# Radio Days – 2009-07-04

## *Tip of the Week – Excess Charges*

A client has mobile internet using a USB device which plugs into his computer. Recently he got a bill from his ISP demanding $2,700 for one month's downloads. He checked his usage on the program which comes with his USB device and saw that he had only used 3 GB of his 12 GB monthly download limit. He had also lent his device to a friend.

There are two things to note here. The first is that he had no idea how much he had used during the month in question: the usage that he was seeing was for the current month. The second was that his friend had the device for a week: quite long enough to download enough to create an enormous headache for my client. To moral of this story is to keep track of your usage and do not lend your internet access or phone as it may cost you a small fortune. You may be able to challenge the cost with the Telecommunications Industry Ombudsman (TIO).

## *Scams and Their Effects*

*Shoulder surfing* is watching somebody (and somebody watching you) enter a username and password into a computer or a PIN at an ATM or checkout. This is becoming more common as people realise that they can make a lot of money just by cloning credit and debit cards. What is now happening is that more people are realising that there can be a lot to be gained by finding out other peoples' PINs and their user names and passwords, especially to their banking login details.

*Social engineering* is the practice of getting people to reveal details which will allow other people to gain access to information to which they do not have authorisation. Most people will be familiar with the Nigerian 419 scam *Please help me get $450 million out of Nigeria* and the *Your bank needs you to verify your login details*. Another favourite for some months was an email promising to show pictures of naked women. This works very well with so many men: don't you be one of them!

Recent years have shown that the more devious schemes to part you (or your employer) from their money is the more targeted scam. The most recent one that I have heard about is where people who worked at a business found lots of USB sticks in the company car park, so they picked them up and started to use them. This put a virus on the company's computers and it lost quite a lot of money.

Even more worrying is the rise in scamming text messages on mobile phones. I have not seen any but they seem to be effective. The scammers continue to scam because their scams are both cheap and effective at getting money. Because people continue to fall for these scams they will continue to be around.

The best ISPs are now stopping most scams from getting through to your inbox, but you still have to be aware that they exist. I urge you to check all unexpected emails, text messages and phone calls from people you do not know or which you do not expect. There are recent scams at this end of financial year which offer you a 30% tax rebate if you hand over certain information like your tax files number. All of this is just too good to be true, and to find out more just get *The Little Black Books of Scams* from the ACCC website.

## *Websites*

| | |
|---|---|
| TIO | www.tio.com.au |
| SCAMwatch | www.scamwatch.gov.au |
| Stay Smart Online | www.staysmartonline.gov.au |
| ACCC | www.accc.gov.au |


Copyright © 2009 Toby Bainbridge