Radio Days – 2014-01-25

Tip of the Week – Setting-Up WiFi

During the week I had a call from a new client who wanted to be able to use her iPad at home and connect it to her home WiFi network. I expected that this would be a simple matter, but as so often happens I was wrong!

Things started badly when she could not find the password for the WiFi modem. We then played a game of "Hunt the password" until I remembered that the it was probably printed on the base of her modem. I checked, and there it was as expected.

After getting the correct password for the WiFi modem I entered it into the correct place in her iPad but it would not work. I tried the same thing using my phone, again to no avail. This was frustrating so I rang Bigpond because it was a Bigpond internet connection. The person I spoke to reminded me that I had to enter upper-case letters in upper-case!

For some reason known only to the gods I had assumed that all numbers and letters were hex digits. Hex (short for hexadecimal or base sixteen) digits are the sixteen symbols used to count to sixteen in computer notation. These hex digits are all the numbers (0 … 9) and the first six letters of the alphabet (A … F or a … f). This was an incorrect assumption (do you know that *assume* makes an *ass* out of *u* and *me*?) as I discovered after entering the password as it was written on the bottom of the modem and on the card which came with the modem.

The moral of this story is that you should always enter passwords exactly as they are written down, and the corollary is that you should always write a password down exactly and in the correct case. If you are one of those people who always writes or types in either all upper-case or all lower-case then please be careful when writing or typing passwords!

This was most embarrassing as I had thought that I would never make that mistake again.

Check That Address!

During the week I received an email which had the following message:

> *We want to inform you that your account was accessed from an unauthorized computer.*

This sentence should immediately raise alarm bells. No, repeat ***NO***, computer has ever been authorised for access to a bank's network. This is easy to work out: how do either you or the bank know which computers you will use, now or in the future. This is impossible so that is why ***ALL*** computers are authorised, and the user is identified by his or her username and password. This is why the scammers need you to give them your identification credentials so that ***THEY*** can access your bank account!

Because I check my emails using MailWasher I noticed that, while the link lower down in the email stated that a click would take me to the ANZ website, MailWasher showed me what the real address was:

> *Please visit* www.anz.com.au *[Links to* www.studiobuehne.de/anz*] and confirm that you are the owner of the account.*

What I would like to draw to your attention is the ease with which scammers can part you from your money. It is so ridiculously easy to make a link look like the one which you are expecting but to take you to another place entirely, and scammers delight in using this sleight-of-hand to help you to send them the access codes to your banking details.

Perhaps you do not bank with ANZ. Would you just delete this email and think no more of it? Would you just laugh and note that only an idiot would be fooled by this sort of scam? Please remember that the reason that these scams continue to plague us is that there are too many people who succumb to the blandishments of your good old regular good-guy scammer.

What would you do if it was from your bank? If the scammers can easily forge one bank's website to part other people from their money they can, just as easily, forge ***YOUR*** bank's website to part ***YOU*** from ***YOUR*** money. Would you be laughing then?

Additional Thoughts

During the last week there have been all sorts warnings about the ease with which people are fooled by scammers. One program on ABC TV showed just how hard it can be to persuade people who are sending money to scammers that this is, in fact, a scam. One man believed that he was sending money to an employee of a European bank who was based in Africa so that he could make enquiries about a friend who had gone missing. It was only when the AFP (Australian Federal Police) gave him a letter on the bank's letterhead stating that nobody of the name that he gave was working, or had ever worked, for the bank that he began to start to realise that the whole matter had been a scam from the beginning.

This man was sending almost all his pension overseas each fortnight. He had no food in his fridge (this was shown on the program) and was living on the throw-outs from a fast-food outlet. (Do you remember the film *Supersize Me*?) Only after he had come to grips with the reality of this scam was he able to feed himself and start saving money. At the end of the program we were shown his fridge, now stocked with food and drink.

Please believe that, if you are sending money overseas with no apparent return, it is a scam. I am not, of course, talking about buying goods from reputable overseas websites. Amazon is real, and it sends books to many people each day. I bought a camera from another overseas website and it took just days to arrive while I checked its progress on a reputable transport company's website. The same thing happened when I saved money buying a mobile phone overseas.

The problem usually comes after you have received an unexpected email, fax or phone call from a stranger. Remember the good old *Stranger Danger* message which we taught our children? This applies just as much to us as adults as it does to our children. Just as we are responsible for keeping our children out of danger so we are also responsible for keeping ourselves out of danger!

SCAMwatch

The ACCC (Australian Competition and Consumer Commission) runs an excellent website called SCAMwatch. If you log on to this website you see a list of twelve scam types, and many of these types are broken down into subtypes. Some of the scam types are:

- Banking & online account scams
- Credit card scams
- Phoney fraud alerts
- Chain letters and pyramid scams
- Pyramid schemes
- Health & medical scams
- Investment (get-rich-quick) scams
- Superannuation scams

As you can see, there are a number of ways (some of them very inventive!) which scammers use to part you from your money. Those which only get money from you are the (relatively) good ones: the (relatively) bad ones are those which steal your identity (this is called *identity theft*) and leave you with enormous bills to pay for the rest of your life.

It is bad enough that some Australians want all your savings without realising that there are other people from overseas who are also getting in on the act!

Money Lost

It is estimated that Australians send more than $7,000,000 (seven million dollars) overseas each month to scammers. This money is often the result of either greed or stupidity on the part of the scammed person (a *get-rich-quick* scheme is one which makes you poorer and the scammer richer), but also it is often people who think that they have met their perfect match overseas, who just needs a little more money to make the trip to Australia so that the two of you can be together.

I do know one person who fell for this scam. He was devastated when he realised that the woman with whom he had fallen in love was just after his money and not his body. He lost several thousand dollars in this scam which appeared to be legitimate as there were photos of all sorts of documents to support her claims that she had spent his money well. The photo of her passport was good enough to fool him, and the photo of her visa to visit Australia for three months was also good enough to fool him but not the Department of Foreign Affairs when he showed it to them.

This scam had obviously been put together with a lot of thought. There were probably a number of people involved, as well as the woman who appeared to be genuine when I saw her on Skype. She spoke with what appeared to be an African accent, and seemed really glad to be talking to her "friend" from Australia. In the end the group of scammers received more than $10,000 (ten thousand dollars) for just a few weeks' work.

They probably had a number of marks on the go at any one time, so would have made enough to keep most of them in the lap of luxury.

My next job will be to work out the perfect scam!

Further Information

MailWasher Free	www.mailwasher.net
MailWasher Pro	www.firetrust.com
SCAMwatch	www.scamwatch.gov.au