

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!

Beyond the ethical failure, Rogue's behaviour raises serious questions about legal accountability as well. As Neprash et al. (2022) argue, when attacks are enabled, even if done so indirectly, a complicity can be argued in modern cybercrime laws. The concept of platforms being mainly providers of hosting services but otherwise not bound to any duty can be considered a simplistic. Governance programs like the UK's Online Safety Act increasingly challenge this passive stance.

Viewed through an ethical lens, Rogue violates not just ACM's principle to avoid harm (1.2), but also the duty to act with integrity and public responsibility, as outlined by both ACM and BCS codes. As Koops et al. (2017) underline, trust in mediated technology depends heavily on the accountability of providers, especially when user data is transmitted or stored through intermediaries. Under this view, Rogue's deliberate inaction cannot be seen as merely passive, but as actively enabling harm through neglect.

References

- Hou, Y. et al. (2024) 'An empirical study of data disruption by ransomware attacks', *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering*. <https://doi.org/10.1145/3597503.3639090>
- Neprash, H.T. et al. (2022) 'Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016–2021', *JAMA Health Forum*. <https://doi.org/10.1001/jamahealthforum.2022.4873>
- Koops, B.J., Newell, B.C., Timan, T., Škorvánek, I., Chokrevski, T. and Galič, M. (2017) 'A typology of privacy', *University of Pennsylvania Journal of International Law*.

[Permalink](#)

[Show parent](#)

[Reply](#)



Peer Response

by [Ali Alzahmi](#) - Friday, 16 May 2025, 5:59 PM

Fahad, thanks a lot for your thoughtful analysis of Rogue Services and its ethical violations in the context of ACM and BCS codes. What I especially liked is how you pointed out the deceptive nature of their "guaranteed uptime" marketing that masks the tremendous dangers that their services are representing to the public safety. You using the Computer Misuse Act and the Cybersecurity Information Sharing Act aligns this ethical debate in the given legal contexts that are very much current (Hou et al., 2024).

Your reference to public trust erosion is most relevant. The trust that clients can have towards digital services can be just as rapidly lost when cybersecurity is an issue. This relates to Cavoukian's, 2011, "Privacy by Design" principle, which emphasizes the necessity for security and trust from the users from the beginning. As you correctly assume, Rogue Services' negligence goes against such an approach as it facilitates the spread of malware and ransomware (Formosa et al., 2021).

Additionally, your observation on the professional integrity corresponds with the norm set by the BCS for the practitioner's interest to be working for the public interest (Elendu et al., 2024). You may also look at the role of proactive transparency. Organizations that have especially come out to be open in dealing with both cybersecurity reports and participate in takedown have stronger reputations and trust networks (Tyagi et al., 2024). Rogue Services' failure in that aspect is a clear demonstration of the fact that bad governance has ripple effects that go beyond just technical harm (Sison, 2023).

All things considered, your post is an argumentative and up-to-date discussion of the ethical, legal, and societal issues surrounding negligent service providers. Thank you for clear presentation of these points.

References:

- Elendu, C., Omeludike, E. K., Oloyede, P. O., Obidigbo, B. T., & Omeludike, J. C. (2024). Legal implications for clinicians in cybersecurity incidents: A review. *Medicine*, 103(39), e39887. Available at: <https://doi.org/10.1097/MD.00000000000039887> (Accessed: 15 May 2025).
- Formosa, P., Wilson, M., & Richards, D. (2021). A principlist framework for cybersecurity ethics. *Computers & Security*, 109, 102382. Available at <https://doi.org/10.1016/j.cose.2021.102382> (Accessed: 15 May 2025).
- Hou, Y. et al. (2024). *An empirical study of data disruption by ransomware attacks*. IEEE/ACM International Conference. Available at: <https://dl.acm.org/doi/abs/10.1145/3597503.3639090> (Accessed: 15 May 2025).
- Sison, A.J.G. and Redín, D.M., (2023). A neo-aristotelian perspective on the need for artificial moral agents (AMAs). *Ai & Society*, 38(1), pp.47-65. Available at: <https://link.springer.com/article/10.1007/s00146-021-01283-0> (Accessed: 15 May 2025).

[Chat to us!](#)

Tyagi, A. K., Kumari, S., & Richa. (2024). Artificial intelligence-based cyber security and digital forensics: A review. In A. K. Tyagi, S. Tiwari, S. K. Arumugam, & A. K. Sharma (Eds.), *Artificial intelligence for cybersecurity applications* (Chapter 18). Wiley. Available at: <https://doi.org/10.1002/9781394303601.ch18> (Accessed: 15 May 2025).

[Permalink](#)

[Show parent](#)

[Reply](#)



Re: Initial Post

by [Ali Yousef Ebrahim Mohammed Alshehhi](#) - Monday, 19 May 2025, 8:26 PM

Thank you Fahad for your careful consideration of the Rogue Services case. You've raised crucial points regarding how willful negligence in computer hosting services can cause system harm to users as well as society at large. Your inclusion of both ACM's professional ethics codes and relevant cybercrime laws conveys a clear grasp of the intersection between computer ethics and legal responsibility.

I particularly agree with your conclusion that violations of ACM principles 1.2 (Avoid Harm) and 1.3 (Be honest and trustworthy) occurred. Their putting uptime ahead of knowingly hosting malicious content shows Rogue Services' obvious disregard for its moral duty to protect users from foreseeable harm. Passive facilitation of immoral activity, as held by Baase and Henry (2021), is as guilty as active facilitation when inaction permits public risk.

Besides, as Pëllumb rightly pointed out, the BCS Code of Conduct also has an emphasis on the duty to act in the public interest and maintain professional integrity (BCS, 2022). Rogue's failure to act in responding to takedown notices is against these standards, at least constituting complicity under regimes like the UK's Online Safety Act 2023, expanding liability to service providers not to exclude online harm.

Furthermore, the erosion of confidence in online platforms, as highlighted by Koops et al. (2017), reflects a broader social impact: consumers increasingly question platforms' ability to safeguard their data, leading to reduced engagement and trust across the platform.

Your entry was successful in relating technical infrastructure to professional ethics and legal mandates—an essential skill in evaluating modern computing challenges.

References

Baase, S., & Henry, T. (2021). *A Gift of Fire: Social, Legal, and Ethical Issues for Computing Technology* (5th ed.). Pearson.
BCS. (2022). BCS Code of Conduct. Available at: <https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/> Accessed: 19 May 2025.
Koops, B. J., Newell, B. C., Timan, T., Škorvánek, I., Chokrevski, T., & Galič, M. (2017). A typology of privacy. *University of Pennsylvania Journal of International Law*, 38(2), 483–575.

[Permalink](#)

[Show parent](#)

[Reply](#)



Re: Initial Post

by [Nasser Al-Naimi](#) - Tuesday, 20 May 2025, 3:49 PM

Hello Fahad, the ethical issues associated with Rogue Services matter a lot, especially when we compare them to the rules of organizations like the ACM and BCS. The company's actions indicate that it does not prioritise its code of ethics or software distribution laws (Gogoll et al., 2021). As noted, the propagation of malware facilitated by Rogue Services leaves individuals and businesses in a hazardous state and weakens trust in digital platforms. It is clear from the ACM Code of Ethics, which aims to avoid harm and benefit people, that these acts are strongly opposed (Green, 2021). Rogue Services is acting against this principle by failing to make an effort to remove problematic content from its platforms. Penalties from the law are severe in such cases. The Computer Misuse Act in the UK and the Cybersecurity Information Sharing Act in the US both establish a clear legal basis for treating these companies responsibly (Button et al., 2025). However, it is concerning that Rogue Services has not taken more action. The interconnected nature of today's world means that businesses are exposed to many serious risks stemming from these weaknesses. If a company relies on digital services for its daily operations, any compromise can severely impact its finances and reputation (Javaid et al., 2023). As a result, businesses like Rogue Services break both legal and ethical rules, contributing to a growing scepticism about the internet's safety.

What further measures should regulatory bodies consider, given that such problems continue, to hold Rogue Services and other service providers answerable for creating these vulnerabilities?

References:

Gogoll, J., Zuber, N., Kacianka, S., Greger, T., Pretschner, A. and Nida-Rümelin, J., 2021. Ethics in the softw.

[Chat to us!](#)

process: from codes of conduct to ethical deliberation. *Philosophy & Technology*, 34(4), pp.1085-1108.
<https://link.springer.com/content/pdf/10.1007/s13347-021-00451-w.pdf> [accessed on: 18-may-25].

Green, B., 2021. The contestation of tech ethics: A sociotechnical approach to technology ethics in practice. *Journal of Social Computing*, 2(3), pp.209-225. <https://ieeexplore.ieee.org/document/9684741?denied=> [accessed on: 18-may-25].

Button, M., Shepherd, D., Blackburn, D., Sugiura, L., Kapend, R. and Wang, V., 2025. Assessing the seriousness of cybercrime: The case of computer misuse crime in the United Kingdom and the victims' perspective. *Criminology & Criminal Justice*, 25(2), pp.670-691. https://pure.port.ac.uk/ws/portalfiles/portal/58162871/Manuscript_for_Pure.pdf [accessed on: 18-may-25].

Javaid, M., Haleem, A., Singh, R.P. and Suman, R., 2023. Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*, 1, p.100016.
<https://www.sciencedirect.com/science/article/pii/S2772918423000048> [accessed on: 18-may-25]

[Permalink](#)

[Show parent](#)

[Reply](#)



Re: Initial Post

by [Radha Murugan](#) - Monday, 26 May 2025, 11:16 PM

The discussion points mentioned are very valid and it actually a good case study for anyone to know why user safety is important and how it is going to impact. Violating the principles of 1.1 and 1.2, contributing to society and human well-being and avoiding harm.

The discussion may include organization principle 3.1, Rogue's refusal to act against malicious activities hosted on its platform reflects a failure to ensure that computing systems are used are responsibly, violating the principle of public good is central concern during all professional computing work.

As mentioned in cliffs notes a better approach would have been to shut down Rogues thru official channel thru legal and regulation which would have less harm to the public (CliffsNotes, 2025). The discussion can insist more on the impact. The blog describes the impact of how Rogue has been leveraged by spam and other fraudulent services and exploit browser vulnerabilities (Mance, 2020).

References

CliffsNotes, 2025. ACM Code of Ethics Case Studies. [online] Available at: <https://www.cliffsnotes.com/study-notes/24129130>
<https://www.coursehero.com/file/69462866/Using-the/>

British Computer Society, n.d. BCS Code of Conduct. [online] Available at: <https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/>

Association for Computing Machinery, n.d. Abusive workplace behavior. [online] Available at: <https://www.acm.org/code-of-ethics/case-studies/abusive-workplace-behavior>

Association for Computing Machinery, 2018. ACM Code of Ethics and Professional Conduct. Available at: <https://www.acm.org/binaries/content/assets/about/acm-code-of-ethics-booklet.pdf>

[Permalink](#)

[Show parent](#)

[Reply](#)

[◀ Initial Post](#)

[Summary Post ▶](#)



Chat to us!

You are logged in as Fahad Abdallah (Log out)

[Policies](#)

Powered by Moodle

[Site Accessibility Statement](#)
[Privacy Policy](#)

© 2025 University of Essex Online. All rights reserved.



Chat to us!