Protect yourself: Recognize phishing attempts

Phishing is the attempt to acquire sensitive information such as user names, passwords and account numbers for malicious reasons by masquerading as a trustworthy entity in an electronic communication.

Who is a target?

Anyone can be a target of a phishing attack. While some attacks may focus on a person or group of people, others cast a much wider net. It is important to remember that the threat actor's goal is to obtain personally identifiable information to gain access to your financial accounts or credentials to gain access to your accounts.

Be careful when using job search websites, social networking sites or any other site that allows you to post personal information. Even a single piece of information could be the basis for a phishing attack.

Common scenarios

Typically, the threat actor uses an email or pop-up window from a company or an organization with which you regularly conduct business (e.g., a bank, broker/dealer, credit card company, government agency, etc.). The message typically asks you to update or validate your account information, such as:

- "We suspect an unauthorized transaction on your account. To ensure your account is not compromised, please click the link below and confirm your identity."
- "During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."
- "Our records indicate that your account was overcharged. You must call us within seven days to receive your refund."

To encourage you to act immediately, the notice may threaten that the account could be closed or canceled if you do not respond. Most emails will ask you to click on a link that takes you to a replica of the company's website. This could result in malicious software being downloaded onto your computer or send you to a website to collect your credentials.

Red flags

- Unexpected requests for personal information
- Urgent or threatening language
- Spelling errors and improper grammar
- A link to a site that seems unrelated to the organization that contacted you
- An address or domain from which the email was sent that appears fake or unrelated to the request
- Missing phone numbers or contact information

Here are some phishing variations you should be aware of:

Pharming: A scam in which malicious code is installed on your computer. This code redirects you to a fraudulent website without your knowledge. Follow established computer safety guidelines to reduce the risk of pharming.

Vishing (voice phishing): Vishing is simply phishing conducted via telephone. This scheme uses social engineering techniques to trick you into providing information that can be used to access your accounts or open new lines of credit. Never disclose personal information during a phone call unless you initiate the contact by using a phone number obtained from a reliable source.

Smishing: Smishing is phishing conducted via text messaging. The text message will often contain a website or a phone number. The phone number will usually have an automated voice response system. Smishing messages will often lure victims with an offer of a free gift card or cash. Don't respond to smishing messages.

Tips to protect yourself

- Do not respond to unsolicited emails asking you to divulge personal information. Reputable organizations with which you legitimately conduct business generally do not request account numbers or passwords unless you initiated the transaction.
- Delete suspicious emails without opening them. If you do open an email that turns out to be fraudulent, do not open any attachments or click on any links it may contain.
- If you initiate a transaction and need to provide personal information through a website, look for indicators that the site is secure. A lock icon on the status bar or a web address beginning with "https://" indicates a secure site. Although no site is foolproof, these indicators can help lessen your risk.
- While Wi-Fi hot spots can be convenient, if you are on an unsecured network or log in to an unencrypted site, other users on the network can see what you see — and what you send.
- Install and regularly update virus protection software. Keep your computer's operating system and web browser current. In addition, a firewall can help block communications from unauthorized sources.
- Review your accounts on a regular basis; it's one of the best ways to notice and stop fraudulent activity quickly.
- Choose passwords that are difficult for others to guess, and use a different password for each online account. Change your passwords frequently.
- Do not choose "remember this device" when logging into your accounts. Multi-factor authentication is there to help protect you against fraud.
- Be suspicious if someone requests your personal information when you haven't initiated the contact. Most legitimate companies and agencies do not operate in such a way. To check whether an email or a phone call is legitimate, contact the company in question through the phone number or email address listed on its website.
- If you fall victim to phishing, pharming, vishing, or smishing, place fraud alerts on your credit files. Contact one of the major credit bureaus to place an alert on your file. Contacting one credit bureau automatically updates the other two.

  Equifax: 888-836-6351
  Experian: 888-EXPERIAN (397-3742)
  TransUnion: 833-395-6938

Reporting a phishing scam

If you believe you have become the victim of a phishing scam, you may file a complaint with the Internet Crime Complaint Center at ic3.gov or the Federal Trade Commission at ftccomplaintassistant.gov. Please contact your financial advisor if you need additional assistance.

Forward phishing emails to spam@uce.gov and to the company, bank or organization impersonated in the email.

Linda Beardsley
Financial Advisor
3151 S Vaughn Way
Ste 110
Aurora, CO 80014-3517
720-615-9235

