RedFame

Journal of Education and Training Studies
Vol. 14, No. 1; January 2026
ISSN 2324-805X E-ISSN 2324-8068
Published by Redfame Publishing
URL: http://jets.redfame.com

Ethical Hacking in the Digital Age: Insights from Twelfth Graders

Mohammed Borhandden Musah[1], Asma Khaleel Abdallah[2], Lokman Mohd Tahir[3], Adnan Mohammad Farah[4], Mohammed Issah1Author[4]

[1]Data Analytics, Policy, and Leadership Division, Emirates College for Advanced Education, Abu Dhabi, United Arab Emirates

[2]Department of Educational Leadership, Sharjah Education Academy, Sharjah, United Arab Emirates

[3]School of Education, Faculty of Social Sciences and Humanities, Universiti Technologi Malaysia, Johor, Malaysia

[4]Department of Education Studies, Bahrain Teachers College, University of Bahrain, Bahrain

Correspondence: Mohammed Borhandden Musah, Data Analytics, Policy, and Leadership Division, Emirates College for Advanced Education, Abu Dhabi, United Arab Emirates. Email: mohammed.borhandden@ecae.ac.ae

Received: July 30, 2025 Accepted: October 18, 2025 Online Published: October 22, 2025

doi:10.11114/jets.v14i1.7848 URL: https://doi.org/10.11114/jets.v14i1.7848

Abstract

Purpose - This study examines the impact of teaching ethical hacking to twelfth graders in a private school from the students' perspective. It analyzes using an ethical hacking pedagogical approach to enhance information security instruction. *Method* - A case study design was employed, and data were collected through semi-structured interviews with three twelfth-grade students who were purposefully selected to investigate their experiences with ethical hacking. *Results* - The findings indicate that ethical hacking positively impacts students' professional development by enhancing problem-solving, critical thinking, teamwork, and communication skills relevant to various fields. Notably, twelfth graders participating in ethical hacking form a close-knit community that collaborates and shares resources, fostering positive social interaction. Additionally, the findings highlight that this teaching method helps twelfth graders prioritise legal aspects, such as obtaining authorisation and respecting privacy laws. Furthermore, teaching ethical hacking challenges stereotypes, promotes responsibility, and encourages a positive attitude towards cybersecurity. The findings suggest that incorporating ethical hacking into information security instruction offers practical and engaging learning opportunities. *Originality* – The results are significant because few studies have examined twelfth graders' perceptions of ethical hacking in the era of digital advancement. This research enhances the likelihood of successful and problem-free information security programmes.

Keywords: ethical hacking, information security instruction, ethical hacking pedagogy, digital advancement, information security

1. Introduction

Ethical hacking, also known as penetration testing or white-hat hacking, is an emerging topic in the technology field. It involves authorised individuals or organisations, known as ethical hackers, who use their knowledge and skills to identify vulnerabilities in computer systems, networks, and software applications (Dhirani et al., 2023; Kumawat et al., 2021; Pike, 2013; Smith et al., 2022; Trabelsi & Ibrahim, 2013).

The main objective of ethical hacking is to assess the security of a target system and provide recommendations for improvement (Brogdon, 2021; Kumar et al., 2024a). Ethical hackers can uncover potential weaknesses that unauthorised individuals could exploit by mimicking the techniques and methodologies used by malicious hackers. This assists organisations in enhancing their security measures and protecting their systems from cyber threats.

Ethical hacking offers several advantages. First, it helps organisations proactively identify and rectify vulnerabilities before malicious actors exploit them. Ethical hackers can help prevent data breaches, system compromises, and other security incidents by conducting thorough security assessments. Additionally, ethical hacking promotes a proactive security mindset, encouraging organisations to stay ahead of emerging threats and continuously improve their security practices. Furthermore, ethical hacking supports compliance with industry regulations and standards. Many sectors, such as finance, healthcare, and government, have specific compliance requirements for data protection and security (Kumar et

al., 2024). Organisations can demonstrate their commitment to maintaining a secure environment and adhering to relevant regulations by conducting regular ethical hacking assessments.

However, it is essential to acknowledge that ethical hacking, like any other activity, has potential drawbacks (Kasim et al., 2022; Kumawat et al., 2021; Pike, 2013; Smith et al., 2022). One concern is the possibility of accidental damage or disruption caused during the testing process. Despite the ethical hacker's best intentions, there is always a small risk that a system could be adversely affected during vulnerability scanning or penetration testing. Therefore, conducting such activities in a controlled and carefully planned manner is essential, with proper authorisation and permission. Additionally, ethical hacking knowledge and tools might fall into the wrong hands. While ethical hackers operate within legal boundaries, malicious actors can still misuse their techniques and tools. Consequently, it is crucial to ensure proper safeguards are in place to prevent unauthorised access to ethical hacking resources (Kasim et al., 2022).

1.1 Theoretical Framework

The teaching of ethical hacking to twelfth graders in the era of digital advancement can be conceptualised through the integration of socio-constructivist learning theory, ethical decision-making models, and digital literacy frameworks. Socio-constructivist theory emphasises learning through social interaction and problem-solving, critical in ethical hacking education as students engage in collaborative activities such as vulnerability analysis and penetration testing (Vygotsky, 1978).

Ethical decision-making models, such as Rest's Four-Component Model, provide a foundation for addressing moral dilemmas in cybersecurity by promoting moral sensitivity, judgment, motivation, and action (James, 1986). These models assist students in distinguishing ethical hacking practices from malicious behaviour, fostering a principled understanding of digital ethics. Digital literacy frameworks emphasise equipping students to critically analyse and responsibly use digital tools (Ng, 2012). Teaching ethical hacking enhances students' digital competencies and prepares them to tackle cybersecurity challenges in a technologically advanced world. This theoretical framework bridges technical skills, moral reasoning, and critical thinking, empowering students to navigate the digital landscape responsibly and contribute to cybersecurity defense.

It is worth noting that ethical hacking is a valuable practice for enhancing cybersecurity and protecting computer systems and networks (Pike, 2013; Smith et al., 2022). It helps organisations identify and address vulnerabilities, maintain compliance with regulations, and develop proactive security measures. However, Pike (2013), Smith et al. (2022), and Trabelsi and Ibrahim (2013) emphasise the importance of approaching ethical hacking with caution in the teaching and learning sector. It should be conducted responsibly, with appropriate permissions, and focused on improving security rather than causing harm. Despite the advantages of teaching ethical hacking, adverse effects have been observed when it is taught to high school students in relation to their professional, social, legal, and cultural aspects (Abu-Shaqra, 2021; Dhirani et al., 2023; Kasim et al., 2022; Quasim et al., 2023; Trabelsi & Ibrahim, 2013). Therefore, this study investigates the effects of teaching ethical hacking on twelfth graders in a private school from the students' perspectives. It also analyses using an ethical hacking pedagogical approach to improve information security instruction. The study poses the following research questions:

1. What are the effects of teaching ethical hacking to high school students on their professional development?
2. How does teaching ethical hacking impact the social interactions and relationships of high school students?
3. What legal considerations are associated with teaching ethical hacking to high school students?
4. What cultural implications arise from teaching ethical hacking to high school students?
5. Does an ethical hacking pedagogical approach enhance information security instruction for high school students?

2. Literature Review

2.1 Ethical Hacking and Professional Development

Professional development in ethical hacking refers to continuously enhancing students' knowledge, skills, and competencies in integrating ethical considerations into their instructional practices (Brogdon, 2021; Hartley, 2015). It involves providing learners with opportunities to deepen their understanding of ethical issues, develop strategies for addressing them, and cultivate a strong ethical foundation in their professional development. This encompasses learners' ethical awareness, knowledge of ethical frameworks, integration of ethics into the curriculum, collaborative ethical decision-making, classroom management, ethical behaviour, and continuous learning and growth (Mooney Simmie et al., 2023; Nyaaba & Zhai, 2024; Roos & Bagger, 2024; Novawan et al., 2024).

Ethical awareness and reflection: Professional development programmes in ethical teaching promote self-awareness and reflection among educators. They encourage teachers and students alike to examine their values, beliefs, and biases and

consider how these may influence their learning and instructional decisions. Educators are encouraged to reflect on ethical dilemmas that may arise in the classroom and develop strategies for addressing them in a principled manner.

Knowledge of ethical frameworks and principles: Professional development programmes teach teachers about ethical frameworks and principles relevant to education. This includes understanding ethical theories, such as virtue ethics, consequentialism, and deontology, and how they apply to educational contexts (Hartley, 2015; Novawan et al., 2024). Teachers learn to use these frameworks to make ethically informed decisions in their teaching practice.

Integrating ethics across the curriculum: Professional development programmes in ethical hacking support teachers in incorporating ethical considerations. They provide strategies and resources for infusing ethical discussions, critical thinking, and moral reasoning into various subject areas (Hartley, 2015). This helps students develop ethical awareness and engage in thoughtful ethical discussions within the context of their learning.

Classroom management and ethical behaviour: Professional development in ethical hacking instruction includes training on classroom management techniques that promote ethical behaviours and foster a positive learning environment. Educators learn strategies for cultivating a sense of community, respect, and empathy among students. They also learn how to address ethical issues in student behaviour, such as cheating, bullying, or discrimination.

Collaboration and ethical decision-making: Professional development programmes in ethical hacking encourage teachers to collaborate with colleagues, administrators, and other stakeholders to tackle ethical educational challenges. This involves engaging in ethical decision-making processes and seeking input from others to gain a well-rounded perspective. Teachers learn to navigate complex ethical dilemmas by considering multiple viewpoints and the ethical implications involved.

Continuous learning and growth: Professional development in ethical teaching underscores the importance of constant learning and growth. Teachers are encouraged to stay updated on moral issues and educational research related to ethics in teaching (Kumar et al., 2024). They are given opportunities to attend workshops, conferences, and seminars to enhance their knowledge and skills in ethical teaching.

According to Younis et al. (2019) and Brown et al. (2024), active participation in ethical hacking activities enhances learners' technical skills in network security, cryptography, web application security, and penetration testing methodologies. These skills are highly valued in cybersecurity and can improve learners' career prospects. Specifically, evaluation data on ethical hacking has shown that more than 85% of surveyed students felt that the dynamic platform gave them greater freedom to experiment and engage, thereby supporting their professional career requirements.

2.2 Ethical Hacking and Learners' Social Interaction

"social interaction" refers to how people engage and communicate in social settings (Hurst et al., 2013; Khan et al., 2024; Kumar et al., 2024a). Regarding ethical hacking, students' development in social interaction can be both positive and challenging.

2.3 Positive Effects

Collaboration and teamwork: Ethical hacking often involves working in teams or groups. Students collaborate to identify vulnerabilities, share knowledge, and collectively address security issues (Abu-Shaqra, 2021; Hurst et al., 2013). This collaborative environment helps develop teamwork skills and encourages effective communication, task delegation, and striving towards a common goal.

Knowledge sharing and learning: Ethical hacking is a multidisciplinary field that requires expertise in various areas, as it encompasses systems across all sectors. Students with different backgrounds and skill sets come together to learn from one another and share knowledge (Hartley, 2015; Hurst et al., 2013). This exchange of ideas and information enhances students' understanding of cybersecurity concepts and promotes a culture of continuous learning.

Networking and Professional Relationships: Engaging in ethical hacking activities can connect students with professionals and experts in the field. They may participate in cybersecurity conferences, workshops, or online communities to meet like-minded individuals, mentors, and potential employers (Khan et al., 2024). These interactions can lead to meaningful professional relationships and expand students' networks.

2.4 Potential Challenges

Lack of Face-to-Face Interaction: Ethical hacking activities primarily occur in virtual or online environments, which can limit face-to-face interaction. Although students can effectively collaborate and communicate through digital platforms, the absence of in-person interaction may impede the development of key social skills, such as non-verbal communication and rapport-building. To address this challenge, it is essential to create opportunities for students to engage in in-person activities, such as workshops, seminars, or local cybersecurity meetups. These events facilitate networking, social skill development, and personal connections among students and professionals (Hurst et al., 2013).

Ethical Dilemmas and Communication Challenges: Ethical hacking introduces students to ethical dilemmas that require thoughtful consideration and decision-making, promoting critical and ethical thinking skills. Students may encounter situations where they must effectively communicate their findings, recommendations, or concerns to stakeholders, including clients or non-technical individuals. Conveying technical information and navigating ethical discussions can be challenging for some students. Including discussions on ethical considerations and communication challenges in ethical hacking training programmes can address this issue (Hurst et al., 2013). By encouraging constructive debates, articulating viewpoints, and practising effective communication techniques, students can enhance their ability to convey technical information to diverse audiences.

Limited Exposure to Diverse Perspectives: Ethical hacking communities and activities sometimes lack diversity in representation and perspectives due to their unique responsibilities. This limitation restricts students' exposure to different viewpoints and experiences, hindering their ability to develop well-rounded social interactions. Promoting inclusivity and seeking diverse perspectives within ethical hacking communities is crucial to foster a more comprehensive learning environment (Hurst et al., 2013; Kumar et al., 2024; Ul Haq et al., 2022). Therefore, actively encouraging the participation of students from diverse backgrounds and seeking out varied viewpoints enriches the learning experience and prepares students for the eclectic nature of the cybersecurity industry.

According to the findings of Pike (2013), students who participate in cybersecurity competitions and learn about ethical hacking experience an expansion of their social interaction skills. The study also reveals that the strength of these social connections affects students' behaviour, as they gain a deeper understanding of ethical hacking practices. Learning institutions organizing ethical hacking competitions provide white-hat hackers with an excellent platform to appreciate the differences between the white-hat and black-hat sides of the cybersecurity industry. The focus is on highlighting the advantages of white-hat hacking and the risks associated with black-hat hacking.

2.5 Ethical Hacking and Learners' Legal Practice

The concept of legal practice involves assessing a learner's ability to recall and apply knowledge, skills, and understanding within a specific timeframe while operating within a defined legal and ethical framework. Teaching learners about ethical hacking introduces them to various legal aspects. According to Yaacoub et al. (2023), ethical hacking increases learners' understanding of legal issues. Engaging in ethical hacking makes learners aware of the legal considerations and regulations surrounding cybersecurity. They must better understand the legal boundaries and restrictions regarding accessing systems, obtaining proper authorisation, and handling sensitive information. This heightened legal awareness can positively impact students' future legal practices, ensuring compliance with relevant laws and regulations. It is worth noting that knowledge of ethical hacking reinforces ethical behaviour. Kumar et al. (2024) and Yaacoub et al. (2023) argue that ethical hacking emphasises the importance of ethical behaviour and responsible practices. Students learn the significance of obtaining proper authorisation, respecting privacy, and adhering to ethical standards. These lessons can influence their legal practices by reinforcing the importance of acting ethically, upholding professional integrity, and avoiding illegal activities throughout their careers.

Moreover, teaching students about ethical hacking deepens their understanding of cybersecurity laws. Ethical hacking activities often require students to navigate cybersecurity laws and regulations. By engaging in ethical hacking, students become familiar with legal frameworks such as computer crime laws, data protection regulations, and intellectual property rights (Dhirani et al., 2023; Ul Haq et al., 2022a; Yaacoub et al., 2023). This knowledge informs their legal practices and enables them to advise organisations on compliance and risk mitigation.

Additionally, findings by Hagendorff (2020) concluded that ethical hacking equips students with professional ethics and responsibilities. Therefore, ethical hacking reinforces the importance of professional ethics and responsibility. Students learn to balance their technical skills with legal and ethical considerations, promoting responsible practices in their future careers. This emphasis on professional ethics can positively impact their legal practices by ensuring they prioritise the law, client interests, and ethical standards in their work.

2.6 Ethical Hacking and Learners' Cultural Development

The concept of an ethical culture often characterises an organisation's principles, conduct, and operational methods. It pertains to how individuals collaborate within the organisational framework, aiming to meet their obligations to colleagues and customers through adherence to a predefined set of fundamental values (Parmar et al., 2016). A robust ethical culture supporting individuals committed to honesty and ethical conduct will cultivate investor trust, contribute to resilient global capital markets, and ultimately bring societal benefits. This underscores the significance of ethical considerations (Parmar et al., 2016). Ethical hacking can contribute to the development of various culturally related aspects.

Ethical hacking exposes students to advanced technical concepts, tools, and methodologies, providing them with a culture of technological literacy. By engaging in ethical hacking activities, students develop a deeper understanding of computer systems, networks, and cybersecurity (Christen et al., 2023; Yaacoub et al., 2023). This increased technological literacy contributes to their cultural development by fostering a sense of curiosity, adaptability, and comfort with technology in various cultural contexts (Christen et al., 2023; Yaacoub et al., 2023). Researchers have found that ethical hacking promotes responsible and ethical behaviour in the digital realm. Ethical hacking activities can positively impact cultural development by teaching students about privacy, authorisation, and ethics, instilling integrity, empathy, and respect for diverse cultural values and norms. Ethical hacking also promotes problem-solving skills, as students must think critically and creatively to identify vulnerabilities and propose solutions (Jumale, 2019; Sahare et al., 2014; Ul Haq et al., 2022).

According to Abu-Shaqra (2021), teaching hacking fosters a culture of problem-solving skills. Ethical hacking requires students to think critically and creatively to identify vulnerabilities and propose solutions, contributing to developing valuable problem-solving skills in various cultural and societal contexts. Students enhance their artistic development by analysing complex situations, evaluating risks, and finding innovative solutions by fostering a proactive and constructive mindset (Abu-Shaqra, 2021).

Ethical hacking also involves teamwork and collaboration. Students work together to address security challenges, share knowledge, and exchange ideas, fostering effective communication, teamwork, and intercultural interactions (Nguyen, 2018; Yaacoub et al., 2021). This collaborative environment helps students navigate cultural differences, respect diverse perspectives, and work effectively in multicultural settings, contributing to their artistic development by promoting cross-cultural understanding and cooperation.

In summary, ethical hacking has a multifaceted impact on students' cultural development. It enhances their technological literacy, moral awareness, problem-solving skills, collaboration and communication abilities, ethical decision-making capabilities, and cybersecurity awareness. These findings highlight the potential of ethical hacking to foster students' cultural development by equipping them with valuable skills, knowledge, and attitudes necessary to thrive in a culturally diverse and technologically driven world.

2.7 Ethical Hacking and Learners' Pedagogical Development

Pedagogical development in ethical teaching refers to enhancing and advancing teaching methods and strategies focused explicitly on ethical education. It involves continuous improvement and refinement of instructional approaches to effectively convey ethical principles, values, and practices to learners (Al-Tawil, 2024; Hartley, 2015; Srivatanakul & Annansingh, 2022). This term emphasises the integration of ethical considerations into the broader context of educational pedagogy, aiming to cultivate a deeper understanding and appreciation of ethical concepts among students. According to Al-Tawil (2024), instructing students in hacking is the only practical method for equipping future cybersecurity professionals with the essential technical skills required for penetration testing. Such pedagogy impacts students' development in various areas, including the practical application of knowledge, active learning, critical thinking skills, technology integration, and ethical and responsible conduct. Employing ethical hacking pedagogy provides students with practical experience in applying theoretical concepts and knowledge (Hartley, 2015; Lund, 2016). In other words, this method equips students to apply what they have learned effectively. Students develop a deeper grasp of the subject matter by using their understanding of cybersecurity principles in real-world scenarios. This practical application enhances their pedagogical development by bridging the gap between theory and practice, fostering a more comprehensive understanding of the concepts being taught.

It is also argued that ethical hacking pedagogy requires students to analyse complex situations, identify vulnerabilities, and propose practical solutions, thereby developing their critical thinking and problem-solving skills (Al-Tawil, 2024; Nguyen, 2018). Consequently, this process cultivates critical thinking and problem-solving abilities, essential for success in various academic disciplines. Students learn to approach challenges systematically and analytically, improving their ability to evaluate information, make informed decisions, and solve problems creatively.

Furthermore, the findings of the study concluded that ethical hacking pedagogy, which involves the use of advanced technology and tools, empowers students with the ability to integrate technology (Hartley, 2015; Kumar et al., 2024b; Southworth et al., 2023; Ul Haq et al., 2022). Ethical hacking exposes students to various technologies and encourages them to explore and embrace new tools. This technology integration enhances their pedagogical development by equipping them with digital literacy skills, adaptability to technological advancements, and the ability to leverage technology for learning and problem-solving purposes.

The pedagogy of ethical hacking promotes ethical behaviour and responsible conduct in the digital realm. It helps students develop a curiosity for accountable and ethical behaviour by teaching them the importance of obtaining proper authorisation, respecting privacy, and adhering to legal and ethical standards. This focus on ethics and responsibility enhances students' pedagogical development by fostering integrity, ethical reasoning, and professional conduct that can

be applied in various academic and professional contexts. The literature review explores ethical hacking and its implications in technology, specifically its benefits and potential drawbacks. It examines professional development, social interaction, legal practices, cultural development, and pedagogical development in ethical teaching. However, more research is needed to understand the effects of teaching ethical hacking to high school students, particularly concerning their professional, social, legal, cultural, and pedagogical development. Further investigation is necessary to comprehend the impact of ethical hacking education on high school students in these areas.

3. Method

3.1 Design

This study utilised a case study approach to examine the impact of teaching ethical hacking to twelfth graders in a private school. The rationale for selecting this approach is based on the unique context of the study, which differs significantly from other educational settings at the upper secondary school level. The descriptive case study was deemed a suitable design given its focus on understanding and analysing the effects of ethical hacking pedagogy on twelfth graders' conceptions (Yin, 2003). This was achieved through an in-depth exploration of the study context, including interviews with the students as they engaged with the course material.

Three twelfth graders (two females and one male) from a private school in Manama were selected for this study. One female student, identified as S, is 16 years old, while another female student, Z, is also 16. The male student, identified as M, is 17 years old. These students were purposefully chosen due to their completion of the course and ability to provide valuable insights into their experiences with the material (Priya, 2021).

3.2 Interviewing and Piloting Procedures

Data were collected through a series of interviews with twelfth graders. The interviews encouraged open discussions and allowed participants to share their viewpoints and experiences regarding specific aspects and phenomena. Each interview lasted approximately fifteen to twenty minutes. Before conducting the interviews, a set of semi-structured questions was prepared to guide the interview process. The interview protocol included an introduction, instructions for the twelfth graders, and an acknowledgment of their involvement in the study. The protocol consisted of five sections explicitly developed for this study.

Before collecting the data, a pilot study was conducted with one twelfth grader who was not part of the actual data collection for this study. During the pilot interview, a few changes were made to the protocol, including modifying lengthy questions and addressing an interview duration that exceeded the expected twenty minutes. The researchers also observed some discomfort experienced by the participant, leading to the omission of specific items to ensure a shorter and more comfortable interview experience. Following these modifications, the interview protocol items were shared with two teachers who instructed the course to assess their relevance. The majority of the teachers agreed on the appropriateness of the items within the context of the study.

3.3 Data Analysis

All three interviews conducted with the twelfth graders were recorded with their permission. The data analysis process consisted of four stages: data organisation, data comparison, data synthesis, and selection of relevant content.

The interview data were transcribed, and essential information from the twelfth graders' narratives was extracted and saved, along with their respective identifications. The transcriptions were carefully reviewed multiple times to gain an understanding of the perceptions of the twelfth graders. Furthermore, the transcriptions were cross-referenced with the actual interview recordings to ensure the accuracy of the data.

The second phase involved selecting and filtering the data. The meaning of the narratives was examined in depth, and the data were categorised into smaller units based on similarities and differences. Coding was applied to all the data. In the third phase, the data were synthesised into patterns and categorised based on similarities. The researchers attempted to identify patterns and derive themes from the smaller units, considering the relevance of emerging themes.

Finally, conclusions were drawn from the interpretations and meanings derived from the data analysis. This was followed by the report-writing process, which incorporated the themes and findings that emerged from the study. In summary, the data analysis process included transcribing the interviews, selecting relevant data, comparing it with the recordings, categorising the data into smaller units, synthesising patterns and themes, drawing conclusions, and writing the report based on the analysis. Ethical considerations were an essential part of the interview process. Consent from the twelfth graders was obtained before data collection through a consent form provided by the researchers. The researchers ensured they reconfirmed the informants' consent before proceeding with the interviews and assured them they could withdraw at any time. Additionally, the researchers took responsibility for protecting the informants' identities, particularly given potential policy and administration implementation issues. As a result, the informants' identities remained anonymous.

4. Findings and Discussion

When interviewing twelfth-grade students to gather their perspectives on teaching ethical hacking and its potential impacts on their professional, social, legal, cultural, and pedagogical development, they aimed to gain insights into their views. To initiate this exploration, the students were asked five research questions to understand how ethical hacking influenced their practices in these five dimensions. The subsequent discussion provides an overview of their responses to the interview questions.

4.1 Ethical Hacking and Professional Development

While exploring the impact of ethical hacking on informants' professional development, Informant Z expressed that the effects of ethical hacking go beyond cybersecurity alone and influence other professional fields. Her statement clearly demonstrates this:

Learning ethical hacking has been a game-changer for me. It's not just about coding and technical skills; it has taught me problem-solving skills and how to think critically. These skills are applicable in so many professional fields, not just cybersecurity.

The broader applicability of ethical hacking skills extends beyond coding and technical aspects. The focus on problem-solving and critical thinking is highlighted, showcasing the multifaceted benefits of the educational programme. Informant Z elaborated on how ethical hacking has contributed to her professional development by providing specific examples. **"In my other classes, especially maths and science, I approach problems differently. Ethical hacking has trained me to break down complex issues into smaller, manageable parts, which has made me more confident in tackling challenging problems across different** subjects." The mention of increased confidence by informant Z suggests a positive impact of ethical hacking on her overall academic performance.

When we asked the informants whether they had observed any changes in how they worked in teams or communicated with others since they started learning ethical hacking, both informants M and Z clearly stated that taking the ethical hacking subject was a game-changer for their teamwork and communication. They have noticed significant improvements in these areas. Informants M and Z stressed that:

> *Absolutely. In ethical hacking, you often work in teams to solve problems. It has improved my teamwork and communication skills because you must clearly explain your thought process and collaborate effectively to succeed. These skills are crucial in any job, not just the tech or cybersecurity industry.*

The informants highlight the collaborative nature of ethical hacking and emphasise enhancing teamwork and communication skills as major takeaways from taking the subject. The recognition of these skills as applicable beyond the tech industry underscores the versatility of the benefits gained.

Regarding informant M, when asked whether learning ethical hacking in high school influenced his future career aspirations, his evolving viewpoint signals a noteworthy change in his professional ambitions. He openly shared, **"Certainly! Until now, I was uncertain about my career path. However, I am now contemplating a serious venture into cybersecurity. This exposure has shed light on a previously unfamiliar domain, and I can discern the burgeoning demand for these skills in today's job market. The possibilities are inspiring to** *contemplate*." This signifies his growing enthusiasm for cybersecurity and recognition of its potential within the professional sphere.

It is interesting to note a clear shift in the informants' career aspirations, attributing it to the exposure and understanding gained through learning ethical hacking. Their excitement about the possibilities indicates a positive and motivated outlook towards their career paths.

Furthermore, the informants' responses were fascinating when asked about their challenges or concerns in learning ethical hacking and how they overcame them**. "Some of my friends and even my parents were skeptical about the subject. They associated hacking with illegal activities. But they understood better when I explained the ethical part — that it is about securing systems, not breaking into them. It is important to clarify that ethical hacking is about being responsible and using your skills for good reasons,"** *as* informants S & M expressed.

Succinctly, the detailed responses from the three informants offer a comprehensive understanding of the positive effects of teaching ethical hacking on the professional development of high school students. The responses cover various aspects, such as skills development, career aspirations, and addressing misconceptions about ethical hacking. These findings align with research conducted by Brown et al. (2024) and Younis et al. (2019), who concluded that ethical hacking can improve students' technical skills in a professional setting, enhance career opportunities, and expedite the fulfilment of professional prerequisites.

4.2 Ethical Hacking and Learners' Social Interaction

Another key aspect investigated in the study was the impact of ethical hacking on the social interactions of twelfth graders. The study aimed to understand the perspectives of twelfth graders regarding the teaching of ethical hacking.

Informants S & Z strongly believe that learning ethical hacking has uniquely impacted their social circles. **"It's like we have formed a close-knit community within the school that revolves around our shared interest in ethical hacking. We often work together on projects and share resources, strengthening our friendships."** The informants' responses highlight the formation of a close-knit community with shared interests and values, providing clear evidence of improved social connections. The mention of collaboration and resource sharing suggests that the educational programme promotes camaraderie and teamwork.

When asked about the influence of working with classmates as part of an ethical hacking community on their interactions with other students not enrolled in the subject, informant Z emphasised, **"It has been an interesting experience. Some students are curious about what we do, while others may have misconceptions."** She explained that **"ethical hacking involves securing systems and using skills responsibly. *These conversations have opened up, and I have even helped some understand the positive aspects of it."*** Informant Z acknowledges the curiosity of some students and the need to address misconceptions. The educational programme serves as a starting point for conversations, allowing her to educate others about the responsible and positive aspects of ethical hacking.

In addition to the technical aspects, the skills developed through ethical hacking have proven remarkably versatile. As informants M and Z aptly put it, **"The problem-solving and teamwork skills we develop in ethical hacking extend beyond the subject itself."** This broader skill set has had a noticeable impact on their approach to group projects in other classes, promoting a logical problem-solving approach and enhancing their communication abilities. The foundation built through ethical hacking goes beyond its technical domain, providing invaluable benefits in various contexts. Perceptions surrounding hacking often carry negative connotations, leading to misconceptions and scepticism. As informant S shares, "There is sometimes this perception that hacking is always associated with something malicious." However, they have experienced the need to clarify that ethical hacking is focused on responsibility and legality. Patience becomes crucial in addressing these misconceptions, but a shift towards open-mindedness tends to occur once people grasp the positive aspects.

In other words, the willingness to explain the ethical aspect and the positive reception, once people understand, reflects a desire to engage in dialogue and dispel misconceptions, thus emphasising the need for patience. The insights from the informants provide a comprehensive understanding of how teaching ethical hacking impacts social interactions and relationships among high school students. This finding aligns with the 2013 conclusion that equipping students with knowledge of ethical hacking through cybersecurity competitions expands their social interactions. Key aspects include forming a hacking community, influencing interactions with students outside the community, the versatility of skills, and the need to address stereotypes.

4.3 Ethical Hacking and Learners' Legal Practice

When teaching ethical hacking, legal considerations play a crucial role. It is essential to prioritise adherence to legal frameworks and regulations to ensure the responsible and ethical use. This includes obtaining proper authorisation and respecting privacy laws, even when engaging in ethical hacking activities. By emphasising legal compliance, individuals are equipped with the knowledge and awareness necessary to navigate the boundaries set by the law and uphold their moral responsibilities. Informants M and Z clearly express their views on the legal considerations of teaching ethical hacking to twelfth graders when asked to share their opinions.

> *Indeed, legal considerations are vital when teaching ethical hacking. The first thing we learn is the importance of obtaining proper authorisation before attempting any hacking activity, even if it is moral. We are taught to respect privacy laws and to only perform activities within the boundaries set by the law. It emphasizes responsibility and ensures our skills are used legally and ethically.*

The educational programme highlights the importance of responsibility, obtaining legal authorisation, and the ethical use of skills. These aspects cultivate and promote legal measures among learners. These findings align with previous studies conducted by Christen et al. (2023), Dhirani et al. (2023), Ul Haq et al. (2022), and Yaacoub et al. (2023). These studies found that engaging students in ethical hacking provides them with knowledge of legal frameworks, such as computer crime laws, data protection, and intellectual property rights.

In the context of ethical hacking education, strict guidelines and rigorous training on legal and ethical standards are crucial. Informant M, who participated in this training, stressed the importance of these guidelines, stating, **"Our school has strict guidelines in place. Before we even begin practical exercises, we receive comprehensive instruction on legal and ethical standards. Our teachers ensure that we understand the boundaries and are consistently reminded of**

the potential legal consequences if these boundaries are violated. Additionally, our activities are closely monitored, and a clear reporting system is in place if anything exceeds the prescribed limits." The emphasis on monitoring and reporting underscores the commitment to preventing unintended legal issues.

It is worth noting that addressing legal considerations is paramount in teaching ethical hacking. Students often face initial uncertainties, particularly when dealing with real-world scenarios. However, educators are dedicated to providing clarity and guidance in such situations. Open discussions about the legal aspects of each exercise are encouraged, and students are urged to seek assistance promptly if any doubts arise. This approach fosters a dynamic learning environment where legal awareness becomes an essential and indispensable part of the educational process. The emphasis on open discussion and seeking guidance contributes to a learning environment prioritising legal awareness.

There have been instances where we were initially unsure about the legalities, especially when dealing with real-world scenarios. However, the teachers are always ready to clarify any doubts. We engage in open discussions about the legal considerations associated with each exercise, and if there is ever uncertainty, we are encouraged to seek guidance immediately. As Informants S and M explained, this creates a learning environment where legal awareness is integral to the process.

When teaching ethical hacking, it is crucial to understand the legal implications of one's actions. This understanding is a game-changer, transforming individuals into more responsible digital citizens. They become conscious of respecting others' privacy and operating within legal boundaries. The impact of this knowledge extends beyond the classroom, encouraging individuals to apply ethical principles to their everyday digital lives and establish a standard for responsible behaviour in the online realm. Informant Z expressed her lamentation when asked about the influence of legal considerations in ethical hacking on her behaviour outside the classroom.

"It's a game-changer. Understanding the legal implications of our actions makes us more responsible digital citizens. We have become more conscious of respecting others' privacy and ensuring our online activities are within legal boundaries. It's not just about what we learn in class; it's about applying that knowledge to our everyday digital lives and setting a standard for responsible behaviour." This finding is consistent with the conclusions reached in previous studies by Kumar et al. (2024) and Yaacoub et al. (2023). These studies highlight the significance of ethical behaviour and responsible practice within ethical hacking.

Interestingly, as the focus on ethical hacking education expands, discussions regarding the importance of legal considerations have emerged in educational circles. Informant M remarked, **"It's essential. Cybersecurity professionals highly value individuals who possess technical skills and understand their work's legal and ethical aspects. By learning about legal considerations in high school, we're better equipped for future careers and contribute to creating a workforce prioritizing responsible and lawful cybersecurity practices."**

The responses of the three informants emphasise the importance of legal considerations when teaching ethical hacking to twelve graders. This includes obtaining proper authorisation, adhering to privacy laws, providing clear and precise guidelines, implementing monitoring measures, and fostering a responsible digital citizenship mindset. Integrating legal knowledge is crucial for personal growth and preparing students for future careers in cybersecurity.

4.4 Ethical Hacking and Learners' Cultural Development

Teaching ethical hacking has gained recognition for its significant cultural implications. It aims to challenge the conventional stereotypes associating hackers solely with illegal activities. Ethical hacking promotes a culture of responsibility and ethical use of technology. Through ethical hacking, individual students can challenge the negative image often associated with hacking and contribute to a more positive and informed approach to cybersecurity. As informant M stated:

> *Certainly! I believe teaching ethical hacking has significant cultural implications. It's breaking down stereotypes about hackers being solely associated with illegal activities. By learning ethical hacking, we're promoting a culture of responsibility and ethical use of technology. It challenges the negative image often associated with hacking and encourages a more positive and informed approach to cybersecurity.*

It has made us more mindful of our digital actions. We are not just consumers of technology; we are becoming responsible users. There is a collaborative spirit among students to share knowledge and ensure everyone knows the ethical considerations. This fosters a culture of shared responsibility in our digital interactions, both inside and outside the classroom.

Undoubtedly, ethical hacking attracts students from diverse backgrounds and fosters an inclusive learning environment. The students' varied cultural perspectives contribute to a rich tapestry of knowledge and understanding, as they bring their unique problem-solving approaches to the table. This cultural exchange enhances the educational experience and cultivates a more diverse and culturally enriched school community.

Absolutely. Ethical hacking is like a universal language. Students from various cultural backgrounds are drawn to it, bringing diverse perspectives. It promotes inclusivity and understanding as we learn from each other's cultural approaches to problem-solving. It creates a more culturally rich and varied environment within our school community.

Notably, integrating ethical hacking into the school curriculum is widely seen as a progressive step by teachers and the school community. There is a shared belief that technology and cybersecurity transcend cultural boundaries. Teaching ethical hacking helps develop a globally aware and culturally sensitive generation. Teachers appreciate the cultural diversity that arises during discussions and projects on ethical hacking. According to informant S's observation:

> *I have observed that teachers and the school community view it as a progressive step. There is recognition that cultural boundaries do not limit technology and cybersecurity. By teaching ethical hacking, our school contributes to a more globally aware and culturally sensitive generation. Teachers appreciate the cultural diversity that emerges in discussions and projects related to ethical hacking.*

\The inclusion of ethical hacking in educational curricula empowers students to advocate for responsible technology use. By understanding the moral aspects of hacking, students aim to dispel fear and suspicion surrounding this field. They believe this education is pivotal in transforming societal attitudes, fostering a better-informed and supportive environment for ethical practices in technology and cybersecurity. Informant Z passionately expresses:

> *Absolutely. As students, we are becoming advocates for responsible technology use. The more people understand the ethical side of hacking, the less fear and suspicion surrounding it. This education can change societal attitudes, making people more informed and supportive of ethical practices in technology and cybersecurity.*

The students' responses reveal the cultural implications of teaching ethical hacking. Their insights emphasise the need to break stereotypes and to promote responsibility, inclusivity, and global awareness within the school community. The potential for student advocacy to influence broader societal attitudes is also recognised. These findings align with previous research conducted by Nguyen (2018), Yaacoub et al. (2023), Christen et al. (2023), Jumale (2019), Sahare et al. (2014), Ul Haq et al. (2022), Yaacoub et al. (2023), and Parmar et al. (2016). These studies highlight the importance of a collaborative environment that fosters effective communication, teamwork, and intercultural interactions. They also emphasise the positive impact of teaching ethical hacking on students' cultural development, promoting integrity, empathy, respect for diverse cultural values and norms, and nurturing curiosity. Additionally, these studies suggest that teaching ethical hacking contributes to the development of various cultural aspects.

4.5 Ethical Hacking and Learners' Pedagogical Development

Regarding instruction on information security, an ethical hacking approach offers a practical and engaging dimension that extends beyond theoretical learning. By providing hands-on experience in identifying vulnerabilities and securing systems, students can grasp the concepts in a tangible and applicable manner. This practicality is crucial for developing a deep understanding of protecting information in the real world. As informant M enthusiastically states:

> *Certainly! An ethical hacking approach adds a practical and engaging dimension to information security instruction. Instead of just learning theories, we get hands-on experience identifying vulnerabilities and securing systems. It makes the concepts more tangible and applicable, which is crucial for understanding how to protect information in the real world.*

Integrating an ethical hacking approach in cybersecurity education brings vitality to the subject matter. Instead of simply memorising information, students are actively involved in exploration and hands-on learning. This approach transforms the learning process into a dynamic and enjoyable experience, akin to solving puzzles. Unlike traditional methods focusing on theory, ethical hacking lets students see firsthand the immediate effects of security measures and vulnerabilities. This provides a more profound understanding that textbooks alone cannot match. According to informants S and M:

> *The ethical hacking approach brings concepts to life. We're not just memorising information but actively exploring and learning by doing. It's like solving puzzles, which makes it more enjoyable and memorable. Traditional methods might focus more on theory, but ethical hacking allows us to see the immediate impact of security measures and vulnerabilities in a way that textbooks can't replicate.*

Arguably, engaging in ethical hacking activities goes beyond traditional defensive cybersecurity approaches by immersing students in the mindset of potential attackers. This responsible exploration enables students to understand cybersecurity issues comprehensively from defensive and offensive perspectives. By thinking like hackers responsibly, students gain valuable insights that help them anticipate and address security challenges more effectively. As informant Z aptly describes it:

> *Ethical hacking activities make us think like hackers in a responsible way. We're not just learning how to defend; we understand the mindset of potential attackers. It provides a holistic view of cybersecurity issues from both defensive and offensive perspectives. This depth of understanding helps us anticipate and address security challenges more effectively.*

Engaging in practical activities that simulate real-world scenarios is crucial to cybersecurity education. These activities offer valuable hands-on experience and have a lasting impact on students' awareness and behaviour. One effective activity involves simulating a phishing attack, which exposes students to the deceptive tactics used by cybercriminals. This experience teaches them how to identify phishing attempts and instills a sense of caution about sharing personal information online. The lessons learned from these activities extend beyond the classroom and shape students' online behaviour in the future. As recounted by informant S:

> *Indeed, in one activity, we simulated a phishing attack. Seeing how easily someone could fall for a seemingly harmless email was eye-opening. The activity taught us how to recognise phishing attempts and made us more cautious about the information we share online. It's a lesson that stays with you beyond the classroom.*

In cybersecurity, ethical hacking has emerged as a game-changer for individuals aspiring to pursue careers in this dynamic industry. Through ethical hacking, students acquire practical skills and develop a mindset that employers highly value. This approach goes beyond theoretical knowledge and equips students with the readiness to tackle real-world challenges. By the time they enter the workforce, these students have already gained invaluable experience in identifying and mitigating security threats. Informant M passionately expresses:

> *It is a game-changer for those considering careers in cybersecurity. Ethical hacking gives us a head start by providing practical skills and a highly valued mindset in the industry. It's not just about theoretical knowledge; it's about being prepared to face real-world challenges. By the time we enter the workforce, we will have already gained experience in identifying and mitigating security threats.*

The students' responses provide valuable insights into how an ethical hacking pedagogical approach enhances information security instruction for high school students. The hands-on and practical nature of this approach, combined with its high engagement factor, fosters the development of a responsible hacker mindset and promotes real-world applicability. Collectively, these factors contribute to a deeper understanding of cybersecurity issues and better prepare students for future careers. These findings align with research conducted by Hartley (2015) and Lund (2016), who concluded that ethical hacking pedagogy equips students with the practical application of theoretical concepts and knowledge. Additionally, studies by Al-Tawil (2024) and Nguyen (2018) found that ethical hacking pedagogy develops students' critical thinking and problem-solving skills. Furthermore, research conducted by Hartley (2015), Kumar et al. (2024), Southworth et al. (2023), and Ul Haq et al. (2022) concluded that ethical hacking pedagogy empowers students with technological abilities.

5. Conclusions

Based on the study results, significant conclusions were drawn regarding the five dimensions associated with ethical hacking. First, in terms of professional development, students reported that learning ethical hacking expanded their problem-solving and critical-thinking skills, which are transferable to various fields beyond cybersecurity. They observed substantial improvements in confidence, ability to tackle complex problems across diverse subjects, and enhanced teamwork and communication skills. This positively impacted their academic performance and reshaped their perspectives on future career aspirations, particularly towards cybersecurity.

Second, regarding social interaction, responses revealed that ethical hacking education fostered a sense of community and collaboration among students, enhancing their social bonds and interactions. It encouraged openness in addressing misconceptions about hacking and prompted students to become responsible advocates for ethical practices in technology. As a result, it broadened their social interactions and cultivated a culture of shared responsibility in digital engagements.

Third, in legal practice, students emphasised the importance of legal adherence, acknowledging that ethical hacking instruction underscored the necessity of operating within legal frameworks. The educational focus on obtaining proper authorisation and respecting privacy laws prepares students for future cybersecurity careers and instills a mindset of lawful and responsible digital citizenship.

Fourth, in relation to cultural development, ethical hacking was portrayed as instrumental in challenging negative stereotypes associated with hacking. It promoted cultural inclusivity and fostered a diverse and collaborative environment. Students embraced the role of advocates, seeking to reshape societal attitudes towards ethical hacking and contributing to a more globally aware and accepting school community.

Lastly, regarding pedagogical development, the ethical hacking pedagogical approach was seen as an emerging need due to its emphasis on practical and tangible learning experiences, going beyond theory to engage students actively in the

material. This hands-on approach gave students a valuable perspective on effectively addressing cybersecurity challenges, fostering a responsible hacker mindset valued in the industry, and preparing them for real-world applications.

6. Implications of the Findings for High Schools

High schools should consider incorporating ethical hacking into their curricula to bolster problem-solving, critical thinking, teamwork, and communication skills, preparing students for various professional fields. This integration can also enhance guidance for cybersecurity career paths and promote a responsible approach to technology use.

To address potential misconceptions, educators play a key role in clarifying the ethical aspects of hacking, thus promoting digital citizenship. Ethical hacking courses have also been shown to enrich social dynamics among students, create a sense of community, and raise legal and cultural awareness. Teachers can inject pedagogical innovation into the classroom by emphasising hands-on, active learning through ethical hacking, fostering a mindset that prepares students for real-world challenges. Educators may require further training to teach this content effectively and navigate the complex moral, legal, and cultural discussions it entails.

Administrative policy and community engagement are also critical, ensuring that ethical hacking is taught safely and openly, aligning with legal standards, and promoting a wider societal understanding of its merits. Ultimately, ethical hacking education can equip students with future-proof skills for the evolving technological landscape.

6.1 Limitations and Future Research Directions

Although the findings have significantly contributed to our understanding of ethical hacking pedagogy at the secondary school level, an area that has received limited research attention, the study has some limitations.

First, the sample size and diversity: The study drew from a small and specific population limited to three twelfth graders from a single private school. This sample size may not reflect the varied experiences, regional educational policy influences, and cultural backgrounds that might affect the generalisability of the findings. As such, future studies could include a broader range of participants from different educational settings, cultural backgrounds, and varied age groups to explore the impacts of ethical hacking education in the wider context.

Second, the limited scope of the literature review: Although it is thorough, it appears to focus predominantly on positive viewpoints, which may overlook the breadth of critical perspectives or studies reporting adverse effects of ethical hacking education. As such, future studies should incorporate comparative studies across different legal and cultural landscapes that can provide greater insight into the diversity of ethical hacking impacts globally.

Third, the case study method: While the case study method provides depth, it lacks breadth, and the findings might not be generalised to other educational settings where ethical, legal, social, and cultural norms may differ. Considering this, employing quantitative methodologies to triangulate qualitative research findings may be beneficial, including performance metrics, standardised testing, or statistical analysis of broader data sets.

Finally, subjectivity in self-reporting: Dependence on self-reported student data may introduce bias, as the informants might provide socially desirable responses or be influenced by their personal aspirations. Therefore, future studies should investigate the perspectives of educators who teach ethical hacking, which could offer additional insights into the pedagogical and moral challenges.

Acknowledgments

The research team expressed their heartfelt gratitude to all individuals who facilitated data collection from the informants.

Authors contributions

Not applicable.

Funding

Not applicable.

Competing interests

Not applicable.

Informed consent

Obtained.

Ethics approval

The Publication Ethics Committee of the Redfame Publishing.

The journal's policies adhere to the Core Practices that the Committee on Publication Ethics (COPE) established.

Provenance and peer review

Not commissioned; externally double-blind peer reviewed.

Data availability statement

The data supporting this study's findings are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

Data sharing statement

No additional data are available.

References

Abu-Shaqra, B. (2021). *Ethical hacking sociotechnology: A sociotechnical assessment of ethical hacking teaching practices in Canadian higher education*. https://doi.org/10.13140/RG.2.2.14630.04161

Al-Tawil, T. N. (2024). Ethical implications for teaching students to hack to combat cybercrime and money laundering. *Journal of Money Laundering Control*, *27*(1), 21-33. https://doi.org/10.1108/JMLC-01-2023-0014

Brogdon, M. (2021). Ethical hacking. In *culture, society, and praxis* (Vol. 13, Issue 2). https://digitalcommons.csumb.edu/cspAvailableat:https://digitalcommons.csumb.edu/csp/vol13/iss2/4

Brown, N., Xie, B., Sarder, E., Fiesler, C., & Wiese, E. S. (2024). Teaching ethics in computing: A systematic literature review of ACM computer science education publications. *ACM Transactions on Computing Education*, *24*(1), 1-36. https://doi.org/10.1145/3634685

Christen, M., Gordijn, B., & Loi, M. (2023). The ethics of cybersecurity. *The International Library of Ethics, Law and Technology, 21*. https://doi.org/10.21428/cb6ab371.d27262ff

Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., & Newe, T. (2023). Ethical dilemmas and privacy issues in emerging technologies: A review. *Sensors*, *23*(3), 1151. https://doi.org/10.3390/s23031151

Hagendorff, T. (2020). The Ethics of AI ethics: An evaluation of guidelines. *Minds and Machines*, *30*(1), 99-120. https://doi.org/10.1007/s11023-020-09517-8

Hartley, R. D. (2015). Ethical hacking pedagogy: An analysis and overview of teaching students to hack. *Journal of International Technology and Information Management*, *24*(4). https://doi.org/10.58729/1941-6679.1055

Hurst, B., Wallace, R., & Nixon, S. B. (2013). The impact of social interaction on student learning. *Reading Horizons: A Journal of Literacy and Language Arts*, *52*(4). https://scholarworks.wmich.edu/reading_horizons

James R. Rest. (1986). *Moral development: Advances in research and theory*. Praeger.

Jumale, P. P. (2019). Impact of ethical hacking on business and governments. *International Research Journal of Engineering and Technology*. www.irjet.net

Kasim, M., Saidu, M. B., Isa, A., & Utulu, S. C. A. (2022). A proposal for a social ethical hacking framework for detecting and managing human-induced vulnerabilities in organizational cybersecurity. *UK Academy for Information Systems Conference Proceedings*.

Khan, N., Liaqat, I., & Islam, A. (2024). Impact of social media on the development of youth personality: a case study of district Attock, Punjab, Pakistan. *Nobel Institute for New Generation*, *3*(1), 1-18.

Kumar, J. R. R., Bhalke, D. G., Nikam, S., Chobe, S., Khidse, S., & Kale, K. (2024a). Evaluation of the extent and demanding roles of ethical hacking in cybersecurity. *Journal of Autonomous Intelligence*, *7*(1). https://doi.org/10.32629/jai.v7i1.1246

Kumawat, V., Pal, P., & Jha, P. (2021). Ethical hacking: white hat hackers. *Computing & Intelligent Systems*. https://doi.org/10.52458/978

Lund, L. (2016). How teachers reflect on their pedagogy: learning from teachers' pedagogical vocabulary. *Journal of the International Society for Teacher Education*, *20*(2), 22-35.

Mooney Simmie, G., O'Meara, N., Forster, A., Ryan, V., & Ryan, T. (2023). Towards a model of teachers' continuing professional development (CPD): A border crossing journey with embedded contradictions, ethical dilemmas and transformative possibilities. *Professional Development in Education*. https://doi.org/10.1080/19415257.2023.2283420

Ng, W. (2012). Can we teach digital natives' digital literacy? *Computers & Education*, *59*(3), 1065-1078. https://doi.org/10.1016/j.compedu.2012.04.016

Nguyen, T. (2018). *Certified ethical hacker v.10 online self-study course: A case study*. https://doi.org/10.1145/3306500.3306547

Novawan, A., Ikeda, O., & Walker, S. A. (2024). The new face of technology-enhanced language learning (TELL) with artificial intelligence (AI): Teacher perspectives, practices, and challenges. *Journal of English in Academic and Professional Communication JEAPCO*, *10*(1). https://doi.org/10.25047/jeapco.v10i1.4565

Nyaaba, M., & zhai, X. (2024). Generative AI professional development needs for teacher educators. *Journal of AI*, *8*(1), 1–13. https://doi.org/10.61969/jai.1385915

Parmar, B. L., Kelly, D. C., Mclean, C., Mehta, N., & Stevens, D. B. (2016). *Ethics and trust in the investment profession*. https://doi.org/10.2469/ccb.v2013.n14.1.(2016)

Pike, R. E. (2013). The "ethics" of teaching ethical hacking. *Journal of International Technology and Information Management* (Vol. 22). https://doi.org/10.58729/1941-6679.1021

Priya, A. (2021). Case study methodology of qualitative research: Key attributes and navigating the conundrums in its application. *Sociological Bulletin*, *70*(1), 94-110. https://doi.org/10.1177/0038022920970318

Quasim, M. T., Naser, A., Hawi, A., Meraj, M., & Nasser, A. (2023). *System penetration: Concepts, attack methods, and defense strategies*. EasyChair Preprint.

Roos, H., & Bagger, A. (2024). Ethical dilemmas and professional judgment as a pathway to inclusion and equity in mathematics teaching. *ZDM – Mathematics Education*. https://doi.org/10.1007/s11858-023-01540-0

Sahare, B., Naik, A., & Khandey, S. (2014). Study of ethical hacking. *International Journal of Computer Science Trends and Technology*, *2*(6). www.ijcstjournal.org

Smith, L. A., Chowdhury, M., & Latif, S. (2022). Ethical hacking: skills to fight cybersecurity threats. *EPiC Series in Computing*, *82*. https://doi.org/10.29007/vwww

Southworth, J., Migliaccio, K., Glover, J., Glover, J. N., Reed, D., McCarty, C., … & Thomas, A. (2023). Developing a model for AI Across the curriculum: Transforming the higher education landscape via innovation in AI literacy. *Computers and Education: Artificial Intelligence*, *4*. https://doi.org/10.1016/j.caeai.2023.100127

Srivatanakul, T., & Annansingh, F. (2022). Incorporating active learning activities to the design and development of an undergraduate software and web security course. *Journal of Computers in Education*, *9*(1), 25-50. https://doi.org/10.1007/s40692-021-00194-9

Trabelsi, Z., & Ibrahim, W. (2013). Teaching ethical hacking in information security curriculum: A case study. *IEEE Global Engineering Education Conference, EDUCON*, 130-137. https://doi.org/10.1109/EduCon.2013.6530097

Ul Haq, H. B., Hassan, M. Z., Hussain, M. Z., Khan, R. A., Nawaz, S., Khokhar, H. R., & Arshad, M. (2022a). The impacts of ethical hacking and its security mechanisms. *Pakistan Journal of Engineering and Technology*, *5*(4), 29-35. https://doi.org/10.51846/vol5iss4pp29-35

Vygotsky, L. S. (1978). *Mind in society: The development of higher psychological processes*. Harvard University Press.

Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2023a). Ethical hacking for IoT: Security issues, challenges, solutions and recommendations. *Internet of Things and Cyber-Physical Systems*, *3*, 280-308. https://doi.org/10.1016/j.iotcps.2023.04.002

Yaacoub, J.-P. A., Noura, H. N., Salman, O., & Chehab, A. (2021). A survey on ethical hacking: issues and challenges. *Computer Science Cryptography, and Security*.

Yin, R. K. (2003). *Applications of case study research.* USA: Sage Publications Inc.

Younis, A. Y., Kifayat, K., Topham, L., Shi, Q., & Askwith, B. (2019). Teaching ethical hacking: Evaluating students' levels of achievements and motivations. *International Conference on Technical Sciences (ICST2019)*.