LinkedIn Security And Brand Protection Checklist

Use this checklist to evaluate your current LinkedIn security posture, professional visibility management, and digital trust readiness.

Check each item that accurately reflects your current practices.

Account Security

☐ 1. I use a strong, unique password for my LinkedIn account.

☐ 2. Multi-factor authentication (MFA) is enabled on my LinkedIn account.

☐ 3. I regularly review login activity and connected devices.

☐ 4. I avoid reusing LinkedIn credentials across other platforms.

☐ 5. I review connected third-party applications periodically.

Privacy and Visibility Management

☐ 6. I have reviewed my LinkedIn privacy settings within the past six months.

☐ 7. My contact information is not unnecessarily exposed publicly.

☐ 8. I intentionally control what information appears on my public profile.

☐ 9. My connection list visibility is appropriately restricted.

☐ 10. I understand how my activity visibility settings function.

Phishing and Social Engineering Awareness

☐ 11. I verify suspicious recruiter outreach before engaging deeply.

☐ 12. I avoid clicking unexpected links in LinkedIn messages.

☐ 13. I evaluate unfamiliar connection requests carefully.

☐ 14. I recognise common social engineering warning signs such as urgency and unusual requests.

☐ 15. I independently verify sensitive or high-risk requests outside LinkedIn when necessary.

Professional Brand Protection

☐ 16. I periodically search for fake profiles or impersonation attempts using my name or image.

☐ 17. I avoid oversharing sensitive operational or organizational information publicly.

☐ 18. My public communication reflects professional standards consistently.

☐ 19. I review AI-assisted content carefully before posting publicly.

☐ 20. I understand that my online behaviour affects professional credibility and trust.

Organisational and Executive Protection

☐ 21. My organisation provides guidance regarding professional social media awareness.

☐ 22. Executives and public-facing employees receive additional awareness regarding impersonation risks.

☐ 23. My organisation has clear reporting procedures for suspicious LinkedIn activity or account compromise.

☐ 24. Company page administration access is reviewed periodically.

☐ 25. Employees understand safe networking and responsible public information sharing expectations.

SCORING YOUR RESULTS

Strong Maturity: 20–25 Checked Items

You demonstrate strong professional security awareness and digital brand protection habits.

You likely maintain:

- intentional visibility,
- strong account security,
- professional networking discipline,

- and healthy cybersecurity awareness.

Your next step is continuing regular monitoring, maintaining evolving awareness, and strengthening long-term digital resilience practices.

Moderate Exposure: 12–19 Checked Items

You have some important protections in place, but gaps may still create unnecessary risk.

Common exposure areas at this level include:

- inconsistent privacy reviews,
- weak connection verification habits,
- insufficient impersonation monitoring,
- or limited organisational awareness.

Your next step is improving routine security habits, reviewing visibility settings, and strengthening professional verification practices.

High Vulnerability: 0–11 Checked Items

Your LinkedIn visibility may currently create avoidable professional and cybersecurity exposure.

Risks at this level may include:

- phishing vulnerability,
- impersonation exposure,
- weak account protection,
- oversharing,
- and poor professional visibility control.

Your next step is establishing stronger account security, reviewing privacy settings, enabling MFA, and improving awareness regarding professional social engineering risks.