Phishing Scams and How to Avoid Them

What is phishing?

Phishing is a type of scam where cybercriminals fool unsuspecting victims into either downloading malware or turning over personal information like credit card numbers, social security numbers, and passwords—sometimes even directly asking for money. They are literally “fishing” for data, but using phony appearances, hence the “ph” spelling.

What You Should Know

Phishing is a scam aimed at tricking you to hand over private information to criminals.

What You Can Do

Be suspicious of unusual or irregular emails and don’t provide private information to any unverified source.

How phishing works:

Cybercriminals often masquerade as legitimate businesses, using email, text message and phone calls to target their victims for info.

An attacker will pose as a credit card company or financial institution or charity.

Victims will get an email saying there is some problem.

Victims are usually asked to click on some link and supply their account information or access to your computer to clear it up.

The link is a fake site that sends the info straight to the attacker, who can now access your real accounts.

How To Spot a Phishing Email

Phishing takes a variety of forms—spear phishing, whaling, vishing, all falling into the “social engineering” category of attack. What they all share in common is these attacks, unlike malware, require the victim to take an action of some kind that results in personal info being exposed. The most common types of “bait” used in phishing scams are:

- An email containing an unknown link and a message urging you to click
- An email masquerading as a “security update”
- A suspicious attachment that you are asked to open and review
- A request asking you to log in to a familiar account or provide personal data so the sender can “verify” your information
- Some form of call-to-action that requires “immediate attention” and action
- A text message from an unknown sender asking you to take some action and/or provide information so you can claim an award
- A phone call from an unknown, unidentified or unverified phone number requesting personal or work related information
- A call from a bank or helpdesk organization asking for PIN, account information or login credentials

Did You Know

In 2015, 53% of overall emails were spam, and 1 out of 1846 was a phishing attempt.

How To Avoid Becoming a Phishing Victim

Trust your instincts
If an email seems suspicious, delete it without opening.

Don't send personal or financial information to anyone
As a general rule, don't reveal personal or financial information to anyone unless you know them. Do not respond to email or text solictations for this information.

Use secure sites beginning with "https://"
If you are sending sensitive information over the internet, check the security of the website by making sure the website's URL uses "https://" instead of "http://". Often there is a lock icon or other indication preceding the URL signaling that the webpage is secured.

Verify the website's URL
Malicious websites often look identical to a legitimate site (like your bank) but the URL may be spelled slightly different or a different domain is used (e.g. .com vs.net)

Contact the company directly
If you are not sure if a request is legitimate, verify by contacting the company directly. Look up the contact information from a statement or other communication you may have. Do not use the info provided in the suspicious email.

Wait before you act
Be very suspicious of communications that require “Immediate action!”

Keep your computer up to date
As a general rule it is always best practice to install OS updates and other app updates as they become available in order to have the latest security protection.

Review the greeting
Know the difference between a generic salutation or inconsistent greeting you receive. If it seems odd or out of place, it probably is.

Check for mistakes
Errors in grammar and spelling can indicate a phishing attempt, as these often come from foreign countries where English is a second language.

Always question attachments
Know what you’re opening and make sure it’s from a reliable source. If you’re not sure, pick up the phone and check.

Look before you click
If a link is included, scroll over it and the destination address will appear. Validate that the link and the destination address match.

Do some research
Known phishing attacks are tracked and identified by groups like the Anti-Phishing Working Group. You can also report phishing to the Anti-Phishing Working Group (APWG).