Professional Email Security Readiness Assessment Checklist

Use the following checklist to assess your organisation's current level of email security maturity and phishing resilience.

Check each statement honestly.

Leadership & Culture

☐ Leadership actively supports cybersecurity awareness
☐ Employees are encouraged to report suspicious emails
☐ Verification culture exists for unusual requests
☐ Staff understand modern phishing risks
☐ Security awareness training is ongoing

Technical Protection

☐ Multi-factor authentication is enabled for email systems
☐ SPF records are configured properly
☐ DKIM protection is enabled
☐ DMARC policies are implemented
☐ Secure email filtering tools are deployed

Employee Awareness

☐ Staff understand phishing manipulation tactics
☐ Employees verify unusual financial requests
☐ Teams understand executive impersonation risks
☐ Suspicious attachments are treated cautiously
☐ Employees know how to escalate concerns quickly

Financial & Operational Controls

☐ Payment verification procedures are documented
☐ Banking detail changes require independent confirmation
☐ Finance approvals involve multiple reviewers where appropriate
☐ Supplier communication processes are verified regularly
☐ Executive payment requests are validated independently

Remote & Hybrid Workforce Security

☐ Remote staff receive cybersecurity awareness guidance
☐ Mobile device security policies are established
☐ Employees understand public Wi-Fi risks
☐ Collaboration platform impersonation risks are discussed
☐ Secure password management practices are encouraged

Scoring Your Readiness

20–25 Checked

Strong Maturity

Your organisation demonstrates strong email security awareness and operational resilience.

Continue refining:

- awareness programs,
- verification culture,
- and incident preparedness.

Regular reinforcement will help maintain resilience as threats evolve.

10–19 Checked

Moderate Exposure

Your organisation has some foundational protections in place but still faces meaningful exposure to phishing, impersonation, and operational email fraud.

Focus on:

- awareness consistency,

- verification procedures,
- and layered protection strategies.

Incremental operational improvements can significantly reduce risk.

0–9 Checked

High Vulnerability

Your organisation may face significant exposure to:

- phishing attacks,
- credential theft,
- impersonation scams,
- and financial fraud.

Immediate focus should include:

- employee awareness,
- MFA deployment,
- verification procedures,
- and incident response preparation.

Modern phishing attacks increasingly target operational behaviour directly.