

RECORDS & SYSTEMS

Protecting Your Business Data: Backups, Passwords and Cyber Basics

Simple, low-cost steps that protect your records, your money and your customers' data from loss, fraud and cyber attack.

FOR: ALL BUSINESS OWNERS • NEW TO CYBER SECURITY

Small businesses are targets too

Owners often assume criminals go after larger firms. In practice, small businesses are attractive because they tend to have fewer protections, hold money and customer data, and can be fooled by a convincing email. The cost of an incident includes lost money, lost time and lost trust, and for many small firms, recovery is hard. The good news is that a handful of simple steps prevents most problems.

Back up what matters

- **Know what you must not lose:** accounting records, customer and supplier details, contracts, designs and the documents you need to run the business.
- **Follow the three-two-one habit:** three copies, on two different kinds of storage, with one copy kept off-site or in the cloud.
- **Automate it.** Backups that depend on remembering do not happen.
- **Test it.** Restore a file occasionally. A backup you have never tested may not work.
- **Protect the backups,** so that malware cannot also encrypt them.

Passwords and sign-in

- **Use a password manager,** so every account has a long, unique password you do not have to remember.
- **Turn on two-step verification** wherever it is offered, especially for email, banking, accounting software and cloud storage.
- **Give each person their own login,** not a shared one, and remove access the day someone leaves.
- **Limit access.** People should see only what they need.

Keep software up to date

Updates fix security weaknesses. Turn on automatic updates for computers, phones, browsers and business software, and replace equipment that no longer receives them.

Who this is for

- Owners who store records on one laptop
- Businesses that hold customer data
- Anyone who has had a suspicious email

Key points

- Back up automatically, and test the backup.
- Use a password manager and two-step sign-in.
- Check before you pay, especially if bank details change.
- Train everyone to spot phishing.
- Know who to call if something goes wrong.

Phishing and payment fraud

Most attacks start with an email, text or call that looks genuine. Typical examples are a supplier who “has changed bank details”, a message from “the boss” asking for an urgent payment, a delivery notice, or a request from the “bank” to confirm a login.

- **Stop and check.** Verify any change of bank details or urgent payment request by calling a number you already hold, not one in the message.
- **Be wary of links and attachments** you did not expect.
- **Use a second approval** for payments above a set amount.
- **Tell your team** about common scams, and make it safe to report a mistake quickly.

Five quick wins

- Turn on two-step sign-in
- Install a password manager
- Automate your backups
- Update everything
- Check before paying

Look after personal data

If you hold personal data about customers or staff, you have legal duties to keep it secure, use it lawfully and tell people how you use it. Keep only what you need, store it securely, and know how you would respond if it were lost. Some breaches must be reported to the regulator within a short time, so decide in advance who will deal with it.

Insurance and certification

Cyber insurance can cover the costs of an incident, from specialist help to lost income, but insurers expect basic protections to be in place. A government-backed scheme called Cyber Essentials sets out the basic controls and is increasingly asked for by larger customers.

A short response plan

Write down, on one page: who to call, how to isolate affected equipment, how to contact your bank, where the backups are, and who tells customers. Keep a printed copy.

Review once a year

Check that backups work, who has access to what, that old accounts are closed, and that software is current. Make it a habit, not a project.

Related guides

If this is useful, you may also want:

- Essential business tools
- Maintaining records
- Outgrowing your systems

How King Street can help

0161 835 2080
client@mtmlp.co.uk

We help you protect your financial records: secure access to your accounting software, safe sharing of documents, and checks on bank details and payment approvals. For wider technology and data protection advice, we can introduce specialists we trust.

Manchester: 3rd Floor, 82 King Street, M2 4WQ · Wilmslow: Cresta House, 42 Water Lane, SK9 5AL