

Small Business Security Checklist

These are the practical security issues we repeatedly encounter while helping small businesses manage websites, email systems, domains, cloud services, and online accounts.

Unveil.AI · Technology consulting for small business · unveil.systems

This checklist helps small business owners address common security risks that are frequently overlooked during normal business operations.

Most technology problems we encounter are not caused by sophisticated attacks. More commonly, they involve:

- Missing access controls
- Poor account ownership practices
- Lack of documentation
- Inadequate recovery planning

The goal is to reduce risk by addressing simple, preventable issues.

Plain terms used below. **MFA** (multi-factor authentication) is a second step when signing in, such as a code sent to your phone. **Administrative access** is the ability to change settings and manage other users. A **single point of failure** is something that stops working when one person or one thing is unavailable. **Business continuity** means keeping the business running when something goes wrong. A **password manager** is an app that stores your passwords securely, so you only need to remember one.

By the end of this checklist, you should understand:

- How to secure access to important systems
- How to reduce account ownership risks
- How to improve recovery readiness
- How to avoid common administrative security mistakes

Print this page or download the PDF, and tick off each item as you finish it.

1. Enable Multi-Factor Authentication (MFA)

OBSERVED ISSUE

During Microsoft 365, email, and account setup projects, MFA repeatedly appeared as one of the simplest security protections available.

When MFA is not enabled, a stolen or guessed password may be all that is needed to access important systems.

LESSON

Enable MFA for:

- ☐ Business email
- ☐ Microsoft 365
- ☐ Domain registrars
- ☐ Google Business Profile
- ☐ Hosting providers

Security is strongest when MFA is enabled from the beginning rather than added later.

2. Review Who Has Access

OBSERVED ISSUE

Businesses often know who currently uses a system but may not know:

- Who still has administrative access
- Which accounts remain active
- Which consultants or vendors still have permissions

This becomes particularly important after staffing or vendor changes.

LESSON

Periodically review:

- ☐ Administrative accounts
- ☐ User accounts
- ☐ Vendor access
- ☐ Recovery administrators

3. Avoid Shared Credentials

OBSERVED ISSUE

Access is sometimes passed informally between individuals.

Over time this can make it difficult to know:

- Who has access
- Who changed settings
- Who is responsible for administration
- Where passwords are stored
- Which services share the same password

LESSON

Whenever possible:

- ☐ Use individual accounts
- ☐ Assign permissions appropriately
- ☐ Document administrative ownership
- ☐ Use a different password for each service
- ☐ Store passwords in a password manager

4. Protect Recovery Methods

OBSERVED ISSUE

Many account recovery challenges are caused by outdated recovery information.

Examples we have discussed include:

- Unknown recovery emails
- Old phone numbers
- Lost administrative access
- Passwords that cannot be recovered because no one knows how

The service itself often works correctly. The problem occurs when recovery is needed.

LESSON

Review and document these before a problem occurs:

- ☐ Recovery email addresses
- ☐ Recovery phone numbers
- ☐ Backup administrators
- ☐ How each password is recovered, and who can do it

5. Know Who Controls Critical Business Systems

OBSERVED ISSUE

A recurring theme across domains, websites, Microsoft 365, and online services is uncertainty around ownership.

Businesses sometimes depend on systems controlled by:

- One individual
- A former consultant
- An undocumented account

LESSON

Identify who controls:

- ☐ Domain registration
- ☐ Business email
- ☐ Microsoft 365
- ☐ Hosting
- ☐ Google Business Profile

The business should always know how to regain access if needed.

6. Maintain Basic Technology Documentation

OBSERVED ISSUE

Troubleshooting often becomes harder when businesses cannot quickly locate:

- Vendor information
- Administrative contacts
- Recovery information
- Account ownership records

LESSON

Maintain a simple inventory that includes:

- ☐ Services
- ☐ Vendors
- ☐ Administrators
- ☐ Recovery methods

7. Reduce Single Points of Failure

OBSERVED ISSUE

We have repeatedly encountered situations where a single person controlled an important system.

Examples include:

- Domains
- Email systems
- Google Business Profile
- Hosting providers

Everything works until that person becomes unavailable.

LESSON

Whenever practical:

- ☐ Assign backup administrators
- ☐ Document ownership
- ☐ Ensure business continuity