BITWISE-IT BUSINESS TOOLKIT

# Cyber Security Checklist

Forty questions, one afternoon, an honest answer

**Bitwise-IT Limited**

Wickford, Essex · 01268 218301

info@bitwise-it.co.uk · bitwise-it.co.uk

## How to use this checklist

> Work through it honestly. The value is in the items you cannot tick — and almost every business finds two or three they assumed were handled and were not.

The controls below follow the five areas that **Cyber Essentials** is built around: firewalls, secure configuration, user access control, malware protection, and keeping software up to date. It is the UK government-backed scheme that most cyber insurers and an increasing number of larger clients now ask about, so working through this also tells you roughly how close you are to certifying.

Set aside an afternoon. Tick what is genuinely true today, not what is intended.

## 1. Accounts and access

- [ ] Multi-factor authentication is switched on for **every** user, not just the directors
- [ ] Nobody shares a login. Each person has their own account
- [ ] Administrator accounts are separate from everyday accounts, and admin rights are given only to those who need them
- [ ] Leavers are removed the day they leave — including their email, files and any shared services
- [ ] You know which third parties and apps have access to your systems, and can name them
- [ ] Default passwords have been changed on every device, including the router and any wireless access points

> **IF YOU TICK NOTHING ELSE, TICK THIS ONE**
>
> Multi-factor authentication on email prevents the large majority of account takeovers we see. Attackers rarely break in these days — they log in, using a password they bought. MFA turns a stolen password into a dead end. It is free, it is built into Microsoft 365, and it takes an afternoon to roll out.

## 2. Devices

- [ ] Every laptop and desktop encrypts its disk (BitLocker on Windows, FileVault on Mac)
- [ ] Screens lock automatically after a few minutes and need a password or PIN to get back in
- [ ] Reputable, actively updating security software runs on every machine
- [ ] Phones used for work email have a passcode and can be wiped remotely
- [ ] You have a written list of the devices in the business and who holds each one
- [ ] Personal devices used for work are covered by some form of agreement

## 3. Updates and patching

- [ ] Windows and macOS updates install automatically, and you can prove it rather than assume it
- [ ] Applications update too — browsers, Office, PDF readers, anything that opens files from outside
- [ ] Nothing in daily use is running an operating system that stopped receiving security updates
- [ ] Router and firewall firmware is current, and somebody is responsible for checking
- [ ] Somebody would notice if a machine quietly stopped updating three months ago

## 4. Email and web

- [ ] Spam and phishing filtering is in place beyond the bare default
- [ ] SPF, DKIM and DMARC records are configured on your domain, so criminals cannot easily send email that appears to come from you
- [ ] External emails are visibly marked as external
- [ ] Staff know to verify bank detail changes by phone, using a number they already had — never a number in the email
- [ ] Somebody has explained what a phishing email looks like, recently, to everyone
- [ ] There is an obvious, blame-free way for staff to report something suspicious

> **THE INVOICE FRAUD PATTERN**
> The most expensive incidents we see rarely involve clever technology. Someone reads a compromised mailbox for a fortnight, waits for a genuine invoice, and sends a polite follow-up with amended bank details. The email is real, the thread is real, the timing is perfect. The only reliable defence is a rule that bank detail changes are always verified by voice, on a number you already held.

## 5. Data and backup

- [ ] You could name, right now, the three most important sets of data in the business and where each lives
- [ ] A backup runs regularly and somebody checks that it succeeded
- [ ] At least one copy is kept off-site or offline, out of reach of ransomware
- [ ] Your Microsoft 365 data is backed up — Microsoft keeps the service running, not your content
- [ ] Somebody has actually restored a file from backup in the last three months
- [ ] Portable drives and USB sticks holding business data are encrypted

## 6. People

- [ ] Staff have had security awareness training in the last twelve months
- [ ] Everyone uses a password manager rather than a notebook, a spreadsheet, or the same password everywhere
- [ ] People know who to call, out of hours, if something goes badly wrong
- [ ] Somebody in the business owns IT security as a named responsibility, even if it is only part of their week
- [ ] New starters are told how things work here on day one, not in month three

## 7. If it goes wrong

- [ ] There is a written plan for what happens in the first hour of an incident
- [ ] Key contacts — IT support, bank, insurer, accountant — are recorded somewhere you could reach without your computers
- [ ] You know whether your insurance covers cyber incidents, and what it requires of you
- [ ] You know that a personal data breach may need reporting to the ICO within 72 hours
- [ ] You know that organisations under live attack can call **0300 123 2040** at any hour

## Scoring yourself

> Count the boxes you could honestly tick. There are around forty.

| Ticked | Where that puts you |
|---|---|
| **Under 15** | There is real exposure here, and it is worth acting on soon rather than eventually. The good news is that the first handful of fixes — MFA, backup, updates — remove most of the risk for very little money. |
| **15 to 25** | A reasonable foundation with visible gaps. This is where most small businesses sit. Pick the unticked items in sections 1 and 5 first; they carry the most weight. |
| **26 to 34** | Genuinely decent. The remaining gaps tend to be the unglamorous ones — monitoring, testing restores, offboarding — which are exactly the ones that catch people out. |
| **35 or more** | Better than the vast majority. Worth formalising: Cyber Essentials certification is probably within reach, and it is increasingly something clients and insurers ask to see. |

### The three that matter most

If the list feels long, start here. In our experience these three prevent more damage than everything else combined:

1. **Multi-factor authentication on every account.** Free, quick, and it stops the most common attack outright.
2. **A backup you have tested, with a copy out of reach.** This is what turns a ransomware attack from an extinction event into a bad week.
3. **Automatic updates you can prove are working.** Most successful attacks use a flaw that was fixed months ago.

> **A NOTE ON PROPORTION**
>
> None of this requires enterprise budgets. A five-person business can be genuinely well protected using tools it is probably already paying for — the difficulty is almost never the technology, it is that nobody owns the job. Deciding who owns it is often the single most useful thing you will do this year.

### Want a second opinion on your answers?

We will go through this with you, look at what is actually configured rather than what is intended, and give you a straight assessment of where the gaps are and what they would cost to close. It is a conversation, not a sales process, and there is no obligation attached.

**01268 218301** · info@bitwise-it.co.uk · bitwise-it.co.uk