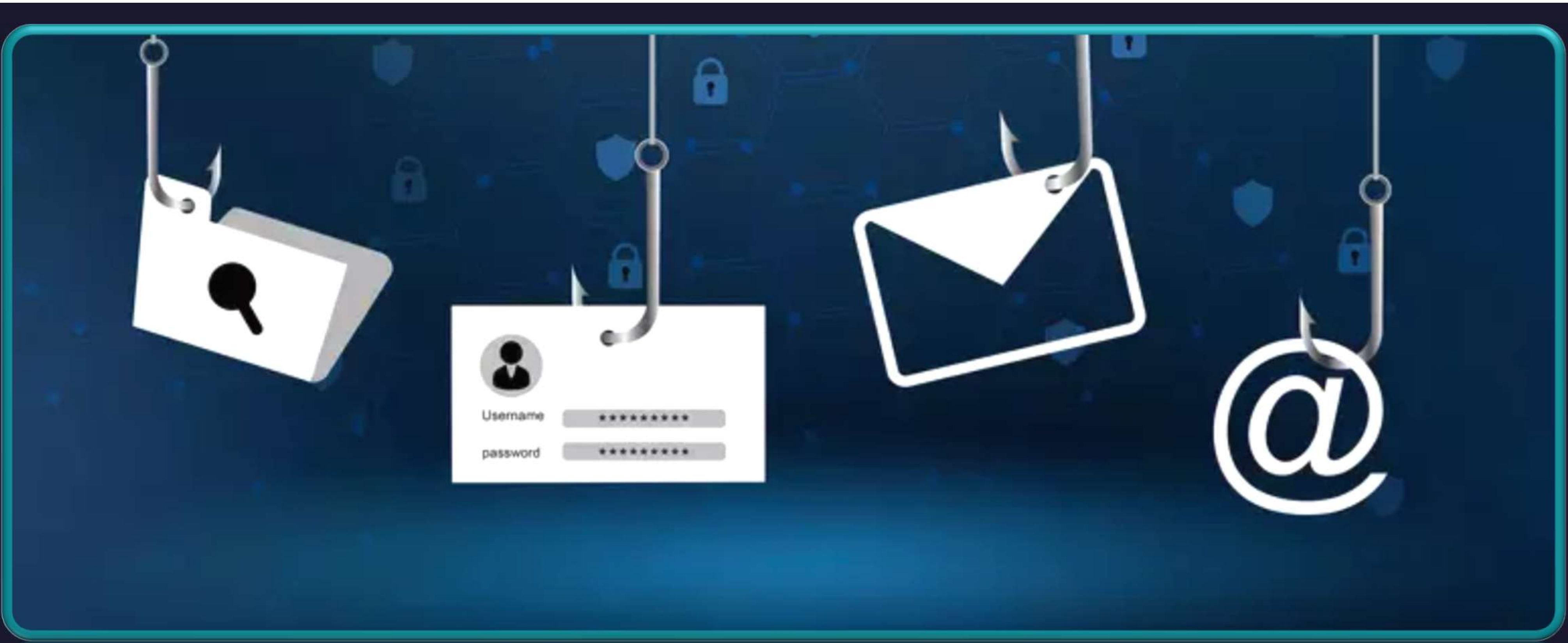
Phishing Awareness

Safeguarding Our Digital World…

Introduction

What is Phishing?

Phishing is a cyber attack method where attackers impersonate legitimate entities to steal sensitive information.



- Common targets: Individuals, businesses, and organizations.
- Purpose: To obtain personal data like passwords, credit card numbers, and other sensitive information.

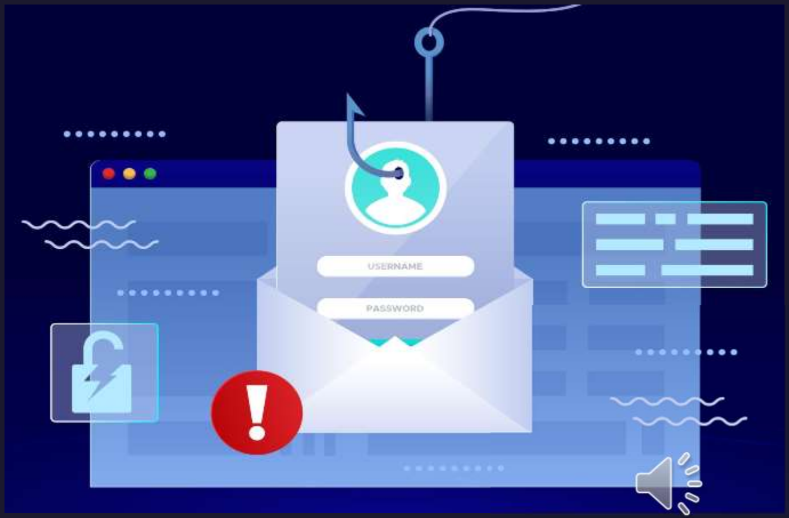
Types of Phishing Attacks

- **Email Phishing:** Fake emails pretending to be from legitimate sources.
- **Spear Phishing:** Targeted phishing aimed at specific individuals or organizations.
- **Whaling:** High-level phishing attacks targeting senior executives.
- **Smishing:** Phishing via SMS/text messages.
- **Vishing:** Phishing through voice calls.
- **Clone Phishing:** Duplicating a legitimate email with malicious links.

Recognizing Phishing Emails

How to Identify Phishing Emails?

- Check the sender's email address: Look for misspellings or unusual domains.
- Watch for generic greetings: Lack of personalization.
- Be cautious of urgent or threatening language.
- Hover over links to check their true destination.
- Look for poor grammar and spelling errors.
- Verify unexpected attachments before opening



Avoiding Phishing Attacks

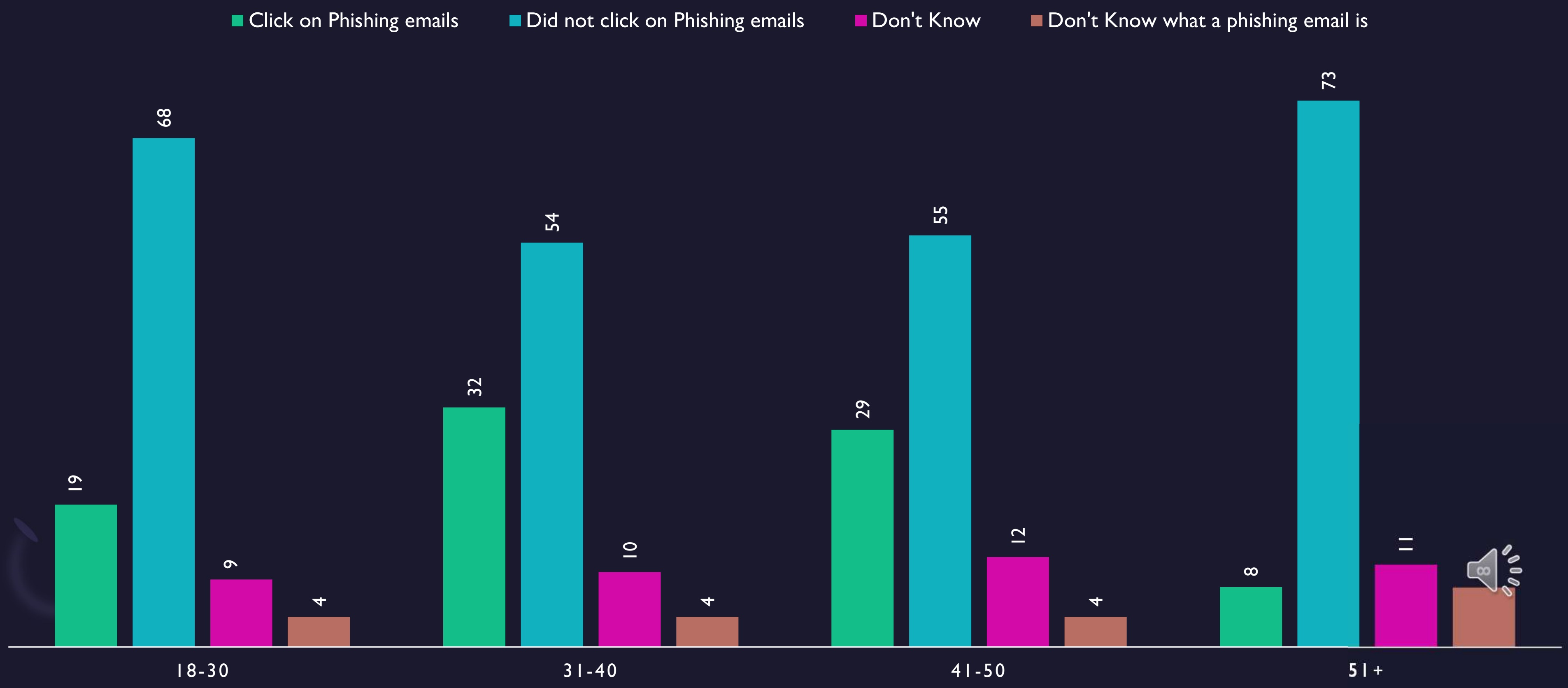
1. Don't click on links or download attachments from unknown sources.
2. Use multi-factor authentication (MFA) wherever possible.
3. Keep software and security systems up to date.
4. Use strong, unique passwords and change them regularly.
5. Educate yourself and others on common phishing tactics.
6. Report suspicious emails to your IT department or email provider.

Recognizing Phishing Websites

How to Identify Phishing Websites?

1. Check the URL: Look for HTTPS and ensure the domain name is correct.
2. Be cautious of pop-ups requesting personal information.
3. Look for website design inconsistencies.
4. Verify the legitimacy of the website by contacting the organization directly.

Phishing Demographics by Age:-



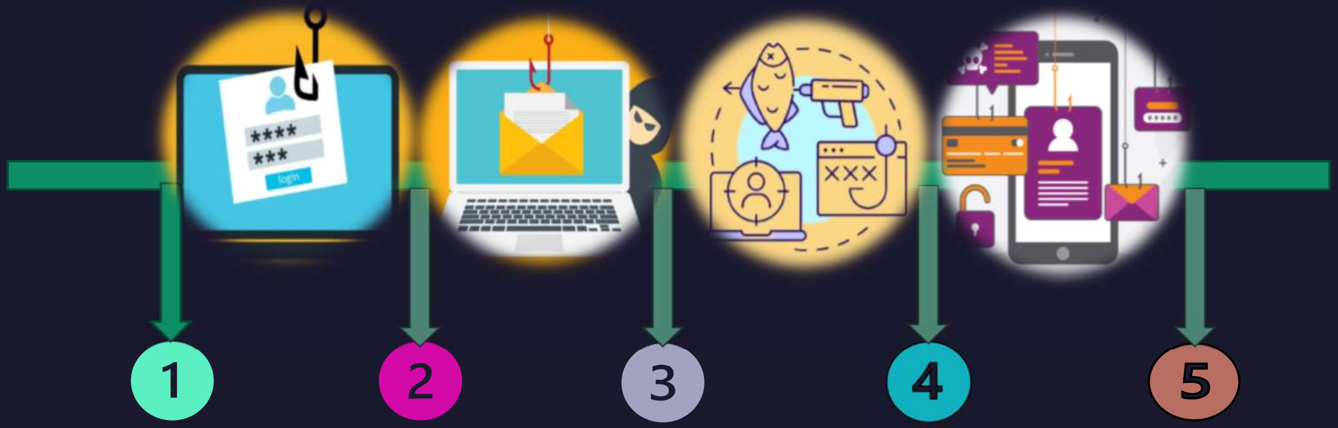
Social Engineering Tactics

Understanding Social Engineering:-

- Definition: Manipulating people into divulging confidential information.
- Examples: Pretexting, baiting, quid pro quo, and tailgating.
- How to protect yourself: Be skeptical of unsolicited requests for information.

What to Do if You Suspect a Phishing Attack?

Responding to Phishing Attempts:



1. Don't panic; stay calm.
2. Do not click on links or download attachments.
3. Monitor your accounts for unusual activity.
4. Change any compromised passwords.
5. Report the phishing attempt to the appropriate authorities.

"In the digital world, not everything is as it seems. Stay vigilant and question unsolicited messages."

Summary

Phishing awareness safeguarding our digital world training educates on recognizing and preventing phishing attacks, which impersonate legitimate entities to steal sensitive information. It include identifying suspicious emails, understanding various phishing methods (like email and vishing), and implementing protective measures like strong passwords and multi-factor authentication.

Thank You!

Palak Singh

palaksingh7361@gmail.com