Don't Get Fooled by Bogus eMails!

Scams are rife, and many seem genuine

I'll be brief and to the point as best I can with this one. You've been warned about scams, particularly those on the Internet; and many appear to be genuine messages from reputable companies; but be warned – if you make the mistake of being too quick with a click or a tap, you could be in big trouble!

Recently there has been a spate of cases in Australia and the UK when people have been advised that a package or letter couldn't be delivered because no-one was home at the time. The advice sounded straightforward and purported to be from the normal postal service. In order for the package to be re-delivered, a small charge of £1.95 was required to be paid. Now, this doesn't seem much; and even if it proves to be a scam, losing a couple of quid isn't going to cause financial ruin; not immediately, anyway. BUT THINK ABOUT IT – once the scammers have your bank details gifted to them by making this simple online transaction, they have the means to strip whichever account is used. If you slip up and get caught like this, contact your bank immediately to report the incident. They will probably cancel your existing card and issue a new one.

It couldn't happen to me, you may say: you'd never be fooled that easily. Don't be too sure. The contact address which looks perfectly genuine could well be fake, and there is a simple way to check. BEFORE opening any email; and definitely BEFORE clicking on a link; verify the sender is genuine. Do this by placing your mouse cursor (usually a hand) over the Company name on the far left. An information tab will appear detailing the full address of the sender. The first part followed by the @ symbol is the usual; but it's what comes after that matters. One sent to us seemingly from Qantas had a spurious string after the @ - media37.chocbocrossing.com. Needless to say, it wasn't from the iconic airline. For more details on recognising scams, have a look at our Internet Tips, in particular IT10 and IT11.

When in doubt, contact whoever is claiming to be the sender; **but don't use the address on the email**: go straight to one you know to be genuine – perhaps on a previous email, letterhead, or from the phone book - and ask the question. Nine times out of ten you will be told that what you received is a scam. So, should the message seem to be from your bank, don't action it there and then – phone your bank for confirmation. More than likely they will give you a flat denial that it came from them.

I received a call supposedly from my bank querying two payments made on my account which were seen to be unusual based on my past transactions. To start with, the rather mechanical American/Asian accent of the caller was suspicious. I thought at first it was one of those annoying tele-marketers. It also sounded like a recorded message. Next, it

was claimed, one of the suspect payments was a $400 purchase on eBay. Now, we do buy the odd item from eBay, but not using that particular account. We have a separate one in my wife's name used specifically for Internet purchases and having a low fixed credit limit. As soon as the recording said:"Press one for..." I cut the call. Shortly after, a check of both credit accounts confirmed no such payment had been made. What would have happened had I pressed "one", I have no idea; but I wasn't about to get fooled. Please, don't you be.

Another insidious scam is the phone call from the tax office or a government department claiming that a sum of money is owed, and if this is not paid immediately legal proceedings will be instituted. Many on hearing this tend to panic, especially older citizens, and quite a few follow the instructions of the caller; then the damage is done. Don't be fooled – government agencies in particular do not conduct business in this way. If there's a problem, they will contact you by letter or email; and even then, be wary. Look up the number of the department in the phone book and give them a ring; just to be safe. Certainly avoid opening any suspect email; and never click on a link unless you are one hundred percent positive the sender is the genuine article.

There are plenty more of these scams out there with new innovative ones popping up all the time. Be cautious, be mistrusting with everything and anything that seems likely to be suspicious. There is always a way to check on the authenticity by going straight to the horse's mouth and posing the question: "Was this from you?" A lot of the time the answer will be nay.