STAY HOME. STAY SECURE.

Working from home can have many advantages. You get to avoid the commute, take the dog for a walk, or even stay in your pajamas. But don't get too casual – cyber criminals thrive on taking advantage of us when we're busy and distracted. To stay secure, ask yourself these three questions about your remote office:

1. AM I USING A SECURE INTERNET CONNECTION?

How you connect to the internet is just as important as what you do once connected.

In public. If you're connecting to a public Wi-Fi, at the local café for example, make sure it's secure. Verify that the network belongs to the establishment (and not a hacker spoofing the ID), and that the network requires a password. Even then, you should use a Virtual Private Network (VPN) and limit the amount of sensitive information you access–just as a precaution.

At home. Your home may be your palace, but that doesn't mean that your personal Wi-Fi router is secure. Take a little time to learn about your router's security settings, and never assume that the default settings keep you secure by default!

SECURING YOUR HOME WI-FI

Here's your checklist for a more secure home Wi-Fi:

- ✓ Update your personal router's firmware
- ✓ Protect your router with a unique password
- ✓ Enable WPA-2 security
- ✓ Never broadcast your router SSID/network name
- ✓ Use a guest network to separate your work devices

2. IS MY WORK AREA PRIVATE?

The information you access must be kept away from unauthorized individuals.

In public. It's normal to be curious about what other people are doing on computer screens or saying on the phone, so avoid situations where others can eavesdrop or shoulder surf–whether they're doing so maliciously, or just out of curiosity. Find someplace out of the way and consider using a privacy filter on your laptop.

At home. It's easy to let your personal and professional lives mix when you're working from home. As much as possible, create space where you can work without life getting in the way. This means making sure people you live with can't access your work information or devices. It also means using common sense, like locking your doors and windows when you leave.. Don't forget about "smart speakers," and other voice-activated devices which might be listening to sensitive work conversations.

3. AM I FOLLOWING SECURITY POLICIES?

Without peer pressure from coworkers, reminders around our facility, or a more security-conscious office environment, you might find yourself forgetting to take some essential actions at home that you probably perform all the time while working in the office.

Our organization's security policies apply even though we're working off-site. Use our Top Ten Tips to follow best practices.

So take advantage of working from home -- walk the dog, work in your pj's -- but don't let cyber criminals take advantage of you.

OFF-SITE SECURITY TOP 10

Keep these tips in mind to apply security best practices while working off-site:

1. Stay alert for social engineering, even in unexpected settings.
2. Keep using strong, unique passwords.
3. Access work systems and information while connected to a VPN or virtual desktop.
4. Utilize approved methods for encrypting files and communications.
5. Use personal devices only once approved by IT.
6. Secure physical records when not in use.
7. Destroy physical records only using a secure shredder.
8. Add a password to video conferences.
9. Remove "smart speakers" and other devices to avoid threatening compliance with privacy regulations.
10. Report incidents right away!