INTERNSHIP ASSIGNMENT REPORT

Details Name: Putta Honna

Tools Used: -social-engineering toolkit, phishing attack

Operating System: Windows 11,kali Linux

1. Obtain a Sample Phishing Email

- **Action:** Search online for "phishing email samples" or "phishing awareness test examples." Many cybersecurity firms and security training platforms offer examples of common phishing lures (e.g., fake banking alerts, suspended account notices, prize winnings).
- **Goal:** The sample should contain all the typical elements: a sender address, a body of text, and a suspicious link or attachment mention.2. E:aming Sgndgr's Email Addrgss fior Spoofiing
- **Concept:** Phishers try to make the sender look legitimate. **Spoofing** means forging the sender's address.
- **Analysis Focus:**
  - **Subtle Mismatches:** Is it support@appple.com (extra 'p' or misspelled company name)? Is it microsoft-security@outlook.com (using a public email domain for a major company)?
  - **Display Name vs. Address:** The display name might say "IT Department," but the actual address might be random letters (e.g., xyd123@publicmail.net).

Example	Analysis
Legit: security@amazon.com	**Suspicious:** amazon_alert@mail-service.com

3. Check Email Headers fior Discrepancies

- **Concept:** The email header is the "postmark" of the email, containing technical routing information. This reveals the actual path the email took and the original server it came from, which often contradicts the claimed sender.

- **Action:**
  1. In your email client (like Gmail or Outlook), find the option to "View Headers."
  2. Copy the entire block of header text.
  3. Paste it into an **online email header analyzer** (e.g., Google's Messageheader tool, or similar free tools).
- **Analysis Focus:** Look at the **"Received from"** lines. If the email claims to be from a bank in London but the header shows it originated from a server in Eastern Europe, that's a major discrepancy.

4. Identifiy Suspicious Links or Attachments

- **Concept:** Phishing emails aim to steal credentials (via links to fake login pages) or install malware (via malicious attachments).
- **Action:**
  - **Links:** If your sample has a link, **do not click it.** Instead, **hover your mouse** over the link text. The actual destination URL will appear in the bottom corner of your browser or email client.
  - **Attachments:** Note the attachment type. Suspicious types include .exe, .scr, .zip, or documents like .docx or .pdf that contain macros.

5. Look fior Urgent or Threatening Language

- **Concept:** Phishers rely on **social engineering** principles like **urgency** or **fear** to bypass critical thinking.
- **Analysis Focus:** Look for phrases that demand immediate action:
  - "Your account has been **suspended**."
  - "Action required **within 2 hours** to avoid termination."
  - "Unauthorized login detected from a new location. **Click here NOW** to verify."
  - "You have won **$1,000,000**! Claim your prize immediately." (Greed/Opportunity)

6. Note Any Mismatched URLs

- **Concept:** This is the most direct evidence of a malicious link. The visible link text is often designed to look legitimate, but the actual destination is different.
- **Action:** Compare the visible link text with the URL revealed by hovering over it (as done in Step 4).

Visible Link Text	Actual Destination URL (on hover)	Result
https://secure.paypal.com/login	http://192.168.4.99/stolenin fo	**Phishing!** The link leads to a suspicious IP address.
https://mybank.com/reset	https://mybank.net.co/rese t	**Phishing!** Wrong domain extension (.net.co instead of .com).

7. Verifiy Presence ofi Spelling or Grammar Errors

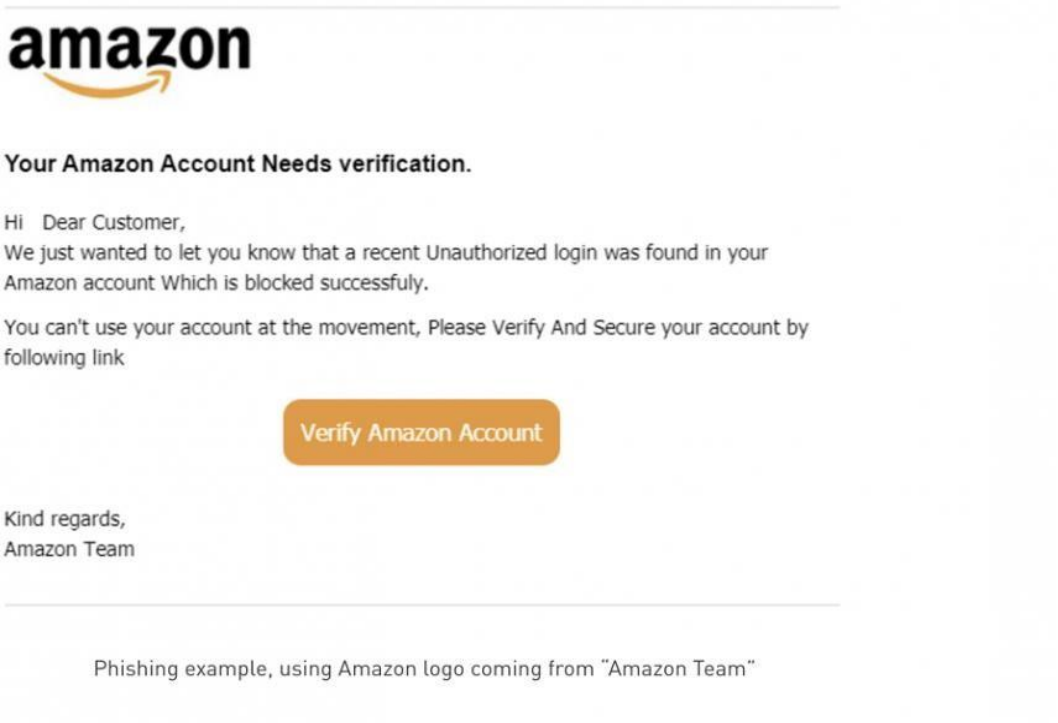
- **Concept:** While professional hackers can write flawless English, many mass-produced phishing kits are poorly translated or quickly written, leading to common errors.
- **Analysis Focus:** Look for:
  - Incorrect capitalization (e.g., "We need your **P**assword").
  - Awkward phrasing or unusual sentence structure.
  - Missing articles (e.g., "You must verify account details.").

8. Phishing Traits Found

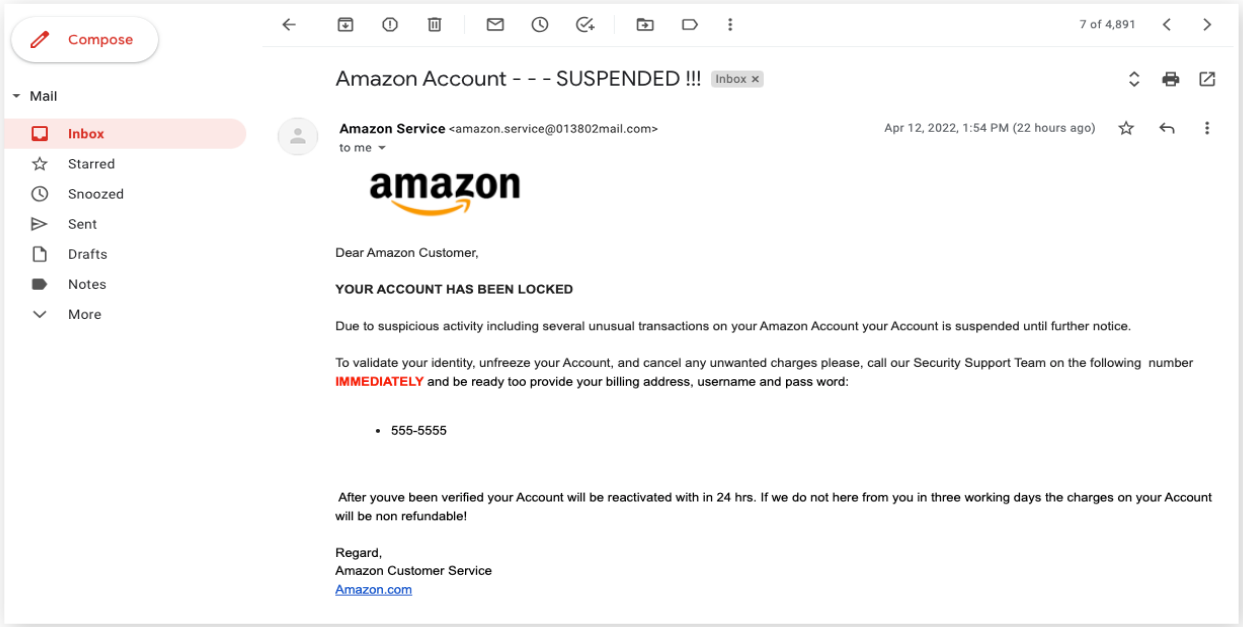
After going through all the steps, you will summarize your findings in a final report.

Phishing Trait	Found? (Y/N)	Details/Evidence from Sample
Spoofed Sender	Y	The email claimed to be from Amazon but came from amzn-security-alert@outlook.com.
Header Discrepancy	N	(If found, detail the difference in origin

		country)
Suspicious Link	Y	Link text said www.verify.com, but the actual URL was www.bad-server.xyz/login.php.
Urgent Language	Y	The subject line was: "**IMMEDIATE ACTION: Account Suspension!**"
Grammar Errors	Y	The body contained the phrase, "Need you respond now."



Phishing example, using Amazon logo coming from "Amazon Team"


Compose
Mail
Inbox
Starred
Snoozed
Sent
Drafts
Notes
More
7 of 4,891
Amazon Account - - - SUSPENDED !!!
Inbox ×
Amazon Service <amazon.service@013802mail.com>
to me
Apr 12, 2022, 1:54 PM (22 hours ago)
amazon
Dear Amazon Customer,
YOUR ACCOUNT HAS BEEN LOCKED
Due to suspicious activity including several unusual transactions on your Amazon Account your Account is suspended until further notice.
To validate your identity, unfreeze your Account, and cancel any unwanted charges please, call our Security Support Team on the following number IMMEDIATELY and be ready too provide your billing address, username and pass word:
555-5555
After youve been verified your Account will be reactivated with in 24 hrs. If we do not here from you in three working days the charges on your Account will be non refundable!
Regard,
Amazon Customer Service
Amazon.com