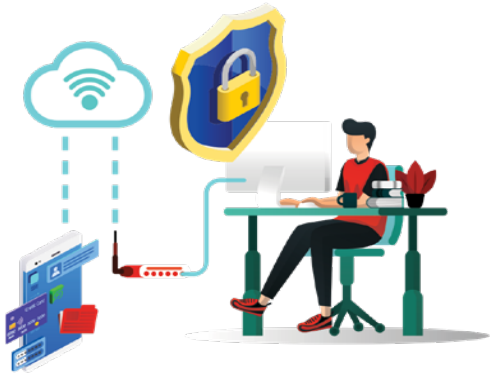
Week 1 Theme: Work, Teach and Learn from Anywhere

Protect Your Home Network Checklist

Review your Home Network Setup

- ☐ Is your computer set to automatically install software updates?
- ☐ Is your personal firewall enabled on your computer?
- ☐ Have you installed antivirus / anti-malware protection on your device?
- ☐ Have you changed all default passwords and logins on your home router?
- ☐ Have you changed the default SSID (also referred to as the “network name”) to something unique and not tied to your identity or location?
- ☐ Do you have a strong password set on your Wi-Fi router?
- ☐ Is WPA2 (WPA3 preferred) security setup for your Wi-Fi connections?
- ☐ Is your Wi-Fi router centralized in your home? (Note: If it is close to the external walls and windows in your home, the signal can broadcast further than is needed)
- ☐ Is the firmware on your router up to date?
- ☐ Are you using a separate wifi network for your smart home gadgets (e.g. TVs, Amazon Echos, Cameras, etc. on their own network away from your laptops and phones)?



What you need to know

As we adapt to learning, teaching and working from home, it is even more important now that we are cyber secure.

A home network with inappropriate security measures can be a target for cybercriminals. A compromised home router can open you up to significant consequences such as information or identity theft, malicious sites and advertisements, fraud and more. An unsecured home network can also be used by cybercriminals for illicit purposes such as launching an attack on other networks and systems.