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 is 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 try 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 did not 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 have 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. Scammers have also been known to impersonate representatives from Telstra.
- 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 have won a prize with a link or phone number to let you claim it.
- You get a friend request on social media from someone you do not know.
- Someone calls you claiming to be a friend asking for money because they have had their wallet stolen while they were on holiday overseas.

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. Some scams try to get 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 are you.

Some scams take advantage of technical tricks:

- Emails and websites can include links that say they will take you to one page, but in fact take you to a different page.
- Some scam websites are designed to look like genuine websites by copying logos, colours, and text — this is called 'spoofing.' If you try to login to these websites with your username and password, the scammers get the information needed to login 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 is 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 you get charged a high call cost, with part of the money being paid to the scammer. For information on 190 numbers, read our article.

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 is safest to end the call or delete the message. If it is 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:

- A phone call or email from someone asking you for money or personal information.
- An offer in an email that sounds 'too good to be true.'
- An email or call from someone you do not know, about a product you have never heard of or from a company you have never dealt with.
- An email or text message that asks you to click a link or download software.
- An email or text message from someone or a company that is unlikely to make personal contact. For example, a company like Microsoft is unlikely to call everyone who uses Windows to tell them about a problem.
- An email that contains a suspicious attachment.

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 is probably a scam.

What to do

- Hang up on suspicious calls.
- Do not open suspicious emails. Delete them.
- Reply 'STOP' to suspicious text messages.
- Regularly update your computer with anti-virus and anti-spyware software.

Further information

The Australian Government runs the SCAMwatch website, which contains information about different types of scams, and what you can do if you think you have been scammed.

You can also report scams to the Australian Cybercrime Online Reporting Network (ACORN).

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