CYBER SECURITY TIPS FOR STUDENTS

As a student there are many things that you are required to keep track of. From classes and homework to extracurricular activities and social gatherings. With so many things to manage you might not prioritise cybersecurity, however in today's digital world, it is more important than ever for you to be aware of cybersecurity threats.

1. Create strong and unique passwords

To create a strong password it is important to use a mixture of upper and lowercase letters, numbers, and symbols. Each password you create should be unique, using the same password across multiple websites is a security vulnerability. If one of your accounts is compromised all your accounts that use the same password also become compromised.

2. Use social media safely

Think before you post on social media and be cautious about the information you share. Avoid sharing personal information, such as your date of birth, address and phone number. Be sure to use strong, unique passwords for each of your accounts. Also, be wary of suspicious links or messages, as they may be attempts at phishing or other forms of cyber crime.

3. Always think before you click

Hackers will create fake emails and messages to trick you into clicking on a malicious link. Before clicking you should ask yourself if this email is genuine, from a trusted source, and where does the link take me to. Hovering your mouse pointer over a link will display the URL that you will be taken to in the bottom left-hand corner of your screen.

4. Protect your devices from physical access

If you take your devices (laptops, tablets, and mobiles) to a public workspace, it is important to keep them secure. Always be aware of your surroundings and if you are required to leave your device lock and store it in a safe place. If you forget to lock your device someone could use your computer to impersonate you or steal sensitive information.

5. Avoid connecting to unsecured WI-FI networks

Free public Wi-fi might be convenient and desirable to use but public Wi-fi has many privacy and security risks. Cybercriminals can create a rogue hotspot and once you connect the criminal can monitor and steal your personal information.

6. Enable two-factor authentication

Two-factor authentication also known as 2FA is an easy way to add an additional layer of security on top of your username and password. With 2FA, you can guard your account with a one-time password or a physical characteristic such as a fingerprint or facial feature. 2FA helps to prevent unauthorised access to your account.