Analyzing Awareness and Security towards Phishing and Cyber Attacks

Dr. Sachin Pandey

Faculty of computer science, Govt. TRS College, Rewa, M.P

Abstract

India's internet usage is expanding quickly. It has opened up new possibilities in a variety of industries, including entertainment, business, sports, and education. For these attacks to be effective, it is necessary to have a thorough understanding of the organizational structure. Cybersecurity is the branch of IT concerned with protecting computer systems, networks, and other information assets against intrusion. It presents the results of a survey administered to 325 users to gauge their degree of security knowledge, their outlook on using related goods, and their level of comfort with potential threats. Despite the apparent high level of confidence, as shown by respondents' assertions that they are aware of the hazards and using many of the necessary protections, a closer look reveals that, in several key respects, knowledge and understanding are lacking. Recent Data on Phishing Attacks The number and complexity of phishing attacks are both on the rise, and the phenomenon itself is spreading.

Keywords: *Cyber-crime, Cyber criminals, Cyber security, Internet, IT Act, Awareness.*

1. INTRODUCTION

India's internet usage is expanding quickly. It has opened up new possibilities in a variety of industries, including entertainment, business, sports, and education. The introduction and widespread use of the internet has allowed firms to access customers all over the world, breaking down the limitations of local marketplaces. Enterprises frequently employ computers not simply to handle information but also to acquire a competitive and strategic advantage. Both beneficial and negative uses of computers are possible. The Information Technology Act of 2000 addresses new age crimes that have emerged as a result of internet abuse. Information is now more easily available globally, but it is also more susceptible to abuse. With the number of cyberattacks on Indian institutions increasing, India is on the minds of cybercriminals. After the US and China, India is the third-highest source of harmful internet activity, the second-highest source of malicious code, and the eighth-highest source or origin of online attacks and network attacks.

Phishing is the malevolent practice of using online deceit to attempt to get sensitive personal and financial information. Phishing frequently uses identity theft and social engineering strategies, like building websites that seem just like genuine ones already on the internet. Potential consumers are driven to the malicious website via a hyperlink in a seemingly trustworthy email in order to provide their personal information and login credentials. One form of phishing is known as "spear phishing," in which fake but seemingly official emails are sent to specific individuals within a company in an effort to gain access to that business's network and steal confidential information. "whaling" is a similar tactic used to target high-ranking executives within that business. For these attacks to be effective, it is necessary to have a thorough understanding of the organizational structure.

The ongoing danger posed by cyberattacks is substantial, to the point where it poses a threat to national security. Cybersecurity lapses are all too regular; it seems like every day there is a new attack, data theft, or penetration that enters the news. The FBI, Secret Service, and Department of Homeland Security are a few of the organizations that look into cybercrimes; the U.S. Cyber Command safeguards Department of Defense networks and tries to defend other federal agencies against harmful activities. To safeguard its networks, however, still falls to the private sector. Asia accounted for about half of all Internet users worldwide in 2017, according to Internet World Stats. However, they are still inexperienced when it comes to cybersecurity, training, or collaboration to stop cyberattacks or incidents.

This essay's goal is to aid everyone in comprehending the legal facets of cyber security and to assist in harmonizing legal frameworks. Its full title is Understanding Cybercrime: Phenomena, Challenges and Legal Response. As such, it seeks to examine the requirements of current national, regional, and international instruments, aid in the establishment of a strong legal framework, and better grasp the national and international implications of developing cyber threats. It focuses on the needs of developing countries and offers a thorough overview of the most important subjects related to the legal aspects of cybercrime. Due to the international nature of cybercrime, both developing and industrialized nations use the same legal tools.

Cybersecurity is the branch of IT concerned with protecting computer systems, networks, and other information assets against intrusion. Cybersecurity is a major problem in today's advanced technological world. Its second goal is to prevent the unauthorised disclosure of private information. Many dangers might befall data both while it is being kept and when it is being transferred. Both current and future assaults represent a significant risk to both commercial enterprises and the general populace. Industries with a heavy reliance on computers have a special need to protect the privacy of their customers' personal information. Several methods and tools in the realm of cyber security ensure the safety of data both at rest and in transit.

Cybercriminals, who hurt individuals via the misuse of digital assets like personal information, are growing and adapting at the same rapid rate as the digital world. One of the most hazardous crimes that affects all internet users is identity theft, which may be described as impersonating another person with the intent to steal money or other valuables by using that person's personal information. Even while social engineering-based assaults are still the primary method, cybercriminals have developed their own methods for collecting this information. One kind of social engineering that may lead to identity theft is the phishing assault. Because so many people utilise the internet, phishing has become a major concern. Phishing is a sort of social engineering in which the attacker pretends to be a trustworthy entity via an email or other form of electronic communication in order to trick the target into handing over personal information. Phishers send emails containing links to harmful websites in an attempt to deceive people into accessing such sites. Voice over IP (VoIP), SMS, and IM might all be used as other attack vectors. To boost their success rates, phishers have moved on to "spear-phishing," a more targeted version of bulk emailing.

2. LITERATURE REVIEW

Therdpong Daengsi et.al (2021) Because cyberthreats are becoming so prevalent in daily life, cybersecurity is essential right now. An examination of the literature revealed that there are no studies on cybersecurity awareness that involved a sizable Thai user base. As a result, Our research focused on assessing the cybersecurity literacy of a large Thai bank's almost 20,000 workers located around the nation. The research consisted of three parts: a first phishing attack, knowledge transfer using a mixed-approach, and a second phishing attempt with new material. Validation of the data and analysis of the results revealed that workers' knowledge of cybersecurity had improved significantly. After being warned about the phishing email, 71.5 percent fewer employees fell for the trap. Accordingly, this strategy has potential for application in enhancing cybersecurity across a variety of enterprises and sectors. Researchers observed that Thai women had a higher degree of cybersecurity knowledge than Thai men, suggesting that gender plays an important role in the Thai cybersecurity ecosystem. Cybersecurity knowledge was also shown to be unaffected by the different generations represented in Thai workforce.

Adam Kavon Ghazi-Tehrani et.al (2021) Phishing has fast advanced past low-skill tactics that focused on casting "a wide net," the fraudulent attempt to gain sensitive information by posing as a reliable institution via electronic contact. Spear phishing attacks use advanced tactics to target a specific high-value person. The purpose of this study is to outline the current state of phishing, anticipated technological advancements and innovations, and the most effective enforcement and preventative measures. The material was obtained through conversations with about 60 information technology security experts, "hackers," and university researchers. Routine Activity Theory offered an operational framework, and while it fits most crimes only loosely, it has sufficient explanatory power for cybercrimes. Most people I spoke with agreed: First, although they make phishing assaults more common, technical advancements also make them easier to spot. A simple attack can be carried out more easily than ever, yet a successful attack takes more work than ever. Second, phishing serves as the major attack vector for ransomware and is directly accountable for financial fraud. Third, the issue will get worse sooner or later as a result of newer tech-based attacks like deepfakes. Fourth, prevention will come via machine learning and public awareness campaigns similar to the development of WIFI security through the use of encryption and password awareness.

Talal Alharbi et.al (2021) Recent technological developments, such as instant messaging and social media websites, have allowed for the rapid and efficient dissemination of information. This has led to an increase in the availability of knowledge. However, new types of cybersecurity dangers have emerged at the same time, often leading to data loss and improper use of information. Since students often make up the bulk of a company's user base, preserving their data privacy in complicated systems is of the utmost importance. Most data breaches and other forms of digital misconduct are the result of student ignorance of cybersecurity and its implications. The researchers at Marjah University wanted to find out how well-versed their undergraduates were in cybersecurity and how many of them really took precautions while online. They did this by administering a comprehensive survey. To prove the need of user education, training, and awareness, we performed a quantitative evaluation of students' knowledge of cybercrime and protection. In this study, we used an ANOVA, a Kaiser-Meyer-Olkin (KMO), and a Bartlett's test to assess and analyse our hypotheses in conjunction with a quantitative research strategy. In-depth analysis of the dangers of spam, malware, phishing, bogus ads, and pop-up windows was conducted for this research. Finally, we use the information to propose solutions to this common problem.

Vaishnavi Bhavsar et.al (2018) Information security currently has several flaws. These days, it doesn't take much for a hacker to enter into a system and steal sensitive data. Phishing is one method used to get access to this data. Phishing is a sort of cybercrime in which the victim's personal information (such as passwords, bank account details, credit card numbers, phone numbers, and text message content) is stolen. Online identity theft constitutes the bulk of phishing attacks. The phisher manipulates the target into giving up their sensitive information and financial details using social engineering. This research article does a great job of summarising phishing attempts, including their many manifestations, detection techniques, and potential defences.

Adamu A. Garba et.al (2020) Due to the evolution of the internet, the prevalence of numerous online programmers, and the pervasiveness of ever-evolving social media platforms, today's students are more vulnerable to online threats. Everyday, kids face risks including phishing, cyberbullying, and other forms of online fraud. Individuals who are aware of the risks they face online and how to protect themselves from them are one step closer to finding a solution. The purpose of this research is to determine whether students have a firm grasp of cybersecurity concepts. Students majoring in computer science at Nigeria's Yobe State University were surveyed using a quantitative methodology and a battery of questions tailored to assess the respondents' understanding of cybersecurity and monitor their online activities. Since all schools have been shut down because to the COVID 19 outbreak, only city-dwelling kids were allowed to participate in the research. The results of the experiment were analysed, and although college students generally have a good grasp of cybersecurity, more of them than usual have gaps in their knowledge when it comes to taking precautions to keep their data safe. According to the study contribution, there is no active cybersecurity awareness programme, and female students are disproportionately vulnerable to cyberattacks. In addition, the study revealed that students were really eager to learn more about cybersecurity.

3. METHODOLOGY

Consider using a questionnaire survey method or poll overview strategy to analyses the awareness of cybercrime and create a useful framework with regard to cyberwarfare for this research paper. The method is widely used in numerous international research articles, as was mentioned above in the literature study. Respondents were given a Likert scale on which to score the selected properties/elements impacting analysis of cybercrime awareness and the building of an appropriate framework with regard to cyber warfare. Heterogeneity in the sample was preserved so that the respondent may accurately reflect the different kinds by moving nearer the groups of selected respondents who were discussing crucial facets of the Indian digital business.

Both the exploratory and descriptive research designs are used in this study. Exploratory research is performed to examine various correlations with variations in cybercrime. The research included Chi-Square and Fisher's exact tests. Descriptive research has been used to evaluate data that has so far been incongruous with either explanatory or exploratory studies. And since that best serves the intended aim, it is preferable to describe them. A sample of 325 respondents was chosen in order to successfully perform market research and learn about respondents' expectations of the government and awareness of cybercrime. The study's geographic focus and sample size are both India as a whole. Through the use of a standardized questionnaire, the customers' primary data for the study's purposes was gathered. For the research, 325 questionnaires were distributed to respondents across the nation. The government's website, reports, publications, journals, and other sources were used to gather secondary data for the study.

4. CONDUCT OF RESEARCH

A systematic questionnaire was distributed to 350 respondents working in the Indian IT sector, and 325 legitimate responses or 43% of the total were obtained. On a Likert scale of 1 to 5, the respondents were asked to rate their responses. The questions were made to be straightforward and basic enough for the respondents to grasp. The questionnaire is broken into the following two sections:

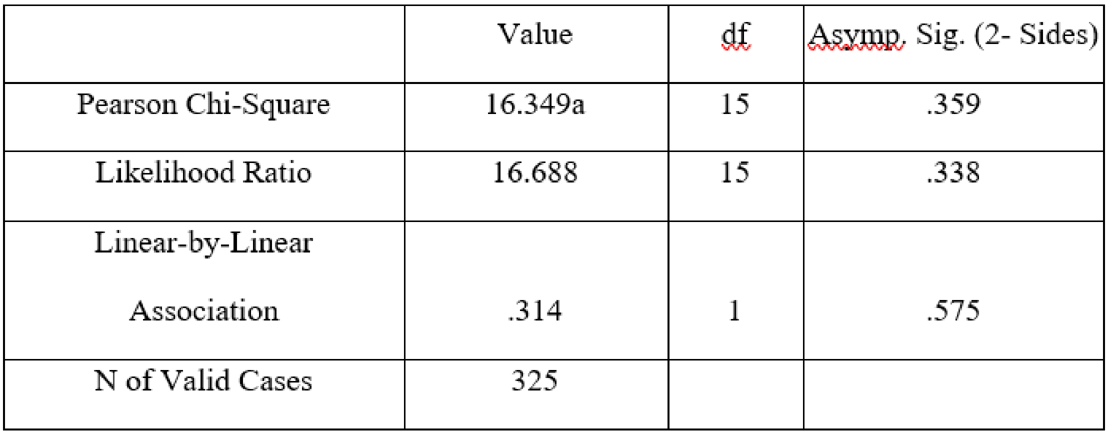
- Overview of the study and the researcher
- the actual questionnaire

The findings of the tests and analysis, which were performed after compiling the replies from the respondents in an Excel data sheet, are shown below. Questionnaire data were analysed using the Chi-Square Test and the Fisher's Exact Test. On a Likert scale of 1 to 5, respondents were asked to rank the elements influencing construction productivity in the questionnaire according to the degree of their effect and impact on the productivity of the industry in India. The numbers given to the reactions did not prove the equivalence of the intervals between the scales, nor did they indicate the absolute quantities.

5. RELIABILITY ANALYSIS

After confounding variables have been removed, it is important to verify that metric analysis measured the correct construct, that is, whether the characteristics of each component framed consistently define a similar measure inside target measures. If characteristics actually define the recognized variable, it is understood that these characteristics should relate to one another in a reasonable manner—not necessarily in the ideal way. We may gauge how closely certain elements are connected by using SPSS to compute Pearson relationships. The estimation of C for all computed attributes is 0.783, which is regarded as excellent.

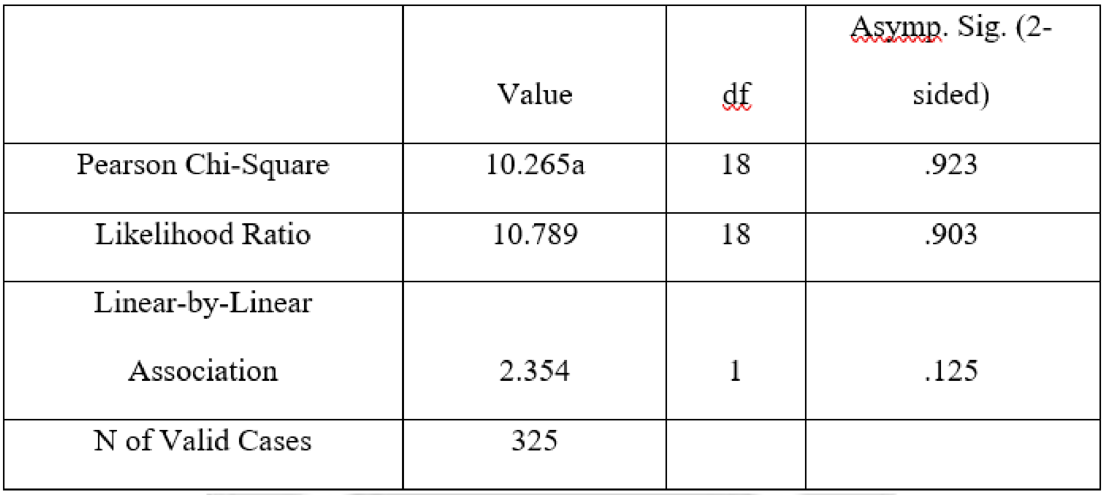
Table 1. Chi-Square test between age of the respondents and their familiarity with Cyber Crime



	Value	df	Asymp. Sig. (2- Sides)
Pearson Chi-Square	16.349a	15	.359
Likelihood Ratio	16.688	15	.338
Linear-by-Linear Association	.314	1	.575
N of Valid Cases	325		

Based on the significance level (0.359), 36% of people were likely to be aware of cybercrime, regardless of their age. As a result, we can draw the conclusion that age and knowledge of cybercrime are unrelated.

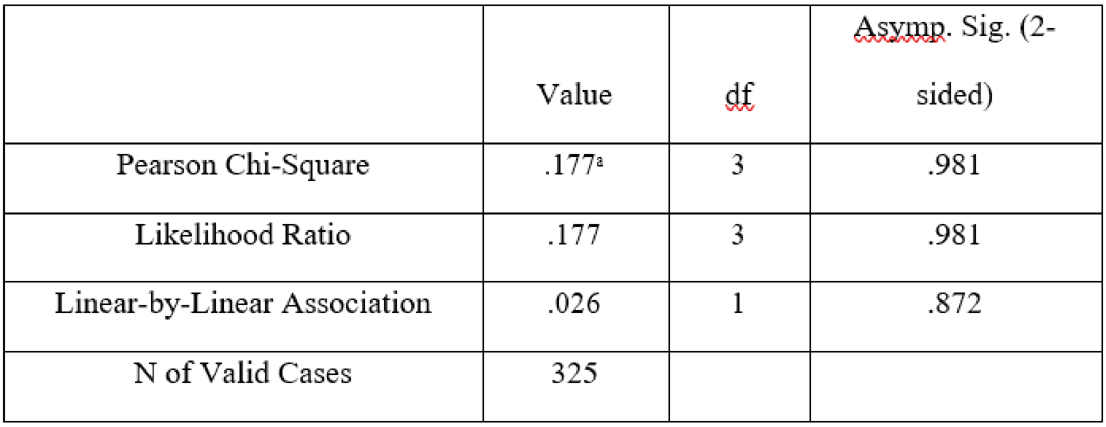
Table 2 Chi-Square test between education of the respondents and their familiarity with Cyber Crime



	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	10.265a	18	.923
Likelihood Ratio	10.789	18	.903
Linear-by-Linear Association	2.354	1	.125
N of Valid Cases	325		

Given the significance level (0.923), there were 92% possibilities that people would be aware of cybercrime regardless of their degree of education. As a result, we can draw the conclusion that education level and knowledge of cybercrime are unrelated.

Table 3 Chi- Square test between computer usage and computer damage due to cyber crime

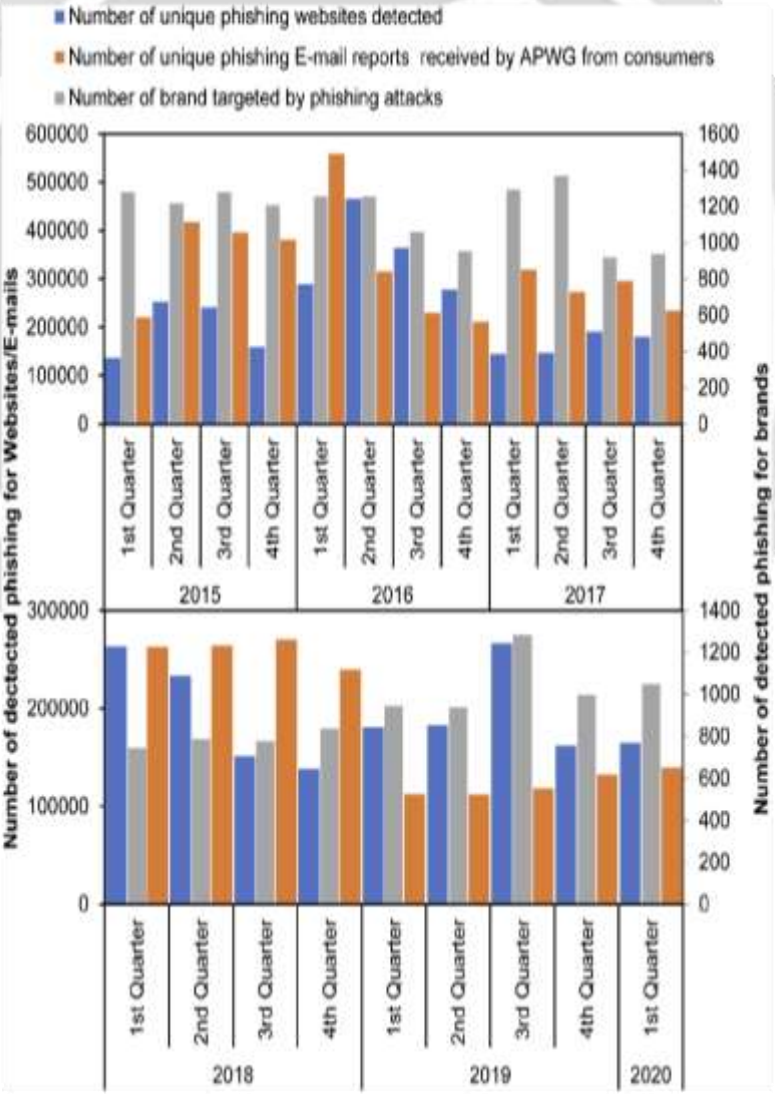


	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	.177^a	3	.981
Likelihood Ratio	.177	3	.981
Linear-by-Linear Association	.026	1	.872
N of Valid Cases	325		

Given the significance level (0.981), there were 98% possibilities that the amount of time spent using a computer had no bearing on the computer damage caused by cybercrime. As a result, we can draw the conclusion that there is no connection between cybercrime and the frequency of computer use.

Every part of the human race has been affected by cybercrime. However, the government and financial institutions are most at risk. These two institutions are especially vulnerable to attacks since they have access to a vast amount of private and financial information. Given the modern enthusiasm to conduct everything online, personal users have a lot at stake; their privacy and financial security are most at risk. The daily activities of an individual, such as work, are the most vulnerable, followed by online banking, explicit web browsing, and internet data sharing. No of your age or level of knowledge, you should be aware of cybercrime. Therefore, it is safe to presume that there are many ways for people to learn about societal developments. This essay has offered a survey of current ideas regarding the difficulties posed by cyberwarfare. It started by examining current definitions of cyberwar and cyberwarfare and discovered two issues that needed to be fixed. First, it was discovered that neither cyberwarfare nor cyberwarfare have a generally agreed meaning. This is problematic because it is challenging to talk about the more serious issues or even identify when cyberwarfare is taking place without an accepted definition.

Recent Data on Phishing Attacks Phishing attacks are growing in frequency and complexity, and they are also getting more pervasive. Phishing attacks have taken many various shapes lately. The attackers deploy a range of threats and strategies to bring in fresh victims. These channels may be VoIP or social networks, which might bring a range of threats include spam calls, phishing emails, instant messaging, embedded URLs, and dangerous file. Criminals continue to focus on social engineering attacks since it is their preferred weapon because they are aware that social engineering-based approaches are efficient and lucrative. Instead of focusing on advanced techniques and toolkits. Phishing assaults have increased to previously unheard-of levels, particularly with the advent of new technologies like smartphones and social media. For instance, phishing assaults against organizations climbed from 72 to 86% between 2017 and 2020 in the United Kingdom, with a significant share of the attacks coming from social media (GOV.UK, 2020). The APWG Phishing Activity Trends Report analyses and quantifies the growth, development, and dissemination of phishing attacks that have been reported to the APWG. Figure 5 displays the quarterly increase in phishing assaults from 2015 to 2020, based on information from the Anti-Phishing Working Group (APWG). Figure 5 shows that in the third quarter of 2019, there were 266,387 phishing assaults, which is the most in three years since late 2016. This was nearly twice as many as the 138,328 recorded in the fourth quarter of 2018 and was an increase of 46% from the 182,465 for the second quarter. In the same quarter, 118,260 distinct phishing emails were reported to APWG. Additionally, it was discovered that 1,283 different brands were targeted by phishing attacks.



6. CONCLUSIONS

After the US and China, India is the third-highest source of harmful internet activity, the second-highest source of malicious code, and the eighth-highest source or origin of online attacks and network attacks. Potential consumers are lured to the malicious website using a seemingly legitimate email that contains a hyperlink in order to reveal their personal information and login credentials. The FBI, Secret Service, and Department of Homeland Security are some of the organizations that conduct cybercrime investigations; the U.S. Cyber Command safeguards Department of Phenomena, Challenges, and Legal Response has been published. Several methods and tools in the realm of cyber security ensure the safety of data both at rest and in transit. The method is widely used in numerous international research articles, as was mentioned above in the literature study. Both the exploratory and descriptive research designs are used in this study. Exploratory research is performed to examine various correlations with variations in cybercrime. For instance, phishing assaults against organizations climbed from 72 to 86% between 2017 and 2020 in the United Kingdom, with a significant share of the attacks coming from social media.

7. REFERENCES

1. Therdpong daengsi et.al (2021) cybersecurity awareness enhancement: a study of the effects of age and gender of Thai employees associated with phishing attacks
2. Adam kavon ghazi-Tehrani et.al (2021) phishing evolves: analyzing the enduring cybercrime
3. Talal alharbi et.al (2021) assessment of cybersecurity awareness among students of majmaah university
4. Vaishnavi bhavsar et.al (2018) study on phishing attacks
5. Adamu a. Garba et.al (2020) a study on cybersecurity awareness among students in yobe state university, nigeria: a quantitative approach issn no. (print): 0975-8364 issn no. (online): 2249-3255
6. Abdullah, a. S., & mohd, m. (2019). Spear phishing simulation in critical sector: telecommunication and defense sub-sector. 2019 international conference on cybersecurity, icocsec 2019, 26–31. Https://doi.org/10.1109/icocsec47621.2019.8970803
7. Ahmed, n., islam, m. R., kulsum, u., islam, m. R., haque, m. E., & rahman, m. S. (2019). Demographic factors of cybersecurity awareness in bangladesh. 2019 5th international conference on advances in electrical engineering, icaee 2019, June 2018, 685–690. Https://doi.org/10.1109/icaee48663.2019.8975603
8. Albladi, s. M., & weir, g. R. S. (2018). User characteristics that influence judgment of social engineering attacks in social networks. Human-centric computing and information sciences, 8(1), 1–24.
9. Aleroud, a., & zhou, l. (2017). Phishing environments, techniques, and countermeasures: a survey. Computers and security, 68, 160–196. article google scholar
10. Anstett, a. (2021). What is spear phishing? Wander, retrieved jul 27, 2021, from Anwar, m., he, w., ash, i., yuan, x., li, l., & xu, l. (2017). Gender difference and employees' cybersecurity behaviors. Computers in human behavior, 69, 437–443. Https://doi.org/10.1016/j.chb.2016.12.040article google scholar
11. Aoyama, t., nakano, t., koshijima, i., hashimoto, y., & watanabe, k. (2017). On the complexity of cybersecurity exercises proportional to preparedness. Journal of disaster research, 12(5), 1081–1090. Https://doi.org/10.20965/jdr.2017.p1081
12. Bahnsen, a. C., bohorquez, e. C., villegas, s., vargas, j., & gonzalez, f. A. (2017). Classifying phishing urls using recurrent neural networks. Ecrime researchers' summit, ecrime, 1–8. https://doi.org/10.1109/ecrime.2017.7945048
13. Baillon, a., de bruin, j., emirmahmutoglu, a., van de veer, e., & van dijk, b. (2019). Informing, simulating experience, or both: a field experiment on phishing risks. Plos one, 14(12), 1–15.
14. Bin Othman Mustafa, m. S., Noman Kabir, m., Erna wan, f., & Jing, w. (2019). An enhanced model for increasing awareness of vocational students against phishing attacks. 2019 ieee international conference on automatic control and intelligent systems, i2cacis 2019 - proceedings, June, 10–14.
15. Khalid, f. (2017). Understanding university students 'use of Facebook for collaborative learning. International journal of information and education technology, 7(8), 595–600. Https://doi.org/10.18178/ijiet.2017.7.8.938