FIVE STEPS to Securely Work from Home

We know that working from home is new to some people and possibly even overwhelming. One of RYMARK's goals is to enable you to work as securely and productively as possible from home. The following five simple steps to working more securely will keep you and your family much safer from cyber attacks.

1) You:

You are your best defense against unauthorized access. Attackers have learned that the easiest way to get your password, work data or control of your computer, is to trick you into giving it to them by creating a sense of urgency, often panic! For example, they may 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. There has been a BIG increase in COVID-19 inspired malicious emails and websites. The most common indicators of this kind of attack include:

❏ ***Urgency:*** *Someone creating a tremendous sense of urgency, often through fear. Cyber attackers are good at creating convincing messages that appear to come from trusted organizations, such as banks, government or international organizations.*

❏ ***Policies:*** *Someone pressuring you to bypass or ignore security policies or procedures, or providing an offer too good to be true (no, you did not win the lottery!) Someone may even pretend to offer advice or health information.*

❏ ***Contacts:*** *A message from a friend or co-worker in which the signature, tone of voice or wording does not sound like them. Watch out for emails that appear to be from high-ranking employees in your organization but have a slight variation from the actual email address of senders. Scan those emails with a sharp eye and do not open attachments unless you are sure they are from a trusted source.*

The best defense against these attacks is you.

2) Home Network:

Almost every home network starts with a wireless (often called Wi-Fi) network. This is what enables all of your devices to connect to the Internet. Most home wireless networks are controlled by your Internet router or a separate, dedicated wireless access point. Securing your wireless network is a key part of protecting your home. We recommend the following to secure your home network:

❏ ***Change the default administrator password:*** *The administrator account is what allows you to configure the settings for your wireless network. An attacker can easily discover the default password that the manufacturer has provided. Not sure how to do this? Ask your Internet Service Provider, check the documentation that came with your wireless access point, or refer to the vendor's website.*

❏ ***Allow only people that you trust:*** *Require a password for anyone to connect to your wireless network. It will encrypt their activity once they are connected.*

3) Passwords:

When a site asks you to create a password: create a strong password. 12 characters or more is best. 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 "crunchypeanutbutter." Using a unique passphrase means using a different one for each device or online account. This way if one passphrase is compromised, all of your other accounts and devices are still safe.

Can't remember all those passwords? Use a password manager such as Passportal, which is a specialized program that securely stores all your passwords in an encrypted format.

Finally, enable two-step verification (also called two-factor or multi-factor authentication) whenever possible. 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. 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.

4) Updates:

Make sure each of your computers, mobile devices, programs and apps are running the latest software version. New vulnerabilities are continually being found in applications and operating systems. When cybercriminals discover vulnerabilities, they use special programs to exploit them and hack into the devices you are using.

The companies that created the software for your devices are hard at work to make them secure by releasing updates. By ensuring your computers and mobile devices install these updates promptly, you make it much harder for someone to hack you. Enable automatic updating whenever possible. This rule applies to almost any technology connected to a network, including not only your work devices but Internet-connected TV's, baby monitors, security cameras, home routers, gaming consoles or even your car.

5) Keep Your Work Separate:

Nearly one-third of users use their company computer for personal use. It not only affects productivity but invites security threats. Also, make sure your family understands they cannot use your work devices.

Contact RYMARK at 651-328-8905 or info@rymarkIT.com with IT security questions, remote support or to request our 15 Ways to Protect Your Business from a CYBER ATTACK checklist.