Password Security Readiness Checklist

Use this checklist to evaluate your current password security habits and digital identity protection readiness.

Check each item that accurately reflects your current behaviour.

Password Habits

☐ 1. I use unique passwords for important accounts.

☐ 2. I avoid reusing passwords across multiple services.

☐ 3. My passwords are long enough to resist common attacks.

☐ 4. I avoid predictable password patterns such as names or simple dates.

☐ 5. I update weak or reused passwords when necessary.

Password Management

☐ 6. I use a password manager or another organised credential system.

☐ 7. I can securely access important credentials without relying entirely on memory.

☐ 8. I store recovery information safely.

☐ 9. I know how to recover important accounts if devices are lost.

☐ 10. I avoid storing passwords insecurely in public or easily accessible locations.

Multi-Factor Authentication

☐ 11. MFA is enabled on my most important accounts.

☐ 12. My email account is protected with MFA.

☐ 13. I understand how authentication apps work.

☐ 14. I do not approve unexpected MFA requests.

☐ 15. I maintain backup access methods for MFA-protected accounts.

Phishing and Credential Theft Awareness

☐ 16. I recognise common phishing warning signs.

☐ 17. I verify suspicious login requests carefully.

☐ 18. I avoid entering credentials into unfamiliar websites.

☐ 19. I monitor breach notifications or suspicious account activity.

☐ 20. I understand how credential stuffing attacks work.

Family, Work, and Device Security

☐ 21. Shared accounts are managed intentionally and securely.

☐ 22. Work credentials remain separate from personal accounts whenever possible.

☐ 23. My devices use screen locking or biometric protection.

☐ 24. I avoid sharing passwords casually through insecure communication methods.

☐ 25. I understand that cybersecurity depends partly on sustainable human habits.

SCORING YOUR RESULTS

Strong Maturity: 20–25 Checked Items

You demonstrate strong password awareness and practical digital security habits.

You likely maintain:

- organised credentials,
- MFA protection,
- password uniqueness,
- and healthy cybersecurity awareness.

Your next step is continuing regular reviews, maintaining good habits, and adapting to evolving digital identity systems over time.

Moderate Exposure: 12–19 Checked Items

You have some strong security habits in place, but gaps may still create avoidable risk.

Common issues at this level include:

- password reuse,
- incomplete MFA adoption,
- inconsistent recovery planning,
- or weak credential organisation.

Your next step is improving password uniqueness, adopting stronger management systems, and strengthening phishing awareness.

High Vulnerability: 0–11 Checked Items

Your current password habits may create significant exposure to:

- account compromise,
- phishing attacks,
- identity theft,
- and credential reuse attacks.

Your next step is establishing foundational password management practices, enabling MFA, and organising credentials more securely.