Cybersecurity Guide for Students Learning at Home

This guide is designed to improve your cybersecurity while learning from home. This is important as it is harder to assist you remotely. If you have a major issue then getting a new device will also be increasingly tricky through this period. If your device becomes compromised it could impact your home network and all other devices on it. We urge you to be as diligent as possible.

There are some basic actions we can all take to ensure we protect our devices from malware and other compromises.

One of the main types of attack is known as “phishing” - it is estimated that up to 95% of attacks occur through this means. Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by the criminal disguising themself as a trustworthy entity in an electronic communication. It is typically carried out by email spoofing or instant messaging. It often directs users to enter personal information at a fake website which matches the look and feel of the legitimate site.

Phishing attacks come in various forms, for example:

- Phishing - for example last year with the launch of the iPhone 11 and even fake COVID-19 information from the World Health Organisation.
- Spear- phishing - more targeted attacks at individuals or schools.
- Angler Phishing - cybercriminals create fake web and social media accounts to pretend to provide customer support. They then ask for security information and passwords which they use to access your system and your other online accounts.

Phishing attacks can cause immense damage. They are the entry point for cybercriminals and can lead to the installation of more malware, ransomware (i.e. locking up all your files) and potentially using your laptop as a way of attacking the school network - this is high risk for the school.

So, the main action is to be very aware of phishing and to be alert for attacks. We suggest you be alert to the following:

- Emails from unexpected sources - e.g. delivery notifications, gifts, offers that are unexpected, etc.
- Emails with spelling mistakes (yes the cybercriminals are often overseas and do not use good English or grammar).
- Emails from what appear legitimate sources (e.g. teachers or other school staff) asking for security credentials, etc. Always verify these requests by phone.
- Do not click on any links or open any document attachments unless you are absolutely sure of the sender being who you believe it is. PDFs, Word documents, web links, etc, can all install malware as soon as you click on them.
- Be careful when searching for online support to ensure the support page you reach is the genuine one. Cybercriminals create fake sites that look very similar. Check the domain (i.e. the www.xyz.com is exactly what you would expect - watch out for subtle spelling mistakes and sites with a word or letters in front of the real site - eg. www.xyx.genuinename.com).

In summary - be very aware and alert and suspicious. If in any doubt do not open attachments or click links.

For more information about phishing please see this Australian Government advice.

Other general advice to stay cyber secure while learning at home includes:

- Backup your device or key files every day. Preferably do this to a separate hard drive or USB drive.
- Ensure your Anti-Virus software is set to auto update on our device and other home computers.
- Update all your apps and browsers to avoid vulnerabilities - set to auto update.
- When on social media or online socialising apps, such as Houseparty, don't befriend people you don't actually know in real life.
- Ensure you have set appropriate privacy settings on your social media accounts.
- Be mindful and cautious of content, including video, that you are sharing with others. Content you share will remain in the virtual world indefinitely and could be used inappropriately by some people. Please think twice about what you share.
- If you are gaming on your devices please ensure you set strong passwords to protect your accounts and only download games from legitimate sites.
- Review your passwords - find out more about keeping your passwords secure here.
- Finally - you can check https://haveibeenpwned.com/ to see if your password has been compromised. If it has please take the time to change your passwords, ensuring they are secure and not shared with anyone.

For further information and resources please see the StaySmartOnline Government website.

This guide has been put together by Superloop CyberHound who provide an industry-leading cybersecurity, student wellbeing and internet compliance platform for K-12 Schools. The company is proudly Australian and has over 20 years experience with K-12 schools across the globe.

Superloop's Intelligent Network helps families work, learn and play.
Find out more about Superloop Home Broadband at superloop.com.