EVERYTHING

you need to know about
password managers

breathetechnology
infrastructure | support | security | cloud

PASSWORDS. A NECESSARY EVIL HATED BY EVERYONE.

Everyone knows they should try harder with their passwords.
Yet everything about them seems difficult.

GREAT PASSWORDS ARE:

- Difficult to think up
- Even harder to remember
- Highly frustrating when you get them wrong *(and have to reset them)*

This is what encourages people into sloppy habits, such as relying on weak passwords, or reusing them across several logins. It's these bad habits that cyber criminals rely on to get into accounts.

It's highly likely that someone, somewhere in your organisation is relying on a weak or reused password to protect their access to a critical system.

This leaves your business at risk, without anyone being aware.

Frustrating.

There is some very good news. Apple, Google and Microsoft are working together to kill the traditional password in favour of **Passkeys.**

These are very simple. To login to something, you'll use your phone to prove it's really you.

Your computer will use Bluetooth to verify that you're seated nearby, then send a verification message to your phone.

Unlock your phone in the usual way, with your face, fingerprint or PIN. And that's it. You're logged in.

Apple's introducing Passkeys first with iOS 16. Google and Microsoft will offer them in the near future as well.

However, it will be a long time before Passkeys completely replace passwords.

So what can you do in the meantime to make your organisation safer, and day to day work easier for your team?

The answer is to use a **password manager.** Here's our full guide on what password managers are, and the benefits of embracing them.

WHAT IS A PASSWORD MANAGER?

A password manager is a software application that stores and manages your credentials for all your accounts, including websites, applications, and any software you use in your organisation.

It'll work on your computer and phone.

It will generate and remember separate lengthy random passwords for each application. So when you log in, it will fill in the login blanks for you.

A password manager is simple and easy. Once it's set up, you only need to remember your master password.

What are the benefits of using a password manager?

There are huge benefits on top of increasing your security and protecting your data:

- You don't have to remember your passwords
- You can autogenerate long, highly secure passwords which are virtually impossible to guess
- You'll save time with autofill
- A good password manager will sync across operating systems and browsers. That means if you use Windows for work, but have an iPhone, it's no worry
- It can help to protect your identity. By using unique passwords across every account you segment your data. If one account is breached it's highly unlikely others will be
- It can alert you to risk. If you land on a fake website your password manager won't autofill your data because it won't recognise the site as being valid
- Some password managers scan the dark web to make sure your credentials haven't been leaked
- Many password managers operate a zero knowledge approach, which means your data is encrypted before it leaves your device. That means it's unreadable

What are the risks of using a password manager?

To give you a balanced view, there are a few potential negatives with a password manager:

- All your sensitive data is in one place, protected by one master password
- It's possible cyber criminals could get hold of your master password, for example if you had malware or a keyboard logger watching what you do
- You definitely need to use biometrics or multi-factor authentication (MFA, where you use a separate device) to prove it's you
- If you forget your master password, it's deliberately difficult to reset it

Many of these risks can be overcome by picking the right password manager in the first place.

Which password manager is right for my business?

There are 3 main types of password manager available, each with their own set of advantages & disadvantages

Browser-based

This is the password manager that's built into your browser such as Chrome, Edge, and Safari.

Browser-based password managers are free and easy to use, but that's where the benefits end. **They're not a solution we'd recommend.**

They only work within their own browser, so if you wish to change to another, you either have to export your data or start over.

They are limited in their use over multiple devices. And you have virtually no control over what information your employees are storing.

This can be an issue when someone leaves.

Cloud-based

These password managers store everything in the cloud.

They're safer than browser-based alternatives as they come with features to enhance security. Firstly, they provide a backup of your vault, meaning your data isn't lost if your device is.

Cloud-based password managers also allow you to store other sensitive data, like credit card details and secure notes, giving an additional level of data protection.

They can detect weak and reused passwords, and generate new stronger ones. Some will even run checks to make sure your data hasn't leaked.

You're also able to share secure data easily, with co-workers or family for instance, even if they don't use the same password management service as you.

Cloud-based password managers have the benefit of working across multiple browsers, operating systems and mobile devices. You don't have to think about anything – your password manager just works.

Desktop-based

Desktop-based password managers can be the safest type, but that all depends on how security conscious you and your team are. Just because something is the safest option, doesn't necessarily mean it's the best option for your organisation.

These store data locally on one of your devices. That device doesn't have to be connected to the internet. That's a benefit because it means the chances of it being breached are lower.

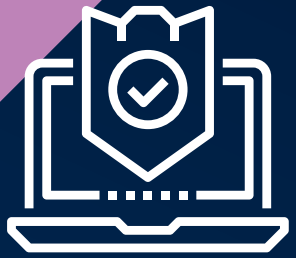
If you use a biometric login for your master password you'll be even safer from rare-but-risky keyboard logger attacks *(this is where malicious software secretly records everything you type into your computer).*

The downside to desktop-based password managers is that you'll need to make sure you take your own regular backups of your data and vault. Otherwise, if your device breaks beyond repair or is stolen, your vault is gone.

Another issue is that you can't access your passwords from other devices, and sharing can be difficult too.

Are password managers safe?

YES!



Although there have been breaches in the past, most professional password managers have an outstanding record.

If you and your team always follow password manager best practice – more on this below – you'll be highly protected from credential theft.

Premium paid-for services also provide significantly more protection. There are more features you can take advantage of for better usability, increased security, and safe sharing… all of which are really important.

Password best practice

There's little point in using a password manager if you don't care about password best practice. If you're not on top of this already, make sure you and your entire team are doing all the right things to keep your organisation and its data safe.

First and most importantly, everyone – and we mean **EVERYONE** – in your organisation should do regular cyber security training. Including you.

This will make sure that all your employees are aware of the up-to-date risks to your organisation and its data. It'll help them stay safe personally, as well.

Your people are your frontline defence against cyber-attacks, so it really is essential that they're armed with the right tools and knowledge to help protect the organisation. If your people aren't following best practice, it doesn't matter how great the security tools you use are, you'll never be as safe as you should be.

Next, make sure everyone on your team uses a password manager supplied by you *(and never their own).* This will give you huge control over what happens to your data when they leave. *This is especially important if your team work remotely or take company devices home.*

Don't ever reuse passwords, even if you're using a password manager. You should make sure passwords are long and complex.

They can be randomly generated by most password managers, and this will give you the highest level of security.

The more complex and nonsensical each password is, the better (by using a password manager, you won't have to remember them anyway, so this makes life a lot easier).

The exception to this is your master password. You will need to remember this one, and it will also need to be very strong. For this, we'd recommend a passphrase.

That's where you take a string of random words that you can easily visualise.

For example, 'neonblueballetshoe'. You could also try a sentence, where the first letter of each word becomes your password, e.g. 'I wish I could eat cake for breakfast 5 days a week' becomes 'Iwlcecfb5daw'.

Enable multi-factor authentication and/or biometrics for additional security. This makes it very difficult for someone to login without your device or you.

You should also avoid using free password managers if possible. While they may be OK for personal use *(and even then we'd question their use),* for protecting sensitive data, free password managers simply don't cut it.

Many don't offer the most essential features, such as syncing across your devices or browsers, multi-factor authentication, and end-to-end encryption.

Finally, create a password policy that all your employees are aware of and follow. It should include never reusing passwords, always using the security tools provided, and never sharing passwords with others.

This should help you avoid the issue of employees cutting security corners and putting data at risk, which sadly, happens from time to time.

As you can see, we'd highly recommend using a password manager in your business to give your data another strong layer of protection against theft.

Would you like to know which one we recommend and use ourselves? Just get in touch and we'll tell you.

www.breathetechnology.com
(live chat available)

01223209920

lucy@breathetechnology.com

breathetechnology
infrastructure | support | security | cloud