

## DAY 2 - TASK 2

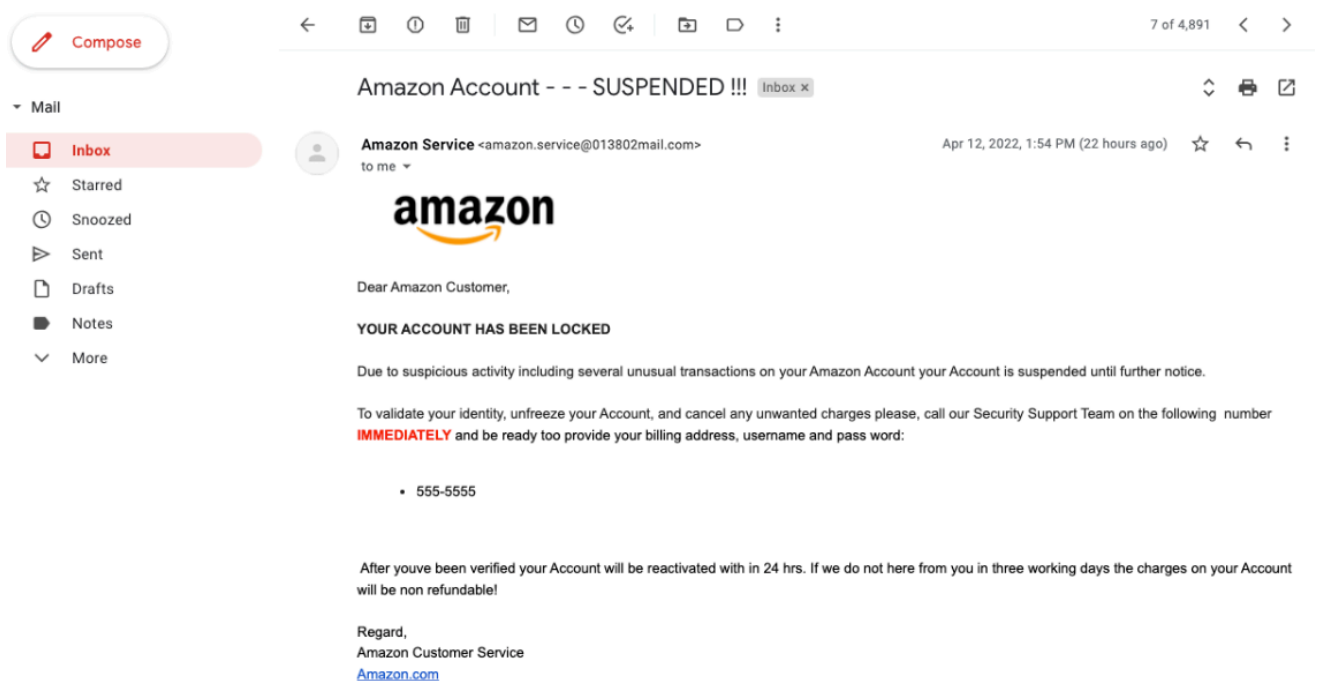
**Objective:** Identify phishing characteristics in a suspicious email sample.

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

**Deliverables:** A report listing phishing indicators found

## Phishing Indicators Report

**Objective:** To identify phishing characteristics in a suspicious email impersonating Amazon.



### Email Overview:

- Subject: Amazon Account – – – SUSPENDED !!!
- Sender Display Name: Amazon Service
- Sender Email Address: amazon.service@013802mail.com
- Date Received: April 12, 2022
- Target Brand: Amazon
- Email Type: Spoofed phishing attempt

### Phishing Indicators Found

#### 1. Spoofed Email Address -

- The sender email ([amazon.service@013802mail.com](mailto:amazon.service@013802mail.com)) is not a valid Amazon domain.
- Official emails from Amazon usually come from domains like [@amazon.com](mailto:@amazon.com).
- The display name "Amazon Service" is used to impersonate legitimacy.

## 2. Suspicious Email Header Traits (*headers not shown but expected to contain these red flags*):

- Possible SPF, DKIM, or DMARC failures.
- Return-path mismatch.
- Use of suspicious IPs or unknown relay servers.

## 3. Suspicious Links or Attachments

- Contains a **hyperlinked “Amazon.com”** text which may lead to a non-Amazon URL.
- Real links are not visible in the image, but hovering over them in an email client would reveal the actual (likely malicious) URL.
- Encourages user to call a **fake support number (“555-5555”)**, a classic phone phishing (vishing) tactic to extract sensitive details.

## 4. Urgent or Threatening Language

- The email includes emotionally triggering statements such as:
  - “YOUR ACCOUNT HAS BEEN LOCKED”
  - “Call our Security Support Team... IMMEDIATELY”
  - “If we do not hear from you... charges will be non-refundable!”
- These are designed to cause panic and prompt hasty action.

## 5. Mismatched URLs

- The visible link says “Amazon.com,” but it is likely spoofed.
- Without being able to hover and inspect, it remains suspicious, especially when paired with the overall phishing context.

## 6. Grammar and Spelling Errors

- Several language mistakes reduce credibility:
  - “After youve been verified...” → missing apostrophe in “you’ve”
  - “be ready too provide...” → “too” should be “to”

- “non refundable!” → should be hyphenated: “non-refundable”
- Awkward or unnatural phrasing like “pass word” instead of “password”

## 7. Psychological Triggers


- The email exploits fear and urgency to manipulate behavior:
  - Fear of losing account access.
  - Threat of financial loss (non-refundable charges).
  - Pressure to call immediately and provide personal details.

## Conclusion

This email is a **clear phishing attempt** designed to steal sensitive information by impersonating Amazon and invoking urgency and fear. It uses spoofed sender information, poor grammar, and manipulative language. Users should **not respond**, **not click links**, and **report the message** as phishing.

Additionally, adding some real- time observations made today using two platforms -

### ✓ PhishTank Verification

<div>  <b>PhishTank</b>® Out of the Net, into the Tank.         </div> <div> <input type="text" value="Username"/> <input type="password" value="*****"/> <input type="button" value="Sign In"/> </div> <div> <a href="#">Register</a>   <a href="#">Forgot Password</a> </div>				
<div> <a href="#">Home</a> <a href="#">Add A Phish</a> <a href="#">Verify A Phish</a> <a href="#">Phish Search</a> <a href="#">Stats</a> <a href="#">FAQ</a> <a href="#">Developers</a> <a href="#">Mailing Lists</a> <a href="#">My Account</a> </div>				
Verify A Phish				
Showing unverified and online submissions				
<a href="#">See all submissions in the phish archive</a>				
ID	Phish URL	Submitted	Valid?	Online?
<a href="#">9174657</a>	<a href="http://allegro.pl-9217435oferta.cfd">http://allegro.pl-9217435oferta.cfd</a> added on Aug 5th 2025 5:28 AM	by <a href="#">Amarena98</a>	Unknown	ONLINE
<a href="#">9174656</a>	<a href="http://allegro.pl-ogloszenia-firmowe-235242.icu...">http://allegro.pl-ogloszenia-firmowe-235242.icu...</a> added on Aug 5th 2025 5:28 AM	by <a href="#">Amarena98</a>	Unknown	ONLINE
<a href="#">9174650</a>	<a href="https://zufangshuo.com/v1/check">https://zufangshuo.com/v1/check</a> added on Aug 5th 2025 5:16 AM	by <a href="#">dms</a>	Unknown	ONLINE
<a href="#">9174647</a>	<a href="https://feilaiman.com/v1/check">https://feilaiman.com/v1/check</a> added on Aug 5th 2025 5:13 AM	by <a href="#">dms</a>	Unknown	ONLINE
<a href="#">9174646</a>	<a href="https://feilaiman.com/card.com/index.jp">https://feilaiman.com/card.com/index.jp</a> added on Aug 5th 2025 5:13 AM	by <a href="#">dms</a>	Unknown	ONLINE
<a href="#">9174642</a>	<a href="https://c72a89e6-a400-478b-b3fa-fe6cc71cb0fd-00-2pftrboxd76kr.nker.re...">https://c72a89e6-a400-478b-b3fa-fe6cc71cb0fd-00-2pftrboxd76kr.nker.re...</a> added on Aug 5th 2025 5:12 AM	by <a href="#">sodlatam</a>	Unknown	ONLINE
<a href="#">9174631</a>	<a href="https://feweixiang.com/v1/check">https://feweixiang.com/v1/check</a> added on Aug 5th 2025 5:10 AM	by <a href="#">dms</a>	Unknown	ONLINE
<a href="#">9174622</a>	<a href="http://scanmytrezor.com">http://scanmytrezor.com</a> added on Aug 5th 2025 5:08 AM	by <a href="#">r3gersec</a>	Unknown	ONLINE
<a href="#">9174605</a>	<a href="https://shoesrunning.store">https://shoesrunning.store</a> added on Aug 5th 2025 4:37 AM	by <a href="#">shershkop</a>	Unknown	ONLINE
<a href="#">9174600</a>	<a href="https://cmq332y.top/">https://cmq332y.top/</a> added on Aug 5th 2025 4:15 AM	by <a href="#">r3gersec</a>	Unknown	ONLINE
<a href="#">9174599</a>	<a href="http://cmq332y.top">http://cmq332y.top</a> added on Aug 5th 2025 4:15 AM	by <a href="#">r3gersec</a>	Unknown	ONLINE
<a href="#">9174593</a>	<a href="https://cpong1.net/">https://cpong1.net/</a>	by <a href="#">r3gersec</a>	Unknown	ONLINE

- URL: <https://feilaiman.com/v1/check>
- Added on: 5th Aug,2025 – 5:13 AM
- Status: Listed as ONLINE and suspicious (unverified but reported)
- Source: PhishTank - Verify A Phish

## ✓ VirusTotal Analysis

3 / 97  
Community Score

3/97 security vendors flagged this URL as malicious

<https://feilaiman.com/v1/check>  
feilaiman.com

Status: 404 | Content type: text/html | Last Analysis Date: a moment ago

Reanalyze | Search | More

DETECTION | DETAILS | COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

G-Data	Phishing	Google Safebrowsing	Phishing
Lionic	Phishing	Fortinet	Spam
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	Antiy-AVL	Clean

Do you want to automate checks?

- URL: <https://feilaiman.com/v1/check>
- Flagged by 4 security vendors:
  - G-Data: **Phishing**
  - Lionic: **Phishing**
  - Google Safe Browsing: **Phishing**
  - Fortinet: **Spam**
- Status Code: 404 (dead page but confirmed malicious in past)
- Content Type: text/html
- Screenshot Timestamp: Just analyzed

These real-time scans confirm the phishing nature of the suspicious link in the email.

https://feilaiman.com/v1/check

Sign inSign up

3/97

Community Score

3/97 security vendors flagged this URL as malicious

ReanalyzeSearchMore

https://feilaiman.com/v1/check  
feilaiman.com

Status404Content typetext/htmlLast Analysis Datea moment ago

text/htmlexternal-resources

DETECTION

DETAILS

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

G-Data	Phishing	Google Safebrowsing	Phishing
Lionic	Phishing	Fortinet	Spam
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	Antiy-AVL	Clean