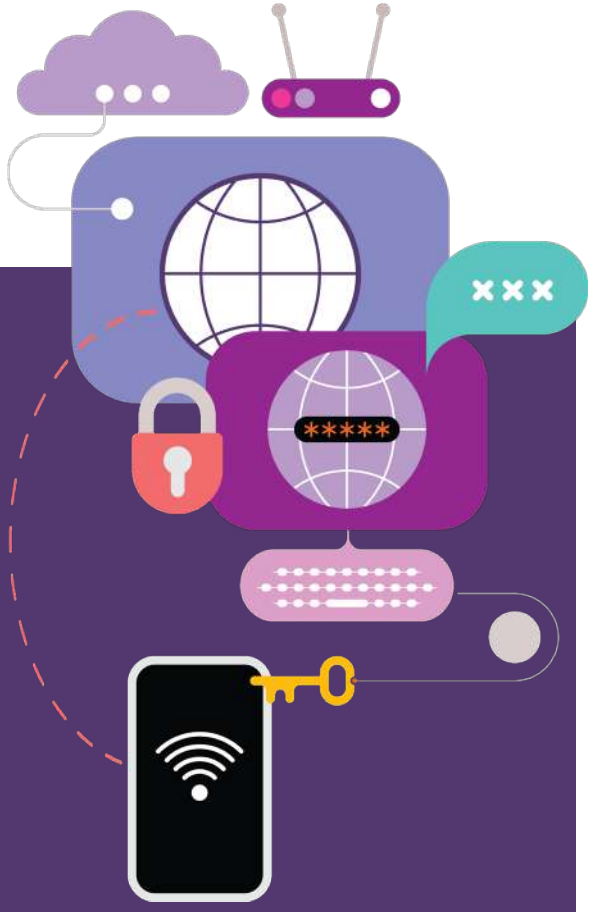
WORKING FROM HOME:
SECURING YOUR HOME OFFICE

When you work from home you likely rely heavily on the internet. As such, protecting your home network is paramount to security.

1. Log in to your router to access its settings. If you're unsure of how to log in, look up your router's model on the internet and you'll find plenty of how-to articles with simple instructions.
2. Change your router's username and password. Most routers ship with default login credentials that are public knowledge and must be changed immediately.
3. Change the SSID (Service Set Identifier). The SSID is the name of your wireless network. Change it to something unique and protect it with a strong password.
4. If available, enable automatic updates so your router is always on the most recent firmware or software version.
5. Use a virtual private network (VPN). A VPN is software that encrypts your internet connection and prevents others from viewing your internet traffic. Many organizations require the use of a VPN for remote workers.



DEVICE DEFENSE

With your network secured, let's highlight a few ways to ensure your workspace is also secured.

Use strong passwords. All accounts and devices require strong, unique passwords. Don't share those passwords with anyone for any reason.

Lock your workstation. When not in use, always lock your workstation and ensure no one else in your household can access work-related information or accounts.

Beware of smart devices. Ensure voice-controlled smart devices can't listen in on any discussions that involve confidential information. Ideally, remove smart devices from your workspace.

Separate work and personal. Don't use work devices or accounts for personal reasons. If you have approval to work on a personal computer, protect it with antivirus software.

Always follow policy. No matter where you work, remember that organizational policies apply and must be followed at all times. Have questions? Please ask!