How to Write Good Passwords

A good password isn't a password at all. Instead, it's a system for creating codes that are easy to remember but hard to crack.

by Sarah D. Scalet, CSO
December 01, 2005

A good password isn't a password at all. Instead, it's a system for creating codes that are easy to remember but hard to crack. And by codes we do mean codes, plural, so that someone who finds out one of your passwords won't know them all. Here's one methodology to help you generate unguessable but memorable gibberish.

Step 1: Choose a core phrase. Start with a phrase that's at least five words long. It could be the first line of a song, a quotation, a book title - anything that sticks in your head. Draw your core password from that, perhaps by using the first letter of each word:

tcith

These are the first letters of the book title "The Cat in the Hat," for example.

The payoff: This simple step protects you from someone who is running what's called a dictionary attack, in which every single word in the dictionary (and many proper names too) are tried until the right one is found. Computers can run through a dictionary attack in no time flat.

Step 2: Replace some lowercase letters with capital letters, numbers or symbols. Now mix things up by creating conventions around letters that you'll always make uppercase or change to symbols or numbers. Do what makes sense to you, so you don't have to write your system down:

Tc!tH

Here, we've capitalized the first and last letters of the phrase, and replaced an "i" with an exclamation point. You could also make "@" stand in for "a," "1" stand in for "l," and so on.

The payoff: This step exponentially increases the amount of time it takes for someone who is running a password-cracking program that burns through every possible combination of characters until it finds the right one. Rather than guessing from the 26 lowercase letters on the keyboard, the program has to try 52 uppercase and lowercase letters, plus 10 digits and at least 10 more punctuation marks.

Step 3: Customize the password for each site or application. You can use the same core password multiple times, but add a character or three to ensure that every passphrase includes a number, and also that the passphrase is at least seven characters long. To get there, think up a system for generating an extra letter and number based on the name of the website or program you're accessing.

o5Tc!tH

Assuming that the password is for a Yahoo webmail account, we've added an "o" - for the last letter of Yahoo - and a 5, for the number of letters in Yahoo.

The payoff: We started with a password of five lowercase letters, which has 11,881,376 variations (26 to the fifth power, for math wonks). After step three, our password has more than 10 trillion combinations of characters (72 to the seventh power). Even a desktop computer that can guess a million passwords per second will need more than three months to run through all those possibilities.

Step 4: Write down your hint. As long as you understand your methodology and rules, now you can write down a mnemonic device that will jog your memory without being obvious to anyone else. You should still keep this piece of paper hidden, though. Author and security expert Bruce Schneier recommends keeping actual passwords on a piece of paper in your wallet, because you guard it closely and know when it goes missing. Keeping hints there should be even safer. This would be enough to make us remember that we used the title "The Cat in the Hat" to generate our basic password.

Step 5: Repeat. While you can use the same core phrase for multiple accounts, make sure that you establish different levels of passwords. You could use the same core phrase for all accounts that don't involve financial information, another one for accounts where you've used your credit card number and a third for online banking. In an ideal world, passwords should be changed at least every 90 days. But most of us would be doing pretty well if we changed them whenever daylight-saving time starts and stops.