# Small Business Cybersecurity Checklist

A practical, printable security review for small businesses


Use this checklist to review the most important areas of everyday business security - from passwords and multi-factor authentication to backups, employee access, cloud services, and incident preparedness. Mark each item as you complete it, then revisit the checklist every 3-6 months or after major technology changes.

> Quick start: If you can only do five things now, turn to the final page and begin with the five priority actions.

## Passwords & Access

- [ ] Use a password manager for business accounts.
- [ ] Create a unique password for every important account.
- [ ] Avoid sharing passwords through email, messaging apps, or spreadsheets.
- [ ] Use strong passwords for administrator and financial accounts.
- [ ] Remove account access promptly when an employee or contractor leaves.
- [ ] Review shared accounts regularly and confirm that everyone still needs access.

## Multi-Factor Authentication

- [ ] Enable multi-factor authentication on business email accounts.
- [ ] Protect banking, payment, and financial services with MFA.
- [ ] Enable MFA on cloud storage and important business applications.
- [ ] Require MFA for administrator accounts wherever possible.
- [ ] Prefer authenticator apps, passkeys, or physical security keys over SMS when practical.
- [ ] Keep account-recovery information up to date.

## Email Security

- [ ] Train employees to recognize phishing and impersonation attempts.
- [ ] Verify unusual payment requests through a second communication method.
- [ ] Be cautious with unexpected password-reset messages.
- [ ] Use spam, malware, and phishing filtering.
- [ ] Avoid opening unexpected attachments or links.
- [ ] Check the sender address carefully before responding to sensitive requests.

## Devices & Endpoint Protection

- [ ] Use reputable antivirus or endpoint-protection software.
- [ ] Enable device encryption on laptops and mobile devices where available.
- [ ] Require screen locks and strong device login credentials.
- [ ] Keep business devices physically secure.
- [ ] Avoid giving employees unnecessary administrator privileges.
- [ ] Separate personal and business devices where practical.

## Software Updates

- [ ] Enable automatic operating-system updates when possible.
- [ ] Keep browsers and business applications up to date.
- [ ] Update security tools regularly.
- [ ] Remove software that is no longer needed.
- [ ] Replace unsupported operating systems and applications.
- [ ] Review important business software periodically for security updates.

## Backups

- [ ] Back up important business files automatically.
- [ ] Keep at least one backup separate from your primary systems.
- [ ] Protect backup accounts with multi-factor authentication.
- [ ] Confirm that backups are completing successfully.
- [ ] Test whether important files can actually be restored.
- [ ] Keep recovery instructions available to the people responsible for business continuity.

## Employee Security

- [ ] Provide basic cybersecurity awareness training.
- [ ] Teach employees how to report suspicious emails or activity.
- [ ] Explain how business passwords should be stored and shared.
- [ ] Limit access according to each employee's responsibilities.
- [ ] Review access when an employee changes roles.
- [ ] Remove former employees and contractors from business systems promptly.

## Data & Permissions

- [ ] Give employees access only to the information they need.
- [ ] Review administrator privileges regularly.
- [ ] Restrict access to financial, customer, and confidential information.
- [ ] Check permissions on shared folders and cloud storage.
- [ ] Remove outdated users, groups, and shared links.
- [ ] Avoid storing sensitive data unnecessarily.

## Cloud & Business Software

- [ ] Review the security settings of important cloud applications.
- [ ] Remove unused user accounts and integrations.
- [ ] Check which employees can access shared cloud files.
- [ ] Enable available security alerts and login notifications.
- [ ] Review software providers before storing sensitive business information.
- [ ] Keep a list of your most important business applications and account owners.

### Incident Preparedness

- [ ] Decide who should respond if a security incident occurs.
- [ ] Document what employees should do after noticing suspicious activity.
- [ ] Maintain contact information for important service providers.
- [ ] Know how to disable compromised accounts quickly.
- [ ] Keep basic recovery instructions for important systems.
- [ ] Review your cybersecurity plan after significant business or technology changes.

## Start With These Five Priorities

If your business cannot address everything at once, begin with these five actions. They cover several of the most common security weaknesses found in small organizations.

1. Use a business password manager.
2. Enable multi-factor authentication on important accounts.
3. Keep devices and software updated.
4. Maintain reliable, tested backups.
5. Train employees to recognize phishing attempts.

**More practical cybersecurity and software guidance at SecureBizTech.com**