Cybersecurity Checklist for Small Businesses - 2025 Edition

ECHO PENTEST

Use this practical checklist to quickly evaluate your organization's overall security posture. If you answer "No" or "Not sure" to several items, it may be time for a deeper assessment or a professional penetration test. This checklist is purposely written in plain language — so any business owner or team lead can understand it without needing a security background.

1.   Accounts, Passwords and Access
- All staff use unique passwords for all work systems
- A password manager is used (1Password, Bitwarden, etc)
- Multi-factor authentication (MFA) enabled on: Email, admin portals, VPN, cloud systems
- Departing staff accounts removed immediately

2.   Keep All Systems Updated
- PC's, laptops, servers all auto-update for latest bug fixes
- Website, plugins, CMS, backend frameworks kept current
- Old/unused systems or portals to be removed

3.   Protect Against Phishing
- Staff trained to spot fake emails
- No opening random attachments from unknown sources
- Payment changes should allways be double checked
- Email security filters should be running at all times

4.   Secure Your Internet-Facing Systems
- Staff should use only HTTPS websites
- Admin areas should be protected with physical access controls
- Do not expose unnecessary services
- Have regular Pentesting done within 12-18 months period

5.   Backups and Recovery Plan
- Have a automatic backups running at all times
- Backups should be stored offsite or on cloud not on host where attackers can access them
- Make sure you have tested restoring the back ups
- Make sure sensitive data access is limited

Unsure Where your Business Stands?

If this checklist revealed uncertainties or gaps, that's exactly where a professional penetration test helps

I identify real-world vulnerabilities in your websites, networks, API's and staff processes, then give you clear, practical steps to fix them