Introduction

Creating strong passwords may seem daunting, especially when you have many online accounts you need to protect. Anyone would be intimidated if they had to create and memorize multiple passwords like **Wt4e-79P-B13^qS**.

As a result, you may be using just one password for all your accounts. Or maybe you follow best practices and do use multiple passwords, but they are all short, simple words that could be easily guessed by a hacker. If so, your password is still at risk of being compromised. Even if you are taking the right steps by using multiple passwords that are hard to guess, if you write them down, you are still exposing your password to compromise if someone finds your list.

By examining the following examples of weak passwords, you will understand why they put you at risk:

- **Password** - The word "Password" and "12345" are among the most commonly used passwords - as are "default" and "blank." These are simple words that are easily guessed.
- **Marshall1968** - Although this uses 12 characters and includes letters and numbers – which is good – names that are associated with you or your family, or references to other identifying information such as birth year, are easily guessed.
- **F1avoR** - Though it mixes letters and numbers, it is too short and substituting the number 1 for the letter l is also easy to guess.

So...What Can You Do?

So what can you do? The key aspects of a strong password are: length (6 characters are good, 9 characters are better); a mix of letters (upper and lower case), numbers, and symbols; no references to your personal information; and no dictionary words (English or foreign). The good news is you don't have to memorize strings of random letters, numbers and symbols in order to create a strong password. You simply need a few tricks. Using these techniques below, you can create strong passwords that you'll actually remember. In fact, creating them can actually be fun, and your payoff is improved security.

Use a phrase and incorporate shortcut codes or acronyms. These examples let you use phrases that either mean something to you, or you associate with a type of website.

- **2BorNot2B** (To be or not to be – from Shakespeare)
- **L8r_L8rNot2d@y** (Later, later, not today - from a childrens kids rhyme)
- **4Skor&7yrs@go** (Four score and seven years ago - from the Gettysburg Address)
- **14A&A41dumaS** (one for all and all for 1 - from The Three Musketeers, by Dumas)

Use passwords with common elements, but customized to specific sites. These examples tell a story using a consistent style, so if you know how you write the first sections, and you're on the login page for a site, you'll know what to add.

- **ABT2_uz_AMZ!** (About to use Amazon)
- **ABT2_uz_BoA!** (About to use Bank of America)
- **Pwrd4Acct-$$** (Password for account at bank)
- **Pwrd4Acct-Fb** (Password for account at Facebook)

Play with your keyboard. You don't have to think of it just as the numbers you see, it can also be a canvas to draw on.

- **1qazdrfvgy7** is really hard to remember unless you know that typing these on a keyboard creates a "W" pattern -that's a lot easier to remember! You can make letters, shapes, and more just by "drawing" on the keyboard.

  Be careful not to use straight row patterns like "Asdfgh" since these types of patterns have been established as easy to guess passwords.

Add emoticons. While some websites limit the types of symbols you can use, many allow a wide range. Make your symbols memorable by turning them into smiley faces for example, to instantly boost your password power.

Commonly allowed symbols:

```
! " # $ % & ' ( ) * + , - . / :
; < = > ? [ \ ] ^ _ ` { | } ~
```

You Too Can Create Passwords

- C?U2canCRE8Pwords

  See? You too can create passwords.

You're now ready to create your own system for selecting strong, memorable mixed-character passwords using one or more of these tricks. Share these tips with others; but remember, don't share your passwords!

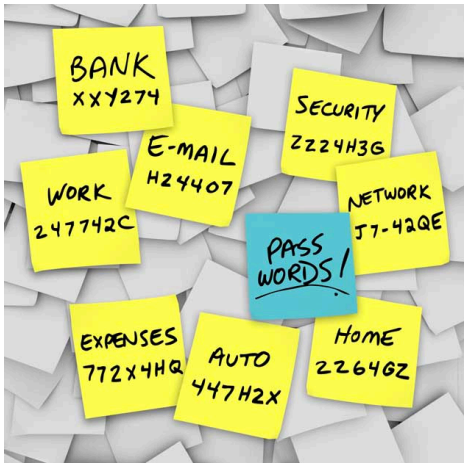
For More Information

- MS-ISAC Newsletters: www.msisac.cisecurity.org/newsletters/
- MS-ISAC Daily Tips: http://msisac.cisecurity.org/daily-tips/
- SANS Ouch Newsletters: http://www.securingthehuman.org/resources/newsletters/ouch/
- Stay Safe Online: http://www.staysafeonline.org/stay-safe-online/
- STOP. THINK. CONNECT – Tips and Advice: http://stopthinkconnect.org/tips-and-advice/

MS-ISAC

MULTI-STATE Information Sharing & Analysis Center™

www.cisecurity.org
contact@cisecurity.org
(518) 880-0699



Smarter Online = Safer Online

Easy Tricks for Creating a Strong Password

CENTER FOR INTERNET SECURITY®

William F. Pelgrin
President and CEO
www.cisecurity.org