### 

### TASK 2

### Introduction to Phishing.

* **What is Phishing?**
  + Definition: Phishing is a cyber attack that attempts to trick individuals into providing sensitive information (like passwords or credit card details) by pretending to be a trustworthy entity.
* **Statistics**
  + Mention recent statistics on phishing attacks to highlight their prevalence.

**Slide 2: Types of Phishing**

* **Email Phishing**
  + Fake emails that appear to be from legitimate sources.
* **Spear Phishing**
  + Targeted attacks on specific individuals or organizations.
* **Whaling**
  + Attacks that target high-profile individuals (e.g., executives).
* **Smishing and Vishing**
  + SMS phishing and voice phishing, respectively.

**Slide 3: Recognizing Phishing Emails**

* **Common Signs of Phishing Emails**:
  + Generic greetings (e.g., "Dear Customer").
  + Urgent or threatening language.
  + Poor grammar and spelling errors.
  + Suspicious links or attachments.
  + Unusual sender email addresses.

**Slide 4: Identifying Phishing Websites**

* **How to Spot a Phishing Website**:
  + Check the URL: Look for misspellings or unusual domains.
  + Look for HTTPS: Secure websites have "https://" in the URL.
  + Verify with official sources: Don’t rely on links in emails; go directly to the website.
  + Check for contact information and website quality.

**Slide 5: Social Engineering Tactics**

* **What is Social Engineering?**
  + Manipulation of individuals into divulging confidential information.
* **Common Tactics**:
  + Impersonation: Pretending to be someone you trust (e.g., tech support).
  + Creating a sense of urgency or fear.
  + Offering something too good to be true (e.g., free gifts).

**Slide 6: Real-World Examples**

* **Case Studies**
  + Share a few high-profile phishing incidents.
  + Discuss the impact on individuals and organizations.

**Slide 7: Best Practices to Avoid Phishing**

* **Stay Vigilant**:
  + Always verify the sender's identity.
  + Hover over links to see the actual URL before clicking.
  + Use anti-phishing tools and security software.
* **Educate Yourself and Others**:
  + Regularly participate in security training.
  + Share knowledge about phishing with colleagues and friends.

**Slide 8: Reporting Phishing Attacks**

* **How to Report**:
  + Report suspicious emails to your IT department or security team.
  + Forward phishing emails to relevant organizations (e.g., the FTC, anti-phishing organizations).
* **Importance of Reporting**:
  + Helps prevent further attacks and protects others.

**Slide 9: Interactive Quiz**

* **Test Your Knowledge**:
  + Create a few quiz questions to reinforce learning (e.g., identifying phishing signs).

**Slide 10: Resources**

* **Helpful Links**:
  + Websites for more information (e.g., FTC, Anti-Phishing Working Group).
  + Security awareness training resources.

**Conclusion**

* **Recap Key Points**:
  + Phishing is a common threat that can be avoided through awareness and vigilance.
* **Call to Action**:
  + Encourage participants to share what they’ve learned and to stay informed about cybersecurity.