Phishing

Phishing is a form of *social engineering* where attackers deceive people into revealing *sensitive information* or installing
malware such as *ransomware*. Phishing attacks have become incresingly sophisticated and often transparently mirror the site being
targeted, allowing the attacker to observe everything while the victim is navigating the site, and traverse any additional security
boundaries with the victim. As of 2020, it is the most common type of cybercrime, with the *FBI's Internet Crime Complaint Centre*
reporting more incidents of phishing than any other type of computer crime.

The term "phishing" was first recorded in 1995 in the *cracking* toolkit *AOHell*, but may have been used earlier in the hacker
magazine *2600*. It is a variation of fishing and refers to the use of lures to "fish" for sensitive information.

Measures to prevent or reduce the impact of phishing attacks include *legislation*, user education, public awareness, and technical
security measures. The importance of phishing of phishing awareness has increased in both personal and professional settings, with
phishing attacks among businesses rising from 72% to 86% from 2017 to 2020.

###**Types**############ ##

Email Phishing
Phishing attacks, often delivered via **email spam**, attempt to trick individuals into giving away sensitive information or login
credentials. Most attacks are "bulk attacks" that are not targeted and are instead sent in bulk to a wide audience. The goal of the
attacker can vary, with common targets including financial institutions, email, and cloud productivity providers, and streaming
services. The stolen information or access may be used to steal money, install **malware**, or spear phish others within the target
organization. Compromised streaming service accounts may also be sold on **darknet markets**.

Spear Phishing
Spear Phishing is a targeted attack that uses personalized emails to trick a specific individual or organization into believing thay
are legitimate. It often utilizes personal information about the target to increase the chances of success. These attacks often target
executives or those in financial departments with access to sensitive financial data and services. Accountancy and audit firms are
particularly vulnerable to spear phishing due to the value of the information their employees have access to.

Threat Group-4127 (Fancy Bear) targeted **Hillary Clinton's** campaign with spear phishing attacks on over 1,800 **Google**
accounts, using the accounts-google.com domain to threaten targeted users.

A study on spear phishing susceptibility among different age groups found that 43% of 100 young and 58 older users clicked on simulated phishing links in daily emails over 21 days. Older women had the highest susceptibility, while susceptibility in young users declined over the study, but remained stable in older users.

Whaling and CEO Fraud

Whaling attacks use spear phishing techniques to target senior executives and other high-profile individuals with customized content, often related to a **subpoena** or customer complaint.

CEO fraud involves sending fake emails from senior executives to trick employees into sending money to an offshore account. It has a low success rate, but can result in organizations losing large sums of money.

Voice Phishing

Voice over IP (VoIP) is used in **vishing** or **voice phishing** attacks, where attackers make automated phone calls to large numbers of people, often using **text-to-speech** synthesizers, claiming fraudulent activity on their accounts. The attackers spoof the calling phone number to appear as if it is coming from a legitimate bank or insitution. The victim is then prompted to enter sensitive information or connected to a live person who uses **social engineering** tactics to obtain information. Vishing takes advantage of the public's lower awareness and trust in voice telephony compared to email phishing.

SMS Phishing

SMS Phishing or **smishing** is a type of phishing attack that uses **text messages** from a cell phone or **smartphone** to deliver a bait message. The victim is usually asked to click a link, call a phone number, or contact an **email** address provided by the attacker. They may then be asked to provide **private information,** such as login credentials for other websites. The difficulty in identifying illegitimate links can be compounded on mobile device due to the limited display of URLs in mobile browsers. Smishing can be just as effective as email phishing, as many smartphones have fast internet connectivity. Smishing messages may also come from unusual phone numbers.

##**Techniques**##

Link Manipulation

Phishing attacks often involve creating fake **links** that appear to be from a legitimate organization. These links may use **misspelled URLs** or **subdomains** to deceive the user. In the following example URL, http://www.yourbank.example.com/, it can appear to the untrained eye as though the URL will take the user to the *example* section of the *yourbank* website; actually this URL points to the "yourbank" (i.e. phishing) section of the *example* website. Another tactic is to make the displayed text for a link appear trustworthy, while the actual link goes to the phisher's site. To check the destination of a link, many email clients and web

browsers will show the URL in the status bar when the **mouse** is hovering over it. However, some phishers may be able to bypass
this security measure.

Internationalized Domain Names (IDNs) can be exploited via **IDN Spoofing** or **homograph attacks** to allow attackers to create
fake websites with visually identical addresses to legitimate ones. These attacks have been use by phishers to disguise malicious URLs
using open **URL Redirectors** on trusted websites. Even digital certificates, such as **SSL**, may not protect against these attacks
as phishers can purchase valid certificates and alter content to mimic genuine websites or host phishing sites without SSL.

Filter Evasion
Phishers have sometimes used images instead of text to make it harder for anti-phishing filters to detect the text commonly used in
phishing emails. In response, more sophisticated anti-phishing filters are able to recover hidden text in images using **optical
character recoginition (OCR)**.

Social Engineering
Phishing often uses **social engineering** techniques to trick users into performing actions such as clicking a link or opening an
attachment, or revealing sensitive information. If often involves pretending to be a trusted entity and creating a sense of urgency,
like threatening to close or seize a victim's bank or insurance account.

An alternative technique to impersonation-based phishing is the use of **fake news** articles to trick victims into clicking a
malicious link. These links often lead to fake websites that appear legitimate, but are actually run by attackers who may try to
install malware or present fake "virus" notifications to the victim.