Title:
Best Passwords

Word Count:
358

Summary:
No sane person would ever like someone else reading her email. Or for that matter some other person using her password and breaking into a financial institution. You should, therefore, choose a strong, secure password in such a manner that would be a hard nut to crack for others and easy for you to remember. The more random and mixed-up you make it, the harder it is for others to crack. Mind you, if your password is compromised, the password crackers will even take over your identity.

Keywords:
Best Passwords, Change Passwords, Password Generators, Password Protection

Article Body:
No sane person would ever like someone else reading her email. Or for that matter some other person using her password and breaking into a financial institution. You should, therefore, choose a strong, secure password in such a manner that would be a hard nut to crack for others and easy for you to remember. The more random and mixed-up you make it, the harder it is for others to crack. Mind you, if your password is compromised, the password crackers will even take over your identity.

A password, if too short, is vulnerable to attack if an attacker gets hold of the cryptographic hash of the password. Present-day computers are fast enough to try all alphabetic passwords shorter than seven characters. We can call a password weak if it is short or is a default, or which can be rapidly guessed by searching a subset of all possible passwords such as words in the dictionary, proper names, words based on the user name or common variations on these themes.

On the other hand, a strong password would be sufficiently long, random, or which can be produced only by the user who chose it, so that 'guessing' for it will require too long a time.

For maximum security, the user should follow some simple guidelines:

1) Passwords should preferably be at least 8 characters long and not more than

14.

2) Passwords should contain a mix of numbers, letters, and special characters (%&3ac_ht4@m7).

3) Passwords should not contain a dictionary word from any dictionary, be it French, Spanish, medical, etc.

4) Each password should be different from the user's User-ID and any permutation of that User-ID.

5) New passwords and old passwords should differ by at least 3 characters.

6) Avoid picking names or nicknames of people, pets, or places, or personal information that can be easily found out, such as your birthday, address etc.

7) It’s wise to stay away from common keyboard sequences, such as dfgh678 or abc345 .

8) Never form a password by appending a digit to a word. That can be easily guessed.

9) Avoid writing your password down or storing it on your computer.

10) Never share your password with anyone else.