Phishing Attacks

INTRODUCTION TO PHISHING

NAME-MOHIT CHOUDHARY
BRANCH-BCA (CYBERSECURITY)
SECTION- J

What is Phishing?

- Definition of phishing

- Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.
- The information is then used to access important accounts and can result in identity theft and financial loss.

- • Basic concept of tricking individuals to reveal sensitive information
- Phishing is essentially a deceptive practice where attackers trick individuals into revealing sensitive information, such as passwords, credit card numbers, or personal details. This is typically done by masquerading as a trustworthy entity in electronic communications.

How is Phishing Carried Out?

- Below mentioned are the ways through which Phishing generally occurs. Upon using any of the techniques mentioned below, the user can lead to Phishing Attacks.
- **Clicking on an unknown file or attachment:** Here, the attacker deliberately sends a mysterious file to the victim, as the victim opens the file, either malware is injected into his system or it prompts the user to enter confidential data.
- **Using an open or free wifi hotspot:** This is a very simple way to get confidential information from the user by luring him by giving him free **wifi**. The wifi owner can control the user's data without the user knowing it.
- **Responding to social media requests:** This commonly includes social engineering. Accepting unknown friend requests and then, by mistake, leaking secret data are the most common mistakes made by naive users.
- **Clicking on unauthenticated links or ads:** Unauthenticated links have been deliberately crafted that lead to a phished website that tricks the user into typing confidential data.

Types of Phishing Attacks

- • Email Phishing: Most common form, disguised as legitimate emails
- • Spear Phishing: Targeted at specific individuals or organizations
- • Whaling: Targeting high-profile individuals like executives
- • Smishing & Vishing: SMS and voice-based phishing
- Clone Phishing

Email Phishing Attacks

- **Email Phishing:** The most common type where users are tricked into clicking unverified spam emails and leaking secret data. Hackers impersonate a legitimate identity and send emails to mass victims. Generally, the goal of the attacker is to get personal details like bank details, credit card numbers, user IDs, and passwords of any online shopping website, installing malware, etc. After getting the personal information, they use this information to steal money from the user's account or harm the target system, etc.

Spear Phishing Attacks

- **Spear Phishing:** In spear phishing a phishing attack, a particular user(organization or individual) is targeted. In this method, the attacker first gets the full information of the target and then sends malicious emails to his/her inbox to trap him into typing confidential data. For example, the attacker targets someone(let's assume an employee from the finance department of some organization). Then the attacker pretends to be like the manager of that employee and then requests personal information or transfers a large sum of money. It is the most successful attack.

Whaling

- A **whaling attack** is a type of **phishing** cyberattack that targets high-profile individuals within an organization, such as CEOs, CFOs, or other executives. These individuals, sometimes referred to as "whales" in the business world due to their influential roles, are targeted with emails or other communication that appears to be legitimate, often mimicking internal or trusted sources.

- Whaling attacks usually aim to:

- Steal sensitive information (e.g., financial details, trade secrets).
- Trick the executive into transferring large sums of money.
- Install malware onto the executive's computer system.

- These attacks are often highly personalized, taking advantage of public information about the executive, such as their name, job role, and other personal details to make the phishing attempt more convincing.

Key characteristics of whaling

- **Key characteristics:**
- Highly targeted and personalized.
- Often involve email communication that seems urgent and important.
- The goal is to deceive the victim into making a significant error, such as sending sensitive information or wiring funds.

Difference Between Phishing, Smishing and Vishing?

- Phishing, smishing and vishing are all methods of identity fraud that differ in how scammers contact you—by email, text or phone—to steal personal details or financial account information.

What Is Smishing?

- Smishing is a kind of fraud similar to phishing, except that it comes in the form of a text message. A smishing text will often contain a fraudulent link that takes victims to a form that's used to steal their information. The link may also download malware such as viruses, ransomware, spyware or adware onto the victim's device.
- These smishing text messages may appear to be urgent requests sent from a bank or parcel delivery service, for example. They may claim that there's been a large withdrawal from your bank account, or that you need to track a missing package. It can be easy to fall for this scam if you think you must take quick action to solve an urgent problem.

What Is Vishing?

- Fraudulent calls or voicemails fall under the category of "vishing." Scammers call potential victims, often using prerecorded robocalls, pretending to be a legitimate company to solicit personal information from a victim.
- Perhaps you get a call about your car's extended warranty. If you answer this call and get connected to an alleged agent, you may be asked to provide information such as:
- First and last name
- Address
- Driver's license number
- Social Security number
- Credit card information

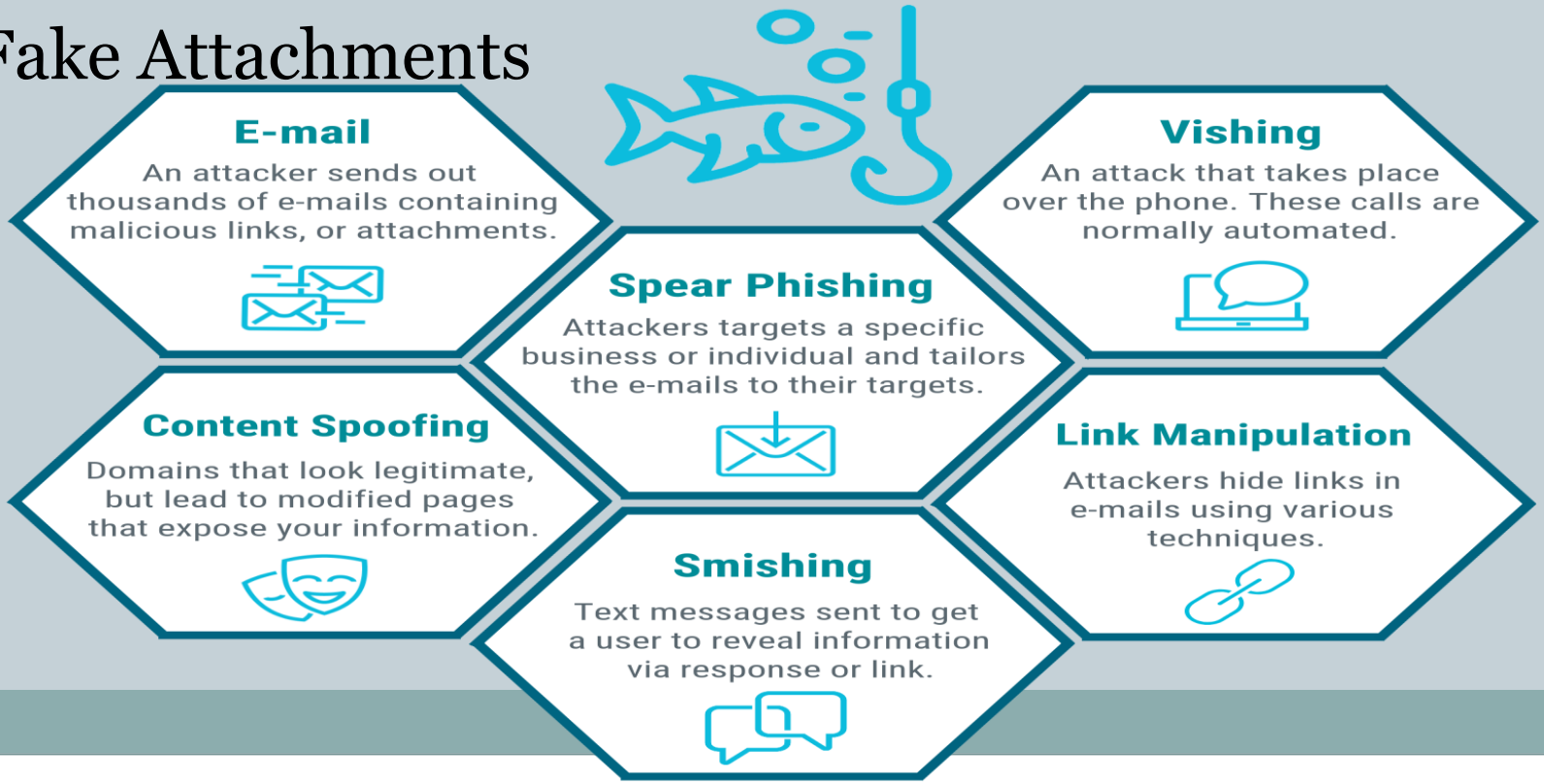
- Some scammers may also record your voice and ask a question you're likely to answer with "Yes." They can then use this recording to pretend to be you on the phone to authorize charges or access your financial accounts.

Clone Phishing Attacks

Clone Phishing: Clone Phishing this type of phishing attack, the attacker copies the email messages that were sent from a trusted source and then alters the information by adding a link that redirects the victim to a malicious or fake website. Now the attacker sends this mail to a larger number of users and then waits to watch who clicks on the attachment that was sent in the email. It spreads through the contacts of the user who has clicked on the attachment.

Techniques Used in Phishing

- • Fake Links
- • Clone Websites
- • Urgent Requests
- • Fake Attachments



Real-world Examples of Phishing Attacks

- **Estonian Cyber War (2007)**: A massive cyberattack targeted Estonia's digital infrastructure using a network of compromised computers. Nearly a million machines amplified the attack's impact.
- **HBGary Federal Attack (2011)**: Hackers associated with Anonymous infiltrated HBGary Federal, compromising sensitive data and threatening to delete backups.
- **Google and Facebook Phishing Attack (2013-2015)**: Evaldas Rimasauskas scammed Google and Facebook out of $100 million through a sophisticated phishing operation.
- **WannaCry Ransomware Attack (2017)**: This global ransomware infected around 200,000 computers in 150 countries, causing significant financial losses.
- **The NotPetya Attack (2017)**: A devastating attack that spread rapidly worldwide, resulting in over $10 billion in damages.

Consequences of Phishing Attacks

- Identity theft
- Credit card fraud
- Ransomware attacks
- Data breaches
- Financial losses
- Reputational damage
- Regulatory issues

How to Identify Phishing Attempts

- • Check the Sender's Email
- • Hover Over Links
- • Look for Grammar Mistakes
- • Too Good to be True Offers
- **Urgency and Fear Tactics**: Scammers create urgency to pressure you. They might claim your account is compromised, your payment failed, or your subscription is expiring. Be skeptical of messages that demand immediate action.

Signs of Phishing

- **Signs of Phishing**
- It is very important to be able to identify the signs of a phishing attack to protect against its harmful effects. These signs help the user to protect user data and information from hackers. Here are some signs to look out for include:

- **Suspicious email addresses:** Phishing emails often use fake email addresses that appear to be from a trusted source, but are controlled by the attacker. Check the email address carefully and look for slight variations or misspellings that may indicate a fake address.

- **Urgent requests for personal information:** Phishing attacks often try to create a sense of urgency to trick victims into providing personal information quickly. Be cautious of emails or messages that ask for personal information and make sure to verify the authenticity of the request before providing any information.

- **Poor grammar and spelling:** Phishing attacks are often created quickly and carelessly, and may contain poor grammar and spelling errors. These mistakes can indicate that the email or message is not legitimate.

- **Requests for sensitive information:** Phishing attacks often try to steal sensitive information, such as login credentials and financial information. Be cautious of emails or messages that ask for sensitive information and verify the authenticity of the request before providing any information.

- **Unusual links or attachments:** Phishing attacks often use links or attachments to deliver malware or redirect victims to fake websites. Be cautious of links or attachments in emails or messages, especially from unknown or untrusted sources.

- **Strange URLs:** Phishing attacks often use fake websites that look similar to the real ones, but have slightly different URLs. Look for strange URLs or slight variations in the URL that may indicate a fake website.

Prevention Methods

- • Use Anti-phishing Software
- • Enable Two-factor Authentication
- • Educate Users
- • Regularly Update Passwords

Protecting yourself against phishing attacks

- Familiarize yourself with common warning signs:
  - Unfamiliar greetings or tone
  - Unsolicited messages
  - Grammar and spelling errors
  - Sense of urgency
  - Suspicious links or attachments
  - Requests for personal information
  - Inconsistencies in email addresses or links
  - Unusual requests
  - Alerts claiming you've won something

How To Stay Protected Against Phishing?

- Until now, we have seen how a user becomes so vulnerable due to phishing. But with proper precautions, one can avoid such scams. Below are the ways listed to protect users against phishing attacks:
- **Authorized Source:** Download software from authorized sources only where you have trust.
- **Confidentiality:** Never share your private details with unknown links and keep your data safe from hackers.
- **Check URL:** Always check the URL of websites to prevent any such attack. it will help you not get trapped in Phishing Attacks.
- **Avoid replying to suspicious things:** If you receive an email from a known source but that email looks suspicious, then contact the source with a new email rather than using the reply option.
- **Phishing Detection Tool:** Use phishing-detecting tools to monitor the websites that are crafted and contain unauthentic content.
- **Try to avoid free wifi:** Avoid using free Wifi, it will lead to threats and Phishing.
- **Keep your system updated:** It's better to keep your system always updated to protect from different types of Phishing Attacks.
- **Keep the firewall of the system ON:** Keeping ON the firewalls helps you filter ambiguous and suspicious data and only authenticated data will reach you.

Fake and Real Website?

- **How To Distinguish Between a Fake Website and a Real Website?**
- It is very important nowadays to protect yourself from fake websites and real websites. Here are some of the ways mentioned to identify which websites are real and which ones are fake. To distinguish between a fake website and a real website always remember the following points:

- **Check the URL of the website:** A good and legal website always uses a secure medium to protect yourself from online threats. So, when you first see a website link, always check the beginning of the website. That means if a website is started with https:// then the website is secure because https:// "s" denotes secure, which means the website uses encryption to transfer data, protecting it from hackers. If a website uses http:// then the website is not guaranteed to be safe. So, it is advised not to visit HTTP websites as they are not secure.

- **Check the domain name of the website:** The attackers generally create a website whose address mimics large brands or companies like www.amazon.com/order_id=23. If we look closely, we can see that it's a fake website as the spelling of Amazon is wrong, that is amazon is written. So it's a phished website. So be careful with such types of websites.

- **Look for site design:** If you open a website from the link, then pay attention to the design of the site. Although the attacker tries to imitate the original one as much as possible, they still lack in some places. So, if you see something off, then that might be a sign of a fake website. For example, www.sugarcube.com/facebook, when we open this URL the page open is cloned to the actual Facebook page but it is a fake website. The original link to Facebook is www.facebook.com.

- **Check for the available web pages:** A fake website does not contain the entire web pages that are present in the original website. So when you encounter fake websites, then open the option(links) present on that website. If they only display a login page, then the website is fake.

Phishing Tools

- **Phishing tools** are software or techniques used by cybercriminals to conduct phishing attacks, which trick individuals into sharing sensitive information (e.g., usernames, passwords, or financial details). These tools can automate or simplify various aspects of phishing attacks, from crafting convincing emails to deploying fake websites that mimic legitimate ones.

- **Gophish**: A phishing simulation tool that helps attackers (and ethical hackers) create and manage phishing campaigns to test security awareness.
- **SET (Social-Engineer Toolkit)**: A framework used to simulate real-world social engineering attacks, including spear phishing and credential harvesting.
- **PhishX**: A phishing toolkit that provides pre-built templates for emails, fake websites, and other phishing campaigns.
- **King Phisher**: A tool used to simulate phishing attacks and assess the awareness of employees by testing their responses to malicious emails.
- **Evilginx2**: A tool that performs advanced phishing attacks by capturing login credentials and session cookies, making it possible to bypass two-factor authentication (2FA).
- **BlackEye**: A popular open-source phishing tool that automates the process of creating phishing pages to replicate well-known websites.
- **ZPhisher**: Another tool used to perform phishing attacks with ready-made templates to mimic login pages of various platforms.

- These tools are widely used for malicious purposes, as well as for ethical phishing assessments to improve cybersecurity.

Anti-Phishing Tools

- **Anti-Phishing Tools**
- Well, it's essential to use Anti-Phishing tools to detect phishing attacks. Here are some of the most popular and effective anti-phishing tools available:

- **Anti-Phishing Domain Advisor (APDA):** A browser extension that warns users when they visit a phishing website. It uses a database of known phishing sites and provides real-time protection against new threats.

- **PhishTank:** A community-driven website that collects and verifies reports of phishing attacks. Users can submit phishing reports and check the status of suspicious websites.

- **Webroot Anti-Phishing:** A browser extension that uses machine learning algorithms to identify and block phishing websites. It provides real-time protection and integrates with other security tools.

- **Malwarebytes Anti-Phishing:** A security tool that protects against phishing attacks by detecting and blocking suspicious websites. It uses a combination of machine learning and signature-based detection to provide real-time protection.

- **Kaspersky Anti-Phishing:** A browser extension that provides real-time protection against phishing attacks. It uses a database of known phishing sites and integrates with other security tools to provide comprehensive protection.

- **Note:** These anti-phishing tools can provide an additional layer of protection against phishing attacks, but it is important to remember that they are not a complete solution. Users should also be cautious of suspicious emails and messages and practice safe browsing habits to minimize their risk of falling victim to phishing attacks.

Conclusion

- **Conclusion**
- Therefore, phishing attacks are a serious problem that can steal your data. When it comes to your personal information, always confirm the person requesting for your data. If you are not sure whether the request is genuine or fraudulent, never share any personal information. Always stay alert to avoid such tricks and protect yourself from fraudsters.

Thank you !!!