Mobile Security Readiness Checklist

Use the checklist below to evaluate the strength of your current mobile cybersecurity habits and operational readiness.

Device Security

☐ My mobile devices use strong screen lock protection
☐ Biometric authentication is enabled where appropriate
☐ My devices receive regular operating system updates
☐ Device encryption is enabled on my smartphones and tablets
☐ I use remote tracking and remote wipe features

Authentication & Account Protection

☐ I use unique passwords for important accounts
☐ Multi-factor authentication is enabled on critical services
☐ My recovery methods and backup codes are current
☐ I use a password manager securely
☐ I review suspicious login alerts promptly

App & Permission Management

☐ I only install apps from trusted sources
☐ I review app permissions regularly
☐ I remove unused or outdated apps periodically
☐ I avoid unnecessary third-party integrations
☐ I understand the privacy implications of app tracking

Connectivity & Communication Security

☐ I use caution when connecting to public Wi-Fi
☐ I verify suspicious emails and messages before responding
☐ I avoid conducting sensitive activity on unsecured networks
☐ I understand the risks of mobile phishing attacks
☐ I reduce unnecessary notification overload

Data Protection & Privacy

☐ Personal and business information are separated where possible
☐ Sensitive files are stored securely
☐ I review cloud-sharing permissions regularly
☐ I minimise unnecessary location tracking
☐ I limit excessive personal information sharing online

Incident Preparedness

☐ I know how to respond if my device is lost or stolen
☐ I maintain secure backups of important mobile data
☐ I understand the signs of possible device compromise
☐ I report suspicious activity promptly when necessary
☐ I maintain regular mobile security maintenance routines

SCORING RESULTS

Strong Maturity (22–29 Checked)

Your mobile security habits demonstrate strong operational awareness and disciplined digital behaviour.

You likely maintain:

- strong visibility,
- reduced exposure,
- healthy mobile security practices,
- and solid long-term resilience.

Continue reviewing and refining your mobile security environment regularly.

Moderate Exposure (14–21 Checked)

You have a reasonable mobile security foundation, but several gaps may still create unnecessary risk.

Focus on improving:

- authentication,
- update discipline,
- app management,
- and public network awareness.

Consistent improvements can significantly strengthen your resilience.

High Vulnerability (0–13 Checked)

Your current mobile security habits may expose you to significant avoidable risk.

Weaknesses in:

- device management,
- authentication,
- connectivity practices,
- or incident preparedness
  can increase vulnerability to compromise.

Prioritise foundational improvements immediately to reduce exposure and improve operational control.