



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

The screenshot shows the PhishTank homepage. At the top, there's a navigation bar with links like Home, Add A Phish, Verify A Phish, Phish Search, Stats, FAQ, Developers, Mailing Lists, and My Account. Below the navigation is a search bar with the placeholder "Found a phishing site? Get started now — see if it's in the Tank:" followed by a button labeled "Is it a phish?". To the right of the search bar, there's a sidebar with sections titled "What is phishing?", "What is PhishTank?", and "Recent Submissions". The "Recent Submissions" section lists 20 entries with columns for ID, URL, and Submitted by. The URLs listed include various suspicious websites like workable-gharial-86cd71.instawp.xyz, inf-y-e-t-t-e-l-ugr.adm.ibsystem.com.br, and www.ddafrika.co.za.

Sample mail:

This screenshot shows a detailed view of a phishing email from "First Generic Bank". The email header information is as follows:

```

From: First Generic Bank <accounts@firstgenericbank.com>
Subject: Please update your account information
Date: Sep 12, 2006 3:23 PM PST
  
```

The body of the email reads:

Dear First Generic Bank user,

As a courtesy to our valued customers, First Generic Bank conducts regular account information verification processes. During the most recent process, we found that we could not verify your information.

In order to ensure your account information is not made vulnerable, please visit <http://www.firstgenericbank.com/account-updateinfo.com>.

Please click on the above link to our Web site and confirm or update your account information. If you do not do this within 48 hours of receipt of this e-mail, you will not be able to use your First Generic Bank account for 30 days. This is an extra precaution we take to ensure your account remains secure.

Sincerely,

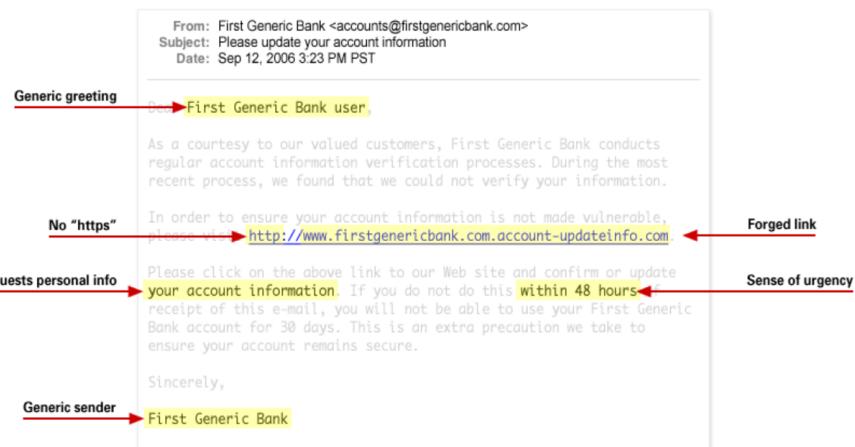
First Generic Bank

At the bottom of the page, there's a footer with the text "What to look for in a phishing email".

These are the Annotations in the Phishing email:

Legitimate organizations would never request this information of you via email.

mail / [Phishing website](#)



mail

g emails are usually sent in large batches. To save time, Internet criminals use generic names like "First Generic Bank Customer" so they don't have to type a
 ion't see your name, be suspicious.
 has a name you recognize somewhere in it, it doesn't mean it links to the real organization. Roll your mouse over the link and see if it matches what appears

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

The screenshot shows the MXToolbox SuperTool interface. In the search bar, the domain `smbc-cardnb.club` is entered, and the "MX Lookup" button is highlighted. The results table displays three tests:

Test	Result
DNS Record Published	DNS Record not found
DMARC Record Published	No DMARC Record found
DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled

Below the table, there are five buttons: dns lookup, dns check, dmarc lookup, spf lookup, and dns propagation. A "Transcript" link is also present. To the right of the main content, there is a sidebar titled "Free MxToolBox Account" with a "Get one (1) Free Monitor to alert you to Email Delivery Issues" button. Other sidebar sections include "Delivery Center", "Inbox Placement", "Recipient Complaints", "Adaptive Blacklist Monitoring", "Mailflow Monitoring", and "SPF Flattening".

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:

The screenshot shows the MxToolbox Email Health report for the domain smbc-cardnb.club. The main summary indicates 10 Problems found across various categories. Below this, a detailed table lists each problem with its category, host, result, and a 'More Info' link.

Category	Host	Result	Action
blacklist	smbc-cardnb.club	Blacklisted by SURBL multi	More Info
spf	smbc-cardnb.club	No SPF Record found	More Info
spf	smbc-cardnb.club	No DMARC Record found	More Info
spf	smbc-cardnb.club	DMARC Quarantine/Reject policy not enabled	More Info
mx	smbc-cardnb.club	DNS Record not found	More Info
mx	smbc-cardnb.club	No DMARC Record found	More Info
mx	smbc-cardnb.club	DMARC Quarantine/Reject policy not enabled	More Info
dmarc	smbc-cardnb.club	No DMARC Record found	More Info

Identify Suspicious links or attachments:

Link: <https://smbc-cardnb.club>

The screenshot shows the VirusTotal URL analysis page for the URL https://smbc-cardnb.club/. The page displays a community score of 7/97 and a summary of 7/97 security vendors flagged the URL as malicious. Below this, a table lists the individual vendor detections.

Vendor	Result
BitDefender	Phishing
Fortinet	Phishing
Google Safebrowsing	Phishing
Sophos	Phishing
Abusix	Clean
ADMINUSLabs	Clean
AlienVault	Clean
Artists Against 419	Clean
ESET	Phishing
G-Data	Phishing
Lionic	Phishing
Trustwave	Suspicious
Acronis	Clean
Allabs (MONITORAPP)	Clean
Antiy-AVL	Clean
benkow.cc	Clean

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.