Top 5 Tips for Securely Working from Home

Working from home is new to many of us. One of our goals is to ensure you work from home as securely as possible. Check out these five simple steps to working securely. The best part is all of these steps not only help secure your work, but will make you and your family far more safe as you create a cybersecure home.

1 YOUR ROLE

You are the best defense against security attacks. Attackers target you, rather than your devices. Common indicators of an attack:

- **Urgency.** This includes fear, intimidation, crisis or an important deadline. Messages may appear to come from trusted organizations such as banks. If you receive an urgent request, respond using a known (and external to the communication) means. If you get a suspicious email, call the organization in question to confirm.
- **Policy Pressure.** Watch for pressure to bypass or ignore security policies or procedures, or an offer that appears too good to be true. Often attackers start small and escalate to more significant requests. If this happens, contact your manager, security or privacy resource to discuss.
- **Be Careful with Contacts.** Watch for messages that appear to come from a friend or co-worker, but do not match their typical signature, tone or wording. If this happens, contact the individual using a known (and external to the communication) means. If you get a suspicious email, call the individual in question to confirm.

2 HOME NETWORK

Almost every home has a wired or Wi-Fi network which enables devices to connect to the Internet. Most home wireless networks are controlled by an Internet router or a separate, dedicated wireless access point. Both work in the same way - by broadcasting wireless signals. Securing your wireless network is a key part of protecting your home. Take these steps to secure your wireless network:

- **Change the Default Administrator Password.** The administrator account allows you to configure the settings for your wireless network. An attacker can easily discover the default password provided by the manufacturer. If the password is not changed upon initial installation, an attacker can connect to the device and log in with the default username and password.
- **Only allow access to those you trust.** Only allow those you trust to connect to your wireless network. Strong security will require a password for anyone to connect to your wireless network. It will encrypt their activity once they are connected.
- **Create strong passwords.** The passwords people use to connect to your wireless network must be strong (not easily guessed) and different from the administrator password. Remember, you only need to enter the password once for each of your devices, as the devices store and remember the password.

If you have questions about the steps above, 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.

Eastern Health Central Health Western Health Labrador-Grenfell Health Newfoundland & Labrador Centre for Health Information

Top 5 Tips for Securely Working from Home

Working from home is new to many of us. One of our goals is to ensure you work from home as securely as possible. Check out these five simple steps to working securely. The best part is all of these steps not only help secure your work, but will make you and your family far more safe as you create a cybersecure home.

3 PASSWORDS

When a site asks you to create a password, create a strong one. The more characters a password has, the stronger it will be, making it harder to guess, and even harder to hack. 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 or online account. This way if one passphrase is compromised, all of your other accounts and devices are still safe.

Can't remember all your passphrases? Use a password manager, which is a specialized program that securely stores all your 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. 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 one of the most important steps you can take to protect your online accounts and it is much easier than you may think.

4 UPDATES

Make sure each of your computers, mobile devices, programs and apps are running the latest version of software and anti-virus software. Cyber attackers are constantly looking for new vulnerabilities in the software your devices use. When they discover vulnerabilities, they use special programs to exploit and hack. The companies that have created the software for these devices work hard to fix these vulnerabilities through regular updates. By ensuring your computers and mobile devices install these updates promptly, you make it much harder for someone to hack you. To stay current, simply enable automatic updating whenever possible. This rule applies to almost any technology connected to a network, including your work devices and Internet-connected TV's, baby monitors, security cameras, home routers, gaming consoles or even your vehicle.

5 CHILDREN AND GUESTS

While working from home, it may be tempting for children, guests and other family members to use your work laptop or other work device. Please ensure family and friends understand they cannot use your work devices, as they can accidentally modify or erase information, or accidentally infect the device.

Eastern Health

Central Health

Western Health

Labrador-Grenfell Health

Newfoundland & Labrador Centre for Health Information

Protecting Information and Privacy While Working from Home

Protect Your Own Privacy

- Blur background when using Teams Video Chat.
- If you are making calls using your personal phone line, block your number - *67, then dial the individual's number.

Protections for Meetings and Calls

- During meetings, ensure you recognize those who are joining.
- Request people identify themselves as they join calls.
- Do not record meetings or calls without permission from all parties.
- Limit discussions to **only the necessary information**, this includes PHI and PI.
- Check email addresses before sending meeting invites.
- If possible, participate in meetings in a quiet area or advise family members of the confidentiality of what they may overhear.
- Never conduct sensitive business near a smart speaker.

Protecting Records

- The record of source should be the electronic record.
- Avoid (if possible) printing records from home.
- **Do not delete records.**
- Name files appropriately, for example: RHACovid19 DSA 2020-03-20.
- Document all business decisions.
- Store final versions of records on the K drive, SharePoint or HPRM.
- When emailing PI or PHI, minimize the information to only what is necessary.

Remember, we are all responsible for the protection of information. Following the pandemic, we will need to demonstrate that we maintained a reasonable protection of information.

Eastern Health   Central Health   Western Health   Labrador-Grenfell Health   Newfoundland & Labrador Centre for Health Information