Identity & Cyber Security Community Aftermath Report 2018

About this Report

This report provides a summary of impacts identity and cyber-related crimes had on the Australian community throughout calendar year 2017.

It aims to inform readers about the experiences of everyday Australians with crimes that impact their personal information, wealth, and well-being.

Unlike other public reporting, IDCARE's Aftermath Report 2018 captures unfiltered views from our community on the good, the bad and the ugly in terms of prevention, detection, preparedness and response. IDCARE does not impose arbitrary thresholds nor is it constrained by legislative remit in supporting those who engage our services. Matters that present from clients are incredibly broad, including both online and offline scams and cybercrimes.

Change Opportunities for the Better

Our insights from 2017 present a number of change opportunities, including:

- Advancing law enforcement's efforts to upskill and pursue cybercriminals and offshore scammers targeting Australia;
- Ensuring key government credential issuers enhance their agility and relevance of response efforts to address community concerns and needs;
- Building and connecting response networks across industry and government;
- Exploring legislative, regulatory and market-driven models that influences market behaviour in avoiding the enabling of cybercrime and related scams;
- Building the evidence base on what is really impacting on our community when it comes to identity and cyber-related crimes.

About IDCARE

IDCARE was launched by the Commonwealth and New Zealand Governments in 2014 and 2015 respectively as a Trans-Tasman national identity and cyber support service for the community. Our organisation is a registered Australian not-for-profit charity and our frontline services are free to the community.

IDCARE is not a reporting entity, like ScamWatch or ACORN, rather it is a supporting entity that receives referrals from over 200 organisations annually, including ScamWatch and ACORN. The vast majority of these contacts result in the provision of specialist identity and cyber security counselling and pragmatic support. The largest referrer to IDCARE in 2017 was the Commonwealth government, and in particular, the Department of Human Services, the ACCC, ACORN, and the Australian Taxation Office.

Australian client experiences have been analysed and presented in this report. These clients reside in every electorate and their stories present a rich picture of Australia's capacity to prevent and respond to what is an enduring challenge to lift the economy's digitisation and underlying innovations.

Member and Advisor Briefings

IDCARE's Managing Director would welcome the opportunity to answer any questions or provide further briefing on this information. Bookings may be made by emailing <contact@idcare.org> or by calling 07 5373 0406.

Identity & Cyber Security Community Aftermath Report 2018 - Australia

During the 2017 calendar year IDCARE's community services responded to 35,033 engagements, resulting in over 46,680 hours in specialist identity and cyber security counselling support. This Aftermath Report captures the community's journey, the impacts felt, and the ways they were exposed to identity and cyber security threats.

Impacted Australians

47.8% of clients were **aged 25-44 years**. The next most represented group were **45-64 years** of age.

57.2% identified as being **female**.

35.4% of clients reside in **regional Australia.**

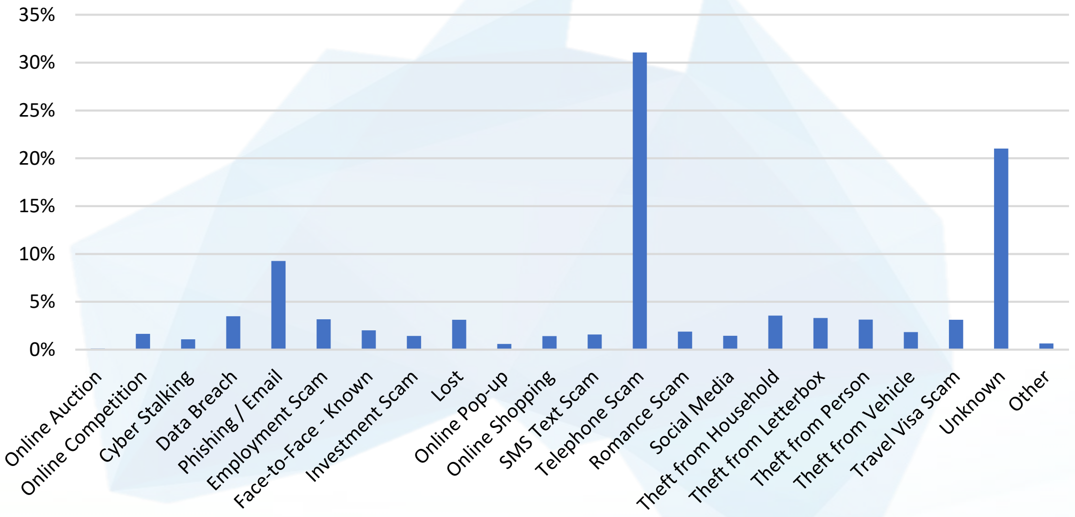
Detecting and Finding Help

1 in **1086** Australians aged 15 years and older engaged IDCARE in 2017.

71.8% of people were the first to detect their identity/cyber security event (not an organisation).

58.6% of clients were referred to IDCARE by a Commonwealth agency**,** 11.4% from telecommunications carriers and 11.3% from State/Territory Govt agencies. It took on average 2.3 stops before the community found IDCARE.

Method of Identity & Cybercrime Incidents Reported 2017



Response Journey

On average it took **27.5** non-consecutive **hours** to respond to an incident, involving the engagement of **8.2** different organisations on average **19.8** times. In more than seven out of ten cases, the community member had to prove to each organisation they were a victim of a crime. The average satisfaction rating provided by the community for engaging these organisations was 4.6/10. IDCARE's average client satisfaction score was 9.4/10. The best responders were financial institutions and Commonwealth agencies. The worst performers were telecommunications carriers, credit reporting agencies and law enforcement.

Crime Insights

31.2% of all compromise events occurred as a result of telephone scams mostly originating from offshore. The next most prevalent event category were phishing emails (9.8% of reports).

24.5% of clients experienced more than one identity and/or cyber crime event.

On average it took Australians **80.4 days** to detect the initial crime. It took criminals on average **23 days** to further target residents who experienced additional crimes (**109 days** was the average for data breaches resulting in subsequent crimes).

Around **7.1%** of clients experienced a direct financial loss as a result of the identity and/or cyber crime. On average these losses were **$17,083**.

Where the method of initial compromise is known, **73.4%** of clients experienced an engagement with the criminal **online**.