Stepp & Rothwell

First Monday Memo
Client Exclusive
July 2023

Don't Take the Bait! Avoiding the Modern Scam

You receive a call from someone claiming to be with the IRS, and they tell you that you are under audit and need to supply financial information immediately to avoid penalties.

You receive an email from someone you think is your broker that claims there has been suspicious activity in your account and urgently requests you log in to verify it using the convenient link in the email.

You are browsing on your laptop and a warning that looks like it is from Microsoft pops up to inform you that your computer has been hacked and you need to call the provided phone number right away to avoid permanent loss of data.

These are examples of three common scams designed to gain access to your data and your money. Scammers today are not teenagers looking for a thrill from their mom's basement. They are organized businesses, and they are becoming increasingly sophisticated. They bait the hook, throw out as many lines as they can, and wait for someone to bite.

The most prevalent types of scams are impostor scams, where scammers pretend to be from an organization you trust, like your bank or brokerage, in an effort to get your personal information or your money. Once they have you on the line, they can be extremely convincing. They might confide to you about suspected fraud in their company and enlist you in helping to catch the criminals by working with them to set up a "test transaction" or tell you that you need to transfer money to another account because your account has already been compromised. They might persuade you not to talk to anyone else at the company in case "other employees might be involved in the scam".

Like legitimate businesses, criminals adapt, which can make it difficult to keep up with all the latest scams. That is why it is important to be extra vigilant about protecting ourselves. Here are some tips to help keep you safe:

- With any surprise email or phone call, ask yourself, "Did I ask for this? Did I sign up for this?"
- Examine the sender's email address. Use your cursor to hover over it to see the whole address and if it matches the company from whom it is supposed to have come.
- Look for grammatical errors, misspellings, capitalization mistakes, poor punctuation, or unusual phrasing in the text of the email.
- Do not click on links or call numbers based on instructions from emails or computer pop-ups. Instead, go online, and use the contact information directly from that entity's website.
- Likewise, never provide any personal information in response to unsolicited phone calls from the IRS or any other financial institution. Hang up, and then call the entity directly using the contact information from that entity's website.
- Remember that no legitimate business, government, or law enforcement agency will ever ask you to pay them in gift cards or cryptocurrencies.
- Be wary of any contact or caller pressuring you to do or provide something "urgently" or "immediately." Always take a breath and ask yourself if it might be a fake.

The sad truth is that the more reliant we are on modern communication, the more open we are to impostor scams. If you find yourself questioning the legitimacy of a call or an email, contact us. We will be happy to help you sort it out and keep you (and your money) safe.

From the Federal Trade Commission…

On the App, On the Line

Scams that started on social media accounted for the most money overall in 2022 ($1.2 billion), but scams that began with a phone call cost the most per person ($1,400 median loss).
Source: Https://comsumer.ftc.gov/consumer-alerts/2023/02/top-scams-2022

Thank you so much to the client family that surprised our staff with a catered lunch. Everyone was thrilled!