Task: Analyze a Phishing Email Sample

File Analyzed: .eml file

Step One: Description of the Email

The phishing email claims to notify the recipient about a successful cryptocurrency withdrawal. The subject line reads:

[Binance] Withdraw Successful - 2023-07-30 51:51:51 (UTC)

It pretends to be an official alert from the Binance exchange about a completed transaction.

Step Two: Analysis of Sender's Email Address

From: Binance noreply-supportbinancewallet.irs@auswestbc.com.au

The sender domain is clearly unrelated to Binance. The legitimate Binance domain is **binance.com**, while this one uses a suspicious **.com.au** domain.

This strongly suggests the sender address is spoofed.

Conclusion: The sender is fake and impersonating Binance.

Step Three: Header Discrepancy and Authentication Check

Method Used: MXToolbox Email Header Analyzer and manual inspection

- The email was sent using Amazon SES (Simple Email Service).
- SPF and DKIM passed, meaning the domain is authorized to send emails.
- However, DMARC is missing, and none of the domains in the header relate to Binance.

Conclusion: The authentication setup is not aligned with real Binance email practices. This is suspicious.

Step Four: Suspicious Links and Attachments

- **Attachments:** No file attachments were found.
- **Hyperlink in Body:** The link says “cancel this transaction” but redirects to a third-party domain:
  `https://shylshom.com`

This domain has no connection with Binance and is potentially dangerous.

Conclusion: This is a clear phishing attempt using a malicious link.

Step Five: Use of Urgent or Threatening Language

The email body contains phrases such as:

“Don't recognize this activity? Please cancel this transaction to protect yourself from fraud.”

This is a common scare tactic meant to push users to act without thinking.

Conclusion: The email uses fear-based language to manipulate the reader.

Step Six: URL Mismatch

The displayed link says one thing, but the actual URL is different.

- **Shown text:** cancel this transaction
- **Actual link:** `https://shylshom.com`

There is no trace of **binance.com** in the destination link.

Conclusion: This is a common phishing trait involving mismatched URLs.

Step Seven: Spelling and Grammar Check

- The time in the subject line is **51:51:51 (UTC)**, which is not a valid timestamp.
- There are awkward sentences and inconsistent capitalization.
- Example: *“Please cancel this transaction including face verification to protect you.”*

Conclusion: Several signs of poor grammar and unprofessional formatting are present.

Step Eight: Summary Table of Phishing Traits

Trait	Status	Explanation
Spoofed Sender	Confirmed	Uses unrelated .com.au domain pretending to be Binance
Header Authentication	Suspicious	SPF and DKIM passed but no DMARC, not Binance-signed
Malicious Link	Confirmed	Link to unknown domain (shylshom.com)
Threatening Language	Confirmed	Attempts to scare the user with fake alerts
URL Mismatch	Confirmed	Text and actual link do not match
Spelling/Grammar	Noted	Contains formatting and grammar issues
Attachments	None	No files were attached

Final Conclusion

This email is a phishing attempt. It impersonates Binance by spoofing the sender’s address and uses urgent messaging to pressure the recipient. The link leads to an unknown domain, likely designed to steal login information or personal data.

Recommendation: This message should be deleted immediately, and the incident can be reported to the legitimate Binance support or a cybersecurity authority.