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.

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

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.

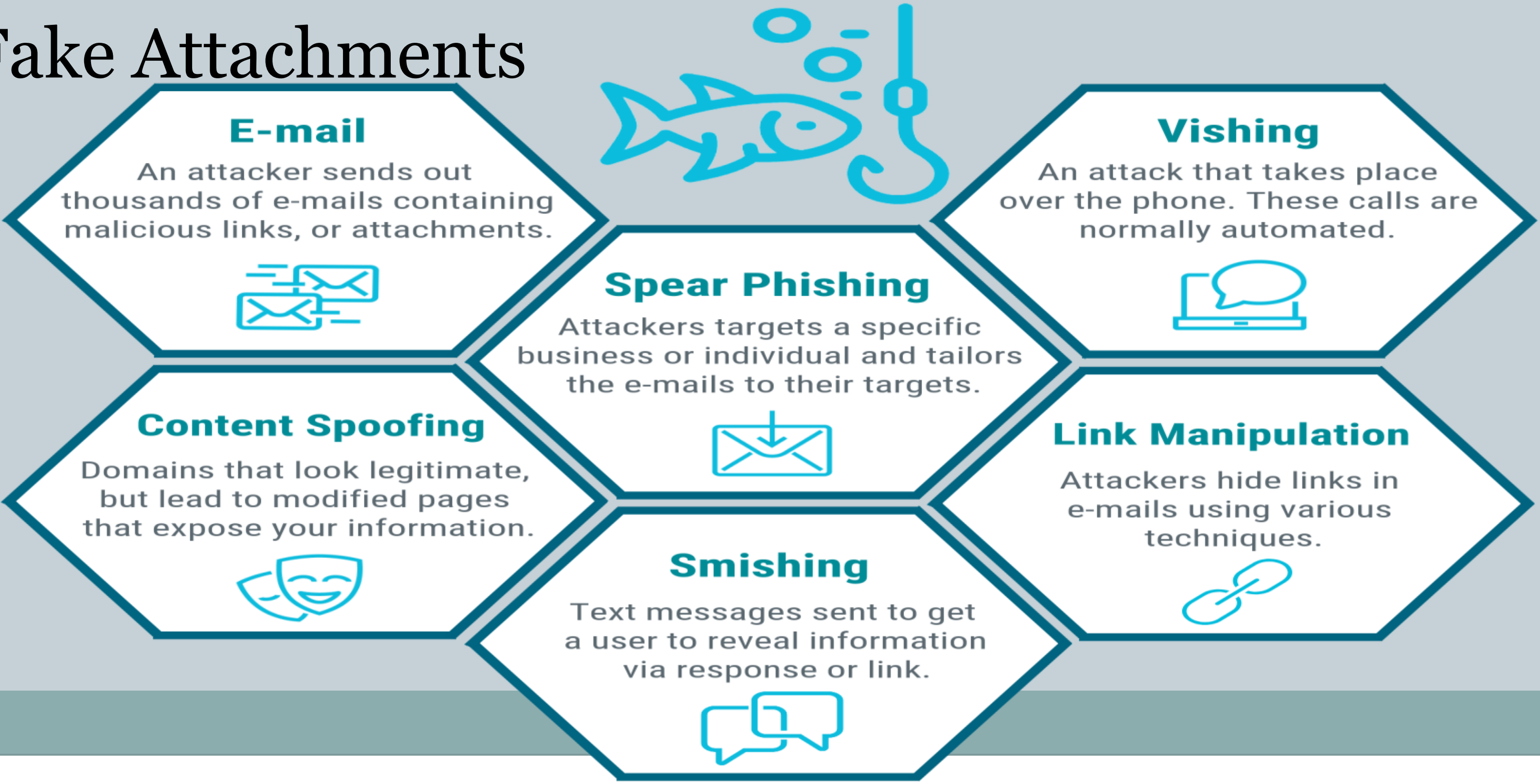
What Is Vishing?

- 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.

Techniques Used in Phishing

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



E-mail

An attacker sends out thousands of e-mails containing malicious links, or attachments.

Vishing

An attack that takes place over the phone. These calls are normally automated.

Spear Phishing

Attackers targets a specific business or individual and tailors the e-mails to their targets.

Content Spoofing

Domains that look legitimate, but lead to modified pages that expose your information.

Link Manipulation

Attackers hide links in e-mails using various techniques.

Smishing

Text messages sent to get a user to reveal information via response or link.

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.

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

Thank you !!!