iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** XII **Month of publication:** December 2022

DOI: https://doi.org/10.22214/ijraset.2022.48122

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue XII Dec 2022- Available at www.ijraset.com

Overview of Key Cyber Security Threats amid COVID-19 Pandemic

Saloni Halwai[1], Ms. Shweta Loonkar[2]
[1]*B. Tech Integrated,* [2]*Department of Computer Engineering, Mukesh Patel School of Technology Management and Engineering, NMIMS University, INDIA*

Abstract: ***This pandemic has not only affected the world physically but has also caused a major rise in the number of cyberattacks and cybersecurity breaches. In these trying times, the entire paradigm has shifted, forcing every individual to adapt to remote working. Since everything has shifted from its traditional offline methods to online portals, the online traffic has increased tremendously. This paper outlines how and why the number of cyberattacks have increased. Moreover, this paper provides real world cases where cybersecurity attacks have been used in order to extort personal information with numerous statistics and also sheds light upon various preventative methods one can adopt in order to prevent falling victim to any cybercrime.***

This paper is assembled into two parts. The first part highlights few of the most common cyberattacks which were observed to have upsurged manifold times during the COVID-19 pandemic and used excessively by cybercriminals to unethically derive the personal information of unsuspecting users for malicious reasons. These three main methods being phishing, malware and data breaches. The second part talks about ways and methods to prevent them.

Keywords: COVID-19, Data Breaches, Pandemic, Phishing, Malware, Security, Cyber-Attacks, Cyber-Crimes, Cyber-Criminals.

I. INTRODUCTION

The society as we know it is facing one of the biggest and worst pandemics: COVID-19. This has had an overwhelming amount of impact and brought the world to a standstill. COVID-19 is considered as one of the most crucial global health calamities and has forced everyone in quarantine and to embrace practices of social distancing and remote working. Hence the demand for digital infrastructure has skyrocketed overnight due to which technology has become a lucrative target for cybercriminals.

Cybercriminals are assaulting the computer networks and systems of people, industries and even international organizations at a stretch when cyber defences might be dropped due to the swing of effort and concentration to the health crisis. The World Health Organisation (WHO) has reported a quintuple upsurge in cyberattacks to innumerable organizations as compared to the previous year. Fig.1 shows the top 10 security threats amid COVID-19 pandemic [1].

Manifold renowned and accomplished businesses and corporations have observed a dramatic upsurge in the number of cyberattacks focused at its staff, and email cheats and scams aiming the community and public all together. This has not only placed the operatives' and employees' information + data in jeopardy but correspondingly the clienteles and customers too. Data that is pilfered is vended and traded and possesses threat to the peoples' lives. The pandemic has brought about a major monetary and economic crisis universally and globally which has left an abundance of individuals unemployed and unwaged resulting in making them anxious and desperate to find methods to make money no matter what it takes. Due to the nature of the Covid-19 virus, working from home is the unsurpassed option to give in to, hence there has been a sheer intensification in online traffic and hackers have held on to the opportunity leading to tremendous increase in the degree of cybercrimes.

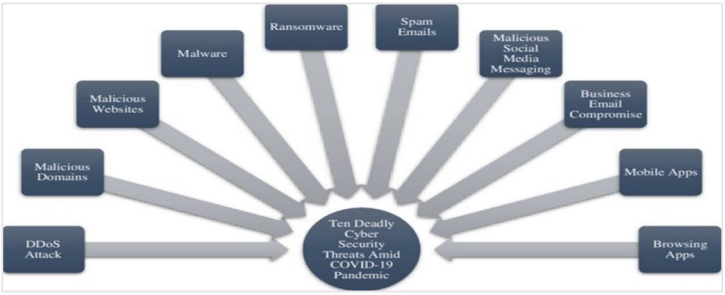


Figure 1: Top 10 Cyber Security Threats Amid COVID-19 Pandemic [1].

Cybercriminals are taking benefit of the widespread, prevalent universal infrastructures and communications on the coronavirus to disguise their doings.

Malware, spyware and Trojans have been found embedded in user-friendly and interactive coronavirus maps and websites [4]. Unsolicited spam emails are also misleading users into clicking on hyperlinks which download and transfer malware to their desktops or mobile devices [5].

There are a significant number of enumerated domains on the Internet that comprise of the terms: "coronavirus", "corona-virus", "covid19" and "covid-19". While some are genuine and legitimate websites, cyber-criminals are fast producing and generating thousands of new-fangled sites on a daily basis to carry out spam campaigns, phishing or to spread malware.

II. PHISHING

Phishing is a fraudulent attempt to obtain personal information of an individual. The targets are contacted by email, telephone or text message by someone who is posing as a legitimate organization or a trustworthy entity in an electronic communication.

As this pandemic has gripped us, there is massive reliance on the online connectivity and this has in turn caused a massive influx in the presence of cyberattacks. Phishing is probably the most used attack during these trying times. Phishing is very successful in providing sensitive information that can benefit cybercriminals.

Cybercriminals are gaining benefit and taking advantage of the pandemic by means of extensive awareness and consciousness of the subject to trick users into revealing their personal data and information or clicking on malicious hyperlinks or website attachments, unintentionally and unsuspectingly downloading, transferring malware to their desktops [10]. They impersonate government bodies, ministries of health, important figures in a relevant country in order to disguise themselves as reliable sources and trick the people. The emails even include legitimate, sincere brand logos to look more authentic.

Figure 2: Phishing sites detected by Google in 2020 [9].

Malicious emails might comprise of numerous attachments that are intended, preordained to provide you with more information about coronavirus. These attachments are very likely to download malicious software programs on your device the moment you click on the hyperlink. As soon as that software program is downloaded it possibly could give cybercriminals admittance, access to your files, documents and archives which would give them access to your personal information and could lead to identity theft and permit them to hold the fort of your desktop and data.

Techniques to help identify phishing**:**

1) They look very comparable/alike to legitimate emails and are from a trustworthy source for instance medical institute, government body etc.
2) They sound urgent and crucial and aim to spread distress amongst the addressee.
3) Claim to encompass and enclose significant information or breaking news.
4) It will very often request you to click on some hyperlink that will ask you for personal information or ask you to download some attachments.

A significant number of phishing websites were found by google during the pandemic itself and innumerable websites are still being developed by cybercriminals. Fig. 2 shows the number of phishing websites detected by Google in 2020.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue XII Dec 2022- Available at www.ijraset.com

III. MALWARE

Malware refers to malicious software program and can be used for troublesome and disrupting services, extracting and mining data and a variety of various different attacks. Ransomware is one of the most common types of malware at the moment [3].

Hackers use phishing or additional methods to introduce malware onto the target's computer system and network that encrypts and encodes the system, rendering the documentations and data on the system which are unapproachable by anyone and inaccessible to the target.

The hackers then attempt and try to extract an economic imbursement from the target in argument for the key required to decrypt and decipher the compromised files and documentations. In some occasions, hackers also threaten to publicly and openly announce the encrypted information by a specified deadline if no compensation is received [16].

The disastrous and devastating spread of COVID-19 is becoming an opportunity and occasion for the cyber-criminals to spread malware or let loose cyberattacks. One such kind of malware attack is with practice 'Coronavirus Maps' – It's a malware infecting PCs, desktops or devices to steal passwords [2].

Malware associated to COVID-19 amplified in prominence all through the pandemic and impacted individuals, organisations, businesses, public, government and corporates across the world. It is the second largest cyberattack, appearing in 65% of cases [3]. Fig. 3 shows the distribution of cyberattacks across various countries.

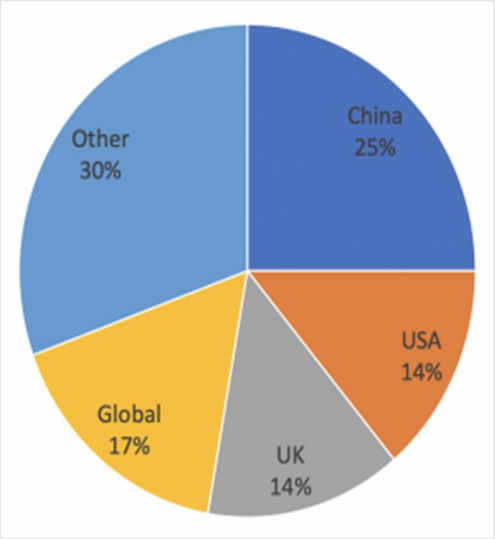


Figure 3: Cyberattack distribution across countries [3].

There's also indication that distant working intensifications the menace of an efficacious malware attack significantly. This intensification is as a result of combination of feebler controls on home-based IT and an advanced probability of users clicking on COVID-19 theme-based malware bait emails, assumed levels of anxiety [11].

Some current malware baits/lures include:

1) Information/data about vaccinations, masks and short-supply merchandises like hand sanitizer.
2) Monetary scams offering compensation of government aid and assistance all through the financial shutdown.
3) Unrestricted downloads for technology resolutions in high demand, for instance video and audio-conferencing platforms.
4) Critical apprises to enterprise partnership and association solutions.

To demonstrate the information and mortalities about the novel coronavirus, Johns Hopkins University (JHU, Maryland) developed and designed a map with a user-friendly, interactive console [6]. Hackers took advantage of it, and they embedded and implanted a java-based malware to it, the victims not only clicked on the map and opened it, but a large number of public even shared it [1].

As stated by Trend Micro Research, they studied and analysed a coronavirus-themed Winlocker which has the feature to lock users out of affected machineries. When this malware is executed, it drops some files and documents and modifies/alters the windows registries. Far ahead it plays a sound and shows a message that the system has been locked, the system restarts and then needs a password to unlock it [7]. Malware and phishing websites have been observed to have the highest upsurge as compared to other threats and attacks. Fig. 4 gives an overview of the upsurge in Malware and Phishing websites being accessed in the present pandemic from February 2020 to March 2020 [1].

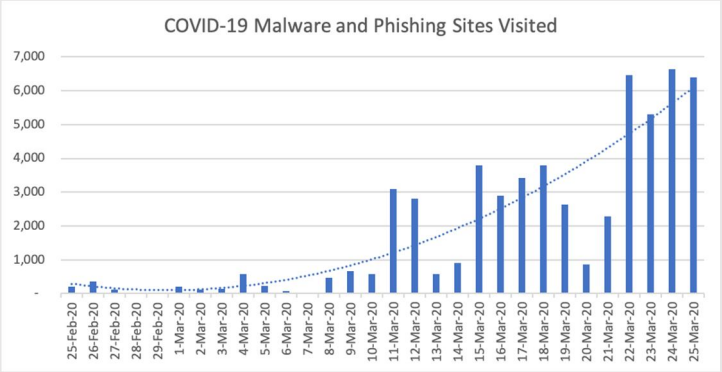


Figure 4: COVID-19 Malware and Phishing Vesting Sites [8].

IV. DATA BREACHES

A data breach is the intentional or unintended release of protected or private/confidential information and data to an untrusted environment. Supplementary terms for data breach include inadvertent information revelation, data leak, information leakage and also data spill. Data breaches may include personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property.

Data breach has been a prevalent problem since a very long time and has been one of the greatest challenges for most of the companies. Every company requires their customers to provide them with their information before using their services in order to keep records. However, asking for personal details comes with great responsibilities because this is confidential information meant to be strictly kept within the organisation and be used for the purpose of the company only. Often the data breach takes place due to an accidental insider- a person with whom the information is shared unintentionally, Malicious Insider- a person who has gained access to the information with the intention to cause harm to the individual or company, Lost or Stolen Devices- this causes unencrypted sensitive data to be accessed, Malicious Outside Criminals- they are hackers who intentionally use different attacks to gain information for their use.

Hence, companies make it their priority to ensure their customers safety and win their trust with their personal information. The pandemic has just added fuel to the fire and there has been a considerable increase in the number of data breaches that have taken place. The methods used to breach data include: Phishing, Brute force attacks and Malware. The common target in these types of attacks are stolen credentials, payment card fraud, third party access, personal mobile devices etc. Due to the absence of physical work everything was moved online as a result of which there was a lot of data available for cybercriminals to hack into and misuse.

Data breaches in 2020:

1) 98% of point of sale data breaches in the accommodation and food services industry were financially motivated. (Verizon)

2) Cybersecurity breaches in healthcare cost the most out of any other industry at $7.13 million. (IBM). Fig. 5 shows the cost distribution of cybersecurity breaches in various industries [12].

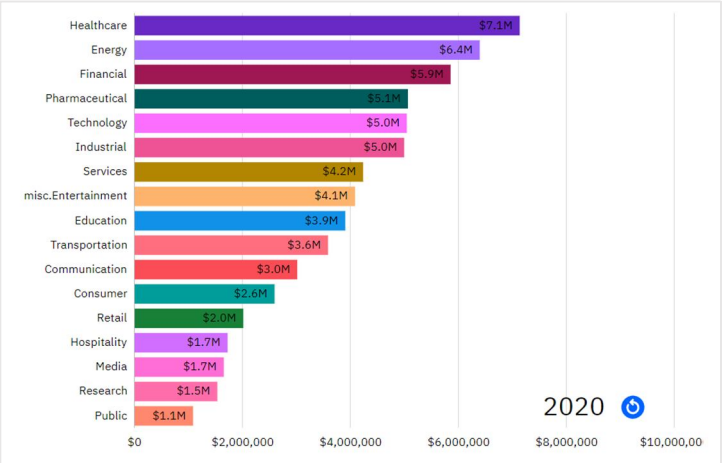


Figure 5: Cost distribution of data breaches in various industries [12].

3) Digital Shadows reported that the access to domain administrator of the local government are sold for an average of around $3,217 in 2020.
4) 8,000 small business owners were impacted because of a data breach of the federal disaster loan applications. (U.S. PIRG)
5) 52% of compliance leaders say the most-increased third-party risk for their organization is cybersecurity. (Gartner)
6) On July 10, the OCIE released a ransomware alert that one or more hackers have orchestrated attacks to penetrate financial institution networks. (SEC)
7) Confirmed data breaches in the healthcare industry increased by 58% this year [15]. (Verizon)
8) Twitter- Hackers surprised the entire internet when they managed to get access to some of the most important verified twitter users like Barack Obama, Elon Musk, Joseph R. Biden Jr., Bill Gates, and many more. Hackers were able to reset 45/130 targeted accounts' passwords. They posted fake tweets offering to send $2000 for $1000 to an unknown Bitcoin address. This scam enabled the attackers to fraud $121,000 in Bitcoin through almost 300 transactions.
9) Marriot- On March 31st, 2020 this famous chain of hotel released that they had suffered a huge data breach impacting over 5.2 million hotel guests who used the company's loyalty application. The hackers obtained login credentials of two of the company's employees who had access to the customers that used the loyalty application. The company believes that the login credentials was acquired either by credential stuffing or phishing nonetheless this led to the hackers gaining access to the customers' personal details for instance names, birthdates, and telephone numbers, travel information, and loyalty program information.
10) Zoom- Due to the Covid-19 pandemic a lot of offices and educational institutes decided to move online, this led to a spike in their users and went on to become one of the most popular and commonly used application. With the rapid increase of user database, the application was prone to various security threats. In April 2020, it was confirmed that stolen zoom passwords of 500,000 users were available for sale on the dark web. Not only were the account login credentials being available but also, the victims' personal meeting URLs and HostKeys.
11) Magellan Health- The healthcare giant happens to be one of the fortune 500 companies making it vulnerable to a lot of cyberattacks. In April 2020, 365,000 patients were affected due to a well-planned cyberattack that took place where allegedly a malware was first installed in order to steal employee login credentials, post which a phishing attack was done to deploy a ransomware attack. The hackers were able to retrieve steal login credentials of employees, personal information, employee ID numbers, sensitive patient details such as W-2 information, Social Security numbers, or Taxpayer ID numbers [14]. Fig. 6 shows the types of breaches because of which the healthcare records were exposed [15].

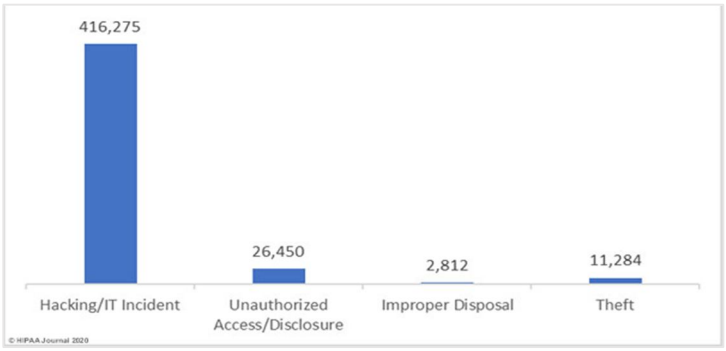


Figure 6: Healthcare Records Exposed by Breach Type [15].

V. PREVENTIVE MEASURES FOR PHISHING, MALWARE AND DATA BREACHES

70% of cyberattacks use an amalgamation of phishing and hacking. 63% of established data breaches involved weak, default or stolen passwords. The top 3 industries affected by security incidents are public, information and financial services [17]. It is very necessary to take preventive measures in such times as everything is moving online and every user wants to protect their data.
Some preventive measures for Phishing would be:

1) Emails should be read carefully. One must not open emails from unknown sources and should not download any unknown attachments.
2) Passwords or any other sensitive information should not be sent by mail.
3) Avoid emails that insist one act urgently. Phishing emails frequently try to create a sense of perseverance or demand instantaneous action.

4) It's important to pay close attention to terminology as cybercriminals also use spear phishing by using the receiver's full name. So, one must check for the language that is normally expected in the types of emails they receive.
5) One must check if the sender's email domain matches that of the organisation he/she claims to belong to.
6) If the email has grammatical/punctuation errors then it's mostly a phishing email.
7) Protect your devices by installing anti-spam, anti-spyware and anti-virus software and make sure they are always up to date.
8) Visit websites by entering the domain tag yourself. Many of the businesses use encryption and Secure Socket Layer (SSL)/Transport Layer Security (TLS). If you receive a certificate error while browsing, consider it as a warning sign that something is not right with the website [10].

Things to do in case you have become a victim of phishing:

- If one has downloaded any attachment then they must start their antispyware software and take a scan.
- Change any login credentials if they have used them to access something.
- Immediately contact the bank or financial institution if one has provided any bank details anywhere.

Some preventive measures for Malware would be [2]:

- Avoid clicking on any UNKNOWN messages with hyperlinks or install applications from unknown sources.
- Think about who sent you the message. Is it a person that you know?
- Keep Your Personal Information Safe.
- Don't Use Open Wi-Fi.
- Use Multiple Strong Passwords for multiple accounts.
- Install Anti-Virus/Malware Software.
- Keep Your Anti-Virus Software Up to Date.
- Secure your network.

Some Preventive Measures for Data Breaches would be [18]:

- Limit access to your most valuable data.
- Third-party vendors must comply.
- Conduct employee security awareness training.
- Update software regularly.
- Develop a cyber breach response plan.
- Difficult to decipher passwords.
- Regular Audits on Security Posture [19].
- Vulnerability and Compliance Management Tool [19].
- Strong encryption for sensitive data.
- Enforcing BYOD security policies, like requiring all devices to use a business-grade VPN service and antivirus protection [20].
- Imposing strong credentials and multi-factor authentication.

VI. FUTURE SCOPE

This paper reviews the increase in the types of cyberattacks caused by the COVID-19 pandemic and the impact it has had on the society. Even though the proposed preventive measures discussed in this paper are exceptionally good and enough to protect one from malicious cyberattacks, there is always room for improvement. Hence, in the future we would like to do a deeper research on the preventive measures that can be taken to minimise these attacks and protect data.

Moreover, we would also like to look deeper into establishing a set protocol in order for the measures that need to be taken into account in order to ensure complete cyber safety. The ongoing pandemic has given rise to a range of cyberattacks discussed in this paper, however with every passing day the hackers are getting creative with different ways to attack the systems and the upcoming new attacks will definitely be a topic to be covered in the future.

VII. CONCLUSION

The COVID-19 pandemic has generated remarkable and unique societal and economic circumstances leveraged by cyber-criminals [3]. The COVID-19 pandemic, and the increased rate of cyberattacks it has invoked have wider implications, which stretch beyond the targets of such attacks.

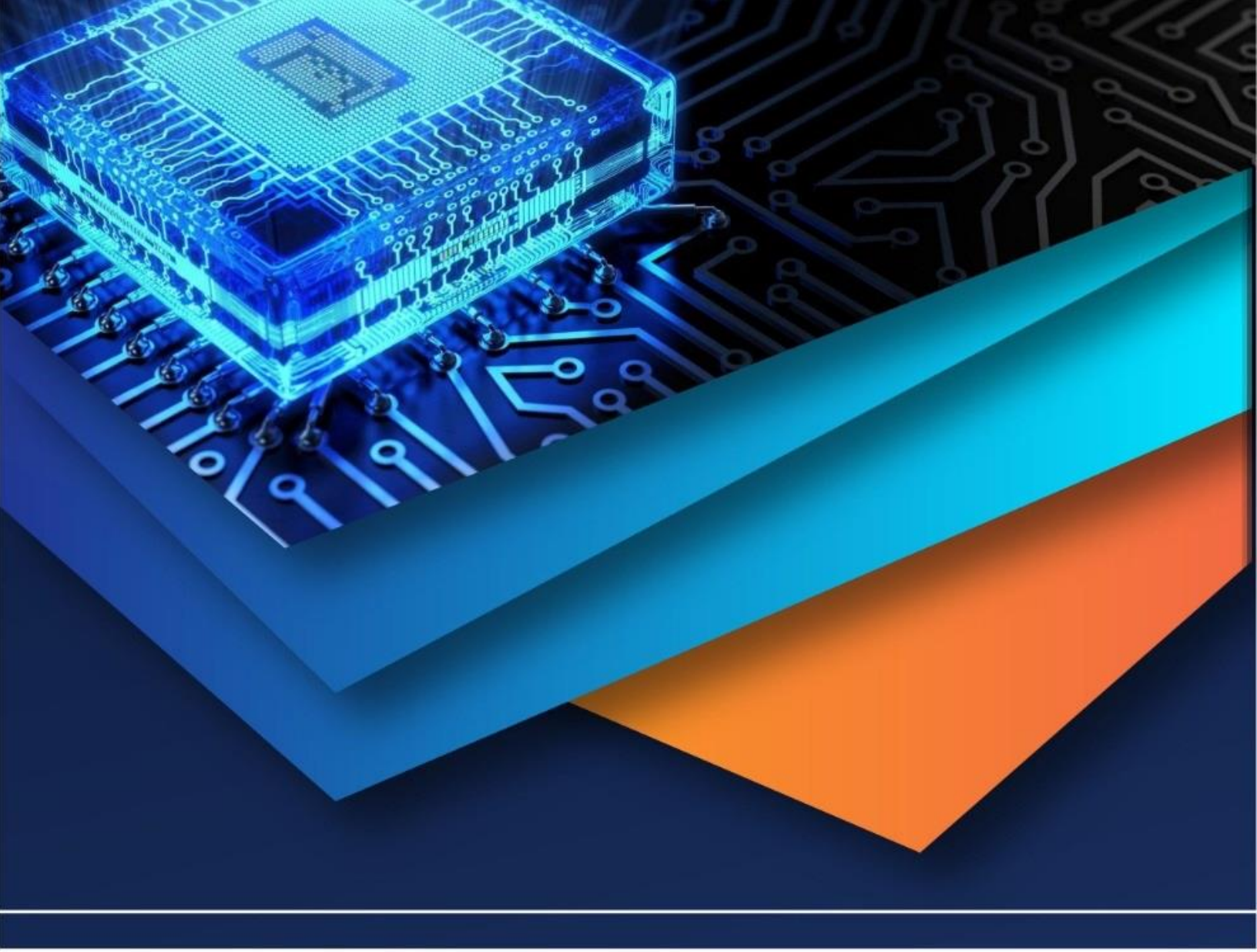
Changes to working practises and socialization, most people are now spending increased periods of time online. In addition to this, rates of unemployment have also increased, meaning more people are sitting at home online thus it is more likely that some of these people will turn to cybercrime to support themselves.

As the world is advancing and the use of ubiquitous computing is increasing daily in a similar manner, there's a sequential increase in cybersecurity threats and privacy issues as well. Interaction online has increased enormously during these difficult times and the bad actors are taking advantage of the situation and becoming more active in hacking and attacking different platforms for some personal financial gains and other interests.

There has been a considerable increase in the registration of malicious domains, websites, and spam emails. The intruders are targeting individuals, government officials, and even medical and health care systems. These Cyber Security attacks have led to some serious privacy issues and concerns. Thus, this paper presented the three main types of attacks that have grown during this pandemic and methods to prevent the same.

REFERENCES

[1] Khan, Navid & Brohi, Sarfraz & Zaman, Noor. (2020). Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. 10.36227/techrxiv.12278792.v1.
[2] https://infosecawareness.in/article/COVID19-cyber-attacks
[3] Harjinder Singh Lallie, Lynsay A. Shepherd, Jason R. C. Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. (2020) Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic
[4] J. W. Han, O. J. Hoe, J. S. Wing, and S. N. Brohi, "A conceptual security approach with awareness strategy and implementation policy to eliminate ransomware," in Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence, 2017, pp. 222–226.
[5] Interpol, "COVID-19 cyberthreats," 2020. [Online]. Available: https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats. [Accessed: 10-October-2020].
[6] JHU, "Coronavirus COVID-19 Global Cases by the Centre for Systems Science and Engineering (CSSE) at Johns Hopkins University (JHU)"," 2020. [Online]. Available: https://coronavirus.jhu.edu/map.html. [Accessed: 14-October-2020].
[7] M, "Developing Story: COVID-19 Used in Malicious Campaigns," 2020. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains. [Accessed: 14-October-2020].
[8] M. Security, "Sophisticated COVID-19–Based Phishing Attacks Leverage PDF Attachments and SaaS to Bypass Defences," 2020. [Online]. Available: https://www.menlosecurity.com/blog/sophisticated-COVID-19-based-phishing-attacks-leverage-pdf-attachments-and-saas-to-bypass-defenses. [Accessed: 14-October-2020].
[9] PCMAG, "Phishing Attacks Increase 350 Percent Amid COVID-19 Quarantine," 2020. [Online]. Available: https://in.pcmag.com/privacy/135635/phishing-attacks-increase-350-percent-amid-covid-19-quarantine. [Accessed: 14-October-2020]
[10] Enisa, "Understanding and dealing with phishing during the covid-19 pandemic," 2020. [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/understanding-and-dealing-with-phishing-during-the-covid-19-pandemic. [Accessed: 14-October-2020]
[11] GT, "Ransomware During COVID-19," 2020. [Online.] Available: https://www.govtech.com/blogs/lohrmann-on-cybersecurity/ransomware-during-covid-19.html. [Accessed: 18-October-2020].
[12] ActiveReach, "Data Breach costs are increasing – what's the impact of COVID?" 2020. [Online]. Available: https://activereach.net/newsroom/blog/data-breach-costs-are-increasing-whats-the-impact-of-covid/. [Accessed: 14-October-2020]
[13] H. Journal, "January 2020 Healthcare Data Breach Report," 2020. [Online]. Available: https://www.hipaajournal.com/january-2020-healthcare-data-breach-report/. [Accessed: 14-October-2020]
[14] K. Blog, "5 Biggest Data Breaches of 2020 (So Far)," 2020. [Online]. Available: https://www.kratikal.com/blog/5-biggest-data-breaches-of-2020-so-far/. [Accessed: 14-October-2020]
[15] Panda MediaCenter, "43 COVID-19 Cybersecurity Statistics," 2020. [Online]. Available: https://www.pandasecurity.com/mediacenter/news/covid-cybersecurity-statistics/. [Accessed: 14-October-2020]
[16] Lexology, "Ransomware Attacks during COVID-19," 2020. [Online]. Available: https://www.lexology.com/library/detail.aspx?g=f85e4ffb-6c32-43ca-8240-33a5d9d94b2b. [Accessed: 18-October-2020].
[17] Phishing Box, "Phishing Facts: Information security statistics every business should know," 2020. [Online]. Available: https://www.phishingbox.com/resources/phishing-facts. [Accessed: 18-October-2020]
[18] TechSupport, "6 Ways to Prevent Cybersecurity Breaches," 2020. [Online]. Available: https://www.techsupportofmn.com/6-ways-to-prevent-cybersecurity-breaches. [Accessed: 18-October-2020]
[19] Cipher, "5 Effective Ways to Prevent Data Breaches," 2020. [Online]. Available: https://cipher.com/blog/5-effective-ways-to-prevent-data-breaches/. [Accessed: 18-October-2020]
[20] Kaspersky, "How Data Breaches happen: What they are and why it matters," 2020. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/data-breach. [Accessed 18-October-2020]



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY