Transformation by Innovation in Distance Education

16/12/20

STAYING SAFE ONLINE: AN OVERVIEW

INTRODUCTION

This document has been developed as a supporting resource for the TIDE programme, ICT & support staff strand 2019 & 202 cohorts, is intended to provide you with a basic overview of some of the key topic areas related to online safety. If you want to find out more we have provided some links to courses that you can take. We also suggest that you do a basic google search to find further information or raise any queries in the TIDE Facebook group https://www.facebook.com/groups/293490331907766/.

When you go online from a computer or a mobile phone, you take aspects of your identity with you, in the way you communicate and also transact with online services. How we communicate online and keep ourselves safe and secure in this digital environment, requires new skills and awareness. We need to manage our 'digital identity' and 'digital security'.

YOUR ONLINE IDENTITY

Social media provides a great way to connect with others and reach large and diverse audiences including friends, family, work colleagues and others who share our interests. The way in which we communicate and present ourselves online is very important. We need to be aware of our audience and their different values, and careful about using emotive language. Remember, when you post online you may be reaching a wider audience than you intended

See 'My digital identity'
https://www.open.ac.uk/libraryservices/beingdigital/activity/XK1020#page1

OUR LIVES ONLINE

We now do many activities online, including shopping, banking, socialising, learning, entertainment and accessing a range of digital services. This makes the Internet, also referred to as cyberspace, a place where criminals are also increasingly active.

Transformation by Innovation in Distance Education

16/12/20

WHAT IS CYBER SECURITY?

To be secure online, you need to carefully evaluate the validity of information you find before accepting it. You need to take precautions in order to stay safe against a variety of threats, such as malware, including viruses and trojans, and identity theft.

WHAT IS MALWARE?

This comes in three forms:

(i) 'ransomware' where payment is demanded in order to refrain from the sender conducting an action that is harmful to you,

(ii) 'spyware' which secretly records information such as an account password and sends it to the person who wrote the malware, and

(iii) 'botnets' which enable an attacker to control a group of computers to gain access to personal information.

WHAT IS PHISHING?

These are attacks resulting from fraudulent emails or fraudulent websites, designed to steal your personal information in order to steal your money. 'Spam' emails referred to as 'ransomware' are very common. These emails and websites may look very similar to ones from real organisations and could offer small prizes or rewards to tempt you to share personal information.

Photo credit: Linux Password File by Christiaan Colen is licensed CC BY-SA 2.0

WHAT IS IDENTITY THEFT?

This is when your personal information such as your name, address, passport or identity card number or credit card information is stolen from you, in such a way that the thief can represent themselves as you (online or in person) and gain some financial advantage at your expense. Personal information could be stolen from a company site where you have shared your data, or via phishing activities.

PROTECTING YOURSELF: ASSESSING THE THREAT

To protect yourself from online theft, take time to assess where are you vulnerable, by considering what information about yourself you are storing online. What sort of personal information and documents have you kept online and where is this held? If you keep track of this, you can then implement a range of strategies that will help protect you.

PROTECTING YOURSELF: COUNTERMEASURES

There are a lot of things you can do to protect yourself. Here are some of the main ones:

- Keep informed about threats by reading news from major media outlets and technology sites
- Install virus protection software which can protect against malware
- Avoid using illegal copies of software which can spread malware
- Look out for the signs of phishing emails
- Keep your software updated for the latest security 'fixes' which protect your computer
- Create passwords that are unique and hard to guess – use symbols and numbers and a mix of upper/lower case letters. Passwords are more difficult to guess if they don't contain a dictionary word
- Ensure that passwords gets encrypted and sent securely to the server when entered
- Wherever possible use two factor authentication for logging into the websites that you use. For examples an online bank may request two pieces of information – a card number and a pin number. This provides enhanced security.
- Don't store your credit card information online.

LEARN MORE ABOUT STAYING SAFE ONLINE

Introduction to cyber security: stay safe online
https://www.open.edu/openlearn/science-maths-technology/introduction-cyber-security-stay-safe-online/content-section-overview

Digital Literacy: Staying Safe Online
https://www.zabai.org/enrol/index.php?id=49