TOP TIPS FOR STAYING SAFE ONLINE

BACK UP YOUR DATA

Using **University approved file storage** with automatic backups is one of the most important things you can do. If you're targeted by a cyber attack you may not be able to access or use your device, but, if your data is backed up you won't lose any of it.

KEEP YOUR OPERATING SYSTEM UP-TO-DATE

Updates often fix vulnerabilities that attackers can find and use to access your system or devices. It is an effective way to help keep them out. Install operating system and application updates as soon as they become available.

CHOOSE UNIQUE PASSWORDS

Create **unique passwords** for each account that you use. That way, if an attacker gets hold of one of your passwords, they can't get access to all of your other accounts too.

THINK BEFORE YOU CLICK

90% of cyberattacks start with an email. Clicking on unsafe links and attachments in an email are two of the most common causes of cyber security breaches. Plus, hackers are smart, so stay alert. If you're unsure if something is safe, don't click!

TURN ON MULTI-FACTOR AUTHENTICATION (MFA)

Choose to add an **additional layer of security** that verifies you are the person you are claiming to be when connecting to UON online services. **Get a notification or code** sent to your phone when logging in - it helps stop hackers getting into your accounts.

INSTALL ANTI-VIRUS SOFTWARE

University managed devices are already protected with **anti-virus software** but for your personal devices, all current staff and students can **download Sophos Home free** to help protect you from viruses and ransomware.

BE CAUTIOUS OF FREE WIFI NETWORKS

Free WiFi and hot spots are very convenient but they are untrusted networks so others could see what you are doing. Try to avoid them, especially for online shopping or checking private information.

BE SMART WITH SOCIAL MEDIA

What you post on social media can give cyber criminals information that they can use against you. Set your privacy so only friends and family can see your details.

DON'T GIVE OUT PERSONAL INFO

Legitimate-looking emails are very clever at trying to trick us into giving away personal or financial information. **Stop and check** if you know who the email is from.

BE CAUTIOUS ABOUT SENSITIVE DATA

Be conscious of sensitive data you download or access. Review the **University's Privacy Management Plan** and the Information Security Data Classification and Handling Manual to understand the University's data protection requirements.