Phishing Awareness Training

TASK 2

Oualid Bellali

December 25, 2025

Agenda

1. Introduction
2. Phishing Emails & Fake Websites
3. Social Engineering Tactics
4. Real-World Examples
5. Prevention Best Practices
6. Interactive Quiz
7. Conclusion

What is Phishing?

- A type of **cyber attack** that tricks users into revealing sensitive data
- Usually delivered via:
  - Emails
  - Fake websites
  - SMS or phone calls
- Goal: steal **passwords, credit card details, or personal data**

Phishing Emails

Common characteristics:

- Urgent or threatening language
- Suspicious sender address
- Unexpected attachments or links
- Requests for personal information

Fake Websites

- Look similar to real websites (banks, social media)
- Slightly altered URLs (e.g., paypa**I**.com instead of paypal.com)
- Lack of HTTPS or valid certificates
- Login pages designed to steal credentials

What is Social Engineering?

- Psychological manipulation to trick users
- Exploits human emotions:
  - Fear
  - Curiosity
  - Trust
  - Urgency

Common Social Engineering Techniques

- Impersonation (IT support, manager)
- Fake rewards or prizes
- Threats of account suspension
- Authority pressure ("Immediate action required")

Example 1: Fake Bank Email

Scenario:

- Email claims suspicious activity on your bank account
- Provides a link to ”verify” your identity

Example 1: Fake Bank Email

Scenario:

- Email claims suspicious activity on your bank account
- Provides a link to ”verify” your identity

Red Flags:

- Generic greeting
- Urgent tone
- Suspicious URL

Example 2: Company Email Scam

Scenario:

- Appears to come from your manager
- Requests gift cards or urgent payment

Example 2: Company Email Scam

Scenario:

- Appears to come from your manager
- Requests gift cards or urgent payment

Red Flags:

- Unusual request
- Pressure to act quickly
- External email address

How to Prevent Phishing Attacks

- Never click suspicious links
- Verify sender email addresses
- Do not share passwords or OTPs
- Use strong, unique passwords
- Enable Multi-Factor Authentication (MFA)

Best Practices at Work

- Report suspicious emails to IT/security
- Verify unusual requests via another channel
- Keep software and systems updated

Quiz Question 1

Which is a sign of a phishing email?

- A) Personalized greeting
- B) Urgent request for personal data
- C) Email from a known colleague

Quiz Question 1

Which is a sign of a phishing email?

- A) Personalized greeting
- B) Urgent request for personal data
- C) Email from a known colleague

Correct Answer: B

Quiz Question 2

What should you do if you receive a suspicious email?

- A) Click the link to check
- B) Reply asking for clarification
- C) Report it and delete it

Quiz Question 2

What should you do if you receive a suspicious email?

- A) Click the link to check
- B) Reply asking for clarification
- C) Report it and delete it

Correct Answer: C

Key Takeaways

- Phishing relies on deception and urgency
- Always verify before clicking or sharing data
- When in doubt, report it

Thank You

Questions?