PASSWORDS

Things you should know and understand about passwords.

In today's world of digital security, everyone has to deal with passwords. They need to create them, remember then and occasionally change them. With so much relying on passwords and the security they offer, it's amazing how little most of us know about them. This little info-bit will try and shed some light on passwords.

Firstly, passwords are not PIN's and passwords do not need to be "words", they can be phrases or sentences.

A PIN is a Personal Identity Number and is usually limited in length from 1 to 10 numeric digits only. Each additional digit increases it's complexity by an order of magnitude or power of ten. One digit has ten possible combinations (0-9). Two digits has 100 possible combinations (00-99). Adding another digit just multiplies the complexity by ten.

I'm sure you're getting a picture now of how complex a password is in comparison to a PIN. Although, using "brute force" alone (guessing random or simply going through all possible combinations of a four digit PIN code) would still take some time, most every system using PIN's make's that impossible by implementing a "lock-out" function after a set number of tries. Fail the PIN entry three times and you're locked out. Sound familiar?

Because passwords are potentially far more complex than PIN's, less use of lock-outs are made and the "brute force" option of cracking it becomes a real possibility. Some systems like Windows implement's short delays on the fourth or fifth failed attempt, so it will still take a very long time to crack, but even without the delay, it's an extremely difficult thing to do, to crack a good password.

So secondly and most importantly, let's examine password complexity. If each digit in a PIN had ten possible combinations, then strictly speaking, including all possible characters a computer can deal with in one simple character set, the possibilities are 256 per character in your password. Now that sounds good in principal but the reality is that some of the character set, referred to as "ASCII" (American Standard Code for Information Interchange, and pronounced "Askey"), are actually reserved for special functions and cannot be represented in a password. An example is a "Carriage Return" generated by the "Enter" key.

Since the original development of ASCII, there has been any number of variations and additions to allow for bigger and bigger tables. That being said, let's isolate ourselves to what is easily available to you on a standard keyboard to type a password, because any hacker will limit a brute-force attack to those characters only.

The full keyboard provides 48 characters and by using the “Shift” key you can double that to 96. That means that every character added result in a x96 multiplier effect on possible combinations. So a one character password has 96 possible combinations and a two character password has 9216 possible combinations.

Now before you get too excited, this does not mean it would take 9216 attempts to find your two character password. Someone trying to crack it starting with “``” would only take 98 tries to get your password “11”, but 9313 if there was just one more character “111”.

So the difference between 98 and 9313 is quite a lot when it comes to your friend typing on your keyboard trying to hack your password, but for a computer it’s the difference between .00001 seconds and .0001 seconds. To you and me, that’s nothing at all. So let’s look at how we can protect against a computer that can try 100000 attempts per second.

The solution is simpler than you think. Just make the password longer. Remember, each extra character makes it 96 times more complex. So let’s look at some examples…

2 characters ?? = 9216 combinations
10 characters ?????????? = 66483263599150104576 combinations

So, with a computer trying 100000 combinations per second it would take 21 million years to test all combinations. If you used every computer in the world on the job you could cut that to 1 week. Add just one more character and it would take every computer in the world working on the problem 24 hours a day over 2 years. Add another character and it’s essentially uncrackable.

The final thing to know is that the “unknown quantity” makes it impossible for someone trying to crack a code to know if you used an upper or lower case, a number or an asterisk. Because they can’t know this, every possibility has to be tested, so the passwords “fred”, “FRED”, “Fred”, “fReD” and “fR3d” are equally complex. No one has any realistic advantage over the other. The real advantage is in length. “fred nurk” is 8 billion times more difficult to crack than “fred”.

So what to take away from this little info-bit. To make your passwords difficult to crack, make them long. An easy way to make them long is use a phrase or sentence you can remember easily.

“My dogs name is Butch” =
more than 4000000000000000000000000000000000000000 possible combinations. Big number!