Avoid Scams That Pose as a Financial Institution

Author: eFraudPrevention

Scams impersonating financial institutions have become increasingly prevalent in our digital age. Falling for one can cost you money and peace of mind. Stay informed and safeguard your financial well-being as we dive into the latest tactics of fraudsters masquerading as legitimate financial institutions.

Recognizing Common Red Flags

A text asking you for details to "confirm" it's you. Your financial institution may text you from time to time – for instance, to confirm a transaction on PC – but financial institution texts will never ask you to confirm details or for passwords. Financial institutions also won't update their apps in this way. If you're suspicious, don't click on the link, and don't call any numbers within the text. Instead, contact your financial institution on its "normal" number – Google it if you don't know – and check whether the text is from them.

Fake fraud alert scam. The scheme tries to scare you into believing the scammers are representatives of your financial institution. The scammers will tell you a fraudulent charge was made to your bank account through a digital instant payment app.

Give you a deadline of 24 hours before your financial institution account erases itself. Many legitimate messages from your financial institution will be marked "urgent" – particularly those related to suspected fraud – but any message with a deadline should be treated with extreme suspicion. Cybercriminals must work fast – their websites may be flagged, blocked, or closed down rapidly – and need you to click without thinking. Financial institutions want you to get in touch – they won't usually set a deadline.

Send you a link with a "new version" of your banking app. Your financial institution will not distribute apps this way – instead, download from official app stores, and ensure yours is up to date.

Use shortened URLs in an email. Cybercriminals use a variety of tricks to make a malicious web page appear more "real" in an email that's supposedly from your financial institution – one of the most basic is URL-shortening services. Be very cognizant when clicking on links in an email. You can hover over the shortened URL to look for red flags. If you have any suspicion that the email may be fraudulent, it's best to visit the financial institution's website (the usual URL you use), or call them on an official number (i.e., not the one in the email).

Email you at a new address without warning. Financial institutions will only add new email addresses with your permission. If you want to be extra careful, create a unique email address for your financial institution. Don't publish it anywhere or use it for anything else – that way, emails that appear to be from your financial institution probably ARE from your financial institution. As always, stay cautious.

Send a personal message with a blank address field. If you receive a personal message from your financial institution, it should be addressed to you – not just in the message but in the email header. Check that it's addressed to your email address – if it's blank or addressed to "Customer List" or similar, be suspicious.

Protection Against Scams

Always confirm the identity of anyone claiming to represent your bank. It's prudent to refrain from sharing sensitive details over email or phone, particularly if you did not initiate the contact. When contacting your financial institution, use the contact details you have on record or those from official sources rather than information provided in unsolicited communications. Furthermore, arm yourself with knowledge.

How to Stay Safe

- Inspect the sender's information to confirm that the message was generated from a legitimate source, but don't click the link or call the number on the text.
- Do not respond to the text. Even writing STOP will let the scammer know your number is genuine, and they may sell your number to other scammers, making the problem worse.
- If a call or text is received regarding possible fraud or unauthorized transfers, do not respond directly, immediately hang up, and do not enter your CVV number. Even if they have the correct caller ID. Using "caller ID spoofing," scammers can make it look like they're calling from your bank's phone number.
- Remember, never click on links provided in unsolicited text messages or emails. Your financial institution will never ask for a CVV or PIN number to verify fraud. Requests to do so and poor spelling or grammar are telltale signs of a scam.
- Always verify the identity of anyone claiming to be from your financial institution. The best way to protect yourself is to say, "Let me call you right back," and then you call the official bank number yourself. A legitimate representative from your bank will never take issue with you hanging up and calling the number on the back of your debit or credit card. Use your contact details for your bank or credit union, not those provided in the unsolicited communication.
- Never answer any questions from a random call from anybody. There may be a call from someone legitimate, but more often than not, it's a scammer.
- Do not post sensitive information online. The less information you post, the less data you make available to a cybercriminal for use in developing a potential attack or scam.
- Avoid sharing personal or financial information over the phone or email.
- Keep an eye out for misspelled words, which are used to bypass a phone carrier's filter system for fraud.