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 they will make you and your family far more safe as you create a cybersecure home.

1. **Passwords**
   - **Change the default administrator password:** The administrator account is what allows you to configure the settings for your wireless network. Be sure to change the default password the manufacturer has provided.
   - **Remember the password:** Remember, you only need to enter the password once to connect them. The administrator password is a key part of protecting your home. We recommend the following steps to secure it:
     - Configure the settings for your wireless network. It will require a password for anyone to connect to your wireless network. The administrator password is what allows you to do this.
     - Make passwords strong: The passwords people use often make it easy for an attacker to guess them. Attackers have learned that the passwords people use are the best defense. Attackers have learned that the passwords people use are the best defense.
     - Do this by enabling strong security so that only people you trust can connect to your wireless network. Strong security means that anyone to connect to your wireless network must be strong enough: You have to enter the password once they are connected.
     - Make passwords strong: The passwords people use are the best defense.

2. **Home Network**
   - **Almost every home network starts with a wireless (often called Wi-Fi) network. This is what allows you to connect other devices to the Internet. Most home networks are controlled by your Internet router or a device called a wireless access point. The access point is connected to your modem. 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.
   - 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.
   - A message from a friend or co-worker in which the signature, tone of voice or wording does not sound like them.

3. **3. Passwords**
   - **When asked to create a password, create a strong password:** The password should be difficult to guess or crack. For example, something you most likely don’t have to worry about at the office is children, guests or other family members using your work computer or other work devices. If they want your password, they are the best defense. Attackers have learned that the passwords people use are the best defense.
   - 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.
   - 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.

4. **Updates**
   - **Software updates:** Cyber attackers are constantly looking for new vulnerabilities in the software your devices use. They discover vulnerabilities, and 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 cyber attackers to hack you. To stay current, simply enable automatic updating whenever possible. This rule applies to almost any technology connected to a wireless network. It will require a password for anyone to connect to your wireless network. The administrator password is what allows you to do this.
   - **Enable automatic updates:** Cyber attackers are constantly looking for new vulnerabilities in the software your devices use. They discover vulnerabilities, and 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 cyber attackers to hack you. To stay current, simply enable automatic updating whenever possible. This rule applies to almost any technology connected to a wireless network. It will require a password for anyone to connect to your wireless network. The administrator password is what allows you to do this.
   - **Enable automatic updates:** Cyber attackers are constantly looking for new vulnerabilities in the software your devices use. They discover vulnerabilities, and 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 cyber attackers to hack you. To stay current, simply enable automatic updating whenever possible. This rule applies to almost any technology connected to a wireless network. It will require a password for anyone to connect to your wireless network. The administrator password is what allows you to do this.
   - **Enable automatic updates:** Cyber attackers are constantly looking for new vulnerabilities in the software your devices use. They discover vulnerabilities, and 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 cyber attackers to hack you. To stay current, simply enable automatic updating whenever possible. This rule applies to almost any technology connected to a wireless network. It will require a password for anyone to connect to your wireless network. The administrator password is what allows you to do this.
   - **Enable automatic updates:** Cyber attackers are constantly looking for new vulnerabilities in the software your devices use. They discover vulnerabilities, and 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 cyber attackers to hack you. To stay current, simply enable automatic updating whenever possible. This rule applies to almost any technology connected to a wireless network. It will require a password for anyone to connect to your wireless network. The administrator password is what allows you to do this.
   - **Enable automatic updates:** Cyber attackers are constantly looking for new vulnerabilities in the software your devices use. They discover vulnerabilities, and 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 cyber attackers to hack you. To stay current, simply enable automatic updating whenever possible. This rule applies to almost any technology connected to a wireless network. It will require a password for anyone to connect to your wireless network. The administrator password is what allows you to do this.

5. **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 your devices use. They discover vulnerabilities, and 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 cyber attackers to hack you. To stay current, simply enable automatic updating whenever possible. This rule applies to almost any technology connected to a wireless network. It will require a password for anyone to connect to your wireless network. The administrator password is what allows you to do this.
   - **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. They discover vulnerabilities, and 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 cyber attackers to hack you. To stay current, simply enable automatic updating whenever possible. This rule applies to almost any technology connected to a wireless network. It will require a password for anyone to connect to your wireless network. The administrator password is what allows you to do this.
   - **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. They discover vulnerabilities, and 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 cyber attackers to hack you. To stay current, simply enable automatic updating whenever possible. This rule applies to almost any technology connected to a wireless network. It will require a password for anyone to connect to your wireless network. The administrator password is what allows you to do this.