How to Securely Work from Home

The Coronavirus epidemic is affecting workers around the globe. As a result, many businesses are transitioning large portions of their workforce to work-from-home situations. While some organizations already had policies, procedures, and technologies in place to facilitate a sizeable remote-work capability, other organizations – **especially small businesses** – are having to improvise and adapt to the new normal quickly.

The purpose of this guide is to help you and your employees be as secure as possible while working from your home. Because your organization may be limited in time and resources and it's impossible to anticipate or address all possible technologies or technical implementation, this strategic guide is focused on **simple and actionable policy recommendations**.

We recommend implementing as many of these as you comfortably can and seek technical assistance from us as required.

If you have any questions about the advice in this guide, please contact ePlace Solutions at cyberteam@eplaceinc.com.

Contents

SECURING YOUR WORK ENVIRONMENT

Securing your work environment means ensuring your home network is safe, the computers you perform work on are adequately secured, and your work is performed in a clean and secure workspace.

Home / wireless router

Your home router is the primary protection you have against most Internet threats. It is designed to keep hackers from reaching directly into your home network. However, there are a few precautions you need to take to ensure it is configured for maximum security. Look up your router's user manual and perform the following:

1. Ensure remote management is DISABLED. If it is enabled, it can allow remote attackers to take over your router and therefore your network.
2. Set the administrative password to be strong[1]. Write the password down and tape it to your router so you do not forget it[2].
3. Configure the wireless network to use WPA2 or WPA3 encryption. Change the password NOW and make sure the password is strong. Yes, you will have to rejoin all your devices, but now you are positive you know every device can connect. Change the password every three months until the quarantine is over, and do not give it out frivolously.
4. Ensure your router is up to date. This can be done in two ways. First, call your ISP and ask them to determine if your router is the latest version and has the latest firmware. If your router is more than three years old, it may have unfixable security problems and may need to be physically upgraded. If your firmware is out of date, the ISP may be able to update it remotely. Otherwise, you may need to do so yourself. (Be very careful with this operation, it is somewhat technical and can brick your router).

Patching

Hackers are under quarantine too. They have even more time on their hands to find and exploit vulnerabilities in popular programs and operating systems. Ensure your system is set up to perform automatic updated. Set a good time for this to happen, like 2 AM on Saturday morning. Make sure at the end of the day Friday you save all your work so the updating can occur.

---

[1] A note about strong / secure passwords: This is a subject with many considerations and much competing guidance. However, it is mathematically demonstrable a password that: a) is at least 12 characters long, b) consists of at least uppercase AND lowercase letters, and c) is changed at least three times per year, is currently secure from brute-force attack without the aid of a nation-state-grade supercomputer.

[2] You always hear about NOT writing down your password, and it is generally good advice. However, if someone is in your closet and reading a password off your router, you may have bigger problems.

Malware protection

Check your malware protection solution. Make sure it is properly installed and up to date. Consider changing the program you use to ensure you are using the best available.

When configuring the anti-malware solution, you want to ensure the following are configured:

1. Full-disk scanning – set this to run once a week, overnight (don't set this to run the same time as automatic updates). This will ensure the whole system is scanned regularly.
2. On-access scanning – this feature scans a file before it is opened. This feature is great for stopping e-mail viruses and viruses hidden in files on CD/DVD/USB you may have been given.
3. Heuristics – virus scanners use "signatures," which are digital fingerprints identifying whether the anti-virus company has seen the file before and whether it could contain malware. This is not a perfect system, as an attacker can easily change one bit of a file and have the signature no longer match. Heuristic scanning performs some behavioral analysis of the file to determine if it looks like it may access critical functions. It provides an additional set of checks on a potentially malicious file and dramatically increases the odds of detection.

Separation of work and home

Keeping work and home separate is good not only for security, but for mental health. If possible, have a separate computer for work that is not used for anything else.

However, not everyone has the luxury of multiple computers. If you must share a computer, then make sure all non-work applications are closed before you start work. When you are done with work, make sure you are safely saving all work, closing all work applications, and closing all remote access before releasing the computer for personal use.

COMMUNICATING SECURELY

Communications are important to keeping in touch with your clients, co-workers, and management. This means ensuring connections to the corporate network are secured, document sharing via e-mail and other apps are secured, and sensitive conversations are kept confidential.

Virtual Private Networks (VPNs)

Your organization may have a VPN to connect to their network to access internal resources. Ensure the VPN client application is up-to-date and configured in accordance with company policy. Make sure you disconnect from the VPN when not using it. This is important both for security and resource management purposes.

Teleconferencing

There are many teleconferencing applications currently in use during this pandemic, such as Zoom, Skype, Slack, Discord, Cisco WebEx, GoTo Meeting, and Microsoft Teams. We recommend you use whatever products you can use in the short term. Research and use recommended security settings for these platforms, such as setting teleconference passwords, to avoid common security problems like "Zoom-bombing."

If you are using Zoom, take the following steps to securely use it.

- Update your Zoom application/software. Zoom recently updated its software and added meeting passwords by default and disabled the ability to scan for meetings. These features are intended to prevent unauthorized access to the meeting. Zoom is constantly making security fixes so always run the latest version of Zoom.
- When creating a meeting, ensure it is **password protected**. Password settings are on the "Settings" page in the web portal under the "Meetings" tab.
- Use the "waiting room" feature. This feature prevents participants from joining the call until approved by the host. Confirm this feature is enabled on the "Settings" page in the web portal under the "Meetings" tab.
- Provide the meeting link directly to specific people. Do not publicly broadcast a meeting link.
- As the host, control participants in your meeting using the "Manage Participants" button. To prevent participants from sharing screens, click "Host Only" in the Advanced Sharing Options under the "Screen Share" button.
- Only record the meeting if you must and be careful where the file is stored. The host can control which participants may record the meeting through the "Manage Participants" button and click "Allow Record."

Sending sensitive documents

Sometimes you will need to send extra sensitive documents to clients or co-workers which you do not wish to send via regular e-mail. There are several ways to accomplish this.

1. Use a ZIP program (WinZip, WinRAR, SecureZIP, 7Zip, etc.) to put the document into a ZIP file and add a strong password. Then give the recipient the password using a different mode, like text or over the phone. Send the secure ZIP via mail.
2. Use a secure file sharing service (Sharefile, DropBox, Box, etc.)

PROTECTING YOUR INFORMATION

Now that your environment is secured and you are communicating and collaborating, it's time to choose and properly configure the applications, tools, and platforms you need to get your business working safely and securely.

Use of cloud services

Most organizations are going to make even more heavy use of cloud platforms for communication and collaboration, whether it's document sharing, teleconferencing, content management, marketing, customer engagement, finances and payroll, or any other major business function.

Regardless of which or how many cloud-based services and applications you use, it's now largely up to individuals to set these up and ensure they are secure, rather than IT support or help desk. Therefore, you need to make sure you are first and foremost using reputable services that have wide adoption and good documentation.

Make sure you research recommended security settings for usage and sharing. If you are using a collaboration platform with many users, make sure to:

1. Create a unique user account for each participant. This ensures you can restrict access to a compromised account or remove a person who no longer needs access.
2. Limit the permissions assigned to each account. Use the concept of Least Privilege to ensure people have the minimum access necessary to perform their jobs.
3. Ensure user accounts are configured to use Separation of Duties. You don't want someone to easily bypass normal oversight by being able to control too much of a given business process.

Multi-factor Authentication

We have already discussed strong passwords. However, for critical business applications and cloud platforms, it is recommended you implement Multi-Factor Authentication.

An authentication "factor" is a piece of information coming in a particular form. These factors are:

1. Something you know (username, password, PIN, etc.)
2. Something you have (computer certificate, PIV card, token, etc.)
3. Something you are (fingerprint, other biometrics, etc.)

Usernames can be guessed, and passwords can be guessed or stolen. By adding an additional factor that makes it difficult for an attacker to gain access, you vastly increase the security of the login process.

Check to see if your cloud platforms use MFA and implement it where possible.

Password Managers

Now you have set up all these cloud services for your users, you (and they) have dozens of new, very strong passwords they must manage. This can be difficult.

Consider using a secure password manager such as LastPass, Keeper, or Dashlane. With a password manager, you don't have to remember the strong, unique password for every website. The password manager takes care of it and even helps you come up with random passwords.

To access the password "vault," the user simply uses a strong Master Password to log into it, and now all their passwords are available for them to use for any app they have configured to use it.

This solution does not bypass or invalidate Multi-Factor Authentication; it enhances it. It also helps for solutions where MFA is not available, and strong passwords are the only line of defense.

WORKING SAFELY

Safe browsing

Use good Internet hygiene on the computer you use for work, even if it doubles as your personal computer. You do not want to accidentally be the cause of a security incident. There are many good tips on safe browsing, and here are a few:

1. Avoid questionable websites – adult websites, gambling websites, hacking forums, and even social networking sites, as they are often used by attackers to pass malware and exploits to unsuspecting users.
2. Don't click on links from strangers, even if they look legitimate. Clicking on a link yourself bypasses many of the protective measures your computer has. They trust you know what you are doing when you click a link, and you may have fallen for a trick.
3. Type in a trusted URL for a company's site into the address bar of your browser to bypass links in an e-mail or instant message.

4. Be careful on social media – increase your privacy settings, don't accept friend invites from strangers, and don't post pictures of your work environment or status updates about working.
5. Only download software from sites you trust. Carefully evaluate free software and file-sharing applications before downloading them.

Secure HTTP (HTTPS)

The security of your login information is also predicated on the use of secure communications protocols.

HTTP (HyperText Transfer Protocol) is the way webpages are transmitted across the Internet. However, HTTP is plaintext and subject to interception. So, login pages and other pages using HTTP-only are not very secure. Secure HTTP (HTTPS) is the preferred method for login pages and pages that are protected by logins.

Ensure websites you share information on are using HTTPS. This can be verified by looking at the URL, which will begin with https://, or by looking at the address bar of your browser, which should display a lock icon. Clicking on this icon will tell you if the connection is secure.

Security awareness

Practice good cybersecurity awareness. You are operating in an environment lacking a lot of the usual protections against malicious actors.

Phishing – this is the practice of sending e-mails that look legitimate but are not. These e-mails try to get you to open an infected attachment, click on a malicious link, or go to a fake website. Any or all of these can expose your computer to attack and malicious takeover. Make sure you are carefully validating e-mails, especially if they seem out of place or unnecessarily urgent or alarming.

Social engineering – this is the practice of attempting to get you to give information or access to your computer, your files, your bank account, or other sensitive information for malicious purposes. Be careful to verify the identity of people who approach you in-person, on the phone, or online. The Federal Trade Commission is diligently tracking Coronavirus scams making heavy use of social engineering.

Lock your screen

Unless you live alone, you should make sure you lock your screen when away from the computer. You don't want someone in your household to accidentally close programs, open other programs, type random things into important work documents, or otherwise disrupt your secure space.

Backups

Hard drive crashes and motherboard failures can and will happen. When you are working from home, your margin for error is very slim. You can't just call IT and have them give you a new computer, recover the old drive, or otherwise do whatever wizardry necessary to recover your files.

Backups of your system and critical files are essential. You can perform local backups using an external drive, or you can use a secure cloud backup system for your files or your whole computer suing solutions such as Dropbox or iDrive.

We recommend you do both. This will allow you access to your files even if there is a loss of internet connection. If there is a catastrophic hardware failure, you can use the local backup to restore to a new system while keeping the integrity of the cloud backup intact.

Dispose of sensitive data securely

You will likely print out several business-sensitive documents or have them sent to you. When disposing of these documents, don't just throw them in the trash or recycling bin. Shred them. Paperwork you no longer need can be a treasure to identity thieves if it includes personal information about customers or employees.

Questions?

If you have any questions about how to securely work from home, please contact ePlace Solutions at cyberteam@eplaceinc.com.

REFERENCES

General

SANS, "Top 5 tips to securely work from home". https://www.sans.org/sites/default/files/2020-03/02-SSA-WorkingFromHome-FactSheet.pdf

MalwareBytes Labs, "Security tips for working from home (WFH)". https://blog.malwarebytes.com/how-tos-2/2020/03/security-tips-for-working-from-home-wfh/

ComputerWorld, "12 security tips for the 'work from home' enterprise". https://www.computerworld.com/article/3532352/12-security-tips-for-the-work-from-home-enterprise.html

Comparitech, "13 cybersecurity tips for staff working remotely". https://www.comparitech.com/blog/information-security/security-remote-working/

Federal Trade Commission, "Online security tips for working from home". https://www.consumer.ftc.gov/blog/2020/03/online-security-tips-working-home

SANS Institute, "SANS Security Awareness Deployment Guide: Securely Working at Home". https://security-awareness.sans.org/sites/default/files/2020-03/01-SSA-WorkingFromHome-DeploymentGuide_1.pdf

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-46 rev. 2, "Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security". https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf

Securing Your Work Environment

Norton Labs, "Router security: How to setup Wi-Fi router securely". https://us.norton.com/internetsecurity-how-to-how-to-securely-set-up-your-home-wi-fi-router.html

Heimdahl Security, "How to Enhance your Home Wireless Network Security". https://heimdalsecurity.com/blog/home-wireless-network-security/

Apple, "Mac App Store: Automatic security updates". https://support.apple.com/en-us/HT204536

TechRecipes, "How to Turn On and Off Automatic Updates in Windows 10". https://www.tech-recipes.com/rx/69127/how-to-turn-on-and-off-automatic-updates-in-windows-10/

PCMag, "The Best Malware Removal and Protection Software for 2020". https://www.pcmag.com/picks/the-best-malware-removal-and-protection-software

Communicating Securely

PCMag, “The Best Video Conferencing Software for 2020”. https://www.pcmag.com/picks/the-best-video-conferencing-software

PCMag, “The Best Business Messaging Apps for 2020”. https://www.pcmag.com/picks/the-best-business-messaging-apps

HelpDeskGeek. "How To Encrypt Zip Files". https://helpdeskgeek.com/how-to/how-to-encrypt-zip-files/

ComputerWorld. "Top 10 file-sharing options: Dropbox, Box, Google Drive, OneDrive and more" https://www.computerworld.com/article/3262636/top-10-file-sharing-options-dropbox-box-google-drive-onedrive-and-more.html

Protecting Your Information

NIST, “Back to basics: Multi-factor authentication (MFA)”. https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication

PCMag, "The Best Password Managers for 2020". https://www.pcmag.com/picks/the-best-password-managers

Working Safely

Webroot, "Best Practices for How to Safely Browse the Internet". https://www.webroot.com/us/en/resources/tips-articles/online-activities-internet-security

Kaspersky," Top 10 Internet Safety Rules & What Not to Do Online". https://usa.kaspersky.com/resource-center/preemptive-safety/top-10-internet-safety-rules-and-what-not-to-do-online

VCPI, "10 Best Practices for Secure Web Browsing". https://www.vcpi.com/blog/best-practices-for-secure-web-browsing

U.S. Federal Trade Commission, "Seven Coronavirus scams targeting your business". https://www.ftc.gov/news-events/blogs/business-blog/2020/03/seven-coronavirus-scams-targeting-your-business

PCMag. "The Best Online Backup Services for 2020". https://www.pcmag.com/picks/the-best-online-backup-services

