Network Security Awareness and Prevention of Cyberattacks

[1] Muhammad Nadeem Khan, [2] Shabina Ghafir
[1]Research Scholar, [2]Assistant Professor
[1] Jamia Hamdard, New Delhi,
[2] Jamia Hamdard, New Delhi,
[1] nadeemkhanmev1@gmail.com, [2] sghafir@jamiahamdard.ac.in

ABSTRACT

This paper tries to give a general overview of network security awareness and avoidance of cyber-attacks. This paper covered the many types of cyberattacks, current developments in cyberattacks, prevention tips, and the awareness of cyberattacks among students. We will first discuss the many forms of cyberattacks, the current trend, the effects of cyberattacks, and protection. The method involved contrasting and examining the findings of 15+ separate articles. The survey's findings would show the conclusions drawn from an analysis of the information gathered from respondents who answered a questionnaire after seeing a movie about cyberattack awareness to raise students' understanding of such attacks. Depending on the results of this survey, we will have a better understanding of the familiarity and awareness of current students with cyber-attacks, enabling us to enhance kids' knowledge of online dangers and the value of cyber security.

Keywords: Awareness, Cyber Security, Cyber-attack, Internet, Network Security, Prevention.

INTRODUCTION

An attempt to gain access to a computer system to size, change, or steal data is known as a cyber-attack. Malware, phishing, ransomware, and man-in-the-middle attacks are just a few of the attack vectors that cybercriminals might use to begin a cyberattack. The US Department of Homeland Security claims that inherent and residual hazards contributed to each of these attacks.[1]

There is a growing need for information security professionals who understand how to use information risk management to reduce their cybersecurity risks[2]. The increasing use and regulatory focus on outsourcing mean that vendor risk management and third-party risk management frameworks are more important than ever, experts say.[3]

By breaking into a vulnerable system, a cybercriminal can take, change, or destroy a specific target. Cyber threats can be as sophisticated as attempting to take down vital infrastructure to install harmful software like malware or a ransomware attack. A data breach, where personal information or other sensitive information is exposed, is a frequent side effect of a cyberattack.

© 2023 Vidya Publications

Although cyber assaults are rather widespread in our society, little research has been done on how people perceive them, and some individuals still do not consider them to be a major issue. More than 85% of Malaysians are expected to use the Internet by 2025, according to the trustworthy statistic site Statista Digital Market Outlook [4]. This percentage increased to more than 85% in 2018. As a result, there will be a higher chance of pupils becoming the target of cyberattacks.

Therefore, the goal of creating this article is to provide readers with a foundational understanding of cyber-attacks in order to increase their awareness and help prevent future attacks. Then there are only a few more. Aside from that, people want to be protected from cyberattacks, therefore understanding them is essential in today's world. Understanding at least the fundamental attack dangers and their attitudes towards cyber-attack defence are also important factors. Most university students are anticipated to possess greater knowledge linked to computer technology than other social groups, and they also have enough information to be alert for cyberattacks [5].

Distributed denial of service (DDoS) attacks, malicious domains, malicious websites, malware, ransomware, spam emails, harmful social media messaging, business email compromise, mobile threats, and browsing applications are the 10 categories of cyberattacks in network security [6]. Hackers utilize a variety of preventative techniques to avoid being detected, including backing up personal data, selecting strong passwords, updating software, and more [2].

Background Study:

Cyber Security

The two most important security practices that any company is concerned with on a daily basis are privacy and data security. Although social networking sites provide a secure environment for users to communicate with friends and family, cybercriminals also use these platforms to steal important information.

Types of Cyber Attacks

- Denial-of-service (DoS) and Distributed Denial of- Service (DDoS) Attacks:
  The system's capacity is depleted during a Denial-of-Service (DDoS) assault, making it unable to respond to service demands. A host machine that has been infected with malicious software starts a DDoS assault. TCP SYN flood assaults and botnets are two examples of different types of DDoS attacks[10]. For instance, a DDoS assault made the website of the U.S. Department of Health and Human Services (HHS) one of its targets. In order to delay the reaction to the Covid 19 outbreak, this attack involved overloading the HHS servers with millions of queries over a period of many hours [10].

© 2023 Vidya Publications

- Man-in-the-Middle (MitM) Attack:
  MITM is an attack that uses real-time conversations, transactions, or information sharing to steal, send, and receive information intended for someone else.

- Phishing Attacks:
  Phishing is a form of technological deception or social engineering that use emails with embedded URLs to deliver harmful files to our system. Its main objective is to get sensitive data, including credentials and personal information.

- Drive-by-Download Attack:
  Drive-by-Download cyberattacks are a common method used by hackers to spread viruses and gain unauthorized access to computer systems. According to the US Department of Homeland Security, this kind of assault occurs whenever a computer becomes infected with malicious software just by visiting a website.

- Password Attack:
  Credential hacking is the process of unlawfully stealing or decoding a user's credentials, such as passwords. It can be done by searching the user's desk, assuming a login database, keeping an eye on the network connection, and more.

- SQL Injection Attack:
  A malicious SQL statement is typed into a fillable field to exploit a weakness in a web app's SQL implementation, resulting in a SQL attack. To access the backend or to access update, or access data, the attacker will, in other words, put code into a field.

- Cross-Site Scripting (XSS) Attack:
  XSS is an injection method used to load a malicious script into a trusted website or private online application. To put it another way, XSS happens when a website's database is accessed by an attacker using malicious JavaScript or script. The victim's browser runs the malicious script inside the response, which sends the victim's cookies to the attacker's server.

- Eavesdropping Attack:
  Assaults that spy on people are sometimes referred to as snooping attacks. Eavesdropping refers to hacker attacks that affect data delivered through digital devices. Through an unsecured network, attackers exchange messages and examine transmitted and received data.

  An attacker may use a sniffer to eavesdrop on a computer or server and grab data as it is being transferred in this form of attack, which is difficult to detect since it doesn't exhibit any odd behaviour during network transmission.

- Birthday Attack:
  Attacks on cryptography, such as birthday attacks, are within the domain of brute force attacks. Its base is the probability theory's birthday puzzle. This technique might be used

to benefit from information sharing between more than two parties. Birthday attacks examine the message's integrity, software, or cryptographic signature using hash methods.

- Malware Attack:
  Malicious software is a dangerous program that is installed on a victim's computer without their knowledge or consent. It can get access to a private network, disrupt it, and steal user data. It can also access additional user information, which can be used to generate money illegally. The most common types of malware are viruses, malicious software, and spyware.
  - **Virus:** A virus is a harmful software that connects to any system program and copies and modifies instructions when it is run. It can spread through software startup or file access.
  - **Worms:** Worms are viruses that spread via email attachments on computers or over the internet. Denial-of-service assaults might result from this.
  - **Trojan Horses:** Trojan Horses are a sort of malware that spreads on its own and disseminates by disguising itself as helpful software.
  - **Ransomware:** Ransomware attacks are also being launched by cybercriminals against schools, hospitals, and other public institutions. Cybercriminals are hoping that these companies would pay the ransom because they can't afford to have their systems shut out at this time [6]. Through URLs, email attachments, or working staff whose credentials have already been stolen as a result of a system flaw, the ransomware targets the system [7]. There is now ransomware-as-a-service offered by online criminals on the dark web. Both parties profit from a successful assault since one party is in charge of creating and manufacturing the ransomware code and another is in charge of coordinating the spread of the virus or an attack campaign [11].
  - **Spyware:** Spyware is nefarious software that secretly tracks user behaviours and alerts hackers to it.

Trends Changing Cyber Security

Some factors that significantly impact cyber security:

- **Mobile networks:** Mobile networks have made it easier to communicate, but they also raise security issues due to the increased use of smartphones, tablets, PCs, and other devices.
- **Web servers:** Online servers can be attacked by malicious software or have data from web apps stolen.

- **Cloud computing and its services:** Companies of all sizes are increasingly progressively adopting the services provided by cloud computing. In other words, the whole world is getting closer to the clouds.
- **Targeted attacks and APTs:** A covert cyber-attack on a computer network known as an advanced persistent threat (APT) occurs when the attacker acquires and maintains illegal access to the targeted network while going unnoticed for a long time. In the interval between infection and cure, the hacker frequently observes,
- **Code encryption:** Encryption is used to protect communication (or information) from being deciphered by snoopers or attackers.
- **IPv6:** Internet Protocol 6 is referred to as IPv6. The IPv4 protocol, which has sustained our networks and the Internet as a whole, will be replaced by this one.

Cyber Security Techniques

Cybercriminals are using new methods to exploit flaws in new technologies, such as changing the fingerprints of viruses and looking for defining characteristics of cutting-edge technology. They are also using the expanding Internet to access a large number of people quickly and easily.

- Access control
- Password security
- Data authentication
- Malware scanners
- Anti-Virus software
- Firewalls

Literature Review

Network security issues are becoming increasingly common due to the Covid 19 epidemic, with hackers and malicious attackers taking advantage of this to gain access to economies and other advantages. Targets include people, financial institutions, governmental agencies, and healthcare facilities. [7].

The transition to an online environment increased the risk of cyberattacks and data breaches in the Covid 19 outbreak.

The work-from-home (WFH) business concept has been embraced by organizations, companies, and businesses, and online education is being forced upon the educational system. However, employees and students must use their own, unsafe, and unprotected home networks and gadgets in order to work and learn[8]. Due to the growing use of remote study and work, Malaysia is experiencing a rise in opportunistic cyberattacks. It is important to give students the correct information in order to raise their understanding and awareness of cyberattacks. [9].

The spread of misleading information about the Covid 19 epidemic is a threat to network security. The Internet is the most often used platform for disseminating inaccurate information, and cyber assaults are more successful due to the general public's anxiety and expectation that the appropriate authorities will provide information. Attackers use phone websites or communications to get people to pay attention, and recent developments and news stories are related to frequent cyberattacks.

IMPACT OF THE CYBER ATTACK

Cyberattacks are a common occurrence and a social phenomenon. Numerous effects of cyberattacks have been observed in recent years [12]. Information loss, money loss, company interruption, and equipment damage are the most common effects of cyberattacks.

Data loss makes some people the targets of cyberattacks. Information such as complete name, full address, birthday, personal identification number, financial data, phone number, email address, password, and others will be accessed and stolen by the hacker [13]. The victim of a cyber-attack could lose important items like money, peace of mind, and security as a result of the attack. [14]. In addition, this may also cause social damage to the victims as the victims may become anxious and lose confidence in the technology and network [15].

Many firms today are creating online brands and need to engage with clients throughout the world online. Cyber-attacks in this situation, like unauthorized access to network security and computer hacking, are escalating and affecting businesses [16], [17]. The purpose of electronic intrusion and attack may be to steal data connected to the company's financial security (Zolkipli Mohamad Fadli), to introduce viruses to keep track of the firm's future online activities, or to deny services to the website of the company [14].

Cyber-attacks are having a negative effect on businesses, as data such as risks and consumer information could be made public and stolen by competitors. [16].Cyber-attacks can reveal bad facts about an organization, leading to a loss of reputation and a decline in sales. This has a major negative impact on the company's reputation and market value. [16].

For instance, hackers who identified themselves as "anonymous" company personnel targeted the PayPal websites. They are attempting to carry out a denial-of-service attack against PayPal in retaliation for halting payment services from Wiki Leaks. Although these hackers were in custody, PayPal had taken significant damage as a result, even though it was still in business. Due to the customer's inability to access the company's online store, these denial-of-service assaults have impacted sales. Long-term income reduction could result from some customers choosing not to use PayPal [14].

PREVENTION OF THE CYBER ATTACK

It is important to use technology to protect data and information in the digital age, as cyberattacks are becoming more sophisticated and can have a negative impact. It is important to spread awareness and take precautions to lessen their impact.[18].

First, more than 75% of businesses will be the victim of a cyber-attack, according to Abdulrahman and Varol [20], since they connect to the internet with weak passwords. Weak Passwords continue to pose the greatest risk to individual privacy since they are easily cracked and lead to data theft [21].

Stricter password regulations must be applied to all devices, including networks, laptops, surveillance cameras, mobile phones, and others, to increase security for businesses' confidential data, such as business records, financial information, employee information, and Wi-Fi passwords.

The most important details are that internet-connected gadgets are vulnerable to cyberattacks due to their close connectivity to the Internet and that understanding the network's susceptibility is important for locating the cyberattack. If a potential cyber-attack is discovered, victims should conduct an initial investigation to determine if it has happened and take precautions to prevent it from happening again [19]. So, the important methods used to prevent cyber-attack will be explored in this section [20].

Develop a strong password to protect against hacker attacks online. It is important to generate a password starting with the first letter and requiring capital letters, small letters, symbols, and numbers. It is also important to avoid using the same password for various accounts or services and to avoid saving passwords. This is due to the fact that using the same lines for all passwords and setting them on any website makes them vulnerable to hackers [18].

Block users from logging into unsecured servers, such as free Wi-Fi, to avoid a cyberattack. This is because hackers could compromise the connection between the source and users, taking control of the devices and accessing data such as phone numbers, credit card details, and other data [20]. Connecting to a computer at a public location can increase the risk of a cyberattack, so it is important to clean your browser's history after each use [13]. In order to prevent a cyberattack, the default password on a new device purchased from a device shop must also be changed to a private password.

Keeping software updated is important for cyber-attack prevention, as it can protect the device and fend off cyber-attacks. Companies often ensure that their software is maintained to safeguard their products from potential abuse and improve them, so it is important to install updates when the device manufacturer sends them. For example, if you receive an update notification from Apple, Google, or Microsoft, don't ignore it and keep your software devices updated because the most recent software updates typically come with bug fixes and security patches [18].

Another way to ensure sure the device is up to date is to set it up for automatic updates, in which case the device will automatically check for the newest version and update. This will guarantee that the devices' hardware is protected as effectively as possible [20].

Making a backup of personal files is the final step in preventing a cyberattack. Data backup methods should be varied, saves data in numerous copies, and modifies access permissions. The information technology team must regularly verify the strategy and integrity of the backups to ensure they are functioning effectively [20].

For instance, if someone keeps copies of all essential information on Google Drive, the cloud, and other hard drives, they will always have a backup copy in case some of the files are lost, stolen, or compromised by hackers [18].

METHODOLOGY

- Literature review:
  The literature review was discussed in the first stage. At this point, we will read roughly 13 articles to do a literature study to learn more about the various forms of cyberattacks, present trends, consequences of cyberattacks, and methods for preventing them.

- Planning:
  The second step discussed planning the content for the cyber-attack awareness video and preparing a questionnaire to get respondents' opinions. Students are involved in the data collection phase and Google Forms will be used to deliver the questionnaire.

- Data collection:
  This study will use a quantitative methodology to collect data from 316 respondents. There will be four sections to the questionnaire: demographics, background, exam, and feedback on the cyber-attack awareness film. All of the queries will focus on the objectivity of the research.

- Data analysis:
  The analysis of a bar chart and pie chart for each question can be used to display the results after data collection, which will help us learn more about the respondent's level of cyber-attack awareness.

- Evaluation:
  Evaluation summary from the final stage. Through this phase, we will learn more about the many kinds of cyberattacks, the prevailing patterns, the effects of cyberattacks, how to prevent them, and what the respondents thought of the cyberattack awareness film.

AWARENESS PROGRAM USING YOUTUBE

The awareness program that discusses "types of cyber-attack and prevention" will be presented on YouTube. The three most common cyberattacks in the world are malware, password theft, and phishing assaults, according to this YouTube video. In addition, each cyberattack's prevention was listed in the video.

Malware is the first and most prevalent type of cyberattack. Malware is a term used to describe unwanted programs or software that, when installed on a target system, exhibit odd behaviour. This range of actions includes blocking the program from running, spreading it to other systems, stealing data, and deleting files. Installing the most recent anti-malware tools and teaching users to spot dubious files, links, and websites are thus the most efficient strategies to prevent infection. Often, a combination of anti-virus and caution is sufficient to resist most of the concerns of malicious software. Password theft comes in second.

Password theft occurs when someone gains access to your account, changes your password, and steals your data. The reality is that an unapproved third party is currently misusing your password after guessing it or stealing it. Two-factor authentication, which requires the usage of a second device to complete the login process, is a robust security mechanism that prevents password theft. Additionally, using challenging logins reduces brute-force attacks.

The final one is a phishing scam. Phishing scams involve social engineering to obtain user data, including usernames, passwords, and financial information. Email phishing and spear phishing are two common varieties of phishing assaults. Users are cautioned against clicking on email links from unidentified senders to prevent falling victim to phishing scams. Additionally, users must not send emails that contain personally identifiable information. Another strategy to prevent phishing attempts is to keep the browsers updated.

In conclusion, the purpose of the awareness movie is to raise student awareness of cyberattacks and provide them with more information about how they happen. The pupils will be able to avoid becoming the next victim of a cyberattack and will be better equipped to identify the different types of attacks when they do occur in real life.

RESULT AND DISCUSSION

The overall Jamia student population is 28,866, and 316 people took part in the examination of awareness level among Jamia students. 203 respondents were between the ages of 21 and 23, followed by 72 respondents (22.78%) between 18 and 20, 37 respondents (11.71%) between 24-26, and the last four respondents (1.27%) between 27 and 30.

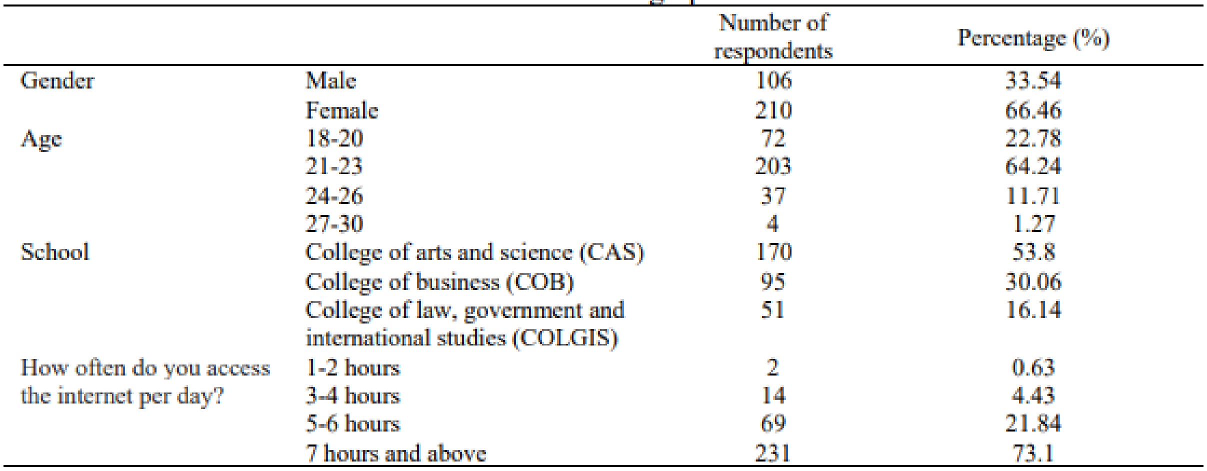
CAS students made up 170 (53.8%) of the respondents, COB students made up 95 (30.06%), and Law, Government & International Studies students made up the remaining 51 (16.14%). In response to the question of how frequently respondents access the Internet each day, 231

(73.10%) of respondents accessed it for seven hours or more each day,69 (21.84%) for five to six hours each day, 14 (4.43%) for three to four hours each day and the remaining 2 (0.63%) for one to two hours each day.

Respondents had a choice of how they acquired information regarding cyber-attacks. 265 respondents (83.86%) said they obtain their information from social media, 219 respondents (69.30%) from the news, 150 respondents (47.47%) from their educational background, 13 responders (4.11%) had never heard of this question, and 278 respondents (87.97%) had installed any antivirus software to thwart cyberattacks. The question if the respondent has ever been the victim of a cyber-attack received 252 no responses, 37 (11.71%) yes responses, and 27 (8.54%) maybe responses.

The most popular response to the question "Who will responder report when faced with a cyber-attack" was family, friends, or relatives, followed by the national cyber security agency (NACSA) and the Royal Malaysian Police (PDRM).

Table 1. Demographic

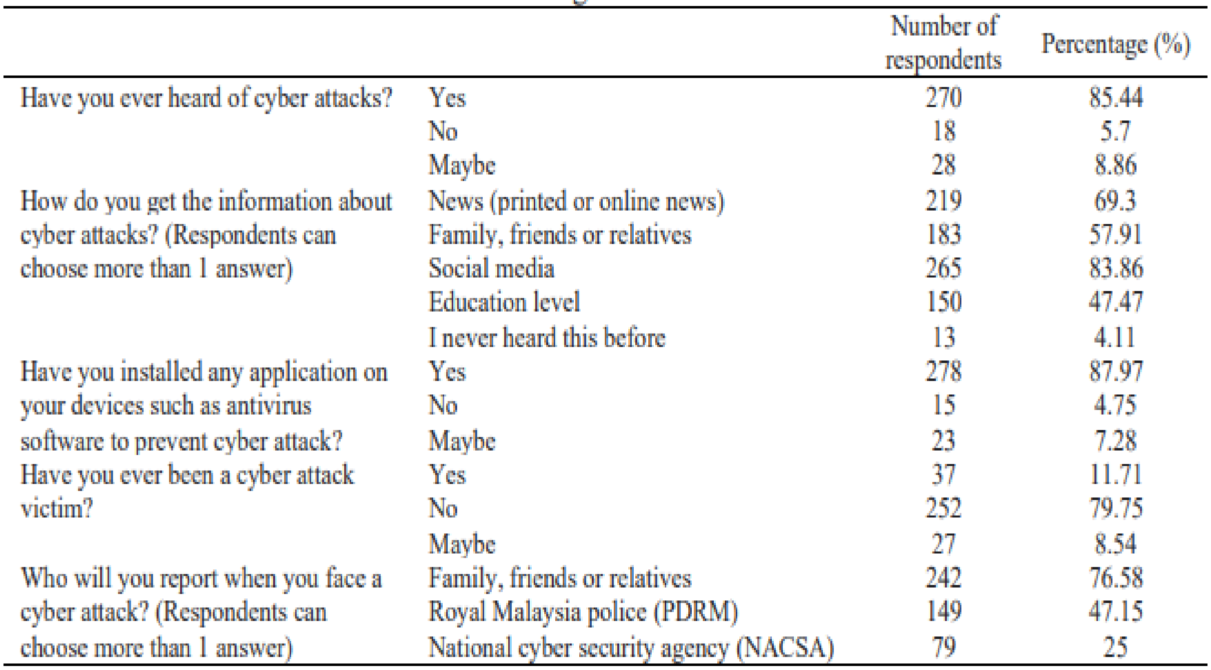


		Number of respondents	Percentage (%)
Gender	Male	106	33.54
	Female	210	66.46
Age	18-20	72	22.78
	21-23	203	64.24
	24-26	37	11.71
	27-30	4	1.27
School	College of arts and science (CAS)	170	53.8
	College of business (COB)	95	30.06
	College of law, government and international studies (COLGIS)	51	16.14
How often do you access the internet per day?	1-2 hours	2	0.63
	3-4 hours	14	4.43
	5-6 hours	69	21.84
	7 hours and above	231	73.1

In response to the second question, "I am aware of the risk when clicking on banners, advertisements, or pop-up screens that appear while browsing the internet," 193 (61.08%) of the respondents strongly agreed that the respondents will always be aware of the advertisements that pop-up on the screen, while 3 (0.95%) of the respondents strongly disagreed with it. This indicates that most survey participants would be reluctant to click on pop-up adverts.

In response to the third question, "I change the passwords of key accounts (such as online banking) frequently," 192 respondents (or 60.76%) agreed, while 13 respondents (or 4.11%) strongly disagreed. This result indicates that the majority of respondents often change their passwords for essential accounts to guard against cyberattacks.

Table 2. Background information



		Number of respondents	Percentage (%)
Have you ever heard of cyber attacks?	Yes	270	85.44
	No	18	5.7
	Maybe	28	8.86
How do you get the information about cyber attacks? (Respondents can choose more than 1 answer)	News (printed or online news)	219	69.3
	Family, friends or relatives	183	57.91
	Social media	265	83.86
	Education level	150	47.47
	I never heard this before	13	4.11
Have you installed any application on your devices such as antivirus software to prevent cyber attack?	Yes	278	87.97
	No	15	4.75
	Maybe	23	7.28
Have you ever been a cyber attack victim?	Yes	37	11.71
	No	252	79.75
	Maybe	27	8.54
Who will you report when you face a cyber attack? (Respondents can choose more than 1 answer)	Family, friends or relatives	242	76.58
	Royal Malaysia police (PDRM)	149	47.15
	National cyber security agency (NACSA)	79	25

In response to the fourth question, "I feel safe using public Wi-Fi," 198 respondents (62.66%) strongly disagreed with the statement, while 10 respondents (3.16%) strongly agreed. According to this finding, the majority of respondents are aware of the dangers of connecting to an unidentified public network.

The majority of respondents strongly agreed with the fifth question, "I often apply software updates," while 15 respondents chose to be neutral and 6 respondents chose to strongly disagree. A total of 187 respondents agreed with the last question "I am wary about clicking on links in an email or social media post," implying caution when clicking on dubious links, getting spam emails, or seeing posts on social media.

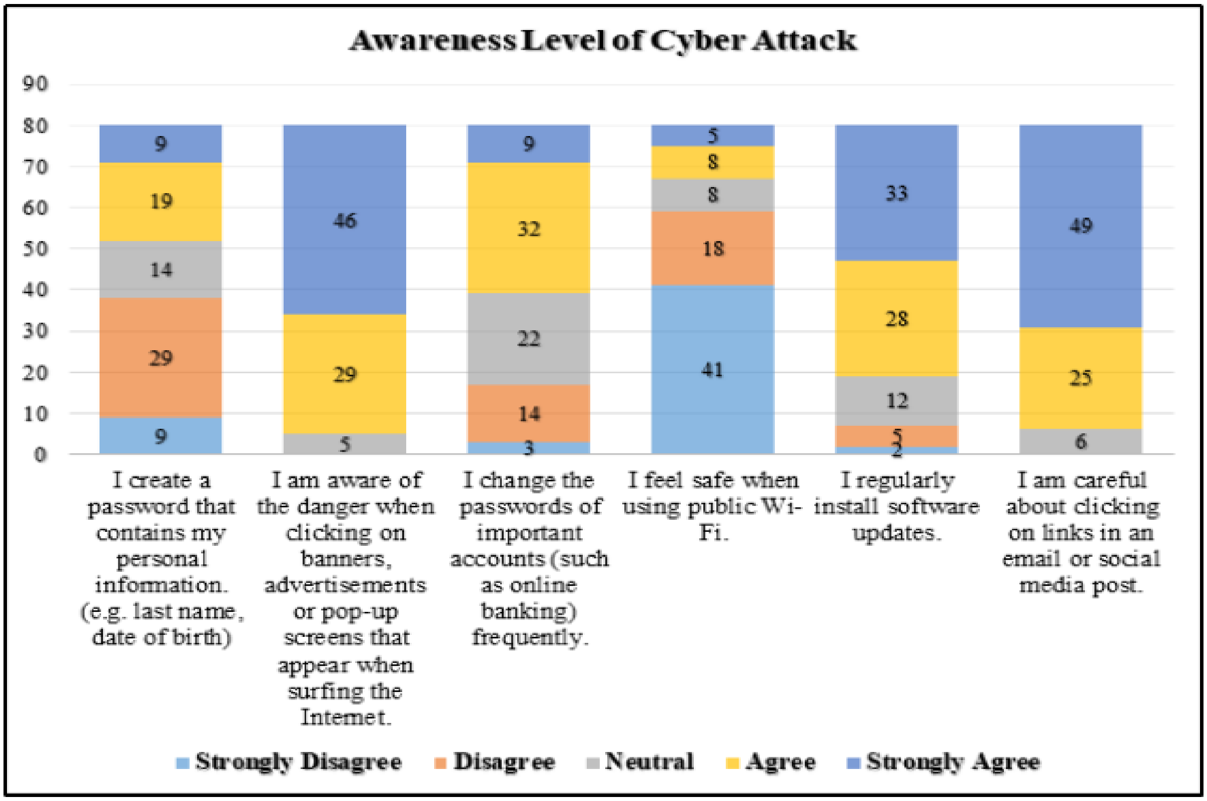
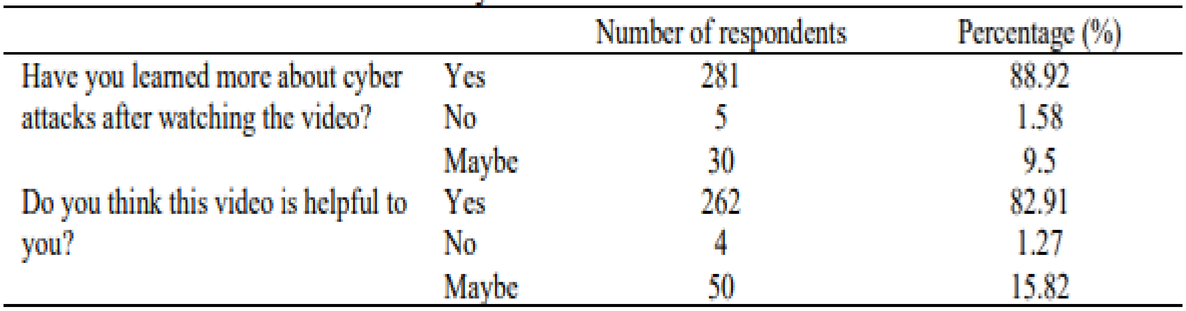


Figure 1. Awareness level of cyber attack

The outcomes of the cyber-attack awareness video were displayed in Table 3. 281 respondents (88.92%) said they had learnt more about cyberattacks as a result of seeing the film, followed by 30 respondents (9.50%) who had possibly learned more and 5 respondents (1.58%) who had not. 262 affirmative responses (82.91%), 50 tentative responses (15.82%), and 4 negative responses(1.27%).

Table 3. Cyber attack awareness video



		Number of respondents	Percentage (%)
Have you learned more about cyber attacks after watching the video?	Yes	281	88.92
	No	5	1.58
	Maybe	30	9.5
Do you think this video is helpful to you?	Yes	262	82.91
	No	4	1.27
	Maybe	50	15.82

© 2023 Vidya Publications

CONCLUSION

In conclusion, this paper identifies the many kinds of cyberattacks, as well as their prevalence, consequences, and methods of protection with regard to network security. The purpose of the paper study was to help students comprehend cyber-attacks better. The results demonstrated that students are well knowledgeable about the many forms, present trends, effects, and preventions of cyber-attacks.

The shift of daily activities from the offline world to the online one increased vulnerability and the potential for cyber-attacks and data breaches in the current environment. The prevalence of network attack crimes is also a result of the development of network attack technology. People of all ages must constantly improve their understanding of cyber security and cyber-attacks to truly avoid becoming the next victim since cyber-attack victims are no longer exclusively members of a particular age group.

REFERENCES

[1] M. Zwilling, G. Klien, D. Lesjak, L. Wiechetek, F. Cetin, and H. N. Basım, “Cyber security awareness, knowledge and behaviour: A comparative study,” Journal of Computer Information Systems, vol. 62, no. 1, pp. 82-97, 2020, doi:10.1080/08874417.2020.1712269.

[2] H. Teymourlouei, “Quick reference: Cyber-attacks awareness and prevention method for home users,” World Academy of Science, Engineering and Technology International Journal of Computer and Systems Engineering, vol. 9, no. 3, pp. 678-684, 2015, Digital Object Identifier: 10.5281/zenodo.1338144.

[3] A. Garba, M. B. Sirat, S. Hajar, and I. B. Dauda, “Cyber security awareness among University students: A case study,” Science Proceedings Series, vol. 2, no. 1, pp. 82-86, 2020, Digital Object Identifier: 10.31580/SPS. v2i1.1320.

[4] J. Müller, “Malaysia: Internet penetration rate,” Statista, 11-Aug-2021. [Online]. Available: https://www.statista.com/statistics/975058/internet-penetration-rate-in-malaysia/ (Accessed: 16-Feb-2022).

[5] M. D. Elradi, A. A. A. Altigani, and O. I. Abaker, “Cyber security awareness among students and faculty members in a Sudanese college,” Electrical Science & Engineering, vol. 2, no. 2, pp. 24- 28, 2020 Digital Object Identifier: 10.30564/ v2i2.2477.

[6] N. A. Khan, S. N. Brohiand, N. Zaman, “Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic,” TechRxiv,12-May-2020, doi:10.36227/v. 12278792.v1.

[7] J. Chigada and R. Madzinga, “Cyberattacks and threats during COVID-19: A systematic literature review,” South African Journal of Information Management, vol. 23, no. 1, pp. 1-11, 2021, Digital Object Identifier: 10.4102/sajim. v23i1.1277.

[8] L. Tawalbeh, F. Muheidat, M. Tawalbeh, M. Quwaider, and G. Saldamli, "Predicting and preventing cyber-attacks during COVID-19 time using data analysis and proposed secure IoT layered model," 2020 Fourth International Conference on Multimedia Computing, Networking and Applications (MCNA), 2020, pp. 113-118, Digital Object Identifier: 10.1109/MCNA50957.2020.9264301.

[9] S. S. Tirumala, A. Sarrafzadeh, and P. Pang, "A survey on internet usage and cybersecurity awareness in students," 2016 14th Annual Conference on Privacy, Security and Trust (PST), 2016, pp. 223-228, Digital Object Identifier: 10.1109/PST.2016.7906931.

[10] R. A. Ramadan, B. W. Aboshosha, J. S. Alshudukhi, A. J. Alzahrani, A. El-Sayed, and M. M. Dessouky, “Cybersecurity and countermeasures at the time of the pandemic,” Journal of Advanced Transportation, vol. 2021, pp. 1–19, 2021, Digital Object Identifier: 10.1155/2021/6627264.

[11] S. Kok, A. Abdullah, N. Jhanjhi, and M. Supramaniam, “Ransomware, threat and detection techniques: A review,” IJCSNS International Journal of Computer Science and Network Security, vol. 19, no. 2, pp. 136-146, 2019.

[12] M. Kravchik and A. Shabtai, “Detecting cyber-attacks in industrial control systems using convolutional neural networks,” in Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and Privacy - CPS-SPC ’18, 2018, pp. 72-83, Digital Object Identifier: 10.1145/3264888.3264896.

[13] A. Bendovschi, “Cyber-attacks – trends, patterns and security countermeasures,” Procedia Economics and Finance, vol. 28, pp. 24–31, 2015, Digital Object Identifier: 10.1016/S2212-5671(15)01077-1.

[14] R. Renu and P. Pawan, “Impact of cyber-crime: Issues and challenges,” International Journal of Trend in Scientific Research and Development, vol. 3, no. 3, pp. 1569–1572, 2019, Digital Object Identifier: 10.31142/ijtsrd23456.

[15] M. Bada and J. R. C. Nurse, “Chapter 4 - The social and psychological impact of cyberattacks,” in Emerging Cyber Threats and Cognitive Vulnerabilities, Elsevier, 2020, pp. 73–92.

[16] S. Kamiya, J.-K. Kang, J. Kim, A. Milidonis, and R. M. Stulz, “Risk management, firm reputation, and the impact of successful cyberattacks on target firms,” Journal of Financial Economics, vol. 139, no. 3, pp. 719–749, 2021, Digital Object Identifier: 10.1016/j.jfineco.2019.05.019.

[17] A. Chowdhury, “Recent cyber security attacks and their mitigation approaches – an overview,” in Applications and Techniques in Information Security, Singapore: Springer Singapore, 2016, pp. 54–65, Digital Object Identifier: 10.1007/978-981-10- 2741-3_5.

[18] P. G Shah, “Detection and prevention of system against cyber-attacks,” International Journal for Scientific Research and Development, vol. 5, no. 9, pp. 576-578, 2017.

[19] V. Farhat, B. McCarthy, R. Raysman, J. Canale, Holland, and K. LLP, “Cyber Attacks: Prevention and Proactive Responses,” in Practical Law Company, 2017, pp. 1-12. [Online]. Available: https://articles.jmbm.com/files/2017/05/Farhat.Article.CyberAttacks.pdf

[20] G. A. Abdalrahman and H. Varol, "Defending against cyber-attacks on the Internet of things," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), 2019, pp. 1-6, Digital Object Identifier: 10.1109/ISDFS.2019.8757478.

[21] Y. K. Peker, L. Ray, S. D. Silva, N. Gibson, and C. Lamberson, “Raising cybersecurity awareness among college students,” Journal of The Colloquium for Information System Security Education (CISSE), vol. 4, no. 1, pp. 1-17, 2016.