PHISHING

WHAT IS PHISHING?

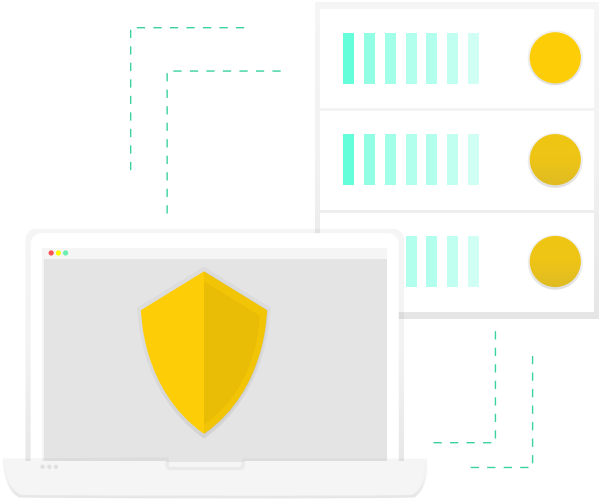
Phishing refers to any attempt to obtain sensitive information such as usernames, passwords, or banking details, often for malicious reasons, by impersonating a trustworthy source in an electronic communication.

Phishing is an example of a social engineering technique used to mislead users and exploit weaknesses in network security. Various attempts have been made to control the increase in reported phishing cases, include legislation, employee and general user training, public education, and standardized network security protocols.

Phishing is typically carried out by direct digital communication – like in an email. An attack will often direct users to enter sensitive information at a fake website, the look and feel of which matches a legitimate site. Correspondence, claiming to have originated from social media, auction or retail sites, financial institutions, network and IT administrators, company executives, or finance departments are used to trap users. Phishing emails may even contain links to distributed malware, further damaging a victim's system.

WHY IT'S IMPORTANT TO EDUCATE EVERYONE ABOUT PHISHING

Phishing is the largest threat to enterprises today with over 90% of all cyberattacks beginning with a phishing email. A successful phishing attack can not only cost money, it can open a company up to much greater security and data breaches, and destroy a company's reputation in a single click. That is why training and education are so important, as they can greatly reduce the rate of successful phishing attacks.



PHISHING TYPES

In addition to standard phishing techniques, specific types of phishing can be used to accomplish various objectives.

- **Spear phishing:** An email-spoofing attack that targets a specific organization or individual, seeking unauthorized access to sensitive information. Attackers usually gather personal information about the intended target to increase their chance of success.
- **Clone phishing:** Where an authentic, previously valid email has its content and recipient address stolen, reverse engineered to create an identical or cloned email. Any real attachments or links in the original email are replaced with malicious software, and then sent from a spoofed email address to trick the victim into believing its authenticity.
- **Whaling:** A phishing attack crafted to target an upper manager or executive based on the person's role in the company. The content of a whaling attack email is often written as a legal subpoena, customer complaint, or executive issue. Whaling scam emails are designed to masquerade as a critical business email, sent from a legitimate business authority.

HOW TO SPOT A PHISH – COMMON FEATURES

It's important to be able to recognize the most common aspects of a phishing attack. Users are often the only reason that phishing attacks are successful, so avoiding major pitfalls can help businesses avoid cyber security threats.

- **Dramatic Statements:** Lucrative offers and eye-catching or attention-grabbing statements are designed to attract people's attention immediately. For instance, many claim that a target won a phone, a lottery, or some other lavish prize.
- **Urgency:** A common tactic among cybercriminals is to ask the victim to act quickly before an opportunity ends. Most reliable organizations give ample time before they terminate an account and they never informally ask their users to update personal details over the Internet.
- **Hyperlinks:** A link may not be all it appears to be. Hovering over a link shows the actual web address URL, and it could be totally unrelated to the link text. Sometimes it might appear to be a safe website, but with slightly altered spelling – for example, with the number "1" replacing a lowercase "L". This is the main way to avoid a phishing scam.
- **Attachments:** Unexpected attachments in emails should be treated with suspicion. They often contain payloads like ransomware or other viruses.
- **Unusual Sender:** Low level spam will often be sent by unknown or suspect sounding users. When receiving an email from someone unknown, who seems to be acting suspiciously, practice control in responding too quickly, if at all. Check the email address of the sender, not just their name, to make sure it has come from a safe sender.

AVOIDING PHISHING ATTACKS

- **Social Responses:** Training people to recognize phishing attempts, and deal with them. Education can be effective, especially where training emphasizes conceptual knowledge.
- **Browser Alerts:** Maintain a list of known phishing sites and check websites against the list. One such service is the Safe Browsing service provided by Google Chrome.
- **Eliminating Phishing Mail:** Specialized spam filters that greatly reduce the number of phishing emails within a person's email inbox.
- **Monitoring and Takedown:** Round-the-clock services to monitor, analyze and assist in shutting down phishing websites.
- **Transaction Verification and Signing:** Using a mobile phone (smartphone) or alternate email address as a backup channel for authentication and authorization of sensitive interactions (like financial transactions).