Too Many Passwords, Too Little Time – How to Create a Strong Password

If you're like many people, you have multiple online accounts serving a variety of purposes. You may have accounts for email, online banking, social networking (at sites like Facebook, MySpace and Twitter), and shopping (at sites like eBay, Amazon, and Craigslist), and many of your other favorite websites may also require a login name and password. Many individuals have between 10 and 20 websites for which they have to remember screen names and passwords. Business persons have even more, sometimes between 50 and 70 websites, since they have additional user names and passwords for business-related accounts.

Most people are now aware of the dangers involved in using the same username and password combinations across multiple sites, yet many still remain lackadaisical about protection. There is a certain temptation to use one password for everything, but it can present a major hazard if someone discovers the password. Some software programs even scour data and identify relevant letter or number combinations. This common technique used by hackers presents a huge risk to the user, depending on how complex the user's passwords are.

Consider this:
The average time it takes for a machine-operated system to discover and reveal your password may be as follows:

Sample Password	Time for Machine to Guess	Password Identity
loginid	0 seconds	Password matching username
elephant	Less than 1 second	Any random word found in dictionary
peter	1 minute	Any common name (even spouse's, etc)
amy66	2 minutes	Any common name or dictionary word with numbers before or after it
Sky15t	4 hours	6 characters using 3 of the 4 character types (upper case, lower case, numbers, and special symbol characters).
EV48op	about 105 hours	6 characters using combination of uppercase, lowercase, and numbers
0Blut91	about 7 months	7 characters using combination of uppercase, lowercase and numbers
Mo88Sty!	150 years	8 characters using all character groups
99+EYE1n2c	More than half a million years	10 characters using all character groups – upper case, lower case, numbers & special symbol characters.

PO Box 19785 – Boulder, CO 80308-2785 / 877-878-6798 / service@wordsecure.com

Note that the example passwords used above and elsewhere in this document are merely examples. DO NOT USE THEM! The mere fact that they are published here means they are likely already in a database of passwords used by hackers.

The reason people often use simple passwords is so they will be easier to remember. A common mistake is choosing words that can be found in the dictionary or common first names as passwords. These become subject to what are called 'dictionary attacks' where the hacker uses a computer program to try passwords from a database of words.

Using simple passwords containing personal information also makes it easier for hackers to figure out your password with a little bit of research. One famous public figure's non-secure Yahoo email account was hacked by a high school student in 2008 because the student was able to use Google to get personal information about the celebrity and use it to figure out the celebrity's password. Things like your birthday, zip code, pets' or children's names or social security number provide no protection against common 'social engineering' practices used to guess your passwords.

Creating Strong Passwords

One measure you can take to create effective passwords you can remember is this: Pick a set of lyrics from a song you like, such as the "Star Spangled Banner". Take the first letter of each word in a given set of lyrics and use it to begin building your password. The lyrics "*Oh say can you see, by the dawn's early light?*" would become:

OSCYSBTDEL

Good start for a password! There is no personally relevant information here, nor can it be found in the dictionary (until it is published on the web, which it has been in this case). Now mix the case of the letters, which increases the protection of the password exponentially:

OscYsBTdeL

Now enhance the security even further by adding numbers or random special characters to the password. Avoid trying to substitute a number 3 for a letter E or a 5 for an S or a 1 for an L. This technique was once commonly used but no longer provides secure protection due to the prevalence of dictionary attacks.

Os6cYsBT#deL

Voila! You now have a very strong password you can remember with a little practice. Also, make sure the password you use is actually easy to type. If it is not and you have trouble even once you know the password, change it to something easier to type, while still doing your best to maintain the password's strength.