1. Phishing

Email
90182naisd@outlook.com

Hello,

We identified a bank transfer from your bank in the value of $300 to another account

Click the link bellow to cancel it, if you don't recognize this transfer

l1nk.dev/jXNVD

Regards

- Phishing is a form of attacking the victim using social engineering. The attacker may try to extract information or even money from the victim. The attacker may also try to infect the victim's machine with malware.
- One of things to pay attention to when receiving an email, message, or other type of contact, is to **check the sender**.
    - Check first, if you know the email and name of the sender;
    - If not, check if it is a suspicious address, like random characters or words that don't make much sense with the context. Example: the sender says he is from Bank X, but the email address doesn't belong to the Bank X domain;
    - Check the name of the sender, even that it can be easily changed to a trustable name;
    - Check for the e-mail address online, it may be or some warning list for suspicious emails, or if it is from a real company, it may appear on the company website.
- Never download or execute files if you're not sure what they are or who sent them, it may contain malicious softwares.
- For the same situation, don't click links either. They may also contain malicious softwares, or redirect you to a malicious website, or even a fake website that reminds you of a legitim one.
- **Reconnaissance**: Process done by the attacker to gather information about the victim, so he/she can make the phishing attack more believable and have more chances of success.
    - Check the victim's social media, where he/she works, etc
    - For example, if the attacker knows where the victim studies, or work, or places he/she goes, it's easier to come up with a more believable story.

1.1. Some techniques used on Phishing attacks to make the message more believable

1.1.2. Typosquatting

A type of URL hijacking, the attacker creates a fake website almost or identical to a legitim one, and with a URL address also very similar to the real one.

The fake website will have only a letter or some very small differences from the original one, this way an user can access the website by accident by

mistyping the real website URL, or receive the website's address and doesn't pay attention to the small differences.

Example:

Original website: www.google.com

Fake website: www.goegle.com

1.1.3. Prepending

The attacker will use expressions on the email to make it look more trustable, like "MAILSAFE:PASSED", "RE:RE"

1.1.4. Pretexting

The attacker pretends to be someone else to extract information from the victim: "Hello, I am from the hospital Y, please inform your home address so we can complete your file register"

1.2. Types of Phishing Attacks

1.2.1. Pharming

Pharming is a type of attack where you attack an entire group of people. For example, if the attacker wants to attack clients from a specific fast food's clients, he or she can **Poison the DNS Server** from the fast food's website, that way, all the customers that try to access the website will be redirected to an identical malicious one. As the bogus website can be almost identical to the original website, it's hard even for the antivirus to detect the fraud.

On Pharming attacks, the attacker performs a mass attack, like poisoning the DNS Server, instead of attacking each individual at a time.

- How would phishing and pharming work together?
  - **Phishing** - stealing credentials with social engineering
  - **Pharming** - mass attack
  - Example: The attacker poisoned the dns server from a legitim website, the user access the website and fills a form with his address information to receive a product.

1.2.2. Vishing (Voice Phishing)

Vishing or Voice phishing, is a phishing attack that is done through a phone call or voice mail.

The attacker may use a technique called **Caller ID Spoofing**, where he spoofs the phone number he is calling from, so it may look like a call from someone nearby.

1.2.3. Smishing (SMS Phishing)

Smishing is when the phishing attack is done by SMS / text message. Caller ID Spoofing can also be used in this attack.

1.2.4. Spear Phishing

Spear Phishing is when the phishing attack is targeted to a specific person or a specific group of people. For example, an attacker can target the financial team from a company to convince them to transfer money to him/her.

1.2.4. Whaling

Whaling is the type of phishing that aims for "high-ranked" people, like CEOs, senior executives, etc. Whaling it's also known as CEO fraud.

2. Example of exam questions about Phishing topics:

a) What type of information is phishing NOT commonly intended to get?

i) Passwords
ii) Personal data
iii) Username
iv) Email addresses

R: Option iv) email addresses. Phishings' targets are personal data, passwords, credit cards, and others. Phishing attacks don't usually try to steal email addresses.

b) When phishing attacks are so concentrated that they target a specific high-ranking or important individual, they are called what?

R: Whaling. Whaling attacks are a type of phishing attack that aims for high-ranking individuals, like companies CEOs

c) How is phishing different from general spam?

R: Phishing attacks intent to acquire credentials or other data. Spams are undesired messages, calls or emails which aren't necessarily malicious, or the maliciousness is not confirmed.

d) Scott is a network administrator for MB Company. He has found that someone has registered a domain name that is spelled just one letter different from his company's domain. The website with the misspelled URL is a phishing site. Which of the following is the best description for this attack?

R: Typosquatting. Typosquatting is a technique used a lot combined with phishing attacks, where the attacker registers a domain name with just one letter or more, or just other small differences, so the victims can be easily tricked into accessing it, without realizing it is not the legitim. website.

e) Ahmed works as a sales manager with a major insurance company. He has got an email that is encouraging him to click on a link and fill out a survey. He is suspicious of the email, but it does mention a major insurance association, and that makes him think it might be legitimate. The best description of this attack is?

R: Spear Phishing. The attacker mentioned an insurance association which he or she knows is related to Ahmed's work to make the email seem legitimate.

f) Lisa received a phone call from someone identifying himself as a representative from a known hardware vendor. He said he's calling customers to inform them of a problem with database servers they've sold, but he said the problem only affects servers running a specific operating system version. He

asks Lisa what operating system versions the company is running on their database servers. Which of the following BEST describes the tactic used by the caller in this scenario?

1) Prepending
2) Tailgating
3) Pharming
4) Smishing

R: Option 1 - Prepending. In this case, it is prepending because the attacker is pretending to be someone he isn't to extract information from the victim. Tailgating is when someone tries to enter with you when you access a building. Pharming is a mass attack.Smishing is phishing by text message.

g) An employee reports that she keeps receiving unwanted emails inviting her to respond to surveys. What does this describe?

i) Phishing
ii) Spear Phishing
iii) Spam
iv) Vishing

R: Option iii) Spam. Spam is an unwanted email from any source for any reason, not necessarily a malicious email or when the malicious is not confirmed. Spear Phishing is a phishing targeting a specific group of people or a specific person. Phishing is a form of stealing information from a victim by using social engineering, but there isn't any evidence of it being a phishing in this case. Vishing is a phishing attack done by phone calls or voicemails.

h) Homer received a text message on his smartphone that appeared to come from Google. It indicated a problem with his account, said it will send him a verification code, and encouraged him to reply to the text with the code. It also stated that his account would be permanently locked if he didn't provide the code. Which of the following BEST describes this activity?

1) Spim
2) Spear Phishing
3) Smishing
4) Vishing

R: Answer 3) Smishing. Smishing is a type of phishing, but sent from text messages (SMS). **SPIM (Spam Over Internet Messaging)** is unwanted messages sent over instant messaging (IM) channels, but all SPIM isn't malicious. Spear phishing is when the phishing is targeting a specific group or person. Vishing is phishing sent by voicemail or phone calls.

i) Management department reported receiving a similar suspicious email. The email included a malicious link, but the employees recently completed training on malicious threats and none of them clicked on the link. Security investigators determined the link was malicious and would have downloaded

ransomware if anyone clicked the link. Which of the following BEST describes the email?

i) Phishing
ii) Spear Phishing
iii) Smishing
iv) Vishing

R: Answer 2) Spear phishing is the best fit in this case, as the attack is directly targeted to a specific department of a specific company. This attack is a type of phishing, but as it is targeted to a specific group of people, spear phishing best describes it. Smishing is phishing sent over text message (SMS), which is not the case, and Vishing is phishing by voicemail or phone calls.

j) Homer is complaining that his system began acting erratically after he visited the comptia.org web site. After checking the proxy server logs, you determine that he was visiting the comptai.org web site and this web site downloaded suspicious files to his computer. Which of the following is the MOST likely explanation for this activity?

1) Smurf
2) Typosquatting
3) Fuzzing
4) Replay

R: Option 2) Typosquatting. In typosquatting attacks, the attacker registers a domain very similar to a legitim web site, with only a small difference like a letter, this way, the victim won't easily realize he or she is on a malicious fake website. Smurf attack is a DDoS attack which an attacker aims at the ICMP protocol. Fuzzing is a type of dynamic code analysis and test application's ability to handle random data. A replay attack attempts to replay data with the intent of impersonating one of the parties.

k) Attacker recently sent some malicious emails to the CFO within your organization. These emails have been forged from blocks and look like they are coming from the CEO of the organization. They include a PDF file that is described as an unpaid invoice. However, the PDF is infected with malware. Which of the following BEST describes the attack type in this scenario?

1) Phishing
2) Spim
3) Vishing
4) Whaling.

R: Option 4) Whaling. Whaling is a phishing attack that aims for high-ranked individuals, such as CEOs, CFOs, etc. This is a type of phishing attack, but phishing isn't as specific as whaling to describe this case. SPIM is Spam Over Internet Messaging, is a general spam over the internet that usually doesn't target any individuals and it's not malicious. Vishing is phishing through voicemails or phone calls.