REPORTING PROCESS & WHO TO CONTACT

Importance of Reporting Phishing

- Early reporting prevents large-scale compromise.
- Helps security teams block malicious senders and links.
- Protects other employees from falling victim.
- Improves incident response readiness.

When You Should Report

When you receive suspicious emails or messages.

When a link or attachment looks unusual or unexpected.

When someone asks for credentials or sensitive info.

Immediately after accidental clicks or data disclosure.

Internal Reporting Channels

- Dedicated security or IT helpdesk.
- Official incident reporting portal or ticketing system.
- Phishing reporting email (e.g., security@company).
- “Report Phishing” button integrated into email platforms.

What to Include in a Report

- Full email or message screenshot.
- Sender details and suspicious link(s).
- Context of how you received it.
- Whether you clicked anything or responded.

Why Timing Matters

- Phishing threats spread fast and target multiple users.
- Early alerts help isolate malicious domains or servers.
- Reduces attacker dwell time.
- Prevents credential misuse by attackers.

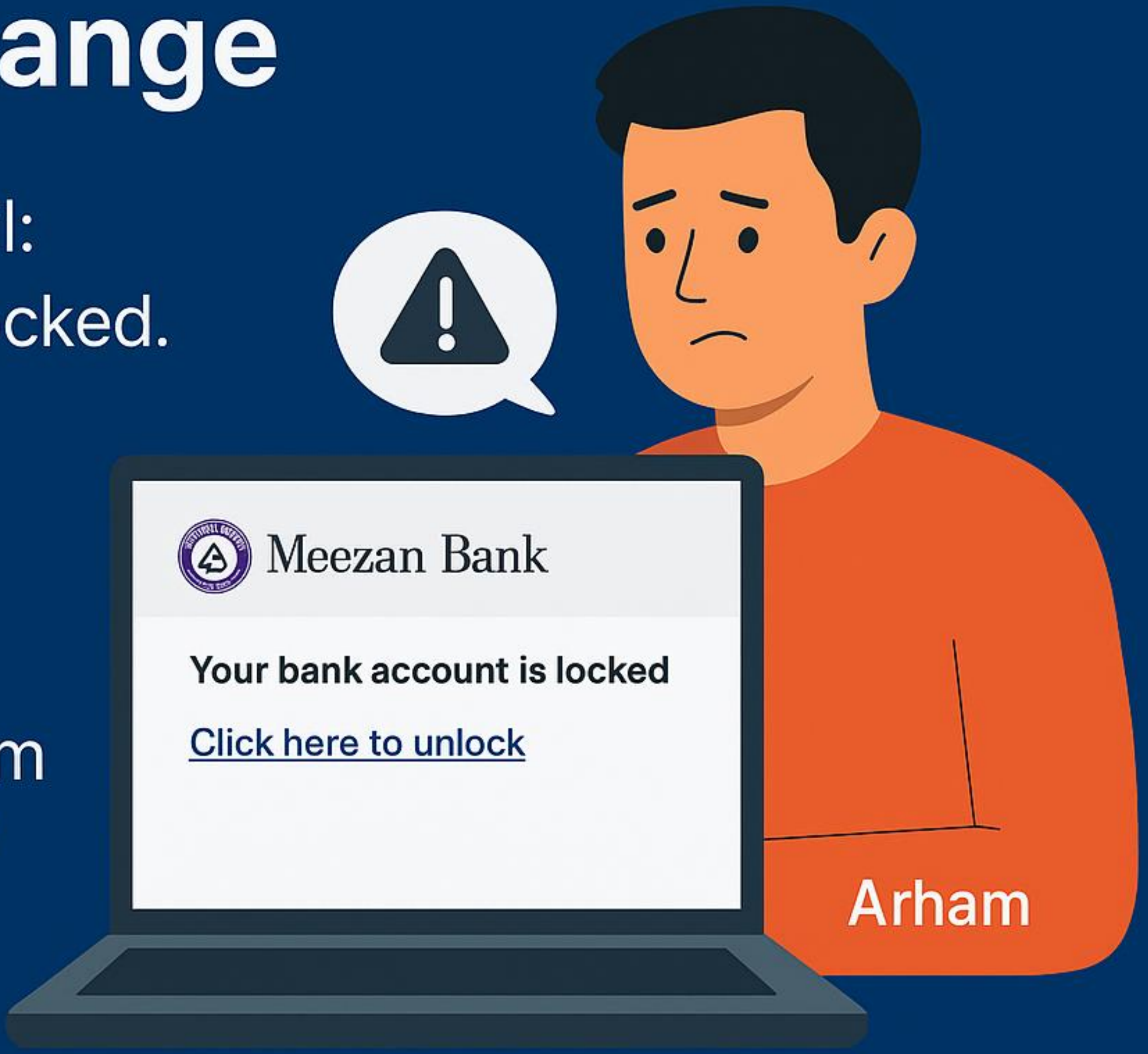
Incident Response Team Responsibilities

- Validate and analyze the reported threat.
- Block malicious domains, IPs, and sender addresses.
- Reset compromised accounts immediately.
- Notify affected users and guide recovery actions.

Arham Notices Something Strange

- Arham receives an email: "Your bank account is locked. Click here to unlock."
- The sender's address looks odd.
- Instead of clicking, Arham reports it to the security team

> The team confirms it was a phishing attack



Meezan Bank

Your bank account is locked

Click here to unlock

Escalation Path

Frontline helpdesk → Security team → Incident response team → Management (if required).

Critical incidents may involve legal teams or external cybersecurity partners.

Escalation depends on the severity of impact.

All steps follow standard operating procedures.