Cyber Hygiene Self-Assessment (0–100) + Personal Report

Premium Edition — Course-Net

Workshop : **Cyber Hygiene 2026** (Proteksi Akun & Keuangan Digital)

Nama Peserta :

Tanggal :

🛡️ **Privacy:** Jangan tulis email/nomor/ID asli di dokumen ini.

---

1) Cara Pakai (2 menit)

1. Isi checklist dan beri skor sesuai poin.
2. Jumlahkan skor per section → total 0–100.
3. Gunakan "Recommendation Engine" di akhir untuk menentukan **3 prioritas** minggu ini.
4. Salin "Personal Report" (bagian 6) dan simpan sebagai PDF.

---

2) Skor & Interpretasi

Total Score (0–100): **/ 100**

Kategori:

- **0–39 (Red):** Risiko tinggi (mudah takeover/cascade)
- **40–59 (Amber):** Ada celah kritis (butuh hardening segera)

- **60–79 (Green):** Cukup kuat (butuh konsistensi & monitoring)
- **80–100 (Elite):** Tahan serangan umum (tinggal maintain + rehearsal SOP)

---

3) Section A — Account & Password Hygiene (Max 20)

Fokus: menghentikan "password reuse" dan cascade.

Checklist (centang jika **sudah**):

1. ☐ Saya **tidak** reuse password di akun penting (Email/Financial/Marketplace) (**4**)
2. ☐ Saya memakai password unik minimal **12+ karakter** untuk akun penting (**3**)
3. ☐ Saya memakai password manager / metode penyimpanan aman (bukan catatan chat) (**3**)
4. ☐ Saya mengganti password jika ada indikasi breach/alert (bukan menunggu) (**3**)
5. ☐ Saya punya "reset order" saat insiden: Email → Financial → Marketplace → Social (**3**)
6. ☐ Saya punya notifikasi login aktif di akun penting (**2**)
7. ☐ Saya rutin audit akun yang terhubung (connected apps/OAuth) (**2**)

Skor A: _____ **/ 20**

---

4) Section B — 2FA Strategy (Max 20)

Fokus: bukan sekadar "aktif 2FA", tapi strategi yang benar.

1. ☐ Email utama memakai **Authenticator** (bukan SMS) (**6**)
2. ☐ Akun finansial memakai 2FA terkuat yang tersedia (Authenticator/biometrik/device binding) (**5**)
3. ☐ Saya menyimpan **backup codes** dengan aman (offline/secure vault) (**4**)
4. ☐ Saya paham risiko "MFA fatigue" dan selalu **deny** push tak dikenal (**3**)
5. ☐ Marketplace/social punya 2FA aktif (minimal satu) (**2**)

Skor B: _____ **/ 20**

5) Section C — Recovery & Session Control (Max 20)

Fokus: recovery sering jadi pintu takeover kedua.

1. ☐ Recovery email juga aman & punya 2FA (**4**)
2. ☐ Recovery phone number masih aktif dan sepenuhnya saya kontrol (**3**)
3. ☐ Saya pernah cek & bersihkan: email **forwarding/rules/filters** dari rule aneh (**4**)
4. ☐ Saya tahu cara **revoke sessions / sign out all devices** (email & akun penting) (**4**)
5. ☐ Saya rutin cek "login activity/device list" dan menghapus device asing (**3**)
6. ☐ Saya tidak menyimpan OTP/backup code di chat/notes publik (**2**)

Skor C: / 20

---

6) Section D — Anti-Phishing & Verification Habit (Max 20)

Fokus: memutus serangan yang viral (IG login attempt palsu, link cancel transaksi, dsb).

1. ☐ Saya punya aturan emas: **verifikasi via aplikasi resmi**, bukan link dari pesan (**5**)
2. ☐ Saya bisa menyebut minimal 3 red flags phishing (urgency, sender aneh, domain mirip) (**3**)
3. ☐ Saya tidak pernah membagikan OTP/PIN meskipun diminta "CS" (**5**)
4. ☐ Saat dapat alert "login attempt", saya cek via app & security settings (bukan klik email) (**4**)
5. ☐ Saya selalu cek domain/link tanpa mengklik (hover/preview/ketik manual) (**3**)

Skor D: / 20

---

7) Section E — Incident Readiness (SOP) (Max 20)

Fokus: kemampuan mengambil keputusan saat panic mode.

1. ☐ Saya hafal urutan "**15 menit pertama**" (secure email → revoke → reset → lock recovery → freeze financial) (**6**)
2. ☐ Saya punya SOP "24 jam pertama" (rotate password, cek rules, monitor alerts, dispute CS) (**4**)
3. ☐ Saya punya template "incident log" untuk catat waktu, bukti, dan nomor laporan (**3**)
4. ☐ Saya pernah latihan tabletop (skenario takeover/transaksi mencurigakan) minimal 1x (**3**)
5. ☐ Saya punya rencana bantuan (kontak CS resmi/IT/teman tepercaya) tanpa share data sensitif (**4**)

Skor E: _____ / 20

---

8) Total Score

Total = A + B + C + D + E = _____ / 100

---

9) Recommendation Engine (Manual "Auto")

Gunakan aturan sederhana ini:

Jika Skor A < 12

Prioritas: hentikan reuse & buat reset order

✅ Next actions:

- Set password unik untuk email & financial
- Susun Action Matrix 2 akun (today/3d/7d)

Jika Skor B < 12

Prioritas: perkuat 2FA master key

✅ Next actions:

- Email → Authenticator + backup codes
- Financial → metode terkuat yang tersedia

Jika Skor C < 12

Prioritas: recovery + session hijack defense

✅ Next actions:

- Audit forwarding/rules/filter
- Revoke sessions + bersihkan device list

Jika Skor D < 12

Prioritas: anti-phishing habit

✅ Next actions:

- Terapkan “verifikasi via app” rule
- Buat checklist red flags pribadi (tempel)

Jika Skor E < 12

Prioritas: incident readiness

✅ Next actions:

- Print/keep SOP 15 menit + 24 jam
- Latihan tabletop 1x per bulan (5 menit)

---

10) Personal Report (Premium)

Cyber Hygiene Personal Report — 2026

Nama: **Tanggal:**

Total Score: / 100 (**Red / Amber / Green / Elite**)

A) My Top Risks (pilih 3)

- ☐ Password reuse / password lemah
- ☐ 2FA belum tepat (email/financial)
- ☐ Recovery lemah (email/phone/rules)
- ☐ Kebiasaan klik link/urgency trap
- ☐ Belum siap SOP insiden
- ☐ Lainnya:

B) 3 Prioritas Minggu Ini (harus spesifik & doable)

1.
   (Deadline: ☐ Today ☐ 3d ☐ 7d)

2.
   (Deadline: ☐ Today ☐ 3d ☐ 7d)

3.
   (Deadline: ☐ Today ☐ 3d ☐ 7d)

C) My "Golden Rule"

"Saya tidak akan verifikasi alert keamanan lewat link dari pesan. Saya akan verifikasi via "

D) Evidence & Help Plan (jika insiden)

- **Official CS source:**
- **Incident log location (safe):**
- **Trusted helper (opsional):**

E) Signature Commitment

Saya berkomitmen menyelesaikan minimal **3 tindakan** dalam 7 hari.

Tanda tangan: Tanggal: