



Series 5 – How Do I Access the Internet, Securely?

Welcome back to a series of computer related articles brought to you by VistaSol Computer Solutions. Over the coming weeks we are going to be featuring articles based on the theme of 'How do I . . .?'

This week we're continuing our series of articles on the subject of 'How Do I Access the Internet' by offering some advice on how to keep yourself secure. In our previous article we looked at the Windows Firewall. In this article I'd like to give you some advice about passwords and password security.

Part 3 – Passwords

Password Protection

Password protection is a very serious subject and should never be taken lightly – it's as much about making the password difficult to guess as it is about making it easy to remember!

Perhaps that sounds like an unreasonable statement, but let me explain my reasoning behind this. Passwords should consist of eight or more characters; most people choose a password based around a word which will be easy to remember, however they don't necessarily consider how easy this will be for someone, with ill intent, to guess.

What makes a Bad password?

I suppose the best place to start, is with what we consider to be bad choices for passwords, so here's a selection of the ones you really should not use:

12345678 – There are at least 12345678 reasons why this password is unacceptable!

qwertyui – For the same reason above because these make up the first eight characters across the top row of your keyboard.

Your birthday/anniversary/child's name – anything directly associated with you should not be used for passwords. It really doesn't take many guesses to realise your password is your first-born's middle name, especially if that's detailed on facebook.

dalglis – Ah yes, you're a Liverpool fan. Try not to use passwords associated with things you like - with the advent of social networking sites they are very easy to figure out.

What makes a Good password?

When thinking about a password please follow these guidelines:

- a. Make your password at least **eight characters** long, longer is better!
- b. Mix it up and add **numbers** and **letters**.
- c. Also include **special characters** such as *, &, or %
- d. Utilise **UPPER** and **lower** case letters

So, if you really must use your partner, spouse, or child's name; add some, or better still, all of the suggestions above.

Let's say your cat's name is "mouse racer" and you're thinking of using that as your password, an example of adding these combinations may finish up looking something like this: **M0us&R4cer**.

Don't use that one, obviously, but if you use one like it then you'll be ticking all the right boxes. I accept that this will make your passwords more difficult to remember, but it's definitely going to be difficult to 'crack'. Talking of which, criminals will use things such as "password crackers" or software programs that can very quickly guess a password by attempting many different combinations very quickly. By following our rules above and adding numbers, upper case letters and special characters, your password will become very difficult to 'crack' and often results in these criminals moving on to easier prey.

Email Hacking

A problem, which we come across all too regularly, is when our customers tell us that their friends and relatives are receiving spam emails from them. This is nearly always because some malicious individual has discovered their email address (most commonly hotmail addresses), and has then run a 'password cracker' program to discover their password. The email account can then be accessed and because the perpetrator now has access to all 'Contacts' in that account's address book, he (or she) can also run their password cracker against each of these contacts – before you know it, they now have many more email accounts they can use! In almost all cases, this is because those individuals have not followed the rules above when choosing their passwords.

If you find that you are ever a victim of this kind of 'hijacking' – change your password immediately!

Password changes

You should also consider changing your passwords on a regular basis; once every couple of months is recommended.

Multiple passwords

We need passwords for almost everything; from social networking sites to mobile phones. Because of this, there is a strong temptation to use the same password for everything. But, as simple as this solution may seem, it's this kind of simplicity we're trying to avoid. You should consider maintaining a selection of passwords. Doing this helps spread the risk if one of your passwords is compromised. If you bank online, you should have another completely unique password – the more important the information being protected by your password, the stronger your protection should be.

Keeping secrets

Having the world's most complicated password isn't a great deal of use if someone can easily find out what it is. Be sure you do the following:

- Don't write your password down on a piece of paper near your computer.

- Don't keep banking passwords or PINs in your wallet/purse.

- Don't keep your passwords stored on your computer.

When you log-in to email accounts etc on your computer, avoid the temptation to allow your browser to "remember" passwords, especially if the computer is shared with other people.

Enjoy your on-line surfing experience, but be safe and think about your security at all times.