COVID-19: WORKING REMOTELY

In response to the ongoing COVID-19 pandemic, many companies around the globe have rolled out work-from-home arrangements. As a result, there has been an influx of employees signing in remotely to corporate networks and using cloud-based applications. This shift could also open doors to security risks and cyber threats. Remote work involves several cyber security risks such as home Wi-Fi security, phishing scams, and insecure passwords. Let’s look at:

Home Wi-Fi Security

Many people can’t be bothered with turning on basic wireless LAN security at home. But even if you aren’t transmitting data that requires confidentiality, you might be opening yourself up to theft of service - that is, someone picking up your signal and piggybacking on your broadband connection to the Internet (the one you pay for and they don’t).

As more ways to use the Internet emerge, your upload/download speeds will become increasingly precious. And as the use of wireless also picks up, you might want to protect your WLAN from providing outside access to your broadband.

How to protect your Wi-Fi

Broadband squatters could be stealing your bandwidth...avoid theft of service in home offices!

When wireless squatters steal your Wi-Fi, they eat up your bandwidth. In extreme cases, they may even steal information off your computer or infect machines on your network with a virus. But fear not. It’s easy to fight back. There is a way to determine if your Wi-Fi signal is being sapped unexpectedly. Nevertheless, managing your wireless network is the first step towards keeping your Wi-Fi setup nice and secure. With WPA2 security enabled, it’s unlikely anyone will ever piggyback on your network.

Since every device connected to your network has a unique IP address and MAC address, you can easily see a list of connected devices — often listed as ”clients” — on one of the settings pages for your wireless router. Many devices broadcast an ID because they’ve been named by their owners, so if you see “John’s Laptop” connected to your network and you don’t have a John in the house, you’ve found trouble! Even if a device doesn’t show a name in the router’s client list, you can count the number of devices connected and compare to the number of devices you know should be there to see if the numbers are off.

Working from home? Make sure you are safe!

Is your home network secure?

Security teams and home office users can minimize the risks that come with remote-working setups by following some practical security measures:

- Secure the gateway: your router. The router is the gateway to all internet-connected devices in your home network. Attackers are known to compromise home routers with default credentials that users often neglect to change. It is good practice to regularly change the password for your router as it may have been previously shared with other users. Passwords that are not prone to dictionary attacks are recommended, i.e., those that have more than 12 characters, with a mix of letters, numbers, and special characters. With a strong password, you shouldn’t ever have to worry about keeping tabs on who connects to your network. Piggy-backers will have to find someone else to mooch off of. Without a password, your wireless network is open for anyone to hop on. But a password isn’t quite all you need to be totally secure. You should also change the router’s login information to something aside from the usual “admin.” That will keep virtually everyone from messing with your router.

- Hide your router SSID.

  Your router can hide its SSID, meaning it won’t show up for anyone searching for connectable networks. Of course, this makes it a bit tougher for welcome guests, such as friends, to get online at your house.

- Use a company laptop for remote work if possible.

  Do not use your personal machine as it may have fewer security controls than your company-owned hardware. Work-issued laptops or machines should be for employees use only, other members of your household should not have access to your dedicated work equipment.

- Use company-designated VPNs and avoid free, public Wi-Fi.

  Use the dedicated enterprise VPN servers only on your work laptop or desktop to make the connection between your network and the outside network. Be wary of phishing attacks that steal VPN-related account credentials.

- Protect smartphones.

  As with laptops and desktops, make sure phones are updated with their latest firmware versions. Download only legitimate apps from official stores and review the app permissions before installing them. Install a mobile security app to prevent malicious apps or codes from running on phones.

- Share bandwidth.

  Ensure seamless productivity by reducing consumption in streaming videos and other activities that throttle the bandwidth, especially during work hours.

- Discuss the importance of online safety.

  Help your family understand the public nature of the internet and its potential dangers. Remind them that they are responsible for ensuring that their online activities are safe and private by securing the way they set up and use their devices.

“Beware: Remote Work Comes with Cyber Security Risks”

Sources:


https://www.cultofandroid.com/9-ways-encryption-protects-your-business/

https://www.forbes.com/sites/carlslabbin/2020/06/19/beware-remote-work-involves-these-3-cybersecurity-issues/


We are Delta Corporation, Brighter Together