BITWISE-IT BUSINESS TOOLKIT

Passwords and Multi-Factor Authentication

What actually works, and what stopped working years ago

Bitwise-IT Limited

Wickford, Essex · 01268 218301

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

Why the old advice was wrong

> For twenty years people were told to use short, complicated passwords and change them every ninety days. It turned out to be exactly backwards, and it is worth understanding why before changing anything.

Complicated passwords are hard for humans and easy for computers. `P@ssw0rd1!` satisfies every complexity rule ever written and is among the first things any attacker tries. Forced regular changes made it worse: people simply incremented a number on the end, and the password got weaker with each cycle rather than stronger.

Meanwhile the actual threat changed. Attackers rarely sit there guessing your password. They buy a list of millions of real passwords from an old breach and try them against your email, on the sound assumption that people reuse them. Complexity does nothing against that. **Uniqueness** does.

> **THE TWO RULES THAT MATTER**
>
> **1. Length beats complexity.** A long password takes vastly longer to crack than a short one, whatever symbols are sprinkled through it.
>
> **2. Never reuse a password.** One password on one site. When that site is breached — and eventually one will be — the damage stops there.

Making passwords you can live with

Three random words

The National Cyber Security Centre recommends building passwords from three random words. Something like `reef-cardigan-tuesday` is long, memorable, and far stronger than anything you would produce by mangling a word with symbols.

The important part is *random*. Words connected to you — your street, your dog, your team — are the first things a targeted attacker tries, and a surprising amount of that is on your own social media.

Where three random words is enough

For the handful of passwords you genuinely have to type from memory: your computer login, and the master password for your password manager. That is roughly it.

Everything else should be random

For every other account, you should not know the password at all. A password manager generates something long and meaningless, stores it, and fills it in for you. You are not supposed to remember it — that is the entire point.

> **STOP FORCING ROUTINE PASSWORD CHANGES**
>
> Current NCSC guidance is that regular forced expiry does more harm than good. Change a password when there is a reason: a suspected compromise, a breach notification, or someone leaving who knew it. Otherwise, leave good passwords alone.

Password managers

> This is the single change that makes everything else realistic. Without one, "a unique long password for every account" is advice nobody can actually follow.

What it does

- Generates a long random password for each account
- Stores them encrypted, behind one master password only you know
- Fills them in on your computer and phone, so signing in is quicker than it was before
- Tells you which of your passwords are weak, reused, or have turned up in a known breach

> **THE UNDERRATED BENEFIT**
>
> A password manager only offers to fill in a password on the site it belongs to. If you land on a convincing fake login page, it will quietly do nothing — and that silence is a better phishing detector than most people's judgement at half past four on a Friday.

Choosing one

- [ ] It is a reputable, established product — this is not the place to save ten pounds
- [ ] It works on the devices you actually use, including phones
- [ ] It supports multi-factor authentication on the account itself
- [ ] For a business: it supports shared vaults, so team passwords are not emailed around
- [ ] For a business: it lets you remove someone's access when they leave

Sharing passwords in a business

Some accounts genuinely have to be shared — the company social media, a supplier portal that allows only one login. Use your password manager's shared vault feature. Do not email them, do not put them in a spreadsheet on the shared drive, and do not write them on a card in the top drawer.

The practical test: when somebody leaves on Friday, can you revoke everything they knew by Monday? If the answer involves changing eleven passwords by hand and hoping you remembered them all, the current arrangement is not working.

What about the browser's built-in one?

Better than reusing one password everywhere, and if that is the realistic alternative then use it. But for a business, a proper password manager is worth the small cost: it works across browsers and devices, handles shared access properly, and does not tie your credentials to one machine's profile.

Multi-factor authentication

> If you do only one thing from this guide, do this. Multi-factor authentication is the difference between a stolen password being a disaster and a stolen password being nothing at all.

It means proving who you are with something beyond the password — a code from an app, a tap on your phone, a physical key. An attacker with your password still cannot get in, because they do not have your phone.

Not all methods are equal

Method	Assessment
Hardware key	The strongest option. A small physical key you tap. Effectively immune to phishing, because it will not authenticate to a fake site. Worth it for directors, finance and anyone with administrator rights.
Authenticator app	The right default for most people. Free, quick, and far stronger than text messages. Better still with number matching, where you type a number shown on screen rather than just approving a prompt.
Text message codes	Much better than nothing, and if it is the only thing you will actually adopt, adopt it. But SIM swapping is a real and growing problem, so move to an app when you can.
Email codes	Weak, because the email account is usually the thing being attacked. Avoid where alternatives exist.

> **APPROVAL FATIGUE**
> If a "was this you?" prompt appears on your phone and you were not signing in anywhere, do not tap approve to make it go away. Somebody has your password and is standing at the door. Deny it, change that password immediately, and tell whoever looks after your IT.

Where to turn it on first

1. **Email.** Everything else resets through it, which makes it the master key to your business.
2. **Banking and payment systems.**
3. **Your password manager.**
4. **Accounting, payroll and anything holding personal data.**
5. **Everything else that offers it.** The list is longer than you would think.

Have you been breached already?

You can check whether your email address has appeared in a known data breach at **haveibeenpwned.com**, a free and well-regarded service. Most people find they are in several. It is not cause for panic — it is a prompt to make sure the password from that breach is not still protecting anything important.

Rolling this out across a team

Multi-factor authentication and a shared password manager are straightforward to deploy across a small business, and both are included in the way we set clients up as standard — along with breach monitoring that tells you when a staff password turns up somewhere it should not.

If you would like help getting this in place without the usual grumbling from the team, we have done it many times.

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