Tammy Rizo
September 20, 2026

Can Lack of Self-Control and Weak Social Bonds Contribute to Juvenile Hacking?

Introduction

Juvenile computer hacking is an important issue in cybersecurity because young people can use technology in ways that pose risks to individuals, organizations, and society. Considering the human factors behind cybercrime helps to understand why adolescents engage in hacking. Social science can help explain how individual characteristics and social relationships may influence risky behavior. In 2018, Sinchul Back, Sadhika Soor, and Jennifer LaPrade conducted a study titled *"Juvenile Hackers: An Empirical Test of Self-Control Theory and Social Bonding Theory"* in the *International Journal of Cybersecurity Intelligence & Cybercrime*. The study examined whether self-control and social bonds were associated with juvenile computer hacking.

Research, Social Science, and Findings

The researchers examined whether self-control theory and social bonding theory could help explain juvenile computer hacking among adolescents from eight countries (Back et al., 2018). The study included five hypotheses. The first predicted that higher levels of low self-control would increase the likelihood of hacking. The other four predicted that stronger parent attachment, parental supervision and involvement, and school attachment would reduce hacking. The dependent variable (DV) was computer hacking during the previous 12 months. The five primary independent variables (IVs) were low self-control, parent attachment, parental supervision, involvement, and school attachment. Gender, birthplace, and city size were also considered in the analysis (Back et al., 2018).

The researchers used quantitative, cross-sectional, self-report data from the second International Self-Report Delinquency Study (ISRD-2). Back et al. (2018) examined 18,985

adolescents from the United States, Venezuela, Spain, France, Germany, Poland, Hungary, and Russia. The surveys were collected between 2005 and 2007. Factor analysis was used to develop measures for the independent variables, and multivariate logistic regression was used to estimate the likelihood of hacking for each country separately. Since the study was cross-sectional, the results show relationships between variables but cannot prove that any factor directly caused hacking.

Several social science principles apply to this study, including empiricism, scientific inquiry, objectivity, and determinism. The study is empirical because the researchers used data collected from adolescents rather than relying only on assumptions. Scientific inquiry and objectivity are shown through hypotheses, measurable variables, systematic data collection, and statistical analysis. Determinism is reflected in the examination of whether individual characteristics and social relationships are associated with hacking. The study also connects concepts such as self-control, social bonding, risk-taking, deviance, and social environment. These concepts demonstrate that cybersecurity is not only a technological issue, but human behavior and social relationships can also contribute to cybersecurity problems.

The results showed that low self-control was a significant predictor of hacking in all eight countries (Back et al., 2018). The findings provided partial support for social bonding theory. Stronger parental supervision was associated with lower hacking in six countries, while school attachment was associated with lower hacking in three. However, parent attachment and involvement were generally not significant predictors. Male adolescents were also more likely than female adolescents to report hacking (Back et al., 2018). Overall, the findings suggest that individual characteristics and aspects of the social environment are associated with juvenile hacking.

Vulnerable Groups, Contributions, and Limitations

The study involved a vulnerable population because the participants were adolescents aged 12 to 15. Asking minors to self-report illegal or delinquent behavior raises concerns about privacy and the accuracy of their responses. In addition, the eight countries included in the study do not represent the entire international juvenile hacking population, which limits the generalizability of the findings (Back et al., 2018).

The study contributes to society by improving our understanding of factors associated with juvenile hacking and demonstrating that cybersecurity involves more than technology. The findings suggest that individual characteristics, parental supervision, and school relationships may be relevant to prevention. Although Back et al. (2018) provides important evidence, I believe other factors may also contribute to juvenile hacking, such as family environment, peers, access to technology, and other social conditions. Future research could examine how these factors interact rather than focusing on a limited number of influences.

Conclusion

Back et al. (2018) provide an empirical examination of juvenile computer hacking based on self-control and social bonding theories. Using quantitative data from adolescents across eight countries, the researchers found a consistent relationship between low self-control and hacking. At the same time, some forms of social bonding were associated with lower levels of hacking. Although the study has limitations, it demonstrates the value of using social science to understand juvenile cybercrime better. Understanding human behavior and social relationships can provide additional insight into juvenile hacking and support more comprehensive prevention efforts.

References

Back, Sinchul; Soor, Sadhika; and LaPrade, Jennifer (2018). Juvenile Hackers: An Empirical Test of Self Control Theory and Social Bonding Theory, *International Journal of Cybersecurity Intelligence & Cybercrime*: 1(1), 40-55. https://www.doi.org/10.52306/01010518VMDC9371