

Stay Secure While Working from Home

Follow these 5 Steps to Remain Safe & Productive While Working Remotely

Remember: At Home YOU Are the IT Department

While your organization takes every possible measure to maintain the security of your remote work, you also have an important part to play.

Know the Risks:

- Insecure home networks
- Inadequate security on personal devices
- Insecure internet connections
- Failure to follow safe practices and organizational policy

01

Plan Ahead

Staying productive while working remotely requires some forethought. What resources may be more challenging to access remotely? What standard processes may have to change? Think through your daily work and make any needed adjustments in line with your organizational IT policies.

Secure Your Network

When working remotely your home network becomes a potential gateway for hackers to gain access to organizational data. To keep it secure ensure you turn on your router's firewall, change the default administrator password, and change the default network name (SSID). Also ensure encryption is turned on and set to the strongest protocol (WPA2).

02

03

Safeguard Personal Devices

While you are likely working on a laptop provided by your organization, that device is now sharing a network with your personal devices. Ensure the security of personal devices is up to date by installing antivirus software and keeping all software up-to-date with the latest updates and patches.

Connect Securely

As you work you will need to transfer information to and from colleagues and office networks or cloud platforms. Ensure that information remains secured by using a virtual private network (VPN). A VPN is a private connection that encrypts the data so hackers cannot trace it. Always follow the specifics of your organizational policy for secure connectivity.

04

05

Practice Good Cybersecurity Hygiene

Working from home can introduce new distractions. When it comes to cybersecurity, it is important to remain vigilant. Continue to look out for phishing scams, avoid clicking on any unknown links, prohibit family from accessing your work devices and follow all policy guidance.