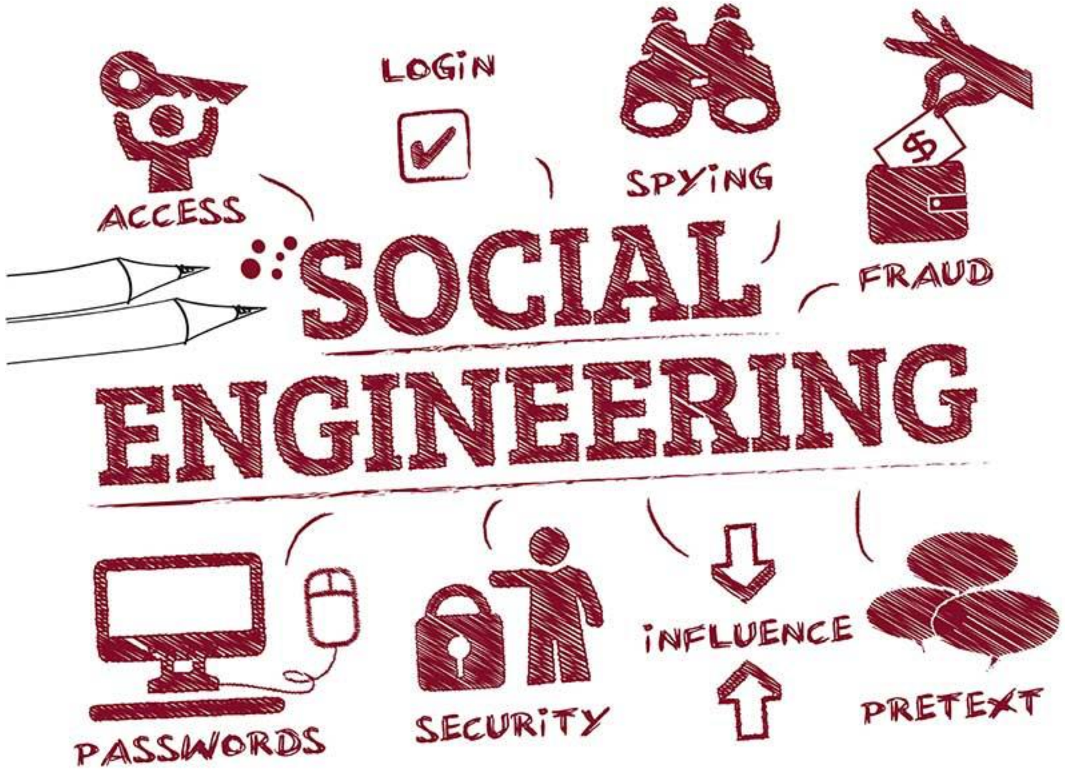
Social Engineering

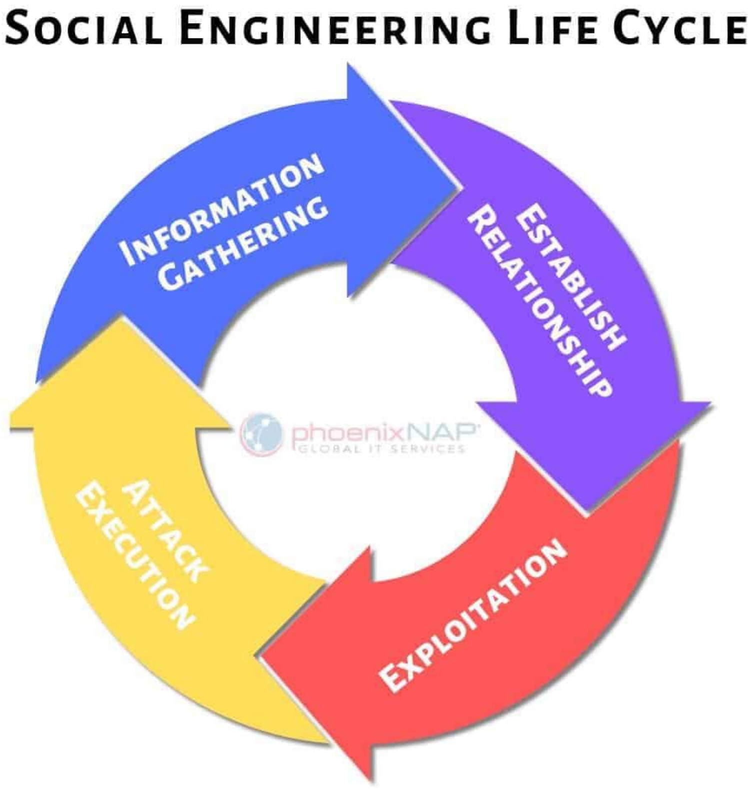
Social Engineering is a component of the attack in nearly 1 of 3 successful data breaches.

Defined as “any act that influences a person to take an action that may or may not be in their best interests”



Life Cycle of Social Engineering

- Information gathering
- Engaging with victim
- Attacking
- Closing interaction



Pretexting

Defined as the practice of presenting oneself as someone else in order to obtain private information

- Good, compelling story
- Fabricated scenario
- Not a one-size fits all

Pretexting - Scenario

The attacker calls an employee at a company, pretending to be from the IT department or an external service provider.

The attacker claims that they are investigating a security breach and need to verify the employee's identity and account information to ensure their account is secure.

To gain the employee's trust, the attacker may use technical jargon or refer to recent cybersecurity incidents to make the story sound plausible.

The attacker then asks the employee to provide their username, password, and other account details under the pretext of verifying their account for security purposes.

Believing the call is legitimate and fearing for the security of their account, the employee may unwittingly provide the requested information to the attacker.

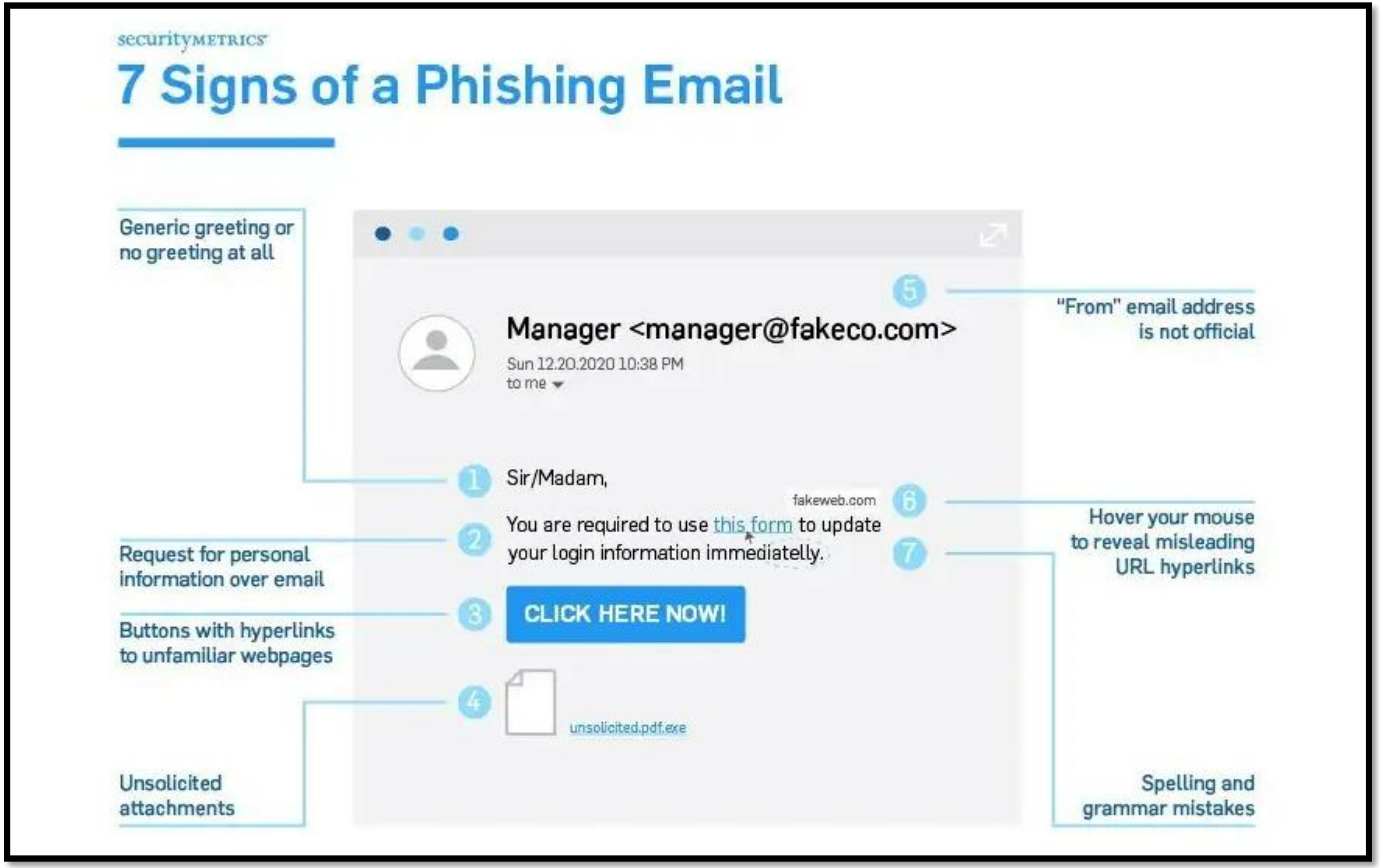
The attacker now has access to the employee's account and can potentially use this information for unauthorized access or other malicious purposes.

Phishing

Most phishing scams endeavor to accomplish three things:

- Obtain personal information
- Redirect users to suspicious websites
- Manipulate the user into responding quickly

Phishing - example



securityMETRICS

7 Signs of a Phishing Email

Manager <manager@fakeco.com>

Sun 12.20.2020 10:38 PM

to me

Sir/Madam,

You are required to use this form to update your login information immediately.

fakeweb.com

CLICK HERE NOW!

unsolicited.pdf.exe

1 Generic greeting or no greeting at all

2 Request for personal information over email

3 Buttons with hyperlinks to unfamiliar webpages

4 Unsolicited attachments

5 "From" email address is not official

6 Hover your mouse to reveal misleading URL hyperlinks

7 Spelling and grammar mistakes

Baiting

- Similar to Phishing
- Different items used to entice victim

- Exploit human curiosity via the use of physical

Baiting - Scenario

- An attacker creates a fake social media account that appears to belong to a well-known company's customer support representative.
- The attacker posts a message on the company's official social media page, pretending to be the customer support representative. The message states, "Special Giveaway for our Loyal Customers! Click the link to claim your $100 gift card."
- The message includes a link that leads to a fake website that looks similar to the company's official website, but it is designed to collect user information.
- Customers who see the post may be enticed by the promise of a gift card and click on the link to claim it.
- Upon clicking the link, customers are directed to the fake website and asked to enter their personal information, such as name, email address, phone number, and even credit card details, to claim the gift card.
- However, the attacker is not giving away any gift card; instead, they are stealing the customers' personal and financial information.

Quid Pro Quo

- Similar to Baiting
- But offers a service

- i.e. fraudsters impersonate the U.S. Social Security Administration (SSA).

I'LL BE HAPPY TO GIVE YOU KIDS SOME CANDY JUST AS SOON AS YOU DIG UP SOME DIRT ON JOE BIDEN FOR ME

Tailgating / Piggybacking

- Trick employees to open doors for attackers
- Existed in every orgnisation except large companies requiring a keycard for entrances

!
BEWARE OF TAILGATERS

Helpful Tips - Defence

- Slow down
- Research the facts
- Don’t let a link be in control of where you land.
- Email hijacking is rampant
- Beware of any download
- Foreign offers are fake