



The Level of Cybersecurity Awareness and Cybercrime Response among Internet Users in Algeria: A Field Study on Students of the Faculty of Humanities and Social Sciences at the University of Djilali Bounaam in Khamis Miliana.

Brada abderrezzaq^{1,*}, dahmani Fatima ²

¹ relizane university (Algeria), abderrezzaq.brada@univ-relizane.dz

² M'sila University (Algeria), fatima.dahmani@univ-msila.dz

Received: 19 / 05 / 2024

Accepted: 29 / 10 / 2024

Published: 30 / 11 / 2024

Abstract:

This study aims to identify and evaluate the level of cybersecurity awareness and cybercrime among Internet users in Algeria. To study the subject optimally, the descriptive field approach was used by conducting a field study on a sample of 355 university students from the University of Djilali Bounaam in Khamis Miliana, utilizing a field questionnaire tool. Ultimately, the study yielded several findings, notably: students' engagement with virtual reality and the significance of the Internet in their lives, with 53.23% using the Internet regularly and 61.97% using it for extended periods daily. There is also a growing interest in cybersecurity, with students acknowledging the importance of cyber awareness in preventing cybercrime at 46.47%. Their level of knowledge of cybercrime was found to be average at 59.15%. In terms of awareness, students recognize the need to encourage cyber incident reporting by 28.73% and provide lessons and workshops on cybersecurity by 27.60%.

Keywords: cybersecurity, cybercrime, awareness, virtual reality, university, student.

* Brada abderrezzaq, relizane university (Algeria), abderrezzaq.brada@univ-relizane.dz

I. INTRODUCTION

Technological advancements in the field of information transmission through the Internet have become pervasive. The United Nations Office has reported a significant increase in the number of individuals connected to the Internet since 2011, with the number of users rising from 2.4 billion to 60 percent of the global population, including those from developing countries. This indicates the widespread adoption of the Internet, extending beyond developed nations, facilitated by its affordability and accessibility, allowing individuals to integrate it into their monthly budgets alongside essential devices such as computers, which are crucial for engaging with virtual spaces (Milano et al., 2017, p. 1802).

Through this technological progress, a new spatial domain of social interaction, known as cyberspace, has emerged, where individuals congregate without the constraints of physical and social boundaries. This space represents a transitional phase for humans from the real world to the virtual world, resulting in the transmission of numerous phenomena and the influx of various changes impacting the field of higher education and the university community.

Additionally, these changes have introduced many new concepts and social distinctions, such as the differences between online and offline, real and virtual, physical and immaterial. Consequently, it has become imperative to consider the cyber awareness of the Algerian university community, particularly as this issue garners significant attention from international and local researchers and academics in the field of social sciences.

Moreover, technological changes have compelled researchers to migrate from physical reality in scientific research to study phenomena prevalent in the virtual world, emphasizing transformation and change within the university environment. The issue of cyber awareness has accompanied the transformation of Algerian universities and academic education following the adoption of the Internet in higher education.

However, addressing the level of cybersecurity awareness and cybercrime among Internet users in Algeria is crucial. Uncovering the changes within the Algerian university community, especially in the context of digitizing university institutions, is an essential step. The physical structure has evolved into an information system where all data is stored and managed using the Internet.

Furthermore, this transformation necessitates that university students achieve safe Internet usage, as any mishandling of digital content, such as uploading documents, lectures, or accessing the university's official websites, can expose their devices to cyberattacks or various types of cybercrime. Therefore, this study aims to determine the level of cybersecurity awareness and response to cybercrime among Internet users in Algeria.

II. The Problem

The world has witnessed rapid advancements in computer and electronic device technologies, bringing profound changes to individuals' lives and institutional operations. The use of personal computers and telephones has become essential in various fields and disciplines, particularly in scientific research and higher education in Algeria, where university institutions rely on electronic networks, including the Internet, computer systems, and digital information, to store critical and important data (Web, 2021, p. 10).

In this context, cyber threats have emerged as significant risks to the electronic networks of institutions such as universities and their human resources, including students, professors, and employees. These threats evolve rapidly, often outpacing the development of security measures designed to counter them. Between 2022 and 2023, over 4,600 cybercrime cases were reported in Algeria, encompassing blackmail, threats, defamation, violations of personal freedoms and private life through social networking sites, the dissemination of false and misleading information, hacking, harassment, and fraud. The proportion of cases affecting individual lives ranged from 65% to 75% of the cases handled, according to the Algerian National Gendarmerie (Sunrise, 2023).

The rise of such crimes in Algeria is attributed to its ongoing digital transformation. Reports such as the We Are Social & Meltwater report (2023) highlight the digital landscape in Algeria, noting that in 2023, there were 32.09 million Internet users in the country, with a penetration rate of 70.9%. Additionally, 23.95 million citizens, or 52.9% of the total population, were social media users. University students, in particular, are heavy Internet users, relying on it for social communication, scientific research, distance learning, and accessing educational content from university platforms. This extensive online engagement, often to the point of addiction, leads to various psychological and social effects (Al-Dhaban et al., 2019, p. 269).

However, the widespread use of the Internet in various aspects of Algerian university students' lives makes them vulnerable to certain types of cybercrimes, such as data theft, device hacking, and attacks on social networking sites. The lack of cyber awareness, which is crucial for protecting personal information and digital data, exacerbates this vulnerability. Students must learn to distinguish between credible information and sources online to protect themselves from fraud and misinformation. Their limited awareness of cybercrime and its dangers, resulting from uninformed Internet usage, increases their likelihood of falling victim to such crimes.

Thus, this study seeks to address the following primary question:

What is the level of cybersecurity awareness and response to cybercrime among students of the Faculty of Humanities and Social Sciences at the University of Djilali Bounaam in Khemis Miliana?

The following sub-questions will guide this investigation:

1. Does students' interaction with virtual reality unconsciously increase the risk of cybercrime and reduce cybersecurity?
2. What is the level of awareness among students regarding the concept of cybersecurity?
3. Are students aware of cybercrime online? What are the most common types of cybercrime they encounter?
4. What measures should students take to enhance their cybersecurity awareness and protect themselves from cybercrime?

1. First: The Importance of the Study

The significance of this study lies in its focus on the critical topic of cybersecurity awareness and the response to cybercrime among Internet users in Algeria. Additionally, the study is important because it explores strategies to enhance students' understanding of cybersecurity concepts and the risks associated with cybercrime. This, in turn, aims to improve their online behavior and strengthen both personal and institutional protection.

2. Second: Objectives of the Study

The study seeks to achieve several key outcomes by examining the level of cybersecurity awareness and the response to cybercrime among Internet users in Algeria, with the following specific objectives:

- Assess the level of students' awareness of cybersecurity concepts and their understanding of its importance in Internet usage.
- Understand how students' unconscious use of the Internet can increase the risk of cybercrime and diminish the level of cybersecurity.
- Identify essential steps students can take to enhance their cybersecurity practices while using the Internet.
- Evaluate students' awareness of common cybercrimes that threaten them while browsing the Internet, including electronic fraud, espionage, hacking, electronic defamation, and others.

3. Third: Study Concepts

3.1. Cybersecurity:

In Arabic, it encompasses notions of safety, preservation, trust, and seeking protection and peace (Jarraya, 2014, p. 19).

Cybersecurity is defined as the field concerned with protecting against cyberattacks from internal or external sources targeting an organization or individuals' electronic devices and media. It relies on technology to safeguard networks, servers, computers, and information connected to the Internet from unauthorized access to ensure security against cyber threats (Von Solms & Van Niekerk, 2013, p. 99).

Procedural definition of cybersecurity according to the researcher's study: It is the protection of networks and systems connected to the Internet through a set of technical and administrative measures designed to prevent unauthorized interference or infiltration of the university's electronic system. These measures ensure the confidentiality, security, and integrity of personal data for professors and students, as well as protect the university's equipment and technologies from damage.

3.2. Cyber Awareness:

Cyber awareness is regarded as the main pillar of cyberspace, allowing individuals to understand the behaviors that protect them from security breaches and electronic threats during their Internet use. It helps individuals maintain their privacy, personal data, and digital information. The higher the degree of awareness, the lower the chances of falling victim to cybercrime (Zwilling et al., 2022, p. 7).

Procedural definition of cyber awareness according to the researcher's study: Cyber awareness is defined as the level of understanding students have about information security best practices during their online activities, such as communicating through social media, blogs, and emails. It also involves students being aware of the security risks they face while engaging in these activities.

3.3. Cybercrime:

Cybercrime encompasses a range of illegal acts and behaviors punishable by law, committed by individuals known as hackers against computers and devices connected to the information technology network. These behaviors are diverse and harmful to devices, individuals' data, and privacy (Phillips et al., 2022, p. 382).

Procedural definition of cybercrime according to the researcher's study: Cybercrime represents an evolutionary stage of traditional crime, characterized by its tools and the context of its practices. It is not confined by political and geographical borders and is often highly organized, facilitated by globalization. Criminals rely on intranets and electronic media, such as computers, telephones, and electronic panels, to commit these crimes, which are recognized as offenses under Algerian law.

4. Fourth: Previous Studies

4.1. Initial Study: A study by Minal Chauhan and Arpna (2012) titled "Cybercrime Prevention: A Study on Cybercrime Awareness in Tricity" aimed to understand the level of cybercrime awareness among different participants and its relationship to their professions. Utilizing the descriptive approach and questionnaires as research tools, the study's simple random sample consisted of 100 individuals. The results revealed that awareness plays a pivotal role in reducing cybercrime; however, no significant relationship was found between the level of awareness and participants' professions. This suggests a shared belief in mitigating cyber threats, influencing individuals' responses to such crimes, particularly among those who perceive the virtual world as unreal (Patel & Patel, 2012, p. 15).

4.2. Second Study: Another study by Anopreet Kor Mokha (2017) titled "A Study on Cybercrime Awareness and Safety in the Delhi Region" aimed to enhance awareness of cybercrime and cybersecurity among Internet users in Delhi. Employing the descriptive approach and the Likert scale, the study's sample comprised 160 individuals. The findings indicated a correlation between age groups and respondents' educational qualifications, underscoring the importance of raising awareness about cybercrime and safety and fostering engagement in spreading this awareness (Mokha, 2017, p. 20).

4.3. Benefits of Previous Studies:

We have gleaned significant insights from prior studies across various aspects of preparing our topic. These studies have provided foundational knowledge and frameworks necessary to initiate our research by:

- Defining the research topic and formulating research questions and hypotheses: Previous studies have enabled us to identify different facets of our topic, comprehend its multifaceted nature, and construct logical research questions and hypotheses supported by evidence.
- Understanding previous references: Through analyzing and reviewing prior studies, we have identified the concepts and methodologies employed, aiding in the construction of the theoretical framework for our research and gaining insights into previous advancements in the field of study.
- Adopting methodologies from previous studies: By studying the methodologies utilized in previous research, we have utilized them to determine the necessary steps for conducting our study, including designing research tools and data collection.

5. First: The Importance of the Study

5.1. Space Transition Theory:

The space transition theory is one of the modern theories explaining cybercrime, introduced in the book "Cybercrime" by Frank Schmallenger, Michael Pittaro, and Prentice Hall. This theory emerged to address the inadequacies of traditional interpretations of cybercrime, (Assarut et al., 2019, p. 10) which failed to comprehensively cover the phenomenon. The theory posits several fundamental hypotheses:

1. Motivation for oppressive behavior: Individuals whose criminal behavior is suppressed in physical reality find motivation to engage in crime in virtual reality.
2. Flexibility of digital identity: The ability to conceal digital identity and the absence of legal deterrence in cyberspace incentivize cybercrime.
3. Transfer of criminal behavior: Criminal behaviors can be transferred between social reality and virtual reality, allowing the application of acquired criminal behaviors in both realms.
4. Evasion from legal deterrence: The virtual environment facilitates evasion from legal deterrence due to insufficient evidence to convict cybercriminals, making it an ideal environment for criminal activities.
5. Impact of closed societies: Individuals in closed societies are more inclined to commit cybercrime compared to those in open societies.

The space transition theory elucidates how criminal behavior shifts from physical reality to virtual reality, along with factors contributing to this transition. By focusing on the unique characteristics of cyberspace, (Danquah, 2011, p. 45) this theory provides a novel framework for understanding and interpreting criminal phenomena in the digital age, enriching our comprehension of criminology in virtual environments.

5.2. Routine Activity Theory:

The routine activity theory concentrates on the fundamental elements that constitute crime and serves as a framework for preventing crime by altering at least one of these elements: the offender, the target, or the presence of a capable guardian. Developed by Marcus Felson and Lawrence Cohen in 1979 in the United States, (Guerra & Ingram, 2022, p. 45) this theory aimed to study the evolution of social and criminal conditions in the country post-World War II, reacting to the inadequacies of functional constructivist theories in explaining crime and delinquency during a period of improving social conditions. One of the core hypotheses of the theory is:

1. Accessibility of a target: The presence of an accessible target.
2. Absence of capable guardians: The lack of guardians capable of intervening and preventing crime.
3. Presence of a motivated offender: The existence of an offender with the motive and opportunity to commit the crime.

These three elements coalesce in routine activities, bringing together offenders and victims in time and space. (Reyns et al., 2016, p. 140) When the offender is present with the target in the absence of proper control, the target becomes vulnerable to crime. According to routine activity theory, the likelihood of crime, including cybercrime, escalates when these three elements converge in the environment.

III. Methods and Materials:

1.First: Type of Study and Methodology

Scientific research necessitates adherence to specific scientific methods and approaches tailored to the researcher's specialization and the type of study to achieve the primary results and objectives of the research. Its principal aim is to attain scientific knowledge that can only be obtained through the scientific method. This study falls within the realm of descriptive analytical research aimed at generalization. The method employed is a field survey with a sample, representing an organized scientific endeavor to gather data and information about the phenomenon under investigation, making it most suitable for use in such studies.

2.Second: Study Population and Sample

The research population pertains to the group of individuals sharing common characteristics that set them apart from other elements and form the basis for research and inquiry. In our study, the research population comprises students enrolled in the Faculty of Humanities and Social Sciences at the University of Djilali Bounaama in Khemis Miliana across various disciplines and academic levels, totaling 2851 students.

Additionally, selecting a scientific sample is crucial when conducting field research, particularly when the study population is large and studying all its members is not feasible. Given the nature of the study, where all students at the Faculty of Humanities and Social Sciences at Djilali Bounaama University in Khemis Miliana rely on the intranet in their daily activities, we employed a stratified random sampling method based on gender and department variables. This method ensures equal representation from all segments of the study population, owing to the homogeneity of all members of the original community.

The Richard Geiger equation was utilized to calculate a representative sample of the study population. With a total community size of 2851 individuals, the study sample consisted of 355 individuals .

3.Third: Data Collection Tools

The questionnaire served as the primary tool for data collection from the study participants. This method was chosen due to its suitability for this type of research, especially given the large sample size. It allows for flexibility in responses, facilitating the acquisition of realistic and authentic data on the research topic.

The questionnaire, comprising 20 questions, was designed on paper and distributed to students during the academic period of the first semester, from January 20, 2024, to February 20, 2024.

The questionnaire consisted of the following axes:

Personal Data Axis: This section included questions concerning the personal details of the students (gender, age, educational level, department type) to discern the respondents' personal characteristics.

First Axis: This pertained to students' engagement with virtual reality, assessing factors such as Internet usage frequency, duration, and types of activities.

Second Axis: Focused on awareness of the concept of cybersecurity and its significance.

Third Axis: Explored awareness of electronic crimes and the types most commonly observed by students.

Fourth Axis: Addressed strategies for enhancing cybersecurity awareness from the students' perspective.

4.Fourth: Form Validation

Form validation, or content validity, pertains to the overall appearance or formal structure of the instrument, encompassing elements such as the clarity of questions, their formulation, and suitability for the intended context. To ensure the validity of the study tool, apparent validation was employed by presenting it to a panel of arbitrators, comprising five professors with expertise and experience in the field.

IV. Results and discussion :

1.Personal Data Axis:

Table (1) : shows the distribution of study sample individuals according to the gender variable.

gender	Repetition	percentage
Male	153	%43,1
Female	202	%56,9
Total	355	%100

Table (2) : shows the distribution of study sample individuals according to the age variable.

age	Repetition	percentage
From 17 to 21 years old	107	%30,1
From 22 to 26 years old	158	%44,5
27 years and above	90	%25,4
Total	355	%100

Table (3) : shows the distribution of study sample individuals according to the educational level variable.

Educational level	Repetition	percentage
Bachelor's	243	%68,5
Master's	112	%31,5
Total	355	%100

Table (4) : shows the distribution of study sample individuals according to the department variable

Department	Repetition	percentage
Social Sciences	173	%48,7
Humanities	182	%51,3
Total	355	%100

The data presented in Table No. (01) reveals that 56.9% of the sample comprises females, whereas 43.1% comprises males. This suggests a growing interest among females in the specializations offered by the Faculty of Social and Human Sciences at Djilali Bounaama University. The availability of diverse specializations catering to their needs in the labor market, such as educational sciences, psychology, media and communication sciences, among others, likely contributes to this trend. These findings reflect the broader trend of increasing female representation in social sciences and humanities, indicating expanding opportunities in these domains.

Furthermore, Table No. (02) indicates that 44.5% of the sample falls within the age range of 17 to 21 years, with 30.1% aged between 22 and 26 years, and 25.4% aged 27 years and above. The significant influx of students aged 17 to 26 suggests a notable demographic within the Faculty of Social Sciences and Humanities. This trend may partly stem from educational reforms across the three phases of education, motivating students to pursue university education at younger ages. Conversely, individuals aged 27 and above may pursue higher educational degrees to enhance professional prospects and skill development.

In addition, Table No. (03) illustrates that 68.5% of the sample comprises bachelor's students, while 31.5% comprises master's students. This indicates a preference among students for bachelor's programs over master's programs. Such preferences may be influenced by Algerian government policies aimed at mitigating unemployment by encouraging bachelor's degree holders to further their education rather than directly enrolling in master's programs.

Finally, Table No. (04) demonstrates that 51.3% of the sample consists of students from the Humanities Department, while 48.7% consists of students from the Social Sciences Department. This suggests a balanced distribution of students between the two departments within the Faculty of Social Sciences and Humanities. Students' choice of majors likely reflects personal and professional preferences, as well as the range of majors available in each department .

2. Analysis of Students' Interaction with Virtual Reality:**Table (5) : Students' Internet Usage**

Internet Usage	Repetition	percentage
Always	189	% 53.23
Sometimes	100	% 28.17
Rarely	66	% 18.60
Total	355	%100

Table No. (05) illustrates that 53.23% of students utilize the Internet regularly, while 28.17% access it intermittently, and 18.60% rarely engage with it. This distribution underscores the diverse Internet access patterns among students, reflecting variations in their reliance on digital technology in daily activities. These percentages underscore the challenges and prospects associated with Internet usage in academic and research settings, emphasizing the importance of comprehending Internet usage patterns and their impact on student behavior and academic outcomes.

Table (6) : Hours Spent by Students on the Internet

Hours Spent on the Internet	Repetition	percentage
Less than 1 hour	75	%21.13
1 to 3 hours	60	%16.90
More than 3 hours	220	%61.97
Total	355	%100

As depicted in Table No. (06), 61.97% of students dedicate over 3 hours daily to Internet usage, whereas 21.13% spend less than one hour daily. Additionally, 16.90% allocate 1 to 3 hours daily for Internet activities. Extensive Internet usage seems to align with the escalating necessity for research and academic tasks, particularly at the undergraduate and graduate levels, driven by the abundance of online academic resources and the growing adoption of e-learning methodologies. Conversely, there appears to be a cohort of students opting for reduced Internet usage, possibly due to preferences for traditional written sources or time constraints. Another subset of students adopts a moderate Internet usage approach, primarily focusing on social networking and entertainment.

Table (7) : Reasons for Students' Internet Usage

Reasons for Students' Internet Usage	Repetition	percentage
Learning	126	%35.49
Work	60	%16.90
Chatting and Making Friends	99	27.90%
Watching Movies and Shows	70	19.71%
Total	355	%100.0

Table No. (07) indicates that 35.49% of students utilize the intranet for educational purposes, while 27.90% engage in social networking and 19.71% use it for entertainment purposes. Moreover, 16.90% leverage the intranet for work-related activities. These findings

underscore a burgeoning interest in online education, with students increasingly relying on it as a primary source of knowledge and educational materials. Conversely, the use of the Internet for social networking serves as a conduit for social interaction and mitigating isolation, reflecting the burgeoning influence of social media on interpersonal relationships and communication. Furthermore, the use of the Internet for work underscores the integration of technology into professional spheres, highlighting students' adaptation to economic shifts and their pursuit of job opportunities or supplemental income through online platforms .

3. Analysis of Cybersecurity Awareness:

Table (8) Shows Students' Level of Cybersecurity Knowledge

Level of Cybersecurity Knowledge	Repetition	percentage
Low	80	%22.55
Medium	210	%59.15
High	65	%18.30
Total	355	%100.0

In Table No. (08), it is evident that 59.15% of students possess a moderate level of cybersecurity knowledge, while 22.55% have low levels, and 18.30% exhibit high levels. These findings indicate a prevalent low-to-moderate level of cybersecurity understanding among students, underscoring the urgent necessity to enhance their comprehension of cybersecurity threats and bolster their capacity to safeguard their electronic devices and data.

Table (9) : Indicates Cybersecurity Awareness According to Students

Cybersecurity Awareness According to Students	Repetition	percentage
Safely Conducting Activities Online	170	%47.90
Awareness of Risks of Cyber Attacks	105	%29.57
Maintaining the Security of My Personal Data	80	%22.53
Total	355	%100.0

As indicated in Table No. (09), 47.90% of students perceive cyber awareness as ensuring safe online activities, whereas 29.57% view it as awareness of electronic attack risks, and 22.53% prioritize maintaining personal data security. This data underscores the imperative to educate students about implementing security measures across various online activities such as learning, communication, work, and e-commerce, highlighting the necessity to enhance cyber awareness and encourage safe internet practices.

Table (10) : Activities Students Avoid on the Internet to Preserve Their Security

Activities Students Avoid on the Internet	Repetition	percentage
Accessing Unsafe Websites	160	%45.07
Downloading Files from Untrusted Sources	80	%22.53
Disclosing My Personal Information	115	%32.40
Total	355	%100

Table No. (10) reveals that 45.07% of students avoid accessing unsafe websites to safeguard themselves, while 32.40% refrain from disclosing personal information, and 22.53% abstain from downloading files from unreliable sources. These findings demonstrate a notable awareness among students regarding the hazards of unsafe online platforms, reflecting their vigilance in avoiding electronic fraud and safeguarding their devices and privacy.

Table (11) : Basic Steps Followed by Students to Enhance Their Cybersecurity

Basic Steps to Enhance Cybersecurity	Repetition	percentage
Updating My Device's Software (Computer/Phone)	145	%40.84
Avoiding Opening Unknown Emails	70	%19.71
Using Strong and Varied Passwords Regularly (Email/Social)	90	%25.35
Installing Antivirus Software (Computer/Phone)	50	%14.10
Total	355	%100

In Table No. (11), 40.84% of students prioritize updating software to enhance cybersecurity, while 25.35% emphasize using strong, varied passwords for email and social networking accounts, and 19.71% refrain from opening anonymous emails. Additionally, 16.90% install antivirus programs on their devices. These results underscore students' recognition of cybersecurity's significance, particularly in terms of software updates and password strength, while also highlighting areas where greater awareness is needed, such as the risks of opening anonymous emails.

Table (12) : Importance of Cybersecurity Awareness According to Students

Importance of Cybersecurity Awareness	Repetition	percentage
Maintaining the Safety of My Information	85	%23,94
Preventing Attacks and Cyber Crimes	165	%46,47
Increasing Security While Using the Internet	105	%29,59
Total	355	%100

In Table No. (12) indicates that 46.47% of students perceive cyber awareness as crucial for preventing cyberattacks and crimes, while 29.59% associate it with enhancing their internet security, and 23.94% emphasize its role in safeguarding their information. These findings underscore students' understanding of cyber awareness's pivotal role in preventing cyber crimes, emphasizing the need to fortify their cybersecurity knowledge to mitigate potential threats and uphold information integrity in the digital realm .

4.Understanding Cybercrime and Its Types:

Table (13) : Students' Level of Knowledge about Cybercrime

Level of Knowledge about Cybercrime	Repetition	percentage
Low	78	22,00%
Medium	167	47,00%
High	110	31,00%
Total	355	100.0%

In Table No. (13), it is evident that 47.00% of students possess a moderate level of knowledge about cybercrime, while 22.00% have low levels, and 31.00% exhibit high levels. This indicates varying levels of understanding among students, necessitating continuous education on cybercrime to equip them with the skills to effectively counter it. Some students may lack knowledge due to their specialization or limited internet usage, emphasizing the need for comprehensive education to prevent underestimation of cyber threats.

Table (14) : Most Noticed Cybercrimes by Students While Using the Internet

Most Noticed Cybercrimes by Students	Repetition	percentage
Threats and Harassment such as	84	23,66%
Defamation and Insults such as (Spreading Fake	99	27,90%
Unethical Crimes such as (Unethical Websites/Sexual Images)	96	27,04%
Financial Crimes (Bank Card Number Theft/Scams in Online	76	21,40%
Total	355	100.0%

From Table No. (14), 27.90% of students identify defamation and insults as the most common cybercrimes, followed by 27.04% recognizing immoral activities like accessing inappropriate websites. Additionally, 23.66% notice threats and harassment, while 21.40% observe financial crimes such as online fraud. These findings underscore the prevalence of electronic crimes, causing social and psychological harm, and necessitate effective measures to protect users and combat these offenses.

Table (15) : Students' Experience with Cybercrimes While Using the Internet

Experience with Cybercrimes While Using the Internet	Repetition	percentage
Experienced One Crime	172	48,45%
Experienced Two to Three Crimes	118	33,25%
Experienced More than Four Crimes	65	18,30%
Total	355	100.0%

Table No. (15) reveals that 48.45% of students experienced cybercrime once, with 33.25% encountering it two to three times, and 18.30% experiencing it more than four times. Prolonged internet use, academic requirements, and online exams increase students' exposure to cybercrimes, emphasizing the importance of enhancing cybersecurity knowledge to mitigate risks effectively.

Table (16) : Cybercrimes Students Have Been Exposed to

Cybercrime Students Have Been Exposed to	Repetition	percentage
Hacking Your Social Media Account	89	25,00%
Identity Theft (Stealing Your Data or Pictures)	75	16,00%
Fraudulent Activity in Online Shopping	45	15,00%
Experiencing Insults and Threats	97	27,00%
Receiving Images and Links to Unethical Websites	58	17,00%
Total	355	100.0%

As per Table No. (16), students commonly face cybercrimes like insults and threats (27.00%), social media account hacking (25.00%), and exposure to unethical sites (16.00%). Additionally, 17.00% experience impersonation, while 16.00% fall victim to online shopping fraud. These incidents highlight the need for improved digital literacy and awareness to promote safe online behavior and reporting of cybercrimes.

Table (17) : Priority of Reporting to the Police Due to Students' Exposure to Cybercrimes:

Priority of Reporting to the Police	Repetition	percentage
Yes	70	% 19,71
No	285	% 80,29
Total	355	%100

Table No. (17) shows that 80.29% of cybercrime victims did not report the incidents to the police, citing difficulties in identifying perpetrators and their advanced concealment techniques. Instances like hacking, fraud, and extortion require advanced technical skills, hindering identification and legal action against the accused.

Table (18) : Reasons for Not Reporting to the Police Due to Students' Exposure to Cybercrimes

Reasons for Not Reporting to the Police	Repetition	percentage
Lack of Awareness That an Action Constitutes a Crime	85	29,82%
Lack of Knowledge about Cybercrime Law	120	42,10%
Absence of Evidence and Unknown Criminal	80	28,08%
Total	285	%100

Finally, Table No. (18) indicates that 42.10% of cybercrime victims refrained from reporting due to a lack of understanding of cybercrime laws, while 29.82% were unaware that the behavior constituted a crime, and 28.08% lacked evidence to identify the perpetrator. These findings underscore the need for comprehensive education on cybercrime laws and their implications to empower students to address cyber threats effectively .

Table (19) : Factors Leading to Falling Victim to Cybercrime from Students' Perspective:

Factors Leading to Falling Victim to Cybercrime	Repetition	percentage
Trust in Strangers	49	13,80%
Lack of Knowledge about Cybercrime	64	18,02%
Browsing Unsafe Websites	58	16,33%
Lack of Knowledge about Cybersecurity	78	22,00%
Lack of Knowledge about Algerian Legislative Laws on	106	29,85%
Total	355	%100.0

From Table No. (19), it is evident that 29.85% of students attribute the lack of knowledge about Algerian legislative laws for cybercrime as a factor leading to cybercrime. Additionally, 22.00% believe insufficient knowledge in cybersecurity contributes to becoming a victim, while 18.02% cite ignorance about cybercrime itself as a reason for victimization. Browsing unsafe websites and trusting strangers are also identified as contributing factors at 16.33% and 13.80%, respectively. These findings underscore the need for education on cybercrime laws and cybersecurity to prevent inadvertent involvement in illegal activities and reduce exposure to online risks.

5.Ways to Enhance Cybersecurity Awareness:

Table (20) : Solutions for Developing Cybersecurity Awareness for Cybercrime

Solutions for Developing Cybersecurity Awareness for	Repetition	percentage
Providing Lessons and Workshops to Train Students on	98	27,60%
Encouraging Reporting Cybersecurity Incidents	102	28,73%
Organizing Awareness Campaigns	78	21,97%
Attending National and International Conferences on	77	21,70%
Total	355	%100.0

Table No. (20) reveals that 28.73% of students advocate for encouraging the reporting of cyber incidents as a solution to enhance cybersecurity awareness in the university community. Similarly, 27.60% suggest providing lessons and workshops to educate students about cybersecurity. Another 21.97% propose organizing awareness campaigns focusing on cyber awareness and cybercrime, while 21.70% recommend encouraging students to participate in national and international forums dedicated to cybercrime. These solutions aim to empower students with the knowledge and skills to recognize and respond to cyber threats effectively. By promoting reporting mechanisms, educational initiatives, awareness campaigns, and participation in relevant forums, universities can foster a culture of cybersecurity awareness among students and contribute to a safer online environment.

V. Conclusion:

Upon presenting, analyzing, and scrutinizing the outcomes of the field study, the following conclusions have been drawn:

- **Virtual Reality Interaction:** The study reveals significant engagement with virtual reality among students. A notable 53.23% utilize the Internet consistently, with 61.97% spending over three hours daily online. Moreover, 35.49% employ the Internet for educational purposes, while 27.90% utilize it for socializing, underscoring its dual role as an educational and social tool in students' lives.

- **Cybersecurity Knowledge:** Findings indicate an average level of cybersecurity knowledge among students, with 59.15% possessing moderate awareness. Interestingly, 47.90% perceive cyber awareness as safe online conduct, while 29.57% associate it with understanding cyber risks. Notably, 45.07% avoid unsafe websites to bolster their safety, while 40.84% regularly update device software, and 25.35% employ robust passwords. Furthermore, 46.47% recognize the importance of cyber awareness in thwarting attacks and cybercrimes.
- **Understanding Cybercrime:** The study unveils that 47% of students possess moderate knowledge of cybercrime, while 22% exhibit low awareness. Predominant cybercrimes observed include slander and insults (27.90%) and immoral activities (27.04%). Alarmingly, 48.45% have encountered cybercrime, with 80.29% opting not to report incidents to authorities, primarily due to a lack of legal knowledge.(%42.10)
- **Enhancing Cybersecurity Awareness:** Students propose various strategies to enhance cyber awareness. Notably, 28.73% advocate for encouraging incident reporting, while 27.60% endorse providing educational workshops. Additionally, 21.97% suggest organizing awareness campaigns, and 21.70% highlight the importance of attending cyber-related forums at national and international levels.

These findings underscore the imperative for educational institutions and authorities to prioritize cybersecurity education and awareness initiatives to mitigate cyber risks and promote a safer online environment.

– **Referrals and references:**

- **We Are Social & Meltwater. (2023).** Digital 2023 Global Overview Report. Retrieved from <https://datareportal.com/reports/digital-2023-global-overview-report> on June 1, 2023.
- **Aldabbagh, A., et al. (2019).** Student Addiction to Social Networking Sites and Its Relationship to Psychological Security and Involvement in Cyber Crimes. *International Journal of Educational and Psychological Studies*, 6(2), 267-293.
- **Jadik Grayeh, A. S. (2014).** Transformations in the Concept of Security in the Face of New International Threats. *Journal of Legal and Political Sciences*, 1(5), 17-31.
- **Von Solms, R., & Van Niekerk, J. (2013).** From Information Security to Cyber Security. *Computers & Security*, 38, 97-102.
- **Zwilling, M., et al. (2022).** Cyber Security Awareness, Knowledge, and Behavior: A Comparative Study. *Journal of Computer Information Systems*, 62(1), 82-97.
- **Phillips, K., et al. (2022).** Conceptualizing Cybercrime: Definitions, Typologies, and Taxonomies. *Forensic Sciences*, 2(2), 379-398.
- **Online El Chorouk. (2023).** The National Gendarmerie reveals the outcome of electronic crimes in Algeria for the years 2022 and 2023. *El Chorouk Newspaper*, 01.
- **Assarut, N., et al. (2019).** Clustering Cyberspace Population and the Tendency to Commit Cyber Crime: A Quantitative Application of Space Transition Theory. *International Journal of Cyber Criminology*, 13(1).
- **Danquah, P. D. P. (2011).** An Empirical Test of The Space Transition Theory of Cyber Criminality: Investigating Cybercrime Causation Factors in Ghana.
- **Guerra, C., & Ingram, J. R. (2022).** Assessing the Relationship Between Lifestyle Routine Activities Theory and Online Victimization Using Panel Data. *Deviant Behavior*, 43(1), 44-60.
- **Milano, G., et al. (2017).** Report on the International Workshop on Drug Prevention and Treatment in Rural Settings Organized by United Nations Office on Drugs and Crime (UNODC) and World Health Organization (WHO). *Substance Use & Misuse*, 52(13), 1801-1807.
- **Mokha, A. K. (2017).** A Study on Awareness of Cyber Crime and Security. *Research Journal of Humanities and Social Sciences*, 8(4), 459-464.
- **Patel, R., & Patel, R. (n.d.).** A Research of the Awareness Level Among Technical and Non-technical Students of Cyber Security in Parul University.
- **Reyns, B. W., et al. (2016).** Guardians of the Cyber Galaxy: An Empirical and Theoretical Analysis of the Guardianship Concept from Routine Activity Theory as it Applies to Online Forms of Victimization. *Journal of Contemporary Criminal Justice*, 32(2), 148-168.
- **Web, E. (2021).** *Internet. Haiti: Earthquake Situation Report*, 26.
- **Brada, A. A., Sally, M. M., & Saeeshi, Y. Y. (2023).** Security measures to protect against cybercrime in university settings. *Al-Rawq Journal*, 9(1), 90-109. Retrieved from <https://www.asjp.cerist.dz/en/article/226310>