Cybersecurity Issues and Challenges during Covid-19 Pandemic

1st Alya Hannah Ahmad Kamal
School of Computer Science & Engineering
Taylor's University
Selangor, Malaysia,
alyahannah@gmail.com

2nd Caryn Chuah Yi Yen
School of Computer Science & Engineering
Taylor's University
Selangor, Malaysia,
carynchuah3@gmail.com

3rd Mah Hui Ping
School of Computer Science & Engineering
Taylor's University
Selangor, Malaysia,
phoebemhp978@gmail.com

4th Fatima-tuz-Zahra
School of Computer Science & Engineering
Taylor's University
Selangor, Malaysia,
fatemah.tuz.zahra@gmail.com

Abstract – The world is currently experiencing COVID-19, one of the worst pandemics that have happened in this century, affecting 10.7 million people worldwide. It has caused massive growth in the number of employees working from home. However, employees have minimal cybersecurity resources unlike organizations with security teams protecting them against attacks. Hence, cybersecurity plays an important role as users can be easily targeted by cybercriminals. This paper examines how cyberattacks have increased during this pandemic and shows how greatly they have affected health organizations, individuals and social networking applications. Results of the attacks include data breaches, false announcements and operations being disrupted. Attacks occurring during this pandemic and how they were handled are also critically discussed. The existing contributions do touch on related attacks but do not provide in-depth solutions regarding the issues. Even though there are many works and findings that were done previously, technology is ever evolving. Therefore, we need to be well versed with current and future issues and provide the latest mechanisms to prevent cybersecurity threats from occurring. On our share, we intend to present our findings on the challenges being faced by the population and its increasing threats as well as presenting unique solutions that can help organizations or related persons understand or spread awareness on the importance of cybersecurity. Through the research performed in this paper, it is found that there are many ways these issues can be alleviated. However, the issue is that there is significant lack of action and investment in terms of actual implementation and application of the available solutions.

Keywords: Cybersecurity issues; cybersecurity challenges; Covid-19; security attacks

1 Introduction

Cybersecurity [1][2] protects information and assets while focusing on confidentiality, integrity and availability. A cybersecurity attack can be randomly or planned, whether it is by a single intruder, multiple intruders, or automated programs. The attack results in disabling computers or networks, data theft, and more. Various other factors have also lead to increase in attacks, such as insecure usage of unmanned aerial vehicles [3][4] methods can be used to launch an attack such as malicious software, DoS, ransomware and phishing. The success rate of an attack depends on the amount of information about the target and the special skills possessed by the attacker.

Attackers start by surveying the target to find potential vulnerabilities [5][6]. During the delivery stage, attackers will find the best route to deliver their exploit to the target's systems. At the breach stage, attackers exploit their vulnerabilities to gain unauthorized access to the system. The attackers could pretend as victims and use their legitimate access rights to access information. Lastly is the affect stage where they carry out activities such as retrieving information and disrupting digital operations within the target's system. Some attackers install automated scanning tools to detect more about the network and take control of them.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 September 2020 doi:10.20944/preprints202009.0249.v1

1.1 Real Attacks

In mid-March 2020, the Health and Human Services Department (HHS) in the U.S suffered the damage of the DDoS attack [7][8] with the inaccuracy of the announcement to the pandemic. They experienced a suspicion of intrusion in the system and investigated the problem as soon as possible to help enhance the security and maintain the integrity of the data being spread. The attacker did not access any of the data, but these cyberattacks were being suspected when the organization suspected the attack in the system with the sudden swarm of views on their website that aimed to slow the system to the point of the system hitting and interruption and resulting in a server crash.

Another real attack that happened was a malware attack called "Zoom-bombing" involving Zoom, a video conferencing platform which its users grew from 10 million to 300 million during this pandemic. Morphisec Labs researchers discovered that Zoom enables attackers to record sessions and screenshot chats without notifying the participants, enabling them to spy on the sessions. Records show that over 500,000 accounts are available on the dark web in April 2020. Zoom has added features such as reporting a user, approval from the host before entering a meeting and passwords to enter meetings with AES 256 bits GCM encryption [9-11].

The next real attack was a data breach [12][13] that involves EasyJet, a Swiss budget airline. EasyJet admitted it was hacked and confirmed the attacker accessed customers' information in the airline's systems between October 2019 and March 2020. They notified the U.K. Information Commissioner's Office and the National Cyber Security Centre. This attack has caused 9 million customers' data and 2000 credit card details to be leaked. EasyJet contacted the customers involved and warned users to be careful of unsolicited communications in case of phishing emails. EasyJet will be fetching £18 billion compensation to its customers.

Unacademy [14], an online educational platform also admitted they suffered a data breach, involving around 11 million users. However, Cyble who discovered the Zoom attack, said that it has acquired the leaked database containing 21 million users' account details, including usernames, passwords and emails from the dark web on May 3. Accounts that are using corporate emails are also on the line if the users use the same passwords on their company network, allowing the attacker to have access to the company networks. Unacademy is currently doing a complete background check to provide a more detailing report to the users involved.

Lastly was the NetWalker [15] ransomware attack [16] against the Illinois Champaign-Urbana Public Health District (CUPHD) website on March 10. They discovered the attack while officials were delivering COVID-19 updates on the website. Email addresses and health records were unaffected although the system went down temporarily preventing employees from accessing certain files. CUPHD has restored the availability of its website and is currently working with the U.S. Department of Homeland Security, Kroll and FBI on the investigation.

1.2 Recent Cybersecurity Attacks

One of the recent attacks [17] that happened during this pandemic was a DDoS attack on March 22 which targeted the Paris Hospital Authority(AP-HP). DDOS attack happens when a large number of systems flood the targeted system with traffic, normally done by using a botnet. AP-HP is the largest hospital network currently in Europe, having almost 39 hospitals with a large number of coronavirus patients. AP-HP offers not only healthcare but also research, education and prevention. In the AP-HP case, it is said that the attack was to overwhelm hospital computers and eventually disrupt digital operations. The attack lasted for an hour, paralyzing internet access to several services. It was then curbed at the right time.

Another recent attack that occurred was a malware attack [18] with coronavirus themed Winlocker which locks users out of affected devices. Malware attack is where attackers intend to infect networks or devices through virtual delivery that can cause the altering of the computer systems. [19] In the recent attack, the machine will drop a number of files with a hidden folder named "COVID-19" and modify the windows registries when the coronavirus-themed malware is executed. It will then play a sound and a virus-themed window with a message saying "System is locked" will be

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 September 2020 doi:10.20944/preprints202009.0249.v1

displayed. The machine will after that automatically restarts and a password is required to unlock the system. Some attacks and threats that are particularly observed during the pandemic period are shown in Fig. 1.

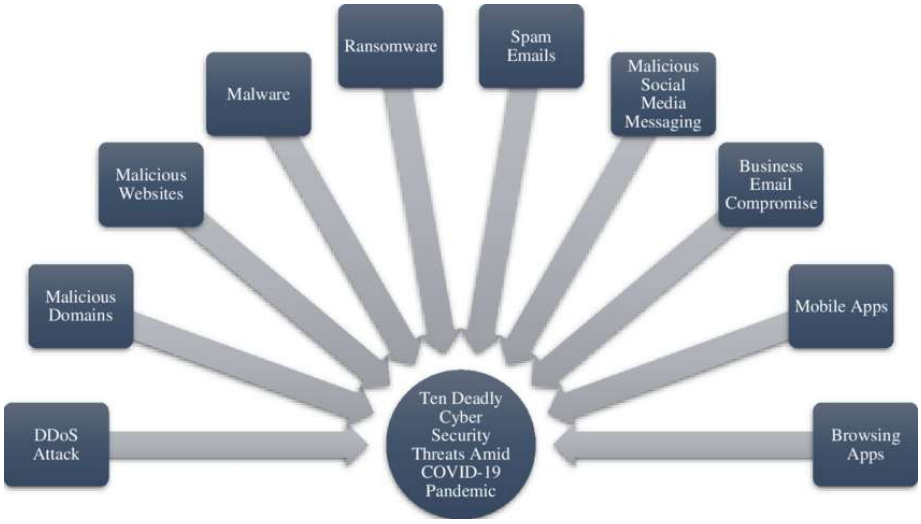

Fig. 1 Famous attacks and threats in the COVID-19 [18]

Phishing attacks happened recently as well where attackers use spam emails to lure the victims to provide them confidential information or to achieve their intended goals. As early as February 2020, attackers have been sending many coronavirus-related emails with malicious attachments to users. There are also attackers who deceive victims using domain spoofing by pretending to be people from the World Health Organization (WHO). They used the email coronavirusfund@who.org instead of the WHO official email that ends with "int" to trick the victims. Fig. 2 shows the rapid increase in malware and phishing websites visited by users during this pandemic.

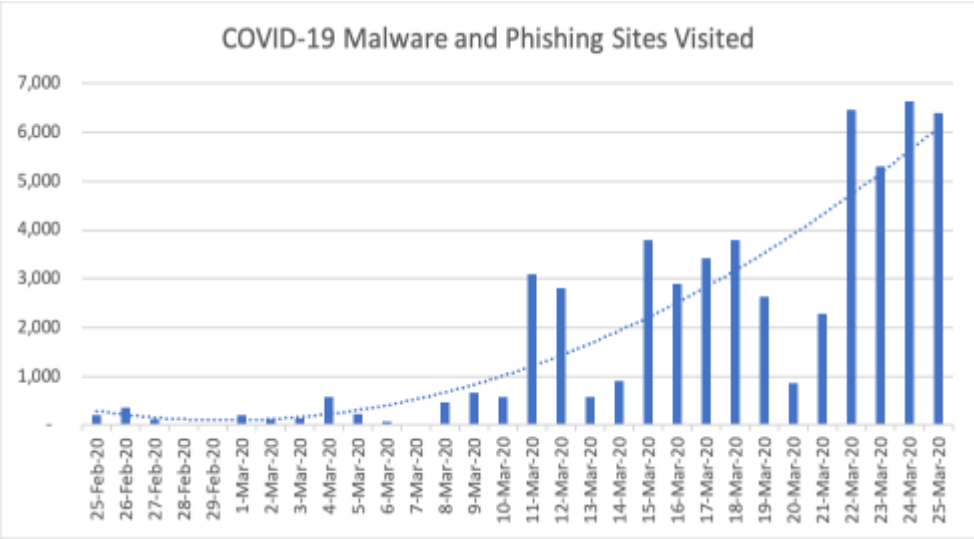

Fig. 2 COVID-19 Malware and Phishing Sites Visited [18]

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 September 2020 doi:10.20944/preprints202009.0249.v1

The next recent attack that happened during this pandemic was malicious apps. Most common malicious apps contain spyware that can record phone conversations, download other malware on the infected device, read location and other data stored in the device. Attackers are creating COVID-19 related apps and launching them in the Apple App Store and Android Play Store. Apple and Google can be seen removing some apps from the platform to reduce the number of victims of these malicious apps. During this pandemic, an android app that provides information about COVID-19 was launched. However, the app is filled with Android-targeting ransomware that is currently known as COVIDLock. The ransomware apparently locks the victim's phone, asks the victim for $100 in bitcoin within 48 hours and threatens the victim that it will erase data such as contacts and media stored in the mobile device.

The last attack that happened recently was the ransomware attack, a type of malware [20][21] that holds the user's device hostage until a "ransom" fee is paid. Ransomware infects systems using attachments from emails, malicious links or by fooling employees whose credentials are compromised. Recently, a new ransomware called CoronaVirus was spread through a fake Wise Cleaner website. Victims who download the fake setup file (malware) will cause their sensitive data such as passwords and information from the system from getting stolen. A text file named CoronaVirus.txt with payment instructions inside is created in each affected directory in the device. CoronaVirus also encrypts files that are in the device. Upon encryption completion, the computer will restart automatically.

2 Literature Review

COVID-19 has changed the world in many different ways and has raised problems that we have to adapt to and strategize on solving them. The main problem that we will be focusing on is the cyberattacks that have been happening more often due to this pandemic. John C. [22] has performed research and reported that there was an increase in the phishing attack on websites that spiked by 250% because of the pandemic and a spike was observed in phishing sites by Google (Fig. 3). The increase in the percentage of the population has hit over 500 thousand people in total in March 2020. Hackers have made a profit out of selling fake drugs and medical tools that were said to cure the disease. There was an increase in the numbers of trafficking the products through these fraud websites that have lured individuals to buy items at a high price, such as hygiene items like facial masks, wet wipes, hand sanitizers and other products. Police even reported that there are cases that revolve around the health industry where attackers will impersonate them to gain funding saying it was to fund the health institutions. The risk has been drastically increasing as people started to adapt to the new norm of being indoor and staying safe, they should also be wary of the safety while being indoors since the only way of being part of the outside world now is through the source of the internet.

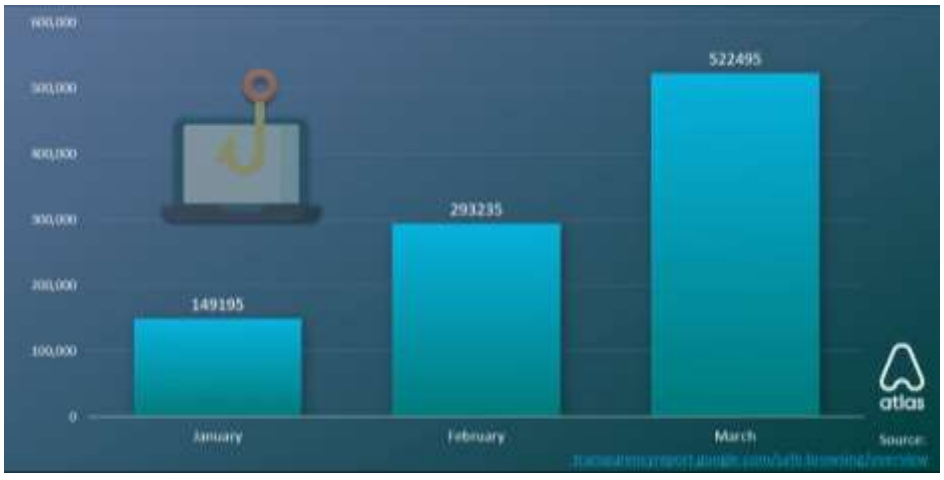

Fig. 3 Phishing websites detected by Google in 2020 during the pandemic [22]

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 September 2020 doi:10.20944/preprints202009.0249.v1

Among all of the cybersecurity threats that have been occurring through the pandemic, phishing attacks have been the subcategories for which all the main threats have been identified and studied in [18]. These attacks have taken a huge toll on individuals ever since the outbreak began and the cases started to drastically increase as the days go on as announced on 31st January 2020. The spread of the disease has completely forced the people of the world to stay indoors for it will help decrease the rate of spreading from happening. But to stabilize or even maintain the economic status of business from being closed down or being damaged. It was important for them to stay in touch with the company and coworkers whereas the use of communicational applications such as Microsoft Teams or Zoom has experienced an increase of 300 million meeting participants daily in April 2020 announced by Eric S. Yuan. But as the numbers increase, the risk of falling victim to cyber-attacks will also rise if they were to not be careful with their platform's security measures. As the research studied by Navid Ali Khan, there are cases regarding the Zoom application where they have experienced a fall out whereas their default settings are no longer safe to the point of them being banned by some of the organizations and even some countries as well.

More individuals or rather organizations have been fallen victim to attacks such as smishing attacks which is a type of performing phishing attacks but with the method of sending SMS text messages, that was researched by Dr. Ben Collier, Dr. Shane Horgan, Dr. Richard Jones, and Dr. Lynsay Shepherd [23]. Their studies show that attackers are taking advantage of this pandemic to be able to gain profit out of it as there is a case where numerous SMS scams targeting individuals were sent a message that they were fined and charged for leaving the house. Apparently, there are more than once per day these cases have been reported to the authorities. This research has also brought up another case that has been occurring a lot during this pandemic, which is fraudulent of mobile applications. These are one of the categories of phishing as well where a text message is generated that has the link that will bring the victims to a website that will request for their confidential data. This was reported by Guardian based on this research where there is an increase in frauds and attackers impersonating them as legitimate applications providing government services.

We will also touch on the platforms that people in a worldwide scale use the most which are social media such as Facebook, Twitter, YouTube, Instagram and TikTok**.** [24] In the research conducted by Marites V. Fontanilla, there is an uproar on the rumors of the health emergency being spread throughout these internet platforms which is creating more confusion among the people. This information is spreading through the spam emails (Fig. 4) that many individuals are receiving. The news will give a sense of emergency through it along with an attachment of a COVID-related URL that will bring the user to a website or a file that contains malware in them that will spread throughout their system. These malicious acts have been happening recently with the numbers of users accessing them coming to 900 thousand people falling for these fraudulent attachments.

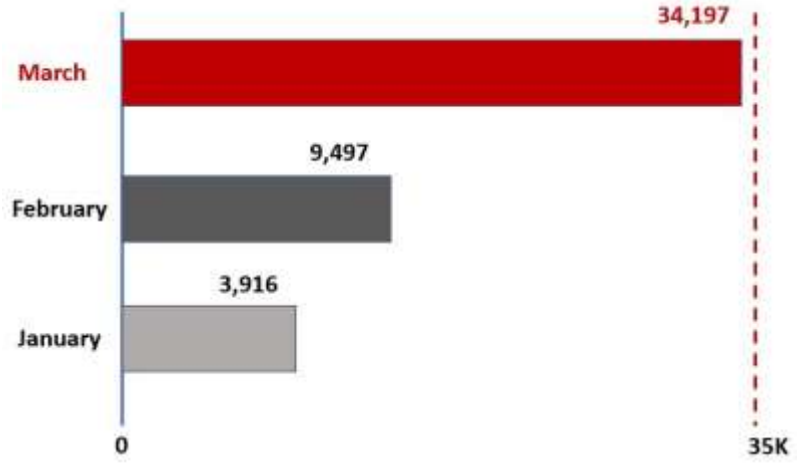

Fig. 4 Statistics of spam email detection between January and March 2020 by Trend Micro Security News

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 September 2020 doi:10.20944/preprints202009.0249.v1

These cybercriminals were disguising themselves as those healthcare institutions such as the World Health Organization (WHO) to find their opportunity to steal as much private information or data from whoever had fallen victim to it. These cybercriminals have or are being provided by companies. Teleworkers are increasing day by day, which in turn exposing themselves to more vulnerabilities and they will take advantage of the unsecured network devices or weak configuration of it. [25] There has been annual damage of $445 billion in a global scale because of the cybercrimes that have been happening, according to the research from Arnold and Edem, and it is said to become more economically damaging if teleworkers were to increase or stay longer since the pandemic requires all people to stay indoors to prevent the spread of the coronavirus. The occurrences of the increase in the cybercrimes are bound to happen, hence there should be an enhancement in the security for the safety of all these teleworkers whilst working. One of the methods that are being discussed in the research of Arnold and Edem is that they will be using a strategy called Social Engineering, which involves the psychological side of manipulation employed by hackers. This study proves that cybercriminals have been coming up with new ways of how they can gather confidential information or compromise the security of the organizations or themselves as well.

3 Implementation Scenarios

One of the organizations that had experienced a cyber-attack incident is the Zoom application. The case of where explicit videos are played to the children has occurred and they have issued a lawsuit for being shown these graphical images during a class session [26]. How they have dealt with this problem is that they followed the procedure where they identified what type of problem it was and found the culprit behind this attack. They have also updated their security measures which will heighten their data security which in turn ensures that the users of Zoom application will have a more secure option when it comes to being communicating with others while maintaining social distancing during the pandemic. With the spike in their popularity, they have also made an effort to have a constant practice on the security policies that are updated and established such as free accounts are required to use a password whenever they want to enter a meeting at all times [27]. They also put a halt in adding new features on the UI and focused on the safety issues. Pulling this move is the best to increase the security status of their application where they are adding more of them such as the clarification of the encryption practices, giving users the guidelines to avoid being a victim of the cyber-attacks as well [28]. They are also adapting to the current issues that are happening and strategize and plan for their future to avoid any of the same attacks such as these from happening.

World Health Organization (WHO) is also one of the organizations that are experiencing events such as attackers impersonating them to gain sensitive data or money from people who have been falling victim to the spam emails. [29] The way they have countered this is that they announced policies for the people so that they will know what is and is not genuine emails that are from them and not an attacker that is disguised as them. WHO was prepared to keep the people safe from this event from happening since the pandemic is something that the attackers will take advantage of. They also provided procedures of when the receivers got an email that was from them. So, targeted victims do not need to be confused when they do receive one before responding to them. The attackers are taking advantage of the COVID-19 pressure and WHO has been aware of this situation from happening. So, it was important for them to show the safety measures before responding to one of those emails. This is the main problem that they are facing and it will be increasingly damaging if they do not establish any policies or procedures for people to follow for them to protect themselves from these attackers.

4 Issues and Challenges

As technology advances every day, cybercriminals are also improving their techniques to reach their goals. Our research shows that most cyberattacks are due to human factors. Humans transmit information online, exchange information with people and organizations, making most of their time to have the highest efficiency. And to get the efficiency, the easiest way to go online, from documentation, messaging to shopping.

One of the factors people are vulnerable in cybersecurity is because we are lacking common practice and training on security [30]. Normal users like company employees who are not professionals in technology will not know how

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 September 2020 doi:10.20944/preprints202009.0249.v1

easily cyberattacks can take place. A small mistake can cost the individual or the company a tremendous financial loss or data loss. The lack of practice and training causes employees to not be aware of social engineering attacks such as phishing and email malware. These attacks involve deceiving people into breaching standard security practices. For company employees, they often fall into attacks when they receive emails from cybercriminals who are faking their identities as superior or colleague. With a click in the email, cybercriminals can easily obtain the information that is stored in the employee's device.

Next is due to humans relying on technology too much. Nowadays, users store their files on cloud services. However, cyberattacks on cloud services have doubled in 2019, making cloud services the third most targeted platform by cybercriminals currently. Users not only store files on cloud services, but also passwords on their browsers for convenience. This eases users during logins by auto-filling the credentials after user's authentication. For example, Google Chrome allows users to save their passwords in his/her Google account. Upon successful login, all the passwords can be read. Hence, if the user's Google account is accessed by an unauthorized user, the unauthorized user will have access to all his/her other accounts. Having a weak password and using the same password across platforms and applications are also very dangerous. Weak passwords can be easily hacked in minutes. This is also why websites have made it compulsory for users to have a strong password which includes alphanumeric, special characters and capitalization.

Other than that, oversharing is also one of the issues and challenges in cybersecurity. Users normally tend to overshare information about themselves or people around them on the Internet, especially users who are into social media such as Instagram and Facebook. They share their daily activities, their list of friends, contact number or even check-in at their location in real-time. Users also share sensitive information such as bank account details or house addresses in messages while chatting. If the messaging platform does not have encryption available, user chats can easily be obtained. All these data can be used as information for cyber criminals when they are planning the attack.

Besides, another issue and challenge in cybersecurity is people risk management, authorization, and access control [31]. This issue points to companies or organizations. The reason why employees are always the factors of cyberattacks occurring is that there is a probability of malicious insiders existing among the employees in a company. A malicious insider threat to a company can be a current employee, a former employee or even a business partner who has authorized access to the company's system and information. This malicious insider intentionally misuses access and does something that negatively affects the company. Organizations must make sure that former employees no longer have access to the organization's data and authorized access to the organization's server. The organization's access control should be enforced, and the access should be granted based on the employee's role in the organization. Employees can also make mistakes due to lack of training as mentioned above or their careless mistakes losing devices such as laptops and company mobile phones that consist of important company information.

Lastly, is the negative attitude to handling information and devices. Users do research and download files and media from the browser without checking properly at the sources. This is extremely dangerous, especially for emails. As mentioned above, the cybercriminal can steal another person's identity and acts as the sender. Checking whether the email address of the sender or checking whether the URL link that you are browsing is correct and secure is very important. The same goes for devices, users always avoid updating their software to save time as updates take time.

5 Solution for Issues and Challenges

5.1 Based on Literature Study

There are many cases that are regarding phishing attacks or relevant attacks to them. One of which is the use of luring the users with text messages and emails that are being sent and the attackers disguising as those from the health industry to gain sensitive data. This is a way that they have been using to trick those targeted victims as discussed previously. These individuals should be informed or rather educated on the practices that are being carried out in order for them to understand the consequences of being attacked by them. This solution is regarding the safety measures

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 September 2020 doi:10.20944/preprints202009.0249.v1

that the people should take to keep themselves safe from encountering fraudulent messages being transmitted to them. When they have a basic understanding of the dangers while receiving something such as an email that is too good to be true. The awareness of cybercrimes will be increased, and people will take extra precautions when they are putting themselves into the world of the internet. This is also a progression that can be made where they start installing Firewalls into their computer systems or having a Virtual Private Network (VPN) in their networks and so many more.

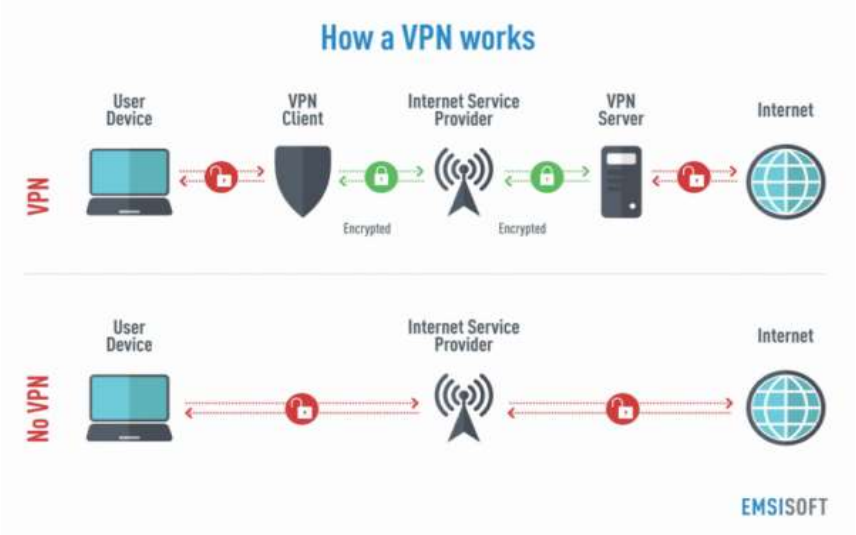

Fig. 5 Virtual Private Network functionality [32]

Not only individuals are being affected but something as big as organizations too where damages on them financially. So, the administration of the organizations should secure the network with website security protocols or tools that can block any suspicious entities through the internet. Protocols that should be applied are using websites that have HTTPS to provide security when they are visiting any websites. This will be a guide for employees in the organizations, which in these times, they have transitioned into becoming teleworkers as discussed in previous sections. Organizations should also prepare and update on their plan for their responses when they have experienced any incidents. It would show that they would be able to quicken the process of responding and recovering themselves in their future challenges. Keeping things such as the security policies, software or hardware updated is also a procedure that should be taken to account for a secure network or visiting sites. So, teleworkers would have been able to avoid the means to communicate with any of the disguised attackers when they have practiced and have basic training when it comes to communicating with them.

5.2 Based on Scenarios

Zoom encountered a security breach that involved a Bible study class where a hacker hijacked and posted graphic images of child abuse during the users' meeting [26]. This unprecedented attack led to the company being filed a lawsuit by the victims which in turn brought the company under intense scrutiny by the masses regarding their security and privacy measures. Zoom took measures such as updating their security policies, heightening security, halting future feature production as well as adaptation. Firstly to allow more prompt actions to be taken especially by users, the company decided to centralize the security features of the application for accessing features such as locking a meeting, enabling virtual wait rooms that are set on default, removing participants, and restricting screen sharing rights to name a few [33]. Taking a step further, the company obtained Keybase, a protected messaging and file-sharing service, to enhance their recently added end-to-end encryption that supports content encryption until AES-256 [34].

On the other hand, the World Health Organization (WHO) has faced cyberattacks of criminals sending fraudulent

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 September 2020 doi:10.20944/preprints202009.0249.v1

emails and messages that expose user's sensitive information. However, WHO tackled this challenge by providing step-by-step guidelines for those who are contacted by hackers impersonating the organization. WHO clearly stated actions that would never be done by the organizations itself such as asking for the users' password and being charged money. The organization also provided advice on how people can prevent phishing attacks. By doing this, WHO not only showed how well prepared they are in stopping cyberattacks but also increased the awareness of cybersecurity and the threats that come with it within the population. Overall, WHO is an example of a company that takes necessary steps to ensure security threats are avoided and mitigated accordingly [29].

5.3 Based on Issues Found

For the issues that were mentioned previously, in this segment we are going to discuss what solutions can be applied to resolve the aforementioned. The first issue, the lack of common practice and training on security. This can be solved by companies themselves taking the initiative to provide in-depth training to employees to ensure the awareness of various cyberattacks. These arrangements can improve the overall security performance of the company as sufficient training will allow the employees to build their own awareness of the importance of understanding why and how to avoid these threats. Hence, reducing the number of cybersecurity attacks occurring within an organization.

Next, the issue of clients and users being too reliant on technology as well as the concern of oversharing and poor data management. This problem can be dealt with by companies providing basic guidelines on how users can be more aware and understand the security risks that lie on their fingertips. Another approach the companies can go for is the use of digital and physical marketing as visualizing the guidelines will definitely catch users' attention and that the steps can be easily digested.

Moving on, people risk management, authorization and access control is another core issue that can be seen in the workforce. This issue can be solved by the companies having a complete and well-defined process and proper communication plan. This approach can lessen miscommunication and coordination troubles as having proper deadlines, clear hand in requirements, as well as established communication channels, contribute to a more efficient workflow. Strict access policy for sensitive data should also be considered. Other than that, training and the welfare of the employees are an important aspect to apply so that the possibility of a malicious insider can be reduced.

Lastly, the issue of negative attitudes in handling information and devices. However, this can be resolved if the companies ensure that the software is up to date, especially antivirus software. This is because cybercriminals are trying to stay one step ahead of antivirus software manufacturers. By updating the antivirus software, it can help prevent malicious attacks. at the same time making sure the software is working with the latest updates from the user's operating system.

Another issue is insecure usage of modern digital devices, such as internet of things. They must be implemented after integration of security component and sufficient security check in the designing and development phase. Several solutions have been proposed for securing communication which occurs through these devices, such as in [35-37] as there has been a steep increase in their deployment. These solutions need to be applied in practical applications of such devices.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 September 2020 doi:10.20944/preprints202009.0249.v1

5.4 Awareness Guidelines

Table 1: Guidelines and implementation strategy and process in an organization are shown in Table 1 [38]:

A. Assessment	***B. Planning***
1. Review current security environment 2. Determine regulations that are applicable 3. Determine all components that provide access 4. Find all potential access points 5. Identify legitimate users and their privileges	6. Equipment replacement plan 7. Change management plan for software 8. Segmentation of network 9. Whitelisting of applications 10. Encrypting transmissions 11. Monitor networks and limiting access 12. Strict authentication plan 13. Response and recovery plan 14. Penetration testing and overall test plans 15. Physical security plans
C. *Deployment*	**D. *Monitor and Log***
16. Ensure compliance with the policies *17.* Prioritize vulnerabilities and threats	18. Keep and always note all discrepancies 19. Maintain a CSIRT, attack response team 20. Have a recovery plan to ensure data can be restored

Measures taken to spread awareness regarding protection from cybersecurity:

A measure that can be applied is awareness training. As we know even if all the prevention methods and security systems are applied, attacks can still occur due to human blunders. Therefore, awareness training is a crucial measure to avoid such errors from persisting. By providing defense training that covers aspects such as current threats, attack red flags, steps on tackling attacks and threat response plans, the organization can give a foundation for employees where they can counteract and be more assertive when issues arise [39]. Also, hand-on training such as organizations having monthly mock training by deploying mock cyberattacks to the employees. This will equip them with the necessary knowledge and experience to prepare for any unexpected situations. Next, organizations should arrange a strategy in regards to data recovery and clearly state the strategy so the clash of responsibilities is avoided. By implementing this measure, the data that would have been lost or damaged by the attacks can be retrieved from the alternate storage [40]. Early detection and planning is another way that can help increase awareness of cybersecurity. Having the ability to quickly identify risks can help organizations to contain the damage and reduce loss from the attack [40]. With all these practices and more, the importance of protecting data with cybersecurity will surely be clear to the persons involved. By taking all these measures into account, it will instill a sense of responsibility amongst the personnel and ultimately embed a culture of cybersecurity enforcement and awareness. As Head of IT for PT IBS, Faisal Yahya said ”The impact of cyberattacks can only be mitigated by promoting initiatives within companies and implementing the best mitigation strategies for customers” [41].

6 Conclusion

Through the research carried out in this paper, it is observed that cybersecurity is a field of study that should not be disregarded as we are moving towards an age of technology that is ever evolving and changing especially during these unexpected times where cybersecurity is more essential than ever. Cybersecurity efforts must be maintained and enhanced as cybercriminals are becoming more frequent and sophisticated. These cybercriminals are attacking and instilling fear into the population, becoming more assertive and fearless as cybersecurity is not enforced enough. These issues and challenges can be overcome by the public and related stakeholders if serious initiative is taken and approach to more robust and secure networks is steered appropriately. Concluding our views, we do trust that with combined efforts, a more protected and well adaptive system can be achieved in cybersecurity. From the analysis carried out in this paper, it is found that many issues are still surfacing in the cyber world and that it is only expanding due to organizations’ lack of resolution and the people's insensitivity towards these current concerns which are becoming more apparent. Furthermore, the advancement in terms of hacking and attacking capabilities of attackers is proving to

be a growing threat against the security and privacy of systems and people who are connected with this these systems. However, it is also observed that increase in developing cybersecurity solutions is becoming an important factor as well and will continue to be a fundamental discipline of interest for research in upcoming years due to the huge involvement of digital technology in our life at individual and organizational level.

References

[1]. J.Niekerk,"From information security to cyber security", Science Direct, 2020. [Online]. Available: https://www.profsandhu.com/cs6393_s19/Solms-Niekerk-2013.pdf. [Accessed: 06- Jul- 2020].

[2]. Humayun, M., Niazi, M., Jhanjhi, N. et al. Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arab J Sci Eng 45, 3171–3189 (2020). https://doi.org/10.1007/s13369-019-04319-2

[3]. Khan, N.A., Jhanjhi, N.Z., Brohi, S.N. and Nayyar, A. (2020). Chapter Three - Emerging use of UAV's: secure communication protocol issues and challenges, Editor(s): Fadi Al-Turjman, Drones in Smart-Cities, Elsevier, 2020, pp 37-55.

[4]. Khan N.A., Brohi S.N., Jhanjhi N. (2020) UAV's Applications, Architecture, Security Issues and Attack Scenarios: A Survey. In: Peng SL., Son L., Suseendran G., Balaganesh D. (eds) Intelligent Computing and Innovation on Data Science. Lecture Notes in Networks and Systems, vol 118. Springer, Singapore. https://doi.org/10.1007/978-981-15-3284-9_86

[5]. A.G. Bardas, S.A. DeLoach, "A Theory of Cyber Attacks | A Step Towards Analyzing MTD Systems", Cse, 2020. [Online]. Available: https://www.cse.usf.edu/~xou/publications/mtd15.pdf. [Accessed: 06- Jul- 2020].

[6]. "How cyber attacks work", National Cyber Security Centre, 2020. [Online]. Available: https://www.ncsc.gov.uk/information/how-cyber-attacks-work. [Accessed: 06- Jul- 2020].

[7]. O. Kupreev, E. Badovskaya and A. Gutnikov, "DDoS attacks in Q1 2020", Secure List, 2020. [Online]. Available: https://securelist.com/ddos-attacks-in-q1-2020/96837/. [Accessed: 06- Jul- 2020].

[8]. S. Stein, J. Jacobs, "Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak", Bloomberg, 2020. [Online]. Available: https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response. [Accessed: 06- Jul- 2020].

[9]. D. Petrillo, "Zoom Malware Can Record Meetings; Attack Simulation Shows How", Security Boulevard, 2020. [Online]. Available: https://securityboulevard.com/2020/04/zoom-malware-can-record-meetings-attack-simulation-shows-how/. [Accessed: 06- Jul- 2020].

[10]. K. Paul, "Zoom releases security updates in response to 'Zoom-bombings'", The Guardian, 2020. [Online]. Available: https://www.theguardian.com/technology/2020/apr/23/zoom-update-security-encryption-bombing. [Accessed: 06- Jul- 2020].

[11]. K. O'Flaherty, "Zoom's 200 Million Users Are Facing A Serious New Threat", Forbes, 2020. [Online]. Available: https://www.forbes.com/sites/kateoflahertyuk/2020/04/20/zooms-200-million-users-are-facing-a-new-threat-heres-what-to-do/#1b0a7b95b83d. [Accessed: 06- Jul- 2020].

[12]. T. Brewster, "EasyJet Hacked For Four Months, Data On 9 Million Customers And 2,000 Credit Cards Stolen", Forbes, 2020. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2020/05/19/easyjet-hacked-9-million-customers-and-2000-credit-cards-hit/#69db98bd1ae1. [Accessed: 06- Jul- 2020].

[13]. N. Goud, "Cyber Attack on easyJet will fetch £18 Billion compensation to customers", Cybersecurity Insiders, 2020. [Online]. Available: https://www.cybersecurity-insiders.com/cyber-attack-on-easyjet-will-fetch-18-billion-compensation-to-customers/. [Accessed: 06- Jul- 2020].

[14]. "Unacademy hacked, data of 20 million users up for sale", The Week, 2020. [Online]. Available: https://www.theweek.in/news/sci-tech/2020/05/07/unacademy-hacked-data-of-20-mn-users-up-for-sale.html. [Accessed: 06- Jul- 2020].

[15]. D. Kobialka, "NetWalker Ransomware Attacks Illinois Public Health District", MSSP Alert, 2020. [Online]. Available: https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/netwalker-attacks-illinois-public-health-district/. [Accessed: 06- Jul- 2020].

[16]. Ren, A.L.Y., Liang, C.T., Hyug, I.J., Brohi, S.N. and Jhanjhi, N.Z. (2020). A Three-Level Ransomware Detection and Prevention Mechanism. EAI Endorsed Transactions on Energy Web.

[17]. Abdullah, "Coronavirus: Paris hospitals hit by a cyber attack", Gizchina, 2020. [Online]. Available: https://www.gizchina.com/2020/03/24/coronavirus-paris-hospitals-hit-by-a-cyber-attack/. [Accessed: 06- Jul- 2020].

[18]. N.A. Khan, S.N. Brohi, N. Zaman, "(PDF) Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic", ResearchGate, 2020. [Online]. Available: https://www.researchgate.net/publication/341324576_Ten_Deadly_Cyber_Security_Threats_Amid_COVID-19_Pandemic. [Accessed: 06-Jul.-2020].

[19]. "Developing Story: COVID-19 Used in Malicious Campaigns -", Trend Micro, 2020. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains. [Accessed: 06- Jul- 2020].

[20]. Kok, S.H., Abdullah, A. and Jhanjhi, N.Z. (2020). Early detection of crypto-ransomware using pre-encryption detection algorithm. Journal of King Saud University - Computer and Information Sciences.

[21]. Kok, S.H., Abdullah, A., Jhanjhi, N.Z. and Supramaniam, M. (2019). Ransomware, Threat and Detection Techniques: A Review. IJCSNS International Journal of Computer Science and Network Security, VOL.19 No.2, February 2019.

[22]. C. John, "Google Registers a 350% Increase in Phishing Websites Amid Quarantine - Atlas VPN", atlasvpn, 2020. [Online]. Available: https://atlasvpn.com/blog/google-registers-a-350-increase-in-phishing-websites-amid-quarantine. [Accessed: 06- Jul- 2020].

[23]. B. Collier, S. Horgan, R. Jones and L. Shepherd, "Research Evidence in Policing: Pandemics", Semantic Scholar, 2020. [Online]. Available: https://pdfs.semanticscholar.org/fea1/fbdca34bc77e87d3ce38051f37987fb7cb0b.pdf?_ga=2.161960572.1530827090.1593388457-407571284.1587968516. [Accessed: 06- Jul- 2020].

[24]. M. Fontanilla, "Cybercrime pandemic", Eubios, 2020. [Online]. Available: https://www.eubios.info/EJAIB52020.pdf#page=33. [Accessed: 06- Jul- 2020].

[25]. A. Abukari and E. Bankas, "Some Cyber Security Hygienic Protocols For Teleworkers In Covid-19 Pandemic Period And Beyond", Tutag, 2020. [Online]. Available: http://tutag.org/wp-content/uploads/2020/05/Some-Cyber-Security-Hygienic-Protocols-For-Teleworkers-In-Covid-19-Pandemic-Period-And-Beyond-1.pdf. [Accessed: 06- Jul- 2020].

[26]. "US church sues after bible study 'Zoombombed' by child abuse", BBC, 2020. [Online]. Available: https://www.bbc.com/news/world-us-canada-52668124?intlink_from_url=https://www.bbc.com/news/topics/cp3mvpdp1r2t/cyber-attacks&link_location=live-reporting-story. [Accessed: 06- Jul- 2020].

[27]. "Zoom Security Guide", Zoom, 2020. [Online]. Available: https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf. [Accessed: 06- Jul- 2020].

[28]. J. Wakefield, "Zoom boss apologises for security issues and promises fixes", BBC, 2020. [Online]. Available: https://www.bbc.com/news/technology-52133349. [Accessed: 06- Jul- 2020].

[29]. "Beware of criminals pretending to be WHO", World Health Organization, 2020. [Online]. Available: https://www.who.int/about/communications/cyber-security. [Accessed: 06- Jul- 2020].

[30]. B. Gyunka and O. Christiana Abikoye, Analysis of Human Factors in Cyber Security: A Case Study of Anonymous Attack on Hbgary. 2017, pp. 10-14. [Accessed: 06- Jul- 2020]

[31]. "Malicious Insider", Science Direct, 2020. [Online]. Available: https://www.sciencedirect.com/topics/computer-science/malicious-insider. [Accessed: 06- Jul- 2020].

[32]. Haylee (2017). VPNs: Your personal tunnel to privacy. EMSISOFT. [image]. Available at: https://blog.emsisoft.com/en/27485/vpn-privacy-2/. [Accessed: 07- Sept- 2020].

[33]. P. Zaveri, "Zoom is making its security features easier to access, as it moves to improve the privacy of its app and stop all the 'Zoombombing'", Business Insider, 2020. [Online]. Available: https://www.businessinsider.com/zoom-security-features-easier-access-stop-zoombombing-eric-yuan-2020-4#:~:text=Zoom%20is%20making%20its%20security%20features%20easier%20to%20access%20by,due%20to%20the%20coronavirus%20pandemic. [Accessed: 06- Jul- 2020].

[34]. R. Hodge, "Zoom security issues: Zoom buys security company, aims for end-to-end encryption", CNET, 2020. [Online]. Available: https://www.cnet.com/news/zoom-security-issues-zoom-buys-security-company-aims-for-end-to-end-encryption/. [Accessed: 06- Jul- 2020].

[35]. A. Diro, H. Reda, N. Chilamkurti, A. Mahmood, N. Zaman and Y. Nam, "Lightweight Authenticated-Encryption Scheme for Internet of Things Based on Publish-Subscribe Communication," in *IEEE Access*, vol. 8, pp. 60539-60551, 2020, doi: 10.1109/ACCESS.2020.2983117.

[36]. M. Saleh, N. Jhanjhi, A. Abdullah and Fatima-tuz-Zahra, "Proposing a Privacy Protection Model in Case of Civilian Drone," 2020 22nd International Conference on Advanced Communication Technology (ICACT), Phoenix Park, PyeongChang,, Korea (South), 2020, pp. 596-602, doi: 10.23919/ICACT48636.2020.9061508.

[37]. Hussain, S.J., Irfan, M., Jhanjhi, N.Z. et al. Performance Enhancement in Wireless Body Area Networks with Secure Communication. Wireless Pers Commun (2020). https://doi.org/10.1007/s11277-020-07702-7

[38]. "How to design and implement a cyber security strategy: Critical Infrastructure Security Guide 2", Taiit Communications, 2020. [Online]. Available: https://www.taitradio.com/__data/assets/pdf_file/0003/156063/Critical-Infrastruce-Guide-2-v2.pdf. [Accessed: 06- Jul- 2020].

[39]. "What is Cybersecurity Awareness Training and Why is it so Important?", FraudWatch International, 2020. [Online]. Available: https://fraudwatchinternational.com/security-awareness/what-is-cyber-security-awareness-training/. [Accessed: 06- Jul- 2020].

[40]. "The Importance of Cyber Security Awareness", OGL Computer, 2020. [Online]. Available: https://www.ogl.co.uk/the-importance-of-cyber-security-awareness#:~:text=When%20an%20enterprise's%20employees%20are,crime%20infiltrating%20their%20online%20workspace. [Accessed: 06- Jul- 2020].

[41]. C. Lago, "How to implement a successful cybersecurity plan", CIO, 2020. [Online]. Available: https://www.cio.com/article/3295578/how-to-implement-a-successful-security-plan.html. [Accessed: 06- Jul- 2020].