



Factsheet 15 – Understanding password security

This factsheet helps:

- provide tips to create and remember strong passwords
- explain the importance of correct password storage and use
- understand when even a strong password can be compromised

What is a password?

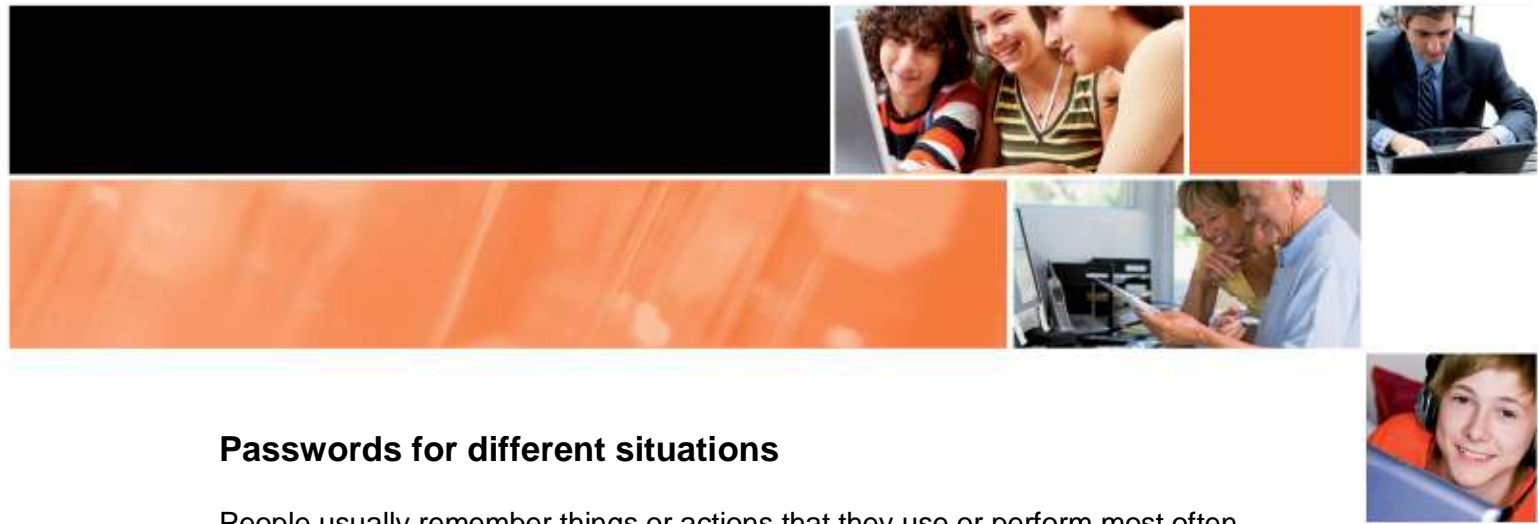
A password is a secret known only to you. A password provides access to a computer system or service for a specific user and is used to verify the identity of the user. The system can be your home computer, your email account, your online bank account or any web account. If your password is captured, guessed or stolen, someone could impersonate you online, steal money from your online bank account, send emails in your name or change files on your computer – to name just a few of the possible outcomes.

Attacks using stolen passwords occur more often than you may think. If you do not take care to choose a strong password and protect it, this could happen to you. You should never record your password somewhere, where it could be found by someone else, and you should never tell anyone your password.

The challenge today – passwords and remembering them!

These days, any typical internet user is faced with the task of remembering large numbers of passwords. Therefore, it is no longer simply a matter of using strong passwords and changing them often! Rather, we need to adopt a more realistic approach to password use and protection.

If it helps to write your passwords down, do so – but hide them somewhere safe, away from prying eyes.



Passwords for different situations

People usually remember things or actions that they use or perform most often. When it comes to passwords, this means that people will most often remember the passwords of accounts they access most often – even if that password is chosen using the methods described in this document. Conversely, trying to remember the password for an extremely important account that is accessed infrequently is rarely successful.

The potential harm from the theft of passwords for a bank account, online stockbroking account or employee web portal is considerable. For these types of accounts it is especially important to create and use a strong password and then protect it.

Web browsers often prompt you to “save” your password. For accounts which have low value or importance to you, it is acceptable to “save” a password to your computer. Understand however, that anyone able to use your computer may have access to the accounts for which you have saved passwords. For this reason, **it is recommended that you do not save passwords for your important accounts.**

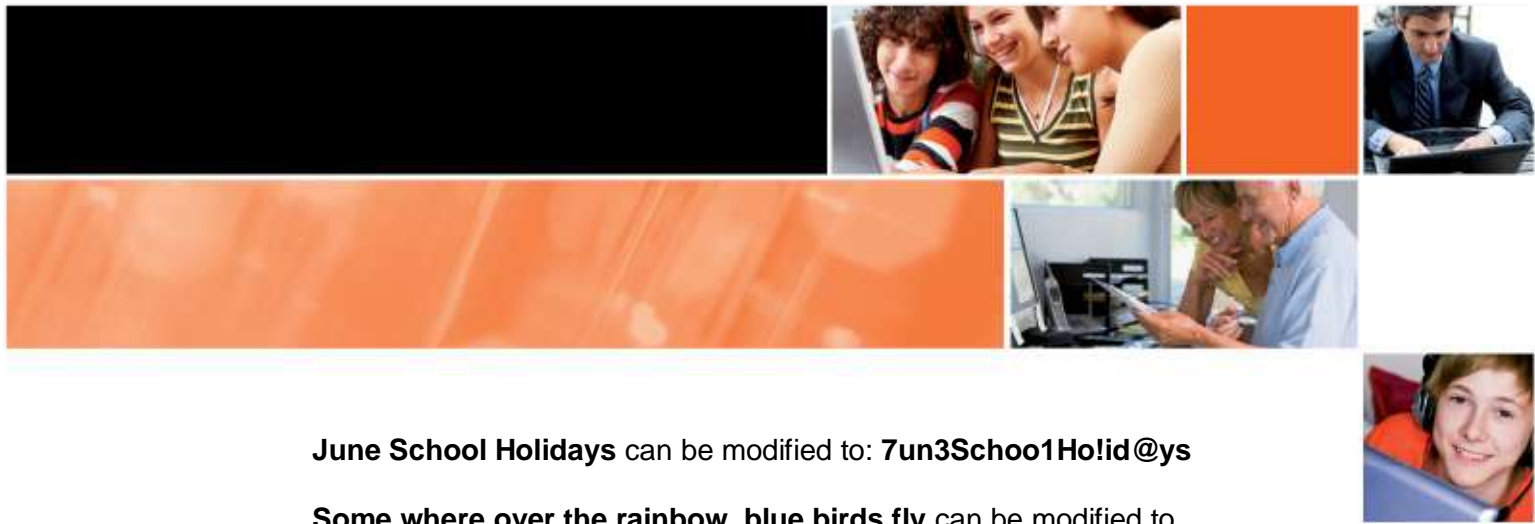
It is **always** better to create and use a **strong** password, **write it down** and **keep it safe** than use a weak password. Always make up a new password for each and every online account that you open – you should not reuse passwords because if one is compromised, it will give an attacker access to other online accounts.

Creating easy to remember strong passwords

Generally, a strong password has the following attributes:

- a minimum length of eight (8) characters; and
- a mix of upper and lower case letters; and
- at least one numeral; and
- at least one non-alphanumeric character; and
- does not include a dictionary word in any language.

The password does not literally have to be a single word. To make a password easy to remember, think of a pass phrase and then change some of the characters to make it a strong password:



June School Holidays can be modified to: **7un3Schoo1Ho!id@ys**

Some where over the rainbow, blue birds fly can be modified to **5w0tR,Bbf}**

I like Australian red wine can be modified to: **IL077ieR3dw!ne***

Be good, be wise can be modified to: **B3g00db3wi5e\$**

Please don't use these examples.

Using strong passwords, particularly for important online accounts, can help protect them from being 'cracked' or guessed. With the computing power and resources available today, it is estimated that a password which has these features will take several years to crack. Passwords consisting of all letters or all numbers are trivial to crack within a few minutes.

How often should I change my password?

If you choose a strong password using the principles above, changing a password once a year is acceptable, unless you believe that it may have been exposed.

Circumstances where this could happen include using your password at an Internet cafe or on a computer that doesn't belong to you, or if your anti-virus program has found malware on your computer.


When you create or change your password, at any time or for any reason, ensure that you follow the principles outlined above each time. Passwords should be created and changed only from a computer you trust.

When is a strong password not good enough?

Understand that while a strong password is an important security mechanism there are ways criminals can still get your password or bypass it completely. Hence a strong password is not a substitute for implementing good security practices more generally.

The two main ways criminals defeat strong passwords is by:

- using malicious software on your computer that monitors your computer to find your password, by looking in the place where passwords are stored, monitoring your key strokes or screen activity; and

- 
- tricking people into disclosing their important passwords, or other sensitive information of value to a criminal – this is called **phishing**. For further information refer to the [Protecting yourself against phishing attacks](#) factsheet.

What if my password is captured or stolen?

If you believe there is a risk your password/s have been captured by another person (accidentally or deliberately) **change the affected password/s immediately**.

If you believe there is a risk your passwords have become compromised due to malware, **immediately change your passwords** for all of your online accounts **on a different, uninfected computer**. **Do not enter any passwords on your computer until it has been cleaned of malware**. If you enter your new passwords on your infected computer, they will be immediately captured in the same way as the old passwords. Refer to the [factsheets that help you to remove malware from your computer](#).

In all situations of a suspected compromise of your passwords, you should notify the organisation/s affected, if warranted. For example, if a password is for your online bank account, notify your bank; if a password gives access to your email and your Internet access, notify your Internet Service Provider.

Always give priority to changing the passwords for those accounts which are most important and valuable.

Report prepared June 2009