2eIihnhe looks like complete (and impossible to remember) jumble but is the second (2) letters of 'We wIll fight them on the beaches' and with the second letter as a capital. So you could write down that password as say 2Churchill without much chance of giving away the password.

Any phrase (with enough words) meaningful and memorable to you will do and may generate several passwords (first letters, second letters, third(or last) letters). These will look completely unrelated should one be compromised, but if you forget or mix them up you can work out a limited range to try.

## Look after *your Passwords*

*Your computer* may remember certain passwords (e.g. Email) and not ask you for them on a regular basis. Or your computer may offer you a PIN instead of a password to start the computer up. In both cases you must still retain the passwords. They will be needed if you get a new computer or additional device (Smartphone etc) or if your computer needs resetting or if you access new services.

## Never Reveal your Password

No reputable company will *ever* ask you for your password at most they will ask for one or two letters from it.

## BUYING ON LINE

Buying on line is actually safer than over the phone because it eliminates your details passing through an individual who could take note of them.

When you do use your credit (and especially debit) card to buy think about unticking (or not ticking) the box which says store my credit card details, in which case the company must 'forget' key details as soon as the transaction is complete.

Consider obtaining a Paypal account. Paypay is bigger than most banks and can be used to pay for many goods and services. The advantage is that only Paypal ever have your credit/debit card details, they pay the supplier then Paypay charges you. This avoids (maybe small) companies with insecure systems ever having your details. Paypay give the address you registered with them to the supplier for delivery.

Still worried about using a credit card online? Then consider a 'Money Card' (such as Pockit). You add cash to the card then use it like a debit card but you (or anyone else) can't spend more than the cash you put on it.

Please note: we cannot guarantee that this document is complete or up to date, we hope you find it useful as a guide.

Centre open Mondays am and Wednesdays all day in The Exchange Sturminster. Tel 01258475272. snclc.org.uk
snclc@btconnect.com

## NewTech – Sturminster Newton Community Learning Centre


# ALL ABOUT PASSWORDS

## Important Passwords

Passwords are important, they are your main and sometimes only security for your money, identity and files.

Web sites on-line for which your password is especially important include:

- Your Email account
- The password for the account with your internet service provider (E.g. BT, Plusnet, TalkTalk)
- Any account that holds your money, credit, shares etc. including Paypal
- Sites that have a lot of details of your identity like Government Gateway
- Any Cloud accounts where you store personal information or photos etc.
- Your computer's account with Microsoft, Google, Apple etc.

## Multiple Passwords

It is likely that your Email address serves as User ID/Name for all the above but you should not use the same **password** more than once for these sites.

Possible exceptions:

- Email and computer (Microsoft/Google/Apple) accounts where separate passwords can lead to considerable confusion.
- Email and broadband service provider accounts if they are both provided by the same company.

Whilst the best advice is not to use the same password twice, this can result in far too many to remember or even record securely.

It is reasonably safe to use a single password for sites that you buy from or regularly visit and require you to sign into. No decent company will allow goods to be sent to a different address (should someone get hold of your password) without asking for the credit card details again.

## Choosing and Remembering Passwords

You must choose "strong" passwords especially for the important sites listed above. Names of people, pets or indeed any ordinary word are not good enough. A strong password contains at least one capital letter and number and possibly other symbols like & * % etc. A strong password must also be at least 6 (preferably 8) characters long.

There cannot be spaces in a password. Small letters ARE different to capital letters.

The main problem that you have with passwords once you have decided upon a strong one is remembering them. Writing them down in a little book is an obvious way but if the book is stolen or lost then so are the passwords. There are some so called Password Managers on the market for small outlays. These remember your passwords and fill them in appropriately. They themselves are protected by a single strong password of your choice. We can't recommend a particular Password Manager but can discuss their use with you at The Learning Centre.

Many people invent their own way of creating and remembering strong passwords, Here are a couple of examples:

Choose a phrase like "I was born in Child Okeford" and take the first letters "IwbiCO", these can form the base of many passwords. Also choose a 3 or 4 digit number such as your birthdate "150" (Jan 1950). Now you can create passwords with the IwbiCO prefix and different number endings BUT when you write down the number add your secret number (150). So you can write;

Email PW is (born) 495
(real password IwbiCO345)

Bank PW is (born) 675
(real password IwbiCO525)

For even better security have other phrases (My first car was a Ford –MfcwaF) and write:

Paypay PW is (car) 273
(real password MfcwaF123)