This task is a great exercise for building awareness around phishing emails, a crucial component of cybersecurity. Here's how you can complete it step-by-step:

1. Research Common Characteristics of Phishing Emails

Start by researching the common signs of phishing emails. Here are the key points you should look for:

Suspicious Sender Address

- Phishing emails often come from email addresses that look suspicious, such as ones that are slightly altered from legitimate addresses. For example:
  - support@micrsoft.com (intended to look like Microsoft but with a typo).
  - security@paypall.com (PayPal with a misspelling).
- Pay close attention to domains and check for slight variations (e.g., pay-pal.com instead of paypal.com).

Generic Greetings

- Phishing emails often use vague greetings like:
  - "Dear Customer," "Dear User," "Dear Account Holder," instead of addressing you by name.
- Legitimate companies usually have your name in their emails if you're a customer.

Urgent or Threatening Language

- Phishing emails often contain phrases that try to rush you into acting quickly or creating fear, such as:
  - "Immediate action required!"
  - "Your account has been compromised, click here to verify your identity!"
  - "Failure to respond will result in account suspension."
- These are designed to pressure you into taking action before thinking critically.

Unexpected Attachments or Links

- Be cautious of attachments or links in unsolicited emails. For example:
  - Emails may contain a link that looks like it's leading to a legitimate site, but the URL is misleading.

- Common phishing links might look like "www.amazon-security-update.com" instead of the real "www.amazon.com."

- Attachments may contain malware or ransomware.

Grammatical or Spelling Errors

- Many phishing emails contain spelling mistakes, incorrect grammar, or awkward phrasing. Example:

  - "We have been noticing unusal activity in you account." (Notice the misspelling of "unusual" and "you" instead of "your").

- Legitimate emails from companies usually go through professional checks.

2. Email Analysis Exercise

To analyze phishing emails, you can look for real examples online. There are websites that provide sample phishing emails for educational purposes. A few reliable sources for this are:

- Phishing Email Databases : Websites like [PhishLabs](https://www.phishlabs.com), [APWG](https://apwg.org), or even government agencies like the [US-CERT](https://www.cisa.gov/uscert).

- Email Security Software Blogs : Many email security companies like [Proofpoint](https://www.proofpoint.com) or [Barracuda](https://www.barracuda.com) provide phishing email examples.

For each sample email, identify and note:

- The suspicious sender address
- The greeting style (generic or personalized)
- Any urgent or threatening language
- Presence of unexpected attachments or links
- Grammatical or spelling errors

3. Report Creation

Once you've analyzed a few emails, create a report with the following structure:

Report Outline

1. Introduction

- Briefly introduce phishing emails and why it’s important to recognize them.

2. Email 1: [Subject of Email]

- Sender : Mention the suspicious or unusual sender address.
- Greeting : Point out the generic or impersonal greeting.
- Urgent Language : Describe the threatening or urgent language used.
- Attachments/Links : Analyze the suspicious attachment or link (if any).
- Grammatical Errors : Mention any misspellings or awkward sentences.
- Suspicious Elements : Summarize why this email is suspicious.

3. Email 2: [Subject of Email]

- [Follow the same structure as above.]

4. Email 3: [Subject of Email]

- [Follow the same structure as above.]

5. Conclusion

- Summarize key takeaways on how to spot phishing emails. You could mention that the combination of poor grammar, suspicious links, urgent demands, and generic language are strong indicators of phishing.

4. Optional: Create a Phishing Email (Educational Purposes Only)

Important : Be sure to create this email purely for educational purposes and never use it for malicious intent. Here’s how you could create a basic phishing email using common tactics:

Example Phishing Email:

Subject : "Immediate Account Suspension – Action Required!"

From : security@amzon.com (a misspelling of Amazon)

Body :

Dear Customer,

We have detected suspicious activity on your Amazon account. To protect your account from being permanently suspended, please verify your identity immediately by clicking the link below:

[Click Here to Verify Your Account](http://www.amzon-verification.com) (note the fake link)

Failure to verify your account within the next 24 hours will result in permanent suspension.

Sincerely,

Amazon Security Team

Suspicious Elements:

- Sender : The email address contains a typo (amzon.com instead of amazon.com).
- Generic Greeting : It uses "Dear Customer" instead of your name.
- Urgent Language : The threat of "account suspension" and the urgency to act within 24 hours.
- Suspicious Link : The link looks suspicious with "amzon-verification.com," which is a fake site.
- Spelling and Grammar Errors : The email uses phrases like "permanent suspension" without proper phrasing.

---

5. Outcome

By completing this exercise, you'll be better equipped to:

- Spot the common signs of phishing emails.

- Safeguard your personal information and avoid falling for phishing attacks.

This is an essential skill in today's digital world to protect yourself from potential fraud, data theft, and other online security threats.

From Vamsi penumalla