PHISHING ANALYSIS INVESTIGATION SOP

Standard Operating Procedure for SOC Analysts

Document Version: 1.0
Last Updated: December 2025
Author: BTuff

1. Purpose & Scope

This SOP gives you a systematic workflow for investigating phishing emails. Whether it's reported by a user or flagged by security tools, the goal is the same: collect artifacts, analyze indicators, determine a verdict, and take defensive actions. Basically, this is the playbook for handling phishing from start to finish.

1.1 Scope

This covers all types of phishing: credential harvesting, malware delivery, business email compromise (BEC), and social engineering campaigns. If it's a suspicious email, this SOP applies.

1.2 Core Principle

GUILTY UNTIL PROVEN INNOCENT. Here's the thing: assume all suspicious emails are malicious until your analysis proves otherwise. Clean reputation scores don't guarantee safety, especially for targeted or brand new attacks. Don't let a clean VirusTotal score fool you into letting your guard down.

2. Safety Requirements

CRITICAL: Never analyze phishing emails on your personal or corporate workstation. Always use an isolated analysis environment. Seriously, don't skip this.

2.1 Required Environment

- Dedicated analysis VM or "dirty" machine isolated from production network
- Disconnect internet when opening attachments for sandbox analysis
- Never click hyperlinks directly. Always copy and analyze URLs safely.
- Never enable macros in suspicious documents (this is how most malware gets you)
- Use text editors to extract artifacts from .eml/.msg files

3. Phase 1: Initial Triage

Objective: Quickly assess the email to see if it's worth a full investigation.

3.1 Red Flag Checklist

Run through this checklist. If you hit 2+ red flags, proceed to full artifact collection.

- ☐ Generic greeting ("Dear Customer") instead of recipient's actual name
- ☐ Urgency language ("IMMEDIATELY", "account suspended", "action required")
- ☐ Threats or fear tactics ("non-refundable charges", "legal action")
- ☐ Sender domain doesn't match claimed organization
- ☐ Spelling and grammar errors
- ☐ Requests for sensitive information (passwords, billing details)
- ☐ Suspicious attachments (macros, executables, password-protected archives)
- ☐ Mismatched hyperlinks (display text vs. actual URL)
- ☐ Reply-To address differs from From address

4. Phase 2: Artifact Collection

Objective: Systematically extract all indicators needed for analysis and documentation.

This is where you grab everything you need. Think of artifacts as evidence. You're building a case.

4.1 Email Artifacts

Artifact	Purpose & How to Get It
From Address	Who the sender claims to be. Visible right in the email client. Keep in mind this can be spoofed, so don't trust it without verification.
Subject Line	Use this to search your email gateway for similar phishing attempts hitting other users in your org.
Recipients (To/CC)	Shows who was targeted. Note: BCC recipients won't be visible here. Search your gateway by sender and subject to find everyone.
Date & Time	Search for correlated emails sent around the same time. Also helps track when your org gets hit with phishing campaigns.
X-Sender-IP	Extract from email headers in the .eml file. Search for "X-Sender-IP" using CTRL+F. Use this for WHOIS and reverse DNS lookups.
Reply-To Address	Search "Reply-To:" in headers. If this is different from the From address, that's a strong spoofing indicator. The attacker needs replies going somewhere they actually control.

4.2 Web Artifacts

Artifact	Purpose & How to Get It
Full URL	Copy from email client (right-click the hyperlink) or search the .eml for "http" or <a href> tags. Always defang before documenting: hxxps://[.]domain[.]com
Root Domain	Extract from the full URL. Important: Check BOTH the root domain AND the full path. Legitimate domains can host malicious content if they get compromised.

4.3 File Artifacts (If Attachment Present)

Artifact	Purpose & How to Get It
Filename + Extension	Get from email client or File Properties. Use for EDR blocking rules. Watch for double extensions like .pdf.exe (classic trick).
File Size	Right-click > Properties. Document for reference.
SHA256 Hash	This is your primary hash for reputation lookups. Use get-filehash in PowerShell or sha256sum in Linux.
MD5 Hash	Secondary hash for legacy systems. Use get-filehash -Algorithm MD5 or md5sum.

Hashing Commands Quick Reference

PowerShell:

```
get-filehash "C:\path\to\file.docx"
get-filehash -Algorithm MD5 "C:\path\to\file.docx"
```

Linux:

```
  sha256sum filename | md5sum filename | sha1sum filename
```

5. Phase 3: Artifact Analysis

Objective: Analyze collected artifacts to determine if the email is malicious.

Now we dig into the evidence. This is where you actually figure out if this thing is a threat or not.

5.1 Sender Verification

Step 1: Check SPF, DKIM, DMARC Alignment

Look for the "Authentication-Results" header in the .eml file. This shows pass/fail status for email authentication checks. Basically, these three work together to verify if the sender is legit.

Check	What It Verifies	Red Flag If...
SPF	Sender IP is authorized to send for claimed domain	FAIL or SOFTFAIL
DKIM	Email was signed by domain owner and not tampered with	FAIL or missing
DMARC	Domain's policy for handling SPF/DKIM failures	FAIL (especially with p=reject policy)

Step 2: Verify Sender IP Ownership

1. Extract X-Sender-IP from email headers
2. Perform WHOIS lookup (whois.domaintools.com or mxtoolbox.com)
3. Perform reverse DNS lookup to get the hostname
4. Compare: Does the IP/hostname belong to the organization the sender claims to be from?

Step 3: Compare From vs. Reply-To

If the Reply-To address is different from the From address (especially if it's a completely different domain), this is a strong indicator the From header was spoofed. Attackers need replies to go somewhere they actually control.

5.2 URL Analysis

5. **Visual Inspection:** Check for typosquatting (securltyblue vs securityblue) and homoglyphs (Cyrillic characters that look identical to Latin letters)
6. **WHOIS Lookup:** Check domain creation date. Recently created domains are super suspicious.
7. **Reputation Check:** Submit to VirusTotal, URLScan.io, URLhaus
8. **Safe Screenshot:** Use URL2PNG or URLScan.io to view the page without actually visiting it
9. **Check Both:** Analyze root domain AND full URL path. Legitimate domains can host malicious content if compromised.

TIP: For shortened URLs (bit.ly, tinyurl), use WannaBrowser or URLScan.io to reveal the full redirect chain without clicking.

5.3 File/Attachment Analysis

10. **Hash Reputation:** Submit SHA256 hash to VirusTotal and Talos File Reputation
11. **Sandbox Analysis:** If reputation is clean but you're still suspicious, upload to Hybrid Analysis for dynamic behavioral analysis
12. **File Type Verification:** Confirm extension matches actual file type. Watch for .pdf.exe double extensions.

Malicious Attachment Categories

There are basically three types of malicious attachments you'll see:

- **Social Engineering Documents:** Not inherently malicious but designed to trick users into giving up sensitive information
- **Lure Documents:** Contain malicious URLs inside the document (bypasses email gateway URL scanning)
- **Weaponized Files:** Contain malicious macros, scripts, or exploit code. These are the dangerous ones.

6. Phase 4: Verdict Determination

Objective: Based on your analysis, classify the email and determine the appropriate response.

This is where you make the call. Use your evidence to back up your verdict.

Verdict	Criteria	Action
MALICIOUS	Confirmed malicious indicators: bad reputation scores, spoofed sender, known malware hash, credential harvesting page	Proceed to defensive actions (Section 7)
SUSPICIOUS	Multiple red flags but no confirmed malicious indicators. Could be targeted or new attack with clean reputation.	Sandbox for behavioral analysis. Escalate if needed. When in doubt, treat as malicious.
BENIGN	All checks pass. Legitimate sender verified. No malicious indicators. User may have just flagged spam as phishing.	Close ticket. Notify user. Document findings.

7. Phase 5: Defensive Actions (If Malicious)

Objective: Contain the threat and prevent similar attacks from hitting your org again.

Once you've confirmed it's malicious, it's time to take action. Here's the checklist:

13. **Block Sender:** Add sender address and domain to email gateway blocklist
14. **Block IOCs:** Add malicious URLs/domains to web proxy blocklist. Add file hashes to EDR blocklist.
15. **Purge Similar Emails:** Search email gateway for emails with same sender/subject/indicators and remove from all mailboxes
16. **Notify Affected Users:** Alert users who received the email. Give them guidance on what to do if they clicked or opened anything.
17. **Check for Compromise:** If users clicked links or opened attachments, check for signs of compromise (credential theft, malware execution)
18. **Update Detection Rules:** Create email gateway rules to catch similar phishing patterns in the future
19. **Share IOCs:** Report to threat intelligence feeds (PhishTank, URLhaus) if appropriate

8. Phase 6: Report Writing

Objective: Create a complete, professional record of your investigation.

This is super important. Reports are the evidence of your work. It needs to be clear, organized, and thorough enough that anyone reading it can understand exactly what happened and what you did about it. Here's the structure I use:

8.1 Universal Report Template

Follow this structure for every phishing investigation report. It covers everything you need and keeps things consistent.

Section 1: Executive Summary

Start with the bottom line. What was the email, what did you find, and what's the verdict? Keep this to 2-3 sentences max. We know decision makers read this!

Example:
"A credential harvesting email impersonating Amazon was reported by [user]. Analysis confirmed the email as MALICIOUS. The phishing page has been taken down, sender blocked, and all similar emails purged from user mailboxes."

Section 2: Collected Artifacts

List every artifact you collected. Use a table format for clarity. Always defang URLs and include full hashes.

Artifact Type	Value
From Address	[sender@domain.com]
Subject Line	[Subject]
Recipients	[List of recipients]
Date/Time Received	[DD MMM YYYY HH:MM:SS]
Sender IP	[X.X.X.X]
Reply-To	[address or N/A]
Malicious URL	hxxps://[.]malicious[.]com/path
Attachment Name	[filename.ext or N/A]
SHA256 Hash	[hash or N/A]

Section 3: Analysis Performed

Document what you checked and what you found. This is where you show your work. Include links to your reputation check results.

Sender Verification:

- SPF: [PASS/FAIL]
- DKIM: [PASS/FAIL]
- DMARC: [PASS/FAIL]
- WHOIS/Reverse DNS: [Findings. Does IP match claimed sender?]

URL Analysis:

- VirusTotal: [X/Y engines flagged] [link to results]
- URLScan.io: [Findings] [link to scan]
- WHOIS: Domain created [date]. [Suspicious if recent]

File Analysis (if applicable):

- VirusTotal: [X/Y engines flagged] [link to results]
- Hybrid Analysis: [Behavioral findings] [link to report]

Section 4: Supporting Evidence

Include screenshots and visual evidence. This makes your report way more credible and easier to understand.

- Screenshot of the phishing email
- Screenshot of the phishing page (from URL2PNG or URLScan)
- Screenshot of VirusTotal results
- Screenshot of email headers showing authentication failures

Section 5: Verdict & Justification

State your verdict clearly and explain why. Connect your findings to your conclusion.

Example:
"VERDICT: MALICIOUS. The email was determined to be a credential harvesting phishing attempt based on: (1) Sender domain 'amaz0n-security[.]com' is typosquatting the legitimate Amazon domain, (2) SPF and DKIM checks failed, (3) The embedded URL leads to a fake login page flagged by 12/89 VirusTotal engines, (4) Domain was registered 3 days ago."

Section 6: Defensive Actions Taken

Document every action you took to contain and remediate the threat.

- [List each action with timestamp]
- Blocked sender domain in email gateway
- Added malicious URL to web proxy blocklist
- Purged X similar emails from Y mailboxes
- Notified affected users
- Submitted IOCs to PhishTank/URLhaus

Section 7: Report Metadata

- **Analyst:** [Your Name]
- **Date/Time of Analysis:** [Timestamp]
- **Ticket/Case Number:** [If applicable]
- **Time Spent:** [Optional but helpful for metrics]

PRO TIP: PhishTool is a great automation tool that can auto-generate professional reports with all artifacts and analysis included!

9. Tools Reference

These are the tools you'll use regularly. Bookmark them.

Tool	Purpose	URL
VirusTotal	URL, file, hash reputation	virustotal.com
URLScan.io	URL scanning, screenshots, network requests	urlscan.io
URL2PNG	Safe website screenshots	url2png.com
URLhaus	Malware URL threat feed	urlhaus.abuse.ch
PhishTank	Phishing URL database	phishtank.com
Talos File Reputation	Cisco file hash reputation	talosintelligence.com
Hybrid Analysis	Malware sandboxing	hybrid-analysis.com
PhishTool	Automated phishing analysis platform	phishtool.com
WannaBrowser	URL redirect chain analysis	wannabrowser.net
MXToolbox	DNS, WHOIS, reverse DNS lookups	mxtoolbox.com
DomainTools WHOIS	Domain registration lookup	whois.domaintools.com
CyberChef	Decode and analyze data (Base64, URL, etc.)	gchq.github.io/CyberChef

10. Personal Notes

This SOP gives you a solid foundation. When I join an actual SOC, I will customize it with my organization's specific stuff!

Revision History:

Version	Date	Author	Changes
1.0	December 2025	BTuff	Initial release