WASHINGTON
WEALTH GROUP
of Steward Partners

PROTECTING YOUR PRIVACY

HELPFUL TIPS FOR EFFECTIVE CYBERSECURITY

Cultivating peace of mind is an important part of what we do as advisors. The strategies we employ are designed to help secure and optimize your wealth, so you can focus on enjoying your life. But with more and more threats to the nation's cybersecurity, that peace of mind doesn't always come easy. It's more important than ever to understand the risks to your personal information, and the steps you can take to protect it. We always adhere to the highest standards of security and confidentiality here at Washington Wealth Group, employing the latest technology that seeks to ensure your data is protected. Here are some additional steps you can take to keep your personal information safe.

USE PASSWORDS WISELY

Make Them Strong and Unique

You've likely heard this before, but using strong passwords (i.e., long ones with multiple symbols, numbers, and letters) is critical. It can feel tedious to create new, complex passwords for every account you establish, but failing to do so puts your personal information—and consequently, your finances—at risk. To make it simple, consider using a reputable passwords manager that generates and stores strong passwords for you.

Use Multi-Factor Authentication

Multi-factor authentication prompts a website to ask you for an additional form of identification before allowing you to login with just a username and password. Typically, the site will send a one-time code to your phone via text message or even call you to verify that you are the one trying to login. Again, while this method can be slightly tedious in the short-term, it's well worth the added security.

SECURE YOUR PHYSICAL DATA & DEVICES

Shred Sensitive Documents

Not all data breaches happen online; some attacks are as uncomplicated as rifling through a trash can. Be sure to shred any documents that include your personal information, such as bank statements, utility bills, investment account summaries, contracts, and anything else that may contain your financial details, Social Security number, or other personal data.

Secure Electronic Devices

Be sure to regularly update apps and operating systems on your phone and computer, as these sometimes address security issues. Use antivirus software and consider a firewall for your home, which acts like a virtual security guard for your network, managing the flow of information to and from the internet. It examines data packets based on established rules, allowing safe traffic while blocking suspicious or unauthorized access.

Guard Against Ransomware Attacks

A ransomware attack is a type of cybercrime where a hacker infects a device or network with corrupt software and locks the user's access to their data or systems. The hacker then demands payment (hence, "ransom"ware) to restore access. Users become vulnerable to these types of attacks by clicking on unsecure links or downloading files from suspicious sources. This is why it's important to be on guard when receiving emails from unknown senders, and why you should verify the source before clicking or downloading anything. Another way to guard against ransomware attacks is to keep secure copies of your data. Conduct regular back-ups, saving your files to an external drive or trusted cloud platform.

PRACTICE INTERNET SAFETY

Remember—Not Everyone Online is Your Friend

Check your credit reports for free at AnnualCreditReport.com and review them regularly for suspicious activity. If you find evidence of unauthorized accounts or inquiries, file disputes with the relevant credit bureaus and creditors. Be sure to keep record of all correspondence, as this documentation will support your case in clearing fraudulent activity from your credit report.

Beware of Public Wi-Fi

Public wi-fi networks are rarely secure, creating prime opportunities for hacking. Avoid accessing sensitive sites (e.g., your bank app or investment account platform, healthcare portals, anywhere you plan to enter payment information, and even your email, as it often contains private information) while using public wi-fi. Or avoid using it altogether. If you must use a public wi-fi network, then it's wise to also use a VPN, which hides your IP address and routes your online activity through a private server, making it difficult for hackers, advertisers, and even the internet provider to track your activity or steal your data.

Use Safe Websites

Before sharing sensitive information on any website (e.g., payment details), be sure the site is secure. If the URL begins with "https," that indicates the website encrypts the data you send and receive. This encryption protects sensitive details, like passwords or payment information, from being intercepted by cybercriminals.

STAY ALERT

Monitor Your Accounts

Even when adhering to these safety measures, it's important to monitor your accounts for suspicious activity. Review your bank and credit card statements regularly to ensure no unauthorized transactions have occurred, and if a breach does occur, act quickly.

We at Washington Wealth Group care deeply about your privacy and peace of mind. We're dedicated to prudent communication practices and secure account management procedures to ensure your financial safety.

WASHINGTON WEALTH GROUP
of Steward Partners

1776 I Street NW Suite 700, Washington, DC 20006
washingtonwealthgroup.com