NAPLES GLOBAL ADVISORS

CASE STUDY

OCTOBER 2023

What to Do When a Fraudster Calls You!

Cyber criminals target us in a myriad of ways, and they are ubiquitous. Every email must be read with scrutiny. Every phone call must be met with skepticism. Click the wrong link and you've got a virus. Take a call and unsuspectingly give up sensitive information to a fraudster. Our goal with this case study, which is based on real events, is to raise awareness of cyber threats and to show how intricate and diabolical these schemes can be. In this instance, the perpetrators posed as Charles Schwab employees and acted cleverly to remotely gain access to a client's computer.

Details of the Fraud Attempt:

On a Friday afternoon, an NGA team member received a call from a client about a matter unrelated to a cyber threat. During the conversation, the client mentioned that members of the Charles Schwab "Cyber Security Team" had called during the week to let him know they were monitoring hackers from either China, Michigan, or New York City who were trying to access his accounts via his login. The imposters even asked if the client had a connection to any of these locations, which he did. The fraudsters attempted to make the threat real by grounding the source in a location the victim knew and had a history. The suspicious interaction raised an immediate red flag for the NGA team member. Foremost, custodians, in this case Charles Schwab, will contact the advisor first in matters of fraud. The NGA team member immediately asked several follow up questions and learned the following:

1) Two members of Charles Schwab's "Cyber Security Team" called the client throughout the week. The first call occurred on Tuesday with an initial alert regarding attempted hacking. On Thursday, the fraudsters called again to notify the client his accounts had been illegally accessed and prompted him to change his password.

2) The client, thinking the callers were legitimate Charles Schwab representatives, shared his computer screen with one imposter and allowed that individual to "help" reset his password. It was likely that while connected to the computer, the cyber thief installed a virus or other malware and was able to identify the client's keystrokes when changing the password. The client's computer was unknowingly compromised.

3) After changing the client's password, the fraudsters said they would call back on Saturday to ensure the client's accounts were safe. The fraudsters claimed to work seven days a week as part of Charles Schwab's enhanced security efforts.

Overall, the cyber thieves were very convincing. They acted professionally. They called the client multiple times and followed up as they said they would. The first call was particularly clever and convincing, as it did not require any action by the client. The imposters did not ask for any information, alluded to working out of a Charles Schwab office in San Francisco, and promised to follow up if action was required. It was an elaborate ruse which made it seem more real to the client. All this shows how crucial it is to verify phone numbers and to be discerning about the intent of unknown callers.

Naples Global Advisors & Charles Schwab Response:

1) After learning of what transpired, and believing the client had been victimized, the NGA team member immediately called Charles Schwab with the client to report the incident.

2) With help from a Charles Schwab representative, web access to the client's accounts was locked so that no one, including the client, could log in. Additionally, via internal systems, the representative confirmed that no one from Charles Schwab had called the client and that similar fraudulent calls had been reported by other clients. Finally, the representative verified that no fraudulent transactions had occurred.

3) Though no fraudulent transactions had been initiated, the representative and NGA team member were still concerned about identity theft. The representative advised the client to leave his computer turned off until it could be swept for malware by a professional technician.

4) As a precaution, the NGA team member advised the client to change his email password and passwords for other critical websites such as bank accounts and credit cards. The client was advised to check for any suspicious activity and fraudulent transactions in those accounts.

5) As an added layer of potential protection, NGA provided the client with a document containing detailed steps on how to freeze credit.

6) NGA referred the client to a trusted computer technician to remove any malware. Several days later, after the computer was cleared by the technician, the NGA team member called Charles Schwab with the client to unlock web access and establish a new username and password.

7) The Monday following the incident, NGA received a call from a Senior Manager with Charles Schwab's Financial Crimes and Risk Management division. The client still had the phone numbers the fraudsters used to call and was able to provide that information to the Senior Manager along with other incident details.

Recognizing Red Flags:

Several red flags manifest during the incident that ought to be noted. First, always be suspicious about a custodian or other institution calling you directly. Most institutions, such as the IRS, Social Security Administration, and financial custodians will not call or text you. Secondly, never share your computer screen with an unverified source. Next, pay close attention to the details of such phone calls and listen for suspicious intent. In this example, how would a "Cyber Security Team" know where the hackers were located? Why would they call back on a Saturday? Why were two different individuals calling the client? It is critical to listen closely for such suspicious indicators. Finally, though not part of this circumstance, be vigilant about emails and text messages you receive. Never click links from unknown sources, watch closely for misspellings and grammatical issues in emails, and be wary of web domains that are slightly different from the real site. Be cautious. Be diligent. If ever in doubt, call us for help.

Additionally, the Investor.gov website provides a checklist to help identify investment fraud.