Checklist minim de securitate pentru IMM-uri

stefanit.org • Versiune: 05.03.2026

Folosește acest checklist ca să verifici rapid dacă firma ta are măsurile de bază care previn cele mai multe incidente (phishing, ransomware, conturi compromise).

1) Conturi & acces

- MFA activ pe email (obligatoriu)
- MFA activ pe conturile critice (hosting, WordPress, DNS, banking)
- Parole unice pentru fiecare cont (fără reutilizare)
- Manager de parole folosit în echipă (unde e cazul)
- Conturi dezactivate imediat când pleacă un angajat

2) Email & phishing

- Filtru antispam activ și actualizat
- Angajații știu să verifice expeditorul și linkurile înainte de click
- Regulă internă: NU se aprobă plăți/IBAN-uri doar din email (confirmare prin al doilea canal)
- Simulare/training phishing cel puțin trimestrial

3) Backup & recuperare

- Backup automat (zilnic/săptămânal) pentru date critice
- Backup offline sau imutabil (protejat de ransomware)
- Test de restaurare făcut cel puțin o dată pe lună
- Știi exact cine răspunde de backup (nume, rol)

4) Update-uri & vulnerabilități

- Update-uri automate pentru OS unde e posibil
- WordPress/temă/pluginuri actualizate regulat
- Aplicații vechi eliminate sau izolate
- Scanare periodică de vulnerabilități (chiar și simplă)

5) Dispozitive & rețea

- Laptopuri cu parolă/biometrie + blocare automată
- Antivirus/EDR activ și actualizat
- Wi-Fi separat pentru oaspeți (guest)
- Acces remote doar prin VPN/soluție securizată

6) Incident response (plan minim)

- Știi cui raportezi intern când apare un incident
- Ai o listă scurtă: ce izolezi, ce oprești, pe cine suni

- Contacte utile: hosting, DNS, IT, banca, furnizori cheie
- Jurnal minim: ce s-a întâmplat, când, ce acţiuni ai luat

Notă: Acest material este educaţional. Adaptează măsurile la contextul firmei tale.