BLOODCODE LABS × ALPHA RED TEAM

Cyber Security Starter Kit

The essential policies, checklists and one-pagers to protect a small business — ready to print and put on the wall.

Business Edition · 2026 | by Stefan Spasov | Bonus with your Awareness Certification

1. Why This Kit

Most small businesses don't get hacked by genius attackers — they get hit by automated, opportunistic attacks that exploit basic gaps: reused passwords, one clicked phishing link, an un-updated laptop. This kit gives you the essentials to close those gaps this week. No jargon, no expensive tools.

> **How to use it:** Print the checklists (Sections 4–6). Assign an owner. Review once a quarter. That alone puts you ahead of most companies your size.

2. Password Policy (copy & adopt)

- Every account uses a **unique** password — never reused across services.
- Minimum a **passphrase of 4 random words** (e.g. *river-tractor-amber-glove*).
- Company provides a **password manager**; staff store all work passwords there.
- **2FA is mandatory** on email, banking, cloud, and admin accounts.
- Shared logins are banned. Each person has their own account.
- When someone leaves, their accounts are disabled the **same day**.

3. Phishing Red-Flags (train everyone)

Signal	What to do
Urgency / threats ("account will be closed")	Slow down. Real institutions don't rush you.
Unexpected attachment or link	Don't open. Verify with the sender directly.
Sender address slightly wrong	Check character by character (paypa1.com ≠ paypal.com).
Asks for password / code / payment	Never provide it via email or link.
Link text ≠ real link (hover to see)	Go to the site directly instead.

> **Golden rule:** When in doubt, verify through a **second channel** — call the person or company using a number you already trust.

4. New Employee — Security Checklist

- ☐ Company account created with unique password + 2FA
- ☐ Added to the password manager
- ☐ Device encrypted and auto-lock enabled (screen locks after 5 min)
- ☐ OS, browser and antivirus updated
- ☐ Read & signed the acceptable-use / data policy
- ☐ Completed the Cyber Security Awareness Certification ✅
- ☐ Knows who to contact to report an incident

5. Monthly Security Checklist

- ☐ All devices and software updated
- ☐ Backups tested — can you actually restore a file?
- ☐ Review who has access to what; remove what's not needed
- ☐ Check for accounts of people who have left
- ☐ Confirm 2FA still active on critical accounts
- ☐ Quick phishing reminder to the team

6. Incident Response — One Page

If you suspect a hack, a lost device, or a data leak — act calmly and fast:

1. **Contain:** Disconnect the affected device from the internet/network.
2. **Change:** Reset passwords for affected accounts from a clean device; enable 2FA.
3. **Report:** Tell the responsible person/IT immediately. Don't hide it.
4. **Preserve:** Don't wipe the device — evidence helps understand what happened.
5. **Assess data:** If personal data may be exposed, note what and whose (GDPR/ZZPL may require notifying authorities within 72 hours).
6. **Learn:** After it's handled, write down what happened and one change to prevent a repeat.

> **Keep this filled in and visible:**
> Incident contact: _____ · Phone: _____
> IT / security partner: _____ · Backup location: _____

7. Zaposleni — 10 pravila (Srpski)

Odštampaj i zalepi pored radnog mesta.

1. Ne kliktaj linkove i priloge iz neočekivanih mejlova. Kad sumnjaš — proveri pozivom.
2. Nikad ne unosi lozinku na stranicu do koje si stigao preko linka iz mejla.
3. Svaki nalog ima **jedinstvenu** lozinku (fraza od 4 nasumične reči).
4. Uključi **2FA** svuda gde možeš.
5. Zaključaj ekran svaki put kad odeš od stola.
6. Ne kopiraj podatke klijenata na privatne uređaje ni javne alate.
7. Ne ubacuj nepoznate USB-ove; ne instaliraj softver iz nepoznatih izvora.
8. Redovno ažuriraj sistem, pregledač i aplikacije.
9. Neobične zahteve (novac, lozinke) uvek proveri drugim kanalom.
10. Prijavi sumnju na napad ili izgubljen uređaj **odmah** — brzina smanjuje štetu.

> **Zapamti:** Bolje jednom previše proveriti nego jednom premalo. Opreznost nije sramota — to je posao.