HOW CYBER SAFE ARE YOU?

Hints and Tips

Presented by Cyber Check.Me
#1 Use Strong Passwords

Have a minimum password length of 12 characters.

Consider using multi-factor authentication option with a 12 character password.

Use a password manager to generate, share and remember complex passwords.

Use a different password for each account and never write down your passwords.

Change default passwords on any smart devices or appliances to a secure and private password.
#2 Protect Your Computer

Enable the firewall that comes with your computer.

Encrypt the hard disk. A quick Google search will give you instructions on how to do this.

Never leave your computer in an unsecured area and always lock your screen.

Flash drives, smart phones and other external devices may contain malware/viruses. Install and maintain anti-malware on your computers and enable automatic updates.
When in doubt, report suspicious mail via the ‘junk mail’ button, or simply delete it.

Regularly clear your cookies and browsing history on your devices.

Check the websites and portals you visit are secure, indicated in the URL by the ‘s’ in ‘https’.

Ignore unsolicited emails and phone calls.

Be wary of attachments, links and forms in an email, and avoid untrustworthy downloads and suspicious links on webpages.

Use encryption when sending confidential or sensitive data.
#4 Use Mobile Devices Safely

Protect your mobile as it contains highly confidential information including bank details and personal identification.

Always lock your device with a pin or password. Consider using a finger scanner and/or facial recognition.

Only install apps from trusted sources and read the terms and conditions of use.

Review app settings monthly including app permissions that can provide access to sensitive areas of your device (i.e. contacts, microphone, camera).

Remove apps you haven’t used in the last 3 months.

Use the ‘Find my iPhone’ service or ‘Android Device Manager’ to prevent loss or theft of mobile devices.
#5 Keep Up-To-Date

Keep your computer, tablet and/or smart phone up to date with the latest updates from the vendors.

Make sure you update your computers, tablets and/or smart phones weekly. Preferably automatically.

If you do not use software for 3 months or longer, consider removing it as it maybe a means of attack for cyber criminals.
#6 Install Malware/Anti-Virus Software

Install malware/anti-virus software on your computers.

Make sure you update your anti-virus software on a daily basis. Preferably automatically.

Scan your computer daily and when you connect an external device like a portable USB hard disk.
#7 Back Up Your Data

Make a weekly backup of all your data including, photo’s, music, projects and reports on some other device or location.

Consider using a cloud service such as OneDrive, Google Drive or Dropbox. Alternatively use a portable USB hard disk that is encrypted.

Do not use the portable USB hard disk for anything else but your backup and store it in a safe location away from your office.

Check and test if your backup was successful.

Most operating systems have built-in functionality to help you make backups.
Be aware that when you use public wireless, the provider of this wireless service can access your communications including your email or password.

Encrypt your communications using virtual private network software, or VPN software.

Check the website addresses you visit have HTTPS.
Stay Informed

Helpful Links:
https://www.staysmartonline.gov.au
https://www.scamwatch.gov.au
Subscribe to the alert service:

We can help. Visit
ecu.edu.au/cybercheckme

ECU is a recognised Academic Centre of Cyber Security Excellence