Peer Response 2

Hi Sherelle

A very interesting post, thank you for sharing.

The Rogue Services case clearly highlights the ethical violations committed by the company (ACM Ethics, 2018) as well as the need for web hosting providers to be proactive in their approach in terms of security and monitoring. Clients' activities should be monitored to ensure that their services are not being used for malicious purposes. However, at the same time General Data Protection Regulations (GDPR) must also be considered. Web hosting providers should invest in strong security measures and implement procedures to detect and prevent malicious activity in line with following the ethical principles of ACM (ACM Ethics, 2018) and BCS (BCS, 2022). In addition, Rogue Services should provide best practices around security when using their services.

Furthermore, the case of Rogue Services raises important ethical questions about the use of malware as a means of disruption. Malware in this case was simply used with good intentions to prevent a stop to Rogue Services, this is often known as malicious code for "righteous" purposes or "righteous malware" (Cobb & Lee, 2014). However, if not used carefully can cause unintended harm and violate ethical principles.

Lastly, governments and Internet Service Providers (ISP's) can play an important role in monitoring and regulating web hosting services ensuring that they are not being used for malicious purposes, this must also be in line with GDPR as mentioned above.

References

ACM Ethics. (2018) ACM Code of Ethics and Professional Conduct. Available from: https://ethics.acm.org/ [Accessed 03 February 2023].

BCS. (2022) The Chartered Institute for IT CODE OF CONDUCT FOR BCS MEMBERS. Available from: https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf [Accessed 03 February 2023].

Cobb, S & Lee, A. (2014) Malware is called malicious for a reason: The risks of weaponizing code', *International Conference on Cyber Conflict* 6(1): 71-84. Available from: https://www.researchgate.net/publication/286594792 [Accessed 04 February 2023].