



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:

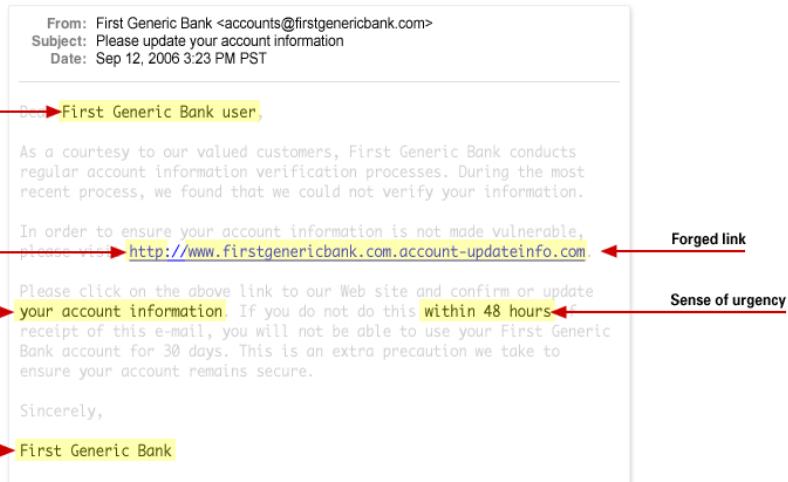
1. Obtaining a sample phishing email

The screenshot shows the PhishTank homepage with a search results page for unverified submissions. The table lists 24 entries, each with a unique ID, the phish URL, the submitter, the validity status, and an 'Online?' indicator. Most entries are marked as 'Unknown' or 'ONLINE'.

ID	Phish URL	Submitted	Valid?	Online?
9135673	https://webmailthermessagingcocomaulogin.grweb.site/...	by souddy	Unknown	ONLINE
9135671	https://nzyyymwl.za.com/espera.html	by theboard	Unknown	ONLINE
9135668	https://vivasorte.ddns.net/	by AllegraMueller	Unknown	ONLINE
9135661	https://sbisec-co-jp.u92.com/pEdHod/	by mely	Unknown	ONLINE
9135657	https://www.solicitudecertificadosdigitales.com/...	by jaykut	Unknown	ONLINE
9135652	http://www.allegro.pl-conformation103.shop	by Amarena98	Unknown	ONLINE
9135612	https://www.sparkoneth.vip/	by c3gsersec	Unknown	ONLINE
9135611	http://www.sparkoneth.vip	by c3gsersec	Unknown	ONLINE
9135592	https://nnggvilledecans.es/DDE	by shakalakaboom	Unknown	ONLINE
9135591	https://brandview.com.ng/wp-loads.php	by shakalakaboom	Unknown	ONLINE
9135590	https://epasvc.com/index.php	by shakalakaboom	Unknown	ONLINE
9135587	https://seguro-pay.com/checkout/?utm_campaign=22692650807&utm_medium...	by NialCottrell	Unknown	ONLINE
9135586	http://www.apex-trust.com/index-961.html	by segasec	Unknown	ONLINE
9135584	https://kaisanmoda.hidrantapele.com	by ReemWills	Unknown	ONLINE
9135574	https://leshopamiga.pages.dev/?gad_source=1&gad_campaignid=226876...	by compartidos	Unknown	ONLINE

Sample mail:

The screenshot shows a Windows 10 desktop environment. A browser window displays the PhishTank 'What is phishing?' page. Below it, a text editor window shows the raw HTML content of a phishing email. The email is from 'First Generic Bank <accounts@firstgenericbank.com>' with a subject of 'Please update your account information'. It contains a generic greeting, a forged link, and requests personal information. A note at the bottom explains what to look for in a phishing email, listing four key points: generic greeting, forged link, requests personal information, and sense of urgency.



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

The screenshot shows the MxToolBox SuperTool interface. At the top, there's a navigation bar with links like Pricing, Tools, Delivery Center, Monitoring, Products, Blog, Support, and Login. Below the navigation is a search bar with 'smbc-bank.co.jp' and a dropdown menu set to 'DNS Lookup'. There are two main sections of results:

- a:smbc-bank.co.jp**: Shows a table with 'Test' (DNS Record Published) and 'Result' (DNS Record not found). It also includes buttons for dns check, mx lookup, dmarc lookup, spf lookup, and dns propagation, along with a transcript link.
- a:smbc-bank.co.jp**: Similar table structure showing the same results for the second query.

On the right side of the interface, there's a sidebar with several monitoring services listed as 'FREE' trials:

- Free MxToolBox Account**: Get one (1) Free Monitor to alert you to Email Delivery Issues.
- Delivery Center**: Real-time insight into the Email Deliverability.
- Inbox Placement**: Know if your campaigns will make the inbox!
- Recipient Complaints**: Get feedback on how recipients perceive your email; complaints, unsubscribes, failures, and more...
- Adaptive Blacklist Monitoring**: Real-time monitoring of all your domain's sending IPs.
- Mailflow Monitoring**: Round-trip monitoring of your email latency.
- SPF Flattening**: Prevent soft delivery failures and easily manage complex SPF configurations.

At the bottom left, it says 'Your IP is: 47.247.94.97 | Contact Terms & Conditions Site Map Security API Privacy Phone: (866) 696-6652 | © Copyright 2004-2021, MXToolBox, Inc. All rights reserved. US Patents 10530033 B2 & 11461738 B2'.

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.

The screenshot shows the MXToolbox Email Header Analyzer interface. At the top, there are five summary boxes: 'Problems' (9 Errors, 0 Warnings, 9 Passed), 'Blacklist' (0 Errors, 0 Warnings, 9 Passed), 'Mail Server' (7 Errors, 0 Warnings, 0 Passed), 'Web Server' (1 Errors, 0 Warnings, 0 Passed), and 'DNS' (1 Errors, 0 Warnings, 0 Passed). Below this, a table titled '9 Problems' lists the findings:

Category	Host	Result	More Info
http	smbc-bank.co.jp	The remote name could not be resolved: 'smbc-bank.co.jp' (http://smbc-bank.co.jp)	More Info
dmarc	smbc-bank.co.jp	No DMARC Record found	More Info
dns	smbc-bank.co.jp	DNS Record not found	More Info
mx	smbc-bank.co.jp	DNS Record not found	More Info
mx	smbc-bank.co.jp	No DMARC Record found	More Info
mx	smbc-bank.co.jp	DMARC Quarantine/Reject policy not enabled	More Info
spf	smbc-bank.co.jp	No SPF Record found	More Info
spf	smbc-bank.co.jp	No DMARC Record found	More Info
spf	smbc-bank.co.jp	DMARC Quarantine/Reject policy not enabled	More Info

[Show All Tests](#)

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 attachments:

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

9/97 security vendors flagged this URL as malicious

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

Status: 200 Content type: text/html; charset=UTF-8 Last Analysis Date: 2 hours ago

Vendor	Result
BitDefender	Phishing
G-Data	Phishing
Lionic	Phishing
Sophos	Phishing
VIPRE	Malware
Fortinet	Spam
Acronis	Clean
AllLabs (MONITORAPP)	Clean
Antiy-AVL	Clean
ESET	Phishing
Google Safebrowsing	Phishing
Phishtank	Phishing
Trustwave	Phishing
Forcepoint ThreatSeeker	Suspicious
Abusix	Clean
ADMINUSLabs	Clean
AlienVault	Clean
Artists Against 419	Clean

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.