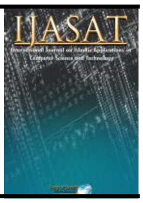


The Impact of COVID-19 on Cybersecurity

Nada Al-shammari[1], Kholood Al-shammari[2], Nouf Muhawwis[3], Nouf Al-shammari[4], Wejdan Alharbi[5] and Nemah Al-shammari[6], Kawther Al-Dhlan[7]

[1,2,3,4,5,6,7] Cybersecurity, College of Computer Science and Engineering, University of Hail, Kingdom Saudi Arabia

[1] Nadaalshammari1996@gmail.com, [2] KholoodAlshammari@outlook.sa, [3] Nouf-m92@hotmail.com ,[4] nouf201215079@gmail.com ,[5] albladiwejdan@gmail.com , [6] dd.nnemmah2@gmail.com, k.aldahlan@uoh.edu.sa[7]

Abstract

COVID-19 pandemic-imposed restrictions on individuals' daily lives and attempted to prevent coronavirus spread and forced many governments to impose social distancing in all sectors, which caused everyone to work remotely. Many challenges have emerged due to the changes that occurred in our lives in 2020. shift to working from home due to the COVID-19 pandemic, which gets a chance of increasing piracy and cyber-attacks by exploiting many vulnerabilities resulting from employees' remote work into their institutions' electronic systems. Many companies were unprepared to counter these changes, which led to many consequences to be attacked. And attackers took advantage of those companies that did not have sufficient protection for work remotely. They exploited the pandemic to publish fake news and impersonated websites to achieve their malicious intent. The research discussed the reasons for a surge in cybercrime during the COVID-19 pandemic and clarified the most affected sector by cyber-attacks during the COVID-19 pandemic. Furthermore, it highlighted the most common cyber-attacks that were carried out during the current period (COVID-19). Also discussed some cyberattacks that target some companies on the pandemic. The research conducted was based on literature reviews and theoretical that defined the reasons for the increased attack through the COVID-19 pandemic. This research reviewed the analytical data that identified the most sector and attack that happened during COVID-19.

Keywords: *COVID-19 pandemic; Cybersecurity; Security threats; Phishing attack; Working remotely.*

1. Introduction

All the world aware of the Coronavirus (Covid-19) has had a significant impact on life, and the severity of this effect varies from sector to sector. This epidemic began in the year 2019 and continued until our current time and quickly turned into a global crisis, which required the mass quarantine of thousands of millions of citizens in various countries around the world. The spread of (COVID-19) is accompanied by another threat targeting the technology community; it is a group of cyber-attacks and cybercrime targeted since the outbreak or beginning of this epidemic, including many attacks and threats. There are reports of fraud impersonating public authorities and institutions, targeting fraudulent support platforms and personal protective equipment. These cyber-attacks target millions of people working remotely (who used to work from home), which has led to unprecedented fears and cybersecurity challenges. This opportunity enabled cybercriminals to use stream situation features to expand attacks using various methods, including phishing. Cyber-attacks also targeted sensitive infrastructure, for example, healthcare services, phishing, communications (for example, Zoom and Microsoft Teams), and malware. Incidents of fraud or electronic deception to obtain personal data increased, with criminals pretended to be "governments or health authorities." During the COVID-19 pandemic, the malware spread with ransom demands with an evolution selected the target for increased damage and financial gain. Increased number of attacks led to disrupting health infrastructure in some countries to demand a ransom payment. cybercriminals exploit internet networks by various means, and there are primary reasons for the increase in attacker's exploitation of cyberspace during the Covid-19 pandemic due to the availability of factors that facilitate this exploitation, the most important of which are:

- First: people's passion for gaining knowledge about the COVID-19 pandemic.
- Second, working remotely (at home) enables cybercriminals to exploit unprotected computer systems.
- Third: The use of insecure applications during the period of the quarantine, especially the unlicensed applications.

This research explained the reasons for the rise of cyberattacks during the Covid-19 pandemic, and it discovered the most types of cyberattacks that appear during this pandemic. Also, this research identified the most sectors are affected during the Covid-19 epidemic.

2. Background of the Research

In this section, we summarized the most five relevant researches to this research: The research (Eboibi, 2020) studies the most common type of attack that occurred during COVID-19. The study used a quantitative method. The study aimed to achieve the goal of objective in our research: determine the most common type of cyber-attacks carried out during the current period (COVID-19) And according to the findings, phishing attack was a common threat to attack during the COVID-19 pandemic in Nigeria, where the proportion of phishing attacks rose on websites increased by 250% due to the spread of the COVID-19 pandemic. Attackers have used fake websites related to COVID-19, more than 9,000 domains have been registered with Coronavirus, and malicious apps have been used during the COVID-19 period.

The researcher (Columbus, 2021)wrote about ten lessons the world discovered after experiencing Covid-19. Before the pandemic, organizations were making efforts for digital transformation, and this trend had two aspects, the first was successful with large revenues and the second failed as a result of the success of many incidents of hacking the electronic system. Then researcher point of view matters that have emerged in cybersecurity in 2020: The attackers took advantage of the need during the distribution of the Covid-19 vaccine and impersonated names and entities of trust to attack the infrastructure of different parties and individuals as well. During the pandemic period, the health sector was the most interactive, used and the most exploited. The hackers had gained accessed to patients and insurance information-commerce and service providers also took advantage of this. As a result, implementation and delivery procedures were reached and amended, and financial crimes occurred. Social media has been hacked using social engineering, the accounts of influencers and celebrities have been hacked, personal files have been sold and become a hotbed of cybercrime. Cloud systems have been hacked as a result of their misconfiguration, the accounts and passwords of the beneficiaries of the cloud have been hacked, and many companies have been affected, which led to the creation of a cloud configuration platform to evaluate and update their protection, secure smart devices that do not depend on trust, and protect device identities from attacks , human is one of the most important weaknesses as a result of the lack of monitoring, work and evaluation, which resulted in raising awareness and training. As well as updating the organized protocols and operating systems continuously. Therefore, additional factories were established during the pandemic to develop and manage these systems, and it prompted government agencies to publish more stringent controls and procedures.

The study (Khan, Brohi , & Zaman, 2020)identified the top ten cybersecurity threats that occurred during COVID-19. which are DDOS attacks, malicious domains, malicious websites, malware, ransomware, spam emails, malicious social media messaging, business email compromise, mobile apps, and browse apps. Where cybercriminals created many websites that contain spam content, malware, or phishing malware. There are many cases where hackers impersonated legitimate organizations such as the World Health Organization. Attackers launch ransomware that targeted the hospital systems, health organizations, public institutions, education, and education. Because they need to work on their systems, the criminals are sure they can pay the ransom. Researchers determine the sectors that most affected by cyber-attacks during the Covid-19 pandemic, which are healthcare systems, financial services, and government and media outlets. Where healthcare systems are the most targeted during the COVID-19 pandemic, financial industries are most vulnerable to cyber threats like phishing attacks, malware, or ransomware attacks and attackers can launch cyber-attacks on the government and the media to spread misinformation among people. The researchers discussed privacy concerns, where are large companies such as Apple, Google, and Facebook collect their users' information for advertising purposes. Also, some applications require disclosure of the health condition and need some personal information. There are concerns that this data may be used even after the end of this epidemic.

Analysis of article. (Buil-Gil, Miró-Llinares, Moneva, Kemp, & Díaz-Castaño, 2021) Cybercrime and shifts in opportunities during COVID-19. In the UK. where they used the quantitative method, which collected data samples from crimes known by police between May 2019 and May 2020 in UK. The study aimed to achieve the goal of objective in our research: reasons for the increase in cyber-attacks (COVID-19). The article explained opportunities for cyber-dependent and cyber-enabled crimes increased during the (COVID-19) crisis. And according to the findings, cybercrime incidents rose during the COVID-19 epidemic. They were exceptionally high during the two months when the most stringent lockout policies and interventions were in place. As the number of increased associated with online shopping and auctions, social media and email theft is the two most popular cybercrime categories in the UK. The study also showed the victim's rise of cyber-related crimes individual more than organizations in the UK.

The study (Eian , Yong , Li, & Fatima, 2020) discussed the concept of the cyber-attacks. It utilized from a statistics analysis that shows how recent attacks have been increased around thousands of malicious emails during the pandemic. Also, it reported some financial and health organizations that have been attacked such as World Health Organization (WHO), US Centers for Disease Control and Prevention (CDC), US National Institutes of Health (NIH),and World Bank and Wuhan Institute of Virology. Additionally, some recent Cyber-attack types had been discussed such as Denial of Services (DoS) and Distributed Denial of Services (DDoS), Man in the Middle (MitM), phishing, spear phishing, password attack, and malware. Also it utilized from some recent literature reviews to define the most types of cyber-attacks during the pandemic, In addition, it show how malware and phishing has been increased graphically. Some companies such as Google and Microsoft took extra precautions from being hacked by implementing further secure system. Additionally, some reasons that make people became vulnerable to cybersecurity had been discussed such as ignoring updates notifications, security bugs in applications, hidden backdoor, Internet of Things (IOT), resource constrained devices, and shortage of security tools. Finally, a solution that enhances the security level had been proposed which is using Artificial Intelligence model to learn, detect and prevent cyber-attacks.

3. Problem statement

In the COVID-19 pandemic, many cyber-attacks had left their impacts on many organizations or individuals. The research addressed the causes of the escalation of cyber-attacks, which required looking forward to current studies about the different types of cyber-attacks to select the most attack during the COVID-19 pandemic. Health, education, and other sectors had affected by these attacks; from here, the research clarified the sectors that mainly had been affected by these cyberattacks that the criminals carried out during this period. Many cyber-attacks occurred frequently and had specific objectives behind the attack, and the research identified most attacks that happened during the pandemic. These cyber-attacks are becoming more effective and robust due to the continuous development of emerging cybercrime methods. Likewise, cyberspace has become an environment in which severe and costly cybercrime thrives.

4. Objectives of the research

This research aims to achieve the following objectives:

1- To determine the reasons for the increase in cyber-attacks during the current period (COVID-19).
2- To identify which sector has been significantly affected by cyber-attacks during the current period (COVID-19).
3- To determine the most common type of cyber-attacks carried out during the current period (COVID-19).

5. Hypothesis of the research

In this study, we imposed several hypotheses:

H1. There are many reasons that led to increasing of cyberattacks during COVID-19 pandemic.

H2. Cyberattacks target only one sector during COVID-19.

H3. The phishing attack is the most attack that happened during COVID-19.

6. Assumptions of the research

This research will be conducted based on these assumptions. First, most people use digital devices, and they have internet connections in Saudi Arabia. Second, users are of different ages, educations, and intentions. Also, most sectors move toward working at home. Most people use their personal devices at home during COVID-19. And the security level of home devices is less than the companies' devices. Finally, not all sectors are ready to conduct on-line work.

7. Importance of the research

When the world is focused on the global threat represented by the Coronavirus, there is no doubt that cybercriminals worldwide are ready to take advantage of this pandemic to launch "electronic-virus". With the rising number of employees had for working remotely in companies, institutions, and government departments, they are extremely vulnerable to cyberattack. Cybercriminals take advantage of the fear and uncertainty created by the unstable economic and social situation caused by the Covid-19 epidemic. The increasing dependence in the world on the Internet also creates new opportunities for attacks, with the presence of many individuals who do not update their ability defense on the Internet.

This research helped to determine the reasons for the increase in cyber-attacks during the current period (COVID-19). The social distancing measures led to the preventing of international travel, the closing of cafes, markets, schools, and partial and total curfews, which have led to an increase in reliance on information and communication technologies, such as the Zoom platform and other platforms. This research will help develop and improve awareness among individuals and employees to counter cyber-attacks such as phishing attacks and electronic fraud that have increased during the current period (COVID-19).

8. LITERATURE REVIEWS

8.1. The impact of COVID-19 on cybersecurity

The article (Taylor, 2021) deals with presenting the challenges that the field of cybersecurity will face as a result of the measures that were forced to take due to the Corona pandemic as a result of stealing tools that can be used for cyber-attacks, Where the attacks will be more specific to the target parties and more comprehensive. The attacks were depending on cyber espionage. The means of protection and cybersecurity had developed, including - Enhancing the intelligence of the edge. Small size DDoS attacks were increased Readiness of the Zero Trust template to apply in the cybersecurity sky- and also whole world was forced to adopt remote work, so the importance of SASE increased and its inclusion in the security infrastructure of most, if not all, institutions.

8.1.1. Increased in cyber-attacks

The study (Chigada & Madzinga, 2021) discovered that cyberattacks and risks are rising exponentially as the international economy pays close attention to the COVID-19 pandemic. During the pandemic, major businesses, the healthcare industry, and government institutions have also become targets of cyberattacks and threats. Cyberattacks and risks have been shown to intensify exponentially during the COVID-19 pandemic, presenting new obstacles to the international economy, which is already recovering from the noob coronavirus. As a result, the financial and human resources devoted to fighting the noob coronavirus are being overworked, with the likelihood that resources will be redirected to fight cybercrime. Companies and individuals should develop cybersecurity interventions to protect their data and information systems infrastructure. Through grouping and evaluating key information, content analysis. Cybercriminals have taken advantage of the pandemonium caused by the COVID-19 pandemic.

This article discussed (ICCWBO, 2020) Targeted medium and small businesses with high attacks due to poor security that increased over the past year. As small businesses benefit from attackers' access to larger companies, the risks had increased. The methods classified used in the attack on small and medium-sized companies, such as hacking networks that employees were using to work remotely. The most important of which was raising awareness of workers in the companies and increased training for them and provided advice by specialists to protect used by the targeted companies. also required companies to communicate with governmental and international organizations for cybersecurity, worked within their procedures, and participate in their activities

Another recent research (Olofinbiyi & Singh, 2020) defined the role of COVID-19 in increasing the cybercrime exponentially. According to US Intelligence units, it reports 21 fraudulent purchases that led to loss £800,000 and most of these purchases were buying imaginary face masks. Also, according to NFCRC, some criminals pretended to be World Health Organization (WHO) and they provided a fake list of infected people, but they are actually asking money. Additionally, based on US Centers for Disease Control and Prevention (CDC), there was hacking for slowing down the system of U.S Department of Health and Human Services and gaining information about vaccine. South Africa Banking Risk Information Center (SABRIC) reported some social engineering crimes by convincing people to give them their private information.

In research (Dwivedi , et al., 2020)The Covid-19 pandemic has forced organizations to close their doors and send employee's home. Around the world, and technology has been the primary factor in change. Along with the increased cyber threats that had encountered in parallel. The growing demand for remote work has been a major reason for the increase in cyber-attacks, with 47% of individuals falling into phishing while working at home. Cyber attackers see the pandemic as an opportunity to ramp up their criminal activities by exploiting the vulnerability of home workers and capitalizing on people's strong interest in coronavirus-related news (such as fake coronavirus malware sites). Research indicates that 12% of companies and organizations did not take preventive measures against cyber-attacks while working from home.

The article addresses (Wirth, 2020) COVID-19 and What It Means for Cybersecurity. The motives of the attackers in the Corona pandemic are (political & financial). discussed how these attacks impacted the health sector during the Corona pandemic, causing physical and cybersecurity convergence. Since there are so many people handling computers, networks are set up easily. Remote health-care programs and work-from-home opportunities are available. Traditional boundaries and controls no longer exist, which is one of the reasons for the rise in Corona pandemic attacks.

8.1.2. Target the healthcare and public health sector and medium and small companies

The article (Columbus, 2021) dealt with the main goal is to shed light on the great damage caused to small and medium-sized companies as a result of the Corona pandemic. The launch of the "Save our Small and Medium Enterprises" campaign, for more cooperation in facing attacks. The contribution of governments in helping them overcome the economic crisis and face challenges. The targeting of medium and small companies for attacks, which was loud due to poor security and has increased over the past year.

Another recent research (Eian , Yong , Li, & Fatima, 2020) discussed the concept of the cyber-attacks which most attacks follow the Cyber Kill Chain Intrusion model, according to a statistics map that shows, how recent attacks has been increased and reports around 60,000 malicious emails during the pandemic. Many organizations have been affected such as World Health Organization (WHO), US Centers for Disease Control and Prevention (CDC), US National Institutes of Health (NIH), World Bank and Wuhan Institute of Virology. Google Company enhanced its security by providing security and privacy experts, improving scanning and encryption technologies, protecting all data by (Transport Layer Security) TLS and (Hypertext Transfer Protocol Secure) HTTPS, and maintaining up to date with security research community. Also, Microsoft Company enhanced the validation and permission techniques.

The security challenges of cloud platforms

This research in (Mandal & Khan, 2020) aimed to identify the security challenges of cloud platforms that serve many areas due to their sudden use during the epidemic and the impact of many cloud resources. Due to a lack of security services, it can be easy to hack some cloud resources. Also, cyber-attacks will increase in the future. Also, attack insecure networks.

The influence of organizations in supporting work from home during the COVID-19 pandemic, as the organization must use and utilize cloud services and resources without restrictions, and must put in place strict security policies, and prevent attackers from discovering vulnerabilities and breaches Cyber criminals can penetrate the cloud if employees use network services Untrusted provided by local service providers or mobile network without privacy protocol. And without the use of authentication tools. The researcher focused on phishing, which is the most common attack and the number of cloud security breach attacks. Finally, the researchers suggested some precautionary measures for cloud computing services, as cloud services face serious breaches by cyber criminals in the event of an outbreak of COVID-19. Such as authentication, creating periodic backup data and make sure to log out after using the cloud services.

8.1.3. **Challenges of cybercrimes during corona virus pandemic**

Another recent research (Ahmad, 2020) defined challenges of cybercrimes during corona virus pandemic. Companies transformed to complete their work remotely but working at home required awareness and knowledge of cybercriminals. And based on global security reports, the level of security becomes worse than before. Wherefore employees should get educated about privacy and cybersecurity. Cybercrime becomes the greatest threat globally. And based on Cybersecurity Ventures estimations, the cost of damage might double by the end of this year. The attackers, especially phishing attacks, exploit the pandemic's anxiety, and they play on emotions since people are urgent to get news about COVID-19. And the researcher said that if employee act immediately toward security, the damage cost will continue at the recent level but if they did not take a serious step, it might cause heavy loss worldwide. Many types of threats have occurred during the COVID-19 outbreak, such as phishing attacks, ransomware, unsecure remote access, credential theft and data theft. Finally, some security suggestions had been mentioned for home-working employees, such as using multifactor authentication, VPN solution, Policy Updating, communicating with IT manager, and securing personal.

8.2. The reasons of the increased of cybercrimes during COVID-19

The article addresses (Kashif, Javed , & Pandey, 2020) examined whether cyber-crimes have risen during the Corona virus pandemic such as data stealing issues and hacking. In this research an online questionnaire was generated and 400 of individuals out of 1088 responded to the questionnaire. The result of the first question shows that 95% of individuals have used smartphones or other digital devices. The second question shows that 53.10% of individuals are agreed that more data is being provided to websites during corona virus. The other question shows that 46.40% of individuals are agreed that the cybercrime has increased whereas 13.40% of individuals are disagreed, and 40% individuals are unsure about this case. Finally, one of the questions shows that 83.70% of individuals were attacked, or their data had been breached during the current period (COVID- 19). The researches had drawn a conclusion that the cybercrime has been increased during the current period (COVID- 19).

This study (Lallie , et al., 2021). studies investigate the cybersecurity problems that have arisen as a result of the coronavirus, as well as if there is a connection between the COVID-19 and an increase in cyber-attacks. Furthermore, the COVID-19 increased anxiety is increasing the success rate of cyber-attacks. As a result of the COVID-19, almost every country in the world has been placed on lockdown. The move to a new way of working in which workers work from home, mostly using home systems that are protected by their employers, has sparked some interest in the industry. If cybercriminals become more aware of the situation, it will become even easier for them to build false messages or websites that look like legitimate authorities.

This study (Furnell & Shah, 2020) discusses the different aspects of cybersecurity affected by the epidemic. The study suggests that attackers are using COVID-19 as a lure to brand impersonation and thereby deceive employees and customers, increasing remote work requests to increase focus on cybersecurity, due to increased exposure to cyber risks. Cyber attackers see the pandemic as an opportunity to ramp up their criminal activities by exploiting the vulnerability of home workers and capitalizing on people's strong interest in coronavirus-related news. Most professionals have lost their livelihoods due to the numerous restrictions on movement by governments around the world. This has encouraged the growth of cybercriminals, as the unemployed with access to the internet who have lost their jobs from the effects of COVID-19 may find an opportunity to make a living from the pandemic.

The Coronavirus has been the subject of global research studies on cybersecurity problems. As a result of the COVID-19 's heightened anxiety and fear, cyber-attacks are becoming more successful. this study has also presented numerous realistic approaches to reduce the risks of cyber-attacks. Cybersecurity problems during the COVID-19 Contagion were examined and analyzed. there is a connection between a COVID-19 and an increase in cyber-attacks. Highlighted and summarized are prominent cyber-attacks and vulnerabilities. A number of realistic approaches to reducing the threats of cyber-attacks, as well as potential mitigation strategies, are addressed. Cybercriminals and APT organizations have taken advantage of the COVID-19 by attacking vulnerable individuals and networks. Where the most prominent was:

8.2.1. The motives of the attackers in the Corona pandemic are (political & financial)

The article addresses (Wirth, 2020) COVID-19 and What It Means for Cybersecurity. The motives of the attackers in the Corona pandemic are (political & financial). He mentioned the health sector's impact from these attacks in the Corona pandemic caused physical and cybersecurity convergence. Because many people handle devices, quickly deployed networks. Deployed Remote health care services and worked from home. And also, Traditional borders and control no longer exist as before, which lead be the reason for the increase in Corona pandemic attacks.

8.2.2. Teenagers and young adults at home & unemployment

As noted by (Collier, Horgan, Jones, & Shepherd, 2020) as a result of various users (including teenagers and young adults) had restricted to their homes for most of the day, it had a driven force behind online petty crime. Furthermore, concern over work cuts and company closures may motivate some individuals to increase their current cyber-criminal activities as a source of income. Therefore, it increased the attack.

8.2.3. Stringent lockout policies during crisis COVID-19

An analysis of Cybercrime and shifts in opportunities during COVID-19. A preliminary examination in the UK (Buil-Gil, Miró-Llinares, Moneva, Kemp, & Díaz-Castaño, 2021) . they collected data samples from crimes known by police between May 2019 and May 2020 in the UK. The study aimed to address the following research questions; first, Opportunities for cyber-dependent and cyber-enabled crimes have increased during the COVID-19 crisis. Second, the growth of cyber-dependent and cyber-enabled crimes has primarily affected individual victims. According to the findings, cybercrime incidents rose during the COVID-19 epidemic, and they were exceptionally high during the two months when the most stringent lockout policies and interventions were in place. The number of frauds associated with online shopping and auctions, social media, and email theft is the two most popular cybercrime categories in the UK. Also, the individual is the victims rise of cyber-related crimes more than organizations.

8.3. The most sector affected by the pandemic.

This study (Abukari & Bankas, 2020) The Corona pandemic has left its mark on several different sectors. Some sectors are still suffering from the effects of this epidemic, while others are still recovering from it. There are also sectors that have been targeted repeatedly, unlike other sectors. All sectors and research agencies must not ignore the potential risk of cybercrime. It is ready for this attack and is equipped with the tools necessary to defend itself from potentially devastating cyber-attacks. We determine the most sectors that has been affected by the Corona pandemic, based on articles, studies and research.

8.3.1. The impact of the pandemic on the health sector

This study (Pranggono & Arabo, 2021)The coronavirus infection COVID-19 could cause havoc in the disease-care industry. Healthcare services are becoming more vulnerable to cyberattacks. Cyber-attacks on healthcare organizations are becoming increasingly frequent. Since the outbreak of COVID-19 began, international and national regulatory agencies have emphasized the urgent need to protect healthcare systems from cyberattacks. It's worth noting that cyber criminals are constantly targeting health-care vulnerabilities during this period. To steal sensitive information such as COVID-19 vaccine development data, modeling, and experimental treatments. As a result, hospitals must be aware of potential cyber-attacks, as well as safe and prepared to respond. Investing in cybersecurity in healthcare organizations has helped reduce the risk of ransomware attacks, particularly during COVID-19 in the event of a glitch, it could lead to the release of personally identifiable medical information. Anyone would likely die as a result. Organizations must be willing to participate. Remote workers must be able to establish a connection to a VPN to build a stable connection over an insecure Internet infrastructure, and applications should not be permitted without prior consent. This infection has had and will continue to have a major impact on healthcare delivery around the world. In a hurry to develop front-line medical facilities and explore new treatments, healthcare institutions and research agencies must not ignore the potential risk of cybercrime; Spirits and groundbreaking treatments can be at stake.

8.3.2. The impact of the pandemic on the universities and educational institutions sector:

This study (Muthuppalaniappan & Stevenson, 2020) COVID-19, coronavirus infection, has caused havoc with increasing cybersecurity risks in the classroom. Foreign and national regulators have stressed the need for universities to protect themselves from cyber-attacks during COVID-19 since the outbreak began. To steal sensitive information such as COVID-19 vaccine development data, modeling, experimental treatments, and experimental results in this race against time by universities and educational institutions. These universities and institutions must be aware of potential cyber-attacks, and they must also respond to these violations and attacks. Academic institutions are exposed to a host of risks, such as leakage of sensitive research data or confidential patient experience data. This may be particularly risky for academic medical centers working on COVID-19 vaccines or new high-demand therapies. Unfortunately, healthcare institutions and universities often lack the tools to defend themselves from potentially devastating cyber-attacks. The breach of protection affects the cost and the long-term effects. The pandemic had a great impact on institutions and universities that were struggling and competing with other institutions to produce an effective vaccine in light of this phenomenon. Universities, institutions and research agencies must not ignore the potential risk of cybercrime; Pollinators and groundbreaking research could be at stake.

8.4. The most attacks happen during COVID-19

The study (Hakak , Khan, Imran , & Choo, 2020) identifies the various cyber threats that occurred with COVID-19. Where the recent statistics showed that the number of cyberattacks bearing the theme of COVID-19 has increased in the last months. These attacks can be classified based on the intent of cybercriminals. First, disabling services which include DDoS attacks that aim to send multipoint to overloading the capability to the target and block all the users once, and spyware attacks are a type of malware used to obtain confidential information for other systems secretly. Second, financial gains which include ransomware attack in which the attacker places restrictions on users' devices and limits availability until the ransom is paid. And digital fraud research has observed an increase in the number of marketing activities bearing the theme of COVID-19 at fictional prices or the sale of counterfeit and unapproved equipment and products. Third, Information theft and data breaches which include vishing calls and phishing where some employees rely on phone and Internet communications to carry out their business operations, including healthcare guidance. This communication channel may have vulnerability exploitation and phishing, where cybercriminals identify and exploit vulnerabilities in systems and platforms.

The researchers (Khan, Brohi , & Zaman, 2020) in identified the most ten common cybersecurity threat during COVID-19 pandemic which was DDoS attack,mobile apps, ransomware, malware, malicious domains,browsing Apps , spam emails, business email compromise and malicious social media messaging . The researchers explained that there was increase in the phising attacks , ransomware and spam emails. The main target of the hacker was individuals, officials, and government systems during the COVID-19 pandemic.These cyberthreats led to privacy concerns, that may violate users' privacy.

In article (Pandey & Pal, 2020)where the authors determined both the phishing attacks and ransomware are the most attacks that occurred during COVID-19 pandemic. The article suggested that attackers were used COVID-19 as impersonated brand to attractive or lure employees and customers. cybercriminals saw the pandemic as an opportunity to launch their criminal activities by exploited the vulnerabilities of home workers and they took advantage from the peoples who interest with coronavirus-related news. the authors mentioned, many companies had business continuity plans, but the impact of a global pandemic as COVID-19 has not been taken into many business continuities plans. We identified the most the most cyberattack that occur during COVID-19 depend on some of articles, studies and research.

The study by (Ramadan, et al., 2021)the Cybersecurity and Countermeasures at the Time of Pandemic. As the data were collected from multiple sources at different time points in the period of the onset of the Corona pandemic (2019-2020) and they used a descriptive analysis method, describing all types of attacks in the Corona pandemic and describing how attacks increased at the time of the pandemic and citing examples of that. The study results indicated the necessity of using a set of measures to counter electronic attacks, followed by general recommendations for companies, organizations, and users according to defense strategies.

8.4.1. Ransomware

The article (Tepper, 2021) focuses on ransomware in the age of COVID-19. It prevents the user from accessing the operating system and encrypts all data stored on the computer. This cyber-attack begins with the arrival of a message or link from an unknown person requesting that the file be downloaded as an important or personal file. Once the file is downloaded to a computer or smartphone, the data encryption process begins, after which the owner of the device becomes unable to access it. According to SecurityBoulevard.com, there were 145 million ransomware attacks in the United States in the third quarter of 2020, up 139 percent year over year. Ransomware applications are increasingly rising in number and complexity. And Bernard Brode's remarks admit that NetWalker is already one of the most dangerous ransomware threats in 2020.

8.4.2. Social engineering

The article (Wirth, 2020) mentioned the phishing attack, which is form of social engineering, they are taking advantage of global crises and the prevalent, popular, and most discussed topics to spread their messages and malware and exploit the largest possible number of people who are interested in the latest developments in the Coronavirus news, an opportunity that cannot be missed for them. As many sites were monitored, which are impersonated many websites with a name related to the Coronavirus belong to fraudsters who take advantage of it to carry out malicious activities.

The research (Alzahrani, 2020) identified social engineering as the most attack during the COVID-19 pandemic, where cybercriminals took advantage of attempts to entice users to become victims. Cybercriminals try to send many phishing messages to users to open and click on content links or download malicious attachments to steal sensitive data or lock users' devices and force them to pay ransom to get their data back. He mentioned the government and organizations need security awareness and training regarding social engineering attacks for their employees. Awareness of social engineering risks may in electronic publications or attending seminars to raise awareness of social engineering risks, especially during the COVID-19 pandemic. He discusses issues related to Coronavirus and social engineering. First, Coronavirus malicious attachments and malware that appeared during the Covid-19 period. Malicious email attachments are designed in the form of PDF files or Microsoft Word documents. Once users open these files, attackers would begin attacking users' computers. Cybercriminals have also taken advantage of the increase in Coronavirus infections by sending attachments containing malicious links to social media applications such as WhatsApp. Or they claim to be from the health organization or one of the doctors and nurses to send harmful attachments in the form of advice or information about the Coronavirus pandemic. The researcher recommended that users check the attachments of messages and ignore or delete any email containing "Coronavirus" or "COVID-19" in its address. And disable macros in Microsoft Office applications. And update the computer operating system and security software.

The research (Hijji & Alam, 2021) where is inventorying the latest social engineering techniques used in cyberattacks during the Corona pandemic and collect the results from many studies about the impact of cyber-attacks based on social engineering. By impersonating a person, for example, a bank employee or a customer service employee for the company to try to take some sensitive information from intended users. Or by phishing websites that may contain a malicious link to steal the credit card information from the users. The most technique used by social engineers is phishing attack, the new offensive electronic campaign has been launched where the attackers used phishing e-mails talking about the danger of the Coronavirus, in order to deceive the user into clicking on attachments with malicious software and infecting the user's device. The researchers determined the procedures to deal with future attacks.

The article (Eboibi, 2020) where the author focusses in this article on cybercriminals and cybercrimes in Nigeria, the United States of America, and the United Kingdom during COVID-19. In this pandemic has changed the world in many ways and created problems that we must adapt to and develop strategies to solve. The author identified the phishing attack as common attack that detected during the COVID-19 pandemic. According to the author article, he determined percentage of a phishing attacks on websites has increased by 250% due to the epidemic. Where attackers used fake websites related to COVID-19 and more than 9,000 domains have been registered with Coronavirus. Also, many of malicious apps appeared during the COVID-19 period. The author offered several solutions to reduce the risk of attacks, educating individuals about the practices used for the attack and understanding the consequences of being attacked, taking additional precautions while in the Internet world such as installing firewalls, using the protocols that must be applied by websites that contain HTTPS to provide security when visiting Any web sites.

This study (Osborne, 2021) view that due to the epidemic, social engineering exploitation has been a common occurrence of phishing, spam, etc. Social media: It is the most commonly used phishing, persuading and deceiving users through means such as emails or phone calls (23% of cases), Using search engines to collect data (29% of cases) for example, then hacking passwords with techniques like Matego. Socio-technical is the most powerful species, as social culture, social behavior, and artistic methods were combined to increase the effectiveness of attacks (44%). And to stop spread these attacks, modern technologies such as artificial intelligence and big data analytics have been used. The researcher stated targets that the attackers were seeking, the physical target being the dominant one, as well as the harm targets. And the author concluded that phishing was the most used by attackers at 35%, then email at 16%. Finally, the author made a number of cybersecurity recommendations during the COVID-19 pandemic.

8.5. Solutions to counter cybercrime during Covid-19

The study (Pandey & Pal, 2020) examined the impact of the Covid-19 pandemic on the use of digital technologies. The researcher presented several solutions to confront the dusty effects of the digital transformation during the Covid 19 pandemic:

- Design safe technologies to increase online education and healthcare activities.
- The policy of organizing the digital infrastructure necessary to increase digital transformation.
- Design technologies to manage secure online interactions - for education, healthcare, and payments.

This study (Baz , Alhakami, Agrawal, Baz, & Khan, 2021) explained that during the COVID-19 pandemic, cyber-attacks have increased because of the work from home. so the researcher suggested several solutions for companies whose employees work remotely to protect against cyber-attacks. The first will be for beginners, as organizations must educate employees about the methods used and ways to protect them. Second, the use of secure technologies and solutions such as the use of a cloud system can help prevent data leakage and protect against threats. Third, the use of secure remote access technology.

8.5.1. Practices for a secure home business

This study (Dwivedi , et al., 2020) examined the potential preparedness of organizations and their employees for the proliferation of unplanned work from home, along with the increasing cyber threats that have been encountered in parallel, 47% of individuals falling into phishing while working at home. The study suggests several basic practices for a secure home business: Protect email with a strong, separate password. Install the latest software and application updates. Turn on two-factor authentication on your email. Use a password manager. Secure smartphones and tablets with a screen lock. Back up your most important data

8.5.2. Regular planning, preparations, risk management strategies, and staff training

The study (Weil & Murugesan, 2020) discussed IT risks and resilience and cybersecurity responses during COVID-19. during the pandemic, many threats and vulnerabilities occurred such as the ZOOM bombing and COVID-19 phishing attack. The researcher provided solutions to face the challenges: regular planning, preparations, risk management strategies, and staff training are required to face future problems.

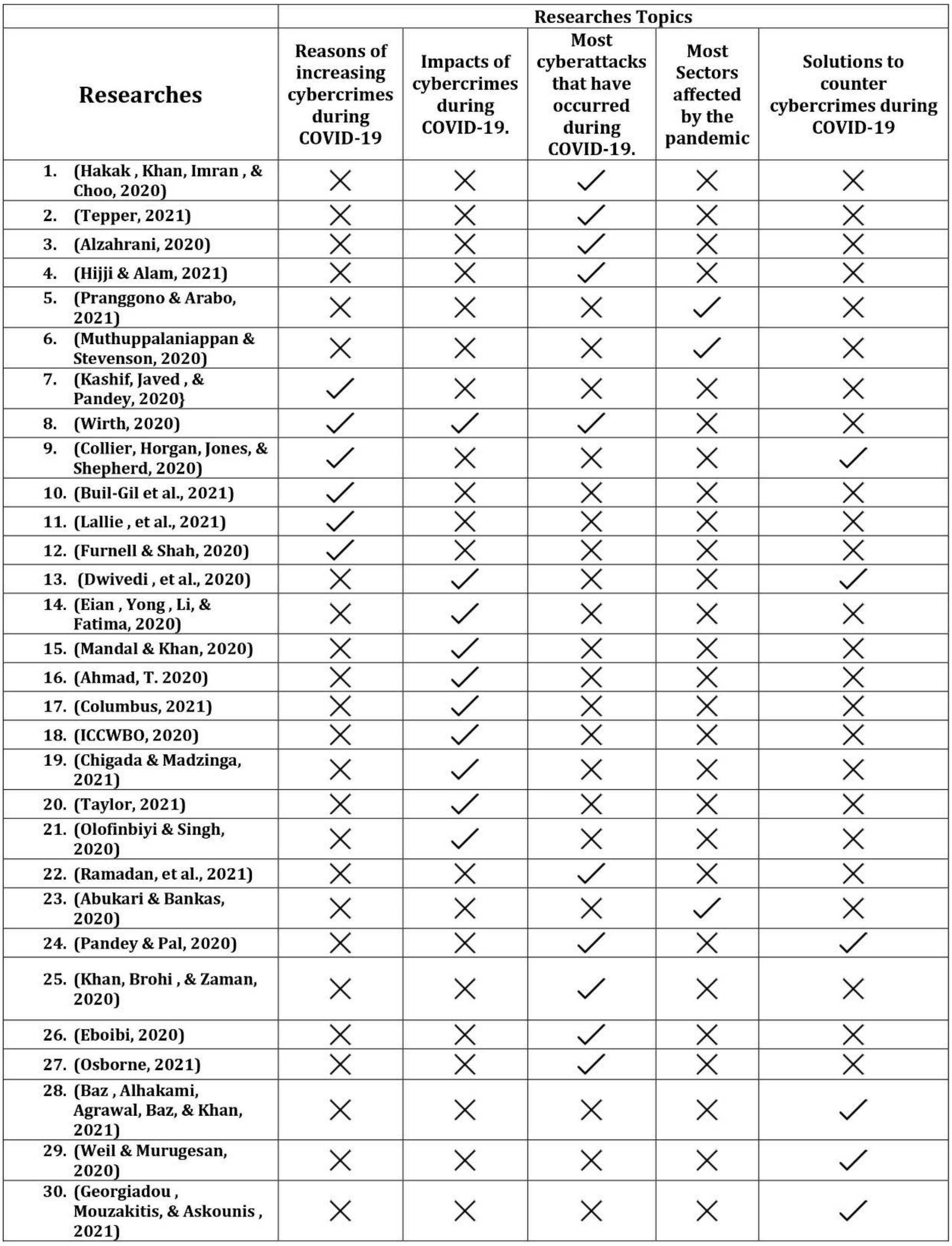
8.5.3. Create the police of Cybercrime:

This study (Collier, Horgan, Jones, & Shepherd, 2020) of Issue the implications of the COVID-19 pandemic for Cybercrime policing in Scotland. The authors are recommended to create the police of Cybercrime. Where is necessary to take the lead in preventing further increases in "volume" cybercrime by using their particular capabilities to provide crime reduction at the local level, including communicating with potential victims and criminals.

8.5.4. Training programs

Researchers conducted (Georgiadou , Mouzakitis, & Askounis , 2021)and based on a survey the result. they Information security is part of concurrent organizations that offer cybersecurity technological solutions such as anti-virus software, intrusion detection systems, security operations centers, etc. Individuals are more aware of security issues and countermeasures than they were in the past, which proves a security culture in the field of information technology. But training is required to increase awareness. Companies are becoming more resilient nowadays due to various technological solutions and availability to adapt to the Corona pandemic. Finally, this survey results show the increase in security culture over time and the changes and training that companies provide to individuals. Information security and culture need to develop and amend policies, procedures, measures, and solutions applicable to the new reality. Staff awareness, familiarity, and experience with security issues should be encouraged and refined through continuous training programs.

Table 1 : summarized literature reviews



	Researches Topics				
Researches	**Reasons of increasing cybercrimes during COVID-19**	**Impacts of cybercrimes during COVID-19.**	**Most cyberattacks that have occurred during COVID-19.**	**Most Sectors affected by the pandemic**	**Solutions to counter cybercrimes during COVID-19**
1. (Hakak , Khan, Imran , & Choo, 2020)	✗	✗	✓	✗	✗
2. (Tepper, 2021)	✗	✗	✓	✗	✗
3. (Alzahrani, 2020)	✗	✗	✓	✗	✗
4. (Hijji & Alam, 2021)	✗	✗	✓	✗	✗
5. (Pranggono & Arabo, 2021)	✗	✗	✗	✓	✗
6. (Muthuppalaniappan & Stevenson, 2020)	✗	✗	✗	✓	✗
7. (Kashif, Javed , & Pandey, 2020}	✓	✗	✗	✗	✗
8. (Wirth, 2020)	✓	✓	✓	✗	✗
9. (Collier, Horgan, Jones, & Shepherd, 2020)	✓	✗	✗	✗	✓
10. (Buil-Gil et al., 2021)	✓	✗	✗	✗	✗
11. (Lallie , et al., 2021)	✓	✗	✗	✗	✗
12. (Furnell & Shah, 2020)	✓	✗	✗	✗	✗
13. (Dwivedi , et al., 2020)	✗	✓	✗	✗	✓
14. (Eian , Yong , Li, & Fatima, 2020)	✗	✓	✗	✗	✗
15. (Mandal & Khan, 2020)	✗	✓	✗	✗	✗
16. (Ahmad, T. 2020)	✗	✓	✗	✗	✗
17. (Columbus, 2021)	✗	✓	✗	✗	✗
18. (ICCWBO, 2020)	✗	✓	✗	✗	✗
19. (Chigada & Madzinga, 2021)	✗	✓	✗	✗	✗
20. (Taylor, 2021)	✗	✓	✗	✗	✗
21. (Olofinbiyi & Singh, 2020)	✗	✓	✗	✗	✗
22. (Ramadan, et al., 2021)	✗	✗	✓	✗	✗
23. (Abukari & Bankas, 2020)	✗	✗	✗	✓	✗
24. (Pandey & Pal, 2020)	✗	✗	✓	✗	✓
25. (Khan, Brohi , & Zaman, 2020)	✗	✗	✓	✗	✗
26. (Eboibi, 2020)	✗	✗	✓	✗	✗
27. (Osborne, 2021)	✗	✗	✓	✗	✗
28. (Baz , Alhakami, Agrawal, Baz, & Khan, 2021)	✗	✗	✗	✗	✓
29. (Weil & Murugesan, 2020)	✗	✗	✗	✗	✓
30. (Georgiadou , Mouzakitis, & Askounis , 2021)	✗	✗	✗	✗	✓

9. The methods of research

This section provides an outline of the research methodology used to answer the research questions. In this research we followed the mix-method design.

To achieve the first objective, we used the qualitative method to determine the causes of the increase of attacks during the COVID-19 pandemic then interpret them, based on studies, articles, and trusted websites.

To achieve the second objective, we used both qualitative and quantitative methods to identify the sectors that had been significantly affected by cyber-attacks and interpret the reasons during the COVID-19 pandemic, based on statistical data and trusted websites. To achieve the third objective, we will use quantitative methods to determine the most common type of cyber-attacks carried out during COVID-19, based on statistical data news, articles, and trusted websites.

10. Results and discussions

This section provides the results that have been obtained through conducting investigation of mixed qualitative and quantitative methods to answer the research questions and support the research hypotheses. The first result clarifies the reasons of increasing of attacks during the COVID-19 pandemic. The second result, identity the sectors that have been significantly affected by cyberattacks during the pandemic. The third result, define the most cyberattacks carried out during the pandemic.

10.1. Reasons of increasing of cyberattacks during the COVID-19 pandemic

- With unemployment rising, more people are sitting at home online, and some of these people are likely to resort to cybercrime to make ends meet (Lallie , et al., 2021).

- The study's analysis of events such as advertisements and news stories showed what appears to be a shaky relationship between the advertisement and the subsequent cyber-attack campaign, which uses the incident as a hook to maximize the chances of success. Due to the rise in cyber-attacks and cybercrime, there could be repercussions for police action in law enforcement. Global must ensure it has the resources to fight cybercrime(Lallie , et al., 2021).

- Securing smart devices that use zero trust and protecting device identities from attacks (Columbus, 2021)

- Cloud systems were hacked as a result of their misconfiguration, accounts and passwords of the beneficiaries of the cloud. (Columbus, 2021)

- Many companies were hacked and affected, which led to the creation of a cloud configuration platform to assess and update their protection. The human factor was one of the most important weaknesses , due to the failure to monitor, work and evaluate (Columbus, 2021)

- Remote workers choose to connect to their organization's computing systems, namely the virtual private network. Protecting VPNs depends on the encryption used. Desktop sharing is a method for remote access to your computer. Desktop sharing is a remote access method that enables organizations to provide ready access to users for real-time file sharing, file sharing, presentation sharing, or application sharing. Authentication threats are related to desktop sharing. Desktop sharing includes authentication threats, raising questions about enterprise protection (Abukari & Bankas, 2020)

- The study revealed a phenomenal growth in cyber-attacks and threats. The analysis presented in this paper also highlights the common method of numerous cyber-attacks during this period. Most cyber-attacks start with a phishing campaign that instructs victims to download a file or visit a URL. As a result of this research, governments, media, and other organizations should be aware that advertising and spreading news are likely to contribute to cyberattack campaigns that capitalize on these events. Events must be accompanied by a note or disclaimer describing how the ad information is transmitted. (Lallie , et al., 2021)

- E-commerce facilitated the means of purchase and authentication to run its business that flourished during this period, as well as facilitated ways for attackers to exploit it with social engineering and the result of penetration and financial crimes were the victims of individuals to a greater extent. (Columbus, 2021).

- The attacks targeted service providers, and customer data were accessed and targeted as well. (Columbus, 2021)

- Social media was compromised by using social engineering, as it penetrated the accounts of influencers and celebrities, and profiles were sold and became a place for cybercrime in a large way (Columbus, 2021)

- Academic institutions are also exposed to a host of risks, such as leakage of sensitive research data or confidential patient experience data. This may be particularly risky for academic medical centers working on COVID-19 vaccines or new high-demand therapies. Unfortunately, healthcare institutions and universities often lack the tools to defend themselves from potentially devastating cyber-attacks. The breach of protection affects the cost and the long-term effects. (Muthuppalaniappan & Stevenson, 2020)

- The attackers took advantage of a need during the distribution of the Covid-19 vaccine and impersonated names and entities of confidence to attack the infrastructure of different parties and attack individuals as well (Columbus, 2021)

Scammers are trying to capitalize on people's vulnerability during the coronavirus epidemic by sending malicious emails, news, and websites with the intent of stealing money or personal information, as well as increasing group anxiety. Cybercriminals depend on people being distracted, worried, or inspired for the purpose to understand more about coronaviruses, and thereby less likely to find mistakes or anomalies that they would normally notice.

- The transition to operate from home as an outcome of the Corona pandemic, including the exacerbation of cyber piracy operations as an outcome of hackers exploiting employees' remote access to their organizations' electronic networks. Attackers have a "greater ability to infiltrate by individuals 'devices for the purpose to gain access to corporations' networks" as they work from home. Often on the same networks are huge organizations. (Purwanto , et al., 2020)

- The company, its devices, and any policies related to it: The worth of a good password, as well as vigilance and double-checking email sources, email trails, and account payment details. The dangers of using public WiFi, and how to stay away from them. The types of applications that can and cannot be accessed from a remote location, the procedure for contacting IT help from a remote location, also the steps that must be taken if anything goes wrong or malicious content is suspected. (Meyer, Prescott, & Sheng, 2021).

10.1.1. Fake websites and the dissemination of false information

Scammers have produced and create a fake-news-pages that often feature attractive stories, often known as "click-bait." They're a convenient target when people look up information about the virus on the internet. These phony websites are often littered with malicious links. If you find anything interesting on the internet, please double-check the website's web address before clicking any article links. (Ahinkorah , Ameyaw , Hagan Jr, Seidu , & Schack, 2020).

10.1.2. Malware tactics and phishing emails

Hackers have set up phishing campaigns using coronavirus-based domain names all over the world. Phishing emails pose as coming from authoritative sources and give advice via attachments or links that can install malware, steal personal information, or attempt to capture login and password credentials. (Lallie , et al., 2021)

10.2. Most affected sectors by cyberattacks during COVID-19 pandemic

All sectors have been affected by the COVID-19 pandemic as 80% of companies restructured their cyberinfrastructure due to the COVID-19 pandemic. As the National Cybersecurity Authority report, in the fourth quarter of 2020 five sectors were affected during Covid-19: the public sector, health sector, education sector, the technology sector, and the Trade sector. (National Cybersecurity Authority, 2020)

10.2.1. Public sector

The public sector is usually comprised state-owned or state-affiliated companies and organizations, public sector not aim to make a profit. As deals with a wide range of our sensitive information (Regzen, 2020), what make the hacker to focus on public sector to attacked, for example Microsoft announced on March 2 that its Exchange Server mail and calendar applications for enterprise and government data centers had vulnerabilities. The flaws date back ten years, and Chinese hackers have been exploiting them since at least January 2021 (Novet, 2021).According to the National Cybersecurity Authority Q4 report on 2020, the public sector ranked first in cyber threats by 19%, when was 14% in Q3 report on 2020. (National Cybersecurity Authority, 2020)

10.2.2. Health sector

The health sector consists of organizations that provide medical services, manufacture medical equipment or drugs, offer medical insurance, or otherwise help patients get healthcare. (STAFF, 2020). In the last 12 months, more records had compromised than in the past 15 years combined. Most significant share according to the Compatriotic report 92 ransomware attacks targeted healthcare institutions, affecting 600 clinics, hospitals, and organizations. Furthermore, these ransomware attacks affected over 18 million health records, a 470 percent rise from 2019. In general, the year 2020 saw the most significant number of ransomware attacks on healthcare providers in the previous five years. The reason is the increase in the value of health records on the Dark Web compared to other records such as Credit card numbers and others. The explanation for this market disparity is perceived value. It can readily delete a credit card number. But Medical reports include a wealth of irreversible details, including a patient's medical and mental health background, demographics, health insurance, ID, and contact information. If the records had hacked, cybercriminals often turn to members of a dark web crime network with backgrounds in drug dealing and money laundering who are willing to purchase medical records to fund their criminal operations. Such as unlawfully buying prescription drugs, filing false medical statements, or simply stealing the patient's name to open credit cards and fraudulent loans. According to IBM Security's 2019 data breach cost report, healthcare companies had the highest data breach costs, which are more than 60% higher than the cross-sectors average (fiercehealthcare., 2019). According to the National Cybersecurity Authority Q4 report on 2020, the health sector ranked second in cyber threats by 14%, when was 16% in Q3 report on 2020. (National Cybersecurity Authority, 2020)

10.2.3. Education sector

The education sector is a series of institutions (ministries of education, local educational authorities, teacher training institutions, colleges, universities, and so on) whose primary aim is to educate children and young people in educational settings. (Wikipedia, n.d.). The COVID-19 pandemic has arguably had the greatest impact on the education sector, with classrooms, colleges, and universities all over the world being forced to close their doors and offer classes remotely. To tackle the spread of COVID-19 disease, many companies have allowed their workers to work from home (Nabe, 2020). Remote meetings and webinars are conducted using online networking channels such as Zoom, Microsoft Teams, and Teams for Education, Slack, Cisco WebEx, and others. New domain registrations are expected to rise in 2020, with names like "Zoom," one of the most common video communication channels in use around the world. More than 1,700 new domains have been registered, with 25% of them occurring in the March 2020. 4% of the domains were found to have questionable assets. (checkpoint, 2021). In addition, the attackers took advantage of the educational institutions' lack of awareness of the technology, as students of all ages use it without proper training. And according to the National Cybersecurity Authority Q4 report on 2020, the education sector ranked third in cyber threats by 9%, when in Q3 report on 2020 was ranked first 18%. (National Cybersecurity Authority, 2020)

10.2.4. Technology sector

Technology sector comprises stocks that are involved in the study, production, or distribution of technology-based products and services. This industry involves companies that produce electronics or develop software, computers, or IT-related products and services. (cdnetworks, 2020) . Some tech companies, such as computing and cloud storage service providers, security software developers, or file-sharing solution providers, can store large amounts of sensitive customer data, which made it a target for cyber-attacks (Moore, 2020) .And one of the most notable examples for the technology sector is the assault on US-based tech vendor SolarWinds in spring 2020. Russia exploited SolarWinds' compromised program to penetrate at least 18,000 government and private networks. User IDs, passwords, financial documents, and source code from these networks can now be assumed to be in the possession of Russian intelligence officers. Wherefore the percentage of attacks on the technology sector is Increased 9%, according to the National Cybersecurity Authority in Q4 report on 2020, while was 8% in Q3 report on 2020. (National Cybersecurity Authority, 2020)

10.2.5. Trade sector

The purchase and sale of products and services, with compensation charged by a buyer to a seller, or the exchanging of goods or services between parties, trade may take place between producers and customers (HAYES, 2021)almost companies in COVID-19 moved to online in order to stay afloat. But Cybercriminals jumped on the opportunity created by this move to fraud and phishing. INTERPOL report shows the most rate of cyberattacks during COVID-19 was phishing and fraud, Where the percentage was 59%. (INTERPOL, 2020) . As where the percentage of attacks on the Trade sector was Increased 7%, according to the National Cybersecurity Authority in Q4 report on 2020. (National Cybersecurity Authority, 2020)

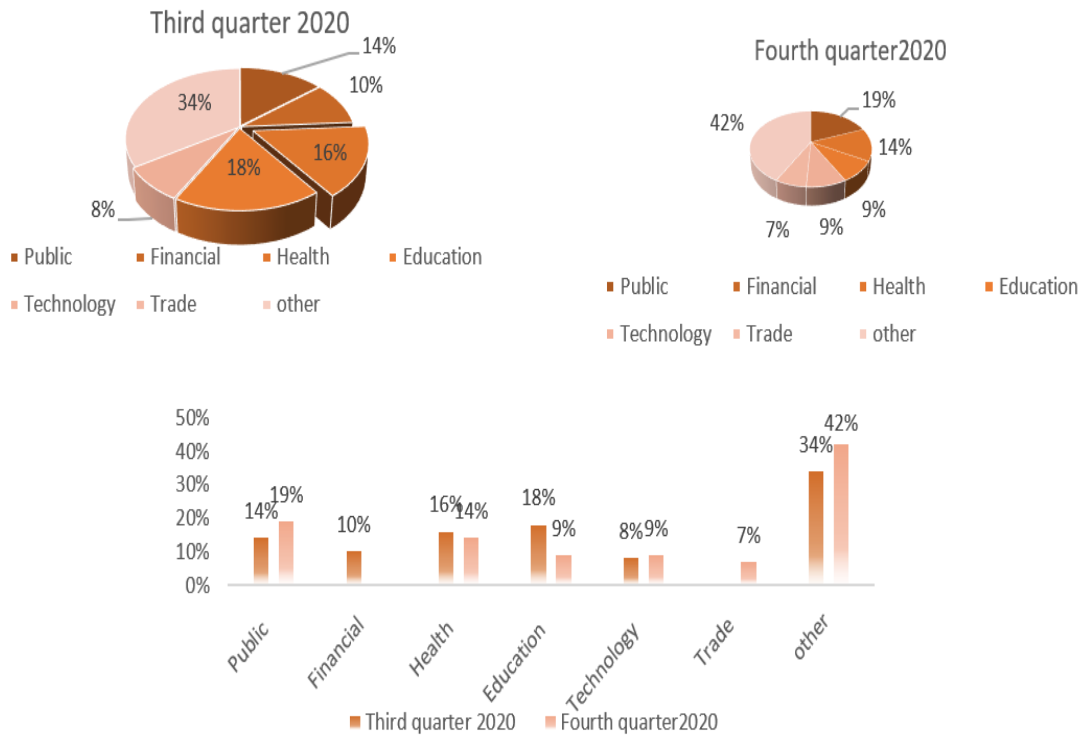


Figure 1: Most affected sectors by cyberattacks during COVID-19 pandemic in Q3 & Q4 of 2020 (National Cybersecurity Authority, 2020)

10.3. Most cyberattacks carried out during COVID-19 pandemic

10.3.1. Most cyberattacks carried out during COVID-19 pandemic in first Quarter of 2020

The most type of cyberattacks occurred in the first quarter of 2020 is Phishing, and cyber criminals take the advantage of anxiety of people and they enhanced social engineering attacks such as providing fake medicine news, and they provide malicious emails about COVID-19, According to (INTERPOL) The international police organization of cybercrimes of 194 member countries, it conducted a survey based on data from the member countries in the first quarter of 2020. And 48 of countries responded to the survey, 42% of them EUROPE, 12% AMERICAS, 17% AFRICA, 10% MENA, and 19% ASP, also 4 privet partners shared their records to conduct this report. The result shows that 14% of cybercrimes is Fake news, 22% malicious domains, 36% Malware/ Ransomware, 59% Phishing/Scam/Fraud as shown in figure2. Kaspersky also as a partner to INTERPOL mentioned to the increasing of phishing websites about COVID -19 that solicit people to provide their private information to these websites. There are different techniques of phishing was appear such as, fake healthcare emails, government commands, and medicine offers. (INTERPOL, 2020)

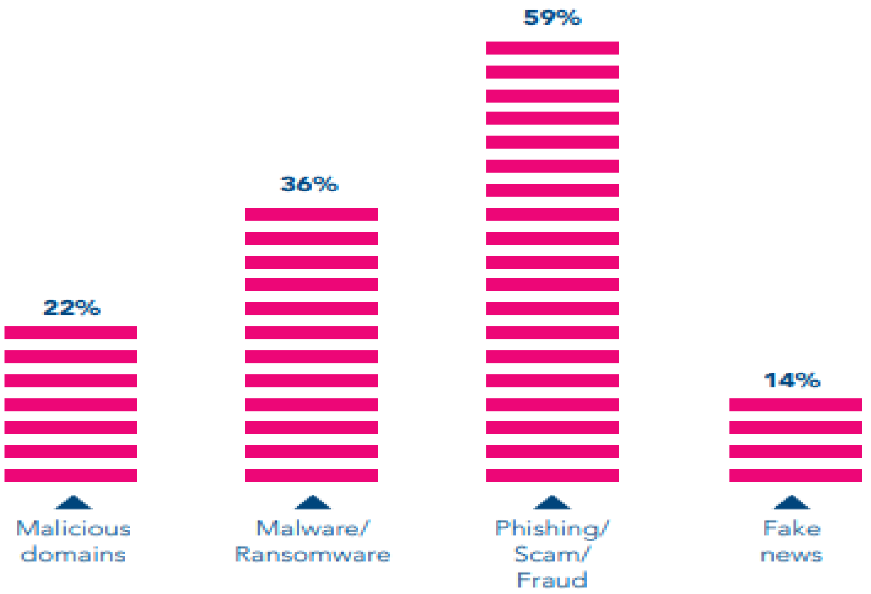
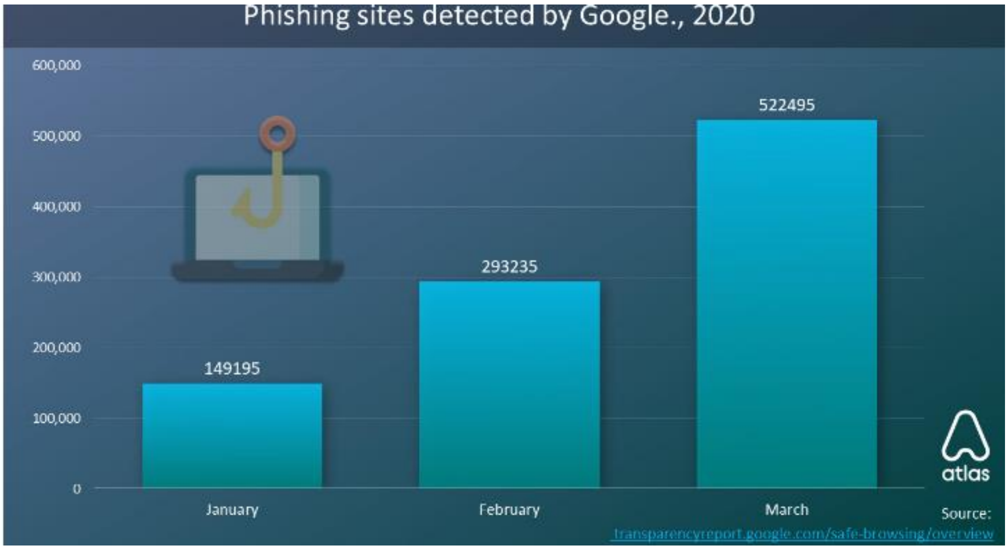


Figure 2: Cyber threats during COVID-19 based on INTERPOL countries Source (INTERPOL, 2020)

Based on Google report, it detected around 149,000 phishing websites in January, and in February the number was increased to 293,235 phishing websites, also in March it reached to 522,495 phishing websites as shown in figure3. (Cohen, 2021)


Phishing sites detected by Google., 2020

Source: transparencyreport.google.com/safe-browsing/overview

Figure 3: Phishing threats detected by Google during COVID-19 (Source Google)

According to UK finance sector report to Information Commissioner’s Office (ICO), that shows the effect of COVID-19 on cybercrimes, as the figure below shows that phishing attack is the most cyberattack in the first half of 2020, and it has been increased compared with the first half of 2019 (from January to March), which was 37 phishing attacks in 2019 and it increased to 63 in 2020 as shown in figure 3. Yoav Keren, chief executive of Israeli cyber–security company said that it was an enormous digital transformation in this year. Since companies enforced into huge changes that he thought to see them in 20 years. And the company assigns specialists to combat the phishing attack based the ICO document (Telling & Almeida, 2020)

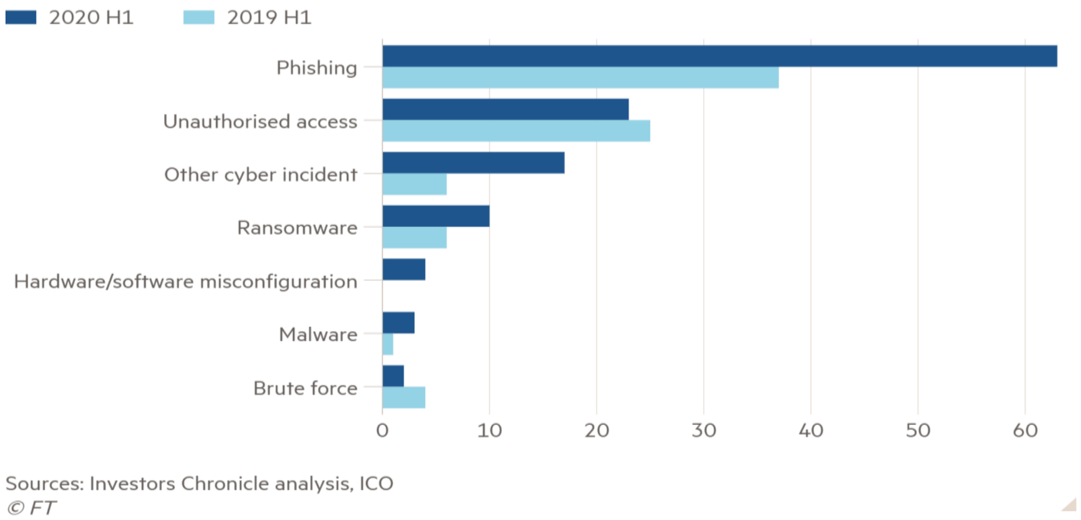
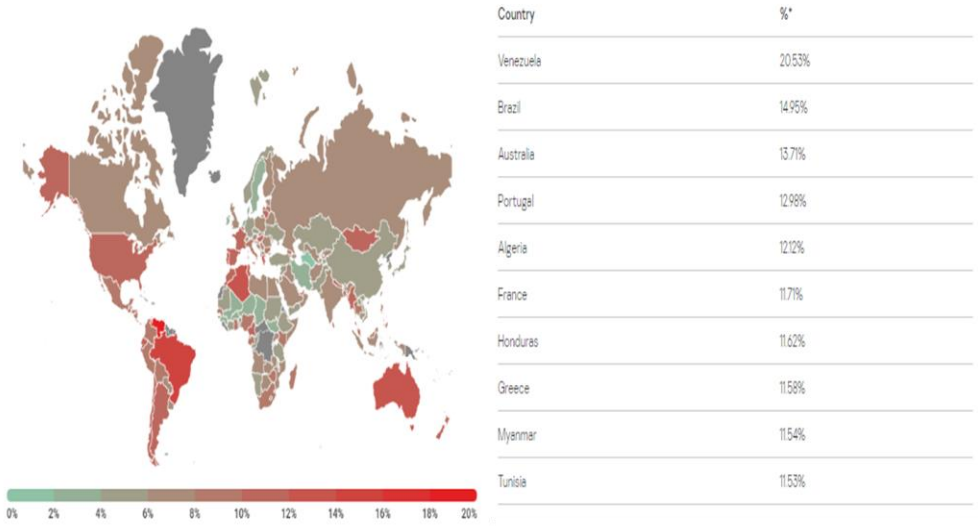


Figure 4: Cyber threats on financial companies during COVID-19 (Source: Investors Chronicle analysis, ICO)

Kaspersky reports that in the first quarter of 2020, The Anti-phishing system stopped 119,115,577 phishing attacks. And the largest countries were infected is Venezuela with the percent of (20.53%), followed by Brazil (14.95%), followed by Australia (13.71%) in figure 5. (securelist, 2020)



Country	%*
Venezuela	20.53%
Brazil	14.95%
Australia	13.71%
Portugal	12.98%
Algeria	12.12%
France	11.71%
Honduras	11.62%
Greece	11.58%
Myanmar	11.54%
Tunisia	11.53%

Figure 5: countries affected by phishing attacks during COVID-19 in Q1 2020 (Source: Kaspersky)

According to a report from Checkpoint Cybersecurity Company in the first quarter of 2020, shows that Apple was the most brand that has been imitated for phishing attack followed by Netflix, then Yahoo, and WhatsApp. Attackers exploit the fame of the Apple Company to perform phishing attacks via emails and applications. Also most people watching streaming contents such as movies, so attackers take the advantage to perform phishing attack imitating Netflix as figure 6 shows. (Mehta, 2020)

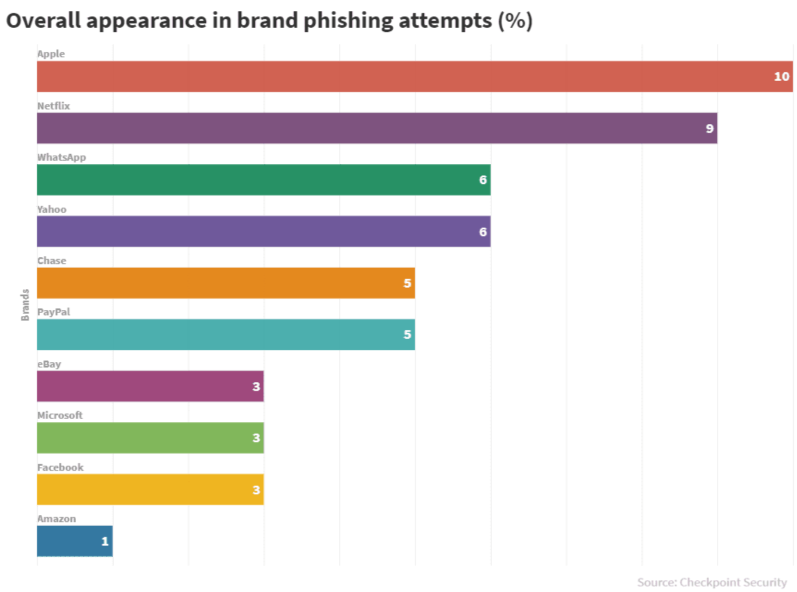


Figure 6: Top phishing brands during COVID-19 in Q1 2020 (Source: Checkpoint security)

10.3.2. Most cyberattacks carried out during COVID-19 pandemic in second quarter of 2020

Several reports for security companies showed in the first half of 2020 an increase in phishing attacks. Among these companies, Trend Micro in Tokyo reported "93.5% of the email threats that discovered contain a malicious file attachment and a malicious link. Also, they mentioned the actors behind the fraud attempts are pursuing more creative practices than ever before, especially in choosing domain names and addresses for the phishing sites they launch. Also, business email compromise (BEC) is a type of payment fraud that involves hacking and forging the original business email or creating an account similar to a domain name for the purpose of illegally transferring funds. Where Trend Micro notes, that the volume of business email frauds have been increased in recent months as the Corona pandemic spreads. Where the fraudster can forge the email account of any executive employee (CEO, CFO, or others), and send a request to transfer funds via a forged email to the accounts department staff. (Schwartz, 2020)

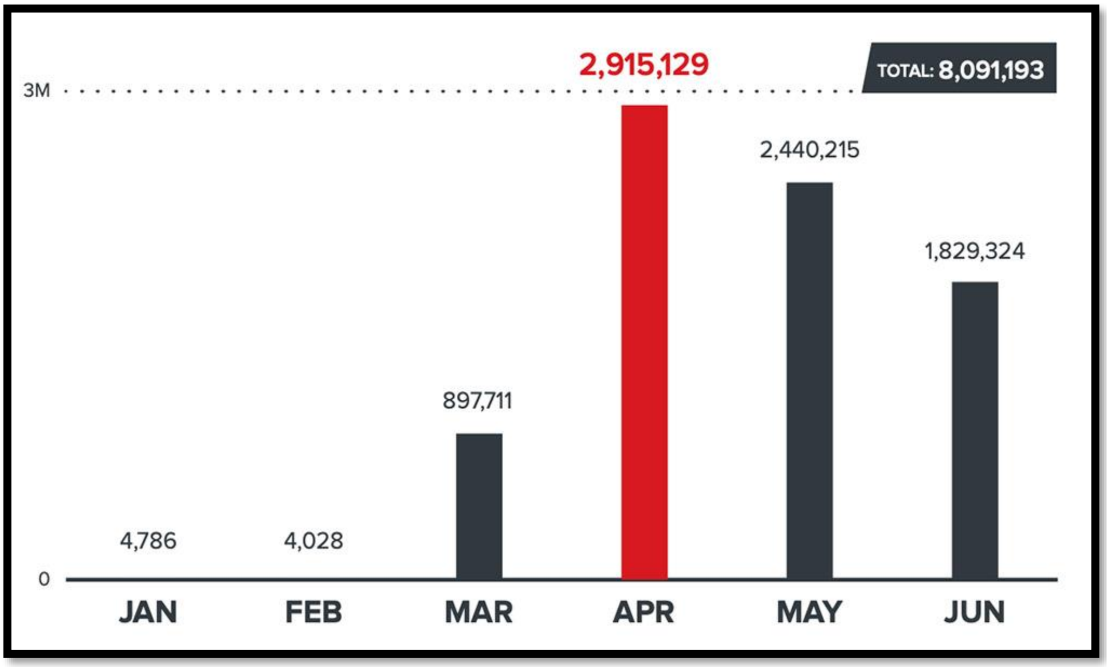


Figure 7: Email Threats Detected Related to COVID-19 in the First Half of 2020 (Source: Trend Micro)

As Trend Micro revealed in its statistics that social engineering attacks, including phishing, increased during the month of April in 2020 with the onset of the Corona pandemic (Schwartz, 2020).

Trend Micro's report revealed 1.2 million email messages containing malware could have appeared in users' inboxes. They intercepted more than 6.9 million phishing messages in 2020, a 19% increase over the previous year. The number of credential phishing threats increased 41% during this period. They also detected nearly 5.5 million attempts to steal user credentials. This was an increase of 14% from 2019. (Micro, 2021)

Singapore-based Group-IB revealed that the Computer Emergency Response Team, CERT-GIB, analyzed hundreds of phishing messages related to the Coronavirus between February 13 and April 1, 2020, and that 65% of the malicious emails contained spyware attached or containing links. For downloading spyware or stealing information, 31% created background towers and 4% ransomware. (Group-IB’s, 2020)

An analytical study conducted by "Kaspersky" reported phishing attacks where the company's security experts have found several new scams that include rejection emails from HR and disguised attacks in the form of order delivery notices. About 2,578,501 phishing attacks were detected in Egypt, Saudi Arabia, Qatar, United Arab Emirates, Bahrain, Oman, and Kuwait. The results were documented in a report on "Spam and Phishing in the Second Quarter of 2020. Whereas the statistics indicated that users in Saudi Arabia are most affected by this type of threat. It detected 973,061 phishing attacks during the three-month second quarter. It was followed by the United Arab Emirates (617,347), then Egypt (492,532), then Oman (193,379), then Qatar (128,356), then Kuwait (106,245), and finally Bahrain (67,581). (Desk E. N., 2020).

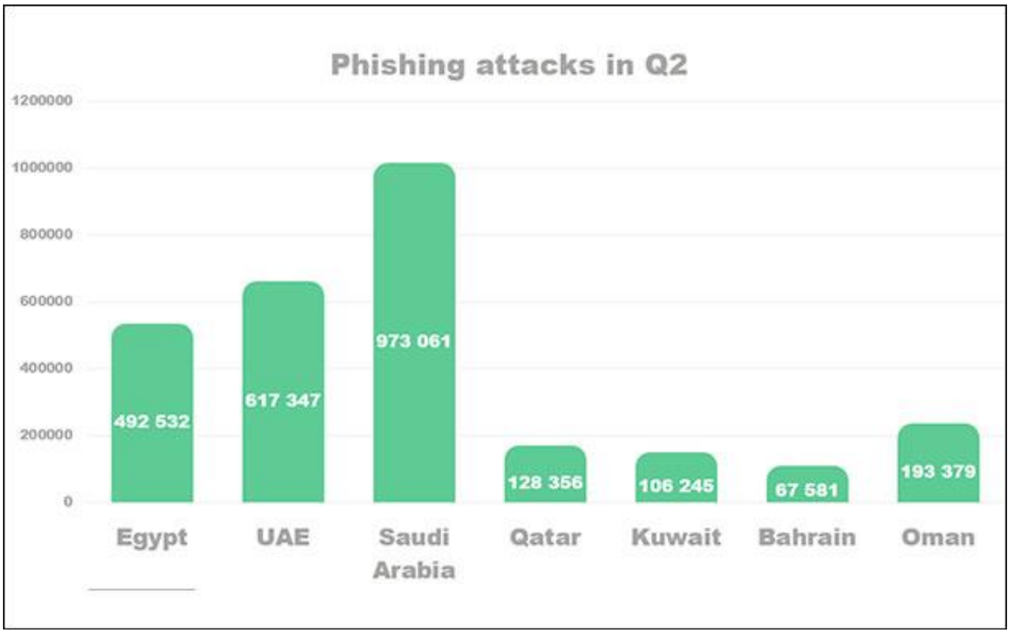
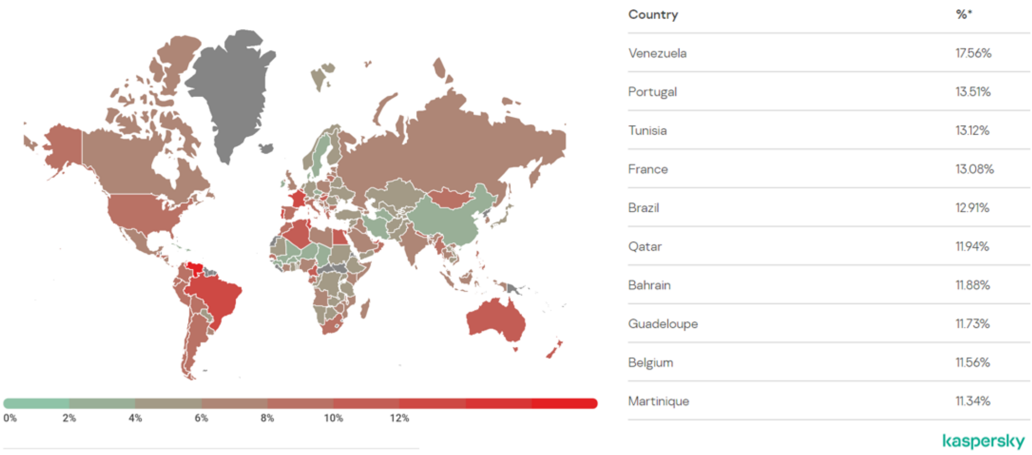


Figure 8: Kaspersky reports phishing attacks in Q2 2020 (Source: Kaspersky)

According to Kaspersky's statistics in the second quarter of 2020, Venezuela was the country most affected in the world by phishing attacks (17.56%). It is followed by Portugal (13.51%), followed by Tunisia (13.12%). Kaspersky's analysis of phishing attacks in the second quarter of 2020 also reported that fraudsters have carried out more targeted attacks, most of which focus on small businesses. To attract attention, fraudsters have rigged emails and websites of well-known entities so that potential victims can purchase their products or services and thus trust, while often not even bothering to make these sites look truly real. (Kulikova T. , 2021)

The bank phishing attacks in the second quarter were often triggered by emails offering various benefits and rewards to credit institution customers as a result of the pandemic. The emails obtained by users included a file with links or instructions to obtain more details about these benefits, which enabled fraudsters, depending on their plans, to access computers, personal data, or users' authentication data that would entitle them to access various services. (Kulikova T. , 2020)



Country	%*
Venezuela	17.56%
Portugal	13.51%
Tunisia	13.12%
France	13.08%
Brazil	12.91%
Qatar	11.94%
Bahrain	11.88%
Guadeloupe	11.73%
Belgium	11.56%
Martinique	11.34%

Figure 9: Geography of phishing attacks during Q2 2020 (Source: Kaspersky)

10.3.3. Most cyberattacks carried out during COVID-19 pandemic in third Quarter of 2020

In the third quarter of 2020, Microsoft was the most targeted by cybercriminals, rising from 5th place 7% in the second quarter of 2020 to 1st place 19% in phishing attempts. According to the blog post, hackers used various methods to carry out the attacks, including attempts to log in with brute force to steal login credentials, as well as phishing attacks where the hackers pretended to be employees of the World Health Organization. (Office Watch, 2020)
According to Kaspersky's report in the third quarter of 2020, Mongolia, the country, was affected by phishing attacks (15.54%), followed by Israel (15.24%), and finally France (12.57%). (Kulikova T. , 2020)

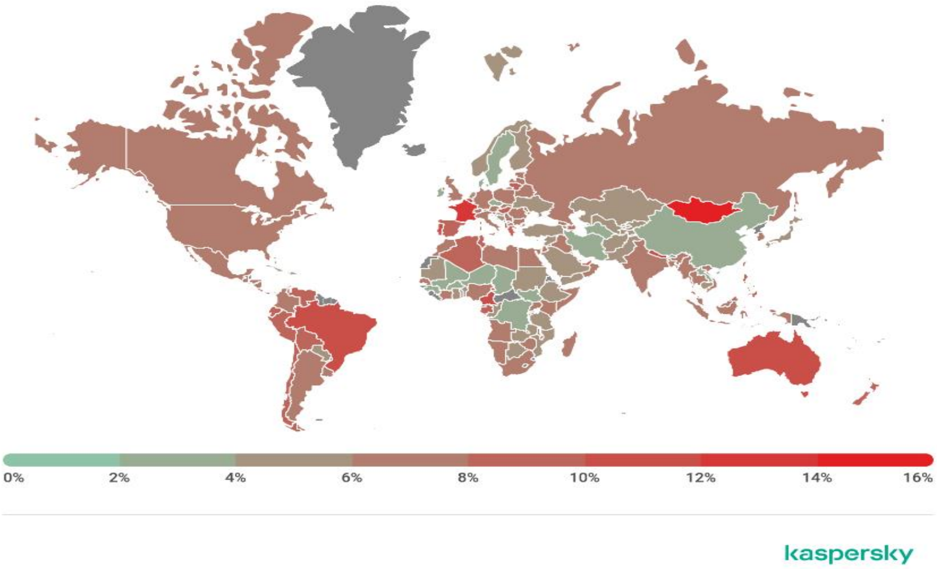


Figure 10: Geography of phishing attacks in Q3 during 2020(Source: Kaspersky)

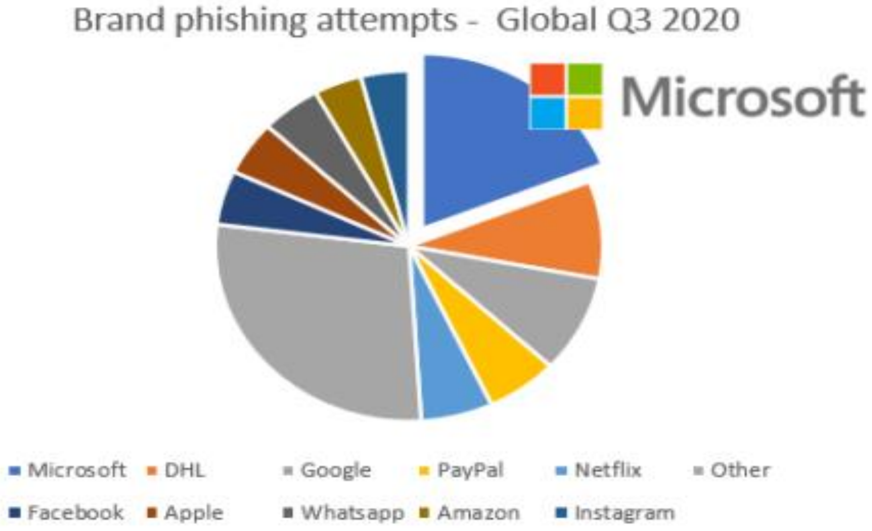


Figure 11: Microsoft the most company affected by phishing attack during Q3 2020. (Source: Checkpoint)

Security researchers are also informed of a phishing attack posing as an automated message from Microsoft "Teams" aimed at notifying the user of a missed conversation and asking them to click on a link for details. In fact, this message, which is trying to target about 50,000 Office 365 users, is a phishing attack attempting to theft login credentials to Office 365 accounts. Teams is a popular collaboration tool from Microsoft, and it has grown particularly popular during the emerging coronavirus pandemic, this made it an attractive for attackers and hackers. And since Microsoft Teams is a message service, receivers of the notification may be more willing to click on it so that they could quickly reply to any message's notification. Especially since the phishing email performs the phrase "There is new activity in Teams", making it appear as an automatic notification from Microsoft Teams. (Fein, 2020)

According to Abnormal Security researchers, there are three links that will appear as “Microsoft Teams”, “(Contact) Send a Message in an Instant Messaging Program” and “Reply in Teams”. Hence, if you click on any of these links may be led to a fake-website that impersonate the Microsoft login webpage, where this phishing or fake-website requests the receiver to enter email and password. Note that the phishing landing page looks convincingly very formal like the Microsoft login page with the beginning of the URL holding “microsftteams”. If recipients are persuaded to enter Microsoft credentials on the page, they inadvertently hand it over to attackers, who can then use them to perform a host of malicious goals that may include account hijacking and private data theft (Security, 2020).

10.3.4. Most cyberattacks carried out during COVID-19 pandemic in fourth Quarter of 2020

According to Kaspersky report, shows how the DDOS (Distributed denial of service) attack has been increased in Quarter four of 2020 in figure 6, since the transmission of education to remote working, Attackers have tried to corrupt the classes by flooding and sending a huge garbage data to the learning platforms in the last months of 2020. Many cities suffered from network malfunctions; initially they thought the incidents come from technical failures, but later they discovered that were from DDOS attack. In December, FBI (Federal Bureau of Investigation) exhorted from the DDOS attack especially educational organizations. They are recommended to use anti-DDoS and strong firewalls. (Kupreev, 2021)

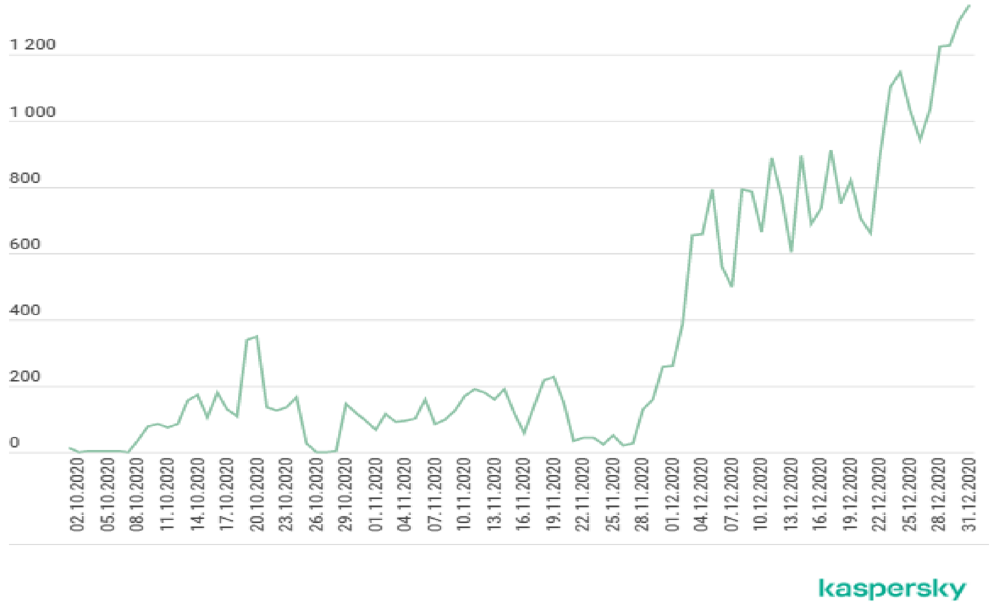


Figure 12: DDOS threats during COVID-19 (Source: Kaspersky)

According to a report from Checkpoint Cybersecurity Company in the fourth quarter of 2020, shows that Microsoft is a top brand that was imitated for phishing attack in order to steal users' username & passwords as figure 7 shows. Next brand is DHL, attackers tried to impersonate shipping companies since the online shopping has been increased during this period. (Check Point Software, 2021)

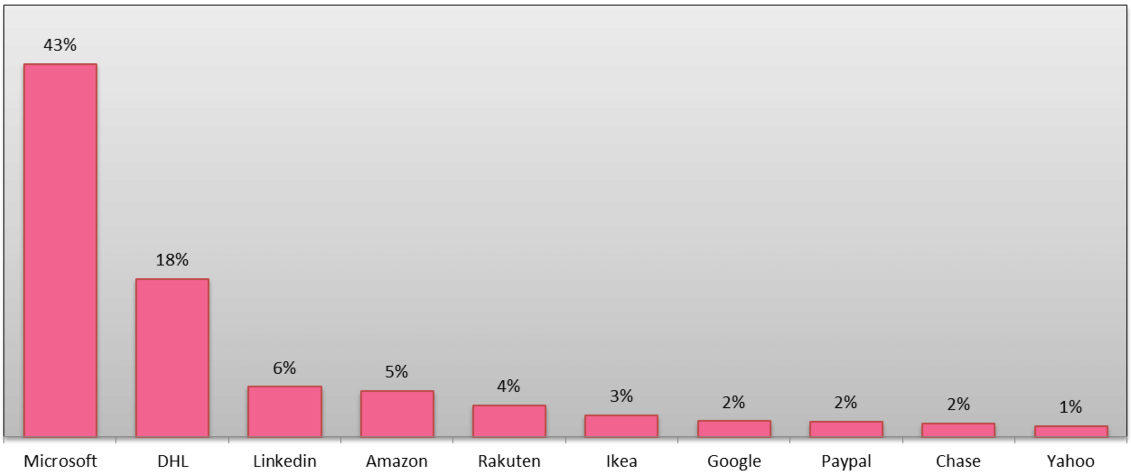


Figure 13: Top phishing brands during COVID-19 in Q4 2020 (Source: Checkpoint security)

11. Conclusion

According to the conducted studies, cybercriminals take advantage of the fear and uncertainty created by the unstable economic and social situation caused by the Covid-19 epidemic to launch their attacks. After a year has passed in the Corona crisis and the emergence of the second and third Corona mutant, some sectors and individuals are still suffering from attacks, for example, the public sector, the health sector, the education sector, the technology sector, and the trade sector. Different causes led to the increasing cyberattacks during the COVID-19 pandemic, such as the lack of infrastructure, unawareness of employees about security, working in insecure home networks, unreliable online shopping, and attractive fake websites. The phishing attack was the most cyberattack that occurred during the pandemic in the first three-quarters. Also, DDOS attacks had increased in the fourth quarter, especially in the education sector. After a year and a half have passed in the COVID-19 crisis and the second and third Corona mutant emergence. Some sectors and individuals are still suffering from attacks. The COVID-19 pandemic imposes difficulties on individuals and governments in avoiding cyberattacks. There is an urgent need to develop a comprehensive framework for information security and make continuous efforts to ensure cyberspace's safety, security, and durability.

The consequences of the COVID-19 pandemic have exacerbated these threats and attacks, which necessitates affected sectors to strengthen their security, preventive, protection, and response measures; To avoid and reduce cyber threats. It should be based on a firm foundation for information security and be compatible with legal and technical aspects. It is imperative to provide networks with a high degree of safety for individuals who work from home. And the provision of secure protocols to protect the transfer of information over the network to avoid access to sensitive data by cybercriminals. Also, the imposition of strong restrictions against phishing, make sure every website you accessed contains security certificates that encrypt the communication between you and the website you are using. Such as a transport layer security (TLS) / secure sockets layer (SSL).

References

Abukari, A., & Bankas, E. (2020). Some cyber security hygienic protocols for teleworkers in COVID-19 pandemic period and beyond. *International Journal of Scientific & Engineering Research*, 11(4), 1401-1407.

Ahinkorah , B., Ameyaw , E., Hagan Jr, J., Seidu , A., & Schack, T. (2020). Rising above misinformation or fake news in Africa: Another strategy to control COVID-19 spread. *Frontiers in Communication*.

Ahmad, T. (2020). orona virus (covid-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity. Available. *at SSRN*.

Alzahrani, A. (2020). Coronavirus social engineering attacks: Issues and recommendations. *Int. J. Adv. Comput. Sci. Appl*, 11(5), 154-161.

Baz , M., Alhakami, H., Agrawal, A., Baz, A., & Khan, R. (2021). Impact of COVID-19 Pandemic: A Cybersecurity Perspective. *INTELLIGENT AUTOMATION AND SOFT COMPUTING*, 27(3), 641-652.

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during COVID-19. *European Societies*.

cdnetworks. (2020). *THE INDUSTRIES MOST VULNERABLE TO CYBER ATTACKS IN 2021* . Retrieved from cdnetworks: https://www.cdnetworks.com/cloud-security-blog/the-5-industries-most-vulnerable-to-cyber-attacks/

Check Point Software. (2021, 1 14). *Brand Phishing Report Q4 2020*. Retrieved from Check Point Software: https://blog.checkpoint.com/2021/01/14/brand-phishing-report-q4-2020/

checkpoint. (2021). *COVID-19 Impact: Cyber Criminals Target Zoom Domains*. Retrieved from checkpoint: https://blog.checkpoint.com/2020/03/30/covid-19-impact-cyber-criminals-target-zoom-domains/

Chigada , J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19. *A systematic literature review. South African Journal of Information Management*.

Cohen, J. (2021, 4 7). *Phishing Attacks Increase 350 Percent Amid COVID-19 Quarantine*. Retrieved from pcmag: https://www.pcmag.com/news/phishing-attacks-increase-350-percent-amid-covid-19-quarantine

Collier, B., Horgan, S., Jones, R., & Shepherd, L. (2020). The implications of the covid-19 pandemic for cybercrime policing in scotland: a rapid review of the evidence and future considerations. *Scottish Institute for Policing Research*.

Columbus, L. (2021). *Top 10 cybersecurity lessons learned one year into the pandemic*. Retrieved from VentureBeat: https://venturebeat.com/2021/03/11/top-10-cybersecurity-lessons-learned-one-year-into-the-pandemic/

Desk, E. (2020, 8). *Kaspersky warns phishing attacks are becoming increasingly more targeted. Enterprise Channels MEA*. Retrieved from ec-mea: https://www.ec-mea.com/kaspersky-warns-phishing-attacks-are-becoming-increasingly-more-targeted/

Desk, E. N. (2020, 08). *Kaspersky warns phishing attacks are becoming increasingly more targeted. Enterprise Channels MEA*. Retrieved from ec-mea: https://www.ec-mea.com/kaspersky-warns-phishing-attacks-are-becoming-increasingly-more-targeted/

Dwivedi , Y., Hughes, D., Coombs , C., Constan, I., Duan , Y., Edwards , J., & Upadhyay, N. (2020). . Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. *International Journal of Information Management*.

Eboibi, F. (2020). Cybercriminals and Coronavirus cybercrimes in Nigeria, the United States of America and the United Kingdom: cyber hygiene and preventive enforcement measuresV. *Commonwealth Law Bulletin*, 1-30.

Eian , I. , Yong , L., Li, M., & Fatima, Z. (2020). Cyber Attacks in the Era of COVID-19 and Possible Solution Domains.

Fein, D. (2020). *Darktrace email finds: Microsoft Teams impersonation*. Retrieved from Darktrace: https://www.darktrace.com/en/blog/darktrace-email-finds-microsoft-teams-impersonation/

fiercehealthcare. (2019). *Healthcare data breaches cost an average $6.5M: report*. Retrieved from fiercehealthcare.: https://www.fiercehealthcare.com/tech/healthcare-data-breach-costs-average-6-45m-60-higher-than-other-industries-report

Furnell, S., & Shah, J. (2020). Home working and cyber security–an outbreak of unpreparedness? *Computer Fraud & Security*.

Georgiadou , A., Mouzakitis, S., & Askounis , D. (2021). Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal*, 1-20.

Group-IB’s. (2020). *ERT-GIB: Phishers prefer Tesla, top 3 malware strains in COVID-19 phishing campaigns, and pandemic-related dilemmas faced by hacker underground*. Retrieved from Group-IB’s Computer Emergency Response Team (CERT-GIB): https://www.group-ib.com/media/covid-phishing-campaings/

Hakak , S., Khan, W., Imran , M., & Choo, K. (2020). Have you been a victim of COVID-19-related cyber incidents? Survey, taxonomy, and mitigation strategies. *IEEE Access*, 8, 124134-124144.

HAYES, A. (2021). *Trade*. Retrieved from investopedia: https://www.investopedia.com/terms/t/trade.asp

hayesconnor. (2020, July 31). *Data breaches and the Public sector* . Retrieved from hayesconnor: https://www.hayesconnor.co.uk/news-and-resources/news/data-breaches-and-the-public-sector/

Hijji , M., & Alam, G. (2021). A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions. *IEEE Access*, 9, 7152-7169.

ICCWBO. (2020, 03 05). *COVID-19 CYBER SECURITY THREATS TO MSMEs.* Retrieved from ICCWBO: https://iccwbo.org/content/uploads/sites/3/2020/05/2020-icc-sos-cybersecurity.pdf

INTERPOL. (2020). *INTERPOL report shows alarming rate of cyberattacks during COVID-19.* INTERPOL. Retrieved from https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Kashif, M., Javed , M., & Pandey, D. (2020). A Surge in Cyber-Crime during COVID-19. *ndonesian Journal of Social and Environmental*.

Khan, N., Brohi , S., & Zaman, N. (2020). Ten deadly cyber security threats amid COVID-19 pandemic.

Kulikova, T. (2020). *Spam and phishing in Q3 2020. Securelist*. Retrieved from securelist: https://securelist.com/spam-and-phishing-in-q3-2020/99325/

Kulikova, T. (2021). *Spam and phishing in Q2 2020. Securelist.* Retrieved from securelist: https://securelist.com/spam-and-phishing-in-q2-2020/97987/

Kupreev, O. (2021, 2). *DDoS attacks in Q4 2020. Securelist*. Retrieved from securelist: https://securelist.com/ddos-attacks-in-q4-2020/100650/

Lallie , H., Shepherd, L., Nurse , J., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, 105, 102248.

Landi, H. (2019). *Healthcare data breaches cost an average $6.5M: report*. Retrieved from fiercehealthcare: https://www.fiercehealthcare.com/tech/healthcare-data-breach-costs-average-6-45m-60-higher-than-other-industries-report

Landi, H. (2019). *The health sector consists of organizations that provide medical services, manufacture medical*. Retrieved from fiercehealthcare: https://www.fiercehealthcare.com/tech/healthcare-data-breach-costs-average-6-45m-60-higher-than-other-industries-report

Mandal, s., & Khan, d. (2020). A Study of Security Threats in Cloud: Passive Impact of COVID-19 Pandemic. In 2020. *A Study of Security Threats in Cloud: Passive Impact of COVID-19 Pandemic. In 2020.*

Mehta, I. (2020, 04). *Apple was the most imitated brand for phishing attacks in Q1 2020. The Next Web*. Retrieved from thenextweb: https://thenextweb.com/security/2020/04/14/apple-was-the-most-imitated-brand-for-phishing-attacks-in-q1-2020/Apple was the most imitated brand for phishing attacks in Q1 2020. The Next Web

Meyer, B., Prescott, B., & Sheng, X. (2021). The impact of the COVID-19 pandemic on business expectations. *International Journal of Forecasting.*

Micro, T. (2021, 3 4). *Cloud-based Email Threats Capitalized on Chaos of COVID-19.* Retrieved from newsroom: https://www.trendmicro.com/en_hk/about/newsroom/press-releases/2021/03-04-cloud-based-email-threats-capitalized-chaos-covid-19.html

Moore, J. (2020, January 28). *Which sectors are most vulnerable to cyber attacks?* Retrieved from ifsecglobal: https://www.ifsecglobal.com/cyber-security/which-sectors-are-most-vulnerable-to-cyber-attacks/

Muthuppalaniappan, M., & Stevenson, K. (2020). Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. *International Journal for Quality in Health Care.*

Nabe, C. (2020). *Impact of COVID-19 on Cybersecurity* . Retrieved from deloitte: https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

National Cybersecurity Authority. (2020). *Cybersecurity Quarterly Bulletin -Q3 /2020.* National Cybersecurity Authority.

National Cybersecurity Authority. (2020). *Cybersecurity Quarterly Bulletin –Q4 /2020.* National Cybersecurity Authority.

Novet, J. (2021). *Microsoft's big email hack: What happened, who did it, and why it matters*. Retrieved from cnbc: https://www.cnbc.com/2021/03/09/microsoft-exchange-hack-explained.html

Office Watch. (2020). *Microsoft leads again! The most impersonated brand on the Internet. Office Watch.* Retrieved from Office Watch: https://office-watch.com/2020/microsoft-leads-again-the-most-impersonated-brand-on-the-internet/

Olofinbiyi, S., & Singh, S. B. (2020). The Role and Place of Covid-19: An Opportunistic Avenue for Exponential World's Upsurge in Cyber Crime. *International Journal of Criminology and Sociology*, 221-230.

Osborne, C. (2021). *COVID pandemic causes spike in cyberattacks against hospitals, medical companies*. Retrieved from Zero Day : https://www.zdnet.com/article/covid-pandemic-prompts-rise-in-cyberattacks-against-hospitals-medical-companies/

Owaida, A. (2021, mar 4). *Cybersecurity risks and challenges facing the financial industry*. Retrieved from welivesecurity.: https://www.welivesecurity.com/2021/03/04/cybersecurity-risks-challenges-facing-financial-industry/

Pandey, N., & Pal, A. (2020). Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. International Journal of Information Management. *nternational Journal of Information Management*.

Pranggono, B., & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. Internet Technology Letters.

Purwanto , A., Asbari, M., Fahlevi, M., Mufid, A., Agistiawati, E., Cahyono , Y., & Suryani, P. (2020). Impact of Work From Home (WFH) on Indonesian Teachers Performance During the Covid-19 Pandemic: An Exploratory Study. *International Journal of Advanced Science and Technology,*, 29(5), 6235-6244.

Ramadan, R. A., Aboshosha, B. W., Alshudukhi, J. S., Alzahrani, A. J., El-Sayed, A., & Dessouky, M. M. (2021). Cybersecurity and Countermeasures at the Time of Pandemic. *Journal of Advanced Transportation*.

Regzen. (2020, Oct 23). *Industries most vulnerable to cyberattacks in 2020*. Retrieved from 10guards : https://10guards.com/en/uncategorized/industries-most-vulnerable-to-cyberattacks-in-2020/

Schwartz, M. (2020). *Cybercrime Review: Hackers Cash in on COVID-19. Bank Info Security.* . Retrieved from Bank Info Security: https://www.bankinfosecurity.com/cybercrime-review-hackers-great-covid-19-cash-in-a-15037

securelist. (2020). *Spam and phishing in Q1 2020*. Retrieved from securelist.: https://securelist.com/spam-and-phishing-in-q1-2020/97091/

Security, A. (2020). *Microsoft Teams Impersonation. Abnormal Security*. Retrieved from abnormalsecurity: https://abnormalsecurity.com/blog/microsoft-teams-impersonation/

STAFF, I. (2020, Mar 23). *Healthcare Sector*. Retrieved from https://www.investopedia.com/terms/h/health_care_sector.asp

Taylor, A. (2021). *In the Midst of COVID-19, We're Seeing a Pandemic of Cyber Attacks*. Retrieved from Enterprisetimes: https://www.enterprisetimes.co.uk/2021/03/12/in-the-midst-of-covid-19-were-seeing-a-pandemic-of-cyber-attacks/

Telling, O., & Almeida, L. (2020). *Finance sector hit by cyber attacks during Covid crisis*. Retrieved from investorschronicle: https://www.investorschronicle.co.uk/shares/2020/11/24/cyber-attacks-on-finance-sector-soar-during-covid-crisis/

Tepper, D. E. (2021). . RANSOMWARE and Other Cybercrimes in the Age of COVID-19: The incidence of hackers holding computer data for ransom was already rising. *APTA Magazine*, 42–48.

Weil , T., & Murugesan, S. (2020). IT Risk and Resilience-Cybersecurity Response to COVID-19. *IT Prof*, 22(3), 4-10.

wikipedia. (n.d.). *Education* . Retrieved from wikipedia.: https://en.wikipedia.org/wiki/Education

Wirth, A. (2020). Cyberinsights : COVID-19 and What It Means for Cybersecurity. *Biomedical Instrumentation & Technology*, 216–219.