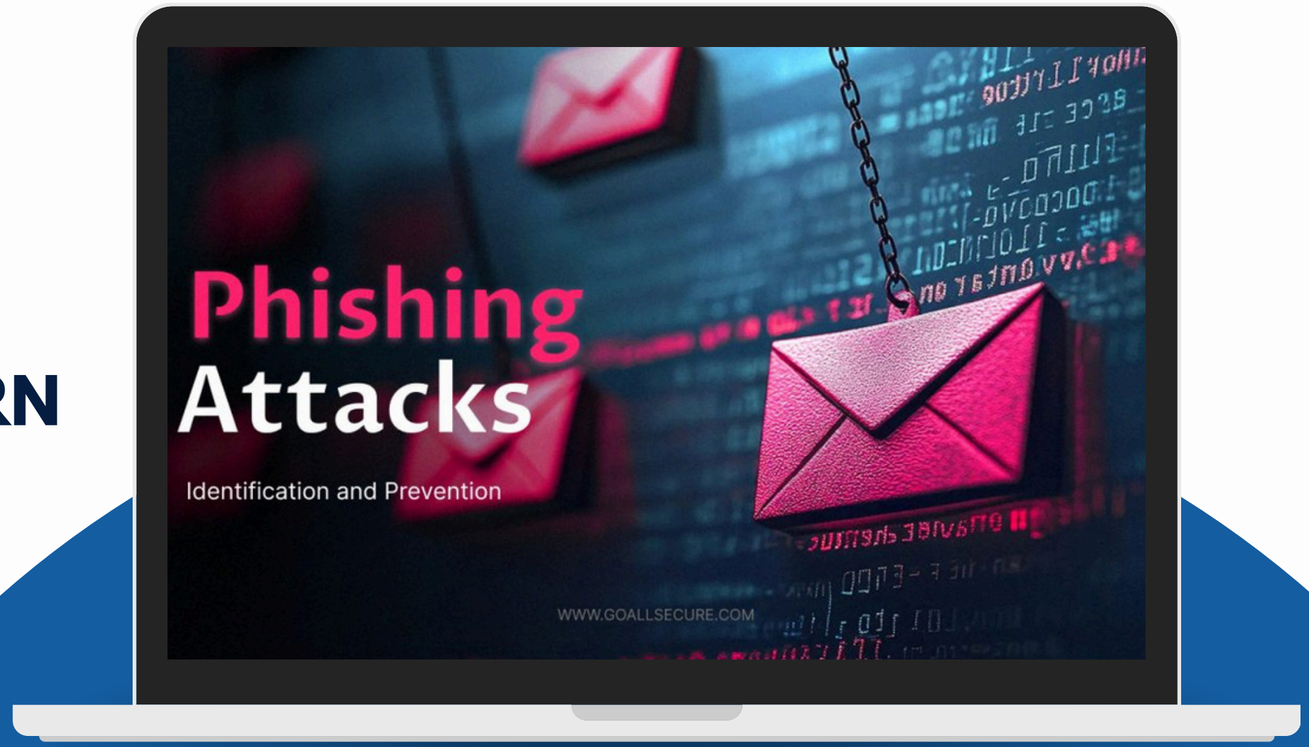
PHISHING AWARENESS

INTERNSHIP TRAINING PROGRAM

BY-RIYA KHATRI | CODE ALPHA INTERN



Overview

- Introduction 01
- Social Engineering 02
- Real world example 03
- Phishing emails 04
- Fake websites 05
- Quick quiz and example 06
- Best practices to avoid 07
- Conclusion 08

Introduction

What is Phishing?

A cyberattack tricking people into revealing personal information.

Often through fake emails, websites, messages.

WHY IT MATTERS:

One click can lead to identity theft, financial loss, or data breach.

Social Engineering?

Social engineering is a trick used by attackers to manipulate people into giving away confidential info — like passwords, OTPs, or access — by pretending to be someone they trust.

It’s hacking the human mind instead of the computer.

Common Social Engineering Tactics:

Tailgating – Physically following someone into restricted areas

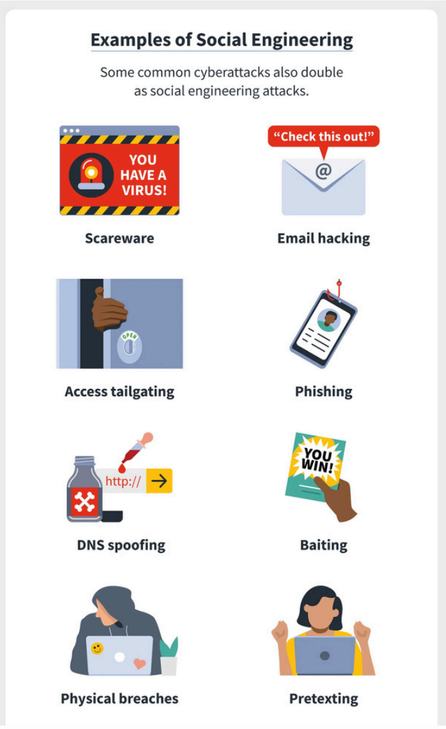
Baiting – Leaving infected USB drives or offering fake rewards

Phishing – Fake emails/websites asking for login details

Vishing – Phone calls pretending to be bank/tech support

Smishing – Fake SMS messages with urgent links

Pretexting – Inventing a scenario to gain trust (e.g., posing as HR)



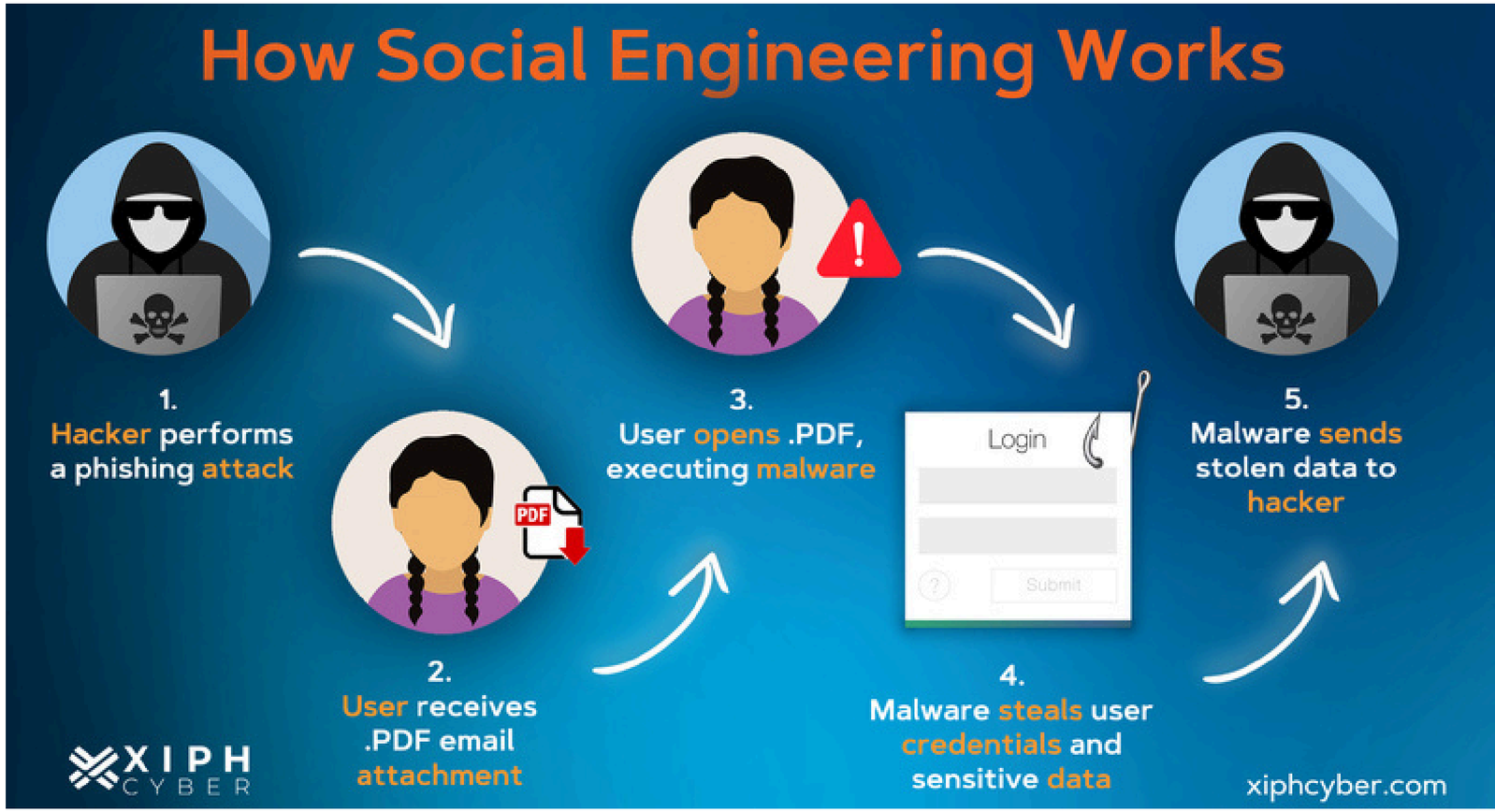
Real-World Example 1: Twitter Hack 2020

What happened? Hackers called Twitter employees pretending to be IT support.

They convinced them to share internal tools access.

High-profile accounts like Elon Musk, Obama, and Apple were used to run a Bitcoin scam.

Loss: Millions of followers deceived and scammed.



Which of the following is a social engineering tactic?

Ⓐ DDoS Attack
Ⓑ Pretexting
Ⓒ Brute-force login
Ⓓ Firewall configuration

How to Recognize Phishing Emails:

1. Generic Greetings – "Dear user" instead of your name
2. Spelling or Grammar Mistakes – Legit companies rarely make language errors
3. Urgent or Threatening Language – “Your account will be suspended!”
4. Suspicious Links – Hover to check the real URL before clicking
5. Unexpected Attachments – Especially from unknown senders
6. Requests for Personal Info – Legit companies won’t ask for sensitive info over email

How to Spot Fake Websites:

1. Look at the URL – Misspelled domains or extra characters (e.g., paypa1.com)
2. No HTTPS – Legit sites use secure URLs (https://)
3. Poor Design or Broken Layout – Unprofessional look is a red flag
4. Pop-Ups Asking for Info – Legit sites don’t use pop-ups for login or payments
5. Too Good to Be True Offers – Extreme discounts or prizes can be bait

Real-World Example – Google Docs Phishing Scam

In 2017, many users got an email that looked like a shared Google Doc.
When clicked, it opened a fake Google login page to steal credentials.
Even tech-savvy users fell for it.

Lesson: Never enter passwords into unexpected pages, even if it looks legit

🧠 Quick Quiz – Can You Spot the Phish?

Email Example:
From: "Amazon Security Team"
Subject: Urgent: Unusual login detected
Click here to verify your account immediat
http://amazon.verify-login.com
Question:
Is this a phishing email?
🅐 Yes 🅑 No
Answer: A
The URL is fake
It’s urgent/scary
Asking for login info

Best Practices to Avoid Falling Victim to Phishing & Social Engineering

1. Think Before You Click
2.Never Share Personal Information
3. Check the Sender & URL Carefully
4. Stay Calm — Don’t Fall for Urgency
5. Use Strong, Unique Passwords
6.Enable Two-Factor Authentication (2FA)
7.Keep Software Updated
8. Don’t Plug in Unknown Devices

Conclusion: Stay Aware, Stay Safe

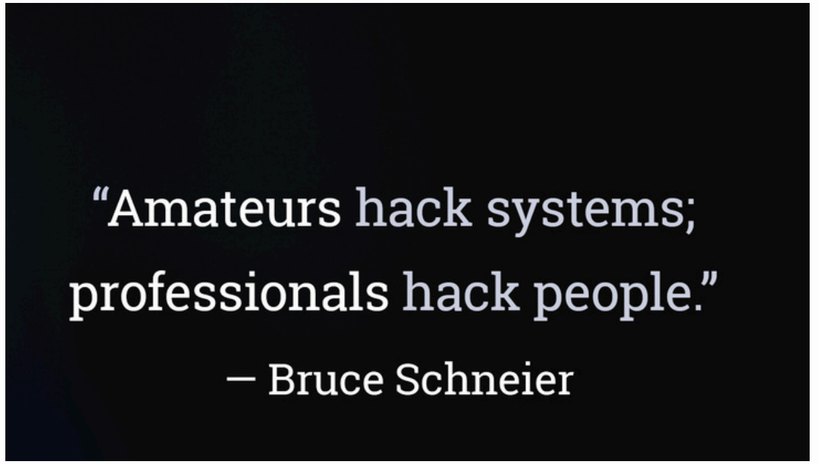
Phishing and social engineering attacks are everywhere — email, SMS, phone calls, even in person.

Attackers don't hack systems — they hack people.

Learn to spot red flags: suspicious links, urgent requests, unknown senders.

Always verify before you click, share, or act — even if it looks "official."

Use strong passwords, enable two-factor authentication, and report anything suspicious.



QUIZ

What is the most common goal of a phishing attack?

Ⓐ To update your email settings
Ⓑ To steal personal or financial information
Ⓒ To fix your internet speed
Ⓓ To advertise a pro
duct

Which website link is MOST likely fake?

Ⓐ www.amazon.com
Ⓑ www.amazon-login-help.com
Ⓒ www.amazon.in
Ⓓ https://www.amazon.com/orders

THANK YOU!

Cybersecurity starts with YOU!!

RIYA KHATRI
CODE ALPHA INTERN