

How to Protect Your Data When Working Remotely

Whether you're working from home, a café, a hotel conference room, or another remote location, all professionals, regardless of the industry they operate in, must observe strong cyber security practices. These will help keep confidential data, both personal and organizational, safe from attempts to steal information.



1

SECURE USER ACCOUNTS WITH STRONG PASSWORDS

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.

USE A VIRTUAL PRIVATE NETWORK (VPN)

A VPN can be used to secure internet connections and encrypt data shared between devices, enabling you to keep sensitive information safe from cyber criminals, regardless of the Wi-Fi network used. Speak to your manager or IT department for software recommendations or guidance through the installation process.

2

3

SET UP FIREWALLS AND ANTIVIRUS SOFTWARE

While most operating systems come with basic precautions built-in, optimizing your firewall and antivirus settings increases your protection level against malicious programs and other threats. Ensure that your devices are equipped with adequate, up-to-date software according to your organization's existing IT or remote work policy.

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.

4

5

KEEP YOUR PROGRAMS AND OPERATING SYSTEM UPDATED

Keeping all your applications and operating system(s) up to date is essential to secure remote work. When you see an available update, install it as quickly as possible, since they often come with critical security patches that help eliminate loopholes hackers can exploit.

INSPECT INCOMING MESSAGES FOR SUSPICIOUS ELEMENTS

Just as you would at an office, it's essential to 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 senders. If confronted with a potentially malicious email, report it immediately based on your organization's existing policies.

6