



Password Security

By Mark Bella

Your computer and online accounts contain much of your personal information. If a criminal steals this information they can use it to make purchases, apply for credit cards, etc. Passwords are a key component in securing your personal information. Many people have passwords on their accounts, but are still victims of identity theft. One of the reasons for this is because most people use weak password. A weak password is classified as being less than 8 characters in length, a common word or name or password that is easily guessed such as 1234, password or asdf.¹

There are many tools available that are used to crack passwords. Many of these tools have multiple methods to crack passwords in a matter of seconds. The most common method is by using a dictionary attack, which goes through a series of common words and names to crack the password. This often works because common words or names are used as passwords. Another method is a hybrid attack. This method uses words and names as in the dictionary attack, but adds numbers and symbols.² For example, if the tool is using the word "orange" if that fails it would try a variation such as "orange1" and if that fails then it would use "orange2" and so forth. Another method used is a brute force attack. This is the most comprehensive method, but also takes the longest. A brute force attack goes through every possible combination of numbers, letters and symbols. A brute force attack can take seconds to years to crack a password depending on how secure your password is.

In order to protect yourself from these attacks it's important to increase the security of your password. A strong password consists of being at least 8 characters long and contains uppercase letters, lowercase letters, numbers and symbols. If someone is attempting to crack your password with a dictionary attack, chances are they will fail. Hybrid and brute force attacks have a chance to succeed in cracking your password, but by adding uppercase letters, lowercase letters, numbers and symbols, you have significantly increased the amount of time it will take to crack your password.

As stated before a weak password contains all lowercase letters and is less than 8 characters in length. Mathematically speaking, a 6 character password would equate to $26^6 = 308.9$ million possible combinations. The number of combinations may seem like a lot, but a password cracking tool can handle anywhere between 10,000 to 1,000,000,000 passwords per second, with the primary limitation being CPU speed.³ With a modern desktop computer, a

¹ Microsoft – <http://www.microsoft.com>

² Last Bit – <http://www.lastbit.com>

³ Lock Down - <http://www.lockdown.co.uk>



weak password can be cracked in about 30 seconds. Adding complexity by including uppercase letters will increase the possible combinations to 52^6 or about 19 billion possible combinations and will increase the time to crack your password to about 33 minutes. Now if a strong password is used, our total number of possible combinations is 96^8 or about 7.2 Quadrillion. This would take someone up to 23 years to attempt all possible combinations.

Another method of producing a password that is stronger than a complex password is known as a passphrase. Passphrases are typically a string of words or a sentence at least 14 characters in length. They are easier to remember than a complex password. Assuming that spaces are used and no uppercase letters are used, a 14 character pass phrase would produce about 109 Quintillion different possible combinations. This would take a brute force attack up to 477,895 years to attempt all possible combinations. If letter casing and symbols are used, the amount of possible combinations increases exponentially.

With passphrases being a more secure method of producing a password, it hasn't been implemented in many places due a couple of reasons. The first reason is due to the length of passphrases, there is a greater chance that a typographical error will occur when the user is entering their password. In many cases after several failed attempts the account will be locked out. According to the Microsoft Incident Response Team, unlocking an account produces an average cost of \$70. The second reason is application compatibility. Applications such as Microsoft's LAN Manager can only encrypt passwords up to 14 characters in length and is required in order to be backwards compatible with older applications.⁴

To address the issue in regards to account lockout producing IT expenses, it has been recommended that account lockout policies be disabled. The reasoning for this is because passphrases have a high number of possible password combinations that it would take an extensive amount of time to crack. Combined with a policy that forces users to change their passwords regularly, it would ensure a user's password is safe from being cracked. In regards to application compatibility, applications will need to be either be upgraded or phased out in order to support longer passwords. This may not be an option because of the expense associated with upgrades. In the event that passphrases cannot be used, it's recommended that complex passwords are used instead.

⁴ Microsoft – <http://www.microsoft.com>