Top Five Steps to Securely Work from Home

We know that working from home can be new to some of you, perhaps overwhelming as you adjust to your new environment. One of our goals is to enable you to work as securely as possible from home. Below are five simple steps to working securely. The best part is all of these steps not only help secure your work, but they will make you and your family far more safe and secure as you create a Cybersecure home.

1. **You**: First and foremost, technology alone cannot fully protect you, you are the best defense. Attackers have learned that the easiest way to get what they want is to target you, rather than your computer or other devices. If they want your password, work data or control of your computer, they'll attempt to trick you into giving it to them, often by creating a sense of urgency. For example, they can call you pretending to be Microsoft technical support and claim that your computer is infected when in reality they are just cyber-criminals that want you to give them access to your computer. Or perhaps they will send you an email warning that your package could not be delivered and pressure you to click on a link to confirm your mailing address when in reality they are tricking you to visit a malicious website that will hack into your computer. Ultimately, the greatest defense against attackers is you.

   Common sense will spot and stop most attacks.

2. **Home Network**: Almost every home network starts with a wireless (or Wi-Fi) network. This is what enables all your devices to connect to the Internet. Most home wireless networks are controlled by your Internet router or a separate, dedicated wireless access point. They both work in the same way by broadcasting wireless signals, the devices in your house connect via these signals. This means securing your wireless network is a key part of protecting your home. We recommend the following steps to secure it:

   - Change the default administrator password to your Internet router or wireless access point, whichever is controlling your wireless network. The admin account is what allows you to configure the settings for your wireless network.

   - Ensure that only people you trust can connect to your wireless network. Do this by enabling strong security. By enabling this, a password is required for people to connect to your home network, and once connected their online activities are encrypted.

- Ensure the password used to connect to your wireless network is a strong password and that it is different from the admin password. Remember you only need to enter the password once for each of your devices, as they store and remember the password.

Not sure how to do these steps? Ask your Internet Service Provider or check their website, check the documentation that came with your Internet router or wireless access point, or refer to their respective website.

3. **Passwords**: When a site asks you to create a password, create a strong and unique passphrase instead. A strong password is long, the more characters it has the stronger it is. We recommend you simply use a series of words that are easy to remember, such as "*bee honey bourbon*". Using a unique passphrase means using a different one for each device or online account. This way if one passphrase is compromised, all of your other accounts and devices are still safe. Can't remember all those passphrases?

   Use a password manager, which is a specialized program that securely stores all your passphrases in an encrypted format (and lots of other great features also). Finally, enable two-step verification (also called two-factor or multi-factor authentication) whenever possible. It uses your password, but also adds a second step, such as a code sent to your smartphone or an app that generates the code for you. Two-step verification is probably the most important step you can take to protect your online accounts and it's much easier than you may think.

4. **Updates**: Make sure each of your computers, mobile devices, programs and apps are running the latest version of its software. Cyber attackers are constantly looking for new vulnerabilities in the software your devices use. When they discover vulnerabilities, they use special programs to exploit them and hack into the devices you are using. Meanwhile, the companies that created the software for these devices are hard at work fixing them by releasing updates. By ensuring your computers and mobile devices install these updates promptly, you make it much harder for someone to hack you. To stay current, simply enable automatic updating whenever possible. This rule applies to almost any technology connected to a network, including Internet-connected TV's, baby monitors, security cameras, home routers, gaming consoles or even your car.

5. **Kids / Guests**: Something you most likely don't have to worry about at work is children, guests or other family members interrupting your work or using your work laptop or other devices. Make sure your family and friends understand they cannot use your work devices as they can accidentally erase or modify information, or perhaps even worse accidentally infect the device.

If you have any questions about how to securely work from home, don't hesitate to contact us. We are here to help you!