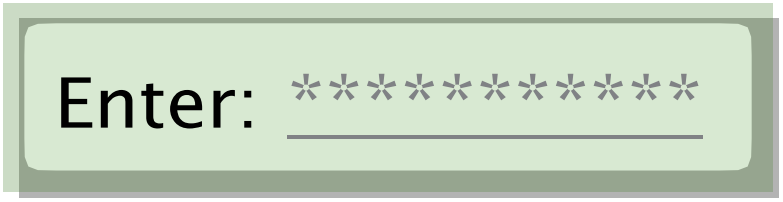
How to Create a Strong Password



E-safety Support

What makes a password strong?

The key to creating a strong password is to consider how your password might be stolen, hacked or guessed.

The most common occurrences of password security being breached are 'phishing' attempts, passwords stolen from unattended computers, and people watching as you type in a password.

- Avoid situations where people can look over your shoulder when you login to your accounts.
- Don't keep your password written on pieces of paper kept on your person, in wallets, or with house or car keys.
- Never respond to emails or phone calls which ask you to provide a username and password.
- Only input passwords on sites you've accessed directly by typing in a website address into your browser, or via a reputable search engine such as Google.com.

Avoid choosing passwords which might be guessed. Passwords such as 'password' or 'letmein' or 'opensesame' are very common and easy to guess. Also avoid birthdays, maiden names and the names of your children. Apparently men often use four letter swear words in passwords, while women prefer the names of partners or children – so avoid these common password mistakes.

Hackers commonly use three methods to 'harvest' passwords.

Dictionary attacks – a computer or server is set up to guess the password using every word in a dictionary. The computer isn't aware of which words are common, and which words are obscure. Therefore it is just as easy for a computer to guess "oranges" as it is to guess "demagogues". It is best to avoid using any dictionary words in your password. Putting a number or symbol at the beginning or end of your word, or using a combination of lower and upper case letters to form your word doesn't make it any more difficult for the computer to guess your word – the computer simply tests all dictionary words and adds numbers and symbols in a 'brute force' attack.

A 'brute force' attack is where a computer, or series of computers controlled by a virus, try to guess your password by using every possible combination of letters, symbols and numbers. With a fast computer, or a number of linked computers, 250000 combinations can be guessed in a second. A dictionary word and number based password can be guessed in 24-48 hours.

Many 'user' based websites, such as blogs, forums and collaborative websites are much easier for hackers to attack if there are common user names. For example, if the administrator of the website uses the name 'admin' as a username – the hacker will already know half of the user/password combination. If the administrator user name is 'Own3R' the hackers will have a much harder task since he cannot attempt to guess the password without first knowing the username. For this reason it is best not to use elements of 'your name', or your email, when creating usernames on profile-based or collaborative websites.

Tips on creating a strong password:

- Your password should be at least eight characters long. The longer your password, the more difficult it will be for a hacker to guess it or brute force to crack it.
- Your password needs to be easy for you, but not other people, to remember.
- Use a sequence of characters randomly composed of numbers, symbols, upper case, lower case and spaces (if spaces are allowed by the website/system).
- Never use a correctly spelled, or almost correctly spelled or dictionary word. This includes foreign languages and slang.
- Don't use the same password for every website, and try to use a different password for each site.
- Use a password you can type in quickly. This makes it more difficult for people to try and look over your shoulder.
- Use a strong password generator application or website.
- Merge two words or numbers you will remember to create a password which a computer will find difficult to guess. For example I went on holiday to Devon in 1983. The password could be "D1e9v8o3n."
- Create a mnemonic to create and remember a password. For example, my #1 favourite record is *I Don't Like Mondays* by the Boomtown Rats. The password might be: "#1IdLmBtBr." The #1 and the full stop make it particularly difficult for a computer to crack.

Things to avoid when creating a strong password:

- Avoid adding a digit or symbol before or after a word or a password – for example: “password1” or “!letmein”
- Avoid writing a word twice or three times, for example: “passwordpasswordpassword”.
- Avoid creating a password by writing a word backwards, for example: “drowssap”. Hacking scripts find these easy to guess.
- Avoid removing vowels or other letters from words to create a password, for example: “psswrd”. Hacking scripts using spell check algorithms find these easy to guess.
- Avoid common letter or number sequences, for example: “abcd1234”.
- Avoid using numbers to substitute letters in common words, for example: “pa33w0rd”. Hacking scripts find substituting letter strings easy to guess.
- Avoid including your name, email address, or any other personally identifying information such as birthdate, location, computer name, telephone number, postcode, car registration number, family names or job in your password.
- Avoid using the same password for more than one site. Also avoid using variations of the same password, or reusing variations of the same password when you change a password.
- Try to change your important passwords every 1-3 months.

Secure password generators:

These sites will generate random, strong and secure passwords:

- http://www.pctools.com/guides/password/ (Useful if your password has to include certain characters or be a specific length.)
- http://strongpasswordgenerator.com/ (This site also suggests how you can remember the password.)
- http://www.random.org/passwords/ (Creates highly randomised passwords which will be difficult for computers to guess.)
- https://www.grc.com/passwords.htm (This site will create military grade cryptographic passwords.)

How to remember and/or store passwords:

Use a secure password safe:

- This is a free password safe: http://passwordsafe.sourceforge.net/
- This is an alternative free password safe: http://keepass.info/

Create an encrypted text file to store your passwords:

- This software is ideal for encrypting files or memory sticks: http://www.truecrypt.org/

Check your password strength:

These sites will help you assess the strength of your password:

- https://www.microsoft.com/security/pc-security/password-checker.aspx
- https://www.grc.com/haystack.htm - This site will estimate how long it would take a computer to hack your password.

Create an annual ‘check and change your password day’:

As part of an e-safety day, or Safer Internet Week, create a ‘check and change your password day’ which can be taught in the ICT curriculum.