ATO staffer leaks phone hacking how-to online, reveals fraud investigation tactics

Exclusive by political reporter Henry Belot

Updated about 6 hours ago

A tax office staffer has been disciplined after publishing a step-by-step guide to hack mobile phones, potentially teaching criminals to steal sensitive information.

The disclosure reveals the Australian Tax Office's (ATO) fraud investigation tactics and a push for powers normally associated with police and intelligence agencies.

The instructions showed how to bypass passwords and obtain data even if the phone battery is flat and does not have a sim card.

The tax office was unaware of the breach when contacted for comment by the ABC. The material was taken offline within an hour.

The employee, who published the material on LinkedIn, claims to have worked on intelligence taskforces and researched the so-called dark web for the Government.

The ABC understands the document was presented within the tax office.

It demonstrates how to retrieve deleted data, access text messages and phone call records.

The staff member lists "security awareness" as one of their key responsibilities on their profile, but the document could reveal their own passcode.

The disclosure has shocked some security experts who did not believe the ATO was developing these technical capabilities.

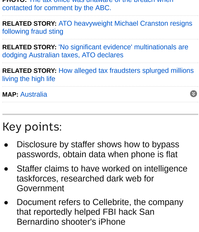


PHOTO: The tax office was unaware of the breach when contacted for comment by the ABC.

RELATED STORY: ATO heavyweight Michael Cranston resigns following fraud sting

RELATED STORY: 'No significant evidence' multinationals are dodging Australian taxes, ATO declares

RELATED STORY: How alleged tax fraudsters splurged millions living the high life

MAP: Australia

Key points:

- Disclosure by staffer shows how to bypass passwords, obtain data when phone is flat
- Staffer claims to have worked on intelligence taskforces, researched dark web for Government
- Document refers to Cellebrite, the company that reportedly helped FBI hack San Bernardino shooter's iPhone

An ATO spokeswoman said phones were only accessed with a warrant under the Crimes Act, or with written consent from the owner.

"For operational reasons, we do not disclose information about when different tools are used as part of our operations," she said.

The staff member has not been suspended, or fired. He has instead been reminded of his responsibilities under the public service act.

Federal Justice Minister Michael Keenan said he was concerned information has been published showing how the Tax Office can break into mobile phones.

Mr Keenan said the Government was taking the issue seriously, but he refused to confirm if the techniques were part of a new fraud strategy.

"I don't really want to go into the ATO's methodologies," he said.

"But the ATO, like other compliance agencies in Australia, do need to keep up with the way technology evolves and they do need to exploit technology like other agencies do.

"Obviously we're very concerned about that (information being published), but we do have robust systems within the ATO to detect that."

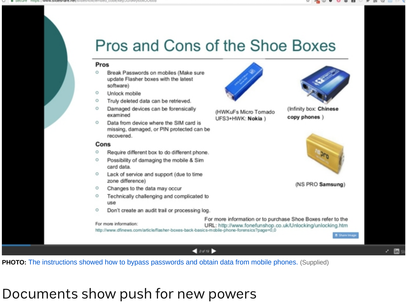


PHOTO: The instructions showed how to bypass passwords and obtain data from mobile phones. (Supplied)

Documents show push for new powers

The disclosure also reveals the growing influence of controversial Israeli company Cellebrite in Australia.

The company reportedly helped the FBI break into the San Bernardino shooter's iPhone — which became a crucial piece of evidence — when Apple refused to help.

The US Justice Department dropped a lawsuit against Apple compelling them to assist when it found a private contractor who would break into the phone for them.

Prime Minister Malcolm Turnbull has referenced this case while pushing for laws to force technology companies to reveal encrypted messages, should there be security concerns.

The document published by the ATO staffer refers specifically to Cellebrite software as a means of breaking into phones.

Last year the ATO paid the company $42,747 to train their staff how to use the software.

"Security staff use a range of technologies, including Universal Forensic Extraction software provided by Cellebrite, as part of our digital forensic capability to support investigations," the ATO spokeswoman said.

Fairfax Media reported last month that several Government agencies, including the Department of Human Services, the Australian Securities and Investment Commission, and Defence, now pay Cellebrite for services or software.

Revealing that information was inappropriate

Greg Austin, a professor at the Australian Centre for Cyber Security, said it was not appropriate for public servants to be sharing this information online.

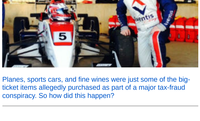
"It does expose a general problem about a lack of awareness, particularly among people who do not know their phones can be accessed as part of criminal investigations," he told the ABC.

"Having a person of his apparent skill suggests the tax office has been serious about accessing phones under warrants for many years."

The ATO and the Australian Federal Police exposed a $130 million tax fraud earlier this year involving one of its highest ranked officials, Michael Cranston.

Troy Hunt, a Microsoft regional director and security researcher, said the instructions were dated but was surprised the ATO were sharing that level of technical advice.

How did the case unfold?



Planes, sports cars, and fine wines were just some of the big-ticket items allegedly purchased as part of a major tax-fraud conspiracy. So how did this happen?

"It's very odd to see the ATO with a PowerPoint presentation on something that's more the domain of signals intelligence," he told the ABC.

Cellebrite has been contacted for comment.

Topics: government-and-politics, tax, security-intelligence, australia

First posted earlier today at 5:01am

AEST = Australian Eastern Standard Time which is 10 hours ahead of UTC (Greenwich Mean Time)