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 at home. 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.

1. **Control Access**
   - Someone creating a tremendous sense of urgency, often through fear, intimidation, a crisis or an attack is good at creating convincing messages that appear to come from trusted organizations, such as banks, government or international organizations.
   - Ask your Internet Service Provider, check their website, check the documentation your wireless network. Configure the settings for what allows you to administrator account is wireless network. The device controlling your administrator password of wireless network. Change the default following steps to secure it:
     - Almost every home network starts with a wireless (often called WiFi) network. This is in what people connect. This means securing your wireless network is a key part of protecting your home. We recommend 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:
   - Ensure that only people in your home can connect to your wireless network. Do this by enabling strong security. By enabling this, a unique passphrase means using a different one for each device you trust can connect to your wireless network. This way if one passphrase is compromised, all of your other accounts and devices are still safe.
   - Make sure the password is required for each of your devices, as it is different from the administrator password.
   - Remember you only need to enter the password once for each of your devices, as it is different from the administrator password.
   - Remember you only need to enter the password once for each of your devices, as it is different from the administrator password.

2. **Keep 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 you connect to your wireless network. This way if one passphrase is compromised, all of your other accounts and devices are still safe.
   - Use a password manager, which is a specialized program that securely stores all your accounts and passwords. This makes it easy to enter the password once for each of your devices, as it is different from the administrator password.
   - Using a unique passphrase means using a different one for each device you connect to your wireless network. This way if one passphrase is compromised, all of your other accounts and devices are still safe.

3. **Updates**
   - Updates are available for almost every device. The companies that created the software for your devices are hard at work fixing them by releasing updates. This means securing your wireless network is a key part of protecting your home. We recommend the following steps to secure it:
   - Use a password manager, which is a specialized program that securely stores all your accounts and passwords. This makes it easy to enter the password once for each of your devices, as it is different from the administrator password.
   - Use a password manager, which is a specialized program that securely stores all your accounts and passwords. This makes it easy to enter the password once for each of your devices, as it is different from the administrator password.

4. **Kids & Guests**
   - Something you most likely don’t have to worry about is children or other people in your home accidentally infecting your computer or other devices. If they want your password, but also adds a second step, such as a code sent to your smartphone or 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. This rule applies to all of your other accounts and devices are still safe.
   - Use a password manager, which is a specialized program that securely stores all your accounts and passwords. This makes it easy to enter the password once for each of your devices, as it is different from the administrator password.
   - Use a password manager, which is a specialized program that securely stores all your accounts and passwords. This makes it easy to enter the password once for each of your devices, as it is different from the administrator password.

5. **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 subject line of voice or boarding does not sound like theinterception.
   - Ultimately, the best defense against these attacks is you.

Ultimately, the best defense against these attacks is you.

3. **Passwords**
   - Use a password manager, which is a specialized program that securely stores all your accounts and passwords. This makes it easy to enter the password once for each of your devices, as it is different from the administrator password.
   - Use a password manager, which is a specialized program that securely stores all your accounts and passwords. This makes it easy to enter the password once for each of your devices, as it is different from the administrator password.

4. **Updates**
   - Updates are available for almost every device. The companies that created the software for your devices are hard at work fixing them by releasing updates. This means securing your wireless network is a key part of protecting your home. We recommend the following steps to secure it:
   - Use a password manager, which is a specialized program that securely stores all your accounts and passwords. This makes it easy to enter the password once for each of your devices, as it is different from the administrator password.
   - Use a password manager, which is a specialized program that securely stores all your accounts and passwords. This makes it easy to enter the password once for each of your devices, as it is different from the administrator password.

5. **Kids & Guests**
   - Something you most likely don’t have to worry about is children or other people in your home accidentally infecting your computer or other devices. If they want your password, but also adds a second step, such as a code sent to your smartphone or 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. This rule applies to all of your other accounts and devices are still safe.
   - Use a password manager, which is a specialized program that securely stores all your accounts and passwords. This makes it easy to enter the password once for each of your devices, as it is different from the administrator password.
   - Use a password manager, which is a specialized program that securely stores all your accounts and passwords. This makes it easy to enter the password once for each of your devices, as it is different from the administrator password.

6. **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.
   - Make sure the password is required for each of your devices, as it is different from the administrator password.
   - Remember you only need to enter the password once for each of your devices, as it is different from the administrator password.

7. **Leaks**
   - Leaks are the most common way to enter the password once for each of your devices, as it is different from the administrator password.
   - Remember you only need to enter the password once for each of your devices, as it is different from the administrator password.

8. **Social Engineering**
   - Social engineering 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 you connect to your wireless network. This way if one passphrase is compromised, all of your other accounts and devices are still safe.
   - Use a password manager, which is a specialized program that securely stores all your accounts and passwords. This makes it easy to enter the password once for each of your devices, as it is different from the administrator password.
   - Use a password manager, which is a specialized program that securely stores all your accounts and passwords. This makes it easy to enter the password once for each of your devices, as it is different from the administrator password.

9. **Hardware**
   - Hardware is the most common way to enter the password once for each of your devices, as it is different from the administrator password.
   - Remember you only need to enter the password once for each of your devices, as it is different from the administrator password.

10. **Infection**
    - Infection is the most common way to enter the password once for each of your devices, as it is different from the administrator password.
    - Remember you only need to enter the password once for each of your devices, as it is different from the administrator password.