KEATING
WEALTH MANAGEMENT

Cybersecurity Checklist

Cybercrime is a serious threat, and constant vigilance is key for prevention. Our firm plays an important role in protecting your assets, but you can take further action to secure your information. This checklist summarizes common cyberfraud tactics, along with tips and best practices to protect yourself. You may already be doing many of these things, but others may be new. The checklist also covers actions to take if you suspect that your personal information has been compromised.

Cybercriminals exploit our heavy reliance on technology. Methods used to compromise a victim's identity or login credentials—such as malware, phishing, and social engineering—are increasingly sophisticated and difficult to spot. A fraudster's goal is to obtain information to gain access to your account and assets. Fortunately, criminals often take the path of least resistance. Following best practices and being cautious when sharing information and executing transactions makes a big difference.

❑ 1. Two-Factor/Multifactor Authentication

- Use an authentication method that requires a one-time numeric passcode in addition to your username and password when you log in. Since the code is typically sent via text to your cellphone, even if criminals obtain your login information, they still will not be able to access your accounts.

❑ 2. Password Management/Aggregator Software

- Use a digital password aggregator such as Dashlane or LastPass to keep track of your log-in information for online accounts, and keep the password for the aggregator with your will.

❑ 3. Strong Password Principles

- Create a unique, complex password for each website, and change it every six months.
- Don't use personal information as part of your login ID or password.
- Never share your login credentials.

❑ 4. Red Flags

- Be suspicious of phone calls, emails or texts asking you to send money or disclose personal information. If someone claiming to be a service representative calls you, hang up and call the company back using a known phone number.
- Never share sensitive information or conduct financial transactions via email.
- Watch out for phishing attempts and malicious links by carefully checking the sender's email address. Urgent-sounding, legitimate-looking emails are intended to tempt you to accidentally disclose personal information or install malware.
- Don't open links or attachments from unknown sources. If an email urges you to click on a link, enter the company's web address in your browser instead.
- Check your email and account statements regularly for suspicious activity.
- Never enter confidential information in public areas. Assume someone is always watching.

❑ 5. Maintain Updated Technology

- Keep your web browser, operating system, antivirus software, and anti-spyware software updated.
- Activate your firewall.
- Do not use free or found USB devices. They may be infected with malware.
- Check the security settings on your applications and web browser to make sure they're strong.
- Turn off Bluetooth when it's not needed.
- Dispose of old hardware safely by performing a factory reset or removing/destroying all data storage devices.

❑ 6. Precautions When Moving Money

- Whenever possible, leverage your financial institutions' electronic authorization tools to move money yourself and verify requests.
- Thoroughly review and verbally confirm all disbursement request details before providing your approval, especially when sending funds to another country. Never trust wire instructions received via email.

❑ 7. Safe Internet Browsing

- Do not visit websites you don't know, such as those advertised on pop-up and banner ads.
- Log out completely when exiting websites where you have accounts.
- Don't use public computers or free Wi-Fi hotspots. Instead, use a personal hotspot or a virtual private network (VPN).
- Hover over questionable links to reveal the URL before clicking. Secure websites start with "***https***," not "http."

❑ 8. Social Media Precautions

- Be cautious when accepting friend requests. A good rule of thumb is to only accept friend requests from people you know in real life.
- Be judicious about liking posts and following links. Consider whether the source is trustworthy.
- Limit the information you share on social media sites. Assume fraudsters can see everything.

charles SCHWAB

Keating Wealth Management uses Charles Schwab & Co., Inc. as the custodian for our clients' assets and accounts. The information below is specific to Schwab, but most other major financial institutions have similar protocols.

❑ 9. Protecting Your Schwab Account

- Enroll in two-factor authentication at Schwab Alliance to obtain a unique 6-digit code each time you access your Schwab account.
- Confirm your identity using Schwab's voice ID service when calling the Schwab Alliance team for support.
- Review the Schwab Security Guarantee, which covers 100% of any Schwab account losses due to unauthorized activity.
- Visit Schwab's Client Learning Center at http://content.schwab.com/learningcenter for more information.

❑ 10. If You Suspect a Breach of Your Schwab Account

- Call our office or call Schwab Alliance immediately at (800) 515-2157 to initiate a watch for suspicious activity and collaborate on other steps to take.
- Request our "**How to Respond to a Data Breach**" flier for more information.