Exported from Obsidian. Formatting Retained for Obsidian Compatibility

**###Phishing Email Analysis Checklist###**

\*\*1. Identification & Confirmation\*\*

- \*\*Analyze Email Content:\*\*

- Examine sender’s email address, reply-to, and domain reputation.

- Sender Email Address:

- Sender IP:

- Sender Display Name:

- Subject:

- Recipient:

- Review email headers and any embedded links or attachments.

- DMARC:

- DKIM:

- SPF:

- \*\*Determine Authenticity:\*\*

- Compare email content against known threats

- VirusTotal Results:

- Spoofable?:

- \*\*Log Evidence:\*\*

( Preserve the original email and screenshots.)

- Email Preview:

\*\*2. Containment\*\*

- \*\*Immediate Actions:\*\*

- Sender and Subject Search:

- Number of Emails from Sender Last 30 days:

- Number of matching Subjects Last 30 days:

- Isolated series of emails or larger campaign?

- If Campaign, finish isolating initial threat ASAP and create side investigation for larger campaign next, repeating template steps

- Quarantine the email on all affected systems.

- Soft Delete/Quarantine Emails:

- Report emails to Security Service as confirmed threats:

- Block sender addresses, domains, and suspicious IP addresses on email gateways/firewalls.

- Exchange Sender Email Address:

- Exchange Sender Domain: ``` example .com ```

- Network Domain Block: ``` example2 .com```

- Network IP Address Block :

- \*\*Notify Affected Parties:\*\*

- Inform end users of email disposition/provide further guidance (not to interact with similar emails, or safe).

- Sent non-malicious notification:

- Sent malicious communication:

- Sent Password Reset request:

- Sent Device Isolation Notification:

\*\*3. Eradication\*\*

- \*\*Update Security Controls:\*\*

- Create Specific Transport Rules blocking Sender Mail Flow (if needed).

- Update threat intelligence feeds:

- Rotate compromised credentials:

- Revoke user access sessions:

\*\*4. Recovery\*\*

- \*\*Verify System Integrity:\*\*

- Check for any lateral movement or signs of compromise from link clicks or attachments.

- \*\*Reinforce User Training:\*\*

- Remind employees of best practices for identifying phishing emails.