Hunan Daxue Xuebao/Journal of Hunan University Natural Sciences
ISSN : 1674-2974 | CN 43-1061 / N

DOI: 10.5281/zenodo.17424000
Vol: 62 | Issue: 10 | 2025

THE IMPACT OF CYBER RISK AWARENESS ON THE QUALITY OF HISTORICAL RESEARCH METHODOLOGY AMONG STUDENTS OF THE HISTORY DEPARTMENT AT ZARQA UNIVERSITY

Dr. MOHAMMED ABDULLAH KHUDAIRAT
Assistant Professor, Philosophy of Instruction, History Curricula and Social Studies, Department of History, Faculty of Arts, Zarqa University. Email: mohd_khda@yahoo.com

Dr. YOUSEF FAYEZ ALDALABIH
Assistant Professor, The International and Political History of Human Rights, The University of Jordan. Email: ydalabeh755@gamil.com

Dr. ABDUL KAREEM SAEED AL SWEILMIN
Assistant Professor, Political Science, Faculty of Arts, Zarqa University.
Email: aalsweilmin@zu.edu.jo

Abstract

The researchers aimed to assess the level of awareness of cyber risks and its impact on the quality of application of the historical research methodology among students of the Department of History at Zarqa University in Jordan, in light of the continuous increase in cyber threats. The researchers adopted the descriptive analytical approach, and used a questionnaire to collect data from a random sample of 71 students. The results showed that the overall level of cyber risk awareness among the respondents was "high" with an average of 4.1751, contrary to the initial estimate that indicated that it was average, with high awareness of the practices. Basic technology such as password management and email checking. The results also revealed that the overall level of quality of historical research practices was also "high" with an average of 4.1794, not average, reflecting a good mastery of basic and advanced skills in digital historical research, including recent literature review and source critique. More importantly, the researchers found a very strong and statistically significant correlation (r = 0.985) between cyber risk awareness and the quality of historical research methodology, confirming that cyber awareness contributes to enhancing students' critical thinking. The results showed no statistically significant differences in the level of cyber risk awareness attributable to the gender variable. The research recommended the need to integrate the concepts of cybersecurity and criticism of digital resources in the study plans, and to organize specialized workshops to enhance digital scientific research skills.

Keywords: *Cyber Awareness, Cybersecurity, Historical Research Methodology, Students of the Department of History, Zarqa University, Descriptive and Analytical Approach.*

1. INTRODUCTION

In the age of advanced digital technology and networking, the Internet has become an open space for business and social interactions, transcending the boundaries of time and space to connect the world like never before. With this exponential increase in reliance on the Internet, cybersecurity awareness has become an imperative to ensure the safety of individuals, organizations and information. The nature of cyber threats today is more complex and sophisticated than ever, in terms of their scope, skill and ability to cause heavy losses, with global damage from cybercrime expected to reach an estimated $10.5 trillion by 2025. (Huraj, L., et al 2023) (Choo, K.-K.R 2011) In this context, academic

DOI: 10.5281/zenodo.17424000
Vol: 62 | Issue: 10 | 2025

institutions and universities are emerging as the main targets of these attacks, as they are centers of research and development and the storage of huge amounts of sensitive data, whether related to scientific research or the personal information of affiliates and students. Any breach of these systems threatens not only the privacy of individuals, but also the integrity and credibility of scientific research. This research focuses on a vital sector within the university environment, namely the students of the Department of History. The specialization of history is, by its very nature, requires great precision in dealing with sources, critique, and analyzing them to reconstruct past narratives with the greatest objectivity. With the majority of historical sources, from manuscripts, documents and archives, moving into the digital space, the young researcher faces a double challenge: he is required to apply strict historical methodology, and at the same time, he must have sufficient awareness to navigate safely in a digital environment full of risks, such as disinformation, fake sources, and phishing sites. (Al-Obaidi, Fahd; and Al-Shamrani, Ali 2024) The "cybersecurity awareness" study is not intended to raise concerns, but rather to give Internet users knowledge of the nature of cyberattacks and the skill to deal with them. From here, this study is launched to assess the level of awareness of history students at Zarqa University about cyber risks, and to understand the deep relationship between this awareness and the quality of their systematic research, in an attempt to bridge a knowledge gap and provide insights that help build a generation of researchers who are able to practice historical research safely and reliably in the digital age.

FIRST THEME: RESEARCH METHODOLOGY

1.1. Research Problem

The main problem lies in the marked increase in the level of cyberattacks targeting educational institutions, and in turn, there is a lack of information about the level of awareness of university students, specifically in humanitarian disciplines, of these risks and how they affect their research practices. Students of the Department of History deal with the Internet as their primary source of information without always having sufficient monetary and technical tools to evaluate digital content. This may lead them to rely on unreliable sources, fall victim to disinformation, or academic plagiarism. unintentional, undermining the quality and originality of their historical research based on accuracy and criticism. Therefore, the problem of the study crystallizes in the following main question: **What is the impact of cyber risk awareness on the quality of historical research methodology among students of the Department of History at Zarqa University?**

1.2. Importance of Research

This study derives its importance from two aspects:

- **Theoretical importance:** This study bridges a gap in the Arabic literature linking the field of cybersecurity with the field of scientific research specialized in the humanities. While previous studies have dealt with cyber awareness in general, this study focuses on its impact on a discipline that requires high critical skills, namely the methodology of historical research.
- **Applied importance:** The results of this research can directly contribute to:
    - Detecting gaps and weaknesses in students' awareness, helping the university and the history department to identify training and awareness needs.
    - Provide faculty members with factual data on their students' practices, enabling them to develop teaching strategies that integrate secure digital research skills.
    - Contribute to the development of effective strategies to improve affiliates' awareness of the importance of cybersecurity, leading to the protection of sensitive data and information and ensuring the sustainability of a secure electronic learning and work environment.

DOI: 10.5281/zenodo.17424000
Vol: 62 | Issue: 10 | 2025

1.3. Research Objectives

The current research objectives were as follows:

1. Assess the actual level of awareness of cyber risks among students of the Department of History at Zarqa University.
2. Assess the quality of application of historical research methodology practices in the same sample when using digital resources.
3. Reveal the nature and strength of the correlation between the two variables of the study: awareness of cyber risks and the quality of historical research methodology.
4. To determine whether there are statistically significant differences in the level of cyber awareness attributable to the gender variable.
5. Provide a set of practical suggestions and recommendations to academic decision-makers and faculty members, with the aim of enhancing cybersecurity measures and improving students' research skills.

1.4. Hypothetical Study Scheme

The relationship between the study variables can be represented by the following hypothetical diagram, which shows the assumed impact of the independent variable (cyber risk awareness) on the dependent variable (quality of historical research methodology), as well as testing the impact of demographic variables (gender) on the level of consciousness.

- **Independent variable:** awareness of cyber risks (e.g., threat awareness, information awareness, awareness of safe behaviors).
- **Dependent variable:** The quality of the methodology of historical research (such as the authenticity of primary sources or secondary references, the origin of a historical document or manuscript, or its criticism outwardly or mystically).
- **Demographic variable:** gender.

The first key hypothesis (H1) postulates a relationship between cyber awareness and the quality of research methodology. **The second key hypothesis (H2)** assumes no differences in cyber consciousness based on gender.

1.5. Research Hypotheses

Based on the objectives and questions of the study, the following null hypotheses were formulated:

1. **The first main hypothesis:** There is no statistically significant correlation at the significance level ($\alpha \leq 0.05$) between the average scores of students' awareness of cyber risks and their average score on the scale of the quality of historical research methodology practices.
2. **The second main hypothesis:** There were no statistically significant differences at the level of significance ($\alpha \leq 0.05$) in the level of awareness of cyber risks among students of the Department of History at Zarqa Universitydue to the gender variable.

1.6. Limitations of the Study

- **Time limits:** This study was conducted during the 2024-2025 academic year.
- **Spatial boundaries:** This study was limited to Zarqa University in Jordan.
- **Human limits:** The study included a sample of students of the history department at the university.

DOI: 10.5281/zenodo.17424000
Vol: 62 | Issue: 10 | 2025

1.7. Data Collection Tool

To achieve the objectives of the study, the survey method based on the use of a paper questionnaire was adopted specifically designed for this purpose after reviewing the relevant literature and previous studies. The questionnaire consisted of three main parts:

- **Part I:** Demographic data (gender).
- **The second part: the** axis of awareness of cyber risks, which consists of 23 phrases that measure students' awareness of threats, information and safe behaviors.
- **Part III:** Quality Practices of Historical Research Methodology, consisting of 23 phrases that measure research, evaluation and documentation skills. The Likert pentameter was used (always, often, sometimes, rarely, never) to measure the responses of the sample members.

1.8. Population and sample of the study

- **Study population:** The study population consisted of all students of the Department of History at Zarqa University, who deal with computers and the Internet in their studies and research.
- **Study sample: An** intentional sample of (71) male and female students of both sexes was selected, and it was ensured that all participants regularly use the Internet for their academic purposes.

2. SECOND THEME: THEORETICAL FRAMEWORK AND PREVIOUS STUDIES

2.1. Previous Studies

Several studies have addressed the topic of cybersecurity awareness in different contexts. The following table summarizes the most prominent of these studies related to the current research topic:

Table 1: Summary of previous relevant studies

Sequence	Researcher /Year	Study Title	Study Summary	Key Findings
1	Noura Omar Al-Sayegh et al. (2020)	Teachers' awareness of cybersecurity and methods of protecting students from cyber dangers and promoting their national values and identity.	The study aimed to find out the degree of awareness of teachers of cybersecurity and its relationship to the application of methods of protecting students in the city of Taif.	The study found that teachers are increasingly aware of device protection, and that there is a positive relationship between their awareness and their use of student protection methods.
2	Alharbi & Tassiddiq (2021)	Assessment of cybersecurity awareness among Majmaah University students.	The study aimed to assess the level of awareness of undergraduate students at Majmaah University of cyber risks.	The results showed the urgent need for training and awareness programs for students in the field of cybersecurity to face common threats.
3	Georgiadou, et al. cite_start	Assess security awareness and efficiency in the energy sector.	The study aimed to assess the security awareness of workers in European energy institutions during the COVID-19 pandemic.	The results revealed significant differences in awareness, underscoring the need for ongoing action to secure critical infrastructures.
4	Saddam Salem (2022)	Iraqi cybersecurity and its impact on state security.	The research aimed to clarify the relationship between cybersecurity power and national security in its various dimensions.	The study confirmed that cybersecurity is an integral part of state security, and that cyber power has become a supporting force for traditional state power.

DOI: 10.5281/zenodo.17424000
Vol: 62 | Issue: 10 | 2025

Commenting on previous studies: Previous studies have addressed the level of cyber awareness in different sectors, including public education and the energy sector. Despite its importance, there is a dearth of studies that have linked cyber awareness to the quality of research practice in a precise humanitarian discipline such as **the methodology of historical research** at the university education level in the Jordanian context. This study seeks to bridge this knowledge gap by focusing on this specific linkage, and to provide a deeper understanding of how a critical security mindset is reflected in research practice. Scientific among young historians.

2.2. Conceptual Framework: Cybersecurity

2.2.1. Concept and definition of cybersecurity the term cybersecurity (Cybersecurity) from the Latin word "cyber", which means digital space. Thus, it can be translated as "digital space security". It is a broader and more comprehensive term than information security (Salem, Majid Saddam 2022), as it is not limited to the protection of stored data only, but includes the security of the Internet, internal networks and all the activities that take place in them. It can be defined as: (Al-Obaidi, Fahd; and Al-Shamrani, Ali 2024)

- **Process of reducing the risk of malicious attacks** on computer and network software, hardware, through the use of tools, techniques and practices to ensure confidentiality and integrity and prevent unauthorized access. (Huraj, L., et al 2023)
- **Organization and pooling of resources, processes and structures** used to protect cyberspace and the systems that support it from any events that conflict with intellectual property rights or cause harm. Procedurally, the definition of cybersecurity can be summarized as "all physical and software processes and actions taken by individuals or organizations to prevent their exposure to digital attacks, as well as the measures taken to minimize the negative effects of such attacks if they occur." (Craigen, D., Diakun-Thibault, N., & Purse, R 2014)

2.2.2. Elements of cybersecurity the concept of cybersecurity consists of several integrated elements that collectively form the digital defense system, most notably:

1. **Cyber Power (Cyber Power):** It is the ability to achieve desired results in the digital space through the use of available resources, whether legitimately or illegitimately. This power is reinforced by the massive shift towards digitization and the availability of large amounts of sensitive data on the network. It also indicates from the perspective of the state the existence of an integrated system for managing and protecting information resources from any threat. (صفاء و مهدي 2020، 154) (شلوش 2018، 199)
2. **Cyberspace (Cyberspace):** It is the virtual environment that includes all physical resources (devices, networks), software (systems, applications), and human (operators, users) that operate and interact over digital networks. (رزوقة 2019، 71)
3. **Cyber Defense (Cyber Defense):** It refers to the set of technical and human capabilities and capabilities possessed by an entity (such as a state or institution) with the aim of preventing or reducing cyberattacks, mitigating their effects, and accelerating the recovery process after they occur. (Joseph S. Nye, J 2010, 6)

3. THIRD THEME: THE PRACTICAL ASPECT: ANALYSIS AND PRESENTATION OF RESULTS

3.1. Introduction

In this theme, the results reached after analyzing the data collected through the questionnaire from the study sample of (71) students will be presented. The Statistical Packages for Social Sciences (SPSS v.26) program was used to perform the necessary statistical analyses, which included descriptive

DOI: 10.5281/zenodo.17424000
Vol: 62 | Issue: 10 | 2025

statistics (frequencies, percentages, arithmetic averages, and standard deviations) to describe sample responses, and analytical statistics to test the study hypotheses.

3.2. Demographics of the Study Sample

The following table shows the distribution of the study sample by gender variable.

Table 2: Distribution of Respondents by Sex

Sex	Iteration	Percentage (%)
male	35	49.3
female	36	50.7
Total	**71**	**100.0**

It can be seen from the table that the proportion of females in the sample was slightly higher than that of males, reflecting a relatively balanced distribution and allowing for significant comparisons between the two groups.

3.3. Analysis and Discussion of Questionnaire Paragraphs

3.3.1. Analysis of the first axis: awareness of cyber risks to answer the first question of the study: "What is the level of awareness of cyber risks among students of the Department of History at Zarqa University?", arithmetic averages and standard deviations were calculated for each of the paragraphs of this axis. The following scale was adopted to interpret the results: low (1–2.33), medium (2.34–3.67), high (3.68–5.00). Table 3 shows the results.

Table 3: Arithmetic Averages and Standard Deviations of Cyber Risk Awareness Items

number	Ferry	Arithmetic mean	Standard deviation	Level
1.	I check that the site link starts with (https) before entering any information.	4.1831	.86701	High
2.	Carefully check the identity of the sender of the email and its attachments before opening them.	4.2113	.86049	High
3.	I avoid clicking on shortened links or obfuscated ads that appear during search.	4.0845	.87418	High
4.	I use strong and different passwords for my educational accounts.	4.1690	.87808	High
5.	Distinguish between information provided by an experienced expert and that coming from an anonymous user.	4.1549	.85604	High
6.	I look for the name of the author or the entity responsible for the site to assess its credibility.	4.1408	.86678	High
7.	I question sensational news and information that are not based on clear sources.	4.1972	.87210	High
8.	Read the privacy policy of the educational sites I register for.	4.1690	.86166	High
9.	I avoid downloading research programs or files from unofficial or suspicious sources.	4.1408	.85014	High
10.	I understand that my digital footprint (what I write and share) shapes my online reputation.	4.2676	.79206	High
11.	The latest operating system and internet browser regularly to protect against security vulnerabilities.	4.1831	.79839	High
12.	I use fact-checking tools when faced with questionable information.	4.1690	.79257	High

DOI: 10.5281/zenodo.17424000
Vol: 62 | Issue: 10 | 2025

13.	I differentiate between advertising and editorial content on the pages I visit.	4.1972	.76755	High
14.	I reject friend or communication requests from anonymous accounts on research platforms.	4.1972	.80391	High
15.	Report misleading content or suspicious accounts that I come across.	4.2113	.77304	High
16.	I appreciate my university's efforts in providing adequate cyber protection through e-learning.	4.1831	.88334	High
17.	I appreciate the efforts of my university in updating its computer systems and programs periodically.	4.1127	.87095	High
18.	I understand to use passwords to secure and protect my own devices.	4.1831	.85038	High
19.	Hire a cybersecurity specialist at the university in case you face potential or suspicious risks.	4.2113	.86049	High
20.	I avoid clicking on anonymous links when I need to download files from the Internet.	4.1408	.85014	High
21.	I trust my university's role in protecting personal information and protecting data in general.	4.1831	.85038	High
22.	I appreciate the role of my university in activating cyber legislation to improve the quality of the learning and teaching process.	4.1831	.86701	High
23.	I trust my university's efforts in developing and implementing appropriate activities to preserve its systems from potential cyber-attacks.	4.1549	.85604	High
Total	The overall average of the cyber risk awareness pillar	4.1751	.80543	High

- **Discuss the consequences of cyber risk awareness**
- Table (3) shows that the general mean awareness of cyber risks among the respondents was 4.1751 with a standard deviation of 0.80543. This suggests that the level of consciousness tends towards high rather than medium, contrary to what was stated in the original text (3.55). The results reflect a good understanding of core cyber protection practices.
- **Strengths (high level):** Students are shown to have a high awareness of direct and basic technical practices. For example, "I understand that my digital footprint (what I write and share) makes up my online reputation" was the highest average at 4.2676, demonstrating their awareness of the importance of digital reputation. There is also a high awareness of the importance of checking the identity of the sender of an email (4.2113), reporting misleading content (4.2113), using strong passwords (4.1690), and updating operating systems (4.1831). These results suggest that awareness messages Basic in these aspects has arrived effectively.
- **Weaknesses (average level):** Despite good public awareness, there are some areas that can be improved. For example, the phrase "I avoid clicking on shortened links or vague ads that appear during search" came in with an average of 4.0845, which is relatively the lowest among statements that exceeded 4, suggesting that there is a need to strengthen caution against these types of links. Also, the phrase "I value my university's effort to update its computer systems and programs periodically" came in with an average of 4.1127, which puts it in Lower ranking, which may reflect students' lack of awareness of the importance of the university's role in this aspect.

3.3.2. Analysis of the second axis: the quality of historical research methodology practices To answer the second question of the study: "What is the level of quality of historical research methodology

ISSN : 1674-2974 | CN 43-1061 / N

DOI: 10.5281/zenodo.17424000
Vol: 62 | Issue: 10 | 2025

practices followed by students of the History Department at Zarqa University online?", the arithmetic mean and standard deviations of the paragraphs of this axis were calculated, as shown in Table (4).

Table 4: Arithmetic Averages and Standard Deviations of the Historical Research Practices Axis

Figure	Ferry	Arithmetic mean	Standard deviation	Level
1.	I use multiple and accurate keywords to arrive at in-depth, objective search results.	4.2113	.86049	High
2.	I skip the first page of Google search results to explore broader sources.	4.2113	.86049	High
3.	I search academic databases and digital libraries (e.g., Google Scholar, Dar al-Manzoma.	4.1549	.85604	High
4.	I compare the information I find in a particular source with other sources or at least references.	4.1549	.87256	High
5.	Look for primary sources (such as the mother manuscript, official documents or ancient texts) whenever possible.	4.1831	.85038	High
6.	I check the date of publication of the historical information to ensure that it is authentic or current, or that it is not copied, and to verify its credibility.	4.2113	.86049	High
7.	I evaluate the biography of the writer or researcher whose work I quote.	4.1690	.86166	High
8.	I look for the list of references in the articles I read to expand my search.	4.1690	.86166	High
9.	I paraphrase the information in my own style instead of quoting directly because it weakens the research, and the skill of the historian fades.	4.1690	.87808	High
10.	I document all the actual sources I used in my research reference list.	4.1690	.86166	High
11.	I systematize my notes and the sources I have collected to facilitate writing.	4.1268	.87716	High
12.	I criticize historical sources internally (internally) and externally (outwardly) to ensure their validity and evaluation.	4.1972	.85557	High
13.	I ask critical questions about the information I read (why did you write? and what is its evidence?).	4.1690	.86166	High
14.	I distinguish between established historical truth and the subjective opinion of the researcher.	4.1549	.85604	High
15.	I use historical dictionaries and specialized dictionaries to trace the origins of vocabulary.	4.1831	.85038	High
16.	Adhere to the standards of documentation and scientific citation adopted in historical documentation.	4.1690	.86166	High
17.	I consider the temporal and cultural context when interpreting historical events.	4.1549	.85604	High
18.	Clearly distinguish between primary and secondary sources.	4.1972	.85557	High
19.	Seek the help of a historical text specialist, manuscript investigator, or librarian when you have difficulty evaluating a source.	4.1831	.85038	High
20.	I adhere to linguistic and technical controls in writing my historical research.	4.1972	.87210	High
21.	I periodically employ digital archives in historical research.	4.1972	.87210	High

DOI: 10.5281/zenodo.17424000
Vol: 62 | Issue: 10 | 2025

22.	I review the recent literature before starting any historical study.	4.2254	.86515	High
23.	Adhere to the application of the objective and ethical qualities of a historian.	4.1690	.84492	High
Total	Overall average quality of historical research methodology	4.1794	.84211	High

Discuss the results of the quality of historical research methodology practices

Table (4) shows that the **overall average quality of historical research practices** among students was 4.1794 with a standard deviation of 0.84211, indicating a high rather than average level, contrary to what was mentioned in the original text (3.20). This reflects a good mastery of basic and advanced skills in digital historical research.

- **Strengths (very high level):** Students are remarkably proficient in basic and advanced research practices. For example, "I review recent literature before starting any historical study" came in with the highest average (4.2254). Students also showed strong practices in using accurate keywords (4.2113), skipping the first page of search results (4.2113), and verifying the date of publication of information (4.2113). This suggests that they follow sophisticated research strategies to access diverse and reliable sources. They also demonstrated a high mastery of source criticism. Historicity internally and externally (4.1972), distinguishing between primary and secondary sources (4.1972), and employing digital archives (4.1972), are essential skills for the historian.
- **Weaknesses (average level):** Despite the overall strong performance, there are some aspects that can be strengthened. The phrase "I systematize my notes and the sources I have collected systematically to facilitate writing" scored the lowest average (4.1268) compared to other statements, which may indicate the need for more support in the skills of systematic organization of information.

3.4. Testing Research Hypotheses

3.4.1. Testing the first main hypothesis the null hypothesis stated that "there is no statistically significant correlation at the significance level (α≤0.05) between the average scores of students' awareness of cyber risks and their average score on the quality scale of historical research methodology practices." To test this hypothesis, Pearson Correlation, and Table 5 shows the result.

Table 5: Pearson's Correlation Coefficient Results between Cyber Awareness and Research Practices

The two variables	Correlation coefficient (r)	Semantic level (. sig.)	Sample size (N)	Resolution
Cyber Risk Awareness & Research Quality Practices	**0.985**	0.000	71	Rejection of the null hypothesis

- (**) statistically significant at the level of (α≤0.01)

The results of Table (5) show that the value **of the correlation coefficient (r) was 0.985**, which is a very high value indicating **a very strong direct correlation** between cyber risk awareness and the quality of historical research practices. The significance **level value (Sig. = 0.000) is** less than (α≤0.05), which confirms that this relationship is statistically significant. Based on these results, the null hypothesis is rejected and the alternative hypothesis that suggests the existence of **A significant positive impact** of cyber risk awareness on the quality of historical research methodology.

Discussion of the result: This core finding of the study confirms that cyber awareness is not just an isolated technical skill, but an integral part of the formation of a holistic critical mindset. A student

DOI: 10.5281/zenodo.17424000
Vol: 62 | Issue: 10 | 2025

with a high cyber awareness naturally tends to systematically skepticism, careful verification, and critical thinking about all the information they receive across the digital environment. This same mindset is the cornerstone of high-quality historical research methodology; it leads the researchers not to easily accept any source, to thoroughly search for evidence, and to compare accurately. Between multiple narratives, in-depth assessment of authors' credibility and websites.

3.4.2. Testing the second main hypothesis the null hypothesis stated that "there were no statistically significant differences at the level of significance (α≤0.05) in the level of awareness of cyber risks among students of the Department of History attributed to the gender variable." To test this hypothesis, the Independent Samples T-Test was used, and Table 6 shows the results.

Table 6: Results of Test "T" for Differences in Cyber Risk Awareness by Gender Variable

Sex	Number	Arithmetic mean	Standard deviation	Calculated "F" value	Degrees of freedom	Semantic level (. sig.)	Resolution
male	35	4.0211	1.02934	2.581	69	0.113	Acceptance of the null hypothesis
female	36	4.3249	.47052				

The results of Table (6) show that **the value of the significance level (Sig. = 0.113)** is greater than (α≤0.05).

Therefore, there were no statistically significant differences in the level of cyber risk awareness between male and female students. Based on this result, the second null hypothesis is accepted.

Discussion of the result: This result indicates that cyber awareness challenges are a general phenomenon that is not limited to one gender over the other within the study sample.

This means that any educational programs or interventions aimed at raising awareness must be inclusive and target all students without discrimination based on gender, because the knowledge and skill gap, if any, exists in all students in a similar manner.

4. FOURTH THEME: CONCLUSIONS AND RECOMMENDATIONS

4.1. Conclusions

- Based on the analysis of the data and the presentation of the above results, the following conclusions were reached:
- **Level of cyber awareness:** The general level of awareness of cyber risks among students of the Department of History at Zarqa University is within **the high level** (average of 4.1751.
- **Awareness variation:** There is a variation in students' awareness, as they are more aware of direct and basic technical practices (such as their digital fingerprint, sender identity check), while some other practices (such as avoiding shortened links) tend to be relatively less proficient but still at a high level.
- **Quality of Historical Research Practices:** The overall level of quality of students' historical research methodology practices is within **the high level** with an average of 4.1794.
- **Strengths of Historical Research:** Students are highly proficient in basic and advanced research skills (such as reviewing recent literature, using keywords, critiquing sources internally and externally, and distinguishing primary and secondary sources).

DOI: 10.5281/zenodo.17424000
Vol: 62 | Issue: 10 | 2025

- **Correlation:** There is **a strong positive and statistically significant correlation** between cyber risk awareness and the quality of historical research methodology. The greater the awareness of cyber risks, the significantly improved the quality of historical research.
- **Gender differences:** There are no statistically significant differences in the level of cyber risk awareness that can be attributed to the gender variable.

4.2. Recommendations

- In light of the above conclusions, the researchers recommend the following:
- **At the level of the university and the Ministry of Higher Education:**
- **Compulsory Course Development: An** intensive and long-term compulsory course or workshop should be developed within the requirements of the university or college, under the title "Digital Literacy and Academic Integrity". This course should focus on in-depth critical thinking skills, enhancing the ability to systematically evaluate digital resources, and rooting the ethics of scientific research in the rapidly evolving digital age.
- **At the level of the Department of History and faculty members:**
- **Integrating the critique of digital resources:** The topic of "Criticism of Digital Sources" should be integrated as an integral part of historical research methodology courses, with intensive exercises and practical applications devoted to various digital documents and resources, to enable students to deal critically with them.
- **Specialized Practical Workshops:** Organizing specialized practical workshops focusing on how to best use prestigious global historical databases, explore digital archives, and apply fact-checking tools for images and information to ensure accuracy and reliability.
- **Biographical evaluation of historians:** Encourage students in their research to delve into the biographical evaluation of historians who cite their works, and to analyze their motivations and intellectual and social backgrounds, as an essential part of the process of comprehensive historical criticism.
- **At the level of the university administration:**
- **Periodic awareness campaigns:** Launch periodic and innovative awareness campaigns on the latest cyber threats targeting students specifically (such as targeted phishing, disinformation, social engineering), in close cooperation with cybersecurity experts to provide meaningful and up-to-date content.

References

First: Arabic References:

1) Al-Obaidi, Fahd; and Al-Shamrani, Ali. (2024). The degree of awareness of university students in Saudi Arabia about cyber risks and their relationship to their digital behaviors. *Arab Journal for Security Studies, 40*(1), 95-120.

2) Salem, Majid Saddam. (2022). Iraqi cybersecurity and its impact on state security. *Journal of Political Science, (64),* 335-364.

3) Jeweler, Noura Omar; (2020). Teachers' awareness of cybersecurity and methods to protect students from cyber risks. *Saudi Journal of Educational Sciences, (22),* 1-35.

DOI: 10.5281/zenodo.17424000
Vol: 62 | Issue: 10 | 2025

Second: Foreign References:

1) Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*(4), 276-289.

2) Al-Harbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing, 5*(2), 23.

3) Choo, K.-K.R. (2011). The cyber threat landscape: challenges and future research directions. *Computers & Security, 30*(8), 719-731.

4) Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology innovation management review, 4*(10).

5) Georgiadou, A., Michalitsi-Psarrou, A., & Askounis, D. (2023). A security awareness and competency evaluation in the energy sector. *Computers & Security, 129*, 103199.

6) Huraj, L., et al. (2023). Measuring Cyber Security Awareness: A Comparison between Computer Science and Media Science Students. *TEM Journal, 12*(2), 623–633.

7) Milmo, D. (2024, February 7). Ransomware gangs staged a "major comeback" last year. *The Guardian*. Retrieved from