

Initial Post

◀ Initial Post

Summary Post ▶

Display replies in nested form

Settings ▾



Initial Post

by [Fahad Abdallah](#) - Tuesday, 13 May 2025, 8:35 AM

The ACM brings attention to ethical issues affecting IT experts, including Rogue Services as a case in point. Even though Rogue Services claims to offer 'cheap, guaranteed uptime, no matter what,' the company allows clients who spread malware and spam on its servers (Association for Computing Machinery, n.d.). Rogue Services allows destructive ads on its platform that use browser flaws to infect computers with ransomware. Even though many takedown requests and reports have been submitted, Rogue Services has not taken action. The case raises many ethical, legal, and professional worries (BCS, 2022).

The ACM Code of Ethics highlights the importance of helping society and avoiding harm. Rogue Services goes against these values publicly by making it easy for cybercriminals to hurt people, businesses, and governments. Also, the code insists on being honest and transparent, but Rogue Services neglects this by making misleading claims while helping spread malicious content (Hou et al., 2024). Significant legal issues are at stake, particularly in places where cybercrime laws exist, such as the UK's Computer Misuse Act and the US's Cybersecurity Information Sharing Act. Such laws allow Rogue Services to be held responsible for distributing harmful software, even if they do not carry out the attacks. People's trust in online services is diminished, and users grow more anxious about their data protection because of what Rogue does. Additionally, businesses that use the internet daily face more risks due to Rogue Services' actions (Neprash et al., 2022).

About this, the British Computer Society (BCS) Code of Conduct places great importance on safeguarding public interests, privacy, and security. Rogue Services does not live up to these standards and disregards society's needs. Working with integrity is expected by ACM and BCS, yet Rogue complaints are ignored by Rogue (Tan et al., 2020).

References

Association for Computing Machinery. (n.d.). *Case Study: Malware Disruption*. Available at: <https://www.acm.org/code-of-ethics/case-studies/malware-disruption> (Accessed: 12 May 2025).

BCS. (2022). *BCS Code of Conduct*. Available at: <https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/> (Accessed: 12 May 2025).

Hou, Y., Guo, L., Zhou, C., Xu, Y., Yin, Z., Li, S., Sun, C., & Jiang, Y. (2024). An empirical study of data disruption by ransomware attacks. In *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering* (Article No. 161, pp. 1–12). IEEE/ACM. Available at: <https://doi.org/10.1145/3597503.3639090> (Accessed: 12 May, 2025).


Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., Rozenshtein, A. Z., & Nikpay, S. S. (2022). Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016-2021. *JAMA Health Forum*, 3(12), e224873. Available at: <https://doi.org/10.1001/jamahealthforum.2022.4873> (Accessed: 12 May 2025).

Permalink Reply



Re: Initial Post

by [Pëllumb Dalipi](#) - Thursday, 15 May 2025, 6:08 PM

My peer Fahad has offered a compelling discussion post on the the ethical negligence of Rogue Services. The discussed c  shows that irresponsibility can turn into a business model. In this situation the prioritisation of uptime over user safety has caused troubling outcomes. As Hou et al. (2024) show, ransomware attacks exploiting browser flaws are not rare but recurring and costly, especially for healthcare and public services. Flawed security enables risks to shift onto everyone within the affected ecosystem.

Chat to us!