JEC | Journal of Educational Chemistry

Journal of Educational Chemistry (6(1), 2024, 11-16)
Website:
https://journal.walisongo.ac.id/index.php/jec/index
ISSN 2715-3029 (p) 2685-4880 (e)
DOI: 10.21580/jec.2024.6.1.17010

Cybercrime: An Empirical Study of its Impact on Society- A Case Study of Chemistry Students

Ahmed Al-Ani[1*], Ahmed A. Yousif[2], Waled Abdo Ahmed[3], Emad Yousif[4]
[1,4)]Department of Chemistry, College of Science, Al-Nahrain University, Iraq
[2)]Department of Mathematics and Computer Applications, College of Science, Al-Nahrain University, Iraq
[3)]Department of Chemistry, Faculty of Education, Thamar University, Yemen
*E-mail Corresponding Author: dr.ahmedalani75@gmail.com

Abstract

Cybercrime is considered one of the most significant crimes effecting people and society. Computer network are involved in this type of crime, with various hackers participating. Through such crime, identities and much information of the victims are stolen. Many students, especially international students and young individuals, fall victim to this fraud. This study focuses on raising awareness among people to avoid scammer's link or unknown websites that seek to obtain their information. This will be achieved by organizing different questionnaires by teaching staff at one of the Iraqi Universities in this field, to be answered by undergraduate and postgraduate students. The statistical analysis conducted on this group showed that students are more educated and aware, making them less likely to fall victim to these types of crime. This is a result of the knowledge and skills these students acquired through technology and various sessions and training at universities or other resources.

Keywords: chemistry students; cybercrime; suspicious links; websites

Abstrak

Kejahatan dunia maya dianggap sebagai salah satu kejahatan paling signifikan yang berdampak pada manusia dan masyarakat. Jaringan komputer terlibat dalam kejahatan jenis ini, dengan berbagai peretas berpartisipasi. Melalui kejahatan tersebut, identitas dan banyak informasi para korban dicuri. Banyak pelajar, terutama pelajar internasional dan generasi muda, menjadi korban penipuan ini. Studi ini berfokus pada peningkatan kesadaran masyarakat untuk menghindari tautan penipu atau situs web tidak dikenal yang berupaya mendapatkan informasi mereka. Hal ini akan dicapai dengan mengorganisir kuesioner yang berbeda oleh staf pengajar di salah satu Universitas Irak di bidang ini, untuk dijawab oleh mahasiswa sarjana dan pascasarjana. Analisis statistik yang dilakukan terhadap kelompok ini menunjukkan bahwa pelajar lebih terdidik dan sadar, sehingga kecil kemungkinan mereka menjadi korban kejahatan semacam ini. Hal ini merupakan hasil dari pengetahuan dan keterampilan yang diperoleh para siswa melalui teknologi dan berbagai sesi dan pelatihan di universitas atau sumber daya lainnya.

Keywords: kejahatan dunia maya; mahasiswa kimia; tautan mencurigakan; website

Introduction

In recent years, with the advancement of technology, cybercrime has increased significantly. This includes fraud, threats, blackmail, and other illegal activities conducted via computers or online resources (Vasileiou & Furnell, 2019; Vincent, 2017). Cybercrime is considered as one of the most important and serious crimes today. The impacts of this type of crime are substantial and catastrophic, leading to bankruptcy and unemployment (Das, Nayak, & technologies, 2013; Melick, 2003; Mokha & Sciences, 2017). Identity theft can result in falling credit scores, loss of reputation, and legal troubles.

Most cybercrime targets information about governments, individuals, and corporations. Although the attacks do not occur on physical bodies, they affect personal or corporate virtual identities, which are the sets of informational attributes that define people and institutions on the Internet (Britt & Sociology, 1994). In other words, in the digital age, our virtual identities are essential elements of everyday life; we are a collection of numbers and identifiers in multiple computer databases owned by governments and corporations. Cybercrime highlights the significance of networked computers in our lives and the apparent vulnerabilities of individual identity (Cantor & Land, 1985).

Cybercrime is a fast growing area of crime. Cybercriminals are exploiting the internet to commit a diverse range of criminal activities. In the past, cybercrime was mainly committed by individuals or small groups, but now cybercriminals consist of various groups/categories such as professional hackers, organized hackers, children and adolescents between the ages of 6-18 years, scammers, phishers, insiders, malware authors, and spammers (Barclay, 2017; Donalds, Barclay, & Osei-Bryson, 2022).

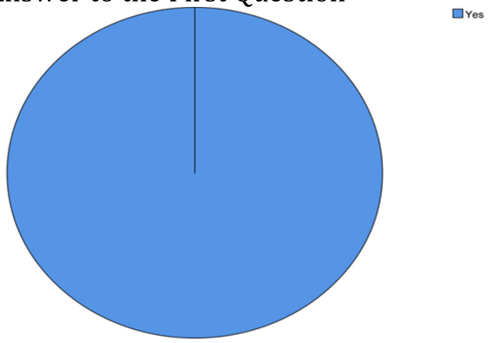
Method

We conducted a survey to gather information about victims of cybercrime and the resources vulnerable to such offenses. It included different questions answered by students. The responses were analyzed and discussed to identify tools and solutions to prevent any type of cybercrime in the future. The survey involved ninety one students who were asked ten different questions about cybercrime. We collected various data through these questions and then performed statistical analysis to finalize the results. The questions related to cybercrime were presented to each participant in the survey.

Results and discussion

In this survey, the random sample (r.s) consisted of ninety one (91) individuals. They were asked ten questions about cybercrime. The survey were analyzed to draw conclusions about the impact and awareness of cybercrime among the respondents. The first question was, "Have you ever heard about cybercrime?" and all respondents in the random sample answered yes, as shown in the Figure 1:

Figure 1
The Answer to the First Question



The second question was, “If so, how?” There were four choices for the respondents: family, friends, social media and others.

Most of the respondents heard about cybercrime through social media, followed by friends, with equal ratio from family and other sources. Other sources may include hearing about cybercrime from colleagues at work, university professors, or any other resources. The percentages are shown in the Table 1.

Table 1
Different Resources Through which Respondents Heard about Cybercrime

	Frequency	Percent	Valid Percent
Family	5	5.49%	5.49%
Friends	16	17.58%	17.58%
Social Media	65	71.43%	71.43%
Others	5	5.49%	5.49%
Total	91	100.0%	100.0%

The third question was, “You can avoid cybercrime by” (Waschke, 2017). There were three choices for the respondents: (1) Not following any suspicious links/websites or answering suspicious calls,(2) Clicking any links received to see what it is, and (3) Others.

Most of the respondents indicated that they could avoid cybercrime by “Not following any suspicious links/websites or answering suspicious calls”, followed by "Others,” and a few chose “Clicking any links received to see what it is.” The percentages are shown in the Table 2.

Table 2
Different Resources Through which Respondents Heard about Cybercrime

	Frequency	Percent	Valid Percent
Not following any suspicious links/websites or answering suspicious calls	80	87.91%	87.91%
Clicking any links received to see what it is	4	4.40%	4.40%
Others	7	7.69%	7.69%
Total	91	100.0%	100.0%

The fourth question was, “There are different types of cybercrime, it could be” (Yadav, Gautam, Rana, Bhardwaj, & Tyagi, 2021). There were five choices for the respondents: Hacking, Malware, Phishing Scams, All of them and others.

Most of the respondents chose “All of them,” with equal ratios for “Malware,” and “Phishing Scams,” followed by “Hacking,” and a few chose ”Others”. The "Others" category included responses such as professional hackers using level 5 and above tools like Kali Linux, which is a cunning, complex and malicious program with several ways to steal information, electronic extortion, identity fraud, and data theft. The percentages are shown in the Table 3.

Table 3
Different Resources Through which Respondents Heard about Cybercrime

	Frequency	Percent	Valid Percent
Hacking	7	7.69%	7.69%
Malware	14	15.38%	15.38%
Phishing Scams	14	15.38%	15.38%
All of them	54	59.34%	59.34%
Others	2	2.20%	2.20%
Total	91	100.0%	100.0%

The fifth question was, "Scammers can use many ways to make victims (students) follow what they need (Button, Nicholls, Kerr, Owen, & criminology, 2014).There were three choices for the respondents: Ask personal questions, ask general questions, and others.

Most respondents chose "Ask personal questions", followed by "Ask general questions," with a few chose "Others." The "Others" category included methods such as finding the student's phone number and retrieving all information from it, advising against giving phone number to unofficial parties or a strangers, buying books from fake websites to send money, and asking personal and general questions. The percentages are shown in the Table 4.

Table 4

Different Ways Scammers Use to Make Victims Follow Their Instructions

	Frequency	Percent	Valid Percent
Ask personal questions	70	76.92%	76.92%
Ask general questions	18	19.78%	19.78%
Others	3	3.30%	3.30%
Total	91	100.0%	100.0%

The sixth question was, "The recipient should be more educated to not be a victim of fraud that may be done by" (Bele, Dimc, Rozman, & Jemec, 2014). There were three choices for the respondents: Different sessions should be done by government to get more information about cybercrime, Doing what people do according to their background or general information, and others.

Most of the respondents chose "Different sessions should be done by government to get more information about cybercrime," followed by "Doing what people do according to their background or general information," and a few chose "Others." The "Others" category included suggestions such as localized forums to educate people, bringing people closer who you do not know well, maintaining superficial relationships, and being smart and committed to avoid exposure to such risks alone. The percentages are shown in the table and figure below:

Table 5

Ways to Avoid Becoming a Victim of Cybercrime

	Frequency	Percent	Valid Percent
Different sessions should be done by government to get more information about cybercrime	76	83.52%	83.52%
Doing what people do according to their background or general information	12	13.19%	13.19%
Others	3	3.30%	3.30%
Total	91	100.0%	100.0%

The seventh question was, "Government should have the responsibility to ban any suspicious links or websites. There were two choices for the respondents: True, False. Most respondents chose "True." The percentages are shown in the Table 6.

Table 6
Responses on Government Responsibility to Ban the Suspicious Links or Websites

	Frequency	Percent	Valid Percent
True	83	91.21%	91.21%
False	8	8.79%	8.79%
Total	91	100.0%	100.0%

The eighth question was, "If someone is a victim of fraud, what should they do?" (Levi & Pithouse, 1992). There were three choices for the respondents: Contacting the hotline available for this purpose, Telling friends, and others).

Most of the respondents chose "Contacting the hotline available for this purpose," followed by "Tell friends," and the lowest choice was "Others" included actions such as trying to contact someone with experience in this field, Telling a family member who cares about them, taking action in a smart way, going to a trusted programming center to recover and secure their account, consulting a trusted hacker to retrieve their information, and contacting the police. The percentages are shown in the Table 7.

Table 7
Actions People Take if They Become Victim of Cybercrime

	Frequency	Percent	Valid Percent
Contacting the hotline available for this purpose	78	85.71%	85.71%
Telling friends	7	7.69%	7.69%
Others	6	6.59%	6.59%
Total	91	100.0%	100.0%

The ninth question was, "Do you think it is important that people need to know about cybercrime?" There were three choices for the respondents: Yes, No and I don't know.

Most of the respondents chose "Yes," followed by "I don't know," and a few chose "No". The percentages are shown in the Table 8.

Table 8
Responses on the Importance of People Knowing About Cybercrime

	Frequency	Percent	Valid Percent
Yes	88	96.70%	96.70%
No	1	1.10%	1.10%
I don't know	2	2.20%	2.20%
Total	91	100.0%	100.0%

The last question was, "Are you interested in knowing more about cybercrime in the future? There were three choices for the respondents: Yes, No and I don't know. Most of the respondents chose "Yes," followed by "I don't know," and a few chose "No." The percentages are shown in the Table 9. From the analysis done in this study, all responses were logical and focused on the main objectives of the report.

Table 9
Responses on the Importance of People Knowing About Cybercrime

	Frequency	Percent	Valid Percent
Yes	82	90.11%	90.11%
No	1	1.10%	1.10%
I don't know	8	8.79%	8.79%
Total	91	100.0%	100.0%

Conclusion

Cybercrime is not only a violation of the law but also an infringement on human rights. It is a dangerous offense that threatens someone's privacy and other material aspects. This can be avoided by following basic logical practices and using common sense. This study primarily focused on students, who are among the most vulnerable groups to cybercrime. It was concluded that students are more mature and mindful about cybercrime, and they have enough information to avoid following or engaging with suspicious websites or links. Additionally, students should enhance their knowledge of technology and the various types of cybercrime by attending educational sessions and utilizing diverse resources. This will help them avoid becoming victim of scammers.

References

Barclay, C. J.. (2017). Cybercrime and Legislation: a Critical Reflection on the Cybercrimes Act, 2015 of Jamaica. *Commonwealth Law Bulletin*, 43(1), 77-107.

Bele, J. L., Dimc, M., Rozman, D., & Jemec, A. S. (2014). *Raising Awareness of Cybercrime--The Use of Education as a Means of Prevention and Protection*: ERIC.

Britt, C. L.. (1994). Crime and Unemployment Among Youths in the United States, 1958-1990: A Time Series Analysis. *American Journal of Economics and Sociology*, 53(1), 99-109.

Button, M., Nicholls, C. M., Kerr, J., Owen, R. J. A., & criminology, N. Z. j. o. (2014). Online Frauds: Learning from Victims Why They Fall for These Scams. *Australian & New Zealand Journal of Criminology*, *47*(3), 391-408.

Cantor, D., & Land, K. C.. (1985). Unemployment and Crime Rates in the Post-World War II United States: A Theoretical and Empirical Analysis. *American Sociological Review*, 50(3), 317-332.

Das, S., & Nayak, T. J.. (2013). Impact of Cybercrime: Issues and Challenges. *International Journal of Engineering Sciences & Emerging Technologies*, 6(2), 142-153.

Donalds, C., Barclay, C., & Osei-Bryson, K.-M. (2022). *Cybercrime and Cybersecurity in the Global South: Concepts, Strategies and Frameworks for Greater Resilience*: London: Routledge.

Levi, M., & Pithouse, A. (1992). The victims of fraud. In *Unravelling Criminal Justice: Eleven British Studies*. London: Springer.

Melick, M.. (2003). The Relationship Between Crime and Unemployment. *The Park Place Economist*, 11(1), 30-36.

Mokha, A. K.. (2017). A Study on Awareness of Cyber Crime and Security. *Research Journal of Humanities and Social Sciences*, 8(4), 459-464.

Vasileiou, I., & Furnell, S. (2019). *Cybersecurity Education for Awareness and Compliance*. Hershey: IGI Global.

Vincent, N. A. (2017). *Victims of Cybercrime: Definitions and Challenges*. In *Cybercrime and its Victims*. London: Routledge.

Waschke, M. (2017). *Personal Cybersecurity: How to Avoid and Recover from Cybercrime*. London: Springer.

Yadav, H., Gautam, S., Rana, A., Bhardwaj, J., & Tyagi, N. (2021). *Various Types of Cybercrime and its Affected Area. Data Mining and Information Security: Proceedings of IEMIS 2020*, Volume 3.