PRIVATE CAPITAL MANAGEMENT

Cybersecurity: Staying Safe Online

August 19, 2024

Amidst large-scale data breaches and cyberattacks, it is important to be reminded of effective ways to keep your personal information & financial assets safe from online adversaries.

In today's digital age, cyber security is crucial for protecting sensitive information as well as financial assets. As businesses and individuals increasingly rely on interconnected systems, the threat landscape evolves rapidly, making a proactive approach to safeguarding data essential. From ransomware to data breaches, staying vigilant against cyber threats has never been more important. The following information focuses on key ways to stay safe online.

- Use strong passwords alongside a password manager
- Turn on multi-factor authentication where available
- Recognize phishing
- Update software and use antivirus
- Freeze and monitor credit reports

STRONG PASSWORDS

Passwords are the keys to your digital castle, and just like your house keys, you want to do everything you can to keep them safe. Passwords can be made more secure with additional authentication methods, such as multi-factor authentication (MFA). While creating, storing, and remembering passwords can be a hassle, they are the first line of defense against cybercriminals and data breaches. Fortunately, maintaining passwords has never been easier with often free, simple-to-use password managers. With a bit of forethought today, you can stay safe online for years to come.

No matter what accounts they protect, all passwords should be created with these three guiding principles in mind:

- **Long**: Every one of your passwords should be at least 12 characters long.
- **Unique**: Each account needs to be protected with its own unique password. Never reuse passwords. This way, if one of your accounts is compromised, your other accounts stay secured.
- **Complex**: Each unique password should be a combination of uppercase letters, lowercase letters, numbers, and special characters (>, %, #, !, ?, @).

PASSWORD MANAGER SOFTWARE

It is not unheard of for many of us to manage 100 or more passwords. Due to the sheer number of passwords we need, it's not uncommon to fall into the habit of using the same password for multiple accounts, or keeping passwords in a notebook. If one password gets stolen because of a breach, it can be used to gain access to other accounts and by extension your sensitive information. By using a password manager to create and store long, unique, and complex passwords you can significantly enhance your online security.

Password managers are software tools that can take the form of apps, browser plugins, or be included in your browser or operating system. A password manager is used to generate secure passwords that are long, unique, and complex. Once a password is generated, password managers store the passwords along with usernames, official web addresses, and notes. One strong master password will need to be remembered to unlock the vault containing the other passwords. This master password should be a long passphrase (series of words that include uppercase, lowercase, numbers, and special characters) to make it easier to remember. Some password managers can autofill your username and password when you visit a site, while others require you to copy and paste the information from the software into the site. It is important to create the habit of using a password manager for all log ins. You can fill in all your passwords at once or add a few key accounts (like email, banking, and social media) over time. Password managers will often prompt you to create and store a password when you log into a site, making it easier to get started.

How to choose a Password Manager

The right software may be different for everyone, it's a personal choice. Considering what devices are to be used, sophistication with technology, cost, and user interface can help narrow down the options. It may take a couple of tries to find the software that works for you, and that's ok. There is no shortage of review articles to be found, New York Times, Consumer Reports, and PC Magazine all have their favorite picks. Most include a recommendation for both a free and a paid option. Below are a few that rise to the top of multiple resources and could be a good start.

- 1Password
- Bitwarden
- Dashlane
- Nordpass

Keep in mind PCM doesn't endorse one software over another. Using a password manager is what is important.

MULTI-FACTOR AUTHENTICATION

Multi-factor authentication (MFA) is a security measure that requires you to prove your identity in an additional way after using a password/username to log into an account. Multi-factor authentication adds an extra layer of security to your login process and is sometimes referred to as two-factor authentication or two-step verification. By requiring a second method of verification, breaches can be avoided if a password has been compromised.

Multi-factor authentication can take several different forms. Here are a few examples:

- Security Question: Answer a pre-determined security question. Be careful about using answers that can be found via a quick social media search.
- One-Time Code: A code is sent to your email or texted to your device and entered within a specific time.
- Biometric Identifiers: Facial recognition or fingerprint scans.
- Authenticator App: Approve access using a standalone application.
- Security Key Hardware: A separate piece of physical hardware, like a key fob, which verifies your identity.

We recommend implementing MFA for all accounts that allow it, especially any account associated with work, school, email, banking, and social media.

AVOIDING PHISHING

Phishing is when criminals use fake emails, social media posts, and text messages with the goal of luring you to click on a bad link or download a malicious attachment. If you click on a phishing link or file, a program can be installed on your device to allow a bad actor access to your information. Phishing emails have become very realistic and convincing, they rely on our busy lifestyles to succeed. The number one method to safeguard yourself is to slow down. Take a moment to review the email details before clicking any links or downloading attachments. With your mouse, hover over links and email addresses to see where the link will send you. All links should correspond to a known location or contact. When in doubt go directly to the website or pick up the phone and call. Don't use a phone number or web address contained in the suspect email. Phishing attempts can be sneaky. With knowledge and vigilance, you can protect yourself from these scams.

Below are some quick tips to identify a fake email and protect against phishing:

- Does it contain an offer that's too good to be true?
- Does it include language that's urgent, alarming, or threatening?
- Is it poorly crafted writing riddled with misspellings and bad grammar?
- Is the greeting ambiguous or very generic?
- Does it include requests to send personal information?
- Does it stress an urgency to click on an unfamiliar hyperlink or attachment?
- Is it a strange or abrupt business request?
- Does the sender's email address match the company it's coming from? Look for misspellings like (pavpal.com or anazon.com), or (example: JaneD0e@phishing.com vs. JaneDoe@phishing.com).

Use the tips below if you spot a phishing email or message.

- If you're at the office and the email came to your work email address, report it to your IT manager or security officer as quickly as possible.
- If the email came to your personal email address, deleting the email is the safest option. Do not reply to the email and do not click on any links. Even the unsubscribe link could be a malicious link.

KEEP SOFTWARE AND APPS UPDATED

An easy way to boost your cybersecurity is to keep your software and apps updated. Software and hardware developers focus on keeping their users and products secure. They constantly look for vulnerabilities that hackers could exploit. If found, updates are released to fix these issues and improve security. By staying up to date, you will receive the best security available, as well as the latest features and upgrades. Remember that updates are part of our digital lifecycle. By keeping your systems up to date, you'll have peace of mind, the latest security, and new features.

Four Easy-to-Remember Tips for Updates:

1. Use Automatic Updates
    - Automate updates to download and install when available. Remember restarts may be required.
    - Schedule updates to happen during times when you aren't using your device.
    - Check your settings quarterly to ensure updates are being installed as expected.
2. Install only official updates
    - Before downloading updates, be sure they are from the software developer.
    - Only download software from verified sources and apps from your device's official app store.
    - The device, software, or app developer itself should be sending you updates, not anyone else.
    - Avoid pirated, hacked, or unlicensed software, they can spread malware, viruses, or other threats.
3. Don't Fall for Fake Updates
    - Pop-up windows that urgently demand you download a software update are always fake. These are common on shady websites or come from malware already on your machine. Don't click and close your browser.
    - Many web browsers will warn you if you are attempting to visit an unsecure web address or one that could contain malware. Heed these warnings.
4. Make Checking for Updates a Habit
    - Check for updates at least monthly If you don't have automatic software updates turned on.
    - Install updates as soon as they are available.

ANTIVIRUS SOFTWARE

Using reliable antivirus software is crucial for maintaining strong cybersecurity. Antivirus software helps detect, prevent, and remove malware, viruses, and other threats from your devices. Below are some tips for using antivirus software effectively:

- Keep Your Antivirus Updated: Regular updates are needed to be effective against the latest threats.
- Schedule Scans: Set your antivirus to perform regular scans of your system to catch threats early.
- Real-Time Protection: Enable real-time protection features that continuously monitor your device for suspicious activity.
- Choose Reputable Software: Opt for antivirus software from well-known and trusted companies to ensure you get the best protection.

CREDIT REPORTS

We recommend all clients freeze their credit and review their credit report at least annually. Freezing your credit is a security measure that restricts access to your credit report preventing new accounts from being opened in your name. When your credit is frozen, lenders and creditors cannot view your credit report and therefor cannot extend new credit. Applying for new credit will require lifting the freeze temporarily, and can be done immediately via a web browser. A freeze does not impact your credit score and is a free service provided by the major credit bureaus.

An update to the Fair Credit Reporting Act in 2003 requires credit reports from each of the three major credit bureaus to be provided to consumers at least annually. Weekly reports are currently available due to recent data breaches. The Annual Credit Report website provides further information regarding identity theft and updates to the frequency of reports. You should review your report for accuracy and report any anomalies to the reporting service.

These services are required by law to be provided free of charge, it is not necessary to purchase additional services offered by the credit reporting companies. Official links for credit freezes and credit reports are below.

- Equifax: https://www.equifax.com/personal/credit-report-services/credit-freeze
- Transunion: https://www.transunion.com/credit-freeze
- Experian: https://www.experian.com/freeze/center.html
- Credit Report: https://www.annualcreditreport.com

Securing your digital assets is more important than ever in today's evolving threat landscape. By adopting strong cyber security practices, you can better protect your personal and financial information. While the digital world presents challenges, taking proactive steps will help ensure your peace of mind as you navigate it with greater confidence.

Sincerely,
The Private Capital Management Team

These materials were prepared for informational purposes only based on sources deemed reliable, but which have not been independently verified. Information contained herein is subject to change without notice. These materials are not a recommendation or offer to buy or sell securities. PCM does not provide tax or legal advice. You should consult an appropriately credentialed tax or legal professional to determine how this information may be applicable to you. These materials do not take into account your particular financial circumstances, and you should consult with your PCM advisor, or other appropriately credentialed individual, prior to making any investment or financial decision. By clicking on the link(s) contained herein, you will be directed to a third-party website. Access to any third-party website is at your own risk, and you acknowledge and understand that linked websites may contain terms and privacy notices which are substantially different from PCM's. This link is provided as a convenience only; PCM does not own the content of this website and is not responsible for its contents.