Online Security Checklist

We consider your account security to be a partnership between you and Schwab. While online security can seem overwhelming, we want you to know we're here to help.

Following these preventative steps can go a long way toward keeping you and your personal information more secure, helping protect you from identify theft, and maintaining more secure accounts.

Partner with Schwab to protect your account.

- ☐ **Schwab Security Guarantee:** Review Schwab's Security Guarantee, which covers 100% of any losses in any of your Schwab accounts due to unauthorized activity.
- ☐ **Two-step verification:** Add an additional layer of security, which requires you to enter a unique security code each time you access your Schwab accounts.
- ☐ **Voice ID:** Confirm your identity using Schwab's voice ID service when you call Schwab for support.
- ☐ **Security alerts:** Go to the Schwab Security Center and sign up to receive notifications related to your account activity.

Follow general best practices.

- ☐ **Be suspicious** of unexpected or unsolicited phone calls, emails, and texts asking you to send money or disclose personal information. If you receive a suspicious call, do not accept it, hang up, and call back using a known contact number.
- ☐ **Be cautious when sharing sensitive information** and conducting personal or confidential business via email, since it can be compromised and used to facilitate identity theft.
- ☐ **Do not disclose personal or sensitive information on social media sites,** such as your birthdate, contact information, and mother's maiden name.
- ☐ **Be cautious when receiving money movement instructions via email.** Call the sender at their known number (not a number provided in the email) to validate all instruction details verbally before following instructions or providing your approval.
- ☐ **Protect yourself from phishing attempts and malicious links** (see glossary for additional information).
- ☐ **Check your email and account statements** regularly for suspicious activity.
- ☐ **Do not verbally disclose or enter confidential information** on a laptop or mobile device in public areas where someone could potentially see, hear, or access your information.
- ☐ **Verify payment requests you receive by phone or email.** Requests for you to make payments using prepaid debit cards, gift cards, or digital currency are frequently associated with fraud or scams.

Keep your technology up to date.

- ☐ **Keep your web browser and operating system up to date,** and be sure you're using appropriate security settings. Old software, operating systems, and browsers can be susceptible to attack.
- ☐ **Install anti-virus and anti-spyware software** on all computers and mobile devices.
- ☐ **Enable the security settings** on your applications and web browser.
- ☐ **Do not use free or found USB thumb drives—** they could be infected with viruses or malware.
- ☐ **Turn off Bluetooth** when it's not needed, to protect against individuals gaining access to your devices using Bluetooth connections.
- ☐ **Safely and securely dispose of old hardware.**

Be cautious with public networks.

- ☐ **Avoid using public computers.** If you must use one, go to the browser settings and clear the browser history (cache) and cookies when you're finished.
- ☐ **Only use wireless networks you trust** or that are protected with a secure password.
- ☐ **Use your personal Wi-Fi hotspot** instead of public Wi-Fi.
- ☐ **Do not accept software updates** if you are connected to public Wi-Fi.

Be strategic with your login credentials and passwords.

- ☐ **Do not use personal information** such as your Social Security number or birthday as part of your login ID.
- ☐ **Create a unique password** for each financial institution you do business with and change it every six months. Consider using a password manager to create, manage, and store passwords that are unique and secure.
- ☐ **Do not share your passwords.**
- ☐ **Use two-step verification whenever possible.**

Be sure you're on a secure website.

- ☐ **Check the URL to see if it's a secure connection.** Secure sites begin with https rather than http, and are generally considered safer.
- ☐ **Check the address bar for site validity** indicators whenever you log in to a Schwab website. Some browsers use green text or security symbols to indicate a secure and verified site.
- ☐ **Download apps only from the Google Play™ Store or the Apple App Store®.**
- ☐ **Do not visit websites you don't know—**for example, websites advertised on pop-up ads and banners.
- ☐ **Log out completely** to terminate access when you've completed a secure session, such as with online banking or a credit card payment.

Beware of phishing.

- ■ **Do not click on links or attachments** in emails and text messages if you question the validity of the sender. Instead, type the real web address, for example https://www.schwab.com, in your browser.
- ■ **Hover over questionable links** to reveal the site's full URL and see where the link really goes. Do not click on links that don't match the sender or don't match what you expect to see.
- ■ **Be suspicious** of emails that have grayed-out Cc: and To: lines—they may have been sent to a mass distribution list.
- ■ **Check the sender's domain name in the email address** (john.doe@schwab.com) to see if it matches what you would expect to see.
- ■ **Activate the spam filters** in your email settings tab. This will help prevent unsolicited emails from coming to your inbox.
- ■ **If you suspect an email that appears to be from Schwab** is a phishing email, forward it to phishing@schwab.com.
- ■ **If you have questions about an email from Schwab** or personal information you entered about your Schwab account after clicking an email link, call us immediately at **800-435-4000**.

Glossary

Two-step verification (aka multi-factor authentication)

A method of confirming your identity using a second step to verify who you are. For example, the first step might be to enter your username and password, and the second step might be to enter a randomly generated number sent to you via email, text, phone call, or token.

Phishing

The fraudulent practice of sending emails or text messages appearing to be from reputable companies or trusted individuals in an attempt to get individuals to reveal personal information such as passwords and credit card numbers. Phishing attempts are usually urgent-sounding, legitimate-looking emails or texts designed to trick you into disclosing personal information or installing a virus on your device. These scams can be sent as attachments or links that, when opened or clicked, may trigger malicious activity or take you to fake sites that resemble the real business websites.

Password manager

An encrypted online or cloud-based program that generates, retrieves, and keeps track of random passwords across countless accounts and also protects information such as passwords, PINs, credit card numbers and their three-digit CVV codes, and answers to security questions.

Domain name

As it relates to an email address, this is the information that comes after the @ symbol—for example, schwab.com in jane.doe@schwab.com.

Spam filter

A program that detects unsolicited and unwanted emails and prevents them from reaching your email inbox. Usually these types of emails are instead sent to a spam folder.

Malware

Software that is intended to damage or disable computers and computer systems.

Learn more

Visit these sites for more information and best practices:

StaySafeOnline.org

Review the STOP. THINK. CONNECT.™ cybersecurity educational campaign.

OnGuardOnline.gov

Focused on online security for kids. It includes a blog on current cyber trends.

FDIC Consumer Assistance & Information

FBI Scams and Safety

charles SCHWAB

Own your tomorrow.