DAY 2 - PHISHING ANALYSIS TASK

BY

SANTHOSHKUMAR

I GOT REAL PHISHING MAILS

Angela Fri, May 9, 12:54 AM
to me

It's been a significant period, I've been wondering if you are holding up and have been out of touch. I had an profound connection to what we had and kinda yearn for our daily conversations. Are things on track in your corner of the world? I hope all is fine for you out there. If not, it would be fantastic to catch up someday or meet up. I'm interested about the sudden silence after our chats. You should've said if something was amiss. I understand things ended abruptly, but it's not pleasant to be left in the dark after our online exchanges. You simply disappeared. I don't even know your real name or what you look like. So, let's be straightforward, did you vanish because I shared my unconventional photos and proposed a friends-with-benefits arrangement?
I just shared with you this http://adultflirt.beauty/?&s_dis=tracking101_3&gallery

---

Hi Santhosh! It's my new e-mail. Inbox ×

Kimberly <evdokiaguranova45@gmail.com> Fri, May 23, 12:25 PM (4 days ago)
to me

Santhosh Hello!

Smartkingsanthosh Inbox ×

Mary <maruntkovala@gmail.com> Tue, May 13, 2:58 AM
to me

Email for you, Smartkingsanthosh.

Nancy Thu, Mar 23, 2023, 12:17 AM
What are you doing Santhosh?

5

Nancy Tue, May 14, 2024, 12:55 PM
Cute Hi, remember me? Lets talk here: http://dating-photos.click/?gallery&s=Beauty_135z ! Find me, My nick name is Beauty_135z

Nancy <dalilomalish@gmail.com> Mon, Dec 9, 2024, 6:00 PM
to me

Cute Hello, remember me?
Lets chat here: http://love-dating.beauty/?gallery&s=Beauty_135z !
Find me, My nickname is Beauty_135z

DOES IS IT SEEM TOO GOOD TO BE TRUE?

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

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

HOW TO ANALYZE A PHISHING EMAIL (REAL-TIME TASK)

✅ Step 1: Get a Phishing Email Sample

Source: Real email received by me (Santhoshkumar).
Saved content directly from Gmail interface.

✅ Step 2: View the Sender's Email Address

From: Angela <evinog3@gmail.com>
- Name looks normal, but email is generic and not associated with any legitimate organization.
📌 Phishing Indicator: Suspicious sender using Gmail, no official domain.

✅ Step 3: Analyze Email Headers

[Header analysis should be done using tools like MxToolbox or Google Admin Toolbox]
- In this case, Gmail marked it as spam and failed SPF check.
📌 Phishing Indicator: Header fails authentication, possible spoofing.

✅ Step 4: Inspect Links

Examples from email:
- http://lovegfriend.fun/?gallery&s=Beauty_135z
- http://adultflirt.beauty/?&s_dis=tracking101_3&gallery
📌 Phishing Indicator: Unsecured HTTP links, adult themes, unrelated to any context.

✅ Step 5: Check for Suspicious Attachments

- No attachments, but dangerous links act as payloads.
📌 Phishing Indicator: Phishing via malicious links instead of files.

✅ Step 6: Look at the Language

- Manipulative emotional bait (“Do you remember me?”)
- Guilt-based text (“You disappeared after I shared my pictures.”)
- Some grammar issues and strange sentence structure.
📌 Phishing Indicator: Social engineering tactics and poor grammar.

✅ Step 7: Summarize the Phishing Traits

- Spoofed or fake sender address
- Suspicious links with hidden intent
- Emotional manipulation and guilt trips
- Likely part of a mass phishing campaign (repeated message over time)

CYBERCRIME AWARENESS

Think Before You Click
Avoid suspicious links and unknown attachments.

Protect Your Passwords
Use strong, unique passwords for every account.

Update Regularly
Keep your software and antivirus up to date.

Beware of Phishing
Don’t share personal info via email or messages.