Dirasat: Human and Social Sciences, Volume 53, No. 3, 2026, 7917

Deanship of Scientific Research

Level of Awareness of Jordanian Universities Professors of Cybersecurity: Skills and Challenges

Samar Y. Makanai[1]*, ***Najm A. Kh. Alhatimi Aleessawi[2]***, ***Mostafa Hussam M. Altarawneh[3]***

[1]Department of Media, Arab Open University, Amman, Jordan
[2]Department of Studies and Research, Association of Arab Universities, Amman, Jordan.
[3]Department of Private Law, Faculty of Law, University of Petra, Amman, Jordan

Received: 10/6/2024
Revised: 12/9/2024
Accepted: 20/10/2024
Published online: 1/10/2025

* *Corresponding author:*
s_makani@aou.edu.jo

Citation: Makanai, S. Y., Aleessawi, N. A. K. A., & Altarawneh, M. H. M. (2025). Level of Awareness of Jordanian Universities Professors of Cybersecurity: Skills and Challenges. *Dirasat: Human and Social Sciences*, *53*(3), 7917. https://doi.org/10.35516/Hum.2025.7917

© 2026 DSR Publishers/ The University of Jordan.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC) license https://creativecommons.org/licenses/by-nc/4.0/

Abstract

Objectives: The study aims to assess the level of awareness among Jordanian university professors regarding cybersecurity, identify the key challenges they face in acquiring sufficient knowledge about it, and explore its implications.

Methods: A descriptive approach was adopted, using a questionnaire distributed to 55 curriculum professors selected through an accumulative sample from a population of 120 professors in the same specialization from four Jordanian universities: Middle East University, Petra University, Amman Arab University, and Applied Science University. The sample was limited to those with at least the minimum knowledge required in higher education.

Results: The findings indicated that faculty members believe there is an organized global cyberwar and that communication applications do not adequately address cybersecurity needs. The most common motivations for cybersecurity violations were identified as extortion, theft, and obtaining information. Faculty members' skills were mainly limited to taking precautionary steps when receiving emails, but the biggest challenge was the lack of cybersecurity awareness courses provided by the universities.

Conclusions: The professors' skills were confined to taking precautionary measures in handling emails and securing their accounts using multiple methods. However, the most significant challenge was the scarcity of awareness activities that universities should organize for both professors and staff.

Keywords: Cybersecurity; digital transformations; Jordanian universities; professors

مستوى وعي أساتذة الجامعات بالأمن السيبر انى في الجامعات الأردنية: المهارات والتحديات

سمريحي مكناي[1]*، نجم عبد خلف الحاتمي العيساوي[2]، مصطفى حسن مصطفى الطراونة

[1]قسم الإعلام، الجامعة العربية المفتوحة، عمّان، الأردن.
[2]قسم البحوث والدراسات، اتحاد الجامعات العربية، عمّان، الأردن.
[3]قسم القانون الخاص، كلية الحقوق، عمان، جامعة البترا.

ملخّص

الأهداف: هدفت الدراسة التعرف على مستوى وعي أساتذة الجامعات الأردنية بالأمن السيبراني، وأهم التحديات التي تواجههم في اكتساب المعرفة الكافية عنه، وانعكاساته.

المنهجية: تم اعتماد المنهج الوصفي باستخدام استبانة تم توزيعها على (55) أستاذاً من أساتذة المناهج تم اختيارهم من خلال عينة متراكمة من مجتمع الدراسة (120) أستاذاً في نفس التخصص من أربع جامعات أردنية هي: جامعة الشرق الأوسط، وجامعة البترا، وجامعة عمان العربية، وجامعة العلوم التطبيقية، وقد اقتصرت العينة على من لديهم معرفة بالحد الأدنى من متطلبات التعليم العالي.

النتائج: أظهرت النتائج أن أعضاء هيئة التدريس يعتقدون بوجود حرب سيبرانية منظمة على مستوى العالم، وأن تطبيقات الاتصال لا ضرورات الأمن السيبراني. كما تبين أن من أكثر الدوافع شيوعاً لانتهاك الأمن السيبراني محاولة الابتزاز والسرقة والحصول على المعلومات. واقتصرت مهارات الموظفين على اتخاذ الخطوات الاحترازية عند تلقي رسائل البريد الإلكتروني. لكن التحدي الأكبر كان قلة الدورات التوعوية التي تقيمها الجامعة للأساتذة.

الخلاصة: انحصرت مهارات أعضاء هيئة التدريس في اتخاذ الخطوات الاحترازية في تلقي رسائل البريد الإلكتروني وتوثيق حساباتهم بأكثر من طريقة، لكن التحدي الأكبر كان قلة الأنشطة التوعوية التي يجب أن تقيمها الجامعة للأساتذة والموظفين.

الكلمات الدالة: الأمن السيبراني، التحولات الرقمية، الجامعات الأردنية، الأكاديميون.

Introduction

Rapid developments have occurred in the last decade in the fields of computing and information technology, leading to far-reaching changes in almost all areas of life. Digital and technological development has shaped intense competition among countries of the world, which has caused what is known as the digital revolution, which has become a worry for many people. These challenges or changes are characterized by rapid performance, strong impact, and almost lack of knowledge of the identity of the attacker and ideological backgrounds, which increase their danger, as the tools of conflict in them are formed by electronic challenges, technical software, and a pack of computerized sabotage programs.

The great acceleration in digital transformation processes and the high rate of electronic attacks and data breaches; in addition to the negative results from criminal and terrorist threats that may be produced by individual groups to obtain political, economic, or propaganda advantages, required strengthening cybersecurity and increasing awareness of its danger. Furthermore, the national security of countries is linked to the extent of their security and strength in protecting their cyberspace in all its institutions in various fields at the local, regional, and international levels. It also requires legislative and security policies based on protection mechanisms and taking the necessary measures to confront them and keep pace with the transformations in the concept of cybersecurity and digital transformation, as digital transformation is the basis of the Fourth Industrial Revolution. Accordingly, this technological boom has brought about a qualitative shift in the performance of various institutions that have realized the importance of catching up with the revolution of modern technologies to be more aware and flexible at work and more capable of innovation, creativity, and innovation (Aleessawi, 2022).

Jordan established the National Cybersecurity Centre and the National Council in 2019 to address cyber challenges and protect government and private networks, build, develop, and organize an effective national cybersecurity system to protect the Kingdom from cyberspace threats and confront them efficiently and effectively in a way that ensures work sustainability, national security, and safety. In addition to the Cybercrime Law, Personal Data Protection Law, Electronic Transactions Law, Credit Information Law, Banking Law, and others, Jordan ranked 10th in the Arab world in cybersecurity according to the latest UN index. The lack of community understanding about cybersecurity, how to safeguard from it, and how to respond to assaults is one of our biggest difficulties in creating a secure and stable cyber environment that supports digital transformation. In addition, industries' aging infrastructure is “not prepared” for contemporary cyber attacks(Petra, 2024b).

Government and commercial entities must coordinate to address cyber threat information and skill gaps. In addition to public awareness campaigns, schools should include cybersecurity topics in their curricula, offer specialized training courses and workshops for companies and individuals, invest in cybersecurity education and training, support all universities to launch specialized academic programs and provide scholarships for students. A major directive emphasizes field communication with residents and public-private cooperation. The National Centre trains qualifies, educates, and empowers public and private sector employees and all segments of society to reduce risks and threats following cybersecurity best practices and ensure maximum efficiency, making Jordan a regional and international centre of creativity and excellence.

Therefore, educating and raising awareness among generations about the importance of cybersecurity, its concept, and its mechanisms is an essential part of the digital transformation movement, as well as clarifying the role of universities as Jordanian national institutions represented by their teaching and administrative members in adopting scientific research programs, qualifying cadres in the field of cybersecurity, and providing the requirements for achieving it. Universities must have a technical governance system to develop cyberinfrastructure to reduce hacking and electronic piracy and develop information programs that allow for the identification of technologies that help detect and deter hacking.

Problem Statement

As the scope of information technology expands day by day and enters almost all aspects of our lives, it creates threats and violations that would not have been easy to occur without the existence of such technology. Examples of such threats and violations are unauthorized use of hardware and software, software theft, copyright infringement of products, computer fraud, privacy violation, use of viruses to disable functions, and hacking, which is another aspect of information technology crimes that creates serious ethical issues, etc. Some of these issues can be classified as computer crimes. On the other hand, one of the problems that IT professionals, groups, and organizations may face is the failure of "safety-critical systems" that can pose a direct threat to people's lives, such as software applications that control aircraft, weapons, radars, nuclear reactor control systems, etc(Bynum & Rogerson, 2003; Himma & Tavani, 2009).

Cybersecurity has become one of the latest technological and digital developments in the current era, and the emergence of the Internet and the rapid flow of information has had a major impact on all areas of life, as digital space has constituted a source of threat to users of the Internet through what is known as cybercrimes or cyberattacks. As it causes losses and problems that may lead to data falsification and manipulation and may lead to threats to electronic accounts and others, cybersecurity derives its importance by including all social, economic, educational, and humanitarian aspects..., therefore it is important to educate and raise awareness among generations about the importance of cybersecurity and its mechanisms as protection. Email, data, and information protection and threats are an essential part and foundation for supporting the educational vision in light of digital transformation, and accordingly; Education and awareness of the concepts, importance, and skills of cybersecurity are an urgent necessity in institutions in general and educational institutions in particular represented by faculty members, especially in light of the spread of communication and information technology technologies and the increasing risks of cyber-attacks.

Accordingly, this requires institutions, including universities, to help their staff and students gain higher efficiency and awareness in dealing with the use of technology and the computer environment.

Therefore, the main question can be formulated as follows: What is the level of awareness of academics in universities about cybersecurity? The following questions can be branched out:

- To what extent are professors aware of cybersecurity?
- What skills and procedures do professors take into account in cybersecurity?
- What challenges do professors face in enhancing cybersecurity awareness?

The importance

Cybersecurity is a new topic, and it is necessary to enhance academic knowledge about it. Especially since cybersecurity is an integral part of the technological revolution that the world is witnessing, including artificial intelligence applications and technologies, and superior capabilities in dealing with and generating data. The importance of the topic is highlighted in this period due to the emergence of many computer-powered technologies and inventions, especially in the last two decades. Universities are also the most in-touch and demanding environments to keep pace with these changes in their curricula, teaching methods, and faculty competencies. On the other hand, the results could help decision-makers in universities address the challenges and difficulties facing academics, which impose awareness of cybersecurity and work to improve it. Its results and recommendations also raise the level of knowledge of the concept of cybersecurity among faculty members in Jordanian universities and enable them to implement educational outcomes in the field of cybersecurity in the best possible way.

The Objectives

The article aims to identify the level of awareness of professors at universities regarding cybersecurity. It also aims to:

- Reveal to what extent are professors aware of cybersecurity.
- Identify the skills and procedures do professors take into account in cybersecurity.
- Discover the challenges professors face in enhancing cybersecurity awareness.

Terminology

**Cybersecurity*: “Cybersecurity is the practice of protecting internet-connected systems such as hardware, software, and data from cyber threats”(Shea & Gillis, 2024). Also, Cybersecurity is defined as a process of protecting systems, networks, and software against digital attacks that typically aim to access, alter, or destroy sensitive information to seize money from users or control it and prevent the owner from using it. Cybersecurity is a challenge today because there are more devices than people, and attackers are becoming more innovative(Aleessawi, 2024).

*Cybercrime. Cybercrime is defined as “the illegal usage of any communication device to commit or facilitate in committing any illegal act.” Also, it is defined as "a type of crime that targets or uses a computer or a group of computers under one network for harm."(Cybertalents, 2023).

**Digital transformation*: Digital transformation is the process of applying digital technologies to renew the way business is done and to perform and deliver new value(Faraj, 2021). Digital transformation is the process of utilizing digital technologies to either create new or alter existing business processes, culture, and overall customer experience to meet the changing business and market requirements. Also, it is a business reimaging process of surpassing all traditional roles of sales, marketing, and customer service(Ris & Puvača, 2024).

Literature review

The study relied on the digital theory that is consistent with the digital development revolution, as this is the only theory that communication and media researchers have agreed is a theory applied to the new electronic media. With the transformation of traditional media to digital, the theory of digital transformation emerged and was developed by researcher Roger Fidel through his book: Media Morphosis, Understanding the New Media. This theory was given the name (Fidler’s approach) to understand the new media accurately(Fidler, 2012), as Fiedler explained the process of radical change that takes place in existing means is called media morphosis. It is a term that Fiedler himself coined in the early 1990s, to indicate the complete transformation taking place in the means of communication imposed by the complex interactions of basic needs, political and social pressures, and technological innovations. Fiedler also demonstrated that all forms of communication are linked. Some of them are tightly woven into the fabric of the human communication system, and they cannot be independent of each other.

This theory assumes that the existing media evolves when a new media outlet appears, as each media works in a way that is closer to the work of the elements forming a vital system, and its development is linked to the development of the media. The theory also explains the relationship between traditional and new media(Bin Trad & Bouza, 2020).

The scientific heritage related to Arab and foreign cybersecurity was reviewed, and the researchers found several studies related to the subject of this study. Nyinkeu et al. (2018) touched on the concepts of cybersecurity and cyber violations that should be promoted among university students. Interviews were conducted with members of the sample. The study showed the need to enhance Internet security and educate students about the concepts of cybersecurity and societal risk. The study recommends the necessity of including Cyber education in academic courses. For their part, Herath et al. (2022) identified the factors that affect online users’ awareness of the security-related features of social media platforms. They adopted an inductive approach through a systematic literature review and aspects related to cyber threats. Cyber awareness, and cyber behavior in using the Internet and social media were considered in the study. The study found that there are many cyber threats present within the social media platform, such as loss of productivity, cyberbullying, cyberstalking, identity theft, social information overload, inconsistent personal branding, damage to personal reputation, data breach, software Malware, service interruptions, hacks, and unauthorized access to social media accounts. The study found that cyber awareness affects cyber behavior (Herath et al., 2022).

Mohamed Alsayyed (2021) clarified the role of media content in achieving security awareness and the impact of media content in achieving intellectual security. This descriptive study was applied to a purposive sample of media and information technology professors and experts in the colleges of media and engineering. The study concluded that organizations must understand the threat landscape to develop media content security strategies against any electronic penetration, and the security of media content has become a major priority for every individual in society who defends networks, data, and computers against Violations of protection against unauthorized cyber damage. Securing content from theft is important to protect media content and is extremely important for building audiences that support the media business model considering Egypt’s 2030 vision.

Regarding the reasons for enhancing the culture of cybersecurity considering the digital transformation, Faraj (2021) concluded that the reason for strengthening the culture of security is teaching cybersecurity at the university in light of the digital transformation at Prince Sattam bin Abdulaziz University. From the point of view of the faculty members, Abdul Aziz received an overall average of (3.55 out of 5), meaning an average degree. As for the axes, the societal reasons for enhancing the culture of cybersecurity considering the university's digital transformation received the highest average (3.70), followed by the cognitive reasons for enhancing the university's cybersecurity culture, which received an average of (3.51), and the technical reasons axis, which received an average of (3.46). The results also showed that there were no statistically significant differences depending on the college variable and academic rank, while differences were found due to the years of experience variable. The study recommends the importance of raising awareness of cybersecurity among students realizing the benefits of software available to combat cyber risks and designing protection to raise awareness of cyber risks.

Al-Manea (2022) identified the reality of achieving cybersecurity in Saudi universities in light of Vision 2030. The researcher used the descriptive analytical approach, and one of the most important findings of the study is that the sample members agreed to a moderate degree on the reality of achieving cybersecurity in Saudi universities in light of Vision 2030, the sample members agree to a very large extent about the obstacles to cybersecurity in Saudi universities in light of Vision 2030. The most important of these obstacles is the low level of experience among employees, and the weakness in cooperation between technology employees in universities to achieve cybersecurity in Saudi universities in light of Vision 2030. 2030. The study also showed that there is a very large agreement among the members of the study sample on the requirements for achieving cybersecurity in Saudi universities in light of Vision 2030. Among the most important proposals adopted by the study are Educating workers about the dangers of using personal devices represented by mobile phones to transfer and store confidential information related to the university and developing material and moral incentives to support and encourage creative employees in the field of cybersecurity.

Al-Otaibi (2020) revealed how the electronic press deals with cybercrime in the Kingdom of Saudi Arabia by identifying the type of security issues, revealing the type of cybercrime, and identifying the journalistic arts that dealt with it, and to achieve the goal of the study Using the descriptive analytical approach by applying the content analysis tool to newspapers Saudi Electronic Newspaper (Sabq – A'jil - Al-Muwatin) The study concluded that A'jil newspaper was published to publish news of cybercrimes, then Sabq and finally Al-Muwatin. Cyber issues were at the forefront of security issues, then social and health issues, and cybercrimes were numerous Cyber, starting with public morals, then recording calls and photographing without permission. The study recommended the importance of educating young people to deal with electronic risks and threats.

Catota et al. (2019) explored the challenges faced by the higher education system in Ecuador in advancing cybersecurity education. Based on the insights gained, the study focused on cybersecurity education for information technology (IT) students, including undergraduate and graduate students in Computer Science (CS) and Computer Networks (CN) programs Factors preventing the initiation and improvement of cybersecurity education in institutions. The development of cybersecurity education is grounded in standards and capabilities that are expected to already exist, including ACA demic programs with strong connections to societal needs, academic infrastructuralism, and a solid research structure. Because Ecuador is still in the early stages of developing such structures, addressing cybersecurity represents a particular challenge. Universities are constrained in the ability to create academic education (i.e., training courses) which is why there is a lack of formally educated faculty in the field of cybersecurity also as technical resources. Integration between academia and business is a serious problem, especially in large cities, which prevents steps (e.g., understanding demand) from being taken to promote development. Developing a cybersecurity workforce is a challenge for many countries.

Burton-Howard & Jordan (2018) aimed to know the difficulties facing managers specializing in information security in protecting information and commercial data, in addition to the extent of protecting intellectual property from security violations and intrusions carried out by hackers over the Internet. The researcher used a qualitative approach through Conducting interviews with (10) managers specialized in information security systems in the state of Washington, America. Among the most important findings of the study were the weakness of the laws used in protecting data and information via the Internet and the weakness of effectiveness, in addition to the lack of a clear application mechanism related to security systems. This is due to the diversity and complexity of Information crimes and security breaches and their constant development. From a practical standpoint, Moskal (2014) indicated the importance of developing a vision for establishing a cybersecurity center at an American university to increase awareness of cyber risks to achieve security in cyberspace. The study was conducted on (100) American universities to determine the extent of interest in teaching cybersecurity and recommended the study emphasizes the need to pay attention to cybersecurity as it is one of the most important pillars of the American economy.

The literature reviewed has emphasized the importance of knowledge of the concept of cybersecurity and the challenges it faces, especially in universities, and this is what was confirmed by Moskal(2014). It focused on the importance of developing a vision for establishing a cybersecurity center at the American University, to increase awareness of cyber risks to achieve security in cyberspace. Faraj (2021) also indicated the importance of raising awareness of cybersecurity among students and realizing the benefits of software available to combat cyber risks, Al-Manea (2022) indicated that the sample members agreed to a very large extent about the obstacles to cybersecurity in Saudi universities in light of Vision 2030, Among the most important of these obstacles is the low level of experience among employees, and the weakness in cooperation between technology employees in universities to achieve cybersecurity in Saudi universities in light of Vision 2030. The study also showed that there is a very large agreement among the members of the study sample on the requirements for achieving cybersecurity in Saudi universities considering Vision 2030. Burton-Howard & Jordan (2018) showed that the weakness and effectiveness of the laws used to protect data and information via the Internet, in addition to the lack of a clear application mechanism related to security systems, is due to the diversity and complexity of information crimes and security breaches and their constant development. Al-Otaibi (2020) also stressed the importance of educating young people to deal with electronic risks and threats.

Cybersecurity concept

At its most basic level, cybersecurity can be understood as confidentiality, integrity, and availability(Olejnik & Kurasiński, 2023): Confidentiality: This means the confidentiality of information and its preservation by granting permission to those authorized to access information and data and preventing it from persons who are not authorized to access that information while ensuring that it is not modified, leaked, or disclosed to persons who are not authorized to do so. Integrity and integrity of information: This means preserving information from modification, change, deletion, or addition except by the persons supervising and specializing in this content. Amending information and making it available: This means the availability of information by specialized persons supervising its provision on time.

The security and defense policies of countries have become linked to their ability to employ digital actors in confronting internal and external crimes, which requires clarifying the concept of cybersecurity and its impact on national security. Bougerara (2018) defined it as a set of technical and administrative means that are used to prevent unauthorized use of computer networks. Or misuse and recovery of the electronic information it contains to ensure and continue the operation of information systems and ensure the protection, confidentiality, and privacy of data belonging to cyberspace actors. Accordingly, the necessary measures must be taken to protect against threats and intrusions and to prevent attacks on computer networks, electronic information, and information systems. As defined by the International Telecommunication Union in its report on trends in telecommunications reform for the year 2010-2011, it is, “a set of tasks such as compiling security methods, policies and procedures, guidelines and risk management approaches, training, best practices and techniques that can be used to protect the cyber environment and the assets of organizations and users.” As defined by the European Digital Security Agency in its first legislation issued in 2001, it is: “the ability of the information system to resist attempted hacking or unexpected incidents targeting data circulated or stored according to a consensus framework.” To achieve the desired security, nationally, regionally, and internationally. Where the concept has emerged in criminal and political security law thought, the concept of cybersecurity adds two dimensions, a legal dimension related to the means of legal protection from everything that would constitute a crime, and a political dimension that falls within the framework of internal and external security policy, and what it requires in terms of strengthening the means and tools of defense, between the state. And various sectors(Jilani & Yaqoub, 2021).

Characteristics and requirements of cybersecurity

Cybersecurity comes to overcome systematic cybercrimes, and therefore cybersecurity has several characteristics, the most important of which are (Al-Manea, 2022):

- Detection and tracking: Cybersecurity aims to detect electronic crime, track its impact, and overcome it.
- Speed and lack of evidence: The difficulties of proving cybercrimes are represented by the hackers' use of modern and constantly evolving technical means, so cybersecurity needed to come up with modern techniques that exceed their techniques and experience.
- The weakness of the security and judicial agencies in dealing with cybercrimes; This is due to the lack of digital expertise among security services, which enhances the role of cybersecurity in achieving digital security for institutions and universities in protecting data and infrastructure.

Cybersecurity requirements include defining security procedures in information networks regarding what is permissible and what is not permissible about information security, providing the necessary mechanisms to implement work policies and how to work with them, determining penalties in the event of breaches, and paying attention to the operation of information networks by human elements trained and qualified to deal with technologies. Modern technology, in addition to the importance of monitoring information activities to discover suspicious activities within the scope of the network (Aleessawi, 2024).

Cybersecurity Challenges at Higher Education Institutions

The universities have distinct cybersecurity concerns intensified by intricate network infrastructures, departmental divisions, and a heterogeneous user population. These universities must address a wide range of cybersecurity vulnerabilities that may jeopardize research integrity, student privacy, and institutional reputation. These challenges are(Hernandez, 2024):

- Advanced Persistent Threats (APTs): A significant and complicated cybersecurity issue for higher education organisations. These threats are typified by their hidden, long-term nature and the high skill of their instigators, either state-sponsored or associated with well-funded criminal businesses. APTs target colleges and universities because they have plenty of personal, financial, and scientific data. Several APT attacks targeting espionage and IP theft have weakened these organisations' ability to secure sensitive data and maintain confidence.
- The wide and distributed network infrastructures of schools and universities might lead to security vulnerabilities, particularly through broader network access points. If poorly secured, these schools' campus Wi-Fi networks and remote access services can be accessed by unauthorised parties. The large number of users and devices needing access to these networks—students, instructors, staff, and visitors—makes monitoring and protection challenging.
- Financial constraints are common in school IT departments at all levels of education. However, K-12 schools and universities have different reactions, with universities having more flexibility to deploy IT resources.
- Regulatory Obligations: Universities and their student data management systems must comply with strict data privacy laws like FERPA, which requires good cybersecurity.
- Rebellious Students: Unauthorised users can engage in pranks, cyberattacks, and academic record infiltration through university IT systems. Their insider knowledge threatens educational institutions' security and integrity. These breaches can damage these organisations' reputations for data security and disrupt instruction. Institutions may take numerous approaches: Enforce stricter access limits, monitor network activities, and define infringement penalties.
- The BYOD movement in higher education complicates cybersecurity efforts by integrating personal devices into university networks, opening new cyber attack options. These devices require strong security measures to prevent unauthorised access and data breaches. Effective methods include a complete BYOD policy that outlines security protocols, network access control systems to segregate and monitor network access, and continuous security training to teach users best device management practices.

Protect against cyberattacks

Educational institutions must protect data actively to reduce cybersecurity risks(StrongBox IT, 2024):

- Regular Risk Assessments: Assess system security to find vulnerabilities and fix them quickly.
- Give Security Awareness Training: Regularly educate students, instructors, and staff about phishing schemes, strong passwords, and other cybersecurity recommended practices.
- Apply Access Control: Follow the concept of least privilege by restricting user access permissions to the minimum needed for their job duties and constantly reviewing privileges.
- Secure Devices and Networks: Install firewalls, encrypt data, protect Wi-Fi networks, and safeguard all networked devices.
- Backup Data Regularly: Backup vital data regularly and test recovery techniques to assure data recovery following a cybersecurity event.
- Detect Suspicious Network Activity: Use network monitoring tools and services to spot and address suspicious conduct that may signal a security breach.
- Plan and Test Incident Response: Create a robust security response plan and perform frequent exercises to ensure everyone knows their responsibilities.

Digital transformation and cybersecurity

The digital communication technology revolution that was witnessed in the second half of the twentieth century brought about major transformations in the political, economic, and social fields. The continuous development of the Internet, which has entered its fifth generation, contributed to the ease and speed of its spread globally and made it an essential means of expressing freedom of opinion in the first century. As of 2022, 69% of the world’s population, or 4.9 billion people, actively use the Internet. Trends indicate that the number of Internet users grows at an annual rate of 4%, meaning that roughly 196 million new people access the Internet each year(World Population Review, 2024).

The Internet represents a communication umbrella that brings together communication systems, their forms, and various digital functions and functions in one system that provides the recipient with multiple options. The concept of digital communication has been closely linked to the concept of digital media, which Abdelhameed (2007) defined as “the process of social communication “in which communication takes place remotely, between parties who exchange roles in broadcasting various communication messages and receiving them through digital systems and means to achieve certain goals.” Technically, the word digital means that the letters, images, and sounds contained in the communication messages are transformed into digital data Ones and zeros (01) can be stored, processed, and sent by computers, and Aho (2005) defines digital communication as “the basic skill for most work that an individual must acquire within the framework of the concepts, production, delivery, and reception of means of communication in their jobs and lives, as digital communication is The ability to create effective communication through various digital means.

With the growth of the technological and information revolution and the digital media industry, the public transformed from a passive recipient to a positive recipient. Many legal and ethical problems emerged and became numerous and complex as a result of the free flow of information and the ease of citizens’ access to social media networks, the lack of limits of time and place, and the absence of censorship, which necessitated the need to reconsider Media legislation to confront the new challenges resulting from the use of digital media, which did not stop at compromising the rights of individuals, but rather threatened the safety and security of the state through threatening messages, hate speech, spreading rumors, provoking citizens, manipulating the content, and exploiting information systems and electronic communication systems(Mohamed Alsayyed, 2021). Many legal frameworks and professional and ethical controls have monitored the process of online publishing, based on social responsibility, copyright, and intellectual property rights. Mechanisms have been identified that can be relied upon for self-regulation, setting possible rules for application, and amending legislation to suit developments in communication technology and development. The level of awareness of the dangers of these methods and commitment to the ethics of their use requires a mechanism to prevent the spread of misinformation and manipulation (Zhang et al., 2017).

Methodology

Method

The article adopted the descriptive method, used a survey approach that is based on collecting data and facts, classifying, and classifying them, in addition to analyzing them with sufficient and precise analysis, and it also includes some degree of interpretation of results.

The population and sample size

The study population is represented by (120) professors of curricula and methods[1] at Jordanian universities in the academic year 2023-2024, while the study sample consisted of (55) professors; (40) males and (15) females. According to universities, (12) from (250) at Middle East University, (13) from (270) at the University of Petra, (13) from (230) at the University of Applied Sciences, (17) from (138) at Amman Arab University.

The reason for choosing the professors of curricula and methods to represent the study community is that they are the exact subject of the study and the problem is to study the extent of university professors' awareness of the use of cybersecurity in teaching academic subjects and programs, and that professors of curricula and methods are more responsible for knowing the cybersecurity environment because they are concerned with providing students with teaching, receiving and education skills and methods and how to deal with challenges. Although the study community is specific and known, communicating with them was not easy, so a snowball sample was used to obtain sufficient responses to achieve the study objective.

Here, a snowball sample is done on the basis that the group is asked to help identify other groups, where the first individual who meets the conditions is considered the starting point for the completion of the ball (sample completion), as it is done through dialogue, or belonging to the same group, country, specialty, and profession, and they have the same characteristics that relate to the subject of the study, in this way, the number required to reach the sample size is met. This is the reason for the name “snowball,” as the first individual is the first point around which condensation will begin to complete the ball, i.e. complete the sample(Tammar, 2010, p. 32).

- *Middle East University, MEU:* The Middle East University was established in 2005 as a university for graduate studies, in a distinguished location in the capital, Amman, a few kilometers from Queen Alia International Airport. The university includes two types of academic programs offered by nine colleges: The first: the master’s program that was organized at the university at the beginning of the second semester of the academic year 2005/2006, with many specializations, currently eleven specializations, in which master’s degrees were awarded to more than 2,978 male and female students. The second is the bachelor’s program, which began its academic career in the academic year 2008/2009, with many specializations, currently twenty-one specializations, in which bachelor’s degrees were awarded to more than 4,214 male and female students (Middle East University website).
- *University of Petra, UOP:* The University of Petra is one of the leading educational institutions in the Hashemite Kingdom of Jordan. The university was established in 1991 and is located in the West Amman region. The university’s campus includes thousands of students from different parts of the world in bachelor’s and master’s programs in the colleges of: Arts and Sciences, Administrative and Financial Sciences, Pharmacy, and Medical Sciences, Information Technology, Design and Architecture, Law, Media, Engineering, and Dentistry. The university is distinguished by its uniqueness in providing a modern and advanced educational environment that combines theoretical and applied education. In addition to academic programs, the university also enhances the importance of research and skills development to meet the challenges of the modern world and encourages the transfer of technology and knowledge to the local and global community. The University of Petra represents a distinguished educational center that always seeks to provide high-quality education and contribute to the development of knowledge, scientific research, and community development(Petra, 2024a).
- *Amman Arab University, AAU:* Amman Arab University was established in 1997 by Higher Education Council Resolution No. (1476) dated 11/24/1997, as a private, non-profit university specializing in postgraduate studies, under the name “Amman Arab University for Postgraduate Studies.” To be the first Jordanian university to specialize in graduate

[1] The authors got these data through direct contact with the human resources departments at universities.

programs for master's and doctoral studies. On September 30, 1998, the Higher Education Council approved the university to begin teaching by its Resolution No. (1625), as the university received its first group of students since the beginning of the second semester of the academic year 1999/200. The university's journey passed in two stages; The first; it was limited to postgraduate programs. The second: It began in 2009 when the university's progress was strengthened by opening bachelor's degree programs, and the university's name was changed to "Amman Arab University."

- *University of Applied Sciences, UAS:* The university began its educational career on 10/19/1991 AD, after obtaining its license on 7/10/1989 AD. The number of registered students at that time was (553) male and female students, and the number of colleges in which study began was three colleges: Arts, sciences, and economics, and included (13) specializations.

Data collection

The questionnaire served as a tool for data collection because it has a series of connected and sequential questions that respondents fill out and answer to provide information and data about the phenomenon or research problem. A five-point Likert scale was adopted to determine the length of the sampling unit's answer category (strongly agree, agree, neutral, disagree, strongly disagree), and the following weights were adopted: weak 1 - 2.33, average 2.34 - 3.66, high 3.67 – 5).

Since the population is known and almost specific, the questionnaire was sent electronically (link) to some Jordanian university professors, so that each respondent could send it to another professor with whom he has contact or knows, provided that he is part of the study community. Since the questionnaire form was electronic, the responses came automatically to the researchers in an Excel file generated from the electronic link. Then the statistical operations on the responses began using the SPSS program in addition to the Excel program.

Results

Awareness of Cybersecurity

Table (1): Sample responses about academics' awareness of cybersecurity

#	Item	Mean	S. D.	Rank	level
4	There is an organized cyber war globally	3.7273	.91195	1	High
1	The concept of cybersecurity is clear	3.6182	.97165	2	middle
5	Most communication applications do not consider the hedges of cybersecurity	3.2364	.92223	3	middle
2	Reading articles and studies on cybersecurity	3.2182	1.08339	4	middle
3	Watching special videos about cybersecurity	3.0909	1.04124	5	middle
6	There is exaggerated and no need to be very cautious	2.2364	.98062	6	low
	Total mean	3.1879	.56570		middle

Source: Spss results

The table above shows that one of the professors' awareness perceptions is "There is an organized cyber war globally" with a mean (3.72) and a standard deviation (0.911) within the high level. It is followed by "The concept of cybersecurity is clear" with a mean (3.61) and standard deviation (0.971) within the middle level. The third level, "Most communication applications do not consider the hedges of cybersecurity" comes with a mean (3.23). On the last level, the professors think "There is exaggeration and no need to be very cautious" with a mean (2.23) at a low level.

Sources of information about cybersecurity

As for how the professors tracked cybersecurity information, (29.1%) of them relied on more than one method; Facebook, WhatsApp, Instagram, YouTube, websites, and television, while (23.6%) of the respondents depended on "Facebook," and the following figure shows this:

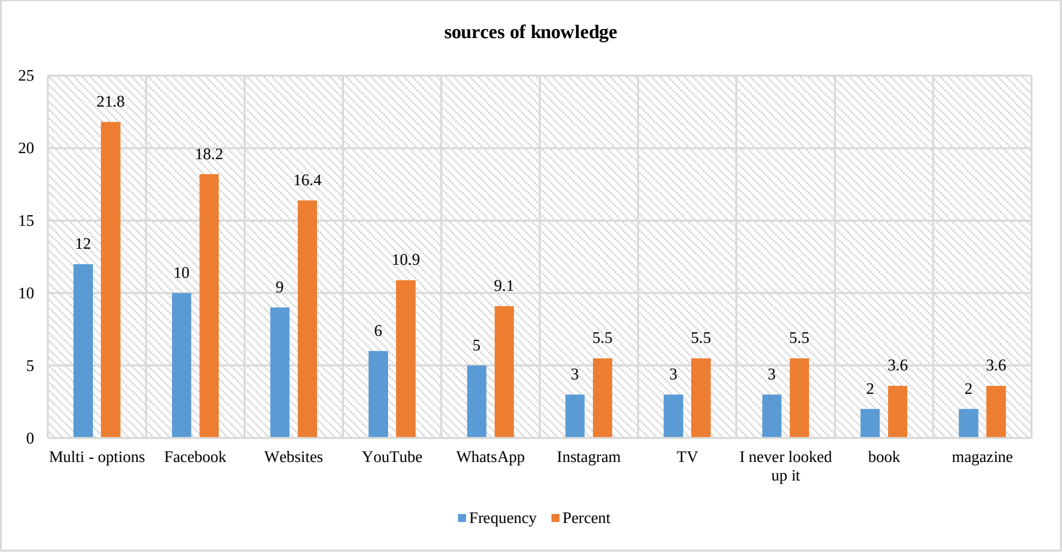

Figure (1): The sample's sources of information about cybersecurity

Source: Spss results

Hacker's Motivations

Regarding the most common motives for violating cybersecurity, (36.4%) of academics confirmed that the most prominent motive is "money," that is, blackmail, embezzlement, and fraud, followed by "information" with (21.8%). (10.9%) answered that there are multiple motives for hacking. The motives of "counterfeiting" and "sabotage and terrorism" received (9.1%) each, and the following figure shows this:

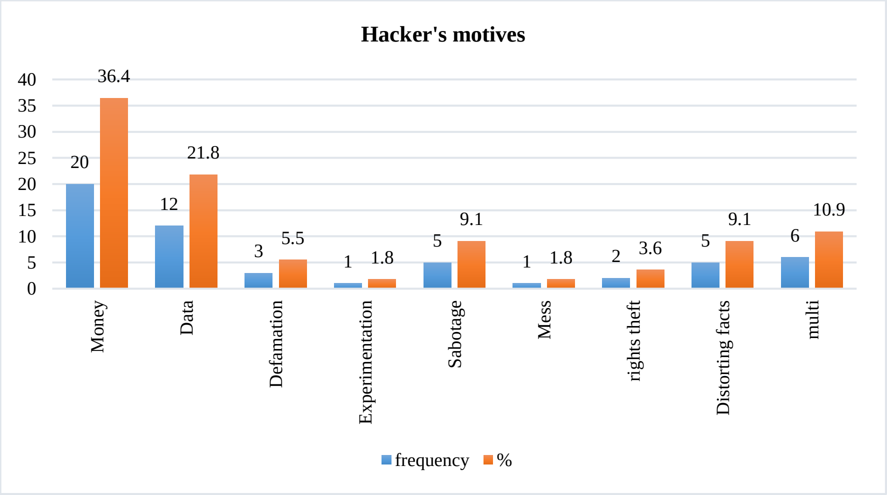

Figure (2): The sample's views towards Hacker's motivations

Source: Spss results

Skills in Cybersecurity

Table (2): The academics' skills and procedures in cybersecurity

#	Item	Mean	S. D.	Rank	level
2	Taking precautionary steps in receiving emails	3.8909	.85359	1	High
3	Verifying accounts on websites	3.6545	1.00403	2	middle
4	Teaching students about cybersecurity as a part of my lectures	3.3636	1.02494	3	middle

#	Item	Mean	S. D.	Rank	level
1	Having experience with cybersecurity procedures on my devices	2.9273	.99730	4	middle
5	Hosting professionals to give lectures on cybersecurity	2.8909	1.04833	5	middle
	Total mean	3.3455	.75567		middle

Source: Spss results

The table above shows that one of the most prominent aspects of academics' skills in cybersecurity is "Taking precautionary steps in receiving emails" with a mean (3.89) and standard deviation (0.853) within the high level. Following this, "verifying accounts on websites," with a mean (3.65) and standard deviation (1.00) within the average level. The last procedure is "Hosting professionals to give lectures on cybersecurity" with a mean (2.89).

Verification method of accounts

Regarding the mechanisms for documenting accounts, the teachers indicated that they resort to "more than one option," that is: a phone number, official authentication, a complex password, and an alternative email. "Phone number" had a (23.6%), and "complex password" had a (21.8%). On the other hand, there were (14.5%) of academics who do not verify their accounts in any way, and the following figure shows this:

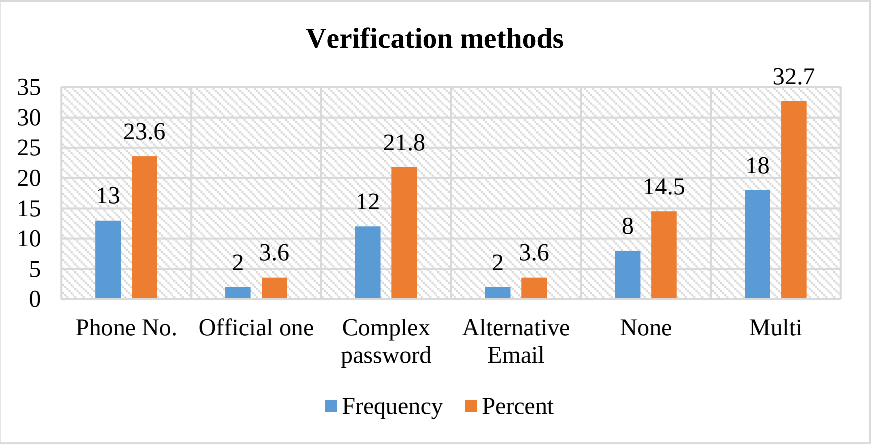

Figure (3): The sample's Verification method of accounts

Source: Spss results

Challenges of Cybersecurity

Table (3): The challenges facing professors in enhancing awareness of cybersecurity

#	Item	Mean	S. D.	Rank	level
3	Scarcity of cybersecurity awareness workshops and seminars by the university	3.7091	.97511	1	High
1	Reluctance to keep pace with rapid transformations in the field of hacking	3.6364	.80193	2	middle
2	limited time due to teaching hours, which causes a lack of focus on cyber precautions	3.6000	.85201	3	middle
4	There is no department or employee specialized in cybersecurity in the Information Technology Department	3.1455	1.12905	4	middle
5	Believing it's not worth it	2.1091	.99392	5	low
	Total mean	3.2400	.57012		middle

Source: Spss results

The table above shows that one of the most prominent challenges facing academics in Jordanian universities to enhance awareness of cybersecurity is " Scarcity of cybersecurity awareness workshops and seminars by the university" with a mean (3.70) and a standard deviation (0.975) within the high level. It is followed by " Reluctance to keep pace with rapid transformations in the field of hacking" with a mean (3.63) and a standard deviation (0.801) within the middle level. The professors added that "the limited time due to teaching hours" is another challenge that does not focus on cyber precautions, adding that "no department or employee specializes in cybersecurity in the Department of Information Technologies." The last challenge is “Believing it's not worth it” with a mean (2.10) at a low level.

Enhancing Awareness of Cybersecurity

To enhance awareness about cybersecurity, (56.0%) of professors asserted the need to provide workshops and courses for cybersecurity for university professors, while (26.0%) drew attention to the importance of carrying out general awareness campaigns for society and institutions, in exchange for (18.0%) he pointed out the importance of including or allocating study courses on cybersecurity for all disciplines as in the following figure:

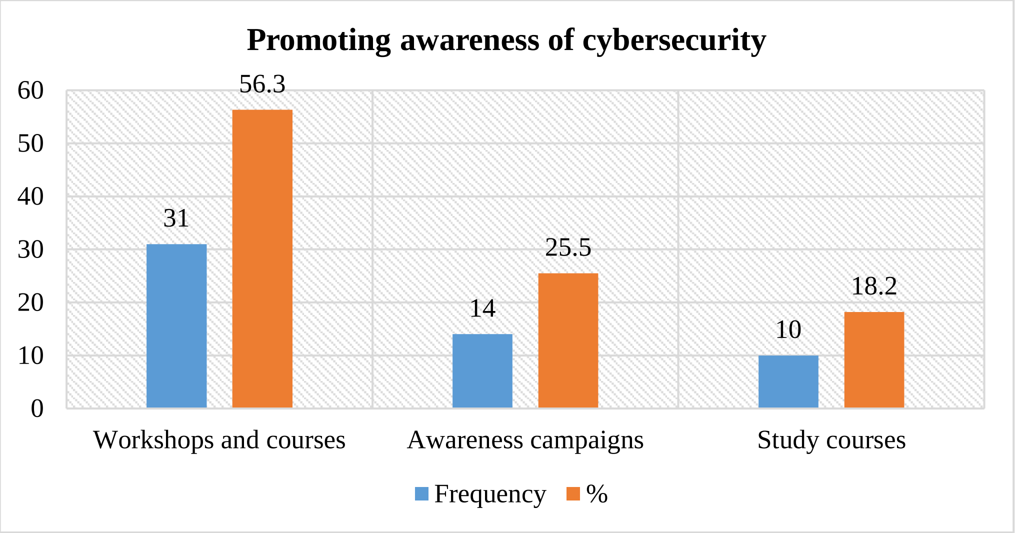

Figure (4): The Promoting Awareness of Cybersecurity

Source: Spss results

Discussion

According to the theory of digital transformation, the process of radical change that takes place in existing media, as expressed by Fidler (2012), reveals the impact of complex interactions of basic needs, political and social pressures, and technological innovations, to indicate the complete transformation taking place in technological innovations and means of communication. This tremendous transformation has led most teaching elites to believe that there is an organized cyber war at the level of countries around the world, and this change and openness have prompted them to become familiar with the concept of cyber security and realize its importance.

Moreover, the results indicated that most communication applications do not consider the hedges of cybersecurity, and this is consistent with what was indicated by the study by Herath et al. (2022), which proved that there are many cyber threats present within social media platforms, such as loss of productivity, electronic bullying, online stalking, and theft. Identity, social information overload, inconsistent personal branding, damage to personal reputation, data breach, malware, service interruptions and hacks, and unauthorized access to social media accounts. It is displayed that professors read information related to cybersecurity, and viewed videos on websites, Facebook, WhatsApp, Instagram, YouTube, and television. The teachers discovered that the most common motives for violating cybersecurity are attempts at blackmail, theft, and obtaining information, and to a lesser extent, counterfeiting, sabotage, and terrorism.

The professors' skills and procedures related to cybersecurity are by taking precautionary steps in receiving e-mails and authenticating their accounts on websites with more than one option, mainly using the phone number followed by official authentication, a complex password, and an alternative e-mail.

The biggest challenges facing professors to enhance awareness of cybersecurity is the lack of awareness workshops and seminars held by the university for professors, and thus the low level of knowledge. This was confirmed by the responses of the respondents regarding the most important visions and proposals to enhance awareness of cybersecurity, as most of them stressed the necessity of providing workshops and courses on cybersecurity. For university professors, as Mohamed Alsayyed (2021) confirmed by calling for the need for institutions to understand the threats and develop security strategies against any electronic penetration. In this context, Al-Manea (2022) indicated the low level of experience among employees, and the study suggested educating employees about the dangers of using personal devices such as mobile phones to transfer and store confidential information related to the university and granting material and moral incentives to support and encourage creative employees in the field of cybersecurity.

In general, the findings agreed with Burton-Howard & Jordan (2018), and Catota et al. (2019) that emphasize the necessity of confronting cognitive challenges first, and technical challenges second, and enhancing Awareness among teachers and students alike. Nyinkeu et al. (2018) and Moskal (2014) also indicated the necessity of clarifying the concepts of cybersecurity and cyber violations that should be reinforced among university students and developing a vision for establishing a cybersecurity center at the university to increase awareness of cyber risks.

Conclusion

The level of awareness of cybersecurity is a fundamental issue for intellectual and national security, and university professors are important elements in educating society and enhancing the knowledge and technical aspects of cybersecurity in society. It was evident through the results that there is an organized cyber war globally, that communication applications do not consider the necessities of cybersecurity, and that the websites, Facebook, YouTube, and WhatsApp are among the most important means of providing cybersecurity information. It also appeared that one of the most common motives for violating electronic security is an attempt to blackmail and theft, obtain information, and to a lesser extent forgery and sabotage. The teaching skills were limited to taking precautionary steps in receiving emails and striving to document their accounts on websites with more than one option, but the most prominent challenge was the lack or lack of awareness activities that the university holds for professors and employees.

Recommendations

Based on the above, we recommend that universities adopt the establishment of a special department for cybersecurity whose mission is to provide workshops and seminars approve cybersecurity courses, and present them within university programs. Also, we recommend professors host cybersecurity specialists regularly to provide professors and students with information on cybersecurity.

REFERENCES

Abdelhameed, M. (2007). *Communication and Media on the Internet* (1st ed.). The Books World.

Aho, K. (2005). Teaching Digital Communication to All Students. *T H E Journal*, 32(10).

Aleessawi, N. (2022). Using the Digital Platforms by Journalists of the Middle East and North Africa (MENA) in Promoting Common Human Values. *Dirasat: Human and Social Sciences*, 49(5), 454–465. https://doi.org/doi.org/10.35516/hum.v49i5.3494

Aleessawi, N. (2024). *Cybersecurity*. Media and Public Relations. https://najmaleessawi.blogspot.com/

Al-Manea, A. A. R. (2022). Requirements for achieving cybersecurity in Saudi universities in light of Vision 2030. *Faculty of*

Education Journal, 38(1), 156–194.

Al-Otaibi, M. (2020). *Electronic journalism's treatment of cybersecurity crimes in the Kingdom of Saudi Arabia, content analysis study* [Master's thesis]. Naif Arab University for Security Sciences.

Bin Trad, W., & Bouza, B. (2020). Theoretical frameworks that explain network media between effectiveness and limitation. *Maalem Journal for Media and Communication Studies*, 1(1), 44–77. https://www.asjp.cerist.dz/en/article/150327

Bougerara, Y. (2018). Cybernetic Security : The Algerian strategy of security and defense in cyberspace. *Journal of African and Nile Basin*, 1(3), 100–119.

Burton-Howard, V., & Jordan, L. (2018). *Protecting Small Business Information from Cyber Security Criminals: A Qualitative Study*. http://chain.kent.ac.uk/login?url=https://www.proquest.com/dissertations-theses/protecting-small-business-information-cyber/docview/2133581243/se-2?accountid=7408%0Ahttps://chain.kent.ac.uk/login?url=https://resolver.ebscohost.com/openurl?sid=&genre=disse

Bynum, T. W., & Rogerson, S. (2003). *Computer Ethics and Professional Responsibility* (1st ed.). Wiley-Blackwell.

Catota, F. E., Granger Morgan, M., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. *Journal of Cybersecurity*, 5(1). https://doi.org/10.1093/cybsec/tyz001

Cybertalents. (2023). *What is Cybercrime? Types, Examples, and Prevention*. Cybertalents. https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention

Faraj, A. O. K. (2021). The Reasons for Promoting Cyber Security Culture in Light of Digital Transformation Prince Sattam Bin Abdulaziz University as a Model. *Educational Journal*, 94(1).

Fidler, R. (2012). *Mediamorphosis: Understanding New Media*. SAGE Publications, Inc. https://doi.org/10.4135/9781452233413

Herath, T. B. G., Khanna, P., & Ahmed, M. (2022). Cybersecurity Practices for Social Media Users: A Systematic Literature Review. *Journal of Cybersecurity and Privacy*, 2(1), 1–18. https://doi.org/10.3390/jcp2010001

Hernandez, J. (2024). *Cybersecurity challenges in education*. https://preyproject.com/blog/cybersecurity-challenges-in-education

Himma, K. E., & Tavani, H. T. (2009). The Handbook of Information and Computer Ethics. *In The Handbook of Information and Computer Ethics*. https://doi.org/10.1002/9780470281819

Jilani, D., & Yaqoub, B. (2021). Bets of National Cybersecurity in Light of Digital Transformation, A Reading of Cognitive Rooting and Legislative Confrontation Strategies. *Journal of the Kuwait International College of Law*, 1(37).

Alsayyed, M. N. (2021). Cyber Security and Its Relationship to Media Content in Light of Egypt's Vision 2030. *Arab Journal of Media and Communication Sciences*, 2021(35), 484–514. https://doi.org/10.21608/jkom.2021.226471

Moskal, E. J. (2014). A model for establishing a cybersecurity center of excellence. *2014 Proceedings of the Information Systems Educators Conference, ISECON 2014*.

Nyinkeu, N. D., Anye, D., Kwedeu, L., & Buttler, W. (2018). Cyber Education outside the Cyberspace: The case of the Catholic University Institute of Buea. *International Journal of Technology in Teaching and Learning*, 14(2). https://doi.org/10.37120/ijttl.2018.14.2.04

Olejnik, L., & Kurasiński, A. (2023). Philosophy of Cybersecurity. In *Philosophy of Cybersecurity*. https://doi.org/10.1201/9781003408260

Petra. (2024). *The University of Petra*. UOP. https://www.uop.edu.jo/ar/pages/default.aspx

Petra. (2024). *Jordan Develops Advanced Infrastructure with Cybersecurity Law*. Petra. https://www.petra.gov.jo/Include/InnerPage.jsp?ID=285846

Ris, K., & Puvača, M. (2024). *Digital Transformation Handbook* (1st ed.). CRC Press, Taylor & Francis Group.

Shea, S., & Gillis, A. S. (2024). *The ultimate guide to cybersecurity planning for businesses*. Tech Accelerator. https://www.techtarget.com/searchsecurity/definition/cybersecurity

StrongBox IT. (2024). *The Role of Cybersecurity in Schools and Universities* . StrongBox IT. https://www.linkedin.com/pulse/role-cybersecurity-schools-universities-strongbox-it-pvt-ltd-jpdte

Tammar, Y. (2010). *Sample in Communication Media Studies*. Baghdadi for publishing.

World Population Review. (2024). *Internet Users by Country 2024*. Worldpopulationreview. https://worldpopulationreview.com/country-rankings/internet-users-by-country

Zhang, Y., Li, M. D., & Zhang, H. B. (2017). Solution of Media Risk and Social Responsibility Governance of Social Media. *ITM Web of Conferences*, *11*, 01007. https://doi.org/10.1051/itmconf/20171101007