Armaan Shamsaasef

Phising

Phishing - SY0-701 - 2.2

Definition: A social engineering attack that uses fraudulent electronic communications to trick a victim into providing sensitive information or deploying malicious software.

1. Phishing (Standard)

- Description: A broad, untargeted attack sent to a large number of people.
- Method: Generic emails pretending to be from well-known companies (e.g., Microsoft, Amazon, a bank) asking the user to "verify their account," "claim a prize," or "update payment information."
- Goal: Steal credentials, credit card numbers, or other personal data.
- Example: An email claiming to be from "Netflix Support" stating your payment failed, with a link to a fake login page that steals your username and password.

2. Smishing (SMS Phishing)

- Description: Phishing attacks sent via SMS/text messages.
- Method: Texts containing a malicious link or instructions to reply with personal information.
- Example: A text message saying, "Your package delivery failed. Click here to reschedule: [malicious link]" or "Your bank account is locked. Text back your username to verify."

3. Vishing (Voice Phishing)

- Description: Phishing attacks conducted over the phone.
- Method: A fraudulent phone call where the attacker impersonates a trusted entity (e.g., IT support, the IRS, a bank fraud department).
- Goal: To create a sense of urgency and pressure the victim into revealing information or performing an action over the phone.

- Example: A call claiming to be from "Microsoft Support" stating your computer is sending errors. They pressure you to install remote access software, giving them control of your machine.

4. Spear Phishing

- Description: A highly targeted phishing attack aimed at a specific individual or group.
- Key Differentiator: The attacker uses personalized information (e.g., your name, position, projects, colleagues' names) gathered from social media or other sources to make the email seem legitimate.
- Goal: Often used for corporate espionage or initial access into a specific organization.
- Example: An email specifically addressed to a company's CFO, pretending to be the CEO, urgently requesting a wire transfer for a "confidential acquisition."

5. Whaling

- Description: A form of spear phishing that targets high-level executives (the "big fish" or "whales"), such as the CEO, CFO, or other senior leadership.
- Method: Extremely researched and personalized emails that often involve legal subpoenas, board matters, or major financial transactions.
- Example: An email to the CEO, forged to look like it's from the legal department, regarding a pending lawsuit, with a link to a "secure document portal" that is actually a credential-harvesting site.

6. Phishing Summary Table

Type	Communication Channel	Key Characteristic
Phishing	Email	Broad, untargeted mass email
Smishing	SMS / Text Message	Phishing via text message

Vishing	Voice / Phone Call	Phishing via phone call
Spear Phishing	Email	Targeted at a specific individual or group
Whaling	Email	Targets high-level executives ("big fish")

Summary

- Phishing is the umbrella term for these social engineering attacks.
- The channel defines the specific type: Email, SMS (Smishing), or Voice (Vishing).
- The level of targeting defines the sophistication: Broad (Phishing) vs. Specific (Spear Phishing) vs. Executive (Whaling).
- The core goal is always to manipulate human psychology to bypass technical security controls.