SMALL BUSINESS CYBERSECURITY

THE ESSENTIAL CHECKLIST

Running a small business is challenging enough without worrying about cybersecurity, but it's a reality you can't afford to ignore. The good news is that protecting your business doesn't have to be overwhelming, especially when you have the proper guidance.

This checklist covers the essential cybersecurity steps every small business should take, focusing on why these actions matter and how a **managed service provider** (MSP) such as us can simplify the process for you.

✓ HARDWARE AND SOFTWARE:

START WITH THE RIGHT TOOLS

Is your hardware and software suited to your business?

It might seem like any laptop or software package will do, but that's not always the case. For example, a laptop purchased from a big department store might come with Windows 11 Home. While it does the job for personal use, it lacks the features necessary for a business environment. Windows 11 Professional, on the other hand, offers stronger encryption, virtualization software, enterprise-level security, and remote PC control, all tools designed to keep your business secure.

Stick to well-known brands

When selecting hardware, consistency is key. It's much easier to manage ten laptops from the same brand with similar chargers and warranties than dealing with a mishmash of different models. Sticking with well-known brands also means you're more likely to get business-level support, which is crucial when something goes wrong.

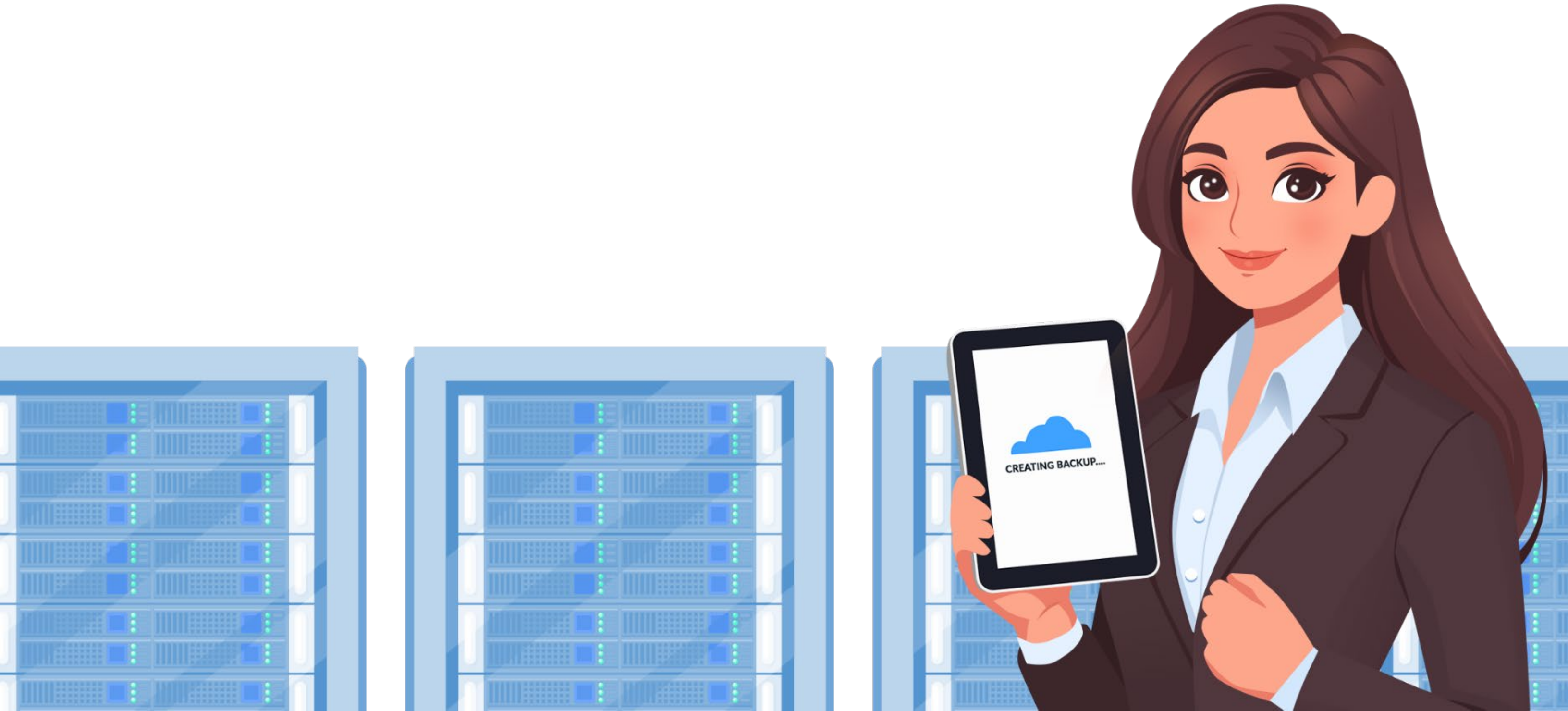
BACKUP: YOUR SAFETY NET

The 3-2-1 backup strategy

Imagine coming to work one day and finding that all your business data is gone. It's a nightmare scenario, but it happens more often than you'd think. That's why regular backups are non-negotiable. The 3-2-1 backup strategy is a simple and effective way to protect your data. Here's how it works:

- **3 copies.** Keep three copies of your data: one in production, one on a local backup, and one offsite.
- **2 different mediums:** Store backups on two different types of media (such as a server and an external hard drive).
- **1 offsite backup:** Store backups on two different types of media (such as a server and an external hard drive).

Daily backups are a must, and hourly backups might be necessary depending on your business.



☑ PASSWORDS:

STRONG AND SHARED SECURELY

How are passwords managed?

Gone are the days when a sticky note under the keyboard was a viable password management system. Today, a password manager such as Bitwarden is a must-have. These tools allow you to create password groups that belong to the business rather than the individual. You can even set up department-specific groups of passwords so that only those who need access to certain information have it.

☑ TWO-FACTOR AUTHENTICATION:

DOUBLE THE SECURITY

Why two-factor authentication matters

Even the best passwords can be compromised. That's why two-factor authentication (2FA) is essential. With 2FA, an additional authentication step is required to gain access even if a username and password are leaked. This could be a code sent to a phone or an authentication app, adding an extra layer of security to your business.

☑ COMPLIANCE:
KNOW YOUR OBLIGATIONS

Understand compliance requirements

You likely have strict data handling requirements if your business operates in industries such as healthcare, finance, or law. Understanding these compliance rules is essential because non-compliance can result in hefty fines and damage to your reputation. Knowing what's required of you is the first step, but implementing those requirements can be a complex task, and this is where an MSP can step in to help.

☑ LEGITIMATE SOFTWARE:
PLAY BY THE RULES

Are you using software legally?

It's tempting to cut corners by using software licenses in ways they weren't intended or by downloading free software. However, this can expose your business to legal risks and security vulnerabilities. Make sure you're obtaining software from legitimate sources and understand the limitations of the licenses you’re using. For example, a single-PC license shouldn't be installed on multiple computers, and some free software may not allow commercial use.

☑ PATCHES AND ANTIVIRUS: KEEP EVERYTHING UP-TO-DATE

Are your systems up to date?

Cybercriminals often exploit vulnerabilities in outdated software. Think of it like leaving a window open in your house; it's an invitation for trouble. Making sure that all your systems are up to date with the latest patches and antivirus software is critical. However, with multiple devices to manage, this can quickly become overwhelming. An MSP can take this off your plate, ensuring every device in your business is secure.

☑ SYSTEM ACCESS: KEEP IT TO A MINIMUM

Limit access to what's necessary

Not everyone in your business needs access to all your systems. For example, your reception staff doesn't need access to accounting data. By limiting access to only what's necessary, you reduce the risk of data breaches and minimize the potential damage if a breach does occur.

✓ MOBILE DEVICES: BUSINESS OR PERSONAL?

What's your policy on mobile devices?

Will you provide employees with business-only mobile devices, or will they use their personal phones and laptops? This decision has significant implications for your business's security. Allowing personal devices introduces risks, such as company data being stored on unprotected devices or an infected personal device spreading malware to your network. A clear policy on mobile device usage is essential to protect your business.

✓ E-MAIL: STAY VIGILANT

Use filters and train your staff

Emails are a common entry point for cyberattacks. Implementing spam and malware filters can catch many threats before they reach your inbox. But technology alone isn't enough. Your staff must be trained to recognize phishing attempts and avoid opening suspicious attachments.

CYBER INSURANCE:
BE PREPARED FOR THE UNEXPECTED

Does your business have cyber insurance?

No matter how prepared you are, breaches can still happen. Cyber insurance can protect your business from the financial fallout of a cyberattack. This includes coverage for business interruption, data loss and restoration, incident-response costs, and liability issues.

If you don't have cyber insurance, it's worth considering as part of your overall cybersecurity strategy.

☑ READY TO PROTECT YOUR BUSINESS?

Keeping your small business secure involves many moving parts, and it can be overwhelming to handle it all on your own. That's where we come in. As a managed service provider, we can implement these essential cybersecurity measures for you so you can focus on what you do best: running your business. Get in touch with us today, and let's make sure your business is protected.

ONE2ONE
TECH SOLUTIONS LLC
SIMPLIFYING TECHNOLOGY FOR SMALL BUSINESS

Phone: **201.490.4600**
Email: hello@teamone2one.com
Web: teamone2one.com

LinkedIn: linkedin.com/company/one2one-tech-solutions
Facebook: facebook.com/njtechservices