How to choose a secure password

Inspection Certificates Online

Your Inspection Certificates Online (ICO) access requires a password with reasonable complexity and with certain conditions to ensure ICO and other Transport and Main Roads (TMR) online systems stay secure. Although these measures may seem excessive, the threat of a cyber-attack is ever present. It is extremely important to choose a secure password for your ICO account and all other online accounts.

ICO Password Requirements

Your ICO password must meet the following requirements:

- Must be 10 or more characters long.
- Must contain an uppercase letter, lower case letter, a number and a special character (for example, !@#$%^&*).
- Must differ from previous three set passwords.

You will be required to change your password every 90 days. In some circumstances, you must enter your old password when setting a new password. Password reset emails will only be valid for 1 hour after they are sent and can only be used once. You will receive an email confirmation once your password has been set.

Tips for Choosing a Strong Password

Here are some tips from the Australian Cyber Security Centre which is the Australian Government's lead on national cyber security:

The key thing to remember when creating a password is that the longer it is, the stronger it is!

Think of a passphrase that is made up of at least four words, including at least 13 characters, for example 'horsecupstarshoe'. Make it meaningful to you so it is easy to remember.

Using strong passwords lowers your overall risk of a security breach, but they do not replace the need for other effective security controls, such as installing anti-virus software and updates to your operating system as soon as they are released.

Do not include the following things in your passwords:

- repeated characters
- arbitrarily mixed letters, numbers and symbols
- single dictionary words, your street address or numeric sequences (such as 1234567)
- personal information
- anything you have previously used.

Maintain password hygiene to keep them safe:

- Don't use the same password for multiple services or websites.
- Don't share your passwords with anyone.
- Don't provide your password in response to a phone call or email, regardless of how legitimate it might seem.
- Don't provide your password to a website you have accessed by following a link in an email—it may be a phishing trap.
- Be cautious about using password-protected services on a public computer or over a public Wi-Fi hotspot.
- If you think your password may have been compromised, change it immediately and check for any unauthorised activity. If the same compromised password has been used on another site, create a new password there as well.

More information can be found at https://www.staysmartonline.gov.au/protect-yourself.