Mike Green

Professor Yalpi

02-11-2024

CYSE-201S

Education and Awareness on Cybercrime in the Metaverse

Article Review #1

Aim of the Investigation

The investigation/research done in this study aimed to provide recognition of problems that may arise through cybercrime victimization in the metaverse with an emphasis on "deepfake-related interpersonal cybercrime…" (Stavola & Choi, 2023, p. 5). And by utilizing the information gathered from the study, create a framework to further prevent cybercrime as well as provide support for those who have been victimized by it.

Research Methods Utilized in the Study

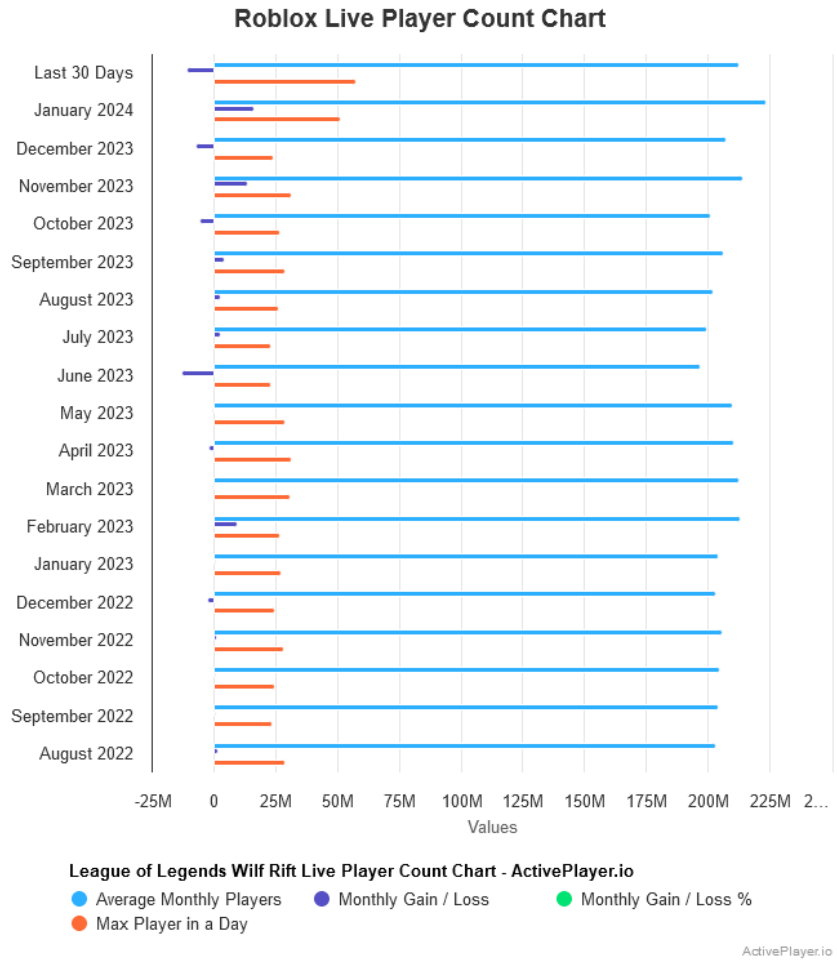
Methods used for conducting research involved purposive and snowball sampling and interviews with "a diverse group of metaverse experts from various sectors in South Korea…" (Stavola & Choi, 2023, p. 11). Purposive sampling entails the selection of candidates/participants who have the expertise and/or qualifications to provide insight on the given topic; and snowball sampling involves the recommendations of other candidates who may have the same, similar, or greater expertise than those candidates chosen from the aforementioned selection (in this context) for the purpose of getting more insight. Qualitative and quantitative information (expert opinion & predictions on specific cybercrimes, profiling of cybercriminals, expert opinions on possible solutions to these cybercrimes, etc.) gathered through these techniques was then applied to the formation of a framework that could aid in the prevention/mitigation of cybercrime that may occur in the metaverse.

Relation to Social Sciences & Concepts

Theory more relating to the field of psychology were used in conjunction with the traditional methods of research mentioned above to reach a resolution regarding the mitigation of criminal behavior online/in the metaverse. Psychology is the most useful social science when it comes to understanding why these acts may be perpetrated. Understanding what personality traits may cause a perpetrator to commit a cybercrime will aid in the creation of methods used to combat it. Stavola & Choi utilized Eysenck's theory (theory pertaining to criminality) to help identify likelihoods of offense as well as what drives cybercriminals to commit crimes; Eysenck's theory places emphasis on biological factors, like personality traits (extraversion, neuroticism, and psychoticism), and how they factor into criminal activity. The principle/concept of objectivity is seen throughout the entirety of the study as the main goal is to advance knowledge on the topic of cybercrime and how it can be prevented. And the research prioritized objectivity by engaging candidates that have valuable knowledge and expertise in the field. They provided insight on the subject with questions asked based on observable trends as well as opinions formed off observable trends as seen by the prior and current research of the candidates.

Concerns for Marginalized Groups

Since cybercrime can take place anywhere on the internet, like social media website, in video games servers, via email, via text, etc., it is important to take note of how big of an issue this can become. The specific example used within the study mention an online game called, "Roblox". Roblox is a game that anyone can play, as long as they have internet access, where games/environments are/can be created for others to play. As of today, there are about 40 million games available to play just to put that into perspective. The article mentioned Roblox was up and coming, but in my opinion, it has been well established for a long time; see live player chart for reference. Monthly players remain steady with little to no loss.



Age is the big issue, as mentioned by Stavola & Choi, in terms of cybercrime relating to Roblox; typically, older individuals and adults are making the maps/games (18+), and the players are usually children. "With the high population of young gamers, it can be concluded that children are at high risk of becoming victims of cybercrime due to accessibility that adult gamers have to them" (Stavola & Choi, 2023, p. 7).

Results of the Study & Contribution to Society

Results of the study included the most probable age of the offenders, related socioeconomic issues and needs, the primary target(s), and best ways to mitigate/prevent the effects of cybercrimes.

> Expert 1 suggests that the age of these motivated offenders is likely to be in their 20s. It was further suggested that the crimes of this age group with strong sexual or economic needs with low social achievement will increase in the metaverse, as it is an entirely online platform…3 of the

> experts agreed that the motivation for these crimes will include financial gain or sexual gratification (p. 12).

Regarding primary targets/victims, typically children or young adults are more likely to be victims of cybercrimes, and for things like deepfakes, the primary targets become younger women.

Solutions proposed to help prevent the effects of cybercrimes involved intervention of parental guardians (capable guardians); school staff and related staff (informal capable guardians); and higher forms of guardians like law enforcement and psychological professionals/experts (formal capable guardians); as well as the implementation of a framework that establishes legal & technological means of detecting and managing the possibilities and actions of individuals who are perpetrating these cybercrimes.

Overall, Stavola & Choi's research advances knowledge on cybercrime and cyber victimization and serves as a reliable resource for society at large in addressing the challenges posed by cybercrime online and in the metaverse.

References

Roblox Live Player Count and Statistics. (2020, November 5). https://activeplayer.io/roblox/

Stavola, J., & Choi, K.-S. (2023). Victimization by Deepfake in the Metaverse: Building a Practical Management Framework. *International Journal of Cybersecurity Intelligence and Cybercrime*, *6*(2). https://doi.org/10.52306/2578-3289.1171