ELEVATE LABS INTERNSHIP - Day-2

Name : Mohamed Riyas J

Role: Cyber Security Analyst

Task: 02

Title: Analyze a Phishing Email Sample.

Date: 24-06-2025

Objective: Identify phishing characteristics in a suspicious email sample.

Tools: Email client or saved email file (text), free online header analyzer.

Deliverables: A report listing phishing indicators found

Tools Used

- **Email Client or Saved Email File** (Text Format)
- **Online Header Analyzer**: MxToolBox, Virus Total
- **Text Editor**: Notepad

Step-by-Step Process

1. **Obtain Sample Phishing Email**
   - Sourced examples from personal inbox.
2. **Analyze Sender's Email Address**
   - Checked for spoofed domains (e.g. <amazon@zyevantoby.cn>).
3. **Review Email Header**
   - Verified discrepancies using header analyzer tools.

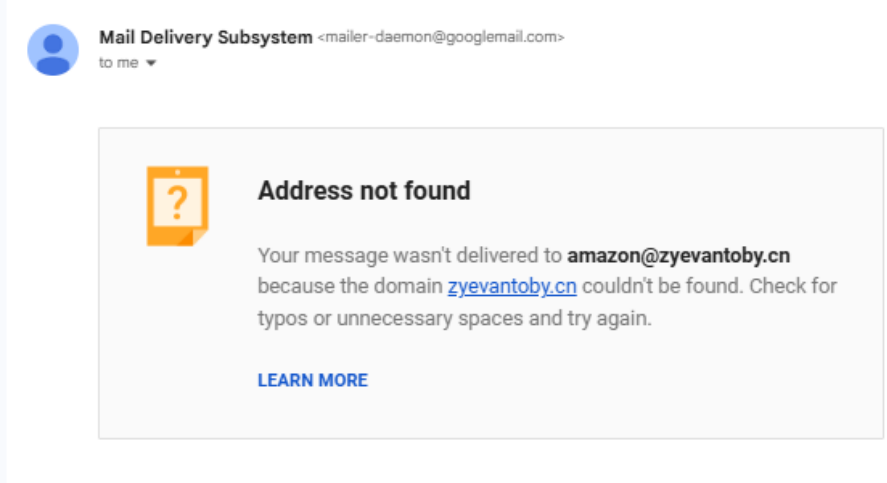
4. **Check Links/Attachments**
    - Hovered over links to detect mismatched URLs.
5. **Analyze Language**
    - Noted urgency and threatening tone in the email body.
6. **Grammar/Spelling Errors**
    - Identified poor grammar or spelling as an indicator.

Step 1 - Analysis Findings

- Sender's Email Address: Spoofed < amazon@zyevantoby.cn >

Step 2 - Email Header

- "Reply-To" address doesn't match sender's domain.



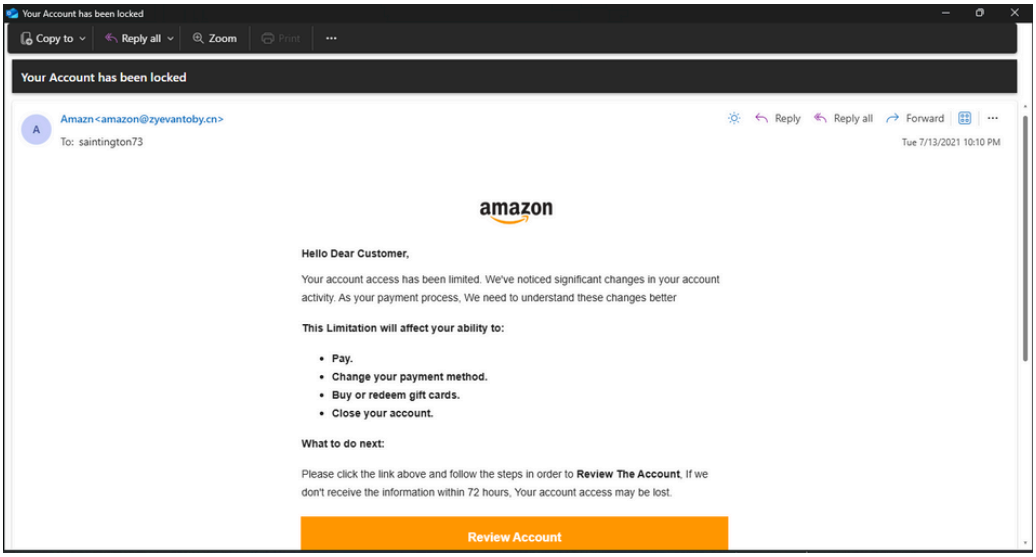
Step 3 - Suspicious Links

- Redirect to malicious domains

https://emea01.safelinks.protection.outlook.com/?url=https%3A%2F%2Famaozn.zzyuchengzhika.cn%2F%3Fmailtoken%3Dsaintington73%40outlook.com&data=04%7C01%7C%7C70072381ba6e49d1d12d08d94632811e%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C637618004988892053%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=oPvTW08ASiViZTLfMECsvwDvguT6ODYKPQZNK3203m0%3D&reserved=0

Step 4 - Urgent Language:

Your Account has been locked



Step 5 - Errors Grammar mistakes detected:

- Amazon is original but acctually appear Amazn

Step 6 - Key Indicators of Phishing

- Mismatched sender address or domain.
- Links redirect to suspicious websites.
- Presence of urgent/threatening tone.
- Poor grammar or spelling errors.

Step 7 - Outcome

- Improved awareness of phishing tactics.
- Gained hands-on experience analyzing phishing emails.
- Enhanced skills in identifying threats and mitigating risks.

Step 8 - Conclusion

- Phishing emails remain a significant threat to cybersecurity. With the right analysis tools and techniques, we can effectively identify and mitigate risks, ensuring better online safety.

Interview Questions

1. What is phishing?

Phishing is a cyber attack where attackers trick users into revealing sensitive information like passwords or credit card details) by pretending to be a trusted entity via email, message, or website.

2. How to identify a phishing email?

- Suspicious or unknown sender address
- Urgent or threatening language ("Verify now!", "Account will be locked")
- Misspellings or grammar errors
- Unusual links or attachments
- Mismatched email and display name

3. What is email spoofing?

Email spoofing is when an attacker forges the "From" address in an email to make it appear as if it came from a trusted source — used commonly in phishing to deceive the recipient.

4. Why are phishing emails dangerous?

- They can steal credentials
- Install malware/ransomware
- Trick users into sending money
- Compromise entire networks if clicked by employees

5. How can you verify the sender’s authenticity?

- Check email headers (Received SPF/DKIM/DMARC results)
- Hover over links without clicking
- Verify sender domain (e.g., @google.com vs @g00gle.com)
- Contact the sender through official channels

6. What tools can analyze email headers?

- MxToolbox (Header Analyzer)
- Google Admin Toolbox
- Mailheader.org
- Splunk / SIEM tools
- Built-in email clients (Outlook, Gmail "Show Original")

7. What actions should be taken on suspected phishing emails?

- Don’t click any links or download attachments
- Report to security team or use “Report Phishing” button
- Isolate the email (don’t forward)
- Use email header analysis tools
- Block sender/domain in email gateway

8. How do attackers use social engineering in phishing?

Attackers:

- Pretend to be someone trusted (CEO, HR, bank)
- Create urgency or fear to manipulate decisions
- Use personal info (from social media, data breaches) to increase believability

COMPLETED DAY 2 TASK ---------- xxxxxxx----------

-