

Small Business Cybersecurity Checkup

Know where your business stands before something goes wrong.

A practical self-assessment for business owners

Cybersecurity is a business continuity issue. Use this checkup to identify where your organization is strong, where it needs attention, and what should happen next. Complete it yourself or review it with your office manager, IT provider, or cybersecurity professional.

How to use this checkup

1. Review each statement and check what is true today.
2. Choose an overall status for each section.
3. Assign an owner, next action, and target date.
4. Finish with your top three cybersecurity priorities.

1. Accounts and Multi-Factor Authentication

Start with the accounts that could cause serious damage if compromised: email, banking, payroll, cloud storage, CRM, website administration, and social media.

- ☐ Multi-factor authentication is enabled on critical accounts.
- ☐ Important accounts use unique passwords or passphrases.
- ☐ We know who has administrator access to key systems.

Overall status: ☐ Yes - covered ☐ Partially ☐ No ☐ Not sure

Who owns this?

Next action

Target date

2. Backups and Recovery

A backup only helps if it is current, protected, and restorable. Know where your backups live and how long recovery would take.

- ☐ Critical business data is backed up regularly.
- ☐ At least one backup is protected from the same incident affecting primary systems.
- ☐ Someone has tested that we can restore data from backup.

Overall status: ☐ Yes - covered ☐ Partially ☐ No ☐ Not sure

Who owns this?

Next action

Target date

Small Business Cybersecurity Checkup

Systems, people, and access

3. Software and System Updates

Security updates often correct known vulnerabilities. Make sure responsibility for updates is clear - not something that happens only when someone remembers.

- ☐ Operating systems and applications receive security updates promptly.
- ☐ Automatic updates are enabled where practical.
- ☐ Website software, network equipment, and connected devices are included in update responsibilities.

Overall status: ☐ Yes - covered ☐ Partially ☐ No ☐ Not sure

Who owns this?

Next action

Target date

4. Employee Awareness

Your employees do not need to be security experts. They do need to recognize common warning signs and know exactly what to do when something looks wrong.

- ☐ Employees receive basic phishing and cybersecurity awareness training.
- ☐ Employees know how to report a suspicious message or request.
- ☐ Staff are expected to verify unusual payment, password, or information requests using a separate trusted method.

Overall status: ☐ Yes - covered ☐ Partially ☐ No ☐ Not sure

Who owns this?

Next action

Target date

5. Access Control

Limiting access can reduce the damage from a compromised account and helps protect sensitive business information.

- ☐ Employees only have access to the systems and information they need.
- ☐ Former employee access is removed promptly.
- ☐ Shared accounts and shared passwords are avoided.

Overall status: ☐ Yes - covered ☐ Partially ☐ No ☐ Not sure

Who owns this?

Next action

Target date

Small Business Cybersecurity Checkup

Vendors and incident readiness

6. Vendors and Third Parties

Cybersecurity risk extends to companies that store, process, or can access your information. Know who has access to what.

- ☐ We know which outside vendors can access sensitive information or systems.
- ☐ Vendor access is limited to what is needed and reviewed periodically.
- ☐ We understand how key vendors protect data and handle security incidents.

Overall status: ☐ Yes - covered ☐ Partially ☐ No ☐ Not sure

Who owns this?

Next action

Target date

7. Incident Response

A cyber incident is not the time to decide who is responsible. Keep essential response information available even if normal email or systems are unavailable.

- ☐ Employees know who to contact first if they suspect a cyber incident.
- ☐ We have current IT, insurance, legal, and leadership contact information available.
- ☐ We have a basic plan for isolating affected systems, restoring operations, and communicating if an incident occurs.

Overall status: ☐ Yes - covered ☐ Partially ☐ No ☐ Not sure

Who owns this?

Next action

Target date

Emergency contacts - keep these somewhere you can reach without your normal systems

IT / cybersecurity contact

Cyber insurance contact

Legal / compliance contact

Cybersecurity Action Plan

Turn the checkup into three concrete next steps

Review the sections you marked Partially, No, or Not sure. Choose the three actions that would most reduce risk or improve your ability to recover, and assign each one a clear owner and target date.

Priority 1

What needs to happen?

Owner

Target date

How will we know it is complete?

Priority 2

What needs to happen?

Owner

Target date

How will we know it is complete?

Priority 3

What needs to happen?

Owner

Target date

How will we know it is complete?

Trusted resources

NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide

<https://www.nist.gov/publications/nist-cybersecurity-framework-20-small-business-quick-start-guide>

FTC Cybersecurity for Small Business

<https://www.ftc.gov/business-guidance/small-businesses/cybersecurity>

FTC Data Breach Response: A Guide for Business

<https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business>

Important

This MSBX resource is an educational self-assessment and starting point. It is not a certification that a business is secure and does not replace professional IT, cybersecurity, legal, insurance, or regulatory advice.