Username Searches

Searches were conducted of international investigative databases for the usernames beat_slaya, slaya_ike, humphreydinkum, tenantdefence, tenancy.disputes, ike_rushton, issacrushton, issac_rushton, zac20, and issac_88, where several results of potential relevance were identified.

The username beat_slaya was identified as being linked to a DubSmash account with an associated email address of [redacted] Technical investigations confirmed that this email address is currently valid and linked to a Google account with ID [redacted] Analysis of the associated Google account identified this user as being located in India and the email address was considered unlikely to belong to the Suspect.

The username issacrushton was identified as being linked to a Zynga account with an associated email address of [redacted] Technical investigations confirmed that this email address is currently valid and linked to the partially revealed email addresses of [redacted] and [redacted] along with a mobile phone number ending in 31. The website allerskog-krantz.se was identified as being a Swedish building company, and it was therefore considered unlikely that the email address [redacted] is linked to the Suspect.

Summary of Assessment

The Client reported that he has been the target of ongoing online impersonation, harassment and cyberstalking through social media and encrypted messaging platforms beginning around 2021. The majority of this offending activity was reported to have taken place in groups on the Telegram app, as well as on the Instagram, Facebook and LinkedIn platforms.

Two accounts in the names of @frost_rich and @The_real_Tony_smith, both with the display names of Tony Smith, were investigated in terms of their posting behaviours on the Telegram platform.

The @the_real_Tony_smith account was identified as being active in the 'Sydney Party Lads' Telegram channel, and revealed to be advertising the

Cybertrace

sale of illicit substances (cocaine, heroin, or methamphetamines) in quantities of points, half grams, grams, 1.75 grams and eight-balls.

The @frost_rich Telegram account was identified as being active in the Sydney Lads Up Late' Telegram channel, and revealed to be advertising the sale of ketamine and cannabis, as well as posting about their purported dark web engagement and potential hacking.

A tracking link was deployed by Cybertrace to the Subject via the @frost_rich account on the Telegram app on 30 April 2025, where an IP address of 103.53.118.254 was obtained. Analysis of the IP address confirmed that it was not linked to a known proxy or VPN. A location of Sydney and an Internet Service Provider (ISP) of Anycast Global Backbone were also identified.

The identity of the individual operating the @frost_rich and @the_real_Tony_smith Telegram accounts was not confirmed.

Anycast technology was understood to be different to regular ISPs in the sense that it is a network addressing and routing method in which incoming requests can be routed to a variety of different locations or "nodes". This means that the same IP address is shared by multiple servers in different locations. Anycast Global Backbone is linked to an operation called Anycast Holdings, which is a subsidiary of the ISP, Swoop.

The Client provided Issac William Rushton as the likely Suspect behind these behaviours. A comprehensive proprietary database, social media, and open source investigation was conducted into Issac, where he was identified as using numerous alias names, and being currently enrolled to vote at Brougham Street, Woolloomooloo NSW 2011. His working history claimed to include a patchwork array of life coaching, insurance brokering, real estate, admin, and web development.

The Suspect had an extensive court attendance history with numerous appearances at the Brisbane Arrests Court between 2015 and 2019, as well as being the protected person in several AVO applications, and having an extensive civil court history as both the plaintiff and defendant, which appears to be primarily related to housing and tenancy issues.

Issac was identified as being linked to the following domains, none of which are linked to currently active websites, through his ABN:

Cybertrace

http://evolvealt.org
parkerrushton.com.au
rentersaustralia.com.au
tenancydispute.com.au
tenantdefence.com.au
tenantdefenders.com.au
tenancydisputes.com.au

The following email addresses were identified as being used to register these domains, confirming them as linked to Issac:

[redacted]

It is also considered highly likely that the following email addresses associated with Issac's domains are operated by him.

contact@tenantdefence.com.au
[redacted]

In addition, the email addresses [redacted] and [redacted] were confirmed as being linked to the Suspect through investigative databases.

Specific investigations of the email address [redacted] confirmed it as being linked to a mobile phone number of [redacted] and a Microsoft account using the name Anthony Smith, providing evidence that the Suspect is using the Client's name online.

Analysis of a number of other email addresses, phone numbers, and social media accounts were conducted, where the Suspect was either confirmed or considered highly likely as being linked to the following:

[redacted]

www.facebook.com/i.crush.the.competition
www.facebook.com/groups/364032873189154

Cybertrace

www.facebook.com/tenantdefenders
www.facebook.com/groups/931393340681530

www.instagram.com/beat_slaya
www.instagram.com/tenant.defenders
www.instagram.com/pottspointcentralhotel
www.instagram.com/rentersaustralia

www.linkedin.com/in/issac-rushton-6740a792/
linkedin.com/in/mark-eldridge-358772223

https://x.com/ike_rushton

https://www.youtube.com/@ikerushton9059

Two further tracking links were deployed to the Suspect via Facebook Messenger, where he was somewhat hostile and extremely cautious, repeatedly querying the engineered pretext. At the time of the close of the investigation, these links had not been engaged with.

This pattern of hostility and mistrust by the Suspect aligned with the same types of communication used by the Subject account @frost_rich.

In terms of intelligence gathered through the course of the investigation, it was considered that the Subject presents with patterns of impersonating people with whom he has had conflict. With likely engagement in the dark web, as a trafficker of illicit substances, fraud and other crimes, such impersonation might serve the dual function of avenging said conflicts, and carrying out illicit activity with impunity. It is therefore vital that law enforcement agencies take action to bring due consequences to bear on the offender, so that he ceases this behaviour.

Recommendations

It is recommended that a request is made of the Telegram application for records pertaining to accounts in the name of @the_real_Tony_smith and @frost_rich.

It is further recommended that a Forensic Data Request be made of Swoop and Anycast Holdings with regard to Anycast Global Backbone and for information pertaining to the specific user of IP address 103.53.118.254 at

Cybertrace

11.04 AM (AEST) in Sydney on 30 April 2025. Given that multiple users can be linked to this IP address at a given point in time, it is crucial that browser histories, network traffic and system logs are analysed to determine which websites have been accessed with this IP address at this time and what was posted on them. It is particularly critical that authorities investigate the matter of the user linked to this IP address who has used Telegram to promote the sale of narcotics using the name of the Client.

Anycast Global Backbone:	5/15 Phoenix Street, Warragul VIC 3820
Anycast Holdings Pty Ltd:	Level 21, 135 King Street, Sydney NSW 2000 +61 3 5622 4600 noc@anycast.com.au
Swoop Broadband:	1a/ 155 Queen Street, Warragul VIC 3820 1300 665 575 support@swoop.com.au

If you have any further questions in relation to this matter, please contact our office on +61 9188 7896.

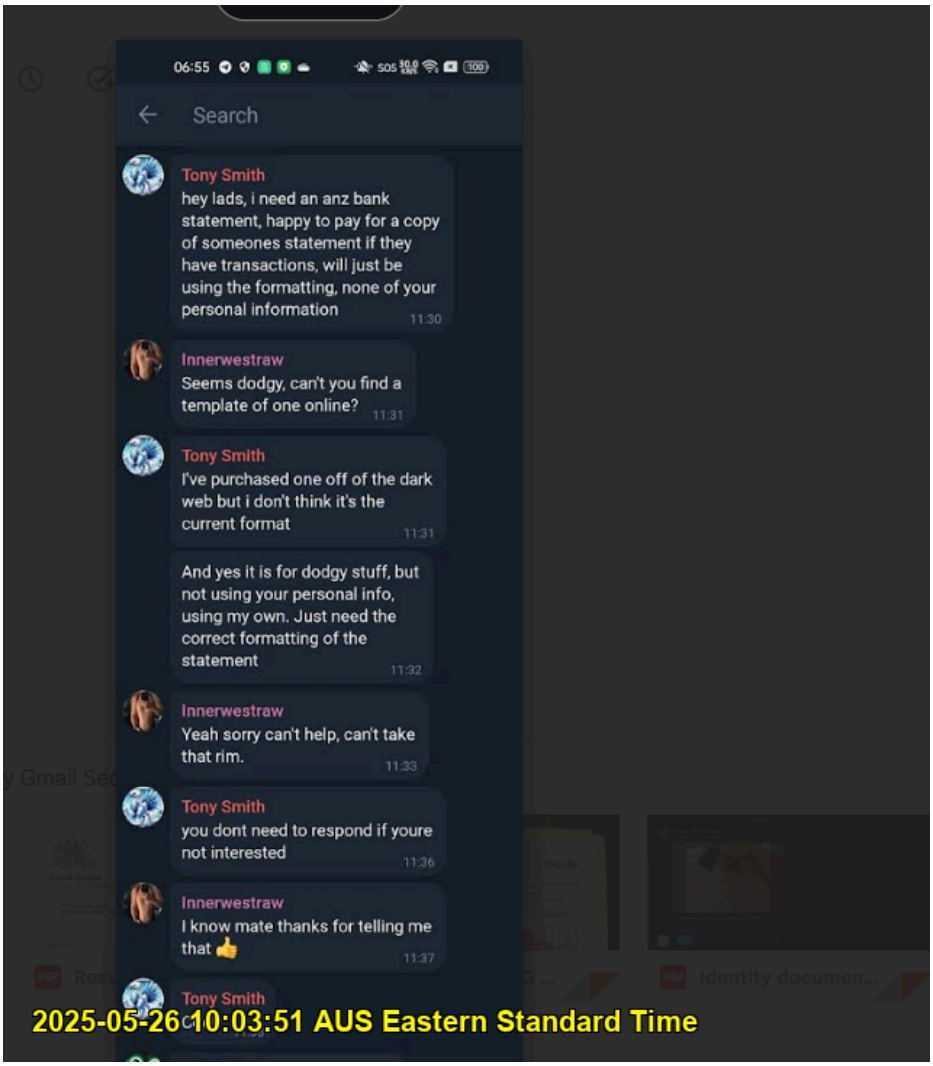
Kind regards,



Dan Halpin
CEO
Cybertrace
www.cybertrace.com.au
E: contact@cybertrace.com.au
Ph. Australia: 1300 669 711
Ph. International: +61 2 9188 7896

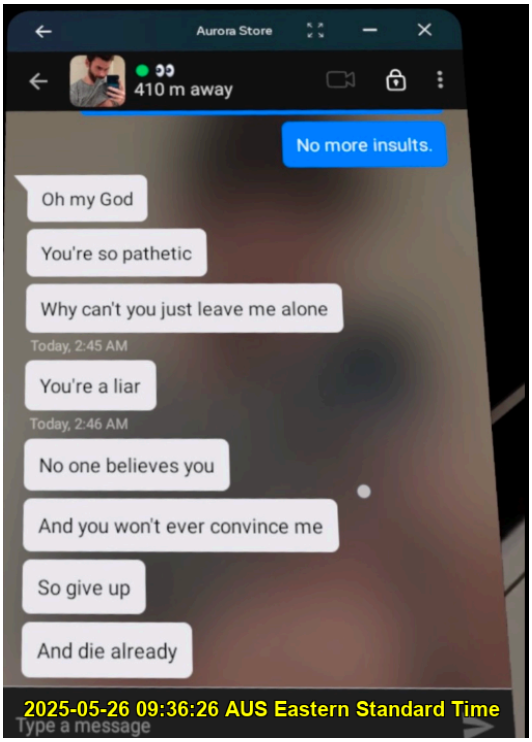
Cybertrace

Appendices

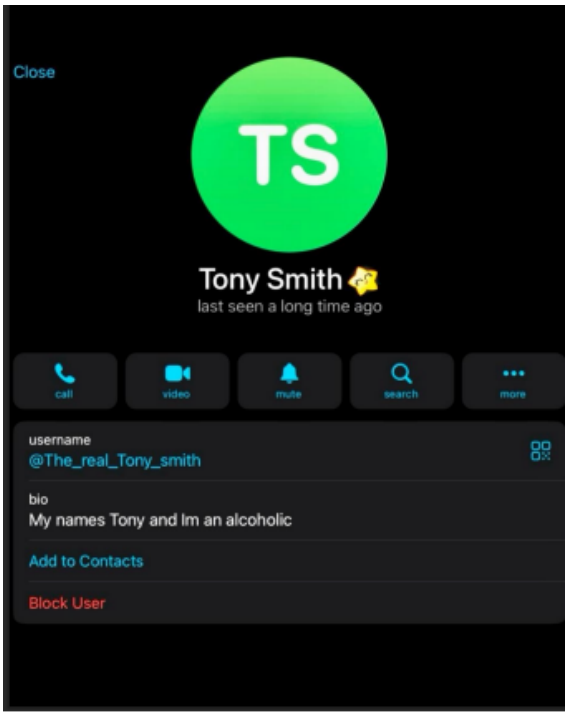


Comment: A Telegram account in the name of Tony Smith requests an ANZ bank statement.
Source: Provided by the Client

Cybertrace

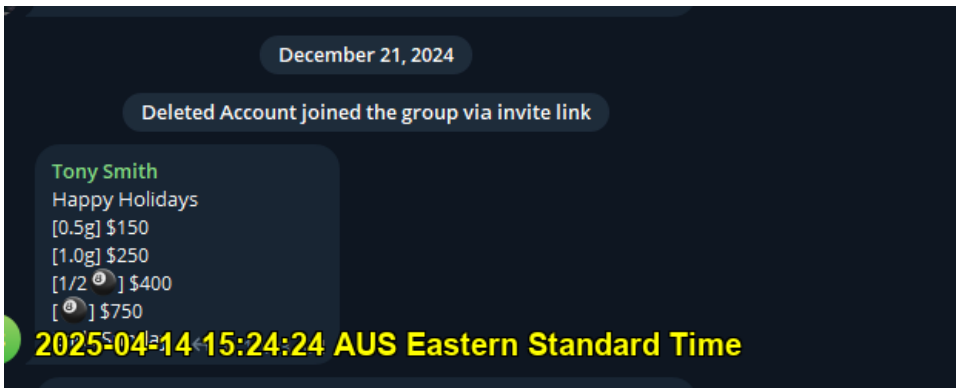


Comment: An exchange between the Subject and the Client.
Source: Provided by the Client

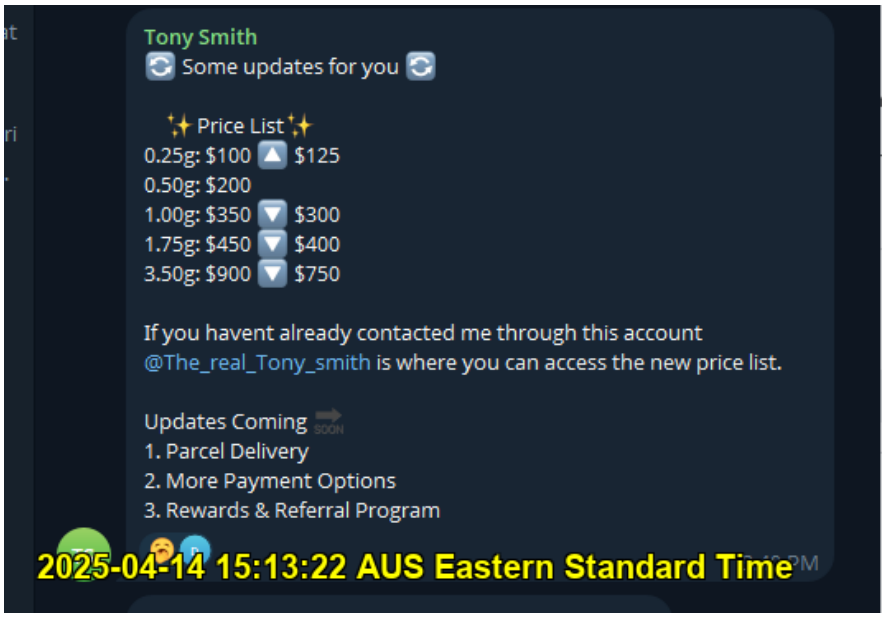


Comment: A Telegram account created in the name of the Client.
Source: Provided by the Client

Cybertrace

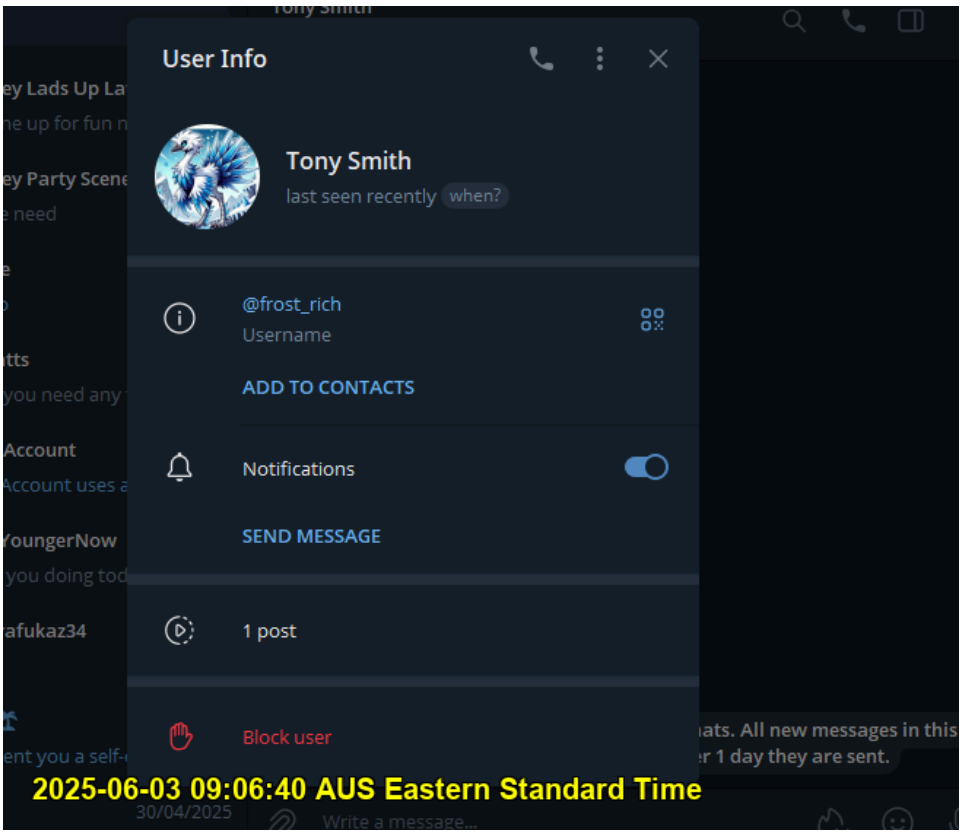


Comment: An account in the name of Tony Smith is in the Sydney Party Lads Telegram channel selling drugs.
Source: Sydney Party Lads Telegram

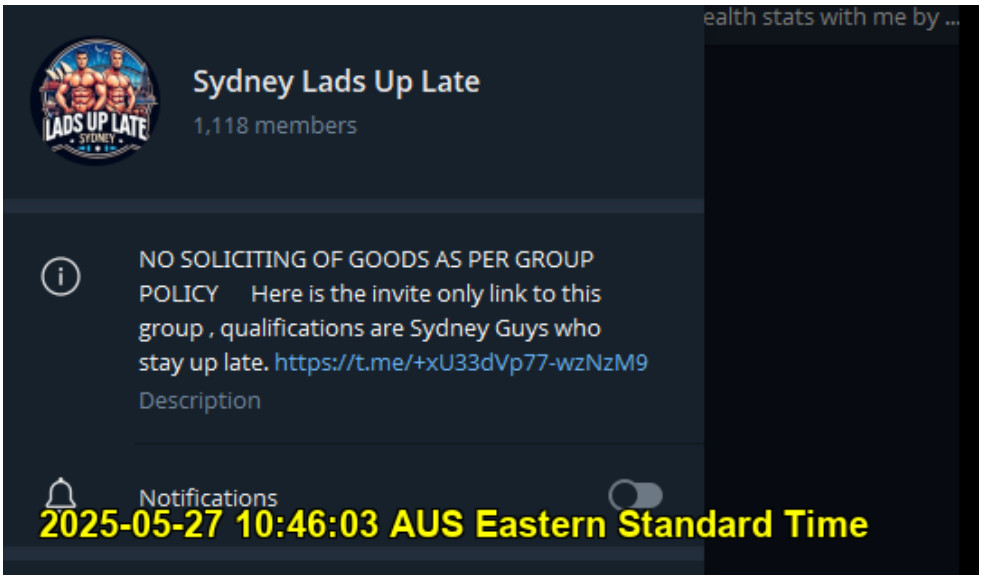


Comment: An account in the name of Tony Smith is in the Sydney Party Lads Telegram channel.
Source: Sydney Party Lads Telegram

Cybertrace

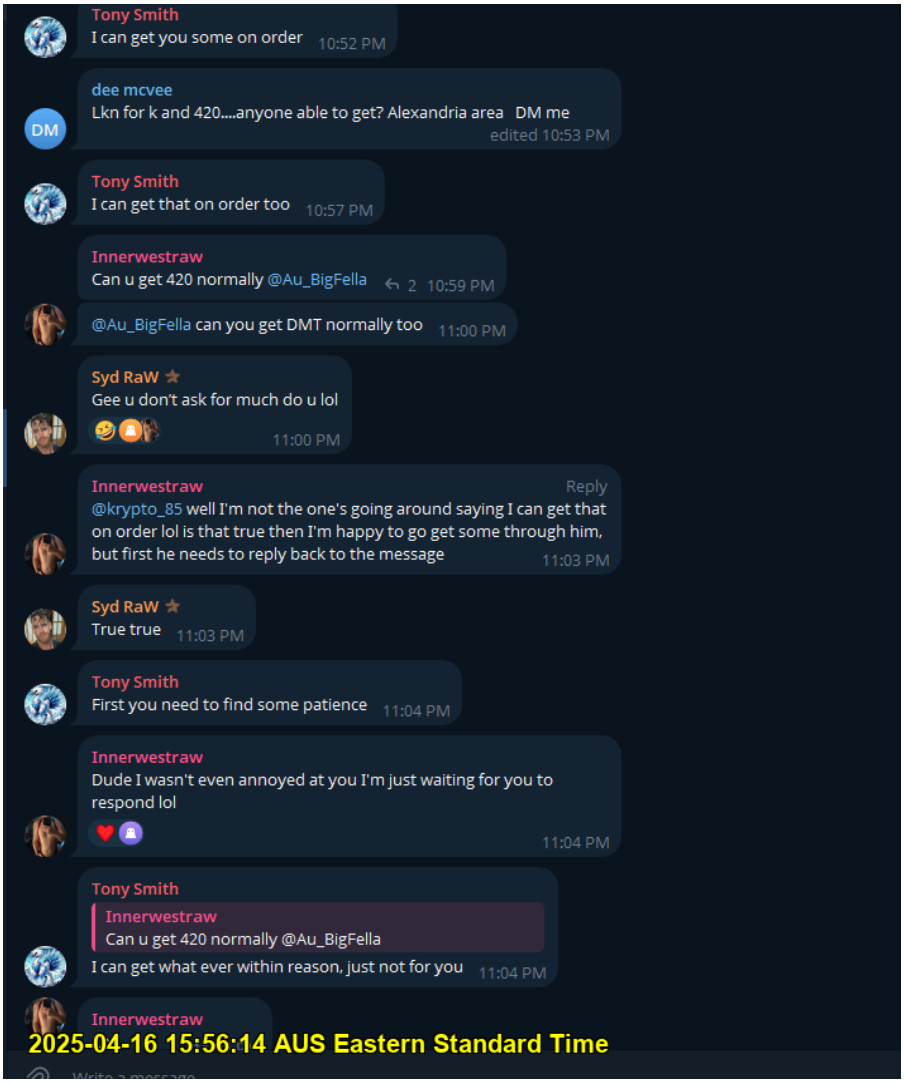


Comment: Subject Telegram account @frost_rich Tony Smith.
Source: Telegram



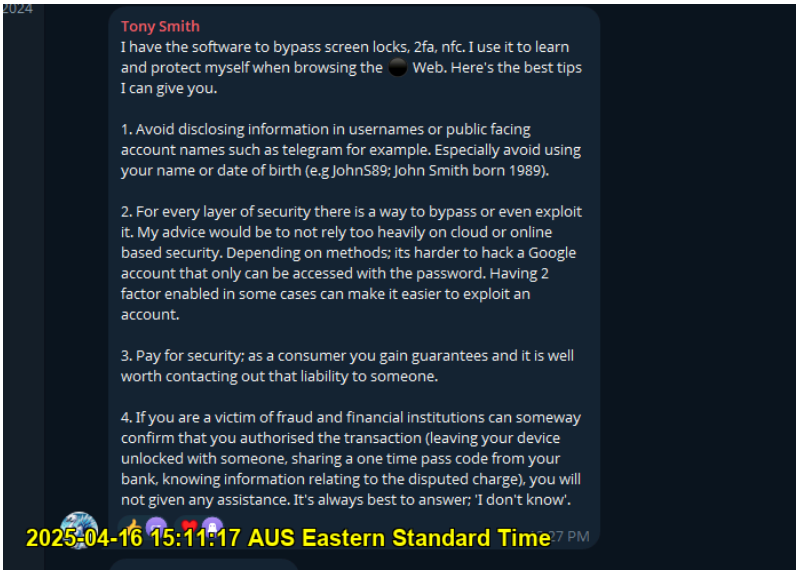
Comment: Channel bio
Source: Telegram Sydney Lads Up Late Telegram

Cybertrace

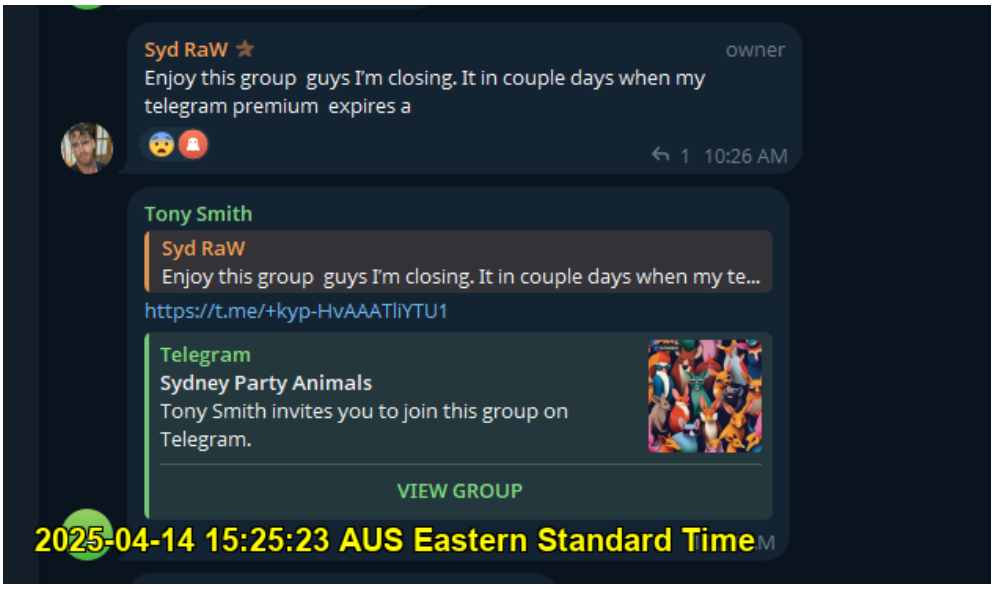


Comment: An account in the name of Tony Smith referring to being able to get cannabis, DMT, and ketamine.
Source: Sydney Lads Up Late Telegram channel

Cybertrace



Comment: An account in the name of Tony Smith giving cyber security advice and advising the use of one's real name.
Source: Sydney Lads Up Late Telegram channel



Comment: Syd Raw runs Sydney Party Lads Telegram channel. Tony Smith profile invited him to join Sydney Party Animals.
Source: Sydney Party Lads Telegram

Cybertrace