Report on Email Phishing

Performer: Aditya Kamble

Tool Reference: saved email file (text), free online header analyzer, Google Search, Gemini.

Report Type: Manual Email Phishing Report

A specified report on Email Phishing and their consequences to make sure that mail came from a trusted organization.

Email Format:

From: Security-Alert@online-banking-support.net

To: aditay.kamble@gmail.com

Subject: Detected unusual login activity on your online banking account

Dear Valued Customer,

We have detected unusual login activity on your online banking account. For your protection, we have temporarily suspended certain functionalities to prevent any unauthorized transactions.

Details of Suspicious Activity:

- **Date:** 2025-05-27.
- **Time:** 11:00 AM.
- **Location:** Pune, India.

To reactivate your account and verify your recent activity, you are required to immediately click on the secure link below and follow the instructions:

Verify Your Account Now

Important: If you do not verify your account within 24 hours, your online access will be permanently locked, and you may need to visit a branch to regain access.

We are committed to maintaining the highest security standards for your account. Thank you for your prompt attention to this matter.

Sincerely,

The Security Department,

> Global Trust Bank,
>
> Customer Support.

Why this is a Phishing Email (Key Indicators):

1. **Suspicious Sender Address:** The "From" address Security-Alert@online-banking-support.net is not the official domain of a real bank. Banks typically use their established domain (e.g., yourbankname.com). The use of .net or other unusual top-level domains is a common trick.

2. **Urgent and Threatening Subject Line:** "Urgent Security Alert," "Unusual Activity Detected," and the threat of "permanently locked" account create fear and pressure to act quickly without thinking.

3. **Generic Greeting:** "Dear Valued Customer" instead of your actual name. While some legitimate mass emails might use this, it's a strong indicator when combined with other red flags.

4. **Sense of Urgency in Body:** Phrases like "immediately click," "required to immediately," and "within 24 hours" are designed to bypass critical thinking.

5. **Call to Action with Suspicious Link:** The text "Verify Your Account Now" looks legitimate, but the underlying URL (http://www.secure-bank-login.info/verify?id=user123456) is clearly not from a reputable bank. It uses a different domain (.info) and is likely designed to mimic a login page to steal credentials. **(Remember: Hover, don't click!)**
6. **Lack of Personalization:** Beyond the generic greeting, there's no specific account number or other personal identifiers that a legitimate bank would often include in such an alert.

7. **Threat of Consequences:** The warning about permanent lock-out if action isn't taken reinforces the urgency and fear.

8. **Poorly Formatted/Generic Closing:** "The Security Department" and "Customer Support" are generic and lack specific contact names or details that a legitimate bank might provide.