



# What we will cover

1. Investment Scams
2. Romance Scams
3. Phishing for information - email and SMSs
4. Viruses
5. Panic Scams
6. Identity Theft
  
7. Discussion

There are too many scams to cover all scam types

# Telltale signs of a scam



It might be a scam if:

- You receive an unexpected request
- There's a promise or a threat
- There's a sense of urgency
- Required payment method is untraceable and unrecoverable
- Something is "off"

Fundamentally scams work by getting you to do what the scammer wants.



# ACCC Scamwatch 2021 Report

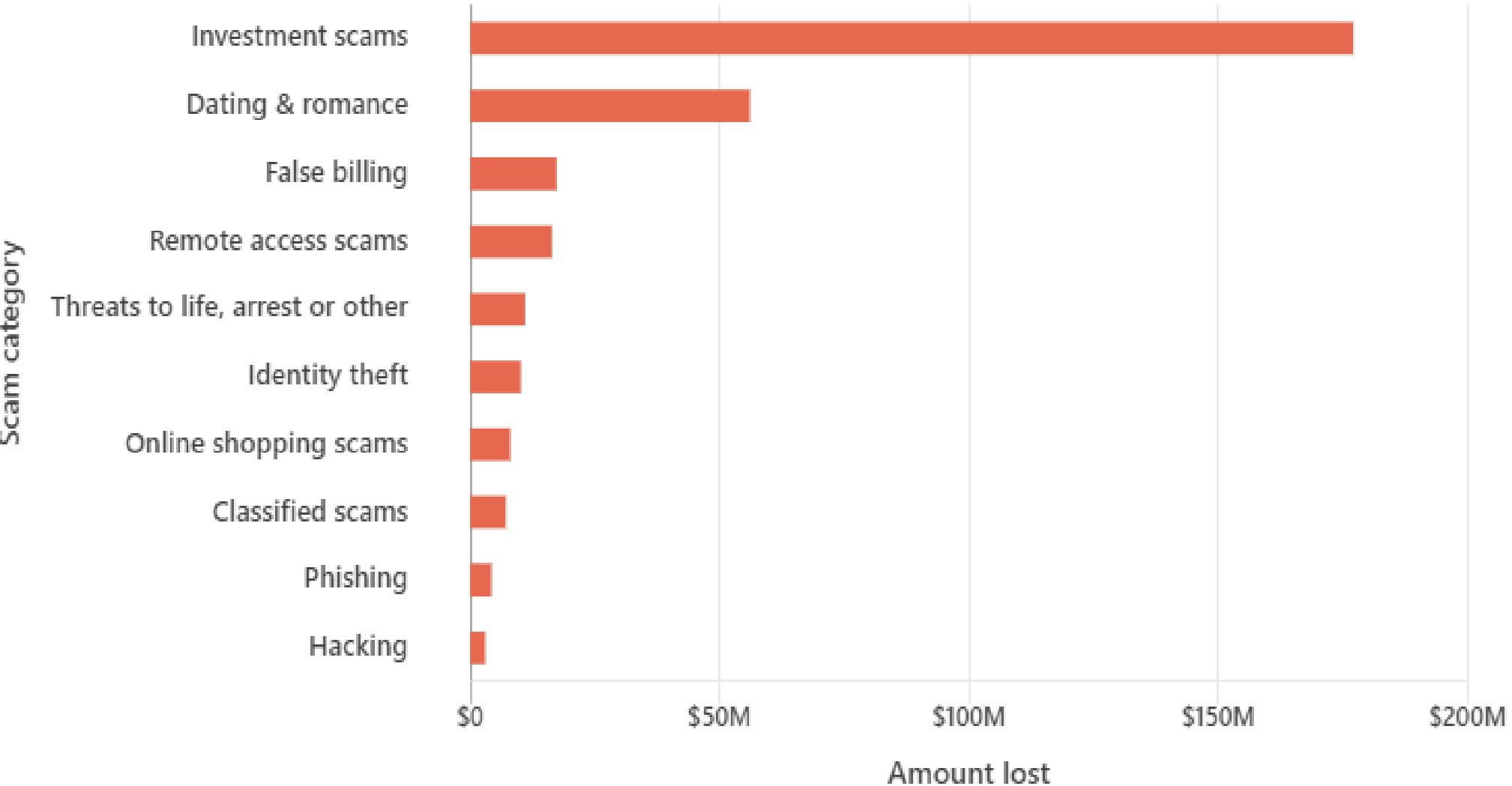
(ACCC - Australian Competition and Consumer Commission)

- 200,000+ scams reported each year in Australia.
- \$280 million lost in reported scams.
- \$2,000 million in investment scams (ASIC)
- **[www.scamwatch.gov.au](http://www.scamwatch.gov.au)**

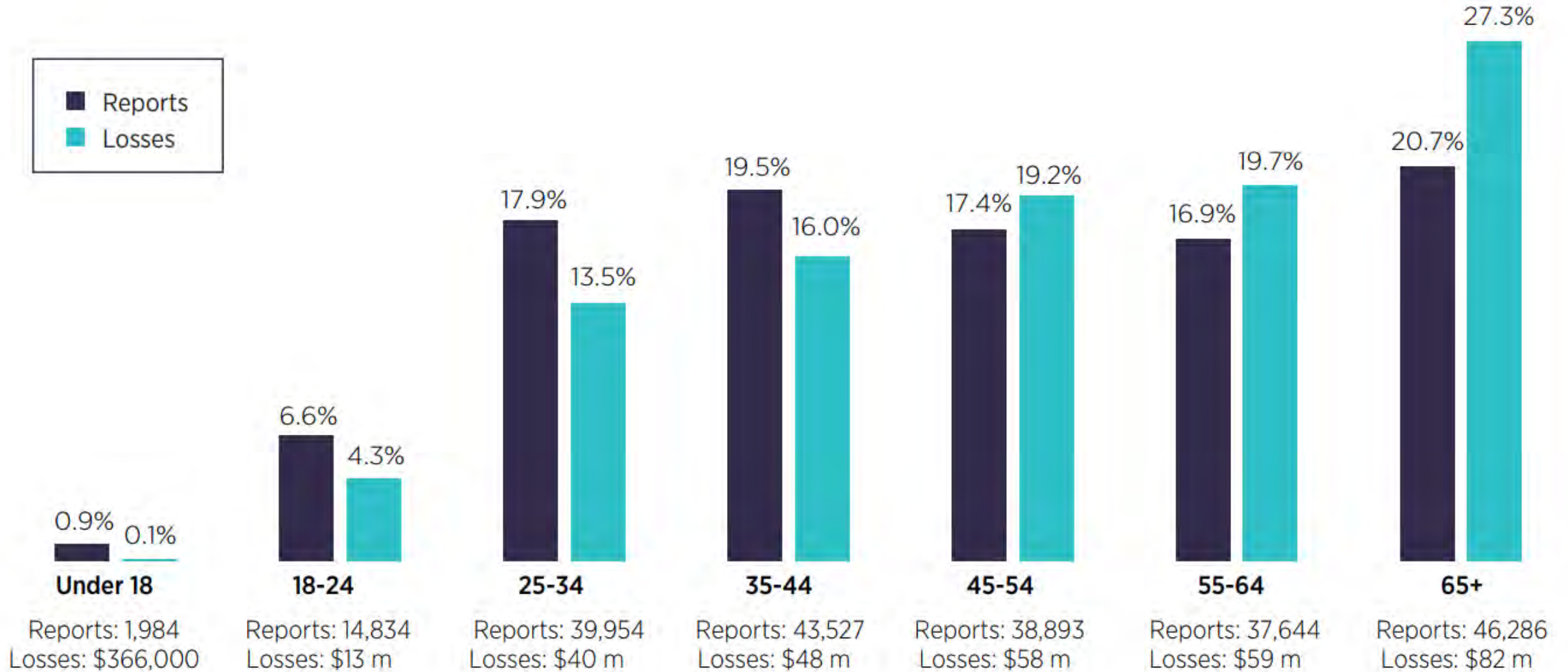
**Table 2.3** Losses and number of reports by category

<b>Scam category</b>	<b>Reported losses 2021</b>	<b>Number of reports 2021</b>	<b>Number of reports with loss</b>
Investment scams	\$177,184,295	9,664	4,068 (42.1%)
Dating & romance scams	\$56,175,428	3,424	1,379 (40.3%)
False billing	\$17,303,665	21,545	1,881 (8.7%)
Remote access scams	\$16,412,258	15,698	1,330 (8.5%)
Threats to life, arrest or other	\$11,077,551	32,426	658 (2.0%)
Identity theft	\$10,159,930	22,354	951 (4.3%)
Online shopping scams	\$8,074,469	20,694	7,436 (35.9%)
Classified scams	\$7,114,830	9,561	3,080 (32.2%)
Phishing	\$4,324,128	71,308	861 (1.2%)
Hacking	\$3,041,484	15,141	547 (3.6%)
Jobs & employment scams	\$2,697,500	3,453	308 (8.9%)
Travel, prizes and lottery scams*	\$1,984,215	4,976	322 (6.5%)
Pyramid Schemes	\$1,341,389	487	215 (44.1%)
Ransomware & malware	\$1,172,034	3,623	54 (1.5%)

# The top 10 scams by amount lost.



# Age





# Top contact methods by reports



**50%**

Phone

**144,603** reports

**\$100 million**  
reported lost



**23%**

Text message

**67,180** reports

**\$10 million**  
reported lost



**14%**

Email

**40,186** reports

**\$48 million**  
reported lost



**4%**

Internet

**12,502** reports

**\$51 million**  
reported lost



**4%**

Social networking/  
online forums

**10,140** reports

**\$56 million**  
reported lost

# 1 - Investment Scams

- Often hard to tell what is a scam. Is a poker machine a scam?
- Often investment scams are legitimate businesses but dealing with them is like gambling in a casino. Some involve cryptocurrencies.
- Investments increasingly easy to make – often like a computer game.
- Seniors are a particular target, seen as having money and wanting higher returns than bank interest.

**Sydney Morning Herald – March 20, 2022**

Professor F... signed up to an investment scheme in October last year after getting **an unsolicited phone call** from a woman representing an investment company called QPE Securities.

“They **had a very impressive website and an ASIC listing,**” he said. ... Professor F... checked the company’s ASIC record and found that it was registered with an ABN and an ACN. It had provided him with a daily report on his investment, a local bank account and an adviser he regularly spoke to using a local phone number. Professor F... initially invested \$10,000 and then \$18,000.

Then his bank contacted him to say it had blocked his account because it had detected “nefarious trading”. He did not believe the bank when it told him that QPE Securities was operating a scam.

He told them the company had an address in Chifley Tower. ‘Oh dear’ was the bank officer’s response - “everyone has an address in Chifley Tower”. When Professor F... visited Chifley Tower to front the company representatives, the concierge could find no record of the company in the building. The concierge told him he received numerous calls each day for companies with a bogus Chifley Tower address.

The bank was able to retrieve the \$18,000, but the earlier \$10,000 deposit had not been returned.

# Typical scam

- Scam starts with a phone or social media approach. Client directed to web site. Offers higher investment returns
- Web site are often very slick and professional. Initial investment goes well.
- Scammers often promised high yields for short term investments.
- Good site is **[www.moneysmart.gov.au/investment-warnings](http://www.moneysmart.gov.au/investment-warnings)**

# **SPECIAL REPORT: Dick Smith's Latest Investment Has Experts in Awe And Big Banks Terrified**

Australia citizens are already raking in millions of dollars from home using this "wealth loophole" - but is it legitimate?

SEPTEMBER 26, 2020



Dick Smith comes out with new secret investment that's making hundreds of people in Australia very rich

(news.com.au) - Dick Smith is an Australian record-breaking aviator, philanthropist, political activist and serial entrepreneur.

Mr Smith, who made his name and fortune with his chain of electronics stores, is famous for his commitment to protect interests of ordinary people.

Lately, he appeared on The Project and announced a new "wealth loophole" which he

## READER RESULTS

PROFIT: AU\$5,552



"I've been using [Bitcoin UP](#) for just over 2 weeks, I've taken my initial deposit from AU\$350 to AU\$5,802. That is far more than I make at work."

**Kyle McLennan**  
Subiaco, WA

PROFIT: AU\$9,200



"I've hit over AU\$9,200 in profit after just a

## 2- Romance Scams

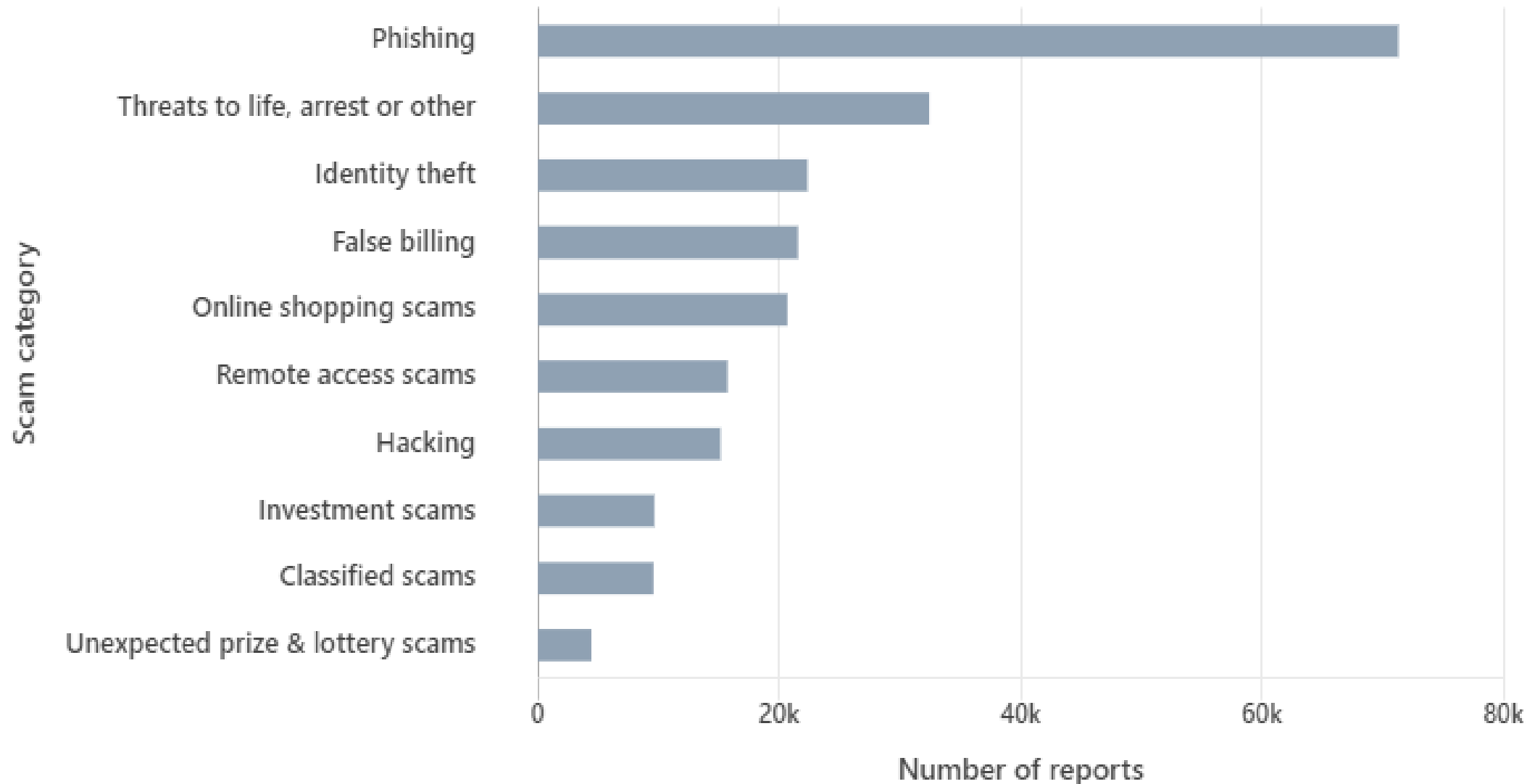
- You meet someone online and after just a few contacts they profess strong feelings for you, and ask to chat with you privately. After gaining your trust – often waiting weeks or months - they tell you an elaborate story and ask for money, gifts or your bank account/credit card details.
- Average loss in Australia \$40,000. \$10 million lost in typical year
- To protect yourself always consider the possibility that an approach may be a scam, especially if the person says they are overseas. Never send money to someone you haven't met in person.

# 3 – Phishing

May come via email or SMS messages or some other method. Asks you to click on a link.

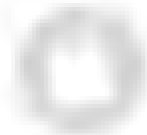


# Top 10 scams reported by number





# URGENT: Your Apple ID Has Been Compromised



Apple Support

to me ↗

12:29 PM (0 minutes ago)



Dear customer,

We have received notice that your Apple ID has been compromised on September 8th 2020 at 04:31 p.m. EST.

Your Apple ID has been blocked for security purposes and will be deleted if you don't take immediate action.

Please note that if you do not visit the following link within 24 hours to provide the necessary information, your Apple ID will be permanently removed. [Click here to access Apple Support and protect your personal information.](#)

Apple Support  
[apple.com](https://apple.com)



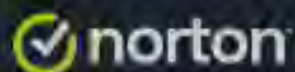
**Norton™** Notification <EXNMWKT VXU@KESNI.antivirus.com>



21/02/2022 11:22 PM

To: jcameron\_448@hotmail.com

## Your Norton™360 Portion My Expire Soon



Your subscription to Norton™360 Total Protection has expired on **February 20, 2022**

After the expiry date has passed your Device will become susceptible to many different virus threats.

**Your PC is unprotected, it is exposed to viruses and other malware**

**Available (50%)** Renewal Discount

**Expired on** : 02/21/2022

**Licenses** : 10 Device

**Email** : REDACTED

[Renew Subscription](#)

## New restriction on your wallet !



Metamask.io <webinarinfo@webinarjam.net>

3:47 PM

To: Robert

Metamask requires all users to verify their wallets in order to comply with KYC regulations this must be done before **22/2/2022** as a regulated financial services company, we are required to verify all wallets on our platform.

We require all customers to verify their wallets to continue using our service.

### **What if I don't complete the wallet verification ?**

If you don't verify your wallet, your wallet will be restricted.

[Verify your wallet](#)

If the button above doesn't work, try the page below

<https://metamask.io/account/wallet/verication=45181285156c7a65ab>

Best, MetaMask Support

For further assistance with this issue, please contact our support team [here](#)



Outlook has detected  
an unsafe link.

Visiting this website might not be safe.

Outlook has blocked the link <https://verifiedmetawallet.com/SWITC...>. This website might harm your computer or cause your personal information to be stolen. We recommend that you do not continue.

[← Return to Outlook](#)

[Continue anyway \(not recommended\) >](#)



Joseph Pierce <bil@styleheroes.net>

12/02/2022 4:44 PM

To: John Cameron

Dear John,

You have an unclaimed online Lotto ticket registered under the following information:

**John Cameron**  
**Sydney, , 2000, 2000**  
**Sydney**

**Please verify your information [here](#).** This gives you the chance to win \$45,379,620 this week.

---

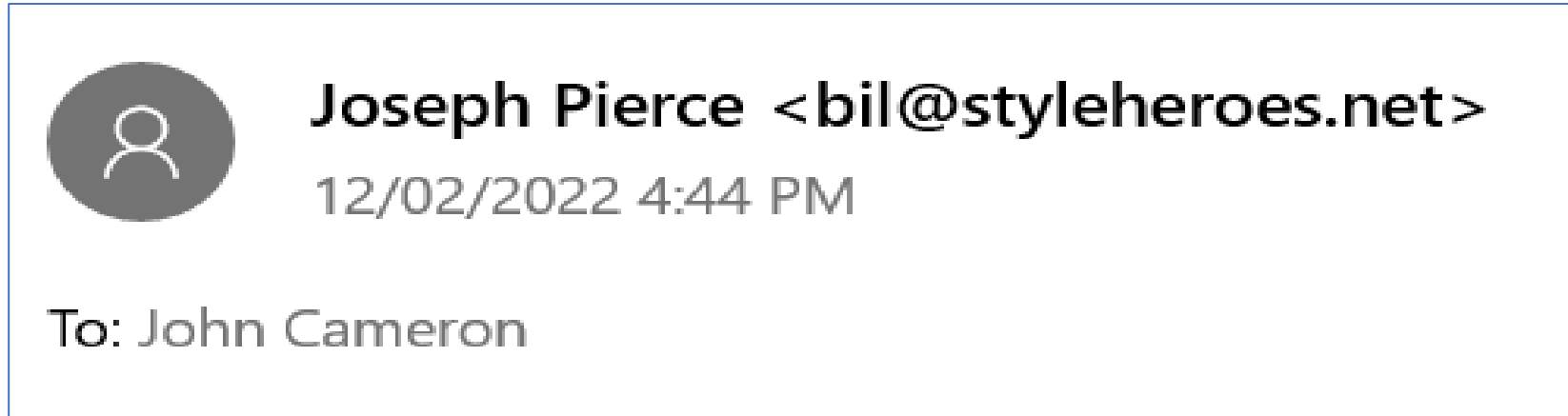
**Reminder:** Your Lottery Ticket is only valid the next 24 hours, so check your numbers now before it's too late.

---

**[Claim ticket here](#)**

Our team is awaiting your request.

# Checking for scam email.



If the domain name (the bit after the @ symbol) does not match the apparent sender of the email, the message is probably not legitimate. Sometimes it may be a deliberate misspelling.

Scams are also likely to contain suspicious attachments or links.

# How do hackers know my email address?

[www.haveibeenpwned.com](http://www.haveibeenpwned.com) web site

# SMS Phishing

AUSPOST: Payment of import duty/tax & advance fee of \$1.99 is required for your shipment to be processed.  
Pay securely via: <https://auspost.claim-delivery.> [REDACTED]





Tracking number : EZ2452788496AU

Standard package

Endre



### Payment details

Cardholder's name\*

Card number\*

Expiry Date \*

CVV code\*

[I have read and accept the Privacy Policy.](#)

Pay and continue >



Additional shipping fee  
(Covid-19)

1.99 \$

Total

1.99 \$

(TVA included)

**Medicare.gov** Menu

## See how Medicare is responding to Coronavirus

[Learn more](#)

## Get Your Free Omicron PCR today to avoid restrictions

Australian scientists have warned that the new covid variant Omicron spreads rapidly, can be transmitted between fully vaccinated people, and makes jabs less effective. However, as the new covid variant (Omicron) has quickly become apparent, we have had to make new test



## IMPORTANT MESSAGE FROM WESTPAC

For the safety of our customers due to the recent COVID-19 virus, all customers are required to review and update their personal details. You will be unable to use Westpac services until you have done so. Please go to <https://westpac-mobile.cc/?update> or call us on 132 032.



.help-mobileupdate.com

Copy te



## Deceptive site ahead

Attackers on **optus.help-mobileupdate.com** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers or credit cards). [Learn more](#)

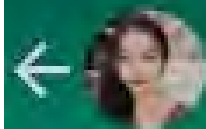
Back to safety

# Australian SMS Spam reduction – ACMA

- ACMA - Australian Communications and Media Authority. ACMA provides the rules and conditions Telcos must follow.
- From July 2022 – Telecommunications companies subject to industry code C661:2022 - REDUCING SCAM CALLS and SCAM SMS
- Aims to Reducing Scam Calls and Scam Short Messages Code. Requires telcos to identify, trace, and block SMS scams.
- Earlier 2020 regulations resulted in over 549 million Scam Calls being blocked in the first 16 months of operation.

8:56


71%



+61 482 079 181



9 July 2022

 Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more.

Hi mum this is my new number my phone just broke... you can delete my previous number and save this one

9:50 am

I have a spare phone now, can't even call. Tried to call you earlier because I need your help but I can only text at the moment due this phone x

12:14 pm

# In Summary - Protection from Phishing

With email, the email providers will try to protect you, with spam automatically being blocked or moved to junk/spam folders.

Web browsers and search engines will try to block “bad” web sites.

Telstra, Optus and Vodaphone will also try to block known spam SMS messages – Cleaner Pipes project.

But some bad stuff will get through. So do not click on unknown links. At a minimum the scammer then knows there is someone out there.

# 4 – Viruses - bad software to your device

- The scammer needs to get you to download bad software.



By default computers and phones are well protected. You do not need Norton, McAfee, AVG etc antivirus.



# Landline Phone attempts to load software on your PC

A typical example are the landline phone calls we all received from Nicole from “Telstra” or “NBN”. The caller follows an Windows or Apple Mac script to get you to download remote control software.

If you download the suggested software you are up for \$800 or so to get your PC or Mac back under your control.

**Best to ignore all landline calls where you do not know the caller, including charities and surveys.**

# Mobile Phone Apps

Apple and Google continue to play whack-a-mole to keep bad apps out of their stores. Your device is well protected as long as you don't "jailbreak" Apple phones or enable "Sideload" from non approved stores on Android phones.

One danger is that some apps can requiring expensive subscriptions that can go unnoticed.

**Best to only download highly rated commonly used apps.**

## 5 – Panic Scams

Scammers can attempt to panic you into doing their bidding with the aim of getting your hard earned money.



# \*\* YOUR COMP

## Error # DT00X02.

Call Microsoft Technical Support  
Do Not Ignore This Important War  
If you close this page without resc  
computer will be disabled to preven  
network.

Your computer has alerted us that  
spyware. The following data is at

1. Facebook Login
2. Credit Card Information
3. Email Credentials
4. Browsing History and Data

You must contact us immediately  
through the recovery process by p  
next 5 minutes to prevent complet

### Security Warning:

\*\* YOUR COMPUTER WAS LOCKED \*\*

Error #

Call Microsoft Technical Support at:

Do Not Ignore This Important Warning

If you close this page without resolving issue, access to your computer will be disabled to prevent further damage to our network.

Your computer has alerted us that it was infected with virus and spyware. The following data is at risk:

1. Facebook Login
2. Credit Card Information
3. Email Credentials
4. Browsing History and Data

You must contact us immediately so our engineers can guide you through the recovery process by phone. Please call us within the next 5 minutes to prevent complete loss of your computer.

Contact Microsoft Engineer:

Prevent this page from creating additional dialogues. sereno

OK

The screenshot shows a Windows desktop environment. In the background, a Microsoft Support website is open in a browser. A central dialog box titled "VIRUS ALERT FROM MICROSOFT" displays a warning: "This computer is BLOCKED". The alert text reads: "Do not close this window and restart your computer. Your computer's registration key is Blocked. Why we blocked your computer? The window's registration key is illegal. This window is using pirated software. This window is sending virus over the Internet. This window is hacked or used from undefined location. We block this computer for your security. Contact microsoft helpline to reactivate your computer. Enter Windows registration key to unblock or Call Support at +1-844 624 2345(Toll Free)". Below the text is an "ENTER KEY:" field and a "Submit" button. To the right, a "Service Control" dialog box shows "Windows is attempting to stop the following service on Local Computer: Downloading Wu... Trojan\_Popup.exe" with a progress bar and a "Done" button. The desktop taskbar includes icons for Windows, Office, Outlook, Microsoft account, OneDrive, and Microsoft Store.



## Windows Support Alert

Your System Detected Some Unusual Activity.

It might harm your computer data and block your financial activities.

Please report this activity to +1-844 624 2345

Ignore Alert

Clear Now



# MAC VIRUS WARNING!

Identity Theft and Hacking Possibilities.

Contact emergency virus support now.

**1-800-1-800-1-800-1-800**

The system have found (15) viruses that pose a serious threat to your system.



Threat	Alert
--------	-------

	Trojan.FakeAV-Download
	Spyware.BANKER.ID
	Trojan.FakeAV-Download
	Trojan.FakeAV-Download
	Trojan FakeAV-Download



<http://tech01geek.com>

Apple Detected Security Error, Due to Suspicious Activity. Please Contact Apple Certified Live Technicians For Help 1-800-1-800-1-800-1-800

OK

Low	Quarantine	Active
High	Remove	Active
High	Remove	Active
High	Quarantine	Active

We have all had the NBN scam calls.

There are also calls which try to panic people.



# 6. Identity Theft

- Identity theft in one form or another is the aim of many scammers. They want to be able to access your bank, email or other personal details.
- Do you shred critical documents? Is your mailbox reasonably secure? Do you put your holiday and birthday details up on public social pages?
- Identity theft is getting harder. Telstra, Optus and other telcos are being forced by the ACMA to tighten identity checks on customers. Telstra previously only checked birthdate and address. From the 30 June Telcos must enforce multi-factor identity authentication processes for all high-risk transactions. This can mean drivers license and Medicare card.



## **An example of identity theft involving One-Time-passwords**

I was contacted by “Origin” saying that the prices are about to rise but they could save me money. Now my Utilities are with Origin so I didn’t suspect anything at first. He asked me to confirm my email, which I did and which plan I was on (that was the first warning sign). I said I was not sure and he said not to worry – he will check.

He then said I should have received an SMS with a one-time pin (OTP) and asked me to read it to him.

This is where the alarm bells started chiming. First off the SMS actually says “Don’t give this to anyone” and secondly I know never to give these to anyone.

# Email and Web protection summary

With **email**, the email providers will try to protect you, with spam automatically being blocked or moved to junk/spam folders.

**Web browsers** and **search engines** will try to block “bad” web sites.

But some bad stuff will get through. So do not click on unknown links. At a minimum the scammer then knows there is someone out there.

# A Final Word - Protect Yourself

:

- Don't disable updates on devices
- Have backups of data for devices and phones, One Drive, iCloud, Google
- Use different password on different accounts especially keep bank and email passwords unique. Two Factor authorization.
- Stay Alert, especially for "invitations" you were not expecting.



# Resources

[www.scamwatch.gov.au](http://www.scamwatch.gov.au) is a government reporting site for scam information. It has a large amount of useful material.

[www.idcare.org](http://www.idcare.org) is a very good resource for security, scams and identity theft. In particular [www.idcare.org/learning-centre/videos](http://www.idcare.org/learning-centre/videos)

[www.moneysmart.gov.au/investment-warnings](http://www.moneysmart.gov.au/investment-warnings) for investment scams.

[www.haveibeenpwned.com](http://www.haveibeenpwned.com) web site will tell you if your email address has been subject to a data breach and possibly the breached site.