Phishing Email Analysis Report

# 1. Summary

A suspicious email was received impersonating the Microsoft account team, claiming an "unusual sign-in activity" from Russia/Moscow. The message is designed to alarm the recipient and lure them into interacting with a malicious 'Report The User' button, which launches an email to a suspicious domain. This is a clear attempt at phishing using social engineering techniques.

🧪 The phishing email sample was obtained from the open-source training project \*\*PhishingPot\*\*, designed for cybersecurity analysis and lab exercises.

# 2. Email Metadata

|  |  |
| --- | --- |
| Field | Value |
| From | ydieo@s43ndybt7g.com (spoofed sender, not Microsoft) |
| To | phishing@pot |
| Subject | Microsoft account unusual sign.in activity |
| Reply-To | info@secaccinfoaccesses.com |
| Date/Time | Fri, 08 Dec 2023 01:45:47 +0000 |
| Platform (claimed) | Windows 10 |
| Browser (claimed) | Firefox |

# 3. Social Engineering Indicators

* Urgency/Fear: Claims login from 'Russia/Moscow' to cause panic.
* Authority Abuse: Spoofs Microsoft branding to build trust.
* Call to Action: Encourages user to click 'Report The User'.
* Technical Misdirection: Uses a mailto: link and odd formatting like 'sign.in'.

# 4. Link and Domain Analysis

Report button hover shows:

mailto:info@secaccinfoaccesses.com?subject=unusual signin activity&body=Report The User

Domain: secaccinfoaccesses.com

Findings:

* - Domain is unrelated to Microsoft
* - Likely recently registered
* - Should be checked on VirusTotal and WHOIS

# 5. Content Red Flags

* Unusual spelling: 'sign.in' instead of 'sign-in'.
* Poor grammar and punctuation.
* Generic signature: 'The Microsoft account team' with no details.
* No personalization of recipient's name.

# 6. Threat Impact

If a user interacts with the phishing email:

* They could begin communication with a malicious actor.
* They might disclose sensitive credentials.
* They could become a victim of further spear-phishing or malware attacks.

# 7. Defensive Measures

* Do not interact with suspicious links or buttons.
* Report the email to security or abuse teams.
* Educate users on phishing red flags and email link inspection.
* Block related domains and IPs in mail and firewall systems.

# 8. Conclusion

This phishing email uses social engineering to impersonate Microsoft and deceive users into taking unsafe actions. It demonstrates the importance of email scrutiny and user training in preventing credential theft and account compromise.

# 9. Tools & Methodology

## Tools Used:

|  |  |
| --- | --- |
| Tool | Purpose |
| Thunderbird | Email client used to view full message source |
| VirusTotal | URL/domain reputation scanning |
| WHOIS Lookup | Identifying domain registration details |
| URLScan.io | Safe inspection of email links and redirections |
| Virtual Machine (Kali Linux) | Isolated lab analysis environment |
| Command-line tools (dig, host, nslookup) | DNS inspection of suspicious domains |

## Steps Taken:

* Opened the phishing email in Thunderbird within an isolated VM.
* Extracted full headers and analyzed sender information.
* Hovered over embedded buttons and links to inspect destination addresses.
* Submitted suspicious domain (secaccinfoaccesses.com) to VirusTotal and WHOIS.
* Parsed the mailto: link to understand attacker intent.
* Documented findings, indicators, and threat potential for this report.
* 📎 Email Sample: The analyzed phishing email was obtained from the open-source GitHub repository \*\*PhishingPot\*\*, specifically the file `sample-2389.eml`, used for educational and training purposes.