ISSN:
Vol. 1, No. 1, Jan. 2024

CORE GATEWAY COLLEGE, INC.
FOUNDED 1948

CGCI - IJAMET

CGCI International Journal of Administration, Management, Education and Technology

Available at
www.cgci-ijamet.org/index.php/cgci-ijamet

Published by
Core Gateway College, Inc.

CGCI International Journal of Administration, Management, Education and Technology

Volume 1 **Number 1**

January 2024

CGCI IJAMET

ISSN:

Recommended Citation

(January 2024) CGCI International Journal of Administration, Management, Education and Technology, Vol.1, No.1. Available at https://www.cgci-ijamet.org/index.php/cgci-ijamet/about

CGCI International Journal of Administration, Management, Education, and Technology (CGCI-IJAMET) accepts original research that addresses the problems of the developing world. This includes education, public administration, political science, management, policy, governance, gender and development, information technology, and other social science studies.

Copyright & Disclaimer

CGCI International Journal of Administration, Management, Education and Technology

Ad Hoc Board of Reviewers

Cybersecurity Awareness of College Students in a Private Higher Education Institution

Buenaventura L. Alabab Jr.[1], Jonathan S. Cubol[2], Michael Angelo C. Pascual[3], Ednalyn S. Ubaldo[4], Divina Roma D. Sario[5], and Marjorie S. Velasco[6]

Core Gateway College, Inc. San Jose City, Nueva Ecija,Philippines[1]
Core Gateway College, Inc. San Jose City, Nueva Ecija,Philippines[2]
Core Gateway College, Inc. San Jose City, Nueva Ecija,Philippines[3]
Core Gateway College, Inc. San Jose City, Nueva Ecija,Philippines[4]
Core Gateway College, Inc. San Jose City, Nueva Ecija,Philippines[5]
Core Gateway College, Inc. San Jose City, Nueva Ecija,Philippines[6]

Corresponding author's email : randy.a257@gmail.com[1], jonathancubol4@gmail.com[2], fishykhel@gmail.com[3], ubaldoednalyn5409@gmail.com[4], ddsario@cgci.edu.ph[5], and msvelasco@cgci.edu.ph[6]

Submitted October 2023, Accepted November 2023, Published online December 2023

ABSTRACT

The study assessed the cybersecurity awareness of college students at CGCI, San Jose City, in response to the rising cyber-attack threats. A quantitative approach, particularly a descriptive-correlational research design, was used in the study. The questionnaire was distributed to 291 students across various programs in the institution. Despite advancements in legislation, Filipinos, including students, remain vulnerable. Thus, this research indicates that even Computer Science students fall victim to cyber-attacks. The result revealed that the respondents strongly agree with cybersecurity awareness, which implies that the institution's students knew cybersecurity-related things. Meanwhile, only age was found to be significantly correlated to the level of awareness of the respondents on cybersecurity, which illustrates that respondents' awareness of cybersecurity risks and threats increases with age. In addition, respondents are becoming more conversant with cyberattacks.

Keywords: awareness, cyber-attacks, cybersecurity, identity theft, phishing,

INTRODUCTION

The first recorded cybercrime in the Philippines was the "I Love You" virus, released on May 4, 2000 (Ibrahim, 2023). The case filed against the virus's author was dismissed at the first stage because no law punished the deed then (Department of Justice, 2012). Since then, Philippine lawmakers have contributed time and effort to pass Republic Act 10175, also known as the Cybercrime Prevention Act of 2012. The purpose of the law is to address legal issues concerning internet online interactions in the Philippines. Cybercrimes punishable by the law include but are not limited to cybersquatting, cybersex, child pornography, identity theft, illegal access to data, and libel.

Cybersecurity awareness is vital to protect information and computer systems from malicious cyber threats and attacks (Gade & Reddy, 2014). Filipinos are susceptible to cyberattacks, particularly to phishing and malware attacks. Likewise, internet security perception is derivative: they practice online measures with a limited understanding of the purpose (Omorog & Medina, 2017). Even "hacker" and "hacking" are misunderstood and stereotyped as illegal and taboo in cyberspace. The Philippines will consistently remain vulnerable to cybersecurity attacks due to Filipino end users lacking IT security knowledge and skills.

According to Liu et al. (2013), Educational institutions face higher risks of losing valuable intellectual property, research data, and personal information about the students, staff, and faculty. Researchers such as Vrana (2012) and Muniandy et al. (2017) claimed that the current students were heavy Internet users.

As had been observed by the researchers, even Bachelor of Science in Computer Science students at Core Gateway College, Inc. (CGCI) are also susceptible and become victims of cyber-attacks like phishing, scams, and identity theft. Sometimes last year, one of the researchers received several messages that said, "*Ikaw ba itong nasa sex video?* (Is this you in the sex video?)" with a possible malicious link attached. Ironically, one of the messages came from a Computer Science student, who should be expected to be aware of cybersecurity. These are possible cases of compromised accounts and were being used to disseminate the

malicious links to escalate the number of victims. Further, the attackers used phishing where they were sending or tagging, especially on Facebook, as many as they could with links they had created, of which, when a victim clicked on it, they could get their login credentials.

Hence, this study was conducted to measure the level of awareness and provide recommendations for enhancing students' cybersecurity knowledge. Likewise, the result of this study may also help the students avoid falling victim to the growing number of cyber-attacks, mitigate the risk, and strengthen their awareness.

METHODS AND PROCEDURE

The researchers used the quantitative method, particularly the descriptive–correlational research design. The study focused on measuring the level of cybersecurity awareness of college students at CGCI during the School Year 2023 – 2024. A researcher's questionnaire was pre-tested on 20 students not included in the respondents. A Cronbach alpha value of 77.86% was obtained on cybersecurity awareness, meaning the instrument was reliable. Moreover, the survey questionnaire was administered to 301 students. However, only 291 voluntarily participated in the study. Before disseminating the questionnaires, necessary permission and approval from the proper authorities were also secured. The researchers personally distributed the questionnaire to the respondents. The data was analyzed using percentage, frequency count, mean, standard deviation, and Pearson Product Moment Correlation (r). A four-point Likert scale was utilized in the study to measure the level of awareness of the respondents on cybersecurity.

RESULT AND DISCUSSION

Profile of the Respondents

The dominant age range is between 17 and 21 (75.60%). Almost all (96.22%) respondents were single, and 3.78% were married. Less than half (33.68%) of the respondents are from the Bachelor of Arts in Political Science (BAPS). Results also showed that 1st-year students have the most significant respondents (36.43%). More than sixty percent (62.54%) of the respondents were females. Moreover, most of them (76.63%) had not been a victim of any cyber-attack. Data is presented in Table 1.

Table 1. Profile of the Respondents

PROFILE	FREQUENCY	PERCENTAGE
Age		
17-21	220	75.60
22-26	44	15.12
27-31	17	5.84
32-36	8	2.75
37-41	1	0.34
42-46	1	0.34
	Mean: 21.15 **SD: 3.69**	
Civil Status		
Single	280	96.22
Married	11	3.78
Course		
BAPS	98	33.68
BEED	16	5.50
BSBA	70	24.05
BSCS	30	10.31
BSED	77	26.46
Year Level		
1st Year	106	36.43
2nd Year	53	18.21
3rd Year	99	34.02
4th Year	33	11.34
Sex		
Male	109	37.46
Female	182	62.54

Victim of cyber-attack		
Yes	68	23.37
No	223	76.63

Cybersecurity Awareness of the Respondents

Based on the results, the cybersecurity awareness of the respondents obtained a pooled mean of 3.26, described as "*Strongly Agree*." It implies that the college students in the institution were aware of cybersecurity. Moreover, the statement "I am informed that updating passwords and using strong and unique ones for different accounts can help protect my data" got the highest mean of 3.50, described as "*Strongly Agree*." It indicates that the respondents were aware of data security processes and methods which is very helpful in protecting their information. In contrast, "I am aware of cybersecurity, threats, and risks" got the lowest mean of 3.01, also described as "*Agree*." It revealed that although the respondents were aware of cybersecurity threats and risks, they only had limited knowledge. Perhaps the respondents have very limited self-enrichment to improve their security awareness.

Cybersecurity is equivalent to computer security, also known as cybersecurity or IT security. It protects computer systems from damaging their hardware, software, or information and disrupting or misdirecting their services (Roca et al., 2019). Research by Rajeswari et al. (2022) revealed that even though Universiti Teknologi MARA (UiTM) Terengganu Faculty of Computer Science students demonstrated a decent level of awareness of some aspects of cyber security such as cyber-attack, cyberbullying, and personal information. Meanwhile, a study by Omorog and Medina (2017) suggests using more than the recommended password length and format to avoid cyber-attacks.

Table 2. Cybersecurity Awareness of the Respondents

	STATEMENT	MEAN	DESCRIPTION
1.	I am aware of cybersecurity threats and risks.	3.43	Strongly Agree
2.	I am familiar with cybersecurity attacks like phishing, identity theft, malware, etc.	3.27	Strongly Agree
3.	I know how to spot potential threats that cause damage to the data.	3.01	Agree
4.	Updating passwords and using strong and unique ones for different accounts can help protect my data.	3.50	Strongly Agree
5.	I know how to update software and operating systems to ensure security.	3.16	Agree
6.	I know how to use privacy settings on social media platforms to protect my personal information.	3.42	Strongly Agree
7.	I understand using multi-factor authentication for online accounts such as Facebook, Google, Yahoo!, Outlook, etc.	3.35	Strongly Agree
8.	I know the risks of using public Wi-Fi networks and take necessary precautions.	3.23	Agree
9.	I know how to identify and avoid phishing scams.	3.09	Agree
10.	I know the risks of using USB drives from unknown sources and take the necessary precautions.	3.17	Agree
	Pooled Mean	**3.26**	**Strongly Agree**

Legend

3.25 – 4.00	Strongly Agree
2.50 – 3.24	Agree
1.75 – 2.49	Disagree
1.00 – 1.74	Strongly Disagree

Relationship Between Profile of the Respondents and Their Level of Awareness of Cybersecurity

Findings show a significant correlation between the respondents' age and their awareness level in Q1 (r = 0.122) and Q2 (r = 0.124). It implies that older respondents become more aware of cybersecurity threats and risks. Additionally, the respondents are getting more familiar with cybersecurity attacks. Since the respondents are in tertiary education, they frequently utilized the Internet or other technological tools in their study. The study by Fatokun et al. (2019) showed that older students were more careful with security

awareness and practiced good cybersecurity. However, those younger students were more familiar with cyber threats. Meanwhile, in a phishing experiment conducted by Mohebzada et al. (2012), younger students between the age of 18 and 21 years were less susceptibility to phishing than older students, which contradicts some other studies (Darwish et al., 2012; Arachchilage, 2014) that states that the younger the age, the higher the susceptibility to phishing and other cyber-attacks.

Overall, only age was significantly correlated to the level of awareness of the respondents on cybersecurity.

Table 3. Relationship Between Profile of the Respondents and Their Level of Awareness

PROFILE	LEVEL OF AWARENESS									
	Q1	**Q2**	**Q3**	**Q4**	**Q5**	**Q6**	**Q7**	**Q8**	**Q9**	**Q10**
Age	0.123*	0.124*	0.049	0.057	0.016	0.057	0.088	0.085	0.082	0.058
Sex	-0.097	-0.03	-0.113	0.064	-0.027	0.096	0.079	-0.048	-0.052	-0.114
Civil Status	0.039	0.063	-0.061	-0.044	0.063	0.012	0.094	-0.048	0.026	-0.081
Course	0.049	-0.02	0.032	0.052	0.066	0.025	-0.004	0.009	0.053	0.05
Year Level	0.025	0.067	0.012	0.100	-0.003	0.053	0.088	0.036	0.051	0.06

CONCLUSIONS

Based on the data gathered and analyzed, it is concluded that the students of CGCI were aware of cybersecurity. However, the contexts about identifying and avoiding cybersecurity threats yield the lowest means; therefore, they were not very aware of it. It is also concluded that only age correlates with the respondents' cybersecurity awareness level.

RECOMMENDATIONS

Although college students at CGCI are aware of cybersecurity, it is also recommended to have at least seminars, training, or disseminate cybersecurity infographics, either by flyers or through posting on the official social media accounts of the school, to further raise awareness and knowledge of the students about cybersecurity. It is necessary because cybercriminals are also developing ways to take advantage of the most significant vulnerability in human nature – trust.

REFERENCES

Arachchilage NAG (2014). Love S. Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior. 2014;38:304-12

Darwish A, El Zarka A, Aloul F, (2012). Towards understanding phishing victims' profiles. 2012 International Conference on Computer Systems and Industrial Informatics; 2012: IEEE.

Department of Justice (2012). Primer on Cybercrime - Department of Justice. https://www.doj.gov.ph/files/2012/Primer_on_Cybercrime.pdf

Fatokun, F B *et al* (2019). The Impact of Age, Gender, and educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities. *J. Phys.: Conf. Ser.* 1339 012098**DOI** 10.1088/1742-6596/1339/1/012098

Gade, N.R. & Reddy, U. (2014). A Study of Cyber Security Challenges and Its Emerging Trends On Latest Technologies.

Ibrahim, A. (2023). The First Computer Virus in The Philippines – ILOVEYOU Virus. https://ticktocktech.com/blog/2023/06/08/the-first-computer-virus-in-the-philippines-iloveyou-virus

Liu, X., Zhang, Y., Wang, B., and Yang J. (2013). Mona: Secure Multi-owner data sharing for dynamic groups in the cloud. IEEE Trans. *Paraller Dist. Syst.* Vol. 24, no.6 pp.1182-1191

Mohebzada J, El Zarka A, BHojani AH, & Darwish A, (2012). Phishing in a university community: Two large scale phishing experiments. Innovations in Information Technology (IIT), 2012 International Conference on; 2012: IEEE.

Muniandy, L. Muniandy, B. & Samsudin, Z. (2017). Cyber Security Behavior among Higher Education Students in Malaysia. *Journal of Information Assurance & Cybersecurity.* 1-13.

Omorog, C., & Medina, R. (2018). Internet security awareness of Filipinos: A survey paper. *International Journal of Computing Sciences Research*, *1*(4), 14–26. https://doi.org/10.25147/ijcsr.2017.001.1.18

Rajeswari R., Nur Hidayah, A., Atif, A. (2022). Cyber Security Awareness in Using Digital Platforms Among Students in A Higher Learning Institution. *Asian Journal of University Education (AJUE) Volume 18, Number 3*. https://doi.org/10.24191/ajue.v18i3.18967

Republic Act No. 10175 s. 2012. Cybercrime Prevention Act of 2012. https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/

Roca, V. Kemer, S. Remy, D. & Me, L. (2019). Cybersecurity Current Challenges and Inria's Research Directions. Le Chesnay Cedex, France: Inria

Vrana, R. (2012). “Internet a safer place: students’ perceptions about Internet security threats,” In Central European Conference on Information and Intelligent Systems, Croatia, 19-21 September 2012.

Call for Papers

The CGCI International Journal of Administration, Management, Education, and Technology (CGCI IJAMET) is open to all research papers from any field of discipline across various themes that contribute to further learning and continuing professional development.

The Research Review Committee looks forward to receiving full research papers from interested scholars and researchers in response to the call before June and December of the year, as this is the scheduled publication of the journal each year. CGCI IJAMET is happy to respond to inquiries from interested parties. Questions may be addressed to CGCI IJAMET at coregatewaycollege@cgci.edu.ph. Your participation in this effort to produce new papers will contribute to the written body of helpful knowledge for the world and human development!

Core Gateway College, Inc.
Maharlika Highway, Cor. Cardenas St., San Jose City, Nueva Ecija 3121
www.cgci-ijamet.org/index.php/cgci-ijamet