an attack on the *availability* of the network.

How encryption can help

So how do wireless networks address these potential security issues?

One commonly used security mechanism is **encryption**, which can help to ensure both the *confidentiality* and the *integrity* of data. The idea of encryption is to take the information you wish to protect and transform it into a different form, such that only the people who are supposed to receive the information are able to reverse the

transformation and recover the original information. This is like having a key to unlock a door; only a person with the right key can open it.

Encryption can help ensure:

- **Confidentiality** – When a message is encrypted using a particular key, it can only be decrypted to recover the original information if the same key is used. This ensures that messages are confidential between the sender and the receiver.
- **Integrity** – Encryption can prevent messages from being modified without the receiver's knowledge.
- **Authentication** – Encryption can contribute to the process of proving the identities of the sender and receiver.

You will look at encryption and decryption in more detail next week when we explain how cryptography works.

Encryption in wi-fi

Since wi-fi was first introduced, a number of security techniques have been used to protect wi-fi networks from unauthorised users and to ensure that the data transmitted across them is secure. The most common methods are based on encryption, using a key known only to the nodes in the wireless network.

The first of these mechanisms was called Wired Equivalent Privacy (WEP), which (as the name suggests) aimed to provide confidentiality comparable to that of a wired network. Since 2001, a number of serious problems have been identified in WEP that allow the encryption key to be computed within a few minutes, using readily available software. Many wireless devices still support WEP to ensure compatibility with older equipment such as old modems, but wherever possible users should switch to a more modern form of encryption.

In 2018, most equipment for Wi-Fi networks use Wi-Fi Protected Access 2 (WPA2), which uses a more secure key to encrypt the transmitted data. This security mechanism has become the default configuration for wi-fi networks, and must be supported by all wi-fi devices in order for them to be compliant with the 802.11 standard.

In 2019, new Wi-Fi devices should start to move to the WPA3 standard that will add higher levels of security. However, many public Wi-Fi networks will continue to run WPA2 and won't provide the enhanced security.

The only way of enhancing security on public Wi-Fi networks is to use a Virtual Private Network (VPN) which we will discuss in Week 6.

In the next section you'll consider how you might use wi-fi more securely.

2.3 Using wireless networking securely

Figure 7

Use the network connection tool on your computer to identify how many wireless networks are within range of your current location.

How many of them use secure connections? If your home wireless network is not configured to use WPA2 or WPA3, find out how to set this up and make sure to do this. The user manual for your wireless router or your internet service provider's website should have information that will help.

Consider how you connect to the internet when you are on the move. Do you connect to your home wi-fi network, your mobile service provider, the free wi-fi in a coffee shop?

Go through the online services you identified in Week 1. Which ones would you choose not to access using public wireless networks?

3 Why we need standards on the internet

Figure 8

As you've learned, when you send data over the internet it is sent across several hierarchies of networks, using different technologies from many different providers and operated by different organisations.

These networks must use a standard form of communication so information from one network can be passed across to another network.

To some extent, the way any one of these separate networks works internally is nobody's business but the owner and users of that network. However, where a network joins to other networks, where it becomes part of the internet, it has to conform to the standards of the internet.

The internet is not owned by a single organisation, so there is no one authority that dictates how it works. Yet all the different people and organisations with their own networks that together make up the internet have to work to common standards, or data would be unable to move between the different networks.

In the next section you'll find out about the TCP/IP protocols.

3.1 Introducing the TCP/IP protocols

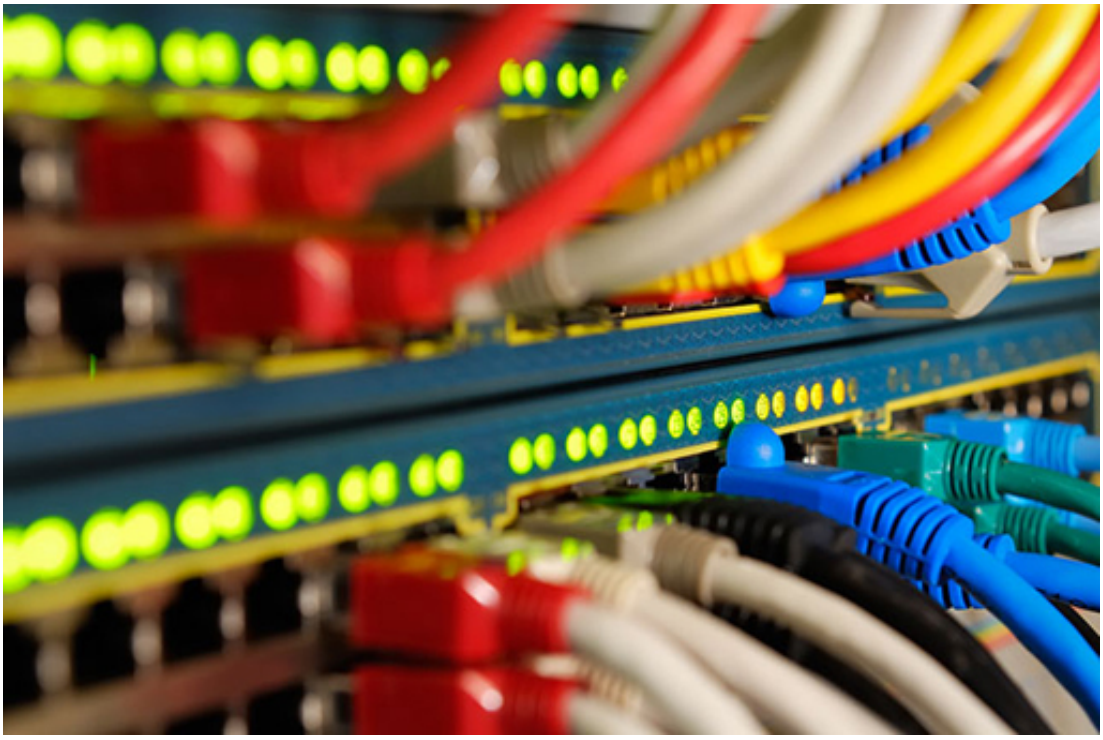


Figure 9

The standards that allow different networks and differing communications equipment to talk to one another are formalised in digital rules known as ‘communications protocols’.

For the internet the two most important are the Transmission Control Protocol (TCP), and the Internet Protocol (IP). They are so inextricably linked that they are often written together as TCP/IP.

TCP

The TCP protocol is responsible for ensuring data can be sent reliably over the internet. It works through a number of software ports that act to keep data separate on the same computer – so it is possible to browse a web page, collect email and listen to streaming music at the same time.

To understand how TCP works you need to know something about ports. A port can mean different things depending on the context. A port can be a physical connection on a device such as the USB port into which you plug your printer or flash drive. But for TCP, it means a number which indicates how data is handled when it reaches its destination. Many ports represent specific protocols such as port 80 representing the well-known port of HTTP.

Common TCP ports include the following:

- port 20 and 21 – File Transfer Protocol (FTP) for sending and receiving files (port 20) and control (port 21)
- port 22 – Secure Shell (SSH) for secure logins to computers
- port 25 – Simple Mail Transfer Protocol (SMTP) for sending email
- port 80 – HyperText Transfer Protocol (HTTP) for browsing web pages.

Data being sent from an application on your computer is divided into TCP datagrams each containing the TCP port number. The TCP application running on the recipient's computer will then examine this port number to determine which application should receive the information in the datagram.

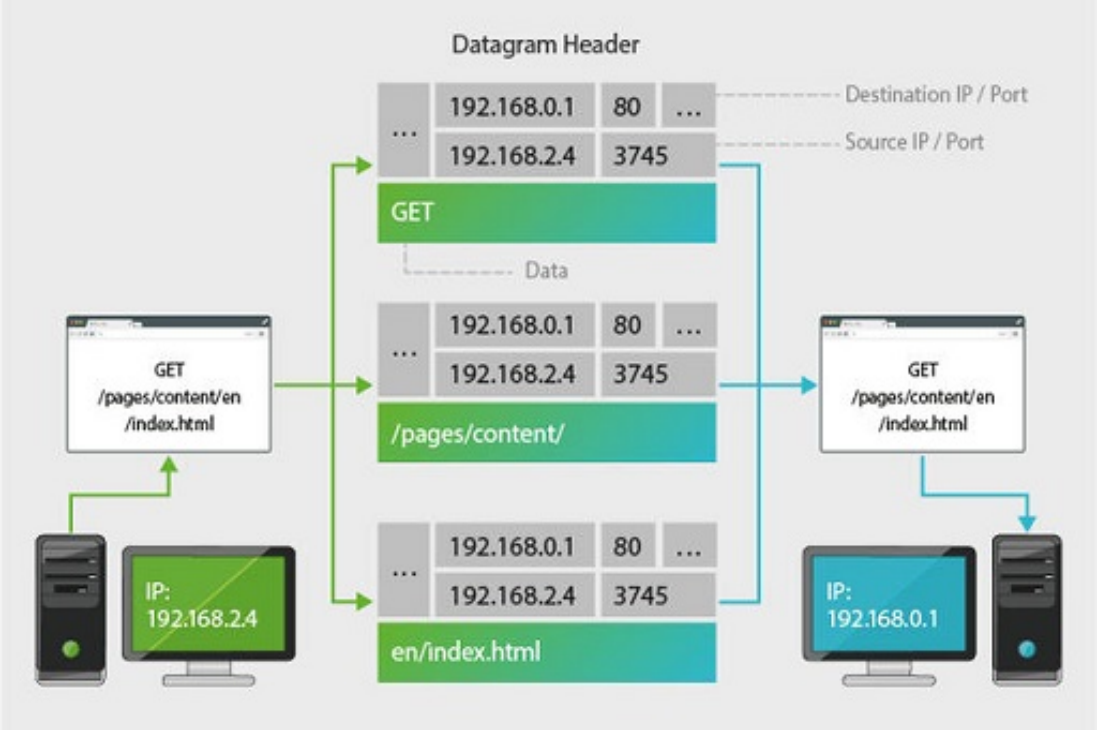


Figure 10

TCP's second major task is ensuring that all data sent from a computer is received by its destination. It waits for acknowledgements from the remote computer, and in the event that a datagram gets lost or damaged in transit, it can resend the missing datagram. For this reason TCP is reliable – but relatively slow.

Applications where timeliness is more important than absolute accuracy – such as streaming media, video games and video conferencing – will use less reliable, but faster, protocols such as UDP (User Datagram Protocol) to send and receive their data.

If you are receiving an email, you want the whole message to arrive with no gaps, but if you are streaming a TV programme, it doesn't greatly matter if a few datagrams get lost.

TCP is not responsible for sending and receiving information; that is performed by a second protocol – most commonly, IP, that we will look at next.

3.2 The internet protocol and IP addresses

Figure 11

The Internet Protocol (known as IP) does the hard work of actually moving data across the internet. IP is only concerned with moving data, it doesn't actually check that data actually arrives (that's handled by TCP).

When IP receives data from TCP to be sent on to the internet it wraps the TCP datagram in its own IP datagram containing a sender's and a receiver's address as well as some other information.

When IP receives data from the internet, it removes the IP datagram information and passes it to TCP which will perform the checking of the contents and reordering of information before it can be passed through the appropriate port to an application.

IP addresses

The internet addresses used by humans (such as www.open.edu) are purely for our convenience, as computers use numeric addresses known as 'Internet Protocol' addresses (or IP addresses, or sometimes IP numbers) for communication. Every computer directly connected to the internet has a unique Internet Protocol (IP) address.

There are two major forms of IP address: IPv4 and IPv6.

IPv4 (Internet Protocol version 4)

This is the most familiar form of IP address consisting of four numbers, each ranging from 0 to 255, separated by full stops (periods) in the form 192.168.0.1. IPv4 has long underpinned the internet although it is now in urgent need of replacement (see below)

because the number of devices connected to the internet has nearly exhausted the total number of available IPv4 addresses.

IPv6 (Internet Protocol version 6)

IPv6 is a a replacement for IPv4, originally outlined in 1998, to accommodate the increasing demand for IP numbers as more people and devices were connected to the internet. It can support a theoretical 3.4×10^{38} devices meaning it is suitable for any conceivable demand.

IPv6 is intended to replace IPv4; however this is an extremely complex process and it has taken a long time with even the most developed countries still far from completing the transition. A measure of compatibility exists in the form of IPv4-mapped IPv6 addresses where IPv4 addresses are stored in the IPv6 format.

Reserved IP numbers

Not all of the numbers in the IPv4 address range are actually available for use. As well as large blocks reserved for specific users in the early days of the internet, some are specifically used for ‘private’ networks outside of the internet.

10.0.0.0 to 10.255.255.255

169.254.0.0 to 169.254.255.255

172.16.0.0 to 172.31.255.255

192.168.0.0 to 192.168.255.255

Your computer will allocate itself an IP address beginning 169.254… if it is unable to connect to a local network. If you have a connection to the internet from your home your computer will almost certainly have an address beginning 192.168… In this case your network hub has a genuine IP address, your computer and other devices attached to the modem have private addresses. Your modem alters IP addresses on packets as they are sent to and from your home network and the internet.

3.3 From numbers to names

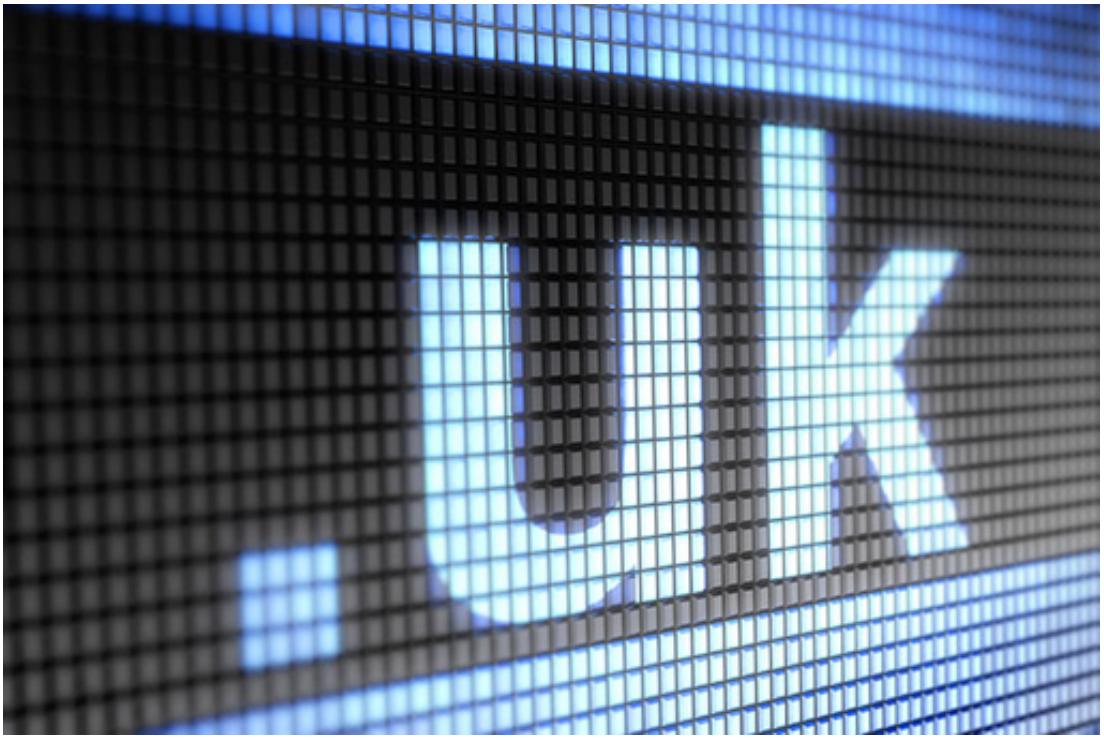


Figure 12

When we type an address (such as www.open.edu) into a browser, the address is translated into a unique IP address by a name server, called a Domain Name Server (DNS), located somewhere on the internet. This IP address is attached to every IP datagram destined for the Open University server.

As an example we will use an IP datagram belonging to an email being sent to Bob who works in the coffee bar at Big University in America (Bob's address is bob@coffee.big.edu). The address is sorted from the most general part of the address to the most specific. First of all, the name server on the sender's machine makes a request across the internet to a computer which holds the addresses of all American universities (most of which use .edu at the end of their address) asking for the IP number of big.edu. Assuming that big.edu exists, the .edu name server then responds with the IP number for the name server at Big University.

The sender's machine then uses that IP number to make a link to the name server at Big University and requests the IP number of the coffee shop computer used by Bob. The big.edu name server will then respond with the address of the coffee shop. The IP datagrams can then all be addressed correctly and sent into the network.

Up until 2019, the DNS information requested was sent as plain text and could be intercepted even when the data being sent or requested was encrypted. From 2019, it has become possible for DNS requests to be encrypted. In Firefox browser go to Settings, then Network settings and select the enable DNS over HTTPS checkbox.

Chrome 78 is also experimenting with this feature, which can be enabled by browsing to 'chrome://flags/' in your Chrome browser, searching for 'dns-over-https' and enabling. You will have to restart the browser for this change to take effect.

3.4 The internet is not the world wide web

Figure 13 British physicist-turned-programmer Tim Berners-Lee devised the specifications for URIs, HTTP and HTML – technologies that underpin the internet as we know it

We've all done it. We've all been browsing a website and said 'I'm on the internet!'.

This is true, but misleading, if for no other reason than the internet dates from 1982 (with its roots as far back as 1969) but the world wide web only came into being in 1990 thanks to Sir Tim Berners-Lee.

Before the advent of the world wide web, not only did fewer people use the internet (it took until 1998 for 100 million people to log on for the first time), but it wasn't anything like the world wide web we know today – almost all commands had to be typed in – often using cryptic instructions, and what you got back – if you got anything at all – was plaintext. The world wide web not only meant that it was possible to use the internet's resources without learning a whole new language, but it allowed for rich text, graphics, animation and sound to be delivered quite literally at the click of a button.

Part of the internet

At its simplest, the world wide web is nothing more than the part of the internet that can be accessed through the HyperText Transfer Protocol (HTTP) – another one of those standards that helps glue the internet together. HTTP allows two computers to exchange information as a series of requests (e.g. a request from your computer for a copy of the To do list page for this course) and responses (e.g. an Open University server delivers the contents of that page).

HTTP relies on TCP to set up the connection between the two machines, and it in turn uses IP to send and receive data. The most common applications that understand HTTP messages are web browsers such as the one you are using right now.

The world wide web is an example of hypertext – documents joined together using links. Every time you click on a link, HTTP is used to request a new page from a web server using TCP port 80. The content for the page is delivered to your computer, again through port 80 and interpreted by a web browser which formats the data in a human readable manner.

Designed to be open

The world wide web was designed from the very start to be an open environment which encouraged people to set up their own web servers and to write web pages. To encourage its uptake, all of the documentation that explains HTTP, and other standards that have grown up around the web, are publicly available to anyone wishing to develop software for the web. Likewise, the computer language used to format web documents, the HyperText Mark-up Language (HTML) is not only fully documented online, but is extremely easy to use.

Apart from the world wide web, the internet itself is used for a much wider range of services including email, instant messaging and file transfers. The internet's flexibility comes down to the flexibility of the underlying protocols – so long as information can be stored in IP datagrams – and just about anything can – it can be moved around the internet.

Interview with Tim Berners-Lee

Audio content is not available in this format.

Listen to this interview. Towards the end, Tim Berners-Lee mentions a number of things that will be needed to make the world wide web achieve its full potential. One of these is digital signatures, which can be achieved using cryptography – our topic for next week.

Next, you have an opportunity to review your learning of the course so far in the Week 4 compulsory badge quiz.

4 Week 4 quiz

This quiz allows you to test and apply your knowledge of the material in Week 4.

Complete the Week 4 compulsory badge quiz now.

Open the quiz in a new window or tab then come back here when you're done.

5 Summary of Week 4

Figure 14

This week you have learned the basics of computer networking and communications, gaining an understanding of how data is transmitted across the networks, including wireless networks.

You are now aware of some of the networking standards that allow different devices to connect to the network and exchange information.

Additionally, you have learned about the difference between the internet and the world wide web, and can describe some security problems that affect networks.

You are now half way through the course. The Open University would really appreciate your feedback and suggestions for future improvement in our optional end-of-course survey, which you will also have an opportunity to complete at the end of Week 8. Participation will be completely confidential and we will not pass on your details to others.

You can now go to Week 5: Cryptography.

Week 5: Cryptography

Introduction

Video content is not available in this format.

Cory explains the focus for this week: cryptography.

Cryptography is a specialised area of mathematics concerned with protecting information so that it can be transmitted and received securely even when there is a risk that a hostile third party might intercept or modify the data. You will recognise it as it's been mentioned before as a technique that can help with protecting information.

We are now going to look at this important aspect of cyber security in a little more detail.

1 The secret of keeping secrets

Figure 1

There have been many applications of cryptography throughout history, ranging from simple ciphers used by Julius Caesar to send military orders to his generals, to the more sophisticated medieval ciphers that withstood most attacks until the late ninteenth century and the famous Enigma codes of the Second World War.

The development of computers in the twentieth century allowed for far more complex means of encryption. Computers could perform:

- the mathematical operations that underpin all cryptography
- much more complex mathematics than could be reasonably expected of a human
- much faster than a human
- on much more data than a human could handle.

Any data that could be represented in binary format, i.e. using 0s and 1s, can be encrypted by a computer. It is not an exaggeration to say that encryption makes much of the modern world possible. Some commonplace applications for cryptography include:

- secure banking and payments systems – cryptography ensures your money is safe when it is transferred between accounts, issued at ATMs or used to shop online
- protecting conversations made over mobile telephones
- safeguarding wireless networks that give access to the internet
- securing files on hard disks and memory sticks
- authenticating electronic documents
- electronic voting

- securing media files such as music or movies from piracy, where it is known as Digital Rights Management (DRM).

1.1 Plaintext and ciphertext

Figure 2

As in previous weeks, there is some terminology we need to introduce:

- **plaintext** – information that can be directly read by humans or a machine (this article is an example of plaintext). Plaintext is a historic term pre-dating computers, when encryption was only used for hardcopy text, nowadays it is associated with many formats including music, movies and computer programs
- **ciphertext** – the encrypted data
- **a cipher** – the mathematics (or algorithm) responsible for turning plaintext into ciphertext and reverting ciphertext to plaintext (you might also see the word ‘code’ used – there is a technical difference between the two but it need not concern us now)
- **encryption** – the process of converting plaintext to ciphertext (occasionally you may see it called ‘encipherment’)
- **decryption** – the process of reverting ciphertext to plaintext (occasionally ‘decipherment’).

1.2 Encryption keys

Figure 3

Keys are pieces of information that determine the output from an encryption (or decryption) process. A single cipher can produce an almost limitless number of different outputs with different key values, allowing secure communication even if the cipher itself is known to hostile third parties.

It might surprise you to know that almost all ciphers are published in the scientific press or in standards documents. Having them available for widespread scrutiny allows many people to check that they are secure and do not contain weaknesses which could be exploited to compromise the security of the data encrypted using that cipher.

A computer encryption key is nothing more than a string of bits where each bit can have a value of either 0 or 1. The number of possible values for a key is simply the total number of values that the key can have. So our one-bit long key can only have two possible values – 0 and 1. If we choose to have a two-bit key it could have one of four possible values – 00, 01, 10 and 11. In fact every time we increase the length of the key by one bit we double the number of possible keys – so a three-bit key has eight possible values – 000, 001, 010, 011, 100, 101, 110 and 111.

The total number of keys can be written in scientific form as $2^{\text{key length}}$; so a key with a length of eight has 2^8 – that is 256 – values.

But how long should a key be? How short is too short?

The problem with short keys

Short keys are vulnerable to what is known as a brute force attack, just like you learned in Week 2 about passwords. A brute force attack is where a computer, or a number of computers, try every possible value for a key until they produce recognisable plaintext.

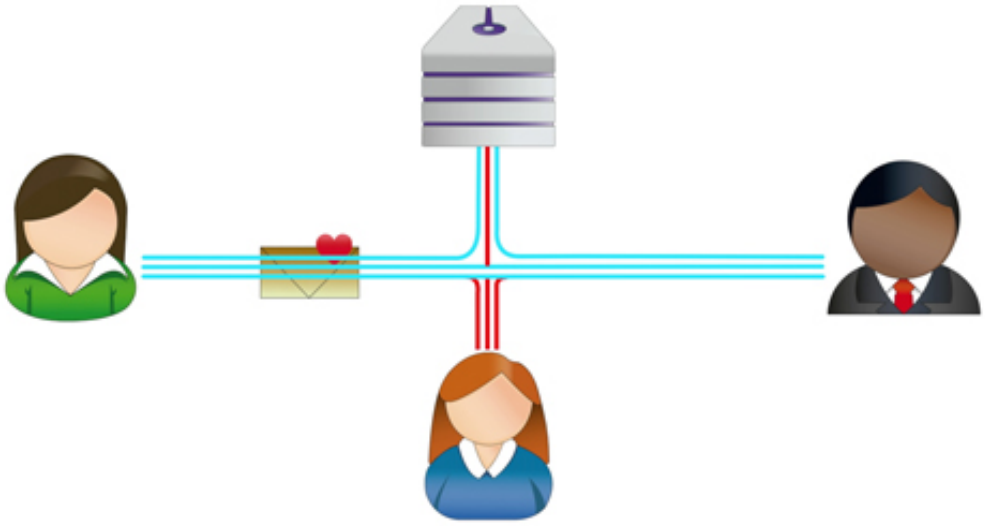
Since computers can work through key values extremely rapidly, keys must be sufficiently long that they offer a very large number of possible values.

Keys may be known to the user in the form of passwords, or they may be stored in a computer's hardware (such as the decryption keys stored on a DVD player that allow it to play the encrypted data stored on the movie disk), or they can be generated by a computer as and when they are needed (such as conducting a secure transaction on a shopping site).

Next, you'll learn about the key distribution problem.

1.3 The key distribution problem

Video content is not available in this format.



Traditionally, symmetric encryption suffered one enormous shortcoming – it was necessary for either the sender or the recipient to create a key and then send it to the other party. While the key was in transit, it could be stolen or copied by a third party who would then be able to decrypt any ciphertexts encrypted with that key.

Another problem is that a large number of key pairs are needed between communicating parties. This quickly becomes difficult to manage the more there are. This can be calculated as n(n-1)/2 where n is the number of communicating parties.

For example, if ten parties want to communicate with each other securely they would need 45 different key pairs: 10(10-1)/2 = 45. This would increase to 4,950 if there were 100 communicating parties!

This problem, called the **key distribution problem**, affected anyone wishing to use encryption until the 1970s when a method of distributing keys without actually sending the keys themselves was developed independently by GCHQ in the United Kingdom and Whitfield Diffie and Martin Hellman in the United States. The British discovery was kept secret for many years, so today the solution is known as the Diffie–Hellman key exchange method.

Symmetric encryption methods have the advantage that encryption and decryption is extremely fast, making them ideal for transmitting large amounts of secure data. In the video you saw how key distribution was achieved between two people, Alice and Bob.

1.4 Asymmetric or public key cryptography

Video content is not available in this format.

Asymmetric cryptography, better known as public key cryptography, side-steps the key distribution problem as each user creates their own keys:

- the **private key** which they keep safe and never distribute
- the **public key** which can be sent to anyone with whom they want exchange encrypted information.

Together the two keys are known as a **key pair**, which is what was used by Alice and Bob.

Unlike symmetric encryption, the two keys behave differently; the public key is the only key that can decrypt ciphertext encrypted using the corresponding private key and the private key is the only key capable of decrypting files encrypted with the corresponding public key. Crucially, the value of one key cannot easily be determined from the other, so even if the public key falls into hostile hands, the value of the private key cannot be determined.

Public keys can be distributed using email attachments or through public key chain servers which act as distributors for large numbers of public keys. The creator of a public key uploads their key to the key chain server and it is freely available to anyone who wants to use it.

Although the mathematics behind public key cryptography is incredibly complex, the process of using it is relatively simple. To send a message using public key cryptography is simple. The sender obtains a copy of the recipient's public key, either by email or from a

key chain server, and uses it to encrypt the message. The resulting ciphertext is then sent to the recipient who uses their corresponding private key to restore the original plaintext.

Public key cryptography is popular because there does not have to be any initial secure exchange of secret keys for an encrypted message to be sent (remember, users only ever exchange their public keys). However, it is generally far slower than symmetric encryption; and because of a quirk in the underlying mathematics, traditional public key cryptographic techniques require far longer keys to offer the same level of protection as symmetric encryption.

A newer type of public key cryptography, known as ‘elliptic curve cryptography’, can be just as secure as symmetric encryption using similar key lengths.

In the next section you’ll discover why these encryption methods aren’t used to keep the internet more secure.

1.5 Why isn’t the internet encrypted?

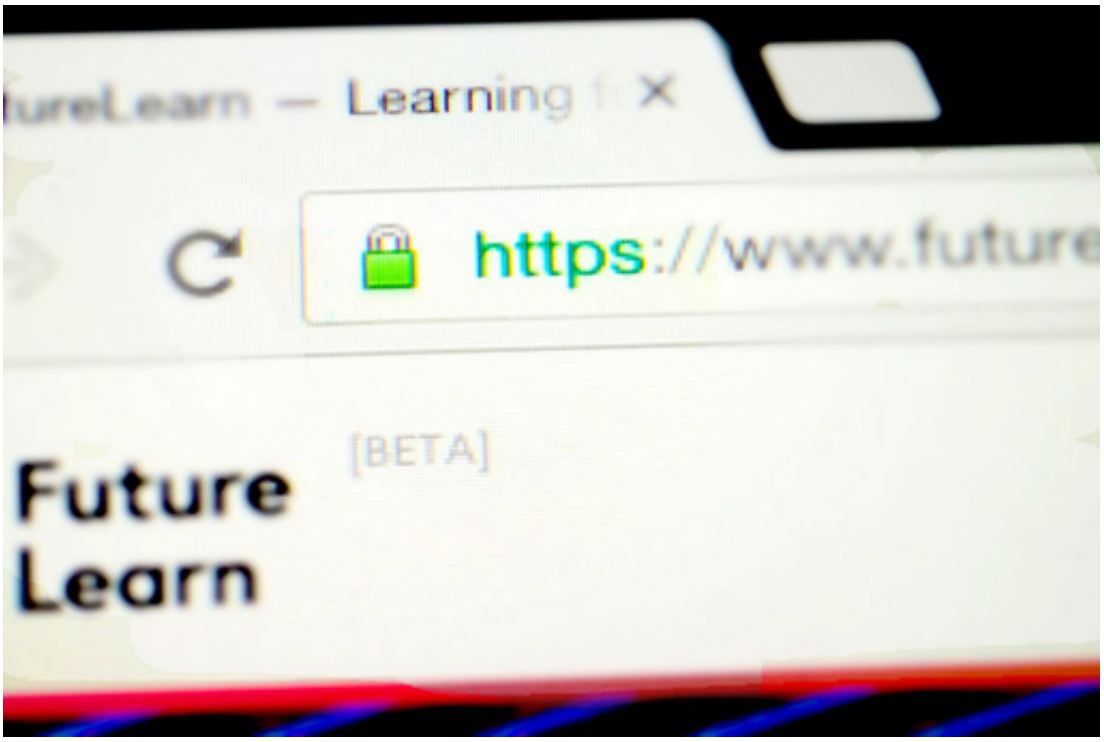


Figure 4

Crucially, one part of everyday life that is not routinely protected by cryptography is the internet itself. The majority of emails and web pages are sent in plain view and can be intercepted and read by a malicious third party.

In theory, the whole of the internet could be protected using cryptography, but this is unlikely to happen because it takes a certain amount of computer power to encrypt and decrypt information so there would be significant costs if it were to be used throughout. Also there are a range of web applications, such as reading news sites or browsing online shops, that do not involve any sensitive information and therefore do not need to use encryption.

Applications running over the internet selectively use cryptography for key tasks (such as processing payments for online shopping) and users may choose to use cryptography for additional purposes (such as securing email).

The data sent by many websites you visit is encrypted in transit. This is sometimes shown by a padlock symbol in the address bar of the web browser. You'll learn more about this later in the course.

Review the list of digital information and online services you compiled in Week 1 of the course. Based on the threats you associated with each item in your list, think about some examples of how you could use cryptography to improve your security.

2 Putting cryptography to use

Figure 5

So far this week you have studied the basic cryptographic techniques that can be used to protect the confidentiality and integrity of your information. Now let's examine how these techniques can be used in practice.

Transport-level encryption encrypts the text of the message between your device and the server that receives the data. One of the most common is STARTTLS. However, your messages may not be encrypted while sitting on a mail server.

End-to-end encryption ensures that the message remains fully encrypted all the way from the sender to the recipient.

Many websites, such as those for internet banking and online shopping, routinely use encryption to ensure that the data sent to and from your computer is safe from eavesdroppers. However, configuring the same technologies to protect activities such as email communication can be quite difficult because the tools involved are complicated to install and configure.

Most end-to-end encryption tools depend on a collection of cryptographic techniques, commonly called 'Pretty Good Privacy', PGP for short. PGP includes algorithms for symmetric and asymmetric cryptography. In order to help software vendors develop systems that can easily exchange encrypted information, a standard called OpenPGP was developed and agreed on by the Internet Engineering Task Force (IETF).

Some examples of tools available for encrypting emails include:

- GPG4Win – provides a set of standalone tools that can be used to encrypt and digitally sign emails, documents and other files. It provides some plug-ins to integrate these features into standard email software, such as Microsoft Outlook and Mozilla Thunderbird.

- GPGMail – this tool is designed to integrate with the Mail software provided by Apple. It can be used to both encrypt and digitally sign your email. It is easier to configure and use than the Windows tools, but is only useful if you use a computer running OSX.
- Enigmail for Thunderbird – this is a plug-in for the Thunderbird email client software that works across all operating systems. However, it requires manual installation of the GNUPG software, an open source implementation of the OpenPGP standard.
- Mailvelope – this is a browser plug-in that uses an implementation of the OpenPGP standard. It works with a variety of browsers and web-based email systems, such as Gmail or Yahoo Mail. However, there is a security problem with such web-based email systems. Although you may have encrypted the message from end to end, the details of the email address it is sent to, as well as who it is from, and the time the message was sent can be logged, and this metadata may compromise your security and that of the recipient.

A secure email service like Protonmail or Tutanota can hide the metadata that links the sender to the recipient of the message.

In its most secure usage pattern, a user logs in to ProtonMail and leaves an email message for another ProtonMail user to log in and collect. The metadata about the users is never revealed and the message is also securely encrypted from end to end.

When the ProtonMail user sends an email to an external email address the metadata of the sender remains secure. ProtonMail sends an invitation to the recipient to view the encrypted message on the server. The mail service of the recipient may record that a message was sent by the ProtonMail server. If the user of ProtonMail uses the free service to send encrypted email to an outside email address they will have to send a key to the encryption to the recipient by some other means for the recipient to log in, such as a text message or phone call. This may reveal a link between sender and recipient.

A paid for service with ProtonMail allows use of PGP, so that a message can be sent to an external address using the recipients public key. No link need be created between the sender and recipient. However, the subject line isn't encrypted.

In the next few sections we will explore an alternative way of using cryptography to protect your email communications.

2.1 Setting up a PGP email client

Figure 6

This section is optional. You'll need to be able to install software on the computer you are using for this course to complete this. If you're not able to do this then please still read through the steps so that you understand the process.

1. Select one of the PGP email clients described in the previous section and explore how to set it up and use it to send mail encrypted with PGP.

   For example if you already use Thunderbird for your email client you could investigate the use of Enigmail. If you use Outlook for your emails you could investigate using Gpg4win. If you use a browser based email you can install a plugin from https://www.mailvelope.com/en/

   Follow the instructions on the Mailvelope website.
2. One of the best ways to test sending and receiving encrypted emails is to use two separate, free, web-based email accounts and open each one in a different browser. For example, use Firefox for one and Brave for the other. Install Mailvelope in both Firefox and Brave and set up one email account in Firefox and a different email account in Brave
3. Now follow the Mailvelope instructions to create and send an encrypted email from one of your accounts to the other.

Disclaimer: The Open University and partners associated with this course have found this software to be robust at the time of checking. However, installing software is done at your own risk and The Open University and their partners cannot be held responsible for any resulting damage to your computer.

2.2 Sending signed and encrypted email

Below is an optional activity.

Activity 1 Optional activities

Allow about

As an alternative to exchanging encrypted emails with a colleague or friends, if you have set up Mailvelope or another PGP email client you can send an encrypted email to an automated mail box at The Open University:

- First send an email that simply says 'public key' to: cybersecurity-mooc@open.ac.uk
- The server will send back an automatic reply that includes the current PGP public key for this mail box.
- Again follow the instructions on the Mailvelope website, or for the PGP encryption software that you are using, use this public key to create a new email with a message 'testing encrypted content'

  Note that you need all the characters including ———BEGIN PGP PUBLIC KEY BLOCK——— and ———END PGP PUBLIC KEY BLOCK———
- Send your email to: cybersecurity-mooc@open.ac.uk. You will receive an email back from us to say that we've successfully decrypted your message! If you don't receive an email within 2 hours, please try again.

To find out more about Mailvelope's features or get help with specific problems visit Mailvelope help.

End-to-end encryption as a service

It can be a problem for organisations and individuals to set up the software for encrypted emails on all the devices that they use.

End-to-end encryption can be provided as a service. At the time of writing, ProtonMail and Tutanota both have a good reputation and also offer a free service.

Follow the instructions at https://protonmail.com/ or https://tutanota.com/ to set up two FREE accounts with the same service in two separate browsers. Then use these accounts to send a message from one account to the other.

In the last few sections you have explored what is involved in using cryptography to encrypt and sign email communications.

- What seemed to be the hardest parts of the process?
- What would you want to improve to make it easier?
- How does the use of ProtonMail or Tutonota compare with the use of Mailvelope or other secure email software?

You may find it useful to compare your experience with the instructions for one of the other tools mentioned in Section 2, Putting cryptography to use.

3 Comparing different cryptographic techniques

Figure 7

The field of modern cryptography is steadily growing with its increased use in everyday life when surfing the internet, using your card in a cash machine etc.

There are hundreds of different cryptography schemes each with different applications, some of the most notable are described below.

DES (Data Encryption Standard)

DES was first developed in the 1970s and was adopted by the United States National Bureau Of Standards as the US government standard for encrypting sensitive information. It is a symmetric cipher using 56-bit keys.

Due to DES's relatively small key size it was discovered that it was possible to crack the encryption with a brute force attack. Although this was a theoretical risk when first proposed, the great increases in computing power over recent years have shown that DES can be brute forced in less than a day. It was this weakness that led to official adoption of other encryption standards, such as AES, by the US government.

A variant of DES, called Triple DES was developed to provide additional security, and be compatible with the previous version, without the requirement to develop a completely new cipher. Triple DES uses three rounds of DES encryption and three separate 56-bit DES keys.

Triple DES was widely used in e-commerce and online payment applications, as well as securing data in Microsoft Outlook, until 2018. When this course was first written it was thought that Triple DES would remain secure from a brute force attack until at least 2030. However, it is now considered to be insecure and was deprecated by NIST (the US National Institute for Standards and Technology) in 2017.

AES (Advanced Encryption Standard)

The realisation that the DES standard was no longer adequate led the United States government to call for a replacement. After an open competition lasting five years, AES was adopted as a US government standard in 2001. AES uses a combination of symmetric ciphers and either 128, 192 or 256-bit keys providing enhanced security over DES. Although some potential weaknesses have been identified in AES, most are theoretical, with the encryption being easiest to break in a situation where it has not been implemented correctly rather than in the case of a brute force attack where every possible key combination must be tried.

AES is now widely used in commercial applications since the underlying specification is freely available for personal or commercial use. It is used to protect archive files, encrypting computer file systems (such as Windows 2000 onwards), encrypting hard disks and for secure file transmission. Such is its importance that many microprocessors now include AES in their instruction sets to speed up encryption and decryption.

Blowfish

Blowfish was developed in the early 1990s as a potential replacement for DES, though AES ultimately became the agreed standard form of encryption. It is a cipher supporting variable key lengths from 1 to 448 bits. To date there has been no known successful attempt to break the encryption in its full implementation, although weaknesses have been identified when Blowfish is used with relatively weak keys. The related twofish and threefish ciphers have been designed to overcome these weaknesses, although most users have switched to AES.

Next, you'll find out how cryptography is used to prove identity online.

3.1 Using cryptography to prove identity

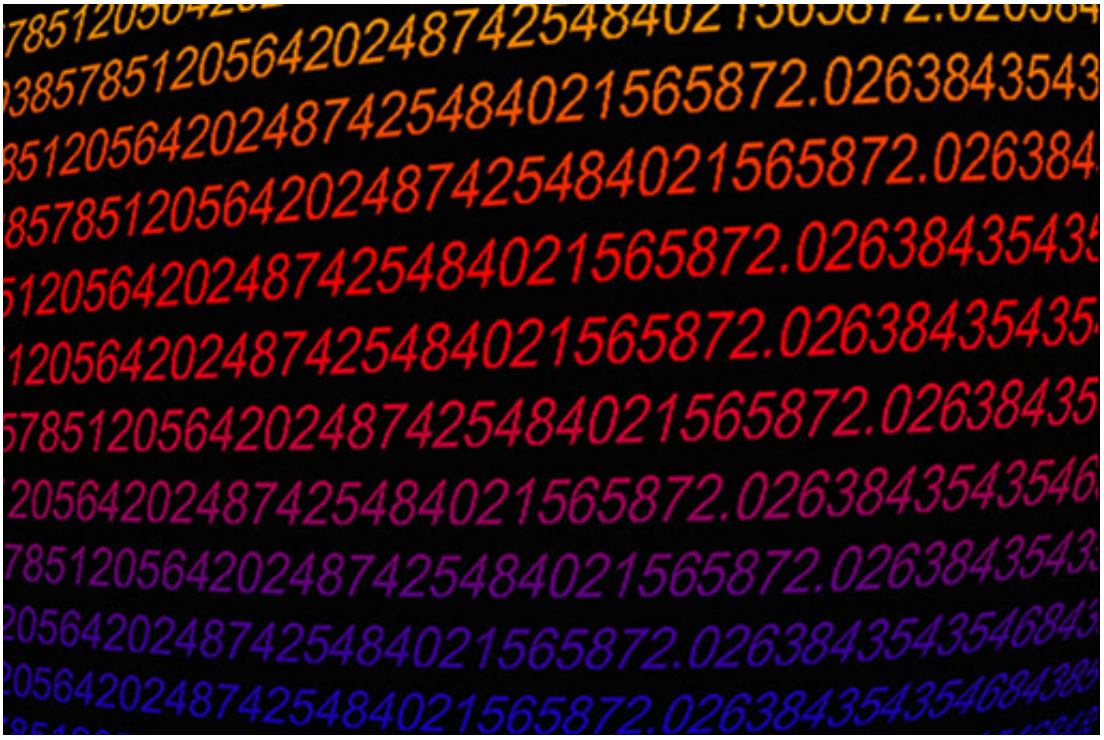


Figure 8

Cryptography isn't just used to hide secrets, it can also be used to authenticate data sent on an insecure network – such as the internet. The process begins by checking that your copy of a piece of data is an exact match for the one you requested.

Hashing

Hashing is the mathematical process of converting data of any size into data of fixed length known as the 'hash' (alternative names include message digest, hash codes, hash sums or hash values).

Hashing operates in one direction only, making it impossible to deduce the original data from the resultant hash. The intention of hashing is not to preserve the contents of the data but to create a unique identifier for every single piece of data. When a file is published on the internet, the author may choose to publish the hash value for that file. For instance, here is some information published by the GnuPG encryption software authors on their website:

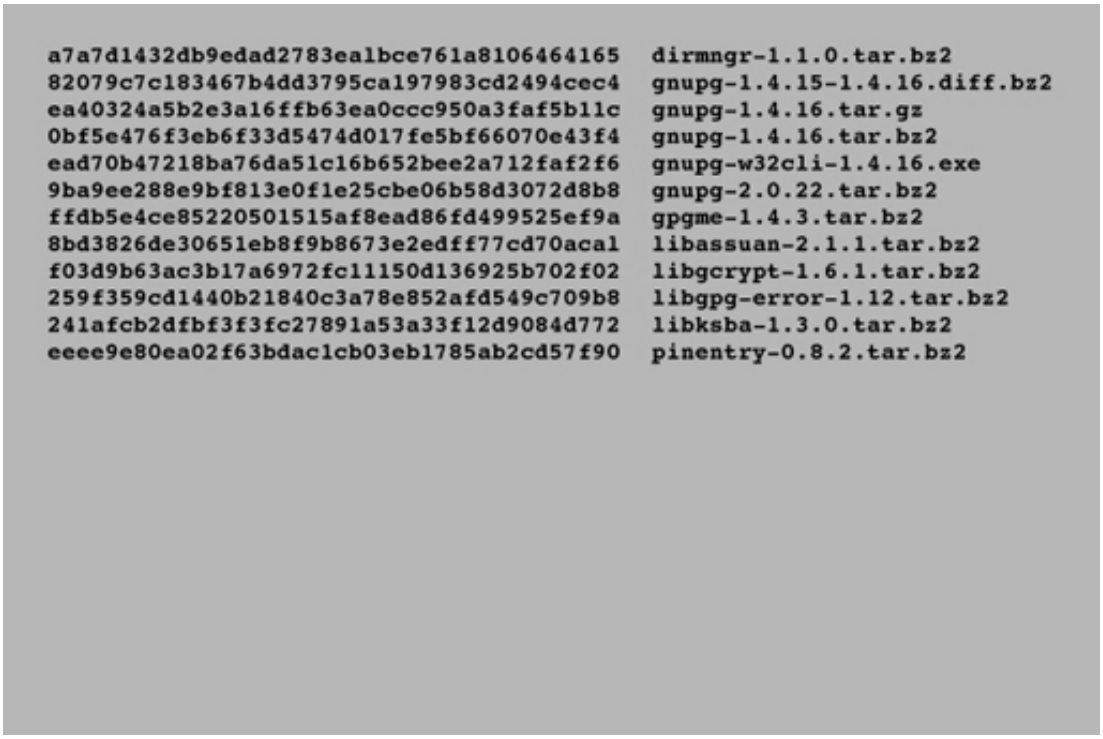


Figure 9

Each long line of numbers and letters on the left is a hash (in this case from a hashing program called SHA-1), the text on the right is the name of the file. If you download one of these programs, you can then run your own copy of SHA-1 on your download and obtain a hash – if your file exactly matches the original the two hashes will be identical.

A variation of a single bit of data between two otherwise identical files will result in vastly different hash values, so any edits to a file between two hashing operations will result in different hash values revealing that the data has been tampered with and should not be trusted.

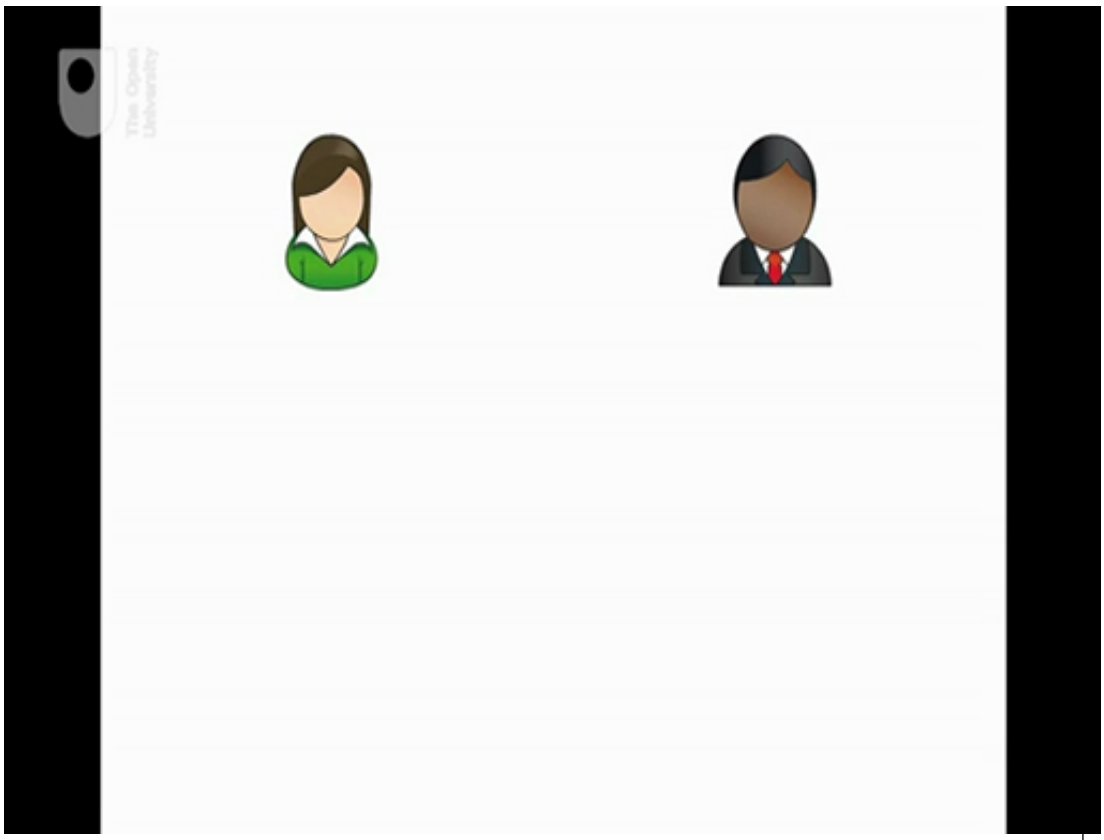
A large number of hashing algorithms have been developed; the most widespread are algorithms called MD5, SHA-1 and SHA-2. Although MD5 and SHA-1 are in common use, both have been found to be flawed. Under certain circumstances ‘collisions’ can occur where two pieces of different data can generate the same hash value (albeit under specifically controlled conditions).

This weakness in the MD5 hashing algorithm has been used in malware targeting Microsoft Windows computers. Since neither algorithm can be guaranteed to generate unique hashes they can be considered ‘broken’ and should not be used. The United States government requires all hashes to be generated using the newer SHA-2 algorithm which has not shown any such weaknesses.

Next, you’ll find out how digital signatures and certificates use cryptography.

3.2 Digital signatures and certificates

Video content is not available in this format.



Hashing can show that data has not changed in transmission, but on its own cannot demonstrate that the data originated with its supposed author. To do that, a digital signature should be used.

Digital signatures use the sender's private key to encrypt the hash. Previously, you learned how documents can be encrypted with a public key which can be used by anyone, but can only be decrypted using the corresponding private key known only to the owner.

Encrypting data using the private key isn't suitable for securing secrets (as anyone with access to the public key could decrypt it). However, it is perfectly possible to encrypt a hash using the private key so that the hash can be decrypted and compared by anyone possessing the matching public key. This can be used to provide authenticity since the encrypted hash must have been produced by the holder of the private key – hence the name digital signature.

Case study 1: Alice and Bob

Imagine that Alice wants to send the company's quarterly profit statement to Bob, who works in the financial markets, for public announcement. Both Alice and Bob want confidence that the quarterly profit statement has not been intercepted by Eve en route and altered.

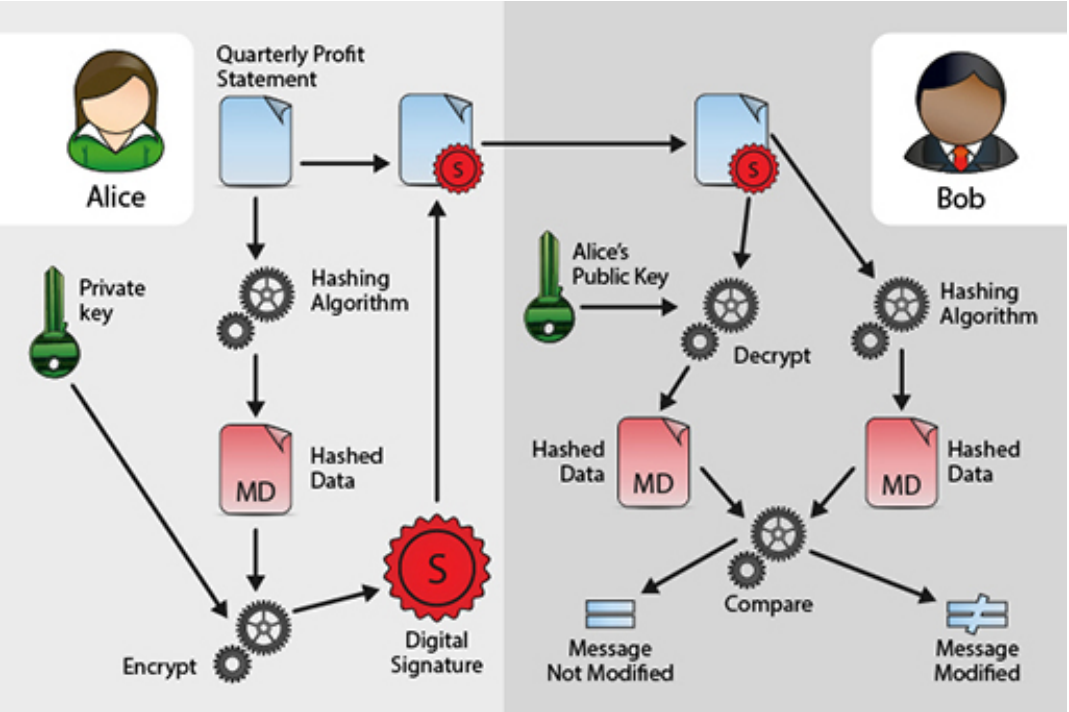


Figure 10

Alice will therefore produce a hash of the quarterly profit statement and then encrypt this with her private key to produce a digital signature. Alice will then include the digital signature with the quarterly profit statement and send this to Bob. Alice may also encrypt the quarterly profit statement and the encrypted hash with Bob's public key so that all details of the message remain secret.

Upon receipt Bob will, if Alice sent the message encrypted with his public key, decrypt the message using his own private key. This will then reveal the encrypted digital signature. He will decrypt the digital signature using Alice's corresponding public key to reveal the hash. Bob will then calculate a hash of the quarterly profit statement and then compare this with the encrypted hash that he received from Alice. If the hashes are the same then both Bob and Alice can be confident that the quarterly profit statement was not altered en route by Eve.

Digital signatures do not provide us with complete confidence of the author or originator. Just because a digitally signed document claims to come from a person or a company it doesn't mean that it actually did, a malicious individual could masquerade as the sender by producing their own public/private key pair and using these to produce digital signatures.

Case study 2: Alice and Bob

Imagine that a digitally signed business invoice arrives in Alice's mailbox from Bob. She uses Bob's public key from a public key server to decrypt the digital signature and validate the business invoice by comparing the hashes. Alice, assuring herself that it is Bob (as the hashes are the same), follows the instructions and transfers money to the account details in the business invoice.

A few weeks later, Alice receives an angry email from Bob because he has not been paid. After a bank investigation she finds out that she had transferred the money to Eve by mistake – so what went wrong?

It's clear that the business invoice and the associated signature did not come from Bob, instead the signed business invoice actually came from Eve. Eve used Bob's personal information to create a new key pair in Bob's name and placed a copy of the public key on a public key server. Eve then used her corresponding private key to sign the business invoice and send it to Alice.

Alice, convinced that the document was a genuine business invoice from Bob (as it included what she believed to be his digital signature), followed the instructions and paid money into an account belonging to Eve – oh dear!

Digital certificates help us overcome this problem. A digital certificate is a means of binding public keys to their owner. These are issued by Certificate Authorities (CAs) who validate the owners of public keys. The CA does this by validating (through various processes), the identity of the owner of the public key. Once it has done this it will bind the public key to a digital certificate and sign it using its private key to attest authenticity. The CA's public key is available to all parties who need to validate the CA's assertion of public key ownership.

However, digital certificates still require a chain of trust to confirm that the certificate belongs to the person or organisation that you think it does and have not been compromised. Criminals have been known to obtain certificates that were then used to sign software that included malware. Stolen certificates have also been used to sign malware. For example, the Stuxnet code was signed with certificates that belonged to Realtek Semiconductor and JMicron Technology Corp.

Case study 3: Alice and Bob

So, using a Certificate Authority prevents Eve from creating a key pair of her own, and claiming that the corresponding public key is Bob's. If Eve were to now send a business invoice appearing to be signed by Bob, when Alice uses Bob's validated public key to try and decrypt the hash and compare them, this will not work; she would know that something was wrong, and (hopefully), not transfer money to Eve.

Note that scams are increasingly being reported where fake invoices are being sent to businesses, or a senior manager is being impersonated to persuade people in the business to make payments to the scammer's account.

All businesses should ensure that all managers, directors etc. have private and public encryption keys, and that their public keys are stored and displayed locally to be used by everyone in the business.They must use their keys in order to sign and validate all non routine instructions for making payments. This is about the only way to avoid the scam reported by the BBC:

> 'Hey, the deal is done. Please wire $8m to this account to finalise the acquisition ASAP. Needs to be done before the end of the day. Thanks.'

The employee thought nothing of it and sent the funds over, ticking it off his list of jobs before heading home.

But alarm bells started to ring when the company that was being acquired called to ask why it had not received the money.

An investigation began - $8m was most definitely sent, but where to?

For the rest of the report see: https://www.bbc.co.uk/news/technology-49857948

3.3 Encrypted network connections

Figure 11

As you learned earlier, web traffic is not encrypted by default. Web pages pass as plaintext across the internet and are vulnerable to interception.

Obviously, this was a problem when companies first began to consider online shopping. At first companies had to ask customers to browse online and then make a telephone call so the company could accept credit card information.

The solution came in 1995 when the web browser pioneer Netscape announced the Secure Socket Layer (SSL) protocol, which has now been replaced by Transport Layer Security (TLS)), which allows web browsers to exchange secure data. It is supported by all modern browsers and allows confidential information to be exchanged over an insecure link.

TLS/SSL

TLS/SSL uses a combination of asymmetric and symmetric encryption to exchange data. When a web browser connects to a server and requests a secure communication the two

computers first engage in what is known as a handshake and agree how future communications will be conducted, including the type of cryptography that will be used.

After agreeing how to communicate, the server transmits its own public key and a digital certificate of authenticity to the user's computer which checks that the certificate is genuine and has not expired. If the certificate is genuine, the user's computer then generates a master secret, encrypts it with the copy of the server's public key and sends that to the server.

The server decrypts the encrypted master secret with its own private key. Both the server and the computer now have copies of the secret and use that to generate identical copies of a symmetric encryption key. Crucially, the key itself has not been transmitted across the network.

Each computer now informs the other that all other transactions in this session will be conducted using the symmetric key (called the session key), by sending 'finished' handshake messages using each other's session keys. The two computers can now perform the secure transaction itself, including sensitive information such as bank account details, addresses, credit card numbers and receipts using the high-speed symmetric key.

At the end of the secure session, the two computers say goodbye to one another and each deletes their copies of the symmetric session key. If the user starts another secure session a completely new key will be used.

TLS/SSL is now used by most websites. It is an automatic process between the browser and the server that keeps data safe in transit. It doesn't mean that any site is genuine. Any website, including criminal ones, can now implement TLS/SSL for free. However, its use means that end users can benefit from the confidentiality and integrity provided by cryptography without having to worry about the technical details of configuring their software or managing keys.

In the next section you'll see TLS/SSL in action.

3.4 How secure is your browsing?

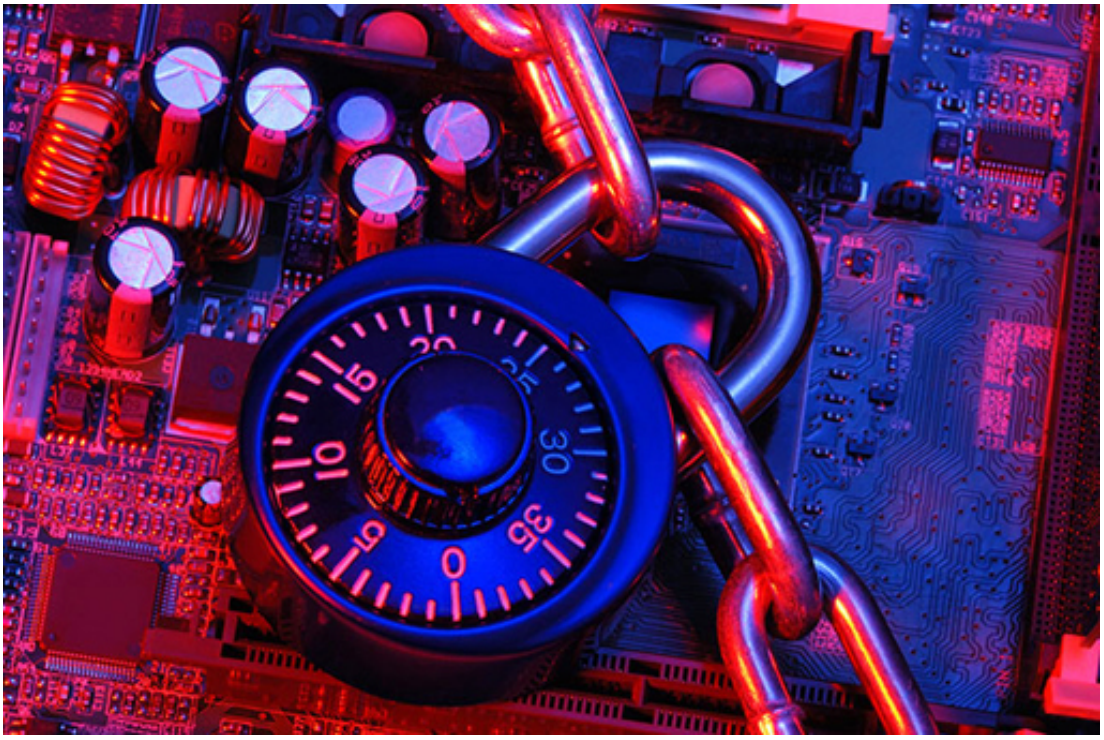


Figure 12

Web browsers have made it easy to determine if a website is using TLS/SSL by:

- Making all secure addresses begin ‘https://’ (rather than ‘http://’) with the s standing for ‘secure’. Examples include Gmail, at https://mail.google.com/; Google defaults to Google Safe Search at https://www.google.com/, which means that your search requests and results cannot be seen by others.
- Showing a closed padlock symbol in or near the top of your browser window.

Activity 2 Your own browsing security

Allow about 15 minutes

Visit a website that you use regularly (it could be this one!) and find a page that you would expect to use a secure network connection. A common example would be your webmail account or online banking website. Use your browser’s help feature and click on the padlock icon to find out about its meaning.

Research browsing security online. You might find that your browser shows different versions of the padlock to highlight potential problems with the secure connection.

Encrypted DNS

Up until 2019, the DNS information requested was sent as plain text and could be intercepted even when the data being sent or requested was encrypted. From 2019, it has

become possible for DNS requests to be encrypted. In a Firefox browser go to settings, then network settings and select the enable DNS over HTTPS checkbox.

As mentioned in Week 4, Chrome 78 is also experimenting with this feature, which can be enabled by browsing to '`chrome://flags/`' in your Chrome browser, searching for 'dns-over-https' and enabling this feature. You will have to restart the browser for this change to take effect.

4 Week 5 quiz

This quiz allows you to test and apply your knowledge of the material in Week 5.

Complete the Week 5 practice quiz now.

Open the quiz in a new window or tab then come back here when you're done.

5 Summary of Week 5

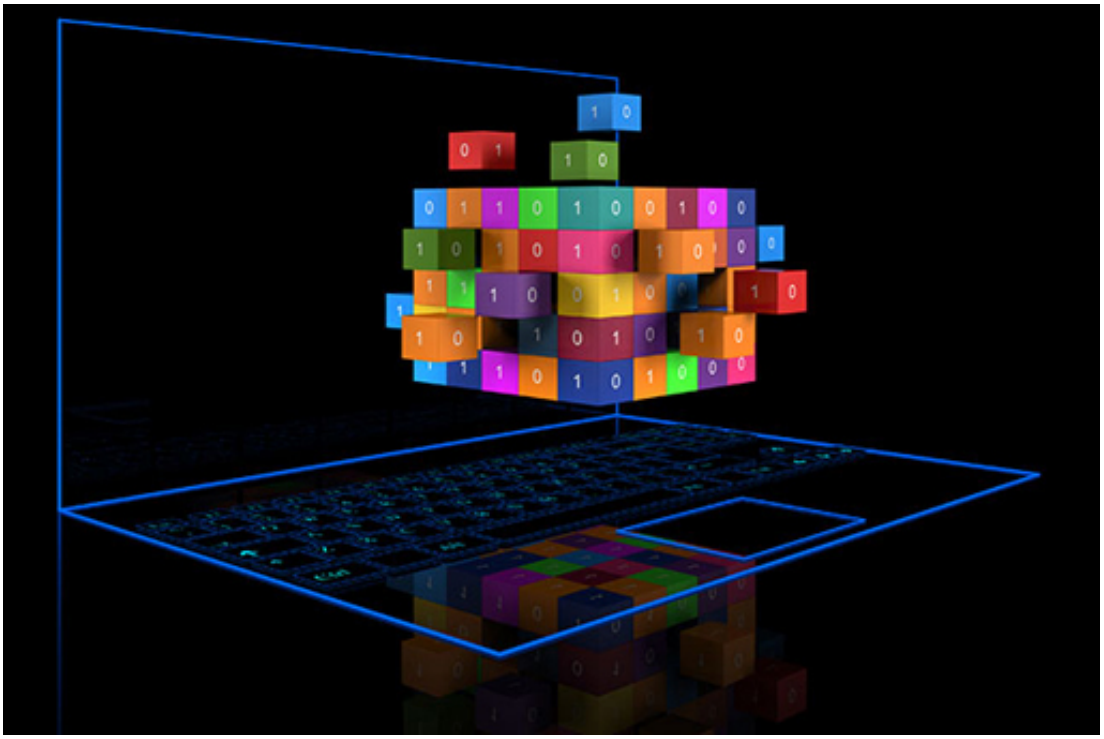


Figure 13

This week has focused on cryptography – a key security technique that allows you to ensure confidentiality and integrity of your data.

You have learned how to use cryptography tools to secure your email and can explain the use of cryptography in common applications, such as the world wide web. As a result, you should now be able to identify where you could use cryptography to improve the protection of your digital life. One example of this, the use of cryptography to protect computer networks, is the topic for the next week of the course.

You can now go to Week 6: Network security.

Week 6: Network security

Introduction

Video content is not available in this format.

Your course guide, Cory, explains that earlier in the course, you looked at a range of security techniques and technologies aimed at protecting your online identity, as well as your digital information, from malware.

This week explores different ways of protecting the underlying communication networks and computers we use from attack and you'll also configure a firewall for the computers you use.

1 Firewall basics

Figure 1

In a building, a firewall is a reinforced masonry wall that is designed to prevent a fire spreading through the structure, allowing people time to escape. Similarly, in a computer network, a firewall is a barrier that blocks dangerous communications from spreading across a network, either from the outside world into a local network, or from one part of a local network to another.

Firewalls can be supplied as dedicated network devices or they may form part of a network router. A firewall might also be included as part of a computer's operating system.

The internet existed for a long time before firewalls were invented. The first discussion of the necessary technologies took place late 1988, and came about after several attacks from organised groups of hackers and the very first malicious software.

At their simplest, firewalls block network communications by looking at the addressing and protocol information in the data packet's header. As a data packet (or datagram) arrives at the firewall's interface, the addressing (usually IP) and protocol information (usually TCP or UDP) is compared to rules programmed into the firewall's software. These rules can be supplied by the firewall's manufacturer, or more often they are created by an administrator or sometimes the user.

So if a packet originating from a hacker conducting a scan of your network or computer arrives at a firewall, it will inspect its addressing and protocol information and then compare this against its set of rules. If the set of rules say that packets from an unknown address (the hacker) are to be blocked, then the firewall may either discard the packet 'silently' or 'close' the connection with the hacker.

Most firewalls store the state of connections to determine if they represent new or existing connections. They will only allow packets belonging to a known, active connection to pass

(provided the rule set allows this). More advanced firewalls can identify the applications responsible for sending and receiving packets, allowing network managers to block applications that use excessive bandwidth – such as media players, or those widely used for distributing copyright infringing content – such as BitTorrent applications, as well as protecting from application attacks.

You'll learn what a personal firewall protects against in the next section.

1.1 Personal firewalls

Figure 2

Most operating systems come with a firewall that is installed as part of an operating system.

This firewall is only able to protect the computer it is installed on (and any devices attached to it) from an attack, so it is called a personal firewall. It is not intended to replace a network firewall which prevents attacks from outside of the network (such as from the internet).

Personal firewalls are especially useful for people with portable computers which will inevitably be connected to a wide range of computer networks. While we all hope and, to some extent, trust the people responsible for maintaining these networks to maintain a safe system, we cannot be sure that these networks are not compromised. The personal firewall on our own computers therefore adds a layer of protection between our personal data and a potentially untrustworthy (but useful) network.

Personal firewalls are the responsibility of individual computer users. If you have complete access to your computer's settings then it is entirely possible to turn off the personal firewall and leave your computer vulnerable.

First of all, you can check your own computer to see how well protected it is at the moment. To do this you can visit a website designed to probe your computer to see what it

can access and what is blocked. The site we are using is https://www.grc.com/shieldsup. Read the information on that page before proceeding.

- Start with the instant UpnP Exposure test probe. The response you want to see is: *THE EQUIPMENT AT THE TARGET IP ADDRESS DID NOT RESPOND TO OUR UPnP PROBES!*
- Next, the file sharing probe. The response you want is: *Your Internet port 139 does not appear to exist! One or more ports on this system are operating in FULL STEALTH MODE! Unable to connect with NetBIOS to your computer. All attempts to get any information from your computer have FAILED.*
- Common ports: You want to see a green 'Stealth' for the status of all ports.
- All service ports: you want to see a complete green 'Stealth' grid of all ports
- Messenger spam: I have mine turned off.

In the next sections, you'll learn how to check that your default personal firewall installed with your computer is running correctly. Once you have updated your firewall settings you can come back to https://www.grc.com/shieldsup and see if the probes are now kept out.

1.2 Configuring your own firewall

In this section you will locate the personal firewall on your own computer and, if necessary, make modifications to its settings to provide the best possible protection.

You will need to have Administrator level access to the computer you use as you will be making changes to important parts of the operating system. If you do not have these permissions, request temporary administrator rights from the machine's owner.

If your computer is in an office environment, or is supplied by your employer, please check that you are permitted to change the firewall settings before attempting this section. Many employers have preferred settings that are maintained by specialist staff and you should not attempt to change them without permission.

If you have Windows 10, your firewall should be on by default. Use the information on Microsoft's support page to check the firewall is turned on: https://support.microsoft.com/en-us/help/4028544/windows-10-turn-windows-defender-firewall-on-or-off.

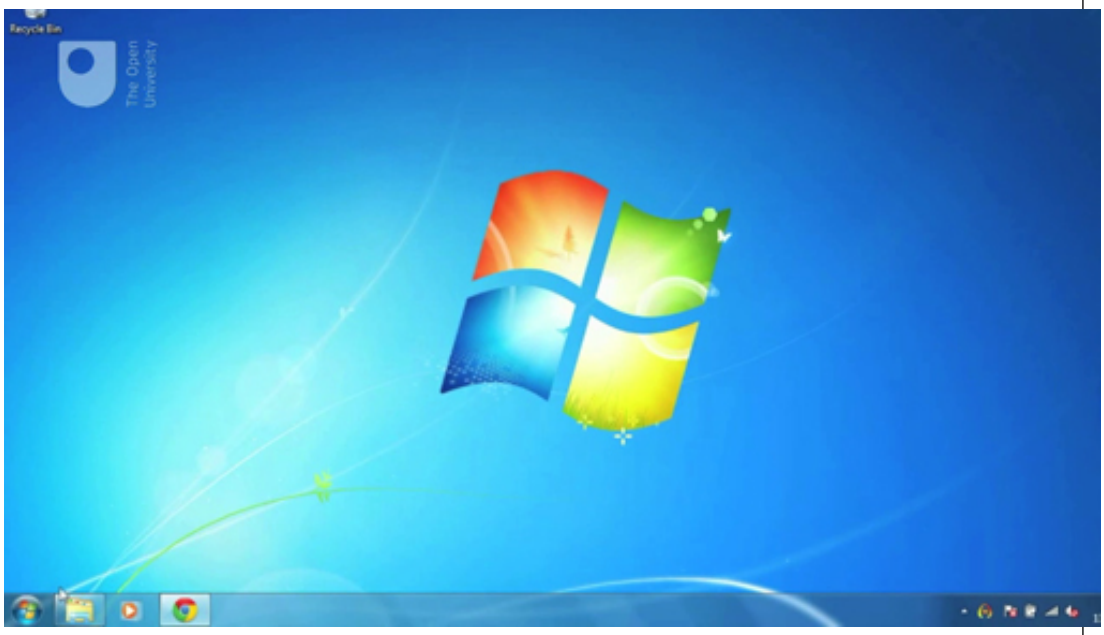
Apple takes responsibility for the security functions of their devices. You can read their latest information at: https://www.apple.com/business/docs/site/iOS_Security_Guide.pdf.

If you are using Linux you have a lot of choice about which firewall to run. See these articles for more information:

- https://www.tecmint.com/open-source-security-firewalls-for-linux-systems/
- https://www.techradar.com/news/best-free-linux-firewall
- https://opensource.com/article/18/9/linux-iptables-firewalld

Configuring your own firewall (Older Windows versions)

Video content is not available in this format.



Locate the personal firewall on your own computer and, if necessary, make modifications to its settings to provide the best possible protection.

Download the PDF of these instructions to keep as reference.

You can skip the next part, unless you also own a Mac and want to configure a firewall for this as well.

Configuring your own firewall (Mac)

Video content is not available in this format.

Locate the personal firewall on your own computer and, if necessary, make modifications to its settings to provide the best possible protection.

Download the PDF of these instructions to keep as reference.

Support on the Apple website can be found here:

- About the application firewall: https://support.apple.com/en-us/HT201642
- Change Firewall preferences on Mac: https://support.apple.com/en-gb/guide/mac-help/mh11783/10.15/mac/10.15

Other firewalls

Other firewalls are available either to download or as software packages that can be bought from retailers. Make sure that any software packages that you download have been fully evaluated by organisations that have the expertise to do such an evaluation. Apps and software that you find using a search engine, or in an Android app store may contain malware.

You may prefer to use one of these programs, but if you do, please remember:

- you should only keep one firewall running at a time since multiple firewalls will not offer significantly better protection and can interfere with one another
- you must keep one firewall running at all times.

Once you've set up your personal firewall, identify a type of traffic that you might want to allow (or deny) on your computer.

2 VPN basics

Figure 3

You've just learned how firewalls can protect individual computers and local networks from attack. Next, you'll learn about the uses of virtual private networks (VPNs).

In some ways, our local networks resemble forts sitting in the Wild West of a Hollywood movie. Inside strong walls, life goes on as normal, with data being exchanged freely between trusted machines. Meanwhile, beyond the firewall there is the lawless frontier of the internet; traffic crossing the internet must make a risky journey largely unprotected.

The problem of secure data transmission is especially acute for organisations based in several physical locations, such as those who need to exchange information with sub-contractors or those with a dispersed workforce such as sales teams or home workers.

Traditionally, companies invested in private communications links (usually called leased lines) whose cost might run to thousands of pounds per month. Most organisations cannot justify such an investment and in any case, leased lines cannot serve a mobile or highly dispersed workforce. So the lawless frontier of the internet is our only choice – this is where VPNs come to the rescue!

A VPN, as the name implies, is a means of creating a private network across an untrusted network such as the internet. VPNs can be used for a number of different purposes such as:

- to securely connect isolated local area networks (LANs) across the internet
- to allow mobile users remote access to a corporate network using the internet
- to control access within an intranet environment.

VPN concepts for a corporate network

VPNs are typically implemented using dedicated network devices (sometimes this might be a firewall) and software. There are two parts to the software; the first, called a **VPN client**, is installed on the computer of anyone who wants to be part of the VPN. The client is responsible for connecting users to the VPN so that it can send and receive information in a secure manner with, in this example, a corporate network. The second part is the **VPN server** which is part of a dedicated network device, usually located on the perimeter of an organisation's network. The server software typically performs the authentication of users and route traffic to the corporate network.

The VPN software creates a path known as a 'tunnel' between the VPN client and the VPN server. It can establish this 'tunnel' by using any third party or untrusted network such as the internet. Unlike other paths through the internet, information which passes through this 'tunnel' can be encrypted to protect it from inspection or modification. So we can use these tunnels to protect our data while it crosses the lawless frontier of the internet back to the safety of our forts!

VPN concepts for an open network

Some parts of the Internet are much more dangerous than others. In particular, public wi-fi connections in cafes, hotels, airports can allow your data to be intercepted and your movements to be tracked. Some countries also routinely monitor all Internet traffic as it enters or leaves the country as well as internal traffic.

A VPN service can offer a VPN client to run on your computer and VPN servers at safe locations around the world which provide a gateway onto the Internet. When you connect with your VPN client to a VPN service an encrypted tunnel connects your computer to the remote VPN server. It appears to the outside world as though your own computer is located at the VPN exit point in another country.

Free VPN services are available but tend to be quite slow. If personal security is particularly important take care to use a service that doesn't log user data in any way. ProtonVPN is an example of such a service https://protonvpn.com/.

VPN concepts for a personal private network

It is quite possible to install VPN server software on your own private computer at home, and leave it running when you are away from home. A VPN client software on your mobile device connects to your own home VPN server. An encrypted tunnel connects your mobile device wherever you are and gives you secure access to your home computer. To the outside Internet it appears as though you are accessing the Internet from home.

2.1 Securing the tunnels

Figure 4

The VPN path or tunnel between the VPN client and the VPN server relies on encryption to protect the data from interception or modification as it travels across the internet.

Encryption

In a VPN, encryption and decryption is typically performed by the client and server software. Early VPN solutions used proprietary encryption techniques, but shortcomings in many of these methods has forced a switch to public encryption standards.

Authenticity and integrity

It is vital to ensure that information can be trusted – that it is coming from an authenticated user and that it has not been altered in transit. VPNs use a number of methods to ensure authenticity:

- **hashes** (see Week 5)
- **digital signatures** (see Week 5)
- **message authentication codes (MACs)**.

MACs are appended to messages and act as an authenticator. They are similar in principle to digital signatures, but the hash is encrypted and decrypted using the same secret key (i.e. using symmetric encryption).

VPN protocols

There are three main forms of VPN protocol currently in use:

PPTP (Point to Point Tunnelling Protocol)

PPTP was designed in a consortium led by Microsoft, which included an implementation of the protocol as a standard component of Windows NT 4. Microsoft also released PPTP as a free add-on to Windows 95 and Windows 98, allowing users of (at the time) the most popular version of Windows to access corporate networks.

PPTP proved unsuited to large companies (being limited to 255 connections per server), but more seriously, the PPTP standard did not settle on a single form of user authentication or encryption; therefore two companies could offer software supporting PPTP, yet each product would be incompatible with the other! From Windows 2000 onwards, Microsoft replaced PPTP with L2TP (see below).

L2TP (Layer 2 Tunnelling Protocol)

This is an adaptation of a VPN protocol known as L2F originally developed by Cisco to compete with PPTP. In an attempt to improve L2F, a successor was devised by a group composed of the PPTP Forum, Cisco and the Internet Engineering Task Force (IETF). L2TP combines features of both PPTP and L2F.

IPSec (Internet Protocol Security)

IPSec was designed by an international committee (*The Internet Engineering Task Force* (IETF)) in 1992 with a first draft standard published in 1995, the revised standard was published in 1998. IPSec is now the most widely supported protocol with backing from Intel, IBM, HP/Compaq and Microsoft (among others).

IPSec has gained a reputation for security thanks to its use of well-known and trusted technologies. Rather than invent new techniques for encryption, the designers of the protocol built their system on top of existing encryption technologies, which had, in themselves been subjected to intense scrutiny.

In the next section you'll discover how secure VPN access can be.

OpenVPN

This is an Open Source VPN developed in 2004 based on the SSL/TLS protocol. It is designed to be simpler to set up and operate. More information can be found at: https://community.openvpn.net/openvpn/wiki/OverviewOfOpenvpn#OpenVPNOSS

2.2 Security risks of VPN

Figure 5

VPNs might sound like a panacea to a number of problems as they can extend, in our example, a corporate network across a wide geographic area via the internet. However, in doing so, they raise a number of new problems.

Security of remote machines

When a remote machine is part of a VPN it effectively creates a new frontier between the 'secure' corporate network and the internet. This remote machine now offers a direct route into a corporate network. Previously, it had been relatively simple to secure machines within a corporate network; now the remote user might be using their own computer, network connection, operating system and software – none of which are controlled by the organisation. Worse still, they might be sharing the machine with a number of other users, some of which might not be employed by the organisation. Perhaps the same PC is used to manage corporate documents, as well as downloading pirated music from the internet and playing video games!

The remote machines must themselves be secured from abuse. That may mean enforcing certain minimum standards with regards to operating system, antivirus software, firewalls and so on. Employers may have to stipulate that antivirus software is kept up to date, and that all patches and service packs are installed.

It might be prudent to severely limit what a remote user can access on the internal corporate network when connecting over a VPN.

Security of the VPN implementation

As you learned earlier, the security of various VPN implementations has come under scrutiny. Protocols themselves might be well designed and apparently secure, but the method of implementation, where programmers have taken shortcuts or offered 'additional convenience' to the user, may compromise the protection offered.

For instance, there are no major problems with the PPTP protocol, but Microsoft's implementation of PPTP was found to have a number of serious defects. Microsoft's implementation of PPTP was introduced in 1996, and hacker software exploiting weaknesses began circulating the following year. Papers describing the weaknesses appeared in 1998, it was only after publication that Microsoft addressed the most serious weaknesses in PPTP by releasing a patch (DUN 1.3), and even then some issues remained unresolved.

In addition to errors in protocol implementations, security vulnerabilities can be introduced if the design or configuration of the overall VPN solution is done incorrectly.

Security of interoperation

VPN is a technology with a number of competing standards, often supported by different vendors. Mixing and matching hardware and software might cause problems. Until technology matures (which is happening at a rapid rate), it might be necessary to use a single technology provider.

Security of network availability

Since VPNs typically rely on the internet for delivering information there are no guarantees about the reliability. The internet cannot guarantee delivery of information from one location to another.

In the next section you are invited to find out more about VPN and share your findings.

2.3 Putting VPN to work

Figure 6

VPN technologies have a range of applications in the real world.

Activity 1 VPN applications

Allow about 30 minutes

Find out about some VPN applications. What are the potential security problems associated with some of the applications?

Use these articles as starting points:

- https://www.pcmag.com/roundup/296955/the-best-vpn-services
- https://www.techradar.com/vpn/most-secure-vpns-best-encryption
- https://www.techradar.com/uk/vpn/best-vpn
- https://www.techradar.com/news/8-reasons-to-replace-your-vpn-client-with-openvpn
- https://www.vpnmentor.com/blog/understanding-five-eyes-concept/
- https://community.openvpn.net/openvpn/wiki/OverviewOfOpenvpn#OpenVP-NOSS

Note down your thoughts in the space below.

Provide your answer...

The TOR browser

The TOR Browser is a web browser designed to maximise the user's security against attacks on the communications between the user and the wider Internet. TOR stands for 'The Onion Router', which is a protocol where the user's traffic is encrypted and routed through three random TOR relays that could be anywhere in the world, and these relays are changed every few minutes. The third TOR relay then sends the traffic as normal HTTPS traffic without revealing the original source.

TOR can offer security over public wi-fi. An attacker monitoring wi-fi can detect you are using TOR, but that is all.

You can use the TOR browser to access secure sites over public wi-fi. In fact, using random public wi-fi sites and the TOR browser is one of the safest ways for a journalist to send communications in a hostile environment.

By using TOR browser to access ProtonMail and send or receive an encrypted email, an attacker won't be able to see that you are using ProtonMail to send and receive messages.

When using TOR, you should keep the following points in mind:

- only download the TOR browser from: https://www.torproject.org/
- don't add any 'addons' to this browser, they may break the security
- don't use a VPN as well as TOR as this may also break some aspects of security.

3 Intrusion detection system (IDS)

Figure 7

So what happens when there's an attack on a computer network? Chances are that you've seen a movie or TV programme where the administrators rush to their keyboards and frantically begin typing, lights flash, sirens sound – it's all very exciting – but does anything like this happen in real life?

As you might suspect, the answer is, no, not really. Computer networks are regularly attacked, but the response is rarely as exciting as filmmakers would like you to believe.

Intrusion detection systems (IDS) may be a dedicated device or software and are typically divided into two types depending on their responsibilities:

- **Network Intrusion Detection System (NIDS)**, which is responsible for monitoring data passing over a network.
- **Host Intrusion Detection System (HIDS)**, which is responsible for monitoring data to and from a computer.

An IDS can support a network firewall. Ideally the firewall should be closed to all traffic apart from that which is known to be needed by the organisation (such as web traffic, email and FTP). An IDS can then be used to scan any traffic passing through the firewall for potential attacks using a NIDS, as well as being able to detect those coming from within – such as from a personal computer infected with malware – using a HIDS.

Intrusion detection may be considered passive; it identifies that an intrusion is taking place and informs an administrator who must take appropriate action. However, they can also be reactive – as well as informing the administrator, the IDS can actively attempt to stop the intrusion, in most cases by blocking any further data packets sent by the source IP

address. These systems are also referred to as an Intrusion Prevention or Protection System (IPS).

Weaknesses

Automated intrusion detection systems have a number of weaknesses. They can be too sensitive, falsely reporting that an intrusion is under way, for example if a network is incorrectly configured or a buggy program begins issuing large numbers of packets.

Conversely, they are sometimes not sensitive enough to certain types of attack that proceed very slowly and do not generate enough traffic data to raise the alarm. Finally, signature IDS relies on the software suppliers issuing regular updates to the list of known signatures, until the IDS receives the update it is effectively blind to the attack.

In the next section you'll learn how IDS works in practice.

3.1 IDS techniques

Figure 8

Intrusion detection typically uses one of two techniques: anomaly detection or misuse detection.

Anomaly detection

Anomaly detection depends on the system having a model of the expected 'normal' network behaviour of users and applications. The basic assumption of anomaly detection is that attacks differ from normal behaviour. This approach has the advantage of being

able to detect previously unknown attacks by simply looking for patterns that deviate from the expected normal behaviour.

For example, consider a user who normally logs on to his computer at 9am each weekday and spends most of the morning accessing an order processing application, before taking a break for lunch. Subsequently the user accesses a number of supplier websites each afternoon before logging off at 5pm. If the intrusion detection system logs the user accessing the system at 3am and installs new software on his machine, the anomaly detection algorithm would flag this activity as suspicious.

Of course a potential disadvantage of this approach would be that some legitimate activities might be incorrectly identified as being suspicious.

Misuse detection

Misuse detection depends on the system having a set of attack patterns, or ‘signatures’, against which all network activity can be compared. The patterns of normal behaviour and attacks are configured by an administrator. Whenever there is a match between users’ activities and one of the attack signatures, or a mis-match between users’ activities and a configured normal use pattern, the system will flag that an attack is underway.

This approach has the advantage of minimising the occurrences of legitimate activity being identified as being suspicious. However, it also has the disadvantage of only being able to identify attacks where there is a known pattern, so attacks of a new unknown pattern can be easily missed.

To find out more about attacks, honeypots are used.

3.2 Honeypots

Figure 9

Sometimes network administrators want to study attacks, either so the attackers' methods can be understood more fully and countermeasures prepared, or as part of an investigation that might lead to civil or criminal prosecutions.

One method of safely studying an attack is to deflect attackers towards an isolated computer or network which appears to be completely legitimate, but is in fact a closely-monitored trap known as a honeypot. There, every action performed by the attacker can be recorded and analysed without risking important data.

Honeypots are also used by researchers to identify new attacks that are circulating in the hacking community, as well as by anti-spam organisations which use them to identify the location and identities of spam email senders.

Next, you'll have the opportunity to review your learning in the end-of-week practice quiz.

4 Week 6 quiz

This quiz allows you to test and apply your knowledge of the material in Week 6.

Complete the Week 6 practice quiz now.

Open the quiz in a new window or tab then come back here when you're done.

5 Summary of Week 6

Figure 10

This week has focused on techniques for network level protection of your digital life.

In particular you have learned the role of firewalls in protecting networks and configured a personal firewall for the computers you use. You have also learned how cryptography can be used to maintain the confidentiality, integrity and authenticity of network traffic and how networks can be automatically monitored to detect potential attacks.

You can now got to Week 7: When your defences fail.

Further reading

Vendors explain firewalls:

Cisco: https://www.cisco.com/c/en_uk/products/security/firewalls/what-is-a-firewall.html

Fortinet: https://www.fortinet.com/resources/cyberglossary/firewall.html

Checkpoint: https://www.checkpoint.com/definitions/what-is-firewall/

Palo Alto Networks:
https://blog.fuelusergroup.org/from-first-gen-to-next-gen-the-evolution-of-the-firewall

Week 7: When your defences fail

Introduction

Video content is not available in this format.

Over the past few weeks, you've learned about technologies that can help improve the security of your digital information. You now have an understanding of how cryptography helps keep information private and prevents information from being modified and how to protect networks from attack.

But, as Cory explains, information cannot be protected by technology alone and it is important to have a good awareness of what kind of things can go wrong when an attack on your information has been successful.

This week will help you to recognise the signs of an attack, to know how and where to report the problem, and to consider what you can do to recover from the security breach and stop it happening again.

1 Identity theft

Video content is not available in this format.

Identity theft is a type of fraud in which an attacker uses stolen personal information to impersonate another person. This video shows an extreme, though by no means unique, example of the possible consequences of identity theft for an individual.

Traditionally, this type of fraud was achieved by an attacker intercepting postal deliveries which contain personal information such as names, addresses, bank account details and so on. Attackers could then open credit card accounts and apply for loans in the victim's name. Victims have had their financial security and lives ruined by identity theft.

The online world has opened up a new, lucrative source of information for fraudsters. Many users have been quite relaxed about sharing their information with online services and other users, but even security conscious individuals are threatened by malware designed to sniff out personal information on a computer, or phishing attacks that persuade users to divulge personal information. Additionally, as we have seen, hacking attacks on big retailers can make millions of personal records available for potential abuse.

Online identity theft is a growing threat – in 2018, it was reported by 23% of internet users in the US according to Statista (2018).

Preventing identity theft

You can greatly limit your risk of online identity theft by following simple security procedures such as running an antivirus program, keeping it up to date and by not responding to phishing emails.

Detecting identity theft

Online identity theft may pass unnoticed for some time, during which great damage can be done to your financial security. Some signs that a victim might notice are:

- unexplained bank withdrawals or credit card charges
- bills and other expected official letters don't arrive
- cards or cheques are declined
- debt collectors make contact about debts the victim knows nothing about
- they receive notice that their information was compromised by a data breach at a company where they do business or have an account
- their bank or credit card provider makes contact about suspicious behaviour on their account.

However, you cannot do much to prevent the loss of your details by other organisations that provide everything needed to steal your identity. In 2017, Equifax, one of the three major credit reporting agencies in the US, announced a data breach that affected 143 million consumers. The hackers accessed social security numbers, birthdates, addresses, and driver's license numbers.

It is worth keeping an eye on your own free credit reports to make sure nothing unexpected is being shown that might indicate identity theft.

Next, you'll learn about what data loss can mean for organisations.

1.1 Loss of data

Figure 1 US Army Private Chelsea (then Bradley) Manning, who was at the centre of a controversial data leak to the Wikileaks website in 2009

Data loss can mean several things ranging from the destruction and deletion of data, to making unauthorised copies that are no longer under your control.

Data can be stolen by people who have direct access to a computer, such as by copying data to a flash memory drive, and also by attackers gaining access over a network connection.

Insider attacks

The hardest attack to defend against is when an attacker has direct access to a computer, especially in an organisation where many people might have access to a single computer, and one, or more, of them might not have the organisation's best interests at heart. Security risks posed by employees (or ex-employees) of an organisation to their employers are known as insider threats.

A 2013 Forrester survey of businesses employing two or more people in the UK, US, Canada, France and Germany found that 36% of information security breaches were caused by insiders and represented the leading threat to organisational security. These findings were supported in a survey of attendees to the Infosecurity Europe conference where 37% of respondents said the biggest threat to their information security came in the form of 'rogue employees'. This placed insider threats ahead of cyber attacks (19%) and device security (15%).

The pattern of attacks does change with time. In 2018, according to Statista, 56% of breaches were caused by malicious outsiders, only 7% by insiders and 34% were the result of accidental loss. However, Verizon suggested that 34% of all breaches in 2018 were caused by insiders (Verizon, 2019).

Case study: Stealing data

In 2012, a programmer for the Federal Reserve Bank of New York was sentenced for stealing source code used to develop the bank's computer systems. Bo Zhang was a third party contractor for the bank with privileged access to software that was under development. He pleaded guilty to copying the code to personal computers in violation of his contract of employment although there is no evidence that he intended to share the programs with anyone.

Similarly, in 2013, the social networking game developer Zynga settled a lawsuit with a former employee, Alan Patmore, who had copied hundreds of files, including unreleased game designs, to a Dropbox cloud storage folder before taking up employment with a rival company. Patmore expressed deep regret for his actions and agreed to ensure all copies of the data were destroyed in exchange for Zynga dropping charges against him.

In 2014, the health insurance company Anthem was breached and the details of 80 million people was extracted. This has put these 80 million people at risk from targeted phishing attacks, identity theft or extortion.

In 2017, the private healthcare provider BUPA reported that 547,000 customer details were stolen by an insider and offered for sale online.

In 2019, an employee of Tesla stole extensive details of Tesla's manufacturing systems.

India's Punjab National Bank discovered $1.8 billion in fraudulent transactions as a result of an employee obtaining a high security password.

In November 2019, Trend Micro, a global security company with over 12,000,000 customers, reported that details of 68,000 of its customers had been copied by an employee who had sold the data to criminals who, immediately started using the data in phishing attacks. The employee appears to have had detailed knowledge of the controls in place to protect that data. Trend Micro was not aware of this theft until customers started reporting phishing attacks. The information used in the phishing attacks pinpointed the source of the data, but it took a lot of time and effort to check all security systems and determine that this was an internal theft.

The case of Chelsea Manning is one of the more significant insider attacks involving the loss of data. It is another example where the attacker simply copied the data and shared it with others, depriving the data owners of control over the confidentiality of the information.

Case study: Chelsea Manning

Chelsea Manning (then Bradley Manning) was a United States Army soldier who leaked confidential information, including 250,000 United States diplomatic messages and 500,000 United States Army reports as well as videos of military action in Iraq, to the WikiLeaks website.

Manning obtained copies of classified materials during service in Iraq in 2009, copying them directly to a data CD disguised as a music disc, from which the materials were transferred to a laptop and then to the WikiLeaks servers for dissemination.

The reports were widely published around the world and caused enormous diplomatic embarrassment for the United States government. Manning was eventually identified after confessing in an online chat to Adrian Lamo, who informed the Army. Manning was charged with 22 offences, including that of aiding the enemy, and pleaded guilty to 10 charges. Manning was found guilty in 2013 and sentenced to 35 years in military prison.

Wikileaks continues to the present day to publish millions of documents that the owners had intended to be kept secret.

The site ‘';–have i been pwned?’ (https://haveibeenpwned.com/) publishes lists of the largest breaches and the most recent breaches at the bottom of its home page.

Next, you’ll find out about the risks of data loss.

1.2 Risks of data loss

Figure 2

As the case studies showed, there are serious consequences of losing data.

These consequences can be expressed as a series of costs, such as:

- the cost of recreating the lost data – either by buying new hardware and software or re-entering the lost data (which may not always be possible)
- the cost of continuing without that data (availability)
- the cost of informing others about the loss.

The costs cannot just be expressed in terms of money. For instance, the last cost, of informing others, is not just limited to, for example, postage and email charges. A company that suffers a data loss can also suffer a loss in its reputation as a professional organisation. This problem is greatly magnified if personal data belonging to other people has been lost.

Case study: Norsk Hydro

In March 2019, Norsk Hydro, one of the biggest aluminium producers in the world, was targeted by a ransomware attack using LockerGoga which encrypted a wide range of files.

Norsk Hydro had detailed plans in place and was able to limit the spread of the attack and revert to manual operation. It also had secure backups of critical files. In spite of that, the latest estimates in May 2019 put the cost at between $45.6m and $51.3m.

While they were recovering from this attack, Norsk Hydro were also aware of phishing attempts being made on their trading partners that attempted to spread the malware, and to divert payments to criminal accounts.

Norsk Hydro did not pay any ransom and provided detailed updates on its response to the attack.

Case Study: American Medical Collection Agency (AMCA) and Quest Diagnostics

AMCA was a company that ran billing and payment services in the US. In August 2018, hackers gained access to its servers and remained undetected until March 2019. The data obtained by the hackers included social security numbers, some credit card and banking details and medical data.

Quest Diagnostics was a medical company that used the services of another company called Optum360 to collect payments due. Optum360 had outsourced this operation to AMCA. Quest Diagnostics was first to report the security breach after customer details were involved in many fraudulent transactions.

LabCorp, BioReference and Opko Health were other medical companies that used the services of AMCA. AMCA filed for bankruptcy but the financial impact on the medical companies that used AMCA services is not yet clear.

The risk of data loss cannot be completely eliminated, but it can be minimised. In 2019, Verizon reported that 34% of breaches involved people inside the business, and 15% of all breaches were the result of misuse by authorised users. However, errors were the cause of 21% of all breaches.

A significant number of security threats are caused inadvertently by employees who are unaware of the risks of their actions, such as copying data to external devices or websites, opening infected emails, clicking malicious links, installing software and so on. Better staff training could reduce the risk of accidental data loss.

The Infosecurity Europe survey revealed that while a slight majority of companies had implemented an internal information security policy to secure computers, networks and data, only a minority had provided staff training to raise awareness of potential security risks. Another important way of minimising the effect of any loss is by backing up data – making secure copies of data either on to a separate device, to a separate disk, or even to a different location.

Think about identity theft and loss of data. Have you ever been affected by these issues? How would you know? Reflect on your personal experience.

- Have you checked your email on https://haveibeenpwned.com/ ?
- How would you recover if your live data was encrypted by ransomware, or simply destroyed?

2 Laws and computers

Figure 3

Now that you have a broader understanding of the kind of things that can go wrong, you'll look at some of the most important laws in the UK that help to protect us against these cyber security threats. These are the Data Protection Act 2018, the Regulation of Investigatory Powers Act 2016, the Computer Misuse Act 1990 and the Fraud Act 2006.

First though, we'll start with a brief introduction to the UK legal system. If you live outside the UK (or work with a multinational organisation) you'll also get a chance to find out what legal frameworks exist in your own country. It is still useful to learn about the UK laws so that you can look for the equivalent in your country.

Criminal and civil law

Law in Britain can be broadly divided into two categories:

- **Criminal law** is concerned with punishing behaviour that is considered unacceptable (murder, serious injury, fraud and so on). The majority of criminal cases are brought by the State against individuals and companies and require a high standard of proof to secure a conviction ('beyond reasonable doubt'). Criminal cases can punish guilty parties with either fines or imprisonment, depending on the nature and severity of the offence.
- **Civil law** is concerned with disputes and these are usually brought before the court by individuals. Civil cases concern (among other things) property law, contracts and noise. There is a lower standard of proof ('on the balance of probabilities') than with criminal law and punishments are usually financial in nature.

Bills, Acts and Laws

An **Act of Parliament** is a law that has been approved by the British Parliament (Britain has a second type of law that has not been passed through Parliament known as Common Law).

An Act starts as a draft called a **Bill** which is debated in the elected House of Commons. If it is approved, the Bill is passed to a specialist committee made up from Parliamentarians for revision. Their changes are discussed further in the House of Commons and possibly revised further.

After a formal vote, the Bill passes from the House of Commons to the House of Lords for further scrutiny and possible amendments. The Lords will vote on the Bill before returning it to the House of Commons which considers their amendments. If the two houses agree (and sometimes they do not), the Bill is given Royal Assent and becomes an **Act**.

Some Acts take immediate effect, but often there is a delay between enactment and implementation as there may need to be processes put in place in order to achieve compliance.

So a Bill does not become law until it becomes an Act.

Keeping up with threats

It is worth remembering that cyber security is a fast moving area and therefore, legislation is constantly being revised based on new threats and court cases. In particular, the outcomes of trials can result in changes to the interpretation of existing laws as well as prompting creation of new laws. Additionally, because cyber threats are global, they can be affected by legislation from other jurisdictions.

Case study: Gary McKinnon

In 2002, the British hacker Gary McKinnon was accused of ‘the biggest military computer hack of all time’ against US Department of Defence and NASA computer systems, resulting in a demand for his extradition to the United States.

McKinnon fought extradition for 10 years, including an appeal to the House of Lords and the European Court of Human Rights, until the British Government blocked extradition in late 2012. He was not prosecuted in the UK due to the logistics of moving evidence and witnesses from the United States, the passage of time and the difficulties of bringing a case in England and Wales.

2.1 Data Protection

Figure 4

The original Data Protection Act (DPA) became law in 1984, which established legal obligations for organisations to act responsibly with respect to personal information. This UK's Data Protection Act 2018 (DPA 2018) replaces earlier data protection legislation to make UK law align to the requirements of the EU's General Data Protection Regulation (GDPR).

GDPR replaces both national data protection legislation and a previous EU law going by the unwieldy name of Data Protection Directive 95/46/EC. GDPR provides a single set of data protection regulations across all EU member states. The introduction of a single EU-wide data protection regime is essential for any business or organisation wishing to operate across national boundaries, since differences in national data protection laws could mean that a data processing operation which was legal in one country would be illegal in another.

GDPR protects EU citizens from abuses of data privacy by companies based in their own country as well as those based in member states. Additionally, any company wishing to process personal data of EU citizens, no matter where they are based in the world, will be obligated to obey GDPR. In the UK, the Information Commissioner's Office (ICO) is the **Statutory Authority** (SA) responsible for enforcing the requirements set out in the GDPR.

The DPA 2018 increases the responsibility on companies to ensure personal data is protected at all time. GDPR requires all organisations employing more than 250 people to have at least one **Data Protection Officer** (DPO) responsible for developing that organisation's data protection policies and ensuring that it is compliant with GDPR. This represents a major change from the DPA which does not require organisations to employ DPOs.

Under the older DPA legislation, businesses were encouraged to report data breaches to the Information Commissioner but were under no obligation to do so. The DPA 2018 not only forces companies to report breaches, but they must inform the SA within 72 hours of the incident being discovered (the actual breach might have taken place long before but gone undiscovered).

Penalties

Alongside greater requirements for organisations to protect data, the GDPR increases the penalties on those that fail to do so with a set of escalating penalties:

- a written warning for relatively minor breaches, first offences or unintentional non-compliance;
- regular data protection audits to ensure a business that experienced a breach has come into compliance with GDPR;
- a fine up to €20 million or 4% of a business's annual global turnover – whichever is *greater*. (Remember, the DPA has a maximum fine of just £500,000).

Pseudonymisation

One area of change in the DPA 2018 is where personal identifiers, such as a person's name, address or social security number is replaced with a new tag to protect that person's privacy; a process known as **pseudonymisation**.

Pseudonymisation is widely used where personal data is exchanged between organisations. An example might be a hospital patient receiving novel treatment. Their patient record containing their genuine name and address is used by their doctors, but a pseudonymised record with a random name might be shared with medical researchers.

Unfortunately, pseudonymisation is not perfect, it can be defeated relatively easily either if the original records are stored without the proper level of security, or if the algorithm that converts genuine personal data into pseudonyms is unsecured. As part of its implementation of GDPR, the DPA 2018 places new responsibilities on organisations using pseudonymisation to ensure that it is not possible to for attackers to easily deanonymise personal data.

The right to erasure

Many people have previously done or said something that now causes them great embarrassment, or which harms their prospects of a settled family life or employment. In previous generations, many of these indiscretions would have been forgotten in a few years, but digital technologies, especially social media, allow people's past failings to come back to haunt them. An example might be a petty crime, such as vandalism, committed by a child who was punished by a court whose hearing was reported by a local newspaper. A few years later, the same individual stands for public office, and is the subject of attacks over their 'criminal history' by political opponents and a hostile media.

A concept of 'the right to be forgotten' was drafted by the European Commission in 2012 which would allow people to request personal data to be removed from search engines and websites because it was untrue or no longer relevant. The GDPR has adopted a more

limited ‘right to erasure’ which will allow people to have personal data removed from computers either if the data was acquired by illegal methods (such as by hacking or unauthorised disclosure), or if the privacy of the person in question is seen to be more important than the interests of the organisation storing their data.

Data protection by design and by default

The Data Protection Act 2018 introduces a requirement on the developers of new data processing systems that they consider the privacy implications of using the system at the outset rather than once it is complete. As part of this, the act requires data processors to process as little personal information as possible to complete a task, requires organisations to delete data when no longer needed for its original purpose and forbids data being passed to other organisations without permission.

With the principles of GDPR included in the UK's 2018 Data Protection Act, they will continue to be important requirements for systems that collect and process UK citizen's data irrespective of the UK's membership of the European Union. It is also important to note that the Act is not limited to enacting the provisions of the GDPR and that it includes aspects for data collection and processing which fall under UK national jurisdiction – such as those relating to immigration and law enforcement.

Next, you’ll learn about The Investigatory Powers Act.

2.2 The Investigatory Powers Act 2016 (IPA)

Figure 5

The Investigatory Powers Act 2016, governs the use of surveillance technologies by public bodies such as the police, the intelligence services and local authorities. It updates

a previous law, the Regulation of Investigatory Powers Act 2000, which was often referred to as RIPA.

Like RIPA, the Investigatory Powers Act (IPA) ensures intrusive powers are subject to strict safeguards. These covert surveillance powers include intercepting communications, using bugs, covert CCTV and undercover agents.

The use of IPA is overseen by the Interception of Communications Commissioner, together with additional judicial commissioners who will be appointed to oversee different aspects of the law. The Investigatory Powers Tribunal, which comprises independent senior lawyers and members of the judiciary, can hear complaints relating to the exercise of powers under the Act.

IPA allows certain public bodies to access communications records from communication providers, such as telephone companies and internet service providers, when necessary and proportionate to do so for a specific investigation. These records may include the names, addresses and telephone numbers of individuals, the time and duration of calls, the source and destination of emails and the location of mobile devices. The IPA extended the record collection powers of RIPA to include a requirement that communications companies retain up to 12 months of data on websites (but not specific webpages) visited by customers.

More intrusive techniques are subject to higher levels of authorisation. Another section of IPA stipulates that the interception of the contents of a communications (such as telephone calls, emails and the details of specific webpages visited) must be authorised under a warrant issued by the Secretary of State. These include “equipment interference” warrants, which would authorize police and intelligence officials to change the operation of targeted computer systems to enable data collection or other surveillance activities, effectively ‘hacking’ these systems to support investigations.

Next, you’ll find out about The Computer Misuse Act.

2.3 The Computer Misuse Act 1990 (CMA)

Figure 6

The Computer Misuse Act 1990 (CMA) is one of the most influential pieces of legislation relating to computers. It has been updated and amended by a number of other acts:

- Criminal Justice and Public Order Act 1994
- Criminal Justice (Terrorism and Conspiracy) Act 1998
- Police and Justice Act 2006
- Serious Crime Act 2015

It has been the inspiration for similar laws being introduced in other countries.

The CMA came about, in part, because of a 1988 case where two hackers broke into the British Telecom Prestel network and obtained access to user accounts including that of Prince Philip.

Prestel was a text-based interactive information system developed by the UK Post Office in the late 1970s. Users could browse numbered pages of text (similar to the contemporaneous Ceefax and Teletext information services) on their television as well as send electronic messages to other Prestel users. Prestel services were expensive and the system did not become widely used, although Prestel technology was sold to many other telecom companies. Prestel was gradually sold off in the early 1990s as the internet became available to domestic users.

The two hackers were originally tried and convicted under a law concerned with forgery and counterfeiting, but the conviction was overturned by higher courts who concluded that the Forgery and Counterfeiting Act 1981 had never been intended to be used for this purpose. This led the majority of legal experts to conclude that hacking was not actually illegal in Britain at the time.

The CMA was drawn up hurriedly and was criticised at the time for not being adequately scrutinised, but its central aims have stood the test of time. The original Act introduced three new criminal offences:

- unauthorised access to computer materials
- unauthorised access with intent of committing or aiding further offences
- unauthorised modification of computer material.

Note that 'unauthorised' in this context means that the attacker must be aware that they are not intended to use the computer in question. So using another person's account details, or breaking in to a computer by a password attack are clearly unauthorised use of the computer.

The CMA has been amended a number of times to cover new offences including denial-of-access or denial-of-service to legitimate users (making denial-of-service attacks a criminal offence in the UK), and criminalising the creation and supply of software and hardware that might aid an attack on a computer. This not only criminalises the development of programs designed to break passwords or the development of certain types of malware, but it could potentially criminalise tools used by forensics experts to investigate computer systems which can be abused by attackers.

The CMA has been successfully used in a wide range of criminal cases including denial-of-service attacks against Kent Police, Oxford University, the United States Air Force, the CIA, Sony and Nintendo; fraudulent activities in online games; illegal access and disclosure of confidential emails and personal information; theft from online banks; stalking; hoax calls to emergency telephone numbers and piracy.

The next act you'll find out about is The Fraud Act.

2.4 The Fraud Act 2006

Figure 7

The Fraud Act 2006 was introduced to simplify a notoriously complex Act of Parliament called the Theft Act.

The previous law defined a large number of types of fraud, often tied to specific circumstances, that made for complex cases that were difficult to prosecute and for juries to understand. In fact, it wasn't until 1996 that obtaining money from a fraudulent bank transfer was specifically illegal in the UK!

The Fraud Act defines fraud in three ways:

- false representation
- failing to disclose information
- abusing power.

In each case, the defendant's conduct must be dishonest with the intention of making a gain, or must cause a loss (or the risk of a loss) to another person or individual. Crucially, no actual gain or loss needs to be proved – the fraud might have been unsuccessful or it was stopped before it could take place.

The Fraud Act can be used against anyone attempting to perform fraud whether or not it takes place over the internet. However, Section 11 of the Act makes specific reference to electronic fraud and can be used to prosecute in response to:

- dishonestly obtaining electronic communications services such as a telephone, ISP or satellite television subscription
- cloning mobile phones so that calls made on one handset are billed to another
- reprogramming mobile phones to interfere with their operation or change their unique identifier information

- breaking encryption on encrypted communications services such as subscription television services or telephone conversations.

In the next section you'll learn about Lawful Business Practice Regulations.

2.5 Lawful Business Practice Regulations

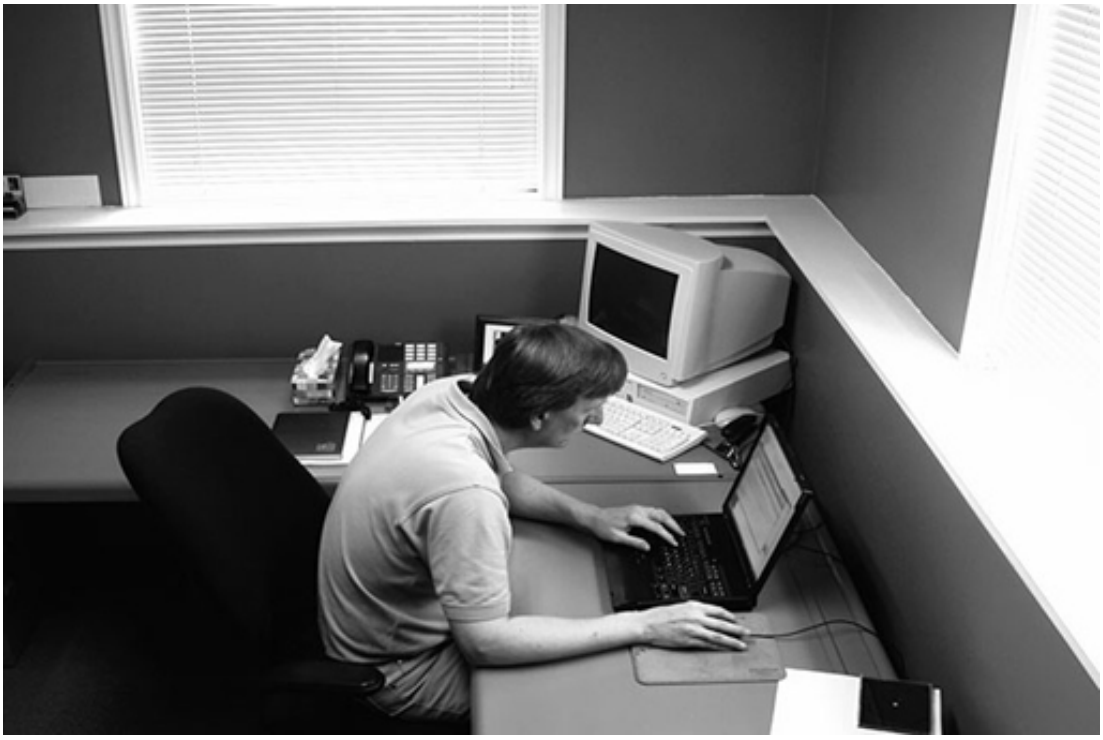


Figure 8

Under UK law, employers have certain rights to monitor communications made by their employees.

They are authorised to do so under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 SI 2000/2699 (sometimes abbreviated to IC Regs). Monitoring can take many forms including recording telephone calls, storing telephone numbers, email addresses and website addresses, storage of email and the inspection of any email attachments.

The regulations exist so that employers can ensure that their networks are used in a manner that does not bring the company into disrepute (such as sending offensive emails would), be used for illegal activities (such as transmitting copyright materials without licence), or to check that company resources are not used for personal reasons.

Companies may also have to monitor their networks to meet legal regulation – such as in the case of financial organisations where 'health warnings' must be offered to customers – and in extreme cases, monitoring may take place in support of national security.

The IC Regs are an exception to the general understanding that it is unlawful to intercept any communications unless an individual or organisation is specifically authorised to do so. This is codified in RIPA – see Investigatory Powers Act 2016 (https://www.legislation.gov.uk/ukpga/2016/25/section/1/enacted and https://www.gov.uk/government/collections/ripa-codes). The IC Regs allow interception to

be made under specific conditions, but only if both parties in the communications consent to it happening. Such consent may be a necessary condition of employment, or it might be an additional agreement between an employer and their employees.

Monitoring of employees is an activity that must be done with care since it has the potential to erode trust between management and workers as well as being intrusive. Employers must abide by legislation including the Human Rights Act and the Data Protection Act to ensure that interceptions take place in a proportionate manner that any intercepted data is used for the correct purposes and that personal information is stored and processed appropriately.

Next you can complete an activity to check what you've learned about cyber security and the law.

2.6 Cyber security and the law

Check what you've learned about cyber security and the law by completing this activity.

Activity 1 The law

Allow about 5 minutes

Q1. Consider a scenario:

A hacker steals the customer database of an organisation by exploiting a well-known vulnerability in their computer systems. This vulnerability hadn't been fixed by the organisation despite the IT department being aware that there was a patch to fix the problem.

In the UK, under which of the following laws would the organisation have committed an offence?

○ Computer Misuse Act

No, the organisation has not made unauthorised use of any computer systems.

○ Data Protection Act

Yes, in failing to patch their software against a known vulnerability, the organisation has not taken adequate measures to secure the personal data of customers and therefore failed to meet its obligations under DPA.

○ RIPA

No, there is no cause to use provisions from the Regulation of Investigatory Powers Act.

You may find 2 Laws and computers useful.

○ Fraud Act

No, the organisation has not committed fraud.

You may find 7.2 Laws and computers useful.

Q2. Thinking about the same scenario:

A hacker steals the customer database of an organisation by exploiting a well-known vulnerability in their computer systems. This vulnerability hadn't been fixed by the organisation despite the IT department being aware that there was a patch to fix the problem.

In the UK, under which of the following laws would the hacker have committed an offence?

- Computer Misuse Act

Yes, by gaining unauthorised access to a computer system the hacker would have committed an offence under this act.

You may find 7.2 Laws and computers useful.

- Data Protection Act

No, the hacker is not bound by the provisions of the DPA.

You may find 7.2 Laws and computers useful.

- RIPA

No, this is an act that gives law enforcement authorities the power to intercept communications as part of an investigation.

You may find 7.2 Laws and computers useful.

- Fraud Act

No, the unauthorised access to the customer records, in itself is not fraud.

You may find 7.2 Laws and computers useful.

Next, you'll think about European laws and consider laws that apply in other countries.

2.7 Cyber security in the EU

Figure 9

In 2017, the European Union (EU) introduced a new framework for cyber security in the EU. This included a new EU Cybersecurity Agency to improve the sharing of threat intelligence and knowledge, to organise and run pan-European cyber security exercises and to ensure that all serious incidents are fully reported. It would also implement an EU-wide certification framework to ensure that all products and services in the EU are secure from cyber-attack. It is also introducing measures to combat fraud and the counterfeiting of non-cash means of payment.

On 10 December 2018, the European Parliament, the Council of the EU and the Commission agreed on the Cybersecurity Act, which reinforces the mandate of the EU Agency for Cybersecurity, (European Union Agency for Network and Information and Security, ENISA) so as to better support Member States with tackling cyber security threats and attacks. The Act also establishes an EU framework for cybersecurity certification, boosting the cybersecurity of online services and consumer devices.

The text of the EU Cybersecurity Act is available here: https://eur-lex.europa.eu/eli/reg/2019/881/oj. An infographic of the act is available from: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-glance.

In the next section, you'll be invited to find out about similar laws in a country of interest and share your results with other learners.

2.8 What laws apply in your country?

Figure 10 British hacker Gary McKinnon, accused of accessing US Department of Defence and NASA computer systems, seen here outside the Royal Courts of Justice in January 2009 as he was fighting extradition charges

If you live or work outside the UK, or work in a multinational organisation or have links with another country, you might be wondering if there is an equivalent set of laws in your country of interest.

Activity 2 Laws in other countries

Allow about 20 minutes

Carry out some research into similar laws that might exist in the country you are interested in and note down the results in the space below.

Look for laws that address one of these aspects of information security:

- data protection relating to living individuals
- misuse of computers
- investigatory powers
- fraud.

Find out:

- if equivalent laws exists
- what are they called

- what the differences are.

Based on your research, does it seem that the laws in other countries are similar, different or non-existent?

Provide your answer...

3 Who should you contact?

Figure 11

So far this week, you've taken a broader look at the threat landscape that was introduced in Week 1 and learned how to recognise when you've suffered a successful attack on your information security. You've also learned about the laws in the UK (and in your own country) that are in place to protect you.

The rest of this week focuses on how to recover from the attack and what you can do to prevent a similar attack being successful in the future.

First, let's consider who you need to tell about the attack and what they need to know.

Responding to identity theft

If you have lost important documentation (such as passports, driving licences, credit cards and cheque books) you should report them immediately to the issuer so that they can be blocked and new copies can be issued to you. You should also report their loss to the police and ask for a crime reference number.

Report any unexplained transactions to your bank or credit card issuer so that they can be investigated by the company's fraud team. You may not be liable for any losses provided that you have acted in a responsible manner and without fraudulent intent.

Almost everyone in the UK has a credit report registered with a credit reference companies. A credit report is used by financial agencies to determine your suitability for financial services such as a credit card, bank loan or mortgage. Every time a user (or an impersonator) requests a new financial product, a credit search is made and included in the credit report. You can ask for a copy of your credit report from a credit reference agency (in the UK they are Callcredit, Equifax and Experian) which will list all searches

made on that account, who authorised the search, what type of search was made and when it was performed.

Credit reference agencies can also provide a credit report checking service (for which they may charge) which keeps a track of any changes to your credit report.

For more information see ActionFraud.

Personal data and security

If you have accidentally opened a suspicious email message

Don't click on any links and don't open any attachments. Don't use any links sent to you in an email to log in. Run a scan with your anti-malware software. Use links that you have previously saved in your browser bookmarks to visit any sites you need to check. Don't be shocked into immediate action by anything you read in an email.

Bank card fraud

If you notice a charge on your card account that you didn't authorise, contact your card issuer as soon as possible. It may be that you've paid for goods you've not received or are suspicious about a website you've used. Give the card issuer as much information as possible – the name of the website, how much you spent, when you did it and so on.

The card issuer will investigate all cases of possible fraud and give you guidance which you should follow exactly. You may have legal protection, which means you're not liable for any losses, as long as you took reasonable care and did not act fraudulently. Note that using PayPal does not give you the same legal protection as using a credit card.

You should also contact the police and complete a crime report. Visit the UK Police's website for reporting online fraud at ActionFraud.

Don't respond if you get email or a phone call saying they are from your bank and they have detected fraud on your account. Don't confirm anything! Don't press any phone keys. Just end the call. Don't call any number they might give you for further information. Put down the phone. Dial your saved message service or another free service just to confirm that the caller has released the phone line.

Look up the contact details for your own card issuer, check your own account, and if there seems to be a problem you can call the safe number that you already have.

Next, you will find out how to get your computer working again after an attack.

3.1 Getting your computer working again

Figure 12

You've realised you have been the victim of a cyber security attack, you've reported it, now what? How do you get your computer working again? If you wait until you have been attacked you may have left it too late. Before you get attacked:

- make a note of all software that you use and all licence keys. Store these separately from your computer
- keep all your data backed up on a write only system
- check that you can install all software and data onto a new system before you get attacked.

Recovering from a virus or other malware

Your aim is to update your antivirus software then isolate your computer so that the malware doesn't spread.

On Windows 10, run the Malicious software removal tool: https://support.microsoft.com/en-us/help/4026667/windows-10-how-to-remove-malware-or-viruses.

If you have suffered a ransomware attack you may be able to use information provided by https://www.nomoreransom.org/ to recover your data. This is a scheme set up by Europol, the Netherlands Police, McAfee and Kaspersky to analyse ransomware and identify the decryption keys to recover data (see https://www.bbc.co.uk/news/technology-49096991).

In a worst case scenario, you may need to reformat your hard drive, reinstall your operating system and reinstall your keys. You will then need to reinstall any programs you

use and then your data from your secure backup files. (You have got them all safe haven't you?)

Note that the reason for a slow running, old computer can be a build up of dust in vents, fans and internal surfaces so that the processor slows down to avoid overheating.

Once you have completed these steps, spend a few minutes thinking about how the malware might have got on to your computer. Did you visit a suspicious website, download a suspicious program or simply click on an attachment in an email message? These are common ways to receive malware, so think about what you can do differently to prevent it happening again.

Recovering from accidentally deleting a file

Deleting a file isn't necessarily permanent. If you have simply moved a file to the trash can (Recycle Bin on Microsoft Windows), then you can recover it by simply dragging the file out of the trash. However, if you have since emptied the trash you will need specialised software to recover the file. The good news is that the data is still on the disk, the bad news is that the operating system cannot find it again. Fortunately, special file recovery software exists that can restore deleted files. Find out about the software available from *About Technology*'s article 19 Free Data Recovery Software Tools.

Stop using the computer immediately you realise the file has been deleted. The less time that has elapsed between deleting a file and trying to recover it, the greater your chance of recovering the whole file. If significant amounts of time have passed, only a partial recovery may be possible, or it may not be possible to recover the file.

You then need to install a file recovery program (some file recovery applications can be run from an optical disk or a flash memory drive). A good selection of free file recovery applications can be found on *About Technology*. Run the file recovery application once you've installed it.

Note: Because of a difference between the way in which Microsoft Windows and Apple Mac OS store files on a disk, file recovery is much easier for Windows computers than Macs. A number of file recovery applications exist for the Mac, but there is much less selection than for Windows.

Once you've got your file back you might want to review your data backup strategy to prevent a future accident.

Recovering from a lost computer, disk or flash memory drive containing confidential data

The first question to ask is, was the data encrypted using a form of strong encryption? If it was, does it require a strong password to decrypt it? Is the password known only to you?

If the answer to any of these questions is 'no' then you may have a problem as the data is potentially vulnerable. If the lost property contains personal information, then you have an obligation to act under the Data Protection Act. Larger companies will have staff responsible for ensuring compliance with the DPA and you must get in contact with them as soon as possible so that steps can be taken to protect individuals. Alternatively, you can contact the Information Commissioner's Office for guidance.

If you have lost material containing confidential information about a company or other organisation, or which is sensitive, then you need to contact the organisation which owns the data so they can take necessary steps. In certain circumstances, this may also require the involvement of the police or security services.

If the data is securely encrypted, then the data is almost certainly safe. You should still contact the relevant authorities to inform them of the loss.

Recovering from an operating system failure

If you use a version of Microsoft Windows (XP or later), you could use the 'Restore Point' feature to revert your computer to a previous working state. Windows automatically saves its configuration daily, when it updates itself and also when certain events, such as the installation of an unsigned driver for a peripheral device, occur.

Versions of Mac OS (10.5 or later) include a feature called Time Machine, which can be used to backup both files and system configurations. If you have Time Machine enabled it is possible to restore your Mac to a previous state, with hourly backups available for the past day, daily backups for the past month and weekly backups for anything older.

In the next section, you'll consider how to make your information less vulnerable to attack.

3.2 Making your information less vulnerable

Figure 13

Some simple steps to make your information less vulnerable to attack in the future.

User accounts and passwords help secure data so that it can only be seen and used by authenticated users. Without a user account and password, an attacker is forced to use much more time-consuming techniques to break into the machine, greatly increasing their risk of being caught.

If you haven't already done so, it is time to configure your computer and mobile devices so that they require a login or passcode when you switch them on and that they lock when left for a certain period. This will prevent anyone tampering with them or impersonating you on social media if you leave them unattended.

Don’t forget to change the default password on your router as well – and keep a note of the password. A network firewall installed on a router and a personal firewall on the computer itself will stop hackers from getting into your computer. Likewise, up to date antivirus software can stop malware from deleting, encrypting or transmitting your files over the network.

If you have very important files that cannot be shared, then you should consider encrypting documents when they are not actively being edited. VeraCrypt is an example of secure encryption software that can be used to secure any files containing confidential data (see https://www.veracrypt.fr/en/Home.html).

User accounts

All modern operating systems allow for different user accounts to be created with different levels of access. These range from a guest who can only perform a small number of tasks and cannot change any important settings, through to an administrator who can install new applications, see any data on the computer and make major changes to settings. In between, are user accounts that have limited access and do not usually allow users to install new software – helping to prevent malware infections.

Even if you are the only user on a computer it can make sense to use a user account for day to day purposes, only using the administrator account as and when new software needs to be installed or the operating system is updated. Never use an administrative account for surfing the web or opening emails.

User accounts can be used to restrict access to files, printers and other resources on a local area network.

File permissions

Every file and folder on your computer has a set of permissions that tell the computer’s operating system what can be done with that file:

- write permission – the file can be edited
- read permission – it can be copied
- execute – the file can be executed as a program (if applicable).

Different users have different sets of permissions – so you may have read and write access to an important document, but you can restrict others to read only (i.e. they cannot edit the file), and deny access entirely to people outside of the group.

Remember, read permission allows a file to be copied and to be read. An attacker can still then use copy and paste to copy important information from a document, or to make a copy of the original and to edit that instead.

Disabling ports

Almost all modern computers come with one or more USB ports through which data can be stolen using flash memory drives, a plug-in hard disk or smart phone or media player. It may be necessary to disable these ports for security reasons.

Data Loss Prevention (DLP) software can temporarily disable the USB ports, or monitor or restrict the copying of files to USB devices.

Locks

The easiest way to steal a large amount of data is to simply steal the computer or the database server itself. Most computers and some external devices have sockets into which a lock, usually attached to a flexible metal chain that is secured to a wall or a desk, can be attached. Also check that a locked computer prevents a thief from opening the computer and simply unplugging data drives and removing them. Any networked storage devices should be in a locked room or a locked cage secured to a wall or floor.

Obviously, if you are working in a shared environment, locking doors and windows is an obvious deterrent to attackers, as is challenging unknown individuals who might be wandering around.

In the next section, you'll create a personal recovery plan.

3.3 Protecting your data for the future

Figure 14

If you have not already done so, now is the time to consider making computer backups.

Backups protect us from threats including:

- accidentally deleting a file or program
- losing disks, computers or memory cards
- hardware failures such as a hard disk crash
- software bugs that prevent data being written to a storage device or cause it to be corrupted as it is written
- disasters such as fire or flooding
- crimes including terrorism, theft and acts of sabotage such as hacking.

Activity 3 Protection for the future

Allow about 30 minutes

Evaluate the list of digital information that you compiled in Week 1 and decide which is the essential data and software that should be safely and securely backed up.

For each type of data you should evaluate how often it should be backed up.

For example, you don't need to back up software like Windows 10, because you can always download it again from Microsoft. However, you do need to make sure that your Windows 10 keys are backed up as you would need these to reinstall Windows.

If you run a business and have purpose written software it might be essential to have a securely stored backup in case it needs to be reinstalled. This might need to be backed up just one time if it doesn't change.

If you write long documents or are handling many transactions a day it could be very important not to lose any. You might want to run a system that keeps a protected backup every time data is changed. This might involve logging all changes to a database on a separate system.

A home user might decide that they want to backup all images to a separate hard drive at full resolution, and to a cloud store in reduced resolution.

In the next sections you will look at how and where you could store your backup data.

3.4 Backup media

Figure 15

It is important and recommended that you have three copies of any important data. One copy for use, one copy as backup and one copy that is stored in a different building.

Depending on the amount of data you need to backup, a range of technologies are available:

Optical storage

Optical storage is the same technology used for CDs, DVDs and Blu-Ray.

The most common technology for optical storage is writeable DVD standards including DVD-R, DVD+R, DVD-RW, DVD+RW and DVD-RAM. Most of these DVD formats can store 4.7 GB on a single disc, although newer, so-called, dual layer discs and drives can store twice that. Blu-Ray technology offers 25 GB and dual layer (50GB) formats with three layer 100GB discs, although they are expensive.

Optical storage is much more bulky and more expensive per GB than the largest hard drives, but comparable in price to smaller hard drives.

Advantages

- Write once writable optical storage is particularly useful as protection of data against malware that encrypts data.
- Some optical discs using gold have a very long life expectancy for archived data if stored at 50% humidity in the dark at a stable room temperature. Each disc should be in a case stored vertically.
- Optical drives and media are extremely cheap and widespread. Most computers have an optical drive or can accept a USB driver and the discs can be bought in supermarkets.
- There are a large number of manufacturers, so there should be no problem with future supplies of discs.
- More modern optical disc technologies (such as Blu-Ray) also support most older types of disc such as DVD and CD.
- The media is robust. Discs can be posted and are able to survive regular use or being dropped. They are immune to strong magnetic fields.

Disadvantages

- Optical drives are relatively slow compared to hard disks, especially when writing data.
- There are a large number of types of disc (especially recordable DVDs). Some of these discs are not widely supported.
- Their capacity is relatively low compared to hard disks. A 1TB hard disk is commonplace on modern computers, so it would take more than 200 DVDs to make a complete backup of the disk. Consequently, DVDs might be best suited to making backups of key data.

Magnetic disks or hard drives

Hard drives are available to store 4TB or more. These are increasingly reliable and the best have a risk of failure of about 0.33% a year (but not when being moved around). Hard

drives offer the lowest cost storage per GB. Don't rely on magnetic discs to archive for much over 5 years – copy to new hard drives every five years.

The magnetic hard disk at the heart of most computers can also be used as a backup device. Most PCs have sufficient internal space for a second hard disk that can be devoted to backups, or a relatively cheap external hard disk can be connected to a USB or Firewire port on a computer.

More expensive disks can be connected directly to a network using Ethernet or wi-fi in which case they are known as Network-Attached Storage (NAS). Disks can be made more resilient to failure by combining several disks together with copies of data stored on multiple disks so that even if one copy is damaged or the disk fails, it is not lost forever; the most common type of this 'redundant' storage is called a Redundant Array of Independent Disks (RAID).

Advantages

- Disks are relatively cheap and capacities are growing rapidly.
- External hard disks can be easily moved between computers.
- There are many disk manufacturers, all of whose products can be used in almost any computer.
- There are a large number of backup programs designed to be used with hard disks. Many external disks are sold with applications to ease the backup process, or offer a 'one touch' backup button.
- Large hard discs are cost effective for archiving data for a few years.

Disadvantages

- Hard disks are fragile and easily damaged if dropped or exposed to extremely high temperatures or magnetic fields.
- If small hard disks are used once to make a backup then archived, the replacement cost is much higher than for tape or optical media.

Solid State Disks

Solid State Disks (SSDs) and memory cards are storage devices that can store data in memory chips without the need for a power source. Capacities up to 1TB are available. The name is somewhat misleading because these devices don't actually contain physical disks. They can be commonly found in the USB memory sticks used for sharing files between computers. As the technology has advanced to increase the storage capacity of SSDs they are now being used in laptops and mobile devices as substitutes for magnetic disks.

Advantages

SSDs have the same advantages as magnetic disks when compared to optical storage technologies. Some additional advantages are:

- SSDs are more robust and are unlikely to be damaged if dropped or exposed to magnetic fields.
- It is possible to read and write data from SSDs much faster.

- There is no noise produced when SSDs operate because they have no moving parts.

Disdvantages

- SSDs are more expensive than equivalent capacity magnetic disks.
- At the moment, the maximum capacity of SSDs available on the market is 1TB although this will increase as the technology advances.
- SSDs cannot be re-written as often as magnetic discs.
- SSDs and memory cards are only useful for short term storage of up to 5 years.

Memory cards are available up to 128 GB, but again they do wear out if constantly being rewritten.

Next, you'll learn about remote backups.

3.5 Remote backups

Figure 16

Large businesses and organisations insure themselves even further against failure by storing backups away from their centre of operation. Individual users can also make use of remote hosting, or data services such as Dropbox, GDrive and OneDrive to keep backups remote from their own devices.

In the event of a disaster, there is much greater likelihood that they can return to normal operations within a short period of time – after all, it is much easier to buy new computers than recreate all of the records.

Offsite backups

Specialised companies offer specialised facilities where companies can hire storage space or machinery to hold backups. These offsite facilities might be nothing more than an extremely secure vault where tapes or disks can be deposited; but increasingly they are large server farms connected to extremely high-speed networks. Users can copy files to these servers as if they were part of their own network; the only bottleneck is the speed of the network between the offsite facility and the user, but with fibre connections and high speed Internet, security and reliability are more important than distance from the servers.

Some of the largest suppliers of remote data services are Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform.

Backing up to the cloud

For many years, offsite backup was restricted to organisations which could afford relatively large monthly fees. cloud technology allows anyone to have offsite storage, and in many cases a certain amount of storage is completely free. Most cloud services are designed for convenience, to allow users to share files between computers, and with other users, rather than specifically as backup services, but they can also offer you some additional security (especially when you encrypt files before putting them in the cloud) if your computer is stolen or stops working.

One strong word of warning if you do use the cloud as a backup, with only a few exceptions, these services will not protect you if a file is deleted. Most cloud services are synchronised – that is, when a file is deleted on your computer, the copy on the cloud server is either immediately, or very shortly afterwards, also deleted. Some cloud services also keep previous version of files each time you update a file.

Cloud backups are obviously limited by the bandwidth of your internet connection. If you have a slow uplink (that is sending data to the cloud) you may not be able to make backups of all your data in a reasonable amount of time. Instead you might have to prioritise which data is backed up to the cloud and which is stored locally. If you have a fast Internet connection, you can set up a folder to contain all the files you want to keep backed up with every small change. You can set the software for the backup service to automatically copy these files to the cloud each time a file is changed, and to sync them between your devices.

Cloud security

Unless you take further steps, once data is stored in the cloud you can no longer be sure that it is entirely secure from prying eyes. Most suppliers have policies claiming that your data will be secure, but they cannot provide absolute insurance from attackers, as experienced by some celebrity users of Apple's iCloud service in 2014. You can read more about this incident, if you are interested, via the link in the Further reading section at the end of this week.

Some businesses have policies forbidding employees from storing information in the cloud as it may not be secure, or it may be stored outside the legal protection of the company's country of origin.

Using encryption to scramble the contents is the only way you can guarantee that your data is safe in the cloud.

One of the best ways to ensure your data is encrypted as well as backed up to the cloud is to keep all your files in encrypted folders inside the folder that you backup to the cloud service. You do need to use your encryption key to open the folder you want to use – but that is good security practice for your files on your own computer.

Note that encrypting the whole drive doesn't encrypt the files that you back up from within the drive.

In the next section, you'll consider your own backup procedures.

3.6 Do you backup your data?

Figure 17

For this activity thin about how you backup your own data.

Activity 4 Do you backup?

Allow about 15 minutes

Write a short description of how you backup data. Describe the different technologies you use, how often you backup and what risks remain.

If you don't perform backups, but you work for an organisation who does, briefly explain their backup procedure (you might need to talk to the person in charge of the company's computers).

If neither of these situations applies, briefly explain what sort of backup procedures you think would offer you a reasonable amount of security.

Warning: Do not identify your company or organisation if you discuss this with others.

Provide your answer...

In the next section, you'll examine archiving data.

3.7 Archiving data

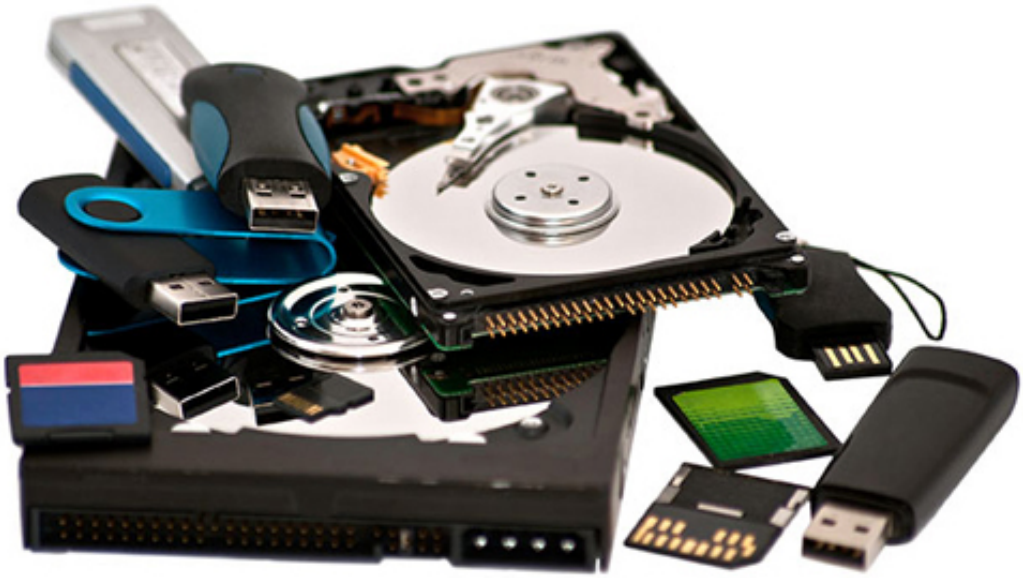


Figure 18

In a perfect world, each of us would keep a backup of every piece of data we ever use, but it is simply impractical for most of us to buy enough media to store our backups.

Instead, most media are reused after a certain period of time with old backups written over by new data. Businesses, in particular, must retain backups for a number of years (for legal and tax purposes) before media can be recycled.

Important files, especially those of historic or legal interest should be archived so that they are never overwritten. In many countries, it is a legal obligation for companies to archive data for auditing purposes. Governments around the world are recognising the importance of archiving data and authorising national bodies to store important digital records. In Britain, this work is managed by the National Archives and the British Library.

Next, you'll have an opportunity to review your knowledge in the end-of-week practice quiz.

4 Week 7 quiz

This quiz allows you to test and apply your knowledge of the material in Week 7.

Complete the Week 7 practice quiz now.

Open the quiz in a new window or tab then come back here when you're done.

5 Summary of Week 7

Figure 19

While most of this week's learning is about how to recover from a disaster, it is worth spending a few minutes reminding yourself what can be done to minimise the risk of a breach in your security.

These relatively easy measures will greatly increase your computer and mobile device security and we have covered many of them over the past few weeks:

- each user has their own personal accounts when using a computer which are not administrative accounts
- use strong passwords (and perhaps a password manager application)
- set your computer and mobile devices to require a login or passcode when you switch them on and when they lock after being left for a certain period
- keep your operating system and key applications up to date
- install antivirus software and keep it up to date
- protect wireless networks using modern (e.g. WPA2) encryption
- enable a personal firewall on your PC and a router firewall.

You could also take these measures, which might require some assistance, or if you are in a business environment, the approval of a system administrator:

- encrypting your hard disk
- encrypting folders that contain confidential files, or files that will be backed up to the cloud
- using encrypted flash memory drives.

Look at the list of security measures above. Do you think any of them apply to you and your computer and mobile devices? Make a note of the security measures that apply to your situation and make some notes on how you could implement them.

You can now go to Week 8: Managing security risks.

Further reading

Apple toughens iCloud security after celebrity breach

Current Icloud security overview

Week 8: Managing security risks

Introduction

Video content is not available in this format.

Cory introduces the final week of the course.

Over the past seven weeks, we have explored different cyber security threats together with actions we can take to prevent these threats from causing harm to our digital lives.

This final week of the course focuses on how to assess the security risks associated with your digital life so that you can effectively plan to protect yourself from attacks.

1 Information as an asset

Figure 1

You'll remember from Week 1 that, when thinking about computer security, it helps to think of information as an asset. Just like money in the bank, it is valuable, possibly irreplaceable, and crucially it can be lost or stolen.

When we think about our assets, traditionally we consider tangible things such as money, property, machinery and so on. Increasingly, it is recognised that information itself is an asset, crucial to adding value. In today's digital world, it is increasingly apparent that information is the most important asset, for both businesses or individuals – just think of the value of music to a media company or a games program to a video game company.

Considering information as an asset allows us to create strategies for protecting information and minimising the consequences of any disaster.

As you have seen earlier in this course, digital information and data assets covers everything that can be stored, processed or transmitted through digital systems. It covers all such personal, business or other digital data anywhere in the world. Since 1990, the world has moved from one where most information existed in paper formats, to one now where the world predominately transacts it business digitally.

Risk management

Information security risk management assesses the value of information assets belonging to an individual or an organisation and, if appropriate, protects them on an ongoing basis.

Information is stored, used and transmitted using various media; some information is tangible, paper for example, and it is relatively straightforward to put in place strategies to protect this information – such as locking filing cabinets, or restricting access to archives.

On the other hand, some information is intangible, such as the ideas in employees' minds, and is much harder to protect. Companies might try to secure information by making sure their employees are happy, or by legal means such as having contracts that prevent people leaving and going to work for a rival. However, note that some industries have blossomed simply because people could easily move and spread new ideas rapidly through many start-up businesses.

Imperatives and incentives

Information security risk management considers the process in terms of two factors: imperatives or incentives. Imperatives are pressures that force you to act. Incentives are the rewards and opportunities that arise from acting.

The imperatives for information security arise from legislation and regulation. The Computer Misuse Act and the Data Protection Act 2018, which is the UK's implementation of the General Data Protection Regulation (GDPR), which we discussed last week, are examples of legislative imperatives. Regulatory imperatives include standards such as the Payment Card Industry Data Security Standard (PCI-DSS), which specifies how merchants should secure all card transactions.

The most important incentive is trust. People and organisations are more likely to work with other people and organisations who have secured their information. Establishing this trust requires that the parties involved examine each others' information security practices to ensure that there are adequate safeguards to protect the information. One way of doing this is to show that the organisation has satisfied the requirements of standards such as PCI-DSS or the ISO27000 family of standards for designing and implementing information security management systems.

In the last few weeks, you have covered all of these aspects – you have learned about a range of threats that confront internet users, you have explored laws that have been drawn up to regulate information and you have seen how the internet is fundamentally underpinned by trust and how technologies such as encryption and signatures can help us feel secure. In the next section, you are invited to apply this to your own information assets.

1.1 Your own information assets

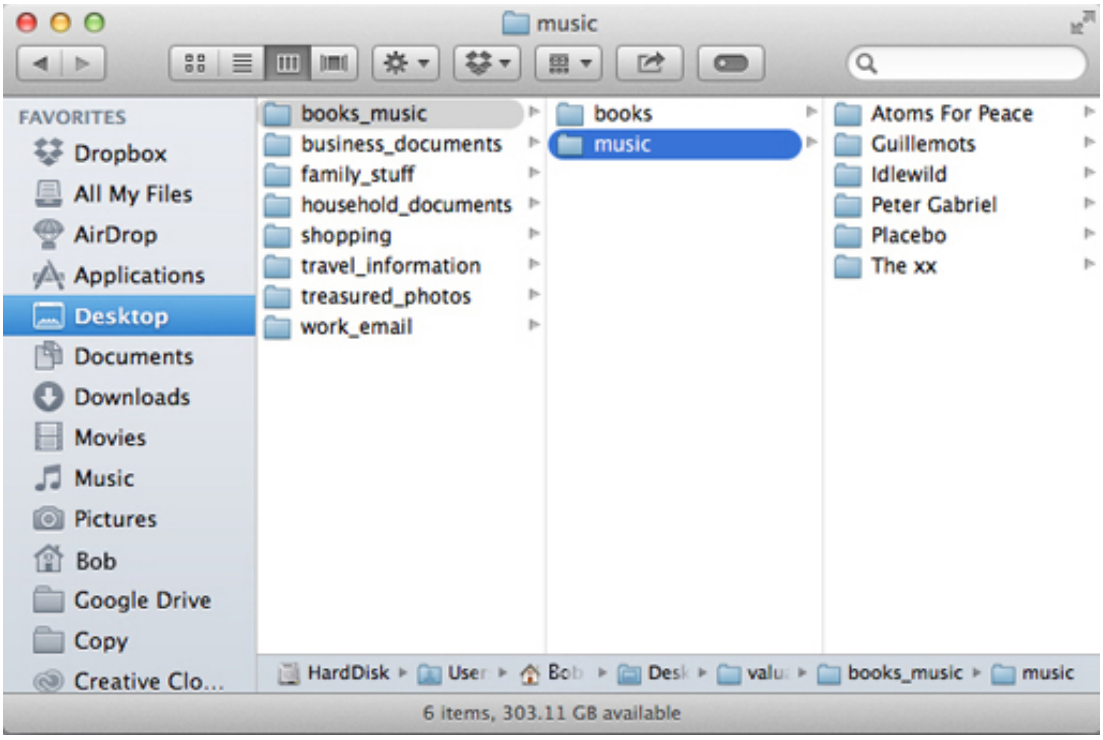


Figure 2

In Week 1, you created a list of information assets that you possess. This was any sort of information that you store on a computer system that you use and which would be expensive, inconvenient, or impossible to replace if it was lost, damaged or stolen.

Spend a few minutes reviewing your list and thinking about whether you need to add anything based on what you have learned over the past eight weeks.

Lewis, a student of The Open University, did the same exercise on his own computers:

- study materials – documents and data relating to his postgraduate studies
- digital photographs – about 20,000 images taken over the last ten years
- music – about 10,000 tracks ripped from CD or bought online
- movies – about 200 films and TV programs
- email – about ten years worth of correspondence
- banking and other financial records
- passwords and account details.

Duplicates of some of these assets could be obtained if he lost the originals, for instance iTunes will allow him to download new copies of any lost music, but it would take a very long time to rebuild the entire library. Some others, such as emails and financial records could be recreated, but only by spending a lot of time asking for information from other people.

Passwords could be changed and other authentication information could be recovered, but again it would take a great deal of time and inconvenience to get back to normal. If these items had been stolen, an attacker might have been able to misuse those assets. The photos would, almost certainly, be lost forever.

Now look back at your own list of information assets. Does Lewis's list prompt you to add any items to yours?

Next, you will learn about risk analysis.

1.2 Risk analysis

Figure 3

We use the term 'risk' in everyday speech, but a whole science has grown up around the identification, analysis and management of risks. You will now look briefly at how to apply some of these ideas to identifying, assessing and reducing risks that affect the security of your information.

Risk can be thought of as the chance of adverse consequences or loss occurring. Generally, risks can be identified and the likelihood of them occurring assessed.

The main technique for a qualitative analysis of risk is to construct a likelihood–impact matrix in which the likelihood and impact of each risk event are assessed against a defined scale and then plotted on a two-dimensional grid. The position on the grid represents the relative significance of each risk. The simplest matrix is formed by classifying both likelihood and impact as either high or low, which leads to a 2 by 2 grid. This basic classification of a high or low value leads to the following rank order for tackling risks:

1. high-impact, high-likelihood risks
2. high-impact, low-likelihood risks
3. low-impact, high-likelihood risks
4. low impact, low-likelihood risks.

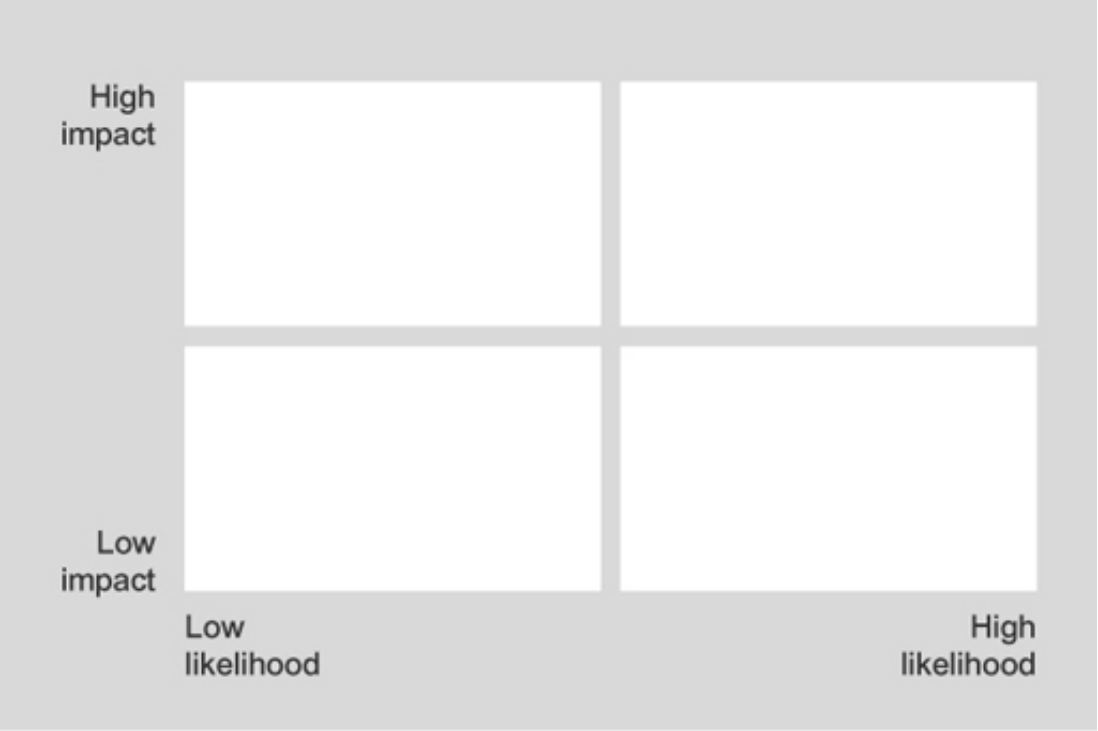


Figure 4 Risk analysis grid

Low-impact, low-likelihood risks are probably not worth expending much effort on (but see the discussion of risk acceptance later this week). You can then look at these high-impact or high-likelihood risks one by one to determine whether there are ways either to reduce the impact if the risk occurs or to reduce the likelihood of the risk occurring, or both.

The next stage is to apply quantitative techniques, based on a financial assessment of the impact of each of the risks, to put the risks into order, with the greatest risks at the top of the list.

It is beyond the scope of this course to discuss these techniques. Sometimes it is hard to reach a decision about the importance of some risks until a corresponding response has been identified as well as any possible interactions between risk events and responses, so risk management is usually iterative in practice.

Next, you'll do some risk analysis on your information.

1.3 Risk analysis in practice

Let's think about a practical example of how qualitative risk analysis could be done for Lewis's information assets.

Any successful attack on email, banking details and password information will have high impact and there is a high likelihood that these attacks will be targeted due to their high value. So they should go in the high-high box.

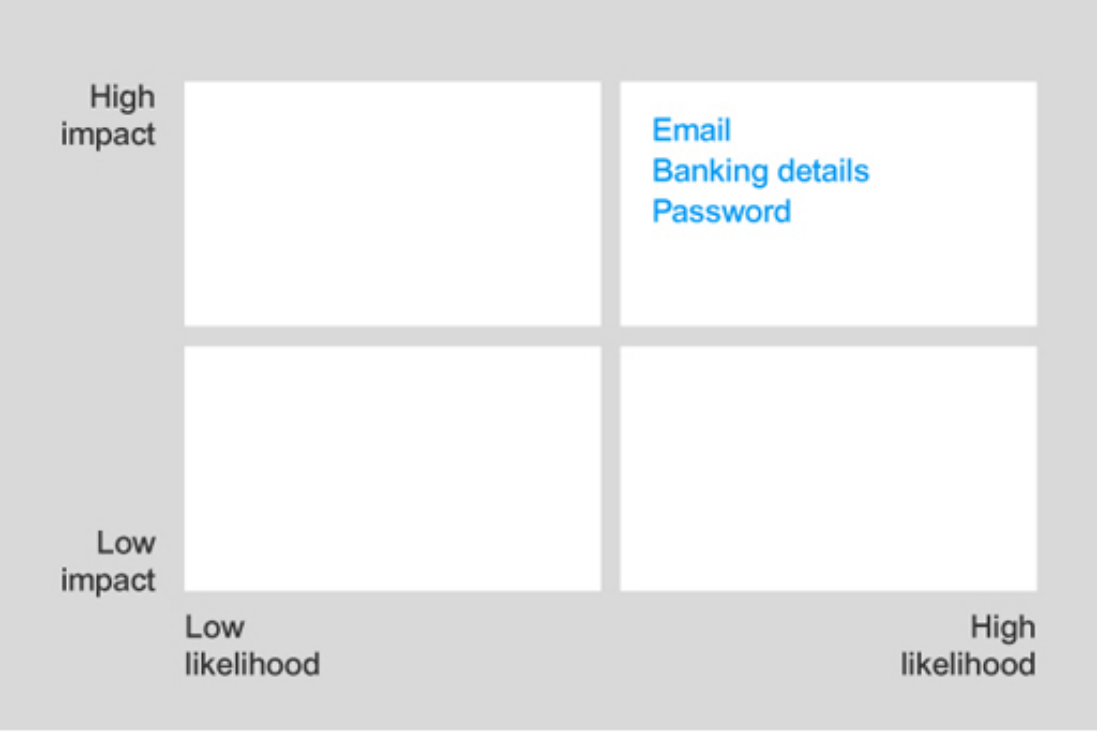


Figure 5

An attack that affects the study materials or digital photographs will have high impact, but there is a low likelihood given that these assets have minimal financial value to an attacker. These should be placed in the high-low box.

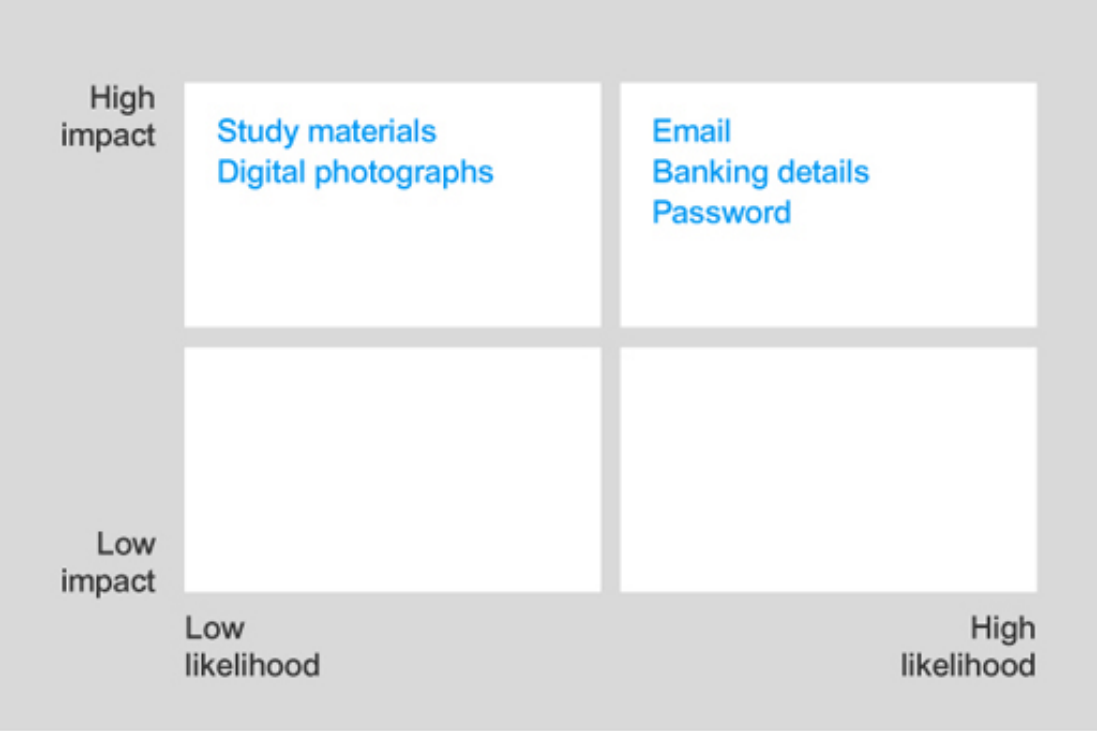


Figure 6

An attack on the digital music or videos will have low impact, since these can be downloaded again easily. However, this will have high likelihood because these assets

can be easily copied and sold, this making these attractive to an attacker. Therefore, they go in the low-high box.

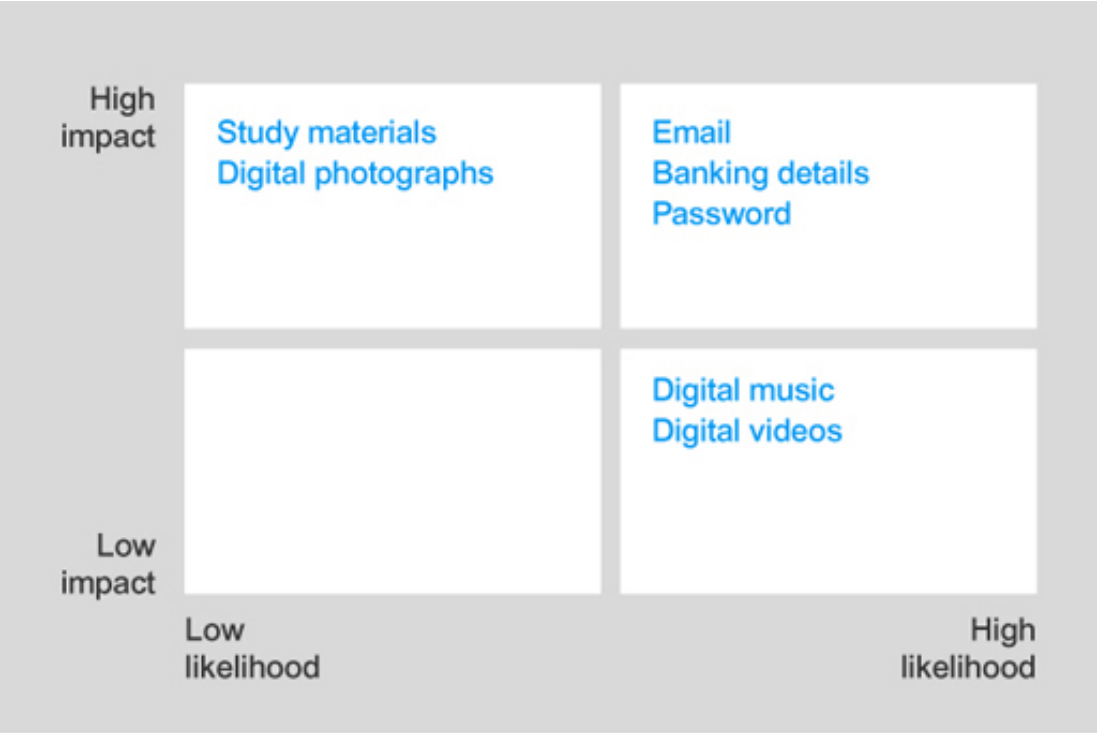


Figure 7

Conducting a risk analysis is an important part of protecting your information assets. Following Lewis's example consider your own list of information assets and carry out a similar risk analysis to determine the impact and likelihood of attack for each type of information.

2 Staying safe online

Figure 8

There are a number of things you can do to stay safe on the internet. Like almost all parts of life, although you hear terrible stories, most people never have serious problems online. By taking a few simple steps, you can make yourself and your computer much more secure.

Stay up to date

Out of date software is one of the biggest problems for computer users. Bugs that have been fixed in newer operating systems or applications may remain unresolved in previous versions, leaving you vulnerable. This is especially important in the case of operating systems, which are responsible for managing files and connecting to the internet.

Check to see if your operating system is being supported by regular updates. For example, for Microsoft software you can search for your operating system at: https://support.microsoft.com/en-us/hub/4095338/microsoft-lifecycle-policy.

Many other applications, such as Microsoft Office, the Java programming language (used by a lot of websites), web browsers and so on, also require regular updating to fix security problems.

If you are using an old operating system that is not supported by its manufacturer, or if you need an application, but your current edition is out of date, it is well worth investing in updated software. First, though, check that your computer can run the updated software, if not, it might be time for a new computer. Or consider installing a new operating system such as a free Linux OS on older equipment. Remember to backup all your data and passwords first.

Do the basics

The basic check list:

- set up a personal firewall
- install an antivirus program (remember, Macs do need antivirus protection)
- get used to making backups
- set up your computer to require passwords to log in and when unlocking the screen
- set up two-factor authentication for all important financial and social media sites
- use a unique strong password for each website
- use a password manager or encrypt your password folder
- use hard disk encryption if you have it – especially on laptops.

It will take a couple of hours to perform these steps, but your computer will be significantly more secure.

Fix your email

Most email applications now come with junk mail screening. If it's not already enabled – turn it on! Your mail program will scan incoming email looking for suspicious messages that might be trying to scam you – or are just annoying spam. It puts any suspect messages into a junk mail folder where you can examine them later, just in case any genuine messages were misfiled.

Most email programs will also let you train the screening process so that any messages that were missed can be treated as junk in the future.

In the next section, you'll learn some tips to improve your web browser's security.

2.1 Fix your browser

Figure 9

Web browsers are steadily developing enhanced security and it is a good idea to use the latest version.

There are several simple things you can do to improve your web browser's security.

- Use a browser such as Brave (https://brave.com/) that is designed to put your security first.
- Use a search engine such as duckduckgo (https://duckduckgo.com) that doesn't track you.
- Use a secure VPN or the TOR browser when using public wi-fi.

Cookies are small pieces of data that can be used to track your use of the web and some websites host cookies belonging to organisations you know nothing about – these are called 'third party cookies' and they're no use to you whatsoever. Use the tools/ preferences menu in your browser to prevent the use of third party cookies.

Once you have checked your settings you can test whether you can be identified by your web browser by visiting the site https://panopticlick.eff.org. Read the information about this site and then hit the 'Test Me' button.

The table shows the test results for a secure browser.

Table 1 Test results for a secure browser

Test	Result
Is your browser blocking tracking ads?	Yes
Is your browser blocking invisible trackers?	Yes

Dows your blocker stop trackers that are included in the so-called '**acceptable ad**' whitelist?	Yes
Does your browser unblock 3rd parties that promise to honour **Do not track**?	No
Does your browser protect from **fingerprinting**?	Your browser has a unique fingerprint

Note the result 'your browser has a unique fingerprint'. Here are my results for this test: 'Your browser fingerprint appears to be unique among the 224,169 tested in the past 45 days. Currently, we estimate that your browser has a fingerprint that conveys at least 17.77 bits of identifying information.'

The table below shows the different attributes of the user's browser and computer that can be detected by a web server.

Table 2 Browser and computer attributes that can be detected by a web server

Browser characteristic	Bits of identifying information	One in x browsers have this value	Value
User agent	7.89	237.97	|Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36|
HTTP_ACCEPT headers	5.77	54.74	|text/html, */*; q=0.01 gzip, deflate, br en-GB,en-US;q=0.9,en;q=0.8|
Browser plugin details	5.25	38.01	Plugin 0: Chrome PDF Plugin; Portable Document Format; internal-pdf-viewer; (Portable Document Format; application/x-google-chrome-pdf; pdf). Plugin 1: Chrome PDF Viewer; ; mhjfbmdgcfjbbpaeojofohoefgiehjai; (; application/pdf; pdf).
Time zone	2.57	5.95	0
Screen size and colour depth	5.77	54.44	1920x1200x24
System fonts	10.32	1280.97	Andale Mono, Arial, Arial Black, Comic Sans MS, Courier, Courier New, Georgia, Helvetica, Impact, MS Gothic, MS PGothic, Times, Times New Roman, Trebuchet MS, Verdana, Wingdings 2, Wingdings 3 (via javascript)
Are cookies enabled?	0.24	1.18	Yes
Limited supercookie test	0.36	1.28	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No
Hash of canvas fingerprint	17.77	224169.0	c317936a22901617dd08dc99390e0fe1
Hash of WebGL fingerprint	13.45	11208.45	dd255d5c1bddffd68d8e0921e64760b1

DNT header enabled?	1.05	2.07	False
Language	3.94	15.39	en-GB
Platform	3.06	8.35	Linux x86_64
Touch support	0.69	1.61	Max touchpoints: 0; TouchEvent supported: false; onTouchStart supported: false

Each result by itself doesn't give much information away. The screen size and colour depth suggests a desktop computer and the platform is identified as Linux. However, in combination all this information creates a digital fingerprint that might identify you wherever you browsed, even if you were pretending to be someone else and had blocked cookies. For most, that probably doesn't matter, but, for example, a whistleblower or journalist reporting news should be aware of how hard it is to keep yourself hidden and safe.

Activity 1 Improving your browser security

Allow about 10 minutes

Note down in the box below how you can further improve your browser security.

Provide your answer...

Next, you will decide what to do about the risks to your digital information and share your resolutions with your fellow learners.

2.2 Risk management in practice

Figure 10

Having analysed the situation, the next stage is to decide what to do about the risks.

For each risk to be managed, we need to identify what cost-effective countermeasures can be applied. Possible countermeasures are:

- **Avoiding the risk** – avoidance would mean stopping the activity that is causing the risk. For example, deleting all banking information and unsubscribing from internet banking would avoid the risks associated with the information assets related to banking.
- **Modifying the risk (likelihood and/or impact)** – this involves choosing and implementing a security mechanism that reduces the likelihood of a successful attack, or the impact that would result from such an attack. For example, installing an up to date antivirus application can prevent the attacker from using malware to gain access to the computer holding the internet banking information.
- **Transferring the risk to others** – typically involves taking out insurance to cover any losses in the event the threat materialises.
- **Accepting the risk** – would mean choosing not to implement any of these countermeasures, choosing instead to monitor the information asset for any attacks.

Consider risks identified in the qualitative risk analysis. Choose one of your information assets and decide on which countermeasures you would apply in this case.

2.3 Protecting your information assets

Figure 11

Now you've done a risk analysis, it's time to look at how we can better protect our information assets.

You've already thought about backing up data and using encryption to protect information – but have you put any of these measures into practice?

Go back to the list of information assets you used in your risk analysis. What steps have you taken to protect them? Think in terms of what you have studied on this course. For example:

- Have you set up firewalls to protect your networked computers from external attack?
- Are you protected by up to date antivirus software?
- Are your operating system and key applications up to date?
- Is important information protected by encryption?

Note, next to each item on your list, the measure you have taken to protect it. If you have not yet implemented that measure, identify it in some way that will remind you to action it.

In the next section, you are invited to create a plan for implementing and maintaining your information security.

2.4 What should I do next?

Figure 12

You have now taken several simple but very important steps to protect your information. Review your list of information assets and work through what else you need to do to improve your own security.

Based on the risk analysis you have done for your information assets, create an information security action plan detailing the countermeasures you could implement to protect each asset.

Before proceeding, you should implement at least one set of countermeasures. In time, you should implement all the countermeasures and also periodically review your risk analysis and action plan to make sure that you are maintaining your countermeasures.

Some of your actions are likely to involve secure encryption and secret passwords. This can result in some significant problems for your business or family should you become incapable of handling these procedures or should you die.

Business users need to analyse how the business would continue to have access to any business documents and systems while ensuring full security at all times. Other users need to evaluate what assets should remain inaccessible on their death, and which assets should be available to family or friends. For the latter, the process by which secure passwords can be passed on to others needs to be planned.

Next you'll learn about some of the recent developments in cyber security.

2.5 Tracking a moving target

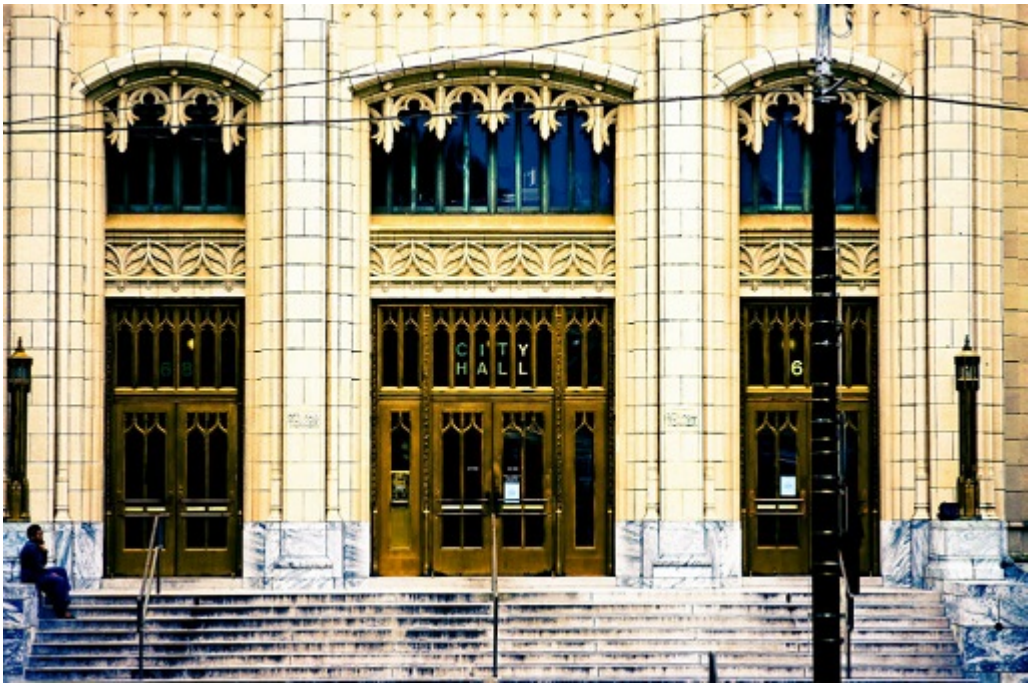


Figure 13

Security is an ever-changing topic. New technologies are always being introduced and they bring new risks, or allow old threats to resurface in a new form.

Old technologies are retired by manufacturers, potentially leaving their users exposed to danger as bugs and security weaknesses remain unaddressed. And there are new threats being discovered every day, such as the WannaCry ransomware attack of 2017 or the more recent SamSam ransomware attack that shut down services across the city of Atlanta.

On 22nd March 2018, Atlanta, Georgia was hit by a cyber attack which rendered parts of the city's government inoperable. The attack was in the form of a piece of malicious software (malware) called SamSam. This is a piece of ransomware – a program that stops users accessing their data until they pay a ransom, usually in a cryptocurrency such as Bitcoin, to receive the keys needed to unlock their data. SamSam demanded a ransom of $51,000; payable in seven days or the data would never be recoverable. Some reports say that the address needed to pay the ransom was made unavailable shortly after the attack; but in any case, there is no evidence that the city paid SamSam's creators.

The attack on Atlanta created a range of problems, it prevented citizens from paying for basic services such as water and parking; the city stopped taking employment applications; business licences could not be issued; court warrants could not be validated; and the malware crippled the city's police computers requiring officers to hand write crime reports. As well as these direct problems, other parts of the city's infrastructure – such as the wireless network at the gigantic Atlanta International airport – were shut down as a precautionary message. More than two weeks after the outbreak, the city was still struggling to restore some services and it is clear that some data was rendered permanently inaccessible.

SamSam spreads on networked computers connected to the internet rather than through emails. Many of the computers that have been infected run Microsoft's Remote Desktop

Protocol (RDP) which allows users to connect to other computers over a network. The most vulnerable computers are those that have been misconfigured or running out-of-date software. It appears that SamSam's owners manually attack these computers before installing SamSam – there are some suggestions that part of Atlanta's computer systems were compromised by SamSam's owners during 2017, although they took no action until March. Once activated, SamSam spreads rapidly across the company's network before locking the data, ensuring that hundreds, if not thousands of computers are crippled – increasing the likelihood that the ransom will paid.

Like many big organisations, Atlanta faces the problem that it cannot function without many different computer systems, managed by many different teams with unclear responsibilities. Like other organisations, Atlanta has not made adequate investment in computer security training and preventative measures to protect against security threats (the same problems were found in the NHS after the WannaCry attack). Indeed, an earlier audit had warned that the city was at risk from cyber attack, but this was not fixed.

Atlanta spent more than $2.6 million on emergency measures recovering from SamSam. The cost included extra staffing, the need to buy additional computer infrastructure from Microsoft as well as consultancy fees and emergency communications.

It is highly unlikely that Atlanta will be SamSam's last victim. Its unknown developers continue to release new versions of the malware, so it is likely another organisation will be harmed. Fortunately, up-to-date antivirus software can identify and destroy most forms of SamSam, so ensure you have antivirus running on your computers and that it is receiving the latest updates.

3 What do you do now?

As we approach the end of the course, it's a good opportunity to reflect on what you have learned and how it has impacted your ability to protect your digital life.

At the beginning of the course, you took a survey on your information security practices. We'd like you to retake it now to see how your practices have changed.

Launch the survey – answer the questions based on your habits **now**. There are no right or wrong answers so you should choose the answer that most closely matches the way you use your computer now that you've completed the course. Don't worry, all the data is anonymous and we will not reveal individual answers.

When you've finished you can compare your answers with those you gave at the start of the course.

When this course was originally run, the results were collated by the author of the course, Arosha, in his blog. You might want to take a look at those results.

3.1 Confessional

Figure 14

In Section 2.4, What should I do next?, we asked that you implement at least one of the countermeasures you included in your security action plan.

Activity 2 A security problem

Allow about 20 minutes

Use the space below to note down the details of a security problem that you spotted and took appropriate countermeasures to address.

Provide your answer...

Next, you'll have the opportunity to review your learning from the whole course in the end-of-course compulsory badge quiz.

4 End-of-course quiz

You can now take the end-of-course quiz, which consolidates your understanding of all the topics you've studied.

Complete the Week 8 compulsory badge quiz now.

Open the quiz in a new window or tab then come back here when you're done.

5 End-of-course guide and round-up

Video content is not available in this format.

Over the past eight weeks you have learned about different types of cyber security threats and techniques that can be used to counter them. You should now have a grasp of cyber security concepts such as confidentiality, integrity and availability as well as understanding the basics of cryptography, network security and security risk management.

Use the below as a checklist to see how your practices have changed since taking this course.

- When you start your computer, do you need to use a password to log in?
- When you leave your computer for a break, does it require you to enter a password before you can start working again?
- Do you keep your passwords for your computer in your head?
- Do you keep passwords for logging on to banking websites and social media in an encrypted folder or encrypted password manager?
- Do you use a separate unique strong password on each website?
- Do you use antivirus software on your computer?
- Do you regularly update the software you use?
- Do you use a firewall on your router or on your computer to protect you from attackers?
- Do you have backups of your important data stored somewhere other than your computer (such as on another disk drive, computer or in the cloud)?

If you would like to find out more about any of the topics covered in the course we have created an area specifically for exploring more about cyber security on OpenLearn.

6 Next steps

Figure 15

Congratulations, you have completed the course! We hope you have enjoyed your journey into the world of cyber security.

Were you inspired by the course? Would you like to continue your learning with The Open University? Then read on!

If you already have a qualification in computing or relevant work experience in the field and want to specialise in cyber security, The Open University offers the following postgraduate courses:

- M811 *Information security*
- M812 *Digital forensics*
- T828 *Network security*.

If you don't have a computing background but your introduction to cyber security has inspired you to learn more about computing, you may be interested in The Open University's BSc (Honours) in Computing and IT, starting with TU100 *My digital life*.

Get careers guidance

The National Careers Service can help you decide your next steps with your new skills.

Tell us what you think

Now you've come to the end of the course, we would appreciate a few minutes of your time to complete this short end-of-course survey (you may have already completed this survey at the end of Week 4). We'd like to find out a bit about your experience of studying the course and what you plan to do next. We will use this information to provide better online experiences for all our learners and to share our findings with others. Participation will be completely confidential and we will not pass on your details to others.

If you found this course through the Skills Toolkit launched by the UK government in April 2020 and would be willing to provide feedback on how this course has helped you, please get in touch by emailing us.

References

Department for Digital, Culture, Media and Sport (2019) *Cyber Security Breaches Survey 2019*. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf (Accessed: 4 December 2019).

Dragos (2019) *Threat Proliferation in ICS Cybersecurity: XENOTIME now targeting electric sector, in addition to oil and gas*. Available at: https://dragos.com/blog/industry-news/threat-proliferation-in-ics-cybersecurity-xenotime-now-targeting-electric-sector-in-addition-to-oil-and-gas/ (Accessed: 4 December 2019).

Sophos (2019) *SophosLabs 2019 Threat Report*. Available at: https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-2019-threat-report.pdf?la=en (Accessed: 4 December 2019).

Statista (2018) *Annual number of data breaches and exposed records in the United States from 2005 to 2018*. Available at: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (Accessed: 4 December 2019)

TechCrunch (2019a) *Millions of Instagram influencers had their contact data scraped and exposed*. Available at: https://techcrunch.com/2019/05/20/instagram-influencer-celebrity-accounts-scraped/ (Accessed: 4 December 2019).

TechCrunch (2019b) *A huge database of Facebook users' phone numbers found online*. Available at: https://techcrunch.com/2019/09/04/facebook-phone-numbers-exposed/ (Accessed: 4 December 2019).

TrendMicro (2019) 2019 *Midyear security roundup: Evasive threats, pervasive effects*. Available at: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/evasive-threats-pervasive-effects (Accessed: 4 December 2019).

ZDNet (2019) *Database leaks data on most of Ecuador's citizens, including 6.7 million children*. Available at: https://www.zdnet.com/article/database-leaks-data-on-most-of-ecuadors-citizens-including-6-7-million-children/ (Accessed: 4 December 2019).

BBC (2019) 'I lost £4,000 in a call centre scam', *BBC News*, 21 October. Available at: https://www.bbc.co.uk/news/technology-50117796 (Accessed 16 December 2019).

Microsoft (2019) *Microsoft security intelligence report*. Available at: https://www.microsoft.com/securityinsights (Acccessed 5 December 2019).

Statista (2018) *Share of internet users in the United States who have been victim of online identity theft as of October 2018*. Available at: https://www.statista.com/statistics/763130/internet-identity-theft-usa/ (Accessed: 9 December 2019).

Verizon (2019) *Summary of findings*. Available at: https://enterprise.verizon.com/resources/reports/dbir/2019/summary-of-findings/ (Accessed 9 December 2019).

Acknowledgements

This course was written by Arosha K. Bandara. It was last updated in December 2019.

The material acknowledged below is Proprietary and used under licence (not subject to Creative Commons Licence). Grateful acknowledgement is made to the following sources for permission to reproduce material in this course:

Images

Introduction and guidance

Course image: Atomic Taco in Flickr made available under Creative Commons Attribution-ShareAlike 2.0 Licence .

Week 1

Figure 1 © Blend Images - Colin Anderson (via Getty Images)

Figure 2 © xxz114 (via iStock photo)

Figure 3 © caracterdesign (via iStock Photo)

Figure 4 © bluebird13 (via iStock Photo)

Figure 5 © agsandrew (via shutterstock)

Figure 6 © Ryan McGinnis (via Getty Images)

Figure 7 © Jasper James (via Getty Images)

Figure 8 © Vetta Collection (via iStock Photo)

Figure 9 © JGI/Tom Grill (Getty Images)

Figure 10 © LeoPatrizi, sb-borg (via iStock Photo); mediaphotos (via Getty Images)

Figure 11 © Danil Melekhin (via Getty Images)

Figure 12 © Jimmy Anderson (via iStock Photo)

Week 2

Figure 1 © agsandrew (via Fotolia)

Figure 2 © beaucroft (via iStock Photo)

Figure 3 © piotr_malczyk (via iStock Photo)

Figure 4 © dcdp (via iStock)

Figure 5 © dsteller (via iStock Photo)
Figure 6 © Garry518 (via iStock Photo)
Figure 7 © Andrey_Kuzmin (via iStock Photo)
Figure 8 © FredFroese (via iStock Photo)
Figure 9 © lek2481 (via iStock Photo)
Figure 10 © David Clark (via Getty Images)
Figure 11 © pagadesign (via iStock Photo)
Figure 12 © Alan Uster (via Shutterstock)

Week 3

Figure 1 © Eraxion (via iStock Photo)
Figure 2 © JordiRoy (via iStock Photo)
Figure 3 © Colin Anderson (via Getty Images)
Figure 4 © vadimguzhva (via iStock Photo)
Figure 5 © Carol and Mike Werner/Visuals Unlimted, Inc. (via Getty Images)
Figure 6 © Yugi Studio (via Getty Images)
Figure 7 © Stephan Zabel (via Getty Images)
Figure 8 © Trina Dalziel (via Getty Images)
Figure 9 © Andrew Levine http://commons.wikimedia.org/wiki/File:PhishingTrusted-Bank.png
Figure 11 © Dimitri Otis (via Getty Images)
Figure 12 © enjoynz (via iStock Photo)
Figure 13 © ryccio (via Getty Images)
Figure 14 © aydinmutlu (via iStock Photo)
Figure 15 © John Lamb (via Getty Images)
Figure 16 © Danil Melekhin (via Getty Images)
Figure 18 © FreezeFrameStudio (via iStock Photo)
Figure 20 © webking (via iStock Photo)
Figure 21 © addimage (via iStock Photo)

Week 4

Figure 1 © Michael Smith (via Getty images)
Figure 2 © bioraven (via Shutterstock)
Figure 3 © Mark Horn (via Getty Images)
Figure 4 © bluebird13 (via iStock Photo)
Figure 5 © olhainsight (via iStock Photo)
Figure 6 © powerofforever (via iStock Photo)
Figure 7 © Bet_Noire (via iStock Photo)
Figure 8 © Scorpions and Centaurs (via Flickr.com)
Figure 9 © no_limit_pictures (via iStock Photo)
Figure 11 © chrisroll (via iStock Photo)
Figure 12 © Pashalgnatov (via iStock Photo)
Figure 13 © Catrina Genovese (via Getty Images)
Figure 14 © John Lund (via Getty Images)

Week 5

Figure 1 © Bletchley Park Trust (via Getty Images)

Figure 2 © Bob Lord - Licensed under Creative Commons Attribution-Share Alike 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Enigma-plugboard.tif.jpg#mediaviewer/File:Enigma-plugboard.tif.jpg

Figure 3 © agsandrew (via Shutterstock Photos)

Figure 5 © peterhowell (via iStock Photo)

Figure 6 © GlobalP (via iStock Photo)

Figure 7 © blackie (via iStock Photo)

Figure 10 © Wavebreak (via iStock Photo)

Figure 11 © choicegraphx (via iStock Photo)

Figure 12 © Vertigo3d (via iStock Photo)

Week 6

Figure 1 © narvikk (via iStock Photo)

Figure 2 © HAYKIRDI (via iStock Photo)

Figure 3 © Underwood Archives (via Getty Images)

Figure 4 © vmedia84 (via Fotolia)

Figure 5 © RapidEye (via iStock Photo)

Figure 6 © OJO_Images (via iStock Photo)

Figure 7 © belterz (via iStock Photo)

Figure 8 © BaderElbert (via iStock Photo)

Figure 9 © Hugh Threlfall (via Getty Images)

Figure 10 © Isantilli (via iStock Photo)

Week 7

Figure 1 © Alex Wong (via Getty Images)

Figure 2 © Herzstaub (via iStock Photo)

Figure 3 © Mdbeckwith http://creativecommons.org/licenses/by-sa/3.0/deed.en

Figure 4 © zimmytws (via iStock Photo)

Figure 5 © peeterv (via iStock Photo)

Figure 6 © RapidEye (via iStock Photo)

Figure 7 © fstop123 (via iStock Photo)

Figure 8 © stayorgo (via iStock Photo)

Figure 9 © Nico Elnino/Getty Images

Figure 10 © Shaun Curry (via Getty Images)

Figure 11 © David Gould (via Getty Images)

Figure 12 © wakila (via iStock Photo)

Figure 13 © scanrail (via iStock Photo)

Figure 14 © Jeff Nagy (via iStock Photo)

Figure 15 © v777999 (via iStock Photo)

Figure 16 © Scorpions and Centaurs (via Flickr.com)

Figure 17 © scyther5 (via iStock Photo)

Figure 18 © kirillm (via iStock Photo)

Figure 19 © Mari (via iStock Photo)

Week 8

Figure 1 © 1joe (via iStock Photo)

Figure 3 © scotto72 (via iStock Photo)

Figure 8 © swilmor (via iStock Photo)

Figure 9 © DonNichols (via iStock Photo)

Figure 10 © ishoot63 (via iStock Photo)

Figure 11 © btrenkel (via iStock Photo)

Figure 12 © mjutabor (via iStock Photo)

Figure 13 © Geoffrey Meyer-van Voorthuijsen / flickr (Creative Commons BY-NC 2.0)

Figure 14 © wakila (via iStock Photo)

Figure 15 © Mordolff (via iStock Photo)

Audio visual

Week 1

1 Online, the new frontline © HM Government

1.3 and 2.1 © The Open University

Week 2

2.1 How to pick a proper password (including transcript) © Sophos

Week 4

2 extract (including transcript) from Datababy: How easy is it to become a phone hacker? © Channel4/ITN

Week 5

2.1 and 2.2 © The Open University

Week 7

1 extract (including transcript) from 'Inside Out' (6/2/12) © BBC

Every effort has been made to contact copyright owners. If any have been inadvertently overlooked, the publishers will be pleased to make the necessary arrangements at the first opportunity.