

Phishing Attacks

Presented by Dhanyasree T

Overview

01 Introduction

02 Social Engineering

03 Types of Phishing

04 Email Phishing

05 Spear Phishing

06 Smishing

07 Vishing

08 Pharming attacks

09 Whaling attacks

10 Clone Phishing

11 Search Phishing

12 Social Media Phishing

What are Phishing attacks?

Introduction

Phishing attacks are fraudulent attempts by malicious individuals or groups to deceive recipients into revealing sensitive information, such as passwords, credit card numbers, or personal identification details. These attacks typically occur through electronic communication channels like email, text messages, or instant messages, where the attacker impersonates a trusted entity, such as a bank, government agency, or reputable organization.



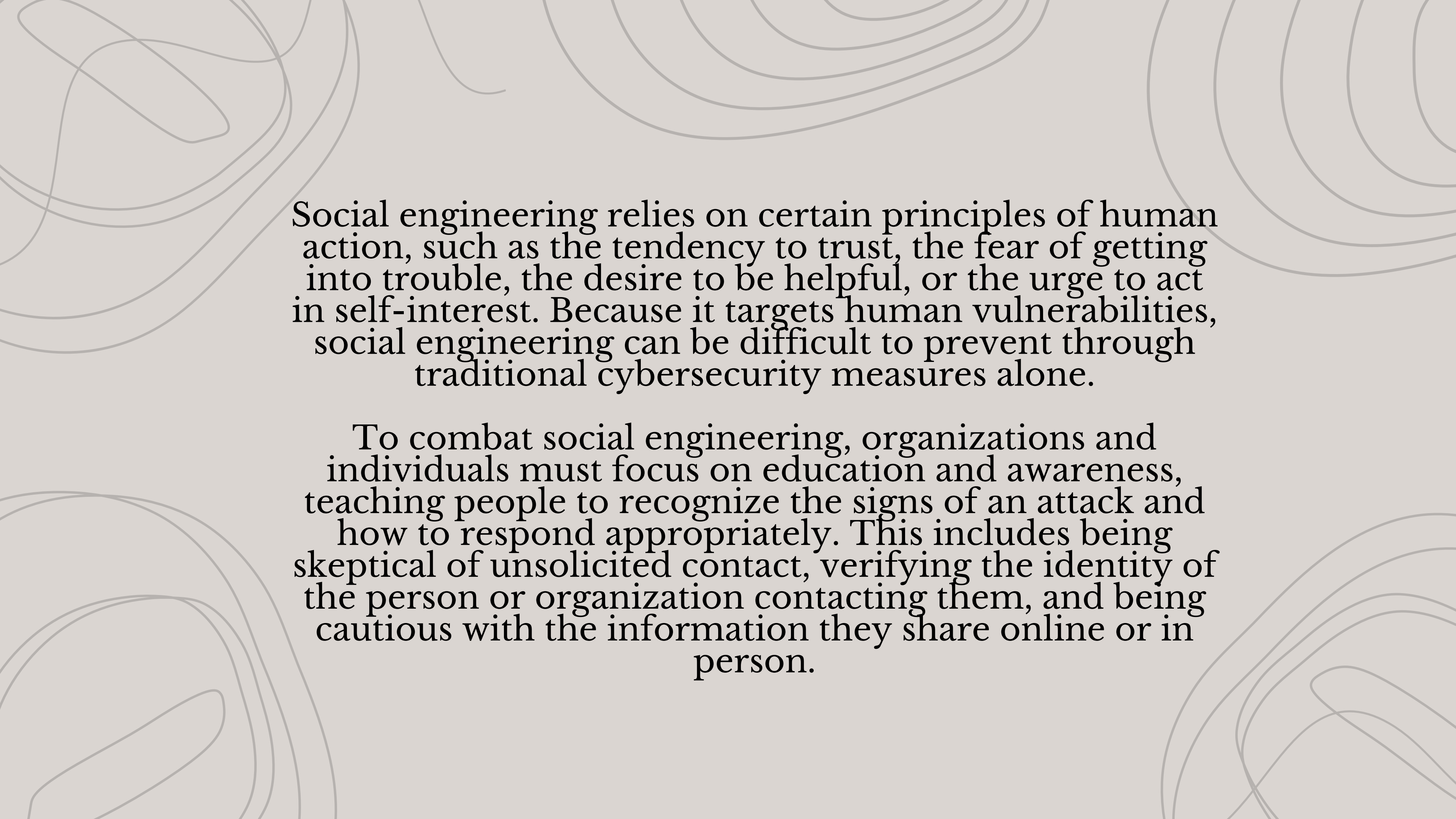
Phishing attacks are fraudulent attempts by malicious individuals or groups to deceive recipients into revealing sensitive information, such as passwords, credit card numbers, or personal identification details. These attacks typically occur through electronic communication channels like email, text messages, or instant messages, where the attacker impersonates a trusted entity, such as a bank, government agency, or reputable organization.

Phishing attacks often employ social engineering tactics to manipulate recipients into taking action, such as clicking on malicious links, downloading infected attachments, or providing confidential information. The ultimate goal of phishing attacks is to exploit the trust of the victim and obtain valuable information that can be used for identity theft, financial fraud, or other malicious purposes.

What is Social Engineering?

Social engineering is a manipulation technique that exploits human psychology, rather than technical hacking methods, to gain access to buildings, systems, or data. Essentially, it involves tricking people into breaking normal security procedures. It's a term widely used in the context of information security but applies to various forms of scamming, fraud, and cyber deception. Social engineers manipulate individuals into divulging confidential information or performing actions that may result in a security breach.





Social engineering relies on certain principles of human action, such as the tendency to trust, the fear of getting into trouble, the desire to be helpful, or the urge to act in self-interest. Because it targets human vulnerabilities, social engineering can be difficult to prevent through traditional cybersecurity measures alone.

To combat social engineering, organizations and individuals must focus on education and awareness, teaching people to recognize the signs of an attack and how to respond appropriately. This includes being skeptical of unsolicited contact, verifying the identity of the person or organization contacting them, and being cautious with the information they share online or in person.

Types of Phishing Attacks:

01 Email Phishing

02 Spear Phishing

03 Smishing

04 Vishing

05 Pharming

06 Whaling

07 Clone Phishing

08 Search Engine Phishing

09 Social Media Phishing

Email Phishing:

Email phishing is a type of cyberattack where attackers send fraudulent emails to individuals or organizations, masquerading as legitimate entities such as banks, social media platforms, or government agencies. Email phishing aims to trick recipients into divulging sensitive information such as usernames, passwords, and credit card numbers, or to prompt them to perform actions that compromise their security, such as clicking on malicious links or downloading malware-infected attachments.

Here's how email phishing typically works:

1. **Creation of Deceptive Emails:** Attackers craft convincing emails designed to appear as if they were sent from a trusted source. They often use logos, formatting, and language that mimic legitimate correspondence to increase the likelihood of fooling recipients.
2. **Sense of Urgency or Fear:** Phishing emails often create a sense of urgency or fear to prompt recipients into taking immediate action. For example, they may claim that there is a problem with the recipient's account that requires urgent attention, such as a security breach or a pending account suspension.
3. **Inclusion of Malicious Links or Attachments:** Phishing emails typically contain links to fake websites or malicious attachments. These links may direct recipients to counterfeit login pages where their credentials are stolen, or to websites that install malware on their devices without their knowledge. Attachments may contain malware such as ransomware, spyware, or keyloggers.
4. **Social Engineering Tactics:** Phishing emails often employ social engineering tactics to manipulate recipients into trusting the sender and complying with their requests. This may involve using familiar or authoritative language, impersonating colleagues or superiors, or referencing current events to increase the email's credibility.

4. Spoofed Sender Information: Attackers frequently spoof the sender's email address to make it appear as if the email is coming from a legitimate source. However, upon closer inspection, recipients may notice discrepancies in the sender's domain or email address that reveal the email's fraudulent nature.

5. Lack of Personalization: many phishing emails are sent en masse and lack personalization. Recipients may notice generic greetings or content that does not address them by name, which can be a red flag indicating a phishing attempt.

Spear Phishing

Spear phishing is a targeted form of phishing attack in which cybercriminals personalize their fraudulent emails to specific individuals or organizations. Unlike traditional phishing attacks, which are typically sent in bulk to a large number of recipients, spear phishing emails are carefully crafted to deceive a particular target or a small group of targets. This level of customization increases the likelihood of success for the attacker, as the emails appear more legitimate and are more likely to bypass traditional security measures.

how spear phishing attacks work:

1. **Research:** Attackers conduct extensive research on their targets to gather information such as names, job titles, company affiliations, and interests. This information helps them personalize their phishing emails to make them appear more credible and convincing.
2. **Crafting the Email:** Using the information gathered during the research phase, attackers craft fraudulent emails designed to deceive the target. They may use familiar language, references to recent events, or internal company information to make the email appear legitimate and relevant to the recipient.
3. **Spoofing Sender Information:** Attackers may spoof the sender's email address to make it appear as if the email is coming from a trusted source, such as a colleague, superior, or reputable organization. By impersonating someone the target knows or trusts, attackers increase the likelihood that the recipient will fall for the scam.
4. **Social Engineering Tactics:** Spear phishing emails often employ sophisticated social engineering tactics to manipulate the recipient into taking a specific action. These tactics may include creating a sense of urgency or importance, appealing to the recipient's emotions, or exploiting their trust in known contacts.

4. Inclusion of Malicious Links or Attachments: Spear phishing emails typically contain malicious links or attachments that, when clicked or downloaded, can compromise the recipient's security. These links may lead to fake login pages designed to steal credentials or websites that install malware on the recipient's device.

5. Objective: The primary objective of spear phishing attacks is typically to steal sensitive information, such as login credentials, financial data, or intellectual property. Once the attacker has obtained this information, they may use it to launch further attacks, exploit vulnerabilities within the target organization, or sell it on the dark web.

Smishing Attack:

Smishing attacks, a portmanteau of "SMS" (Short Message Service) and "phishing," involve the use of text messages (SMS) to deceive individuals into divulging sensitive information or performing actions that compromise their security

Here's how smishing attacks typically work:

- 1. Receipt of Fraudulent Text Messages:** Individuals receive text messages on their mobile devices that appear to be from legitimate sources, such as banks, government agencies, or reputable organizations. These messages often contain urgent or enticing offers, warnings about account security, or requests for personal information.
- 2. Sense of Urgency or Fear:** Similar to email phishing, smishing messages often create a sense of urgency or fear to prompt recipients into taking immediate action. For example, they may claim that there is a problem with the recipient's bank account that requires urgent attention, or that they have won a prize that must be claimed immediately.
- 3. Inclusion of Malicious Links or Phone Numbers:** Smishing messages typically contain links to fake websites or phone numbers that recipients are instructed to call. These links may lead to counterfeit login pages where recipients are asked to enter their credentials, or to websites that install malware on their devices. Alternatively, recipients may be prompted to call a phone number where automated systems attempt to extract sensitive information from them.

- 1. Spoofing Sender Information:** Attackers may spoof the sender's phone number to make it appear as if the text message is coming from a trusted source. This can make it more difficult for recipients to recognize smishing attempts, as the messages may appear to be from familiar contacts or organizations.
- 2. Social Engineering Tactics:** Smishing messages often employ social engineering tactics to manipulate recipients into trusting the sender and complying with their requests. These tactics may include using persuasive language, posing as a legitimate authority figure, or referencing current events to increase the message's credibility.
- 3. Objective:** The primary objective of smishing attacks is typically to steal sensitive information, such as login credentials, financial data, or personal details. Attackers may use this information to commit identity theft, financial fraud, or other forms of cybercrime.

Vishing Attacks:

Vishing, short for "voice phishing," is a form of cyberattack where attackers use phone calls to deceive individuals into divulging sensitive information or performing actions that compromise their security. Vishing attacks typically involve automated voice messages or live callers impersonating trusted entities such as banks, government agencies, or tech support services.

Here's how vishing attacks work:

- 1. Initiation of the Call:** Vishing attacks may begin with an automated voice message or a live caller reaching out to the victim via phone call. The caller ID may be spoofed to make it appear as if the call is coming from a legitimate source, such as a bank or government agency, or it may be withheld altogether.
- 2. Sense of Urgency or Fear:** Similar to other forms of phishing attacks, vishing calls often create a sense of urgency or fear to prompt recipients into taking immediate action. For example, callers may claim that there is suspicious activity on the victim's bank account that requires immediate verification or that they are at risk of legal action if they do not comply with the caller's instructions.
- 3. Request for Personal Information:** During the call, the attacker may request sensitive information from the victim, such as their account credentials, social security number, or credit card details. Alternatively, they may instruct the victim to visit a fake website or call back on a fraudulent phone number to provide this information.
- 4. Social Engineering Tactics:** Vishing calls often employ social engineering tactics to manipulate victims into trusting the caller and complying with their requests. These tactics may include using persuasive language, posing as a legitimate authority figure, or exploiting the victim's fear or concern to extract information from them.

1. Spoofing Caller Information: Attackers may spoof the caller's phone number to make it appear as if the call is coming from a trusted source. This can make it more difficult for victims to recognize vishing attempts, as the calls may appear to be from familiar contacts or organizations.

1. Objective: The primary objective of vishing attacks is typically to steal sensitive information or money from the victim. Attackers may use the information obtained during the call to commit identity theft, financial fraud, or other forms of cybercrime.

Pharming Attacks:

Pharming is a type of cyberattack that involves redirecting website traffic from legitimate websites to fraudulent ones without the user's knowledge or consent. Unlike phishing, which relies on deceiving users through email or other communication channels, pharming attacks manipulate the Domain Name System (DNS) or compromise users' hosts files to achieve their goals.

how pharming attacks work:

DNS Spoofing or Cache Poisoning: One method of pharming involves attackers compromising DNS servers or poisoning their cache. DNS servers translate human-readable domain names (e.g., www.example.com) into the numerical IP addresses that computers use to connect to websites. By poisoning the DNS cache, attackers can redirect users who type in the legitimate domain name of a website to a fraudulent IP address controlled by the attacker. As a result, users unknowingly access the fake website instead of the intended legitimate one.

2. Compromising Hosts Files: Another method of pharming involves compromising the hosts files on users' computers or devices. The hosts file is a local file that maps domain names to IP addresses, allowing users to override DNS resolution for specific websites. Attackers can modify this file to redirect users attempting to access legitimate websites to fraudulent IP addresses controlled by the attacker. This way, even if the DNS is functioning properly, users will still be redirected to the fake website.

3. Creation of Fake Websites: Once users are redirected to the fraudulent website, they may encounter replicas of legitimate websites, such as banking portals, e-commerce platforms, or login pages for popular services. These fake websites are designed to closely resemble the originals to trick users into entering sensitive information, such as login credentials, credit card numbers, or personal details.

4. Data Harvesting and Exploitation: When users enter their information on the fake website, the attackers harvest this sensitive data. They may use it for various malicious purposes, such as identity theft, financial fraud, or unauthorized access to online accounts.

5. Duration and Persistence: Pharming attacks can be persistent, as they do not rely on tricking users through individual interactions like phishing. Once the DNS servers or hosts files are compromised, all users attempting to access the affected websites may be redirected to the fraudulent ones until the issue is identified and remediated.

Whaling Attacks:

Whaling attacks, also known as "whale phishing," are highly targeted cyberattacks that specifically target high-profile individuals within an organization, such as executives, CEOs, or other senior executives. The term "whaling" is derived from the idea that these individuals are considered "big fish" or "whales" in the context of the organization, making them lucrative targets for cybercriminals.

Here's how whaling attacks typically work:

- 1. Research and Selection:** Attackers conduct thorough research to identify high-profile individuals within an organization who have access to sensitive information or hold positions of authority. This may include executives, CEOs, CFOs, or other senior managers who have control over financial transactions or valuable company assets.
- 2. Personalization and Social Engineering:** Whaling attacks often involve personalized and sophisticated social engineering tactics to trick the target into divulging sensitive information or performing actions that compromise security. Attackers may use information gathered from public sources or social media profiles to craft convincing emails or messages tailored to the target's interests, responsibilities, or relationships within the organization.
- 3. Deceptive Emails or Messages:** Attackers send fraudulent emails or messages to the targeted individual, posing as trusted colleagues, business partners, or other reputable entities. These messages may appear to be urgent requests for sensitive information, such as login credentials, financial data, or confidential company information, or they may contain malicious links or attachments designed to compromise the target's device or network.

4. Spoofing Sender Information: To enhance the credibility of their phishing attempts, attackers may spoof the sender's email address or use email spoofing techniques to make it appear as if the message is coming from a legitimate source. This can make it more difficult for the target to recognize the phishing attempt and increase the likelihood of a successful compromise.

5. High-Stakes Objectives: The objectives of whaling attacks often involve stealing sensitive information, such as intellectual property, financial data, or trade secrets, or gaining unauthorized access to company systems or networks. Attackers may use the information obtained from successful whaling attacks to commit financial fraud, initiate wire transfers, or launch further cyberattacks against the organization.

Clone Phishing

Clone phishing is a type of phishing attack where cybercriminals create replicas of legitimate emails that the victim has previously received, making minor alterations to include malicious links or attachments. The altered emails are then sent to the victim, typically from an email address that closely resembles the original sender's address or a compromised email account.

Here's how clone phishing attacks typically work:

- 1 Selection of Targets:** Attackers select their targets and identify emails that the targets have previously received and are likely to trust. These emails may contain legitimate requests, invoices, or notifications from trusted sources such as banks, service providers, or colleagues.
- 2. Replication of Emails:** Attackers create exact replicas of the legitimate emails, including the sender's name, email address, subject line, and content. They may use publicly available information or previously compromised email accounts to accurately replicate the original emails.
- 3. Inclusion of Malicious Links or Attachments:** Attackers make minor alterations to the cloned emails, such as inserting malicious links or attachments disguised as legitimate documents or URLs. These links or attachments may lead to fake login pages designed to steal credentials, malware-infected websites, or phishing forms requesting sensitive information.
- 4. Delivery to Targets:** Once the cloned emails are prepared, attackers send them to the targeted individuals, often with a sense of urgency or importance to prompt quick action. The emails may appear to come from the same sender as the original emails, making them more convincing and increasing the likelihood of the victim falling for the scam.

4. Victim Interaction: If the victim falls for the scam and clicks on the malicious links or downloads the attachments, they may inadvertently compromise their security by providing sensitive information or enabling malware to infect their devices or networks.

5. Exploitation of Compromised Accounts: In some cases, attackers may compromise legitimate email accounts to send out cloned phishing emails to the victim's contacts, further spreading the phishing campaign and increasing its chances of success.

Search Engine Phishing:

Search engine phishing, also known as search engine redirection phishing, is a type of phishing attack where cybercriminals manipulate search engine results to lead users to malicious websites posing as legitimate ones. This form of phishing takes advantage of users' trust in search engine results to trick them into visiting fraudulent websites and divulging sensitive information.

Here's how Search Engine phishing attacks typically work:

1 Manipulation of Search Engine Results: Attackers use various techniques to manipulate search engine algorithms and rankings to ensure that malicious websites appear prominently in search results for specific keywords or queries. This may involve search engine optimization (SEO) tactics, such as keyword stuffing, link farms, or cloaking, to artificially inflate the rankings of fraudulent websites.

2. Creation of Fake Websites: Attackers create fake websites that closely mimic the appearance and functionality of legitimate websites, such as online banking portals, e-commerce platforms, or login pages for popular services. These fake websites are designed to deceive users into believing that they are accessing a trusted site.

3. Inclusion of Malicious Content: The fake websites created by attackers often contain malicious content, such as phishing forms, malware-infected downloads, or fake login pages designed to steal users' credentials. These elements are carefully crafted to trick users into entering sensitive information or downloading malware onto their devices.

4. Redirection from Legitimate Search Results: When users perform a search using a search engine, the manipulated search results lead them to the fraudulent websites instead of the legitimate ones they were expecting to find. This redirection occurs without the users' knowledge or consent, making it difficult for them to distinguish between legitimate and malicious websites.

5. Objective: The primary objective of search engine phishing attacks is typically to steal sensitive information, such as login credentials, financial data, or personal details, from unsuspecting users. Attackers may use this information for various malicious purposes, including identity theft, financial fraud, or unauthorized access to online accounts.

Social Media Phishing:

Social media phishing is a type of cyberattack that targets users of social media platforms, such as Facebook, Twitter, LinkedIn, or Instagram. It involves the use of deceptive tactics to trick users into divulging sensitive information or performing actions that compromise their security. Here's how social media phishing typically works:

Here's how social media phishing typically works:

1 Creation of Fake Profiles or Pages: Attackers create fake profiles or pages on social media platforms, often using stolen or fabricated identities. These profiles are designed to mimic legitimate users, businesses, or organizations to appear trustworthy to potential victims

2. Impersonation and Social Engineering: Attackers use social engineering tactics to impersonate trusted individuals, such as friends, colleagues, or reputable organizations, in messages or posts. They may send friend requests, direct messages, or comments to target users, claiming to offer enticing offers, urgent requests, or other persuasive messages to gain the victims' trust.

3. Deceptive Links or Attachments: Attackers may include malicious links or attachments in their messages or posts, directing users to phishing websites or malware-infected downloads. These links often lead to fake login pages designed to steal users' credentials, fraudulent surveys requesting personal information, or websites hosting malware.

4. Fake Contests or Promotions: Attackers may create fake contests, giveaways, or promotions on social media platforms to lure users into providing their personal information. These scams often promise valuable prizes or rewards in exchange for participation, but are designed to collect sensitive information or spread malware to participants.

4. Manipulation of User Trust: Attackers exploit users' trust in social media platforms and their connections to friends and colleagues to make their phishing attempts more convincing. By impersonating familiar individuals or organizations and leveraging social engineering tactics, attackers increase the likelihood of victims falling for their scams.

5. Objective: The primary objective of social media phishing attacks is typically to steal sensitive information, such as login credentials, financial data, or personal details, from unsuspecting users. Attackers may use this information for various malicious purposes, including identity theft, financial fraud, or unauthorized access to online accounts.

Conclusion

Phishing attacks aren't just a nuisance; they can have significant financial and personal consequences.

Individuals can lose money, sensitive data, and even become victims of identity theft. Businesses can suffer financial losses, reputational damage, and disruptions to their operations. By understanding the common tactics and taking preventive measures, we can all play a role in protecting ourselves and our organizations from these costly attacks.

Recommendation

- 1 **Be cautious with emails and messages:**
 - **Don't click links or attachments from unknown senders.** Even if the sender name or email address looks familiar, be wary if you weren't expecting a message from them.
 - **Check sender email addresses carefully.** Phishing emails often have subtle typos or use look-alike domains (e.g., gmail.com vs [invalid URL removed]).
 - **Be suspicious of urgency or threats.** Phishing emails often try to pressure you into acting quickly by creating a sense of urgency or using scare tactics.
- 2 **Verify information independently.**
 - **Don't enter personal information on websites linked to in emails or messages.** If you're unsure about a website's legitimacy, go to the official website directly by typing the address in your browser.
 - **Call the company directly to verify a message's legitimacy.** If an email claims to be from your bank or another institution, call their customer service line (using a number you know is correct) to confirm the message.

Recommendation

3. **Keep your software up to date.**
 - **Use an up-to-date web browser and antivirus software.** These can help identify and block phishing attempts.
 - **Enable pop-up blocker and spam filters.** These can help reduce the number of phishing attempts you encounter.
4. **Be mindful of social media.**
 - **Don't share too much personal information on social media.** This can make you a target for phishing attacks.
 - **Be careful about clicking on links or sharing information in social media posts.**

Recommendation

5. **Use strong passwords and enable two-factor authentication (2FA).**
 - **Use strong, unique passwords for all your online accounts.** A password manager can help you create and manage strong passwords.
 - **Enable two-factor authentication (2FA) whenever possible.** This adds an extra layer of security to your accounts, making it more difficult for attackers to gain access even if they steal your password.
6. **Be Phishing Aware and Educate Yourself:**
 - Stay informed about the latest phishing tactics. Phishing scams are constantly evolving, so it's important to be aware of the latest tricks attackers are using.
 - If you're unsure about something, it's always best to err on the side of caution and not click or respond.

Borcelle University

Thank You

Presented by Juliana Silva