Phishing Investigation Report
A Digital Detective's Case File

Srikanti Krishna Sai Pavan May 27,

2025

File Name: Phishing_Investigation_Report.pdf

Case File: The Suspicious Email Mystery

Let's dive into the evidence!

1. Tools of the Trade

Every detective needs their gadgets:

- **Email Client:** My magnifying glass to inspect the email's surface.
- **Online Header Analyzer:** A high-tech device to trace the email's origins.

2. The Evidence: A Suspicious Email

I obtained a sample email that raised my suspicions. Here's the exhibit:

```
Subject: Urgent: Your Account Will Be Deactivated!!!

Dear Customer,

We've detected unusual activity on your account. If you don't verify your

Click here to verify: http://secure-login.net/update

Best regards,
Your Bank Team
support@yourbannk.com
```

3. Step-by-Step Investigation

3.1 Step 1: Examining the Sender's Identity

The email claims to be from "Your Bank Team" with the address `support@yourbannk.com`. A closer look reveals a clue: "yourbannk" is misspelled—it should be "your-bank"! This is a classic sign of spoofing, where the sender pretends to be a legitimate entity.

3.2 Step 2: Digging into the Email Headers

I copied the email headers and ran them through an online header analyzer. The results showed the email originated from a domain in a foreign country, not matching the bank's official domain (`yourbank.com`). The "Received" fields also indicated multiple suspicious hops—a clear red flag!

3.3 Step 3: Investigating Links and Attachments

The email contains a link: `http://secure-login.net/update`. The domain `secure-login.net` doesn't match the bank's official website. Hovering over the link (without clicking!) reveals it redirects to a completely different URL:

`http://shady-site.xyz`. No attachments were present, but the link alone is highly suspicious.

3.4 Step 4: Analyzing the Language

The email screams urgency with phrases like "Urgent: Your Account Will Be Deactivated!!!" and "within 24 hours." This pressure tactic is a common phishing trick to make the recipient act without thinking.

3.5 Step 5: Spotting Spelling and Grammar Errors

The email contains a glaring typo: "permanantly" instead of "permanently." This sloppy mistake is a telltale sign of a phishing attempt, as legitimate companies usually proofread their communications.

4. Evidence Summary: Phishing Indicators

After a thorough investigation, I compiled the following clues:

- **Spoofed Sender:** The email address `support@yourbannk.com` has a misspelled domain.
- **Header Discrepancies:** The email's origin doesn't match the bank's official domain.
- **Suspicious Link:** The link leads to a shady domain, not the bank's website.
- **Urgent Language:** The email uses threatening phrases to create panic.
- **Spelling Error:** "Permanantly" is misspelled, indicating a lack of professionalism.

5. Key Takeaways

This case taught me that phishing emails are like wolves in sheep's clothing—they disguise themselves as trustworthy but reveal their true nature upon closer inspection. Always verify the sender, check links carefully, and never fall for urgent threats!

6. Closing Thoughts

Like a true digital detective, I've learned to spot the hidden tricks of cybercriminals. This investigation not only honed my email analysis skills but also deepened my appreciation for staying vigilant in the wild world of the internet.