(Cybersecurity)

Phishing Atteck And Its Types in a nut shell

1. Email Phishing

Email Phishing is the most common type of phishing. Hackers send emails that appear to come from legitimate sources to trick users into clicking a malicious link or downloading an infected file. When the user click the link or download the file, malware then installed, granting the hackers unauthorized access to your credentials, such as login information, etc. Never click links or download any file sent to you through emails attachments, unless the sender is verified.

2. Spear Phishing

Spear Phishing is a type of phishing in which the hackers targets only one person, instead of many, at a time. The attackers uses victim's name, job title, etc. sometimes disguising as a coworker or a friend, tricking the victim to reveal some confidential information, such as business data, etc. Spear Phishing is usually used to break into corporate networks, and in stealing confidential data.

As a worker, always try to verify the real person that contacted you before taking any action.

3. Whaling

Whaling is another type of Spear Phishing that is used to target high-profile individuals such as CEOs, CFOs, government officials, or any high-ranking officials. It is used to trick those officials to authorize large fund transfers or reveal internal business strategies. It is done through creating extremely well-crafted emails in which business terms, personalized info, and logos are included.

As a top official, always verify sources before taking any action.

4. Smishing

Smishing is also called "SMS Phishing". In this type of phishing, attackers use text messages instead of emails: it is phishing via SMS. They send the SMS (which contains malicious links), pretending to be from banks, mobile providers, delivery companies, etc. asking the user to click the link in order to obtain their personal or financial information.

As a customer, always try to know the real contact your organizations use to send SMS, or the real header of their SMS.

5. Vishing

Vishing is also called "Voice Phishing". It is a type of phishing in which the attackers call the users, pretending to be from their trusted organizations, such as banks, government, tech support, etc. asking the users to verify their identities by giving personal or financial information. Many people complained that their banks called them to verify their card numbers, and in the process, someone get access to their accounts.

As a customer, always try to know the contact info of your organization and how they contact customers.

6. Pharming

Pharming is another type of phishing used to redirect users from a legitimate websites to fraudulent ones without their knowledge or consent, even if they typed the correct URL. It is used to steal financial data or login credentials. It is done through malware, DNS poisoning, or hijacking. Users will visit a website, logging with their credentials, thinking it is the real site, while it's not. In the process, their credentials are captured.

As an internet user, be very careful while logging into any plaform.

7. Clone Phishing

Clone Phishing is the one in which the attackers create a nearly identical replica of a legitimate email that was recently received by the user. They resend the email, adding some malicious links or file to it, asking the user to click the link or download the file. The email will appear as if it is from trusted or known source. When the users click the link or download the file they get hacked.

As a user who receives emails, always try to differentiate between the real emails and fake ones.

8. BEC

BEC stands for Business Email Compromise: a type of phishing that is used to target businesses and professionals. The attackers tries to gain control of a business email or pretends to be a trusted vendor or manager, tricking employees into transferring money, sharing business data, requesting urgent payments, asking to change account numbers, etc. Many companies lose millions to this type of fraud.

As an employee, working in a business organization, always verify sources before taking any action.