Phishing Email Detection & Awareness Report

Educational Phishing Analysis

Prepared By: Tanmay Bundele

Phishing Email Detection & Awareness Report

Cyber Security Internship – Future Interns (2026)

Prepared By: “Tanmay Bundele”

Scope: Educational Phishing Analysis (No exploitation performed)

1. Objective

The objective of this task is to analyze a phishing email sample, identify key phishing indicators, classify the associated risk, and create an awareness document to help users recognize and avoid phishing attacks.

2. Tools Used

- VirusTotal (URL Reputation Analysis)
- WHOIS Lookup (Domain Investigation)
- Manual Email Content Analysis
- Browser-based security investigation tools

3. Email Sample Overview

Subject: ⚠ Urgent: Your Account Will Be Locked

The email claims suspicious account activity and pressures the user to verify their details using an external link within 24 hours.

4. Identified Phishing Indicators

- Generic greeting (“Dear User”)
- Urgent and fear-based language
- Suspicious HTTP link
- No official company identity or signature

5. Domain & URL Investigation

The URL provided in the email was analyzed using VirusTotal and WHOIS lookup.

- The domain is not associated with any legitimate organization.

- The link uses HTTP instead of HTTPS.

- Domain reputation was low or limited.

- WHOIS information suggests suspicious or limited domain registration data.

5.1 VirusTotal Analysis

The suspicious URL was analyzed using VirusTotal to check reputation across multiple security vendors.

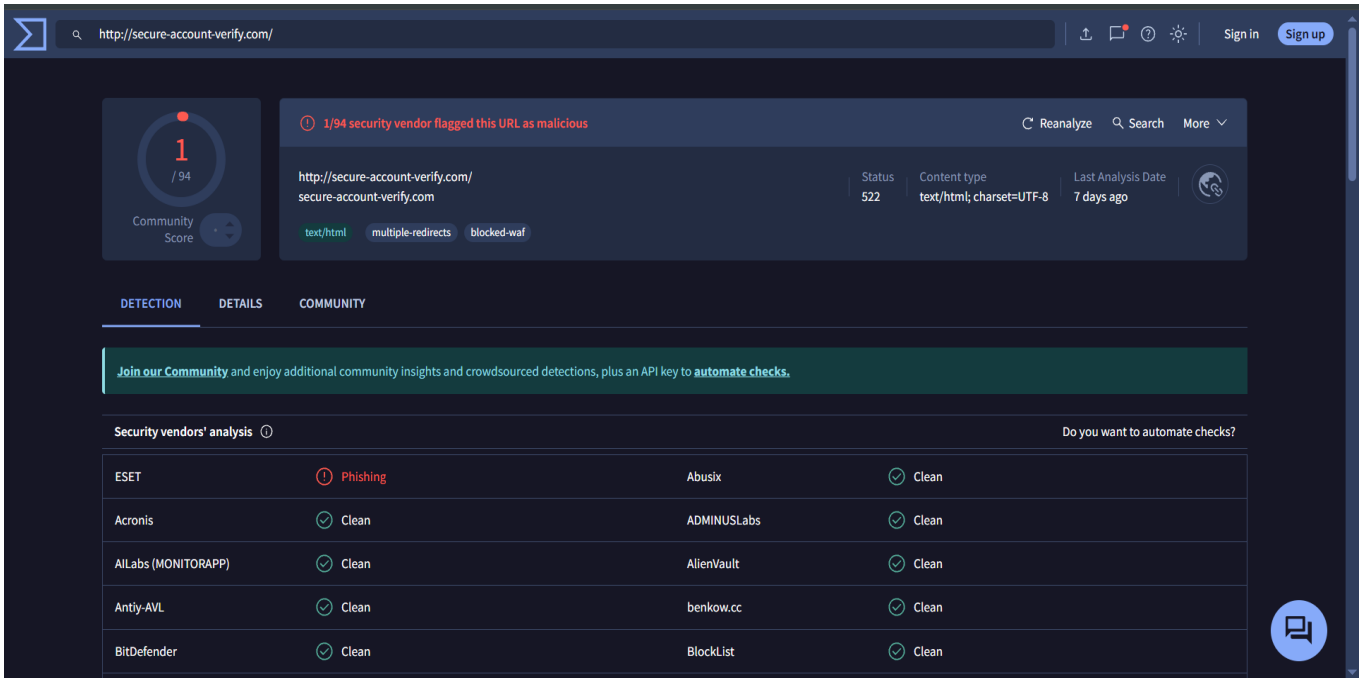

Figure 1: VirusTotal analysis showing phishing detection flag.

5.2 WHOIS Domain Investigation

WHOIS lookup was performed to examine domain registration details and ownership transparency.

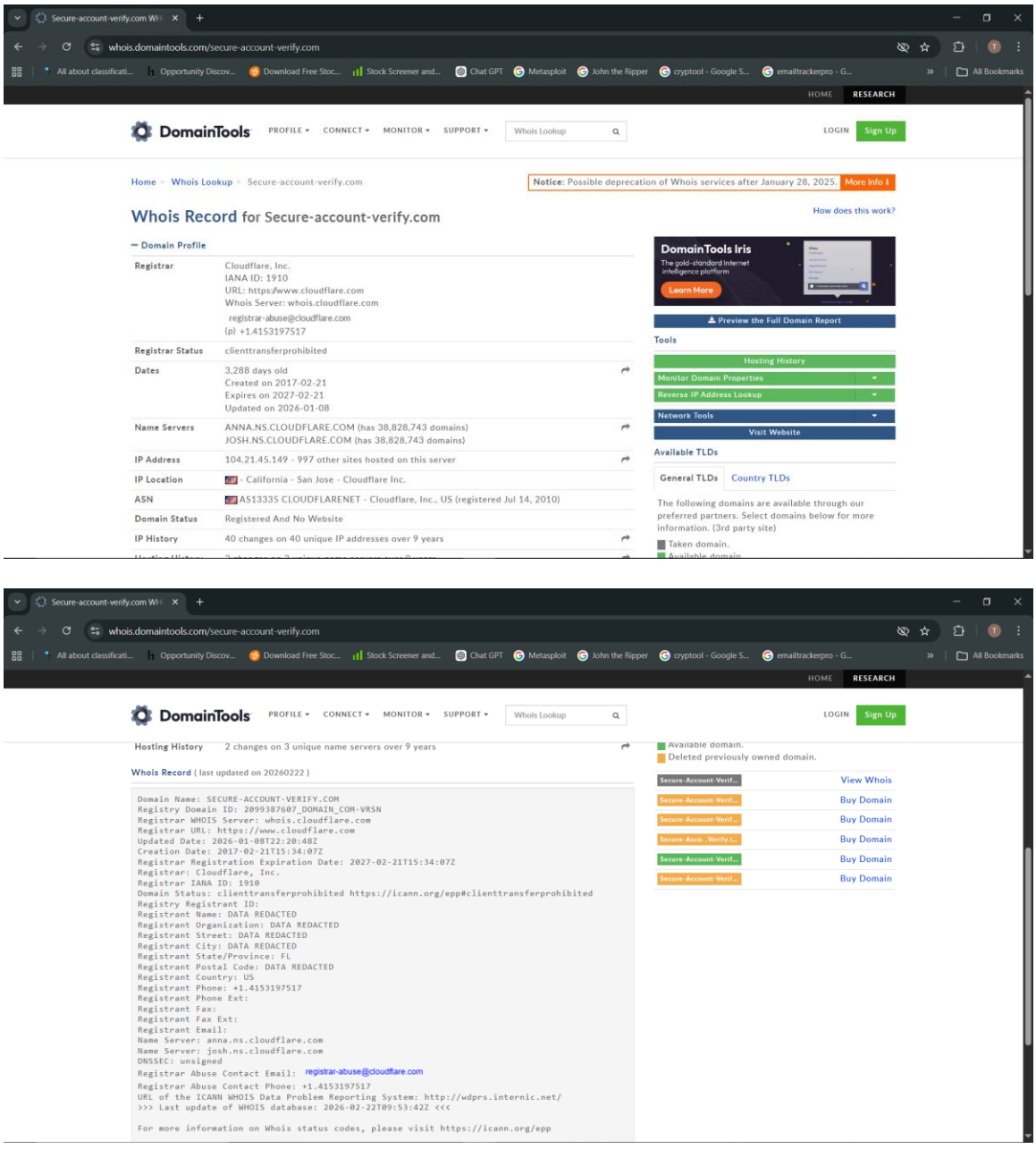

Figure 2: WHOIS lookup showing domain registration and redacted owner details

Analysis Summary:

- Domain registered via Cloudflare
- Registrant details redacted
- Suspicious behavior observed
- Classified as High Risk

6. Risk Classification

Email Type: Phishing

Risk Level: High

The email contains multiple phishing indicators and attempts to trick users into providing sensitive information via a suspicious external link.

7. How the Phishing Attack Works

The attacker sends an urgent message to create fear. The user clicks the malicious link. The fake website may collect credentials or sensitive data.

8. Prevention & Awareness Guidelines

How Users Can Protect Themselves:

- Verify sender domain carefully.
- Avoid clicking urgent links.
- Hover over links before clicking.
- Never share passwords or OTPs.
- Enable Two-Factor Authentication (2FA).
- Report suspicious emails immediately.

Do’s and Don’ts for Employees:

DO:

- Verify suspicious emails.
- Check formatting and spelling errors.
- Use security scanning tools.

DON’T:

- Click unknown links.
- Download unexpected attachments.
- Share login credentials.
- Trust generic greetings.

9. Conclusion

This analysis demonstrates how phishing emails exploit urgency and user trust. Proper awareness and verification practices significantly reduce the risk of phishing attacks in organizations.