Working From Home:

Seven Easy Ways to Keep You and Your Workplace Safe Online

August 2022

No matter where you are in the world, chances are you've been affected in some way by COVID-19. The pandemic has sent workers and students home, canceled social events like graduations and weddings, and put mass populations—especially the elderly and immunocompromised—at risk.

In light of the restrictions around COVID-19, many employers are asking their employees to work from home. If you are fortunate enough to have this option, it's important to make sure you're not putting yourself and your workplace at greater risk of digital harm. Phishing and ransomware attacks are increasing as COVID-19 spreads; Cloudflare reported that cyber-attacks grew 37 percent in the United Kingdom in March 2020.

> You wouldn't ask a doctor or nurse to work without personal protective equipment. Neither should you.

Gear Up: Follow these easy tips to secure the work you do in your home and on your home network.

1. Keep Your Smart Assistants Out of the Room While You're Working.

Smart assistants are always listening for a "wake" word—like how your Amazon Echo will start paying attention to audio when it hears "Alexa". This makes smart assistants a potential unintended eavesdropper on confidential work conversations during video and phone calls.

An easy fix is to turn off or move your smart assistant to another room while you hold your work conversations. You won't need it to play music, update your grocery list, or ask it a quick question during your calls. If you still want it around, make sure that you disable the listening mode or simply unplug it during conversations. If you accidentally hold a work conversation within range of a smart assistant, you may be able to delete the recording manually. For example, you can delete saved audio files from Siri in the "Settings" of an Apple device, and delete recordings from Google Home devices. Note that the service provider may still maintain a copy of recordings even though the user has deleted them from their account, and this may or may not be evident to the user. Thus, it is best to err on the side of caution and disable the devices during work calls as described above.

2. Use Unique Passwords and a Password Manager.

It may be convenient to use the same password for everything work-related, but this puts your workplace at greater risk of a data breach or an account hack. Once someone discovers your password, they can easily gain entrance into all your work systems and compromise both your and your employer's data.

Since it's hard to remember unique passwords for every single work system, consider using a password manager. This lets you save all your unique passwords in one place, and often includes a feature that automatically inputs your passwords when logging into different accounts. The benefit of this solution is you only must remember one master password to get access to all your accounts. Many different sites and platforms offer guidelines on how to pick the password manager that's right for you; check out a few resources here, here, and here.

End-to-end (E2E) Encryption This kind of encryption is highly secure and ensures that only the sender and intended recipient can read messages and information. With E2E encryption, even the communication service cannot access the information.

3. Implement Two-factor Authentication Wherever Possible.

Unique passwords and password managers are helpful and important, but you can and should go even further to protect your work systems if possible. If you want to take password security to the next level, find out which of your work systems offer two-factor authentication.

There are various types of two-factor authentication. One way is to have a code sent to you via SMS or email when you're logging into a work system. Keep in mind that this method is not completely secure because SMS and email are often not encrypted. When your only choice is SMS, it is important that you protect your mobile number from a SIM swap attack. Some mobile operators allow users to enable a PIN or secret password to prevent such attacks.

A better option would be to use an authenticator app, which can either allow you to open the app to prove that it's really you logging in, or it can generate different codes for you to enter every time you log in to a work system. The codes are often time-limited, so even if an attacker got access to them through your emails or SMS messages, they wouldn't be able to use them again later.

An even better option would be to use a physical authentication token (e.g., Yubikey). This is a small USB key that you can put on your keychain and use whenever you're logging in to a service that supports it.

4. Opt for Online Services with Strong Encryption.

Encryption is the best way to keep your data safe as you work from home. It is one of the strongest tools that online systems can use to protect user information, data, and core information systems. If you aren't using systems secured by strong encryption, your own data and your employer's information are at greater risk of a security breach.

> Systems with strong encryption make it harder for others to access your communications, ensure that your content isn't readable even if someone does get access, and help prevent an attacker from changing the information.

For both existing and new work systems, find out whether or not an online system automatically encrypts communications and data by taking a look at their privacy and security statements (aka “policies”). You can also do a simple online search to see if specific services use encryption and what they encrypt, but as with everything you search for, make sure any resources you rely on are credible and up-to-date. End-to-end encryption offers the strongest level of communications security, so make sure it’s in place before using new software. Sometimes applications don’t automatically turn on encryption, so be sure to check that you can turn it on yourself. Make sure your smartphone, tablet, laptop and/or any other connected devices you use are encrypted and protected with a strong and unique password wherever possible.

5. Use a VPN—Even on Your Home Network.

When you're logged into your employer’s network while in the office, you may not always think about making sure that your connection is secure. Your company may do part of that for you through an intranet accessed via a secure portal. But when you're working remotely, make sure you're protecting all your traffic. A Virtual Private Network (VPN) may be an appropriate tool.

Some employers may automatically include VPNs on work laptops that employees take home. If you are working on a personal computer or your work computer doesn't already have a VPN, read up on how to choose and download one that will secure your online activity on your workplace systems. But be wary of “free” VPNs: if they don’t charge their users, it’s possible they are making their money by selling your personal data - which may include your browsing history.

6. Update Your Software.

It's easy to click "remind me tomorrow" when your software notifies you of updates, but updates often come with more than just new features. They also include fixes to bugs or security vulnerabilities. You can significantly improve your computer and data security by staying on top of software updates. This will also keep your employer's network safer in the process.

Updating your software is even easier when you're working from home. Try updating your software while you're getting ready in the morning, on a lunch break, or after you've finished your work for the day.

7. Back Up Your Files.

Anyone can be the victim of a ransomware attack. In these kinds of attacks, criminals will block access to data, systems and saved information, and hold the information hostage until the victim

pays a ransom. While your workplace should always be backing up files, you should be extra diligent to secure your files while working from home.

Start by asking your employer for guidance on how to back up your files when working remotely. This can be done using a cloud provider and/or an external storage device. Make sure to disconnect the device holding your backed up files when not in use so you can still access them if your original files are compromised. The backup should be encrypted and password protected.

For more information on how you can stay secure at your workplace, check out our factsheet with Next Century Cities.

For more information on how encryption plays a critical role in securing our day to day activities, go to https://www.internetsociety.org/issues/encryption/