developing Employability

STUDENT RESOURCES

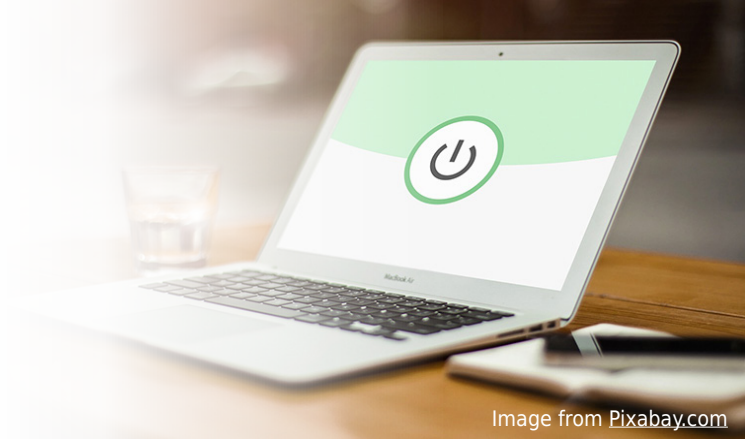
Image from Pixabay.com

Internet security tips for remote learning during Covid-19 and beyond

As the Covid-19 pandemic raged on in 2020, the world began to realise that we would have to learn to live a new type of normal. People in multiple cities lived through some of the toughest coronavirus lockdowns in the world and the student community was one of the hardest hit groups.
The onset of the corona virus pandemic forced the majority of colleges and universities to embrace a fully online learning model and forced the majority of teachers and students to learn fast!

Greater Risk of Cyber Attacks

Cyber criminals exploited the heightened anxiety caused by Covid-19 to target individuals and businesses. More than ever before, college students began accessing the internet for communication, entertainment, online shopping, and learning. The vast amounts of data these individuals generate online puts them at a greater risk of a cyber attack. Here are some of the common cyber risks facing Australian students.

Public Wi-Fi Attacks

Students are notorious for using public Wi-Fi hotspots. There's a good reason for that: they're convenient, widely available, and free. But free Wi-Fi hotspots can lead to identity theft, data compromise, and financial loss in the event of a public Wi-Fi attack such as WIFIPHISHER and MITM.

Phishing

Phishing is a social engineering tactic used to trick people into sharing sensitive data or downloading malware onto their systems. Phishers increasingly use social media profiles, email addresses, and spoof websites to manipulate a victim's trust and gain access to sensitive data.

Malware

We have become more digitally connected during the Covid-19 pandemic. Hackers are taking advantage of our dependency on digital infrastructure to infect systems with malware that can hijack online banking sessions, steal personal files, and log keystrokes.

One of the more popular types of malware in recent years is Ransomware. Ransomware attacks are designed to lock you out of your system or device and then prompt you to provide payment for service to be restored. Whilst this type of attack is usually targeted at businesses, all users are vulnerable to this threat.

How to Increase Protection

The Covid-19 pandemic prompted us to become more digitally connected and this greatly increased the risk of cyberattacks. Luckily, there are steps we can take to increase protection and reduce the risk of a successful attack. These include:

- **Using a VPN**. Install a VPN on your devices to reduce your digital footprint when surfing the web. A VPN encrypts your web traffic and hides your location, making your online presence completely anonymous.
- **Email Security**. Cybercriminals often use email to spread malware and steal data via phishing. Improve your email security through best practices and security awareness. Don't click links or attachments from suspicious sources.
- **Trusted Sources**. Exercise caution when downloading files from the internet. Sometimes hackers create fake free apps and other software to lure potential victims. Only download software from trusted, reputable sources.
- **Strong passwords**. Having strong passwords for all your online accounts is one of the most effective ways to protect your data.
- **Regular Updates**. Updates are essential for security. Software developers find vulnerabilities in their code, fix them, and release patches, updates, or new versions. Perform regular updates to keep your programs and systems secure.
- **Virus Protection**. Use antivirus software on your devices, even if you are using a mobile or non-windows device. A strong antivirus solution will usually include multiple defence measures like a Firewall, Intrusion Detection System and Data Loss Prevention in a single software package.
- **Two-Factor Authentication**. Enable two-factor authentication on your online accounts for an extra layer of protection.

The novel coronavirus left many Australians confined to their homes and increased the amount of time people spend at home for work and study. The risk of cyberattacks increased drastically as learning institutions turned to remote learning options to keep students, staff, and faculty safe during the pandemic.

Regularly review internet security tips and increase your cybersecurity awareness to protect yourself online. Remember also to behave responsibly in order to protect others.

About the contributor
Amy Cavendish is a content strategist at TechFools, a tech blog aiming to inform readers about the potential dangers of technology and introduce them to the best ways to protect themselves online. As an outspoken advocate for digital freedom, Amy is dedicated to empowering her readers to take control of their digital lives with her thought-leadership articles.

Acknowledgement

Developing Employability is led by
Professor Dawn Bennett, Curtin University, Australia.
The work is supported by the Australian Government Department of Education and Training.