

Radio Days – 2011-12-03

Discussion - Scam Phone Calls

While preparing my cheat sheet for a recent radio show, I received a phone call from an Indian woman who promised that she could help me get rid of the problems on my computer. The call went through a number of phases and I will go through them as they happened. A few days later I received another phone call from the same organisation and went through a similar process.

The first step was to convince me that I should listen to them and follow their directions. I said that I was watching the news and asked her to ring back in an hour. She did!!! We then went through the following steps, as she followed her script to convince me that I needed her help. These are the steps:

1. She started by informing me that they had received errors from computers in my vicinity and that these errors were sufficiently serious that they needed to be fixed immediately. The problems which they reported were an infection by the *Malaysian Flu* virus and that this virus would do massive (but unspecified) damage to my computer. I googled this virus and found no evidence that it existed, even as a hoax!
2. She got me to display the *Computer Management* screen and then tried to convince me that the *Warning* and *Error* displays were sufficiently serious that I needed their help to fix these problems.
3. She then got me to display the *assoc* listing to convince me that the warnings which had appeared on their computers had, in fact, come from my computer. There is nothing in their “facts” which “prove” that any warning came from my computer.
4. The final step before the sting was to get me to open their website. This was an almost attractive website with pretty pictures of a blue-eyed blonde wearing a headset and available to fleece me. It was at this stage that the two callers parted company.
5. In the first call she then attempted to get me to buy an unspecified support package. There was some mention of the free version of AVG anti-virus, but this was not displayed on their website. The second caller asked me to allow a technician to take control of me computer. This was when I stopped.

All of the steps above are quite safe for you to follow. Please, however, be careful if you click on either the **Buy** button or the **Remote Support**: both of these options could cost you more than you would like. I do, however, urge you to follow all the preceding steps so that you are familiar with them should you ever get one of these calls.

While all of the above steps purport to show that my computer is infected with the mythical “Malaysian Flu” virus, they do not succeed. They do, however, succeed in convincing a lot of people who are not as fluent in computing as I am that there is a problem. This has to be the case because the scam is continuing.

Please follow these steps as I go through them. It is quite safe to do all of them on your computer: in fact I encourage you to do this so that you will recognise the scam if it comes to a phone near you or someone you know.

Forewarned is forearmed!

The Introduction

While I was writing this report I received my third call (first on Friday 18 November, second on Monday 21 November and third on Wednesday 23 November). The introduction uses long words which sound impressive if you do not listen carefully.

- We are from the extended phase of Windows operating system [sic]
- We help you check your computer by your own self [sic]
- You do not have a wirus [sic] but there are many wiruses [sic] in your area

Years ago I was doing contract work for Honeywell and they produced an excellent Buzz-Phrase Generator. This consisted of three columns of words: to produce a buzz-phrase you selected a word from each column in turn. The acid test was that, if your audience thought they understood the result, it showed that they were absolutely clueless.

This is that good old buzz-phrase generator:

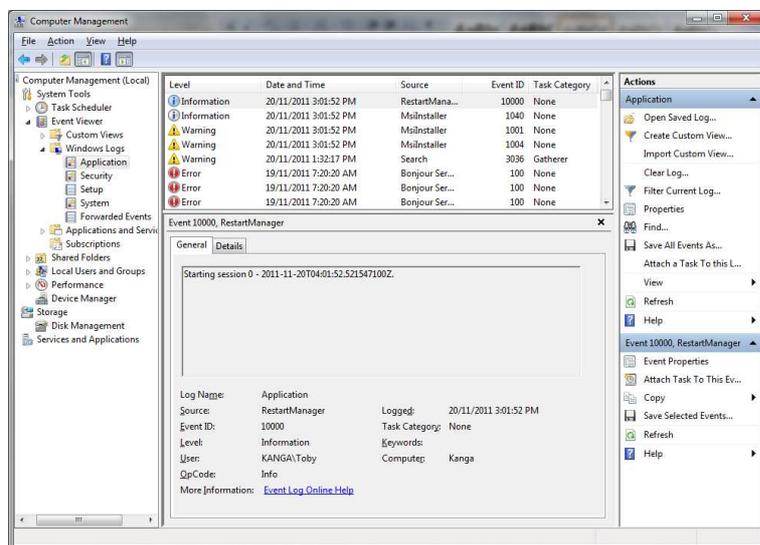
Column One	Column Two	Column Three
integrated	management	options
total	organisational	flexibility
systemised	monitored	capability
parallel	reciprocal	mobility
functional	digital	programming
responsive	logic	concept
optical	transitional	time-phase
synchronised	incremental	projection
compatible	third-generation	hardware
balanced	policy	contingency

Thus you could come up with:

- Compatible digital contingency
- Total transitional projection
- Parallel monitored concept

This version was produced in the 1970s and managed to confuse people then, so the Indians who ring you will have used some more modern version of this buzz-phrase generator and they still manage to confuse you! As the French say: the more things change, the more they stay the same!

My Computer



The first step in the scam is to get you to click on *Start*, and then to right-click on *Computer*. This brings up a context menu (as all right-clicks do).

You will then be asked to click on *Manage* to show *Computer Management*. It shows technical data which most people never see and cannot interpret if they do see. This makes it ideal for confusing those people who are likely to be susceptible to a scam like this one. Please be careful!

This is why I urge you to try these steps so that you can resist

your attacker more easily.

After you have been shown all this screen by your friendly scammer, who is just trying to get you to trust her (or him), you will be asked to agree that your computer has a problem. On one call I was reassured with phrases like:

- We respect your privacy
- We comply with all Australian laws
- We will not ask you to do anything which will damage your computer
- You are in charge every step of the way

This stage aims to convince you that your details really are private and that they really are trying to help you. If only this were true!

The point of this screen, for your scammer, is to convince you that there is a major problem with your computer.

This is nowhere near the truth!

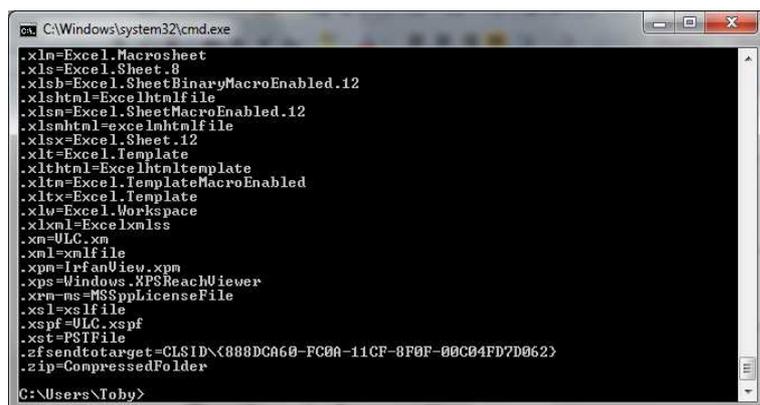
This screen shows what Windows reports in its log files. These log files are there to help very experienced Windows experts diagnose serious errors when they occur. They are also used by scammers to convince you that you have major problems with your computer.

If you fall for this trick you will also want to be assured that the word *gullible* has been removed from the English language. I laughed when my nephew told me about his experience with this furphy, but I am not laughing when I hear about people who have been conned out of more money than they can afford because they chose to believe a slick scammer reading from a script.

The scammer does not know enough about Windows to fool you: they are just doing what their masters have told them to do. This is akin to the people who ring you when you are eating dinner to tell you that you have won the lottery and that you need to send them \$1,000 so that they can start the recovery of your winnings.

This is all part of the modern world which we live in.

Assoc



```

C:\Windows\system32\cmd.exe
.>assoc
. xln=Excel.MacroSheet
. xls=Excel.Sheet
. xlsb=Excel.SheetBinaryMacroEnabled.12
. xlsmhtml=Excelhtmlfile
. xlsm=Excel.SheetMacroEnabled.12
. xlmhtml=excelhtmlfile
. xlsx=Excel.Sheet.12
. xlt=Excel.Template
. xlthtml=Excelhtmltemplate
. xltm=Excel.TemplateMacroEnabled
. xltx=Excel.Template
. xlw=Excel.Workspace
. xlxml=Excel.xmlss
. xnl=ULC.xml
. xnl=xmlfile
. xpn=IrfanView.xpn
. xps=Windows.XPSReachViewer
. xrn=ns-MSSpplLicenseFile
. xls=xlfile
. xpf=ULC.xpf
. xst=PSFile
. zfsendto=arget=CLSID\{888DCA60-FC0A-11CF-8F0F-00C04FD7D062}
. zip=CompressedFolder

C:\Users\Toby>

```

The next step is to convince you that the messages which they get “from your vicinity” are, in fact, from your computer.

They get you to press and hold the *Windows* key then press *R* for *Run*. You then type *cmd* and press *Enter*. This displays a box with a black background and some white writing on it.

You will be asked to type *assoc*. This command has two uses:

- List all file associations. These are a list of all file types on your computer and the program which runs them when you double-click on a file of that type.
- Allow you to change the file association for a particular file type. This can be an excellent way to brick your computer (or your best enemy’s computer!).

You will then be asked to check the third line from the bottom. On my desktop computer you see this screen, but on my laptop there are some more lines after the third one up. They then repeat the long number starting with **888DCA60** to “prove” to you that the messages they are seeing are from your computer. This number is there on *ALL* (repeat *ALL*) Windows computers, so this is just another part of the con.

This reminds me of an incident which happened when I worked in telephone tech support for MYOB last century. I was helping a woman who had rung in and told her what to look for on her screen. She asked, an absolute horror, “Can you see what is on my screen?!?!?!?”

I replied, “No. I have a copy of MYOB open on my screen. It is the same version as yours so we are seeing the same thing. Please do not worry.”

If you stay with them as far as this you may well be the sort of mark that they can fleece, so please be wary of their intentions. Despite your worst fears they cannot see your screen nor can they control your computer. Just do not let them get control: this is the next step!

Website

The next step is to get you to open their website. They do this by asking you to close the screen shown on page 3, then you press *Windows + R*. You will be asked to type their website address: www.wteksupport.com and press Enter. This opens their website in your browser. They will point to the the picture of a smiling woman wearing a headset so you will associate the voice that you are hearing (Indian) with a nice white woman and be reassured that all is well and that you are in good hands.

Nothing could be further from

the truth!

I have so far had three calls. I followed the first two through to their conclusion but hung up on the third as I had done enough research. In both calls the woman told me that she would transfer me to a support specialist who would be able to help me. On both occasions the support specialist asked me to note the “Microsoft certification” on the right hand side of their web page. This is an image which can be copied from many web pages on the internet and has absolutely **NO** meaning here except to reassure that you will be scammed by people who want your trust, and isn't this how all con merchants work?

The first two calls went like this:

1. Much reassurance that they would follow all Australia privacy laws (yeah, right!) so you have nothing to fear. After mind-numbing palaver they asked me to click on the Australian flag which took me to a page where I could buy a support plan. If you click on one of these options you will be asked to give them your payment details. These payments are processed by PayPal and include the usual cards as well as PayPal. This is a good place to stop, if you have got this far.
2. Again there was much reassurance that everything you did would be safe. This time I was asked to click on *Remote Support* on the right hand side of the screen. This takes you to a program called *LogMeIn*. This program is a well-known support program and is used by many reputable organisations to help you in the same way that I use CrossLoop to help some of my clients. You are safe until you enter the pin number which your support specialist will give you. If you do enter this pin and press *Connect to Technician* then all bets are off and you can find that many things are done to your computer without your real permission.

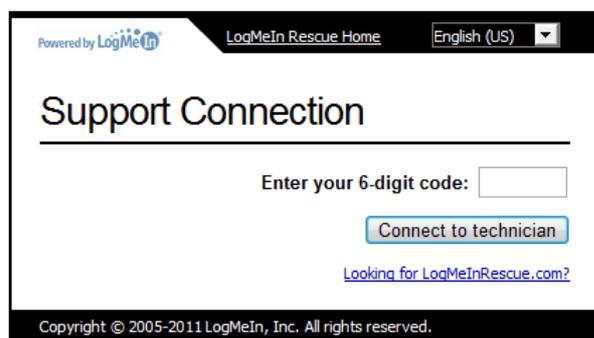
If you have come this far you are on your own because you have only yourself to blame for what happens now. I suspect that you will have a badly infected computer. You will probably also have your credit card maxed out as they fleece you of all your hard-earned readies.

You have been warned!

Up till now, you have done nothing (I repeat **NOTHING**) which can damage your computer. You have wasted an Indian technician's time (and, perhaps, your own time) but as this is just the prelude to the actual scam you have done nothing which can, in any way, damage your computer.

It is only in the next stage that any damage can occur, so please be very careful if you choose to continue past this point.

LogMeIn



This program is used by many technical support companies to help you when you get into trouble. They will ask you to click on a link and then they will be able to fix a problem or show you how to perform a task. Like all tools, LogMeIn can be used both for good and for bad purposes. When used by a person whom you trust, LogMeIn is an excellent tool which can be used to help you learn how to perform a difficult task. It can also be used by people who know what they

are doing to access their home or work computer when they are out of the office. Both of these uses are legitimate uses for this excellent tool.

Your friendly scammer will then ask you to enter their access code into the little box in this window. Please note this states, at the top of the window, that you are accessing *LogMeIn Rescue Home*. If you do enter the access code which their support technician gives you, you have given the technician complete access to your computer. This means that they can do some or all of the following:

- Install their favourite virus on your computer
- Block access to your data until you pay them money
- Search your computer for any signs of banking logins
- Steal confidential data for later use, including blackmail if you are involved in illegal activities
- Access your bank account
- Steal your identity

I hope that I have encouraged you to be very careful if you get this scam. Again, please follow these steps on your computer so that you will recognise them when you get the call.

Again, you have been warned!

Windows Error Reports

While preparing this talk I asked some clients about their experiences with this problem. One question which I had not thought of came up a couple of times. The question people asked is: *Is it safe to send a Windows Error Report, or is this where these people get your name?*

Windows Error Reporting is a service first provided by Microsoft in Windows XP. It initially allowed Microsoft employees to access these reports to find out what was causing errors in Windows and programs. Using the 80/20 rule (80% of computer problems are caused by 20% of programs) Microsoft was able to fix a large proportion of the errors which happened in Windows XP when they released XP SP1 (Service Pack 1 for Windows XP). This service pack, and all subsequent service packs for XP and all later versions of Windows, was able to reduce dramatically the number of problems which plagued users of Windows computers.

This is yet another reason for keeping your computer updated with the latest updates from Microsoft!

In the beginning, Microsoft only allowed Microsoft employees to access the data which people like you sent in as the result of a problem with their computer. Times have changed, and the companies which would like access to the data have increased in number. For this reason, Microsoft has changed the rules allowing who can access the data. Still, to protect you and your privacy, Microsoft only allows the most secure companies to access the data which you provide if you do allow the error reporting module to report the problem to Microsoft.

This is for your protection, and you can be sure that the company which rings you pretending to be from Microsoft, or from Windows, is not getting your name from any error reports which you may have sent in. In fact, they seem to be ringing from a normal call centre like those used by companies like Telstra. I state this because, when they have rung me, there is a gap before I hear a voice and then they seem to be reading (badly) from a computer screen. Each time the person whom I speak to has an Indian accent and cannot pronounce my name. For a native English speaker my name is not that difficult to pronounce!

Whois

Many years ago, the main networking computers ran an operating system called Unix. In those early days of networking someone wrote a program called *whois*. This program gave you the name of the computer which was accessing your computer, so you could tell if it was friend or fiend.

Nowadays *whois* is a system run by many websites, and it allows you to check who owns the website in question. Doing a *whois* lookup for *wteksupport.com* provided the following information about the owner of this domain name:

Subodh Sonthalia
theitheaven.com
51/6 Grand Trunk Road
Pilkhana, Howrah
West Bengal 711101 India
Tel. +091.3326661423

If you would care to ring the owner and complain I would be delighted, but I shall not hold my breath waiting for you to do that! You may have noticed that the web address for the owner of *wteksupport.com* is located at *theitheaven.com*: checking that website reveals that it has lots of bling on the front page (just like *wteksupport.com*!) but no substance behind it. In England this is called ***Queen Anne front and Mary Anne behind***.

Just the right place for a shyster!

I have checked this address using Google Maps and it appears to be a residential area (the photo was not clear: it could be an industrial park) full of concrete slabs with windows (no, not *that* sort of Windows!) which could easily house a small call centre.

I hope that this information has helped you to feel more comfortable should you ever get a call from this company. They are a nuisance, but only because they catch a number of people out and the money keeps rolling in.

I have included the website details for two *whois* providers because the first (NetRegistry) specialises in Australian websites and the second specialises in international (.com and .net) websites, though it can be forced to do Australian lookups as well.

Enjoy exploring the internet!

Further Information

Buzz-Phrase Generator	www.brianjford.com/anonscic.htm
Their websites	www.wteksupport.com www.theitheaven.com
LogMeIn	www.logmein.com
Whois	whois.ausregistry.net.au www.whois.net
Google Maps	maps.google.com