Radio Days – 2013-02-09

Tip of the Week – Don't Believe Emails

During the week I received a panic call from a client. About a month ago I had installed an updated version of his commercial, and paid-for, anti-virus program. The way to do this was to download and install the trial version of the program. When the program's trial version was installed it automatically recognised the presence of a current version so updated itself to be activated and valid for a further 640 days.

During the download process I had provided my client's email address, as requested, and he kept getting emails stating that his trial version was about to expire. He did not notice that his actual program stated that there were, by now, 609 days until expiry.

The panic started when the latest email from security firm stated that he was no longer safe because the trial period of the anti-virus program had expired. It was at this stage that he panicked and rang me. I soon realised what had happened and put his mind at ease.

What Did I Learn From This?

What I learnt from this episode was that you do not give out a real email addresses when you download a trial version of an anti-virus program to update a current program. This, in many cases, is the only way to get an update for an existing anti-virus program. You often have to give an email address because they will not allow you to download the program without one.

So, if you have to give an email address so that they can send you unwanted, and frightening, emails, it is better to give out an email address like *donald@duck.com* as this is a valid email address. I sent an email to this address (which is now owned by Google!) and it bounced! This means that any anti-virus program which sends an email to *donald@duck.com* will get a bounce message.

This system is automated so it will probably not worry the sender, and it certainly will not worry you because you will not see the message. If, however, all this does worry you, you could try using *minnie@mouse.com* instead. This address works without bouncing.

The joys of being able to think like a feral computer consultant!

An Ounce of Prevention …

During the week I had a call from a long-time listener who had just turned his computer on to discover a message on his screen. The message stated that he owed the Australian Federal Police a sum of money for downloading pornography or copyright music and other articles. The message stated that his computer would be locked until he had paid his "fine".

I have not seen the message myself so cannot vouch for the accuracy of this description, but it is not the sort of message which sends a warm cuddly feeling into one's heart.

My caller thought that this was a scam. He obviously did not understand what a scam is, so let me explain.

What is a Scam?

A scam is an email which purports to send you lots of money at no cost to you. This sounds like a free lunch to me, and we all know that there is no such thing as a free lunch! The first scams were called 419 scams after the section of the Nigerian Criminal Code which prohibited them. They scam works like this:

- You get an email which states that the sender is the widow of a Nigerian general who had amassed a fortune worth some hundreds of millions of dollars and she is asking for your help in getting this money out of the country. In exchange you will be given 10% of the money that is brought safely out of Nigeria.
- You reply that you would be delighted to help in this way.

- You are then asked for a little something to get the ball rolling.
- There are other problems which arise during the course of the scam which need that little extra bit of money (*yours*) to make things happen.

I have heard of one occasion where the scammer did deposit some money, as proof, into the scamee's bank account, but usually it is the other way around.

As an example, a friend was involved in an internet conversation with a lovely West African woman. She had recently graduated from nursing school (she said) and wanted to come to Australia. When I saw her photograph I was amazed at just how young and beautiful she was. After some weeks of talking (both Skype and email) she asked for a little money to get her passport to come to Oz.

I told him that this was an obvious scam because she was only 20 and he was over fifty. He replied that no woman would ever do such a thing! He sent the money requested and, in return, he received a photograph of her West African passport. This is proof of her good intentions, he told me.

I told him that he had been scammed.

She then asked for a larger sum of money, some $2,000, for the return ticket to Australia. We looked up her location on Google maps and then tried to find a return air ticket from there to Australia without success. Eventually we found a way to get from her city to Melbourne by air and it cost about the $2,000 that she had asked for.

I told him that the next demand would be for even more money. He said that I was wrong.

The next demand (oops, request!) was for $5,000. This was needed because the Australian government wanted to see that amount before they issued a visa so that she could prove that she could support herself without working during her stay in Australia. He sent it, and the conversation continued. He was besotted with her until the last moment when she reported that there had been a hitch in her plans and she needed even more money.

At this stage he stopped, refusing to have anything more to do with her.

Now ***that*** is a scam!

The AFP Virus

This is a virus which demands money. I don't know if paying any money will unlock your computer but I suspect not. The only way to get your computer back will be to remove the virus. There are, as usual, removal instructions on the internet but they need you to have access to a uninfected computer. They also need *your* computer to be able to boot from a USB drive: many older computers will not. To see these instructions please go to the website at the bottom of this page and look for a virus with the word *Ucash* in the title.

For many people, these instructions will be too complex to follow so the best option will be to take your computer to a competent virus remover. They will remove your hard disc from your computer and place it in their computer so that it can be scanned with a good anti-virus program or two.

The virus remover will then replace all those parts of Windows which were corrupted when the virus was installed. This is an essential part of virus removal which is often overlooked by those who are not as competent as they purport to be.

This process will take about three days because of all the work involved.

Another option which you could try is to reinstall Windows and all your programs, then restore all your data. Of course, this option should only be considered if you have a current, and complete, backup of all your data and the discs and installation keys of all the programs which you will reinstall. Most people will fall at this hurdle.

I do not recommend this option because every time a client has used it they have lost data.

Prevention

It will be obvious to most of my readers that it is better to try to stop the virus before arrival than to remove it afterwards. The easiest way to do this is to have a current good anti-virus program on your computer.

It is not only necessary to have an anti-virus program on your computer but also to keep it up to date. My caller did have an anti-virus program on his computer but he had managed, as so many people do, to ignore all the warnings about it being out of date. These warnings had been arriving for the last two or three years (he was not quite sure for how long they had been coming) but they were carefully ignored because he did not know what to do.

You, dear listener, will know what to do: you will ring me on 0419-131-459!

This, to my mind, reinforces the need for an anti-virus program which does not need to be updated every year. There is only one program which I know which is both free and does not need to be updated every year and that is Microsoft Security Essentials (MSE). This program can be downloaded from the internet and installed on your computer quickly and easily.

If you do download and install MSE you will probably have to remove your existing anti-virus program. The program that I use for removing other programs is Revo Uninstaller. It is the best uninstall program that I know and I recommend it to you for this purpose.

So, if you are not sure which anti-virus program to use, or your anti-virus program is out of date, please download and install MSE and Revo Uninstaller: install them both then use Revo to uninstall all your other anti-virus programs.

Further Information

Remove AFP Virus	www.malwaretips.com/blogs
Microsoft Security Essentials	www.microsoft.com/mse
Revo Uninstaller	www.revouninstaller.com