Online Journal of Communication and Media Technologies, 2023, **13**(2), e202312
e-ISSN: 1986-3497

OPEN ACCESS

Research Article

Cybersecurity awareness factors among adolescents in Jordan: Mediation effect of cyber scale and personal factors

Anas Mohammad Ramadan AlSobeh [1,2,3*]
0000-0002-1506-7924

Iyad AlAzzam [1]
0000-0001-7539-0822

Amani Mohammad Jomah Shatnawi [1]
0000-0002-5096-9405

Iman Khasawneh [1]
0000-0002-0457-1666

[1] Department of Information Systems, Faculty of Information Technology and Computer Science, Yarmouk University, Irbid, JORDAN
[2] College of Information Technology, Kingdom University, Riffa, BAHRAIN
[3] School of Computing, Southern Illinois University, Carbondale, IL, USA
[*] Corresponding author: anas.alsobeh@yu.edu.jo

Citation: AlSobeh, A. M. R., AlAzzam, I., Shatnawi, A. M. J., & Khasawneh, I. (2023). Cybersecurity awareness factors among adolescents in Jordan: Mediation effect of cyber scale and personal factors. *Online Journal of Communication and Media Technologies, 13*(2), e202312. https://doi.org/10.30935/ojcmt/12942

ARTICLE INFO

Received: 18 Oct 2022
Accepted: 29 Dec 2022

ABSTRACT

Cybersecurity for Jordanians' adolescents/teens has become a complicated phenomenon representing complex socio-technical concerns for the personalities of adolescents in Jordanian society. Recent cyberattacks have had a significant impact on teens in Jordan, both personally and in terms of their quality of life. As such, it is important to develop strategies to increase cybersecurity awareness among teens in Jordan. This research was conducted in both planned and random areas in Jordan, with the aim of understanding the differences in risk-aware cultures and teens' opinions and activities after introducing cybersecurity awareness in cyberspace. The study was based on 400 responses, and numerous statistical analyses were applied to the responses from each area, including the validity and reliability test, feasibility test of a variable, correlation test, and carried out using SPSS. Moreover, multiple coefficients of determination, hypothesis testing and partial statistical tests were carried out. The research hypotheses indicate that there is a mediation effect of the cyber scale and personal factors (planned/random) with a 76% acceptance rate. This suggests that understanding the significant association between the cyber scale and the quality-of-life scale is important, and that effective cyber-risk management is critical to realizing the importance of cybersecurity awareness. As such, it is recommended that national cybersecurity programs be launched in all sectors in Jordan. Overall, this research highlights the importance of increasing cybersecurity awareness among teens in Jordan. It is essential that teens are educated on the risks associated with cyberattacks, and that effective strategies are developed to protect them from such attacks. By doing so, teens in Jordan can be better equipped to protect themselves and their society from the dangers of cyberattacks.

Keywords: cybersecurity, awareness, SPSS, adolescent, teens, Jordan, quality-of-life factors, personal factors

INTRODUCTION

The development, multiplication, and openness of the web, interaction, and smartphone innovations have created openings for teenagers of all ages to engage in online transactions; this can be done by progressively creating advanced information, which is ordinarily put away on servers (cloud) remotely. To protect the

information and help diminish the number of conceivable cybercrimes that start from illicit online activities, those endowed with significant data, for instance financial information. Jordan isn't separated this fast developing; information and communication technology (ICT) is right now encountering exceptionally quick development with such vulnerabilities due to the fast world of innovation that led to the raise of various forms of the internet issues between teenagers (Brewer et al., 2018; Salgado et al., 2014). Cybersecurity awareness has become an integral part of our Jordanian society. The primary motivation is the cyber criminals seems to be the increased among teens in Jordan, such as acquiring sensitive information and using it for blackmail. Hackers may also benefit from behaviors of teens on social networks (e.g., Facebook, TikTok, Instagram, YouTube, Twitter, Discord, etc.), so it becomes a primary source of exposing their information to a variety of security risks. Jordanian teen and youth between the ages of 13 and 35 make up the largest segment of social media users. Around 6.3 million Jordanians are social media users, most to the point of addiction weekly and monthly (Abu-Saad, 2022; Durkee et al., 2012; Waldo, 2014). This is heavy dependence on social media has led to some emerging and raising cybercrimes, such as attacks, viruses, worms, misinformation, and theft identity (Al Sayed & Al-Beheiry, 2020). Due to in COVID-19 pandemic, teens use the internet more than usual as education was converted to distance and online, therefore, they spent a lot of time on the internet without parent's controls. The cybersecurity has a significant impact on the Jordanian personality of the adolescent considering teens using the internet to the same extent, and in similar ways, as adults. Moreover, they also often engage in risky behaviors such as downloading illegal copies of movies, music, files, applications, and images.

In accordance with the national cyber security strategy 2018-2023, the Jordanian government seeks to provide "an effective and long-term commitment from the government, the private sector and citizens with basic cyber hygiene being relevant to boardroom and home alike. Education is critical to this understanding and academia has an important role to play in equipping Jordanians to keep themselves safe online and to ensure that we have the right people with the right skills protecting our national security and prosperity from those who would seek to do us harm" (MICT, 2018).

The National Cybersecurity Initiative (NCI) was established in 2008 by former President George W. Bush in order to provide increased protection of the country's critical infrastructure. This initiative is composed of twelve distinct goals which prioritize the security of networks, the development of a public-private partnership, and efforts to raise public awareness of cyber threats (U.S. Computer Emergency Readiness Team). Since then, many agencies and departments within the government have adopted cyber security policies and frameworks in order to ensure the protection of all government systems (American Bar Association). These efforts have allowed the government to stay ahead of rapidly evolving cyber threats, such as ransomware or phishing attacks (CISA, 2020). Ultimately, NCI is an essential step in lessening the potential damage that can occur from cyber-attacks. National Cyber Security Center works to legalize cyber security in Jordan, including developing national cyber security capabilities to ensure that threats to Jordan's systems and infrastructure are confronted, and creating a secure environment. Therefore, Jordan needs a holistic monitoring policy for the national cyberspace, as there is a need to find a management plan that implements an assessment of the user's information security conditions while raising the level of common and complete national security for individuals, and creating capabilities, hindering, observing, cautioning, and reacting to cybersecurity occurrences and controlling their destruction.

Cybersecurity awareness has received inadequate interest as a result of the rapid increase in cybercrimes in Jordan, especially as the internet and electronic devices become more available and affordable which has led to increase the number of teens turning to technology. The definition of the problem that can be settled is what is the esteem of the completeness and development of data security mindfulness in Jordan. Since hacking attacks of data systems in different technologies and platforms (e-games, social networks, mobile applications, etc.) are becoming more widespread in Jordan among teens, they must understand the implications and issues of cybersecurity. There is a pressing need to design a comprehensive national program to raise awareness of the consequences of personal information loss, which may undermine their confidentiality and privacy. A main role in providing the information security to teens is their ability to recognize the content threats and how to protect personal information in the network. The study investigates the factors that influence Internet use among adolescents in Jordan under the supervision and approval of their parents, especially those aged 16 to 19 years old, with the assurance of saving the data confidentially.

The Significance and Hypotheses

The significance of this research comes from the importance of cyber-psychology and its impact on the personality style of the adolescent. In Jordan, adolescents are the most category of users of the internet that reach the stage of addiction to it, as the use of the internet leads adolescents to move towards social isolation, by doing excessive use of the internet and this isolation generates alienation from reality and leads to sits evasion from their real responsibilities towards themselves and towards their community, where using social networking websites and microblogging platforms wherein people build online groups to exchange information, thoughts, or private messages (Tariq, 2021; Wasiński & Tomczyk, 2015).

The research conducted to evaluate the teens' cybersecurity understanding and exercises was a very important step in understanding the current state of cybersecurity among teens. The research was conducted in Irbid, Jordan, and focused on the most common security vulnerabilities that teens face when using applications. The research addressed a cybersecurity awareness assessment, which was conducted with teens from schools in planned and random areas of Irbid based on quality-of-life and major personality factors, such as repeating password security, browser security, and social media; An investigation was conducted to assess the teens' level of awareness of security issues, particularly cyber anxiety, cyber behavior, social relation, isolation, food (eating disorder), educational mismatch, and cyber-attacks. The data was collected through survey questionnaires, and based on the responses, the results of the statistical analysis were estimated.

By studying the quality-of-life scale and key personality features, new traits are discovered in order to investigate the connection between cyberspace and the doles (Alobedi & Saeed, 2021). Teenagers frequently deal with information security challenges like phishing, technical problems, and communication dangers. At the same time, the possibility of encountering the online risks is strongly influenced by the low level of digital competence in areas such as orientation in various information sources, the search for necessary digital content and assessment of its quality, knowledge of personal data protection techniques. Fraud and hacking in this environment do occur more likely by social engineering, one-sided transactions and stealing identity. Moreover, adolescents often underestimate the negative consequences of reckless online behavior in their future lives.

Cybersecurity in Jordan is a major concern, as the country is increasingly becoming a target for data penetration and successful attacks. To address this issue, we conducted a research to design a solution that provides a cyber security awareness plan based on a security analysis of the quality-of-life scale, and key personal factors for Jordanian adolescents. The result of this research is an evaluation or reference to improve cyber security awareness and management aimed at forming digital competencies for adolescents, which allows them to move freely in the modern information environment and be critical towards digital content and use appropriate methods of information protection.

We believe that understanding the level of digital competence of adolescent is an opportunity for high school to analyze security shortcomings and prepare adequate methods to improve them. To this end, we have developed a comprehensive cyber security awareness plan that includes the following components:

1. **Education and training:** We believe that education and training are essential components of any cyber security awareness plan. We have developed a comprehensive curriculum that covers topics such as cyber security basics, online safety, data protection, and digital literacy. The curriculum is designed to be interactive and engaging and is tailored to the needs of Jordanian adolescents.
2. **Awareness campaigns:** We have developed a series of awareness campaigns that are designed to raise awareness about cyber security among Jordanian adolescents. These campaigns include posters, videos, and other materials that are designed to educate adolescents about the importance of cyber security and the risks associated with it.
3. **Monitoring and evaluation:** We have developed a monitoring and evaluation system that is designed to track the progress of the cyber security awareness plan. This system will allow us to measure the effectiveness of the plan and make necessary adjustments as needed.

We believe that this comprehensive cyber security awareness plan will help Jordanian adolescents to become more aware of the risks associated with the digital world and to develop the necessary skills to protect

themselves from cyber threats. We are confident that this plan will help to improve the overall security of Jordan and to ensure that Jordanian adolescents are able to move freely in the modern information environment.

The security component is planned to survey participants' understanding of the security of the social media applications and browsers they frequently utilize. Finally, the cybersecurity blog examined participants' understanding of the dangers of utilizing different social networking platforms and how to respond to the occurrence of cybercrime. As a result, we investigated participants' cybersecurity awareness, quality of life factors, and self-perceptions. These questions were distributed to the participants and a total of 400 answers were received from each area.

In order to better understand the effects of different types of attacks on the level of cybersecurity awareness among adolescents in Jordan, the authors should have tailored their questions and hypotheses to focus on specific types of attacks. To be more specific in our questions and hypotheses in order to better understand the effects of different types of attacks on the level of cybersecurity awareness among adolescents in Jordan. Each type of attack has different characteristics and requires different levels of awareness to be effectively defended against. For example, social engineering attacks rely heavily on psychological manipulation and require a high level of awareness in order to be identified and avoided. Phishing attacks, on the other hand, rely on deception and require a different type of awareness in order to be identified and avoided. Therefore, the responses were again categorized according to hypothesis and analysis. Here are the main research questions:

RQ1: What is the effect of the main personality factors of adolescents on the level of cybersecurity awareness in Jordan when it comes to social engineering attacks?

H1: Personal factors have a positive impact on the level of cybersecurity awareness among adolescents in Jordan when it comes to social engineering attacks.

RQ2: What is the impact of quality-of-life factors for adolescents in Jordan on the level of cybersecurity awareness when it comes to phishing attacks?

H2: The quality-of-life factors have a positive impact on the level of cybersecurity awareness among adolescents in Jordan when it comes to phishing attacks.

To analysis these questions and prove hypotheses, we investigated through the study the influence of cybersecurity awareness and the most important of them on the personal issues of adolescents with different quality of life; a statistically significant correlation between the cyber scale and the key personality factors scale; and a statistically substantial correlation among the cyber scale and quality of life. Intrinsically, creating a cybersecurity mindfulness linked to realizing internet protection actions in high schools. This leads to a critical ought to actualize a common approach to make strides cybersecurity mindfulness between teens understudies, increment their knowledge of cyber concerns, and teach them methods to secure their accounts from possible attacks.

LITERATURE REVIEW

Cybersecurity Awareness: Jordanian Adolescents

In many recent Jordanian and foreign studies, it justified, the need to have cybersecurity competencies, related to the search for information, its processing and systematization, skills of virtual self-presentation, and digital environment threats understanding. Awareness of cybersecurity among adolescents is still being investigated to enhance identify their attitudes, knowledge, behavior and further pertinent influencing factors. Jordanian adolescents are the most vulnerable group in terms of information security, since communication is their main activity, and with the high availability of tools in the internet environment, this led to the formation of internet addiction and many other negative effects. It was strong-minded that the main badly-behaved with cybersecurity awareness In Jordan is not only a lack of cybersecurity awareness, but rather lies in the way teens apply that knowledge in real-world situations, therefore, information and security is one of the components of the system, which is an individual's protection (subject, psyche, and consciousness) from negative information and psychological influences (Prasad et al., 2019). Cybersecurity is associated to cyber threats that might impact adolescents and the countermeasures to support them.

Adolescent security and confidentiality have long been a point for investigators in the children's and teen's computer interaction research community (Mohammad et al., 2022; Walsh et al., 2022). The theory of the information society "post-industrial society" was developed in 1973, where there is an impact of technological relations newly in modern society and social relations, differently. The community awareness was explanted considering these changes and effects of electronics achievements and its social consequences (Hatfield, 2018; Kumari & Verma, 2015). The author referred to the transition from goods to a service community, and takes it that theoretical knowledge is a central resource for society which produces innovations in technology and the emergence of a new "intellectual technology", where he sees that the information society distances are the direct influence which is one of the usual frameworks of practical life, and when people learn to live with each other a new situation arises influenced by factors that help in these relationships known as the new technological revolution where he sees the computer as a symbol and material embodiment of the modern technological (El Nadir, 2021). The theory has been reviewed in order to clarify the extent to which society has been affected by this era and transformed into electronic in the majority of them of which is social such as (connection, communication and acquaintance) and of which is material, such as (sales and purchases, banking, govern mental and administrative, transactions different). This theory is also used to understand the relationship of society with a cybersecurity perspective in this era being a new type of security linked to the current information society.

In Jordan, cybersecurity is an increasingly important topic in our modern digital world, but it is often overlooked or taken for granted by many individuals and organizations. The purpose of this essay is to explore the various pathways to developing greater cybersecurity awareness as well as the protection behaviors that may be needed to help prevent cyber threats. By analyzing and examining these pathways, we can better understand the critical steps for enabling better cybersecurity for ourselves and for our organizations. Lee and Kim (2022) presented a cybersecurity is a growing concern in the modern world, and its importance is particularly evident in South Korea. With a technology-dependent population, South Korea is especially prone to cybersecurity breaches and cyber-attacks, making it necessary to promote awareness of cybersecurity threats and protective behaviors. In this essay, I will provide an overview of the pathways to successful cybersecurity awareness and protection behaviors in South Korea. Specifically, I will provide an analysis of the best practices for companies and private citizens, as well as the challenges South Korea faces in creating a safe and secure cyberspace. By looking at recent policies and initiatives implemented in South Korea, this essay aims to provide insight into the most effective approaches for securing the nation's digital environment (Lee & Kim, 2022).

Cybersecurity Awareness: Social Engineering and Awareness Framework

Social engineering is the silent attacker that is usually overlooked every day. Cybercriminals use more "old school" brute force methods to gain access. In today's cyberwars, it's not just about how someone accesses a router, switch, server, or website; however, how did they manage to make a simple phone call and act as a legitimate representative of the company to get information from the victim (Hatfield, 2018). In a social engineering attack, the hackers take advantage of individual interaction (social skills) to acquire or cooperate knowledge about an organization or its computer systems. The hackers may appear modest and respectful and may pretend to be a new member of staff, reformer, or scholar, and even display credentials to support that identity (Hatfield, 2018). Most common social engineering techniques such as, phishing, familiarity, exploiting human greed, exploiting human curiosity, dumpster diving, hoaxing, reverse social engineering, and more. The number of Jordanian accounts on five major social networks is estimated at about seven million, 61% of which are Facebook accounts, with this huge number of Jordanian social networking accounts, we need to raise awareness about social engineering attacks, especially with the various age groups that use these accounts and the different of security background of users. The rumors on social media what ramifications there might be to spreading false rumors and whether social media might be used by companies to spread rumors about competitors or even many people open accounts on social media sites with celebrity names and exploit them to abuse them and publish comments or tweets under criticism for the purpose of defamation (Corron, 2018), electronic crimes law in Jordan contain set of the provisions to such these crimes in addition to financial fines (Irtaimeh, 2020; Kumari & Verma, 2015). Al-Tajer and Ikuesan (2022) presented a framework for a series of steps to provide effective K12 education approaches in Qatar. They applied the

approach of creating a functional operational framework consisting of four stages: identifying threats and attacks, discovering current awareness, creating an awareness approach, and evaluating an awareness approach. One of the highlights was specifically for the K-12 age group, which promotes cybersecurity emojis. Consequently, by exploring this approach, the security community can enroll and entice adolescents into cybersecurity and raise the degree of security awareness (Al-Tajer et al., 2022).

Hamdi (2022) conducted a systematic literature review on cybersecurity awareness in Saudi Arabia. He found that a majority of previous studies focused on the awareness and knowledge of individuals, such as students and employees, about cybersecurity issues and practices. This highlights the need for increased awareness and education about cybersecurity among the general public and organizations in Saudi Arabia. Hamdi identified several challenges in improving cybersecurity awareness in Saudi Arabia, including a lack of regulations and laws, inadequate awareness and education programs, and a lack of cooperation between the government and private sector. He suggests that future research should focus on developing and evaluating targeted awareness and education programs for specific groups, such as small and medium-sized enterprises, and developing methods to measure the impact of these programs on cybersecurity awareness. (Hamdi, 2022).

The lose control is insufficiency of auto reactivity has been hypothesized to explain how it transforms internet activities saturated into habits and sometimes to potentially harmful consequences, deficiencies in self-reactive influence refers to behaviors that lacks control as the practical measures of the variable indicate. For example, I tried to reduce the time spent on the Internet, until individuals had tried to modify their behavior without success. For example, the scale was associated with compulsive internet use "(How many times have you tried in vain to take time less online? How often do you find it difficult to stop using the Internet when you are connected to it?)" (Leung, 2004). Al-Lassameh and Al Majali (2022) discussed the role of faculty members in Jordanian universities in raising awareness of cybersecurity among their students. The authors centered on the threats and consequences of cyberbullying; "The first includes electronic harassment, defamation, impersonation, masquerading, outing, deception, ostracism, and exclusion. They propose a set of educational ideas to prevent or reduce the likelihood and impact of different types of cybersecurity threats, and finally suggest strategies to prevent such threats and their impacts" (Al-Lassameh & Al Majali, 2022).

The quality of life factors according to the psychoanalytic school which holds that the individual lives in a series of conflicts to satisfy his needs, including the need for security, the need for self-affirmation, and the need for self-confidence and emotional satiation, and there-fore it resorts to addiction, including Internet addiction and sitting for hours long in front of it, as he lives a virtual life far from reality to compensate for the feeling of security and belonging and to escape from problems, as the individual can say or do what he wants, making it an opportunity for him to express in it from his inclinations and satisfies his desires from the need for love and appreciation, he immerses himself in his virtual world the theoretical basis provided by the theory of socio-cultural orientation, in which it emphasized that a psychological disorder can only be explained when one considers its cultural and social environment and that mental disorders vary according to gender, age, social class and background, and they see that the reason for abnormal behavior is not in terms of the human soul, but rather in community terms (El Nadir, 2021; Al Shamsi, 2019; Luciana, 2010).

DeSmet conducted a review concerning the electronic games (e-games) for utilize by children and recognized threats to which they are exposed. The author revealed the influence of e-games on children and adolescents from 9-19 years old in cyberspace and he demonstrated the positive and negative effects of e-games on children and adolescents. The most important characteristics of e-games are fun and excitement, a self- educational entertainment method (DeSmet. 2015). On the other side, e-games cause excessive addiction to play, the acquisition of bad habits and the formation of a distorted culture, weakness academic achievement, homework neglect, and social isolation due to solo play and social tension (Liaropoulos, 2013; Subrahmanyam et al., 2001). de Paula Albuquerque et al. (2020) investigated 26 studies on the privacy threats to teenagers associated with intelligent e-gaming. The authors focused on technical and domain-specific risks. The authors reported the three most common privacy risks in smart games: use, retention, and limiting disclosure; consent and selection; transparency, and warning. Furthermore, the authors proposed technical and domain-specific resolutions to avoid privacy threats in intelligent e-games (de Paula Albuquerque et al., 2020).

Brewer et al. (2018) explored the ways in which adolescents experience the internet as a way of potentially criminal source. So far, little research has explored the possible links between the ubiquitous use of digital communication technologies by youth and participation in delinquency in Internet contexts. The current pilot study seeks to address this part, by examining how a young person's digital endeavors relate to (relative access technical competencies, exposure to related technologies, websites, and services), as well as different development considerations, in illegal online confrontations if it was temporary engagements of a naïve, non-criminal, or more serious form of criminality technologically mediated.. Based on data collected from a bunch of adolescents enrolled in a high school in a large Australian city, the results establish significant relations among numerous of these perceptions, simply also the knowledge that online reprobate experiences between adolescents are improbable to compare with criminal presence, and the results also highlight the need to better understand the role of digital communication technologies in pathways to cybercrime. The authors further break down the risks related to the content into illegal content (child sexual exploitation), harmful or age-inappropriate subjects (such as pornography), harmful advice about alcohol and drugs, suicide, mental and nutritional disorders, cyber-bullying, and cyber-grooming. Along with categorizing the risks, the study also presents a high-level software architecture outlined to account for modern online security and protection. Moreover, analysts have already appeared that utilizing social media increments the chance of hurt for teenagers (Livingstone et al., 2012; Staksrud et al., 2013). In our questionnaire development, we considered in the personal factors such extraversion measures that strengthen the cyber and social interactions and the level of activities needed for excitement, and the ability to have fun. Among the dimensions of this social factor is enjoying the company and sharing of others, the love of parties, many friends, and love, competitiveness, leadership, and activity that indicates speed, strength of movement, and a sense of energy are preferred with the fast pace of life (Brewer et al., 2018).

Abu-Sare'e (2019), in her thesis, identified the social and environmental repercussions of the various social networking sites on adolescents, and from this goal emerges a set of the sub-objectives which are the detection of the motives for adolescents' use social networks. The results of this study are indicated that the most important motives that adolescents use by social net-working sites, respectively: entertainment, getting to know everything new, watching photos, movies, series and songs, get rid of boredom and occupying leisure time, learning about news and information, because it contains what I do not find in traditional media, as for the sample of experts, they indicated that it is one of the most important motives of adolescents. The use of social networks is: people's communication, leisure, entertainment, the means for adolescents to express what is inside them, family preoccupation and family disintegration, knowledge regarding everything that is new, ease of use, and trying to answer the questions of existence in the surrounding environment, and the results of the study indicated that the most important social networking sites from the point of view of teenagers is respectively: Facebook, WhatsApp, Instagram, YouTube, Twitter, Google Plus, and My Space. As for the sample of experts, the vocabulary of the study sample that was indicated by experts found that the most important websites used by teenagers were, respectively: Facebook, WhatsApp, Twitter and Snapshot. In our research we focus on the side effects of different aspects of internet use among adolescents, making it more comprehensive in the Jordanian context in cyberspace. That makes it possible to provide a simple solution to adolescents' perceptions of misusing the Internet into misbehavior that exposes them to threats of hacking and fraud (Abu-Sare'e, 2019).

Cybersecurity Awareness- Personality Factors

Quayyum et al. (2021) investigated the state-of-art research and practices in cybersecurity awareness for children. The authors analyzed 56 peer-reviewed articles spanning 2011 to mid of 2020. They provide a detailed report on various cybersecurity risks, awareness-increasing approaches, the effectiveness of the approach and its evaluation, and a list of factors that investigators considered when assessing security awareness methods. The authors classified the risks into five groupings: content risks, communication risks, children intended as consumers, economic risks, and online privacy risks. Moreover, the study also revealed that there are other gaps and risks that need more research and attention, and there are awareness tools and programs that did not measure their impact on awareness or did not accurately assess a child's awareness of cybersecurity. In our hypotheses, These factors are human life variables that are not limited to meeting the basic and essential needs for surviving, but it goes beyond it to include everything to improve the

quality of human life and its distinction from other creatures, such as mental and personal components both emotional and social, with the ability to think and social relationships that it includes religious beliefs, cultural and civilization values, and financial and economic conditions, every person can determine the thing that brings him happiness and satisfaction in life, so it must be in life that the human being is something of quality and the adolescence stage in which the adolescent passes with having physical and personal developments and changes are affected by the previous stages, and it is a multiple stage as the adolescent grows physically, mentally, emotionally, socially and professionally (Quayyum et al., 2021).

Burton and Lain (2020) discussed the theory that is assumed the conditions of anonymity or isolation in computer communication enhance social character and strong group-based ties. In the deficiency of classifying personal data identity, the social identity model theory of the effects of individuation confirms that individuals minimize their personal characteristics and highlight the social character they share with their buddies in virtual communication. Accordingly, people may focus on related identities such as membership in common groups or symbolic methods rather than being in a measured environment filled with apparent impersonations. The social identity model frames the effects of individuation in computer communication as a publicly environment, in that gifts based on groups are exaggerated and attributable in the lack of exclusivity data (Burton & Lain, 2020).

Other research emphasized the super-personal theory that the relative lack of nonverbal gifts on the internet and enhances social interaction so that social goals can be pursued appropriately and more effectively online than in face-to-face dialogues as described by (Walther, 1996), as super personal communication is “computer communication more socially desirable than we tend to encounter in direct, parallel interaction face to face”. According to the personal perspective, there is opportunity to adapt to and take advantage of the nonverbal gifts that diminish in communication via computers in ways that enhance their ability to achieve the desired goals between people. For example, it is easier to control the verbal content that dominates the interactions to communicate and strategically address non-verbal behaviors on a computer. Specifically, computer communication asks individuals to enter their replies ahead of posting them, which means that it can revise or discard destructive communications more easily than in direct conversations that are done face to face (Al Shamsi, 2019).

The findings and thoughts all these outcomes are related to our research design, they are used as inputs to support us in the designing and developing a research methodology that helps address gaps in cybersecurity awareness among adolescents in Jordan. Such the personality factors depression, disruption of social relationships, educational mismatch, sleep disturbance, lack of social skills, the personal factors scale is indispensable for description of the human personality. In our study, we search for a tight classification of personality trait. It is based on the idea of individual differences indicating the daily interactions of people with others. Personal factors scale is a hierarchical structure of personality traits that includes many factors. The first which is neurotic, which measures compatibility versus emotional instability, and identifies individuals who have unrealistic thoughts, impulsive responses and are maladaptive. Its dimensions are neurotic depression, which refers to a tendency to feel lonely, hopeless, and impulse-controlled which refers to keeping calm and not easily aroused by others and not being disturbed or upset by any disturbances in normal everyday situations, and impulsivity that indicates inability to control in urgent desires such as (sleeping, eating). This came in support of such studies of (Gilad et al., 2020; Khader et al., 2021) that included more than thirteen thousands of adolescents in seven European countries. Therefore, we care about experiments concentrated on all types of cybersecurity threats intended for adolescents. In our work, we investigate the raising cybersecurity awareness among Jordanian’s adolescents and study cybersecurity awareness assessment procedures along with the threats. To the best of our understanding, there is no such study is similar in work and scope in Jordan.

CYBERSECURITY AWARENESS PERCEPTIONS MODEL (CAPM)

The research methodology is designed based on a cross-sectional, comparative descriptive design in different stages: defining the population and sampling strategy, determining the data collecting the identification of cybersecurity factors, and data synthesis. Using this design is beneficial to achieving the goal

of this study because data collection is completed all at once, providing the necessary efficiency in terms of time and cost.

CAPM is a cross-sectional, comparative descriptive design that is used to study the perceptions of cybersecurity awareness among different populations. This design is beneficial to achieving the goal of this study because data collection is completed all at once, providing the necessary efficiency in terms of time and cost. CAPM consists of four stages: defining the population and sampling strategy, determining the data collecting the identification of cybersecurity factors, and data synthesis. In the first stage, the population and sampling strategy are defined. This involves identifying the target population, selecting the appropriate sampling method, and determining the sample size. The second stage involves collecting the data. This includes collecting information on the participants' demographics, their knowledge and attitudes towards cybersecurity, and their behaviors related to cybersecurity. The third stage involves identifying the cybersecurity factors that are associated with the participants' perceptions of cybersecurity awareness. This includes identifying the factors that influence the participants' knowledge, attitudes, and behaviors related to cybersecurity. The fourth stage involves synthesizing the data. This includes analyzing the data to identify patterns and trends in the participants' perceptions of cybersecurity awareness. CAPM is a useful tool for studying the perceptions of cybersecurity awareness among different populations. It is efficient in terms of time and cost, and it provides a comprehensive view of the participants' perceptions of cybersecurity awareness. Furthermore, it allows researchers to identify the factors that influence the participants' knowledge, attitudes, and behaviors related to cybersecurity. This can help researchers to develop strategies to improve cybersecurity awareness among different populations.

The population of this study are adolescents in Jordan. Not all teens may be residing in the same area (planning vs. random area); These two groups have significant overlap, but they are not identical. We can determine the population from all current adolescents in Jordan and all adolescents using the Internet. The sample that is collected is a subset of the population. Sample size (n=400), a random sample from a planned area and a random area in Jordan.

This design relieves study participants of the burden of answering the questionnaire more than once, relieves the researcher of the difficulty of maintaining contact with participants for a long time, and allows the principal investigator to study many participants in a relatively short period of time. To this end, a weblog with photos, videos and articles has been developed to inform teens of any cyber-attacks. This blog also shows several ways to protect themselves from these cyberattacks by training themselves in dealing with these risks and how to protect them from harm (viruses, data theft, fraud, etc.), as well as explaining the side effects that will occur if they do not protect themselves.

After translating the study tools into Arabic, a pilot study was conducted to test the tools and to explore any unexpected obstacles or difficulties that might be faced children or adolescents during the actual data collection phase of the study. Piloting also helped in determining the time needed for the participants to fill the evaluation tool, readiness, and clearness of questions. Scale of quality of life of cyber influence: It was adapted due to improve the validity and reliability criteria that reflect the attributes of cybersecurity for children and adolescents. The scale consists of 8 items to which the school children respond to five-point scale and have psycho-cybersecurity factors used in other studies as mentioned above. Considering the major personality factors scale, and a measure of quality-of-life participants. Reviewers suggested scale items in terms of expression and wording. 80% of the reviewers' consensus on wording of the scale items was adopted by researchers and therefore the scale became composed of eight items.

With examinations, the relationship between cybersecurity mindfulness, comprehension, and action with assurance teens in Jordan. The findings indicate that in spite of the fact that most teens had satisfactory cybersecurity mindfulness, it was rarely utilized in practice. Preliminary research results revealed that adolescents had fundamental cybersecurity information but were uncertain how to secure their data., to measure their mindfulness of phishing endeavors, emphasizing understanding and responses to cybersecurity risks.

The blog also provides information on how to protect oneself from cyber-attacks, such as using strong passwords, avoiding clicking on suspicious links, and using two-factor authentication. The blog also provides information on the side effects of not protecting oneself from cyber-attacks, such as data theft, fraud, and

viruses. The blog also provides information on how to report cyber-attacks and how to contact the authorities if needed. The blog is an effective way to inform teens of cyber-attacks and to train them in dealing with these risks. It relieves the researcher of the difficulty of maintaining contact with participants for a long time and allows the principal investigator to study many participants in a relatively short period of time. The blog also relieves study participants of the burden of answering the questionnaire more than once, as they can access the blog at any time and can review the information as needed. The blog also provides a platform for participants to interact with each other and to share their experiences and tips on how to protect themselves from cyber-attacks. Overall, the blog is an effective way to inform teens of cyber-attacks and to train them in dealing with these risks. It relieves the researcher of the difficulty of maintaining contact with participants for a long time and allows the principal investigator to study many participants in a relatively short period of time. It also relieves study participants of the burden of answering the questionnaire more than once, as they can access the blog at any time and can review the information as needed. The blog also provides a platform for participants to interact with each other and to share their experiences and tips on how to protect themselves from cyber-attacks.

Data Collection and Analysis

An overview approach was utilized to meet the study's objectives and collect qualitative information on the degree of cybersecurity mindfulness among teens' understudies in Jordan. The consider was carried out online to guarantee that a blended gather of male and female pupils' reactions were collected rapidly and responsibly. There were 13 items within the survey covering all aspects of cybersecurity, including five demographic items. Data were collected from 400 distributed questionnaires according to inclusion criteria. We excluded 150 who did not meet the inclusion criteria. Inclusion criteria included: school students (male/female); Each participant has internet access, and PC/laptop/mobile; and the participant signed a letter of consent or his/her parent/responsible singed it under the confidentiality responsibility. The questionnaire included different parts and it is based on a four-point Likert scale scoring system. A four-point scale is (strongly disagree, disagree, agree, and strongly agree). Demographic variables: participants were asked to fill out their age, internet use experience, family monthly income, parent academic degree (diploma, bachelor, master, PhD, and MD), gender. The questions in the cybersecurity awareness section were designed to elicit information about teens' online behavior. The nine items used to assess cybersecurity awareness aspects, such as passwords, phishing, social media, spam emails, unknown messages, viruses, counterfeit advertisements, popup windows, and further attacks, are important for teens to understand in order to protect themselves online. The questions drafted to assess teens' cybersecurity awareness include questions about cyber anxiety, cyber addiction, educational perspectives, lack of social skills, feeling nervous when not using social media daily, and more. These questions are important for teens to answer in order to understand their own online behavior and how it can affect their safety. When it comes to passwords, teens should be aware of the importance of using passwords that are 8-12 characters long and include a combination of letters, digits, or special characters. Teens should also be aware of the importance of not sharing their passwords with friends or family members, and of not accessing their accounts from public devices. When it comes to browsing history and cookies, teens should be aware of the importance of regularly deleting their browsing history and cookies for any unusual activity. Teens should also be aware of the importance of saving passwords for their accounts on browsers, checking the logo and address of important sites, and not posting private photos on social media. Finally, teens should be aware of the importance of not accepting invitations from strangers. This is especially important for teens, as they are more likely to be targeted by online predators.

Overall, the questions in the cybersecurity awareness section are important for teens to answer in order to understand their own online behavior and how it can affect their safety. By understanding the importance of passwords, browsing history, cookies, and more, teens can protect themselves online and stay safe; Posting your daily life on social media; Liking and follow unintended pages or groups.

The study sample consists of high school students (Jordanian and Syrian Refugees) from various schools of the Jordanian Ministry of Education. Several public and private schools in Irbid have been selected using (Convenience Sampling). It is consisted of 800 participants, 400 random areas, which means unlimited use of internet and sleep because of lack of awareness of internet usage in general, 400 planned areas which means

Table 1. Distribution of respondents based on demographic data (n=400/area)

Variable	Category	Number of participants area		Ratio (%)
		Planned	Random	
Gender	Male	140	252	49.0
	Female	260	148	51.0
Age	16 years old	212	264	59.5
	17 years old	48	24	9.0
	18 years old	140	112	17.5
Family Income	Less 400 JD	64	155	27.3
	401 JD-700 JD	272	85	44.6
	701JD-900 JD	103	24	15.8
	More 900 JD	81	16	12.1
Internet skills	Beginner (less three years)	112	208	40.0
	Intermediate (three-five years)	295	104	49.8
	Advance (more five years)	68	13	10.1

organized and limited internet use, organized sleeping and eating hours because of high awareness of internet usage.

This study incorporates quantitative data analysis, with the quantitative portion of the study playing a significant role. Analysis was conducted using statistical package for social sciences (SPSS) version 22.0 for windows. The data were tabulated by unpacking them using SPSS. In this study, the following evaluation tests have been applied:

1. Stability test through Cronbach's alpha coefficient to test stability the scale.
2. The internal consistency validity tests through the Pearson correlation coefficient (PCC) (ρ) between the dimensions the total scale.
3. Finding the impact of demographic variables on the level of cybersecurity awareness among adolescents using multiple variance tests, linear regression, frequencies, and percentages.
4. Finding the correlations with the PCC for the dimensions of the study to prove its validity study assignments.
5. t-test (ANOVA) to clarify the differences between the study samples.

Demographic Data

Demographic data in this study in the form of respondent data: gender, age, planned area or random area, family income, and internet skills as shown in **Table 1**. **Table 1** demonstrates that the number of female respondents was 51.0% from planned and random areas. The average age was 17 years old for both areas. About half of the respondent's family income is between 450-700 Jordanian Dinar (JD); and only 27.3% of their family income is 400 JD or less.

An independent sample t-test (t) was run to determine if there were differences in cybersecurity awareness score according to gender and age. The mean score for cybersecurity awareness was non-significantly higher in males (4.21) than females (4.11), $t(408)=1.305$, and p-value significant ($p=0.139$). The mean score for cybersecurity awareness was significant higher in planned area (4.24) than in random area (4.02), $t(408)=-3.021$, $p=0.003$.

A one-way ANOVA test was performed to investigate differences in cybersecurity awareness according to students' parent education level, family monthly income, internet experience, internet usage, and area. Results showed significant differences in adolescents' cybersecurity awareness a according to students' parent education level F-test ($F[4, 295]=3.075$, $p=.017$), family monthly income ($F[2, 297]=9.261$, $p<0.0.001$), and internet experience ($F[5, 294]= 8.208$, $p<0.0.001$), but not to internet usage ($F[2, 297]=0.459$, $p=.633$), nor to area ($F[3, 296]=1.327$, $p=.266$). Therefore, this is showed that adolescents with one to three years of internet experience have lower cybersecurity awareness compared to adolescents with more intermediate experience. The test results revealed that student who live in planned areas have a higher awareness of cybersecurity compared to random areas. Moreover, the family of adolescents with a monthly income of less than 400 JD o had lower cybersecurity awareness than the family of adolescents with a monthly income of 400-700 JD or more. A positive linear trend was found between the increases in the degree of cybersecurity

Table 2. The quality-of-life factors associated with the cyber impact

Factors	PCC with cybersecurity variables	Personal factors scale	
		Planned area	Random area
Depression and cyber withdrawal	0.609	0.368	-0.242
Cyber anxiety	0.656	-0.212	-0.272
Cyber addictive behavior	0.624	0.200	-0.207
Disruption of social relations	0.517	0.245	-0.322
Social isolation	0.690	-0.198	-0.183
Educational mismatch	0.505	0.327	-0.152
Sleep disturbance	0.687	0.402	-0.211
Eating disorder	0.575	-0.209	-0.210
Lack of social skills	0.562	0.500	-0.301

awareness, reaching the highest significant level in the five-year experience group (4.14±0.53). Test results revealed that teens who live in a random area have lower awareness compared to the planned area.

The Independent Variable–Quality-of-Life and Personal Factors

A correlation is a process to test the independent and dependent variables to determine the level of understanding of the relationship between two variables. **Table 2** shows the correlation values among the variable quantities used in the analysis. The focus of this test is to define the level association of each independent variable (personal factors and quality of life variables), and cybersecurity awareness. To facilitate the interpretation of the strength of the relationship between the two variables. The stability of the independent's quality-of-life variables using Cronbach's alpha presents a high coefficients value, where the alpha value (α) of the overall scale reliability coefficient is 0.0837. Therefore, the quality-of-life scale of the correlation coefficients are statistically significant at the level significance (0.05) for quality-of-life measures, which confirms the validity of the internal consistency of the quality-of-life, as shown in **Table 2**. This indicates that every statement used in the variable is reliable enough, with the result that all statement items used in this study are suitable for research. **Table 2** shows the Pearson's correlation that reveals of strong positive relationship between quality-of-life variables scale, the personal factors, and quality-of-life scale, associated with the cybersecurity awareness. The test is carried out to assess the validity analyzed using Pearson's factor analysis. The validity of the quality-of-life scale associated with the cyber influence. **Table 2** also shows the Pearson's correlation reveals a strong positive relationship among quality-of-life scale, and the personal factors associated with cybersecurity awareness.

RESULTS AND DISCUSSION

The findings of hypothesis analysis using the t-test show that the positive and negative personal, quality-of-life factors and significantly affects cybersecurity awareness (p-value=0.0001).

Result of H1: Personal Factors Have a Positive Impact on the Level of Cybersecurity Awareness Among Adolescents in Jordan

Figure 1 and **Figure 2** show the coefficients for the personal factors scale for each type of populations. It illustrates an inverse correlation with a statistical significance at the level of significance (0.05) between the personal factors scale and all the cybersecurity variables for a random sample.

In the planned area, the model shows a positive statistically significant correlation among the Personal Factors Scale and each of cybersecurity awareness variables: neuroticism, extraversion, openness, approval, and vigilance of conscience, whereas there is a statistically significant inverse correlation with such cybersecurity awareness variables: cyber anxiety, social isolation, and eating disorder.

In nutshell, the coefficient summary indicates that the personal factors have a significant positive impact on cybersecurity awareness level given that the significance level is >0.05. As a result of such factors, there is an openness to new experiences, as well as a desire for exploration and enduring mystery. The approval also shows an adolescent's social competence. Therefore, the awareness of conscience demonstrated the degree of adolescents in the system and the realism in their goal-oriented behavior, which including the dimensions of self-responsibility that expresses the adolescent's responsibility for their personal actions and bearing their

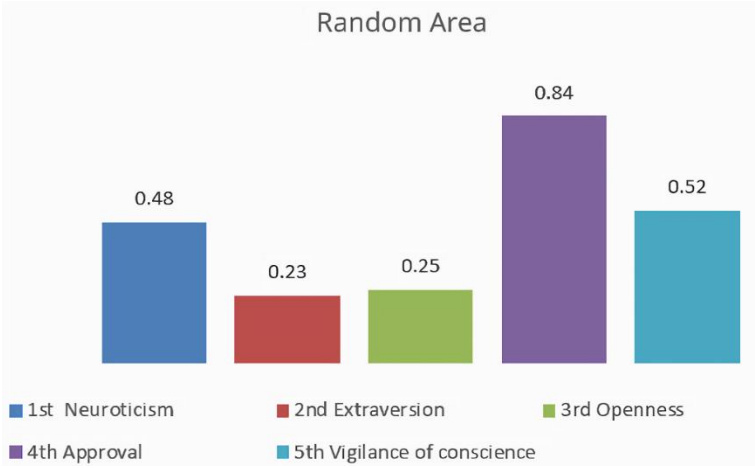

Figure 1. Coefficients for the personal factors measurement (random area) (Source: Authors' own elaboration)

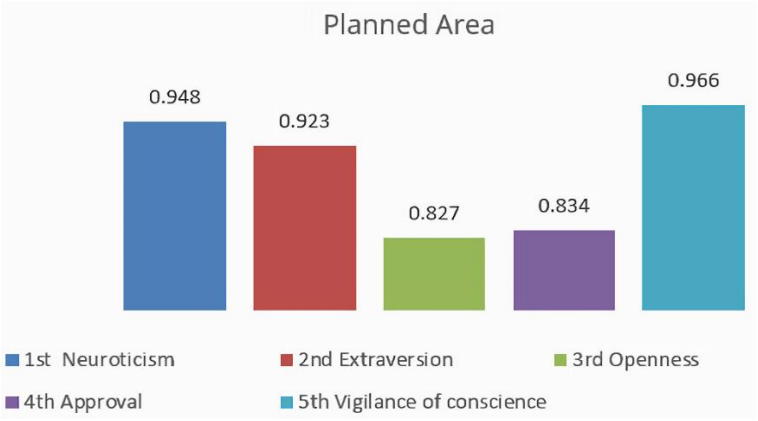

Figure 2. Coefficients for the personal factors measurement (planned area) (Source: Authors' own elaboration)

consequences, and cyber responsibility, which is the adolescent's responsibility for the group to which he belongs. Major personality factors are basic personality traits that have the ability to distinguish between an individual and another, from the dimensions of the first neurotic factor is extraversion, which refers to a person who has fears such as pathological, irritable, self-conscious, which are the emotions of shame and confusion and embarrassment, shyness. It indicates an inability to control motivations and the inability to control cravings. Extraversion indicates a low degree of introversion and reservation, and openness to experiences that indicate feelings. It includes an individual's internal feelings, emotions, and feelings of happiness or unhappiness, as well as signs of external emotion appearance. While the approval factor that reflects how you interact with others, and conscientiousness, which includes perseverance and organization to achieve the desired goals.

The p-value<0.05 indicates that the respondents in this study already have an awareness of cybersecurity awareness, but it is still low in the random area; this is because they do not take more or actual actions to implement cybersecurity in their personal activities and lives. Therefore, there is a correlation between the cyber dimensions and the five personality factors. The results support the relationship between each personality factor, number of friends and time on the social networking site, in view of the importance of using technological innovations and the means of communication in identifying the different personality styles.

H1 was applied with the social identity model of the individuated consequences of another principle, which assumes that individuals adapt to the shortage of nonverbal guidance online rather than pretending that individuals are restricted to fewer nonverbal cues online. The social identity model assumes the effects of individuation are in interactions guidelines are limited on the internet, adolescents emphasis their awareness

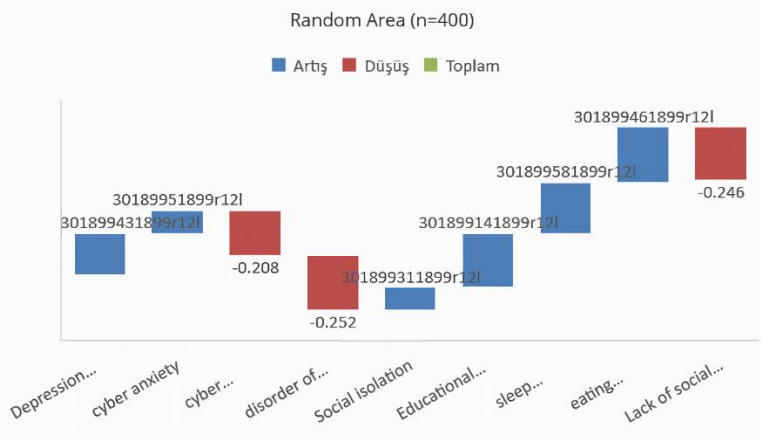

Figure 3. Coefficients for the quality-of-life factors scale (random area) (Source: Authors' own elaboration)

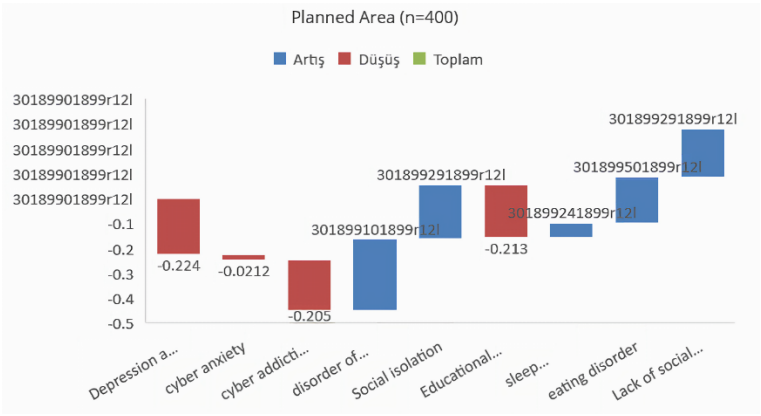

Figure 4. Coefficients for the quality-of-life factors scale (planned area) (Source: Authors' own elaboration)

on background cues and knowledge related to the social position of the participants. These findings came in agreement with many studies that mentioned the impact of the internet and its contribution to the formation of dimensions of different personality traits as these studies (Brewer et al., 2018; Subrahmanyam et al., 2001), as well as Abdul Samad (2021), which concluded that the internet is linked negatively with the mental health of the individual.

There is consistency between the results of the cyber scale and the major personality factors, where there are differences that are statistically significant according to the living area variable for all dimensions of the cyber scale and personality factors. Moreover, the presence of statistically significant differences according to the living area variable (random/planned) for males and females for the cyber scale, where are significant differences for the female with the personal factors scale, except for the (dimension: approval), while there are no statistically significant differences according to the living area variable (random/planned) for the male sample of the personal factors scale, except for (dimension: approval). As a result, the associated research hypothesis (**H1**) was accepted.

Result of H2: The Quality-of-Life Factors Have a Positive Impact on the Level of Cybersecurity Awareness Among Adolescents in Jordan

Figure 3 and **Figure 4** display shows a negative statistically significant correlation among the quality-of-life scale and each of cybersecurity awareness variables: depression, cyber withdrawal, addictive behavior, disruption of social relations, educational mismatch, sleep disturbance, deficiency social skills, and the total score of the cyber scale. Whereas there is a positive statistically significant correlation among the measure of quality-of-life with such cybersecurity awareness factors: disruption of social relationships, social isolation, eating disorder, lack of social skills, and the total score of the cyber scale.

In an overall view, the total sample shows a positive relationship between the quality-of-life and such cybersecurity awareness variables: depression and cyber withdrawal, cyber anxiety, cyber addictive behavior, social disorder, social isolation, educational mismatch, sleep disturbance, eating disorder, and the lack of social skills. In nutshell, the coefficients summary indicates that the quality-of-life scales have a significant positive impact on cybersecurity awareness level given that the significance level is >.05. The results of this hypothesis revealed that the excessive and unproductive use of the internet by most of Jordanians' adolescents/teenagers to fill their spare time for recreational and social purposes comes from their weak ability of facing life pressures and daily problems, not occupying leisure time with useful activity. This led to a poor ability to establish social relationships due to lack of self-confidence, shyness and introversion, a loss of emotion and love, or feeling lonely and psychologically empty, and escaping from facing others creates an urge to create an imaginary atmosphere, leading to suffering from quality-of-life problems such as depression, anxiety, behavior addiction, social disorder, social isolation, sleep disorder, eating disorder, lack of social skills. The Internet addicted scale for Jordanian teens scale indicated that teens tend to be isolated from social activities and immerse themselves in the cyberworld, they spend most of their time in this world away from the real world in which they live. This result also shows Internet addiction, which may cause adolescents to be dissatisfied with their lives, and thus negatively affect the stability of their quality-of-life. This supports El-Sayed Borham et al.'s (2022) study, which indicates an association between Internet addiction and adolescent feelings in Egypt, such as depression and anxiety. Therefore, this explains the increase in inconsistent adolescent behavior, and the various social and environmental repercussions of social communication have an impact on adolescents, as reported in Al Sayed and Al-Beheiry (2020).

There is consistency between the results of the cyber scale and the quality-of-life scale, as there are statistically significant differences among the study sample members according to the living area for all dimensions of the cyber scale and the quality-of-life scale. On the other hand, there is contradiction between the results of the cyber scale and the quality- of-life scale according to the gender variable. The cyber scale model showed that there are statistically significant differences in the collected data between the study samples according to the gender variable. While the measure of quality of life proved that there were no statistically significant differences between the study sample according to the gender variable.

The hypotheses confirmed that there is a statistically significant relationship between the cyber scale and both the quality-of-life scale and the personal factors scale, but there is no significant difference between the random and planned areas.

CONCLUSION AND RECOMMENDATIONS

Contribution

The findings of this study suggest that knowledge of personality and quality-of-life factors significantly influence cybersecurity awareness in adolescents. The results of this study indicate that adolescents who have higher levels of cybersecurity awareness tend to have higher levels of personality and quality of life. This suggests that adolescents who are more aware of cybersecurity are more likely to have better mental health and overall well-being. Furthermore, the results of this study suggest that quality of life is a mediator factor that affects cybersecurity awareness. This means that adolescents who have higher levels of quality of life are more likely to be more aware of cybersecurity and take steps to protect themselves online. However, in practice, teens' levels of cybersecurity awareness are still lacking, especially when it comes to online protection. Adolescents usually do not pay much attention to using good and correct internet use to protect their accounts or websites. Especially, Jordanian adolescents/teens use the internet in the same way that adults do, but they also engage in harmful activities such as downloading pirated movies and music. Adolescents might be exposed to a range of security concerns by using popular social media websites like Facebook. Also, this time the adolescents use the internet more than usual because their education in COVID-19 has been converted to online, thus so they have spent a lot of time on the internet without the supervision of their parents.

This study contributes to the literature by considering a cross-sectional research approach that aims to investigate the impact of cybersecurity awareness on the personality of the adolescent by understanding the

factors that affect personality, and quality of life in different type of areas. Furthermore, it investigates the impact of quality of life as a mediator factor and how it affects cybersecurity and then reveals future considerations and provide and provide recommendations based on the research results analysis and observation during this work. Understanding these factors may direct cybersecurity stakeholders and policymakers to implement policy changes that help improve satisfaction with using a secure internet environment, which will help improve privacy and data protection and ultimately better secure usage outcomes. The outcomes are reflected directly on the cybersecurity awareness adolescents, who are the core attention of secure usage. On the other hand, lower levels of cybersecurity awareness may lead to a low personality and low quality of life scales. Practically, this study can serve as a springboard for improving cybersecurity by helping policymakers to enhance related strategies and initiatives and enhance the adoption of cybersecurity systems across all internet providers. This study was implemented for the first time in Jordan Kingdom, where Jordanian authorities work to improve the cyber services provided with introducing new technology such as cybersecurity systems to improve the quality of life. Overall, this study provides important insights into the relationship between cybersecurity awareness and personality and quality of life in adolescents. It is important for policymakers and stakeholders to understand the factors that influence cybersecurity awareness in adolescents in order to develop effective strategies and initiatives to improve cybersecurity. Furthermore, this study provides a foundation for future research on the topic, which could further explore the relationship between cybersecurity awareness and personality and quality of life in adolescents.

Recommendations

The most important recommendations of this study are summarized in the need to establish a high level of cybersecurity awareness. To achieve this, the cooperation of the concerned authorities is essential to strengthen family members with the new concepts associated with the field of cyberspace and ICT. Disseminating cyber almost the foremost successful implies of communication to teach and prepare young people to bargain with cyber dangers in all its shapes is also necessary. Preparing learning awareness programs for high school and university students to familiarize them with the principles of dealing with social networks and internet security threats to protect their privacy is also essential. These programs should include topics such as cyberbullying, online predators, identity theft, and other cyber threats. Furthermore, these programs should also provide students with the necessary skills to protect themselves from these threats. Moreover, it is important to create a culture of cybersecurity awareness in the society. This can be done by providing educational materials to the public, such as brochures, posters, and videos, to raise awareness about the importance of cybersecurity. Additionally, it is important to create a safe online environment for children and young adults by providing them with the necessary tools and resources to protect themselves from cyber threats. Finally, it is important to create a legal framework to protect the rights of individuals in cyberspace. This includes the establishment of laws and regulations to protect the privacy of individuals and to ensure that their data is secure. Additionally, it is important to create a system of accountability for those who violate these laws and regulations. In conclusion, the most important recommendations of this study are summarized in the need to establish a high level of cybersecurity awareness. This can be achieved by strengthening family members with the new concepts associated with the field of cyberspace and ICT, disseminating cyber almost the foremost successful implies of communication to teach and prepare young people to bargain with cyber dangers in all its shapes, and preparing learning awareness programs for high school and university students to familiarize them with the principles of dealing with social networks and internet security threats to protect their privacy. Additionally, it is important to create a culture of cybersecurity awareness in the society, create a safe online environment for children and young adults, and create a legal framework to protect the rights of individuals in cyberspace. On the academic dimension, the results of this study may envision the integration of the information technology preparation in the primary cyber-education programs, which will facilitate the future cybersecurity adolescents' usage and promote their security and privacy in using internet. Moreover, computer skills, and cybersecurity training courses are highly recommended to be implemented at the internet security and privacy facilities where an internet is planned to be used in safe manner.

The study results in some recommendations, the most important of which is the dissemination of information about cyberspace on the most actual means of communication to educate individuals and train them to deal with electronic risks in various forms, preparing educational awareness programs for high school and university students to inform them about the origins of dealing with social networking sites and the dangers of the Internet and how to protect themselves from its harms. Most of key grasp points as following: spoofing could be a fairly common issue on social networks. Teenagers ought to know how to form solid pass codes and must be instructed not to share their personal information with others; Social systems, and other online situations that empower adolescents to share data approximately them, can expose teenagers to "identity theft". Teenagers ought to be instructed not to allow out their full title and to never give out their sensitive info online; Aside from the moral concerns almost downloading pilfered music and recordings, this moreover incredibly increments the hazard of downloading infections or other malware; Therefore, this recommendation supports front line enforcement authorities, e.g., The Cybercrime Directorate and the Community Peace Directorate in Public Security in case specific action to achieve cybersecurity awareness such as tactical plans. Talking to teenagers around about the threats related with downloading computer program and going by to scrappy websites and making beyond any doubt any computers or portable gadgets they utilize are prepared with a great security program; teach teens to always check out strange offers or requests on a good anti hoax site such as www.snopes.com. At the operational, the creation of a cybersecurity awareness product, that supports in planning cybersecurity defense activities to achieve an organizational operational objectives. Therefore, the findings revealed the need for cybersecurity campaigns to raise cybersecurity awareness, which would empower them to utilize their browser's private browsing mode at whatever point they make online buys and to not let any site store their delicate data. In nutshell, the recommendations guide the activities of cybersecurity law enforcement Jordanian's institutions to decide upon cybersecurity attacks and seek to influence long term organizational objectives and to contribute to discussions of cybersecurity policy and strategy.

Limitations of the Work

Based on the following, some things can be done to expand the cybersecurity awareness of adolescents through socialization activities related to cybersecurity. It should be noted that this investigation still has some limitations, such as the quality level of address reliability, which is still not very stable, and the restricted use of common factors. This investigation, however, did not address all cybersecurity concerns. In the future, it is recommended to include more factors that may influence cybersecurity awareness. Based on the following, there are many ways to expand the cybersecurity awareness of adolescents through socialization activities related to cybersecurity. By providing them with the necessary resources and tools, involving them in activities that promote the importance of cybersecurity, and giving them the opportunity to practice their cybersecurity skills, adolescents can become more aware of the importance of cybersecurity and how to protect themselves online.

Future Work

Future studies are recommended to replicate this study to evaluate the relationships among variables in other cybersecurity and social engineering adolescents' population to better understand the association. Large scale studies at the government authorities and in different ICT sectors in Jordan, including educational institutions, and high schools are highly recommended. Other factors that may affect the security and privacy need to be investigated in further research, including the user involvement in the process of cybersecurity protection implementation, timesaving in using the cybersecurity awareness, and the effect of implementing the ICT on the workflow of the different units and wards. Defining the relationships among the study variables and the direction of the relationships may assist in developing conceptual frameworks that can be utilized in future research locally and internationally to compare the results and add more practical and theoretical contributions to a variety of ICT sectors in Jordan. Moreover, future research may apply a qualitative instead of quantitative approach to provide a holistic understanding of how to improve cybersecurity awareness from the perspective of industry and decision-makers among those conducting personal interviews.

Author contributions: All authors were involved in concept, design, collection of data, interpretation, writing, and critically revising the article. All authors approved the final version of the article.

Funding: The authors received no financial support for the research and/or authorship of this article.

Ethics declaration: Authors declared that the research was conducted in accordance with the ethical guidelines of Yarmouk University and the collaborating organization. Informed consent was obtained from all adolescent participants and their legal guardians in accordance with the ethical guidelines at Yarmouk University and the collaborating organization in the research in Jordan. The consent was obtained through electronic or paper-based documents, which were sent to the participants and their legal guardians, either personally or through the participants' schools. All personal data was collected and handled in confidentiality. All personal data were stored anomalously and on one private computer, which only authorized researchers had access to. Data was destroyed soon after the study was completed to protect participant's anonymity and confidentiality. Authors further confirm that data presented in this paper is original and has not been published elsewhere.

Declaration of interest: Authors declare no competing interest.

Data availability: Data generated or analyzed during this study are available from the authors on request.

REFERENCES

Abdul Samad, A. M. (2021). The relationship between styles of abnormal parenting treatment and school bullying among primary school students. *Journal of the Faculty of Social Work for Social Studies and Research, 23*(1), 15-70. https://doi.org/10.21608/jfss.2021.156674

Abu-Sare'e, S. H. 2019. *Social networking sites and their social repercussions and the environment on adolescents* [Unpublished master's thesis]. Ain Shams University.

Al Sayed, S. A., & Al-Beheiry, M. R. (2020). Using Facebook and its relationship with the psychological resilience of a sample of orphaned teenagers. *Journal of Southwest Jiaotong University, 55*(6), 1-18. https://doi.org/10.35741/issn.0258-2724.55.6.40

Al Shamsi, A. A. (2019). Effectiveness of cyber security awareness program for young children: A case study in UAE. *International Journal of Information Technology and Language Studies, 3*(2), 8-29.

Al-Lassameh, A. K. S., & Al Majali, F. A. Q. (2022). The academic and awareness role of Jordanian public universities in cyber security from faculty staff perspective. *Annals of the Arts of Ain Shams, 50*(3), 82-96.

Alobedi, N., Saeed, S. (2021). Cyberspace and its relationship to psychosocial compatibility (Snapchat as a model). *Al-Adab Journal* [*Literature Journal*]*, 1*(137), 319-348. https://doi.org/10.31973/aj.v1i137.1147

Al-Tajer, M., & Ikuesan, R. A. (2022). *Cyber security threat awareness framework for high school students in Qatar*. http://arxiv.org/abs/2207.00820

Brewer, R., Cale, J., Goldsmith, A., & Holt, T. (2018). Young people, the Internet, and emerging pathways into criminality: A study of Australian adolescents. *International Journal of Cyber Criminology, 12*(1), 115-132. https://doi.org/10.5281/zenodo.1467853

Burton, J., & Lain, C. (2020). Desecuritizing cybersecurity: Towards a societal approach. *Journal of Cyber Policy, 5*(3), 449-470. https://doi.org/10.1080/23738871.2020.1856903

CISA. (2020). Avoiding social engineering and phishing attacks. *Cybersecurity and Infrastructure Security Agency*. https://www.cisa.gov/uscert/ncas/tips/ST04-014

Corron, L. (2018). *Social cyber threats facing children and teens in 2018*. https://staysafeonline.org/online-safety-privacy-basics/social-cyber-threats-facing-children-teens-2018/

de Paula Albuquerque, O., Fantinato, M., Kelner, J., & de Albuquerque, A. P. (2020). Privacy in smart toys: Risks and proposed solutions. *Electronic Commerce Research and Applications*, *39*, 100922 https://doi.org/10.1016/j.elerap.2019.100922

DeSmet, A. (2015). *Understanding adolescent bystander behavior in cyberbullying and the potential of serious digital games to promote prosocial behavior and other healthy lifestyles*. Consulté à l'adresse https://biblio.ugent.be/publication/6937148

Durkee, T., Kaess, M., Carli, V., Parzer, P., Wasserman, C., Floderus, B., Apter, A., Balazs, J., Barzilay, S., Bobes, J., Brunner, R., Corcoran, P., Cosman, D., Cotter, P., Despalins, R., Graber, N., Guillemin, F., Haring, C., Kahn, J. P., … Wasserman, D. (2012). Prevalence of pathological internet use among adolescents in Europe: Demographic and social factors. *Addiction, 107*(12), 2210-2220. https://doi.org/10.1111/j.1360-0443.2012.03946.x

El Nadir, A. T. M. (2021). Information society and knowledge gap in the third world–A conceptual approach–. *Online Journal of Communication and Media Technologies, 5*(September 2015-Special Issue), 53-63. https://doi.org/10.30935/ojcmt/5690

El-Sayed Borham, Y., Ahmed, A. I., & Gad, R. M. (2022). Assessment of internet addiction among adolescents in Mansoura City. *Mansoura Nursing Journal, 9*(1), 124-132. https://doi.org/10.21608/mnj.2022.259010

Gilad, A., Pecht, E., & Tishler, A. (2020). Intelligence, cyberspace, and national security. *Defence and Peace Economics, 32*(1), 18-45. https://doi.org/10.1080/10242694.2020.1778966

Hamdi, R. (2022). Cybersecurity awareness in Saudi Arabia: A systematic literature review. In *Proceedings of the EDULEARN22* (pp. 4805-4815). https://doi.org/10.21125/edulearn.2022.1142

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers and Security, 73*, 102-113. https://doi.org/10.1016/j.cose.2017.10.008

Irtaimeh, W. S. (2020). Criminal protection of privacy in the Jordanian Cybercrime Law No. 27 of 2015. *Asian Social Science, 16*(12), 64-79. https://doi.org/10.5539/ass.v16n12p64

Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. *Information*, *12*(10), 417. https://doi.org/10.3390/info12100417

Kumari, A., & Verma, J. (2015). Impact of social networking sites on social interaction–a study of college students. *International Journal of Humanities and Social Sciences, 4*(2), 55-62.

Lee, C. S., & Kim, D. (2022). Pathways to cybersecurity awareness and protection behaviors in South Korea. *Journal of Computer Information Systems*. https://doi.org/10.1080/08874417.2022.2031347

Leung, L. (2004). Net-generation attributes and seductive properties of the internet as predictors of online activities and internet addiction. In *Cyberpsychology and Behavior,* 7(3), 333-348. https://doi.org/10.1089/1094931041291303

Liaropoulos, A. (2013). Exercising state sovereignty in cyberspace: An international cyber-order under construction? *Journal of Information Warfare, 12*(2), 19-26.

Livingstone, S., Hasebrink, U., & Görzig, A. (2012). *Children, risk and safety on the Internet: Research and policy challenges in comparative perspective*. Bristol University Press. https://doi.org/10.2307/j.ctt9qgt5z

Luciana, R. P. (2010). One minute more: Adolescent addiction for virtual world. *Procedia-Social and Behavioral Sciences*, *2*(2), 3706-3710. https://doi.org/10.1016/j.sbspro.2010.03.576

MICT. (2018). National cyber security strategy 2018-2023. *Ministry of Information and Communication Technology*. https://modee.gov.jo/ebv4.0/root_storage/en/eb_list_page/national_cyber_security_strategy_2018_2023.pdf. 2018

Mohammad, T., Mohamed Hussin, N. A., & Husin, M. H. (2022). Online safety awareness and human factors: An application of the theory of human ecology. *Technology in Society, 68*, 101823. https://doi.org/10.1016/j.techsoc.2021.101823

Prasad, A., Ruiz, R., & Stablein, T. (2019). Understanding parents' concerns with smart device usage in the home. In A. Moallem (Ed.), *HCI for cybersecurity, privacy and trust* (pp. 176-190). Springer. https://doi.org/10.1007/978-3-030-22351-9_12

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. In *International Journal of Child-Computer Interaction, 30*, 100343. https://doi.org/10.1016/j.ijcci.2021.100343

Salgado, P. G., Rial Boubeta, A., Braña Tobío, T., Varela Mallou, J., Barreiro Couto, C., Salgado, P. G., Boubeta, A. R., Tobío, T. B., Mallou, J. V:, Couto, C. B., Gámez-Guadix, M., Orue, I., & Calvete, E. (2014). Evaluation and early detection of problematic internet use in adolescents. *Psicothema* [*Psychothema*]*, 26*(1), 21-26.

Staksrud, E., Ólafsson, K., & Livingstone, S. (2013). Does the use of social networking sites increase children's risk of harm? *Computers in Human Behavior, 29*(1), 40-50. https://doi.org/10.1016/j.chb.2012.05.026

Subrahmanyam, K., Greenfield, P., Kraut, R., & Gross, E. (2001). The impact of computer use on children's and adolescents' development. *Journal of Applied Developmental Psychology, 22*(1), 7-30. https://doi.org/10.1016/S0193-3973(00)00063-0

Tariq, F. (2015). The impact of cyber on the personality of the adolescent in light of the quality of life and major personality factors (a comparative study between a random area and a planned one). *Journal of the Faculty of Education in Humanities and Literary Sciences, 27*(1), 141-174.

Waldo, A. D. (2014). Correlates of internet addiction among adolescents. *Psychology, 5*(18), 1999-2008. https://doi.org/10.4236/psych.2014.518203

Walsh, K., Pink, E., Ayling, N., Sondergeld, A., Dallaston, E., Tournas, P., Serry, E., Trotter, S., Spanos, T., & Rogic, N. (2022). Best practice framework for online safety education: Results from a rapid review of the international literature, expert review, and stakeholder consultation. *International Journal of Child-Computer Interaction, 33*, 100474. https://doi.org/10.1016/j.ijcci.2022.100474

Walther, J. B. (1996). Computer-mediated communication: Impersonal, interpersonal, and hyper personal interaction. *Communication Research, 23*(1), 3-43. https://doi.org/10.1177/009365096023001001

Wasiński, A., & Tomczyk, Ł. (2015). Factors reducing the risk of internet addiction in young people in their home environment. *Children and Youth Services Review, 57*, 68-74. https://doi.org/10.1016/j.childyouth.2015.07.022