International Journal of Advanced Engineering Research and Science (IJAERS)
Peer-Reviewed Journal
ISSN: 2349-6495(P) | 2456-1908(O)
Vol-8, Issue-8; Aug, 2021
Journal Home Page Available: https://ijaers.com/
Article DOI: https://dx.doi.org/10.22161/ijaers.88.27

Covid-19 effects on cybersecurity issues

Thiago José Ximenes Machado[1], Luís Borges Gouveia[2]

[1]Technologist in Data Processing; Bachelor in Law; Post-Graduated in: Computer Networking; Digital Forensics and Computer Forensics (in progress); Criminal Law and Criminal Procedural Law; Criminology; Criminal Sciences; Public Safety Policy and Management; Electronic Law; Constitutional Law (in progress) Master in Criminology and PhD in Information Science (in progress) - Fernando Pessoa University - Porto City (Portugal).
[2]Luis Borges Gouveia. Completed the Academic Title of Aggragate in 2010 by the Universidade de Aveiro and the Doctorate in Computer Sciences in 2002 by the Lancaster University (United Kingdom) and the Masters in Electrotechnical and Computers Engineering in 1995 by the Universidade do Porto. Full Professor at the Universidade Fernando Pessoa.

Received: 02 Jul 2021,
Received in revised form: 08 Aug 2021,
Accepted: 15 Aug 2021,
Available online: 21 Aug 2021

***Keywords*— Pandemic, Cybercrimes, Vulnerable, Cybercrimes, Technology, Internet, Cyberspace.**

***Abstract*—** *This scientific initiation article will bring up current and very relevant questions about the effects suffered in the virtual world after the announcement of a pandemic, with regard to the growing number of crimes committed by virtual means, considering that the use of the internet for practically any and all daily activities became mandatory. We will show the activities that needed to adapt to the new reality, as well as the increase in cybercrime that came to affect, in particular, those whose expertise and technological knowledge do not match reality. We will also talk about the victims of these crimes and conclude with a cybersecurity protocol which can be applied to minimize risks and hinder the actions of opportunistic offenders.*

I. INTRODUCTION

In the 21st century, the world began to live with a somewhat limited and dark reality, making people, even those with no affinity for technology, feel the need to use digital equipment, especially those connected to the Internet. Such resources minimize idleness, facilitating the maintenance of work, educational, and other activities.

We will show the methodology that was used to develop the research for this paper and why we decided this was the best method.

First of all, we will discuss the use of technologies associated with the Internet in times of pandemics, where the potentialization of online services and the increase in the number of hours of access to the world wide web have awakened in cybercriminals an unparalleled opportunity to practice their crimes, often taking advantage of the vulnerability and lack of knowledge of Internet users.

Next, we will address the issue of criminal opportunity in the face of the new global scenario scenario, namely, the officialization of a pandemic. In this aspect, we will make a brief analysis of how cybercriminals have taken advantage of the virtual services that have become part of people's daily lives, in order to put into practice their cyberattacks and obtain illicit profits.

In the third part we will expose the criminal opportunity in the face of the new global scenario, since people, due to social isolation because of the pandemic, had the need to resort to technological resources connected to the Internet to perform their daily and work activities, becoming more vulnerable to cybercriminals who took advantage of the moment to practice cybercrime.

Continuing the subject, the fourth part brings a specific explanation about a work model called home office, which consists of obeying social isolation, making company employees work remotely from their own homes. However, we will show that due to the habit of not practicing cybersecurity protocols, they ended up being targets for cybercrimes, which brought irreparable damage to companies and organizations.

The fifth part of the article will bring to the reader a reflection on the greater vulnerability of children and adolescents in face of the greater time spent accessing the Internet in times of pandemics, since this excess, considered as something normal by the vulnerable, can bring about a digital addiction and thus lead to a series of problems, both in terms of mental health and physical integrity.

In the penultimate part, we will address a very relevant point that sometimes gets forgotten, that is, the victim being considered guilty for the cybercrimes he/she suffers. We will show that most victims of cybercrime do participate, but we cannot blame them for not having the expertise to enter the virtual world.

The last one will bring the reader two tables of protocols that can be used, both in the enterprise and in the home, to minimize the chances of being being targeted by cybercriminals.

We will end with a reflection on the consequences brought about by the worldwide spread of a deadly virus called Sars-cov-2, or simply COVID-19 or Coronavirus, which besides causing changes in real life, has brought about major changes in the activities developed in the virtual environment, that is, in cyberspace.

II. METHOD

The methodology applied was qualitative, characterized by the analysis of other articles and official documents that bring information related to the theme addressed.

From this content, extremely current, we can describe the modification which begins with the user's behavior, as well as the delinquents who, taking advantage of this pandemic moment and of people's great vulnerability, have invested in the practice of cybercrime.

The study relied on a considerable volume of scientific articles, so that the necessary knowledge was extracted from each one to develop relevant information to compose our scientific research.

Based on the explored content, we extracted several information ranging from the association of Internet use in times of pandemic to the main resources to minimize cyberattacks.

Finally, we show the conclusion that was drawn after the study and that will certainly contribute to society in general, since the connectivity, nowadays, reaches a large part of the world's population, regardless of social class.

III. RESULTS AND DISCUSSION

USE OF INTERNET-ASSOCIATED TECHNOLOGIES IN TIMES OF PANDEMIC

In face of the new scenario in which the world found itself, that is, the announcement of the spread of a virus called COVID-19, or popularly called the new CoronaVirus (Sars-cov-2), people had the need to adapt to changes in their lives, whether at home, in education, in the family, or at work.

The use of the Internet has become a more than essential tool, due to the prohibition of physical contact between people. Virtual communication has gained strength, so much so that all areas in which our lives are involved have needed to adapt, in order to reduce the damage caused by this dangerous and deadly virus.

The potential of the internet, especially social networks, has brought a series of benefits for people, as they feel the need to keep in touch with each other. Several activities have gained prominence in this current moment, lives have become a word of everyday life, where artists have found space to perform their shows, politicians run electoral campaigns, physical educators promote activities that can be performed at home, many run solidarity campaigns, and a series of entertainments that help to improve the psychological and physiological factor of those isolated by quarantine.

On the other hand, the media started to spread news of chaos and despair all over the world, and every day the news, whether on television or social networks, showed death and more deaths caused by COVID-19. And due to this excess of information, many have acquired anxiety and other psychological disorders. We can still highlight the misinformation, which leads to disbelief in science, with respect to epidemiological knowledge, as well as health guidelines, bringing more risks to the population.

Taking advantage of the intense flow that the World Wide Web is producing thanks to this new context experienced in pandemic times, the cybercriminals' attentions have turned to committing crimes practiced with the help of technological resources and equipment, making, in this moment of crisis, victims all over the world.

Due to people's desperation, and the anxiety to know how the pandemic scenario is, both globally and regionally, the evildoers began to create sites containing fake news and make available applications that had the purpose of showing viral maps, but behind these small programs, available for download, there was malware, responsible for the capture of various types of personal data.

Conferences through videos started to be used to shorten the distance between people, and for this reason the use of platforms such as Zoom increased, which fell victim to cybercriminals who discovered flaws and had access to the data of millions of users.

In Brazil we have the law 13.709/18 (General Law of Data Protection) that had its wording changed in August 2019. This, addresses the topic and provides administrative punishments to companies that do not take the necessary care to protect their users' data. Such objective is brought in the first article of this law, providing

This law provides for the processing of personal data, including in digital media, by natural persons or legal entities of public or private law, in order to protect the fundamental rights of freedom and privacy and the free development of the personality of the natural person.

We infer that technology was and is a fundamental ally for the continuity of daily activities, however, people need to be aware that the misuse of these tools can bring irreparable damage, be it to property or even psychological.

CRIMINAL OPPORTUNITY IN THE NEW WORLD SCENARIO

Even before it became a pandemic, the world learned that a deadly virus had started in China, and soon Internet users began to search for information on the subject on search engines. Thus, cybercriminals have already started to prepare for their attacks, based on the interests shown by the population in their searches.

It is important to highlight that with the family confinement that had been interrupted, the number of crimes against property and even the illicit drug trade had a considerable decrease. However, this new model of life has created a virtual refuge, that is, the cyber environment, which has its virtues and its dark side.

According to IBGE (Brazilian Institute of Geography and Statistics), there are currently approximately 220 million active smartphones in Brazil, considering that our population is around 211 million inhabitants. And using these, some services began to be operated in a more common way, such as delivery applications.

These applications have awakened criminals to lure their victims into giving them their credit card data and passwords, using a technique called phishing. This type of fraud is also used to issue fake bank slips, making users believe that they are really paying for a certain product or service, but that the amount is sent to an unknown account.

The Phishing technique has the help of another technique called Pharming, which is to direct the user to a fake site, but showing itself as a reliable copy of the original site. Thinking that he is accessing the real site, the user enters personal data related to his account, and has these stolen.

Still in this vein, a very relevant factor has been the high number of companies going bankrupt and others drastically reducing their staff. Thus, the number of unemployed people has grown, and the evildoers have taken advantage of this to lure and steal data from these people, by means of links leading to sites with false job offers, making them fill out forms with personal data, which would be stolen.

Google's official blog reported that more than 240 million spam messages were sent daily, containing the word COVID in their text, and these often directed users to the 42,000 web sites created from the beginning to the end of March (chart below), which use the same technique mentioned above to illegally capture data.

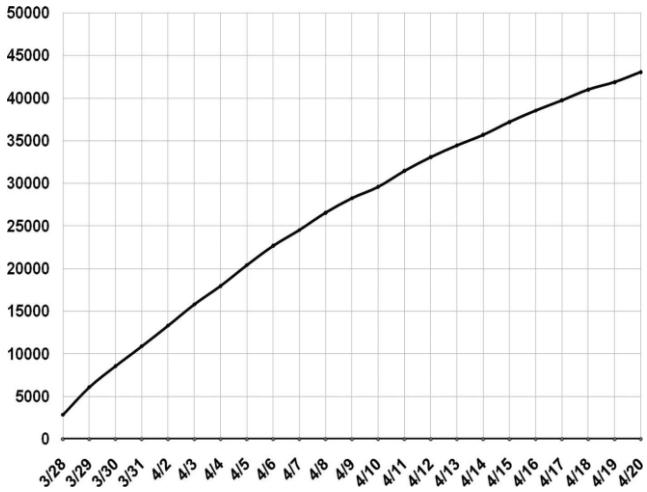

Fig.1: Cumulative number of COVID-related domains that have been registered.

Many were the fraud schemes employed by cybercriminals, characterized by the moment of desperation experienced by the world in a frantic search for the vaccine. Thus, the criminals requested contributions from Internet users so that it would be possible to create the vaccine against COVID-19, which in fact were nothing more than fraudulent gimmicks.

Another resource that has been used to negotiate products is the so-called e-commerce, where people advertise sales of the most varied things. Taking advantage of the data entered on these sites, the criminals manage, through social engineering, to trick the victims into providing codes that are sent to their cell phones, thus causing their WhatsApp application to be cloned, starting the crime of fraud, since they start asking the contacts for money, misleading the victim, because they pretend to be the owner of that account.

Due to the lack of expertise of Internet users, the social engineering technique succeeds in 80% of the scams that are applied. And the pandemic, without a doubt, has provided the ideal opportunity for cybercriminals to act, leading to a significant growth in cybercrime.

We deduce that after the WHO (World Health Organization) declared the pandemic, people started to use technologies more frequently and even unbridled, especially those connected to the Internet, since communication and physical contact became dangerous and even deadly. Thus, the barriers of distance and social isolation were minimized by virtual communications. However, along with this resource, came the problems, especially the increase in cybercrime.

THE RISKS OF HOME OFFICE FOR USERS WITH NO TECHNOLOGICAL EXPERTISE

Small and medium-sized companies were the ones that suffered most from the pandemic announcement, because, to avoid contamination among their employees, they had to take urgent measures, and, one of them was to adopt the work system called home office, which in its literal translation would be work at home.

According to the company Kaspersky, through its senior manager of social media Kaspersky - Brazil, says that "The bad news is that every time something big happens, cybercriminals take advantage of the opportunity", since employees were transferred from companies or offices to their homes without adequate protection for performing tasks over the Internet, making them easy targets to be affected by ransomware.

In an analysis, the director of Kaspersky's global research and analysis team in Latin America states that

> What cybercriminals do is attack a hospital or any other entity to steal information. Later, they encrypt it and threaten to make the stolen data stolen data public. Ashamed and afraid of the distrust and fines generated security incident like this, most organizations give in to blackmail.

He further adds "These groups are responsible for attacks on hospitals and healthcare organizations, critical services during this pandemic, but they also target banks, insurance companies, law firms, accounting firms among others and are here to stay."

For experts, these attacks have occurred with great frequency in Latin American countries, especially in Brazil, which had an increase around 350% in the first quarter of 2020, and this is due to the factor of bad corporate online access habits, of which, three stand out: use of weak passwords, use of pirated programs and lack of application of software patches.

Besides ransomware and phishing attacks, there are many other types of cybercrime that can be committed, such as data destruction, fraud, and system downtime, among others. According to specialized reports, these will cost the world $6 trillion by 2021.

Another malware widely used is the keylogger, which after being installed on the victim's computer, captures the information typed and sends it to the criminal's e-mail, as a recent example of this type of file infected with such a malicious program, we have the Eeskiri-COVID-19.chm (Estonian Rules), which apparently would show sites that help combat COVID-19.

We find that cybercriminals' expertise and opportunism are always on alert. Just as companies have visualized a way to keep their services running in the period of social isolation caused by the pandemic, so too have the criminals perfected their malicious techniques. Therefore, we must emphasize that cybersecurity protocols must always be prioritized before implementing any and all activities that involve technological resources, especially those that are directly connected to the World Wide Web.5.

THE INCREASED VULNERABILITY OF CHILDREN AND ADOLESCENTS TO LONGER INTERNET ACCESS DURING PANDEMIC TIMES

As everything had to reinvent itself in times of pandemic, education could be no different. Teachers have

been forced to use new teaching methods, even though many have never had contact with online classes. On the other hand, students had to adapt to a new classroom model, that is, distance learning, which for many is very difficult to learn this way.

Besides classes, children and teenagers have an excessive amount of time using Internet-connected technologies, and due to the large amount of information about the deadly virus, these vulnerable people can acquire a high level of stress and anxiety, since many are the conflicts that can torment their minds, which can lead to depression.

For the professor and researcher Gustavo Lins Ribeiro, the Internet with its multiple activities can provide a good or bad experience, bringing the following conclusion,

> The coronavirus pandemic is the first to be experienced in online time. The Internet, with its multiplication of the capacity of capillary communication, at the same time that it provides a global awareness, creates an expectation and paranoia in the expectation that the large numbers of sick and dead, supposedly defined in a millimeter daily, do not reach with the same intensity the places where we live.

The problem is even worse when these vulnerable people already have compromised mental health, because then the probability of idealization and suicide attempts increases. It is worth pointing out that excessive use can lead to some addictive disorders, such as cyber sex, net gaming, social networks, and others.

Another very imminent risk is that of being a victim of cyberbullying, as a result, especially for teenagers, of exposing their images with the objective of reaffirming an expectation of recognition before other internauts, and who knows, maybe even become famous as a digital influencer. However, constant criticism and insults can cause psychological damage and, not to mention, the configuration of crimes against honor.

Adolescence is a time of many discoveries, which may be accompanied by some psychological disorders, which can generate the desire for self-mutilation and even suicide, and the Internet, at this time, becomes a fertile ground for this idealization. A classic example is the challenge that became known as Blue Whale, where participants had to perform a series of tasks (challenges) and the last one was suicide.

In this same context of online challenges, in the current situation of the pandemic, where the product alcohol gel became known for being a way to eliminate the virus, they took advantage of the situation and created the "Alcohol Gel Challenge", where participants made videos inhaling, drinking, spitting the product into flames and even setting fire to their own bodies, i.e., extremely dangerous practices for health and physical integrity.

On the other hand, the criminals, using the innocence of children, began to create videos with children's cartoon characters, who communicated in a dissimulated and persuasive manner so that these vulnerable people would provide the credit card data of their parents.

We deduce that children and adolescents can become dependent on the use of technologies, especially those connected to the Internet, and that due to the scenario in which we are directly involved, social isolation associated with cybercriminals' traps can bring harm to both the vulnerable and their parents.

THE VICTIM BEING CONSIDERED GUILTY FOR CYBERCRIMES

In the criminal scenario, the victim plays an important role and should be the target of study, that is why we have victimology, which is a science that will study the role of the victim in crime. In the context of cybercrimes it is fundamental to analyze the behavior of those who have been targeted by cybercriminals.

Within the classification of victims we have: Completely innocent victim or ideal victim is the one who had no participation in the criminal action; Victim by ignorance or victim less guilty than the delinquent is the one who contributes in some way to the occurrence of the offense; Victim as guilty as the delinquent is the one whose participation in the crime is fundamental, i.e., he becomes a victim due to ambition, as much as that of the criminal; and Victim more guilty than the delinquent or provoking victim is the one who brings the blame to himself, i.e., he became a victim due almost exclusively to his own fault .

In Brazilian criminal law, the victim's behavior is taken into consideration when determining the penalty that will be attributed to the offender. However, if the victim is exclusively to blame, no penalty is applied, and the perpetrator is exempted.

As we have already studied, Internet users, especially teenagers, tend to behave inappropriately with regard to some conducts, making them partly to blame for

some of the crimes they have committed. However, we cannot blame the victim exclusively, since the criminal is someone else, and the crime cannot be justified by a possible "mistake" of the inexperienced, careless or uninformed internet user.

In many types of cybercrime, however, there is no participation of the victim, since his actions on the Internet are commonplace, and one fine day, what looked like a file sent by your bank, may be malware that will be installed on your electronic device, making you become a new victim of cybercriminals.

With the pandemic, digital communication networks have had to open up to accommodate a greater number of users, i.e. companies have had to provide access through remote tools, which are connected to the Internet. Thus, the vulnerability and amplification of risks inherent to cybercrime have increased considerably, and because of this digital acceleration in times of COVID-19 propagation, that the challenges related to cybersecurity techniques have multiplied.

With such network openings, the victims have also become more vulnerable, since, due to their lack of preparation for this new model of "virtual life", they are not very concerned about digital security issues or often rely on the structure offered by the companies where they perform their work activities.

We realize, then, that in most cases of cybercrime, the victim has a certain share of guilt, because his or her careless behavior when accessing the Internet comes as a real gift to cybercriminals, who are always on the prowl, waiting for the unwary and careless Internet users. On the other hand, we have the victims who do not contribute to the criminal action, having in their cases security flaws in the systems used.

CYBERSECURITY PROTOCOL

The use of any and all technology, especially those connected to the internet, want essential care so that this useful and practical tool does not become a hidden villain in a criminal scenario.

Cybersecurity, especially for ordinary internet users, never seemed so important, until they fell victim to the cybercriminals. And when it comes to organizations, whether public or private, this security that used to be important, is now extremely important and essential for the full functioning of their activities.

Let's start with the protection of personal computers that are used to surf the Internet and carry out everyday activities (bill payments, research, online classes, and others). In the following table we will show the main rules of digital security.

Protection Software	Antivirus and anti-malware programs must always be up to date and ready to detect threats.
Social Engineering	Guidance is the best weapon against this kind of attack. So it should be taught that passwords and other personal data should not be passed on to anyone via the Internet.
Education Protocol	It shows users at least the main types and techniques of attacks used by cybercriminals. These range from care when clicking on unknown links to the expertise in identifying the social engineering technique.
Security Policies	It consists of creating documents that address the policies to be followed to maintain better security. These range from monitoring to audits that will be performed on the organization's computers.
Password Manager	It is very important that users have distinct passwords for each system accessed, and that these passwords are strong, i.e. long and with several types of characters. And in order not to forget them they can use password manager programs.

As seen, it is of great importance that people, before entering the world of technologies connected to the World Wide Web, know the main concepts of security, because the terrain is very fertile for cybercriminals who take advantage exactly of this lack of knowledge to then reach their victims.

With regard to cybersecurity protocols that can be used by companies in this current scenario that makes the home office service available to their employees, we have a short list shown in the following table[1].

VPN (Virtual Private Network)	The VPN will create a tunnel, where data is encrypted, thus making it harder for intruders to decipher.
Authentication	It is important that all systems are

[1] ABUKARI, Arnold Mashud; BANKAS, Edem Kwedzo. *Some Cyber Security Hygienic Protocols For Teleworkers In Covid-19 Pandemic Period And Beyond*. Recovered in 18 de july, 2020, from https://www.researchgate.net/publication/341098664_Some_Cyber_Security_Hygienic_Protocols_For_Teleworkers_In_Covid-19_Pandemic_Period_And_Beyond.

	accessed through authentication, requiring strong passwords from the user.
Protection Software	Antivirus and anti-malware programs must always be up to date and ready to detect threats.
Social Engineering	Users should be advised not to give out passwords or any data without being sure that they are talking to the real technical support.
Password Manager	It is important that companies guide their employees to use strong and different passwords for each system accessed, thus making it more difficult for cybercriminals. Password management software can be used as a resource.
Firewall	The importance of using firewall systems, as a way to prevent the invasion of computers, closing the main communication ports used by the systems.

In analysis, we can infer that we all got to know a new world scenario that was changed after the pandemic was announced, thus, both people and organizations, public or private, had to reinvent themselves in order not to enter into an economic crisis and even the decree of bankruptcy. However, due to the short period of time that everything had occurred, there was not enough time to prepare the staff to deal with the new work method, which is the resources connected to the Internet.

IV. CONCLUSION

The pandemic scenario brought to the whole world a new vision of life, changing people's behavior in their daily lives, however, the purpose of this article was to show the influences and changes brought to cyberspace, that is, the impact caused in issues related to cybersecurity, considering that the time of access to the World Wide Web has grown in an exorbitant way.

Technologies, especially those connected to the Internet, are increasingly entering our lives, whether to facilitate daily tasks, for school learning, to automate work activities, for socialization and communication between people and peoples, or even for entertainment. However, of one thing we are sure, many can no longer live without these technological resources.

With the tragic announcement of the spread of the Sars-cov-2 virus, or popularly called the Coronavirus or COVID-19, many have been forced to use technological means as, perhaps, the only way out to continue with their daily tasks, and thus ensure, in times of crisis, the support for their families.

On the other hand, due to, many times, the lack of skills and habits with such resources, Internet users have become easy targets for cybercriminals, who take advantage of the moment and of their naivety to apply their techniques and thus ensure success in their criminal enterprise.

Starting from this premise, the subject of cybersecurity began to be more explored and even valued by those who never worried about it. Thus, security protocols had to be created with more rigor, since data integrity became paramount to ensure the full and safe operation of online services.

When it comes to children and teenagers, perhaps more important than cybersecurity protocols is to control the amount of time they spend using the Internet, since their exposure can bring about several harmful consequences, which may even irreversibly affect their mental health.

We conclude then that caution and safety rules should always be observed before diving so deeply into the virtual world, that is, cyberspace, since besides the many benefits it can provide, we have the harms it can bring to life, whether related to physical or psychological integrity.

REFERENCES

[1] ABUKARI, Arnold Mashud; BANKAS, Edem Kwedzo. *Some Cyber Security Hygienic Protocols For Teleworkers In Covid-19 Pandemic Period And Beyond*. Recovered in 18 de july, 2020, from https://www.researchgate.net/publication/341098664_Some_Cyber_Security_Hygienic_Protocols_For_Teleworkers_In_Covid-19_Pandemic_Period_And_Beyond.

[2] AHMAD, Tabrez. *Corona Virus (Covid-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity*. Recovered in 12 july, 2020, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3568830.

[3] AVAST. *O guia essencial sobre phishing: Como funciona e como se proteger*. Recovered in 12 de july, 2020, from https://www.avast.com/pt-br/c-phishing#topic-1.

[4] BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Recovered in 11 july, 2020, from http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

[5] DESLANDES, Suely Ferreira; COUTINHO, Tiago. *O uso intensivo da internet por crianças e adolescentes no*

contexto da Covid-19 e os riscos para violências autoinflingidas. Recovered in 17 july, 2020, from https://www.scielo.br/scielo.php?pid=S1413-81232020006702479&script=sci_arttext.

[6] DOMINGUES, Vinícius. *Em tempos de pandemia, é preciso ter muita atenção com os cibercrimes*. Recovered in 11 july, 2020, from https://www.conjur.com.br/2020-mai-13/domingues-cibercrimes-tempos-pandemia.

[7] GONÇALVES, Victor Minarini. *VITIMOLOGIA: CONCEITUAÇÃO E APLICABILIDADE*. Recovered in 17 de july, 2020, from https://jus.com.br/artigos/36073/vitimologia-conceituacao-e-aplicabilidade.

[8] GOUVEIA, Luis Borges. *Covid-19 e Desafios para a Cibersegurança num Tempo pós-Pandemia*. Recovered in 17 july, 2020, from https://www.idn.gov.pt/pt/publicacoes/idnbrief/Documents/2020/IDN%20brief%209%20july%202020%204%C2%AAvers%C3%A3o.pdf

[9] Jaiswal, M. (2021). Virus Origin and Evaluation with Data Analytics. *International Journal Of Creative Research Thoughts*, *9*(3), 6270-6280.

[10] JESUS, Helder Fialho de. *Ciberespaço e Mundo Físico – As Duas Faces da Mesma Moeda*. Recovered in 19 july, 2020, from https://www.idn.gov.pt/pt/publicacoes/idnbrief/Documents/2020/IDN%20brief%209%20july%202020%204%C2%AAvers%C3%A3o.pdf

[11] KASPERSKY. *O que é ransomware?*. Recovered in 11 july, 2020, from https://www.kaspersky.com.br/resource-center/definitions/what-is-ransomware.

[12] MALAVÉ, Mayra Malavé. *O papel das redes sociais durante a pandemia*. Recovered in 11 july, 2020, from http://www.iff.fiocruz.br/index.php/8-noticias/675-papel-redes-sociais.

[13] NAIDOO, Rennie. *A multi-level influence model of COVID-19 themed cybercrime*. Recovered in 09 july, 2020, from https://orsociety.tandfonline.com/doi/full/10.1080/0960085X.2020.1771222.

[14] RAHAL, Carla; TURRINI, Janaína; FIORESE, Urbano; FURTADO, Felipe. *Crimes digitais e prevenção em época de pandemia*. Recovered in 12 july, 2020, from https://cryptoid.com.br/banco-de-noticias/crimes-digitais-e-prevencao-em-epoca-de-pandemia/.

[15] RIBEIRO, Gustavo Lins. *Medo Global. Boletim n. 5. Cientistas sociais e o coronavírus.* Anpocs. Recovered in 14 july, 2020, from http://www.anpocs.com/index.php/ciencias-sociais/destaques/2311-boletim-n-3.

[16] RODRIGUES, Renato. *Brasil é líder em empresas atacadas por ransomware na epidemia*. Recovered in 11 july, 2020, from https://www.kaspersky.com.br/blog/empresa-brasil-ransomware-pandemia/15527/.