

**Computer Troubleshooters  
Wairarapa**  
432 Queen Street, Kuiripuni  
Masterton

info@ctw.co.nz  
www.ctw.co.nz

**T: 06 378 8770  
F: 06 378 8780**

#### Offices Worldwide

Australia, Austria, Bulgaria,  
Botswana, Canada, Egypt,  
Ghana, Greece, Hong Kong,  
India, Kenya, Kuwait,  
Malaysia, Mexico,  
Netherlands, New Zealand,  
Nigeria, Portugal, Republic of  
Ireland, Romania, Singapore,  
South Africa, Spain, United  
Kingdom, United States of  
America

#### International Website

www.comptroub.com

Computer Troubleshooters  
The World's #1 computer  
service franchise network

OVER  
**450**  
LOCATIONS WORLDWIDE



## Global Newsletter November 2007

### The Password Is ...

Passwords are your keys to accessing electronically stored information. In many cases you may not notice until it is too late that important details, regarding your identity or your business, have been used. It is critical to create 'strong' passwords and keep them well protected, whilst also being able to remember them.

A strong password is one that appears complex and would be difficult to guess. To achieve this:

**Make it lengthy** - Each character that you add increases the amount of tries needed to correctly guess the password. Your passwords should be at least 8 or more characters in length and can contain multiple words and sometimes spaces.

**Add letters, numbers, and symbols** - A greater variety of characters makes your password harder to guess. Punctuation symbols are very valuable for password strength, including those not found on the upper row of the keyboard (e.g. ? { [ ] ).

**Include words that are easy for you to remember, but difficult for others to guess** - The name of your first pet or your mother's maiden name is easy to remember because it is meaningful to you, but not easy for others to guess.

**Avoid sequences or repeated characters** - "12345678," "222222," "abcdefg," or adjacent letters on your keyboard are common combinations that hackers will try.

**Avoid your name** - Any part of your name, birthday or similar information should be avoided, especially if it is displayed on common identification cards which can be lost or stolen (e.g. your driver's license).

**Avoid using only a single dictionary word** - Hackers use sophisticated computer software that will attempt to guess passwords using multiple language dictionaries, including words spelled backwards, common misspellings, and substitutions.

**Use more than one password** - If any one of the computers or systems using a password is compromised, all of your other information



protected by that same password may be compromised as well. It is critical to use different passwords for different systems.

#### So, for memorable, complex passwords:

-Select a base word that is easy for you to remember. For example, say you once lived in **New York**.

- Add at least one capital letter and either a number or special character e.g. **n3wyorK?**

- Add more words and numbers to create a phrase e.g. **n3wyorK?wascold in '87**

**Store your password safely** - Now you can write down a password hint that reminds you of how your password is constructed. E.g. **c1tY? in winter in the eighties** will remind you to substitute the 3 and K! in the city name, then add the wascold in '87. This would remind you of your password whilst revealing nothing to any roaming eyes.

**Keep your passwords secret** - Treat your passwords with as much care as the information that they protect. Keep your passwords to yourself. Never provide your password via e-mail or based on an e-mail request. Change your passwords regularly, so as a hacker progresses with guessing your password, they have to start their process all over again when you change it.

**Be careful on shared computers** - Computers such as those in Internet cafés and airport lounges should not be used for anything requiring your password, including checking sensitive e-mails or bank transactions. These computers may contain devices or software that can capture your passwords.

**Monitor all password-protected information** - such as your bank statements and online shopping accounts. If you notice any suspicious activity, change all of your passwords immediately and notify any relevant authorities.

Talk to your local Computer Troubleshooter about other security tips and strategies to protect your valuable information.

**Contact your local Computer  
Troubleshooters**

**Steve Colebrooke  
0800 728 768 or 06 378 8770**

