Passwords are often the first and only barrier between your information and anyone who might want to read, use or destroy it without your permission.

In general, when you want to protect something - whether a house or an email account - you lock it up with a key. All keys, physical and electronic, have one thing in common: they open their locks just as effectively in the hands of somebody else. You can use the most advanced security tools, but if your password is weak, or if you allow it to fall into the wrong hands, they will not do you any good.

# How to make a strong password

A password should be difficult for a computer program to guess, difficult for others to figure out, and should be chosen so as to minimise damage if someone does learn it.

* **Make it long:** The longer a password is, the longer takes to guess it. Use more than ten characters or ideally a long phrase or sentence. Short passwords of any kind, even totally random ones, are not strong enough for use with encryption today.
* **Make it complex:** Include upper case letters, lower case letters, numbers and symbols.
* **Don't make it personal:** Don't choose a word or phrase based on information such as your name, telephone number, child's name, pet's name, birth date, or anything else that a person could learn by doing a little research about you.  
  ? Keep it secret: Do not share your password with anyone unless it is absolutely necessary. If you must share a password with a family member or colleague, you should change it to a temporary password first, share that one, then change it back when they are done using it. Often, there are alternatives to sharing a password, such as creating a separate account for each individual who needs access. Keeping your password secret also means not allowing anyone to see you typing it in.
* **Make it unique:** Avoid using the same password for more than one account. Otherwise, anyone who learns that password will gain access to even more of your sensitive information.
* **Keep it fresh:** Change your password on a regular basis, at least once every three months. The longer you keep one password, the more opportunity others have to figure it out and use it.
* **Make it memorable:** If you have to write your password down because you can't remember it, you may end up facing a whole new category of threats that could leave you vulnerable to anybody with access to your work area. If you are unable to think of a password that is long and complex but still memorable, the remembering secure passwords section, below, might be of some help. If not, you should still choose something secure, but you may need to record it using a secure password database such as [KeePass](umbrella://lesson/keepassx), outlined in our Advanced section. Other types of password-protected files, including Microsoft Word documents, should not be trusted for this purpose, as many of them can be broken in seconds using tools that are freely available on the internet.

# Remembering secure passwords

There are a few tricks that might help you create passwords that are easy to remember but very difficult to guess.

* **Vary capitalisation, such as:** 'My naME is Not MR. MarSter'
* **Alter numbers and letters, such as:** 'a11 w0Rk 4nD N0 p14Y'
* **Incorporate symbols, such as:** 'c@t(heR1nthery3'
* **Use multiple languages, such as:** 'Let Them Eat 1e gateaU au ch()colaT'
* **Use acronyms:** 'Are you happy today?' becomes 'rU:-)2d@y?'

A little effort to make the password more complex goes a very long way. Increasing the length of a password even just by a few characters, or by adding numbers or special characters, makes it much more difficult to crack.

You can check the strength of passwords on [Passfault](https://passfault.appspot.com/password_strength.html).

# Security Questions

Be aware of the ?security questions? (such as ?What is your mother?s maiden name?? or "What was your first pet's name?") that websites use to confirm your identity if you do forget your password. Honest answers to many security questions are publicly discoverable facts that a can be easily found, and therefore bypass your password entirely. Instead, give fictional answers that, like your password, no one knows but you. For example, if the password question asks you your pet?s name, you may have posted photos to photo sharing sites with captions such as ?Here is a photo of my cute cat, Spot!? Instead of using ?Spot? as your password recovery answer, you might choose ?Rumplestiltskin.?

Swipe right for this lesson's checklist

Go to the Advanced lesson for advice on how to manage your passwords.

[Go to Advanced Lesson](umbrella://lesson/passwords/1)

Go to the Expert lesson for advice on what to do if you think you might be forced to hand over your password.

[Go to Expert Lesson](umbrella://lesson/passwords/2)