Discussion – Viruses Behaving Badly

During the Christmas break I received a number of phone calls from people whose computer would not start. It began to load Windows then stopped with a message. Clicking on the message started the whole process over again. This was obviously an interesting virus which had an unexpected problem.

If the virus had been better written it would not have been nearly so obvious and the callers' computers would have started normally yet still been infected with this virus. The worst part of these calls was telling my callers that I could not fix their problems, and that the only people that I knew who could fix the problem would be on holidays until 14 January: next Monday!

This meant that the unfortunate owners of these problem computers would be without email access, banking access or, indeed, any other sort of access to their computer for a period of up to three weeks.

This is sobering information to all those who feel that their computer is not worth protecting because there is nothing valuable on it. The modern virus writer does not want valuable data from a computer: owning the computer (or the bragging rights for owning the computer) is usually more than enough for the vast majority of computer virus writers.

Some Sobering Statistics

In the beginning there were no computer viruses and the world was all brand-new and shiny. Then came along a series of viruses: the first to come to my attention was the *Stoned* virus which declared *Your computer is stoned!* when a computer was first turned on. This virus appeared at CIT (Chisholm Institute of Technology), now the Caulfield campus of Monash University, in March 1989.

Roger Riordan, a lecturer in Computer Science, wrote a program to remove the Stoned virus from the College's computers. This program was called *Vet*, and Roger gave to the students as shareware. They found it so useful that it was passed on to parents, who then passed it on to their employers. Some more viruses were found at CIT and added to the repertoire of VET. By the end of the year Vet had become so popular that Roger retired from CIT to concentrate on his anti-virus program.

Vet was later bought by Computer Associates (now CA) who have do all updates and sales.

We have now come to the stage in the computer virus writing epidemic where there are more viruses written each year than in all the preceding years. The corollary of all this is that the number of viruses in the wild doubles every year. Not only does the number of viruses double each year but, for the best (or worst) viruses, the quality is getting better (or worse).

This means that you must, if you want to continue using your computer, make sure that you have the best available protection. The best news about this protection is that it is all free! So, even if you are a fully paid-up member of the *I don't need protection* brigade, I still suggest that you download and install the free protection which is available on the internet.

From my experience over the last few weeks, and the experience of my clients (both new and old), the cost of protection is far outweighed by the potential cost of correcting the problems caused by a computer virus.

One type of virus which has recently been upgraded is the ransom note virus. This takes a deceptively simple form: you get an email which states that you have lost access to your data so please pay a ransom to get the key to unlock your data. If you have a current and complete backup of all your data then you can simply wipe your hard disc then reinstall both Windows and all your programs. Then, after installing your programs, it is a simple matter to restore all your data. There: your computer is all brand-new again.

You now have a shiny new computer, complete with all your data snugly in place. Perhaps it is about now that you wonder if the hackers can use the data which they probably stole from your computer. This is the time when you wonder if, or indeed how, you could have protected your data from the catastrophe of falling into the wrong hands.

If you hold sensitive data which could be used to create a false identity then the answer to this question is a definite ***YES!***

How Can I Protect My Computer?

I have spoken on this on many occasions. There are a number of free anti-virus programs which you can download from the internet. The one which I recommend for the vast majority of people is Microsoft's *Security Essentials* for people running Windows XP, Vista and 7. For Windows 8, Microsoft has an updated version of the free *Windows Defender*. This program is essentially a renamed *Security Essentials* so is the same program by another name.

This program is easy to download and install. It is also the easiest anti-virus program that I know to keep up to date. All the other free anti-virus programs which are worth using need to be updated every year and this task appears to be too difficult for many of my clients to do. There are three steps to updating a computer program:

- Know that it needs updating
- Download the update
- Install the downloaded update

Far too many of my clients fall at the first hurdle because they do not read the warning which appears periodically asking them to update the program. For those who do read the warning it seems to be too difficult to know how to download the update, and for those who actually download the update the next step of installing this update is a hurdle too far. For this reason I suggest that people use an anti-virus program which does not need to be updated.

How Can I Protect My Data?

There are many sources of information on the internet about protecting your data. The best way is to encrypt the folders, like *My Documents*, which hold your important files. If you have an accounting program then it is best to encrypt the folder which holds your accounting data files if it is not inside another encrypted folder.

When done correctly, encryption is not noticeable in your daily computing. There is just one extra step needed: enter the encryption key when you start your computer. It is best if your key is not stored on your computer but on an external device. USB memory sticks which are attached to your key ring are perhaps the best way of storing this sort of information.

Further Information

Microsoft Security Essentials www.microsoft.com/mse