PHISHING ATTACK

"Protection of computer systems and data from digital threats."

Apsana.G.Dange

What is Phishing?

Phishing email messages, websites, and phone calls are designed to steal money or sensitive information. Cybercriminals can do this by installing malicious software on your computer, tricking you into giving them sensitive information, or outright stealing personal information off of your computer.

Types of Phishing Attacks

Social Engineering

Link Manipulation

Spear phishing

Voice phishing

Clone phishing

Social Engineering -

On your Facebook profile or LinkedIn profile, you can find: Name, Date of Birth, Location, Workplace, Interests, Hobbies, Skills, your Relationship Status, Telephone Number, Email Address and Favorite Food. This is everything a Cybercriminal needs in order to fool you into thinking that the message or email is legitimate

Link Manipulation

Most methods of phishing use some form of deception designed to make a link in an email appear to belong to the spoofed organization or person. Misspelled URLs or the use of subdomains are common tricks used by phishers. Many email clients or web browsers will show previews of where a link will take the user in the bottom left of the screen or while hovering the mouse cursor over a link

Spear phishing

Phishing attempts directed at specific individuals or companies have been termed spear phishing. Attackers may gather personal information (social engineering) about their targets to increase their probability of success. This technique is, by far, the most successful on the internet today, accounting for 91% of attacks.

Clone phishing

A type of phishing attack whereby a legitimate, and previously delivered email containing an attachment or link has had its content and recipient address(es) taken and used to create an almost identical or cloned email. The attachment or link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender.

Voice Phishing

Voice phishing is the criminal practice of using social engineering over the telephone system to gain access to personal and financial information from the public for the purpose of financial reward. Sometimes referred to as 'vishing', Voice phishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.

Voice Phishing

Voice phishing is the criminal practice of using social engineering over the telephone system to gain access to personal and financial information from the public for the purpose of financial reward. Sometimes referred to as 'vishing’, Voice phishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.

Examples of Phishing Attacks Spear Phishing

Email phishing
An attacker sends a legitimate-looking email that tricks the recipient into giving out information. The information may be used to steal or sell the recipient's data.

Spear phishing
An employee receives an email that appears to be from a colleague or manager, asking for sensitive information or urgent action. The email may reference specific projects or internal processes.

Smishing
A criminal sends a text message that appears to be from a company, such as a bank, asking for account information. The criminal may also send links to websites where they can steal the information.
Vishing

Vishing

A hacker uses a voice call to disguise themselves and get the victim's personal information. For example, the hacker may pose as a bank employee or someone from a company like Microsoft and tell the victim they've found a virus on their computer.

Whaling

Attackers target a "big fish", like a CEO, and spend time profiling the target to steal their login credentials.

Bulk phishing

Cybercriminals send fraudulent messages in bulk that make false promises, such as the recipient has won money, qualified for a refund, or their account is delinquent.

Clone phishing

An attacker creates a nearly identical replica of a previously received email, complete with malicious links or attachments.

CONCLUSION

Phishing is a form of scam in which an attacker poses as a legitimate entity or person via email or other forms of communication.