International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 03 | March - 2022 ISSN: 2582-3930

CYBER PANDEMIC AND CYBER CAUTION IN THE WAKE OF COVID-19

Lakhansingh Jayramsingh Pardeshi

Keraleeya Samajam (Regd.) Dombivli's Model College

Abstract -The COVID-19 global pandemic has forced the business community, academic institutions and individuals to embrace new practices such as social distancing and remote working. The pandemic has taught the business community the inestimable value of the digital space, with the popularization of lockdown measures and movement restrictions, technology has been the means of connecting to the outer world. Schools now learn via digital platforms, religious centers now use digital platforms to communicate with their worshippers, even the health sector where physical consultations are the prescribed norm, the usage of software like Telemedicine i.e. diagnosis and treatment by videoconferencing, are now being implemented by Health Techs like Helium Health. While racing to halt the virus and to trigger the economy, governments globally are reconsidering ways to ensure that their countries are stable by developing and enforcing new economic policies. However, since the world is focused on the health and economic threats posed by COVID-19, cyber criminals around the world undoubtedly are capitalizing on this crisis to breach security firewalls with the popular "twitter crypto hack" , business email compromise, and installation of ransomwares on devices of individuals.

Key Words: Cyber,Global,Pandemic,Security, journals

1.INTRODUCTION

The global epidemic of COVID-19 has compelled businesses, academic organizations, and individuals to adopt new practices like social distancing and remote working. The epidemic has taught the business world the incalculable value of human capital.With the popularity of lockdown mechanisms and movement restrictions in the digital domain,Technology has served as a conduit for communication with the outside world. In today's schools, students are taught over the internet.Religious institutions now use digital channels to communicate with their congregations.Even in the health industry, where physical consultations are required, worshippers,the use of software such as Telemedicine, which involves diagnosing and treating patients via videoconferencing,Health Techs like Helium Health are now implementing them.

IMPACT OF COVID-19 ON CYBERSECURITY

In a bid to preserve the business community and academic environment after lockdown orders have been levied by the government, the adoptions and usage by individuals'

businesses, academic institutions, religious centers, entertainment artists, platforms such as Zoom, Go To Webinar, Google Meeting, and various social media platforms have been frequent and popular. Notwithstanding that these video conferencing tools aid the business continuity of many organizations, it may interest you to note that phishing, malspams/malware and ransomware attackers are using COVID-19 as bait to impersonate brands, breach the cyber firewalls of companies thereby misleading employees and

customers. Also, users who may utilize personal computers to perform official duties could also pose a great risk to organizations. This will result in more infected personal computers and phones. Not only are businesses being targeted, end-users who download COVID-19 related applications are also being tricked into downloading ransomware, malspams/malwares disguised as legitimate applications. Recently, it was widely reported that the popular video conferencing application, Zoom, received backlash, including law suits from its shareholders, over security concerns resulting from the several "Zoom bombings" that interrupted zoom calls over that period. These involved hackers entering into chat rooms, posting improper content and attempting a theft of users' data.2 With the uncensored rush to the usage of digital communication systems, and the need to preserve digital confidentiality, accessing the cybersecurity of users would be of necessity. Some video conferencing tools have been recently accused of violating privacy and data protection regulations specifically, these platforms were reported to have shared the information of the platform users with third party organizations without the consent of the users. This is in contravention of one of the core principles of privacy and data protection (as contained in the European Union General Data Protection Regulation (EU GDPR) and the Nigeria Data Protection Regulation (NDPR), 2019) which is the obligation

imposed on data controllers to request for the consent of data subjects before collecting, using and processing the personal data of the data subjects, thereby leading to a breach where a data controller does otherwise.

USERS CYBER CAUTION

Cyber criminals have used the pandemic for commercial gain, deploying a variety of ransomware and other malware as bait to rip user's off their finances. Also, these Cyber criminals have used the COVID-19 pandemic to exploit cyber users. Frequent threats observed include:

• Phishing, using the subject of coronavirus or COVID-19 as a lure.

• Malware distribution, using coronavirus- or COVID-19- themed lures.

• Registration of new domain names containing wording related to coronavirus or COVID-19, and • Attacks against newly and often rapidly deployed remote access and teleworking infrastructure.Keep your information safe

• Backup all your important files, and store them independently from your system (e.g. in the cloud, on an external drive);

• Always verify you are on a company's legitimate website before entering login details or sensitive information as cloned websites are being created.Check your software and systems

• Ensure you have the latest anti-virus software installed on your computer and mobile devices;

• Secure email gateways to thwart threats via spam;

• Strengthen your home network;

• Secure system administrations vulnerabilities that attackers could abuse;

• Disable third-party or outdated components that could be used as entry points;

• Download mobile applications or any other software from trusted platforms only;

• Perform regular health scans on your computers or mobile devices.Be vigilant

• Talk to your family including children about how to stay safe online;

• Regularly check and update the privacy settings on your social media accounts;

• Update your passwords and ensure they contain strong (a mix of uppercase,

lowercase, numbers and special characters);

• Do not click on links or open attachments in emails which you were not expecting to receive, or come from an unknown sender

3. CONCLUSIONS

In conclusion, COVID-19 will change our lives forever with new work styles, new cybersecurity issues, new proposed policies, personal hygiene and so on. The fight against

COVID-19 is not just for the organization, employee or customer but a joint effort from everyone. It is also apparent that Post COVID-19, organizations will need to rethink their

cyber risk management measures, trainings on cyber risk and security should be conducted and the Data Privacy regulatory agency should ensure compliance by checkmating these

companies.

REFERENCES

[1] https://www.google.com