Radio Days – 2013-09-14

Tip of the Week – Update Windows

There have been many studies which show that computers whose Windows and programs are patched but have no anti-virus program are less likely to be infected with a virus than a computer with unpatched Windows and programs but a good anti-virus program. This shows me that patching a computer is one of the most important ways of keeping a computer safe from attack.

I was, as you can imagine, horrified to fine a new client with a computer which had not been patched for about five years. He was worried that it was behaving badly – this is why he rang me – so I set about installing all the updates. Fortunately he had a fast internet connection so the downloads only took an hour or two in all. Once all the updates had been installed (and this took a number of download-and-install sequences) the computer started to behave itself.

Please ensure that your computer is set to receive and install updates when they are available. Not installing updates can lead to your computer behaving badly. Not installing updates can also lead to your computer being unable to resist attacks which a patched computer shrugs off. This is like having an excellent diet so that your immune system ensures that you do not catch every winter cold as compared to a diet of fast "foods" so that your immune system allows every passing sniffle, cold and flu to keep you feeling miserable all winter and even into summer.

Do you want your computer to be as healthy as you are?

Unsafe Surfing

Last week I was asked if you should have an anti-virus program on your smartphone or tablet computer. My answer was that it was important if you did potentially dangerous things like internet banking on your device. It turns out that there is a far more subtle reason to be wary of using your smart device on the internet, especially if you do sensitive things like internet banking.

The ABC's Four Corners program on Monday 9 September 2013 talked about the hidden data which is sent by smart devices when they connect to the internet. This program is available on the ABC's iView, and it will expire on Monday 7 October 2013. Also, as I discovered in Vietnam, you cannot view iView programs outside Australia. This is frustrating when I want to catch up on favourite programs when travelling! I suggest that you review this program – or watch it for the first time – if you are at all concerned about who may be doing what with your internet access on your smart device.

I found it fascinating that so much could be done with the signals that your smartphone uses to send data over the internet. It specifically talked about a family which has, like so many other families, a WiFi network at home to connect all their devices to the internet. This is the sort of connection that you may have in your home (I have a WiFi connection at home so that I can use my main computer, my laptop and my phone on the internet at higher speeds than I can get over the phone network) and that you can use when you are surfing at a public hotspot.

These hotspots are available at many locations – hotels, motels, cafes and some small country hamlets like Newstead – and are routinely used without thought by most of the people who go there because it is free.

There are other people who want to go to free hotspots, but for more nefarious reasons!

How Do They Get Your Data?

There are programs, the type is called *packet sniffers*, which are used by computer network technicians to diagnose network errors. They are also used by people who want to steal your personal data. What sort of data can they steal?

This was demonstrated on the program on Four Corners. The network technician hired by the ABC was able to get just about all the information needed to clone your identity. This is called *identity theft* and is increasing both in the number of people who have their identity cloned and in the value of data stolen.

Watch the program and you will see, on screen, the data that the ABC's white-hat technician managed to capture using the family's home WiFi network.

A WiFi network has a range of between ten and thirty metres depending on the surroundings. WiFi networks operate on the frequencies are used by satellite internet connections, and you will know if you have a satellite internet connection that it slows dramatically on cloudy or humid days. This is because water absorbs the signal.

WiFi signals are also absorbed by people (we are, after all, mostly water!) by thick walls and by metal. These signals are designed, like Bluetooth signals, to only work for short distances. This is a great help in preventing interception.

Interception is done with a packet sniffer. All my checking on the internet so far found that the consensus is that Wireshark is the best packet sniffer program. This is a free program and has legal uses for network administrators. It also has illegal uses for those who want to steal your personal data.

Badly-Written Programs

There is an interesting example, in the Four Corners' program, of a badly-written program. This program sends all its data unencrypted over the device's connection to the internet. Once this had been discovered the organisation which produced the program changed it to ensure that all data between the app on your phone and the company was encrypted so that it would be much harder to steal and use to clone your identity.

How do you know what data is being sent from your smart device? The only way that I know is to use a packet-sniffer program like Wireshark to check and see what is travelling over the internet. You may need to be a bit of a nerd to actually interpret the data which a packet-sniffer captures, but it will give you some insight into what is possible in skilled hands.

How Do I Prevent This Data Theft?

About twenty years ago Jeff Kennett, the former Victorian premier, was caught dissing John Howard – then Prime Minister – over his mobile phone. This was an analogue phone, and the old analogue mobile network was easy to bug. Modern phones use the digital network which is encrypted so much more difficult to bug.

This encryption does not stop organisation like the American NSA from intercepting mobile phone traffic but it will stop most other people. There is no such thing as perfect encryption, just as there is no perfect safety in other aspects of life, but it offers the best way of keeping your data safe. This means that you should use the mobile phone network to transport your data if you use WiFi to connect your smart device to the internet. The charges for data are higher, and the speed is slower, but your data is much safer than using WiFi, especially if you are in a public hotspot.

Further Information

Wireshark www.wireshark.org