Cybercriminal Mindset Awareness Checklist

20-point defensive thinking audit

☐ Do I understand that attackers choose easy targets?
☐ Are important passwords unique?
☐ Is MFA active?
☐ Do I distrust urgent digital requests?
☐ Do I verify before clicking login links?
☐ Do I question polished scam messages?
☐ Do I understand that automation targets everyone?
☐ Do I know attackers use reconnaissance?
☐ Do I monitor suspicious account activity?
☐ Do I report odd emails quickly?
☐ Do I recognise social engineering pressure?
☐ Do I understand silent persistence tactics?
☐ Do I avoid panic money transfers?
☐ Do I slow down payment approvals?
☐ Do I inspect unusual login prompts?
☐ Do I discuss cyber weirdness openly?
☐ Do I understand attackers monetise predictability?
☐ Do I maintain account visibility?
☐ Do I think in terms of friction and verification?
☐ Am I becoming less predictable online?

Scoring:

17–20 = Strong attacker-awareness maturity
12–16 = Moderate predictable exposure
0–11 = High behavioural vulnerability