FIELD GUIDE · 2026 EDITION · LAST CHECKED 28 AUGUST 2026

Cyber security that a small business can actually keep up with

A practical UK guide for small offices, growing companies and home users. What changed in 2026, what matters most, and the exact order to do it in. Written by the engineers at Verge Tech Solutions.

43% of UK businesses had a breach or attack in the last 12 months	**~612k** UK businesses affected over the year	**28%** of UK charities hit in the same period
#1 Phishing is still the most common way in		

IF YOU ONLY DO FIVE THINGS

1 **Turn on multi-factor sign-in, or passkeys, for every email and cloud account.**

Email is the

master key to everything else.

2 Put a password manager in place

so every account has its own long password and nobody reuses one.

3 Let devices update themselves.

Operating system, browser, apps and your router. Most attacks use a hole that a patch already fixed.

4 Get one backup you can restore from

that an attacker cannot reach or encrypt, and test a restore.

5 **Agree a rule that no payment or bank detail changes on the strength of an email alone.**

Always confirm by phone on a known number.

01

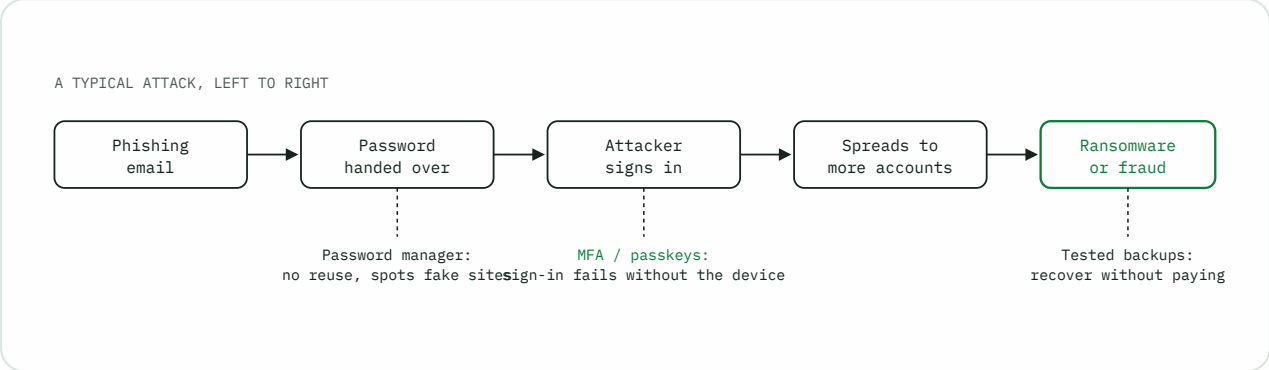
Where the risk is now

Cyber crime is a daily reality for ordinary businesses and households, not a problem only large companies have.

> **The short version:** most attacks are not clever. Someone is tricked into handing over a password or clicking a link, the attacker signs in, and the damage follows. The controls in this guide are aimed squarely at breaking that chain.

The UK government's Cyber Security Breaches Survey 2025/2026 found that 43% of UK businesses and 28% of charities had a breach or attack in the previous 12 months, which works out at roughly 612,000 businesses. The National Cyber Security Centre (NCSC) is consistent that smaller organisations are targeted often, usually by automated attacks that do not care how big you are.

Phishing is still the most common route in. What has changed is speed and polish. Attackers now use AI to write convincing messages, clone voices, and find weak spots faster, so "it looked wrong" is a less reliable defence than it was.



Most incidents follow this path. Each control below the line breaks a **different** link, which is why layering them matters more than perfecting any single one.

02

What changed in 2026

Four updates worth knowing about, with dates so you can check them yourself.

Cyber Essentials technical baseline updated to v3.3

The NCSC's Requirements for IT Infrastructure v3.3 (April 2026) adds a few clarifications:

- Passwordless authentication now formally includes FIDO2 security keys and passkeys.
- Eligible cloud services cannot be left out of scope. If your data lives there, it counts.
- Patching timelines and the importance of backups are stated more firmly.

IASME, the body that runs Cyber Essentials, has confirmed the current question set (named "Danzell") applies to assessment accounts created from 27 April 2026. Earlier assessments continue under the previous v3.2 "Willow" set.

NCSC now recommends passkeys as the first choice

In April 2026 the NCSC said plainly that people should choose passkeys where a service supports them, and fall back to a password manager plus two-step verification where they do not. A passkey cannot be phished, because there is no code to read out or type into a fake page.

The regulator has raised the alarm on AI-assisted attacks

The Information Commissioner's Office (ICO) guidance from May 2026 highlights AI-enhanced phishing, deepfake social engineering and faster exploitation of weaknesses. The ICO is clear this is a present duty under UK GDPR Article 32, not a future one. If you hold personal data, your security measures are expected to account for AI-driven risk now.

Smart devices sold in the UK must meet a security baseline

Since 29 April 2024 the Product Security regime has required consumer connected products to ship without universal default passwords and to state how long they will get security updates. Check that support window before you buy.

03

Know your risk profile

The controls are similar across all three groups. The order of priority is not.

Filled dot = high exposure, **ring** = worth planning for, faint dot = lower. Green marks the risks that grow sharply once you have staff and shared systems.

Small office and home office

Little or no dedicated IT help, heavy reliance on cloud email and file sharing, and one compromised account can stop the business. The classic hits are phishing, reused passwords across web apps, unpatched laptops and routers, and fake supplier invoices.

Businesses with staff

A mix of cloud and on-site systems, several teams, and a larger amount of personal data. The added risks are a stolen login being used to move between systems, ransomware through remote access, misconfigured cloud settings, and problems arriving through a supplier.

Home users

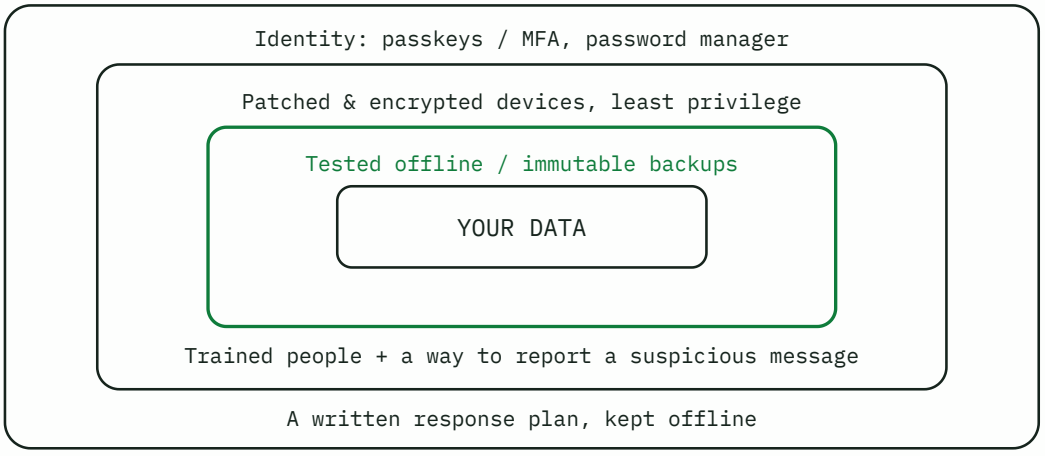
Many online accounts, mostly used from a phone, plus shared family devices and smart-home kit. The main risks are reused passwords being tried automatically, scam calls and

texts, and takeover of a main email account, which is the recovery route for everything else.

04

The baseline everyone needs

Nine controls that apply whether you are one person or fifty. The rest of the guide is detail on top of these.



Each layer buys time and limits damage when the one outside it fails. **Backups are the layer that still works** even if an attacker gets all the way in, which is why they have to be genuinely out of reach.

CONTROL	WHAT GOOD LOOKS LIKE
Phishing-resistant sign-in	Passkeys or FIDO2 keys where supported. Multi-factor or two-step verification on every important account otherwise.
Password hygiene	A password manager, a unique password per service, and no shared logins where you can avoid them.
Patching discipline	Automatic updates on for operating systems, browsers, apps and firmware. High-risk fixes applied quickly.
Endpoint hardening	Disk encryption on, modern antivirus or endpoint protection, no everyday admin rights, screen lock enforced.
Tested backups	At least one copy an attacker cannot reach or encrypt. Restores tested on a schedule, not just assumed.
Least privilege	People get only the access they need. Admin rights are time-limited and reviewed.

CONTROL	WHAT GOOD LOOKS LIKE
Secure cloud settings	Sign-in enforcement, conditional access, sharing limits and logging all checked in your Microsoft 365 or Google Workspace tenant.
An anti-phishing process	A one-click way to report a suspicious email, mailbox protection turned on, and the odd practice run.
Response readiness	Named contacts, agreed priorities and first-hour actions, with a printed copy kept offline.

Our Cyber Essentials checklist maps these onto the certification if you plan to get certified.

05

SMALL OFFICE & HOME OFFICE

If you run a small or one-person business

Sole traders, micro businesses and partnerships. Keep the setup simple, and keep it locked down.

> **Target setup:** a cloud productivity suite, a cloud backup with version history, managed security on every work device, a password manager, and a firm rule that payments need a second check.

Minimum standard

Accounts

- Multi-factor or two-step verification on every cloud account and on email. Passkeys where available.
- No shared inbox passwords. If a shared mailbox is needed, use proper delegated access.

Devices

- Automatic updates on. Full-disk encryption on. No admin rights on the account you use day to day.

Data

- Cloud backup of important files with version recovery. A monthly test restore of a few real files.
- Keep finance, legal, HR and customer data separated rather than in one shared folder.

Payments

- No bank detail changes on an email alone. Confirm any supplier change by phone on a number you already had. Two people approve high-value transfers.

Keeping going

- A one-page response checklist, printed and kept offline. Primary and backup contacts for IT help.

A 14-day quick start

DAYS 1–2

List every account, device and cloud service. Turn on multi-factor everywhere. Reset weak or reused passwords in the password manager.

DAYS 3–5

Force automatic updates on all devices. Turn on endpoint and ransomware protection. Review sharing and public links in your cloud apps.

DAYS 6–8

Set backup policies and retention. Restore three real files and one full device image. Write down how long it took and what got in the way.

DAYS 9–11

Write your invoice-fraud and phishing procedure. Train everyone on the payment verification rule.

DAYS 12–14

Talk through a "phishing leads to account takeover" scenario out loud. Note the gaps and fix them.

Track these each month

- Share of accounts with multi-factor or a passkey.
- Share of devices fully patched.
- Whether the last restore test worked, and how long it took.
- Number of suspicious emails reported.
- Open high-severity issues, and how old they are.

06

BUSINESSES WITH STAFF

If you have employees and IT systems

More people, more accounts and more personal data means the plan needs owners, a routine, and detection, not just controls.

Who owns what

ROLE	OWNS
Senior leadership	Cyber risk overall, how much risk is acceptable, and the budget.
IT or security lead	Putting controls in place, monitoring, and leading an incident.
Data protection lead	Personal-data safeguards, impact assessments, and breach reporting.
Team managers	Risk in their own process: finance, operations, HR, customer service.

Run a monthly risk review, a quarterly recovery test, and an annual strategic review with an outside check.

Technical baseline

Identity and access

- Multi-factor for all users, all admins and all remote access.
- Extra protection on privileged accounts. Joiner, mover and leaver changes handled promptly.

Network and devices

- Central endpoint protection policy. Separate network zones for staff, servers, management and guest or smart devices. Remote admin access restricted and watched.

Email

- SPF, DKIM and DMARC set up and monitored. Safe-link and attachment checks on. External sharing limited by how sensitive the data is.

Logging and detection

- Collect logs from sign-in, devices, email, firewall and cloud services in one place. Alert on impossible travel, mass downloads, privilege changes and suspicious app permissions. Keep logs long enough to investigate.

Vulnerabilities and backups

- An asset list with an owner for each item. A patch deadline based on risk. Regular authenticated scans.
- Recovery targets set per business service. Backup logins kept separate from normal logins. Restore drills for whole systems, not only files.

Incident response

Keep a short playbook for each of: phishing-led account compromise, ransomware, payment fraud, suspected data theft, and a supplier being compromised. Every playbook should name the trigger, the person in charge and their deputy, the first 60 minutes of containment, communication templates, and when to bring in legal and regulatory advice. NCSC guidance is clear that you should check your backups are clean before you restore from them.

A 90-day hardening plan

PHASE 1

See what you have. Confirm the asset list, the identity baseline (multi-factor, admins, dormant accounts) and whether you can actually recover from backup today.

PHASE 2

Cut the biggest risks. Clear the critical patch backlog, tighten remote access and least privilege, and strengthen the technical anti-phishing controls.

PHASE 3

Build resilience. Centralise the key logs, run a tabletop and a real recovery drill, and put a cyber readiness report in front of the board.

Compliance and assurance

- **Cyber Essentials and Cyber Essentials Plus.** A sensible baseline and a clear signal to customers. Check the scope carefully, including cloud services.
- **UK GDPR.** Apply security measures in proportion to the personal data you hold. Factor AI-related risk into impact assessments.

- **Suppliers.** Security clauses in contracts, due diligence on the higher-risk ones, and a minimum-control statement from anyone critical.

07

HOME USERS

If you want to protect your home

Families and individuals. Protect the email account first, then the devices, then the network.

Accounts

- Use passkeys where a service offers them. This is now the NCSC's preferred approach.
- Where passkeys are not available, use a password manager plus two-step verification.
- Lock down your main email account first. It is the reset route for everything else.
- Remove old recovery phone numbers, old recovery emails and devices you no longer recognise.

Devices

- Keep phones, tablets, laptops, smart TVs and games consoles updated. Turn on automatic updates.
- Use a screen lock or biometrics and turn on device encryption. Install apps only from the official stores.

Home Wi-Fi and router

- Change the router admin password straight away. Use WPA2 or WPA3 with a unique passphrase.
- Turn off remote management if you do not use it. Keep the firmware updated and replace a router that no longer gets updates.
- Put smart-home devices on a separate guest network where you can.

Smart devices

- Avoid devices that are close to the end of their update support.
- Turn on two-step verification in the companion app. Turn off remote access you do not need. Install updates promptly.

Family basics

- Teach the scam red flags: urgency, pressure to pay, secrecy, and odd links.

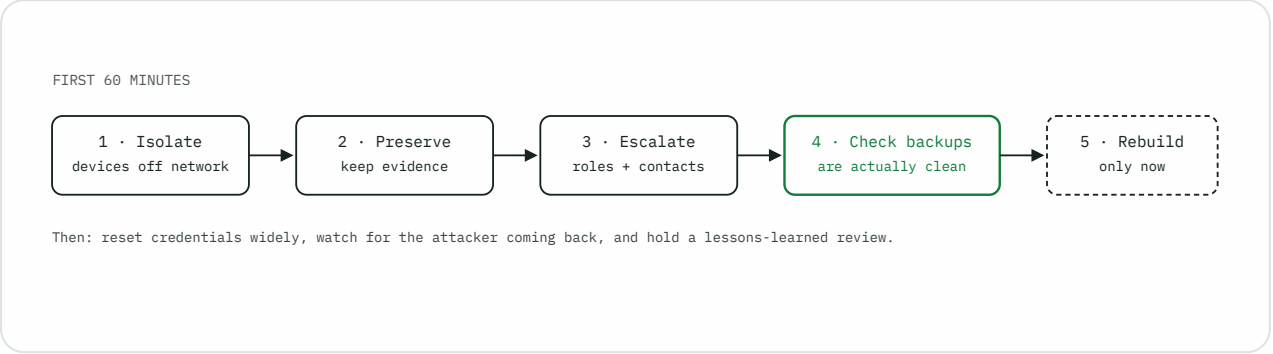
- Agree that any unexpected bank or "support" call gets ended and called back on a known number.
- Set parental controls on children's devices. Keep an offline copy of important family records and recovery details.

08

Ransomware and recovery

The one scenario worth rehearsing, because the first hour decides how bad it gets.

> **The rule that matters:** do not rush the restore. Rebuilding from a backup that is still infected, or before you understand how they got in, is how businesses get hit twice.



Steps 1 to 4 come before any restore. **Validating the backup is the checkpoint** that stops a second, worse incident.

Prevent

- Patch fast, especially anything facing the internet. Multi-factor on all remote access and admin accounts. Endpoint protection with script controls. Offline or immutable backups with a tested restore.

Recover

- Rebuild from trusted images. Reset passwords broadly, especially privileged ones. Watch for the attacker returning. Review what happened and improve the controls.

09

Plain-English glossary

The terms in this guide, without the jargon.

TERM	WHAT IT MEANS
Passkey	A sign-in method tied to your phone or laptop that replaces the password. It cannot be phished because there is no code to steal.
FIDO2	The open standard behind passkeys and physical security keys.
MFA / 2SV	Multi-factor authentication, or two-step verification. A second proof of identity on top of the password, such as an app prompt or a code.
Password manager	An app that creates and stores a unique strong password for every account, so you only remember one.
Endpoint protection / EDR	Security software on a device that blocks and reports attacks. EDR adds detection and investigation tools.
Immutable backup	A backup that cannot be changed or deleted for a set period, so ransomware cannot destroy it.
Cyber Essentials	A UK government-backed certification covering five basic security controls. Cyber Essentials Plus adds a hands-on technical check.
SPF, DKIM, DMARC	Email settings that prove a message really came from your domain and make it harder to impersonate you.
Least privilege	Giving each person and system only the access they need, and no more.
Lateral movement	An attacker using one compromised account or device to reach others inside the same organisation.
Business email compromise	Fraud where an attacker uses a real or spoofed email account to redirect a payment or invoice.

10

How often to review

EVERY	CHECK
Month	Patch status, account review, backup health.
Quarter	A phishing exercise, a restore test, a review of who has supplier access.
6 months	Refresh policies, run an incident drill, review the architecture.
Year	A strategic risk review, and re-certification if you hold Cyber Essentials.

11

How Verge Tech helps

We are a team of senior engineers based near Slough, working across London, Berkshire and Surrey. Verge Tech Solutions has run since 2018. Our engineers are Microsoft and CompTIA certified, and one named engineer owns your account from start to finish.

We can set up and run the controls in this guide for you

Most small businesses do not need a full-time IT person. They need this done once, properly, and then kept running. That is what a managed service is for.

Managed IT support
Patching, backups, security baselines and monitoring for a fixed monthly cost.

Cyber security
Multi-factor rollout, phishing protection, endpoint hardening and Cyber Essentials help.

Backup and recovery
Offline and immutable backups with restores that are actually tested.

Microsoft 365
Tenant hardening, secure sharing, and managed devices with Intune.

Free IT health check
A practical look at your devices, backup, accounts and obvious gaps.

Managed device guides
How device management works for Windows and for Mac in a small business.

020 3376 1140

12

Sources

Authoritative references, all UK-focused where possible. Checked 28 August 2026.

[1] UK Government — Cyber Security Breaches Survey 2025/2026

[2] NCSC — Cyber Essentials: Requirements for IT Infrastructure v3.3 (April 2026)

[3] IASME — Preview the Cyber Essentials self-assessment questions

[4] NCSC — Leave passwords in the past, passkeys are the future (April 2026)

[5] ICO — Five steps to protect your organisation from AI-powered cyber threats (May 2026)

[6] GOV.UK — The UK Product Security regime

[7] NCSC — Smart devices: using them safely in your home

[8] NCSC — What to do when cyber attacks disrupt your organisation

[9] NIST — Cybersecurity Framework 2.0 Small Business Quick-Start Guide

[10] CISA — Cyber Guidance for Small Businesses

13

A few notes

This is practical guidance, not legal advice. Your obligations depend on your sector and the data you hold. Review your controls whenever your business model, your suppliers or your critical systems change.

Verge Tech Solutions is a mobile IT support company. We provide computer repair, network support, cyber security and business IT support across London, Berkshire and Surrey.

Verge Tech Solutions
Cyber Security Field Guide · 2026 edition

vergetech.co.uk · 020 3376 1140
London · Berkshire · Surrey