SANS SECURITY AWARENESS

Top 5 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 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. Or perhaps they send you an email warning that a package could not be delivered, fooling you into clicking on a malicious link. The most common indicators of a social engineering attack include:

- Someone creating a tremendous sense of urgency, often through fear, intimidation, a crisis or an important deadline.
- Pressure to bypass or ignore security policies or procedures, or an offer too good to be true (no, you did not win the lottery!).
- A message from a friend or co-worker in which the signature, tone of voice or wording does not sound like them.

Ultimately, the best defense against these attacks is you.

2 Home Network

Almost every home network starts with a wireless (often called Wi-Fi) network. This is what enables all of your devices to connect to the Internet. Most home wireless networks are controlled by your Internet router or a separate, dedicated wireless access point. Both work in the same way: by broadcasting wireless signals to which home devices connect. 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:** The administrator account is what allows you to configure the settings for your wireless network. An attacker can easily discover the default password that the manufacturer has provided.
- **Allow only people that you trust:** Do this by enabling strong security so that only people you trust can connect to your wireless network. Strong security will require a password for anyone to connect to your wireless network. It will encrypt their activity once they are connected.
- **Make passwords strong:** The passwords people use to connect to your wireless network must be strong and different from the administrator 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, check their website, check the documentation that came with your wireless access point, or refer to the vendor's website.

3 Passwords

When a site asks you to create a password, create a strong password: the more characters it has, the stronger it is. Using a passphrase is one of the simplest ways to ensure that you have a strong password. A passphrase is nothing more than a password made up of multiple words, 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 has lots of other great features, too!). 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 not only your work devices but 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 the office is children, guests or other family members using your work laptop or other work devices.

Make sure family and friends understand they cannot use your work devices.

They can accidentally erase or modify information, or, perhaps even worse, accidentally infect the device.

Want to learn more?

You can dive into more about each of these topics by visiting the OUCH! Newsletter website – **https://sans.org/ouch**

SANS SECURITY AWARENESS