GUARDSIGHT

https://www.guardsight.com

Cybersecurity Tips When Working From Home

YOUR AWARENESS IS THE BEST DEFENSE

Cyber attackers know that targeting you may be the path of least resistance to accomplishing their objectives. They'll often try and trick you by creating a sense of urgency. Be aware of this and carefully review all communications before clicking or responding. Common sense is your friend!

PRO TIPS

- Be aware of email and SMS phishing
- Patch your personal laptops, phones, & firewalls
- Secure your home networking devices
- Use multifactor authentication
- Use a password manager
- Prohibit others from using company devices
- Use antivirus or endpoint detection software
- Use common sense

For additional advice or to learn more contact us: info@guardsight.com

01 AVOID PHISHING ATTACKS

Email or text messages from unknown sources that convey a sense of urgency, or crisis laden deadlines, could be a phish. Mark those as spam.

02 UPDATE PERSONAL DEVICES

Enable the software auto-updater features for personal devices and home networking equipment. This helps reduce vulnerabilities.

03 SECURE YOUR HOME NETWORK

Change the default administrator passwords on your home network devices. Use strong passwords for your wireless access points and consider disabling the SSID broadcast.

04 USE MULTIFACTOR AUTH

Enable two-step verification whenever possible. This method adds a second step, in addition to your strong password, to the authentication process.

05 PROHIBIT OTHERS FROM USING COMPANY DEVICES

Company devices are equipped with controls to help defeat attackers. Unauthorized use could result in those controls becoming ineffective or cause security teams to disable those devices.

06 USE A PASSWORD MANAGER

A password manager is an application that securely stores all your passphrases in an encrypted format. Use it to create a unique password for each personal site, such as social media, email, and banking.