HOW TO PROTECT YOUR DATA WHEN WORKING REMOTELY

Whether you're working from home, a café, or another remote location, it's paramount that all professionals, regardless of the industry they operate in, observe strong cyber security practices. It will help keep confidential data, both personal and organizational, safe from attempts to steal your information.

1 Fortify all your user accounts

Ensure that you're using strong passwords (a combination of uppercase and lowercase letters, numbers, and special characters), as well as unique passwords for each account. For an added layer of protection, activate two-factor authentication for all your user accounts.

2 Use a Virtual Private Network (VPN)

A VPN can be used to secure internet connections and encrypt data shared between devices, enabling employees to keep confidential individual or organizational data safe from cybercriminals, regardless of the Wi-Fi network used. Please speak to your manager or IT department for compatible software recommendations or guide you through the installation process.

3 Set up firewalls, anti-virus software

While most operating systems come with basic precautions built-in, optimizing your firewall and anti-virus settings increases your protection level against malicious programs and other threats. Check with your IT department to ensure that your device(s) are equipped with adequate, up-to-date software.

4 Secure your home Wi-Fi router

If you're working from home regularly, securing your home Wi-Fi router is a critical step that will help safeguard data exchanged over your network. Be sure to change your password, especially if it's the original one provided by your internet service provider, and install the latest firmware updates to minimize vulnerabilities.

5 Keep your programs, operating system updated

Though some may find the process cumbersome, keeping all your applications and operating system(s) up to date is essential to secure remote work. These updates often come with critical security patches that help eliminate vulnerabilities that hackers may have previously exploited.

6 Inspect incoming messages for suspicious elements

Just as you would at an office, it's essential to be vigilant and pay attention to a cyber threat's common warning signs. Carefully inspect each incoming message and avoid clicking on unexpected links or opening attachments, even if they come from familiar email senders or organizations. If confronted with a potentially malicious email, report it immediately based on your organization's policies.