We know that working from home can be new to some of you, perhaps overwhelming as you adjust to your new environment. 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 will make you and your family far more safe as you create a cybersecure home.

1. **Home Network**

   - **Secure your access point**
   - **Strong security is a key part of protecting your home.** We recommend the following steps to secure it:
     - **Configure the settings for your wireless access point.** This is what allows you to configure the settings for your wireless network. To access the configuration settings, you need to log in to the device. Here’s a link to the default password that the manufacturer has provided:
     - **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:
   - **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.
   - **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.

2. **Passwords**

   - **Password strength:** The passwords people use are often not strong enough. After all, password as a concept can be easily discovered by attackers. An attacker can easily discover your wireless network. An attacker can easily discover your wireless network. That came with your wireless access point, or refer to the vendor's website.

3. **Updates**

   - **Updates**

   - **Avoid the OUCH! Newsletter website – [https://sans.org/ouch](https://sans.org/ouch)**

4. **Kids & Guests**

   - **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 you 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 attackers to bypass or ignore security policies or procedures, or an offer too good to be true (no, you did not win the lottery!).

5. **Kids & Guests**

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

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

   - **Password manager:** A password manager is a specialized program that securely stores all your passwords and login information on an encrypted device. A password manager makes it easier to remember your passwords. It is impossible 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 you use. If you use the same passphrase for each of your devices, as you create a cybersecure home.

   - **Almost every home network starts with a wireless network, often through a home Internet service provider.** This is what enables all of your devices connect. This means securing your wireless network is a key part of protecting your home. We recommend the following steps to secure it:

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

   - **Almost every home network starts with a wireless network, often through a home Internet service provider.** This is what enables all of your devices connect. This means securing your wireless network is a key part of protecting your home. We recommend the following steps to secure it:

   - **Ask your Internet Service Provider, check their website, check the documentation provided.**

   - **Ask your Internet Service Provider, check their website, check the documentation provided.**

   - **Almost every home network starts with a wireless network, often through a home Internet service provider.** This is what enables all of your devices connect. This means securing your wireless network is a key part of protecting your home. We recommend the following steps to secure it:

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

   - **Almost every home network starts with a wireless network, often through a home Internet service provider.** This is what enables all of your devices connect. This means securing your wireless network is a key part of protecting your home. We recommend the following steps to secure it:

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

   - **Almost every home network starts with a wireless network, often through a home Internet service provider.** This is what enables all of your devices connect. This means securing your wireless network is a key part of protecting your home. We recommend the following steps to secure it:

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