

SME Cyber Readiness Checklist 2026

25 questions • 15 minutes • one clear score.

Most attacks on small and mid-sized businesses don't rely on advanced hacking. They rely on a missing basic: an account without MFA, a backup nobody tested, a payment nobody double-checked. This checklist covers the basics that matter most in 2026.

How to use it

1. Answer each question **Yes** or **No**. Not sure? Answer **No**.
2. Score **1 point for every Yes**, per section and in total.
3. Read what your score means on page 3, and start with the **quick wins** in any section scoring 3 or less.

A Phishing & people

		YES	NO
01	Everyone, including management, has had security awareness training in the last 12 months.	☐	☐
02	There's one simple way to report a suspicious email, and people actually use it.	☐	☐
03	Our email domain has SPF, DKIM and DMARC, with DMARC set to quarantine or reject.	☐	☐
04	Staff know how to check a link, and know we never ask for passwords or codes by email, chat or phone.	☐	☐
05	Someone monitors for lookalike domains that impersonate our brand.	☐	☐

Quick wins: add a "Report phishing" button · check your DMARC record with a free online checker · run a 20-minute briefing with our Phishing Red Flags cheat sheet.



> trust = 0; verify --all

Why these 25 questions

They cover the gaps attackers use most: **phishing, identity, AI and payments, patching and backups, and response.**

Best done together

Fill it in with the person responsible for IT (in-house or external) and someone from management or finance. The most useful answers come from where you disagree.

What it is (and isn't)

A self-assessment of common basics. It isn't a full audit, a penetration test or a legal compliance review.

Why Alphatechs

24/7 security operations with a 30-minute response, penetration testing, and Sphere TI, our own threat intelligence platform.

Take the Next Step

Scored lower than you'd like? Free 30-minute call with our team:
alphatechs.al/contact

B Identity & access

	YES	NO
06 MFA is switched on for every email account, including executives and shared mailboxes.	☐	☐
07 MFA is required for VPN, remote access and all cloud admin consoles.	☐	☐
08 Admin accounts are separate from everyday accounts, and there are as few of them as possible.	☐	☐
09 We use a password manager, and staff don't save work passwords in their browsers.	☐	☐
10 We check whether credentials for our domain appear in data breaches or infostealer logs.	☐	☐

Quick wins: list every account without MFA and fix the email ones this week · disable legacy authentication · get a free Sphere TI Exposure Report at sphereti.com.

C AI, data & payments

	YES	NO
11 We have a written policy on which AI tools staff may use and what data they may put into them.	☐	☐
12 Approved AI tools use business accounts, with training on our data switched off.	☐	☐
13 New payees and changed bank details are always verified by calling back a number from our own records.	☐	☐
14 Payments above a set amount need two approvers, with no exceptions for “urgent” executive requests.	☐	☐
15 We know which AI tools, browser extensions and third-party integrations can access company data.	☐	☐

Quick wins: adopt our free AI Acceptable Use Policy template · write the call-back rule into your payment process · review app permissions in your email and cloud admin portals.

D Devices, updates & backups

	YES	NO
16 Updates install automatically; critical patches go in within 14 days, faster for internet-facing systems.	☐	☐
17 Every laptop and server runs modern endpoint protection (EDR), not only basic antivirus.	☐	☐
18 Devices and software that no longer get security updates have been replaced or isolated.	☐	☐
19 We follow the 3-2-1 backup rule, with at least one copy offline or immutable.	☐	☐
20 We have successfully tested restoring from backup in the last 6 months.	☐	☐

Quick wins: turn on automatic updates everywhere · list your end-of-support systems · schedule a test restore of one important system this month.

E Detection & response

	YES	NO
21 Security logs are collected, and someone reviews alerts 24/7 (in-house or through a provider).	☐	☐
22 We have a written incident response plan with named roles and decision-makers.	☐	☐
23 Emergency contacts (IT, provider, management, legal, insurer) are printed and stored offline.	☐	☐
24 We know our legal reporting duties and deadlines (e.g. GDPR 72 hours, NIS2 24-hour early warning).	☐	☐
25 We ran an incident exercise (a tabletop "what if") in the last 12 months.	☐	☐

Quick wins: print an emergency contact sheet today · read our First 60 Minutes card · run a one-hour ransomware tabletop with management.

Your score

A · Phishing & people	___ / 5
B · Identity & access	___ / 5
C · AI, data & payments	___ / 5
D · Devices, updates & backups	___ / 5
E · Detection & response	___ / 5
Total	___ / 25

What your score means

21–25 · Strong foundations
You've covered the basics. Now test them: phishing simulations, restore tests, tabletop exercises and continuous exposure monitoring.

14–20 · Gaps attackers can use
Fix every "No" in sections B and D first. Those are the gaps attackers most often use to get in.

0–13 · Act this month
Start with MFA on all email (Q6), a tested offline backup (Q19–20) and the payment call-back rule (Q13).

Also important: any section scoring 3 or less

A low score in one area can undo strong scores elsewhere. One account without MFA or one untested backup is often all an attacker needs. Treat any section at 3/5 or below as a priority, whatever your total.

Take the Next Step

Free 30-minute call: walk through your results with an Alphatechs security specialist and leave with your top three priorities. Remote, for companies of 10+ employees, until 30 November 2026. alphatechs.al/contact

 **Free Exposure Report from Sphere TI:** check whether your domain's credentials already appear in breaches or stealer logs (Q10). sphereti.com