**Implementing Cyber Security Tools and/or Techniques in the Reduction of Cyberbullying**

***Introduction***

Today, almost everybody, including children and older people, has accepted the technology wave. The Internet is essential since it assists people in doing their work or learning online without traveling every day. Life has transformed even the people who do not work or learn online; they can accomplish other productive things like shopping, navigation, entertainment and socializing. Unfortunately, others have decided to use this enjoyable Internet by exploiting weaknesses in the architecture becoming hackers and cyber bullies. In that case, cybersecurity analysts have considered cybersecurity tools and tactics to solve this issue. Cyberbullying is a high-priority strategy challenge in numerous OECD nations. Cyberbullying has increased, shedding perceptions into the prevalence of the concern, and highlighting the features that make people ‘cyberbullied’.

***Literature review Statement***

* The paper will focus on putting cybersecurity tools into effect to minimize cyberbullying by focusing on an overview of the topic, research design, and the methodology of dealing with this issue.

***Body***

1. ***Overview***

* Cyberbullying is explained as worldwide hurtful conduct carried out by a cluster and is redone using contemporary updated technology.
* Cyberbullying has made cyber analysts put into action cyber security tools. These cyber security tools are developed in various forms of safeguarding computer plus network settings.
* The paper has also concentrated on the study design and methodology used in this topic.

1. ***Cyber Security Tools***

* Cybersecurity analysts have used different ways to minimize cyberbullying. In this case, the paper will concentrate on the following cybersecurity tools;

1. Network security monitoring tools (Fuentes-García et al., 2021).
2. Encryption tools (Das et al., 2014, 888).
3. Antivirus software (Al-Saleh and Crandall, 2011).
4. Network intrusion detection settings (Vinayakumar et al., 2017, 1285).
5. Web vulnerability scanning tools (Makino and Klyuev, 2015, 401).
6. Penetration testing (Arkin et al., 2005, 86).
7. ***Methodology***

* An article highlights an inference suggestion made up of a platform that targets to foil and minimize cyberbullying, which is experimentally authenticated (Garaigordobil and Martínez, 2018).

***Conclusion***

* Since cybersecurity analysts have implemented cybersecurity tools, cyberbullying is progressively minimized.
* People are also being educated on effective ways of handling the Internet to avoid being hacked or bullied online.

**References**

Al-Saleh, M.I. and Crandall, J.R., 2011. {Application-Level} Reconnaissance: Timing Channel Attacks Against Antivirus Software. In *4th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET 11)*.

Arkin, B., Stender, S. and McGraw, G., 2005. Software penetration testing. *IEEE Security & Privacy*, *3*(1), pp.84-87.

Das, Subrata Kumar, Md Alam Hossain, Md Arifuzzaman Sardar, Ramen Kumar Biswas, and Prolath Dev Nath. "Performance Analysis of Client Side Encryption Tools." *International Journal of Advanced Computer Research* 4, no. 3 (2014): 888.

Fuentes-García, M., Camacho, J. and Maciá-Fernández, G., 2021. Present and future of network security monitoring. *IEEE Access*, *9*, pp.112744-112760.

Garaigordobil Landazabal, M. and Martínez Valderrey, V., 2018. Technological Resources to Prevent Cyberbullying During Adolescence: the Cyberprogram 2.0 Program and the Cooperative Cybereduca 2.0 Videogame.

Makino, Y. and Klyuev, V., 2015, September. Evaluation of web vulnerability scanners. In *2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)* (Vol. 1, pp. 399-402). IEEE.

Vinayakumar, R., Soman, K.P. and Poornachandran, P., 2017, September. Evaluating effectiveness of shallow and deep networks to intrusion detection system. In *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 1282-1289). IEEE.