Workplace Phishing Awareness Audit Checklist

20-Point Team Anti-Phishing Audit

☐ Do employees understand modern polished phishing?
☐ Are fake invoice scams discussed?
☐ Is CEO fraud explained?
☐ Are display-name tricks understood?
☐ Are fake login pages recognized?
☐ Are MFA fatigue scams explained?
☐ Are SMS/chat phishing risks discussed?
☐ Do employees verify links before clicking?
☐ Are suspicious attachments treated cautiously?
☐ Is manual login encouraged over emailed links?
☐ Is suspicious message reporting easy?
☐ Is false-alarm reporting encouraged?
☐ Are payment changes voice-verified?
☐ Are executive urgent requests confirmed?
☐ Are remote staff given extra verification rules?
☐ Are mobile approvals treated cautiously?
☐ Does leadership encourage calm verification?
☐ Is no-shame reporting part of culture?
☐ Are phishing reminders repeated monthly?
☐ Would one rushed click still create major damage?

Scoring:

17–20 = Strong workplace phishing maturity
12–16 = Moderate employee exposure
0–11 = High social engineering vulnerability