Phishing Investigation Step Guide

This guide walks you through the key steps to investigate a suspicious email that might be a phishing attempt. Each step is designed to help you analyze and identify malicious activity, ensuring you protect yourself and your organization. Here's how you can approach it:

1. Examine the Content of the Email

What to Do:

Check the company name, sender, and contact details. Verify that the email is from the legitimate company it claims to be from. Look for signs of misspelled names, incorrect or fake company addresses, and suspicious email addresses.

Look for the email's intent. What does the email want you to do? Is it asking for personal information, account login details, money transfers, or suspicious attachments?

Why: Phishing emails often impersonate trusted organizations and may contain urgent or alarming messages urging you to click on links, download attachments, or share sensitive information. Identifying these behaviors can help spot the phishing attempt early.

Example:

You receive an email appearing to be from your bank, asking you to "verify your account" by clicking a link. Upon inspection, the sender's email address is slightly altered (e.g., "support@my-securebank.com" instead of "support@mybank.com"). This inconsistency is a red flag.

2. Examine Indicators of Compromise (IOCs)

What to Do:

Review the attachment hashes. Use tools like VirusTotal to check if the attachment is known to be malicious.

Inspect URLs within the email. Hover over the links without clicking to see the actual URL. Phishers may use URLs that are similar to, but slightly different from, the real website (e.g., "www.bank-secure.com" instead of "www.bank.com").

Look at the sender domain. Ensure the domain of the sender matches the legitimate domain of the company it claims to be from. A slight variation in the domain name, such as "exmaple.com" instead of "example.com," could indicate malicious intent.

Why: Indicators of compromise (IOCs) such as suspicious file hashes, misleading URLs, and irregular sender domains are powerful clues to determine if the email is part of a phishing attack. These elements help in identifying whether the email is associated with known malicious campaigns.

Example:

The email includes a link to "www.bank-verification-info.com" instead of "www.bank.com." A quick search or examination of this URL reveals it is linked to known phishing domains.

3. Examine Email Headers

What to Do:

Review the email’s headers for internal servers. Analyze the route the email took to reach your inbox. Look for any inconsistencies or unfamiliar internal servers that might suggest the email was spoofed. Specifically, check the “Received” field in the header, which shows the list of servers that handled the email before it arrived in your inbox.

Check SPF, DMARC, and DKIM results. These authentication protocols help verify that the email was sent from an authorized server.

SPF (Sender Policy Framework): Ensures the sending server is authorized to send emails on behalf of the domain.

DMARC (Domain-based Message Authentication, Reporting, and Conformance): Helps prevent domain spoofing by verifying the alignment of SPF and DKIM.

DKIM (DomainKeys Identified Mail): Verifies that the email was not tampered with in transit.

Why:

Internal servers: Examining internal servers is crucial because legitimate emails typically come from a set of authorized servers linked to the company’s domain. If you notice an email that has passed through an unfamiliar or suspicious server, it could suggest that the email was forged or sent from an unauthorized source. This is often a tactic used in phishing to make an email look legitimate.

For example, if an email from "bank.com" has passed through a server that belongs to a completely different or obscure domain, this may indicate the email was spoofed or routed through a malicious server to hide its origin.

SPF, DMARC, and DKIM checks: These checks ensure that the email is authentic and has not been altered. If these fail, it is a strong indicator that the email could be a phishing attempt, as legitimate emails from trusted senders will pass these authentication checks. Failure often means the sender’s domain was spoofed or the email was tampered with.

Example:

When checking the email headers, you notice that the email has passed through an unfamiliar server, such as "unknownserver.com," which is not part of the legitimate "bank.com" network. Additionally, the SPF check fails, and the DKIM signature is invalid. This suggests the email was likely sent by a malicious actor attempting to spoof the bank’s email.

Conclusion

By following these three steps—examining the content, analyzing indicators of compromise, and reviewing the email headers—you can effectively investigate and identify phishing emails. Always stay cautious, especially if something seems suspicious or too urgent. When in doubt, contact the legitimate company directly through trusted communication channels.

Why

It is generally best to start with Step 1: Examine the Content of the Email when investigating a phishing attempt, but you can technically start with Step 2: Examine Indicators of Compromise (IOCs) or Step 3: Examine Email Headers depending on the situation. Here's why Step 1 is typically the best place to start, and how it relates to the other steps:

Why Start with Step 1 (Content of the Email)?

Why:

Reveals attacker’s intent and psychological tactics (urgency, fear, authority).

Quickest first step to flag suspicious language, requests, or behavior.

Helps frame the rest of the investigation (e.g., if suspicious content links to a file, jump to IOCs).

When:

As a first response to reported phishing.

When reviewing emails without obvious payloads or links.

When performing fast triage across a high volume of reports.

How:

Look for red flags:

Unusual requests (login, money transfer)

Suspicious or generic greetings

Poor grammar or formatting

Sense of urgency or fear

Mismatched branding

Where:

Subject line, email body, signature, call-to-action (CTA).

Who:

Anyone: SOC analyst, help desk, or even a trained end user.

Example:

“Your account will be locked in 1 hour. Click here to reset now.”

The tone is aggressive, the request unusual, and the domain is slightly misspelled.

Limitations:

Sophisticated phishing may have perfect grammar and mimic real brands.

False positives possible—some legitimate emails are just poorly written.

Hard to rely on content alone in automated phishing kits or internal spoofing.

Start Somewhere Else When:

Scenario Start With Why

The email is visually flawless and includes a link/attachment Step 2 (IOCs) Content won’t reveal the danger—technical payloads might

Suspicion of spoofed internal sender with vague text Step 3 (Headers) Content looks fine—auth failure will confirm spoofing

Step 2: Examine Indicators of Compromise (IOCs)

Why:

Provides concrete, technical evidence of malicious behavior.

Validates suspicion by tying emails to known malware, phishing infrastructure, or bad reputation.

Enables threat intel correlation and broader campaign detection.

When:

The email includes links, attachments, or suspicious domains.

Content raised a red flag that needs verification.

Your organization relies on IOC-based blocking (e.g., proxy, AV, EDR, SIEM alerts).

How:

Hover over URLs → verify destination.

Hash attachments → submit to VirusTotal, sandbox.

Query domains/IPs in internal or external threat intelligence platforms.

Where:

Email body (URLs), attachments, embedded images, shortened links, or known bad file names.

Who:

SOC analysts, detection engineers, threat hunters.

Example:

The Excel attachment’s hash returns multiple AV hits on VirusTotal for “Trojan:Downloader,” even though the content seemed okay. IOC confirms this is phishing with payload delivery.

Limitations:

False positives: Security vendors may flag benign files, especially with heuristics.

Zero-day/phishing infrastructure: Brand-new phishing kits may have clean IOCs.

IOC evasion: Use of public services (e.g., Dropbox) can make detection harder.

Start Somewhere Else When:

Scenario Start With Why

No attachments or links; only vague content Step 1 (Content) IOCs don’t exist—focus on tone, behavior, urgency

Suspected spoofing/internal phish with no payload Step 3 (Headers) IOC tools won’t help—authentication failures will

Step 3: Examine Email Headers

Why:

Verifies sender identity via SPF, DKIM, DMARC.

Reveals true source via mail relay path (“Received” headers).

Identifies spoofing, forgery, or misrouted emails.

When:

You suspect spoofing, especially internal-to-internal phish.

The sender address looks valid but something feels off.

SPF/DMARC failure is flagged by the email gateway.

Email has no payload, but a user received it unexpectedly.

How:

Extract headers (e.g., Outlook > File > Properties).

Analyze:

Return-path, From, Reply-To fields

SPF: Does the sending IP match allowed senders?

DKIM: Was the message tampered with?

DMARC: Did SPF/DKIM pass and align?

Where:

In the email header section; often hidden or requires tools to parse.

Who:

Advanced SOC analysts, email admins, IR leads.

Example:

The “From” field says “HR@company.com,” but SPF fails, and the “Received” path shows the message came from a foreign, unrelated IP. That mismatch confirms spoofing.

Limitations:

Legit emails sometimes fail SPF/DMARC due to misconfigurations or email forwarding.

Forwarded or bounced emails may distort header data.

Headers are harder to interpret without proper tooling or training.

Start Somewhere Else When:

Scenario Start With Why

The email has a known malicious link or file Step 2 (IOCs) Header analysis is secondary once the threat is confirmed

The content is clearly phishing (“Reset your password now!”) Step 1 (Content) No need to verify headers if intent is obvious