Security Tips for Working from Home

Given these circumstances, we figured it would be useful to share some of the security tips we have for WFH (working from home), not just for IT teams who suddenly need to secure their entire remote workforce, but for individuals to take their own precautions.

Physical security

The first so-obvious-it's-not-obvious tip is to make sure your work devices are physically safe, and that you avoid offering unauthorized views of confidential information. Here are a few ways to shore up physical security while WFH:

- If you need to leave your home for supplies or other reasons, make sure your work devices are either shut down or locked—including any mobile phones you might use to check email or make work phone calls.
- If you live with a roommate or young children, be sure to lock your computer even when you step away for just a bit. Don't tempt your roommates or family members by leaving your work open. This is true even for the workplace, so it is imperative for WFH.
- If you can't carve out a separate work space in your home, be sure to collect your devices at the end of your workday and store them someplace out of sight. This will not only keep them from being accidentally opened or stolen, but will also help separating your work life from your home life.

System access

Perhaps your office network was so protected that little thought was given to restricting access to servers with sensitive data. Or perhaps you now have to work on your personal laptop—one that you didn't think much about securing before coronavirus upended your life.

Either way, it's time to start thinking about the ways to guard against unauthorized access. If you think cybercriminals (and regular criminals) will be sensitive to global events and refrain from attacking remote workers.

- Access to the your computer's desktop should at least be password protected, and the password should be a strong one. If the system is stolen, this will keep the thief from easily accessing company information.

- If office network permissions previously gave you unfettered access to work software, now you may be required to enter a variety of passwords to gain access. If your workplace doesn't already offer a single sign-on service, consider using a password manager. It will be much more secure than a written list of passwords left on your desk.
- Encryption also helps protect information on stolen or compromised computers. Check whether data encryption is active on your work machine. If you're not sure, ask your IT department whether you have it, and if they think it's necessary.
- If you're connecting your work computer to your home network, make sure you don't make it visible to other computers in the network. If you have to add it to the HomeGroup, then make sure the option to share files is off.

Separate work and personal devices

Just as it's important to carve out boundaries between work life and home life while WFH, the same is true of devices. Do you have a child being homeschooled now and turning in digital assignments? Are you ordering groceries and food online to avoid stores? Best not to cross those hairs with work.

While it may seem cumbersome to constantly switch back and forth between the two, do your best to at least keep your main work computer and your main home computer separate (if you have more than one such device). If you can do the same for your mobile devices—even better. The more programs and software you install, the more potential vulnerabilities you introduce.

- Don't pay your home bills on the same computer you compile work spreadsheets. You can not only create confusion for yourself, but also end up compromising your personal information when a cybercriminal was looking to breach your company.
- Don't send work-related emails from your private email address and vice versa. Not only does it look unprofessional, but you are weaving a web that might be hard to untangle once the normal office routine resumes.
- Speaking of homeschooling, it's especially important to keep your child's digital curriculum separate from your work device. Both are huge targets for threat actors. Imagine their delight when they find they can not only plunder an organization's network through an unsecured remote worker, but they can also collect highly valuable PII on young students, which garners a big pay day on the dark web.

Secure connections

- Make sure you have access to your organization's cloud infrastructure and can tunnel in through a VPN with encryption.

- Secure your home Wi-Fi with a strong password, in case VPN isn't an option or if it fails for some reason.
- Access to the settings on your home router should be password protected as well. Be sure to change the default password it came with—no 12345, people!

Cybersecurity best practices

Other security precautions may not be all that different from those you should be practicing in the office, but they are easy to forget when you are working in your own home environment. A few of the most important:

- Be wary of phishing emails. There will be many going around trying to capitalize on fear related to the coronavirus, questions about isolation and its psychological impacts, or even pretending to offer advice or health information. Scan those emails with a sharp eye and do not open attachments unless they're from a known, trusted source.
- Related to phishing: I'm pretty sure we can expect to see a rise in Business Email Compromise (BEC) fraud. Your organization may be sending you many emails and missives about new workflows, processes, or reassurances to employees. Watch out for those disguising themselves as high-ranking employees and pay close attention to the actual email address of senders.
- Beware of overexposure on social media, and try to maintain typical behavior and routine: Do you normally check social media on your phone during lunchtime? Do the same now. Once again, watch out for scams and misinformation, as criminals love using this medium to ensnare their victims.

Other security precautions

Not every organization was prepared for this scenario, so it's only natural that some may not have the level of RemoteSec in place that others do. Make sure to get yourself up to speed with the guidelines that your organization has in place for remote work. Ask for directions if anything is unclear. Not everyone has the same level of tech savvy—the only stupid question is one that isn't asked.

I have listed some of the questions you may need to have answered before you can rest assured that is not going to be a security disaster. Here are some to consider:

- When you are working remote for long periods, make sure you know who is responsible for updates. Are you supposed to keep everything up to date or can your IT department do it for you?
- Your system may require additional security software now that it has left the safer environment of your organization's network. Check with your IT department on whether you should install addition solutions: Will you need a security program for your Window PC or for your Mac (which was hit with twice as many threats as

Windows computers in 2019)? If you're using an Android device for work, should you download security software that can protect your phone? (iOS doesn't allow outside antivirus vendors.)

- How will data storage and backup work? Can you save and back up your local files to a corporate cloud solution? Find out which one they prefer you to use in your specific role.

On a different note

This is a big adjustment for many people. Your first few days of WFH may leave you irritated, uncomfortable, unmotivated, or just plain exhausted. Adding security tips to the list may just add to your fatigue right now. We understand. Take it a day at a time, a step at a time.

When working from home, find a comfortable working area where you can assume a healthy posture, minimize the distraction from others, and where your presence has the least impact on how others have to behave. Take breaks to stretch your legs, and give your eyes a rest. And if you enjoy WFH, now is the time to prove to your employer that it's a viable option in the long run.

Stay safe, everyone! Now more than ever.