Radio Days – 2014-02-01

Discussion – The Year of the Hacker

This year is shaping up to be the Year of the Hacker. All indications suggest that the world's hackers are conspiring to do something to your computer which will part you from your money. There are many ways that this can be done: some of them are targeted at anyone who will respond while others are targeted at a specific person or computer.

There are many means that hackers use to get your money, and there ingenious variations of all of them. They fall into a number of categories: here are some of the most common.

- **Love Interest** – the way to your heart leads your friendly scammer directly to your bank account.
- **Free Money** – the classic Nigerian 419 scam, named after the article of the Nigerian penal code which covers this crime.
- **Work From Home** – the classic "get rich quickly" scheme guaranteed to make you get poor quickly.
- **Locked Computer** – your computer is locked and you need to pay to get the unlock code.
- **Encrypted Data** – your data is encrypted and you need to pay to get the decryption code.

Your Mission Impossible, should you accept it, is to ensure that you and your computer (or computers) remain untouched by hacker hands.

Love Interest

One of the best sorts of legitimate businesses to run in the modern world is an internet dating site. This is because so many people have run out of patience with the old process of going to a meeting place and just not meeting the person of their dreams. Somehow, however, out of the blue, the one just right for you turns up.

This person is ideal! She / he has everything that you are looking for: wealth, looks, position, sex, etc. This person is almost be too perfect to be true, and that is the moment that you are hooked. You start an online romance then, out of nowhere, communication stops. It is not until later that you get an email stating that your inamorata / inamorato is too ill to continue and needs money for medical treatment.

You are devastated! You send money! Your inamorata / inamorato needs more TLC. You offer to fly to her / his bedside! This would ruin the scam so you are dissuaded from arriving. Should you decide to arrive anyway you will find that there is something wrong and that you have lost everything.

Please do not send money until you have met your beloved in person, not just by email, not just on Skype nor just on the phone. Your beloved may be in another country or even on another planet but that does not preclude you from using what brains are left after your hormones have finished messing with your mind.

THE RULE: SEND NO MONEY!

Free Money

You get an email from somebody – often a rich widow – who has money to get out of a foreign country and needs your help to do this. There is a catch (isn't there always?) and it is that there are costs or bribes which need to be paid to get past the gatekeepers and, without access to all those millions of dollars, she needs your help to pay the costs.

The first call is usually just a small one, just enough to get you hooked. Once you have been hooked there is another, slightly larger, impost for you to pay. Once you have paid this

further impost there are still more fees, each larger than the previous one. This process continues until you have run out of patience with the process or you have run out of money.

At this stage you may at last realise that all scams end in the same way. As my grandfather told me so many years ago: *heads they win, tails you lose, and that's fair, isn't it*.

THE RULE: SEND NO MONEY!

Money Lost

It is estimated that Australians send more than $7,000,000 (seven million dollars) overseas each month to scammers. This amount of money is often greed on the part of the scammed person (a *get-rich-quick* scheme which makes you poorer and the scammer richer), but it also 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 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 some thousands of 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 the 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!

Work From Home

Recently I was looking at a website that I had not visited for some time and saw an article which stated that you could make a lot of money working for just a few hours per week from home. This seemed too good to be true (the featured person lived in Australia and made over $8,000 in her first month) so I checked the website on Google. There were many warnings about this site plus the obvious one: this site asked for your credit card details before it told you what you would have to do and what you would get.

This is a danger signal. No reputable site asks for your credit card details before you have even seen the second page.

Most of these *work from home* advertisements are scams: figures suggest that there are at least six scams for each genuine ad. The most dangerous *work from home* scam is where the scammers pay you to allow them to place money into your bank account then you send cash by wire transfer to them in another country.

This is called *money laundering* and will land you in goal, plus you will have to repay the stolen money. You then lose all the money that they placed in your bank account plus spend time behind bars. Not a good investment!

THE RULE: SEND NO MONEY!

Locked Computer

This scam involves a warning, purportedly from the Australian Federal Police (AFP), that you have broken some law and stating that your computer will be disabled until you pay the outstanding fine. Despite the AFP logo on the warning it is known as the *FBI Scam*, for obvious reasons, and there is no reason to reward the scammers by sending them money.

This is just a simple virus and it is relatively easy for an skilled and experienced person to remove it.

THE RULE: SEND NO MONEY!

Encrypted Data

This is, perhaps, the worst one of all. The scammers place a virus on your computer which encrypts all the data on all the discs which are attached to your computer at the time of the attack. They then demand money for the password to unlock your data. It is easy to remove the virus, but the damage has been done and your data will still be locked.

Because it encrypts the data on all your attached discs it is especially vicious for those who keep their backup disc attached to their computer at all times because their backup, which is the only way to get their data back, is also encrypted.

This is why your backup disc should only be attached to your computer when you do your backup. This may involve more work but, in the long run, is the safest way to keep your data safe.

THE RULE: SEND NO MONEY!

Getting Help

Keep Your Mind Awake

The main way that scammers get through your defences is to make sure that you do not detect the scam. They do this in all sorts of ways, and most of these rely on the fact that most people are not fully aware of their surroundings most of the time.

I have watched many clients click merrily on all sorts of obvious scams then being amazed at the pops-up on their screen. Just because a button on a website or email says ***CLICK HERE*** does not mean that clicking here is a good thing.

Install a Good Anti-Virus Program

Please ensure that you have an anti-virus program so that you have more chance of beating the scammers. There are many good anti-virus programs on the market: my preferred one is Kaspersky.

There are a number of free anti-virus programs available so cost should not stop you from installing one. If you are not sure how to download and install a program from the internet then help is available from all sorts of places.

SCAMwatch

The ACCC (Australian Competition and Consumer Commission) runs an excellent website called SCAMwatch. If you log on tho 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 o 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 bad ones are those which steal your identity (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!

Australian Federal Police (AFP)

The AFP has an much shorter, but much broader, section on cybercrime. This sort of crime in all its glory is spreading and is the wave of the future. As criminals discovered so many years ago, banks are delighted to prosecute those who rob them and their customers at gunpoint because they can then boast that they have good security systems.

They are more reluctant to prosecute those who rob them using a computer because it shows that their digital security is lacking and that that something they do not wish to advertise. This means that the smart money will be on computer (or cyber) crime as there is both less chance of getting caught and less chance of getting goal.

Both good reason for the scammers to get to your bank account over the internet.

Further Information

SCAMwatch	www.scamwatch.gov.au
Australian Federal Police	www.afp.gov.au/policing/cybercrime