Phishing Awareness Training

By
Tohid Bhati
(Cybersecurity Intern at CodeAlpha)

Table of Contents

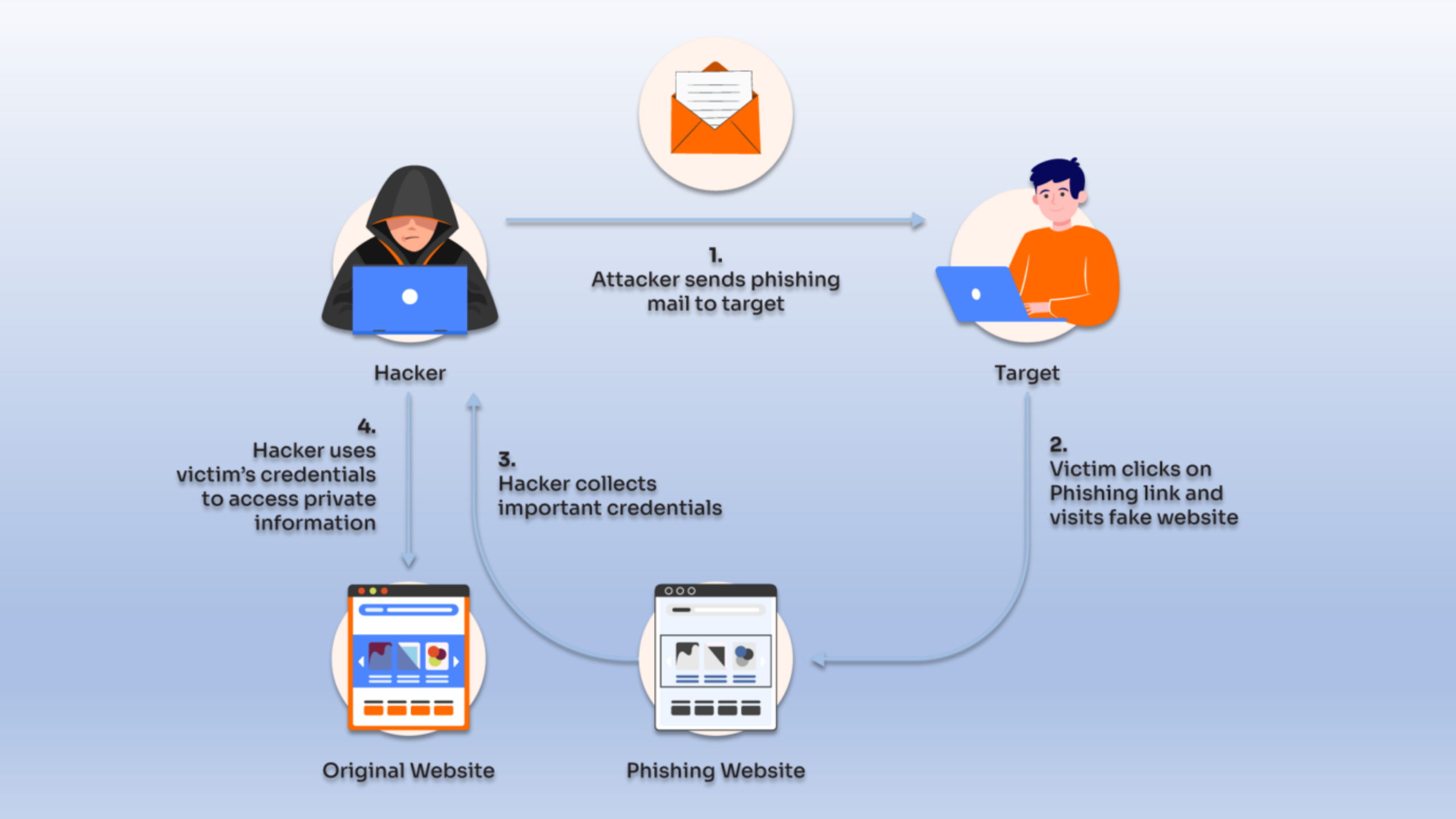
- Introduction to Phishing
- Types of Phishing Attacks
- Techniques of Phishing
- How to recognize Phishing Emails
- What to do if a phishing Email is Received
- Phishing Campaign For Awareness
- Conclusion

Introduction

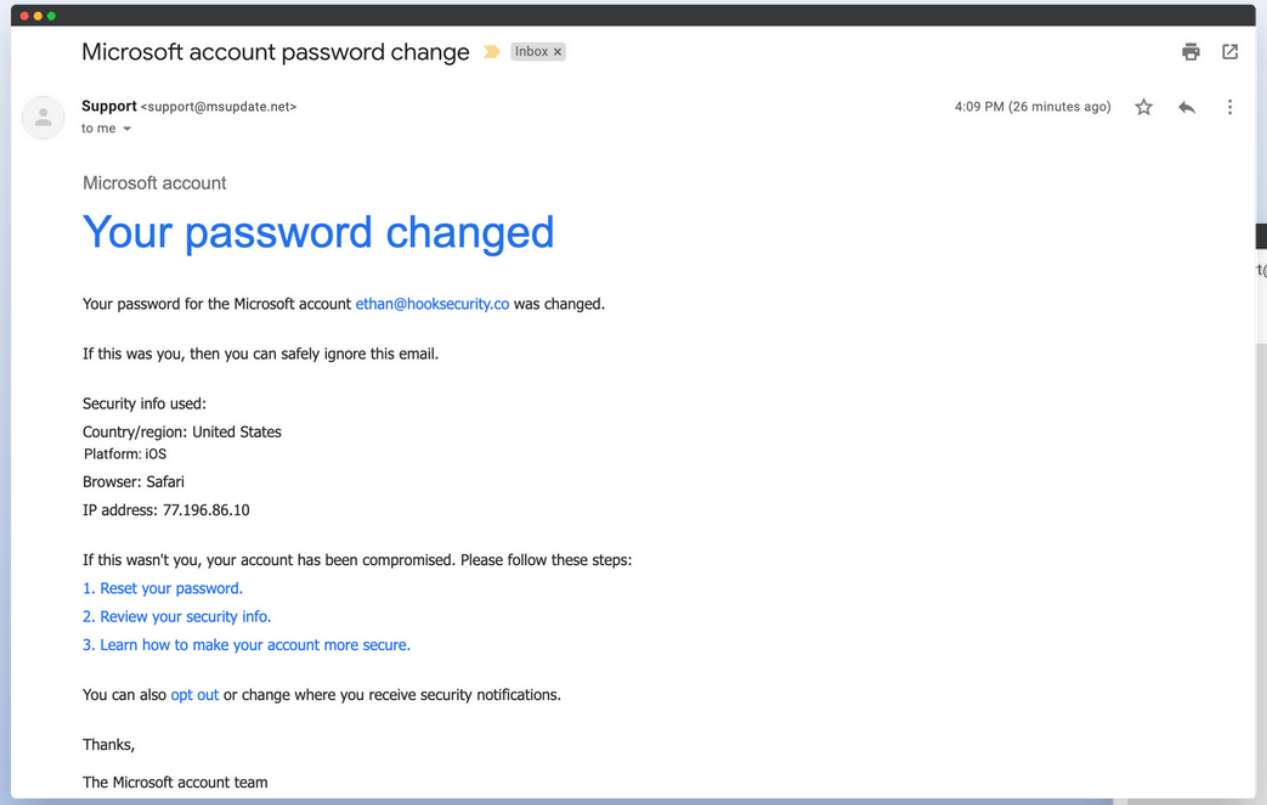
- Phishing is a cybersecurity attack, in which a malicious actor/ hacker sends messages pretending to be a trusted person or an entity.

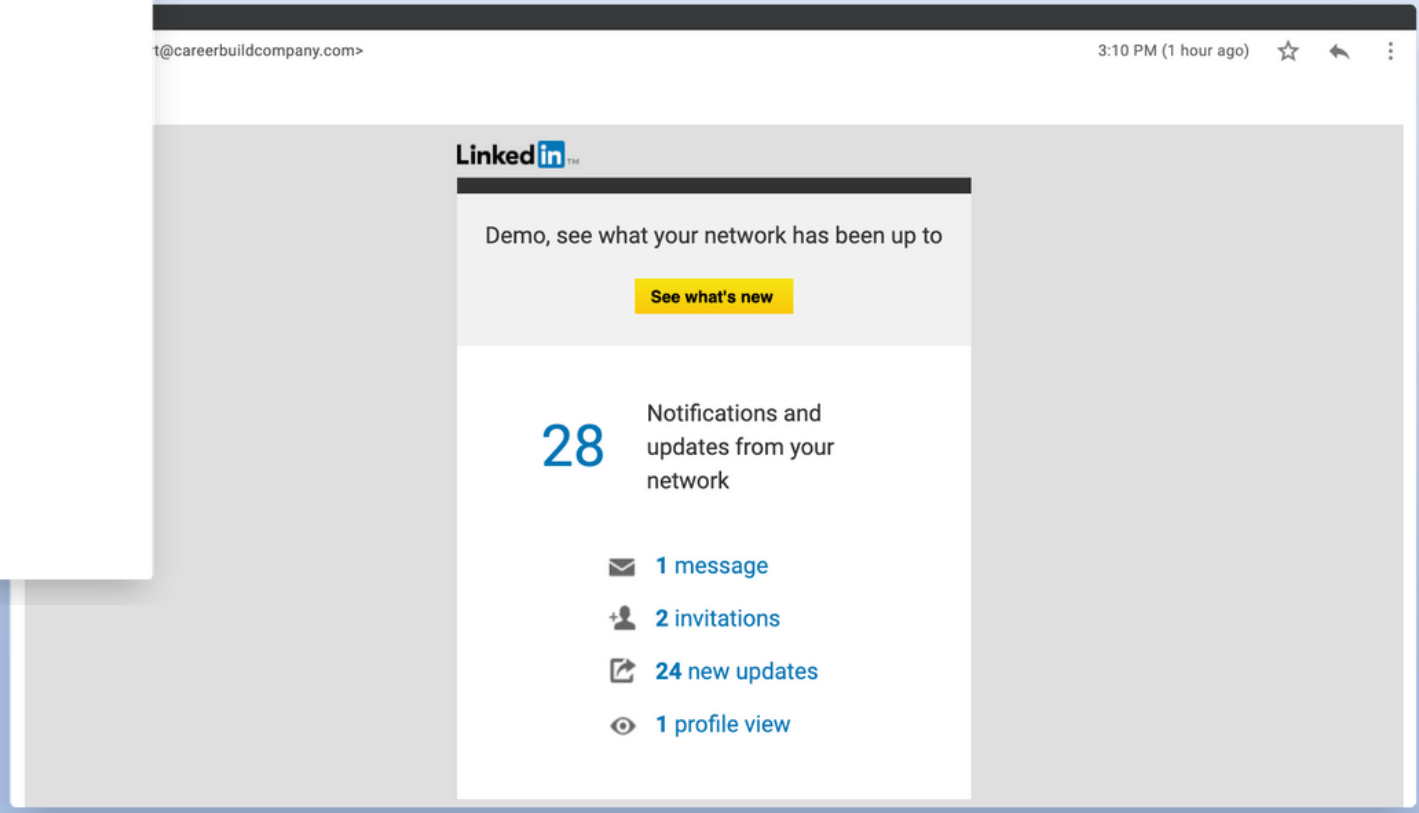
- The goal of phishing attackers is to trick individuals into revealing personall or confidential information.

- Phishing attacks can occur via email, text messges, social media, or even phone calls.


1.
Attacker sends phishing mail to target
Hacker
Target
2.
Victim clicks on Phishing link and visits fake website
3.
Hacker collects important credentials
4.
Hacker uses victim's credentials to access private information
Original Website
Phishing Website

Example:



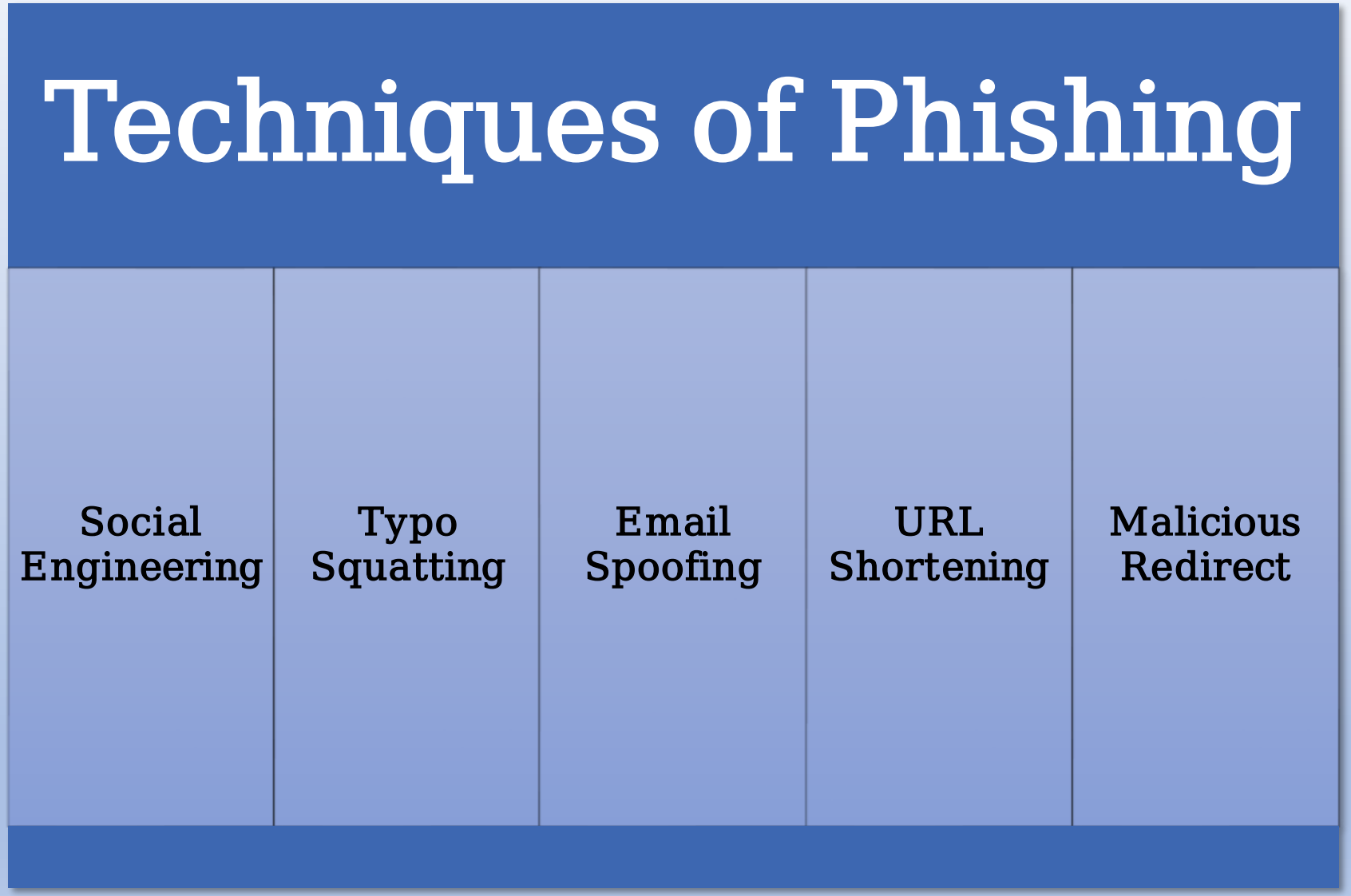


Fake Emails

Types Of Phishing Attacks

Common Types of Phishing Attacks

- Email Phishing - The most common type where attackers send deceptive emails.
- Spear Phishing - Targeted phishing aimed at specific individuals or organizations.
- Whaling - Targeting high-profile individuals like executives.
- Smishing & Vishing - Phishing through SMS and voice calls, respectively.



Techniques of Phishing

Techniques Of Phishing

Social Engineering:

- This technique manipulates individuals into divulging confidential information.

- By exploiting trust through deceptive communication, such as fake customer support or urgent requests.

Typo Squatting:

- Attackers create websites with URLs that are common misspellings of legitimate sites.

- Tricking users into visiting these fake pages and disclosing sensitive information.

Email Spoofing:

- Attackers send emails that appear to be from trusted sources by forging the sender's address.
- Tricking recipients into clicking malicious links or providing personal details.

URL Shortening:

- Attackers use shortened URLs to hide the true destination of a link, making it difficult for users to identify if the link leads to a malicious website.
- Often used in phishing attempts on social media or emails.

Malicious Redirect:

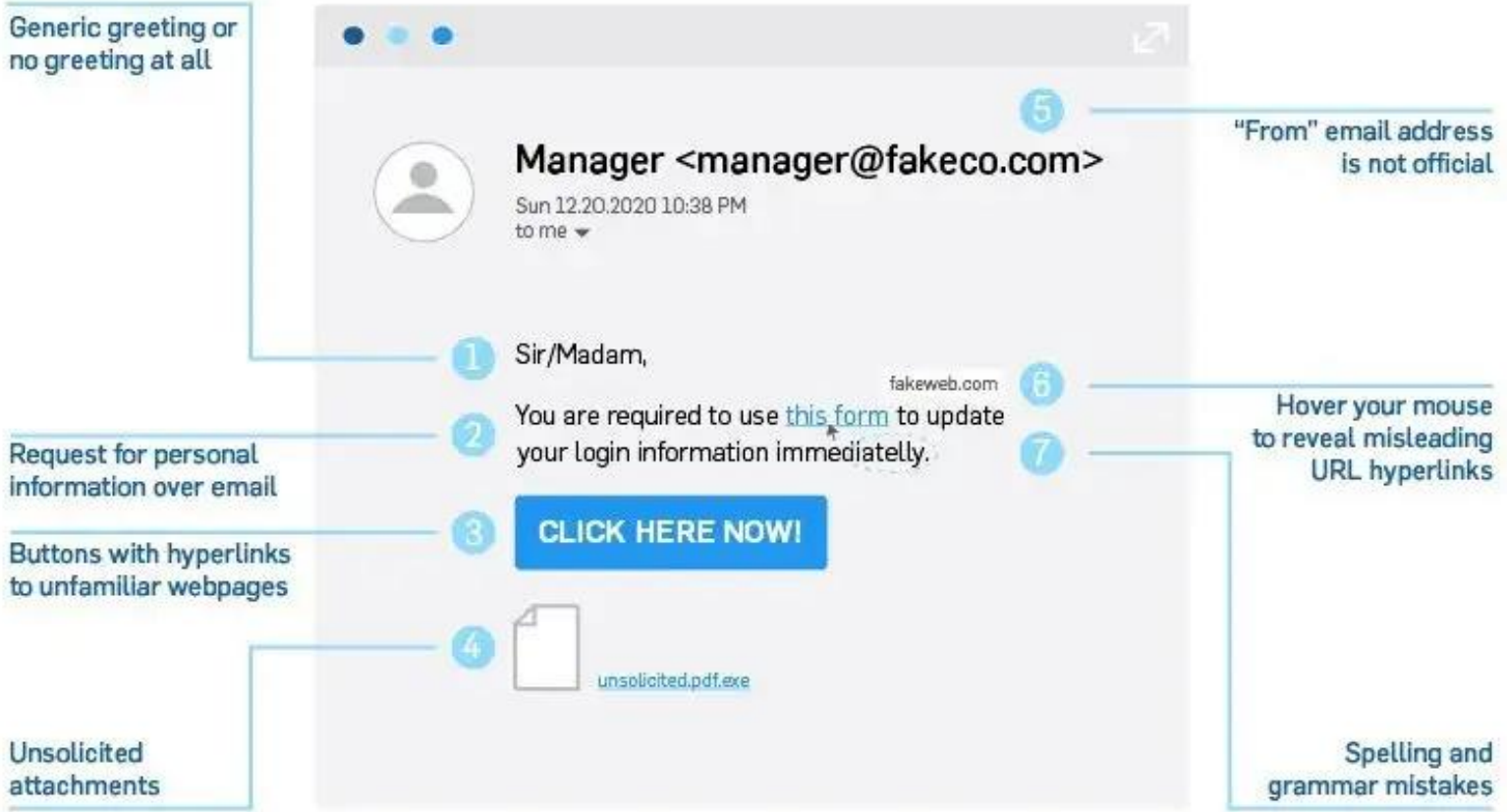
- This technique involves redirecting users from legitimate websites to harmful or fraudulent sites without their knowledge
- Typically through compromised web pages or malicious scripts.

How to recognize Phishing Emails

- Grammatical and spelling errors in the email.
- Urgency or threats demanding immediate action.
- Suspicious sender email addressed or URLs that don’t match the purported sender
- Links that lead to unfamiliar or suspicious websites

securitymetrics

7 Signs of a Phishing Email



What to do if a phishing email is received

Protecting Yourself From Phishing Attack

1.Verify The Sender

- Always verify the sender's email address before clicking on any links or providing information.
- Check for the legitimacy of the sender's domain.

2. Be Skeptical of Urgent Requests

- Be cautious of emails that create a sense of urgency or fear, pressuring you to take immediate action.
- Verify the authenticity of the request through other means before responding.

3. Hover Over Links

- Hover over links to preview the URL before clicking.
- Ensure that the URL matches the purported destination.

4. Use Security Software

- Install and regularly update antivirus and anti-malware software on your devices.
- Enable spam filters on your email accounts.

5. Educate Yourself and Others

- Stay informed about the latest phishing tactics and share knowledge with colleagues, friends, and family.
- Conduct regular phishing awareness training sessions in organizations.

Reporting Phishing Attempts:

- Report Phishing emails to the appropriate authorities, such as your email provider, the Anti=Phishing Working Group (APWG), or the Federal Trade Commission (FTC).
- Provide as much information as possible to help in the investigation and prevention of future attacks.

Phishing Campaign For Awareness

A simulated phishing campaign among employees to increase more awareness

- Where, a fake phishing emails is send to every employee to understand how the employee will react to it and what will they do and then train them to protect themselves and recognise or spot the fake emails

Conclusion

- Phishing attacks continue to be a prevalent threat in today’s digital world.
- By staying vigilant, educating ourselves and others, and adopting best practices for online security, we can protect ourselves and our organizations from falling victim to phishing scams.