**PHISHING EMAIL RUN BOOK**

**L1**:

|  |  |
| --- | --- |
| 1 | LOGOS |
| 2 | Is the email Poorly written? |
| 3 | Does the email create the sense of urgency? |
| 4 | Does email direct you to click on the link or download the attachment. |

**Step 1**:

Email body analysis

**Step 2**:

|  |  |
| --- | --- |
| 1 | Reputation of the sender Domain. |
| 2 | Is the Domain lookalike/Misspelled? |
| 3 | IP reputation of the sender |

Sender Analysis

**Step 3**:

|  |  |
| --- | --- |
| 1 | SPF, DKIM, DMARC- Pass/Fail |
| 2 | SCL, BCL Scores |
| 3 | From and Return to path are same. |

Header Analysis

**Step 4**:

|  |  |
| --- | --- |
| 1 | URL/Attachments are submitted to analysis |

Dynamic malware analysis

**L2**:

**Step 5**:

Check how many of them have received this email- from email Gateway. More the numbers-higher the priority.

|  |  |
| --- | --- |
| Email Gateway: Barracuda | Overview>Message log |

**Step 6**:

Purge the email by intimating your shift lead.

|  |  |
| --- | --- |
| KnowBe4 | Phish Rip |

**Step 7**:

Check how many Users have opened link

|  |  |
| --- | --- |
| Zscaler | Analytics>Web Insights |

**Step 8**:

Raise a ticket (incident) to IAM (Identity Access Management team

|  |  |
| --- | --- |
| ServiceNow | Incident>Create New>export>add attachment |

**Step 9**:

Block the sender email ID on email gateway.

|  |  |
| --- | --- |
| Barracuda | Inbound Settings>Sender policy |

**Step 10**:

Block the IP on firewall by raising the INCIDENT to NOC team

**Step 11**:

Intimate team lead and manager to block URL if same URL is sent by different email.