Identity & Cyber Security Community Aftermath Report 2018

About this Report

This report provides a summary of impacts identity and cyber-related crimes had on Queensland, as well as broader Australian community trends throughout calendar year 2017.

It aims to inform readers about the experiences of 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. We are physically co-located at the University of the Sunshine Coast, a major contributor to IDCARE's operations.

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.

We call members of the community who reach in to receive our free frontline support our Clients. The experiences of our Clients throughout 2017 have been analysed and presented in this report. These clients reside in every corner of our country and state. Their stories present a rich picture of their journey and our capacity to prevent and respond to what is an increasing threat to our community.

IDCARE's Community Service

IDCARE's frontline community support service can be contacted online via idcare.org or by calling 1300 432 273 (1300 IDCARE). IDCARE's funding allows our services to operate between 8am and 5pm Monday to Friday. Our frontline service is free, anonymous and confidential.

Identity & Cyber Security Community Aftermath Report 2018 - Australia

During the 2017 calendar year IDCARE's community services responded to 35,013 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 **female**.

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

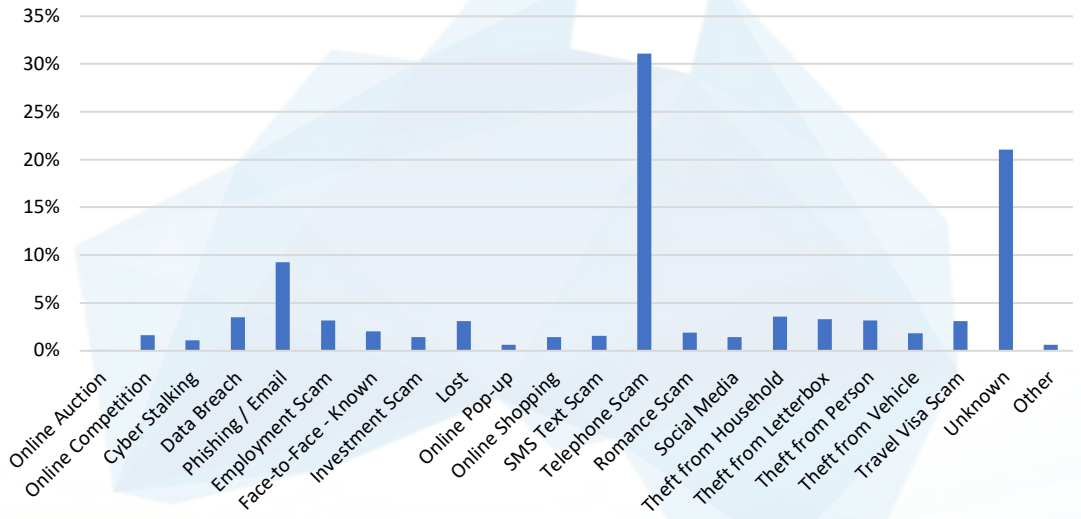
Detecting and Finding Help

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**.

Identity & Cyber Security Community Aftermath Report 2018 – Queensland

In 2017 IDCARE's community services responded to 9,118 engagements from Queensland residents, investing around 12,149 hours in specialist counselling support. Around half of Queenslanders impacted resided outside of metropolitan areas (the largest representation of regional Australia compared with any other State). Queenslanders were most impacted by telephone scams. Just over one in ten did not know how their personal information was compromised, but felt the impact of the compromise.

Impacted Residents

1 in **998** residents aged 15 years and over engaged IDCARE during 2017.

37.40% of clients were aged between 25 and 44 years old.

61.91% identified as **female**.

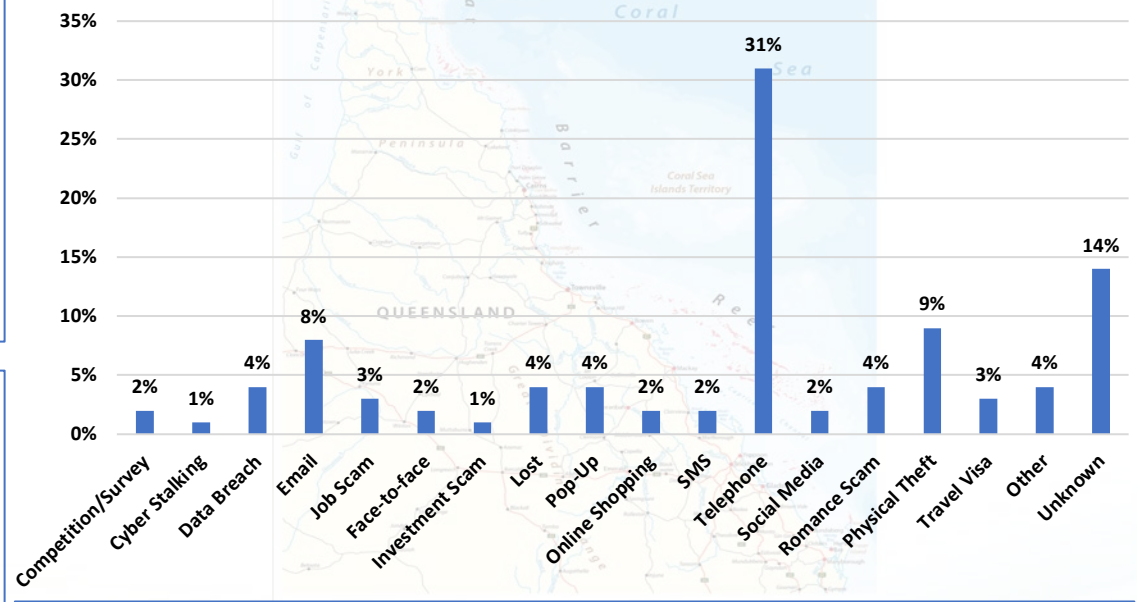
Detecting and Finding Help

68.11% of residents were the first to detect their cyber and identity security event (not an organisation).

31.15% of clients were referred to IDCARE by an organisation. Of these referrals, **33.59%** came from Commonwealth agencies.

It took residents on average **20.28 days** to detect their incident, with an average loss of approximately **$14,282**

Method of Identity & Cybercrime Incidents Reported 2017



Response Journey

Financial institutions were rated by residents as the best responders to identity and cyber crimes (averaging **6.82/10** for satisfaction). The worst performers were telecommunication service providers (averaging **4.35/10** for satisfaction). IDCARE's client satisfaction score for residents was **9.43/10**.

On average residents made **17.12** contacts to **8.3** separate organisation in response to their incident over an average of **30.64** non-consecutive hours.

Crime Insights

It took on average **9.84 days** for the criminals to commit further crimes following the initial identity or related cybercrime event.

23.75% of residents experienced the misuse of their identity credentials and **14%** did not know how the initial crime occurred.

Where the compromise event is known, **31%** of residents responded to a **telephone scam**, **9%** of residents experienced a **physical theft** of their credential(s) or device(s), and **8%** responded to a **phishing email.**

Around two-thirds of clients experienced an event that originated online (i.e. cybercrime) where the criminal was believed to originate from offshore.

IDCARE Community Aftermath Report 2018 – When Transnational Crime Comes Calling

In 2017 around one in three clients of IDCARE experienced a scam where they had direct communication on the telephone to a transnational crime group. Telephone scams dwarfed all other compromise types impacting the Australian community. These scammers appeared to almost exclusively operate from offshore. There were two distinct varieties of telephone scams reported to IDCARE. The first aim to deceive individuals to provide personal information, credentials and payment information (including the purchase of gift cards and vouchers). The other variety aimed to deceive individuals to provide remote access to their device in order for the criminals to access Internet-banking, other online accounts and related personal information. At times the two methods blurred. The fallout, impacts experienced and response journey for most Australians to engage IDCARE had similarities.

Autopsy of the Scams

72.4% of telephone scammers attempted to deceive the recipient into believing that they were engaging one of four brands.

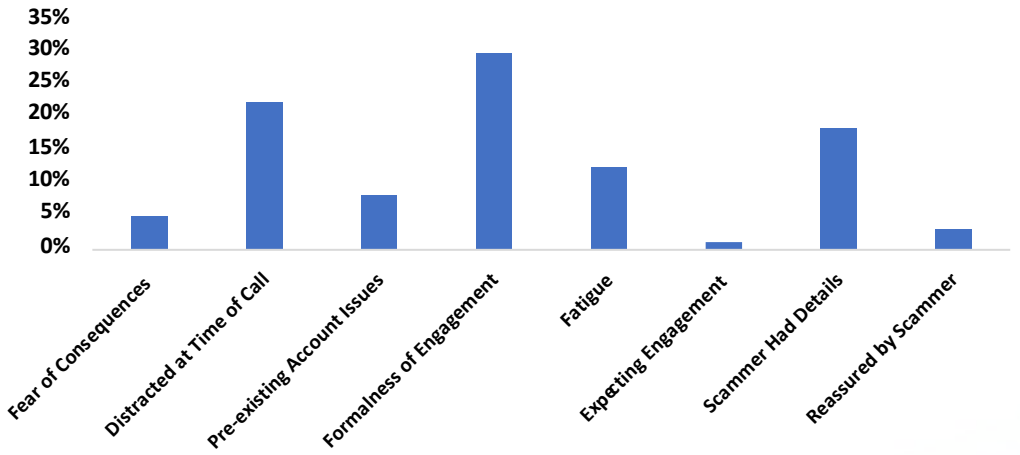
27.5% of telephone scams led to a person providing remote access to their computer or laptop.

20.3% of telephone scams resulted from an initial contact from the suspected criminal via means other than the telephone (such as Internet pop-up, email, or text message).

14.2% of Australians experienced further misuse of their identity information and/or accounts following the initial telephone scam.

The three most common misuse events reported were *unauthorised access of bank accounts* (**58.1%**), *new credit card applications* (**6.8%**) and *unauthorised spend on existing credit cards* (**6.6%**).

Stated Reasons for Believing the Telephone Scam



Detection & Response Journey

Almost a third of Australians believed the scammers because they created a sense of bureaucracy and formality to their engagement (eg. Scammer provided an employee ID or escalated to other departments or their supervisor). **74.6%** of individuals reported that they first detected the telephone scam themselves. Also playing a significant role was the family and friend "bystander" as the initial detector in **17.3%** of cases. On average it took **1.6 days** to detect the telephone scam (the mode and median were reported as the day of the scam).

Australians spent **20.4** non-consecutive hours on average responding to their telephone scam, engaging **7.8** different organisations a total of **16.1** times.

Communication Exploitation

Over the six months from October 2017 to March 2018, IDCARE received information about **212** unique telephone numbers believed to be used by telephone scammers.

197 of these phone numbers were tested by IDCARE during the period and found to be active and suspected of impersonating a number of industry and government brands.

60.8% of these numbers were linked to service providers that exclusively provided Voice over Internet Protocol (VoIP) communications.

7.1% of all numbers reported as suspected scams were either inactive or disconnected at the time of testing or were believed to be "spoofed" numbers (impersonations).

Spoofed numbers are a growing trend in other parts of the world. A spoofed number is one where the Caller ID presents a number different to the one that is calling, and this Caller ID number belongs to an innocent third party.