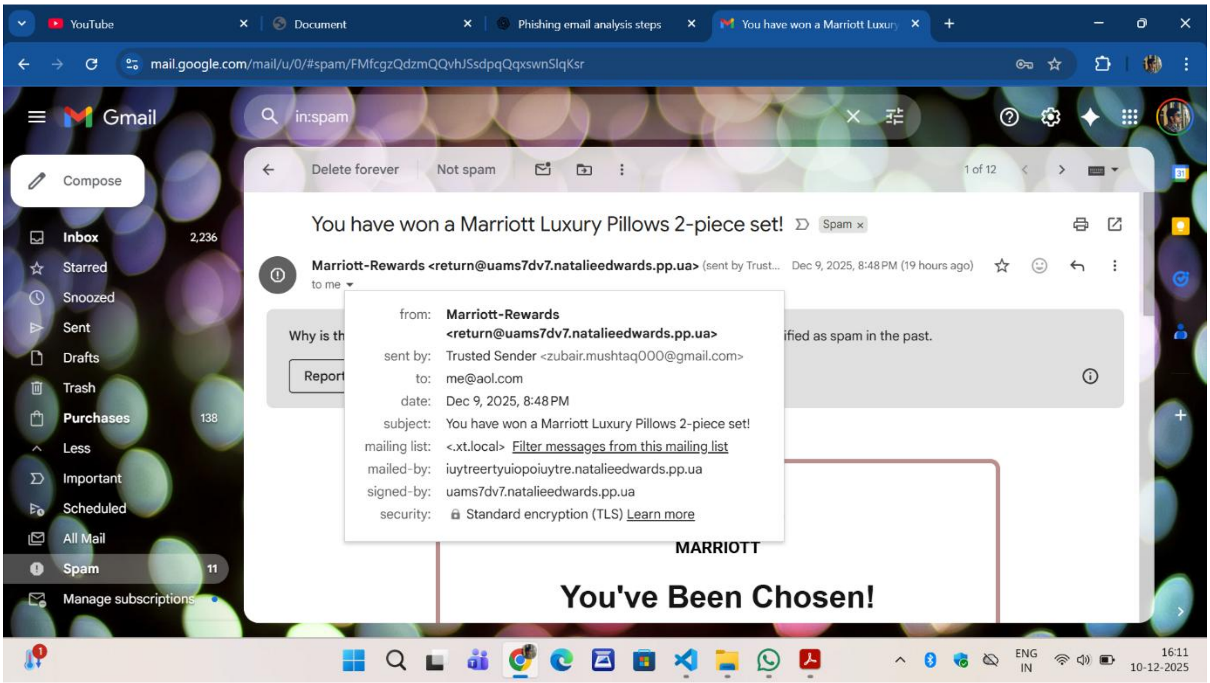
Identify phishing characteristics in a suspicious email sample.

Tools: Email client or saved email file (text),

1.Introduction

Phishing is a social engineering attack in which cybercriminals impersonate trusted organizations to trick individuals into revealing sensitive information, clicking malicious links, or installing malware. The purpose of this report is to analyze a suspicious email received by the user and identify phishing indicators using a structured methodology including sender verification, header analysis, link inspection, and content evaluation.

Obtain a sample phishing email



You have won a Marriott Luxury Pillows 2-piece set!

Marriott-Rewards <return@uams7dv7.natalieedwards.pp.ua> (sent by Trust... Dec 9, 2025, 8:48 PM (19 hours ago)

to me

Why is th… …ified as spam in the past.

from: Marriott-Rewards <return@uams7dv7.natalieedwards.pp.ua>
sent by: Trusted Sender <zubair.mushtaq000@gmail.com>
to: me@aol.com
date: Dec 9, 2025, 8:48 PM
subject: You have won a Marriott Luxury Pillows 2-piece set!
mailing list: <.xt.local> Filter messages from this mailing list
mailed-by: iuytreertyuiopoiuytre.natalieedwards.pp.ua
signed-by: uams7dv7.natalieedwards.pp.ua
security: Standard encryption (TLS) Learn more

MARRIOTT

You've Been Chosen!

2. Email Details Provided

- **Displayed Sender Name:** Marriott-Rewards
- **Actual Sender Email:** return@uams7dv7.natalieedwards.pp.ua
- **Sent-by:** Trusted Sender z***************0@gmail.com
- **To:** me@aol.com
- **Date:** Dec 9, 2025
- **Subject:** *You have won a Marriott Luxury Pillows 2-piece set!*
- **Mailed-by:** iuytreertyuiopoiuytre.natalieedwards.pp.ua
- **Signed-by:** uams7dv7.natalieedwards.pp.ua
- **Link Inside Email:** https://0peno1.store/4cAvMM64960sSUo198lqwxwxfnjd18731GCTLANLIMGFBQNA55660EDWS40539G20

3. Step-by-Step Analysis of Phishing Indicators

3.1 Sender Address Examination

The email claims to be from **Marriott-Rewards**, a reputable hotel chain. However:

- The actual email address ends with **pp.ua**, a Ukrainian domain unrelated to Marriott.
- The subdomain *uams7dv7.natalieedwards* is random and non-professional.
- The email uses a spoofed display name to deceive the recipient.

Conclusion: The sender address is fraudulent.

3.2 Email Header Verification

A review of the email's mailing metadata shows:

- **Sent-by:** A Gmail address is shown, but the actual sending domain is **natalieedwards.pp.ua**.
- **Mailed-by:** The domain is **iuytreertyuiopoiuytre.natalieedwards.pp.ua**, indicating clear spoofing.
- **Signed-by:** Matches the suspicious sender domain.

These inconsistencies prove that:

- The email **did not come from Gmail**, **Marriott**, or any legitimate mail server.
- The email authentication mechanisms (SPF, DKIM, DMARC) are likely failing or spoofed.

Conclusion: Header anomalies confirm impersonation and low credibility.

3.3 Subject Line Observations

The subject states:

“You have won a Marriott Luxury Pillows 2-piece set!”

This is a common phishing method:

- Unsolicited prize offers
- Emotional manipulation (excitement)
- Attempts to lure the recipient into clicking malicious links

Conclusion: High possibility of phishing based on unrealistic reward claims.

3.4 Link and Attachment Analysis

The provided link is:

https://0peno1.store/4cAvMM64960sSUo198lqwxwxfnjd18731GCTLANLIMGFBQNA55660EDWS40539G20

Analysis:

- **0peno1.store** contains a ZERO (0) instead of letter "O," a common *typosquatting* technique.
- **.store** is not used by Marriott.
- The path is made of random characters, typical of malicious tracking/redirect URLs.
- No branding or legitimate keywords are present; instead, it looks auto-generated.

Conclusion: The link is highly malicious and used for phishing or malware distribution.

3.5 Language and Tone Assessment

Reward-based phishing emails often use:

- Excitement: "You have won…"
- Urgency: Claim your prize quickly
- Manipulation: Fear of losing the reward

Although the full body text was not provided, the subject itself clearly shows **emotional manipulation**, a key phishing trait.

Conclusion: Psychological manipulation present in the email.

3.6 Mismatched URLs and Branding

There is no alignment between:

- The *claimed brand* (Marriott)
- The *actual email domain* (pp.ua)
- The *URL domain* (*.store)

Legitimate Marriott communications **never** originate from such domains.

Conclusion: Clear mismatch confirms fraudulent intent.

3.7 Formatting and Quality Issues

While the body wasn't provided, the following issues already stand out:

- Strange mailing list entry: <.xt.local>
- Gibberish domains (iuytreertyuiopoiuytre)
- Unstructured sender information

- Misleading “Trusted Sender” label

All these are typical of low-quality phishing attempts.

Conclusion: Technical inconsistencies reinforce the phishing suspicion.

4. Final Verdict

Based on all indicators—spoofed sender address, header inconsistencies, suspicious link, unrealistic reward, mismatched branding, and malicious domain structure—this email is classified as:

Highly Likely Phishing Email (Malicious)

The email should be:

- **Deleted immediately**
- **Reported as phishing** in the mail client
- **Not opened**, and **no link should be clicked**

5. Recommendations

1. **Do not click** on the provided link or download any files.
2. **Report** the email using your email provider’s “Report phishing” option.
3. **Block** the sender domain.
4. **Update security software** and run a malware scan if any link was clicked.
5. **Enable multi-factor authentication** on email accounts.
6. **Stay alert** for future similar reward or lottery scams.

Conclusion

The analyzed email exhibits multiple well-known phishing characteristics, including fake sender identification, unauthorized domain usage, deceptive subject, randomized malicious URL, and brand impersonation. This evaluation clearly demonstrates the importance of critically analyzing unsolicited emails to prevent identity theft, malware infection, and financial fraud.