Cybersecurity Best Practices

Nicholas A. Perrine, CPA, CFP®
Director of Wealth Strategies

Graves Light Lenhart
Build. Protect. Thrive.

Schwab Security Guarantee

Schwab will cover 100% of losses in any of your Schwab accounts due to unauthorized activity.

To ensure your protection under this guarantee, it is your responsibility to:

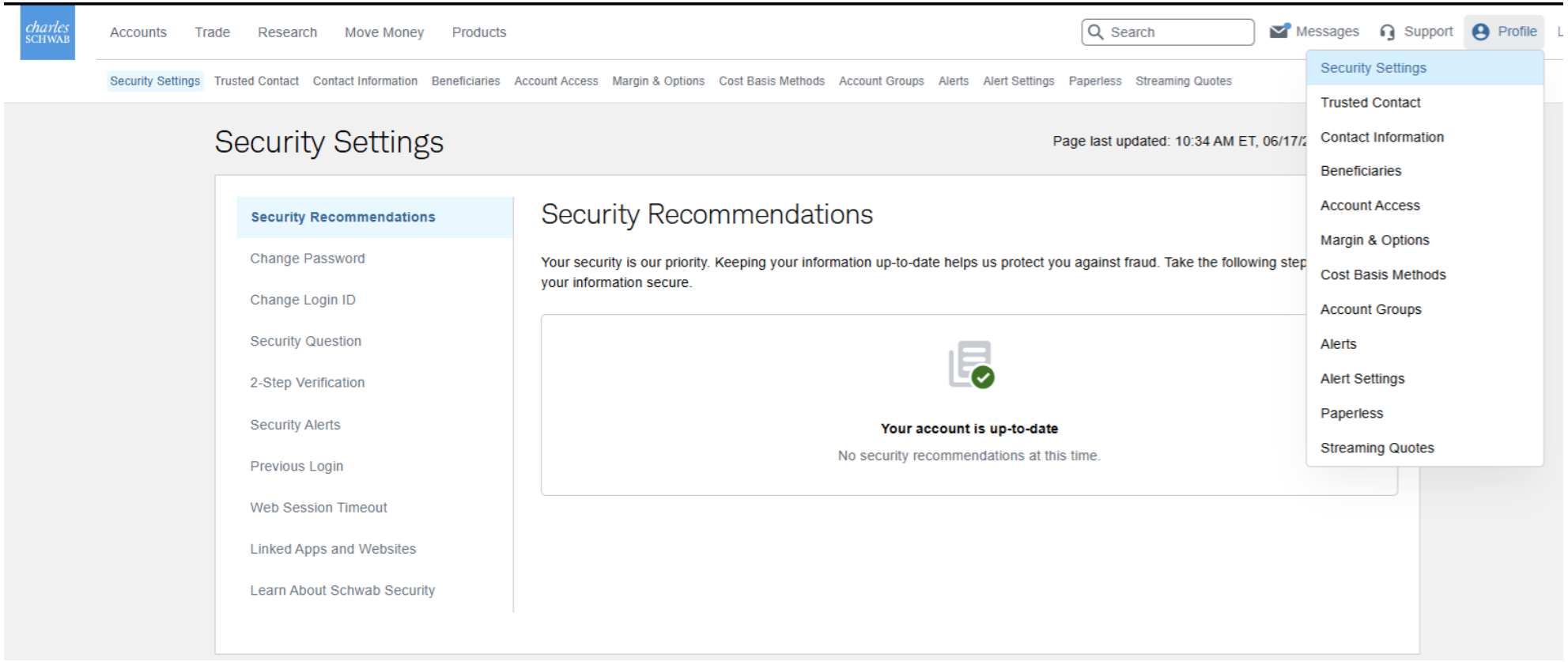
- Safeguard your account access information. Please do not share your account access information, including but not limited to your login ID, password, PIN and transaction codes, with anyone. If you share this information with anyone, Schwab will consider their activities to have been authorized by you.
- Report any unauthorized transactions to Schwab as quickly as possible. If you suspect you are a victim of fraud, please contact Schwab immediately at 888-3-SCHWAB.

Schwab Security Guarantee

Exclusions:

- If you share your Schwab account access information (such as your login ID and password) with anyone, Schwab considers any resulting activity as authorized by you, and the guarantee does not apply.
- If you authorize account access through a third-party app or service that is not officially partnered with Schwab, any losses resulting from that access are not covered by the guarantee.
- If you allow another person (other than a Schwab employee or Schwab company) remote access to your device or Schwab account, any activity they perform is not covered under the guarantee.

Schwab Security Settings



Graves Light Lenhart
Build. Protect. Thrive.

General Best Practices

- Review account statements regularly for suspicious activity.
- Be suspicious of unexpected or unsolicited phone calls, emails, and texts.
- Be cautious when sending or receiving sensitive information via email.
- Do not disclose personal information on social media sites.
- Protect yourself from phishing attempts and malicious links.
- Regularly install available software updates on your computer and cell phone.

General Best Practices

Be cautious with public networks.

- Avoid using public computers and open Wi-Fi networks.
- Only use Wi-Fi networks that you trust and are protected with a secure password.
- Use a Virtual Private Network (VPN) if you must connect to a public Wi-Fi network.
- Use your personal Wi-Fi hotspot on your cell phone instead of a public Wi-Fi network.
- Do not accept software updates if you are connected to a public Wi-Fi network.

Be strategic with your login credentials and passwords.

- Do not use personal information as part of your login ID.
- Create a unique password for all accounts and consider using a password manager.
- Use two-step verification whenever possible to make your sign in more secure.

Types of Scams

- Sweepstakes/Lottery
- Government Impersonator
- Tech or Fraud Support

QR Codes

Best Practices for Safety

- Only scan QR codes from trusted sources.
- Preview the destination website before opening.
- Avoid entering sensitive information after scanning a QR code unless you are certain of the destination's legitimacy.
- Use your device's built-in camera or trusted QR code reader apps, not third-party apps with unknown reputations.
- Be cautious of QR codes received in unsolicited emails or posted in public areas.

Identity Theft Protection Software

Key Features

- Continuous monitoring of credit reports and personal data.
- Dark web and data breach surveillance.
- Alerts for high-risk transactions and changes to accounts or records.
- Identity restoration support, including expert guidance and legal help.
- Identity theft insurance to cover recovery expenses.
- Additional tools: password managers, antivirus, spam blockers, and safe browsing tools.

Considerations

- Costs vary by provider and plan; premium features come at a higher price.
- No service can guarantee complete prevention—vigilance is still required.

How to Handle Fraud or Identity Theft

Reporting

- Contact your advisor at GLL, we are here to help you understand what steps need to be taken.
- Immediately report the fraud or identity theft to your financial institutions and creditors.
- Place a fraud alert by contacting one of the three credit bureaus (Equifax, Experian or TransUnion).
- Report the crime to your local police.

How to Handle Fraud or Identity Theft

Securing your Systems

- Check your device for viruses, malware and spyware by performing a full scan.
- Change account passwords after you've ensured your device is not infected.
- Place a freeze with all three credit bureaus (Equifax, Experian and TransUnion).
- Request an Identity Protection PIN from the IRS and your state tax department.

How to Handle Fraud or Identity Theft

Additional Steps

- Monitor account statements to look for additional unauthorized activity.
- Monitor your “my Social Security” account for any changes: https://www.ssa.gov/myaccount/.
- Call the Social Security Administration’s fraud hotline at 800-269-0271 if you suspect your Social Security number has been compromised.
- Order a free credit report at: www.annualcreditreport.com.
- File a complaint with the Federal Trade Commission (FTC) at www.ftc.gov or by calling 877-ID-THEFT.

How to Place a Fraud Alert or Credit Freeze

Contact Information for the Credit Bureaus

Experian	TransUnion	Equifax
888-397-3742	800-916-8800	800-685-1111
www.experian.com	www.transunion.com	www.equifax.com
Experian P.O. Box 9554 Allen, TX 75013	TransUnion LLC P.O. Box 2000 Chester, PA 19016	Equifax Consumer Fraud Division P.O. Box 740256 Atlanta, GA 30374

(540) 433-3076
100 South Mason Street, Suite C | Harrisonburg, VA 22801
www.GLLwealth.com