Data Security and Privacy in Times of Pandemic

Luis Fernandes

Lusófona University, Porto - Portugal
a21805177@mso365.ulp.pt

Abstract. Our present is marked with the corona virus appearance, which lead to a worldwide pandemic situation declared by the world health organization. This situation leads to several different measures to prevent the virus from spreading, which includes online classes from schools and universities, homeworking in various organizations among a lot more of other measures. The data security and privacy are a matter that always concerns organizations and all the general public who uses internet. In these days that matter worries double or triple because most of this organizations were not prepared for this situation and most of them had to rush and made changes on their network to keep working and keep making money. For hackers this is a great opportunity to strike, make damage and profit from that. This paper will present several risks that the pandemic brought along in terms of cybersecurity. This paper will also show some possible preventions to these risks and responsibilities from several organizations that provides important services, that will keep our privacy and the data safe from intruders. This paper will also see some examples that happened during these times and what learn from those examples.

Keywords: Pandemic, Cybersecurity, Riscks, Preventions, Data security, Privacy.

1 Introduction

The coronavirus impact on the world was so big that the world health organization had no other options then declaring pandemic situation. This happen on 11th March 2020 [1] and forced governements and organizations to take measures, that include closing countrys, citys and curfew measures. Organizations and the population had to adapt to this measures wich revealed some vulnerabilities and opportunities for hackers to strike. Since the appearence of internet and it's integration on our lifes,work and in pretty must everything, the data security and privacy has been a consourne. This consournes increased because organizations were not prepared to make this changes, and were forced to maked them quickly in addiction this virus is new and the information about it was not transperant and a lot of wrong information was circulanting on the internet. Data security means protecting our digital data, from those who, without access, get our information, stored on the digital world, commonly known as hackers. This is a responsibility from the companies where we store our data, but it's more our responsibility then them, because most of the times we are the ones who give access to

10.11228/dpsc.03.01.003

that people without realising it. This happens because people don't take serious this matter and facilitate, thinking that the problems envolving this subject only happens to others. When we talk about data security problems, we talk about cyber attacks and data breachs. Data security is linked with privacy, because if we don't take data security serious and we see our information leaked this affects our privacy. On this report, will be analyzed the trend of cyberthreats during the covid-19 pandemic, defining the most common threats, showing some examples about them and how to prevent it. Further on this report will be explored the teleworking subject, the concerns and measures to improve cybersecurity.

2 Most common cyberthreats during covid-19 pandemic

A cyber attack is an attempt to change or disturb the three principles of cyber security, confidenciality, integrity, availability. Confidenciality means restricting access and share of the information on the system. Integrity means protecting the information from being changed or destroyed. Availability is keeping the system available for those who have access to it and unavailable for those who don't have access or not logged into the system. Inevitably, the pandemic lead to an raise on the use of computers and internet, this was a gold opportunity for hackers. This is a challenge for engineers who are responsible to keep systems safe, increasing data security, and people, by protecting their privacy.

2.1 Trend of cyberthreats

On the previous years, this cyber security challenges were already tough for engineers, because tecnology keeps changing, hackers keep evolving and it keeps being an exhaustive task with hackers only needing to find one vulnerability and engineers need to try find all vulnerabilities and keeping it from becoming a threat. Currently the challengs are even harder due to this virus and the necessaries measures that lead to an increase and change to the trend on the cyber attacks. According to the FBI Internet Crime Complaint Center (IC3) cyber attacks have increased with the pandemic [2]. The best way to protect from cyber attacks is to work from the organizations with strong security policies, but the best way to protect from the virus is to stay home where the security policies are weaker [3]. This balance is hard to manage and makes a big vulnerability for the organizations who saw their systems very vulnerables for hackers to strike.

Top cyberthreats 2019-2020	Trend
1. Malware	---
2. Web-based attacks	
3. Phishing	
4. Web application attacks	
5. Spam	

Table 1. Top cyberthreats 2019-2020 [4]

Following this report the covid-19 pandemic had direct impact on the changes from the previous years [5]. As mentioned this crisis lead to several changes, this changes alone are already significant and have a big impact on making systems vulnerabels to strangers. But this changes came with other problem, time, systems had to be adapt quickly because the covid-19 doesn't wait and every day more and more cases were detected. Making this changes quickly are risky because the probability of bringing other vulnerabilities to the table are big, also mistakes could happen and the impact won't be only on the system, this could implate all the organization. Phishing was one of attacks that went up on the ranking from the previous years [5]. The miss information and the fast appearance of the virus made an opportunity for hackers to profit from this social engineering attack. Hackers impersonated hospitals and other entities/business using possible fake cures to the virus [6], for example. Even the world health organization was impersonated by hackers on the hunt for information. These hackers have multiple intentions but the major one revealed on the report was for financial matters [4].

2.2 Definition and examples of the most common cyberthreats

To prevent a cyber attack is important to know all the different attacks, knowing how they work is the first step to prevent them from happening and affecting our systems.

2.2.1 Malware

Malware is the most common cyberthreats out there it comes in form of malicious software. On malware we include cryptominers, viruses, ransomware, worms and spyware. Hackers have a lot of intentions on attacking a system but the most common objetives are information or identity theft, espionage and service disruption [4]. The main inicial point for this attacks are steal the e-mail protocols, but due to covid-19 was noticed an increase of malware embedded in interactive coronavirus maps and websites[7]. In the malware family the ransomware was one of them that increased with the pandemic. Ransomware is an attack that target multiple directories encrypting the information on those directories. The encryption methods are very complex taking

years to unencrypt the information. Usually hackers send an email to their victims asking for money in exchange for the password to unencrypt the directory. The problem with this malware type is that hackers keep asking for money threatening to encrypt data again. The coronavirus made more preassure on hospitals, health centers, education and public institutions. Hackers toke this opportunity and lunched ransomware attacks to this organizations since they can't afford to be locked out of their systems. Hackers thought that these organizations would pay due to this reasons [7]. According to ENISA malware report [4] 71% of organizations experienced malware activity that spread from one employee to another, 46,5% of all malware in e-mail messages found in '.docx' file types, 50% increased in malware design to steal personal data and 67% of malware were delivered via encrypted HTTPS connections. The following chart shows the numbers of successful attacks using URLs that include the terms "COVID" or "coronavirus".

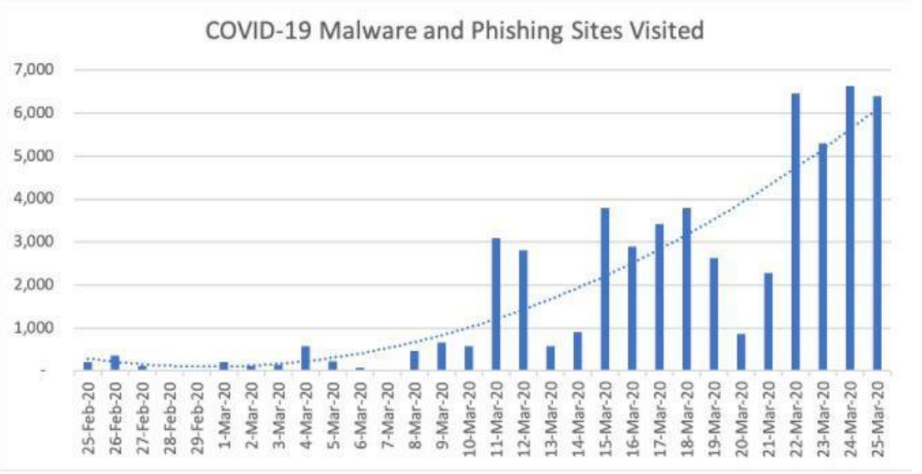

Fig. 1. COVID-19 Malware and Phishing Sites Visited [8]

Analysing the chart there is an exponential increase on the numbers on March 11, that was the day that World Health Organization declared the outbreak pandemic [1]. After that day, and has the trending line confirms, the number of successful attacks increased as the world population were searching for informations related to the pandemic.

2.2.2 Web-based attacks

On the past few years, the usage of web services have been increasing, due to the various advantages, including the no need to install software to have the same functions. The increased usage of this type of systems lead hackers to explore, find more and sophisticated ways to explore vulnerabilities on this systems. Web-based attacks are an attractive method since the increased usage of this kind of systems. There are multiple

attacks envolving this systems, for example malicious URLs or malicious scripts that directs the victim to a malicious website or even to download malicious content. Another common attack is to inject malicious code into a legitimate but compromised website to steal information, and other data. Other concern with these systems are the web browsers, although the browser are continuous updating and improving security measures, hackers always manage to find vulnerabilities. Different than previous years, the brute force attack increased on login systems in order to get on other users accounts. This kinda of attack affect the availability of web sites, APIs and could compromising confidentiality and data integrity. The most common attacks that happened on this systems are formjacking to steal user data, browser extentions and using online converters to download malicous software.

Description of the differents kind of attacks [4]:

- Formjacking - is an attack that injects code into legitimate websites. This attacks happen mostly on payment forms whos objective is to capture banking and other personal informations from the victims. When a victim is introducing their information on this infected forms, the injected code will also send this information to the attacker. The problem is that the original website works as intended, making it hard to know if this attack happened. With the pandemic the online shopping increased, making this type of attack a common one, taking advantage of the pandemic situation on the world.
- Browser extensions – There are several extensions, a lot of them are used because they help the users with functions that are not native on the browser. Anyone can make extensions, inclusive hackers making them with second intentions with the porpose of steal personal data and another types of attacks.
- Online converters – this is a common tool used by a lot of users, in most cases this tools ask the users to download the final data, converted. They use this to trick users and make them download malware to their computer. Hackers use this method to download various types of malware, but in the most cases ransomware is the most used type of malware [4].

During this pandemic another new cyber-attack was found, hackers used victims router more specifically the Domain Name Server(DNS) settings on D-Link or Linksys routers [7]. This attack opens the victims browser automatically, showing a notification from an malicious app. This notification tricked the victims to download an app called “COVID-19 Inform app”, this malware intended to steal browser cookies, stored passwords, browser history, transaction information and other data.

2.2.3 Phishing

Social engineering attacks on the past few years have been growing, becoming one of the most used attacks in the world. This kinda of attacks different than the others, it attacks the systems through the people instead of finding vulnerabilities and exploiting them or through very sophisticated and technical attacks. Phishing is the most common

attack on the social engineering family attacks. This attack is a fraudulent attempt to steal user data such as login credentials, credit card informations and other types of personal data. The majority of this attacks happens through e-mails, impersonating other entities or even the institutional e-mail of the organization. The objective with this e-mails is to persuade users to open malicious attachment or click on malicious URLs. For these tecniques make success hackers need to make a previous search to make appear the messages more authentic. This attack is based on emotional responses from victims. Even though most of the attacks use e-mails to connect with the victims the trend has been changing, appearing more and more cases using social media messaging for example via whatsapp. The methods are also changing and becoming more sophisticated, for example with the adoption of adversarial Artificial Intelligence algoritms to prepare and send messages. This attacks leads most of the time to unintentional insider threats. According to ENISA phising 2020 report, 26.2 billion of losses in 2019 with business e-mail compromise attacks, 42.8% of all malicious attachments were microsoft office documents, 667% increased in phishing scams in only 1 month during covid-19 pandemic and 32.5% of all the e-mails used the keyword 'payment' in the e-mail subject[4].

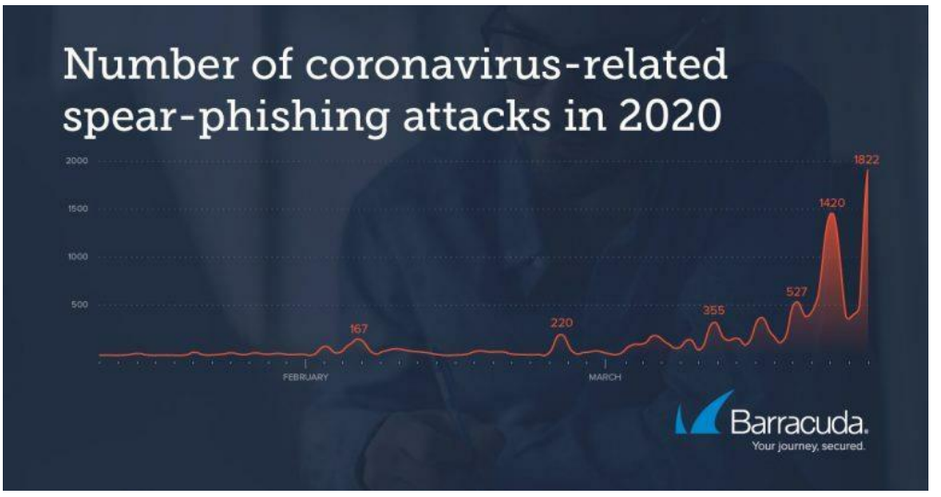

Fig. 2. Number of coronavirus-related-spear-phishing attacks in 2020 [9]


Subject: YOUR URGENT SUPPORT IS NEEDED
Charset iso-8859-1 *
Hello,

Good Day,

The death toll from the monthlong coronavirus outbreak has continued to climb in 27 Countries rising to 870 Cases.
New cases have surged by double-digit percentages in the past 14 days, with no sign of a slowdown,due to lack of individual consign.
More people have now died in this epidemic than in the SARS outbreak of 2002-3 in mainland China.
Health communities in the world have
Organized a Fund rising program (US$675 million is needed) to support the control of the epidemic in Noneremote areas in the world.
Let's save Humanity: Your support is needed.

WORLD HEALTH COMMUNITY BITCOIN WALLET FOR DONATION IS BELOW,

BITCOIN WALLET DETAILS: 1JTpX5T4ks9vfL1yaftL1Z3LisDdatkSQC

No amount is too small.

Thanks and Best Regards
Hugo Yeung
Support Committee Member
World Health community
+8606430910,+8037535467

Fig. 3. Example of phishing scam related to the covid-19 pandemic [9]

This example is one of the many e-mails that were sent to inumerous of people trying to delude people to make donations that are allegedly to help an found rasing program.

2.2.4 Web application attacks

This attacks are similar to the one explained above. Web application and technologies become a part of our reality by adopting different uses and funcionalities. This applications through the years are becoming more complex, consequently growing the challenges to keep this applications safe and protecting the tree principles of cybersecurity. The common motivations with this attacks are financial or reputation damage and theft of critical or personal information. This services depend mostly on databases to store information. There are two big types of attacks on this systems, SQL (responsible for data bases) injection and Cross-site scripting (XSS) [4].

- SQL injection – This is a type of an injection attack, making it possible to execute SQL statements. These statements control a database server and this vulnerabilities bypass the application security measures. Hackers most commonly uses forms to input SQL statements, and possibly returning a complete database, compromising the confidenciality and integrity of the information [10].
- Cross-site scripting (XSS) – This is a client-side code injection attack. The hackers aim is to execute mailicious code on the victims browser, including the malicious

code in a legitimate web application. The common objective of this code injection is to steal the victims cookies, that has stored sessions, that can be used to get on the victims accounts [11].

According to ENISA Web applications report 20% of companies and organizations reported DDoS attack on their application services on a daily basis, 52% increase in the number of web application attacks in 2019 compared with 2018 and 84% of observed vulnerabilities in web applications were security misconfigurations [4]. With the pandemic hackers used the applications made to inform and give statistics to attack and profit from this world situation.

2.2.5 Spam

Spam consists of sending unsolicited messages in bulk. This is considered a cyber attack threat when used as an attack vector to distribute or enable other threats. Receiving spam is inconvenience, but it may also create an opportunity for a hacker to steal personal information or install malware. The most used way to send this messages is through e-mails. The difference between phishing and spam is that phishing is a social engineering technique that aims to steal user information and spam is just sending unsolicited e-mails to a bulk list. Phishing campains most of the times use spam techniques to distribute the messages. According to ENISA Spam report 85% of all e-mails exchanged in April 2019 were spam, 13% of data breaches were caused by malicious spam and 83% of companies were unprotected against e-mail-based brand impersonation. The covid-19 opened new doors, in middle February 2020 only a few hundred covid-19 attacks per day were reported, but on March 2020 more than 2500 attacks were happening per day [4]. One organization that was very inpersonated by hackers was the WHO (world health organization), the attackers used an e-mail such as coronavirusfund@who.org. The official website of the WHO is www.who.int , it ends with an .int different than the .org used by hackers.

2.3 How to prevent this cyberthreats

Every case is a case and for that reason there are different measures to prevent this cyberttacks from happening. But there are some common measures to prevent this attacks, this measures should be adopted on organizations and also on a personal level to secure and protect the information. One vulnerability that every organization has in common are the people, the system could be well protected but the people is always a concern because if one person is not responsible, hackers could exploit that and bypass security levels, even if the system is well protected. To prevent this from happing organizations and governements should countinue with formation lectures and campains to teach and show what this attacks can do and what precautions should they take. A most common problem is that people don't take this matter serious and keep doing the same mistakes, until something bad happen.

2.3.1 Malware

- Implement malware detection for all inbound/outbound channels, including email, network, web and application systems in all applicable platforms.
- Inspect the SSL/TSL traffic allowing the firewall to decrypt what is being transmitted to and from websites, email communications, and mobile applications.
- Establish interfaces between malware detection functions and security incident management to establish efficient response capabilities.
- Use the tools available for malware analysis for sharing malware information and malware mitigation.
- Develop security policies that specify the process to be followed in the event of infection.
- Understand the capabilities of various security tools and develop new security solutions. Identify gaps and apply the defence-in-depth-principle.
- Employ mail filtering for malicious e-mails and remove executable attachments.
- Regulary monitor the results of antivirus tests, and keep those up do date.

2.3.2 Web based attacks

- Update internet browser and related plugins to keep them up to date and patched against known vulnerabilities.
- Make sure that endpoints and installed software are updated, patched and protected.
- Isolate applications and create a sandbox to reduce the risk of drive-by-compromise attacks.
- Websites owners, should hardening servers and services to mitigate web-based attacks. This includes controlling the version of the content scripts as well as scanning locally hosted files and scripts for the web server or service.
- Restricting web-based content is a technique to protect against this attacks. Facilitating tools such as ad blockers or javascript blockers will decrease the possibility to execute malicious code.
- Monitor web e-mail and filter content for detecting and preventing the delivery of malicious URLs and files/payloads.

2.3.3 Phishing

- Educate staff to identify fake and malicious e-mails and stay vigilant.
- Consider the use of a security e-mail gateway with regular maintenance of filters.
- Apply security solutions that use machine-learning techniques to identify phishing sites in real-time.
- Disable automatic execution of code, macros and preloading mailed links at the email clients and update them.
- Implement one of the standards for reducing spam e-mails, such as SPF, DMARC and DKIM.
- Use secure e-mail communication using digital signatures or encryption for critical information.

- Do not click random links, especially short links, checking always the domain name of the websites.
- Activate the two factor authentication to protect the accounts.

2.3.4 Web application attacks.

- Use input validation and isolation techniques for injection type attacks.
- Implement web application firewalls for preventive and defensive measures.
- Incorporate application security processes into the application development and maintenance life-cycle.
- Restrict access to inbound traffic for required services only.
- Deploy traffic and bandwidth management capabilities.
- Perfom vulnerability and risk assessments before and during the web application development.
- Conduct regular penetration testing during implementation and after deployment.

2.3.5 Spam

- Implement content filtering to locate unwanted attachments, mails with malicious content, spam and unwanted network traffic.
- Regular update the hardware, firmware, operating system and any driver or software.
- Avoid logging into new links received in e-mails or SMS messages.
- Use a secure e-mail gateway to regulate and automate maintenance of filters.
- Disable automatic code execution, macro enabling, preloading of graphics and mailed links.
- Regularly update whitelists, reputation filters and the real-time blackholeList.
- Use AI and machine learning for anomaly detection checks.

3 Teleworking and cybersecurity

There were inumerous measures taken by the governments across the world, according to the covid-19 numbers on their respective countries. But among all the measures there was one that almost every contry used, all the population needed to be in confinement. This lead to a major economy problem to pretty must every country if the population needed to stay home, how did the organizations work ? The organizations had no choice and as recommended by the WHO people had to start working from home, teleworking. The term teleworking before the pandemic was becoming popular but lot of organizations had issues implementing it. Most of organizations administrators have concerns letting their employees working from home, because it is hard to supervise and keep track on worked hours and satisfaction. Administrators had to put uncertainties aside and implement this measure. Another problem with the teleworking were the systems, if before the pandemic a lot of organizations were

already attacked, with teleworking the probability to be vulnerable was even higher. This implicates, private documents, messages, and other informations to be on the internet in order to communicate with other employees and with the applications. If it is hard to protect the information inside the organization with complex cybersecurity policies, engineers had a bigger problem in their hands to make this work without compromising cybersecurity. Information technology devices at home are generally perceived to be poorly configured compared to the work environment IT devices hence the IT devices at home are highly prone to cyber attacks especially due to these measures [12]. With employees on their homes, their network and their personal machines hackers can take advantage of the unsecured off-site routers, modems, unsecured network devices and poorly configured home network devices to exploit the vulnerabilities associated with teleworkers and compromising the security of the organization. That said its fair to say that organizations and people where not ready for these measures and because of that data security and privacy could become compromised.

3.1 Major security concerns with teleworking

As mentioned the teleworking presented IT engineers a lot of challenges, like those below, in order to protect the organization information [13]:

- Lack of physical control;
- Unsecured networks used for remote access;
- New threats for organizations through allowing external unsecured access to sensitive resources;
- Teleworkers may be using their own unstructured and unsecured resources to access their organizations valuable resources;
- The security measures assumes individuals uses computing devices from their employers wich is not applicable in all cases;

3.2 Measures to ensure data security and privacy with teleworking

To protect the organization from intruders and keep working using telework, the organization should take some measures like the ones below [13]:

- Developing and enforcing a telework security policy, such as having tiered levels of of remote access;
- Requiring multi-factor authentication for enterprise access;
- Using validated encryption technologies to protect communications and data stored on the client devices;
- Ensuring that remote access servers are secured effectively and kept fully patched;
- Securing all types of telework client devices, such as desktop and laptop computers, smartphones and tablets against threats;
- Train employees on cybersecurity in order to protect the organization;

4 Conclusion

Before the covid-19 pandemic data security and privacy were already a battle between hackers and engineers, the battle was not easy and the appearance of this virus was bad for the general world population health but also bad for the data security and privacy, with a lot of new attacks possibilities for hackers to explore. Helped wih the little time that engineers had do adapt the systems to the measures taken by governments and organizations, hackers profited a lot from this situation. Important now is to keep improving the security policies and hoping for this situation to end. It is also important, when this ends, to make more studies about the real problems that this situation brought and analyze what could be done better and learn from that and hopefully if something similar happens again we are prepared to face these kind of challenges.

References

1. Declaration of pandemic situation by WHO, https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020, last accessed 2020/11/06.
2. FBI public service announcement, https://www.ic3.gov/Media/Y2020/PSA200401, last accessed 2020/11/06.
3. André Barrinha.: Cibersegurança em Tempos de Pandemia. In CIBERSEGURANÇA E CIBERDEFESA EM TEMPOS DE PANDEMIA. IDN 2020.
4. ENISA Threat Landscape.: List of top 15 threats, From January 2019 to April 2020.
5. ENISA Threat Landscape Report 2018.: 15 Top Cyberthreats and Trends, January 2019.
6. Advisory: Covid-19 exploited by malicious cyber actors, https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory, last accessed 2020/11/11.
7. Navid Ali Khan, Noor Zaman and Sarfaz N. Brohi.: Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. ResearchGate (2020).
8. Sophisticated COVID-19–Based Phishing Attacks, https://www.menlosecurity.com/blog/sophisticated-covid-19-based-phishing-attacks-leverage-pdf-attachments-and-saas-to-bypass-defenses, last accessed 2020/11/25.
9. Threat Spotlight: Coronavirus-Related Phishing, https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/, last accessed in 2020/12/06.
10. What is SQL Injection (SQLi) and How to Prevent It, https://www.acunetix.com/websitesecurity/sql-injection/, last accessed in 2020/12/06.
11. Cross-site Scripting (XSS), https://www.acunetix.com/websitesecurity/cross-site-scripting/, last accessed in 2020/12/07
12. Arnold Mashud Abukari and Edem Kwedzo Bankas.: Some Cyber Security Hygienic Protocols For Teleworkers In Covid-19 Pandemic Period And Beyond. 4, April-2020
13. Karen Scarfone, Jeffrey Greene, and Murugiah Souppaya.2020. Security for Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Solutions. ITL BULLETIN MARCH 2020.
14. Alya Hannah Ahmad Kamal, Caryn Chuah Yi Yen, Mah Hui Ping and Fatima-tuz-Zahra. September 2020. Cybersecurity Issues and Challenges during Covid19 Pandemic.
15. Bernardi Pranggono and Abdullahi Arabo. 2020. COVID-19 pandemic cybersecurity issues.