Passwords and Password Generation.

The title of this post is always going to be in the news as far too many of you forget that where ever you go on the internet the bad guys are out there and after you and your information **in particular your passwords and login details**.

In the last month or so there have been security breaches over at **LinkedIn and it was reported that Facebook** come under a sustained attack a while ago. Fact is this will continue and you have to protect yourself.

So what to do? Let me outline for you a simple set of solutions that will keep you out of trouble and provide unbreakable security (well close).

Over at the offices of Richard Smith we take data **protection seriously and encrypt all of our data using a couple of simple tools and a Yubikey** which generates either a random string of numbers/letters or a fixed string dependent on how you set it up. But it's another process to worry about and some of you just don't need that level of protection – there is another way.

The purpose of this very short article is not to give you chapter and verse on your options, even if you have the time I know you will just get bored with my techno speak about passwords.

So here is

Richard Smith's Guide To Extremely Safe Passwords.

Firstly make them long, **the longer the better**. The longer your password the longer it will take for someone to guess it by brute force cracking or by using a password generator.

You also need to be putting a **little bit of YOU in your passwords** so this short post will help. For the techies out there looking to pull the post to pieces, yes I know I skimmed a couple of bits.

Let me explain.

If we select the password as richard (note that you will often need a user name and a password and you should always make it a bit complex, not an email address).

Back to richard.

How long do you think it will take to crack that as a password?

The times below assume that the attempt is made using something other than a dictionary/name attack. Often the computer programme used to break into websites contains all of the words in a dictionary and then a name book and repeated attempts are made guessing the password. It also tries 123456 and password first!

Still can't believe these are often used passwords still!

Further still for some reason login attempts are not limited by many internet sites which means attempts can be made time and time again.

So how long would it take to crack richard?

(all times are supplied by Steve Gibson).
3.19 months Offline Fast Attack Scenario:
0.0835 seconds Massive Cracking Array Scenario:
0.0000835 seconds at one hundred trillion guesses per second.

Back to the password.

By adding some numbers to my name richard123

Getting better now.
43.05 thousand centuries Offline Fast Attack Scenario:
2.24 weeks Massive Cracking Array Scenario:
22.56 minutes at one hundred trillion guesses per second.

Which is a worthy increase.

By adding an underscore, now richard_1234
3.76 billion centuries

37.58 centuries

3.76 years at 100…….

Seems now we are getting somewhere, who has this kind of time. GCHQ maybe.

You should have my point by now, the shorter the password is the less time t will take to crack. But there is a problem with longer passwords in that you need to remember them and often they are just too long to remember.

There is an easier way – damn long password plus a little something,

Now I make this easy for myself.

It is possible to pop over to http://www.random.org/passwords/ generate a very long random password indeed.

Here is one I generated earlier.

wkwEgdLrzHJWTkQ

Now that should be acceptable for most website hosts. Problem is you still can't remember it.

For those of you that can you should also throw in a few .?>! or whatever other characters are allowed.

Now when we compare the break in attempts.

Online Attack Scenario:
17.82 trillion centuries

1.78 hundred thousand centuries no need for the last calculation honestly.

Now that's a little better, kind of uncrackable or at least the bed guys would have moved on by now hopefully.

Long passwords make sense.

The key is how to remember them.

Well if you add some data to this random string it is possible to create a very powerful password that you can alter to suit.

A simple example would be this.

Take the random string and store this inside a normal .txt file on your computer. Then email it to yourself for extra security (assuming your email is backed up).

You can now get creative with your password.

You should have s**eparate logins for all of your accounts.**

By combing a very long text string (something you have) with something you know now this starts to become interesting.

For example below are some attempts using my random string.

House Number/ Car Registration

21wkwEgdLrzHJWTkQLGU11VHD

Pin/Housenumber
3244wkwEgdLrzHJWTkQ46

Dogs Name/Pin
PetuniawkwEgdLrzHJWTkQ3244

You can randomise these passwords for different logins and if required write these down whoever sees these written down will be thinking great they now have the passwords for all of the family silver. Only there is more to come.

For example

Online Banking
Dogs Name

Facebook
Car Registration

Email
House Number

It will be possible to use the house number at the front of your password, and you can document this wherever you like. The rest of the information (the random number) can be hidden within a text file on your hard drive .

It matters not that you have made a note of it as not many people are going to work it out and without the long number it's useless.

Now we introduce some that you know.

So.

Your Online banking could be the Dogs Name + The Long Key + Banking Pin

How long do think it would take to for someone to guess that? A while I think, even if they were looking on your computer for a .txt

file (on windows machine there are normally hundreds). Importantly you have not had to rely on your memory and created something that is going to be hard to crack.

Other alternatives are to use plugins like Lastpass but this does mean giving up some information to a third party which will either work for you or not.

For those of you wishing to provide a bit more security you can use locknote (for Windows) Free of Charge (not sure of anything similar for the Mac but you can certainly use Truecrypt to create a secure area on your hard drive/server.

You could also install Lastpass (Google it).

I hope this helps you sort out this password problem once and for all. If you would like me to provide a short walk through (Video) of how to do this please be sure to leave a comment.

Richard Smith

0845 226 9106

PS if you get stuck then please call.