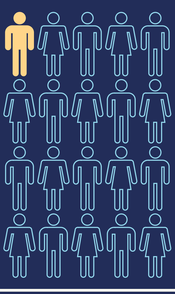
In a project funded by ACCAN, researchers at the Australian National University and IDCARE, Australia's national identity support service, analysed 4000 Australian identity theft cases. Here are some of the findings.

Identity Theft and Information and Communications Technology (ICT)

While identity theft is not new, communications devices have made attacks easier and quicker to execute.

1 in 20
identity theft attacks was associated with social media



1 in 10
identity theft attacks began with the telephone

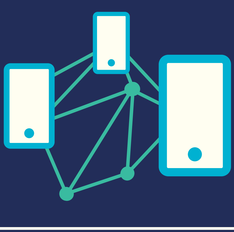
The most common ICT identity information to be compromised in an identity theft attack:

Online account usernames and passwords

Identity thefts involving only one single attack typically involved:

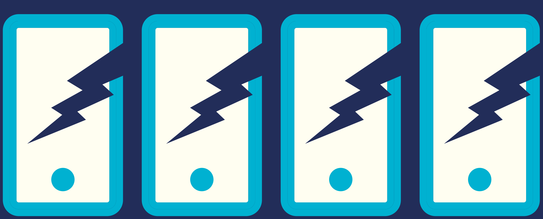
Social media, cyber stalking or the telephone

Social media
was the largest source of identity theft attack, controlling for dollar amount lost



Controlling for the duration of the identity theft attack, the most common target of attack was:

The user's mobile device



Most social media identity theft attacks were conducted on

Females

Cyber stalking
was more likely to be reported by male victims of identity theft

If you think you've been a victim of identity theft, you need to act quickly—
CALL IDCARE **1300 432 273** or visit **www.idcare.org** (free community service that provides assistance, advocacy and response plans).

Graphic design by Joanne Leong: **www.joannejyleong.com**
For research enquiries contact Dr. Sigi Goode: **sigi.goode@anu.edu.au**

The operation of the Australian Communications Consumer Action Network is made possible by funding provided by the Commonwealth of Australia under section 593 of the Telecommunications Act 1997. This funding is recovered from charges on telecommunications carriers.

idcare accan Australian National University