Phishing – Process Flow

```
START
Email Detected/
Reported to
Phishing DL
```

Type of Phish?

Payload Downloader (URL or Attachment)

IT Messaging: Block Sender & Purge Emails

Is Malware Blocked By AV or EDR?
- No → Escalate to GSO IR for investigation
- Yes → Notify All Recipients → END

Credential Harvester

Only Includes URL Blocked by Microsoft?
- No → URL or Attachment Not Blocked by Microsoft
- Yes → Was the URL Clicked by User?

URL or Attachment Not Blocked by Microsoft → Notify All Recipients

Total Recipients?
- <25 → (to Was the URL Clicked by User?)
- 25 to 100 → IT Messaging: Block Sender
- >100 → IT Messaging: Block Sender & Purge Emails

Was the URL Clicked by User?
- Yes → (to Total Recipients flow / Were Credentials Shared?)
- No → END

Were Credentials Shared?
- Yes → Escalate to GSO IR for investigation
- No → END

Escalate to GSO IR for investigation → END

END