Phishing Checklist

This document is a Standard Operating Procedure (SOP) style checklist to use when responding to a phishing alert.

Status	Step	Description
I. Identification & Triage		
[X]	Confirm Email Headers	Confirmed sender's true source IP and reviewed DMARC/SPF/DKIM alignment for sender authenticity.
[X]	Check Link Reputation	Checked malicious URLs or file hashes against public threat intelligence (VirusTotal/OTX).
II. Containment & Eradication		
[X]	Identify Affected Users	Identified all users who received the email and any who clicked the link.
[X]	Isolate Endpoints	Isolated any endpoint that executed the malicious payload or submitted credentials (Crucial step).
[X]	Delete Malicious Email	Deleted the threat email from all company mailboxes (using an automated tool or mail gateway).
III. Post-Incident & Reporting		
[X]	Notify Stakeholders	Notified necessary stakeholders (C-Suite/Legal/HR Department).
[X]	Evidence Acquisition	Initiated volatile data collection (netstat, memory dump) on affected systems for forensic analysis.
