PROTECT YOUR DATA

Introduction

Today we live in a world where digital life is deeply intertwined with the physical world. The lines are blurred; we now manage our finances, build relationships, conduct business, and entertain ourselves in the digital world. The convenience granted by this technology does not come without great risks.

Criminals have also become intertwined with the digital world, evolving new strategies to take advantage of our reliance on technology. It's no longer about just keeping your password safe-it's now become about protecting your entire digital life. By securing your accounts, devices, and mindset, we can create a powerful layered defense that will protect your data.

Secure Your Accounts

Your online accounts are gateways to your personal information. Whether it's your email, social media, or bank account, a breach can start a domino effect that could compromise your entire digital life. Follow these guidelines to ensure your accounts are protected.

Strong Passwords

Passwords have been the cornerstone of account security since account security was a consideration. Make sure your account is secure by following these guidelines to create a strong password:

- **Make it long**. The longer, the stronger. Try to create a password with least 14 characters.
- **Make it complex**. A combination of lowercase, uppercase, numbers, and symbols can create a difficult-to-crack password.
- **Make it memorable (for only you).** Use a "passphrase" instead of a password. A phrase or sentence that you can easily remember, but others can't identify.
- **Make it unique.** Create a password that only you can come up with… It's tempting to do "password123!" but know that millions other have tried and learned a hard lesson.
- **Make it yours.** Don't share your passwords. Passwords can spread like wildfire.

These are a lot of rules, but there is a cheat code to this… password managers! Password managers can create strong passwords, store them securely, and you only need to remember one password. Just make sure you select a reputable vendor, create a strong password for this account, and secure it with MFA.

Multi-Factor Authentication (MFA)

MFA adds an additional layer of security by requiring not just your username and password, but also another form of identification. This can be a push notification sent to an authenticator app, a code texted to your phone, a fingerprint scan or a security key you plug into your device. This prevents hackers from accessing your account, even if they get your credentials. Most service providers offer MFA, so be sure to use it when possible.

Security Alerts

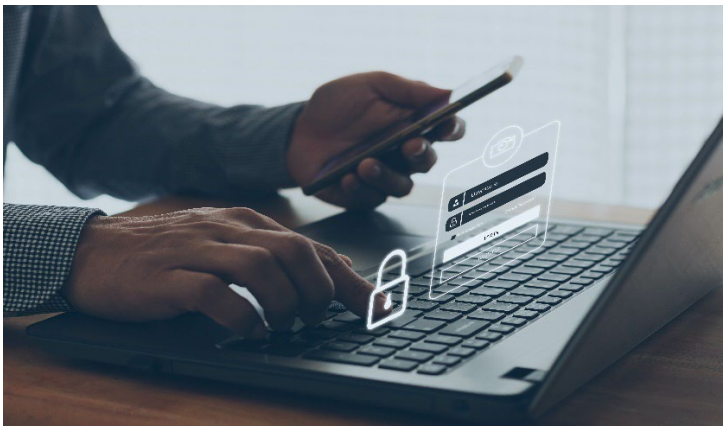
Security alerts can give you real-time notifications about unusual and/or unauthorized activity on your account. Whether there is a login attempt from a strange location, password reset attempts, or changes to your account, you'll be able to quickly act and protect your account. These settings are typically found in the security settings of your account.

Stay In the Know

In the past decade, data breaches and password leaks have struck companies such as Equifax, Facebook, Home Depot, Marriott, Target, Yahoo, and countless others. If you have online accounts, its likely hackers have leaked data from at least one of them. Luckily, some security professionals have created a website, haveibeenpwned.com, which tracks breaches and allows for users to search if their email was part of the breach. Aside from that, following the latest cybersecurity news will ensure that you're in the know about the things that could affect your digital life.

Too Long; Didn't Read, Here Are Account Protection Recommendations

- Use strong passwords with MFA to prevent unauthorized access to your accounts.
- Use a password manager with MFA to create, store, and retrieve your passwords.
- Enable settings to receive security alerts such as account sign-in failures and password changes.
- Keep up with cybersecurity news to stay up to date with breaches and vulnerabilities



Secure Your Devices

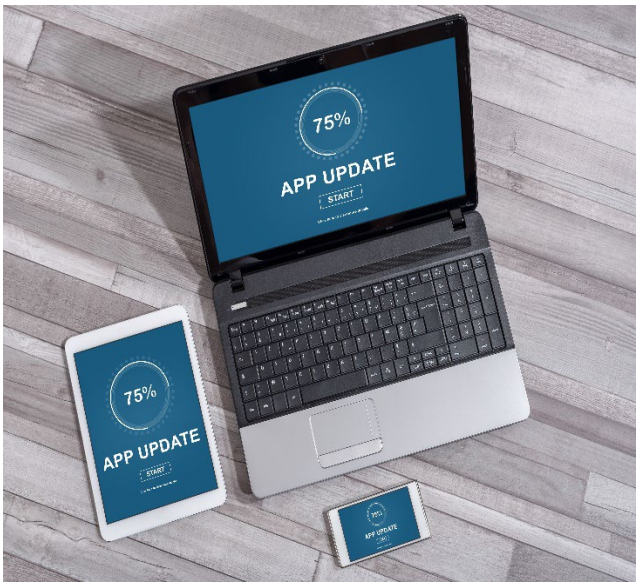
Your devices are just as important as your accounts, so securing your accounts should go hand-in-hand with securing your devices. Without your devices you wouldn't be able to access your accounts, but just the same goes for hackers. Follow these guidelines to make sure you're the only one with access.

Use an Antivirus and Firewall

Antiviruses and Firewalls are an important defense in your arsenal. They act as a first responder when a hacker or malware attempts to compromise your device.

Windows devices come preinstalled with Microsoft Defender, which has both an antivirus and firewall. Defender provides sufficient security for most people, especially if you are running a current version of Windows with the latest updates. Make sure to enable automatic updates, so you're protected from the most current threats. MacOS devices also come preinstalled with an antivirus called XProtect and a Firewall. Like Defender, XProtect and the MacOS Firewall with automatic updates, will provide sufficient security for most people. Be sure to double check that both the Antivirus and Firewalls are turned on.

If you choose to use a third-party antivirus, make sure it is a reputable vendor. Some vendors may push their "advanced capabilities," but don't fall for the trap. Look for solutions with a good track record of detection and prevention, minimal system impact, and positive community outlook. Also remember that most of the time, if its free, you're the product. That doesn't mean the solution is bad, just that if you're unsure of how they make money, it's probably off your data.



Keep Devices and Software Updated

Updates are important to maintaining a strong security posture. Outdated devices and software could contain vulnerabilities that let hackers simply walk in and take your data.

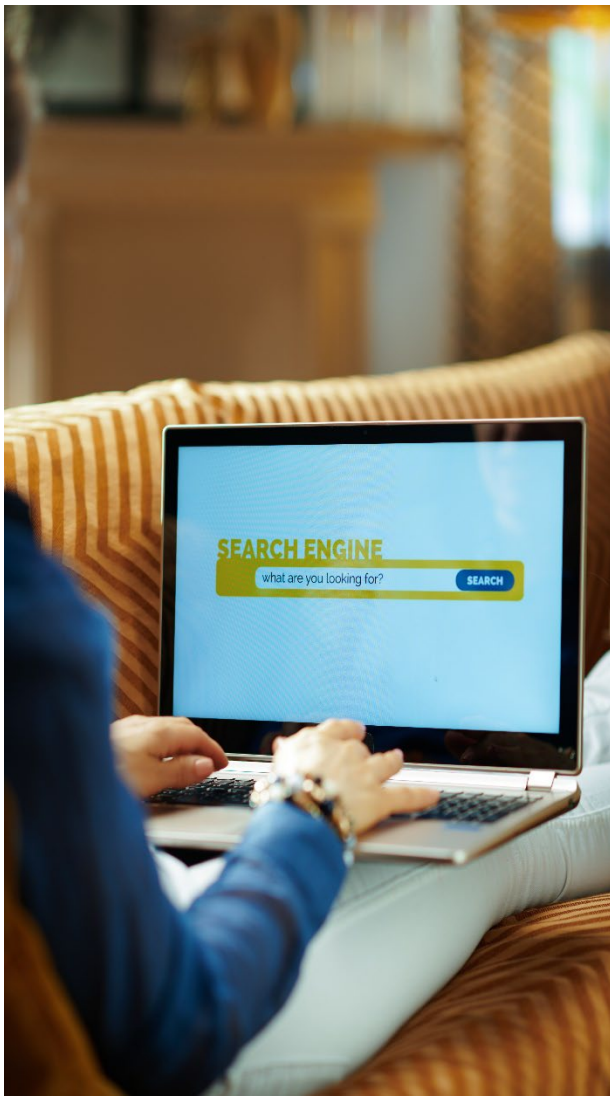
Automatic updates are a powerful feature that is typically included in your operating system and applications. It's worth your time to do a quick check to ensure this setting is enabled.

Sometimes we forget that our computers and phones aren't the only devices that need to be updated. Our routers, smart devices, cameras, even refrigerators nowadays need to be updated. If it can connect to the internet, it must be updated. And yes, smart refrigerators have been hacked before.

Secure Your Browser

Your browser is your portal to your digital life; your emails, bank information, social media can all be accessed through your browser, so it's important to make sure that it remains secure. Use the following guidelines for a secure browsing experience.

- **Select a reputable browser.** Your browser is a car that will take you to where you want to be, so don't drive a lemon. Stick to reputable browser vendors, such as Firefox. Some vendors may track your activity less than others or provide greater security features, so be sure to do your research and pick one that fits your privacy and security needs.
- **Keep it updated**. Vendors will often release updates to fix vulnerabilities, improve performance, and improve user experience. Automatic updates are typically enabled but be sure to double-check that is the case.
- **Enable HTTPS-Only mode**. HTTPS encrypts the connection between your browser and the website you visit, making sure others can't easily intercept your data. Make sure this setting is enabled in your browser.
- **Carefully select browser extensions**. Extensions can greatly enhance your browsing experience, but they can also introduce great risks. Install only the extensions you need, make sure they come from a reputable developer, and review the permissions that the extensions require to make sure it doesn't need more than it does.



Use Encryption

Encryption will make your data unreadable without the encryption key. If your device is lost or stolen, this will protect the data on your device. On Windows computers, you can use BitLocker and on MacOS, you can use FileVault. These will encrypt your device and files, ensuring that only you can access them.

Backup Your Data

Backups are a key part of a defense strategy. If you lose your device, experience a device failure, or if you get hit with ransomware, backups will get you up and running quickly. Make sure you schedule your important files to be backed up regularly and encrypted.

Too Long; Didn't Read, Here Are Device Protection Recommendations

- Use a reputable Antivirus and Firewall.
- Keep your operating system and software updated to protect against cyber vulnerabilities.
- Make sure you are using a reputable browser with secure settings.
- Use encryption to protect your important devices and files.
- Ensure you have current and encrypted backups of your important devices and files.

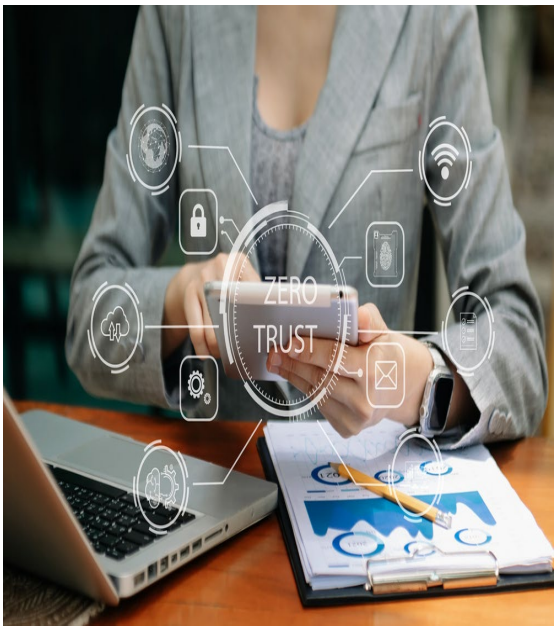
Secure Your Mentality

When you think about security, you may think about how to protect your account or how you can lock down your computer. However, before you take any action, your brain is taking into account all your knowledge of the security world. To make good, conscientious security decisions, you must build first build a framework of thinking that enables them. Follow these guidelines to help secure your mentality.

Cyber Hygiene

Taking care of your health is important; however, just as important is taking care of your digital health. Cyber hygiene is the practice and steps that you take to maintain a strong security posture and it all starts with mentality. If you're reading this article, you've already decided to take steps to better your cyber hygiene. Follow these tips to ensure your cyber hygiene is healthy:

- **Understand the "why" and "how."** Learn importance and the methods of securing your accounts and devices (with this guide and others!)
- **Practice caution and patience.** It is rare that you don't have time to act, even if someone tells you otherwise.
- **Always verify.** When receiving an email or text message, remember to validate every piece of information you can: phone number, email address, sender, message content, spelling mistakes, tone, links, etc.
- **Be suspicious.** If you are suspicious of someone who has contacted you, lean into that suspicion. Disengage and verify their identity by looking up their contact info on a verifiable source like the official company website.
- **Limit information sharing.** Limit sharing information online, whether it is for a new account, service, or posting on social media.
- **Learn to love encryption**. Use it for your devices, files, chatting, and connections.



Zero-Trust

When talking security, you may have heard of "trust, but verify." Zero-Trust is a different mindset that assumes no one should be trusted by default. "Never trust, always verify." It can be cumbersome to build this type of mentality, but you can break it up and implement this in small parts where they are applicable. Consider doing the following:

- **Assume breach.** Use encryption where applicable and limit access with segmentation and least-privilege
- **Secure it.** Implement security controls, settings, and alerts where you can.
- **Never trust.** Require re-authentication with MFA when accessing your accounts, services, and devices.
- **Inventory and classify.** Make sure you know every asset in your home or org, what they do, and the value it presents.

Privacy

You may have heard the phrase, "If you have nothing to hide, you have nothing to fear," when discussions about privacy arise. However, privacy isn't about hiding your data; it's about protecting it. From your email that you use to sign in to important accounts like banking, to your phone number that you use for personal conversations, even your DNA that you sent in for your ancestry report, they are all up for grabs. If you've given your information to the wrong people or organizations, you'll find that privacy was never their concern. Be conscious of the choices you make when it comes to sharing your information. Take your privacy back by following these guidelines to protect your privacy:

- **Use securely.** Use services that focus on security and privacy.
- **Browse securely and privately.** Use a secure browser with privacy functionality, such as DuckDuckGo or Firefox with privacy settings enabled.
- **Limit information sharing.** Avoid or limit sharing your data online, whether it is for a new account, service, or social media.
- **Exercise your rights.** The California Consumer Privacy Act (CCPA) grants you the right to know what is collected about you, opt-out of the sale and sharing of that data, limit the use of that data, and request its deletion.

Too Long; Didn't Read, Here are Mental Protection Recommendations

- Ensure that you maintain a healthy cyber hygiene by practicing patience, caution, and implementing the items in this guide.
- Incorporate concepts of Zero-Trust into your life and organization.
- Choose to use only necessary and security/privacy-oriented services.
- Limit the data that you share online.
- Exercise your right granted by the CCPA.