CYBERSECURITY:

10 Tips To Protect Yourself and Your Personal Data

As major companies continue to experience system compromises that result in the theft of personal data, it is more important than ever to take steps to keep your personal financial information secure. The following tips provide a starting point to help ensure your private information remains private.

#1: Keep Electronics Secure

Don't say, "It won't happen to me," because the odds are that it will. We are all at risk, and the stakes for your personal and financial well-being are high.

- Keep your computer, phone, tablet or other electronics secure by having them password-protected.

#2: Keep Software Up-to-Date

Installing software updates for your operating system and programs is critical. Always install the latest security updates for your devices:

- Turn on "automatic updates" for your operating system.
- Use web browsers such as Chrome or Firefox that receive frequent, automatic security updates.
- Make sure to keep browser plug-ins (Flash, Java, etc.) up-to-date.
- Make sure you have an anti-virus installed at all times, regardless of the system you are running.

#3: Beware Of Suspicious Emails And Phone Calls

Phishing scams are a constant threat. Using various social engineering ploys like pretending to be a company or person you know or do business with, cyber criminals will attempt to trick you into divulging personal information such as your login ID and password, banking or credit card information.

- Phishing scams can be carried out by phone, text, or through social networking sites but are most common by email.
- Be suspicious of any official-looking email message or phone call that asks for personal or financial information.

Mariner WEALTH ADVISORS

#4: Practice Good Password Management

We all have many passwords to manage and it's easy to take short-cuts, like reusing the same password. Consider using a password management program. It can help you maintain strong, unique passwords for all of your accounts. These programs generate strong passwords for you, enter credentials automatically and remind you to update your passwords periodically.

There are several online password management services that offer free versions, and KeePass is a free application for Mac and Windows.

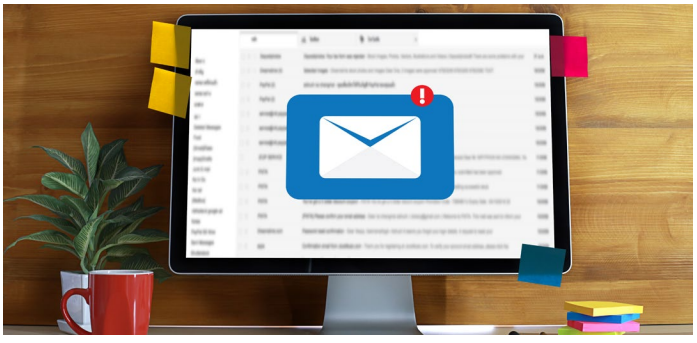
Here are some general password tips to keep in mind:

- Use long passwords - 20 characters or more is recommended.
- Use a strong mix of characters and never use the same password for multiple sites.
- Don't share your passwords and don't write them down (especially not on a post-it note attached to your monitor).
- Update your passwords periodically, at least once every six months (every 90 days is even better).

#5: Be Careful What You Click

Avoid visiting unknown websites or downloading software from untrusted sources. These sites often host malware that will automatically, and often silently, compromise your computer. If an attachment or link in an email is unexpected or suspicious, don't click on it.

This is the number one method of delivering a malicious virus known as Ransomware to your computer.



#6: Never Leave Devices Unattended

The physical security of your devices is just as important as their technical security.

- If you need to leave your laptop, phone, or tablet for any length of time, lock it up so no one else can use it.
- If you keep sensitive information on a flash drive or external hard drive, make sure to keep these locked as well.
- For desktop computers, shut down the system when not in use, or lock your screen.

#7: Use Two-factor Authentication (2FA)

Utilizing this feature for your bank, primary email and social media is a relatively easy way to prevent a compromise.

- It ensures that if your password is stolen, these sites will still require input of a unique code that will prevent your identity from being compromised.
- Most of the time, these pass codes can be sent via text message or from using an app on your mobile device, which will force your approval of all logins.

#8: Use Mobile Devices Safely

Considering how much we rely on our mobile devices and how susceptible they are to attack, you'll want to make sure you are protected:

- Lock your device with a PIN or password and never leave it unprotected in public.
- Only install apps from trusted sources.
- Keep the operating system on your device updated.
- Don't click on links or attachments from unsolicited emails or texts.
- Most handheld devices are capable of employing data encryption. Consult your device's documentation for available options.
- Use Apple's Find my iPhone or the Android Device Manager tools to help prevent loss or theft.
- Back up your data.

#9: Freeze Your Credit

Usually your credit is only checked when you are making large purchases that could have an impact on your financial life. Freezing your credit at the three major bureaus is simple to do and can be done online via their websites. To have your credit checked after it is frozen requires a manual lift of the freeze. Freezing your credit will prohibit any hacker from opening accounts in your name.

#10: Back Up Your Data

Although it was mentioned above, it is worth mentioning again. Always back up your data on a regular basis. If you are a victim of a security incident, the only guaranteed way to repair your computer is to erase and re-install the system. There are many software vendors that will protect your data for as low as $50/year. This also covers you in an event where your system fails and all of your data is unable to be recovered. We recommend both CrashPlan and Backblaze, but there are many others.

Additional Tips To Help Keep You Safe And Secure Online

Use a firewall. Both Mac and Windows have basic desktop firewalls as part of their operating system. These can help protect your computer from external attacks.

- Use public wireless hot-spots wisely. Remember, these are not secure lines and therefore you should not review private information while using them.
- Be conscientious of what you plug in to your computer (flash drives and even smart phones can contain malware).
- Be careful of what you share on social networking sites. For example, those fun surveys could be alerting people to where you have lived, your favorite teacher, pet or best friend. These are common answers to security questions and you've just armed a hacker with the information!
- Monitor your accounts for suspicious activity.
- Bank or shop online only on trusted devices and networks and log out of these sites after you've completed your transactions.