BDO

IDEAS | PEOPLE | TRUST

Forensic Services

Australian Scam Culture Report

December 2023 Quarter

Introduction

As we reflect on the trends and developments of the past quarter, it becomes evident that the landscape of scam activities is continually evolving. In the latest edition of the Australian Scam Culture Report, December 2023 Quarter, we examine the trends and patterns in scam activities, exploring their implications and proposed countermeasures.

Text messages and emails remained the primary conduits for the distribution of fraudulent schemes throughout the 2023 calendar year. We also saw the 45 and over age groups overall, experience a 7 per cent decline in reported scam activity, however this was predominantly due to a decline in reported scams from the over 65 age group. Despite this decline, the over 65 age group remained the primary target group for scam activity at 26 per cent. Interestingly, we also observed an increase of 5 per cent in scams reported by the 35-44 age group.

Activity across the dark web continues to play a significant role in the global landscape of cybercrime and scams. Interestingly, we have seen a substantial increase in the cost of some of the stolen credentials, financial information, and personal identification details available for sale on the dark web. This increase in cost may be attributed to recent high-profile crackdowns, resulting in greater difficulty in obtaining such data and prompting scammers to elevate their prices in response to heightened demand and diminished supply.

We saw a 24 per cent decline in total dollars lost to scams during the December 2023 quarter compared to the previous quarter. This was coupled with a 14 per cent decline in the average number of reported incidents, even amidst the typically heightened scam activity observed during the festive season. Proactive initiatives such as those led by the Australian Securities and Investments Commission (ASIC) and the National Anti-Scams Centre (NASC), together with high profile media coverage of cyber breaches and scams are likely contributing to an overall increase in public awareness of scams and strategies for self-protection.

In an environment of increased responsibility placed on the victims, we strongly advocate for all Australians to educate themselves on the prevalent types of scams within the community and adopt better protection and risk mitigation practices.

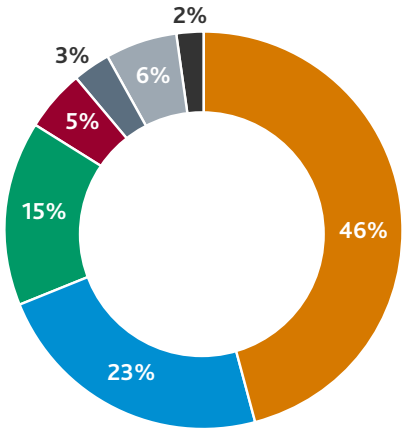
Michael Cassidy
BDO National Forensic Services Leader

The results

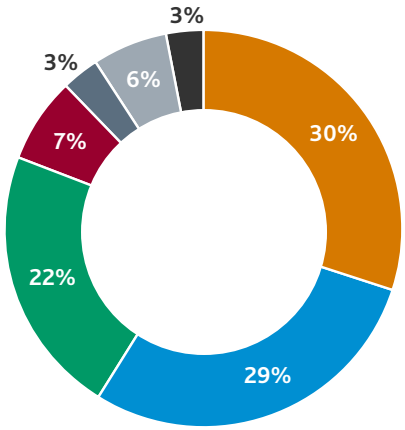
Scam delivery method (four-quarter comparison)

During the 2023 calendar year, text messages and emails remained the predominant channels for delivering scams. This is likely due to a combination of cost effective widescale distribution, uniform adoption by users, accessibility, and the increasing sophistication of phishing techniques.

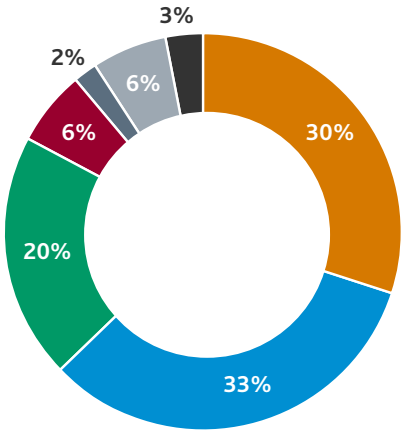
March 2023 quarter scam delivery method



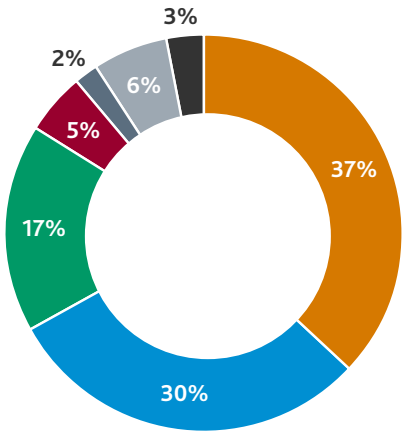
June 2023 quarter scam delivery method

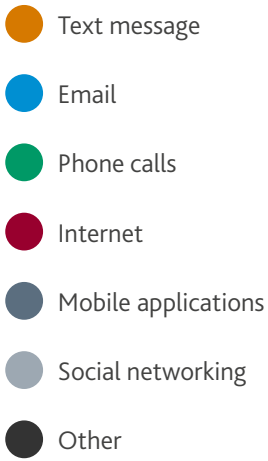


September 2023 quarter scam delivery method



December 2023 quarter scam delivery method



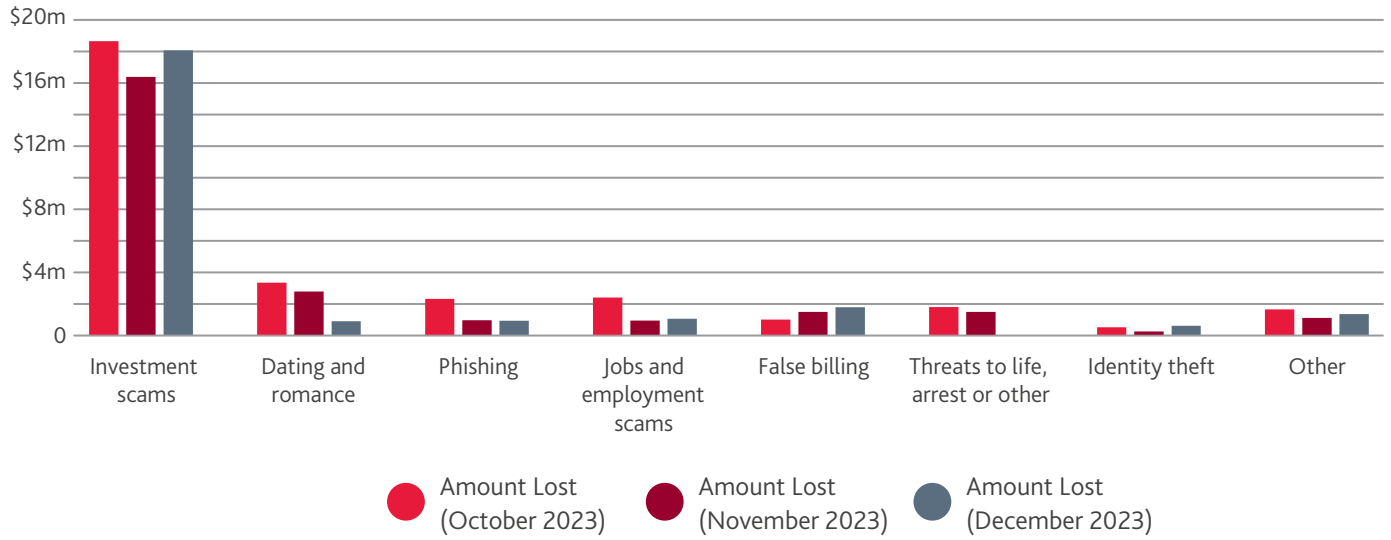


Source: 2023, All scam types stats - Scamwatch, Australian Competition and Consumer Commission, ©Commonwealth of Australia

AUD$ lost by scam type

Despite investment scams continuing to lead in terms of monetary losses, there has been a decline in the total dollars lost overall during the December 2023 quarter compared to the previous quarter. In the September 2023 quarter, losses to investment scams exceeded AUD $69 million. However, during the December 2023 quarter, this figure decreased by 24 per cent, but remains significant at just under $53 million.

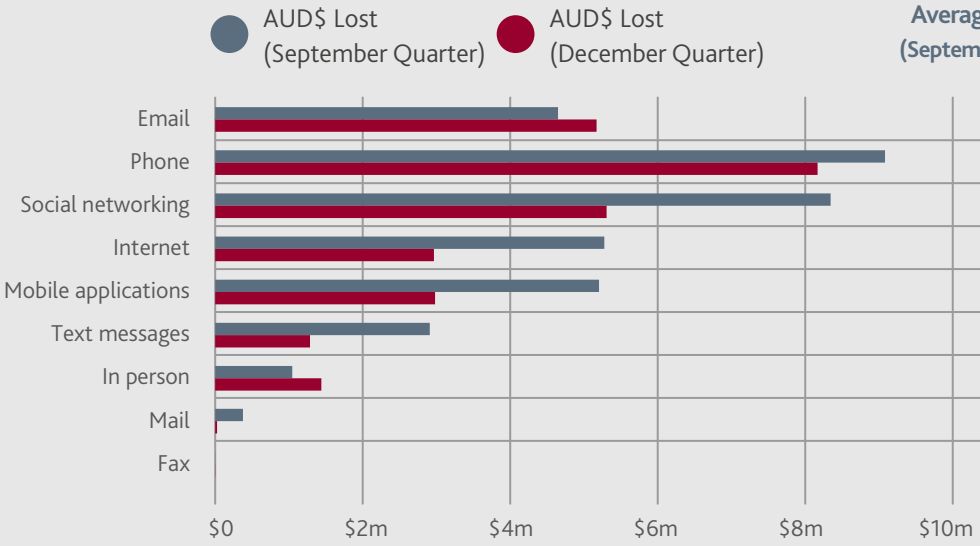
*Other includes: Remote access scams, classified scams, rebate scams, online shopping scams, pyramid scheme, and health medical product scams.



AUD$ lost by delivery method (two-quarter comparison)

Text messages and emails remained the primary delivery method for scams in the December quarter, however the average number of reports dropped by 14%, despite the festive season, which typically sees a rise in scam activity.

There are several factors which could be contributing to the decline in reported scam activity. These include recent proactive cyber strategies announced by the Australian Government, along with extensive media coverage of cyber breaches and scams. These initiatives are likely enhancing public awareness of scams and fostering the adoption of self-protection strategies.

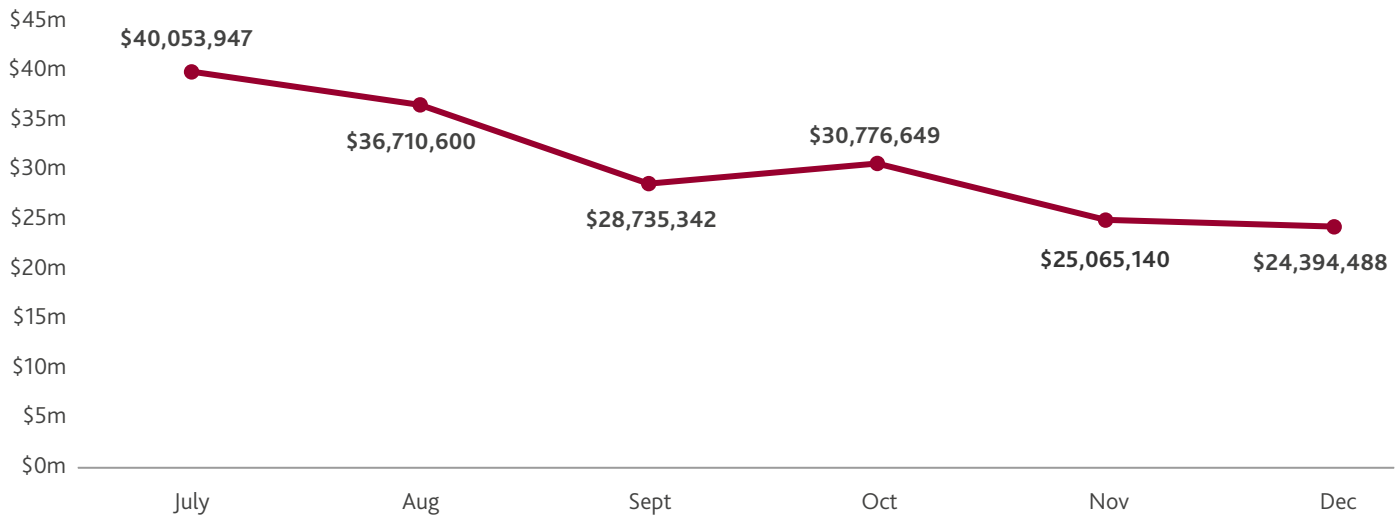


	Average no. of reports (September Quarter 2023)	Average no. of reports (December Quarter 2023)
Email	8,667	6,634
Phone	5,311	3,759
Social networking	1,410	1,265
Internet	1,604	1,239
Mobile applications	578	471
Text messages	7,925	8,414
In person	348	340
Mail	231	210
Fax	3	6

Source: 2023, All scam types stats - Scamwatch, Australian Competition and Consumer Commission, ©Commonwealth of Australia

Total AUD$ lost by scams (two-quarter comparison)

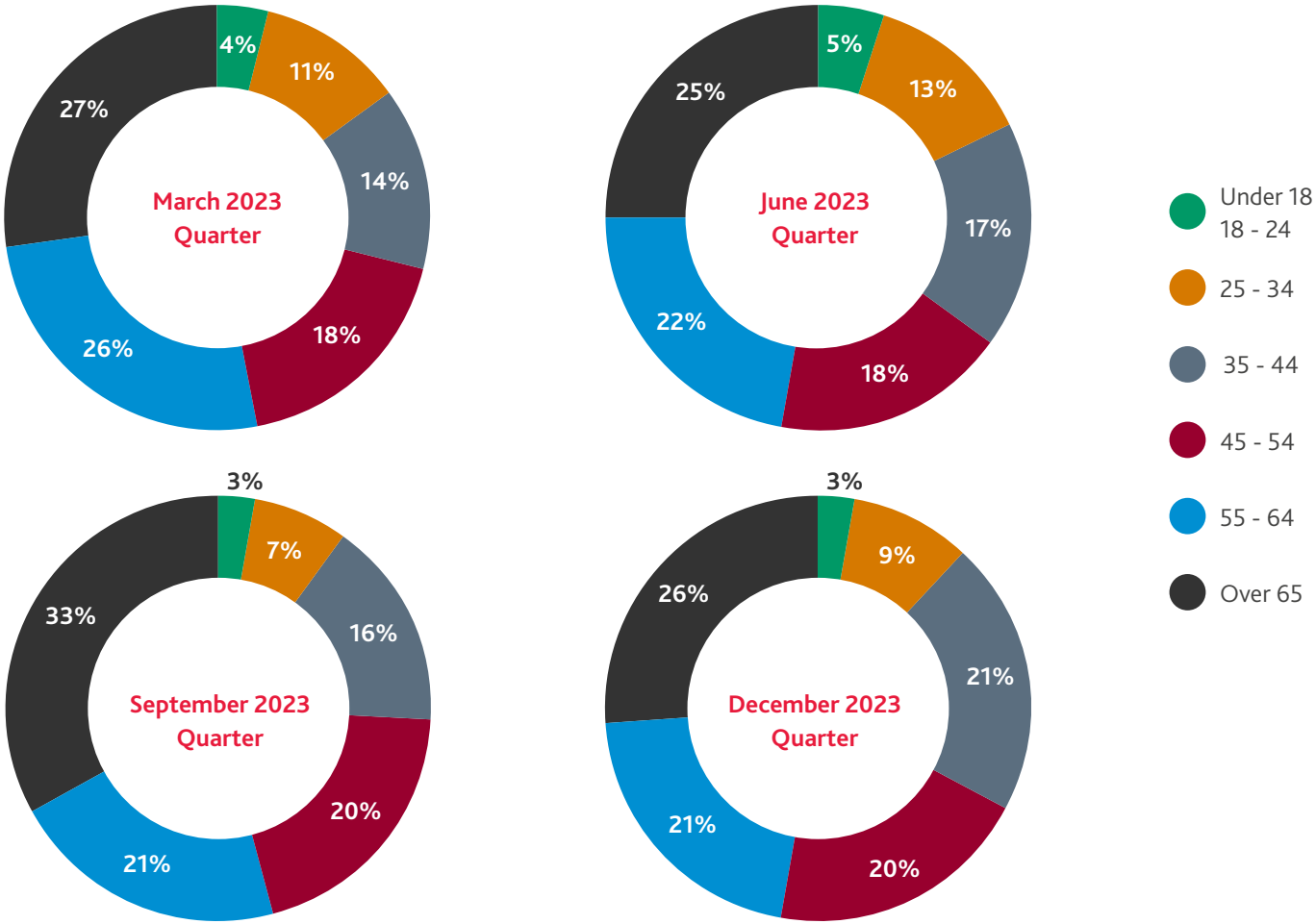
The cumulative losses in AUD resulting from the top 10 reported scams in the December quarter decreased by approximately $25 million. In the September quarter, the total losses amounted to $105,499,889; in the December quarter, they reduced to $80,236,277.
We observed a significant decrease of 42 per cent in AUD lost to reported scams from the June to December quarters, totalling $59,043,598.



Source: 2023, All scam types stats - Scamwatch, Australian Competition and Consumer Commission, ©Commonwealth of Australia

Age groups targeted in scams (four-quarter comparison)

During the December 2023 quarter, there was a notable shift in demographics concerning reported scam activity by age group. The 45 and over age groups overall, experienced a 7 per cent decline in reported scam activity, however this was due to a decline in reported scams from the over 65 age group, whilst the 35-44 age group recorded a 5 per cent increase.

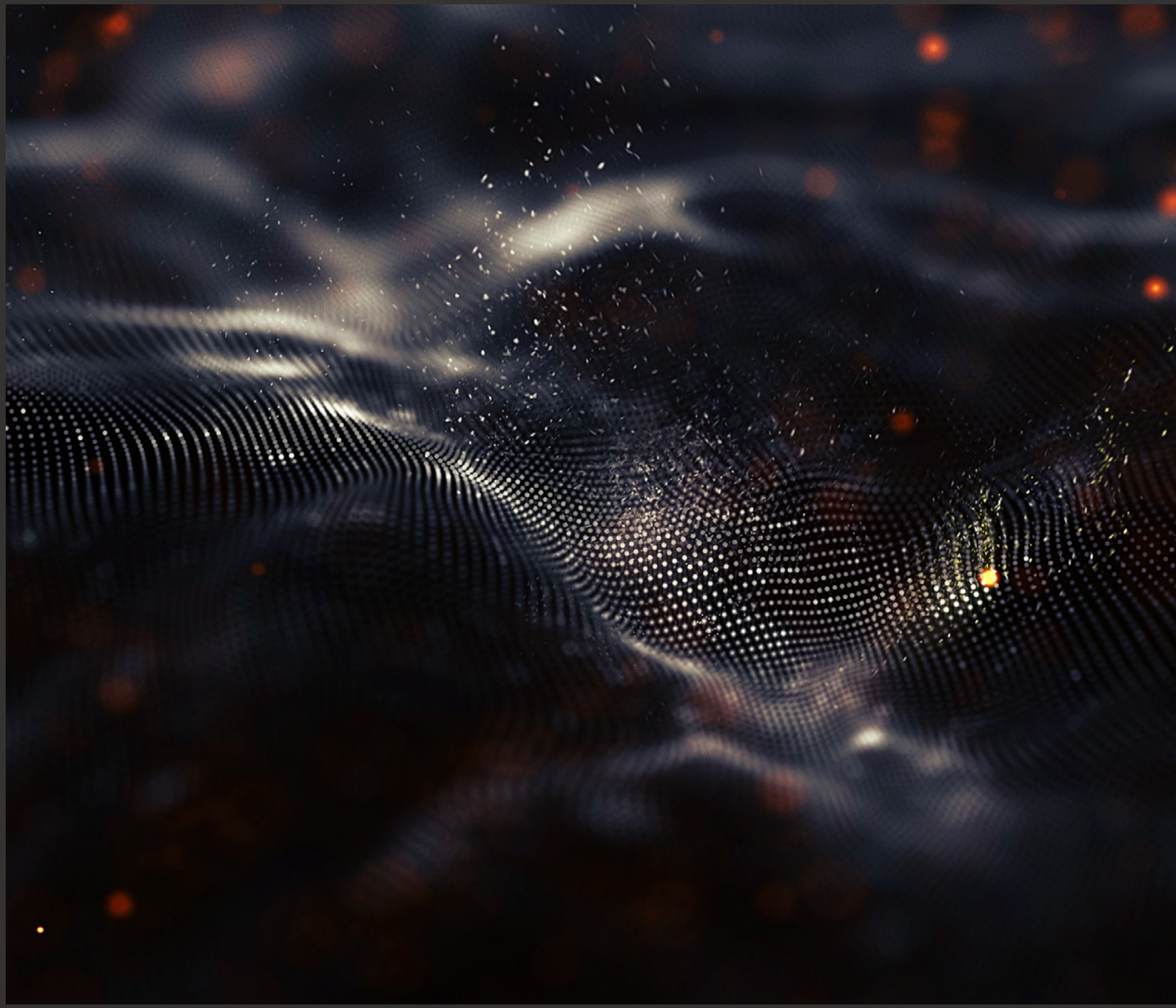


Source: 2023, All scam types stats - Scamwatch, Australian Competition and Consumer Commission, ©Commonwealth of Australia

A snapshot: dealings on the dark web

The term dark web – refers to a hidden part of the internet that is not indexed by traditional search engines. Accessing the dark web is done using specific software to anonymise activity, and as such it provides a great deal of protection and anonymity for the illegal sale or trade of personal data, including stolen credentials, financial information, and personal identification details. Scammers can purchase this data to execute a range of scams including identity theft.

All figures are in comparison to the September 23 quarter (next page):



Dealings on the dark web

Identity Information

- **Australian Visa + $4,000 credit card balance:** $165 (not previously reported on)
- **Passport (various nationalities):** $2,372 (up from $1,399)
- **Covid-19 Certificate:** $157 (up from $139)
- **Drivers Licence:** $844 (up from $465)
- **US Fullz (identity theft):** $25 (up from $16)
- **US Identity Cards:** $299 (down from $854)

Account hacking

- **Email:** $262 (down from $668)
- **Facebook, Instagram, Snapchat, WhatsApp:** $299 (down from $310)
- **WeChat:** $224 (up from $154)
- **LinkedIn Company Profile:** $17 (up from $11)
- **Phone/SMS/Email:** $411 (down from $1,089)

Carding (Visa, MasterCard, American Express (AMEX)

- **Mastercard/Visa $3,000 USD balance:** $138 (down from $163)
- **American Express $3,000 USD balance:** $187 (not previously reported on)

Distributed denial-of-service (DDoS) attack

A DDoS attack is a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites.

- **Clearnet:** $486 (up from $139)
- **ToR network:** $1,143 (up from $249)

Money transfer costs

- **Payment transfers $900** - $165 (down from $187)
- **Payment transfers $1,300** - $209 (down from $249)
- **Western Union Transfer $5,000** - $125 (up from $78)

Latest trends

Traders and buyers continue negotiating terms to resolve disputes, including moderation. Like any marketplace, trust is crucial for successful transactions – particularly where the parties involved are anonymous. Sellers inviting buyers to negotiate with them and reach a solution has become a standardised feature.

- There has been a significant increase in costs of many of the stolen credentials, financial information, and personal identification details on the dark web.
  - The increase in costs is likely due to a combination of factors including recent high-profile crackdowns and an increase in security awareness resulting in greater difficulty in obtaining source data as well as an increase in embedded security measures in identity documents. The elevation of prices is ultimately a response to increased demand and diminished supply.

- We have witnessed a notable uptick in discussions or indications within the dark web community regarding cyberattacks that are believed to be sponsored or orchestrated by nation-states. This increase in activity is occurring against the backdrop of heightened global tensions and unrest.

About BDO

BDO's forensic experts work with organisations to effectively identify and respond to suspicious activity. The multidisciplinary team includes certified accountants, certified fraud examiners and forensic accountants, forensic technology professionals, licensed investigators, financial analysts, and former members of law enforcement.

Michael Cassidy
National Leader, Forensic Services
michael.cassidy@bdo.com.au
+61 8 6382 4761

Stan Gallo
Partner, Forensic Services
stan.gallo@bdo.com.au
+61 7 3237 5995

Karyn Lander
Director, Forensic Services
karyn.lander@bdo.com.au
+61 8 6382 4914

John Karamoschos
Director, Forensic Technology,
Forensic Services
john.karamoschos@bdo.com.au
+61 2 8221 2235

Conor McGarrity
Partner, Forensic Services
conor.mcgarrity@bdo.com.au
+61 7 3237 5841

Katie Bourne
Director,
Forensic Services
katie.bourne@bdo.com.au
+61 2 8221 2266

Michael Tarnawsky
Senior Forensic Technology Specialist,
Forensic Services
michael.tarnawsky@bdo.com.au
+61 7 3237 5693

1300 138 991
www.bdo.com.au

NEW SOUTH WALES
NORTHERN TERRITORY
QUEENSLAND
SOUTH AUSTRALIA
TASMANIA
VICTORIA
WESTERN AUSTRALIA

AUDIT • TAX • ADVISORY

This publication has been carefully prepared, but is general commentary only. This publication is not legal or financial advice and should not be relied upon as such. The information in this publication is subject to change at any time and therefore we give no assurance or warranty that the information is current when read. The publication cannot be relied upon to cover any specific situation and you should not act, or refrain from acting, upon the information contained therein without obtaining specific professional advice. Please contact the BDO member firms in Australia to discuss these matters in the context of your particular circumstances.

BDO Australia Ltd and each BDO member firm in Australia, their partners and/or directors, employees and agents do not give any warranty as to the accuracy, reliability or completeness of information contained in this publication nor do they accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it, except in so far as any liability under statute cannot be excluded.

BDO Australia Ltd ABN 77 050 110 275, an Australian company limited by guarantee, is a member of BDO International Ltd, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

BDO is the brand name for the BDO network and for each of the BDO member firms.

© 2024 BDO Australia Ltd. All rights reserved.

24-02-1268