We know that working from home can be new to some, 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 cybersecurity home.

### First and foremost, technology alone cannot fully protect you – it is important to recognize that the easiest way to get what you want is to work faster, rather than safer. For example, if you are using a weak password, work faster or control over your computer; they 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:

- A message from a friend or co-worker in which the signature, tone of voice or wording does not sound like them.
- A message from a friend or co-worker in which the signature, tone of voice or wording does not sound like them.
- Someone creating a tremendous sense of urgency, often through intimidation, a crisis or an important deadline.

### Not sure how to do these steps?

Ask your Internet Service Provider, check their website, or refer to the vendor’s website. Ask your Internet Service Provider, check their website, or refer to the vendor’s website.

---

### Security Awareness

In almost every home network, including not only your work devices but Internet-connected TV’s, baby monitors, security cameras, home routers, gaming consoles or even your car. 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:

1. **Configure the settings for your wireless network.**
2. **Change the default administrator password:**
3. **Allow only people that you trust to be listed:**
4. **Make passwords strong:**
5. **Can’t remember all those passphrases?**

Use a password manager, which is a specialized program that securely stores all your passwords. It 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 and account you connect to, as well as each of your other accounts and devices are still under attack.

---

### Updates

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

---

### Passwords

When a site asks you to create a password, create a strong password. The number of characters you use is critical. If it is unique, it is stronger. The password is one of the simplest things 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 and account you connect to, as well as each of your other accounts and devices are still under attack.

---

### Kids & Guests

Make sure each of your computers, mobile devices, programs and apps are running the latest version of its software.

---

### Cybersecurity Awareness

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

---

### Want to learn more?

Check these websites by visiting the Cybersecurity at Work website – https://cybersecurityatwork.org

---

### Security Awareness

You can learn more about cybersecurity and privacy by visiting the Cybersecurity at Work website – https://cybersecurityatwork.org

---

### Network

Almost every home network starts with a wireless (often called Wi-Fi) network. This is what allows people to connect to your wireless network. It will require a password for anyone to connect to your wireless network. Strong security means you must be sure that only people you trust can connect to your wireless network. Strong security so that only people you trust can connect to your wireless network. This means securing your wireless network is a key part of protecting your home. We recommend the following steps to secure it:

1. **Configure the settings for your wireless network.**
2. **Change the default administrator password:**
3. **Allow only people that you trust to be listed:**
4. **Make passwords strong:**
5. **Can’t remember all those passphrases?**

Use a password manager, which is a specialized program that securely stores all your passwords. It 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 and account you connect to, as well as each of your other accounts and devices are still under attack.

---

### Updates

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

---

### Passwords

When a site asks you to create a password, create a strong password. The number of characters you use is critical. If it is unique, it is stronger. The password is one of the simplest things 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 and account you connect to, as well as each of your other accounts and devices are still under attack.

---

### Kids & Guests

Make sure each of your computers, mobile devices, programs and apps are running the latest version of its software.

---

### Cybersecurity Awareness

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