

FREE COMMUNITY ASSET

Phishing Awareness & Rapid Incident Response Protocol

Practical telemetry and tactical steps to dissect modern AiTM proxies, QR-code lures, analyze email headers, and execute rapid session revocations.

1.0 THE MODERN PHISHING LANDSCAPE

Phishing attacks have evolved beyond generic spelling errors and fake lottery winnings. Attackers utilize sophisticated tactics that evade standard mail filters:

- * **Adversary-in-the-Middle (AiTM):** Reverse-proxy sites that clone real Microsoft/Google login pages, intercepting user credentials AND active session cookies simultaneously.
- * **Quishing (QR Code Phishing):** Embedding QR codes inside PNG/PDF attachments. Because email filters scan text rather than image pixels, these bypass standard gateways.
- * **Executive Impersonation & Wire Fraud:** Registering lookalike domain names (e.g., 'bvrn-1.com' vs 'burn-1.com') requesting urgent vendor wire changes or gift cards.

2.0 FORENSIC EMAIL HEADER ANALYSIS IN 60 SECONDS

When an email looks suspicious, examine the raw headers before clicking. In Outlook, select: File > Properties > Internet Headers. Inspect these three critical lines:

- * **SPF (Sender Policy Framework):** Must return 'spf=pass'. If 'softfail' or 'fail', the sending server is unauthorized.
- * **DKIM (DomainKeys Identified Mail):** Cryptographic signature verifying the message body was not altered in transit. Look for 'dkim=pass'.
- * **DMARC (Domain-based Message Authentication):** Specifies what happens if SPF/DKIM fail. Look for 'dmarc=pass'.

IMMEDIATE TRIAGE RULE

If an email demands urgent financial transactions, requests credentials, or prompts multi-factor approvals, NEVER reply or click. Pick up a phone and call the purported sender using a known, trusted telephone number.

3.0 THE 4-MINUTE INCIDENT RESPONSE CHECKLIST: CLICK -> QUARANTINE

- * **[] 00:00 - Disconnect & Revoke:** Do NOT shut down the machine. Unplug ethernet or disconnect Wi-Fi to stop lateral movement. Open <https://mysignins.microsoft.com> from a secondary phone/PC and select 'Sign out of all sessions'.
- * **[] 01:00 - Credential Reset:** Immediately reset the account password from the clean secondary device. Ensure the new password is at least 16 characters.
- * **[] 02:00 - Audit Mailbox Forwarding Rules:** Open Outlook Web App > Settings > Mail > Rules. Check for hidden rules created by attackers (e.g., rules named '.' or 'auto' moving emails to RSS Feeds or Deleted Items).
- * **[] 03:00 - Review Connected OAuth Apps:** Navigate to <https://myapps.microsoft.com>. Audit third-party apps granted mailbox or file permissions. Revoke any unrecognized integrations.

- * [] **04:00 - Offline Endpoint Scan:** Initiate a full offline antimalware scan (Windows Defender Offline or Mender runtime sweep).

4.0 ESTABLISHING A BLAMELESS CULTURE

Punishing employees who fall for phishing attacks incentivizes them to hide breaches until it is too late. Reward rapid reporting. A reported compromise mitigated within 5 minutes saves an organization hundreds of thousands in ransomware remediation.

5.0 OFFICIAL THREAT INTEL RESOURCES

CISA Phishing Guidance: <https://www.cisa.gov/resources-tools/resources/avoiding-social-engineering-and-phishing-attacks>

Microsoft Incident Response: <https://learn.microsoft.com/en-us/security/incident-response/>

Burn-1 Threat Advisory: <https://burn-1.com/tools.html>