PHISHING

Different Types of Phishing

Social engineering is a common tactic used in all forms of phishing to persuade victims to act, however, there are other techniques and targets outside email:

> **Vishing:** which is short for "voice phishing," describes spam calls in which a caller poses as a representative of the victim's bank or police enforcement in an effort to obtain personal information.
>
> **Smishing:** is when an attacker sends a malicious link through text message, they are said to be "smishing," short for "SMS phishing."

Whom it targets is another way to classify phishing. In an effort to catch a victim in a large net, many phishing efforts send out bulk spam emails to people and organizations. However, there are situations when an attacker designates a specific target and emails that target specifically. Spear phishing is what this is. Whaling is used when the target is highly sought-after, such as the CEO of a firm.

Phishing uses humans as its initial attack vector, whether it's employed to mislead a victim into paying money, collect login information, or download malware.

How Does Phishing Work?

Phishing attempts can occasionally be as simple as emails or phone calls that ask the victim to give money or personal information to the attacker. Others call for much more technical skill, including those that persuade users to click on links that download malware onto their devices. For instance, an attacker may socially engineer a user into downloading and opening a PDF or Word document that has malicious code included in it or attach it to a phishing email.

The ability to spread the infection by sending more phishing emails to the user's contacts is frequently included in this harmful code.

Email Spoofing

When an attacker forges email headers to make it appear as though the email is coming from someone else, this is known as email spoofing. Up to 90% of email fraud assaults employ spoofing, which is a prevalent component of phishing emails.

Normally, the "from" field is already filled up when you send an email. My acquaintance will be able to tell that I sent an email to them if I use the email address john johnson[@]gmail[.]com. But you can also send emails using straightforward scripts (here are instructions for sending an email in Python).

When you write and send an email using a programming script, you can configure the email headers to be whatever you want - meaning that an attacker can put any email as the “sender”, even yours.

In order to really see what is going on in an email, you can download it and open it in a code editor, but most email providers allow you to see the email headers from within your email. For instance, with Gmail, you may view the email headers if you open an email that piques your curiosity, click on the three vertical dots in the top right corner, and select "Show original."

These email headers provide crucial data that can be used to identify phishing, such as the "return-to" address, sender IP, and whether any anti-spoofing measures like SPF and DKIM were ineffective (they are the reason emails are automatically sent to your spam folder). Before responding to a suspicious email, it is always advisable to read the headers to check for "failed" protection fields and to see the original sender's IP.

Not Just Emails: Webpages That Steal Your Password

Particularly successful phishing tactics are websites that collect login information. The user is unaware they were phished because these pages frequently direct users to legitimate websites after collecting their login information. These websites may also tempt you to unknowingly download malware.

A typo-squatting domain like iceconsulting.cm or icconsulting.com could be used to steal ICE Consulting logins if a user types in the erroneous domain on purpose. To entice someone to click through to a hidden domain, a malicious actor could potentially mask their domain with a link shortener like bitly.

Conclusion

Phishing is a challenging issue to deal with because to the wide range of phishing kinds, the low cost to construct phishing pages, and the simplicity with which one can do so. Furthermore, no system in the world can guarantee against a human employee clicking on a bad link, regardless of how sophisticated it is. As a result, it's critical to report any questionable emails or links to the relevant department at work so that they can block the senders and sites. One person can do a lot to defend a business and oneself against phishing attempts if they pay attention to the little things and report questionable content.