European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 07, Issue 03, 2020

Covid-19 Impacts On Organization Infrastructure Via Exploiting Society Digital Illiteracy: The Rise Of Electronics

Haitham Hilal Al Hajri[1], Badar Mohammed Al Mughairi[2], Mohammad Shahadat Hossain[3], Asif Mahbub Karim[4]

[1,2]PhD Research Fellow (Viva Completed) , Binary University of Management & Entrepreneurship, Malaysia
[3]Professor , Department of Computer Science & Engineering, University of Chittagong and
[4]Professor and Dean , Binary Graduate School, Binary University of Management and Entrepreneurship, Malaysia

Abstract: Globally, the COVID-19 pandemic has been the headline over the past few months and forced the institution and individuals to work remotely and practices such as social distancing. Consequently, the cybercriminals urgent implementation of technology to enable the organization to work remotely by conducting cyber-attack targeting critical organization within countries. This article discusses the different type of cyber threats and its impact to the organizations during COVID-19 pandemic by exploiting the digital and technology.
Keywords: COVID19, Cyber-attack, Critical Organization

1. INTRODUCTION

Even though we are living on the most anticipated year 2020, a reality check has forced the world to slow down and take a moment, to consider alternatives to our life routines. By what means we could change our accustomed living routine, how to work but not from the office, how to meet but not in person, and how to communicate but not face to face. In certain countries, the government prohibits the use of VOIP apps without proper permissions and licensing. However, due to the circumstance of corona covid-19 outbreak pandemic, they have uplifted the ban temporarily to facilitate and ease the digital means of communication. By allowing the use of VoIP apps, the society is exposed to a number of cyber threats and challenges, leveraging the literacy of the society on how to best utilize the technology on safe manner (Al Mughairi et al., 2019).

The society makes and develops the country resources and capabilities. The society compose of the same individuals who works in different aspects of country's organizations. Hence, when the society is educated and aware of the digital development and all associated risk and challenges, the chances of misuse or abuse of technology resources will have a minimal impact or losses from electronic and cybercrimes (Alshamsi et al., 2019)

Technology illiteracy does not only mean the inability of an individual to use or cope with technology advancement. It extends to those whom are below average on technology use, definitely not considered as tech savvy (Amgad et al, 2019). Those individuals use technology but at very minimal level and most of the time they do not have much of digital footprints within the cyber world. Therefore, they are not aware of the effective approach and measures in dealing with any technology predicaments. The cyber criminals leverage, such individual's incompetence's on a secure usage of technology and trick them to carry on their own deed and benefits.

Cyber criminal's ultimate gain varies on the type of target they want to achieve or conclude like crypto jacking (Al Mughairi et al., 2019). Some cyber criminal's definitive goal is to collect money and get rich, where others may be interested on collecting data and gain power of control. Some wants both money and power; in any direction a malicious act will be carried to achieve the cyber criminal's objectives and the technology illiterate society is the golden mine for such cyber criminals.

Methods used by cybercriminal to ultimately, exploit society digital illiteracy

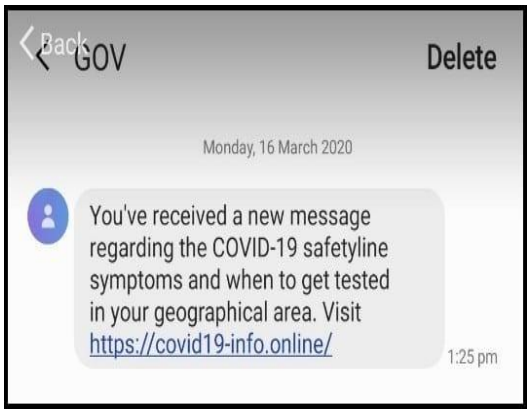
- *Society exploits Approach (Attack Vector)*
  - *Phishing*

Phishing is a technique used by cybercriminals to exploit individual's illiteracy and incompetency of technology inner workings. Therefore, they specially design (emails, text messages, social media posts etc.) to trick the victim into taking some destructive set of actions. An example illustrated by contacting the victim via electronic mean urging the victim to click on a malicious hyperactive link that will result on downloading rigged application or violating victim privacy by stealing sensitive and private information.

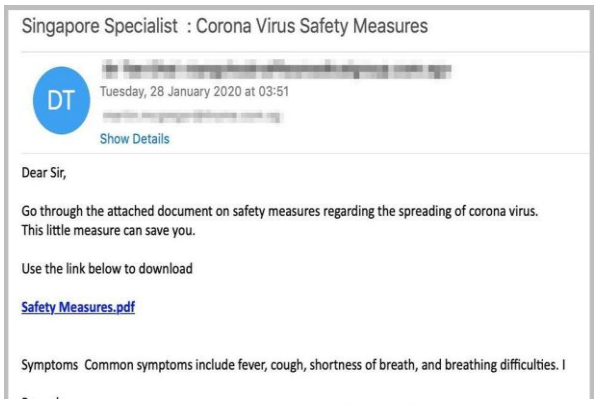
Phishing takes many forms and shapes where the cyber criminals always find lucrative methods to bait the victim. Methods used can vary, depending on the target nature. Organizational employee's phishing campaign may vary from consumer phishing attempt. Although they share similar attributes, customization is required to make it more believable and attractive to bait the victim.

During the Corona Virus (covid-19) outbreak, society is encouraged to stay up to date on the development of Covid019 and to what the government is issuing in relation to plans of control and isolation along with public health announcements. Cyber criminals spares no time to leverage such situation for their own benefit. Cyber criminals are exploiting the (Covid-19) pandemic through the deployment of crafted Electronic and digital phishing campaign, which poses as legitimate (public announcements, medical or health organizations, news feed, official applications or false advertisements and fake promotional offers) all in the aim to steal victim's private information and violate their privacy. The Banks, Netflix, YouTube, google, WhatsApp, coffee, mobile operator, insurance renewals, banking services, bills payment links, health apps, etc has been targeted during and utilized to conduct phishing attack during covid-19 (Schools, n. d). Also, many phishing emails are relatively rudimentary and sent to thousands of potential victims. However, there are some that are crafted specifically high value targets (victims), on attempt to obtain privileged information or gain access to device or networks for further process.

The below are example of the ongoing attacks during the COVID-19 pandemic as mentioned above



Source: (Exchange, n.d.)



Source: (Break, n.d.)

- *New Malicious Covid-19 status update Apps.*

While the covid-19 Pandemic outbreak and the recommendation of social distancing from the world health organizations (WHO), Conferencing / Meeting applications have become very popular and that have interested cyber criminals to focus their attacks and leverage any potential weaknesses on the applications to exploit sensitive materials.

- *Malware*

Malware is a malicious software, designed to cause harm and damage to the infected machine (computer, server, smart phone or any digital devices) malware include all variants of macro viruses, Worms, viruses and Trojans to grant the attacker access and take control of the infected system remotely.

- Ransomware — is a type of malware that blocks user access to their content either by method 1 locking the system or method 2 by encrypting the hard-drive files and making it difficult to recover or access the system without the decryption key unless a ransom is paid.
- .exe File infector — is one of most common method of infraction used by cyber criminals, where the virus find an executable host (.exe) and infect by attaching itself to be part of the executable code. Consequently, when the file is activated and run, the virus will also be activated and run on the victim machine or device. These days, the mobile operating systems have been the main target for such an attack and more such infected apps are being hosted online.
- Macro viruses —this kind of viruses specifically made to infect popular and daily use applications such as Microsoft products (Word or Excel) or similar products. Macro functionality is aimed to save the user time by initiating a routine work that is frequently carried by the user manually, however cyber criminals have attempted to abuse this functionality by creating viruses that is mimicking macro routine but maliciously to infect and spread.
- Trojans — a Trojan horse in the world of technology comes in a form of an application or legit program that looks and acts useful or harmless. However, there are a number of hidden malicious functionalities, which operates within the shell of the legit or useful tool / program. Trojans regarded as advanced malware, due to its ability of being a multi-tasking tool, for the cyber criminals. Trojans enable cyber criminals to violate the victim's (availability, integrity and confidentiality) data. It has the ability to be used as remote application terminal or eavesdropping or interception tool.
- Logic bombs — A malicious code that is attached to any application, so it can be triggered by a specific condition, usually in a pre-determined date and time.
- Worms — Worms are self-contained programs that propagate across networks and computers, commonly via email attachments that can result in slow network functionality to a full scale of denial-of-service attacks against all machines within the infected network.
- Malvertising – is a type of attack, where cybercriminals attempt to infect legitimate online advertisements with malicious codes, to redirect victims / users to malicious websites.

- *Drive-by attack*

As the title indicates, users are falling as victims from just by browsing the internet and exploring different kind of websites. Users may not need to interact with website by clicking or activating a download link. A drive-by download can take advantage of the lacking of critical and security updates to the browsing app or operating system, which will lead to abuse security flaws by cyber criminals. Some websites are insecure due to lack of Hardening from the webmaster or it has been purposely left unsecure by an attacker or cybercriminals who utilize the domain name to attract and bait visitors. Cyber criminals abuse the insecure

(domain / websites) and plant a malicious script to install malware directly onto the visitor machine or device, or it might re-direct the user to another website, which is under control of cybercriminals. To protect from such a threat, users are advised to always

- Update their systems,
- Avoid visiting unknown domains,
- Keep their digital footprint to minimum, to avoid being a victim.

- *Password (Recovery / Update) bait*

During the pandemic of covid-19 , the society have been bombarded with a lot of malicious requests, one of them is the password reset / update bait, where the user (receives an email or while visiting an infected website) is been prompted to update or reset his password. While doing so in an infected website, cybercriminals will acquire the latest password of the victim and that will compromise all of his accounts on social media or businesses, especially where the user is using the same password for all.

2. CONCLUSION

This paper have looked at the most common cyber-security threats and attacks on society via exploiting the digital and technology illiteracy which cyber criminals disrupt and compromise information and digital assets for their malicious gain. As have been indicted cybercriminals, don't spare any occasion or assaults technique from simple malware infection, interception, password guessing and brute forcing to most advance social engineering methods, all to gain unauthorized access to personal / corporate information and data.

To successfully mitigate, against such threats, requires a deep understanding of the society background component, to study the development, structure, and functioning of the specific society, as each society have different background and acceptance of use and trust of digital technology, which leads to the need of a study on Digital sociology. Digital sociology will look in to understanding the use of digital technologies as a part of everyday life and how technologies affect human behavior and influence the social life in digital space. One thing for sure, that the modern era is making a change within the society and sooner or later the society will have to fully adopt to the digital life and become digital citizen within digital society. The need to learn and improve on society literacy have become a necessity and way of life, without which the society will be left behind and they will be an easy target for the cyber criminals leveraging the ever-changing technology to their malicious gains. Cyber Security Training and Awareness for the society have become an essential approach on reducing the cybercrimes and it should be ongoing in the form of national campaigns to remind the society of advanced persistent threats that poses serious risk to modern society.

3. REFERENCES

[1] Amgad S D. Khaled, Salma Ahmed, Mosab I Tabash, Eissa A. Al-Homaidi, Mohammad Imtiaz Hossain (2019).The Impact of Technological and Marketing Innovations on Retailing Industry: Evidence of India. Journal of Reviews on Global Economics,2019, 8, 948-957

[2] Break, N. (n.d.). *watch-out-for-coronavirus-phishing-scams*. Retrieved from News Break: https://www.newsbreak.com/news/0O0yY669/watch-out-for-coronavirus-phishing-scams

[3] Badar Mohammed Al Mughairi, Haitham Hilal Al Hajri, Mohammad Imtiaz Hossain, Dr Asif Mahbub Karim. Crypto jacking a Technique to Leverage Technology to Mine

Crypto currency. International Journal of Academic Research in Business and Social Sciences, 9(3), 1210–1221.

[4] Badar Mohammed Al Mughairi, Haitham Hilal Al Hajri, Dr Asif Mahbub Karim & Mohammad Imtiaz Hossain (2019). An Innovative Cyber Security based Approach for National Infrastructure Resiliency for Sultanate of Oman. International Journal of Academic Research in Business and Social Sciences, 9(3) 1180–1195.

[5] Exchange. (n.d.). *https://exchange.telstra.com.au*. Retrieved from Telstra Exchage: https://exchange.telstra.com.au/watch-out-for-coronavirus-covid-19-phishing-and-malware/

[6] Yaser Alraei Alnekhaira Buti Alshamsi, Oo Yu Hock, Asif Mahbub Karim, Mohammad Imtiaz Hossain (2019). Developing a Framework on Performance and Challenges of Strategic Management Information System: A Case study on Ministry of Interior, UAE. International Journal of Academic Research in Business and Social Sciences, 9(5), 633 – 646.

[7] Schools, M. C. (n.d.). *Montgomery County Public Schools.* Retrieved from Montgomery County Public Schools: https://www.montgomeryschoolsmd.org/departments/techlit/docs/Definition%20of%20Technology%20Literacy.pdf