How cybercriminals are using bogus login pages to steal your banking information

abc.net.au/news/2023-11-18/bank-bogus-octo-scam-apps-phishing/102992426

Danny Tran November 17, 2023

By Danny Tran

Posted Sat 18 Nov 2023 at 5:24amSaturday 18 Nov 2023 at 5:24am, updated Sun 19 Nov 2023 at 8:33amSunday 19 Nov 2023 at 8:33am

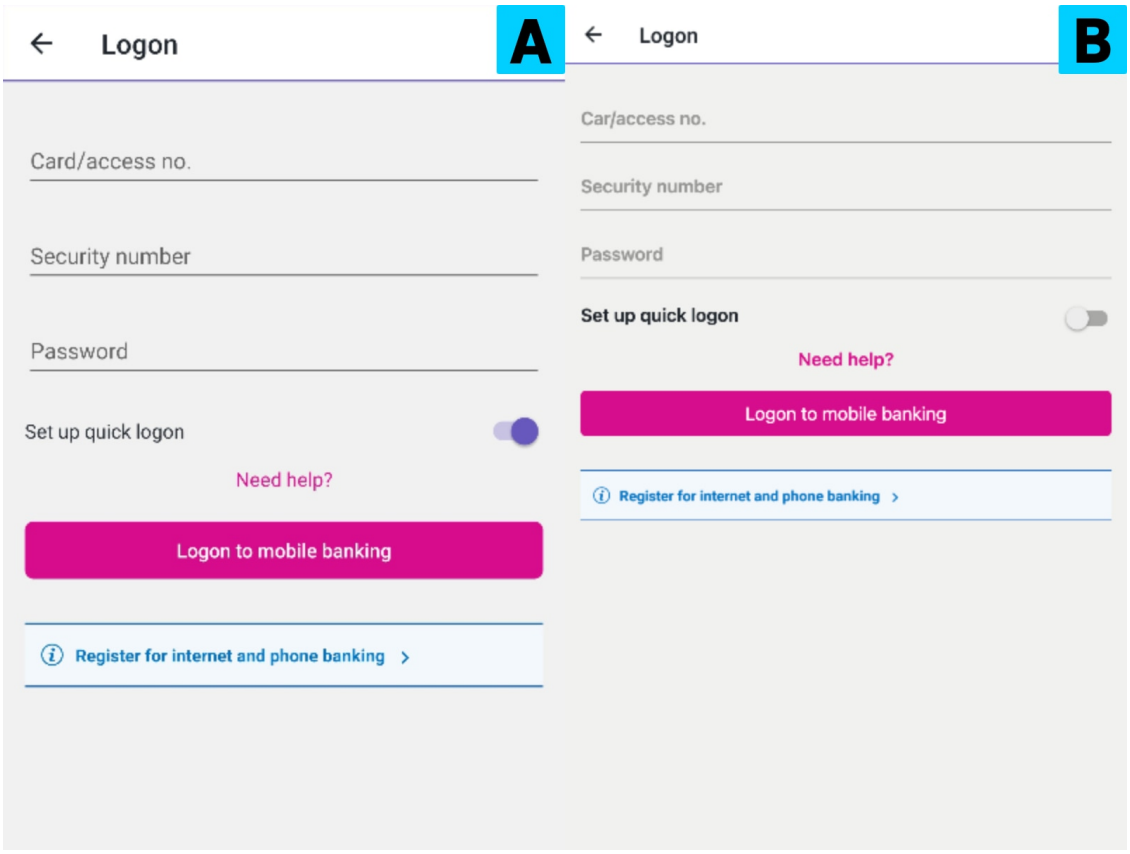
Maliciously coded fake apps like the 'Octo' malware are being used to trick unsuspecting victims.*(ABC News: Shane Willner-Browne)*

Russian cybercriminals have taken aim at the nation's major banks with a sophisticated new malware campaign, with Australians specifically in their sights.

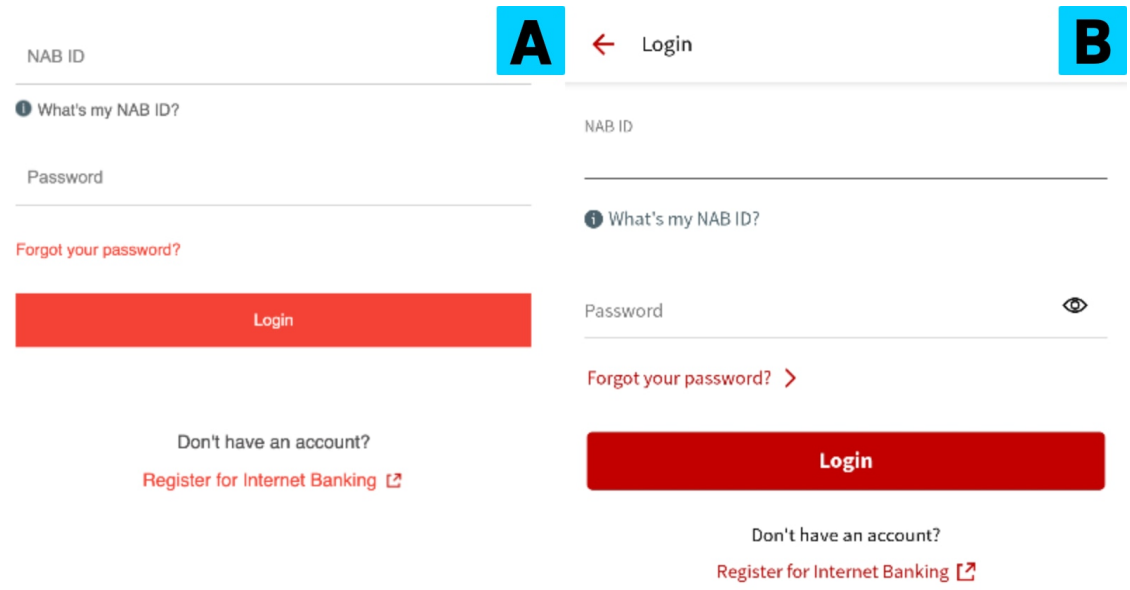
Unsuspecting victims are being swindled with bogus login pages on their banking apps, which appear authentic to even the technologically savvy eye.

Before we explain how it works, let's see if you can pick the scam.

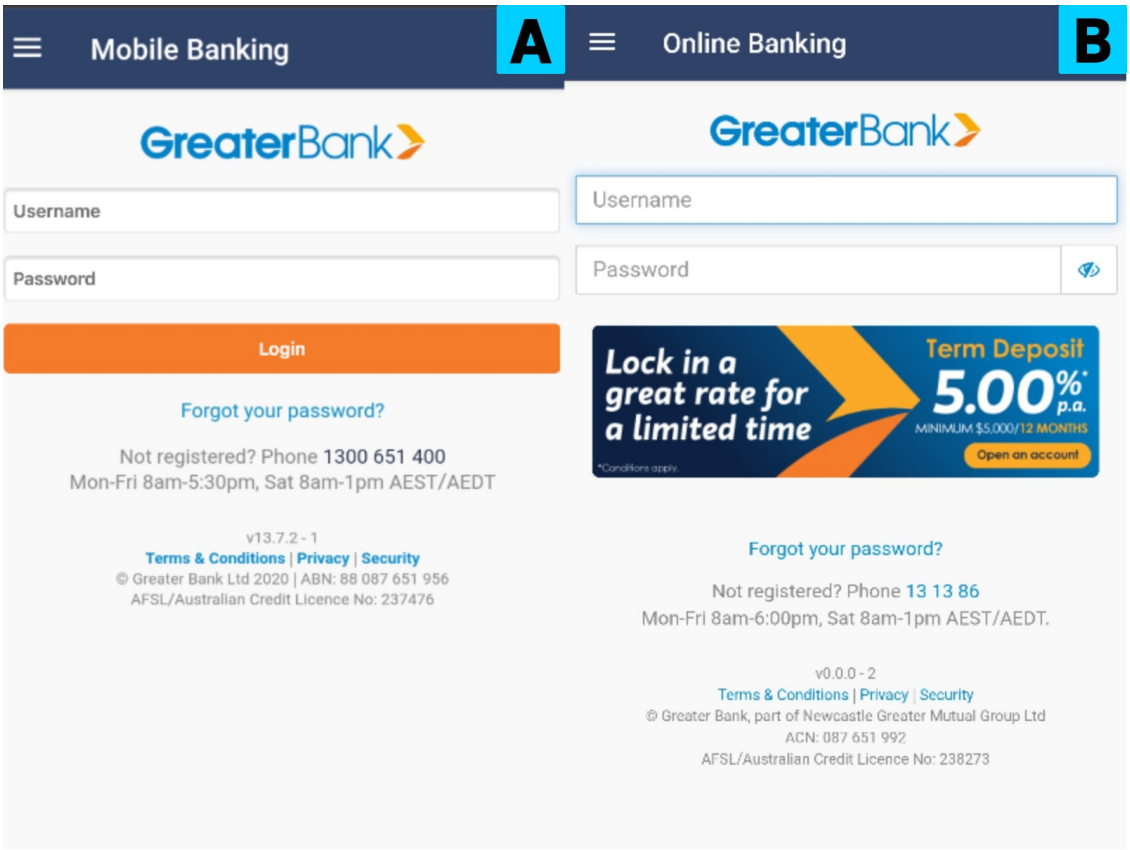
Q1: Which one is a real login portal for Bank of Melbourne?



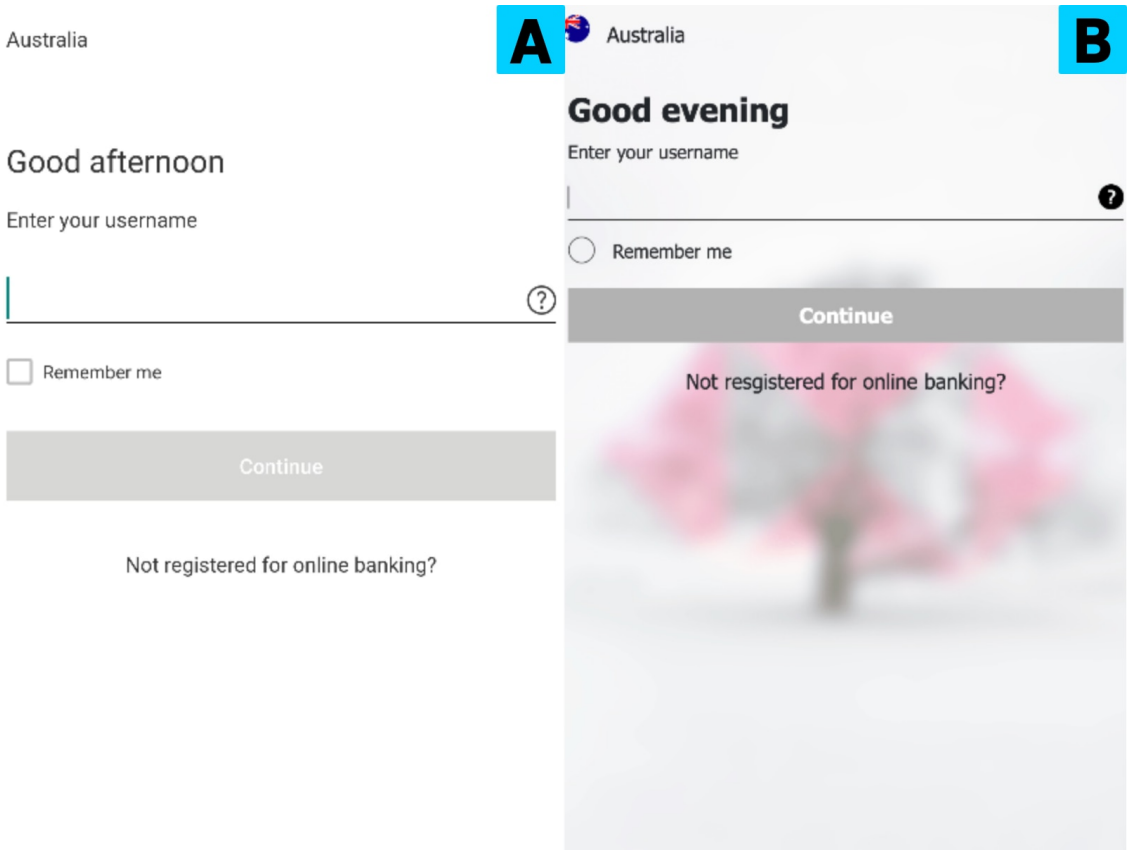
Q2: Which one is a real login portal for NAB?



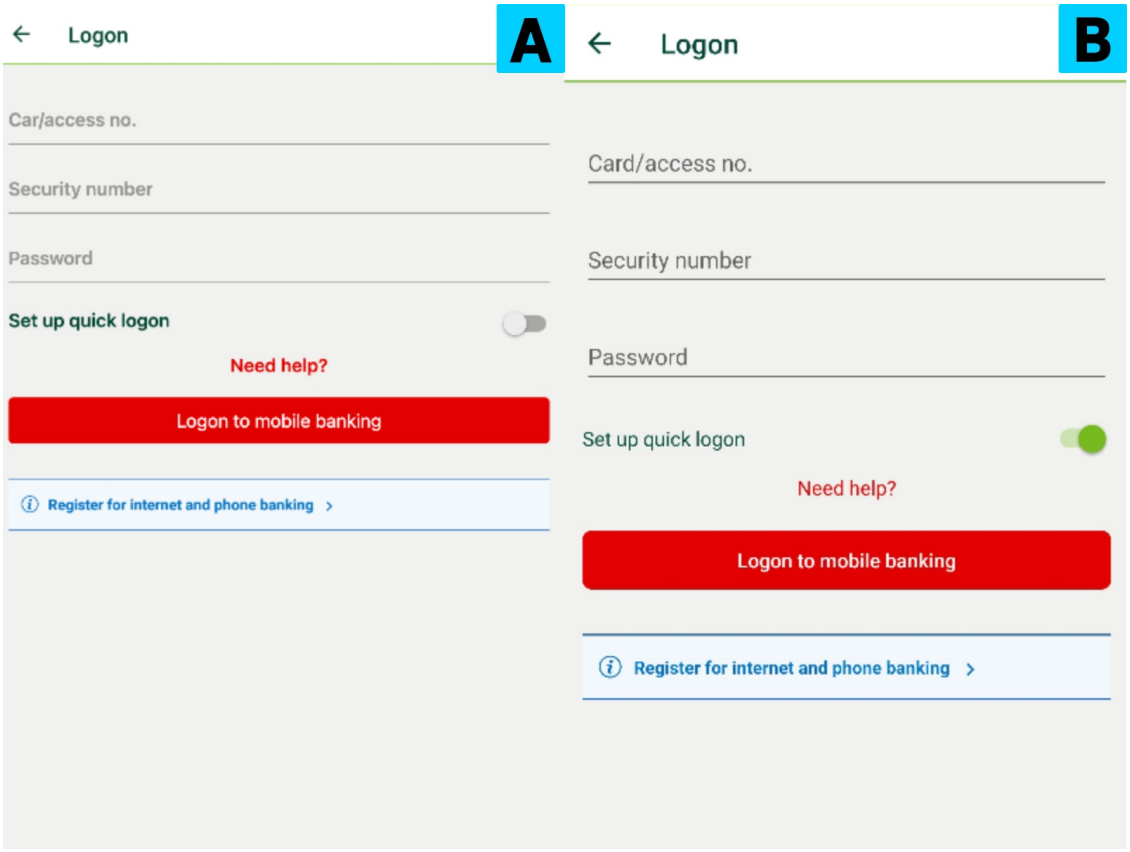
Q3: Which one is a real login portal for Greater Bank?



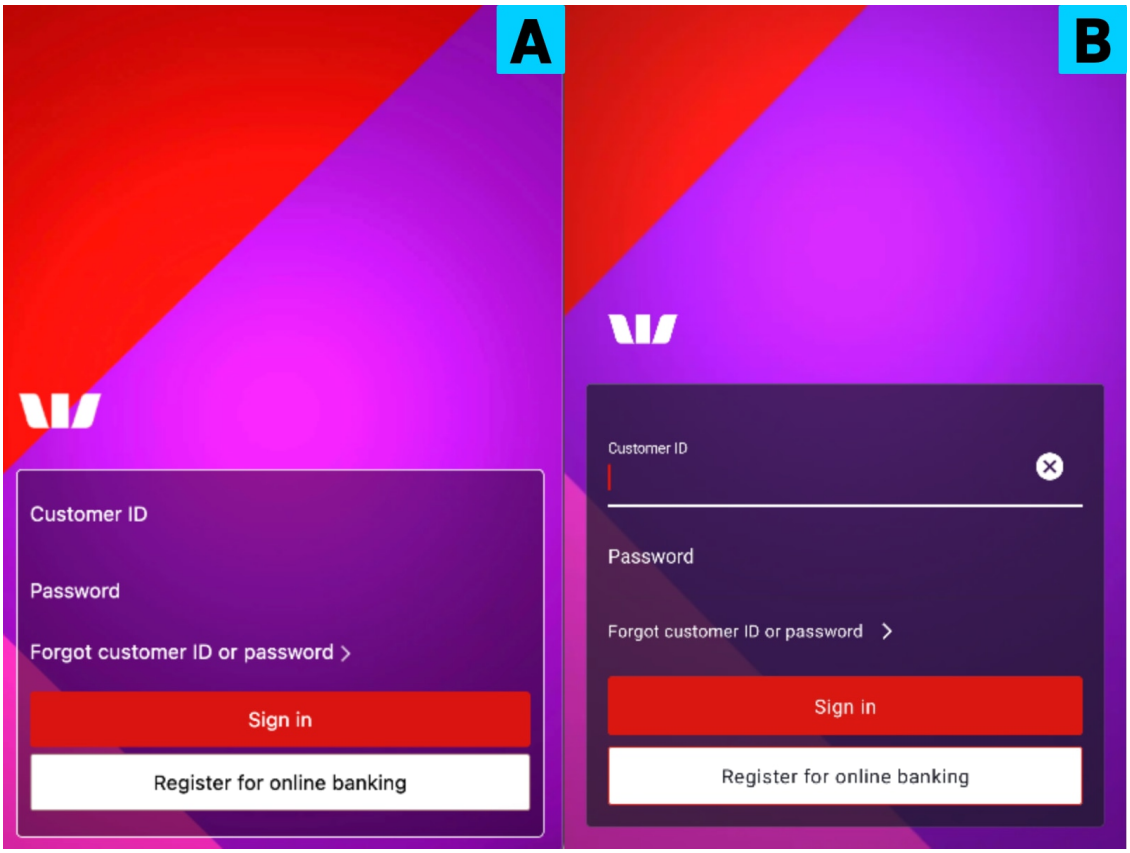
Q4: Which one is a real login portal for HSBC?



Q5: Which one is a real login portal for St George?



Q6: Which one is a real login portal for Westpac?



Quiz Results

Score: 0 / 0

6 questions left

If you punched in your details into any one of these bogus login pages, your bank details would've been sent directly to scammers.

This is a relatively new malware called Octo and it's the latest offering from cybercriminals which can be privately purchased on the dark web.

Its creator is a shady figure (or figures) who call themselves the Architect or "goodluck".

The malware is powerful — it can record your calls, harvest your contacts, evade antivirus, bypass multi-factor authentication, log what you type and send you text messages.

It can also perform what's known as overlay attacks, which is what happens when hackers superimpose a fake login page over an authentic app, like the ones above, to trick you into giving up your credentials.

Exclusive new data obtained by the ABC has uncovered what appears to be the first major distribution campaign of the malware, with Australians identified as specific targets.

Many of the nation's major banks are caught up in the scam, including:

- ANZ
- Bank Australia
- Bank of Melbourne
- BankSA
- BankWest
- Beyond Bank
- Bendigo Bank
- Commbank
- Greater Bank
- HSBC
- myRAMS
- NAB
- St George
- Westpac
- UBank

Hundreds of Australians have been lured into downloading the vicious malware onto their devices within days of it appearing in the wild.

It comes as consumer advocates warn that Australians are being targeted because the nation is seen as a soft target.

Octo targets Android phones — think brands like Samsung, Google, HTC — and can be hidden in what look like legitimate apps on the Google Play store, which is trusted by most users because it's run by one of the biggest tech companies in the world.

It can also be downloaded and installed independently of the Google Play store, because of the way software on Android phones works.

A malicious malware called Octo has been designed to target phones that use the Android operating system.(Unsplash: Daniel Romero)

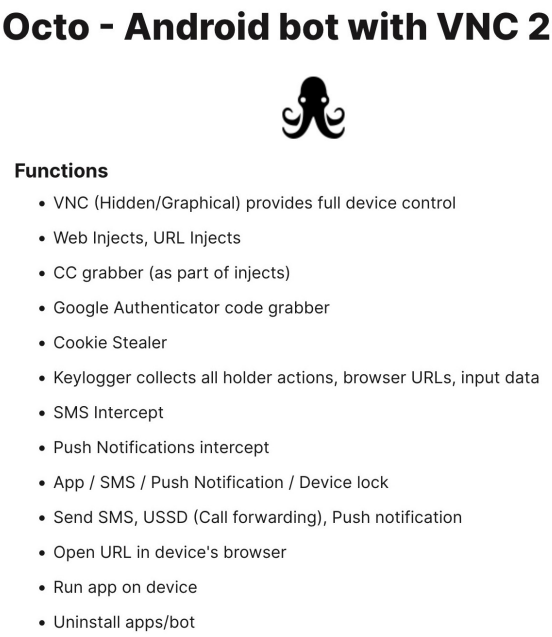
The number of people in your life with Android phones might seem small, but there are actually more than you think.

In Australia, 52.9 per cent of people own an Android device compared with 47.1 per cent of iPhone users, according to Kantar WorldPanel, a market research company based in London.

It means that even if you own an iPhone, there's probably someone in your orbit who has an Android device.

Hackers selling 'malware as a service'

This latest campaign against Australians was uncovered by Dario Durando, a senior threat analyst from ThreatFabric, a banking security platform based in the Netherlands.



Cybercriminals offer malware such as Octo as a product for other scammers to purchase. (Supplied)

He found the malware posing as an update for the Google Chrome mobile browser.

A hidden counter in the website's back-end revealed that there were 533 downloads in Australia, 362 downloads in Spain and just 64 downloads in the United States.

That counter has since been taken down.

Mr Durando said it was part of an increasing trend called "malware as a service" which is where hackers create something like Octo before renting it out to other criminals who then distribute it.

"All of these people collaborate just as normal businesses would do. So they have subscription schemes, they have discounts, they have support channels, it's very, very concerning," Mr Durando said

Dario Durando says there is a growing trend of malicious software being rented out as a service to wannabe scammers.(Supplied)

An advertisement spruiking Octo boasts the malware has a "high survival rate", gives hackers "full device control" and has the ability to steal two-factor authentication codes.

It's the same thing that happened with the malware that once solely targeted desktop computers.

"Nowadays with the predominance of mobile …criminals are deciding well it is the time to actually invest research and create more mobile malware because that's where the money's at," Mr Durando said.

What do we know about the 'Architect' behind this?

Eward Driehuis, vice president of fraud engineering at ThreatFabric, said the group responsible for Octo was Russian-speaking and possibly linked to the Russian cybercrime underworld.

"They are after your hard-earned cash," Mr Driehuis said, differentiating them from politically motivated groups which are run by foreign nations.

"There's definitely more than average attention to Australia."

Mr Driehuis urged Australians to be more cautious but his message was different for the nation's banks.

"I think you can never rely on awareness to be your first and last line of defence, that would not be fair to shift responsibility to your customers," he said.

Eward Driehuis says banks cannot leave the responsibility of cybersecurity solely to their customers.(Supplied)

Last year more than $3.1 billion was lost to scams — an 80 per cent increase from 2021 — according to a report from the Australian Competition and Consumer Commission.

Phishing, which is where people are tricked into handing over sensitive information like bank details, was responsible for $24.6 million in losses, an increase of 469 per cent from 2021.

Most of that money — $20.1 million — was stolen through bank transfer.

Another report from the corporate regulator, ASIC, found the big four banks reimbursed customers at a rate of between 2 and 5 per cent.

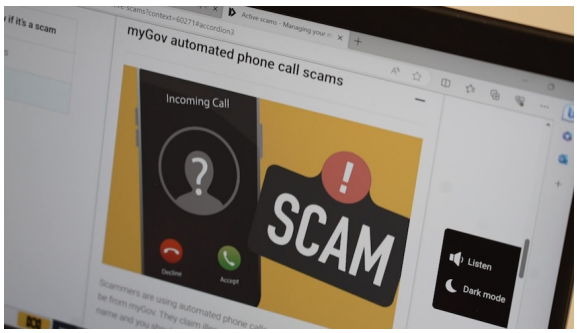
Calls for Australian government to protect 'soft target'

Stephanie Tonkin from the Consumer Action Law Centre said Australian banks weren't doing enough to protect customers, who were being hoodwinked by increasingly sophisticated scams.

"The scams that we hear about on our front lines every day are so complex, so involved that it is near impossible to detect," Ms Tonkin said.

Tips to protect yourself against scams

Scams are everywhere. So how do you protect yourselves? We asked experts from banks, police, telcos and fraud agencies. Here's what they recommend.



Read more→
"Australia is a soft target for scammers because we don't have the laws and systems in place to prevent scams from taking place," she said.

She urged the banking sector to take more responsibility because the scams were taking place on their platforms.

"Right now in Australia, we have banks posting multi-billion dollar record profits, yet Australians are the ones who are having to pay for being scammed through no fault of their own," she said.

"What we have in Australia is a vacuum in laws, a vacuum in responsibility, when it comes to scams and therefore what happens is the innocent victims are left to pick up the pieces.

"What we need is the Australian government to implement laws that put the banks on the hook for reimbursing scams victims that will drive the incentive for banks to invest in their systems to prevent and detect scams."

Stephanie Tonkin says urgent reform is needed in the banking sector to help protect scam victims.(ABC News: Margaret Paul)

A spokeswoman for the Australian Federal Police said Australians were facing "increasing, persistent and pervasive cybercrime threats".

"The AFP are innovating and exploring further opportunities to disrupt cybercriminals, particularly through our joint operations with Australian Signals Directorate," she said.

"We are coordinating national joint task forces against business email compromise, ransomware, remote access scams and identity fraud."

Banks back their own cybersecurity

Most of the banks contacted for this story spruiked their cybersecurity teams and told the ABC they take security seriously.

Both NAB and Beyond Bank said there has not been any fraud activity attributed to Octo.

A spokeswoman for the Australian Banking Association said its members will be holding discussions about anti-scam measures that could be implemented across the industry.

When asked about whether banks should be compensating customers for scams, she quoted a 2022 speech from the Assistant Treasurer, Stephen Jones, pouring water on the proposal.

"Some people are suggesting that the banks should always be liable. I don't support this approach, there should be a high bar on what is expected by all of our institutions – but if they meet all of their obligations it doesn't seem right that they are liable," Mr Jones said.

"If banks always pay, the net result creates a honey pot for scammers."

Here are the tips from our experts, which mostly covers both iPhone and Android users

Be suspicious

Just because someone has your private information, it doesn't mean they're legitimate.

"That information they can have gathered from different leaks. Leaks are happening pretty much every single day and criminals are buying that information," Mr Driehuis, from ThreatFabric, said.

"Don't just trust anyone … if you're getting a phone call, politely hang up and say you'll call them back on the official number."

Question everything

If you get a message from a loved one saying they need something, it might not be what it seems.

"Don't just believe people who say they are your son, your daughter, your mum or whomever," Mr Driehuis said.

The same goes for people asking for your personal information.

"Be careful what you give out because at the back end, there might be criminals collecting that kind of information in order to use that later in the scam," he said.

Be careful what you put on your phone

This advice is specifically for Android users who can sideload apps onto their phones. Stick with the Google Play store and pay attention to what you're installing.

Don't turn on accessibility services unless you absolutely need it. Be suspicious of apps which request it.

Our experts say that 99 per cent of mobile malware relies on accessibility services, which are designed to help people who have a disability.

It's a powerful tool which gives users a lot of capabilities and privileges, and one which hackers can take advantage of.

"All malware will be pretty much asking for this privilege from the get go, the moment the application [is] started, they will request for this," Mr Durando, from ThreatFabric, said.

"They will try to paint it as like a very essential thing for the execution of the application they're posing as.

"[You] shouldn't grant this kind of privileges to any app really, I personally cannot really see a reason to do so unless you're a power user, or … if you're a person with disabilities."

How do I know if my phone has been hacked?

One way to check is going to your phone's Settings and then the Accessibility page to see if there are any suspicious apps like file managers or QR code scanners.

If your device is infected, you might not even be able to get to this page because your phone might start flashing or automatically exit the Settings page, as though you tried to return to the home screen.

"That is for sure a indicator that you have an infected device because many malware families have … some sort of defence mechanisms that forces the user out of the settings page whenever it enters specific parts, which are the ones where you can uninstall the application," he said.

What do I do if my phone has been infected?

The safest thing to do is a full factory reset.

Posted 18 Nov 202318 Nov 2023, updated 19 Nov 202319 Nov 2023