Systematic Literature Review

Primary drivers for teenagers' illegal hacking, as evidenced by criminological literature from the past five years: A systematic literature review

Antonina Savka

University of Essex Online

Abstract

From the traumatic experience victims face due to an intrusion into their private world to expensive ransomware needed to protect both data and national security, the impact of hacking has shown steady growth in recent years. Nevertheless, policy recommendations concerning this topic remain controversial. Despite ample empirical research in cybercrime deterrence, the motivations behind teenage hacking are lacking and require further study. The current systematic literature review aimed to examine this gap and, thus, contribute to policy improvements. The relevant literature was selected from four scholarly databases through the application of inclusion and exclusion criteria to identify the main themes used to explain cyber-dependent crime among teenagers. Among the reviewed literature, six main themes emerged: internal motivators as a natural characteristic of this age group, seduction by attractive opportunities to hack, masculinity, the criminal nature of hackers, the need for social acceptance, and weak social bonds. While the theme of internal motives was predominant, the theme of weak social bonds as an instigator in hacking was neither supported nor disproved due to the conflicting findings. The review concluded by acknowledging the limitations and advising on the policy implications and further research.

Keywords: cybercrime, hacking, motivation, systematic literature review, teenagers

Date of Submission: 28.04.2025 **Date of Acceptance:** 01.10.2025

Acknowledgements

I would like to thank Dr Christine Weirich for inspiration and guidance.

Essex Student Journal, 2025, Vol. 17(1)
DOI: https://doi.org/10.5526/esj.428

Primary drivers for teenagers' illegal hacking, as evidenced by criminological literature from the past five years: A systematic literature review

1. Introduction

Since its emergence in the past century, cybercrimes have evolved in different forms, shifting offensive physical behaviour to the virtual realm (Tcherni *et al.*, 2015). Its advantages in remoteness and anonymity, in combination with poor cybersecurity and availability of technical skills, may seduce those who would not commit a crime in the physical world to offend online (Goldsmith and Wall, 2022). In fact, Rokven *et al.* (2018) identified two subgroups of cybercrime: cyber-enabled and cyber-dependent. Cyber-enabled crime (such as cyberbullying, online fraud, and similar) usually mirrors an offline offence on the Internet. In contrast, cyber-dependent crime (such as hacking) is impossible outside of computers, and its impact resembles that of organised crime (Choo and Grabosky, 2014). For example, in 2021, a cyberattack on the Irish Health System exposed the private population data of close to 90,000 patients, causing ongoing distress to all affected (HSE, 2023). From a financial perspective, the most expensive cyberattack, known as NotPetya, was committed in 2017 across multiple countries and caused damage of ten billion dollars (Steinberg, Stepan and Neary, 2021).

Obviously, such a diversity of cybercrimes and the scale of their impact requires a thoughtful policymaking approach (Holt *et al.*, 2021). However, Soesanto and Smeets (2021) noted that there is no agreement between scholars on recommendations. In fact, they identified three groups of different opinions on cybercrime policy: (1) the existing policies for offline crimes should be applied to cybercrimes due to their similarity, (2) cybercrimes are unique and require a different deterrence approach, and (3) cybercrimes cannot be deterred. In addition, studies like Goldsmith and Wall (2022) and Lee and Holt (2020) show an early onset at the age when an offender is unlikely to be prosecuted, but rarely address this factor when advising on policy. Soesanto and Smeets (2021) suggested that the issue is in the misapplication of the deterrence concept to cybercrime. Thus, to understand which deterrence policy is effective, policymakers must first understand what motivates adolescents to make their first hacking attempt.

The contemporary literature explains hackers' motivation at different levels, from defining hackers' typology to focusing on a particular subgroup's motives. For example, Chng *et al.* (2022) aggregated hackers into thirteen groups (novices, cyberpunks, insiders, old guards, professionals, hacktivists, nation states, students, petty thieves, digital pirates, online sex offenders, crowdsourcers, and crime facilitators) which are driven by seven primary motives (curiosity, financial, notoriety, revenge, recreation, ideology, and sex impulses). They found financial and revenge motives to be prevailing. Meanwhile, Weulen Kranenbarg (2021) highlighted the domination of intrinsic motives as the main differentiator between online and offline offenders. However, the limitation of contemporary studies is their focus on experienced successful hackers, leaving a gap in understanding why teenagers choose this path in the first place. Hence, to address this oversight and support policymaking decisions, the current systematic literature review aims to identify the main themes used to explain cyber-dependent crime among young people. In particular, this research will identify what primarily drives teenagers to commit illegal hacking. While acknowledging the limitations, it will conclude by advising on the policy implications and further research.

 Essex Student Journal, 2025, Vol. 17(1)
DOI: https://doi.org/10.5526/esj.428

2. Methodology

2.1. Inclusion and exclusion criteria

With the increased diversity of cybercrime, the research focus on this subject has also been dispersed (Parder, Gryffroy and Juurik, 2024). Interestingly, while early research prevalently concentrates on hacking, due to the growing popularity of social media, the focus has since shifted to cyber-enabled crimes such as cyberbullying, identity fraud, and online stalking (Rokven *et al.*, 2018). Hence, hacking was selected as a subject of this review for a couple of reasons: first, cyber-dependent crime relies on rapidly evolving technologies and technical skills, which, over time, may change the primary drivers for hacking; second, compared to cyber-enabled crime, hacking poses a significant threat (Szpor and Gryszczyńska, 2022).

This systematic literature review is focused on teenagers motivated by the age-related phenomenon of cybercrimes: an early onset by the age of 12, with more severe hacks being committed in late teens (Lee and Holt, 2020). In addition, the nature of cybercrime allows hackers to operate from anywhere worldwide (Choo and Grabosky, 2014). Therefore, this study includes research done in any country of the world. Further, as hackers turn to the most recent technologies, it is tempting to assume that the research concerning hackers should keep up with the rapid evolution of these technologies (Shwedeh, Malaka and Rwashdeh, 2023). Hence, the current review analyses literature only from the last five years specifically: the selection range is from January 1st, 2020, until the final search date, which was conducted on September 11th, 2024. The decision not to include the full five years from September 11th, 2019, to September 11th, 2024, is due to some scholarly databases' inability to specify dates more granular than in years.

The inclusion and exclusion data are provided in Table 1 in Appendix A.

2.2. Final query and database search

The research query was created using the SPIDER tool (Cooke, Smith and Booth, 2012). However, to reduce the number of irrelevant findings, the original formula proposed by Cooke, Smith and Booth (2012, p. 1438) – "[S AND P of I] AND [(D OR E) AND R]" – was adjusted to become [S AND P of I] AND [E AND (D OR R)] and the NOT operator was added to the final search query:

(juvenile* OR adolescent* OR teen* OR youth* OR young) AND (cybercrim* OR "cyber crim*" OR cyber-crim* OR cyberattack* OR cyber-attack* OR "cyber attack*" OR cyberdeviance OR cyber-deviance OR "cyber deviance" OR hacking OR hacker* OR "digital crime*") AND (character* OR reason* OR motiv* OR why OR cause OR explain* OR explanation OR factors OR behavio* OR attitud* OR benefit*) AND (questionnaire OR survey OR interview* OR "focus group*" OR "case stud*" OR observ* OR data* OR sample* OR qualitative OR "mixed method*" OR quantitative OR "dynamic panel model*" OR longitudinal) AND NOT (sharing OR orthography OR messenger OR stem OR sexting OR suicid*)

DOI: https://doi.org/10.5526/esj.428

The search was performed in four scholarly databases:

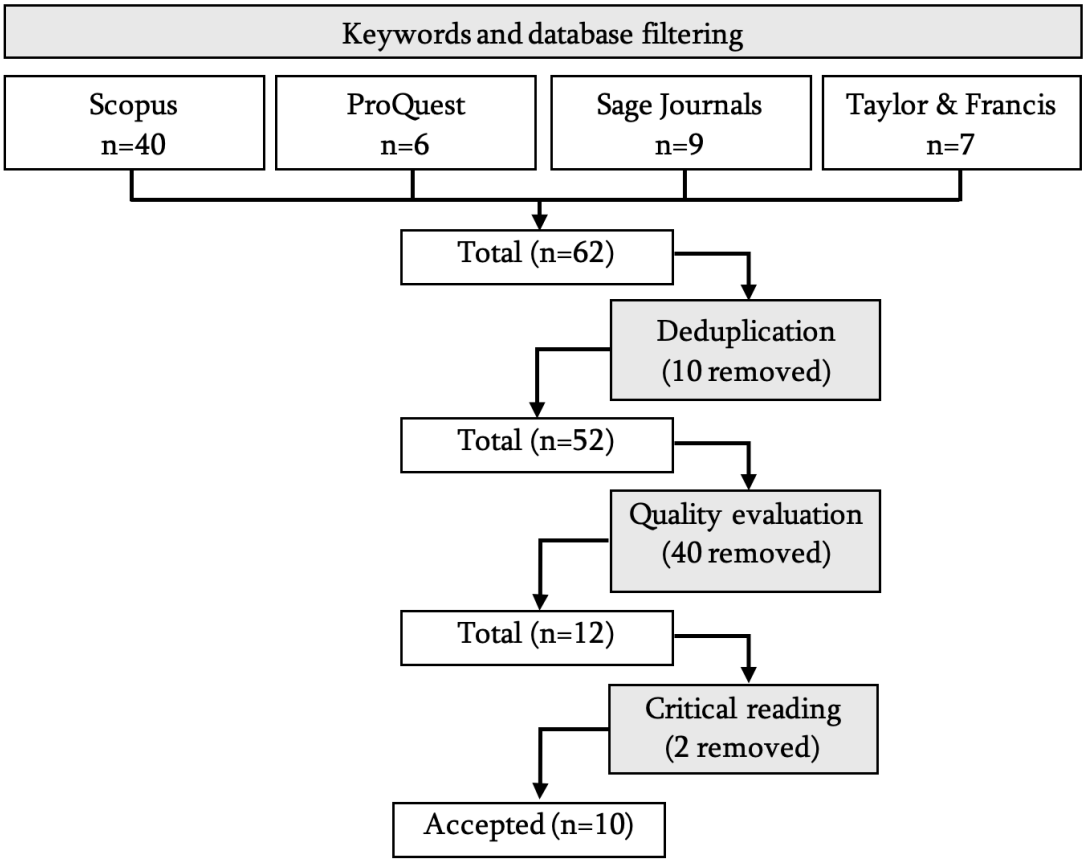
- Scopus
- ProQuest
- Sage Journals
- Taylor and Francis

Due to each database's limitations, the query was split and adjusted to achieve the maximum rigour result.

2.3. Evaluating results

The selection process (Figure 1) produced ten documents, all journal articles. Each accepted document was critically analysed to identify the research samples' characteristics, the drivers behind teenage hacking, and proposed policy implications. The findings of this systematic literature review, the synthesis of extracted data by themes, critical analysis of the reviewed literature, and the limitations are further outlined in the following sections.

Figure 1 - Selection process flow



DOI: https://doi.org/10.5526/esj.428

3. Findings

After applying the abovementioned methods, ten documents were found relevant to the question of primary drivers for teenagers' illegal hacking. A few key characteristics emerge among the found literature, which include:

- All documents are quantitative research.
- Half of the studies use the ISRD-2 dataset of self-reported youth delinquency (Enzmann *et al.*, 2015).
- The prevalent explanation of teenage hacking behaviour centred around the General Theory of Crime, Routine Activity Theory and Social Learning Theory (Bandura, 1977; Cohen and Felson, 1979; Gottfredson and Hirschi, 1990).
- Eight of ten findings discuss gender as a characteristic of hackers.
- Half of the studies consider a drift between online and offline delinquency.
- Four of ten papers include an impact of social bonds.
- A small number of documents briefly touch on the environment, education or technical skills, and positive attitude to violence as stimuli for hacking among teenagers.

The full analysis of the findings is provided in Table 2 in Appendix B.

Ultimately, six main themes were determined: internal motivators, attractive opportunity, masculinity, criminal nature, need for social acceptance, and weak social bonds. Table 3 in Appendix C provides a breakdown of how the findings were categorised.

4. Discussion

Despite teenage illegal hacking being a serious crime, this review has demonstrated a shortage of literature which seeks to explore the primary motivators behind it. Some findings in this review emphasise ample qualitative research (Holt, Navarro and Clevenger, 2020). Yet, this research (for example, Holt (2007) and Taylor (1999)) is over 15 years old and, therefore, excluded from the current review. Furthermore, half of the quantitative studies in this review rely on the almost twenty-year-old self-reported ISRD-2 dataset (Enzmann *et al.*, 2015). Accounting for the rapid digitalisation of our lives, such slow progression in the criminological study of youth hacking makes the current policy rely on obsolete data and, hence, carries a risk of being ineffective (Wall, 2024). Still, the current review identifies six main themes explaining the primary drivers of teenage hacking.

4.1. Themes

4.1.1. Internal motivators

The majority of findings (80%) approach teenage hacking from a low self-control perspective (Aiken *et al.*, 2024; Fox and Holt, 2021; Guo and Wang, 2024; Holt *et al.*, 2021; Holt, Navarro and

 Essex Student Journal, 2025, Vol. 17(1)
DOI: https://doi.org/10.5526/esj.428

Clevenger, 2020; Kim, Leban and Lee, 2024; Lee and Holt, 2020; Whitten *et al.*, 2024). Indeed, as Holt, Navarro and Clevenger (2020, p. 1537) mentioned, the scholars suggest the relationship between adolescent hacking and "the general turbulence often seen in this period of development." As an underlying factor of teenagers' low self-control, the researchers list such motivators as impulsivity, violent temperament, self-centeredness, and risk-taking (Aiken *et al.*, 2024; Fox and Holt, 2021; Holt *et al.*, 2021; Lee and Holt, 2020). Additionally, Fox and Holt (2021) included emotional trauma as a motivator among 15% of researched hackers. This is contrary to the research done by Guo and Wang (2024) utilising machine learning on the same ISRD-2 dataset, which found self-control to be a low-risk factor for hacking.

4.1.2. Attractive opportunity

The second popular theme among findings (70%) is the opportunity to hack or, as Goldsmith and Wall (2022) put it, seduction (Aiken *et al.*, 2024; Fox and Holt, 2021; Guo and Wang, 2024; Holt *et al.*, 2021; Holt, Navarro and Clevenger, 2020; Lee and Holt, 2020; Wright, 2020). These works identify unrestricted access to digital devices, time spent online, and engagement in piracy and gaming as instigating factors for hacking. Nonetheless, some researchers disagree on whether good technical skills boost the desire to hack. While Aiken *et al.* (2024) and Lee and Holt (2020) considered that enhanced tech skills stimulate hacking by reducing the sense of detection and responsibility, Holt *et al.* (2021) degraded the importance of high-tech skills for such simple forms of hacking as password-guessing. Therefore, one may conclude that the simplicity of the crime itself rather than the hacker's ability fuels the desire to hack.

4.1.3. Masculinity

Another popular theme among researchers (60%) is a desire for hacking as a phenomenon prevalent among males (Aiken *et al.*, 2024; Fox and Holt, 2021; Guo and Wang, 2024; Holt, Navarro and Clevenger, 2020; Kim, Leban and Lee, 2024; Walters, 2023). In particular, Kim, Leban and Lee (2024, p. 1986) concluded that hacking gives "boys ... a sense of power and domination," while Walters (2023) excluded the female samples from the results as they appear to be statistically insignificant. However, gender per se is seen as a characteristic rather than a stimulus. Particularly, Wright (2020, p. 1721) argued that gender is "an inconsistent predictor," which is supported by Holt *et al.*'s (2021) research showing an increase in female hackers. Hence, Wright (2020) suggested that researchers should instead look at aggression provoked by masculinity rather than gender to understand what motivates teenage hackers.

4.1.4. Criminal nature

Similarly, 60% of papers explain hacking via a willingness to commit a crime (Aiken *et al.*, 2024; Guo and Wang, 2024; Holt, Navarro and Clevenger, 2020; Kim, Leban and Lee, 2024; Walters, 2023; Whitten *et al.*, 2024). In particular, Aiken *et al.* (2024) believed that hacking is driven by a positive attitude to violence, which aligns with the conclusion of others that hackers are capable of drifting

DOI: https://doi.org/10.5526/esj.428

between online and offline delinquency. Nevertheless, while Guo and Wang (2024) supported offline/online dependency, they considered the criminal attitude to be a low-risk factor.

4.1.5. Need for social acceptance

Surprisingly, only 40% of reviewed literature considers hacking a peer-motivated crime (Fox and Holt, 2021; Holt, Navarro and Clevenger, 2020; Kim, Leban and Lee, 2024; Lee and Holt, 2020). Adolescence is when social acceptance is the most important for self-development (Tomova, Andrews and Blakemore, 2021). Based on the time young people spend gaming and socialising online, it is possible to conclude that most of their peers share the same virtual space. As older researchers suggest, hacking is a subculture: adolescents who become part of the hacker community need to prove their hacking skills to achieve exposure and respect from their peers (Lee, 2018; Sela-Shayovitz, 2012). Interestingly, no research among findings disproves peer-instigation as a significant factor for hacking.

4.1.6. Weak social bonds

The role of social bonds with family and school in motivating hackers received less attention and support among findings. Here, the scholars' opinions divert: while Aiken *et al.* (2024) and Lee and Holt (2020) supported the idea that strong family and school bonds act as demotivators, Guo and Wang (2024) and Kim, Leban and Lee (2024) found low to no relation between hacking and social attachment. Hence, there is not enough literature to prove or disprove the impact of weak social bonds on illegal teenage hacking. More research using more recent data is required to cover this theme.

4.2. Policy implication

This review also uncovers conflicting opinions among scholars on policy implications. Holt *et al.* (2021), Holt, Navarro and Clevenger (2020) and Lee and Holt (2020) concluded that the researched motivations align with the existing criminological theories well and, therefore, there is no need for a new policy. Conversely, Fox and Holt (2021) acknowledged the need for a new approach based on the hacking drivers' uniqueness. After looking at the approach each of these scholars used to answer the question, it is possible to conclude that advice on policy implications depends on whether the research focuses on the crime itself or on applying existing theory.

4.3. Limitations

The current review has a few limitations. Firstly, the search query restricts results to papers with the age group mentioned in the title. Such a specific requirement overlooks any other research on hackers' motivation, even with a suitable sample age group; for example, Holt and Steinmetz (2021) and Owen and Head (2022). Secondly, the applied criteria excluded publications prior to 2020, as well as the grey literature, except for conference papers. As Soesanto and Smeets (2021) noted, most

DOI: https://doi.org/10.5526/esj.428

research and publications on cybercrime were conducted by 2016, which falls outside the current research date range. For example, while Aiken, Davidson and Amann's (2016) work on youth pathways into cybercrime supports the proposed themes, it also extends the approach beyond criminological theories. On the other hand, this limitation highlights a problem: there is still a lack of effective policies while hacking is on the rise (for example, Tidy (2025) and Townsend (2025)).

5. Conclusion

A hacker's professional path starts with a little knowledge and an initial toolkit (Van Beveren, 2001). Different hacker typologies refer to them using different terms like "newbies," "novices," or "script kiddies," but the definition remains the same: "[lowly] skilled hackers who heavily rely on online toolkits" (Chng *et al.*, 2022, p. 4). As with any other crime, demotivating young people from entering the criminal path is a proactive way to reduce the number of cybercrimes. This systematic literature review has found that, in the last five years, scholars have tried to explain teenage hacker motivation by applying the General Theory of Crime, Routine Activity Theory and Social Learning Theory (Bandura, 1977; Cohen and Felson, 1979; Gottfredson and Hirschi, 1990). Among the reviewed literature, six main themes emerged: internal motivators as a natural characteristic of this age group, seduction by attractive opportunities to hack, masculinity, the criminal nature of hackers, the need for social acceptance, and weak social bonds. Importantly, half of the reviewed research was conducted on almost twenty-year-old self-reported data, which may compromise the relevance of defined motivations to starting hackers.

This review has also found that none of the analysed literature gives much attention to how the age of hackers impacts their perception of cybercrime. When turning focus to recent social and traditional media content, one may notice that academic studies do not directly address the idea that adolescents may perceive hacking just as another form of gaming (Irish Tech News, no date). However, it is possible to consider that internal motivation, attractive opportunities, and the need for social acceptance indirectly contribute to such teenagers' perceptions. Additionally, the findings do not address the impact of cybercrime remoteness on the hacker's mindset, which may cancel the effectiveness of most existing deterrence methods. Surprisingly, monetary gain as a motivator was not included in any of the reviewed studies.

Thus, a few policy implications should be considered. Firstly, policymakers should focus on teenagers' rebellious and adventure-seeking nature to tackle their involvement in deviant interaction in the virtual world (Zhang and Li, 2022). Deriving from Filley's (1999) conclusions, cybercrime deterrence through defence only instigates teenagers into delinquent behaviour, while cultivating mindfulness helps reduce the chance of harm in risky situations. Hence, it is worth investing in educating teenagers to understand the direct and indirect impact of cybercrime on all affected. Secondly, as our daily interactions in the virtual world increase, the policies must also define cyber-etiquette, emphasising respect for virtual privacy and personal data. Lastly, the skills and inspiration of adolescents already engaged in hacking can be re-used to enhance cyber-defence.

DOI: https://doi.org/10.5526/esj.428

Both modern society and national security may greatly benefit from converting young black-hat hackers into white-hat ones, as in examples with Reuben Paul and Cal Leeming (Leeming, 2022).

However, the mentioned policy implications must be taken cautiously due to the limitations of the current and reviewed studies. To test the proposed deterrence approaches, it is advisable to perform another review on the correlation between harm awareness and delinquency among youth. Additionally, to understand how technological evolution encourages hacking, it is worthwhile to conduct further research using the most recent data (for example, the ISRD-4 dataset) and trace a change in hackers' motivation between generations (Marshall *et al.*, 2022). Lastly, instead of applying the fit-in-theory approach, it may be beneficial to revisit the issue of hacking from a psychological perspective to understand and deter this youth crime of the digital age.

References

Aiken, M., Davidson, J. and Amann, P. (2016) *Youth Pathways into Cybercrime*. Available at: https://www.europol.europa.eu/cms/sites/default/files/documents/pathways-white-paper.pdf (Accessed: 30 September 2025).

Aiken, M. P. *et al.* (2024) 'Intention to Hack? Applying the Theory of Planned Behaviour to Youth Criminal Hacking', *Forensic Sciences*, 4(1), pp. 24-41. Available at: https://doi.org/10.3390/forensicsci4010003

Bandura, A. (1977) *Social Learning Theory*. USA: Prentice Hall.

Chng, S. *et al.* (2022) 'Hacker types, motivations and strategies: A comprehensive framework', *Computers in Human Behavior Reports*, 5, pp. 1-8. Available at: https://doi.org/10.1016/j.chbr.2022.100167

Choo, K.-K. R. and Grabosky, P. (2014) 'Chapter 24 Cybercrime', in L. Paoli (ed), *The Oxford Handbook of Organized Crime*. Oxford University Press, pp. 482–499.

Cohen, L. E. and Felson, M. (1979) 'Social Change and Crime Rate Trends: A Routine Activity approach', *American Sociological Review*, 44(4), pp. 588-698. Available at: https://doi.org/10.2307/2094589

Cooke, A., Smith, D. and Booth, A. (2012) 'Beyond PICO: The SPIDER Tool for Qualitative Evidence Synthesis', *Qualitative Health Research*, 22(10), pp. 1435-1443. Available at: https://doi.org/10.1177/1049732312452938

Enzmann, D. *et al.* (2015) *Second International Self-Reported Delinquency Study*, 2005-2007. Available at: https://doi.org/10.3886/ICPSR34658.v2

Filley, D. (1999) 'Forbidden Fruit: When Prohibition Increases the Harm It Is Supposed to Reduce', *The Independent Review*, 3(3), pp. 441-451. Available at: http://www.jstor.org/stable/24560928 (Accessed: 2 October 2025).

DOI: https://doi.org/10.5526/esj.428

Fox, B. and Holt, T. J. (2021) 'Use of a Multitheoretic Model to Understand and Classify Juvenile Computer Hacking Behavior', *Criminal Justice and Behavior*, 48(7), pp. 943-963. Available at: https://doi.org/10.1177/0093854820969754

Goldsmith, A. and Wall, D. S. (2022) 'The seductions of cybercrime: Adolescence and the thrills of digital transgression', *European Journal of Criminology*, 19(1), pp. 98-117. Available at: https://doi.org/10.1177/1477370819887305

Gottfredson, M. R. and Hirschi, T. (1990) *A general theory of crime*. Stanford University Press.

Guo, S. and Wang, Y. (2024) 'Investigating predictors of juvenile traditional and/or cyber offense using machine learning by constructing a decision support system', *Computers in Human Behavior*, 152. Available at: https://doi.org/10.1016/j.chb.2023.108079

Holt, T. J. (2007) 'Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures', *Deviant Behavior*, 28(2), pp. 171-198. Available at: https://doi.org/10.1080/01639620601131065

Holt, T. J. *et al.* (2021) 'Assessing the Role of Opportunity and Low Self-Control in Juvenile Hacking', *Crime & Delinquency*, 67(5), pp. 662-688. Available at: https://doi.org/10.1177/0011128720978730

Holt, T. J., Navarro, J. N. and Clevenger, S. (2020) 'Exploring the Moderating Role of Gender in Juvenile Hacking Behaviors', *Crime & Delinquency*, 66(11), pp. 1533-1555. Available at: https://doi.org/10.1177/0011128719875697

Holt, T. J. and Steinmetz, K. F. (2021) 'Examining the Role of Power-Control Theory and Self-Control to Account for Computer Hacking', *Crime & Delinquency*, 67(10), pp. 1491-1512. Available at: https://doi.org/10.1177/0011128720981892

HSE. (2023) *Cyber-attack and HSE response*. Available at: https://www2.hse.ie/services/cyber-attack/what-happened/ (Accessed: 27 April 2025).

Irish Tech News (no date) *Interview with Reuben Paul: Cyber Security Wake-Up Call – Hacking is Child's Play*. Available at: https://irishtechnews.ie/interview-with-reuben-paul-cyber-security-wake-up-call-hacking-is-childs-play/amp/ (Accessed: 27 April 2025).

Kim, J., Leban, L. and Lee, Y. (2024) 'Theoretical Explanations of the Development of Youth Hacking', *Crime & Delinquency*, 70(8), pp. 1971-1992. Available at: https://doi.org/10.1177/00111287221115639

Lee, B. H. (2018) 'Explaining Cyber Deviance among School-Aged Youth', *Child Indicators Research*, 11(2), pp. 563-584. Available at: https://doi.org/10.1007/s12187-017-9450-2

Lee, J. R. and Holt, T. J. (2020) 'Assessing the Factors Associated With the Detection of Juvenile Hacking Behaviors', *Frontiers in Psychology*, 11. Available at: https://doi.org/10.3389/fpsyg.2020.00840

DOI: https://doi.org/10.5526/esj.428

Leeming, C. (2022) *UK's youngest convicted hacker and youth work*. Available at: https://pjp-eu.coe.int/en/web/youth-partnership/cal-leeming (Accessed: 27 April 2025).

Marshall, I. H. *et al.* (2022) *International Self-Report Delinquency (ISRD4) Study Protocol: Background, Methodology and Mandatory Items for the 2021/2022 Survey*. Available at: https://www.ssoar.info/ssoar/handle/document/78879 (Accessed: 27 April 2025).

Owen, K. and Head, M. (2022) 'Motivation and Demotivation of Hackers in Selecting a Hacking Task', *Journal of Computer Information Systems*, 63(3), pp. 522-536. Available at: https://doi.org/10.1080/08874417.2022.2081883

Parder, M., Gryffroy, P. and Juurik, M. (2024) 'Ethical considerations in a pan-European project targeting adolescent cybercrime prevention', *Research Ethics*, 20(3), pp. 471-489. Available at: https://doi.org/10.1177/17470161241247803

Petrosyan, A. (2024) *Annual number of data compromises and individuals impacted in the United States from 2005 to 2023.* Available at: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (Accessed: 27 April 2025).

Rokven, J. J. *et al.* (2018) 'Juvenile Delinquency in the Virtual World: Similarities and Differences between Cyber-Enabled, Cyber-Dependent and Offline Delinquents in the Netherlands', *International Journal of Cyber Criminology*, 12(1), pp. 27-46. Available at: https://doi.org/10.5281/zenodo.1467690

Sela-Shayovitz, R. (2012) 'Gangs and the Web: Gang Members' Online Behavior', *Journal of Contemporary Criminal Justice*, 28(4), pp. 389-405. Available at: https://doi.org/10.1177/1043986212458191

Shwedeh, F., Malaka, S. and Rwashdeh, B. (2023) 'The Moderation Effect of Artificial Intelligent Hackers on the Relationship between Cyber Security Conducts and the Sustainability of Software Protection: A Comprehensive Review', *Migration Letters*, 20(S9), pp. 1066-1072. Available at: https://migrationletters.com/index.php/ml/article/view/4947 (Accessed: 27 April 2025).

Soesanto, S. and Smeets, M. (2021) 'Cyber Deterrence: The Past, Present, and Future', in F. Osinga and T. Sweijs (eds), *NL ARMS Netherlands Annual Review of Military Studies 2020*. Asser Press, pp. 385-400. Available at: https://doi.org/10.1007/978-94-6265-419-8_20

Steinberg, S., Stepan, A. and Neary, K. (2021) *NotPetya: A Columbia University Case Study*. Available at: https://www.sipa.columbia.edu/sites/default/files/2022-11/NotPetya%20Final.pdf (Accessed: 27 April 2025).

Szpor, G. and Gryszczyńska, A. (2022) 'HACKING IN THE (CYBER)SPACE', *GIS Odyssey Journal*, 2(1), pp. 141-152. Available at: https://doi.org/10.57599/gisoj.2022.2.1.141

Taylor, P. (1999) *Hackers: Crime and the Digital Sublime*. Routledge.

DOI: https://doi.org/10.5526/esj.428

Tcherni, M. *et al.* (2015) 'The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave?', *Justice Quarterly*, 33(5), pp. 890-911. Available at: https://doi.org/10.1080/07418825.2014.994658

Tidy, J. (2025) *Children hacking their own schools for 'fun', watchdog warns'*. Available at: https://www.bbc.com/news/articles/c203pedz58go (Accessed: 30 September 2025).

Tomova, L., Andrews, J. L. and Blakemore, S. (2021) 'The importance of belonging and the avoidance of social risk taking in adolescence', *Developmental Review*, 61. Available at: https://doi.org/10.1016/j.dr.2021.100981

Townsend, K. (2025) *The Rise of the Teen Hacker: Big Breaches, Zero Experience*. Available at: https://www.intercede.com/the-rise-of-the-teen-hacker-big-breaches-zero-experience/ (Accessed: 30 September 2025).

Van Beveren, J. (2001) 'A Conceptual Model Of Hacker Development And Motivations', *Journal of E-Business*, 1(2), 1-9.

Wall, D. S. (2024) *Cybercrime: The Transformation of Crime in the Information Age*. 2nd edn. Polity.

Walters, G. D. (2023) 'The Person-Computer Interface in Delinquency Research: Proactive Criminal Thinking as a Moderator of the Hacking with Peers–Juvenile Offending Relationship', *Journal of Police and Criminal Psychology*, 38(3), pp. 584-592. Available at: https://doi.org/10.1007/s11896-023-09581-7

Weulen Kranenbarg, M. (2021) 'Cyber-Dependent Crime Versus Traditional Crime: Empirical Evidence for Clusters of Offenses and Related Motives', in M. Weulen Kranenbarg and R. Leukfeldt (eds), *Cybercrime in Context*. Springer, pp. 195–216. Available at: https://doi.org/10.1007/978-3-030-60527-8_12

Whitten, T. *et al.* (2024) 'Exploring the Role of Self-Control Across Distinct Patterns of Cyber-Deviance in Emerging Adolescence', *International Journal of Offender Therapy and Comparative Criminology*, OnlineFirst. Available at: https://doi.org/10.1177/0306624x231220011

Wright, M. F. (2020) 'The Role of Technologies, Behaviors, Gender, and Gender Stereotype Traits in Adolescents' Cyber Aggression', *Journal of Interpersonal Violence*, 35(7-8), pp. 1719-1738. Available at: https://doi.org/10.1177/0886260517696858

Zhang, Z. and Li, C. (2022) 'Adolescent Rebellion: Causes and Guiding Strategies', *Science Insights*, 40(4), pp. 485-487. Available at: https://doi.org/10.15354/si.22.re050

DOI: https://doi.org/10.5526/esj.428

Appendices

Appendix A

Table 1 - Inclusion and exclusion criteria

Criterion	Inclusion	Exclusion
Sample	Teenagers (age 12-19)	• cybercrime victims • hackers out of the age range of 12-19 • ethical hackers
Phenomenon of interest	Illegal hacking	• cyber-enabled crimes, such as harassment, bullying, promotion of violence and fake news, distribution of pornography and sexual abuse, sexting, fraud, scams and similar • cybersecurity awareness evaluation • 'hacker' and 'hacking' applied to the domains outside cybercrime • research where the author's or cited scholar's last name is the same as one of the search keywords while the content is irrelevant to the cybercrime theme
Design	Questionnaires, surveys, interviews, focus groups, case studies, observations, data and samples	
Evaluation	Characteristics, reasons, motives, causes, explanations, factors, behaviour, attitude and benefits	unclear purpose
Research type	Dynamic panel model, longitudinal, qualitative, quantitative and mixed methods	analysis with no empirical data involved
Date range	January 1st, 2020 – September 11th, 2024	any document published earlier than January 1st, 2020
Language	English	any other language than English as the only language of the document
Geography	Global	
Document type	Article, conference paper	book, letter
Access	Full text, available via either the University of Essex or open access	restricted for the University of Essex Online account

DOI: https://doi.org/10.5526/esj.428

Appendix B

Table 2 - Analysis of motivations for hacking

#	Authors	Title	Year	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
1	Aiken et al.	Intention to Hack? Applying the Theory of Planned Behaviour to Youth Criminal Hacking	2024	+	+	+				+	+	
2	Fox and Holt	Use of a Multitheoretic Model to Understand and Classify Juvenile Computer Hacking Behavior	2021		+		+	+	+	+		
3	Guo and Wang	Investigating predictors of juvenile traditional and/or cyber offense using machine learning by constructing a decision support system	2024	-	-	-		+		+		+
4	Holt et al.	Assessing the Role of Opportunity and Low Self-Control in Juvenile Hacking	2021		+			+		-	-	
5	Holt, Navarro and Clevenger	Exploring the Moderating Role of Gender in Juvenile Hacking Behaviors	2020		+		+	+	-	+		+
6	Kim, Leban and Lee	Theoretical Explanations of the Development of Youth Hacking	2024		+	-	+			+		+
7	Lee and Holt	Assessing the Factors Associated With the Detection of Juvenile Hacking Behaviors	2020		+	+	+	+				
8	Walters	The Person-Computer Interface in Delinquency Research: Proactive Criminal Thinking as a Moderator of the Hacking with Peers–Juvenile Offending Relationship	2023							+		+
9	Whitten et al.	Exploring the Role of Self-Control Across Distinct Patterns of Cyber-Deviance in Emerging Adolescence	2024		+							+
10	Wright	The Role of Technologies, Behaviors, Gender, and Gender Stereotype Traits in Adolescents' Cyber Aggression	2020					+		-		

Legend:

(1) Positive attitude to violence
(2) Self-control
(3) Social bonds/control (parents, school)
(4) Social learning (peers, subculture)
(5) Opportunity and routine activity (computer, gaming, time online, piracy)
(6) Environment (neighbourhood)
(7) Gender
(8) Grade/tech knowledge
(9) Online/offline crime correlation

"+" – the paper supports motivation as significant.

"-" – the paper degrades or does not support motivation as significant.

Essex Student Journal, 2025, Vol. 17(1)
DOI: https://doi.org/10.5526/esj.428

Appendix C

Table 3 - Identified themes of motivations for hacking

Theme	Author(s)	Articles	Year	DOI
Internal motivators	Aiken et al.	Intention to Hack? Applying the Theory of Planned Behaviour to Youth Criminal Hacking	2024	10.3390/forensicsci4010003
	Fox and Holt	Use of a Multitheoretic Model to Understand and Classify Juvenile Computer Hacking Behavior	2021	10.1177/0093854820969754
	Guo and Wang	Investigating predictors of juvenile traditional and/or cyber offense using machine learning by constructing a decision support system	2024	10.1016/j.chb.2023.108079
	Holt et al.	Assessing the Role of Opportunity and Low Self-Control in Juvenile Hacking	2021	10.1177/0011128720978730
	Holt, Navarro and Clevenger	Exploring the Moderating Role of Gender in Juvenile Hacking Behaviors	2020	10.1177/0011128719875697
	Kim, Leban and Lee	Theoretical Explanations of the Development of Youth Hacking	2024	10.1177/00111287221115639
	Lee and Holt	Assessing the Factors Associated With the Detection of Juvenile Hacking Behaviors	2020	10.3389/fpsyg.2020.00840
	Whitten et al.	Exploring the Role of Self-Control Across Distinct Patterns of Cyber-Deviance in Emerging Adolescence	2024	10.1177/0306624X231220011
Attractive opportunity	Aiken et al.	Intention to Hack? Applying the Theory of Planned Behaviour to Youth Criminal Hacking	2024	10.3390/forensicsci4010003
	Fox and Holt	Use of a Multitheoretic Model to Understand and Classify Juvenile Computer Hacking Behavior	2021	10.1177/0093854820969754
	Guo and Wang	Investigating predictors of juvenile traditional and/or cyber offense using machine learning by constructing a decision support system	2024	10.1016/j.chb.2023.108079
	Holt et al.	Assessing the Role of Opportunity and Low Self-Control in Juvenile Hacking	2021	10.1177/0011128720978730
	Holt, Navarro and Clevenger	Exploring the Moderating Role of Gender in Juvenile Hacking Behaviors	2020	10.1177/0011128719875697
	Lee and Holt	Assessing the Factors Associated With the Detection of Juvenile Hacking Behaviors	2020	10.3389/fpsyg.2020.00840
	Wright	The Role of Technologies, Behaviors, Gender, and Gender Stereotype Traits in Adolescents' Cyber Aggression	2020	10.1177/0886260517696858

DOI: https://doi.org/10.5526/esj.428

Masculinity	Aiken et al.	Intention to Hack? Applying the Theory of Planned Behaviour to Youth Criminal Hacking	2024	10.3390/forensicsci4010003
	Fox and Holt	Use of a Multitheoretic Model to Understand and Classify Juvenile Computer Hacking Behavior	2021	10.1177/0093854820969754
	Guo and Wang	Investigating predictors of juvenile traditional and/or cyber offense using machine learning by constructing a decision support system	2024	10.1016/j.chb.2023.108079
	Holt et al.	Assessing the Role of Opportunity and Low Self-Control in Juvenile Hacking	2021	10.1177/0011128720978730
	Holt, Navarro and Clevenger	Exploring the Moderating Role of Gender in Juvenile Hacking Behaviors	2020	10.1177/0011128719875697
	Kim, Leban and Lee	Theoretical Explanations of the Development of Youth Hacking	2024	10.1177/00111287221115639
	Walters	The Person-Computer Interface in Delinquency Research: Proactive Criminal Thinking as a Moderator of the Hacking with Peers–Juvenile Offending Relationship	2023	10.1007/s11896-023-09581-7
	Wright	The Role of Technologies, Behaviors, Gender, and Gender Stereotype Traits in Adolescents' Cyber Aggression	2020	10.1177/0886260517696858
Criminal nature	Aiken et al.	Intention to Hack? Applying the Theory of Planned Behaviour to Youth Criminal Hacking	2024	10.3390/forensicsci4010003
	Guo and Wang	Investigating predictors of juvenile traditional and/or cyber offense using machine learning by constructing a decision support system	2024	10.1016/j.chb.2023.108079
	Holt, Navarro and Clevenger	Exploring the Moderating Role of Gender in Juvenile Hacking Behaviors	2020	10.1177/0011128719875697
	Kim, Leban and Lee	Theoretical Explanations of the Development of Youth Hacking	2024	10.1177/00111287221115639
	Walters	The Person-Computer Interface in Delinquency Research: Proactive Criminal Thinking as a Moderator of the Hacking with Peers–Juvenile Offending Relationship	2023	10.1007/s11896-023-09581-7

DOI: https://doi.org/10.5526/esj.428

	Whitten et al.	Exploring the Role of Self-Control Across Distinct Patterns of Cyber-Deviance in Emerging Adolescence	2024	10.1177/0306624X231220011
Need for social acceptance	Fox and Holt	Use of a Multitheoretic Model to Understand and Classify Juvenile Computer Hacking Behavior	2021	10.1177/0093854820969754
	Holt, Navarro and Clevenger	Exploring the Moderating Role of Gender in Juvenile Hacking Behaviors	2020	10.1177/0011128719875697
	Kim, Leban and Lee	Theoretical Explanations of the Development of Youth Hacking	2024	10.1177/00111287221115639
	Lee and Holt	Assessing the Factors Associated With the Detection of Juvenile Hacking Behaviors	2020	10.3389/fpsyg.2020.00840
Weak social bonds	Aiken et al.	Intention to Hack? Applying the Theory of Planned Behaviour to Youth Criminal Hacking	2024	10.3390/forensicsci4010003
	Guo and Wang	Investigating predictors of juvenile traditional and/or cyber offense using machine learning by constructing a decision support system	2024	10.1016/j.chb.2023.108079
	Kim, Leban and Lee	Theoretical Explanations of the Development of Youth Hacking	2024	10.1177/00111287221115639
	Lee and Holt	Assessing the Factors Associated With the Detection of Juvenile Hacking Behaviors	2020	10.3389/fpsyg.2020.00840

Copyright Statement

This article is licensed CC BY 4.0 (Antonina Savka) Essex Student Journal, 2025, Vol. 17(1)
DOI: https://doi.org/10.5526/esj.428