

SMALL BUSINESS CYBERSECURITY CHECKLIST

10 things you can check today to make your business a harder target.

A free resource from Tivarden Technology Group

1. Turn on MFA

Enable multi-factor authentication on email, banking, Microsoft 365, social media, accounting, cloud storage, and other important accounts.

2. Stop reusing passwords

Use strong, unique passwords. Consider a reputable password manager so one stolen password does not unlock several accounts.

3. Keep systems updated

Install security updates for computers, phones, browsers, applications, routers, and security software. Enable automatic updates where practical.

4. Back up important information

Maintain backups of critical business data and periodically test that you can restore them. Keep at least one backup protected from ordinary user access.

5. Stop before you click

Treat unexpected links, attachments, QR codes, shared documents, and password-reset messages cautiously. Verify through a separate trusted method.

6. Verify requests involving money

Independently confirm new banking details, wire transfers, gift cards, payroll changes, and unusual invoices before acting.

7. Reject unexpected remote access

Do not allow an unsolicited caller or pop-up to take remote control of a business computer. Contact your trusted provider independently.

8. Review account access

Remove former employees and contractors promptly. Give users only the access they need and avoid administrator accounts for routine work.

9. Protect business email

Use MFA and watch for unusual forwarding rules, password resets, or sensitive requests. A familiar display name does not prove who sent the message.

10. Have an incident plan

Make sure employees know who to contact immediately after a suspicious click, exposed password, lost device, fraudulent payment, or unusual account activity.

WARNING SIGNS

Unexpected urgency or secrecy
Changed payment instructions
Unexpected links, files, or QR codes
A sender address that is almost right
Unsolicited tech-support calls
Requests to bypass normal procedures

IF SOMETHING HAPPENS

1. Report it immediately.
2. Disconnect an affected computer if remote access or malware is suspected.
3. From a known-safe device, protect compromised accounts.
4. Contact your bank quickly if money is involved.
5. Preserve messages/details and get qualified help.

REMEMBER: Urgency should never override verification. If a request involves money, passwords, remote access, or an unusual account change, verify it independently first.

Tivarden Technology Group | Protect. Prepare. Advance.

Tivarden.com | tim@tivarden.com

For expanded guidance and cybersecurity resources, visit [Tivarden.com/cybersecurity-checklist.php](https://tivarden.com/cybersecurity-checklist.php)

General cybersecurity awareness information only. Incident circumstances vary and may require professional, legal, insurance, financial, or law-enforcement assistance.