Professional Cyber Readiness Self-Assessment Checklist

Score each item:

- Yes = 2 points
- Sometimes = 1 point
- No = 0 points

Daily Protection Habits

☐ I pause before clicking urgent email links or attachments.
☐ I verify unusual payment or approval requests independently.
☐ I use unique passwords across important accounts.
☐ I use a password manager consistently.
☐ Multifactor authentication is enabled on key work accounts.
☐ I review login alerts and MFA prompts carefully.
☐ My devices are updated promptly.
☐ I lock my laptop and phone when unattended.

Device & Access Control

☐ I avoid using unsecured public Wi-Fi without protection.
☐ I do not leave work devices unattended in public areas.
☐ Sensitive files are not stored casually on unsecured local drives.
☐ I regularly sign out of unused sessions and admin panels.
☐ I avoid mixing personal and business accounts unnecessarily.

Cloud & File Sharing Discipline

☐ I review file sharing permissions before sending links.
☐ Temporary external access is removed when no longer needed.
☐ I know who currently has access to sensitive shared folders.
☐ I avoid oversharing documents using public unrestricted links.

Communication Awareness

☐ I inspect sender details rather than trusting display names alone.
☐ I am cautious with executive urgency requests and invoice emails.

☐ I do not submit credentials through emailed login prompts without verification.
☐ I question messages that pressure immediate action.

Public Visibility & Professional Behaviour

☐ I avoid posting operationally sensitive work information publicly.
☐ I think carefully before sharing travel, vendor, or internal timing details online.
☐ I maintain consistent cyber habits whether in office, remote, or traveling.
☐ I follow a repeatable short cyber hygiene routine during the workweek.

SCORING RESULTS

40–50 Points → Strong Maturity

You demonstrate strong professional cyber discipline and reduced day-to-day exploitability. Continue refining consistency.

25–39 Points → Moderate Exposure

You understand many cyber basics but still maintain several workflow habits that attackers can exploit under pressure.

0–24 Points → High Vulnerability

Your current professional routine likely contains multiple avoidable weaknesses that increase risk of account compromise, fraud, or operational disruption.