# Essential Guide to Password Creation

### ****PASSWORDS ARE IMPORTANT****

Just think for a minute of your front door key. How many different doors does this key open? Would you be happy using a universal key to get into your house? Passwords are just like that unique key, they are an effective way of identifying and authenticating who you are. It is the first, and sometimes the only layer, that stands between you accessing your money, data, social media accounts and email, or someone else accessing those assets and possibly compromising them, stealing from you, or locking you out.

The most common passwords still are, password, password1 and 12345678.  Even a password of 8 characters can be cracked in about 5 hours using a standard office computer, and many passwords that are made up of dates of birth, names of your pets and children, your favourite band or football team can be easily worked out by reading your social media pages or googling you.

### ****ONE PASSWORD – ONE ACCOUNT****

One of the biggest human-factor risks to businesses is staff re-using their passwords. If your work account access password is the same as your Facebook password, potentially a Facebook breach (or any of the other accounts where you use that username-password combination) could equal a big security problem for your organisation.

When an online company is breached, thousands of pieces of customer information can be stolen, including email addresses and passwords. The cyber criminals will immediately go through as many accounts (e.g. utility companies, eBay, Instagram, Amazon, Hotmail, insurance companies) as they can, trying those user-name-password combinations hoping to open up an access point for more crime. This is the reason you need a separate password for each online account.

Your email address is the gateway for all your other accounts and the place where you reset your passwords. With this in mind, if a criminal gets access to your email account, they can take control of most other user accounts that you have. At the very least, have a complex and unique password for your email account that no one could guess. Password length and complexity attribute how much time it can take to crack the password by a cyber criminal.

Cyber criminals can use computers to guess people’s passwords and break into their computers in what is called a Brute-force attack. The computer will try every combination of letter, literally working through the dictionary till they have found the words that work. Some programs are sophisticated enough to search logical substitutions such as ‘4’ for an ‘A’ , ‘I’ for ‘1’ etc. For this reason, it is recommended that you use a password that is over 8 characters long, or better still, 12 characters or more, make it complex and hard to guess, and if available you should lockout your accounts after a certain number of unsuccessful login attempts.

## **HOW DO YOU THINK UP A UNIQUE SECURE PASSWORD FOR EACH OF YOUR USER ACCOUNTS AND ALSO REMEMBER THEM?**

### ****HOW TO MAKE A STRONG PASSWORD****

[The National Cyber Security Centre](https://www.ncsc.gov.uk/collection/small-business-guide/using-passwords-protect-your-data) has a great deal of useful advice about passwords. They recommend that you use three random words which you can remember but do not naturally go together. It is also a good idea to use numbers and special characters (\*&%F£) in your password as well as a combination of upper and lower case letters. The longer your password the better. It is recommended selecting long passwords for your admin and other crucial systems’ accounts (i.e. email account, banking account). Do not share your password with anyone, this is private information.

### ****LOOKING AFTER YOUR PASSWORDS****

The good news is that you do not need to remember all those long and complex passwords. You can use a piece of software called a Password Manager.

You may have noticed that your browser already asks you if you’d like it to create and store passwords for you. This is a browser integrated Password Manager and is safe to use for personal use, however there are security issues linked to this kind of password manager.

It is recommended you use an independent, stand-alone password manager such as Last Pass or Dashlane. Do research third party password managers and use the one you feel is the safest. It is often as simple as downloading their software from their website and signing-up with your email address.

You will then only need to remember one really good complex password to the Password Manager itself and after that, the Password Manager will remember your user names and create and remember extremely secure passwords for each of your accounts. It will be able to operate across multiple devices and on different browsers, it can also be asked to remember additional information such as addresses, Wi-Fi codes, credit cards, passports; all organised and encrypted. Password managers provide an option to configure multi-factor authentication to provide another layer of security.

### ****ANOTHER LAYER OF SECURITY****

Another great way to add a layer of security to your password is to use 2 factor authentication (2FA) or multi-factor authentication (MFA). This process is being used more and more and involves using your finger print, retina scan, or a code being sent to a separate device e.g. your mobile phone to further verify your identity. If you have the option for 2FA or MFA\*, use it where possible. **(see article**[***ABOUT 2 FACTOR AUTHENTICATION***](https://iasme.co.uk/cyber-blog/what-is-two-factor-authentication/)**)**

### ****HAS YOUR PASSWORD BEEN ALREADY BEEN MADE PUBLIC?****

If you are curious how many times your email and password have been exposed due to security breaches, check it out on the website: [haveibeenpwned.com](https://haveibeenpwned.com/) . Don’t worry too much if you have been ‘pwned’ - most emails have been breached. The important thing is to change your password if you believe it may have been compromised. If you suspect that you have a virus in your system, if the manufacturer notifies you of a security weakness in their product or someone on your contact list gets emails from you that you didn’t send, immediately go onto the relevant accounts and change the password. Do not forget to update your passwords on the password manager.