Fortra | Terranova Security | Microsoft Security

7 ways to protect yourself from phishing

Phishing is a scam where criminals try to get information or access through deception and trickery. Scammers will pretend to be a business or person you trust, or they may disguise their malware into something that looks innocent in hopes you'll install it onto your system.

Common phishing attacks

Content injection

This type of phishing attack injects a familiar website, such as an email login page or an online banking portal, with malicious intent. This can include a link, form, or pop-up that directs users to a secondary website, where they're asked to input confidential information.

Link manipulation

A phishing scam can sometimes come in the form of a malicious link that appears to come from a trusted source, like big companies and famous brands. If the link is clicked, it takes users to a spoofed website, where they are prompted to enter account information.

Email

By far the most common tactic on this list, a phishing email may arrive to either your personal or professional email address. This email can include instructions to follow, a web link to click, or an attachment to open.

Man-in-the-middle

Man-in-the-middle phishing attacks occur when a cybercriminal tricks two people into sending information to each other. The scammer may send fake requests or alter the data being sent and received by each party.

Spear phishing

A more advanced form of phishing, spear phishing targets specific individuals rather than random targets.

Falling for a phishing attack can lead to leaked confidential information, infected networks, financial demands, corrupted data, or worse, so here's how to prevent that from happening:

1

Inspect the sender's email address. Is everything in order? A misplaced character or unusual spelling could signal a fake.

2

Be wary of emails with generic greetings ("Dear customer," for example) that asks you to act urgently.

3

Look for verifiable sender contact information. If in doubt, do not reply. Start a new email to respond instead.

4

Never send sensitive information by email. If you must convey private information, use the phone.

5

Think twice about clicking unexpected links, especially if they direct you to sign into your account. To be safe, log in from the official website instead.

6

Avoid opening email attachments from unknown senders or friends who do not usually send you attachments.

7

Install a phishing filter for your email apps and enable the spam filter on your email accounts.

Explore more cybersecurity awareness topics and skilling opportunities at https://aka.ms/cybersecurity-awareness.

Fortra | Terranova Security | Microsoft Security