Tip Sheet

Avoiding phone and internet scams

Scams are an unfortunate fact of using the internet and your phone. Although there are ongoing efforts to shut down scammers, it's important for you to be aware of possible scams so that you can avoid being caught out.

Types of scams

There are a lot of scams out there. Many of them attempt to take your money. Others attempt to access your personal information, which could be used for identity fraud. Some attempt to gain access to your computer. A few examples of these scams include:

- You get an email from an overseas relative you didn't know you had asking for you to provide money, bank details, an address, or other piece of information.
- You get a call from someone claiming to be from Microsoft or another computer or communications company telling you they've detected a problem with your computer, and that you should go to a particular website or download a particular piece of software so that they can fix it for you.
- You get a call from someone claiming to be from your bank, phone company or other service provider asking you for your account details, passwords, or personal information like your date of birth.
- A website pops up telling you that your computer has been infected with a virus and that you should click a particular button to clean it.
- You get an SMS telling you that you've won a prize with a link or phone number to let you claim it.
- You get a friend request on a social network like Facebook from someone you don't know.
- Someone calls you claiming to be a friend who has had their wallet stolen while they were on holiday in another country—especially if you don't know anyone on holiday in that country.

Of course, sometimes a call might sound suspicious but turn out to be genuine—maybe your long lost cousin has found you and wants to send you a letter—but if you get a surprising email, phone call or text message, you should be careful.

How these scams work

The exact way a scam works will vary from scam to scam. Some scams just try to convince you to send money or buy a dodgy product. More modern scams will try to convince you to hand over your passwords or other security details. This could include your address, date of birth or other information that you can use to prove your identity to genuine companies like your telco. Remember that if you can use the information to prove who you are, someone else can use the information to prove that they're you.

Some scams take advantage of technical tricks:

- Emails and websites can include links that say they'll take you to one page, but in fact take you to a different page. For example, even though this link—<www.google.com>—says that it will take you to the Google home page, it will actually take you to the ACCAN home page.
- Some scam websites are designed to look like genuine websites by using copies of the genuine logos, colours, and text—this is called 'spoofing'. If you try to log in to these websites with your username and password, the scammers get the information needed to log in to your real account.
- Some 'missed call' scammers try to trick people into returning a missed call or a call that hangs up as soon as it's answered. When you return the call, there may be a message telling you about a prize or offer and giving you a number to call to claim it. This new number is often a premium rate ('190') number so that you get charged a high call cost, with part of the money being paid to the scammer.

Things to watch out for

It can be difficult to tell some scams apart from legitimate calls, messages, emails or websites. If in doubt, it's safest to end the call or delete the message—if it's important, you can always try calling back your friend, the bank, or the phone company to check that a message was genuine. Some signs that it might be a scam include:

- The message asks you for money or information.
- The message includes an offer that sounds 'too good to be true'.
- The message is from someone you don't know, a product you've never heard of, or a company you've never dealt with.
- The message asks you to click a link or download software.
- The message claims to be from someone who is unlikely to make personal contact—a company like Microsoft, for example, is unlikely to call everyone who uses Windows to tell them of a problem.

Some companies take action to help you avoid scams. For example, Australian banks will never send an email with a link in it, so if you get an email with a link claiming to be from a bank, it's probably a scam.

What to do

The simplest and best way to deal with a call that you think is a scam is to hang up. If you think an email is a scam, simply delete it. If you receive an unwanted text message, text 'STOP' to the number. If you are unsure whether a call or message is genuine, try calling the person or organisation on a number that you know is the right one.

Further information

The WA Deaf Society and ACCAN have created a series of accessible videos with information on avoiding scams, available on YouTube <http://www.youtube.com/user/internetscamsprotect>.

The Australian Government runs the website <http://www.scamwatch.gov.au/>, which contains information about different types of scams, and what you can do if you think you've been scammed.

Many banks, phone companies and other service providers include information on their website about how to detect and avoid scams.