Phishing Email Analysis Report

1. Sender

Name: Angela

Email: evinog3@gmail.com

Not a known contact; suspicious Gmail sender

2. Subject & Language

Emotionally manipulative content

Claims past relationship to bait user

Social engineering via guilt and adult themes

3. Suspicious Links

http://lovegfriend.fun/?gallery&s=Beauty_135z

http://adultflirt.beauty/?&s_dis=tracking101_3&gallery

Unsecure (HTTP), unrelated to any legitimate service

Likely scam or malware redirection

4. Attachments

None, but links serve as payload

5. Repeated Behavior

Same message sent on multiple dates (June 2024, Nov 2024, May 2025)

Signs of automated or bulk phishing

Phishing Email Analysis Report

6. Header Analysis

[Pending - use header analyzer to confirm SPF/DKIM]

Likely spoofed or sent from a botnet

Conclusion

This is a phishing email attempting to lure the recipient into clicking malicious links by pretending to be a long-lost acquaintance. The message uses emotional manipulation, suspicious links, and unsafe domains. It should be reported and deleted.

Action Taken

Marked as spam

Did not click links

Shared with cybersecurity instructor for analysis

Key Learning Points

What is phishing?

- Fake messages that trick users into clicking or giving personal info

How to identify phishing?

- Unknown sender, emotional bait, unsafe links, urgency

What is spoofing?

- Faking the sender's address

Phishing Email Analysis Report

Why is phishing dangerous?

- Can steal data, install malware, or trick users into payment

How to verify sender?

- Analyze headers, domain, check links

Header analysis tool?

- MxToolbox, Google Admin Toolbox

Action on phishing?

- Report, don't reply, don't click, delete

Social engineering?

- Using emotion or fake relationships to manipulate you