LPL Financial

Protecting Yourself From Phishing Attacks

Learn about the many avenues of phishing and next steps for staying safe.

Phishing is a form of cybercrime in which cybercriminals deploy fraudulent communications to a user or organization that are created to appear as if they are from a legitimate source. These communications are made to trick recipients into giving out sensitive information such as bank account information or credit and social security numbers. According to an IC3 Annual Report, there were around 298,878 victims of phishing attacks in 2023 which incurred losses of around $18,728,550. As phishing attacks increase in frequency, it is important to understand the different types of phishing attacks and how to best protect yourself from them.

Email

These bad actors create realistic looking emails with malicious links or attachments. These emails are designed to get you to immediately interact with the content and not think twice on if its legitimate or not. Investigate every email and ensure you trust the sender before clicking on any links or attachments within the emails. Verify if an email is legitimate and locate the website by typing it in to confirm any actions on your account rather than clicking on an email. If you receive an email from a person you know, verify with them if they indeed send that communication by using other trusted channels.

Phone

Smishing

Smishing is a form of phishing attack that is carried out by text or SMS message. Smishing attacks are created to look like a legitimate text message. The contents of the sent text messages often contain links that contain malware or instructions that are meant to trick users into revealing sensitive information. These attacks are particularly dangerous because people may be more inclined to trust a text message rather than an email. Many individuals are unaware that phishing attacks could be carried out via text message and these attacks can be just as dangerous as a traditional phishing email. Avoid clicking on links or attachments from random text messages. Always confirm the identity separately before interacting with the message.

Vishing

Vishing is a form of cybercrime where cybercriminals disguise themselves as a reputable business or entity and uses phone call or voicemail message to contact their targets to trick in them into providing them with sensitive information. Cybercriminals will often use threats and harsh language to convince their targets to feel pressured into releasing their information. Examples of this can be seen with fake tech support scams and IRS call center scams as well. When identifying a vishing scam always attempt to confirm the identity of the individual that is contacting you, if you do not feel comfortable with an inbound call, hang up and contact a business or individual directly

QR Codes

A new and trending attack is quishing. Quishing involves the scanning of a QR code from your mobile device that leads you to a malicious website. With QR codes, a website's URL isn't exposed within an email and renders email security scans ineffective. To avoid Quishing, never scan any unsolicited QR code and review a QR code's URL carefully. Be sure that the URL matches the website you are expecting to visit before opening it.

Phishing Checklist:

- ☐ Avoid clicking on links and delete and block the sender of unwarranted emails.
- ☐ Block unwanted text messages and callers.
- ☐ Practice not picking up the phone unless you recognize the caller. If it is someone you indeed know, they can leave you a voicemail.
- ☐ Limit the amount of personal information you have posted publicly (phone number, email address, physical address, etc.)
- ☐ Stay cautious of QR codes and unfamiliar places that might ask you to scan the code. Ensure the URL link matches the correct site before continuing to that page through the QR code scan.