9 Security Best Practices for Remote Workers

CAMPUSGUARD®

Working from home may make you feel more comfortable than working in an office environment. However, the threat of cybersecurity attacks still exist— in fact, employees working remotely can be the largest threat to the security of your organization's network. All employees need to be vigilant and proactive to help prevent cyberattacks.

Here are 9 security tips to secure your remote working environment:

1 Use secure Wi-Fi connections

Verify your home Wi-Fi network is password-protected (and not with the default password). Secure connections will keep strangers from easily accessing your network. Consider setting up separate virtual networks for each person or group (i.e. "work" network for parents, "school" network for kids) to provide some separation. For better security, create separate virtual networks for your family and another "guest" one for friends or relatives who come to visit and need access.

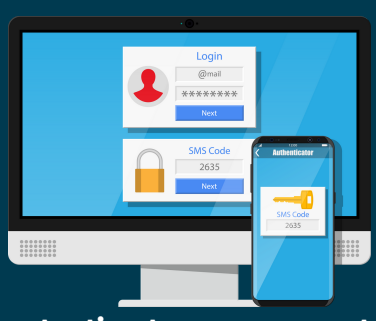
2 Check privacy and security settings

Review and adjust privacy settings on web applications, games, social media, and videoconferencing tools so your profiles are set to the strictest privacy setting. Check the safety and security settings on any new programs that are downloaded. Use parental controls to help block child accounts from accessing specific websites, applications, or functions.

3 Use a VPN

Using a VPN (Virtual Private Network) encrypts your internet traffic to ensure that any data shared with your company's network is safe from attackers. Since VPNs protect your online activity from being intercepted by hackers, they are ideal for remote work setups.

4 Setup Two-factor Authentication



Two-factor authentication (2FA) provides an extra layer of protection to your accounts and validates your employee identity more efficiently. The extra step could be an email, a text message, a randomly generated PIN, which only you would be able to provide. While two-step authentication is not hacker-proof, it will add yet another protection to prevent an unauthorized intrusion into your company accounts and systems.

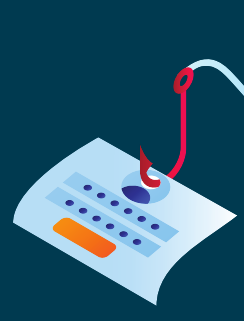
5 Use strong passwords

Reinforce the need to create strong passwords and explain why it is important not to share passwords with anyone else. Use unique passwords for each website or application. Do not reuse the same password for more than one computer, account, or website. Reusing passwords can result in multiple systems or accounts becoming compromised if one account is.

6 Install security updates regularly

Remote workers need to be vigilant and ensure strong anti-virus software is installed and up-to-date on your devices. Regular scans should be performed to detect any malware threats on your devices. Keep in mind that a breach of one person's device can quickly spread to all other devices on the same network.

7 Avoid phishing scams

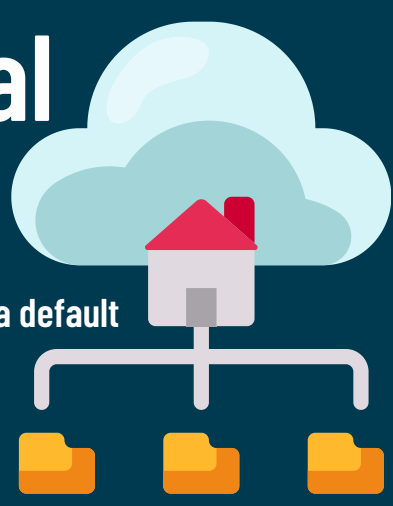


Think before you click! Know the risks associated with clicking links and opening attachments from unknown senders and the need to verify the legitimacy of an email before responding or providing any information. Spot a phishing email by checking the sender's email address. Spelling errors , poor grammar, and suspicious-looking links are signs of a suspected phishing email. It's best not to open an email unless you're expecting it or it's from a trusted sender.

8 Use a password manager

Password managers, like LastPass or Keeper, generate strong passwords to help secure your accounts. With password managers, you cannot reuse passwords. You will only need to remember the main password to your vault, which eliminates the need to remember all passwords you use for work.

9 Protect your personal network



You may not be aware that your household router comes with a default password when its first installed. Not changing the default credentials for your devices is an easy way for a hacker to access your network. Protect your personal network and remote working devices from malicious invasions by changing your router's password. Also, make sure to upgrade your WiFi router to a newer model every few years as older models don't support newer, more secure standards.

Contact CampusGuard to discuss cybersecurity assessments, ongoing vulnerability management, awareness training, and more to keep your organization secure.

CAMPUSGUARD®