Portfolio Strategy Group | WEALTH ADVISORS

50 Main Street, Suite 1280, White Plains, NY 10606 | PSGwealth.com
914.288.4900 tel | 800.535.5110 toll-free | 914.328.6670 fax

Staying Safe Online:

Simple Steps Every Investor Should Know to Help Protect Your Personal and Financial Information

At The Portfolio Strategy Group, protecting your wealth is about more than just managing your portfolio. It's also about helping you safeguard what matters most: your identity, your accounts, and your peace of mind—not to mention your time.

Cybercrime continues to rise and, unfortunately, wealthy individuals are frequent targets. That's why we recently hosted a cybersecurity event for our clients featuring two consultants from Charles Schwab who educate financial firms across the country. The stories and insights they shared are worth repeating—not because they were scary (though some were), but because they were *practical*.

Here's what the team at Charles Schwab recommended to help clients like you stay safe online—and some practical steps you can take today to protect yourself:

---

1. The Most Powerful Tool You Have? Pause Before You Click

Cybercriminals rely on speed and emotion. They want you to click a link, open an attachment, or respond to a message without thinking. But one moment of hesitation can stop a mistake before it happens.

What to do:
If something doesn't feel right—**pause and verify**. Approach each message with a healthy dose of skepticism. Whether it's a strange message from your bank or a request for information, trust your instincts and double-check. Verify by calling a number you recognize and trust, *not* one provided in the message.

2. Email Is a Common Entry Point for Fraud

Email is widely used and relatively easy to exploit. Today's phishing emails, where criminals impersonate a trusted person, brand or organization to trick you, look shockingly real. They use stolen logos, familiar language, and sometimes even mimic your contacts in order to impersonate the victim to target others, harvest data like passwords and financial data, and spread the attack.

Smart email habits:

- Hover your cursor over the sender's name or email address to view their full email address in a small popup or tooltip. Verify the sender's email address carefully.

- Don’t open unexpected attachments or click on suspicious links.
- Don’t store personal or financial information in your email folders.
- Never click “unsubscribe” in suspicious emails. Use your email provider’s tools to unsubscribe or report it as junk, spam, or phishing. This helps block similar messages later.
- Reconsider or reset your email password per the “Strong and Unique Password” section below.

Think of email like a postcard. If you wouldn’t write something sensitive where others could read it, don’t send it in an email.

3. Strong and Unique Passwords Are Essential

Reusing simple passwords is one of the easiest ways for attackers to get in. If a data breach exposes one of your passwords, criminals can try it on dozens of sites in seconds.

What you can do:

- Never reuse passwords.
- Use long passwords or memorable passphrases.
- Use a **password manager** to store strong, unique passwords for each account.
- Turn on **multi-factor authentication** (MFA) wherever it’s offered.

If you've ever received an alert that your information is on the dark web, updating your passwords and turning on MFA are two of the most effective ways to respond.

4. Avoid Public Wi-Fi for Sensitive Tasks

Whether you're traveling or working from a coffee shop, using unsecured Wi-Fi can leave your information vulnerable. What’s public Wi-Fi? Any Wi-Fi outside of your home.

Instead:

- Use your mobile phone’s hotspot feature, which lets you create a secure Wi-Fi connection using your cellular data, when possible.
- If you must use public Wi-Fi, connect through a **trusted VPN** (virtual private network) to encrypt your activity.
- Make sure your devices and software are always up to date with the latest security patches.

5. You May Be a Target Without Realizing It

Cybercriminals often target individuals based on wealth or perceived access to sensitive information. You may not think of yourself as a target, but they do.

Simple steps to protect your identity:

- **Freeze your credit** at all three major credit bureaus (Equifax, Experian, and TransUnion) **directly** with each bureau—it's **free** and easy to do. Don't lose these passwords! Keep them safe and accessible for times when you need to unfreeze your credit.
- Use a **secure portal** (not email) to share financial documents.
- Consider a **dark web monitoring service** to keep an eye on exposed data.

6. Cybersecurity Is About Habits, Not Hardware

The majority of successful cyberattacks happen not because systems fail—but because people do something the attacker is hoping for: click a bad link, use a weak password, or trust a fake message.

Good habits go a long way:

- Be cautious, especially with unexpected messages.
- Use strong passwords and multifactor authentication.
- Keep your devices clean, updated, and secure. Use trusted antivirus and anti-malware software, remove programs and extensions you don't use, scan regularly for threats and manage settings and permissions.
- **Back up** your important data to protect you in case of malware or device failure.

7. Ask Before You Act

One final rule: if something feels unusual, don't take the chance. Instead, take a moment to pause, verify, and **ask someone you trust**—your advisor, your firm, or your family.

The Portfolio Strategy Group
The Family Behind Your Family