Remember: When in doubt, do not act!

Email scams are on the rise and have increased 111% from 2018 to 2022, with losses totaling over $2.7 billion in 2022, according to the FBI Internet Crimes Report.

Using social engineering, email scammers gain the trust of a targeted person with the goal of getting them to send funds to a different person or entity than originally intended. Here are some things to know about email scams, so you can help protect yourself and your assets.

How they target you:

Scammers typically interject themselves into your normal transactions to change the destination of the funds. Common occurrences include:

- **Real estate closings:** Scammers will impersonate the identity of the title/real estate agent, or closing attorney, and send different payment details.
- **Vendor impersonation:** They can also pose as representatives of a company or government agency and advise that an invoice must be paid immediately to avoid a negative consequence. They often ask for a wire transfer to a fraudulent bank account or other means of payment, such as a check or ACH transfer.
- **CEO/executive impersonation:** Scammers will also impersonate the CEO or executive of a company. They request that an employee within the accounting or finance department transfer funds to an attacker-controlled account

What to do and what to look for:

Knowing what to do and what to look for is critical to avoid becoming a victim of an email scam.

- **Account changes:** Always verify and confirm details with the parties involved, especially with messages regarding funds transfers. Some email scammers use hacked email accounts, so it's important to use a different method to verify that the sender is not a scammer. You can call or text an associated phone number or interact on a trusted mobile app or chat channel.
- **Email sender validation:** Scammers can also use fraudulent email addresses that closely resemble a legitimate email address that you may have been communicating with previously. The addition or removal of a single character in an email address may be difficult to spot at first glance:
  - Google.com vs. Google.corn: In this case, the scammer replaced .com with .corn, with the letters "r" and "n" replacing the letter "m"
  - JONDOE@BUSINESS vs. JON.D0E@BUSlNESS: For this example, the scammer used a zero instead of a capital O, and added a period in between "JON" and "D0E". They also used a lowercase "L" in place of the capital "i"
- **Urgent or priority emails:** Emails may contain a header in the subject line or phrases in the content of the email, such as "urgent" or "confidential." If you receive an email marked urgent or confidential, please review it carefully for accuracy and reach out directly to the individual to validate the request.

Bookmark our new site, citi.com/fraudprevention, and visit often for the latest updates on common scams and how to spot them.