

Vision Tech

Small business IT Handbook

18 free step-by-step guides in plain English

Free to print and share.

guides.visiontech336.com - admin@visiontech336.com

Contents

Backups & recovery

The 3-2-1 backup rule for a small business	3
What to do after a suspected breach in a small business	4
What to do when a work laptop is lost or stolen	5
Disaster recovery on one page	6

Staff, passwords & access

Sharing files safely: OneDrive, SharePoint and Google Drive basics	8
IT checklist for a new starter and a leaver	10
Who should have admin rights on business computers?	11
A password policy that actually works	12
Phishing training for staff in 10 minutes	13

Security & compliance

Keeping software up to date across several PCs	14
Cyber Essentials in plain English	16
Do I need to register with the ICO? How to check	17
Encrypting laptop drives with BitLocker or FileVault	18
Protecting shop or office Wi-Fi and separating card terminals	20

Email, equipment & suppliers

Setting up business email on your own domain	21
How to choose a good IT support provider	22
A simple IT equipment register and replacement cycle	23
Domain names and renewals: do not lose your domain	25

Small business IT | Easy | 2 min read

The 3-2-1 backup rule for a small business

Losing your customer records, invoices or photos can stop a small business overnight. The **3-2-1 rule** is a simple way to make sure that never happens.

What 3-2-1 means

- **3** copies of your important data: the original plus two backups.
- **2** different types of storage, for example your computer and an external drive, or a drive and a cloud service.
- **1** copy kept away from your premises, so a fire, flood or theft cannot take everything.

A newer version, 3-2-1-1, adds one copy that cannot be changed or deleted (an "immutable" copy), which helps against ransomware.

What to back up

1. List the things you could not do without: accounts files, customer lists, contracts, photos, email.
2. Note where each lives: a laptop, a shared drive, a cloud app.
3. Remember that cloud apps such as Microsoft 365 or Google Workspace are not automatically a full backup. If a file is deleted or encrypted by ransomware, it can be gone for good after a short time.

A practical set-up

- Copy one: your working files on the computer or shared drive.
- Copy two: an external drive that you plug in, back up to, then unplug and store safely. A drive left plugged in can be encrypted by ransomware along with everything else.
- Copy three: an automatic cloud backup service, ideally with several days or weeks of old versions kept.

Keep it working

- Set backups to run automatically, not from memory.
- Turn on email alerts if a backup fails.
- **Test a restore** every few months by recovering a few files. A backup you have never tested is only a hope.
- Encrypt backup drives and keep any recovery keys somewhere safe.

When to get more help

Ask for help if you are unsure what is and is not being backed up, if backups have been failing, if you hold sensitive customer data, or if you need to restore after a loss. We can set up and test a proper backup plan with you.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Small business IT | Medium | 2 min read

What to do after a suspected breach in a small business

Finding out that an account may have been taken over, or that data may have leaked, is stressful. Calm, quick steps limit the harm. This is general information, not legal advice.

First hour: contain it

1. **Tell the person in charge** straight away, and do not blame anyone. Speed matters more than fault.
2. Disconnect affected computers from the network and Wi-Fi. Do not switch them off yet if you suspect ransomware, unless advised.
3. Change passwords on affected accounts from a different, clean device, and turn on two-step sign-in.
4. Sign out of all sessions where the service allows it.
5. Contact your bank at once if money or payment details are involved.

Next: find out what happened

- Write down what you saw, when, and who noticed it.
- Note which accounts, devices and data might be affected.
- Keep emails and screenshots as evidence.
- Check for odd forwarding rules in email, which attackers often add.

Recover safely

- Restore from a **clean backup** taken before the problem, after the cause is removed.
- Update and scan all devices.
- Tell customers or suppliers if they might receive scam messages from your account.

Personal data and reporting

If personal data was lost, stolen or exposed, UK GDPR has rules. You must decide whether it must be reported to the **ICO**, and this generally has to be done within 72 hours of becoming aware of it, where it is a risk to people. Check the ICO's website, which has a self-assessment and a reporting line. You can also report cyber crime through Action Fraud (in England, Wales and Northern Ireland) or Police Scotland.

Afterwards

Keep a record of what happened and what you changed, and review how it got in.

When to get more help

Call for help early if you suspect ransomware, large data loss, fraud against your bank, or if you cannot tell how far the problem has spread.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Small business IT | Easy | 2 min read

What to do when a work laptop is lost or stolen

It happens to many businesses. Acting quickly protects your data and your customers. This is general information, not legal advice.

Straight away

1. **Tell the person in charge**, and make a note of when and where it was lost.
2. If stolen, **report it to the police** and get a crime reference number, which is useful for insurance.
3. From another device, change the password of the account used on the laptop, including email, and the password manager.
4. **Sign out all sessions** and remove the device from your cloud accounts, for example in Microsoft 365 or Google account settings.
5. Use "Find my device" for Windows or Mac to locate, lock, or wipe it, if you set it up beforehand.
6. Contact your IT provider if you have one.

Think about what was on it

- Was the drive **encrypted** with BitLocker or FileVault? If so, risk is much lower.
- Was there customer or staff data stored on it?
- Were passwords saved in the browser, or was the laptop signed in to payment or banking systems?
- Were files stored only on the laptop? Restore them from your backup.

Personal data

If personal data may have been exposed, consider whether you must report it to the ICO. Under UK GDPR this is usually within 72 hours of becoming aware, if there is a risk to individuals. The ICO website has guidance and a self-assessment. Tell affected people if there is a high risk to them.

Afterwards

- Update your equipment register.
- Replace the device and set it up with encryption and a screen lock.
- Tell your insurer, and check your policy for cover.
- Review how it happened and how to prevent it.

When to get more help

Get help if the laptop held unencrypted customer data, if it was signed in to banking or payment tools, or if you do not know what was on it.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Small business IT | Medium | 1 min read

Disaster recovery on one page

A **disaster recovery plan** says what you will do if IT stops working: fire, flood, theft, ransomware or a failed system. It does not need to be long. One clear page is far better than none.

What to put on the page

1. Contacts

- Who makes decisions, and their phone numbers.
- Your IT provider, broadband provider, bank, insurer and software suppliers.
- Keep a printed copy, since you may not be able to reach files on screen.

2. Your critical systems

List the three to five things you must get back first, such as email, accounts software, customer records, phones and the website. Give each an **order** and a rough time you could manage without it.

3. Where the backups are

- What is backed up, how often, and where.
- Who can restore it, and where the passwords and recovery keys are kept safely.

4. Where you will work

- Can people work from home, a laptop, or a temporary space?
- Do you have a spare laptop, and a way to take payments?

5. How you will tell people

- Staff, customers and suppliers: who tells them and how.
- A prepared message helps.

First steps in an emergency

1. Make sure people are safe.
2. Stop the problem spreading by disconnecting affected devices.
3. Call the right contact from the page.
4. Write down what happens and when.

Keep it alive

- Review the page twice a year.
- **Test restoring** a backup.
- Update it when staff or systems change.

When to get more help

Ask for help if you do not know how long a restore would take, if your backups have never been tested, if you depend on one person who knows everything, or if you want to practise a drill.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Small business IT | Medium | 2 min read

Sharing files safely: OneDrive, SharePoint and Google Drive basics

Cloud storage makes teamwork easy, but one wrong sharing setting can expose customer files to the world. These basics apply to OneDrive, SharePoint and Google Drive.

Know the difference

- **Personal storage** (such as OneDrive) is for one person's files. If they leave, access can be awkward.
- **Shared storage** (SharePoint sites, Teams, or Google shared drives) belongs to the business, not an individual. Put anything the business depends on here.

Set it up sensibly

1. Create shared folders by purpose, for example Finance, Customers, Staff.
2. Give access to **groups or named people**, not "everyone".
3. Use **view only** unless someone really needs to edit.
4. Name the owner of each area, so someone is responsible.

Be careful with links

Sharing links are convenient but risky. The choices usually include:

- **Anyone with the link**: anybody who gets the link can open the file. Avoid for anything private.
- **People in your organisation**: safer for internal files.
- **Specific people**: safest for sensitive material.

Where possible, set an expiry date on links and remove them when the job is finished.

Regular tidy-up

- Every few months, review who can see each shared folder.
- Remove access when people leave or change role.
- Check what is shared with outsiders, such as former contractors.
- Turn on two-step sign-in for every account.

Do not forget backup

Cloud sharing is not a backup. Deleted or overwritten files can be lost, and ransomware can sync encrypted files to the cloud. Keep a separate backup.

When to get more help

Get help if you have personal data about customers or staff stored in shared folders, if you are unsure who can see what, if files have been shared by mistake, or if you are moving from one system to another. We can review permissions and set up a clean structure.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Small business IT | Easy | 2 min read

IT checklist for a new starter and a leaver

People joining and leaving are the moments when IT mistakes happen. A short checklist keeps your business tidy and secure.

Before a new starter arrives

1. Create their **own named accounts** for email and any systems. Never share logins.
2. Give them access only to what their job needs.
3. Set up two-step sign-in on every account.
4. Prepare their computer: updates installed, security software on, drive encrypted, standard (non-admin) user account.
5. Decide who is the person they ask if something goes wrong.

On day one

- Show them how to use a password manager.
- Spend ten minutes on spotting scam emails and what to do if they click something.
- Explain how to save files in the shared area and not only on their desktop.
- Have them read your simple rules on personal devices, USB sticks and Wi-Fi.
- Record the equipment you handed over in your equipment list.

When someone leaves

1. Agree the date and time access will end, and do it on time.
2. **Disable the accounts** rather than deleting straight away, so you can retrieve their mail and files.
3. Change shared passwords they knew, such as the Wi-Fi or social media logins.
4. Remove them from shared folders, mailing lists, cloud tools and payment or banking systems.
5. Collect laptops, phones, keys, cards and tokens.
6. Move their files and email to a colleague, and set an out-of-office or forward for a time.
7. Remove business accounts from any personal phone they used.

Keep a record

Write down the date each step was done. A one-page form, filled in each time, is enough.

When to get more help

Ask for help if you are not sure which systems a person had access to, if someone leaves on bad terms, if you suspect they took data, or if you have no list of your accounts. We can help you build the checklist and tidy access.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Small business IT | Medium | 2 min read

Who should have admin rights on business computers?

An **administrator** account can install software and change almost any setting. That power is also what malware wants. Fewer admins means fewer ways in.

Why it matters

If someone with admin rights clicks a bad link or opens a dodgy attachment, a virus can install itself fully and take over the computer. If they are a **standard user**, the damage is often limited. Limiting admin rights is also part of Cyber Essentials.

A simple rule

- Everyday work should be done on a **standard account**.
- Admin rights are for the person or provider who looks after IT, used only when needed.
- Business owners are often the worst offenders. Being the boss does not mean you need admin for emails and spreadsheets.

How to put it into practice

1. List everyone who has admin rights on each computer and cloud service, such as Microsoft 365, Google Workspace, your website, and your domain name.
2. Ask of each person: do they need this to do their job every day? If not, change them to standard.
3. Create a **separate admin account** for admin tasks, with a strong, unique password and two-step sign-in. Do not use it for email or browsing.
4. Make sure at least two trusted people can reach the main admin accounts, so you are never locked out.
5. Store admin details safely, for example in a password manager or a sealed note in a safe.

Things to watch

- Staff may ask for admin so they can install a program. Create a simple request process instead.
- Remove admin rights when people leave or change role.
- Review the list a couple of times a year.

When to get more help

Get help if you do not know who the admins are, if software will not run without admin rights, if you have shared admin passwords, or if you need to move people to standard accounts without breaking their work.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Small business IT | Easy | 2 min read

A password policy that actually works

Strict password rules that nobody can follow lead to sticky notes and reused passwords. A better policy is short, realistic and backed by tools.

The core of a good policy

- Everyone uses a **password manager** to create and store passwords.
- Every account has a **different** password. Reuse is how one leak becomes ten.
- **Two-step sign-in** is switched on for email, banking, accounting software, cloud storage and anything holding customer data.
- Long passwords beat complicated ones. Three random words strung together is easier to remember and harder to guess than a short mix of symbols. The NCSC recommends this approach.

What to stop doing

- Forcing staff to change passwords every month. Change a password when there is a reason, such as a suspected leak.
- Sharing one login between several people.
- Writing passwords on notes stuck to screens.
- Using personal details such as pet names or birthdays.

Putting it in place

1. Choose one business password manager and set it up for everyone.
2. Have each person create a strong master password, and keep it to themselves.
3. Turn on two-step sign-in, using an authenticator app where possible rather than text messages.
4. For tools that must be shared, use the manager's sharing feature so you can remove access later.
5. Write your policy on one page and go through it with new starters.

If something goes wrong

Tell staff to report suspected problems straight away, and make sure nobody is blamed for reporting. Change the password on the affected account and any account that used the same one.

When to get more help

Ask for help if you want to choose a manager for the team, if accounts have already been taken over, if some systems do not support two-step sign-in, or if you need to clean up lots of old shared logins.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Small business IT | Easy | 2 min read

Phishing training for staff in 10 minutes

Most small business attacks begin with a message that tricks someone into clicking, paying or sharing a password. Ten minutes of regular, friendly training makes a real difference.

Minute 1 to 3: what phishing looks like

Phishing is a fake email, text, call or message designed to steal money, logins or data. Common disguises are the bank, HMRC, couriers, Microsoft, and, most dangerous of all, your boss or a supplier.

Minute 4 to 6: the warning signs

- It creates **urgency** or fear: "pay today", "account suspended".
- It asks for **passwords, codes or bank details**.
- A **change of bank details** for a supplier, or a request to buy gift cards.
- The sender's address is slightly wrong, or does not match the name.
- Links go somewhere unexpected. On a computer, hover over a link without clicking to see where it goes.
- Unexpected attachments, especially zip files and invoices.

Minute 7 to 9: what to do

1. **Stop and do not click.**
2. Check by another route, such as phoning a known number, not one in the message.
3. Report it to the person in charge, and use your email's Report phishing button.
4. If you did click or type a password, tell someone at once and change that password. Reporting quickly saves the day.

Minute 10: agree your rules

- Money and bank detail changes always need a second person to confirm by phone.
- Nobody gets in trouble for reporting a mistake.

Keep it going

Repeat a short refresher every few months, share real examples you receive, and consider the NCSC's free guidance for staff. Two-step sign-in means a stolen password alone is far less useful.

When to get more help

Ask for help if money has been sent to a scammer, if someone entered a password on a fake page, or if you would like a tailored session for your team.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Small business IT | Medium | 2 min read

Keeping software up to date across several PCs

Updates fix security holes that criminals actively use. With one computer it is easy to keep up. With five, it is easy to miss one.

Why it matters

Out-of-date software is one of the most common ways attackers get in. Cyber Essentials expects security updates to be applied promptly, generally within 14 days for those rated high or critical.

Step 1: know what you have

List every computer, phone and tablet, plus what runs on it: Windows or macOS version, browsers, Office, PDF readers, and so on. Also include the router and any other network devices, since they need updates too.

Step 2: turn on automatic updates

1. Windows: Settings, then Windows Update. Make sure updates are on and set active hours so restarts happen outside work.
2. macOS: System Settings, General, Software Update, and turn on automatic updates.
3. Browsers and apps such as Chrome, Edge and Office: leave automatic updates on.
4. Phones and tablets: turn on automatic updates in settings.

Step 3: check regularly

- Once a month, spend 15 minutes looking at each machine to confirm updates are installed and nothing is waiting for a restart.
- Ask staff to restart at least weekly. Many updates only finish after a restart.
- Keep a simple sheet noting date checked and by whom.

Deal with old software

- Check which version of Windows each PC runs. If a system no longer receives security updates, it should be upgraded or replaced.
- Remove programs nobody uses.
- Old printers and routers also stop getting updates, so plan to replace them.

When something breaks

Before large updates, make sure your backups are working. If an update causes a problem, do not turn updates off for good; ask for help instead.

When to get more help

Get help if you have more than a handful of machines, if some will not update, if you run old software for a special reason, or if you would like updates managed for you.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Small business IT | Medium | 2 min read

Cyber Essentials in plain English

Cyber Essentials is a UK government-backed scheme that helps organisations protect themselves against the most common internet attacks. It was developed with the National Cyber Security Centre (NCSC) and is delivered through licensed certification bodies.

What it covers

Cyber Essentials focuses on five basic technical controls:

- **Firewalls:** protecting your network and devices from the internet.
- **Secure configuration:** removing unneeded software and changing default settings and passwords.
- **User access control:** only giving people the accounts and permissions they need.
- **Malware protection:** using anti-malware software or other safeguards.
- **Security update management:** keeping devices and software up to date.

Two levels

- **Cyber Essentials:** you complete a self-assessment questionnaire, which is checked by a certification body.
- **Cyber Essentials Plus:** includes the same basics plus a hands-on technical check of your systems.

Why bother

- It reduces the risk of common attacks.
- Some customers, public sector contracts and insurers ask for it.
- It gives you a sensible checklist to follow even if you do not certify.

How to start

1. Check the NCSC website for the current requirements and find an accredited certification body.
2. List your devices, accounts and cloud services, since the scheme covers all of these.
3. Fix gaps: updates, admin rights, two-step sign-in, backups, and firewalls.
4. Complete the questionnaire honestly and keep copies of your evidence.
5. Renew every year.

Prices and details change, so check the current information with the NCSC or the certification body, who can give you a quote.

When to get more help

Ask for help if the questions are confusing, if you cannot tell whether a device or cloud service is in scope, or if you want to get the technical side ready before you apply. We can help you prepare, though the certificate itself is issued by a certification body.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Small business IT | Easy | 2 min read

Do I need to register with the ICO? How to check

The **Information Commissioner's Office (ICO)** regulates data protection in the UK. Many organisations that handle personal data must pay a data protection fee, which is often called registering. This is general information, not legal advice.

Who this affects

If you process personal information, such as customer names, addresses, staff records or photos of people, you probably need to pay the fee unless an exemption applies. Sole traders and limited companies are included. Some organisations are exempt, for example some not-for-profits, and some small organisations processing data only for limited purposes such as staff administration, advertising their own business, or accounts.

How to check

1. Search for the ICO's **data protection fee self-assessment**. It is a short online questionnaire on the official ICO website (ico.org.uk).
2. Answer honestly about your type of organisation and what you do with personal data.
3. It will tell you whether you need to pay and, if so, which tier applies. Do not rely on memory about amounts; use the ICO's own tool for current details.
4. Keep a screenshot or copy of the result.

If you do need to pay

- Pay through the ICO's official site only. Beware of copycat websites and unsolicited letters or calls asking for money.
- Set up a reminder for renewal each year.
- Keep your contact details up to date.

Paying the fee is not the same as being compliant

You still need to follow UK GDPR. That includes:

- Only collecting the data you need.
- Keeping it secure, with strong passwords, two-step sign-in, backups and encryption.
- Knowing what to do if there is a breach.
- Having a short privacy notice, if you collect data from customers.

When to get more help

Ask for help if you are unsure about the answers in the self-assessment, have received a letter from the ICO, or need to improve how you store personal data. For legal questions, consider a solicitor or the ICO's small business advice service.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Small business IT | Medium | 2 min read

Encrypting laptop drives with BitLocker or FileVault

If a laptop is lost or stolen, **encryption** stops a thief from reading the files on it. It is one of the simplest ways to protect customer and business data.

What these tools are

- **BitLocker** is Microsoft's drive encryption for Windows. It is available on Pro and higher editions, and some PCs use a simpler version called device encryption.
- **FileVault** is Apple's built-in drive encryption on Mac.

Before you start

- Make a **current backup**.
- Plug the laptop into power.
- Make sure you can sign in as the account owner or administrator.

Turn it on

Windows:

1. Open Settings, then Privacy and security, then Device encryption, or search for Manage BitLocker.
2. Follow the prompts to turn it on.
3. When asked how to back up the **recovery key**, choose your Microsoft account, work account or a printed copy, and keep it safe.

Mac:

1. Open System Settings, then Privacy and Security, then FileVault.
2. Turn it on and choose how to unlock your disk if you forget your password.
3. Store the recovery key safely, or use your iCloud account.

Warnings about recovery keys

- **Without the recovery key, you may never get your data back.** Store it somewhere other than the laptop.
- Do not save it only on the encrypted drive itself.
- Record which key belongs to which device. A password manager or secure shared admin folder works well.
- Windows may ask for the key after hardware or update changes, so make sure someone can find it.

Also remember

Encryption protects a switched-off or locked device. You still need a strong sign-in password, a screen lock, and updates.

When to get more help

Get help if the option is missing, if you are managing many laptops, if you are asked for a recovery key you cannot find, or before encrypting an older computer.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Small business IT | Medium | 2 min read

Protecting shop or office Wi-Fi and separating card terminals

A weak business Wi-Fi network can give attackers a way to reach your computers and customer data. Separating your card payment equipment adds another layer. This is general guidance; always follow your payment provider's instructions.

Secure the Wi-Fi

1. Change the router's **admin password** from the default, and make it long and unique.
2. Use **WPA2 or WPA3** security with a strong Wi-Fi password. Never leave it open.
3. Change the Wi-Fi password when staff leave.
4. Keep the router's software up to date, and replace routers that no longer receive updates.
5. Turn off features you do not use, such as remote administration, and WPS.

Give visitors their own network

Create a **guest Wi-Fi** that is separate from your business network. Customers and visitors can get online without reaching your till, files or printers. Most business routers offer this in a few clicks.

Separate the card terminals

- Card machines should not share a network with staff computers and guest devices. If they connect through your network, ask your payment provider how.
- Many terminals use their own mobile data connection or a dedicated line, which keeps them apart.
- If they must use your network, use a **separate network or VLAN** if your equipment supports it.
- Do not use the card terminal's network for general browsing or tills with weak security.
- Keep the terminal in sight, check for tampering, and know your supplier's contact details.

Other good habits

- Position the router out of customers' reach.
- Keep a list of devices connected to your network and remove those you do not know.
- Put smart devices and cameras on their own network if you can.

When to get more help

Get help if your router is old, if you are not sure how to create separate networks, if you accept card payments and are asked to complete a payment security form, or if you see unknown devices on your network.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Small business IT | Medium | 2 min read

Setting up business email on your own domain

Email such as you@yourbusiness.co.uk looks more professional than a free address, and you control it. Setting it up involves a few technical pieces. Here is what they mean in plain words.

What you need

- A **domain name** that you own.
- An **email provider**, for example Microsoft 365 or Google Workspace, or the mail service from your host.
- Access to your domain's **DNS settings**, which are like a directory telling the internet where to send things for your domain.

The main DNS records, very simply

- **MX record** tells the world which mail service receives your email. Without the right MX records, email will not arrive.
- **SPF** is a list of the services allowed to send email for your domain. It helps stop others pretending to be you.
- **DKIM** adds a digital signature to your outgoing mail so receivers can see it was not changed and really came from you.
- **DMARC** tells receivers what to do if SPF or DKIM checks fail, and can send you reports.

Steps

1. Choose your provider and add your domain in their admin area.
2. The provider will show you the records to add.
3. Log in to wherever your DNS is managed, which is usually your domain registrar or web host.
4. Add the records exactly as shown, then wait. Changes can take from minutes to a day.
5. Send test emails both ways, and to a different provider, to check nothing lands in spam.
6. Turn on two-step sign-in for all mailboxes.

Take care

- Before changing MX records, write down the existing ones in case you need to go back.
- Do not delete records unless you know what they do, since your website may depend on them.
- Move old email across before switching.

When to get more help

Get help if mail stops arriving, goes to spam, if you are moving from an existing system, or if you are not sure who controls your DNS. A mistake here can interrupt your business email.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Small business IT | Easy | 2 min read

How to choose a good IT support provider

Good IT support saves time and prevents disasters. A poor one leaves you exposed. These questions help you tell the difference.

Before you ask

Write down what you have: number of staff, computers, key software, and the things that would hurt most if they stopped working. Also decide whether you want help only when something breaks, or regular looking-after for a monthly fee.

Questions to ask

1. **What is included?** Ask for a clear list of services and what costs extra.
2. **How quickly will you respond**, and what are your hours? What happens out of hours?
3. **Who will I deal with?** Is it one person or a rota? Can I speak to someone on the phone?
4. **How do you keep my data safe?** Ask about their own security, two-step sign-in and how they handle your passwords.
5. **Do you handle backups, and will you test restores?**
6. **Do you document my set-up**, and will I own that document?
7. **Who holds the admin passwords?** You should always be able to get them.
8. **What is the notice period** and can I leave without being tied in?
9. **Can you give me references** from similar small businesses?
10. **Do you have insurance**, and will you sign a data protection agreement if they handle personal data?

Warning signs

- Pressure to sign quickly.
- Jargon with no clear answers.
- Refusing to share admin details or documents.
- No written agreement.
- Promising to fix everything for a very low price.

After you choose

Start with a trial period or small job if possible. Agree what a good job looks like, and ask for a short review every few months. Certifications such as Cyber Essentials can be a helpful sign, but they are not a guarantee.

When to get more help

If you are unsure about a quote or contract, or want a second opinion on your current provider, ask a trusted adviser or us to take a look.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Small business IT | Easy | 2 min read

A simple IT equipment register and replacement cycle

You cannot protect what you do not know you have. A simple list of equipment helps with security, insurance and budgeting.

What to record

A spreadsheet is enough. For each item, note:

- What it is, such as laptop, phone, router or printer.
- Make, model and **serial number**.
- Who uses it, and where it is kept.
- Date bought, price, and warranty end date.
- Operating system version, and whether the drive is encrypted.
- Date of the last check.

Include phones, tablets, routers, printers, card machines, external drives and anything else that connects. Add a second sheet for software and cloud services with renewal dates and the person responsible.

Keep it up to date

1. Add new items when they arrive.
2. Record when equipment is handed to a new person.
3. Mark items as retired, with the date and what happened to the data.
4. Review the list once or twice a year.

A replacement cycle

Most business laptops and desktops give around four to five years of useful service, though this varies. Plan for it:

- Look at the age of each item every year.
- Replace machines that are slow, failing, or no longer receive security updates.
- Spread purchases so you are not buying everything at once.
- Put money aside each month.
- Keep a spare charger or two, and consider one spare laptop.

When equipment is retired

- Back up anything needed, then **securely wipe** the drive. Deleting files or a normal reset may not be enough.
- Use a reputable recycler who provides a certificate for WEEE disposal.
- Remove it from your list and from any accounts it was signed in to.

When to get more help

Ask for help if you are not sure what is on your network, if you need to wipe data safely, or if you want help planning a replacement budget.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.

Small business IT | Easy | 2 min read

Domain names and renewals: do not lose your domain

Your **domain name** is your web and email address. If it expires or somebody else controls it, your website and email could stop working, and you may even lose the name for good.

Know who owns it

- The **registrant** is the legal owner. Make sure this is your business, not a web designer or ex-employee.
- The account is held with a **registrar**, which is the company you buy the domain from. Find out who this is and who can log in.
- Check the details with a **WHOIS** search for your domain, although some details may be hidden for privacy.

Protect the account

1. Use a **unique, strong password** and turn on two-step sign-in.
2. Use a business email address that more than one trusted person can read, not a personal one.
3. Record the login in your password manager or other secure place.
4. Turn on a **registrar lock** if offered, to prevent unauthorised transfers.

Do not miss renewals

- Turn on **auto-renew**, and make sure the payment card on file is valid and not about to expire.
- Note the renewal date in your calendar well ahead.
- Watch for reminder emails, but beware of fake renewal invoices from unknown companies. Only pay via your own registrar account.
- Consider renewing for several years at a time.

If you have already let it lapse

Contact your registrar quickly. There is often a short grace period when you can still renew, sometimes for a higher fee.

Keep a record

Write down:

- Domain names you own and where each is registered.
- Expiry dates.
- Who handles DNS, website and email for each.

When to get more help

Get help if you do not know where your domain is registered, if someone else holds the account, if you have received a suspicious transfer or renewal message, or if your site or email stopped working suddenly.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.