

# Tech it Easy

## PASSWORDS

### CREATING PASSWORDS

#### 3 RANDOM WORDS *with* SPECIAL CHARACTERS

e.g. Beauty-Beast-Young | Sun+Majorca=Beach

#### ONE WORD BASE

Choose a memorable word or phrase and change some of the letters.

E.G: PIZZA becomes P1774. The idea is to commit this part to memory. Then, create the second half to complete the password for each account  
- e.g. P1774-4ma7On

#### PASSWORD MANAGER

A Password Manager can generate a complex password, such as:

g^h6&ttf;"dyR@57\$!

The Password Manager will remember all your passwords, as well as your user names, and will log you into your online accounts whenever you ask it to. You will need to remember one password to log you into the Password Manager - the Master Password. So make sure that particular password would be too difficult for a scammer to guess but you are able to remember it – because that's the only password that the Password Manager won't store for you.

#### 2 FACTOR AUTHENTICATION – 2FA

This is a useful additional level of security. But how does it work?

If you set up 2FA on your *Buy-Gold-Bars-For-Birthdays* account... whenever you try to log into the account, the website will send you a secret code (a one-time passcode) via a text message. To be able to log into your account, you will need to type the code that they've sent you into the box on their website.

So if a scammer does happen to find your *Buy-Gold-Bars-For-Birthdays* login details, they would also need your phone for the secret code. Most UK banks use 2FA to keep their customers' accounts safer.

## AUTHENTICATOR APP

An authenticator app creates one-time passcodes. The codes change regularly (e.g. every 30 seconds) for extra security. Google Authenticator is one example - and it's free from your phone's official app store.

## COMPROMISED PASSWORDS

You can check if your passwords - or any of your data - have been stolen in a hack at:

[HaveIBeenPwned.com](https://haveibeenpwned.com)

If you do find that an account password has been stolen, immediately change that password. And if you've used the same password elsewhere, change that too. Best to use unique passwords to stay safer.

## EMAIL

It's recommended that you use a very secure password for your Email account. Why? If you ever click "Forgot Password", your reset-password link is likely to be sent to you in an email. If a scammer can get access to your emails, it would be possible for them to change all your passwords and steal your accounts.

## FINAL TIPS

1. Use a unique password for everything.
2. A 12-character password (using upper and lower case letters, numbers and symbols) is harder to crack than a short recognisable word.

There's much more tech-made-easy at  
[TechitEasyWorkshop.co.uk](http://TechitEasyWorkshop.co.uk)