

Cybercrime Community: How “Hanging Out” Online Facilitates Organized Crime

It may be surprising to some that a job characterized by deception can establish a strong, protective online community. Many hackers start largely because a friend volunteers their time to teach them. From one connection to globalized forums, the cybercrime community is unique in its ability to establish trust on large, anonymous online networks.

Author
River McFarlane, Honors Student

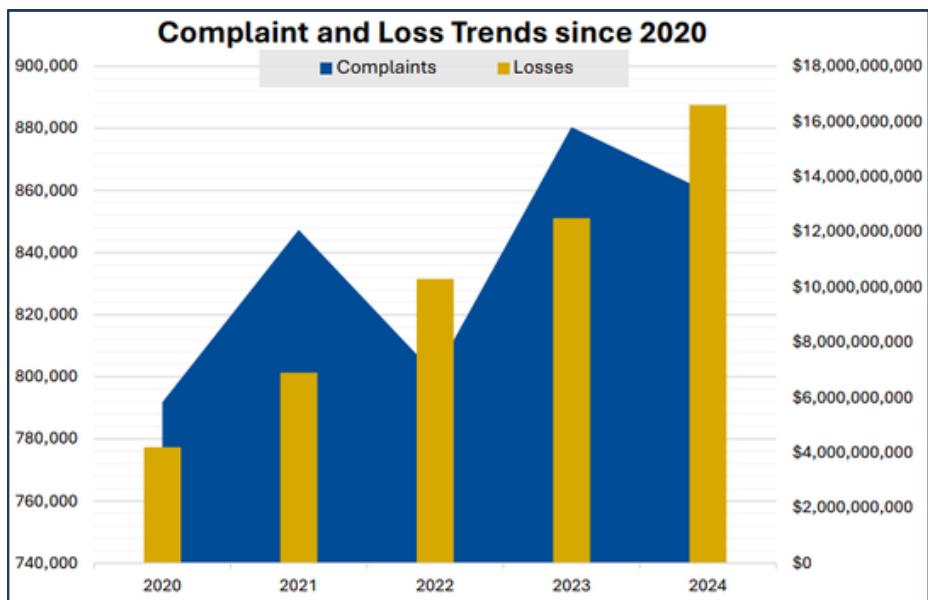
Affiliations
University of North Texas



1 Demographics and Stats

- The average hacker is in their 30's, and a large majority are male and white. However, ages can range from teens to sixties and a growing proportion of hackers are female.
- In 4 years losses have increased by \$14 million

Cybercrime has become increasingly prevalent:



Source: FBI. (2024). *Complaint and loss trends since 2020* [Infographic]. FBI.gov. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

3 Trust and ‘Rippers’

Working together and division of labor is an essential aspect of the hacker community, partly because it helps avoid detection:

“There’s a whole community out there of thousands of people that can solve any one of the problems online or make up any link of the chain if you don’t want to get involved [...] And it’s when they start working together like that detection’s much harder.” (Law Enforcement Officer #1) (Hutchings, 2014, p. 11)

Working together and establishing trust with others is a necessity, but how do you know who to trust? Many forums allow reputation ranking- the ability to review others based on the quality of their service. This is how people attempt to avoid ‘rippers,’ people who don’t deliver their product. For the most part, the threat of a bad review works to discourage ripping. Community ties also work to decrease deception between hackers.

Hiding in a sea of hackers helps to prevent detection:



Source: Graham, D. (2024). [Zebra Herd] [Photograph]. BBC Wildlife Magazine. <https://www.discoverwildlife.com/animal-facts/do-optical-illusions-work-on-animals-2>

2 Community, Forums, Initiation, and Culture

It’s easier to feel community with people who look, act, and speak like you (‘l33t speak’). While forums mainly exist to spread information and guides/how-to’s and to exchange services, there are sub-threads based purely on other interests.

Many people begin hacking because of an interest in computers, video games, and/or an attraction to the community.

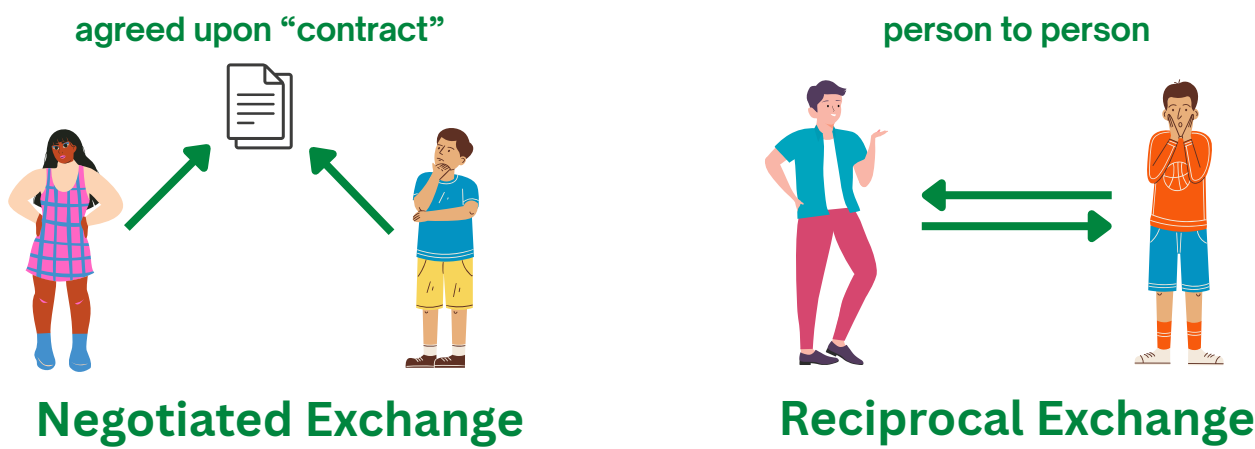
“... when offenders worked together it was not always considered to be organised crime, particularly with younger, less experienced offenders. Sometimes it was ‘just dudes hanging out’” (Hutchings, 2014, p. 9)



4 Reciprocal & Negotiated Exchange

One way to establish trust is through reciprocal exchange: choosing to help someone out on the principle that they might return the favor in the future. Negotiated exchange is more formal (quid pro quo) and associated with weaker ties.

Does the hacking community have high reciprocal exchange, as a way of building trust and defenses? Or is it more focused on achieving monetary gains through negotiated exchange?



- The hacker network is so vast and has such high turnover that establishing prolonged relationships with other hackers is rare. Some hackers even avoid working with the same person twice.
- However, initiation into the hacking community is characterized by reciprocal exchange, and the existence of a hacker culture and the protective nature of the community points to high prevalence of reciprocal exchange, even in the absence of long-term connections with other hackers.

Conclusion

The nature of the hacking community can be difficult to study and to understand. Overall, there is certainly a hacking culture, and with an established culture comes integrative norms. Most hackers start because of a personal connection with another hacker, and that one tie connects a beginner hacker to vast online communities. **Despite anonymity and a fear of detection, hacking communities manage to build trust through their interactions with one another.**

References

Dupont, B., Côté, A. M., Savine, C., & Décary-Héty, D. (2016). The ecology of trust among hackers. *Global Crime*, 17(2), 129–151. <https://doi-org.libproxy.library.unt.edu/10.1080/17440572.2016.1157480>

Gerstenfeld, J. (2023). Understanding the connection between hackers and their hacks: Analyzing USDOJ reports for hacker profiles. *International Journal of Cybersecurity Intelligence and Cybercrime*, 6(1), 59–76. <http://doi.org/10.52306/NSWY2537>

Hughes, J., Pastrana, S., Hutchings, A., Afroz, S., Samtani, S., Li, W., Marin, E. (2024). The art of cybercrime research. *Association for Computing Machinery*, 56(6), 1–26. <https://doi-org.libproxy.library.unt.edu/10.1145/3639362>

Hutchings, A. (2014). Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. *Crime Law Soc Change*, 62, 1–20. <https://doi-org.libproxy.library.unt.edu/10.1007/s10611-014-9520-z>

Jordan, T., Taylor, P. (2008). A sociology of hackers. *The Sociological Review*, 46(4), 757–780. <https://doi.org/10.1111/1467-954X.00139>

Molm, L. D., Whitham, M. M., & Melamed, D. (2012). Forms of exchange and integrative bonds: Effects of history and embeddedness. *American Sociological Review*, 77(1), 141–165. <https://doi-org.libproxy.library.unt.edu/10.1177/0003122411434610>

Steinmetz, Kevin F. (2015). Becoming a hacker: Demographic characteristics and developmental factors. *Qualitative Criminology*, 3(1), 31–60. <https://dc.swosu.edu/qc/vol3/iss1/2>