Think Before You Click

Social engineering is a general term used to describe how bad actors manipulate individuals into giving them access to personal information. Phishing is the most common form of social engineering for stealing an individual's personal information. But it's not the only threat, as more and more malware can be used for various purposes, including ransomware attacks.

300% Rise in ransomware attacks in the US in the past year.

94% Of malware on computers found their way there via phishing email.

67.5% Of individuals that click on a phishing link are likely to enter their credentials on a phishing website.

2 Million+ Phishing sites have been found and registered as malicious by Google as of January 2021.

Phishing attacks are easier to avoid when you know how to spot them.

It only takes one wrong move for cybercriminals to access your data or your company's systems. Protect yourself, your family, and your organization by learning how to recognize common phishing tactics.

Email Phishing
An email sent with the intention of deceiving you to act, such as updating a password or clicking on an attachment.

96% of all phishing attacks come via email.4

Smishing
Phishing via text. The fraudulent text may appear to come from a reputable business, but is designed to trick you into revealing personal information.

Vishing
Also known as voice phishing occurs via phone. The caller typically leaves an "urgent" message, making recipients believe they will be fined or miss out on a potential windfall if they don't respond immediately.

Evil Twin Hotspots
Fraudulent Wi-Fi access points designed to trick users to connect to them so they can steal sensitive information or redirect links to malicious sites.

Pop-up Phishing
Fraudulent messages that "pop up" on otherwise legitimate websites that have been infected with malicious code and entice you to click on them to corrupt your device or data.

Angler Phishing
Targets social media users. Bad actors will direct message disgruntled customers, pretending to be customer service agents, to obtain personal information or other account credentials.

Social engineering is a general term used to describe how bad actors manipulate individuals into giving them access to personal information. Phishing is the most common form of social engineering for stealing an individual's personal information. But it's not the only threat, as more and more malware can be used for various purposes, including ransomware attacks.

Don't take the bait. Verify before you act.

Avoid unknown senders. Check the sender name and email address before responding.

Don't open risky links or attachments in untrusted emails.

Be suspicious of emails marked "urgent.

Consider before clicking on a link to a website that looks legitimate by checking the URL in your browser's Address bar.

Don't be lured by "deals." They are usually too good to be true.

Understand your service provider's policy for tracking and stopping phishing.

Be wary of generic greetings, such as dear sir or ma'am.

Don't give stranger or unsolicited help access to your computer.

It's time to rethink email security. Don't take the bait. Verify before you act. Here's how.

Scam? Click here for more information about the Anatomy of a Modern Phishing Attack

Secure email is the first line of defense against cybercrime. Cisco Secure Email rapidly detects, quarantines, investigates, and remediates phishing and other cyberattacks that target your email. Plus, our built-in SecureX platform, included with each email license, provides enhanced visibility, automation, and a layered approach to security across all of our Cisco Secure products.

Learn more

© 2021 Cisco and/or its affiliates. All rights reserved.