You

Someone creating a tremendous sense of urgency, often through fear, intimidation, a crisis or an important deadline.

Almost every home network starts with a wireless device called an access point. This device is used to let your devices connect to the Internet. Most home networks use an access point installed by your Internet Service Provider, 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. **Change the default administrator password:** The administrator password allows you to configure the settings for your wireless network. The attacker can easily discover your wireless network. An attacker can easily discover your wireless network. The default password that the manufacturer has provided.

2. **Secure your wireless network:** If you are using a separate, dedicated wireless access point, then strong security so that only people you trust can connect to your wireless network. Strong security means using a strong security setting, such as WPA2, for each of your devices, as well as strong passwords. The passwords people use.

3. **Passwords:** Use manager, which is a specialized program that securely stores all your passwords 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. 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.

- **Two-step verification:** 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.
- **Password managers:** The people use to connect to your wireless network must be strong and different from the password you use for other accounts. You only need to remember one password, and all of your other accounts and devices are still safe.

4. **Updates:** Cyber attackers are constantly looking for new vulnerabilities in the software you 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 attackers to hack you. To stay current, simply enable automatic updating on your devices.

5. **Kids & Guests:** Children, guests, or other family members using your work laptop or other work device.

- **Make sure family and friends understand they cannot use your work devices.** They can accidentally erase or modify information, or, perhaps worse, accidentally infect the device. Something you most likely don’t have to worry about at the office.

- **Make sure your work data or control of your computer is not compromised, someone to hack. To stay current, simply enable automatic updating on your devices.”

- **Updates:** Cyber attackers are constantly looking for new vulnerabilities in the software you 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 attackers to hack you. To stay current, simply enable automatic updating on your devices.”

- **Kids & Guests:** Children, guests, or other family members using your work laptop or other work device.

- **Make sure family and friends understand they cannot use your work devices.** They can accidentally erase or modify information, or, perhaps worse, accidentally infect the device. Something you most likely don’t have to worry about at the office.