[redacted]

From: [redacted]
Sent: Tuesday, 24 September 2024 8:41 PM
To: Scams Policy
Subject: Thanks for the legislation!

[redacted] [redacted]

[redacted]

Thanks for the new legislation. I think this is great. I like the document layout, the presentation and the logical way in which the legislation is laid out. I also like the descriptions and the steps outlined to combat scammers.

On a voluntary basis I work to detect crypto arbitrage scams on youtube.com. I your see Example 1.10 in your explanatory materials covers this issue. Here are some details: https://lemmy.world/post/19342865

Your legislation, after a brief read seems to address this content. However I still have concerns:

1. The scam marketplace seems to change more rapidly that large organisations like YouTube can adjust. This makes their reactions always delayed. My concern is that they will not be able to keep up with new scams and reacting to them in a timely fashion. I notice in the legislation that an entity has some time to respond but how can Australia be optimistic that entities will react in a timely manner?
2. Scammers use a combination of social media technology typically at the same time, for example YouTube and telegram. In these scams I investigate some of them require a combination of the two in order for customers to get hooked. This also effectively hides the scam. Is there anything in the legislation that addressed scams across multiple social media platforms simultaneously? I think the legislation should at least recommend cooperation between entities on this matter. This could be similar to how virus are handled where this is sharing between anti-virus companies. For example a scammer could have signature (e.g. web site, name, identity) that could be shared. See also section 58BX.
3. Fake web sites appear to be the foundation of many, if not all, scams. However I cannot find any recommendations on the legislation that focuses on this root feature. Again I think that the legislation should encourage information sharing and even proposing a centrally managed database of scammer "signatures" (e.g. web sites). See also 1.30 in the explanatory material.
4. Scammers seem to frequently use hacked accounts or channels, sometimes with hundreds of thousands of subscribers (some are listed in the links). This can be very deceptive for customers. Yet the likes of YouTube don't seem to do anything about eliminating this common source of scams and fraud even when frequently reported and after someone loses money. It appears to be the case that scammers can operate with impunity for years without any action. Entities seem to have an innate inability to identify a scam or differentiate between the legitimate and the fraudulent. What steps need to be taken in order to assist in the identification of the actual source of a scam (without someone suffering loss)? E.g., how are scams being investigate by authorities and how can this legislation assist this process?
5. It seems there also is a disconnection between the comprehension that a scam is involved, an associated report on the scam, investigation (if any) and action. Obviously the legislation attempts to address this, hopefully so that the links in the handling chain remain intact (i.e. a scam is addressed). However I am not that optimistic that complicated scams, e.g., those related to cryptocurrency, will be adequately investigated. I find it difficult to imagine how, for example, entities will understand that a scam is an MEV bot scam (examples are included in the links). This involves reverse engineering the smart contract code that will typically show that funds are sent to the scammer rather than returned to the customer. Therefore, how can investigation experts, even myself for example, be involved in addressing this problem, perhaps across some common reporting platform?
6. The legislation mentions reporting to government. However there is no mention of inter-agency cooperation and reporting. For example cybercrime is mentioned (1.78) yet there is a cross over between this type of crime which typically starts as a scam. Furthermore how is reporting to cyber.gov.au get

actioned and will information sharing and cooperation occur between the different regulatory bodies? For example in the first instance can information on scams reported to cyber.gov.au be made available to entities affected in the crime, e.g. Facebook in the case of some falsely advertising on the platform? Likewise can scams reported on your legislation framework be reported to police investigation cybercrime, and how is this written into the legislation?

Regards,
Brian Taylor
Logos Technology