TASK 2: ANALYZING A PHISHING EMAIL SAMPLE

Cybersecurity Lab Report

VOONNA VENKATESH
ELEVATE LABS

Task 2:

Analyze a Phishing Email Sample

Index

1. Obtain a sample phishing email
2. Examine senders email address for spoofing
3. Check email headers for discrepancies.
4. Identify suspicious links or attachments
5. Look for urgent or threatening language in the email body
6. Note any mismatched URLs
7. Verify presence of spelling or grammer errors

Objective

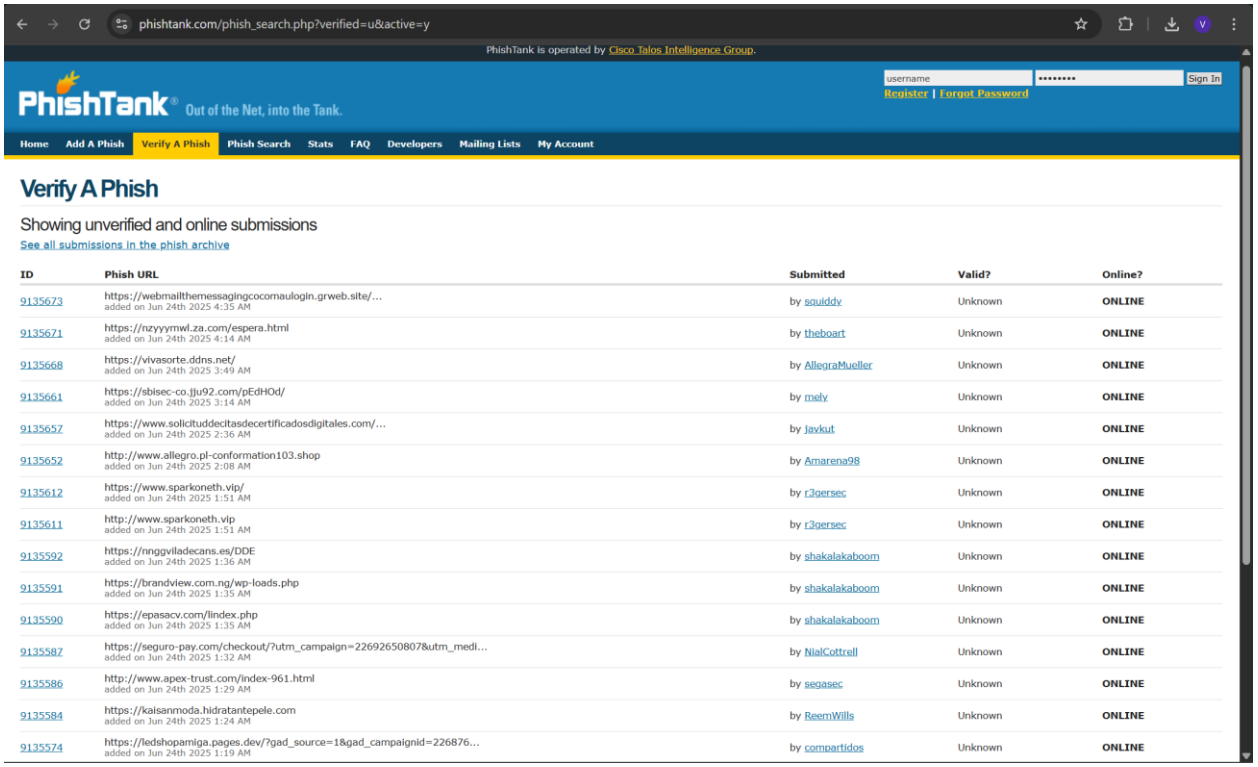
Identify phishing characteristics in a suspicious email sample.

Tools Used

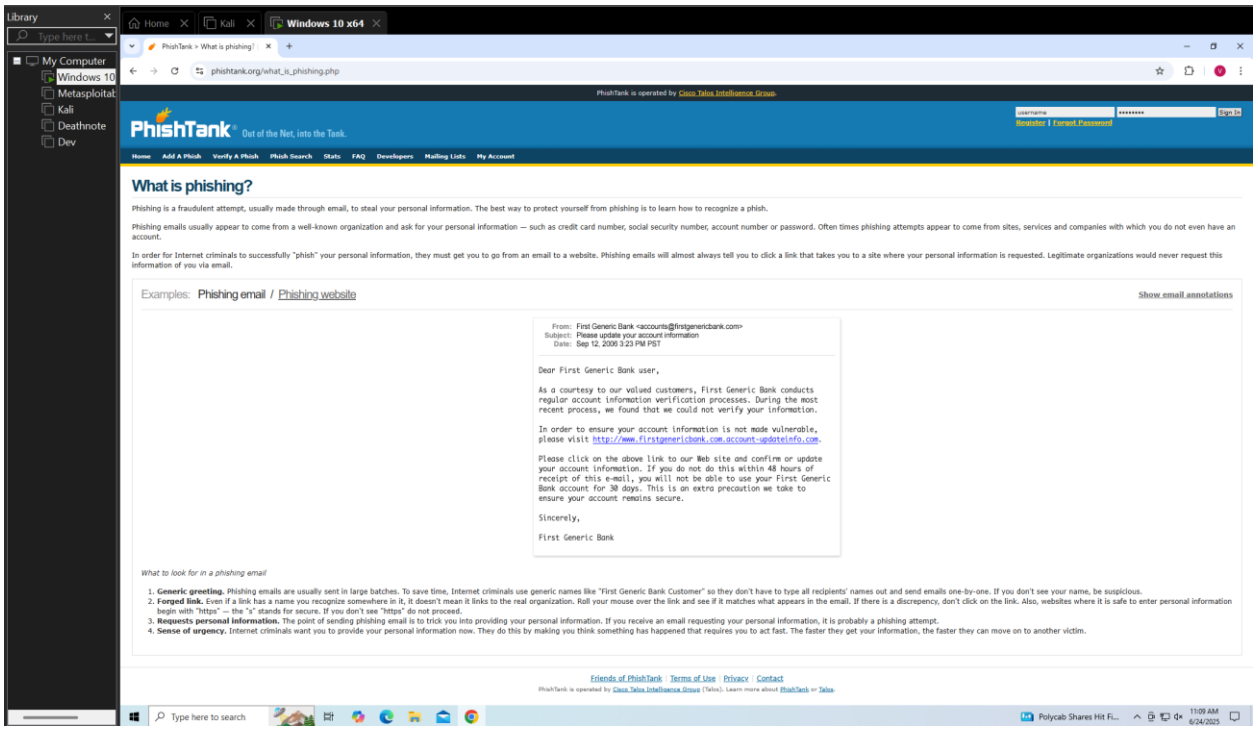
- PhishTank
- MXToolbox
- Virustotal
- WHOIS Lookup

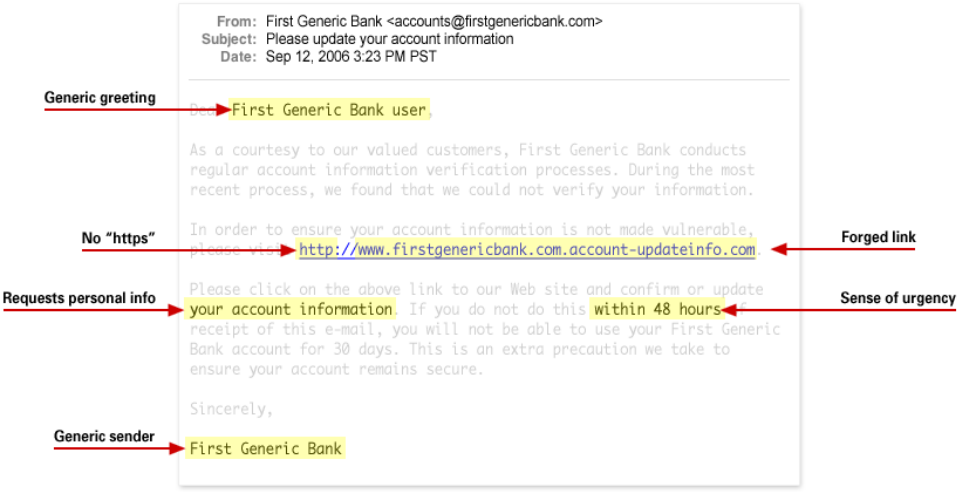
Steps Performed:

1. Obtaining a sample phishing email



Sample mail:





As we cannot get the original/actual phishing email lets create a phishing email which consists of a phishing link.

Link: https://smbc-cardbv.icu/login.php

From: SMBC Bank support@smbc-bank.co.jp
To: user@example.com
Subject: URGENT: Suspicious Activity Detected in Your SMBC Account

Dear Customer,

We have detected suspicious login attempts to your SMBC account. To protect your account, we require you to verify your information immediately by logging in at the link below:

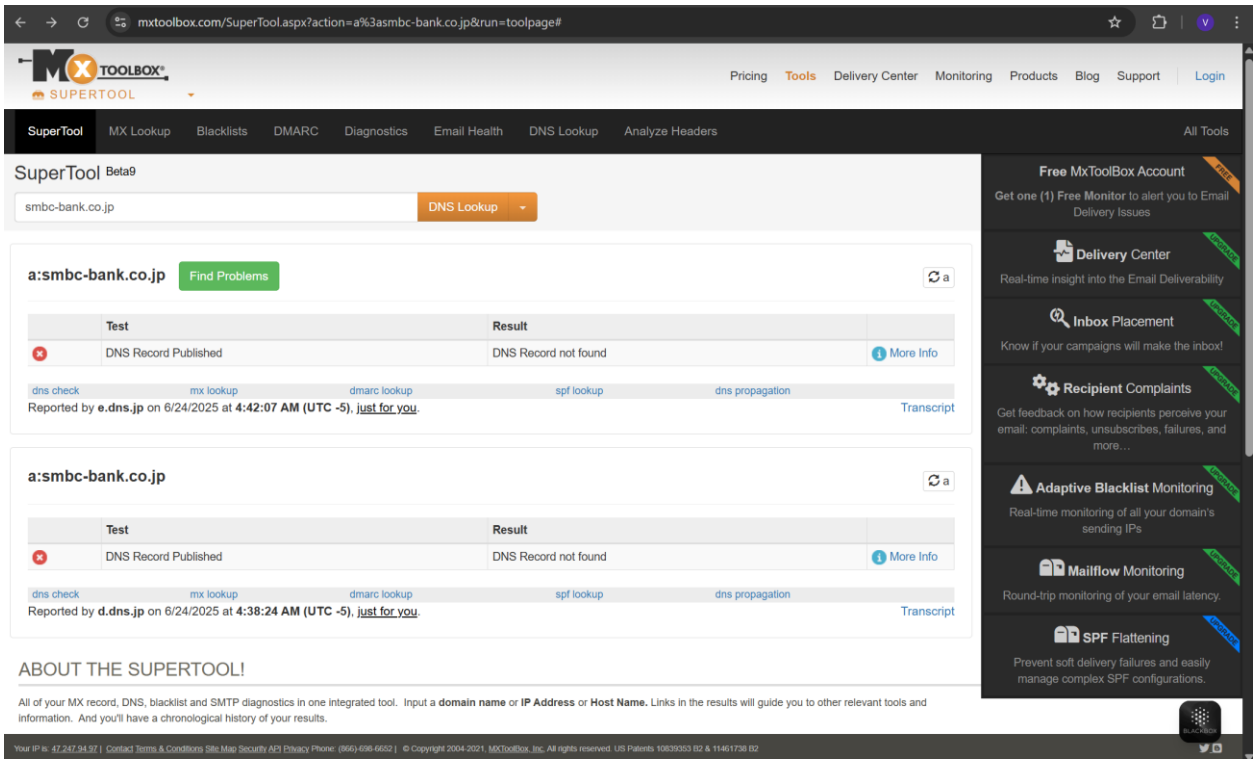
👉 Login to Your Account :https://smbc-cardbv.icu/login.php

If you fail to verify within 24 hours, your account will be locked permanently.

Thank you,
SMBC Online Security Team

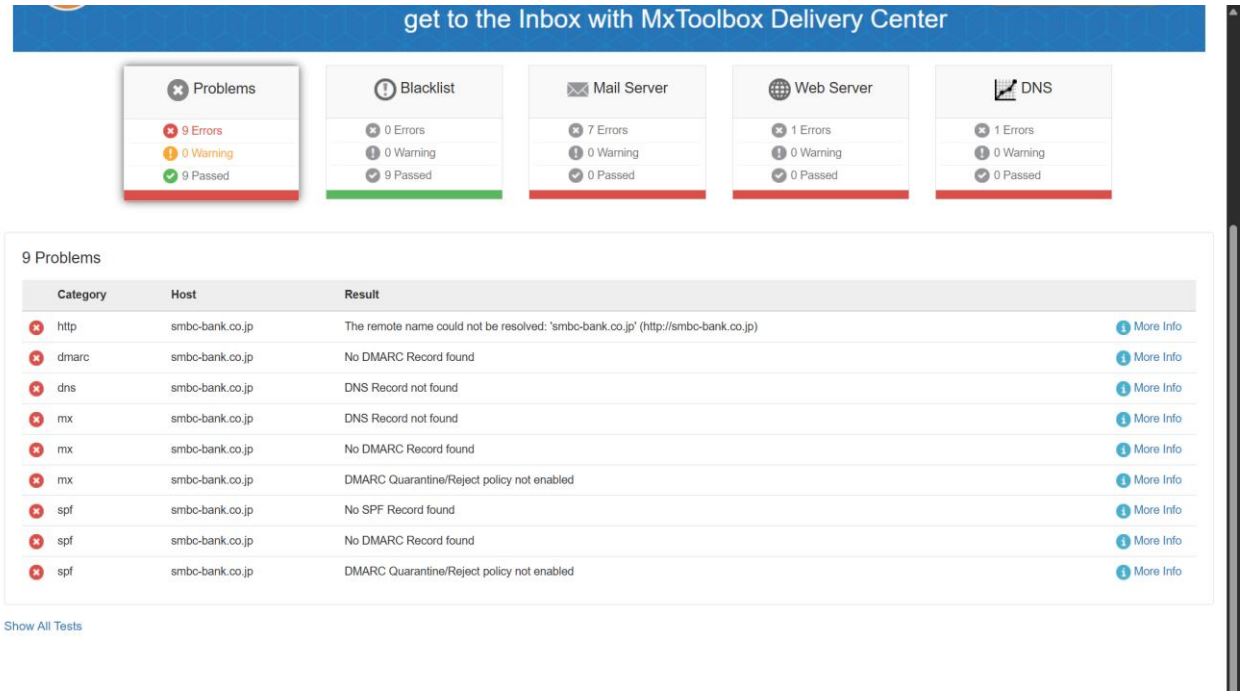
2. Examine senders email address for spoofing:

Senders email address: support@smbc-bank.co.jp



As we can see the domain smbc-bank.co.jp, referenced in the phishing email, has no DNS records, no email verification records and is not a valid operational domain. This proves that the email sender address was spoofed, and the domain was likely created to deceive recipients by imitating the real SMBC domain (smbc.co.jp).

3. Check email headers for discrepancies.



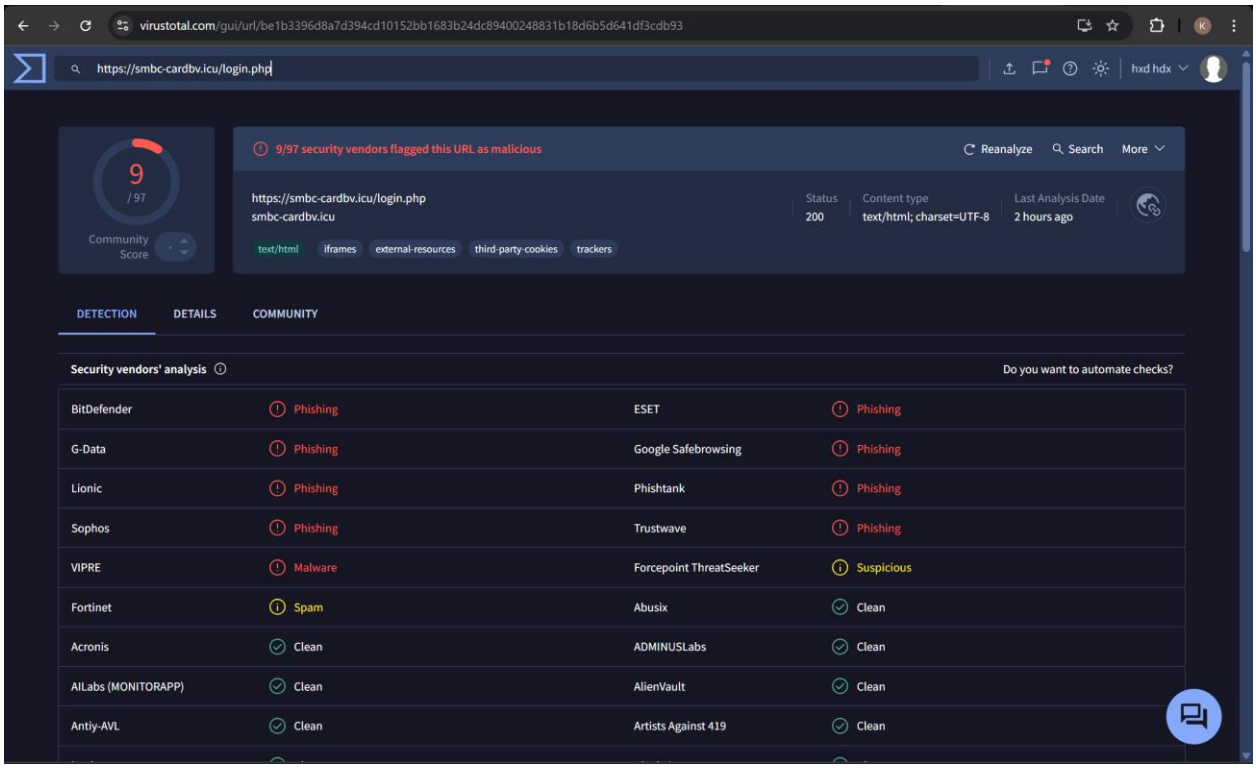
We analyzed the email header using MXToolbox Email Header Analyzer. The results showed:

- SPF: No SPF record found for smbc-bank.co.jp
- DKIM: Not configured or missing
- DMARC: No DMARC policy found
- DNS Lookup: Domain not resolved, indicating a possible fake or inactive domain

These issues confirm that the sender's domain is not legitimate and is likely spoofed. Email headers show that the domain has no authentication mechanisms, making it vulnerable to phishing and spoofing.

4. Identify suspicious links or attachements:

Link: https://smbc-cardbv.icu/login.php



5. Look for urgent or threatening language in the mail:

From: SMBC Bank support@smbc-bank.co.jp
To: user@example.com
Subject: URGENT: Suspicious Activity Detected in Your SMBC Account

Dear Customer,

We have detected suspicious login attempts to your SMBC account. To protect your account, we require you to **verify your information immediately** by logging in at the link below:

👉 Login to Your Account :https://smbc-cardbv.icu/login.php

If you fail to verify within 24 hours, your account will be locked permanently.

Thank you,
SMBC Online Security Team

The fake email looks like it's from SMBC Bank and tries to scare the person. It says things like:

- "We have detected suspicious login attempts"
- "verify your information immediately"
- "If you fail to verify within 24 hours, your account will be locked permanently"

These messages are meant to make people panic and click the link. It's a common trick used in phishing to **steal personal information**.

6. Note any mismatched URLs:

The link shown in the email says:
👉 "Login to Your Account"
But the actual URL behind the link is:
🔗 https://smbc-cardbv.icu/login.php

This link does not belong to the real SMBC Bank domain (which would be something like smbc.co.jp). This is a mismatched and suspicious URL, designed to trick users into entering their credentials on a fake page

Conclusion:

This phishing attempt uses **spoofed branding, urgency, and a fake login page** to trick users into revealing their credentials. The phishing domain (.icu) is a red flag, and header inspection would likely reveal deeper spoofing. Always hover links and verify sender authenticity.