Benefit Financial Services Group

BFSG Insights

# Tips for Preventing Fraud

August 17, 2018

Cybercrime and fraud are serious threats and constant vigilance is key. While BFS Wealth Management plays an important role in helping protect your assets, you can also take action to protect yourself and help secure your information. This checklist summarizes common cyber fraud tactics, along with tips and best practices. Many suggestions may be things you're doing now, while others may be new. We also cover actions to take if you suspect that your personal information has been compromised. If you have questions, we're here to help.

Cyber criminals exploit our increasing 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 access to your account and assets or sell your information for this purpose. Fortunately, criminals often take the path of least resistance. Following best practices and applying caution when sharing information or executing transactions makes a big difference.

## How we can work together to protect your information and assets

### Safe practices for communicating with our firm

- Keep us informed regarding changes to your personal information.
- Expect us to call you to confirm email requests to move money, trade, or change account information.
- Establish a verbal password with our firm to confirm your identity.

### How Schwab protects your account

Schwab takes your security seriously and leverages protocols and policies to help protect your financial assets. Below are actions you can take to reinforce their efforts and resources to assist you in keeping your account safe:

- Confirm your identity using Schwab's voice ID service when calling the Schwab Alliance team for support (800-515-2157).
- Use two-factor authentication, which requires you to enter a unique code each time you access your Schwab accounts. If you wish to set-up two-factor authentication, please call Schwab Alliance.
- Review the Schwab Security Guarantee, which covers 100% of any losses in any of your Schwab accounts due to unauthorized activity.

To learn more, visit Schwab's Client Learning Center.

## What you can do

- Be aware of suspicious phone calls, emails, and texts asking you to send money or disclose personal information. If a service rep calls you, hang up and call back using a known phone number.
- Never share sensitive information or conduct business via email, as accounts are often compromised.
- Beware of phishing and malicious links. 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. Enter the web address in your browser.

- Check your email and account statements regularly for suspicious activity.
- Never enter confidential information in public areas. Assume someone is always watching.

### Exercise caution when moving money

- Leverage Schwab's electronic authorization tool to verify requests. Featuring built-in safeguards, this is the fastest and most secure way to move money.
- Review and verbally confirm all disbursement request details thoroughly before providing your approval, especially when sending funds to another country. Never trust wire instructions received via email.

### Adhere to strong password principles

- Don't use personal information as part of your login ID or password and don't share login credentials
- Create a unique, complex password for each website, Change it every six months. Consider using a password manager to simplify this process.

### Maintain updated technology

- Keep your web browser, operating system, antivirus, and anti-spyware updated, and activate the firewall.
- Do not use free/found USB devices. They may be infected with malware.
- Check security settings on your applications and web browser. 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 and destroying all storage data devices.

### Use caution on websites and social media

- Do not visit websites you don't know, (e.g., advertised on pop-up ads and banners).
- Log out completely to terminate access when exiting all websites.
- Don't use public computers or free Wi-Fi. Use a personal Wi-Fi hotspot or a Virtual Private Network (VPN).
- Hover over questionable links to reveal the URL before clicking. Secure websites start with "https," not "http."
- Be cautious when accepting "friend" requests on social media, liking posts, or following links.
- Limit sharing information on social media sites. Assume fraudsters can see everything, even if you have safeguards.
- Consider what you're disclosing before sharing or posting your résumé.

### What to do if you suspect a breach

- Call our office (888-726-9378) or your Schwab Alliance team immediately (800-515-2157) so that they can watch for suspicious activity and collaborate with you on other steps to take.

### 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, https://www.fdic.gov/consumers/assistance/index.html.
- FBI Scams and Safety provides additional tips, https://www.fbi.gov/scams-and-safety.

**IMPORTANT DISCLOSURE INFORMATION**

Benefit Financial Services Group (BFSG) is a Registered Investment Advisor. Please remember that past performance may not be indicative of future results. Investments involve varying degrees of risk, and there can be no assurance that the future performance of any specific investment, investment strategy, or product (including investments and/or strategies recommended or undertaken by BFSG), or any non-investment related content, referenced directly or indirectly herein will be profitable, equal to any corresponding indicated historical performance level(s), be suitable for your portfolio or individual situation, or prove successful. Due to various factors, including changing market conditions and/or applicable laws, the content may no longer be reflective of current opinions or positions. Content provided herein is for informational purposes only and should not be used or construed as investment advice or a recommendation regarding the purchase or sale of any security outside a managed account. Moreover, you should not assume that any discussion or information contained in this newsletter serves as the receipt of, or as a substitute for, personalized investment advice from BFSG. To the extent that a reader has any questions regarding the applicability of any specific issue discussed above to his/her individual situation, he/she is encouraged to consult with the professional advisor of his/her choosing. A copy of the BFSG current written disclosure statement discussing our advisory services and fees is available for review upon request.

This material may not be reproduced in whole or in part in any form whatsoever without the prior written permission of BFSG.