Our ref: ACCC Flubot Information: 21 September 2021

Contact officer: Emma Robinson
Contact email: emma.robinson@accc.gov.au

To whom it may concern,

Re: Flubot scams, and potential for mobile banking compromise

The Australian Competition and Consumer Commission (ACCC) is currently contacting banks across Australia to make them aware of an emerging scam trend which may have significant impacts for Australian consumers.

Why is the ACCC contacting Australian banks?

We are currently contacting Australian banks to highlight the ACCC's concern that the next phase of the 'Flubot' malware scam is likely to evolve to include attempts to imitate mobile banking apps and access consumer's financial information. We seek your urgent attention to help minimise consumer losses.

What is the 'Flubot' scam?

We received our first report of the Flubot scam on 2 August 2021. To date, we have received over 12,000 reports of this scam.

Initially the scam involved consumers receiving text messages about voicemails or missed calls. Most recently the scam has evolved to now relate to messages about parcel delivery (examples available here). All messages contain a link. If a consumer clicks the link and downloads the app presented, their phone will be infected. Once installed, the application is able to read and send text messages, make calls and access contacts. We also understand the app uploads the infected devices' contact lists to a central server, which then distributes these to other infected Australian phones, so that those phones can send the Flubot messages to the numbers copied from contact lists. Our understanding is that while Flubot can only infect Android devices, clicking the links in the messages may case iPhones to download other malware.

More information on the Flubot scam, including steps consumers can take if they believe they have downloaded malware is available on Scamwatch at https://www.scamwatch.gov.au/news-alerts/missed-call-or-voicemail-flubot-scams.

How could this affect banks in Australia?

We are concerned that the next phase of the scam may involve mobile banking compromise. Following Flubot's emergence in Europe earlier this year, scammers have developed a html page overlay for banking apps in those countries. This means that if consumers download the malware, they will download all available overlays from the central Flubot server. These are designed to be identical to the login screens for their banking apps. When they open their banking app, consumers see a page identical to the login screen they are used to and enter their account and personal details, which are then sent back to the Flubot control server and can be used to access consumers bank details from then on. A technical analysis of the European variant discussed here is available on this archived webpage.

We are aware that at least one Australian banking overlay has been developed and are extremely concerned that these will be deployed for other Australian banking apps in the coming weeks. We are concerned that other Australia-specific banking login pages are being prepared for all banks and will soon be uploaded to the central server and widely disseminated to infected devices. This will result in infected users having their banking credentials compromised and will likely cause significant financial losses.

We note that we have also already received a report of a consumer with an infected device losing money in Australia due to entering their credentials into a "Google Pay" login screen as this overlay has already been developed.

Our expectation is that all banks will take steps to minimise the ability for scammers to compromise and access consumer accounts. We also expect all banks to support affected consumers to minimise losses and recover access to their accounts.

Please feel free to reach out to the ACCC directly for more information about Flubot scams.

Yours sincerely

Jayde Richmond

Director

Consumer Strategies and Engagement Team