**What is it Phishing**

Phishing is a cyber crime that leverages deceptive emails, websites, and text messages to steal confidential personal and corporate information.

Victims are tricked into giving up personal information such as their credit card data, phone number, mailing address, company information, etc. This information is then used by criminals to steal the victim’s identity and commit further crimes using this stolen identity.

Criminals who use phishing tactics are successful because they carefully hide behind emails and websites familiar to the intended victim. For example, the email address might be administrator@paypal.org.com instead of administrator@paypal.com and urge the recipient to update their account credentials to protect them from fraud.

Phishing is a type of social engineering that criminals use to steal data, infect computers, and infiltrate company networks.

**Email**

This is the most common phishing tactic. An email is sent to multiple recipients urging them to update personal information, verify account details, or change passwords.

Typically, the email is worded to promote a sense of urgency, sometimes highlighting the recipient’s need to protect themselves or their organization. The email is designed to appear to come from a legitimate source, such as customer service for PayPal, Apple, Microsoft, a bank, or other known companies.

**Content Injection**

A familiar-looking webpage, like an email account login page or online banking page, is injected with malicious content. The content can include a link, form, or pop-up that directs people to a secondary website where they are urged to confirm personal information, update credit card details, change passwords, etc.

**Link Manipulation**

A carefully worded email arrives with a malicious link to a familiar website such as Amazon or another popular website. When the link is clicked, it takes people to a fake website designed to look exactly like the known website, where they are then prompted to update their account information or verify account details.

**Fake Websites**

Hackers create fake websites that look just like a highly frequented website. This fake website has a slightly different domain, for example, outlook.you.live.com instead of outlook.live.com. People believe they’re on the right website and accidentally open themselves to identity theft

**Evil Twin Wi-Fi**

A fake Wi-Fi access point is created that acts as a legitimate Wi-Fi hot spot. This tactic is common in coffee shops, airports, hospitals, or locations where people routinely need Wi-Fi access. People log into this Wi-Fi access point thinking they’re using the legitimate spot, allowing criminals to intercept any data communicated on this fake Wi-Fi account.

**See it so you don’t click it.**

The signs can be subtle, but once you recognize a phishing attempt you can avoid falling for it. Before clicking any links or downloading attachments, take a few seconds (like literally 4 seconds) and ensure the email looks legit. Here are some quick tips on how to clearly spot a phishing email:

* Does it contain an offer that’s too good to be true?
* Does it include language that’s urgent, alarming, or threatening?
* Is it poorly crafted writing riddled with misspellings and bad grammar?
* Is the greeting ambiguous or very generic?
* Does it include requests to send personal information?
* Does it stress an urgency to click on an unfamiliar hyperlinks or attachment?
* Is it a strange or abrupt business request?
* Does the sender’s e-mail address match the company it’s coming from? Look for little misspellings like pavpal.com or anazon.com.

**Uh oh! I see a phishing email. What do I do?**

Don’t worry, you’ve already done the hard part, which is recognizing that an email is fake and part of a criminal’s phishing expedition.

If you’re at the office and the email came to your work email address, report it to your IT manager or security officer as quickly as possible.

If the email came to your personal email address, don’t do what it says. Do not click on any links – even the unsubscribe link – or reply back to the email. Just use that delete button. Remember, DON’T CLICK ON LINKS, JUST DELETE.

You can take your protection a step further and block the sending address from your email program.

<https://staysafeonline.org/resources/phishing/>

https://terranovasecurity.com/what-is-phishing/