Essential Guidance for Students on Staying Secure Online

Staying Secure Online

- Keep your identity safe e.g. Don't reuse passwords or use similar passwords across the accounts you have, use strong passwords and a password manager to help you remember them. Use a passphrase, which is three or four random words. For passwords, always think longer the better. Use MFA (2FA) (second layer of protection), Biometric access can help, too. Never disclose your password to anyone, not even your tutor. If someone ever asks you for OU login details, including email address, never disclose it, as this information can be used to try and scam you.
- Be vigilant for scams, especially now Gen AI has made it hard to trust what you see and hear as well as what you are reading. To spot AI, look out for known legitimate emails and see if similar language, formatting, processes, and sending addresses/senders are used. If in doubt, report the email.
- Hover over links and verify legitimacy before engaging and check the sender's name/sending address matches a legitimate address. Tutor names can be easily found online, so be wary of emails from people impersonating tutors and or any supposed OU member of staff.
- Keep your devices up to date. Ensure automatic updates are turned on for devices/software. If auto updates can't be applied, ensuring the latest version of software is used, and if software is no longer required, remove it from devices. Make sure all software uses MFA/2FA. Check the software you're using/downloading is from the official vendor, so always check you're on the official vendor's website. When you've finished a module, check you still need a piece of software. Put in reminders to check software is still needed after the end of each module.
- Don't disclose your OU email address to any third party or use it to log in to other accounts/services. Your OU email displays first and last name which is classed as personal data which you also need to protect and only use for OU study purposes. Often Essay Script writers/other support services will email students hoping to tempt you into sharing your information and log in credentials. But of course, you won't because this could put yours and

other students' personal data and OU intellectual property at risk. This would also be a beach of student policy regarding Plagiarism. Even if you think something is allowed, never disclose your OU credentials to anyone.

- Don't click on browser pop-ups, instead, restart your device and check your pop-up permission settings and click block.
- Never use Wi-Fi that you can automatically connect to. Make sure any network you connect to requires you to input a password. For example, studying in a public library or café and about shoulder surfing in public spaces to remember to protect your password and login credentials. Try to use screen protectors and keep your brightness levels down to maximise security.
- Click 'use only essential cookies' when entering websites to minimise risk.
- Keep your social media accounts private and minimise the amount of information set to public.
- Use the checkout as guest option where you can, when shopping online, rather than setting up accounts with more companies, for instance, when shopping for any study materials or supporting equipment.

How to Protect yourself from Phishing

- Check the sender's name and the sending address – do they match?
- Is the email address/sender name an exact match to a trusted email address you can verify?
- Is the formatting different from any known legitimate emails you've received before?
- Is the email encouraging a sense of urgency, trying to make you act quickly?
- Does the email contain spelling or grammatical errors that seem out of place for the purported sender?
- Hover over any links or attachments; hover over links to see if the URL matches the legitimate website. If in doubt, directly contact the supposed sender using a verified contact method instead of replying to the suspicious email.
- If you think an email is suspicious, please click the report button in your email and calendar application for your computer, for example the Report Message button in Outlook. Alternatively, contact the Student Computing Helpdesk.

- Never forward the email on to anyone other than information-security, as this could increase the risk of someone else engaging with a potentially suspicious email.
- Don't reply to the email itself to find out if it's genuine.
- Look out for some of latest phishing trends like business email compromise and QR code phishing. Even if an email comes from a legitimate address you can authenticate, please check to see if what the email is asking you to do matches what the company/person would normally say. With QR code phishing, never scan the code until you can verify the sender is legitimate. Even then, request a copy of the link first so you can hover over and confirm it's safe to engage with.

How to spot AI generated Phishing Attempts

AI is something that will impact you daily as you go about your lives, including your studies. AI is being used to-make phishing emails more believable by adding 'Deep Fakes' through to helping attackers make their text and formatting more believable.

AI will transform cyber security in multiple ways. It can help us in some ways, assisting us in defending the OU from Cyber Attack with enhanced threat protection and analysing vast amounts of data to identify potential vulnerabilities, which can help us respond to potential incidents more swiftly and accurately. AI is constantly learning, and the more it learns, the more it can predict and pre-emptively mitigate risks, ensuring a more robust defence mechanism against cyber-attacks.

On the other hand, AI also provides cybercriminals with sophisticated tools to execute more complex and harder-to-detect attacks. Techniques such as AI-generated phishing emails and Deep Fake technology can deceive even the most vigilant individuals, making the impersonation of trusted entities more convincing than ever. To get over this, there are several things you can do beyond what I mentioned to spot phishing in general:

- If the email is purportedly from the OU, is the language used like any other email from this person?
- Does the branding exactly match?
- Even if the sending address is the same, contact the person using a known contact point to verify it is genuine.
- If they're from the OU, are they following OU policies/procedures? Check before you engage with any email/text/call.

- AI can imitate voices and the physical appearance of trusted individuals, so even if you hear a voice of someone you recognise, check that the number they're calling from can be verified and if they're following OU procedures/policies.
- If in doubt and if the correspondence is from outside of the OU, don't engage and check with either the Student Computing Helpdesk or information-security@open.ac.uk.

Checks to make before using AI

You must check and confirm any Artificial Intelligence (AI) platform you want to use does not contain malicious material before using it.

Most AI platforms have built-in security protection, but it does not completely block or even restrict malicious material from being downloaded.

Action to take

If you want to use AI, please check if they've been marked as unsafe before using them. The AI platform should flag if it's unsafe.

If they have, do not engage with the AI platform until it can be confirmed it is safe.

Even if they haven't been flagged as unsafe, you should check that those developing the platform can confirm that they have used tools to help identify AI vulnerabilities to optimise security posture.

If in doubt, please email information-security if it relates to your studies.

You are our best form of defence, so keep in contact with us, look out for Information Security updates on StudentHome, and make sure you stay informed about the latest AI-driven threats, information security best practices, and encourage your peers, colleagues, family, and friends to foster a culture of awareness and vigilance to information security risk, which will be crucial in navigating this dynamic and challenging environment.