Radio Days – 2014-05-31

Tip of the Week – The NBN Is Not Optional

We are standing at the brink of a new era: an era which will herald a new way of working for a large number of people. This new era is the start of the switch-off of Telstra's copper network. This means that, for those people in the switch-off areas who have not yet been connected to the NBN, their landline will stop working.

This is why I say that the NBN is not optional!

Why No NBN?

There is only one reason not to get the NBN delivered to your door and that is because all of these reasons apply to you:

- You will never die
- You will never sell your existing house until it falls down and needs to be rebuilt
- You will never need another landline
- You will never care about your descendants selling your house without NBN access

If one or more of these conditions does not apply then you would be extremely foolish if you did not get the free NBN access to your home.

Free NBN Access

When I say "free" I mean that there is no cost to get connected to the NBN. As soon as the NBN is available in your area you should get connected as quickly as possible. When you have been connected to the NBN you will need then to contact your telephone provider or your ISP (Internet Service Provider), or both, to arrange their connection. I suspect that your best bet will be to have both your telephone and your internet through the one provider as I expect that this will be the cheapest way to go.

This connection may incur charges, and you will need to pay for things like internet access and telephone calls, although many people will find that their best option is one which has all phone calls included in the basic tariff. This is how the world seems to be going, and with calls effectively free over the NBN's internet connection you will probably have the best deal going.

NBN Internet

I have spoken to a number of clients who have been connected to the internet through the NBN and they are, without exception, delighted with the service. The speed is consistently high (unlike satellite or mobile coverage which can vary depending on the weather and, it seems to me, the passing traffic) because the NBN company ensures that the towers and other infrastructure are never overloaded.

As Clark's Shoes' slogan said when I was a boy: *Room For Toes To Grow!* This is why the current infrastructure is truly the best. Other designs would need upgrading very soon. The whole system is being designed and constructed to be the basis for a piece of infrastructure which will last for as long as possible.

Connect to the NBN as soon as you have the chance. As the website says, its rollout is starting with those areas of the country which are too far from telephone exchanges to be able to get ADSL. Thus, if you look at the rollout map, you will see that Maryborough is being ringed on three sides by areas which already have wireless access to the NBN network. Because we in Maryborough have good ADSL access we will get the NBN after the outlying areas have been connected.

Locked iPhones

Are you one of the many proud iPhone users who have had to pay a ransom to get access to your beloved iPhone? iPhone users Australia-wide have been caught with their darling Apple devices locked by Apple's own mechanism to prevent a thief from taking advantage of a stolen device.

There seems to be some confusion about how the hackers have gained access to a phone to be able to report it stolen. Some say that the iCloud way of storing all the data on all your linked Apple devices is to blame, and this seems to be, if nothing else, at least a plausible way for the hacker or hackers to get access to your iPhone.

There seem to be a number of ways in which hackers can access your phone (and other, linked, devices). The good news is that there is, it seems, a simple way of preventing this attack if you have not already been caught and that is to setup two-factor authentication.

Unfortunately, it appears that having an anti-virus program on your iPhone would not stop this sort of attack so that is another line of defence which will not work.

How Are You Attacked?

There are, it seems, a number of ways to get at you but they all boil down to one thing: the attacker must be able to change apparent ownership of your iPhone from you to him or her. Once your friendly hacker "owns" your phone he or she can then report it as stolen and put the Apple mechanisms for recovering a stolen phone to work to make you cough-up a ransom for your own iPhone!

Oh! The joys of modern technology! If only we were not so reliant on it!

The first step in the attack, it seems from some reading on the internet, is to change the details in your iCloud subscription. As far as I can determine, the most obvious attack route is to get your sign-in details, often from Apple itself. This attack, in at least one case, came from a hacker who was able to get Apple support staff to provide the password for a iCloud user!

This makes the so-called "privacy" provisions and hoops that you have to go through to get a provider, like a bank, to talk to you appear a nuisance at worst and irrelevant at best.

It has long been stated that the weakest link in any sort of attack is the people involved. This ability to get around the people who are supposed to protect you is essential in so many areas. Planes have been blown up because a bag was carried on a plane but the passenger didn't fly, and there are many other cases that I could quote. For more details look up

Two-Factor Authentication

Two-factor authentication is one way to protect yourself from having your phone hacked. It is one way to ensure that you are the person who is trying to change your password. So, how does it work?

First you have to set two-factor authentication up for that service. Because so many people have mobile phones the most obvious sort of two-factor authentication is for the service provider to text a number to your registered phone so that you can enter that number into the webpage to prove that you are who you say you are.

This, of course, only works if you actually have control over your phone. If your phone has been stolen then, of course, all bets are off.

For example, if I want to make a payment from my bank account to a new account the bank sends me a text with an authorisation number which I have to enter into my bank's webpage before the transaction can proceed. This is how two-factor authentication works.

If you have not set it up yet then please do it now!

Pay The Ransom?

If your phone has been attacked then there is the dilemma of how to recover the situation. There are a number of options presented on the internet, and some people say that one works while other people say that is wrong and that another is the only one which works. This is a problem which I find familiar as I am often asked how to do something and, from experience, I usually know the answer.

Unfortunately this is a new situation and I have no idea which is the best method to recover ownership of your phone. The most promising means of iPhone recovery seems to be to contact Apple support directly and to persist until you get someone who will admit that iPhones can be hacked. There are far too many people who insist that anything that Apple produces is immune from any sort attack.

Apple's People

One of the worrying implications of this attack is that Apple itself can be an enabling factor. Apparently at least one person was attacked because Apple support people provided the password for iCloud based on incomplete information. It appears that all Apple needs for identification checks are the last four digits of your credit or debit card and your date of birth, and both of these are, apparently, easy to find.

Oh happy day!

Please ensure that you have two-factor authentication setup as soon as possible.

What's Next?

The obvious (well, obvious to me at least) next move is to ensure that you have a backup on an external device (hard disc or USB stick) which you can restore when / if you lose all your data. Recent events have shown two things:

- Apple computers and other devices can be attacked
- Data loss can happen at the most unexpected times

You can lose access to your iPhone, iPad and iMac at the same time. This is what happened to a Wired journalist who was hit by this attack. He lost everything, including access to his iPhone, iPad and iMac. The next step is make sure that you have control of all your devices and that you have created two-step authentication so that you cannot succumb so easily to a similar attack in the future.

Once you have recovered control of all your devices (possibly easier said than done) the next step is to reset them then restore your data from a (recent?) backup so that you can get your life back.

No all you have to do is regain control of your Facebook and Twitter accounts! Again, this may well be easier said than done but at this stage you have nothing to lose so just do it ™!

Further Information

NBN www.nbnco.com.au