PHISHING ATTACKS

Phishing is a type of cyberattack where scammers use fake emails, text messages, phone calls, or websites to deceive people into giving away sensitive information, downloading harmful software, or falling victim to other types of cybercrime.

Phishing is based on the word “fishing”, based on the concept of bait.

Types Of Phishing Attacks

- Spear Phishing: this type of phishing is to a specific target, as the name implies. This method is used to steal or compromise the device of a specific user.
- HTTPS Phishing: this type of phishing creates fake websites using https to trick you into believing it's secure, for instance it could be a link to learn free online courses or a link sent to your email , all to get your private information.
- Vishing: this is also known as ". social engineering". This method involves attackers using phone calls or messages , that is , communication with their target(s), to trick them into giving out personal info like bank 4-digit pin, email password, phone number, etc.
- Smishing: this method involves the use of SMS or text messages into downloading a malware or revealing personal or financial information, or even downloading software .
- Pharming: is the use of malicious codes to redirect users to fake websites without their consent , for instance, clicking a movie website but it loaded a bet9ja website, and lots more.
- Email Phishing: this is a type of phishing involves malicious emails using urgent language and fake links.
- Whaling: this type of phishing targets individuals with high profiles in an organization, attackers do thorough research on that person and pretend to be a senior staff to gain the trust of their target. This method employs social engineering, you can call whaling "CEO FRAUD".
- Clone Phishing: this is a type of cyberattack that duplicates a legitimate email to make it look legit to exploits victims.
- Evil Twin Phishing: this involves fake Wi-Fi networks to steal information.

How To Identify Some of These Phishing Attacks

- Email Phishing: phishing emails often impersonate legitimate organizations (banks, services, etc.) to trick victims into clicking malicious links or giving up credentials, an example of a phishing email website is “caniphish”. Common Phishing cues are:

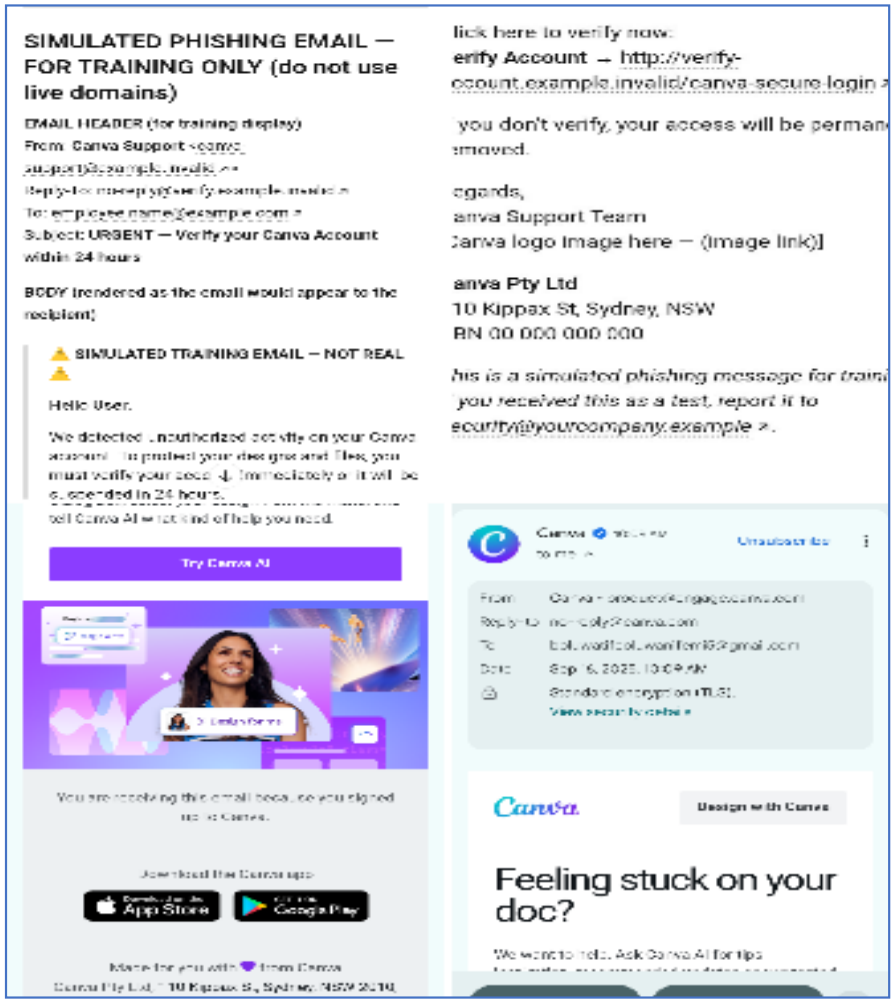
i. Unfamiliar or Urgent Tone: phishers often create a fake urgency (e.g. warning, deadline) to pressure immediate action.

ii. Spelling/grammar errors: legitimate companies rarely send emails with obvious mistakes.

iii. Generic greetings: emails that say “Dear customer” or “Sir/Madam” instead of your name can be suspected .

iv. Sender Mismatches: Check if the email domain truly matches the organization(e.g. a message “from” Microsoft should use @microsoft.com).

v. Suspicious links or attachments: Hover (or long press on mobile phone) to preview URLs . Phishing messages often link to fake domains that look similar to real ones.



Avoiding Phishing Emails

1. Never click links or open attachments in unsolicited or suspicious emails. Instead navigate to website manually(e.g type the bank's URL or use a known bookmark) or call the organization using a verified phone number.
2. If the email appears to be from a colleague or vendor but seems odd, call that person separately to confirm.
3. Keep your software and antivirus and antispyware updated , also use email filters.
4. Report any suspected phishing mail
5. Legitimate organizations will never email asking for passwords, social security numbersor direct payment via odd methods.

Social Engineering Attacks

What is Social Engineering? Social engineering uses psychological manipulation to trick people into revealing sensitive information or bypassing security practices. Attackers might impersonate authority figures, use fear or reward tactics, or exploit natural trust. “Phishing” is a form of Social Engineering.

These tactics exploit human emotions and authority. For example, fraudsters once tricked a company by emailing “ Change of Bank Details” from a seemingly real supplier, inducing staff to quickly pay a fake invoice. That scam used urgency (“early payment discount within 24hours”) and personal details to succeed.

Preventing Social Engineering: Key advice includes:

- Don’t trust unsolicited requests: Never click links or download attachments from unknown sources. If an email or call requests personal or financial details, assume it’s suspicious.
- Verify Identities.
- Be cautious with odd giveaways.