

Cyber attack awareness and prevention in network security

Zolkipli Mohamad Fadli, Shu See Yong, Low Kai Kee, Gan Hui Ching

School of Computing, UUM College Arts and Sciences, Universiti Utara Malaysia, Kedah, Malaysia

Article Info

Article history:

Received Dec 24, 2021

Revised May 30, 2022

Accepted Jun 06, 2022

Keywords:

Awareness

Cyber attack

Network security

Prevention

ABSTRACT

This article aims to provide an overview of cyber attack awareness and prevention in network security. This article discussed the different types of cyber attacks, current trends of cyber attacks, how to prevent cyber attacks and uum students' awareness of cyber attacks. First, we will go over the different types of cyber attack, current trend, impact of cyber attack and the prevention. The approach entailed comparing and observing the outcomes of 13 different papers. The survey's findings would demonstrate the results obtained after analyzing the data collection which are the questionnaire filled out by respondents after watching the cyber attack awareness video to improve awareness of students through the cyber attack. Depending on the outcome of this survey, we will have a better understanding of current students' knowledge and awareness of cyber attacks, allowing us to improve students' understanding of cyber threats and the necessity of cyber security.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Gan Hui Ching

School of Computing, UUM College Arts and Sciences, Universiti Utara Malaysia

Sintok, 06010 Bukit Kayu Hitam, Kedah, Malaysia

Email: gan_hui_ching@soc.uum.edu.my

1. INTRODUCTION

With the growth of the online world, the Internet has become one of everyone's essential needs, and individuals can now readily get cross-border and borderless information. Although the network can benefit people, it also exposes network security to a variety of threats, such as hacker assaults, network viruses, and the spread of illicit and unconfirmed information. Cyber attack has become a major source of concern around the world. Information security could be compromised by cyber-attacks. As the rate of data usage and internet consumption continues to rise, cyber awareness has become more critical [1].

When someone gains or attempts to obtain unauthorized access to computer systems with the intent of deliberately harming systems or stealing important information, this is known as a cyber attack [2]. The advent of four new characteristics of cyber attacks in recent years has resulted in an increase in the frequency of cyber attacks. The first characteristic is that attack methods are becoming extremely advanced. The second feature is that obtaining tools for conducting cyber attacks has become easier. The third distinguishing feature is the increased frequency of cyber attacks. The fourth characteristic is the emergence of large-scale coordinated cyber attacks. The original network security protection technology (such as data encryption, security authentication, firewalls, and so on) can no longer entirely prevent complex network attacks due to the new characteristics of the network security scenario.

Cyber attack is a rapidly developing field. Nowadays, most transactions are done in the online environment, which is why there is a need for effective and completely secure high-quality network security. People are often unable to protect their important information in the increasing technological innovation, which is the reason for the increase in cyber attacks. People should stay vigilant on this issue, so as not to fall into cyber attack and become one of the victims. Cyber security knowledge may be utilised to counter some

fundamental assaults on individuals, therefore the more users are aware of basic cybersecurity concepts, the less successful cyberattacks will be [3].

Although cyber attacks are widely common in our world, the awareness of the cyber attack in the minds of the people has not been extensively analysed and some people still don't think this is a serious matter. According to the reliable statistic resource provided by statista digital market outlook [4], from the year 2018, more than 85% of people in Malaysia were using the internet, and this proportion is still forecast to the year 2025. This means that there will be an increased risk of students falling victim to cyberattacks. Therefore, the purpose of writing this paper needs to introduce the basic knowledge about cyber attack in order to raise their awareness and prevent cyber attack from happening again. After that, there are only a few research or review papers that are related to the awareness of the cyber attack. Hence, our study aims to investigate in more details about the type of cyber attack, impact and prevention of cyber attack.

Besides that, cyber attacks awareness plays a critical role in our lives today, as users expect to be understand at least aware of basic attack risks and their attitudes on how to protect themselves from the cyber attacks are also a key factor. Most of the university students are expected to have more knowledge that related with the computer technical than other category in society which also includes sufficient the knowledge about the awareness of the cyber attack [5].

This paper aims to identify the awareness level towards cyberattacks among students in UUM. This paper also seeks to determine if a cybersecurity awareness campaign is required to raise the cybersecurity knowledge and awareness among university students. Another aim of the paper is to improve the awareness of the university student and encourage the students to have and learn more awareness from that to do the prevention when they are facing the cyber attacks.

There are ten types of cyber attack in network security which are distributed denial of services (DDoS) attack, malicious domains, malicious websites, malware, ransomware, spam emails, malicious social media messaging, business email compromise, mobile threats, and browsing apps [6]. Various prevention methods are used to prevent the cyber attack from the hackers such as backup the personal file, choosing strong different passwords, keeping the software up to date and so on [2]. We will present a paper on cyber attack based on type, their impact on network security and prevention to avoid it. The rest of the paper is carried out as follows. Section 2 introduces that literature review which is related to the type of cyber attack and current trends. Section 3 summarizes with impact and the prevention of cyber attack. Section 4 explores research methodology about the way to collect and analyze the data collection from respondents after watching the cyber attack awareness video. Section 5 analyzes the result and makes the discussion on it. Section 6 concludes this article in the conclusion part and follows with acknowledgement and references.

2. LITERATURE REVIEW

Network security concerns are becoming more prevalent with the speedy digitization of society. The breakout of the Covid 19 epidemic has resulted in a considerable increase in the number of individuals interacting online. Intentionally, hackers and malicious attackers are getting increasingly active in exploiting such situations. They infiltrate and assault multiple platforms in order to obtain access to certain economies and other advantages. Individuals, financial services, government authorities, and even healthcare institutions are all targets of intruders [7].

In the scenario of the Covid 19 epidemic, the shift of everyday operations from physical to online settings increased susceptibility and potential for cyber attacks and data breaches. By relocating to an online environment, organizations and businesses all over the globe have embraced the work from home (WFH) business model. In addition, the education system is being compelled to implement online learning, often known as study from home (SFH) [8]. This implies that workers and students must work and learn on their own home networks and personal devices, which are inherently insecure and lack industry-standard security protections. The network security of the home is not as reliable as the security level of an organization's network security architecture. In this circumstance, the widespread adoption of remote work and learning has increased the number of opportunistic cyber attacks in Malaysia. Therefore, it is necessary to provide the right information to students who are potential targets for exploitation to increase their knowledge and awareness on cyber attacks [9].

Furthermore, owing to people's concern, worry, and uncertainty about the Covid 19 outbreak, the internet material and information relating to Covid 19 may readily capture people's attention. The proliferation of false material concerning Covid 19 problems is also posing a threat to current network security. The Internet is the most common medium for spreading false information regarding Covid 19. It is tough for Internet users to identify and determine whether the information they want is a credible source and reliable advice. Hence, cyber attacks are more successful during the Covid 19 epidemic due to the fact that most individuals are apprehensive and expect relevant authorities to offer information on Covid 19. Cyber

attackers develop phoney websites or communications that imitate the appearance of legitimate government agencies and use urgent terms as bait to draw people's attention. The following section will discuss the current trends and related news to the common cyber attacks nowadays.

2.1. Distributed denial of services attack

DDoS attack is a kind of cyber attack where the cyber attackers try to intercept the authority or online materials unreachable to their end-user, either permanent or temporary. Denial of service is generally performed by assaulting the target network or resource with unnecessary requests in order to overwhelm it and prevent any or all genuine requests from being fulfilled [10]. The primary targets of such attacks are institutions that distribute public information about the Covid 19 epidemic. In the current epidemic, most government authorities and healthcare organisations have observed a dramatic surge in DDoS attacks owing to Covid 19. Hackers and malicious attackers overwhelm organisations' internet sites or networks with phoney or bot users in order to wreck the system's regular operation and so disrupt the communications network. For instance, the website of the U.S. Department of health and human services (HHS) had become one of the targets of a DDoS attack. This assault consisted of flooding the HHS servers with millions of requests over a period of several hours, with the goal of delaying the response to the Covid 19 outbreak [10].

2.2. Malicious domains

Cyber attackers use the internet to build bogus domains in order to fool their victims. Cyber attackers utilise these malicious domains to deceive individuals and gain personally identifiable information for unscrupulous reasons. A lot of Covid 19 related malicious domains may be found mostly in Germany, Italy, the United States, and Russia. According to the US centers for disease control and prevention (CDC), World Health Organization (WHO), Google, and the world economic forum (WEF), the Covid 19 epidemic has generated nearly 86,000 new operational but problematic or malicious sites [7]. According to the check point risk intelligence analysis, over 4,000 domains associated with coronaviruses have been launched internationally since January 2020 and 3% of them are malicious domains [6].

2.3. Malicious websites

Impersonating and malicious websites that pretend to be applications that protect users against Covid 19 have become more prevalent in this circumstance. For example, an application named "Corona antivirus" from the website www.corona-antivirus.com stated that it was created by Harvard University experts [6], [7]. However, the PC will be infected with malware known as BlackNET RAT by installing the application. In addition, the US Department of Justice has issued a temporary restriction order against the coronavirusmedialkit.com bogus website in another case. It is claimed that the website sells Covid 19 vaccination kits that have been authorised by the world health organization. But in reality, valid Covid 19 vaccinations are not currently available on the market [6].

2.4. Malware

Cyber attackers are leveraging the power of the present scenario by embedding dynamic coronavirus maps and webpages to disseminate malware, Trojans, and spyware [7]. Spam emails are one of the most common ways to trick users into clicking on a link or installing malware, and users can be victims through their mobile devices or PCs. For example, Johns Hopkins University had created a map with an interactive dashboard to display facts and deaths related to the coronavirus [6]. Cyber attackers tried to take advantage of this as well by inserting java-based malware inside it.

2.5. Ransomware

Cyber attackers are also attacking hospitals, healthcare facilities, schools, and other public organisations with ransomware assaults. Cyber attackers are hopeful that these firms would pay the ransom as they can't really afford to remain locked out of the systems due to the present circumstance [6]. The ransomware attacks the system through URLs, email attachments, or working personnel whose credentials have already been compromised as a result of a system weakness [7]. Ransomware-as-a-service is now available on the dark web from cyber attackers. One party is in charge of developing and producing the ransomware code, while another is in charge of orchestrating the distribution of the infection or an attack campaign, and both parties earn from a successful attack [11].

2.6. Spam emails

Spam emails were often utilized on a massive scale by fraudsters and attackers to accomplish their intended aims, whether in a regular or emergency circumstance. Covid 19-related emails with harmful attachments were noticed on a big scale being sent to individuals in the present pandemic scenarios. In a number of situations, intruders have pretended to be from legitimate organisations such as the WHO [6], [7].

Cyber attackers utilize fake email addresses to make the victim believe the email seems to be from WHO and encourage them to contribute to bitcoins or other digital currencies. Anyone that doesn't identify their email address might be a victim.

2.7. Malicious social media messaging

Currently, social media is incredibly popular and practically everyone has access to it. Cyber attackers see this as a fantastic opportunity and target social media applications that are popular like Facebook, Instagram, and WhatsApp [7]. Scammers and hacking attempts have been reported on multiple occasions on Facebook Messenger and other social media platforms. The scammers usually attract users into signing up for free memberships, such as a Netflix premium account [6]. The victim is sent to their phishing website when they click on the link provided. It may require users to input their account information in certain scenarios. This allows cyber attackers to either acquire users' credentials or install malicious software to their web browsers, and devices in order to steal cookies and information, making the user a victim.

2.8. Business email compromise

In the present conditions, coronavirus illness is being used as a tactic in business email compromise frauds. The deception works by persuading or duping victims into conducting transactions with an invader posing as a legitimate employee of the same organization [7]. For example, agari cyber intelligence division has been attacked in Covid 19 circumstance by Ancient Tortoise, a cybercrime group that has previously been linked to multiple business email compromise (BEC) instances [6]. The cyber attackers utilise the data of their customers to send them emails and ask them to update their bank details and payment methods. The cyber attackers pretend to be from legit organizations or businesses.

2.9. Mobile threats

Smartphone usage is at an all-time high in this current age of information overload computing. Life will become unthinkable without smartphones and gadgets, and their usage is expanding on a regular basis. Simultaneously, it's a fantastic chance for evil actors to exploit. For example, a rogue android software called CovidLock is allegedly used to track Covid 19 instances. The software encrypts victims' phones and gives them 48 hours to pay USD100 in bitcoin to get them unlocked [7]. The erasure of phone data and the disclosure of account information on social media are both threats. Another example is an Android app that provides face masks and safety equipment to anyone who is concerned [6]. When a user installs the programme, it will install a SMS Trojan, which gathers the victim's phone directory's contact information and sends SMS automatically to spread itself.

2.10. Browsing apps

Browsers are already a commonly used programme due to the rapid expansion and simple access to the internet all over the world, and they are used by essentially anyone that has an internet connection. The cyber attackers gain access to the router's domain name system (DNS) configuration, which causes the browsers to open automatically and show the malicious software's alert or notification. There was only a button labelled "COVID-19 Inform app" that appeared. The "Oski info stealer" virus will be installed on the device when the user presses the download button [6]. This will obtain the cookies, passwords, history, and transaction information from the browsers.

3. IMPACT OF THE CYBER ATTACK

Cyber attack is a ubiquitous situation and it is a social phenomenon. In recent years, many impacts of cyber attacks have been reported [12]. The impacts of cyber attack usually involve information loss, loss of revenue, business interruption and equipment damage.

Some people are the victims of cyber attacks due to information loss. The hacker will access the information and steal the information such as full name, full address, birthday date, personal ID, financial data, phone number, email address, password and others [13]. Due to the cyber attack, the victim of a cyber attack may lose their valuable things such as money, peace security and others [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].

Nowadays, many companies are developing online businesses and need to connect with global customers by using the internet. In this case, cyber attacks such as unauthorized access to the company's network security and the hacking of the company's computer are gradually increasing and causing impacts to the companies [16], [17]. The aim of electronic enter and attack may be to steal information that is related

with the financial of the company, to install viruses to monitor the online activities of the company in the future or reject services to the website of the company [14].

Cyber attacks with the purpose of accessing, removing and destroying important data is causing a big impact to the company. The data such as the common risks of the company and the list of customers that are accessed by the hackers may reveal to the competitors and cause a big hit to the company. The competitors may attack the company by targeting the risks faced by the company and grab potential customers from the company [16].

Cyber attacks appear to reveal unfavorable information and this leaking of information will adversely affect the company. The cyber attack may cause the company to lose the reputation as the cyber attack indicates that the management of the company is not good as previously thought. It has a significant negative impact on the sales growth of a company as the cyber attack is weakening the customer confidence in the attacked company. Hence, the credibility of the attacked company will decrease and the market price of the company will become worse [16].

For example, the PayPal websites were attacked by hackers who claimed to be "anonymous" members of the organization. They are trying to retaliate against PayPal for stopping payment services from Wiki Leaks in order to carry out a denial-of-service attack. Although these hackers were being arrested, it had caused a big hit to PayPal though it was not completely bankrupt. These denial-of-service attacks had led to reduced sales because the customers cannot access the online store of the company. If some customers decided not to do business with PayPal, this may lead to reduced revenue in the long term [14].

4. PREVENTION OF THE CYBER ATTACK

In this digital era, the increasing use of technology is extremely important to protect data and information. More data and information are starting to be transmitted over the network and stored in computers. However, the complexity of attackers is increasing day by day. Therefore, it is very beneficial to educate and do some actions to prevent cyber attack. Although cyber attacks cannot be completely prevented, this can reduce their effectiveness [18].

Security is one of the biggest issues related to the devices that are connected to the internet. Cyber attacks of any size are starting with the use of vulnerable links in the security system and the hackers will actively detect weak links or websites and use them to obtain benefits. Any content that is connected with the network is more vulnerable to cyber attack. In the rapidly evolving Internet, they can do this more easily than ever. Since all the devices can be closely connected with the Internet, all the hackers can find one vulnerability and obtain control of the entire data that was received. To identify the cyber attack, it is significant to understand the vulnerability of the network. If a potential cyber attack is discovered, victims should conduct an initial investigation to determine whether the cyber attacks have happened and should take some precautions to prevent this from happening again [19]. So, the important methods used to prevent cyber attack will be explored in this section [20].

First, according to Abdalrahman and Varol [20], more than 75% of the business will become the target of the cyber attack because they are using the weak password when connected to the internet. Weak passwords are remaining the biggest threat to personal privacy and can be easily cracked resulting in data theft [21]. All devices including networks, computers, surveillance cameras, mobile phones and others must implement stricter password regulation which can help to improve the security level for the enterprises. By adding more security protections to the private data of the company, this can help to reduce the possibility of data are falling into the hands of malicious people. These private data include the business documents, financial report, information of the worker, Wi-Fi connection password and others [20].

Furthermore, there are some tips that can be used to create a strong password to protect our information or prevent cyber attacks from hackers. First, in order to create a super strong and unique password, it needs to make sure that your password is difficult to guess from the others by creating the password starting with the first letter and must include the capital letter, small letters, symbols and numbers to become a sentence. In addition, it also needs to prevent the use of simple words or sequences that are easy to guess such as "123", "abc", "0000" and any other password that is easy to guess. Secondly, it is important to make sure that the same password is not used for multiple accounts or services and don't save the passwords when using public devices. This is because if using the same sentences for all of the passwords and set that password on any website, this will be easy to attack by the hacker and the hacker is able to access all the accounts by using the obtaining password [18].

After that, preventing login into the system that uses insecure servers such as public Wi-Fi is also another method to prevent cyber attack. This is one of the dangers associated with public Wi-Fi or free Wi-Fi that the hackers may infiltrate the connection between the source and people. The data will be sent to the hacker instead of the devices after connecting to the hotspot. So, the hacker will obtain all of the data that you send or the data that save in the devices such as the password of the bank account, phone numbers, credit

card information and other data [20]. For example, you may connect your phone or computer at the coffee shop, library and other places, this may increase the chances of getting a cyber attack. However, try not to do this frequently and ensure that you had cleared the history of the browser when you had finished using it [13]. In addition, it needs to change the default password to a private password when purchasing the new device from the device shop in order to avoid cyber attack.

Next, another method used to prevent cyber attack is often keeping the software up to date. People need to frequently check the software and make sure that the software is the latest version as this can protect the device and prevent cyber attack. Outdated software may be riddled with vulnerabilities that permit hackers to easily access the information in the devices. So, the company is usually making sure that their software is updated to protect their products from possible misconduct and enhance their products. Hence, when the device manufacturer sends the updated information through your devices, please remember to install them as this may repair the security bugs. For example, if Apple, Google and Microsoft send the update message to you, please do not ignore those annoying messages and keep your software devices updated because the latest version updated software usually will contain bug fixes and security patches [18]. In order to make sure the device is up to date, it also can be done by setting the device as an automatic update which the device will check for the latest version and update automatically. This will ensure that the equipment of the devices is protected as up to date as possible [20].

The last step to prevent cyber attack is to backup the personal files. Backup can become a good alleviation platform for cyber attack. It is important to make sure that your data backup strategy is diversified, saves the data into many copies and changes the data access permission to read and write with the authorization settings. The team must continuously verify the strategy and verify the integrity of the backups, so that the information technology team can be an effective resource for performing backups and regular inspections to make sure that the backups are working properly [20]. For example, the person can keep the copies of all important files in google drive, cloud and other hard drives, hence the person can get a backup copy if some of the files are damaged or hacked by the hacker [18].

5. METHODOLOGY

5.1. Literature review

First stage described about the literature review. From this stage, we will review around 13 articles to do the literature review to know more information about the types of cyber attack, current trends, impact of the cyber attack and the prevention of cyber attack.

5.2. Planning

Second stage explained about planning. In planning, we will plan the content that suitable to create the cyber attack awareness video. We also will create the questionnaire to collect the feedback from the respondents after they view the cyber attack awareness video. The participants involved in the data collection stage are UUM students. The questionnaire will be distributed to UUM students through Google Form.

5.3. Data collection

Third stage explored about data collection. The method we use in this paper is quantitative method. To prove our paper, we will provide questionnaire to 316 respondents. The questionnaire will be divided into four sections. Section A is demographic of respondent, Section B is background information of respondent, Section C will test the respondent's awareness level of cyber attack and the last section which is Section D will be the feedback of cyber attack awareness video from respondent. All the questions are referring to the research objectivity.

5.4. Data analysis

Fourth stage introduced about data analysis. After collecting data, the result can be shown through the analysis of bar chart and pie chart for each question. There will be a total of 4 sections contained in the questionnaires and answered by a total of 316 respondents. Based on the data, we will know more information about the respondent's awareness level to the cyber attack.

5.5. Evaluation

Last stage summarized about evaluation. Through this phase, we will know more about the types of cyber attack, current trends, impact of cyber attack, prevention of cyber attack and the respondents' feedback of the cyber attack awareness video.

6. AWARENESS PROGRAM USING YOUTUBE

The youtube will be used to present the awareness program that talks about the "types of cyber attack and prevention". From this youtube video, there are 3 most popular cyber attacks in the world which are malware, password theft and phishing attacks. Besides that, the video also listed the prevention for each cyber attack.

First, the most common form of cyber attack is malware. Malware refers to unwanted programs or software that cause unusual behavior when it installs itself on the target system. This scope includes denying access to programs, spreading itself to other systems, stealing information and deleting files. So, the most effective ways to prevent malware are installing the latest anti-malware programs and the users need to recognize suspicious files, links and websites. Often, a combination of anti-virus and caution is sufficient to resist most of the concerns of malicious software.

Second is password theft. When you connect into an account, your password is changed and your personal information is stolen, this is referred to as password theft. The truth is that an unauthorized third party has stolen or guessed your password and is now running amok with it. The prevention for password theft is two-factor verification is a strong security measure since it necessitates the use of a second device to complete the login process. Using difficult logins also prevents brute force attacks.

The last one is the phishing attack. Phishing attacks are social engineering scams that steal user information such as usernames and passwords or banking information. Common types of phishing attacks are email phishing and spear phishing. Users are advised not to click on email links from unknown sources in order to avoid becoming vulnerable to phishing attacks. Users must also refrain from sending personally identifying information through email. Keeping the browsers up to date is another way to avoid phishing attacks.

In conclusion, the awareness video is used to increase the awareness level among UUM students to the cyber attacks and gain more knowledge about how the cyber attacks occur. This can let the students prevent being the next cyber attack victim and make them easily recognize the type of cyber attack when it happens in their life.

7. RESULT AND DISCUSSION

Next, on the result and discussion part, the total number of UUM students is 28,866 students according to the year 2021. From the total number of UUM students, the 1.09 % population will be taking part in the evaluation form. So, a total of 316 respondents are participated in an evaluation of this awareness level among UUM students

Table 1 showed the number of respondents based on their demographic. Referring to Table 1, the respondents' gender consists of 210 (66.46%) females and 106 (33.54%) males. There were 203 (64.24%) of the respondents in the age group 21-23, followed by 72 (22.78%) of respondents in the age group 18-20, 37 (11.71%) of the respondents were in the age group 24-26 and the rest 4 (1.27%) of the respondents were in the age group of 27-30 age group.

170 (53.80%) of the respondents were the students from college of arts & science (CAS), 95 (30.06%) of the respondents were the students from the college of business (COB), and the rest 51 (16.14%) of the respondents were the students from college of law, government & international studies (COLGIS). For the question of how often the respondents access the Internet per day, 231 (73.10%) of the respondents access the Internet 7 hours and above per day, 69 (21.84%) of the respondents access the Internet 5-6 hours per day, and 14 (4.43%) of the respondents access the Internet 3-4 hours per day and the rest 2 (0.63%) of the participants access the Internet 1-2 hours per day.

Table 2 showed the number of respondents based on their background information. Referring to this table, the respondents who have ever heard of cyber attacks consist of 270 (85.44%) of the respondents answered they have heard of cyber attacks, 18 (5.70%) of the respondents answered no and 28 (8.86%) of the respondents answered maybe in this question.

For the question "how the respondents get the information about cyber attacks", respondents were allowed to choose more than one answer. In this question, 265 (83.86%) of the respondents stated they get the information from social media. 219 (69.30%) of the respondents stated they get information from news (printed or online news). 150 (47.47%) of the respondents stated they get information from education level. On this question, there are 13 (4.11%) of the respondents who said they never heard this before.

According to the question that asked respondents installed any application on devices such as antivirus software to prevent cyber attack, 278 (87.97%) of the respondents answered they have installed antivirus software on their device, 15 (4.75%) of the respondents answered no and 23 (7.28%) of the respondents answered maybe.

Continue with the question that asked if the respondent ever has been a cyber attack victim, there were 252 (79.75%) of the respondents answered no, 37 (11.71%) of the respondents answered yes and 27 (8.54%) of the respondents answered maybe in this question.

Other than that, for the question "who will respondent report when faced with a cyber attack". In this question, respondents also can choose more than one answer, therefore most of the respondents answered family, friends or relatives which were 242 (76.58%) of the respondents. 149 (47.15%) of the respondents answered royal Malaysia police (PDRM) and 79 (25.00%) of the respondents answered national cyber security agency (NACSA).

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
	31-33	1	0.31
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
	Other	1	0.31
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

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 Figure 1, there are six questions for awareness level of cyber attack. Most of the respondents 197 (62.34%) disagreed with the statement "I create a password that contains my personal information such as last name, date of birth and others" while 17 (5.38%) of the respondents chose to strongly agree and neutral with this statement, respectively. From this result, it means that the respondents would not include their personal information when creating the password.

Regarding the second question of "I am aware of the danger when clicking on banners, advertisements or pop-up screens that appear when surfing 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 there were 3 (0.95%) of the respondents strongly disagreed with it. This means that most respondents would not readily click on pop-up ads.

For the third question of "I change the passwords of important accounts (such as online banking) frequently", 192 (60.76%) of the respondents rated agree while 13 (4.11%) of the respondents rated strongly disagree in this question. According to this result means most of the respondents will change their password in important accounts frequently to prevent cyber attack occur.

In the fourth question of "I feel safe when using public Wi-Fi", 198 (62.66%) of the respondents strongly disagreed with this question and there were 10 (3.16%) of the respondents who strongly agreed with the question. This result indicates that the majority of respondents know that connecting to an unknown public network is unsafe.

In the fifth question of "I regularly install software updates", 182 (57.59%) of the respondents strongly agreed with this question and there were 15 respondents (4.75%) who chose neutral with the question and 6 respondents (1.90%) who chose to strongly disagree. This means that most of the respondents strongly agreed with this statement as they always update the software on their system.

For the last question of "I am careful about clicking on links in an email or social media post", A total number of 187 (59.18%) respondents rated strongly agree while 2 (0.63%) of the respondents strongly disagreed with this question. This means that the respondents will be careful when click some unknown links, receive spam email and social media posts.

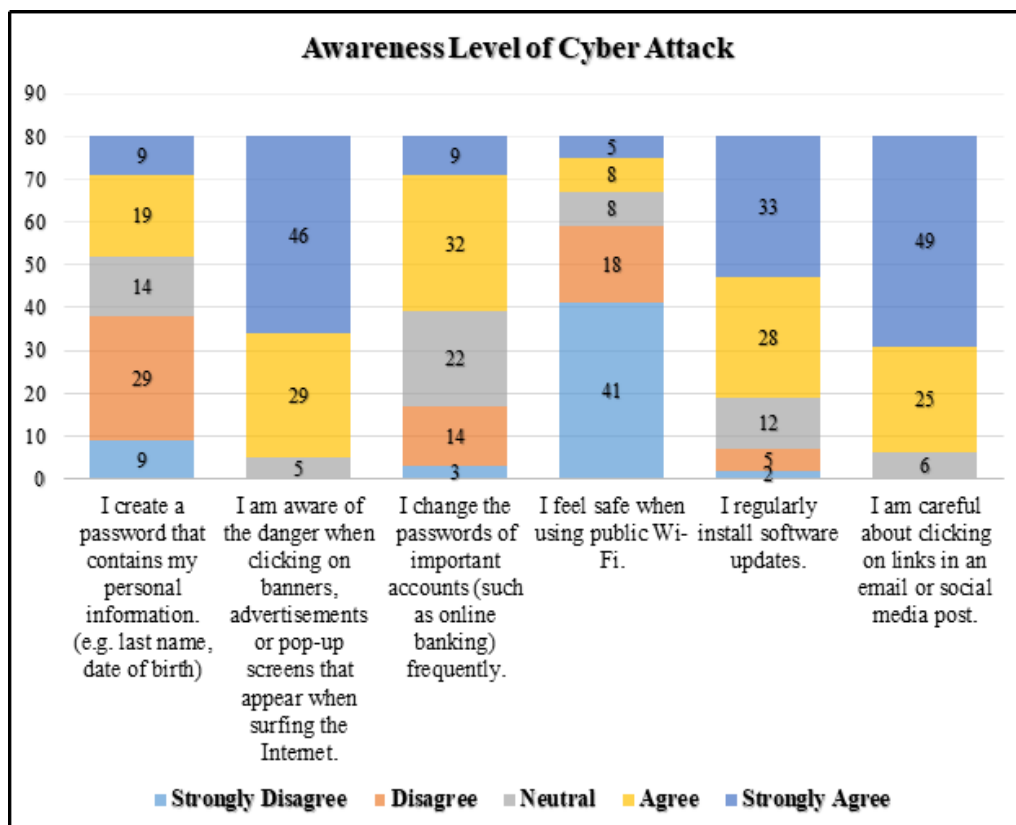


Figure 1. Awareness level of cyber attack

Table 3 showed the results related to the cyber attack awareness video. Referring to Table 4, 281 (88.92%) of the respondents answered yes for the question "Have you learned more about cyber attacks after watching the video?" and followed by 30 (9.50%) of the respondents answered maybe while the rest 5 (1.58%) respondents answered no. After that, on the statement of "Do you think this video is helpful to you?", 262 (82.91%) of the respondents answered yes while 50 (15.82%) of the respondents answered maybe and the remaining 4 (1.27%) of the respondents answered no.

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

8. CONCLUSION

In conclusion, this paper determines the types of cyber attacks, current trends, impact of cyber attacks and its prevention on network security. The paper study has sought a better understanding of the cyber attack among the UUM students. The findings showed there is a high level of awareness of the types, current trends, impacts and preventions of cyber attacks among UUM students. The change of routine activities from physical to online environment enhanced susceptibility and the possibility for cyber attacks and data breaches in current circumstances. In addition, network attack crimes continue to be common due to the growth of network attack technology. Cyber attack victims are no longer limited to people of a certain age group, so people of all ages must constantly enhance their understanding of cyber security and cyber attacks in order to truly avoid becoming the next victim.

ACKNOWLEDGEMENTS

The authors would like to thank to all School of Computing members who involved in this study. This study was conducted for the purpose of System and Network Security Research Project. This work was supported by Ministry of Higher Education Malaysia and Universiti Utara Malaysia.





REFERENCES

- [1] M. Zwilling, G. Klien, D. Lesjak, L. Wiecheteck, F. Cetin, and H. N. Basim, "Cyber security awareness, knowledge and behavior: 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, doi: 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, doi: 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 doi: 10.30564/ese.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/techrxiv.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, doi: 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, doi: 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, doi: 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 pandemic," *Journal of Advanced Transportation*, vol. 2021, pp. 1-19, 2021, doi: 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, doi: 10.1145/3264888.3264896.
- [13] A. Bendovschi, "Cyber-attacks – trends, patterns and security countermeasures," *Procedia Economics and Finance*, vol. 28, pp. 24-31, 2015, doi: 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, doi: 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, doi: 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, doi: 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, doi: 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.

BIOGRAPHIES OF AUTHORS







Ts. Dr. Mohamad Fadli Zolkipli     is an Associate Professor at the School of Computing, Universiti Utara Malaysia (UUM). He completed his doctorate degree in Computer Science at Universiti Sains Malaysia (USM) in 2012. His career in academia started when he joined KUKTEM / Universiti Malaysia Pahang (UMP) in July 2002 as academician. His teaching expertise includes Data Communication and Networking, Switching & Routing and Network Security. His research interests cover the broad area of digital security. He has published numerous articles in the area of computer systems and networking especially in security domain such as intrusion detection systems, malware analysis and cloud security. As a part of research community, he also involves as a reviewer for conferences and journals. He is currently active in supervising research students of master and doctorate degrees. He can be contacted at email: m.fadli.zolkipli@uum.edu.my.







Shu See Yong     currently is pursuing a bachelor degree of science with information technology in the School of Computing, Universiti Utara Malaysia (UUM) and major is networking. She is a student that was awarded Dean's List for 5 semesters and will be graduating in November 2022. She hopes to join the internship program in the information technology department in the near future. She can be contacted at email: shu_see_yong@soc.uum.edu.my.



Low Kai Kee     is pursuing a Bachelor of Science with Honours (Information Technology) at the School of Computing, Universiti Utara Malaysia (UUM). She is majoring in the networking course. She will be graduating in November 2022. She can be contacted at email: low_kai_kee@soc.uum.edu.my.



Gan Hui Ching     is pursuing a Bachelor of Science with Honours (Information Technology) at the School of Computing, Universiti Utara Malaysia (UUM). Her majoring course is networking. She was a student that was awarded Dean's List for 4 semesters. She will graduate in November 2022. She can be contacted at email: gan_hui_ching@soc.uum.edu.my.