CHOOSING AND USING SECURE PASSWORDS

Since the Arabian nights “Open Sesame,” passwords have been used to control access to restricted areas. Computer systems generally use a username/password combination – the username tells the computer who you are, and the password is the shared secret that only you and the computer system both know. By giving both, you gain access to the parts of the system you have been permitted to use.

If someone else discovers your password and username, they can access the computer system and do anything you could to it, all in your name.

These days most people understand that computer security is of great importance.

Too many passwords

The number of times we are now faced with the task of choosing a password has grown huge. Every conceivable interaction on the web seems to require a password secured login.

With so many situations in which a password is requested, it become increasingly difficult to remember which password to use on each of them.

Too complex passwords

This task is made more difficult as more systems insist we use passwords that are more complex.

A common method used by those who want to break into a secure system is what is known as a brute force attack. This means trying every possible combination of letters up to a certain length to login until one is found that works. The shorter the password, the smaller the number of possible combinations there are to try before you hit on the right one. So most times you are asked to choose a password, it must be over a certain length.

Another way of making these brute force attacks more difficult is to increase the number of possible characters in the combination. Adding numbers and characters such as ?, !, #, & and spaces to a password means the ne’er do wells have to try even more combinations. MiXiNg cases also helps, as most password systems will count capital letters as different to their lower case counterparts, increasing the number of possible combinations.

As you can see, secure passwords have to be longer and stranger – which unfortunately means harder to remember.

Choosing passwords

More sophisticated brute force attacks, called dictionary attacks, use lists of words that are commonly used in passwords rather than changing one character at a time. These lists might include every word in the English dictionary or a foreign language, meaning even rare words are not as secure as you might think.

A better approach is to think of pass phrases rather than passwords. A phrase can be as memorable as a word, but much longer, and far less likely to be guessed or broken by brute force.

Some people also use numbers in place of some letters. For example, 3 is often used instead of the letter E because it looks similar. Beware that dictionary attack lists often include words where this method has been used.

More passwords are better than one

A common approach to the problem of needing to use complicated passwords or pass phrases is to come up with one you can easily remember, and use this everywhere. Many people will add numbers to the end of the password if a system requires it is changed regularly.

Consider the damage that could be done across your life if someone found out your one single password – what would they have access to you, and what havoc could they wreak? Even if you change the number at the end, they might only have to try a few possible variations before successfully breaking into your system.

A truly secure password or pass phrase is used for only one purpose and cannot easily be guessed, even if the guesser knows another of your passwords.

Managing your passwords

So you need to have lots of hard to guess (and hard to remember passwords) or phrases. How can you manage this effectively so you don't struggle to get into your own systems? The following steps outline a method for simplifying how you use passwords whilst maintaining your security.

Reduce the number of passwords you must remember

One password is not enough, but do you really need a different password for every occasion? This might sound contrary to what I have been saying, but the answer is "probably not"!

The basis of this system is asking yourself how important security is for each situation in which you are asked to come up with a password.

When security is not important

There are many times when you are asked to give a password where you ask – what is in it for me? Some websites require you register in order to view content that is other wise free. How concerned are you about someone else logging in as you and viewing this content in your name? Why would someone bother? It is easy to see that security is not of great importance to you in such situations. In these cases, it is fine to use the same simple password for all such cases.

Wow – that's probably a large percentage of times you need passwords covered.

When security is fairly important, but not critical

A further level of security can be attained by coming up with a much harder to guess password to use in situations where security is a bit more important. Perhaps you frequent web-based forums where someone else impersonating you would be embarrassing.

In such cases, you should probably rethink passwords as pass phrases. A sentence is a lot harder to guess than a word, yet often just as easy to remember.

Come up with a handful of these pass phrases for times where security is important to you, but not critical.

When security is of absolute importance

In situations where security is of the utmost importance, it is important to go for the most secure passwords.

The most secure password is unique to the purpose it is used for – this generally means a randomly generated string of characters that has no meaning. An attacker would have to try every combination of characters in order to find out the correct one.

The problem with these passwords is first how to come up with them, and then how to remember them.

A variety of websites will help you come up with random passwords – Security Guide for Windows has a Password Generator that allows you to specify the length and complexity of passwords. DataDefender recommends, in its articleChoosing A Strong Password, using the first letters of a phrase that means something to you followed by a random word and optionally using a non-alphabet character in place of a letter.

Remembering these passwords is a greater challenge. Really complex passwords defy memorising for those of us without photographic memories, so you will need to record them somewhere. This is where password management tools come in handy. A number of password managers for web browsers are

available that will securely store passwords and even fill your username and password on the appropriate website. These are usually secured by a master password (make this a secure one that you can remember!) Mozilla Firefoxhas a built in password manager included, whilst users of Internet Explorer can download RoboForm as an add-in – the free version will store up to ten passwords.

These web password managers aren't much use for passwords used other than on the web. In these cases, a tool like security guru Bruce Schneier's Password Safe is a good option. Password Safe stores passwords very safely behind a master password (Schneier wrote the textbook on encryption, so you can be sure this is as good as it gets), and will generate complex random passwords for you.

Be aware that when using these tools if you forget your master password, everything else is lost too.

Microsoft security guru Jesper Johansson has advocated writing passwords down on paper and storing them securely. Secure storage in this case means putting them in your purse or wallet – not writing them on a post-it note stuck on your*monitor*. Also, don't write the purpose of the password, or the username next to it – in the unlikely event that someone steals your password list it would be like handing them the keys to your car, telling them the number plate and where it was parked.

Good password selection and management means you can keep your systems secure without getting a headache trying to remember hundreds of different passwords.

Source : http://www.ictknowledgebase.org.uk/choosingpasswords