Business, Management and Economics Engineering
ISSN: 2669-2481 / eISSN: 2669-249X
2022 Volume 20 Issue 2

A QUANTITATIVE RESEARCH ON AWARENESS ABOUT PHISHING ATTACKS AMONG COLLEGE STUDENTS IN MADURAI.

Dr.N.Prakash[1] and Mrs.P.Reshma[2]
[1]Assistant Professor, Department of Management Studies, The American College.
[2]Assistant Professor, Department of Management Studies, The American College
Email: prakash@americancollege.edu.in [1], reshma@americancollege.edu.in[2]

ABSTRACT

Cyber attacks have been widespread since the rampant usage of the internet. They are either web-based attacks or system-based attacks. Phishing is one of the oldest web-based crimes that has been the choice of hackers and cybercriminals worldwide. Emerging technologies like cloud computing, smartphone technologies are subject to new attack patterns that exploit personal security. Lack of awareness among students makes them volatile in being exploited by others. Through this paper, the researchers wish to establish awareness about phishing attacks among the college-going students and to understand the security awareness among the students against phishing. This paper also aims to enable students to sense phishing attacks and raise complaints to relevant authorities. Data was collected from 92 college students within Madurai, Tamilnadu. It is found that the younger generation students are mostly aware about phishing and its security methods.

Keywords: Phishing attacks, Cyber security, Awareness

INTRODUCTION

The act of tricking individuals into divulging their sensitive information and using it for malicious purposes is not new. Social engineering attacks have occurred on the internet throughout its existence. Before widespread use of the internet, criminals used the telephone to pose as a trusted agent to acquire information. Cyber-attacks can be classified into web-based attacks and system-based attacks. Web-based attacks occur in websites or web applications. DNS spoofing, injection attacks, session hijacking, Denial of Service and phishing are some of the web-based attacks.

The term “phishing” originated in the mid-1990s, when it was used to describe the acquisition of internet service provider (ISP) account information. However, today the term has evolved to encompass a variety of attacks that target personal information (Jason Milletary, 2005). Phishing attacks are of different types like email phishing, spear phishing, vishing and smishing, clone phishing, pharming, HTTPS-Phishing, Pop-Up Phishing, Evil-Twin Phishing.

- Email phishing - Email is the most popular phishing medium. Scammers register fake domains that impersonate real organizations and send thousands of requests to their targets.
- Spear phishing attack - targets a specific individual or set of individuals rather than sending generic messages to many users in the hope that one falls for the trick.

- Vishing and smishing - With smishing, the attackers send text messages with similar deceptive content to a phishing email. Vishing involves phone conversations, with the scammer directly speaking to the target
- Clone phishing - the attacker copies legitimate emails previously sent by trusted entities.
- Pharming - Pharming is a highly technical form of phishing, making it harder to detect
- HTTPS-Phishing - attackers can leverage HTTPS to make their links appear legitimate and increase the success of their phishing campaigns.
- Pop-Up Phishing - Malicious actors may place malicious code in small notifications (pop-ups), which people see when they visit a website.
- Evil-Twin Phishing - Evil twin attacks often use fake WiFi hotspots that appear legitimate but can intercept sensitive data in transit.

Today, we live in a networked society with cloud computing, online transactions and other interactions made possible by Internet technology (Bendovschi, 2015). Unfortunately, the growing importance of IT also fosters an ever-growing wave of cybercrime that impacts citizens, businesses and governments (Interpol, 2017). We use cybercrime as an umbrella term to describe different online threats such as malware, scams and hacking (Verdegem, Teerlinck, & Vermote, 2015). In 2017, cybercrime reached new heights with ransomware.

The rapid growth in internet technology has made the entire society dependent on it. However, its evolution has also increased cyber fraud, thus, becoming a severe problem worldwide (Kamruzzaman, Islam, Islam, Hossain, & Hakim, 2016). Cyber fraud involves usage of internet services with internet access (Zahari, Billu, & Said, 2017).

The use of the internet has come with many cyber-related risks, these risks include cyber addiction (Annansingh, F., & Veli, T. (2016), personal information exposure (Muniandy, L & Muniandy, B (2012), personal information exposure (Anderson, G. Ktoridou, D., Eteokleous, N., & Zahariadou, A. (2012), and online fraud addiction (Mosalanejad, L., Dehghani, A., & Abdolahifard, K. (2014) & (Ratten, V. (2015). During COVID-19, 53% of the cybersecurity professionals reported a drastic increase in phishing attacks (Phishing Attack Landscape Report, 2020)

Colleges and universities have been tracking cyber-attacks rates, with many hacking attempts onto the information systems. Most of the time, students are unaware of the implications of cybercrime and predominantly girls are the most common victims of cyber-crime. While social networks and bank account details are also at higher risk, education institutions are facing risks of losing valuable intellectual property and their research data such as patents awarded to the professors and students, and also the personal information about the students, staff and faculty. Because of the higher frequency of hacking attacks on higher education institutions, the need for cyber security awareness has increased (X. Liu, Y. Zhang, B. Wang, and J. Yang, 2013).

LITERATURE REVIEW

Aida Rozihan Mohamad Asri and Irni Eliana Khairuddin (2022) in their paper titled " A theoretical framework for the awareness of Phishing attack" identified three variables influence of social engineering, anti-phishing knowledge and security concerns as the influencing factors on Generation Y's Phishing Awareness

Vishnu Renganathan, Ekim Yurtsever, Qadeer Ahmed and Aylin Yener (2022) did an in-depth analysis of the system along with privacy constraints to prevent unauthorised access and extortion of private information. In their research paper titled, "Valet attack on privacy: a cybersecurity threat in automotive Bluetooth infotainment systems".Identified Threat with respect to privacy constraints of the system was identified, a standardized rating metric used and then possible countermeasures to prevent the attack was provided.

Nur Farhana Mohd Zaharon, Mazurina Mohd Ali, and Suhaily Hasnan (2021), discussed in their paper titled "Factors Affecting Awareness of Phishing Among Generation Y" and found that the factors like social engineering, anti-phishing knowledge and security concern are significantly influencing the awareness of phishing among Generation Y in Malaysia. Asia-Pacific Management Accounting Journal, Volume 16 Issue 2.

Benjamin Reinheimer, Lukas Aldag, Peter Mayer, Mattia Mossano, Reyhan Duezguen, Bettina Lofthouse, Tatiana von Landesberger, Melanie Volkamer (2020), analyzed in their paper titled "An investigation of phishing awareness and education over time: when and how to best remind users", that Programs for security awareness and education are being implemented in more and more organisations. The effectiveness of these reminders over time and the proper intervals to raise users' awareness and knowledge are still up for debate. When phishing emails are accurately identified immediately after and four months following the program's adoption, we observe a noticeably enhanced performance. After six months, this was no longer the case, indicating that it is advisable to remind consumers every six months. The analysis of the reminder strategies reveals that those that include interactive examples and films perform best and last for at the minimum of six months.

Adamu A. Garba, Maheyzah Md.Siraj, Siti Hajar Othman and Musa M.A (2020), discussed about cybersecurity awareness in their paper titled "A Study on Cybersecurity Awareness Among Students in Yobe State University, Nigeria: A Quantitative Approach", that the awareness about the cybersecurity is at satisfactory level and the students are not well aware about protecting their data and it is more than average level only. And they found that there were no active cybersecurity awareness program for students and most of the students are becoming victims for this kind of cyber attack. They found that female respondents were more prone to cyber attacks than male counterparts.

Mohammed I Alwanain (2020), analysed in his research paper titled "Phishing Awareness and Elderly Users in Social Media" studies the level of security awareness on elderly users and their ability to detect phishing attacks in social media. He found that phishing awareness training has a significant positive effect on the ability of elderly users to identify phishing messages, and to avoid the attacks.

Senthilkumar.K and Sathishkumar Easwaramoorthy (2017), discussed in their research paper titled "A Survey on Cyber Security awareness among college students in Tamil Nadu", that cyber threats are one of the gravest national security problems that everyone is facing nowadays. Visiting the websites which are infected with malware, replying to phishing emails, strong logging information in a third-party location, or even sharing confidential information over the phone, exposing personal information to social networking tend to steal personal

information of common people. It was found that the college students in Tamil Nadu are having above average level of awareness on cyber related threat issues which can help them to protect themselves from the cyber-attacks. IOP Conf. Ser.: Materials science and Engineering.

M. S. Hasan, R. A. Rahman, S. F. H. B. T. Abdillah and N. Omar (2015), in their paper "Perception and awareness of young internet users towards cybercrime: Evidence from Malaysia" have discussed the relationship between various factors like age, of the respondents, their knowledge and awareness on cybercrime with the risks involved. They found that female students were more aware of cybercrimes than their male counterparts . Students between the age group of 18-23 were more aware of cybercrimes.

Fadi. A. Aloul (2012) in his research paper "Need for Effective Information Security Awareness", did a comprehensive wireless security survey, identified access points which were either unprotected or had weak protection across Dubai and Sharjah. This was based on several security awareness programs conducted for students and working professionals in the year 2010. The importance of assessing security awareness through audit programs were stressed.

RESEARCH METHOD AND DESIGN

An Information Schedule was created and circulated among the student fraternity using Google Forms. A quantitative approach was used to prepare the Information schedule. Apart from the demographic data, the schedule consists of questions on the phishing awareness and cyber security awareness of the students. Suitable questions were identified and customized to fit under the sub heads. In order to ensure validity, the age of the respondents has been obtained. The data was further analyzed using SPSS software.

Convenience sampling method was used to select the sample.

OBJECTIVES

1. To establish awareness about phishing attacks among the students.
2. To understand the security awareness among students against phishing attempts.
3. To assess the ability of students to sense phishing attacks and raise complaints to relevant authorities

HYPOTHESIS

Ho: Ther is a significant association between age and awareness about cybercrime toll free number.

Ha: There is no significant association between age and awareness about cybercrime toll free number.

RESULTS AND DISCUSSION

Duration of Usage of Social media per day

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0-2 hours	31	33.7	33.7	33.7
	3-5 hours	43	46.7	46.7	80.4

	6-8 hours	11	12.0	12.0	92.4
	9-11 hours	4	4.3	4.3	96.7
	> 12 hours	3	3.3	3.3	100.0
	Total	92	100.0	100.0	

Inference: It is inferred that 47% of the respondents use social media for 3-5 hours per day and 34% of the respondents use it for 0-2 hours per day.

Online shopping Frequency

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Frequently	6	6.5	6.5	6.5
	Occasionally	14	15.2	15.2	21.7
	Sometimes	34	37.0	37.0	58.7
	Rarely	31	33.7	33.7	92.4
	Never	7	7.6	7.6	100.0
	Total	92	100.0	100.0	

Inference: Nearly 37% of the respondents sometimes use online shopping and nearly 34% of the respondents rarely use online shopping methods and 15% of the respondents occasionally use online shopping.

Phishing Awareness

Phishing Awareness [I am aware that phishing is a cyber fraud...]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	40	43.5	43.5	43.5
	Agree	35	38.0	38.0	81.5
	Neutral	15	16.3	16.3	97.8
	Disagree	2	2.2	2.2	100.0
	Total	92	100.0	100.0	

Inference: From the above table it is inferred that 43% of the respondents Strongly agree that they are aware about phishing is a cyber fraud

Phishing Awareness [I read about phishing on bank websites..]

	Frequency	Percent	Valid Percent	Cumulative Percent

	Strongly Agree	28	30.4	30.4	30.4
	Agree	40	43.5	43.5	73.9
Valid	Neutral	18	19.6	19.6	93.5
	Disagree	5	5.4	5.4	98.9
	Strongly Disagree	1	1.1	1.1	100.0
	Total	92	100.0	100.0	

Inference: From the above table it is inferred that 44% of the respondents agree that they read about phishing awareness at bank website.

Phishing Awareness [I would immediately report to the banks..]

		Frequency	Percent	Valid Percent	Cumulative Percent
	Strongly Agree	39	42.4	42.4	42.4
Valid	Agree	32	34.8	34.8	77.2
	Neutral	18	19.6	19.6	96.7
	Disagree	3	3.3	3.3	100.0
	Total	92	100.0	100.0	

Inference: From the above table it is inferred that 43% of the respondents Strongly agree that they would report to the banks immediately if they sense about phishing.

Security Awareness

Security awareness [I would scan all removable drives before using..]

		Frequency	Percent	Valid Percent	Cumulative Percent
	Strongly Agree	33	35.9	35.9	35.9
	Agree	35	38.0	38.0	73.9
Valid	Neutral	20	21.7	21.7	95.7
	Disagree	2	2.2	2.2	97.8
	Strongly Disagree	2	2.2	2.2	100.0
	Total	92	100.0	100.0	

Inference: From the above table it is inferred that 38% of the respondents agree that they would scan all removable drives before using.

Security Awareness [I install antivirus software on my devices]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	39	42.4	42.4	42.4
	Agree	34	37.0	37.0	79.3
	Neutral	13	14.1	14.1	93.5
	Disagree	5	5.4	5.4	98.9
	Strongly Disagree	1	1.1	1.1	100.0
	Total	92	100.0	100.0	

Inference: From the above table it is inferred that 42% of the respondents Strongly agree that they will install antivirus software on their devices.

Security Awareness [I would ensure that my passwords have eight or more characters with alphanumeric]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	48	52.2	52.2	52.2
	Agree	25	27.2	27.2	79.3
	Neutral	12	13.0	13.0	92.4
	Disagree	5	5.4	5.4	97.8
	Strongly Disagree	2	2.2	2.2	100.0
	Total	92	100.0	100.0	

Inference: From the above table it is inferred that 52% of the respondents Strongly agree that they ensure that their passwords size will be eight or more characters with alphanumeric.

Awareness about Toll free number

I am aware about the cyber crime Toll free number

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	14	15.2	15.2	15.2
	Agree	31	33.7	33.7	48.9
	Neutral	21	22.8	22.8	71.7
	Disagree	15	16.3	16.3	88.0
	Strongly Disagree	11	12.0	12.0	100.0

Total	92	100.0	100.0	

Inference: From the above table it is inferred that 34% of the respondents agree that they are aware about the cyber-crime toll free number.

Cross Tabs

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
I am aware about the cyber crime Toll free number * Age	92	100.0%	0	0.0%	92	100.0%

I am aware about the cyber crime Toll free number * Age Crosstabulation

		Age				Total
		16-19	20-25	26-30	Above 30	
I am aware about the cyber crime Toll free number	Strongly Agree	0	13	1	0	14
	Agree	0	30	1	0	31
	Neutral	0	21	0	0	21
	Disagree	1	13	0	1	15
	Strongly Disagree	0	9	1	1	11
Total		1	86	3	2	92

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	**13.716[a]**	**12**	**.319**
Likelihood Ratio	12.700	12	.391
Linear-by-Linear Association	1.645	1	.200
N of Valid Cases	92		

a. 15 cells (75.0%) have expected count less than 5. The minimum expected count is .12.

Interpretation:

The calculated value is 13.716 and it is significant at 0.319 level of significance at 12 degrees of freedom. If the significant difference value is less than 0.05 then reject the null hypothesis and accept alternative hypothesis. In the above result, the significant value is greater than 0.05, so accept the null hypothesis.

Hence, there is no significant association between age and I am aware about the cybercrime Toll free number

T-Test

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
How long will you use the Social media per day	92	**1.97**	.966	.101

One-Sample Test

	Test Value = 6					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
How long will you use the Social media per day	-40.044	91	**.000**	**-4.033**	-4.23	-3.83

Interpretation

Here, the mean value obtained using One Sample T test is 1.97 and the mean difference is -4.033. Based on the result generated, the significance value is 0.000 which is less than 0.05 so reject the null hypothesis.

Hence, there is a significant difference between the sample mean and the population mean.

CONCLUSION

It is concluded that the student's community was very much aware about phishing and its consequences. Also, they agree that the phishing awareness was attained from bank websites and they ensure that reports about phishing attacks will be given to the banks immediately. From this research it is found the security awareness among the students was very high and they will scan the removable drives and also, they are very sure about installing the anti-virus software's. Awareness related to setting the strong password among students are very high. The relationship between age and awareness about cybercrime was rejected. One sample T test

confirms that there is a significant difference between the sample mean and population mean on usage of social media per day. It is concluded that the current generation students are very much awareness about the phishing attacks and they are very much carefully on security aspects with their online dealings.

REFERENCES

- https://www.usenix.org/conference/soups2020/presentation/reinheimer
- https://www.bluevoyant.com/knowledge-center/8-phishing-types-and-how-to-prevent-them
- Garba, A. A., Siraj, M. M., Othman, S. H. and Musa, M. A. (2020). A Study on Cybersecurity Awareness among Students in Yobe State University, Nigeria: A Quantitative Approach. International Journal on Emerging Technologies, 11(5): 41–49.
- Son, J., Kim, D., Hussain, R., & Oh, H. (2014). Conditional proxy re-encryption for secure big data group sharing in cloud environment. Proceedings - IEEE INFOCOM, 541–546.
- Aida Rozihan Mohamad Asri and Irni Eliana Khairuddin (2022), A theoretical framework for the awareness of Phishing attack, Journal of Information and Knowledge Management (JIKM) Vol 1 Special Issue
- M. S. Hasan, R. A. Rahman, S. F. H. B. T. Abdillah and N. Omar, Perception and awareness of young internet users towards cybercrime: Evidence from Malaysia, Journal of Social Sciences, vol. 11, no. 4, pp. 395–404, 2015.
- Fadi. A. Aloul (2012), Need for Effective Information Security Awareness", Journal of Advances in Information Technology, Vol. 3, no. 3