Task 2: Analyze a Phishing Email Sample

Cybersecurity Lab Report

KANDI TEJASREE
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 grammar errors.

Objective:

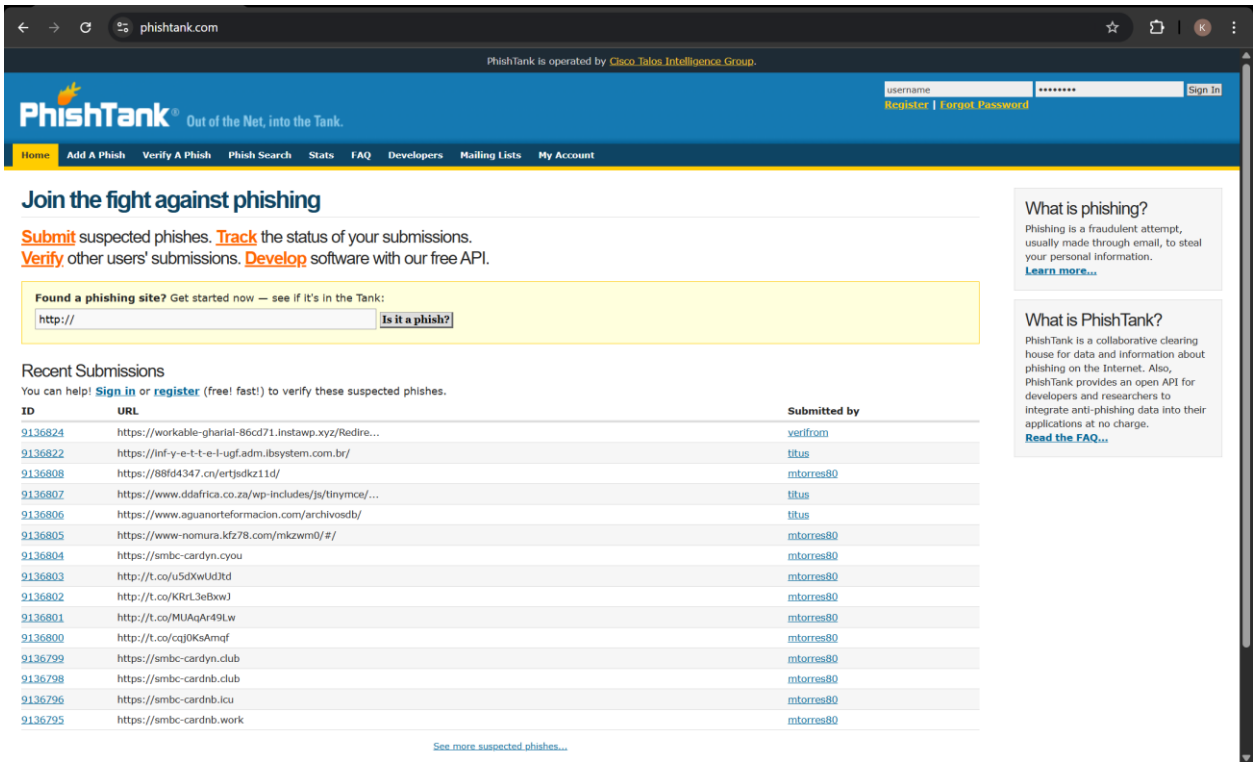
Identify phishing characteristics in a suspicious email sample.

Tools Used:

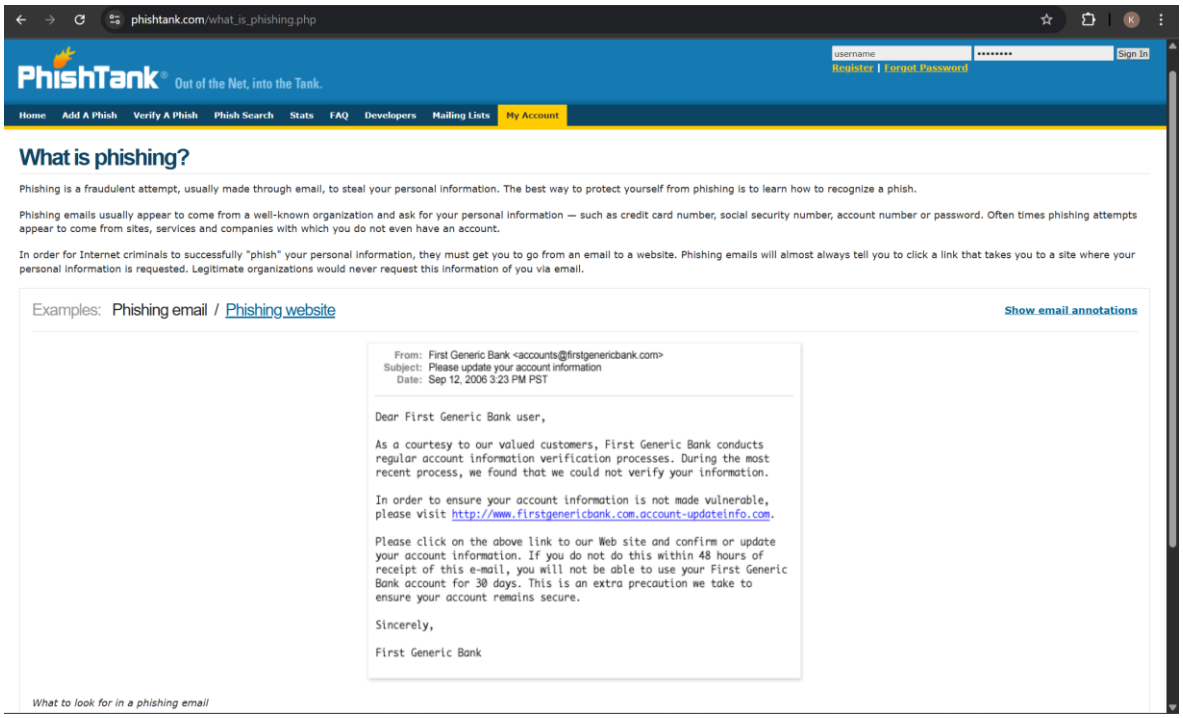
- PhishTank
- MXToolbox
- Virustotal
- WHOIS Lookup

Steps Performed:

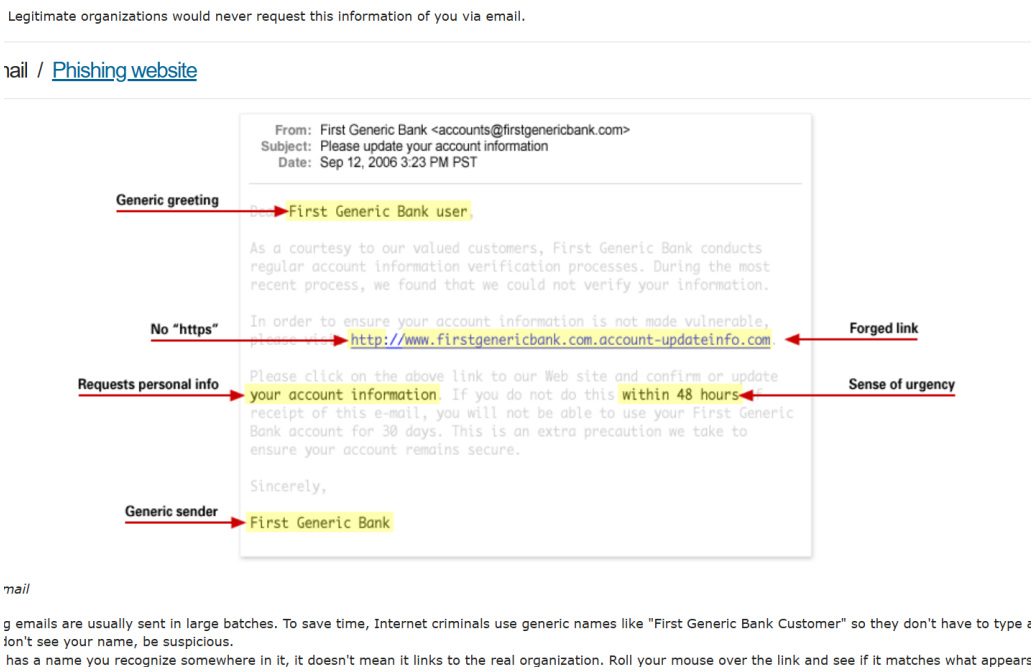
Obtain a sample phishing email



Sample mail:



These are the Annotations in the Phishing email:



As we cannot get the original phishing email because for that we have to receive the email. So let's create a phishing email

Link: https://smbc-cardnb.club

Subject: [Important] Your SMBC Card Account Needs Immediate Attention
From: noreply@smbc-cardnb.club

Dear Customer,

We have detected suspicious activity in your account and have temporarily suspended access for your protection.

To restore full access, please verify your information immediately using the secure link below:

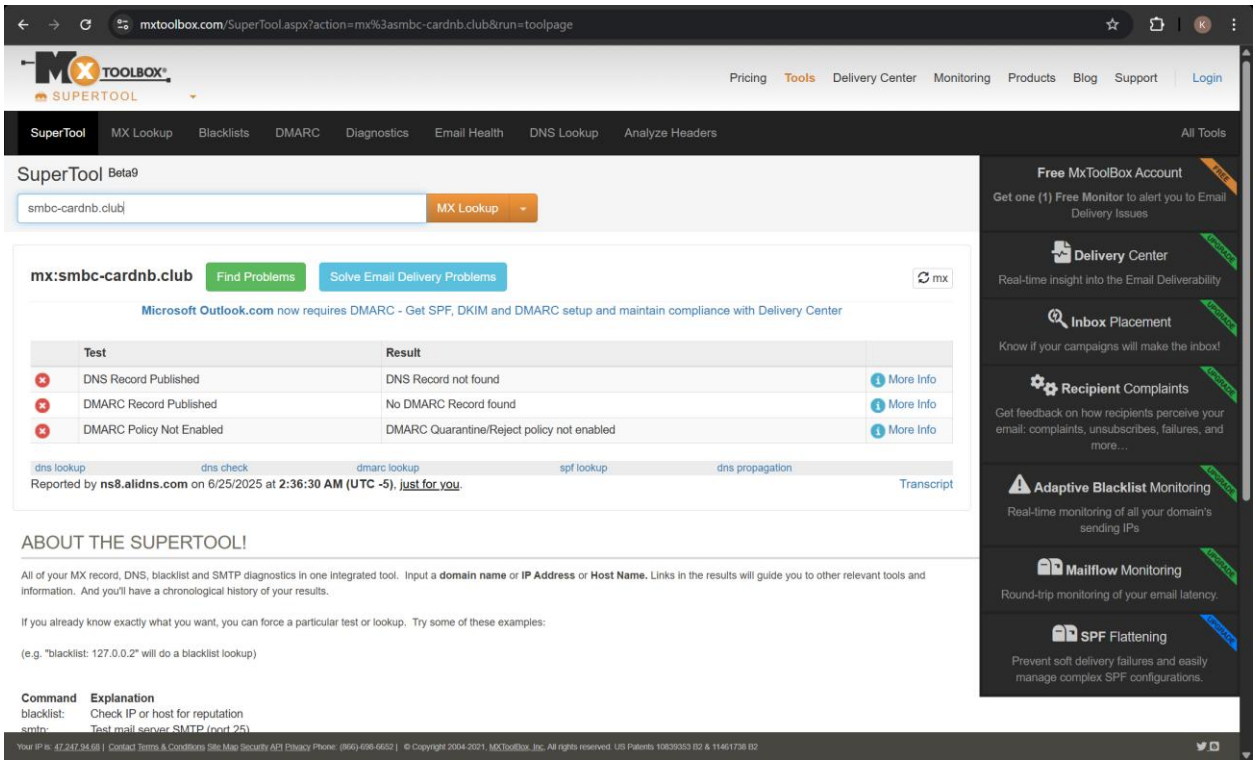
👉 Verify My Account: https://smbc-cardnb.club

Failure to act within 24 hours may result in permanent account suspension.

Thank you for your cooperation,
SMBC Card Security Team

Examine senders email address for spoofing:

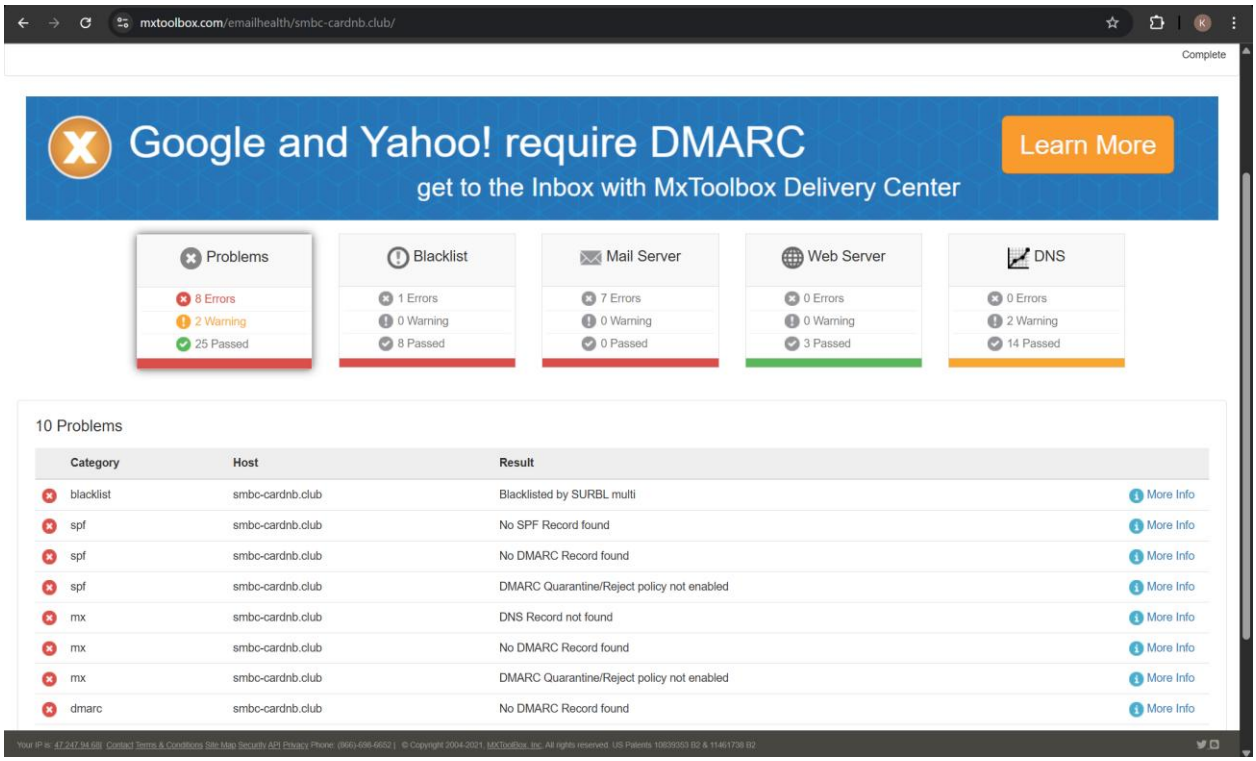
Senders email address: noreply@smbc-cardnb.club



As we can see from the MXToolbox diagnostics:

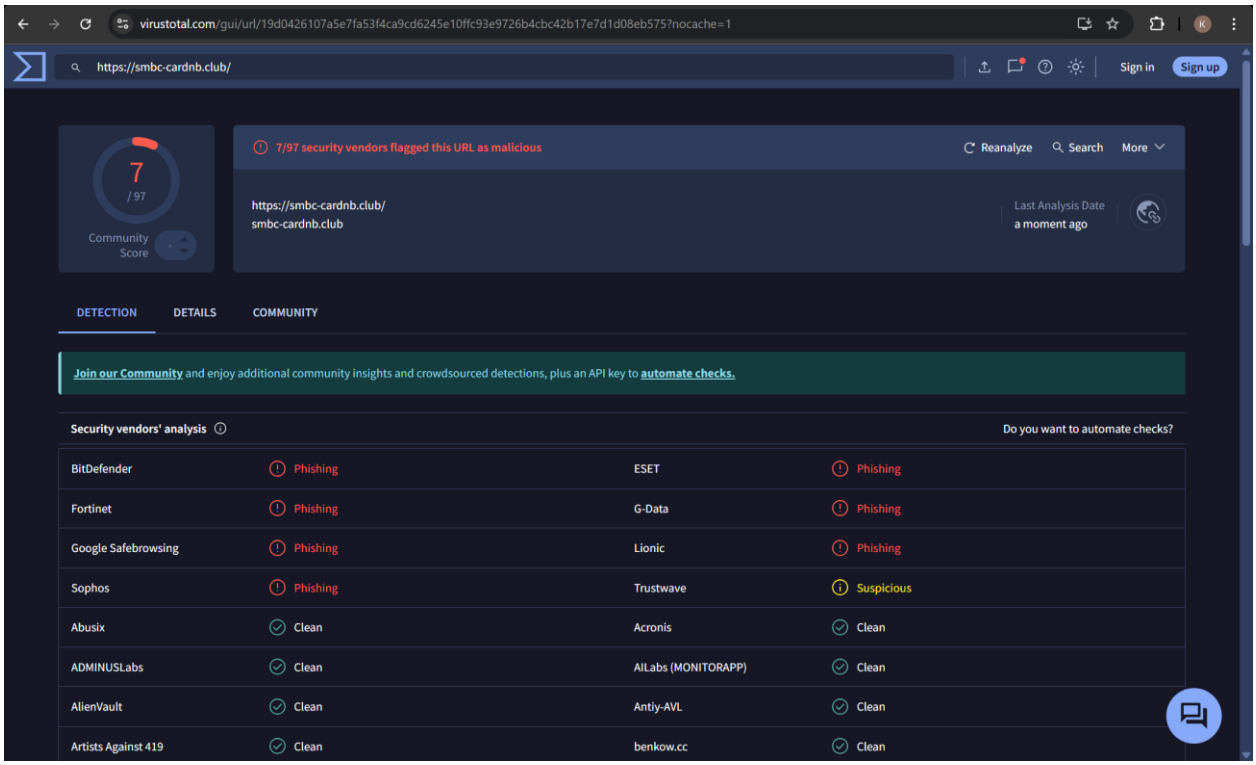
- No DNS Record Published – The domain does not have valid DNS records, indicating it may not be configured for legitimate email or web services.
- No DMARC Record Found – There is no DMARC policy in place, which means there's no protection against email spoofing or phishing using this domain.
- DMARC Policy Not Enabled – Even if a DMARC record were to exist, no enforcement policy (quarantine/reject) is set, making it easier for attackers to impersonate this domain

Check email headers for discrepancies:



Identify Suspicious links or attachments:

Link: https://smbc-cardnb.club



Look for urgent or threatening language in the mail:

Subject: [Important] Your SMBC Card Account Needs Immediate Attention
From: noreply@smbc-cardnb.club

Dear Customer,

We have detected suspicious activity in your account and have temporarily suspended access for your protection.

To restore full access, please verify your information immediately using the secure link below:

👉 Verify My Account: https://smbc-cardnb.club

Failure to act within 24 hours may result in permanent account suspension.

Thank you for your cooperation,
SMBC Card 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

Note any mismatched URLs:

The link shown in the email says:
👉 "Verify My Account"
But the actual URL behind the link is:
🔗 noreply@smbc-cardnb.club

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:

Based on the detailed analysis of the phishing email sample and the associated domain smbc-cardnb.club , it is evident that this email is a well-crafted phishing attempt designed to deceive recipients into divulging sensitive information. The sender's email address, noreply@smbc-cardnb.club, is associated with a domain that lacks essential DNS, DMARC, and SPF configurations, making it vulnerable to spoofing and indicating that it is not set up for legitimate communication. The body of the email uses urgent and threatening language, such as warnings about suspicious login attempts and threats of permanent account suspension unless immediate action is taken. This kind of language is commonly used in phishing campaigns to create panic and prompt the recipient to act without caution. Furthermore, the email includes a deceptive link labeled as “Verify My Account,” which, when inspected, actually redirects to the suspicious domain rather than the legitimate SMBC Bank domain (smbc.co.jp). This mismatch between the visible text and the underlying URL is a classic phishing tactic. Overall, the combination of domain misconfiguration, urgency in language, mismatched URLs, and impersonation of a trusted entity strongly indicates a phishing attack. Users should be trained to recognize these signs and avoid interacting with such emails to protect their personal and financial information.