Cybersecurity Staying safe online

Who is this session designed for?

- Students currently studying at any level with the OU who use
- Students who have just started their first level 3 module

Purpose of session

- To identify a range of cyberthreats that we may be exposed to.
- To give tips on how to avoid or respond to cyberthreats.
- Highlight key resources to help

Cyber threats

- Viruses
- Spear-phishing
- Phishing
- Spoofing
- Data beaches – id used
- Ransomware

Check if your details have appeared in any other public data breaches: https://haveibeenpwned.com.

Consequences

- Loss of data
- Compromise other systems
- Identity theft
- Financial loss
- Compromise friends or family

Staying Safe Online 1

- Update your computer or device's operating system regularly.
- Use up-to-date anti-virus and anti-spyware software
- Set your computer preferences to run security updates when they are available.
- Regularly back up your files.
- Be careful when sharing files on the cloud
- Verify software is from a reputable source
- Use strong, unique and secret passwords.
- Always verify the sender before engaging with an email.

OU guide to Being safe and secure online
https://help.open.ac.uk/being-safe-and-secure-online/general-safety-tips

Staying Safe Online 2

- Know how to spot ‘phishing’ emails
- Don’t open files, click on links, download programs or respond to emails you are not expecting,
- When shopping or banking online, stick to sites that use encryption to protect your information
- Ensure you're using a secure internet connection
- If you’re using a public wi-fi network only use it if you need to input a password to access the network and/or use a virtual private network (VPN) if possible.
- If you can't be sure that your information will be sent over a secure connection, wait.
- Ensure your home router is password protected

Individuals & families - NCSC.GOV.UK
https://www.ncsc.gov.uk/section/information-for/individuals-families

When the worst happens 1

- Report cybersecurity breaches to OU ASAP
- Focus - undoing or minimising impact - not placing blame.
- Data breach – Change passwords ASAP
- Login or password compromised – change password ASAP

information-security@open.ac.uk
Contacting the Computing Helpdesk
https://help.open.ac.uk/contact#computing

When the worst happens 2

- Hacked account – follow guidance at: https://www.ncsc.gov.uk/guidance/recovering-a-hacked-account
- Ransomware
  - do not pay the ransom fee,
  - do not click on any links
  - do not engage with the ransomware attacker.
  - power off your device
  - disconnect ethernet cable
  - power off

Computing | Student Policies and Regulations | The Open University
https://help.open.ac.uk/documents/policies/computing

Your questions

We will now answer your questions from the chat.

Summary

- Latest versions of software
- Use cloud storage for TMAs etc
- Use your OU email address for OU work
- Change passwords regularly
- Avoid using unsecured public wifi
- Consider using a virtual private network (VPN)
- Respond to data breach emails and change passwords
- Do not follow suspicious / unexpected links
- Report anything suspicious
- Act quickly if you have been or think you might have been compromised

Feedback please

Please use the following link to provide feedback to help the studenthublive team to continue to improve what we do

https://forms.office.com/e/gAu965bpAm

Upcoming sessions

14-Nov	7pm	Workshop	Creative problem-solving
21-Nov	4pm	Connect LIVE	Studying with disability
26-Nov	11am	Community	Support and Wellbeing for Student Carers
28-Nov	7pm	Workshop	Memory and Learning
03-Dec	7pm	Workshop	Power reading: boost your reading skills
05-Dec	11am	Workshop	Learning from feedback
10-Dec	11am	Connect LIVE	Keeping motivation
18-Dec	6.30pm	Connect LIVE	SHL Christmas Party! (Orc and pet edition)

Details and booking information from

http://studenthublive.open.ac.uk/

Past student hub live online study skills sessions here

Visit us at http://studenthublive.open.ac.uk/ and subscribe for events as they are announced. Send us feedback at studenthub@open.ac.uk