Image from Shutterstock Free Photos

REGISTERED INVESTMENT ADVISOR SINCE 1982

NEWSLETTER

DECEMBER 2024 • VOLUME 32 • ISSUE 12

Fraudsters Don't Take Holidays!

Fraudsters are building fake Schwab websites & impersonating Schwab employees

Source: Schwab Cybersecurity Resource Center

We are in the throes of the holidays and fraudsters are ready to take full advantage of any opportunity, knowing that we are busy traveling, shopping, and spending time with friends and family.

There are two threats that you should be aware of:

1. Imposters are posing as Schwab employees and contacting advisors and clients via phone and other channels, including email and text messages.

2. Scammers are using search engine optimization (SEO) to create fake websites that appear in search results to be the trusted institution, like Schwab. When clients visit these sites, they are exposed to phishing attacks aimed at stealing their information and assets.

Fraudsters posing as Schwab employees:

- First, the fraudster gains access to the client's personal information, like first and last name, phone number, and home address, potentially from the dark web or a hacked website for example: social media.

- The imposter may spoof a Schwab phone number to call the client and then identify themselves as an employee in the fraud department.

- The fraudster alleges that a suspicious charge has been found in a client's Schwab account and makes the client aware that the charges will need to be reversed.

- The fraudster will use social engineering to get the client to provide them with their Schwab Alliance username; then, when the system sends an automated SMS for verification, the fraudster requests the code from the client.

- Once the fraudster has the SMS code, they will update client's Schwab Alliance password, log into the client's account, and initiate unauthorized transactions.

- Fraudsters will take advantage of people's emotions and all the activity of the holidays to get them to let their guard down and act quickly.

Using SEO to drive clients to fake "Schwab" phishing sites:

- Fraudsters use sophisticated techniques to create websites that appear in search engines when clients are looking for Schwab or other trusted institutions. The websites are designed to look legitimate, and their position in the search results trick users into believing the top search hits are the most credible.

- This phishing tactic is very effective as not every user will scrutinize every search result to ensure the link they're about to click is legitimate.

- Once the client clicks on the phishing website and attempts to log in with their credentials, they receive an error message stating there's a login issue and to contact a hotline number noted in the message for further assistance.

- When the client contacts the fraudulent number, the bad actor posing as a Schwab employee states that there's been a security breach, and someone is attempting to steal money from their account.

- Then the bad actor attempts to convince the client to download software to their device. The overall goal is to gain access to the device and continue to facilitate additional fraud attacks, which can ultimately lead to unauthorized activity and ID theft.

We want to help mitigate fraud this holiday season by sharing these fraud prevention tips with you:

- Clients should avoid supplying any personal identifying information in an email or over the phone, even if they think they're talking to Schwab. **Note:** Clients can verify that they're speaking with Schwab by ending the call and calling a Schwab phone number that is known to them.

- If Schwab sends you an SMS text code to verify account access, do not share this with anyone. Legitimate Schwab representatives will never ask for this information.

- Download your financial institutions app and utilize biometric authentication if available. **Note:** be cautious to read reviews and check the number of downloads to ensure you're downloading the legitimate app.

- Scrutinize email addresses, URLs, and spelling used in any correspondence.

- Hover your mouse cursor over the email address and check the sender's domain *(look for the "abc.com" in the address john.doe@abc.com)* to ensure it's what you would expect.

- Avoid using Google, Safari, and Firefox to search for Schwab or other important websites. Use your saved bookmarks or type the known website in your browser, for example: *www.Schwab.com, or use the app, and save important websites to your web browser's favorites/bookmark*.

- Use good cyber hygiene when surfing the internet, avoid visiting unsecure websites or public WiFi.

- Please contact Schwab immediately to report all suspicious or fraudulent activity.

Our Southern Capital Team:

Terry E. Nager
Wendy Nelson Bailey
David E. Lindsey
Charlotte Straight
Michelle Z. Hunt
Larry “Trace” Dixon
Morgan Dawson
Ashleigh Donnelly
Eric M. Nager

Please remember to notify us if you have had any material changes in your financial circumstances.