

**dd802\_1**

**The psychology of cybercrime**

**About this free course**

This free course is an adapted extract from [DD802 Investigating forensic psychology.](http://www.open.ac.uk/postgraduate/modules/dd802).

This version of the content may include video, images and interactive content that may not be optimised for your device.

You can experience this free course as it was originally designed on OpenLearn, the home of free learning from The Open University –[https://www.open.edu/openlearn/health-sports-psychology/psychology/the-psychology-cybercrime/content-section-0](%20https://www.open.edu/openlearn/health-sports-psychology/psychology/the-psychology-cybercrime/content-section-0)

There you’ll also be able to track your progress via your activity record, which you can use to demonstrate your learning.

Copyright © 2020 The Open University

**Intellectual property**

Unless otherwise stated, this resource is released under the terms of the Creative Commons Licence v4.0 <http://creativecommons.org/licenses/by-nc-sa/4.0/deed.en_GB>. Within that The Open University interprets this licence in the following way: [www.open.edu/openlearn/about-openlearn/frequently-asked-questions-on-openlearn](http://www.open.edu/openlearn/about-openlearn/frequently-asked-questions-on-openlearn). Copyright and rights falling outside the terms of the Creative Commons Licence are retained or controlled by The Open University. Please read the full text before using any of the content.

We believe the primary barrier to accessing high-quality educational experiences is cost, which is why we aim to publish as much free content as possible under an open licence. If it proves difficult to release content under our preferred Creative Commons licence (e.g. because we can’t afford or gain the clearances or find suitable alternatives), we will still release the materials for free under a personal end-user licence.

This is because the learning experience will always be the same high quality offering and that should always be seen as positive – even if at times the licensing is different to Creative Commons.

When using the content you must attribute us (The Open University) (the OU) and any identified author in accordance with the terms of the Creative Commons Licence.

The Acknowledgements section is used to list, amongst other things, third party (Proprietary), licensed content which is not subject to Creative Commons licensing. Proprietary content must be used (retained) intact and in context to the content at all times.

The Acknowledgements section is also used to bring to your attention any other Special Restrictions which may apply to the content. For example there may be times when the Creative Commons Non-Commercial Sharealike licence does not apply to any of the content even if owned by us (The Open University). In these instances, unless stated otherwise, the content may be used for personal and non-commercial use.

We have also identified as Proprietary other material included in the content which is not subject to Creative Commons Licence. These are OU logos, trading names and may extend to certain photographic and video images and sound recordings and any other material as may be brought to your attention.

Unauthorised use of any of the content may constitute a breach of the terms and conditions and/or intellectual property laws.

We reserve the right to alter, amend or bring to an end any terms and conditions provided here without notice.

All rights falling outside the terms of the Creative Commons licence are retained or controlled by The Open University.

Head of Intellectual Property, The Open University

# Contents

* [Introduction](#Introduction1)
* [Learning outcomes](#LearningOutcomes1)
* [1 What is cybercrime?](#Session1)
* [2 Types of cybercrime](#Session2)
  + [2.1 Trolling](#Session2_Section1)
  + [2.2 Non-consensual distribution of sexual images](#Session2_Section2)
  + [2.3 Hacking](#Session2_Section3)
  + [2.4 Malware](#Session2_Section4)
  + [2.5 Online fraud](#Session2_Section5)
* [3 Victim’s experience of cybercrime](#Session3)
  + [3.1 Impact of cybercrime on victims and coping strategies](#Session3_Section1)
  + [3.2 Victim blaming](#Session3_Section2)
* [4 What are the motivations for cybercrime?](#Session4)
* [5 Intervention on cyber criminality](#Session5)
  + [5.1 Where cybercrime and online anti-social behaviour meet](#Session5_Section1)
* [6 Reflecting on your experiences](#Session6)
* [7 Conclusion](#Session7)
* [Glossary](#Glossary1)
* [References](#References1)
* [Acknowledgements](#Acknowledgements1)
* [Solutions](#Solutions1)

## Introduction

In this free course, The psychology of cybercrime, you will explore different questions about cybercrime from a psychological angle in an attempt to better understand this relatively recent field of psychology. You will consider the realms and limits of cybercrime, distinguishing between the different types of cybercrime (e.g. trolling, cyber-stalking, fraud, hacking), the experiences of being victims of cybercrime and the causes behind engaging in these types of criminal activity. Finally, current interventions will be highlighted.

Even though cybercrime is broadly encompassing all the different types of crime committed online, it is important to emphasise very early on that it is likely to be committed by offenders with different characteristics, motivations and behaviours than those who commit other types of crime. As a result, those online criminal activities share similarities with offline equivalents (e.g. fraud and online fraud). The interest in studying the psychology of cybercrime both from the perpetrator and victim perspectives has arisen in an attempt to understand what makes cybercrime unique or similar to its offline counterpart.

Start of Box

**Content warning**

Cybercrime victimisation can affect both adults and children who engage online. Please find links to two useful guides that give tips on to stay safe online:

1. [Cybercrime and online safety](https://www.westyorkshire.police.uk/sites/default/files/a_guide_to_cyber_crime_and_online_safety_0.pdf) developed by West Yorkshire police.
2. [Supporting your child’s wellbeing](https://www.net-aware.org.uk/news/supporting-your-childs-wellbeing-online/) by the NSPCC.

End of Box

This Open Learn course is an adapted extract from the Open University course [DD802 Investigating forensic psychology.](http://www.open.ac.uk/postgraduate/modules/dd802) Explore the collection of [Postgraduate study in psychology and criminology](https://www.open.edu/openlearn/health-sports-psychology/psychology/postgraduate-study-psychology-and-criminology).

## Learning outcomes

After studying this course you should be able to:

* outline the impact on victims
* distinguish different types of cybercrime, considering the similarities and differences in the definitions and behaviours
* identify the motivations and behaviours of cybercriminals
* illustrate the current interventions to tackle cybercrime.

## 1 What is cybercrime?

Cybercrime refers to criminal activities that are committed using internet technology. The internet has only been in widespread use by the general public for a few decades (a ‘start date’ could be considered to be the launch of the World Wide Web on the 6 August 1991), but online activity has already become ubiquitous in the developed world and is becoming progressively more common in much of the developing world as well (Naughton, 2016).

Psychologists studying cybercrime, including its perpetrators and victims, are interested both in what makes cybercrime unique (e.g. does online anonymity increase the propensity of some people to commit crimes of harassment?) as well as what it has in common with offline crime – although the emphasis is often on the former rather than the latter.

Before reading further complete Activity 1. In order to help you complete the activity, please watch the following video and then consider your perspectives on living online.

Start of Media Content

Video content is not available in this format.

Video 1 Everyday perspectives: engaging online

[View transcript - Video 1 Everyday perspectives: engaging online](" \l "Session1_Transcript1)

Start of Figure



End of Figure

End of Media Content

Start of Activity

**Activity 1 Thinking about cybercrime**

Allow 20 minutes

Try to answer the following questions about cybercrime, drawing on your experiences and understandings. Type your responses (up to 100 words for each question) in the box below, and then select ‘Save’. Your responses are not published anywhere.

Start of Question

1. Think about how you engage online. Make a list of the things you do online (e.g. social contact, looking for information, news, weather, sports, entertainment, studying online, shopping, bank, holiday booking and so on)

End of Question

*Provide your answer...*

Start of Question

2. Looking at your answers above, try to guess how much time you spend on a weekly basis on each activity and your potential victimisation

End of Question

*Provide your answer...*

[View discussion - Part](" \l "Session1_Discussion1)

End of Activity

As already indicated in the content warning in the introduction, you can download a comprehensive guide on cybercrime and online safety developed by [West Yorkshire police](https://www.westyorkshire.police.uk/sites/default/files/a_guide_to_cyber_crime_and_online_safety_0.pdf) in order to get tips about how to increase your online safety. Alternatively, the NSPCC has developed [a range of resources](https://www.net-aware.org.uk/) regarding child safety online. More guidance about online safety regarding specific online activities will be provided towards the end of the course.

## 2 Types of cybercrime

As you have probably identified from engaging in Activity 1, the internet offers a wide range of activities and opportunities for criminals to engage in anti-social and/or deviant behaviours. Therefore, the term cybercrime encompasses a variety of different activities, which goes beyond the fact that they are either a function of, or are facilitated by, the internet. Indeed, real-world crimes can be seen to achieve different goals; for example, theft for financial gain compared to murder for the purpose of revenge. In the same respect, criminal activities falling under the umbrella of cybercrime follow the same pattern. Usually, a distinction is made between:

1. **instrumental crimes** (i.e. crimes where the harm to the victim is not the ultimate aim) and
2. **expressive crimes** (i.e. crimes are based on an offender’s emotional response to a situation that provokes anger, leading to a desire to cause harm to the victim) (Canter and Youngs, 2009; Youngs, Ioannou and Eagles, 2016).

Similarly in an online environment, some forms of crime seem to principally be for financial gain (e.g. **ransomware** attacks, online identity theft), whereas others may be carried out for personal reasons, such as revenge (e.g. cyberstalking) or for the purposes of furthering an offline crime (e.g. a paedophile grooming a child online). However, there are also offences/anti-social online behaviours such as ‘hacking’ and ‘trolling’, which may be carried out for a variety of other reasons.

Start of Activity

**Activity 2 Classifying the different types of cybercrime**

Allow 20 minutes

Start of Question

Many categorisations of cybercrime distinguish between crimes against the person/morality and crimes again property/government. Use your common knowledge to decide whether this falls under crimes against the person or crime against the property or both. Put some text into the boxes you think are the right option.

Start of Table

Table 1 Classifying the different types of cybercrime

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Crime against the person** | **Crime against the property** | **Both** |
| **Malware** |  |  |  |
| **Trojan** |  |  |  |
| **Virus** |  |  |  |
| **Worm** |  |  |  |
| **Ransomware** |  |  |  |
| **Phishing** |  |  |  |
| **Online financial crimes** |  |  |  |
| **Online Fraud** |  |  |  |
| **Password cracking** |  |  |  |
| **Hacking** |  |  |  |
| **Photo-hacking** |  |  |  |
| **Sextortion** |  |  |  |
| **Image-based sexual crimes** |  |  |  |
| **Revenge Pornography** |  |  |  |
| **Cyberstalking** |  |  |  |
| **Trolling** |  |  |  |
| **Cyberbullying** |  |  |  |

End of Table

End of Question

[View discussion - Activity 2 Classifying the different types of cybercrime](" \l "Session2_Discussion1)

End of Activity

## 2.1 Trolling

The term trolling has been widely used since the apparition of the internet and it refers to all online deviant behaviours generated by individuals towards other individuals and/or groups that are repetitive and disruptive in nature (Fichman & Sanfilippo, 2016). However, this is slightly simplistic as trolling behaviours do evolve constantly in line with how the online environment itself changes. Vaisman and Fichman (2012), cited in Fichman & Sanfilippo, (2016, p.6) consider four factors to explain the variety within trolling behaviours depending on:

1. Location: The distinction between asynchronous (when people communicate but not at the same time such as blog comments) and synchronous communication (live conversation such as chat room). Both types of trolling exist but it is more difficult to account for within synchronous settings as the context is not recorded (Fichman & Sanfilippo, 2016).
2. Relationships: Trolls usually target random, innocent people as well as the community. When they start targeting individuals, it overlaps with other online deviant behaviours such as harassment or bullying. According to Fichman and Sanfilippo (2016), trolls usually act individually and usually hide their identity, though they can coordinate their behaviours with other trolls as there are evidence of camaraderie between trolls such as in the controversial online platform [TATTLE.life](https://tattle.life/) where people gather to openly and freely troll about social media influencers, even referring themselves as trolls (e.g. tattle trolls….), or reflecting on [what is an online troll?](https://tattle.life/threads/what-is-an-online-troll.4791/) – See [#tattlelife](https://twitter.com/hashtag/tattlelife?lang=en). The reasons why this website has received so much attention is that the purpose of the site is to group people with trolling tendencies together. Therefore, group trolling not only normalises this type of behaviour but also it intensifies the damage under the greatest anonymity with made up usernames (Fogarty, 2019).
3. Intentions: Originally trolling behaviours were thought as being unintentional because it was just for fun (Buckels, Trapnell, & Paulhus, 2014). While you could find up to 135 different types of trolls identified from many online resources (Nuccitelli, n.d.), psychological evidence has been more reserved in categorising the different types of online trolls. Indeed, research has mostly focused on motivations or intentions either looking at personality (e.g., Buckels et al., 2014), or explanations of intentions such as being ideological, non-ideological, religion driven, grief driven, fun driven, or political (Fichman & Sanfilippo, 2016). However, as Coles and West (2016) argued, beyond the broadness of the term ‘troll’ and the many subtypes, it is important to look at the term as having variable meanings, intentions, and varied sub-types between different platforms and the course of interaction.
4. Behavioural practices: Trolls themselves usually do not identify their behaviour as being aggressive but more as being opiniated. However, the pattern is that trolls usually set ‘discursive’ trap to create a reaction through controversial comments or questions. What truly defines someone as a troll is the repetitive action of their behaviour towards the same individual or online community, repeating the same ideas and ignoring the responses and challenges directed at them (Shachaf & Hara, 2010).

Start of Activity

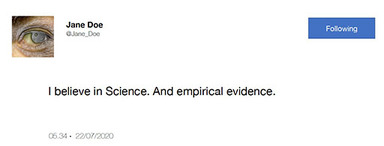
**Activity 3 Which of these examples is trolling?**

Allow 10 minutes

Start of Question

Jane Doe posted the following on a popular social media site.

Start of Figure



[View description - Uncaptioned Figure](" \l "Session2_Description1)

End of Figure

Look at the six examples of trolling below and decide whether you feel it falls under the trolling category or being opiniated. Type your anwer into the box.

Start of Table

Table 2 Replying to @Jane\_Doe:

|  |  |
| --- | --- |
| ‘… and very poor grammar 😱’ | *Provide your answer...* |
| ‘I don’t have opinions; I have facts at my disposal.’ | *Provide your answer...* |
| ‘As my friend Phoebe Buffay would say… ‘this is brand new information’’ | *Provide your answer...* |
| ‘You are just an idiot who don’t understand science. It’s not about belief!’ | *Provide your answer...* |
| ‘I disagree, I don’t think scientific evidence and religious beliefs are incompatible.’ | *Provide your answer...* |
| ‘Interesting statement. Belief in science? that's an oxymoron.’ | *Provide your answer...* |

End of Table

End of Question

[View discussion - Activity 3 Which of these examples is trolling?](" \l "Session2_Discussion2)

End of Activity

Internet trolling provides a good illustration of some of the definitional and practical difficulties, and the challenges that these present for legislative and criminal justice responses. Indeed, offending people and being antagonistic is not necessarily criminal. Herring et al. (2002) provide an interesting analysis of attempts to manage a troll on a feminist web-forum, in which the troll employs a number of tactics (for example name calling, deliberately misunderstanding other users, pretending to be sincerely trying to understand the issues). This troll was clearly a source of ongoing annoyance, and at times was offensive, but the attempts to control him (albeit with limited success) did not resort to criminal sanctions.

## 2.2 Non-consensual distribution of sexual images

Image-based sexual crimes are multi-faceted and incorporate crimes that involve obtaining sexual or degrading imagery of individuals and then threatening to distribute these images, as a means of blackmailing victims into producing more imagery or committing harmful acts towards others.

Even though these types of crime are not restricted to one particular gender, it is important to note that most victims are females (Mc Glynn, Rackley, & Houghton, 2017). Furthermore, the ease of obtaining and distributing sexual imagery online without consent and using sensitive materials as a means of blackmailing victims, means that the frequency and scale of the problem has mushroomed. The nature of the harassment being sexualised and misogynistic means that victims are often blamed for sharing the images in the first place. However, because the images are used in a way that is not intended means that the person who originally shared the images is not responsible and should be treated as a victim in its own right.

Non-consensual distribution of sexual images can also unveil other forms of cybercrime such as revenge pornography, child pornography, sextortion and many other types. The most common type of non-consensual obtention or distribution of sexual images are related to child pornography and by extension it could also results in the solicitation of in-person sexual contact known as online grooming. Due to the sensitive nature of some of those sub-types of image-based sexual crimes, this course will only cover sexting, photo hacking as examples of this type of cybercrime.

Start of Figure



[View description - Uncaptioned Figure](" \l "Session2_Description2)

End of Figure

### Sexting

The ready availability of mobile communication technologies and the increase in the use of the internet has seen the development of what is known as ‘sexting’. ‘Sexting can be understood as the sending or posting of sexually suggestive text messages and images, including nude or semi-nude photographs, via mobiles or over the Internet’ (Cooper et al., 2016, p. 706). ‘Sexting’ becomes problematic and falls into the cybercrime category when the images are shared without the victim’s knowledge. This might be through ‘**hacking**’, where the images are stolen from the legitimate recipient, or it could be through the intended recipient sharing them (either with other acquaintances or in online forums etc.) without the consent of the sender. Senders might be unaware about the possible distribution of their images, or a previously trusted receiver may turn out to not merit such trust (such as an ex-partner who shares images – sometimes known as ‘revenge pornography’). Research has found that women usually only send sexual images in the context of a relationship where there is trust (Samimi and Alderson, 2014), and therefore at the time the images are sent, there is little reason for the sender to think that they will be passed on without consent.

However, the harm is constant and amplified due to the permanency of the images stored on the internet. Even if the original images/videos are removed, copies could have been made and could circulate indefinitely (Langos, 2015). As a result, the long-term impact of such crime could be far more damaging than originally intended, permanently discrediting the victim’s reputation on a personal and professional level.

### Photo-hacking

As you have read in the previous section, self-taken sexual images may sometimes be produced non-consensually by tricking or coercing the victim, while in other situations production of the image may have been consensual but it is non-consensually distributed beyond the intended recipient(s). Sometimes this non-consensual distribution is achieved by hacking into private images that have been stored online. A high-profile example of this was the celebrity photo-hacking scandal in 2014, where nude images of celebrities were stolen from online accounts and disseminated publicly. Bates (2017) suggests that these cases of celebrity photo-hacking and non-consensual pornography, targeting well-known women such as Jennifer Lawrence and Kate Upton, have led to deeper discussion in the media of issues around non-consensual pornography, consent, and the oppression of women. Jennifer Lawrence termed what happened to her as a ‘sex crime’ (Kashner, 2014) and described how violated she felt by the experience (Oppenheim, 2017).

However, although the theft and distribution of the images was a crime, legally it was not considered a sex crime, and some commentators (e.g. Mackie, 2014) suggest that it is the responsibility of internet users to understand that the worldwide web is not a private space, placing the responsibility for the crime with the victims, rather than the perpetrators.

Start of Activity

**Activity 4 How does photo hacking affect victims?**

Allow 15 minutes

Start of Question

While the large-scale theft and distribution of images of celebrity photo-hacking victims has been important in drawing attention to the issues around non-consensual access and distribution of intimate images, not all victims are in the public eye. Listen to the following audio clip from Danger in the Download, in which Angie describes her experience of having her private images hacked. Make some notes on the questions below as you listen:

1. How does Angie describe her feelings about what happened to her?
2. Are there aspects of the online nature of the crime that make it particularly troubling for Angie?

Start of Media Content

Audio content is not available in this format.

Audio 1 Danger in the download

[View transcript - Audio 1 Danger in the download](" \l "Session2_Transcript1)

End of Media Content

End of Question

[View discussion - Activity 4 How does photo hacking affect victims?](" \l "Session2_Discussion3)

End of Activity

## 2.3 Hacking

In the previous section, you have learned that private images are sometimes accessed by **hacking** the accounts of other users. The term hacking might make you think of computer geniuses cracking complex codes, and therefore that increasingly sophisticated computer security is the solution to the problem; in reality, while hacking can sometimes require advanced skills, many instances require little technological expertise on the part of the hacker. For example, in 2014, a number of former employees of the now defunct News of the World were convicted on phone hacking charges, having accessed messages belonging to both celebrities and crime victims to provide material for the newspaper (BBC News, 2014). In many cases they had been able to gain access to voicemail messages quite easily, by exploiting the fact that users had not reset the default voicemail PIN code. Phone service providers have since made changes to their systems so that default PIN codes no longer exist, but many users still use meaningful information such as their birthdates as PIN codes, making them easy to guess (BBC News, 2011). This highlights the importance of considering both technological and human aspects when developing security measures.

As explained above, gaining access to other people’s accounts can sometimes be accomplished very simply because people choose simple passwords such as ‘123456’ and ‘password’ (Morgan, 2017). The reason why people choose simple passwords or reuse across sites is due to a poor fit between system and user (Conklin et al., 2004). When password authentication was introduced as a security measure online, there were only a limited number of systems and users, and it was effective in that context. However, this approach is less effective in the current situation with millions of systems and many millions of users. Indeed, designers did not take into account that users now have multiple usernames and passwords to remember. This means that users have been left to develop their own individual strategies to manage their various online accounts, and sometimes these strategies (e.g. writing down passwords, reusing details) can compromise security.

Start of Figure



[View description - Uncaptioned Figure](" \l "Session2_Description3)

End of Figure

Another possible explanation could be that people don’t know what constitutes good password security. However, in a survey by Tam et al. (2009), respondents showed an ability to distinguish between strong and weak passwords, and an understanding of poor password management behaviours, but there was a trade-off between convenience and security. People were more willing to engage in password management practices that were inconvenient, but which increased security, for accounts where they could foresee an immediate negative consequence for themselves should security be breached (e.g. a bank account), and less willing to do so for accounts where they could not (e.g. email). However, a hacker with access to an email account can use this to reset passwords and learn other personal information that could facilitate access to other user accounts, including bank accounts, so this approach may be short-sighted.

Attempts to alter user behaviour at a system level, by introducing mandatory rules for the creation of passwords (e.g. forcing account holders to use a combination of letters, numbers and punctuation), reduce vulnerability by making it less likely that a stranger could guess the password. However, they simultaneously increase the likelihood that the genuine account holder will forget their password, thereby increasing the use of memory strategies which introduce other sources of vulnerability (Gehringer, 2002; Conklin et al, 2004). Therefore, it is important that security systems are carefully designed to take into account the human behaviour of the people who use them, as well as the ingenuity of those who wish to hack them.

## 2.4 Malware

As you are accessing this course online, you are already likely to be familiar with the need to protect your system against attacks from viruses and other types of **malware**.

Start of Figure



[View description - Uncaptioned Figure](" \l "Session2_Description4)

End of Figure

However, as with hacking, those who produce malware are inventive, and are often able to exploit weaknesses in the system and make use of social engineering to introduce malware to a computer or network despite existing safeguards. There are two aspects of the criminal use of malware: firstly, creation of the malware; and secondly, distribution (Kirwan and Power, 2013). The term ‘malware’ encompasses a number of different types of malicious program, and in common with the other types of cybercrime you have explored so far, motivations for creating and distributing malware are varied. While psychological research on creators of malware is limited, Kirwan and Power (2013) suggest that the underlying motivations may have changed over time, and that while early creators of malware were often motivated by a desire to identify system vulnerabilities, or by the intellectual challenge, there is an increasing tendency towards creation and distribution of malware for financial gain.

You can learn more about the different types of malware as part of the free OpenLearn course: [Introduction to cyber security: stay safe online](https://www.open.edu/openlearn/science-maths-technology/introduction-cyber-security-stay-safe-online/content-section-overview).

## 2.5 Online fraud

So far you have learned how social engineering can be a useful tool for those who wish to distribute malware. However, it can also be used to gain access to personal information, which may allow unauthorised individuals to access accounts, facilitating photo hacking. However, perhaps the most familiar form of social engineering used by cybercriminals is the **phishing** email, which is normally used to gain information that can be used to commit online fraud. This phishing email often appears to be from a legitimate business or bank and asks for an immediate response from the recipient in order to prevent serious consequences (for example, the account being frozen). When the recipient clicks on the link in the email, they are taken to a fake website and asked to enter their account details. By doing so, they provide fraudsters with the information needed to access their genuine account and steal money. As in the previous examples, by manipulating human behaviour, cybercriminals can gain access to private accounts without being skilled in hacking.

Advance fee fraud is another online scam with which you might be familiar with. There are many variants, but the basic format is the same. The fraudster sends an email in which they claim to need help in moving a large amount of money from one country to another and are prevented from doing so due to some unfortunate set of circumstances. The recipient of the email is asked to assist by sending a small amount of money and is offered a share of the large sum of money as their reward (Action Fraud, 2020). Of course, the large sum of money does not exist, and anyone who sends money will never see it again. Online dating romance scam (Buchanan and Whitty, 2014; Whitty and Buchanan, 2012; 2016) is a subtype of advance fee fraud, in which the scammer or scammers pose as someone interested in forming a relationship with their victim. They use photographs of attractive people to create fake profiles and make contact with their victims via social networking sites or online dating sites (e.g. Aransiola and Asindemade, 2011; Rege, 2009; Whitty and Buchanan, 2012). This is sometimes termed ‘catfishing’. The focus in this type of crime is on building a relationship with the victim so that they will then comply with requests for money.

Start of Activity

**Activity 5 Why does online dating scam succeed?**

Allow 10 minutes

Start of Question

Watch the video of FBI Special Agent Christine Beining describing romance scams. As you watch the video, note down any information related to the victims’ likely characteristics and techniques used to gain trust and obtain the desired result.

Start of Media Content

Watch the video at [YouTube.com](https://www.youtube.com/watch?v=BmIvqOYwGGU&hl=en&fs=1&rel=0).

Video 2 Romance scams

End of Media Content

End of Question

[View discussion - Activity 5 Why does online dating scam succeed?](" \l "Session2_Discussion4)

End of Activity

Buchanan and Whitty (2014) also found that higher scores on ‘idealisation’ of romantic partners were associated with an increased likelihood of being a romance scam victim, but the other factors they investigated – including extraversion, agreeableness, sensation-seeking, neuroticism, and loneliness – were not associated with the likelihood that someone would become a romance scam victim.

You can read about the many different types of online fraud at the [Action Fraud website](https://www.open.ac.uk/libraryservices/resource/website:118067&f=30574).

## 3 Victim’s experience of cybercrime

You have seen in the previous sections that the accurate distinction between different types of cybercrime can be difficult.

However, regardless of the specific type of cybercrime experienced, a common research finding is that it can have adverse consequences for its victims. Cyber-victimisation can be seen to have similar social, psychological and physiological effects to those experienced by people victimised in the parallel offline offences. This suggests that cybercrimes should be responded to with equal concern to their offline equivalents. For instance, the effects of cyberbullying are similar to those of traditional bullying (Smith et al. 2008). In the same respect, Dreßing et al. (2014) identify that the impact of cyberstalking is similar to that of offline stalking. However, there is, as yet, little research that looks at the effects of trolling on those targeted.

Start of Figure



[View description - Uncaptioned Figure](" \l "Session3_Description1)

End of Figure

## 3.1 Impact of cybercrime on victims and coping strategies

It is important to add that for certain types of cybercrime, the victimisation is multi-faceted. For instance, while the negative impact of online fraud on the victims might appear to be solely financial, a study by Button et al. (2014) found that in addition to financial hardship, some victims might experience negative effects on their mental health, physical health and personal relationships. Whitty and Buchanan (2012; 2016) argue that victims of online dating romance scams suffer a ‘double hit’, as they suffer the loss of a relationship as well as experiencing financial loss. The survey conducted by Buchanan and Whitty (2014) showed that there are large individual differences in the degree of emotional distress reported by victims, and they found that sometimes emotional distress was high even where there was no financial loss. More in-depth interviews with a small number of victims identified that people who had lost money to online romance scams reported greater distress at the loss of their relationship than their money. Their distress was exacerbated by a lack of social support, with some victims reporting that they experienced anger and blame from family and friends.

Start of Table

|  |  |
| --- | --- |
| The literature has identified the following consequences on cyber-victimisation:   * Social withdrawal/anxiety * Depression * PTSD * Obsessive behaviours * Loss of confidence * Reduction in self-esteem. * Headaches * Abdominal pain/stomach problems * Eating disorder * Sleep disorder * Not feeling safe * Self-harm * Suicide tendencies * Feeling helpless * Panic attacks * Mistrust of others   (Låftman et al., 2013; Sourander et al., 2010; Schneider et al., 2012; Bates, 2017) | Start of Figure  An image of a person looking at a computer tablet.  [View description - Uncaptioned Figure](" \l "Session3_Description2)  End of Figure |

End of Table

Similarities in coping strategies for victims of cybercrime were also found, with victims initially tending to turn to negative coping strategies such as alcohol use and avoidance, before engaging with more positive approaches such as seeking counselling and undertaking advocacy work. However, with cybercrime directed at the person, the issue of victim blaming is important to consider, drawing more specifically on research into public attitudes towards sexual violence that place the blame for onto the victims.

## 3.2 Victim blaming

When a crime is committed, the victims themselves and other members of society often seek to understand why the crime happened. Victims may ask questions like ‘why me?’, ‘why did that have to happen to me?’. Friends, family and other members of society might ask ‘why did that happen?’ but may also ask questions like ‘could the victim have avoided being targeted?’ or ‘did the victim do something to make themselves vulnerable?’. These latter questions lead to the idea that the victim is at least partially responsible for their own victimisation.

The notion of victim blaming has long been the subject of academic study. Early victim typologies (such as those developed by Mendelsohn in the 1930s for crimes against the person) considered the role victims could be seen to play in their own victimisation. Modern academic study has moved away from this type of victim blaming, and it is more widely understood that the perpetrator of a crime should be the one held to blame. Nonetheless, victim blaming is still frequently encountered. Victims who are seen as making themselves vulnerable are particularly likely to be blamed (e.g. Gray, 2015). This type of blaming forms part of a wider set of beliefs and attitudes towards online victimisation where blame and responsibility is put on the failure to avoid victimisation due to victims’ greediness and/or gullibility for instance in relation to online dating scams (Cross, 2015) or initial consent given to take/send the picture to someone else in cases of non-consensual pornography and revenge porn. Bates (2017) refers this type of thinking as the ‘she should have known better’ argument. In offline contexts, this type of thinking can be seen in rape myth beliefs that suggest rape victims are to blame because of something that they did, for example: ‘they walked down a dark alley on their own’; ‘they got drunk’; ‘they invited them back to their house’.

Start of Figure



[View description - Uncaptioned Figure](" \l "Session3_Description3)

End of Figure

The theory of just-world beliefs (Lerner, 1980) has been used to account for why people may blame victims. The underlying principle is that the world is a fair place, and therefore if people are good, then nothing bad will happen to them. The consequence of this is that if something bad happens to people (i.e. being a victim of a crime), then they must have done something to bring this bad thing upon them. In this context, this allows people to feel safe if they avoid doing the things that they believe that the victim has done. For example, victim blaming in this context can consist of arguments that people do not have to go online, do not have to use social media and can always log off if they do not like what is happening online. If people do use social media, and do not deactivate their accounts in response to harassment, then they are often characterised as having put themselves in the way of harm. Conversely, it this type of reasoning allows cybercriminals such as trolls and other online abusers to rationalise their behaviour by saying that the victim can always avoid being victimised by not going online, or not posting comments. However, this means that it is the abused, rather than the abuser, who is expected to change their behaviour.

## 4 What are the motivations for cybercrime?

In this section you will move to consider the reasons that have been identified to explain cybercrime. When looking at the motivations, the key aspects to consider are:

* Individual differences (e.g., personality traits)
* The context of the online environment
* The characteristics given by observers to those performing the various types of cybercrime.

Psychological research has been able to identify personality correlations of self-reported cyber-criminality or trolling, particularly the ‘dark tetrad’ of personality which includes the personality traits of narcissism, Machiavellianism, psychopathy and sadism. Buckels et al. (2014) used personality inventories to assess these traits; hence these are not clinical assessments. They found that sadism, psychopathy and Machiavellianism all predicted trolling behaviour, with sadism being the strongest predictor. Similarly, Craker and March (2016) found psychopathy and sadism to be predictors of trolling on Facebook. In their research, Craker and March also included a measure of negative social potency (obtaining social reward from negative actions), and this was found to be a stronger predictor of Facebook trolling than any of the personality characteristics.

In a nutshell, cybercriminals’ motivations are wide-ranging, and it depends on the crime being looked at. For instance, all cybercrimes linked to ransomware, phishing, online financial crimes, online fraud, password cracking, malware, hacking, sextortion are mainly motivated by financial gain but for some of them motivation can be due to pranks, activism, cyber theft, espionage (e.g. malware). Cybercrimes against the person such as cyberstalking, cyberbullying, trolling, revenge pornography are likely to be motivated by hatred, desire to inflict pain and harm to either known or unknown individuals, groups or community. Lastly, for image related crimes, it could be motivated by a desire to control, to intimidate, sexual gratification, social status building (Henry, Powell, and Flynn, 2017).

As you can see, cybercriminals’ motivations are largely determined by the crime itself and due to the versatility of the different online crimes, it is difficult to consider the motivations for cybercrime on a general level. Additionally, research around motivations for cybercrime can be difficult to investigate because it relies to some extent on the words of criminals who may not see their behaviour as being deviant (e.g. such as in the case of trolling), they may not wish to disclose their reasons for engaging in criminal activities, or may not have complete insight into their own motives.

## 5 Intervention on cyber criminality

Earlier on in the course, you have looked at the different types of criminal activities that fall within the cyber criminality, and the different ways in which they are connected. So far you have learned about crimes committed via the internet, which have financial and/or psychological consequences for the victims. While online versions of offline crimes might once have been viewed less seriously, there is increasing recognition that the impact of online crimes can be as great as, or in some cases greater, than offline versions of the crime (for example, victims of online image-based sexual offences suffer longer-term effects due to wider distribution and longevity of images on the web). Initially the law struggled to address online criminality, as existing laws did not always fit the online crimes. However, in some cases (e.g. revenge porn), specific laws have now been developed (Nigam, 2018) to address these more effectively. There is information about the way in which these crimes are being tackled in jurisdictions across the world on the [Centre for Internet & Society](https://www.open.ac.uk/libraryservices/resource/website:118207&f=30596) website.

In some cases, the match between online and offline versions of a crime make it simple to define criminality and pursue the perpetrator using existing laws. For example, it is easy to see that both physically stealing money from a bank, and electronically stealing money from an online bank account, are forms of theft: regardless of the means used to take the money, the financial loss is the same. However, what if the theft was of virtual money or objects that belong to someone in an online world? Should laws be developed to regulate behaviour in virtual settings?

## 5.1 Where cybercrime and online anti-social behaviour meet

In some cases, behaviours labelled as trolling for instance, such as threats to rape and kill, or persistent harassment, can be clearly identified as possible criminal offences that should be investigated and potentially prosecuted. At the other extreme, there are online behaviours that fall within the above definition that are not criminal offences. For example, on forums or other internet sites it is quite common to see irrelevancies, pointless questions, arguments and suchlike that can all be forms of trolling. While these may be disruptive or aggravate other users, they do not seem to merit criminal justice responses.

There is currently no legislation that specifically targets trolling (at the time of writing, 2020). However in England and Wales there are a number of pieces of legislation that can be used to prosecute trolling, and the Crown Prosecution Service identifies the Malicious Communications Act 1988 and the Communications Act 2003 as being the relevant legislation. Depending upon the content of the behaviour, other potentially relevant legislation includes the Protection from Harassment Act 1997 and the Criminal Justice and Courts Act 2015. Even considering just England and Wales, the legislative framework for these offences is complex, and different jurisdictions handle these behaviours differently.

Having considered two extremes of trolling, this leaves a significant question as to where the line should be drawn between the offensive/annoying types of trolling and those that warrant a criminal justice response. At present there is not a clear answer to this question, but the issue of where to draw the line is something to be aware of when considering cybercrime.

## 6 Reflecting on your experiences

The material covered so far in this course has shown that there are a variety of different types of online victimisation. As well the direct victims of cybercrime, the awareness of the possibility of being a target may influence other internet users. This therefore can be seen as a type of secondary victimisation that may serve to alter and constrain our online behaviours. In this final activity you are going to consider what you have learned and whether this might change how you will engage online.

Start of Activity

**Activity 6 Keeping yourself safe online, or secondary victimisation?**

Allow 20 minutes

Start of Question

Reflect on the following questions:

1. Based on the content of this course, what steps might you take to try to reduce the likelihood of being targeted by cybercriminals and internet trolls?
2. What are the implications of these measures?
   1. Do these measures contain an element of victim blaming?
   2. How do you feel about these measures?

End of Question

*Provide your answer...*

[View discussion - Activity 6 Keeping yourself safe online, or secondary victimisation?](" \l "Session6_Discussion1)

End of Activity

## 7 Conclusion

This course has provided an introduction to some of the different types of cybercrime, considering the similarities and differences in the definitions and behaviours. You have looked at how it is challenging to recognise the differences between anti-social and criminal behaviour. You have also learned about the impact of cybercrime on victims and the motivations for cybercrime, as well as the challenges that some of these crimes raise in terms of crime prevention and legal redress.

Start of Table

|  |  |
| --- | --- |
| Now that you are at the end of this course, you should be able to:   * outline the impact on victims * distinguish different types of cybercrime, considering the similarities and differences in the definitions and behaviours * identify the motivations and behaviours of cybercriminals * illustrate the current interventions to tackle cybercrime. | Start of Figure  An image of a person sat at a table with one arm in the air, palm up. Above the palm is an image of a love heart, similar to that of a like option found on social media platforms.  [View description - Uncaptioned Figure](" \l "Session7_Description1)  End of Figure |

End of Table

This Open Learn course is an adapted extract from the Open University course [DD802 Investigating forensic psychology.](http://www.open.ac.uk/postgraduate/modules/dd802)

Explore the collection of [Postgraduate study in psychology and criminology](https://www.open.edu/openlearn/health-sports-psychology/psychology/postgraduate-study-psychology-and-criminology).

## Glossary

Cyber bullying

Cyberbullying has been defined as ‘an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself’ (Smith et al., 2008, p. 376).

Cyberstalking

Cyberstalking is aimed at a specific individual and entails ‘using the Internet as part of a targeted campaign that causes fear, distress or alarm’ (Cavezza and McEwan, 2014, pp. 955-956).

Hacking

Bypassing security systems to make an unauthorised intrusion into a computer or network.

Image-based sexual crimes

The use of nude/sexual images of a victim for criminal purposes.

Malware

Malicious software that interferes with the normal functioning of a network or computer.

Online financial crimes

Illegally obtaining money or other financial rewards using online methods.

Online Fraud

Fraud that is committed using online methods. You can read about the many different types of online fraud at the [Action Fraud website](https://www.open.ac.uk/libraryservices/resource/website:118067&f=30574).

Password cracking

The process of recovering or guessing the correct password needed to gain access to a system or account.

Phishing

Techniques used to persuade people to divulge information that can be used in online fraud (e.g. bank account passwords).

Photo-hacking

Hacking that is specifically targeted at gaining unauthorised access to photos, particularly nude images.

Ransomware

A type of malware that renders a computer and/or its files inaccessible, with a demand for payment to unlock it/them.

Revenge Pornography

Kamal and Newman (2016, p. 361) describe revenge pornography as ‘the online release of explicit photographs or videos of an individual without permission for the purpose of humiliation.’

Sextortion

‘Situations in which perpetrators threaten to expose sexual images to coerce victims to provide additional pictures, engage in sexual activity, or agree to other demands’ (Wolak et al., 2017, pp. 1).

Trojan

A malicious piece of software that misleads users into activating it by masking its true intent. For example, a file that destroys software which is named ‘virus protection program’.

Trolling

‘The act of ‘trolling’ is generally defined as being a negative online behaviour intended to disrupt online communications, aggravate internet users and draw individuals into fruitless debates’ (Coles and West, 2016, p. 44).

Virus

Software that replicates by inserting its code into other programs and files, often causing damage by corrupting data or creating a ‘back door’ to allow attackers to access the system.

Worm

A stand-alone malware program that can self-replicate and spread to other computers.

## References

Action Fraud (2018) 419 emails and letters. Available at: <https://www.actionfraud.police.uk/a-z-of-fraud/419-emails-and-letters> (Accessed: 04 November 2020).

Aransiola, J. O. and Asindemade, S. O. (2011) ‘Understanding cybercrime perpetrators and the strategies they employ in Nigeria’, Cyberpsychology, Behavior, and Social Networking, 14, pp. 759−763.

Bates, S. (2017) ‘Revenge porn and mental health: A qualitative analysis of the mental health effects of revenge porn on female survivors,’ Feminist Criminology, 12(1), pp. 22−42.

BBC News (2011) ‘Who, What, Why: Can phone hackers still access messages?’, BBC News 6 July. Available at: <https://www.bbc.co.uk/news/magazine-14044499> (Accessed: 04 November 2020).

BBC News (2014) ‘Hacking Trial: the verdicts’, BBC News 4 July. Available at: <https://www.bbc.co.uk/news/uk-27145187> (Accessed: 04 November 2020).

Bishop, J. (2014) ‘Representations of ‘trolls’ in mass media communication: a review of media-texts and moral panics relating to ‘internet trolling’, International Journal of Web Based Communities, 10(1), pp. 7-24.

Buchanan, T. and Whitty, M. T. (2014) ‘The online dating romance scam: causes and consequences of victimhood’, Psychology, Crime and Law, 20(3), pp.261–283.

Buckels, E. E., Trapnell, P. D. and Paulhus, D. L. (2014). ‘Trolls just want to have fun’ Personality and individual Differences, 67, pp. 97–102.

Button, M., Lewis, C. and Tapley, J. (2009) Fraud typologies and the victims of fraud literature review. London, National Fraud Authority.

Button, M., Lewis, C. and Tapley, J. (2014) ‘Not a victimless crime: The impact of fraud on individual victims and their families’, Security Journal, 27(1), pp. 36−54.

Canter, D. and Youngs, D. (2009) Investigative Psychology: Offender Profiling and the Analysis of Criminal Action, Chichester, Wiley.

Coles, B. A. and West, M. (2016) ‘Trolling the trolls: Online forum users constructions of the nature and properties of trolling’, Computers in Human Behavior, 60, pp. 233–244.

Conklin, A., Dietrich, G. and Walz, D. (2004) ‘Password-based Authentication: A System Perspective’, Proceedings of the 37th Annual Hawaii International Conference on System Sciences, pp. 1−10.

Cooper, K., Quayle, E., Jonsson, L. and Göran Svedin, C. (2016) ‘Adolescents and self-taken sexual images: A review of the literature’, Computers in Human Behavior, 55, Part B, pp. 706−716.

Cross, C. (2015). ‘No laughing matter: Blaming the victim of online fraud’, International Review of Victimology, 21(2), pp. 187–204.

Dreßing, H., Bailer, J., Anders, A., Wagner, H. and Gallas, C. (2014) ‘Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims’, Cyberpsychology, Behavior, and Social Networking, 17(2), pp. 61–67.

Fichman, P. and Sanfilippo, M.R. (2016). ‘Online trolling and its perpetrators: Under the cyberbridge’. Lanham, Maryland: Rowman & Littlefield.

Fogarty, P. (2019) ‘ What is tattle life? Harmless forum or hotbed of harassement?’ Available at: <https://www.hitc.com/en-gb/2019/06/27/what-is-tattle-life-mrs-meldrum-harassment-bullying-petition/> (Accessed: 04 November 2020)

Gehringer. E. F. (2002) ‘Choosing passwords: security and human factors’, 2002 International Symposium on Technology and Society, pp. 369−373.

Gray, J. M. (2015) ‘What constitutes a “reasonable belief in consent” to sex? A thematic analysis’, Journal of Sexual Aggression, 21(3), pp. 337−353.

Henry, N., Powell, A., & Flynn, A. L. G. (2017). Not Just ‘Revenge Pornography’: Australians’ Experiences of Image-Based Abuse: A Summary Report, RMIT University. Available at: <https://researchmgt.monash.edu/ws/portalfiles/portal/214045352/revenge_porn_report_2017.pdf> (Accessed: 04 November 2020).

Herring, S., Job-Sluder, K., Scheckler, R. and Barab, S. (2002) ‘Searching for safety online: Managing “trolling” in a feminist forum’, The Information Society, 18, pp. 371–384.

Kashner, S. (2014) ‘Both Huntress and Prey’, Vanity Fair, 20 October. Available at: <https://archive.vanityfair.com/article/2014/11/both-huntress-and-prey> (Accessed: 04 November 2020).

How People Use the Internet in 2020 (2020). How people use the internet in 2020. Available at: <https://www.broadbandsearch.net/blog/most-common-uses-internet-daily-life> (Accessed: 04 November 2020).

Kirwan, G. and Power, A. (2013) ‘Cyberbullying and Cyberstalking’, in Kirwan, G. and Power, A. Cybercrime: The Psychology of Online Offenders, Cambridge, Cambridge University Press, pp. 147–168.

Låftman, S. B., Modin, B. and Östberg, V. (2013) ‘Cyberbullying and subjective health: A large-scale study of students in Stockholm, Sweden’, Children and Youth Services Review, 35, pp. 112–119.

Langos, C. (2015) ‘Cyberbullying: The shades of harm’ Psychiatry, psychology and law, 22(1), pp.106–123.

Lerner, M. J. (1980) The Belief in a Just World: A Fundamental Delusion, New York, Plenum Press.

Mackie , J. (2014) ‘Jennifer Lawrence’s nude photo leak is not a sex crime, however much she’d like it to be’, The Independent, 10 October. Available at: <https://www.independent.co.uk/voices/comment/jennifer-lawrences-nude-photo-leak-was-a-scandal-but-legally-speaking-it-was-not-a-sex-crime-9786886.html> (Accessed: 04 November 2020).

McGlynn, C., Rackley, E. and Houghton, R. (2017) ‘Beyond ‘revenge porn’: The continuum of image-based sexual abuse’ Feminist Legal Studies, 25(1), pp. 25–46.

Mendelsohn, B. (1956) ‘The Victimology’, Etudes Internationales de Psycho-Sociologie Criminelle, 3, pp. 25–26 (in French).

Morgan (2017) ‘Announcing our Worst Passwords of 2016’, TeamsID [Online]. Available at: <https://www.teamsid.com/worst-passwords-2016/> (Accessed: 04 November 2020).

Naughton, J. (2016). ‘The evolution of the internet: from military experiment to general purpose technology’, Journal of Cyber Policy, vol.35, no. 1, pp.5-28.

Nigam, S. (2018) ‘Revenge Porn Laws across the World’, The Centre for Internet and Society [Online] Available at: https://cis-india.org/internet-governance/blog/revenge-porn-laws-across-the-world (Accessed: 04 November 2020).

Nuccitelli, M (n.d.) 130+ types of internet trolls and online provocateurs. Available at: <https://www.ipredator.co/troll/> (Accessed: 04 November 2020).

Ofcom (2020). Adult’s media use and attitudes 2020. Available at: <https://www.ofcom.org.uk/__data/assets/pdf_file/0031/196375/adults-media-use-and-attitudes-2020-report.pdf> (Accessed: 04 November 2020).

Oppenheim, M. (2017) ‘Jennifer Lawrence addresses nude photo hack: “It was so unbelievably violating”’, The Guardian, 21 November. Available at: [https://www.independent.co.uk/ arts-entertainment/ films/ news/ jennifer-lawrence-nude-photo-hack-pictures-video-leak-celebrity-addresses-issue-violating-a8067121.html](https://www.independent.co.uk/%20arts-entertainment/%20films/%20news/%20jennifer-lawrence-nude-photo-hack-pictures-video-leak-celebrity-addresses-issue-violating-a8067121.html) (Accessed: 04 November 2020).

Rege, A. (2009) ‘What's love got to do with it? Exploring online dating scams and identity fraud’, International Journal of Cyber Criminology, 3, pp. 494−512.

Samimi, P. and Alderson, K. (2014) ‘Sexting among undergraduate students’, Computers in Human Behavior, 31, pp. 230−241.

Schneider, S. K., O’Donnell, L., Stueve, A. and Coulter, R. (2012) ‘Cyberbullying, school bullying, and psychological distress: A regional census of high school students’, American Journal of Public Health, 102, pp. 171–177.

Shachaf, P. and Hara, N. (2010) ‘Beyond vandalism: Wikipedia trolls’, Journal of Information Science, 36(3), pp. 357–370.

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S. and Tippett, N. (2008) ‘Cyberbullying: its nature and impact in secondary school pupils’, Journal of Child Psychology and Psychiatry, 49(4), pp. 376–385.

Schneider, S. K., O’Donnell, L., Stueve, A. and Coulter, R. (2012) ‘Cyberbullying, school bullying, and psychological distress: A regional census of high school students’, American Journal of Public Health, 102, pp. 171–177.

Sourander, A., Brunstein Klomek, A., Ikonen, M., Lindroos, J., Luntamo, T., Koskelainen, M., Ristkari, T. and Helenius, H. (2010) ‘Psychosocial risk factors associated with cyberbullying among adolescents: A population-based study’, Archives of General Psychiatry, 67(7), pp. 720–728.

Tam, L., Glassman, M. and Vanderwauver, M. (2009) ‘The psychology of password management: a tradeoff between security and convenience’, Behaviour & Information Technology, 29(3), pp. 233−244.

Whitty, M. T. and Buchanan, T. (2012) ‘The online dating romance scam: A serious cybercrime’, Cyberpsychology, Behavior, and Social Networking, 15(3), pp. 181−183.

Whitty, M.T. and Buchanan, T. (2016) ‘The online dating romance scam: The psychological impact on victims – both financial and non-financial’, Criminology & Criminal Justice, 16(2), pp. 176−194.

Williams, M. L., & Levi, M. (2017). ‘Cybercrime prevention’. In N. Tilley & A. Sidebottom (Eds.), Handbook of crime prevention and community safety (pp. 454−469). London: Routledge.

Youngs, D., Ioannou, M. and Eagles, J. (2016) ‘Expressive and instrumental offending: Reconciling the paradox of specialisation and versatility’, International Journal of Offender Therapy and Comparative Criminology, 60(4), pp. 397–422.

## Acknowledgements

This free course was written by the DD802 module team and rewritten for OpenLearn by Axelle Philippon.

Except for third party materials and otherwise stated (see [terms and conditions](http://www.open.ac.uk/conditions)), this content is made available under a [Creative Commons Attribution-NonCommercial-ShareAlike 4.0 Licence](http://creativecommons.org/licenses/by-nc-sa/4.0/deed.en_GB).

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 free course:

Course image: Adapted from Jacob Morch / unsplash and geralt / pixabay (asset 293456)

Section 2.1 activity image: Axelle Philippon (asset 294436)

Section 2.2 image: Photo by Oladimeji Ajegbile from Pexels (asset 294086)

Audio 1: © BBC

Section 2.3 image: Image by Robinraj Premchand from Pixabay (asset 294338)

Section 2.4 image: Photo by cottonbro from Pexels (asset 294082)

Section 3 image: Photo by Ekaterina Bolovtsova from Pexels (asset 294083)

Section 3.1 image: Photo by Oladimeji Ajegbile from Pexels (asset 294084)

Section 3.2 image: Photo by Aliyah Jamous on Unsplash (asset 294344)

Conclusion image: Photo by Oladimeji Ajegbile from Pexels (asset 294089)

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.

**Don't miss out**

If reading this text has inspired you to learn more, you may be interested in joining the millions of people who discover our free learning resources and qualifications by visiting The Open University – [www.open.edu/openlearn/free-courses](http://www.open.edu/openlearn/free-courses?LKCAMPAIGN=ebook_&MEDIA=ol).

## Solutions

## Activity 1 Thinking about cybercrime

### Part

#### Discussion

According to Ofcom (2020), 87% of UK adults spent an average of 25 hours online per week. People go online for the following reasons (How People use the internet, 2020):

* social networks (including video calling)
* email
* be entertained (watching videos, music, online radio and podcasts)
* get information (search, blogs)
* news (including online newspapers, magazines)
* online games
* banking
* work (either earning money online or using the internet to work remotely)
* shopping
* education
* other access.

You might have put online fraud (such as issues around scams and various security breaches when paying or banking online. You might have thought about more subtle forms of victimisations such as trolling or cyberbullying on social media for instance or issues around protection of identity and reputation.

[Back to - Part](" \l "Session1_Part2)

## Activity 2 Classifying the different types of cybercrime

#### Discussion

Under that assumption, cyberbullying, trolling and cyberstalking, revenge pornography, image-based sexual crimes, sextortion, photo-hacking, hacking are likely to fall under the crime against the person category. Malware (including trojan, virus, worm), online financial crimes (including online fraud and password cracking) are more likely to fall under the crimes against the property category. However, you have probably realised that for many crimes it is not as clear cut and could be both directed at the person and the property (even if one is a by-product of obtaining the desired object or status) such as image-based sexual crimes who at face value could be seen as a crime against property (i.e. stealing an image) but ultimately it is a crime against the person. Moreover, cybercriminals usually combine criminal behaviours such as cyberstalking, sextortion, revenge pornography and possibly cyberbullying, therefore people can easily be victim of two (or more) types of cybercrimes simultaneously. Now have a look at some of them in details in the next sections.

[Back to - Activity 2 Classifying the different types of cybercrime](" \l "Session2_Activity1)

## Activity 3 Which of these examples is trolling?

#### Discussion

Those 6 examples illustrate different online behaviours. The first example is typical of ‘grammar trolls’ and it is not clear whether it falls under the definition of trolling or not. The intention could well be to patronise the author of the post, but it could also be a way to divert the post into less relevant discussion or ultimately, the author of this reply might just want to be humorous. This type of trolling is referred as ‘kudos trolling’ (Bishop, 2014).

The second example is a clever, non-aggressive reply that subtly point out the contradiction in the post (i.e. science and belief). It is done without attacking the author of the post and for that reason, it falls under the category of being opinionated.

The third example seems innocent on the surface, but the author here is making a cultural reference to a television show (Friends - popular in the 90s), and the tone here is sarcastic and the message itself indicate that Jane Doe post has no real informative purpose. This is another example of ‘kudos trolling’ and even more difficult to spot than the first example.

The fourth example, however, is more typical of common understanding of trolling. Indeed, the comment is aggressive, malicious with the intention of causing harm. Name calling is a way to intensify the abuse and this type of trolling is known as ‘flame trolling’ (Bishop, 2014).

The last two examples are other examples of opiniated posts rather than coming under the label of trolling due to adding something to the discussion and not personally attacking the author of the post.

Start of Table

Table 2 Replying to @Jane\_Doe: (answers)

|  |  |
| --- | --- |
| ‘… and very poor grammar 😱’ | trolling |
| ‘I don’t have opinions; I have facts at my disposal.’ | being opinionated |
| ‘As my friend Phoebe Buffay would say… ‘this is brand new information’’ | trolling |
| ‘You are just an idiot who don’t understand science. It’s not about belief!’ | trolling |
| ‘I disagree, I don’t think scientific evidence and religious beliefs are incompatible.’ | being opinionated |
| ‘Interesting statement. Belief in science? that's an oxymoron.’ | being opinionated |

End of Table

[Back to - Activity 3 Which of these examples is trolling?](" \l "Session2_Activity2)

## Activity 4 How does photo hacking affect victims?

#### Discussion

Like Jennifer Lawrence (Oppenheim, 2017), Angie expresses a feeling of violation. She is a victim of the initial theft, but this is compounded by the widespread distribution of the images, which is facilitated by the internet. She has the uncomfortable knowledge that people she has never met may have seen private images of her without her consent. She also highlights the potential damage on a professional level, as prospective employers may be able to access the images, and because of the permanence of images online they can never be truly erased.

[Back to - Activity 4 How does photo hacking affect victims?](" \l "Session2_Activity3)

## Activity 5 Why does online dating scam succeed?

#### Discussion

Christine Beining explained that:

* Scammers usually target vulnerable women (though men can be targeted but less so than women) , using the internet, with money and willing to give it. More specifically, they target people not in existing relationships and looking for love (divorced or widowed)
* they will use information available on the internet to find common grounds and use information to manipulate victims and get their trust. The relationships become intense very quickly. So, they can start asking for money using different excuses and promising to repay back the money.
* Scammers are usually part of criminal organisations and data about victims are recorded in ‘sucker lists’, which make them even more vulnerable and easily targeted to repeat victimisations (Button et al., 2009).

[Back to - Activity 5 Why does online dating scam succeed?](" \l "Session2_Activity4)

## Activity 6 Keeping yourself safe online, or secondary victimisation?

#### Discussion

Like you have seen in the video in Activity 1, everyone takes a different approach when it comes to engaging with the online world. Some people are heavily involved online (e.g., social media, online shopping, banking and so on) whereas others are taking a lighter approach to it (i.e. being reluctant to invest themselves more than necessary). Regardless of where you place yourself, up to now it might have been done without reflecting too much about its impact to your virtual and real lives, as well as the risks associated with it. While it cannot be said that cybercrime does not exist, it is probably erroneous to look at it as being the modern-day plague (Wall, 2008). Indeed, the risks associated with online activities are real. However, it is important to emphasise that actual cases of cybercrime are not as common as the media seems to portray its prevalence. This discrepancy could be because the problem has been exaggerated by the media instilling moral panic but could also be because cybercrime remains largely unreported and unprosecuted due to shame or lack of evidence. The best strategy to reduce cybercrime victimisation rates is to raise awareness (Williams and Levi, 2017). Therefore, reflecting upon how you personally engage online is useful since there are not ‘one size fits all’ model and what one person might find acceptable, another may not. Regardless of how much time you have spent on this activity, it is worthwhile as it is important to think about the best (and current) ways to protect yourself. The internet itself is a great source of information but it is always important to favour official guidance such as the UK government (National Cyber Security Centre). The NCSC is offering a wealth of useful advice on how to stay secure online. You can find, below, a selection of such guidance that might be relevant to you:

* [Protect devices from viruses and malware](https://www.ncsc.gov.uk/files/Protecting-devices-from-viruses-malware-infographic.pdf)
* [Phishing attacks: dealing with suspicious emails](https://www.ncsc.gov.uk/files/Phishing-attacks-dealing-suspicious-emails-infographic.pdf)
* [Using passwords to protect your devices and data](https://www.ncsc.gov.uk/files/Using-passwords-protect-devices-data-infographic.pdf)
* [Shopping online securely](https://www.ncsc.gov.uk/guidance/shopping-online-securely)
* [Sextortion phishing scams: how to protect yourself](https://www.ncsc.gov.uk/files/Sextortion-how-to-protect-yourself.pdf)
* [A guide to recovering your hacked online accounts](https://www.ncsc.gov.uk/files/Recovering-hacked-online-accounts-infographic.pdf)
* [Video conferencing: using services securely](https://www.ncsc.gov.uk/files/vtc_infographic.pdf)
* [Video chatting: a guide for protecting primary school age children](https://parentinfo.org/article/video-chatting-a-guide-for-parents-and-carers-of-primary-school-age-children)
* [Video chatting: a guide for protecting secondary school age children](https://parentinfo.org/article/video-chatting-a-guide-for-parents-and-carers-of-secondary-school-age-children)
* [Smart devices: using them safely in your home](https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home)
* [Smart security cameras: Using them safely in your home](https://www.ncsc.gov.uk/guidance/smart-security-cameras-using-them-safely-in-your-home)
* [Securing your devices](https://www.ncsc.gov.uk/guidance/securing-your-devices)
* [Online gaming for families and individuals](https://www.ncsc.gov.uk/guidance/online-gaming-for-families-and-individuals)
* [Social media: protecting what you publish](https://www.ncsc.gov.uk/guidance/social-media-protect-what-you-publish)
* [Revenge Porn Helpline](https://revengepornhelpline.org.uk/)
* [Information about cyberbullying and how to respond to it](https://www.internetmatters.org/issues/cyberbullying/learn-about-it/)
* [Cyberstalking support website](https://www.victimsupport.org.uk/crime-info/types-crime/stalking-and-harassment)

[Back to - Activity 6 Keeping yourself safe online, or secondary victimisation?](" \l "Session6_Activity1)

# Uncaptioned Figure

## Description

An image of a social media post that says I believe in Science. And empirical evidence.

[Back to - Uncaptioned Figure](" \l "Session2_Figure1)

# Uncaptioned Figure

## Description

An image of a person with their head in their hands looking at a laptop.

[Back to - Uncaptioned Figure](" \l "Session2_Figure2)

# Uncaptioned Figure

## Description

An image of a person in a dark room looking at a laptop.

[Back to - Uncaptioned Figure](" \l "Session2_Figure3)

# Uncaptioned Figure

## Description

An image of a child drinking from a mug with a computer screen in the background.

[Back to - Uncaptioned Figure](" \l "Session2_Figure4)

# Uncaptioned Figure

## Description

An image of a young person leaning against a bed with a laptop on their lap, arms folded and looking at the laptop.

[Back to - Uncaptioned Figure](" \l "Session3_Figure1)

# Uncaptioned Figure

## Description

An image of a person looking at a computer tablet.

[Back to - Uncaptioned Figure](" \l "Session3_Figure2)

# Uncaptioned Figure

## Description

A close up image of someone’s eye with a tear rolling down their cheek.

[Back to - Uncaptioned Figure](" \l "Session3_Figure3)

# Uncaptioned Figure

## Description

An image of a person sat at a table with one arm in the air, palm up. Above their palm is an image of a love heart, similar to that of a like option found on social media platforms.

[Back to - Uncaptioned Figure](" \l "Session7_Figure1)

# Video 1 Everyday perspectives: engaging online

## Transcript

OMER

It's, wherever I can, whenever I need it, I think. I'm not a really big social network user. Unless I have to get in contact with someone, I don't think I'll jump on it. It's a really good means of getting in contact with everyone and keeping up with everyone and what not. But usage terms, I don't think I use it too much.

JASON

With a mobile phone in your hand now it's pretty much the way of communicating with everybody. I mean, I use social media obviously. I use Facebook for personal usage, keeping in touch with friends and family that are all across the globe. And obviously, Twitter we use obviously as work purposes.

But I think, yeah, constantly, it's the first thing you check when you get up to see what's been going on the night before or, so that sort of stuff. So I think, yeah definitely, I'm quite a heavy Facebook user, if you like.

NOEL

I look things up. I occasionally order things on the internet. I am on Facebook. I'm not on Twitter. When I was working with asylum, I used it all the time for research. I do write a little bit now, and I use it for research. Mostly recipes, it must be said, at the moment. But yeah, I use it for those sorts of things, to find things out.

JESS

I use the internet a lot. I have a Facebook. I rely on emails for everything. Facebook, which is obviously for friends, I use that a lot for work. I know that I've got jobs in the past that I wouldn't have got without a Facebook. I don't own a television, so if I watch anything, that's online. Keeping in touch with friends is almost exclusively online, I'd say. Yeah, a lot of my life is online.

ALEX

So I've had my Facebook account since I was 15 years old at the pressure of all my peers, as most of the people. I've got a LinkedIn account since I've been in the professional world. I love LinkedIn. I've got a Twitter account that I only set up about three months ago together with my blog. I don't have an Instagram.

I think that's about it from the social media interaction. 80% of the time I'm on all these social media networks through my mobile. 20% in the evening when I get home or sometimes on the weekend. But mobile is the, by far, number one.

[Back to - Video 1 Everyday perspectives: engaging online](" \l "Session1_MediaContent1)

# Audio 1 Danger in the download

## Transcript

INTERVIEWER

Today cyberspace has grown beyond anything that its architects could have imagined. Up to a third of humanity has access to the Internet and an increasing proportion of them have come to depend on it for education, entertainment, social interaction, even their livelihoods. And inevitably among those two and a half billion souls there are some you might want to steer well clear of.

ANGIE

The first pictures that out were just me in bikinis. And then the second ones that came out were lingerie, like a bra and panties, a bunch of stuff like that. At that point I didn’t know that people could hack into that website. I thought it was secure.

INTERVIEWER

This is Angie. Aged 14 she decided to store some mildly suggestive pictures of herself online securing them in a password protected website. They were meant only for her boyfriend.

ANGIE

So, one summer my friend messaged me and he was like, oh you have to see this. He sends me a link and all the pictures that I thought were secure had been hacked and linked on to like a different website. At that point I realised that it wasn’t just going to stop at one friend who saw it.

INTERVIEWER

Before long the hacked information went viral on the open Internet.

ANGIE

Even now it’s still very popular on the Internet and it’s been four years and it’s only getting bigger.

INTERVIEWER

How many people in the end do you think have viewed these pictures of you?

ANGIE

A lot. Millions.

INTERVIEWER

Millions.

ANGIE

Yeah.

INTERVIEWER

That must be a weird feeling?

ANGIE

Yeah. And there’s no way that I could fully ever get rid of all the pictures. Once it’s on the Internet it’s there for good. It got to the point where I realised like what kind of future can I have knowing that my reputation is this bad. Imagine like what happens when a job comes between me and someone else and they can’t take me because of what’s happened. So basically it feels like my life is over.

[Back to - Audio 1 Danger in the download](" \l "Session2_MediaContent1)