REMOTE WORKERS

Cybersecurity threats for employees working from home

Did you know that cyber-attacks are becoming increasingly common?
Remote workers are often the victims of these attacks as they may not adhere to the standard office-based security model.
To help manage the risk for remote workers, it is imperative to understand what steps you can take to protect yourself.

1. Using unsecured Wi-Fi networks

Many Wi-Fi routers used by remote workers are not secure and are susceptible to cyberattacks. We recommend removing the default password on your router and creating a secure password to prevent malicious hackers accessing your home network.

2. Use a VPN to protect your information

A virtual private network, or VPN, is a private network that encrypts and tunnels your internet traffic through a public server. This helps to keep your data safe and secure. By using a VPN while working remotely you can securely log into the shared company network, while also providing data protection for projects and files.

3. Configure firewalls and Antivirus software

You can protect your computer from online threats such as malware and hackers. This can be achieved by using a firewall to block incoming connections from potentially dangerous sources. Antivirus software will help to protect from viruses, spyware, malware, rootkits and trojans.

4. Password reuse and weak passwords

Another common threat and serious vulnerability is password reuse. This problem is created by using the same password across multiple websites and accounts. If one account is compromised all accounts are compromised. Users should avoid default and weak passwords as this can be easily guessed during a brute force attack.

5. Theft of sensitive information or personal items

Cyber criminals can use social engineering techniques to act as an employee of your organisation and then attempt to contact remote workers. This is an attempt to harvest personal or sensitive information such as names, addresses, and financial information.

6. Keep your applications and operating system updated

Keeping your applications updated is important for security and will help to keep your computer running smoothly. New updates will often provide vulnerability fixes, performance improvements, and new features.

info@phishingtackle.com | https://phishingtackle.com