



Memorandum

Date: July 20th, 2023

To: Joe Rinaldi
President and CIO

From: Hayden Tran
Investment Analyst

Re: Recent Updates on Cybersecurity News from Charles Schwab – Our Platform Partner

Imposter scams refer to a scam where a fraudster impersonates a trusted individual, business, or organization to convince a target to transfer money. In an imposter scam, fraudsters will often:

- Contact you via a phone call, email, text, online advertisement, or social media post.
- Claim to be security/technical support for a known and reputable company or a trusted financial institution
- Ask you to download software and/or request remote access to your computer.
- Send you an email or text message with a link or attachment, which may ask you to approve/deny a transaction, set up new credentials, or take some other action regarding your account.

To prevent imposter scams, you should notice red flags and take the following steps:

Step 1

Confirm the legitimacy of the organization or person trying to reach you, especially if you did not initiate the contact. If you have any doubts, reach out to your advisor before communicating further.

Step 2

Do not assume you are speaking with an institution based on caller ID. Text messages, emails, and phone calls can appear to come from a trusted institution when they are actually from a fraudster.

Step 3

Use caution and take time to research if you receive a request to send money urgently. Again—your advisor will be happy to help you decide if these situations are legitimate.

Step 4

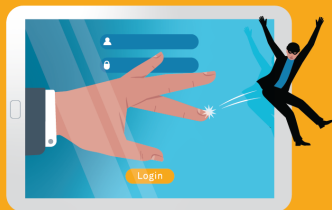
Check the URL of the website or link sent to you by email to validate it is a legitimate site address

Cyber Security News



How to notice and protect yourself from imposter scams.

At Schwab, working closely with your advisor to protect your assets is our top priority. That's why we're letting you know about a recent increase in imposter scams, how these scams happen, and steps you can take to protect yourself.



Imposter scams

Imposter scams refer to a scam where a fraudster impersonates a trusted individual, business, or organization to convince a target to transfer money.

In an imposter scam, fraudsters will often:

- Contact you via a phone call, email, text, online advertisement, or social media post.
- Claim to be security/technical support for a known and reputable company, such as Microsoft, or a trusted financial institution like Schwab.
- Ask you to download software and/or request remote access to your computer.

- Send you an email or text message with a link or attachment, which may ask you to approve/deny a transaction, set up new credentials, or take some other action regarding your account.

Preventing imposter scams requires noticing red flags and taking simple steps.

You should:



Confirm the legitimacy of the organization or person trying to reach you, especially if you did not initiate the contact. If you have any doubts, reach out to your advisor before communicating further.



Do not assume you are speaking with an institution based on caller ID. Text messages, emails, and phone calls can appear to come from a trusted institution when they are actually from a fraudster.



Use caution and take time to research if you receive a request to send money urgently. Again—your advisor will be happy to help you decide if these situations are legitimate.



Check the URL of the website or link sent to you by email to validate it is a legitimate site address (e.g., www.schwab.com versus www.schwab.co).

Report concerns you have.

If you are ever concerned about a text message, email, or phone call, please contact your advisor and also contact Schwab directly at **800-515-2157**. Forward suspicious emails or screenshots of suspicious texts to phishing@schwab.com.

For more information about the wide variety of imposter scams, red flags, and ways to protect yourself and others, read our article: [Avoid Imposter Scams](#).

Check out our online resources.

For more security tools, resources, and steps you can take to help safeguard your personal information and assets, visit [SchwabSafe®](#). And