How to recognize phishing attempts

Last Modified on 09/07/2026 2:07 am PDT

Phishing is an attempt to deceive a person into disclosing sensitive information, visiting a fraudulent website, downloading malicious software, sending money, or approving an unintended action. Phishing attempts can arrive through email, text messages, telephone calls, social media, messaging applications, online advertisements, and search results. The message may impersonate a cryptocurrency exchange, wallet provider, bank, government agency, employer, or someone the recipient knows. No single warning sign conclusively proves that a message is fraudulent, but several warning signs appearing together should lead the recipient to stop and independently verify the request.

Watch for Urgency, Fear, and Unexpected Requests

Phishing messages often attempt to create urgency so the recipient acts before carefully reviewing the situation. The message may claim that an account has been compromised, a withdrawal is pending, access will be suspended, or immediate verification is required. Other attempts use excitement rather than fear by offering an unexpected refund, reward, airdrop, investment opportunity, or job. The Cybersecurity and Infrastructure Security Agency identifies urgent language, requests for personal information, shortened URLs, and unexpected attachments as common phishing indicators.

Examine the Sender and Website Address Carefully

A familiar display name or company logo does not establish that a message is authentic. Review the complete sender address and look for misspellings, added words, substituted characters, unfamiliar domains, or unusual domain endings. Fraudulent websites may closely resemble the real service while using a slightly different address. The FBI's phishing guidance warns that spoofed websites may look nearly identical to legitimate sites. Spelling and grammatical errors can be warning signs, but a professionally written message should not be assumed legitimate based on its appearance alone.

Be Cautious With Links, Attachments, and Downloads

Avoid clicking unexpected links, opening unsolicited attachments, scanning unfamiliar QR codes, or installing software at the sender's request. A link's visible text may differ from its actual destination, and an attachment may contain malicious software. If a message appears to concern a real account, access the company through its official application, a trusted bookmark, or a web address entered independently. Do not use the link or telephone number supplied in the suspicious message. The Federal Trade Commission also recommends keeping security software and devices updated and using multi-factor authentication to limit the effect of stolen credentials.

Recognize Crypto-Specific Phishing Attempts

Cryptocurrency phishing frequently attempts to obtain a seed phrase, private key, exchange password, authentication code, or wallet approval. A message may claim that a wallet must be verified, synchronized, migrated, or connected to resolve a security problem. Fraudulent websites may also imitate token claims, airdrops, decentralized applications, or customer-support portals. MetaMask states that its support personnel do not initiate unsolicited contact or request a user's Secret Recovery Phrase. Users should also review every wallet connection, transaction, and signature request before approving it. A malicious approval may expose tokens even when the seed phrase remains private, as explained in our guide to crypto drainers and approval phishing.

Verify Security Alerts Through a Separate Channel

If an email, text, or call claims to come from an exchange or other financial service, end the communication and contact the company through independently verified information. Do not provide login credentials, authentication codes, identification documents, or wallet information to an unsolicited caller. The FBI has warned that scammers impersonating cryptocurrency exchange employees may claim an account is under attack and pressure the user to click a link or disclose information. A genuine account concern can be investigated by signing in through the official application or contacting support through the company's verified website.

What to Do After Interacting With a Phishing Attempt

If a password was entered into a suspected phishing website, change it promptly through the legitimate service, review active sessions and recovery settings, and enable or reset multi-factor authentication. If a seed phrase or private key was disclosed, the associated wallet should no longer be relied upon for storing assets; follow the wallet provider's official procedures for creating a new wallet and moving any remaining funds. If a suspicious transaction or wallet approval was signed, review the resulting blockchain activity and applicable token permissions. Preserve the message, sender information, website address, transaction hashes, wallet addresses, and related communications. Phishing and spoofing incidents can be reported to the relevant service and, where appropriate, to the FBI's Internet Crime Complaint Center.