Strong new tool to keep phone scammers at bay

PAUL FLETCHER

We all depend on telephones —- fixed and mobile — as we lead our busy lives.

But not every call we receive is a call we welcome. And sometimes the call is from someone trying to rip us off.

According to the ACCC, Australians lost nearly half a billion dollars to scammers in 2018 — and a significant amount of that was in scams carried out over the phone.

Typically these scams are organised by criminals based overseas.

One way they operate is by generating huge numbers of calls — using automated dialling technology — into Australia.

If only a tiny share of people fall for their tricks they can make a lot of money. So Australians need to be on alert.

If you get a call to your mobile which ends before you can pick it up, from an overseas number you don't recognise, think twice before you call back. It could be a scam designed to get you to call the number — where you will be hit with a very high per minute charge.

If you get a call which appears to be from the number of a well-known or trusted organisation in Australia such as the Australian Taxation Office, the police, or one of the big banks or utility providers — also be on your guard.

With modern technology, callers can "overstamp" the true number they are calling from with another number.

This can be done for legitimate reasons — but it can also be done by scammers. If criminals are using technology to scam Australians, we need to make sure we are using technology to fight back.

That is why we have set up the Scam Technology Project. It is led by the telecommunications regulator — the Australian Communications and Media Authority — and includes experts from Australia's major telecommunications companies.

The Project is looking at the latest telecommunications-based scams and is working out if there are technology-based solutions.

The first scam we are targeting is one which has been used to clean out the bank accounts of unsuspecting Australians.

It takes advantage of "mobile number portability" — the fact that by law customers can move their service easily from one mobile operator to another while keeping their mobile number.

Under this scam a criminal steals the personal information of a victim and uses that information to have the victim's mobile number "ported" across to a new phone held by the criminal. This enables the criminal to get around any identity verification process that involves sending a text to that mobile number.

For example if a criminal is able to log on to the victim's banks' website, the criminal can then enter a request to transfer money from the victim's bank account to another account controlled by the criminal. Typically the bank will then send a text to the victim's mobile number giving a code — which when entered into the bank's website will authorise the transfer.

Normally this is an effective check that the person requesting the transfer actually is the holder of the account.

But if the number has been fraudulently ported, this step simply gives the criminal the information needed to complete the crime.

The solution is to add an extra layer of safety to the porting process — so that additional information must be provided before the port can proceed.

Already the largest mobile phone companies — including Telstra, Optus and Vodafone — are implementing this extra level of safety, meaning this scam will not work if the criminal seeks to port a number fraudulently to these companies.

But there are still some smaller operators which are not yet implementing this extra layer of safety — which creates an opportunity for criminals and a vulnerability for Australians.

This is an unacceptable risk. So I have used my powers as Minister for Communications to direct the Australian Communications and Media Authority to require all mobile phone companies to add this extra level of safety to their systems by April 30, 2020.

Criminals will continue to look for new ways to rip off Australians using the telephone system.

But at the same time we need the Australian telecommunications industry to use its technical expertise to find ways to combat scam calls through their networks.

That is a priority for the Morrison government — which is why I am announcing the first action today, with more to come over the months ahead.

Paul Fletcher is federal Minister for Communications, Cyber Safety and the Arts