



Hot & Spicy Spam
(Only available in Guam)

Eric Pinkerton
AUSNOG
September 5th and 6th 2024



PHRONESIS
SECURITY

Whoami?



<https://www.linkedin.com/in/epinkerton/>

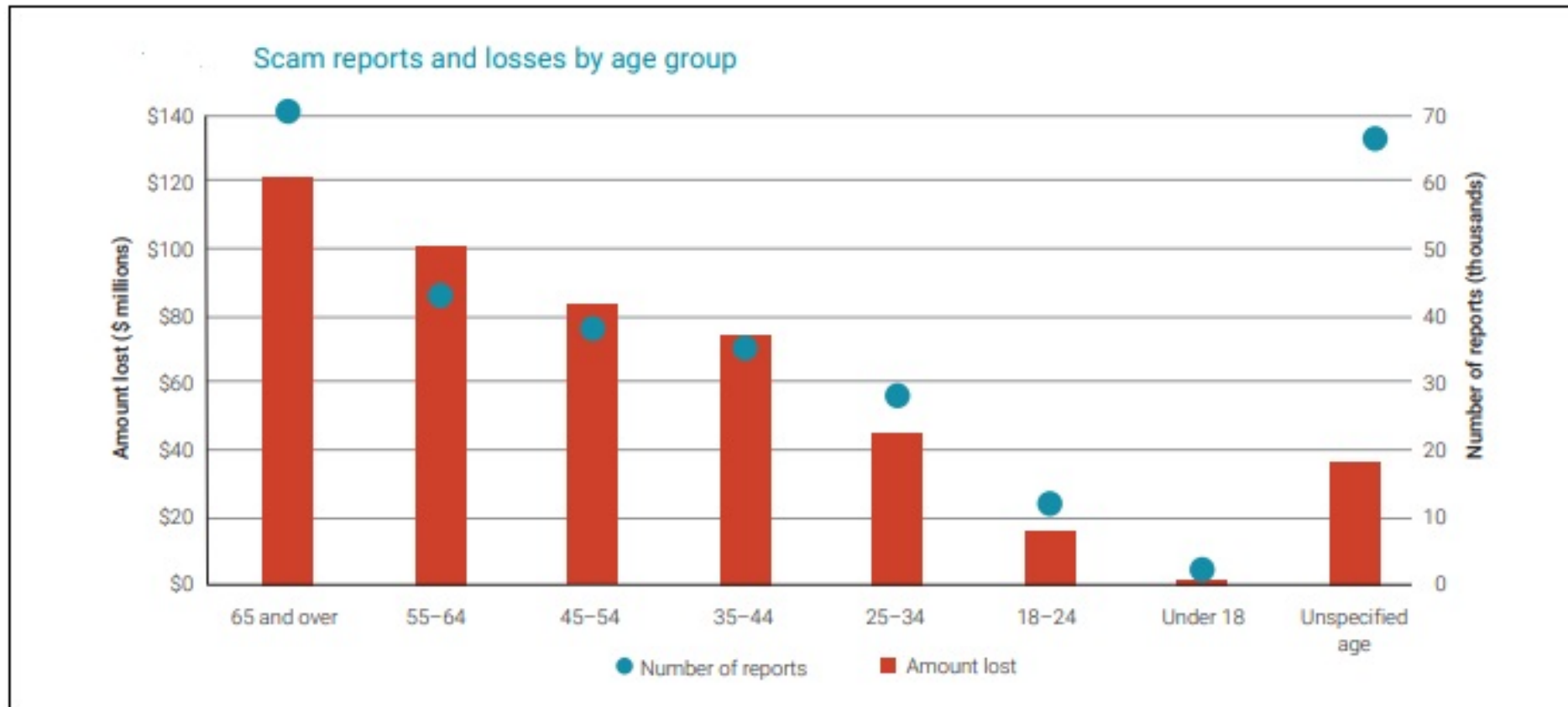


“By 2030, Australia will be the world’s most cyber secure country”





So Many Stats



Source: ACCC National Anti-Scam Centre



Contact methods reported to Scamwatch

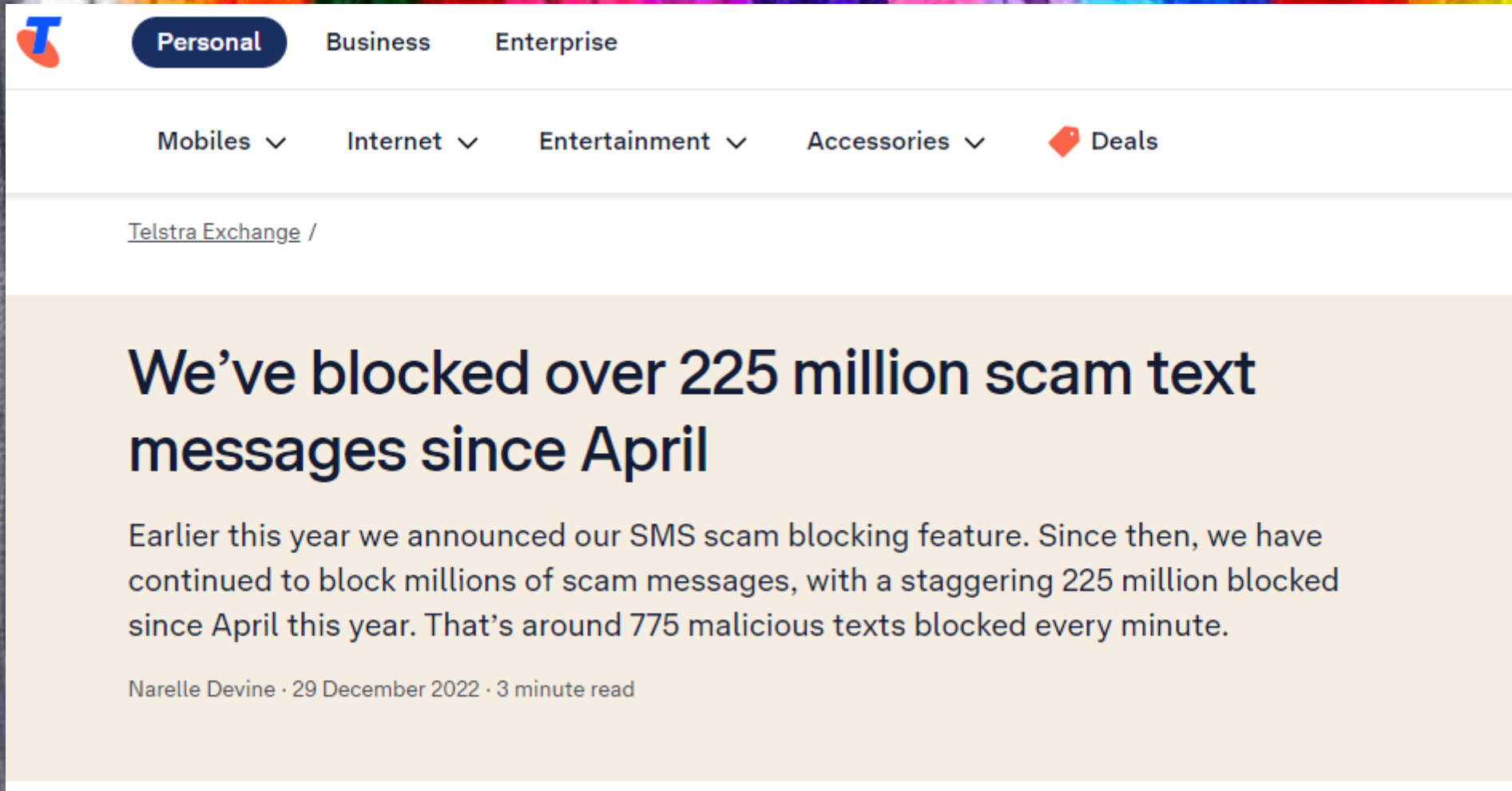
Table 5: Contact methods by loss and reports³³

Contact Mode	2022 losses (m)	2023 losses (m)	2022 reports	2023 reports
Phone call	\$141.0	\$116.0 ▼	63,816	55,418 ▼
Social media ³⁴	\$80.2	\$93.5 ▲	13,427	17,542 ▲
Email	\$77.3	\$80.0 ▲	52,159	85,941 ▲
Internet	\$73.5	\$69.7 ▼	13,692	17,568 ▲
Mobile apps	\$71.7	\$64.8 ▼	10,057	8,101 ▼
In person	\$30.6	\$21.5 ▼	2,186	3,614 ▲
Text message	\$28.5	\$26.9 ▼	79,835	109,621 ▲

Source: ACCC National Anti-Scam Centre



Pipe Cleaners



The screenshot shows the Telstra website interface. At the top, there is a navigation bar with the Telstra logo (a stylized 'T' in blue and red) on the left, and three tabs: 'Personal' (highlighted in a dark blue pill), 'Business', and 'Enterprise'. Below this, a secondary navigation bar contains links for 'Mobiles', 'Internet', 'Entertainment', 'Accessories', and 'Deals' (which has a red tag icon). The main content area features a breadcrumb trail 'Telstra Exchange /'. The headline of the article is 'We've blocked over 225 million scam text messages since April'. The sub-headline reads: 'Earlier this year we announced our SMS scam blocking feature. Since then, we have continued to block millions of scam messages, with a staggering 225 million blocked since April this year. That's around 775 malicious texts blocked every minute.' At the bottom of the article preview, it says 'Narelle Devine · 29 December 2022 · 3 minute read'.

Telstra Personal Business Enterprise

Mobiles ▾ Internet ▾ Entertainment ▾ Accessories ▾ Deals

[Telstra Exchange](#) /

We've blocked over 225 million scam text messages since April

Earlier this year we announced our SMS scam blocking feature. Since then, we have continued to block millions of scam messages, with a staggering 225 million blocked since April this year. That's around 775 malicious texts blocked every minute.

Narelle Devine · 29 December 2022 · 3 minute read



An Experiment

DISCLAIMER

the following experiment was performed by me, a highly trained professional in carefully controlled conditions, and under expert supervision, please don't try this at home.

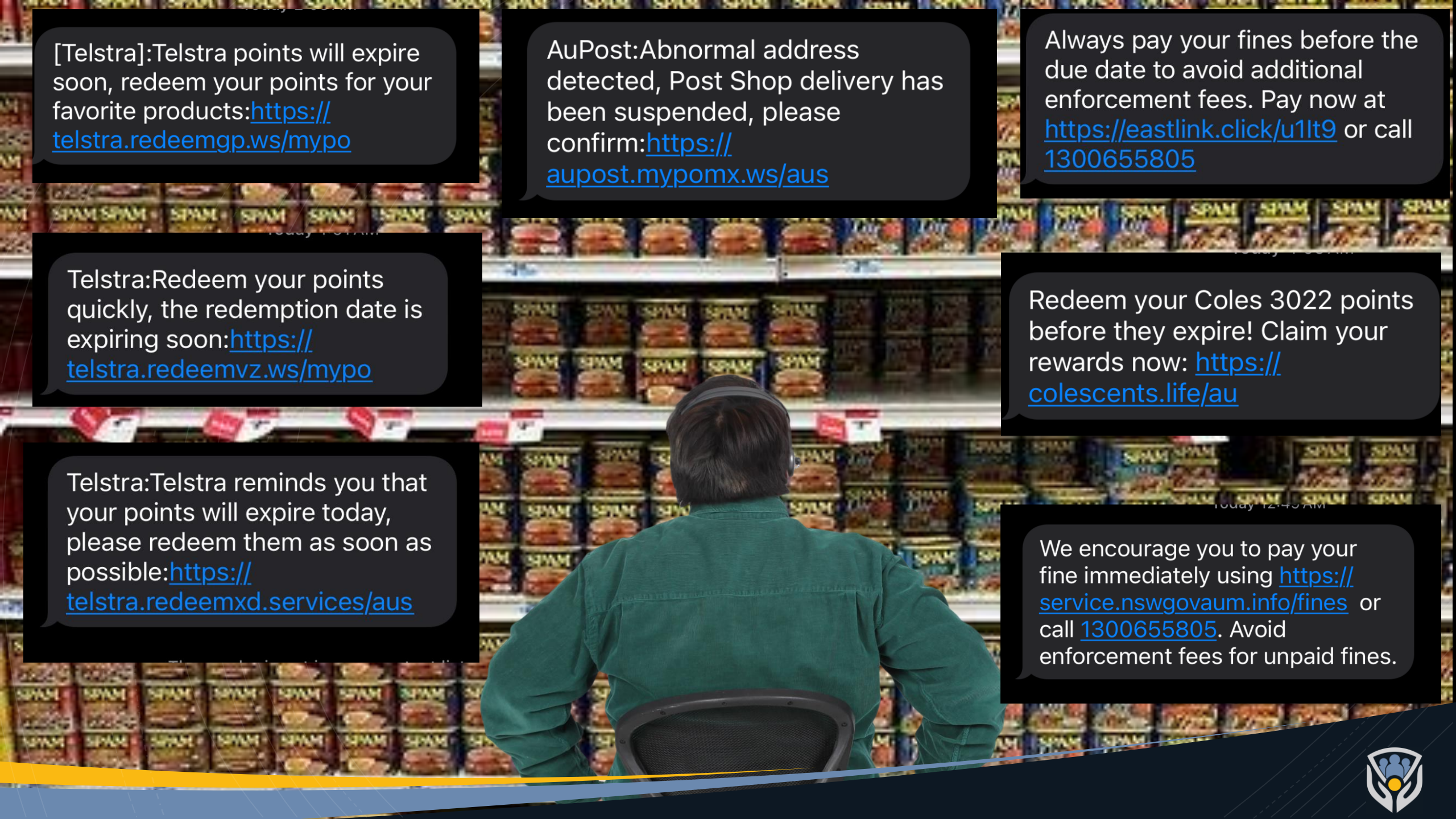
Filter off

Filter off

FILTER OFF

The SMS Scam Filter is now OFF for this service. To turn on, text FILTER ON to [0438214682](tel:0438214682)





[Telstra]:Telstra points will expire soon, redeem your points for your favorite products:<https://telstra.redeemgp.ws/mypo>

AuPost:Abnormal address detected, Post Shop delivery has been suspended, please confirm:<https://aupost.mypomx.ws/aus>

Always pay your fines before the due date to avoid additional enforcement fees. Pay now at <https://eastlink.click/u1lt9> or call [1300655805](tel:1300655805)

Telstra:Redeem your points quickly, the redemption date is expiring soon:<https://telstra.redeemvz.ws/mypo>

Redeem your Coles 3022 points before they expire! Claim your rewards now: <https://colescents.life/au>

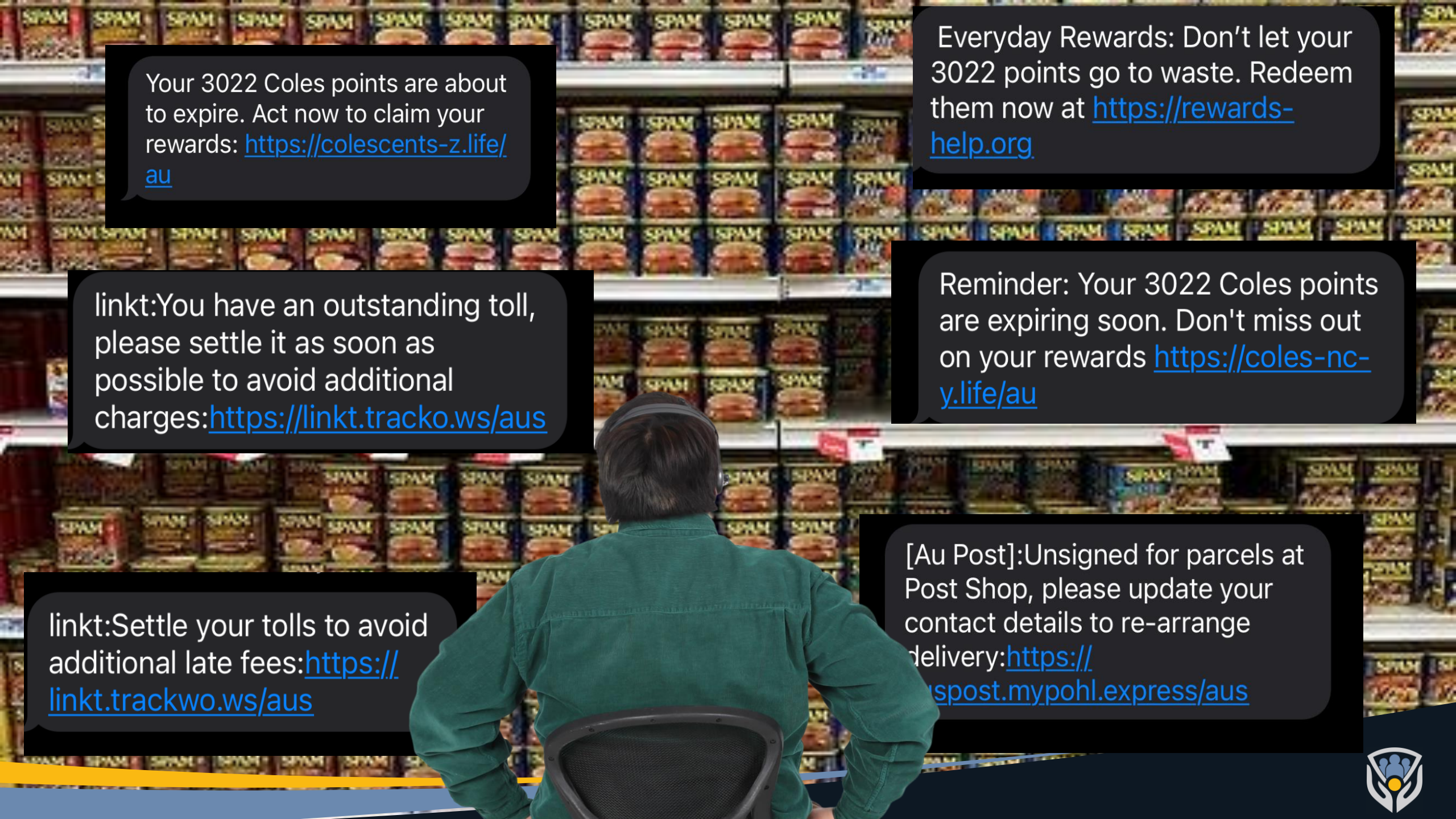
Telstra:Telstra reminds you that your points will expire today, please redeem them as soon as possible:<https://telstra.redeemxd.services/aus>

We encourage you to pay your fine immediately using <https://service.nswgovaum.info/fines> or call [1300655805](tel:1300655805). Avoid enforcement fees for unpaid fines.



Filter on

The SMS Scam Filter is now activated for your mobile service. This technology is designed to reduce the number of SMS Scam messages delivered to your mobile service. You can opt out of this service by texting FILTER OFF to [0438214682](tel:0438214682)



Your 3022 Coles points are about to expire. Act now to claim your rewards: <https://colescents-z.life/au>

Everyday Rewards: Don't let your 3022 points go to waste. Redeem them now at <https://rewards-help.org>

linkt:You have an outstanding toll, please settle it as soon as possible to avoid additional charges:<https://linkt.tracko.ws/aus>

Reminder: Your 3022 Coles points are expiring soon. Don't miss out on your rewards <https://coles-nc-y.life/au>

linkt:Settle your tolls to avoid additional late fees:<https://linkt.trackwo.ws/aus>

[Au Post]:Unsigned for parcels at Post Shop, please update your contact details to re-arrange delivery:<https://post.mypohl.express/aus>



Filter on



FILTER OFF



**Telstra's Cleaner pipes only blocked 14.29%
of my SMS SPAM in 1 month period**



How Can We Stop SMS SCAMS?

Education

Detection and
Avoidance

Reporting

Attackers

Children

Media Outreach

Law Enforcement

State

Federal

International

Collaboration

Govt

Carriers

Banks

Tech Companies

Community Orgs

Regulation

Carriers

Banks

Tech Companies



How to stay protected

1

STOP – Don't give money or personal information to anyone if unsure

Scammers will offer to help you or ask you to verify who you are. They will pretend to be from organisations you know and trust like, Services Australia, police, a bank, government or a fraud service.

2

THINK – Ask yourself could the message or call be fake?

Never click a link in a message. Only contact businesses or government using contact information from their official website or through their secure apps. If you're not sure say no, hang up or delete.

3

PROTECT – Act quickly if something feels wrong.

Contact your bank if you notice some unusual activity or if a scammer gets your money or information. Seek help from IDCARE and report to ReportCyber and Scamwatch.



How Can We Stop SMS SCAMS?

Education

Detection and
Avoidance

Reporting

Attackers

Children

Media Outreach

share a story stop a scam

Scams Awareness Week | 26 – 30 August

#ShareAScamStory



Everyone has a part to play in shutting down scammers. This Scams Awareness Week we're encouraging all Australians to speak up, share and report scams as a way to protect each other.

We need to talk about scams

Anyone can be scammed. Sharing your story helps others to spot, avoid and report scams, and to recover from them.

If you have identified or encountered a scam, it is important that you share your story with someone – it could be your friends, family, colleagues, social networks, or community. When



How Can We Stop SMS SCAMS?

Education

Detection and
Avoidance

Reporting

Attackers

Children

Media Outreach

Law Enforcement

State

Federal

International

Collaboration

Govt

Carriers

Banks

Tech Companies

Community Orgs

Regulation

Carriers

Banks

Tech Companies



Law Enforcement



How Can We Stop SMS SCAMS?

Education

Detection and
Avoidance

Reporting

Attackers

Children

Media Outreach

Law Enforcement

State

Federal

International

Collaboration

Govt

Carriers

Banks

Tech Companies

Community Orgs

Regulation

Carriers

Banks

Tech Companies



How Can We Stop SMS SCAMS?

Education

Detection and
Avoidance

Reporting

Attackers

Children

Media Outreach

Law Enforcement

State

Federal

International

Collaboration

Govt

Carriers

Banks

Tech Companies

Community Orgs

Regulation

Carriers

Banks

Tech Companies



Regulatory Options

Carriers	<ul style="list-style-type: none">• About 1000 CSP• Low Difficulty• Low yield	Industry Code C661:2022 ACMA SMS Sender ID Registry STIR/SHAKEN
Financial Institutions	<ul style="list-style-type: none">• About 1800 (APRA)• Medium Difficulty• Medium yield	APRA, ASIC, AUSTRAC Commonwealth Fraud and Corruption Control Framework ePayments Code Banking CoP Scam-Safe Accord (ABA & COBA)
Tech Companies	<ul style="list-style-type: none">• Pick a number• High Difficulty• High yield	?????

The
Sweet
Spot





STIR/SHAKEN



The same old
threats, in ever
evolving
contexts



Telco Regulation



Australian
Communications
and Media Authority

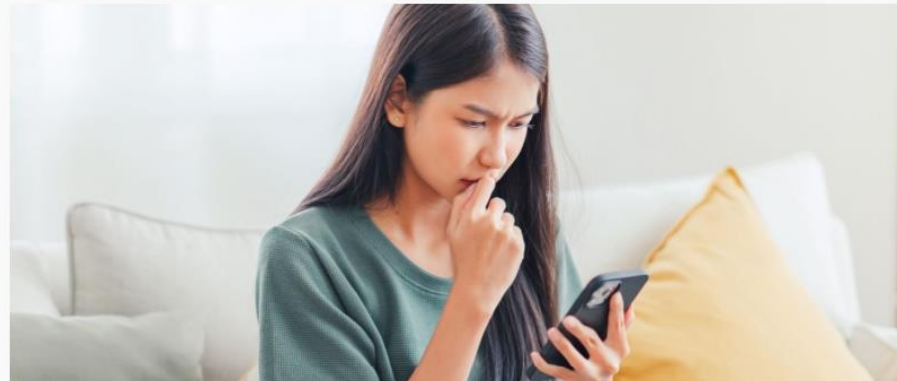
New rules to fight SMS scams

12 July 2022



Five telcos breached for allowing SMS scams

15 February 2024

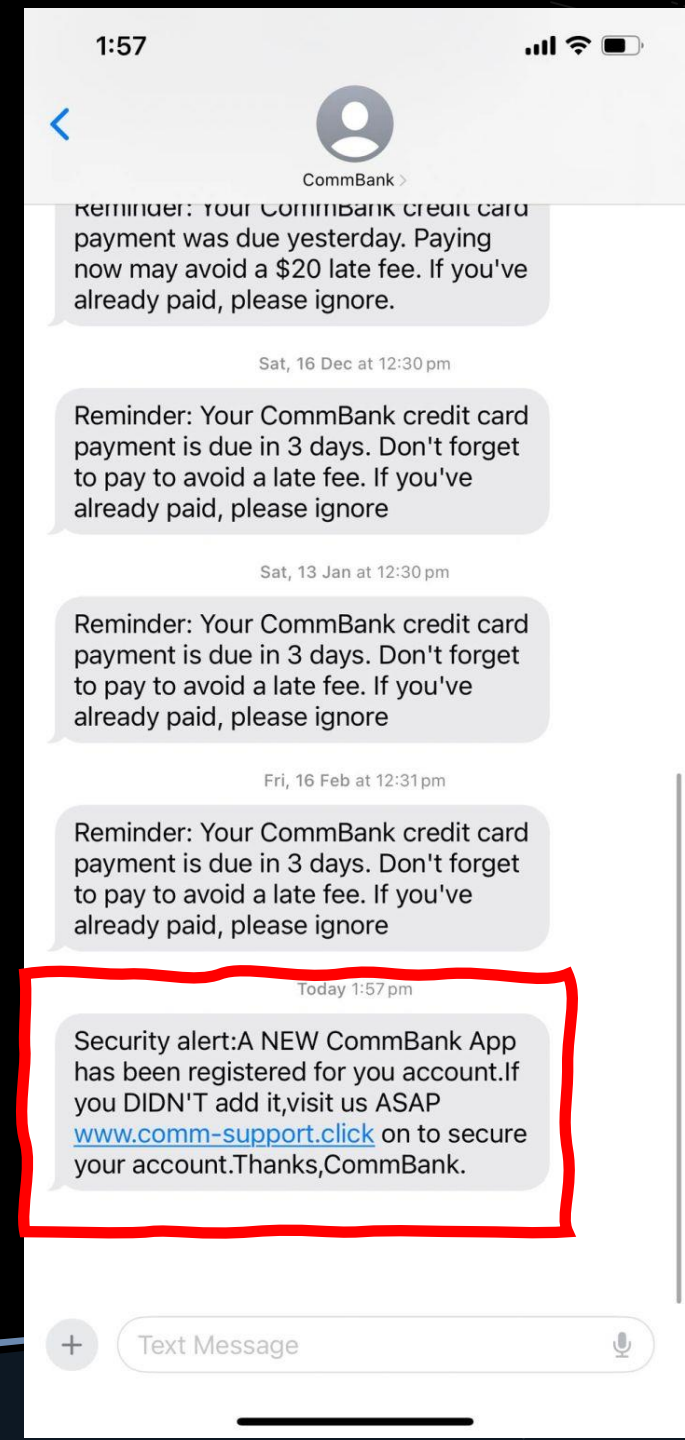


CLI Over Stamping



Legit

Not
Legit



CLI Over stamping

The screenshot displays the 'russiancoms' website interface. At the top, there's a navigation bar with 'Home' and 'Web App' links, and 'Register' and 'Log In' buttons. The main content area is divided into two columns for different subscription durations.

1 Month	3 Months
<ul style="list-style-type: none">✓ 5,000 minutes✓ Web Phone✓ Auto Call✓ Call anywhere, from anywhere✓ Encrypted calls✓ No cell sites✓ Off-shore private network✓ No call cut off time✓ No logs✓ No server downtime✓ 24/7 customer support	<ul style="list-style-type: none">✓ 15,000 minutes✓ Web Phone✓ Auto Call✓ Call anywhere, from anywhere✓ Encrypted calls✓ No cell sites✓ Off-shore private network✓ No call cut off time✓ No server downtime✓ 24/7 customer support
£ 350	£ 1,000
Buy Now	Buy Now



CLI Over stamping

Send instant SMS right here.

We have the most competitive SMS rate on the market!

[How to access the SMS API](#)

SenderID: 61 [redacted] 7 ▼

Enter destination mobile number :

e.g. 04xxxxxxxx OR

You have Characters left.

* To send a SMS to any Australian mobile phone just enter the phone number as is, for example 04xxxxxxxx.
To send an international SMS please use this format: [country code] + [phone number],
e.g. SMS to UK: 44xxxxxxxx

SMS cost to most Australian mobile is 5c per message if message length is 160 characters or less. [redacted]

If message is longer than 160 characters we will split it up and send them in **two** separate SMS and the cost will be 10c. Most modern mobile handset can/will assemble the two separate SMS and display them as a single message upon receiving them.

SMS to most international mobile number is 10c per 160-character SMS. Please check with us to confirm the international SMS cost if you are not sure.

The screenshot shows a dark-themed website interface. At the top right, there are 'Register' and 'Log In' buttons. Below them, a '3 Months' subscription offer is highlighted in blue. The price '£1,000' is displayed in large white text. A prominent blue 'Buy Now' button is at the bottom. The background is dark blue with some white text and icons.



CLI Over stamping

Send instant SMS right here.

We have the most competitive SMS rate on the market!

[How to access the SMS API](#)

SenderID: 61 [redacted] 7

Enter destination mobile number :

e.g. 04xxxxxxxx OR

* To send a SMS to any Australian mobile phone just enter the phone number
To send an international SMS please use this format: [country cod
e.g. SMS to UK: 44xxxxxxxx

SMS cost to most Australain mobile is 5c per message if message length is 1
If message is longer than 160 characters we will split it up and send them in t
10c. Most modern mobile handset can/will assemble the two seperate SMS a
upon receiving them.

SMS to most international mobile number is 10c per 160-character SMS. Ple
international SMS cost if you are not sure.

Burp Suite C

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer

1 x 2 x 3 x +

Send Cancel < >

Request

Pretty Raw Hex

```
1 POST /cust/send_sms.php HTTP/1.1
2 Host: www.[redacted].com
3 Cookie: PHPSESSID=b0rhp8v7jkqdasce3ivfc3r44; __utma=155429225.90118538.1721947922.1721947922.1721947922.1;
  __utmz=155429225.155429225.1721947922.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); __ga=
  GA1.1.1773929269.1721947922; __ga_9MFE32XZ9Z=GS1.1.1721947922.1.0.1721947927.0.0.0
4 Content-Length: 606
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126", "Google Chrome";v="126"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Dnt: 1
10 Upgrade-Insecure-Requests: 1
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0
  Safari/537.36
12 Origin: https://www.[redacted].com
13 Content-Type: application/x-www-form-urlencoded
14 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
  signed-exchange;v=b3;q=0.7
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer: https://www.[redacted].com/cust/send_sms.php
20 Accept-Encoding: gzip, deflate, br
21 Accept-Language: en-AU,en-US;q=0.9,en;q=0.8,en-GB;q=0.7
22 Priority: u=0, i
23 Connection: keep-alive
24
25 from_mobile=TEST&to_mobile=0419827312&sms_mobile=&smstext=This+is+a+test&countdown=305&sub=+Send+SMS+
```

Response

Pretty



Banking Regulation (REP 790)

Anti-scam practices of banks outside the four major banks



\$232m

in total scam transactions made by customers.

Note: These were payments made by customers in total, including those that were subsequently detected and stopped and recovered.



96%

of total scam losses were born by reviewed bank customers

Note: Scam losses are total scam transactions less amounts detected and stopped and/or recovered.



19%

of these transactions by value were detected and stopped.

Note: Detected and stopped excludes other scams that were prevented by the bank prior to the customer performing the transactions.



2%

was the share of scam losses reimbursed and/or compensated by the reviewed banks if the customer did not complain. That share increased to 7% where the customer complained.

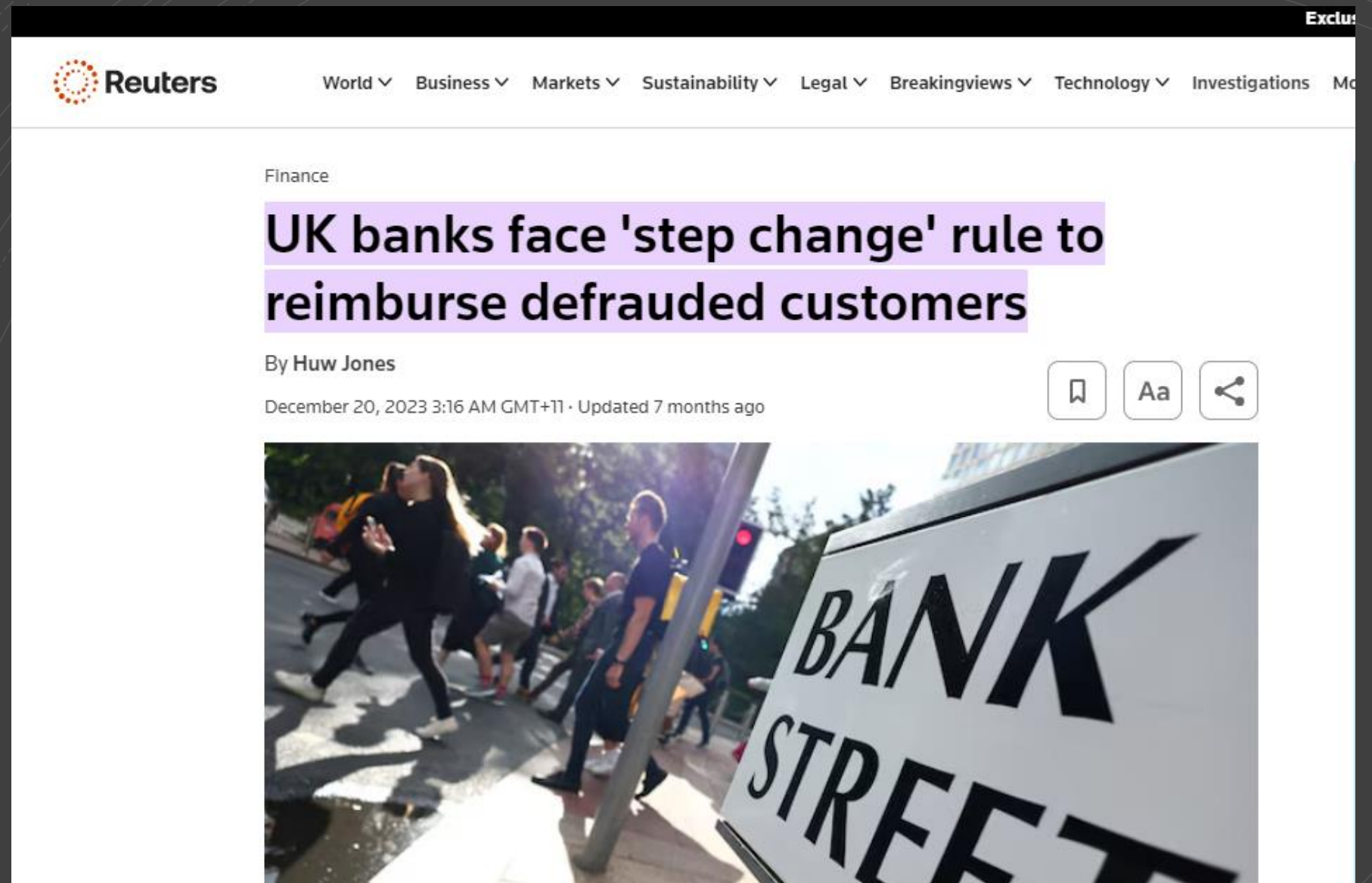
20%

of funds transferred were recovered from the receiving banks/financial institutions.

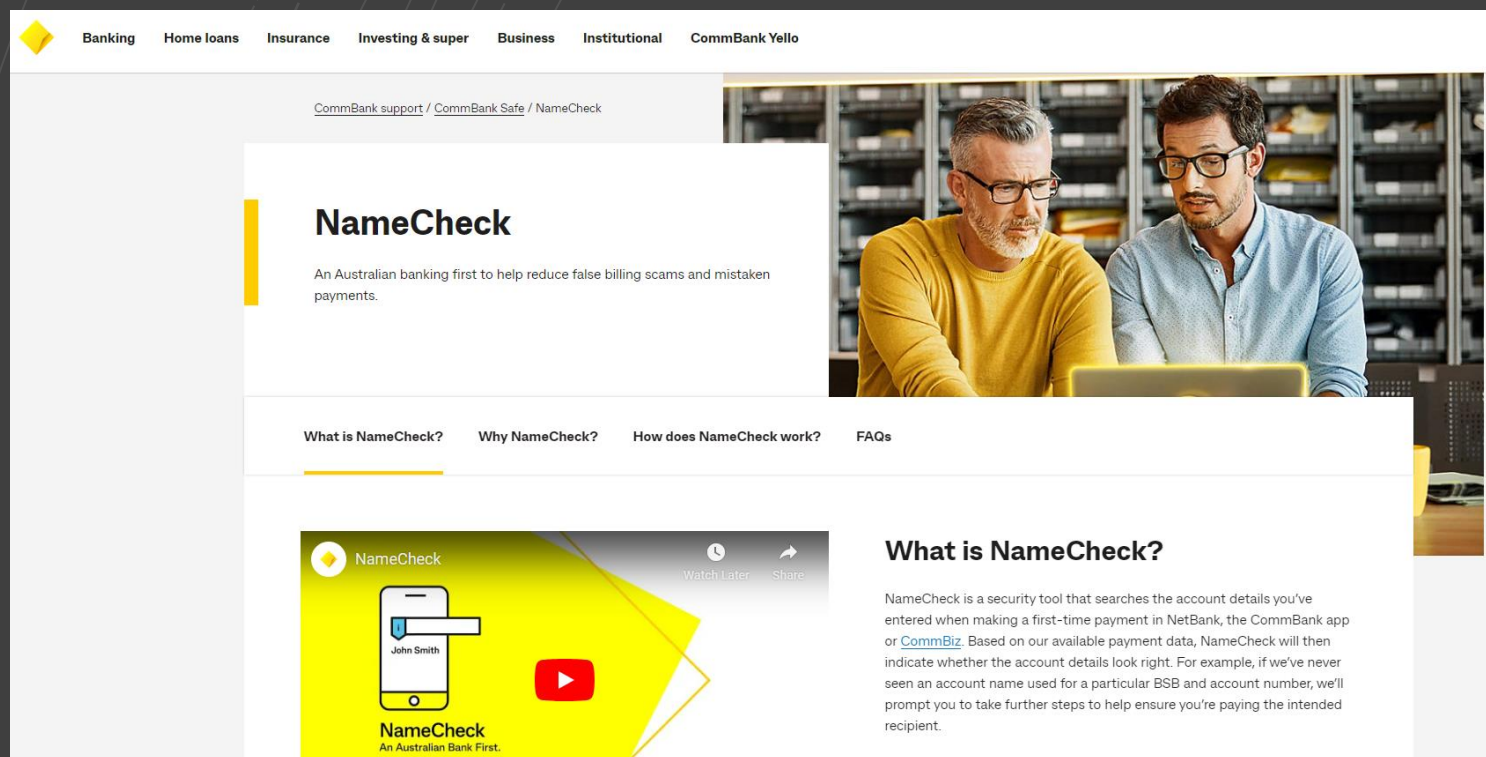
Source: Australian Securities and Investments Commission



Step Change



Name Check



The screenshot shows the NameCheck webpage. At the top is a navigation bar with links: Banking, Home loans, Insurance, Investing & super, Business, Institutional, and CommBank Yello. Below the navigation bar is a breadcrumb trail: [CommBank support](#) / [CommBank Safe](#) / NameCheck. The main heading is "NameCheck" with a subtext: "An Australian banking first to help reduce false billing scams and mistaken payments." To the right of the text is a photo of two men looking at a laptop. Below the main heading is a tabbed interface with four tabs: "What is NameCheck?", "Why NameCheck?", "How does NameCheck work?", and "FAQs". The "What is NameCheck?" tab is active. It contains a video player with the NameCheck logo and a red play button. To the right of the video player is the text: "What is NameCheck? NameCheck is a security tool that searches the account details you've entered when making a first-time payment in NetBank, the CommBank app or [CommBiz](#). Based on our available payment data, NameCheck will then indicate whether the account details look right. For example, if we've never seen an account name used for a particular BSB and account number, we'll prompt you to take further steps to help ensure you're paying the intended recipient."



The account name you entered seems to match the account



The account name doesn't seem to match the account



There's a different name more commonly used for this account



We haven't seen enough payments to indicate if the account details look right



BSB and account number not found



Tech

Bulk SMS/MMS LTE simbox 64

aliexpress.com/item/[REDACTED].html

AliExpress EURO2024 OFFICIAL PARTNER

hello kitty pants

Download the AliExpress app

Camperdown/EN/AUD

Welcome Sign in / Register

Cart 0


Telecom Store

0.0% Positive Feedback | 11 Followers

+ Follow

Message

Store Home Products Feedback

 X64

AU\$5,847.08

Bulk SMS/MMS LTE simbox 64 ports 4G 64 Channels SMS Gateway support HTTP SMPP API

Coupons & discounts

AU\$1.26 off
On orders over AU\$1,0...

Ship to Camperdown, New South W...

Delivery >

Free Shipping
Estimated delivery on Jun 03
Collect a AU\$1.00 coupon for late delivery

Service >

Free returns • Delivery guarantee

Quantity

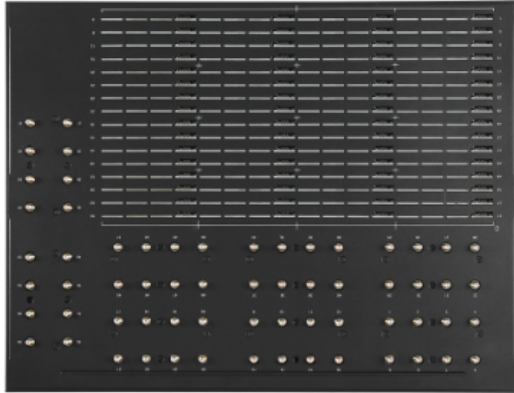
1


1000 Pieces available

Buy now

Add to Cart

Share







Why choose SK gateway ?

A lot of clients now are complaining about the blocking issues. First, you may know why the Operator blocks you frequently?

Second, what are the rules for the blocking?

Third, how can we reduce it, even avoid it? There are some rules I have found out for you.

#1 Carrier detects the calls of its continuous minute. Once the SIM cards reach a certain continuous minute, SIM cards block. Solution: Our SK smart gateways can be inserted 4 SIM cards each port and support the SIM cards making calls circularly itself. For this advantage, you can set when 1 SIM card reaches a certain continuous minute, then goes to next SIM card to make calls. Also, we can set it sending SMS more frequently to reduce the blocking.

#2 Carrier detects the IMEI No. of SIM cards and blocks it.

Solution: Our SK gateways can be set to change IMEI No. Automatically to avoid blocking issues.

#3 Carrier detects you SIM cards are abnormal. The explain is because the Operator affirms your SIM cards are not being used by a human, instead some certain devices. Solution: On one hand, the SK gateways are designed with a function which copies a human's behavior of using a SIM card and makes it look like a human is using it. On the other hand, the SK gateways also can copy a human's behavior of sending SMS and making calls among the ports. All the functions can be set by the setting page of the SK gateways.

Features

- 1) Each channel Support 1 port work
- 2) IMEI Change
- 3) AT command directly
- 4) Base Station Change
- 5) Support USSD balance enquiry, billing
- 6) Direct to monitor Status of Sending SMS
- 7) Support to do sms route
- 8) Auto suffer the internet to use Internet traffic
- 9) Support SIMS hot-swap
- 10) Support SMPP server/client
- 11) Support HTTP/SIP SMS API



Hey hey, I'm looking at your 64 port sms gateways, just have a few questions.. what is the lead time for these, and have you sold many of these in Australia, and if so do you know which carriers are the best for the purposes of sending out bulk sms? ie which ones allow you to change IMEI etc?

1:46 pm ✓✓

hi dear sir this is Kevin from [REDACTED] 1:47 pm

Hi Kevin 1:48 pm ✓✓

yes we have sold many device to Australia , lead time like 4-7 working days after you pay 1:48 pm

Ok cool 1:48 pm ✓✓

yes i knew which carriers good for bulk sms 1:48 pm

sk device support imei auto change 1:49 pm

Australia Telstra this sims is the best for bulk sending sms 1:49 pm



this is sk 64-64 device support smpp api http connection , and support imei change auto , 1:50 pm

you can change imei by manual as well 1:51 pm

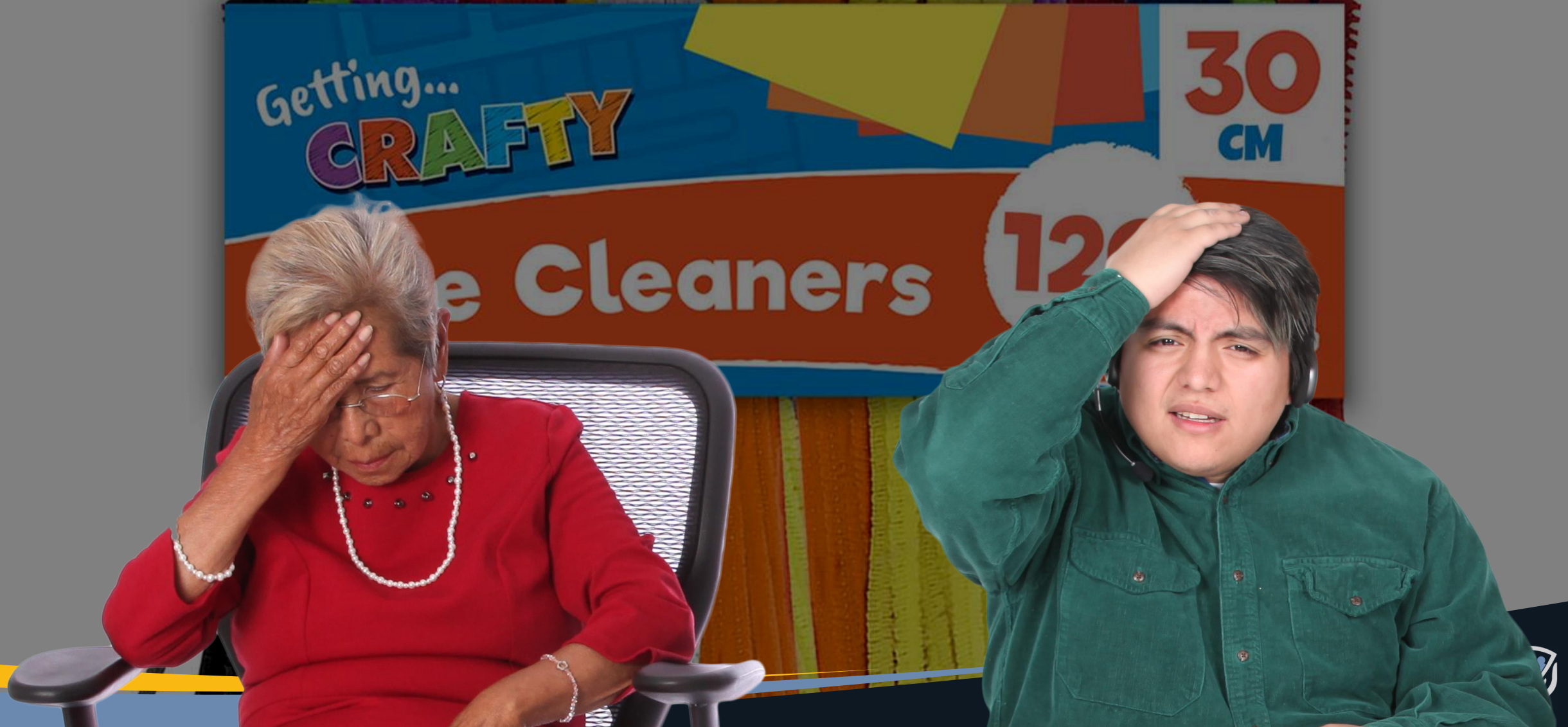


In Conclusion

- If you work for Telstra, pls check the hoover bag on your filter.
- If you work for a FI, watch what happens in the UK.
- If you work for the Gov't, focus on:
 - End User Education
 - Better media outreach
 - Regulation for FI's and Tech Companies
- And don't forget we can all learn a lot from North Korea



Q&A and or Story Time (time permitting)



Storytime

Hi mum this is my new number
Can u save it please?

Ok no probs

Your brother is back in prison by
the way

Stupid f^{👁️👁️}👁️k left his fingerprints all
over the crime scene





I'm really sorry baby I had no choice, mad Eddie came around here looking for you, he says he wants what you owe him and threatened your father with a machete, we had no choice but to give him this number

If I were you I would bin this phone asap, you know he has mates in the police..



Don't f👁️k with this guy Kayla you know what he's capable of

theage.com.au



YOUR HOME OF THE OLYMPICS

STARTS
JULY 26

Advertisement

National Victoria [Crime](#)

This was published 1 year ago

'They wanted to execute': Balaclava-clad offenders targeted wrong house in home invasion



[Marta Pascual Juanola](#)

Updated December 7, 2022 —

1.48pm, first published at 11.15am



Save

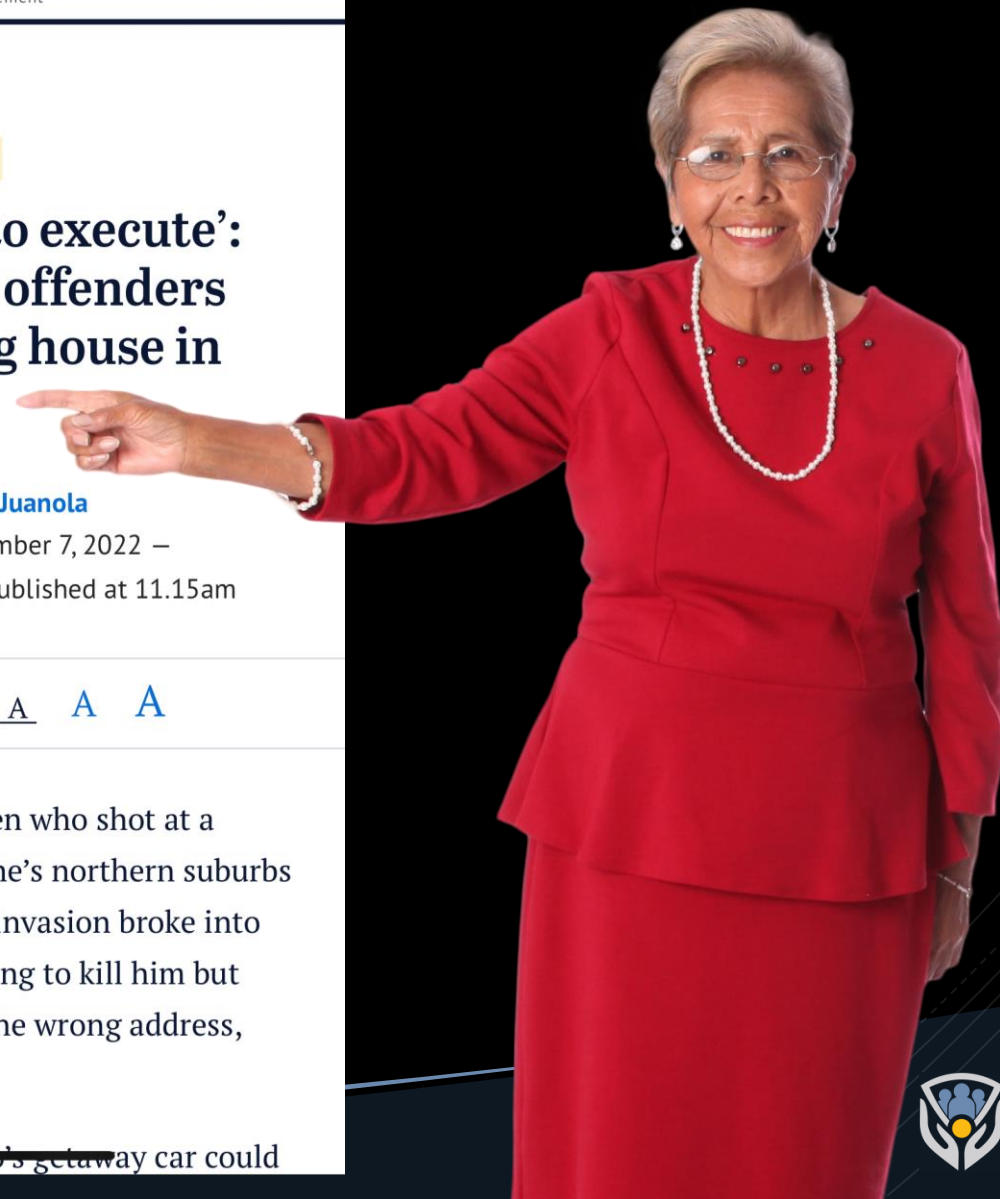


Share



Three balaclava-clad men who shot at a homeowner in Melbourne's northern suburbs during a botched home invasion broke into the man's house intending to kill him but later realised they had the wrong address, police believe.

Police also think ~~the trio's~~ getaway car could



Sydney Today 8 ° / 20 °



news.com.au

Sign Up

Log In



National World Lifestyle Travel Entertainment Technology Finance Sport Shopping



Technology > Online > Hacking

Melbourne man charged in relation to cruel 'Hi Mum' text scam

A Melbourne man has been charged in relation to the cruel "Hi Mum" text message scam that dupes kind-hearted parents out of "substantial" sums of money.



Lauren McMahon

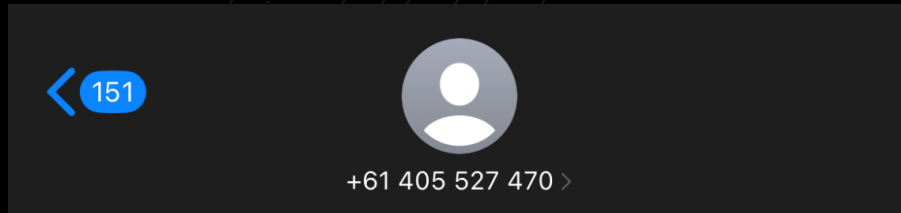
@lauren_mcmah 2 min read January 21, 2023 - 10:09PM news.com.au



Ad 1 of 2 : (0:15)



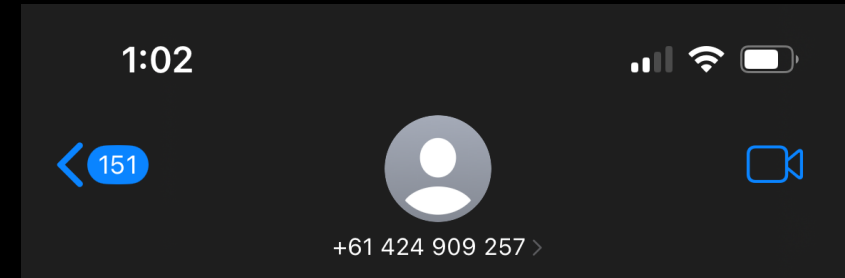
Storytime 2.0



Text Message
Today 12:43 PM

Hey dad my phone is badly damaged I can't contact anyone. I need you to text me on my new number urgently it's [+61424909257](tel:+61424909257) x

The sender is not in your contact list.
[Report Spam](#)



iMessage
Today 12:45 PM

Hey what's up?

Hey , my phone fell and now it's fully broken. I am in the phone shop now getting my new phone. I will call you after I've got my phone

Don't get a new one we have heaps of burner phones

If you get one from a shop we can't be sure the cops won't be able to trace it back to you

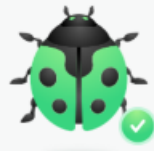
Just make sure you don't give anyone your real drivers license

Where are you I'll send one of the boys over?



Storytime

New Token Created!



Your Web bug Canarytoken is active!

Copy this URL to your clipboard and use as you wish


Canarytoken URL

`http://canarytokens.com/tags/static/90ieywgpmjfp0c4kib00hynk/submit.aspx`



Remember, it gets triggered whenever someone requests the URL.

TINYURL

 Your Long URL

`http://canarytokens.com/tags/static/90ieywgpmjfp0c4kib00hynk/submit.aspx`

 TinyURL

`https://tinyurl.com/mr32ux4w`



QR

Share

Copy

My URLs

Shorten another





Storytime

Hey is this that onlyfans chick from the clubhouse?


Pale Blue Dot
tinyurl.com









Your Canarytoken was triggered
Web bug Canarytoken has been triggered by the Source IP
52.112.49.196





Reminder
Hello Mum Scammer @0424909257



Source IP
52.112.49.196

 Date
2024/08/27

 Time
02:52 UTC



User agent
Mozilla/5.0 (Windows NT 6.1; WOW64) SkypeUriPreview
Preview/0.5 skype-url-preview@microsoft.com

IP address details

52.112.49.196

 Johor Bahru, Johor, Malaysia

 cloud

 hosting



Storytime

Saya ada beberapa kawan di Jabatan Siasatan Jenayah Komersial yang akan singgah dan memberi salam sebentar lagi.

- "Saya ada beberapa kawan" = I have some friends
- "di Jabatan Siasatan Jenayah Komersial" = in the Commercial Crime Investigation Department
- "yang akan singgah dan memberi salam" = who will stop by and say hello
- "sebentar lagi" = in a few moments/soon

