

How Long Would It Really Take To Crack Your “Strong” Password?

How many @’s, %’s and other crazy symbols are in your password right now? Are they really all that necessary? According to a recent Carnegie Mellon study, the answer is no. The only thing that really influences your password strength is its length! Not whether it has X minimum characters or Y maximum characters. And not whether it has a kazillion combinations of numbers, letters and other doodads that are bound to confuse most anyone.

Regular Password Changes Decrease Security

In the recent past, regularly scheduled password changes were a common friend of network security. However, with most computer users now requiring upwards of 20-30 passwords between work and home, this whole password security game has gotten a bit out of control. When pressed to change their password regularly, your users start to use “sucky” passwords pretty quickly because they need something that is easy to remember. Or just as bad, they create a good password and then write it on a sticky note to put on their computer monitor so they don’t forget!

How To Choose A Strong Password

You want to choose a password that is hard for anyone to guess. Ideally you would want to use a lengthy string of letters, numbers and odd characters AND still be able to remember it easily. One way to do this is by creating a random phrase and using the first letter of every word, substituting +’s or &’s for the word “and” or numbers like 4 for the word “for” (or any similar tricks that are easy for you to remember). As an example, the phrase “I love my computer guys and they are the best company for me!” would translate to a password of “ilmcg+trtbc4m.” That’s easy to remember and almost impossible to crack. In fact, you can test out your password at http://passfault.appspot.com/password_strength.html to see just how strong it really is. The password we created above would take 1,306,628,104 centuries to crack.... Now that’s a strong password!

Using A Password Management Solution

Even if you have a strong password, you should never use the same password on different websites. Your online banking password should be different than Facebook, which should be different than Gmail, which should be different than your network password at work. A quick and easy way to remember all of these unique strong passwords is to use a “Password Management Solution.” A few of the most popular tools you can test out are KeePass, RoboForm and AnyPassword. These tools allow you to securely keep track of all of your passwords while remembering only one.