BUSINESS SERVICES
CONNECT

CYBERSECURITY CHECK LIST FOR SMALL BUSINESSES

businessservicesconnect.com

Interactive Cybersecurity Checklist

Use this checklist to strengthen your business's cybersecurity in 30 minutes or less. Whether you're starting from scratch or just need a quick refresh, this tool helps you cover the essentials. You don't need a tech background — just a clear plan and a few small actions to make your business safer.

Section 1: CARE (Culture, Awareness, Reporting, Engagement)

☐ **Foster a culture of alertness**

Treat information as a critical resource, like money or facilities. Executives set the tone by showing they care about security.

☐ **Build continuous awareness**

Keep security top of mind with regular reminders, quick huddles, or training refreshers. Make it part of everyday business, not a once-a-year task.

☐ **Encourage reporting**

Make it simple and safe for employees to report suspicious activity. Consider incentives to reward people who raise potential issues.

☐ **Engage leadership**

Executives should speak openly about the value of information and model good security behavior. When leadership cares, teams follow.

Section 2: Access & Authentication

☐ **Enable multi-factor authentication (MFA)**

Add a second layer of security to logins using a code, app, or device.

☐ **Require strong, unique passwords**

Avoid reused or weak passwords like “admin123.” Use long combinations with letters, numbers, and symbols.

☐ **Use a password manager**

Simplify password storage and sharing with a secure tool that your team can access safely.

☐ **Remove old or unused user accounts**

Deactivate access for former employees or unused services to reduce risk.

☐ **Review admin access levels**

Confirm that only the right people have full control over systems and settings.

Section 3: Backups & Recovery

☐ **Back up critical business data weekly**

Create regular backups of your most important files, such as customer info or financial records.

☐ **Store backups in a secure, encrypted location**

Use cloud storage or offline devices that are protected against theft or tampering.

☐ **Test backup restore functionality**

Make sure you can actually recover your files if needed — don’t wait for a crisis to find out.

☐ **Identify who is responsible for backups**

Assign a team member to own this task and check in regularly.

Section 4: Updates & Patching

☐ **Turn on automatic software and OS updates**

Let devices update in the background so you don't miss important security fixes.

☐ **Audit devices for outdated systems**

Look for older machines or apps that may no longer receive updates.

☐ **Replace unsupported or vulnerable hardware**

If a device can't be secured, it may be time to retire or replace it.

☐ **Schedule regular tech check-ins**

Block off time each quarter to review your systems and spot risks early.

Section 5: Team Awareness & Training

☐ **Schedule a phishing awareness refresh**

Teach your team how to spot suspicious emails and messages.

☐ **Share a "how to report a scam" process**

Make it easy and expected to report anything that seems off.

☐ **Conduct a short cyber hygiene huddle (15 min)**

Hold a quick meeting to go over common scams and simple safety steps.

☐ **Assign one person to watch for suspicious activity**

Designate someone to flag login alerts, odd emails, or system warnings.

Section 6: Business Continuity & Planning

☐ **Create a simple response plan**

Outline what to do if your systems are hacked, including who to call and how to respond.

☐ **Identify go-to contacts for tech support**

List the vendors, IT providers, or advisors you can reach out to quickly.

☐ **Document key tools, contacts, and access info**

Keep a printed or offline copy of system logins and essential information.

☐ **Review cybersecurity insurance (if applicable)**

If you have coverage, know what's included and how to use it.

Cybersecurity doesn't have to be complicated. By checking off a few of these steps each quarter, you'll build habits that keep your team, customers, and operations more secure. Bookmark this checklist, share it with your team, and revisit it regularly to stay ahead of evolving threats.