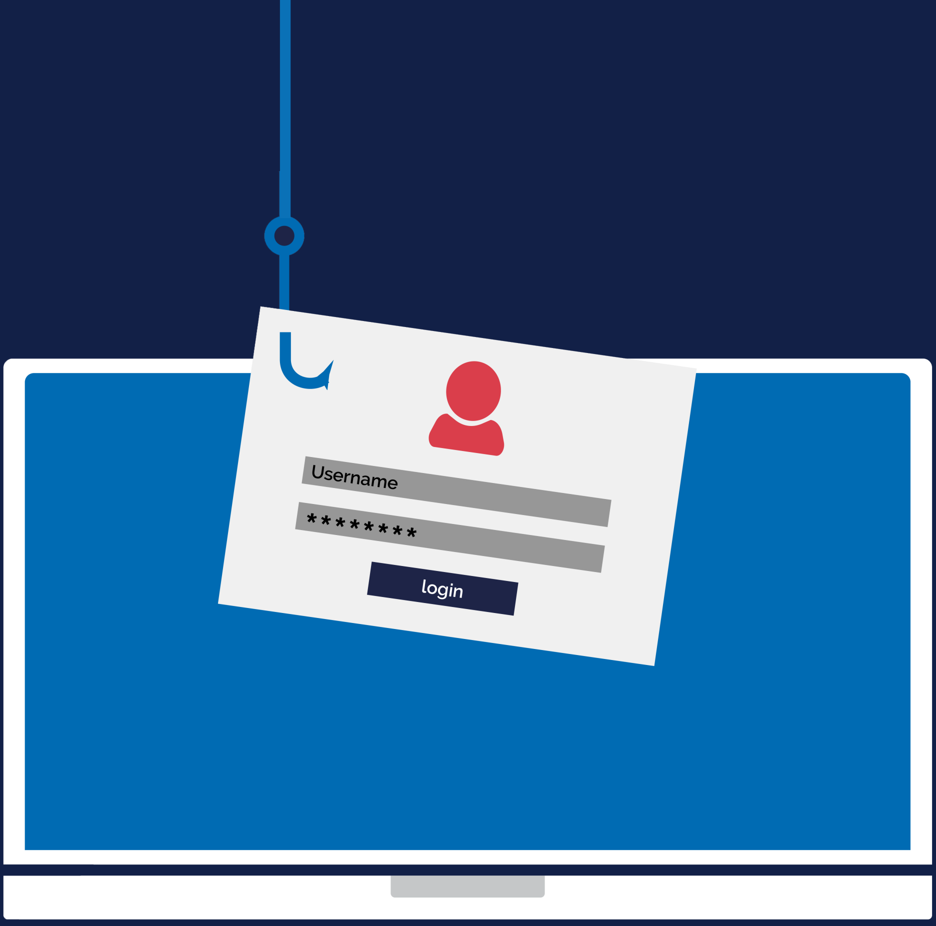


Password Hygiene

A guide on creating, storing and managing your passwords.

www.breakwaterit.co.uk

breakwater IT

PASSWORD HYGIENE

Password hygiene is all about how you manage your passwords. In this guide, we'll cover everything from password creation to storage, and what to do if your password gets leaked.

CREATING A NEW PASSWORD

It's time to create yourself a new account, but that also means choosing a new password. Here are our do's and don'ts...

DON'T

Use a name, date, or anything that could be public knowledge

These are all commonly used and cracked passwords. And don't forget how easily someone could find your pets name on your social media account...

Use the same password twice

If you are using the same password on multiple accounts, and that password is leaked, all your accounts will be at risk. You would then need to retrace and change that password on each account.

Use a keyboard pattern

For example: qwerty, 12345, lkjhg. These are easy to guess and easy for criminals to test against your username.

DO

Use three random words

The National Cyber Security Centre recommends using three random words for a password. It's easier to remember but harder to crack. Example: ghostcrownlemon.

Use a password generator

But make sure you can store the password properly as it will be a random selection of letters, numbers and symbols.

Use a long mix of characters

Include letters, numbers and symbols and make that password as long as possible.

STORING YOUR PASSWORDS

You've used a different password for each account, you've used random words, letters, numbers and symbols, so HOW do you remember your passwords?

DON'T

- **Write them on a sticky note and stick it on your desk** - this also goes for sticking it to your laptop, or even putting it in an unlocked drawer. Think about who could see it: colleagues, visitors, suppliers, or impersonators. What happens if that sticky note is accidentally included in a company image that ends up on social media?

DO

- **Use a password manager** - there are a range of free and paid password managers on the market, including personal and workplace accounts. Let's take a further look...

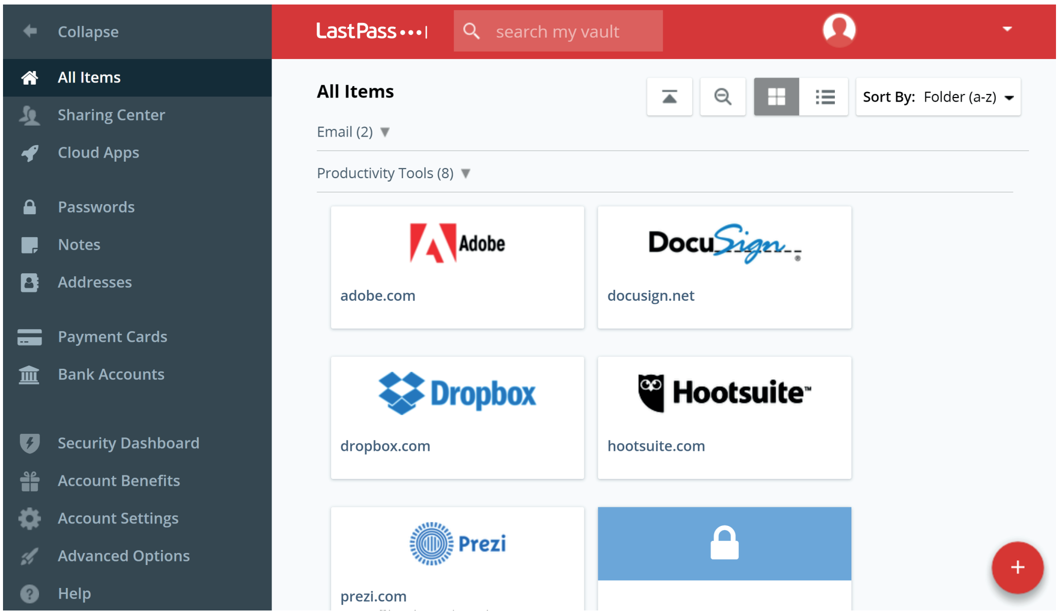
What is a Password Manager?

A password manager is a site or app which stores your passwords in one place. This means the only password you'll need to remember is the one to access your password manager.

Password managers can also generate secure passwords, and auto-fill login credentials through a browser extension.

We would also strongly recommend enabling multi-factor authentication (MFA) for an extra layer of security.

Below is a screenshot of LastPass, one of the password managers on the market:



SECURING YOUR ACCOUNTS

A password manager is a great way to secure your passwords, but don't forget that adding multi-factor authentication on each account, as well as your password manager, makes your accounts even more secure.

What is Multi-Factor Authentication?

Multi-factor authentication (MFA) is an authentication method that requires two or more verification factors. For example, entering your password and a one-time code from an MFA app.

There are three types of MFA, including:

Something you know

A password, pin or combination.

Something you have

A key, smart phone or token device.

Something you are

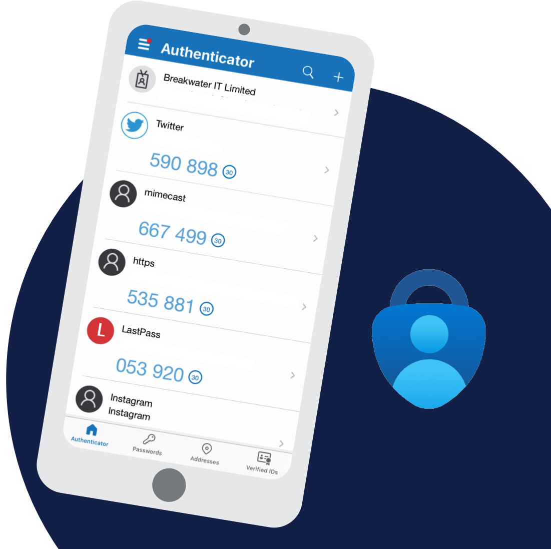
Facial, fingerprint or voice recognition.

Now, you might be thinking that this sounds like a lot. But much of this process can happen without interference.

As previously mentioned, your password manager can save you time by auto-filling your credentials. And devices can be marked as safe so that you don't need to enter an MFA code every time you login, so long as you are accessing your account from that device.

TOP TIP

MFA apps like Microsoft Authenticator are free to download and use!



Authenticator

Breakwater IT Limited

Twitter

590 898

mimecast

667 499

https

535 881

LastPass

053 920

Instagram
Instagram

TYPES OF PASSWORD ATTACKS

At this point, you may be wondering why all these steps for your password is necessary. Well, there are many different password security threats, and following good password hygiene means you have the best chance of not being a victim.

Here are some of the most common password attack types:

- **Phishing** - cyber criminals attempt to trick you into giving them your login credentials. Typically, they will impersonate a legitimate company or individual via email, telephone, SMS, websites and more. Avoid this by not engaging with any unexpected contact from a business or individual.
- **Dictionary Attacks** - programs are used to test every word within a dictionary as your password. Avoid this by using a variety of words with symbols and numbers mixed in.
- **Password Spraying** - a list of frequently used passwords is tested against your username. Avoid this by not using passwords such as 'password' or 'qwerty'.
- **Credential Stuffing** - stolen credentials from a previous breach are tested against your username. Avoid this by creating unique passwords for each account.

WHAT TO DO IF YOUR PASSWORD IS LEAKED

Sites like haveibeenpwned.com allow you to check whether your login credentials have been involved in a breach.

If you find that your credentials have been involved in a breach, you should change your password immediately and make sure you have MFA enabled on that account.

If there's any risk that sensitive data, such as financial information has been involved, keep a close eye on your accounts or consider freezing them.

For any additional help with password hygiene, or anything else you need, get in touch:

Service Desk:
01603 709301 | servicedesk@breakwaterit.co.uk

Enquiries:
01603 709300 | enquiries@breakwaterit.co.uk