

## Using passwords

### How strong is your password?

You are required to use passwords more and more with computers and as we come to rely on technology to store secure information it is inevitable. Consequently, passwords are becoming more important because of the need to protect personal information, both as an individual and as a responsible person holding data on others (regulated under the Data Protection Act).

Passwords are used to gain access to computers and other hardware, programs and data. If you lose a password it can be the same as if someone has stolen your equipment or information. If your password is 'weak' someone could 'crack' it which is really the same as someone stealing your kit or information.

So, remember your passwords and make sure they are strong. But, you might have 20 or more passwords. If you run a network this is likely. In addition you might be having to log software serial numbers and authentication codes. You need to record all this information and keep it safe. Attach a level of importance to the information you are recording, such as:

- 1 Passwords which give access to personal information about me/organisation
- 2 Passwords which give access to financial information about me/organisation
- 3 Passwords and usernames which give access to email accounts
- 4 Passwords and usernames which give access to computers and the network
- 5 Passwords which give access to hardware or software configurations
- 6 Serial numbers or authentication codes which are required to reinstall software or prove ownership.

Do not keep all this information recorded in the same place. As a simple rule of thumb, secure this information to the same extent to which you would secure the thing it is protecting (in other words, if you don't leave your pin number for your credit card on a post-it on your computer, don't leave your internet banking password there!).

So having worked out what you are going to record and where it is going to be recorded, give a thought to how you construct your passwords.

- 1 **Make your password strong.**
  - a. Ideally it should be at least 14 characters long.
  - b. Use the full keyboard, not just letters and numbers. Remember case can be important
  - c. Do not use personal information (e.g. National Insurance number) as your password
  - d. Do not use sequences or repeats (1234 or 55555)
- 2 **Make your password memorable**
  - a. Consider a memorable phrase or personal set of events
  - b. Put them in a sentence and maybe only use part of it. Remember to include numbers and characters.
  - c. Whenever you create a password, write it down.
- 3 **Store your usernames and passwords on paper.**
  - a. Keep the paper separate to your computer, ideally in a different location
  - b. Allow yourself personal prompts

You can check the strength of your password here:

[http://www.microsoft.com/athome/security/privacy/password\\_checker.msp](http://www.microsoft.com/athome/security/privacy/password_checker.msp)

Now you have secure passwords, keep them secret

•**Don't reveal them to others.** Keep your passwords hidden from friends or family members (especially children) who could pass them on to other less trustworthy individuals.

•**Protect your passwords.** If you write down your passwords, do not leave them anywhere that you would not leave the information that they protect.

•**Never provide your password over e-mail or based on an e-mail request (or over the phone unless you are very sure whom you are speaking to).** Any e-mail that requests your password or requests that you go to a Web site to verify your password is almost certainly a fraud.

•**Change your passwords regularly.** This can help keep criminals and other malicious users unaware. The strength of your password will help keep it good for a longer time.

•**Do not use the same password for different accounts.** This will reduce the risk of more than one area of information or bank account being attacked.

•**Do not type passwords on computers that you do not control.** Computers such as those in Internet cafés, computer labs, shared or borrowed systems, training centres, and airport lounges should be considered unsafe for any personal use other than anonymous Internet browsing. Do not use these computers to check online e-mail, chat rooms, bank balances, business mail, or any other account that requires a user name and password. Make sure that you are logged out when you have finished and if possible delete the cache and cookies.

**If you (or the organisation you work for) are the victim of fraud:**

- Don't keep it to yourself (tell the most senior/finance person you can)
- Close any affected accounts
- Change the passwords on all of your online accounts
- Place a fraud alert on your credit reports
  - Experian: <https://www.creditexpert.co.uk/UK/index.aspx>
  - Equifax: <https://www.econsumer.equifax.co.uk/consumer/uk/>
- Contact the proper authorities
- Record and save everything

Finally, make sure all your staff are aware of their responsibility for security and make sure that this is included in the IT acceptable use policy. If you, for example, hold information about individuals and a member of staff uses a weak password to access that information, who is responsible? Has due care been taken over the security of that information?

**Password quiz**

Which of the following passwords is more secure? Rank them in order of security.

Password	Level of security	Comment/how long should it be used for
JohnS		
Spotthedogisoldbutilovehim		
January15th		
1866		
Myhusbandis43		
Mhi43		
1234567890		
a1b2c3d4e5f6		
A1b2c3d4e5f6		
~Myagein2000was26		
!"\$%&^*()		

The bottom one is blank because some people don't bother putting one in at all! There is only one 'best' password in this list which would be very difficult to crack. Remember that your password might be case sensitive. If your password is weak, change it immediately. There are never any promises in security, but if your password is medium, change it every week, strong every fortnight, very strong every month and best will probably hold for years. The better your password, the more you reduce the risk of it being 'cracked'.

*There are no solutions to the quiz – just use the password checker and common sense!*