PHISHING AWARENESS TRAINING

Eric Thimi Alappatt
CodeAlpha

Cybersecurity Internship Task-2

WHAT IS PHISHING?

- Phishing is an online scam where criminals send fraudulent email messages, appearing legitimate. The emails contain links or attachments that trick recipients into entering confidential information (e.g. account numbers, passwords) into fake websites, or they infect computers with malware.

- Phishing attempts involve deceiving individuals through messages, e-mail to reveal sensitive data.

- Attackers often masquerade as a legitimate entities and mimic popular online services.

HOW PHISHING WORKS?

- **Email Delivery**:- Attackers send email disguised as legitimate sources, often using similar logos and mimicking as real time software.
- **Clicking the Bait**:- The email contains a link or attachment that, when clicked, triggers the next step.
- **Fake Website**:- This link leads to a fraud website, duplicating the look and feel of a legitimate website.
- **Information Sharing**:- Unaware of deception, the victim enters their login, personal details on fake site.
- **Data Theft**:- The Attacker successfully captures the entered information for

TYPES

Phishing

1

SPEAR PHISHING

Targeted attempt to steal sensitive information, typically focusing on a specific individual. These types of attack use personalized facts in order to appear legitimate.

2

VISHING

Phone scam, and has the most human interaction of all the phishing attacks. Calls are often made through a spoofed ID, so it looks like a trustworthy source.

3

WHALING

Steal sensitive information from senior-level. Whaling emails contain highly personalized information about the target organization, so they are more difficult to detect.

4

SMISHING

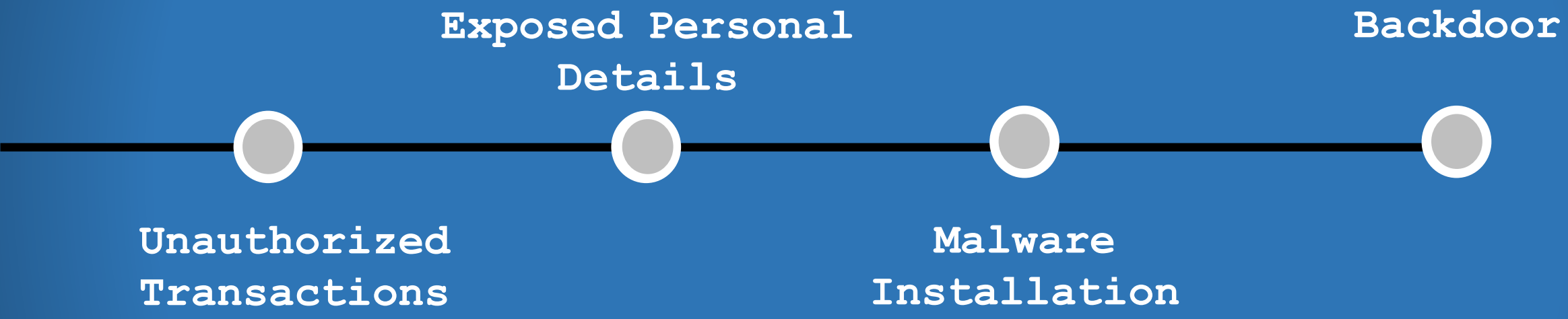
Use of text (SMS) messages, as opposed to emails, to target victims. Fraudsters send a text message to an individual, usually calling for the individual to act.

5

CLONE PHISHING

Used to create an identical email with malicious content. The cloned email will appear to come from the original sender and will contain malicious attachments.

SUCCESSFUL ATTACKS RESULTS IN


Exposed Personal Details
Backdoor
Unauthorized Transactions
Malware Installation

TIPS

To Identify Phishing

1

MISMATCHED URLS

2

POOR GRAMMAR/ MISPELLINGS

3

SUSPICIOUS LINKS

4

REQUEST FOR SENDER INFORMATION

5

SENSE OF URGENCY

RESPONDING TO PHISHING ATTACKS

- Act Fast.
- Don’t Panic.
- Change Passwords.
- Shut of Internet.
- Notify Authorities.
- Seek Professional Help.
- Educate Yourself.

If It looks Phishy, It probably is