Cybersecurity When You Work From Home

Author : Cat

Date : March 14, 2020

Working from home is quickly becoming the new norm. But home networks and setups are rarely as safe as their corporate counterparts.

Whether you are a seasoned worker from home or new to it, there are precautions you should take to ensure you are protecting both your own and your company data. Here are a few tips to get you set up safely.

Secure the Access to Your Network

First things first, let's look at the actual router you are using. Three things you can, and should do:

- **Password protect** your home Wifi, otherwise anyone has access to your homes devices.
- Make sure your router has ALL **available software updates applied** (that's how critical bugs are fixed. Without those updates you likely have vulnerabilities).
- **Do not use public WiFi** to sign into any existing accounts. Public WiFi should be considered transparent are recordable. (i.e. looking up movie times is okay, signing in to your email account is not). If you must use public WiFi, use a VPN (see below).

Use Safe Transfers

Data can be intercepted in transfer and should be protected. Like sending a secret message to a friend and making sure it is coded.

- Make use of **company provided software, processes, and tools**. If you are in a company with a savvy IT team, they will have set this up for you. Many cloud services are well protected.
- If not provided, **use a VPN for Remote Access**. A VPN, or Virtual Private Network, protects you by hiding your IP address and moving your data through a secure service. This will help with messages and files not using cloud services.
- When sending company emails or files, **encrypt where possible**. The VPN will do this for you.

Upgrade Your Passwords

Passwords are literally the key to accessing your accounts and your data. You wouldn't use the same key for your house, your car, your bank account, and access to your office. Don't use the same key here.

- Use **multi-factor authentication** whenever possible. This includes a combination of something you know (password) and/or something you have (phone for texts or a number generator) and/or something you are (biometrics like face or finger prints).

- Ensure your **accounts have different passwords**, especially key accounts like email, financial, and work access.
- Use **complicated passwords** that are not dictionary words. You can use a reliable password keeper to generate and store these for you.

Watch Out for Scams

We should always be wary of scams but without the fancy firewalls and phishing prevention that companies have, we become more susceptible in our own home.

- **Do not click on links or open files** that are not from trusted sources and are not expected. If a colleague sends you a file you didn't ask for, double check it. Another popular scam is an email that appears to be from a colleague with a personal number to call. The numbers can have tolls associated with them.
- **Install anti-virus software** on your home laptops and computers.
- **Check URLs for websites**. The main website is the last part of the URL. For example takeout.google.com is Google (a site that lists all your data) but google.takeout.com would be Takeout (a site that helps you order dinner).

Be Wary of the IoT

The Internet of Things (IoT) are all connected devices, machines, and toys. Anything that is connected in your home is a gateway to your server. It's like adding a new door to your home. Protect it.

- **Change default passwords**
- **Apply all updates** to the software. Like your router, updates are how companies fix vulnerabilities that allow hackers in.
- If you **don't trust it, don't buy it**. There is no universal regulation on IoT which means there are low standards on how safe the products are. Watch out for products that are too

good to be true in price and service. Keep in mind also that even reliable companies (Rumba, Nest) have had cameras turn on "accidentally".

Additionally, if you are responsible for setting up remote access for your company/team, check out this article on finding the right remote access solution**.**