Data Security and Privacy in Times of Pandemic

David Marques

Lúsofona University of Porto, Portugal
davidmiguelmarques9@gmail.com

Abstract. During what it seems like a big revolution in our lives marked by the presence of this whole new pandemic, each and everyone's life is being put to the test! The covid-19 pandemic had a huge impact in the world and not a single person was able to escape the need to adapt facing this new reality. In continuous and accordingly to what was mention above, this paper will focus on reporting the changes brought by the virus *SARS-CoV-2* into our personal and professional lives. The goal is to emphasize the new lifestyle implemented and the consequences it brought, specifically in terms of the dramatic increase in cyber-attacks.

This paper will be based on real facts in order to contextualize the main theme and it will also put-on display impressive and unbelievable number data registered during this pandemic, focusing on its impact.

The covid-19 rebound in society caused a great threat in the cyber-security levels and for that motive this paper aims to elucidate the importance of good security methods and describes ways and procedures to avoid and react to the majority of cyberattacks that continue to take place during the outbreak of corona virus.

Keywords: Cybersecurity, Security Methods, COVID, Type of attacks during Pandemic, attack prevention

1 Introduction

During this trouble time, cyber security had one of the greatest challenges and it promptly carried out to become the most significant impact in the technological world in the present year. Security in its more informatic meaning was always an essential

10.11228/dpsc.03.01.002

area in the enterprise and companies world, as well as in peoples private lives but due to confinement this topic is now more present in our day-to-day lives than ever.

The goal is to emphasize the new lifestyle implemented and the consequences it brought, specifically in terms of the dramatic increase in cyber-attacks. Sarcastically and with a touch of humour and wordplay we could even say that this new virus allowed a great number of "virus" into our computers. We can surely assume that the pandemic and the lockdown created a huge culture shift in which people have become increasingly relaxed about screen time hours in comparison to life previous to covid-19.

During what seems to be a great revolution in our lives with the presence of this whole new pandemic, the lives of each and every one are being put to the test!

Not only is our health in danger, but also our personal data because during confinement time people spent more hours in front of their computer and the majority of them without any formation in the area. People used computers in order to stay in touch with friends and family but also for work purposes.

This tremendous mobilization to the front of the computer screen, gave the opportunity and the means for those with malicious intensions to launch more cyber-attacks.

With workplaces closed and all the employees working from home in the context of teleworking, the Security department of public companies and big enterprises had to set this operation in a quite rapidly manner by configurating the operations in a remote way. In general, nowadays people are working with unsafe devices which means the hackers can easily get access to companies information. In addition to this, the increased stress felt by the system and the gaps in the collaborative tools intensify the vulnerability to such attacks.

The increase number of cyberattacks happened inevitably because a great amount of companies and organizations didn't have any kind of preparation able to fight off and resist this pandemic. The strategy implemented by these major companies was to simply transport the computers from a safe workplace with the right configuration to their employees personal houses in order to allow them to work safely. Unfortunately, most of the companies focused only on the goal to keep the profit up and keep the work going, they didn't pay attention to the most important factor, the area of security, which has led to the action of several hackers who have managed to obtain much inside information which has put many institutions in danger.

During the course of this year the pandemic challenged, in an unmatched way, the health services and cybersecurity. As result of SARS-COV-2 the number of incidents was the highest ever seen, culminating with the loss of privilege information by several companies, putting them in risk not only in an economical way but also causing mental exhaustion.

Because of everything mentioned above my paper is going to focus on digital security in times of pandemic. It is a very actual theme with a worldwide reach that it is worth discussing in order to improve in the future. To make it more credible I am going to use scientifical references and real-life cases to bring in the humanity factor to highlight the must needed gain of awareness.

2 Pandemic and impact in world

The covid-19 pandemic had a huge impact in world, and nobody was able to live indifferent to that. The public health consequences of the pandemic have led to a sudden and significant gap in teleworking. Unexpectedly, millions of people and businesses around the world have radically changed their lifestyles by adopting the teleworking regime.

After a few months some people and companies revealed that teleworking was here to stay. We might say that this change brought both advantages and disadvantages.

We will start with the advantages of teleworking, which from a business point of view has reduced operating costs (employee travel, consumption, electricity). The company has achieved exponential environmental gains due to the reduction in traffic and the increase in the number of employees.

On a personal level the advantages of teleworking consist on having facilitated autonomy, flexibility and better work-family reconciliation. The increase in productivity has also been highlighted in analyses as there are no interruptions or distractions that occur while not in the workplace.

Regardless of this, not everything was a sea of roses when it comes to teleworking. The disadvantages began to be revealed as the days were passing and it emerged in an alarming way.

Remote work led to the disappearance of the boundaries between work and family life leading to abusive working hours. Social isolation and individualism at work have occurred in recent months and people have been deprived of face-to-face contact between friends, colleagues and family. This has led to an increase in communication electronics tools such as (Zoom, WhatsApp, Microsoft Teams).

In line with what has been mentioned above and according to what will be addressed more comprehensively in this paper, we will be concluding that the major disadvantage that was brought by this pandemic was in the area of security.

Teleworking has caused thousands of people to start working from home and it has made it easier for them to communicate and for organisations to keep the business going. Unfortunately, it is mandatory to look at the other side of the coin, which refers to the increase number of cyber-attacks. Especially, the remote regime brought more demands for closer monitoring. Like the pandemic if we are not careful, there is a constant exposure. The user, by being unprotected, makes it necessary to be in a constant observation regarding the integrity of the equipment that connects him remotely to the corporate infrastructure.

What happened with teleworking and what was evident in several companies were the vulnerabilities and threats duo to the present situation, which was impossible to predict, appearing unexpectedly. In a way. we can draw a positive balance from this pandemic which has made people more concerned and brought up a number of computer security issues to users and companies.

Organizations have achieved as much as possible in order to have their employees working efficiently from home, but in terms of security the biggest challenge falls on the employees themselves. They connect to non-secure Wi-fi networks, that most likely have no security measures at all, due to the fact that they probably never give it much thought and it actually makes it easy for the hacker to get on the network.

With several people teleworking and students learning online, this year 2020 has been marked by this pandemic. The confinement and intensity of the news coming to the TV and the excessive research made it difficult for people to distinguish the real from the so famous fake news. As a result, and because of the age we live in, people cling more than ever to the internet as entertainment/leisure and work time, causing Internet traffic to increase intensively.

The security landscape around the world has changed. The COVID-19 effect has been to decree social isolation in several countries in order to mitigate its spread. This adaptation was not guaranteed by many companies because they were not prepared both in terms of equipment and security.

As the days and months went by, it was noted that the gradual increase in contagion from the pandemic led to an exponential increase in malicious activity. Hackers began to take advantage of several people working at home, publishing advertisements in order to deceive users as they worked remotely and began to spend more time connecting to the internet and carrying out activities and looking for information.

Table 1. Most used platforms for attack

Tools	Features	Website
Zoom	Easy to use	https://zoom.us/pt-pt/meetings.html
Google Meet	Secure video meetings	https://meet.google.com/
FaceTime	Best for iPhone, iPad, or other iOS users. The app is only available on the App Store for iPhone and iPad.	https://apps.apple.com/us/app/facetime/id1110145091
WhatsApp	For international chats: Voice and video calls for up to 4 users.	https://web.whatsapp.com/
Google Duo	Best for Android: video calling app	https://duo.google.com/
Skype	No sign ups, downloads.	https://apps.apple.com/us/app/facetime/id1110145091

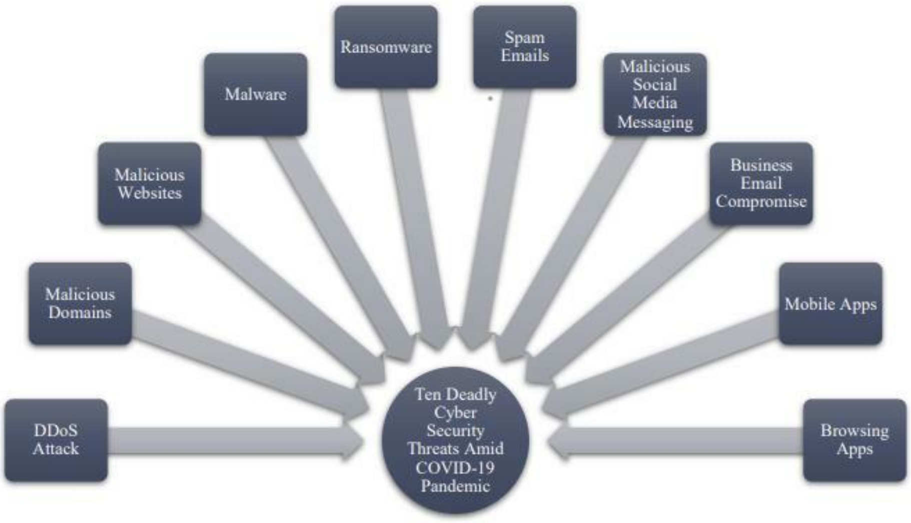
Many students had a great exposure to security due to the need to use tools to hold meetings in a virtual way such as "Microsoft Teams" or "Zoom". The growth of this platform has led to some security problems and cybercriminals have taken advantage of it by creating malicious campaigns. However, it was noted that during this pandemic there was an increase in phishing campaigns as part of Social Engineering.

3 Security Threats

As society has become more and more dependent on technology, it has also become increasingly vulnerable to cybercrime. Cyber security threats are estimated to cost the world $6 trillion a year by 2021, doubling from $3 trillion in 2015[1]. One of the main reasons cybercriminals thrive during pandemics is because heightened emotional states, such as fear, make victims more susceptible to falling into fraud [2]. According to the World Health Organization (WHO), the number of cyber-attacks launched increased fivefold during the COVID-19 pandemic [3]

Since the first cases of COVID-19 in Portugal and the implementation of the new containment measures, there has been an increase in cyber-attacks that use social engineering to take advantage of the fragility of the victims. The most reported attacks during the pandemic were:

Fig. 1. Ten Deadly Cyber Security Threats [5]


Ransomware
Spam Emails
Malware
Malicious Social Media Messaging
Malicious Websites
Business Email Compromise
Malicious Domains
Mobile Apps
DDoS Attack
Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic
Browsing Apps

3.1 DDOS Attack

Most of the government and healthcare organizations have seen a rapid increase in the Distributed Denial of Services (DDoS) [4]. DDOS attacks are those carried out by cybercriminals against websites or web services, with the aim of stopping them and making them offline. A recent example of this happened when a DDoS attack targeted the website of the Department of Health and Human Services (DHoS) in the U.S. by flooding millions of users at a time [5].

3.2 Malicious domains

The impact of this pandemic has also caused a lot of fake news and fake applications that circulate through social networks and messaging applications, which only generate disinformation. That is why several major social platforms such as Facebook, Google, LinkedIn, Microsoft, Twitter, Reddit and YouTube have joined forces in the fight against misinformation and the scams surrounding the pandemic. The words "coronavirus," "corona-virus," "covid19," and "COVID-19" have appeared in a wide number of registered domains on the internet recently, and daily more and more increase has been witnessed. These domains are used to carry out different scams, or they are used to act as a honeypot for the target users. Hackers get personal data through this procedure and then use it for their intended purposes. One of the main sources to lure the user into clicking on the link or downloading the malware are spam emails, for which the user becomes victim through mobile device or computers [6].

3.3 Malware and Ransomware

The covid-19 pandemic has accelerated the digital transformation in the world. From day to night, companies had to review their work models and offer their employees ways to enable remote work, thinking about the health and safety of their teams. This high number of professionals working from home and, at least at first, without adequate protection for companies access, networks, data, and intellectual property would naturally draw the attention of cybercriminals. Several surveys on digital threats have been published during this period and all point to an exponential growth of ransomware attacks, which are malware created and disseminated with the aim of blocking access to files or systems to release them after payment of a specified amount as if it were a virtual hijacking. The ransomware infects the system via email attachments, links, or through working employees whose credentials are already compromised by exploiting a vulnerability in their systems [6].

3.4 Spam emails

Another piece of true news during this time of pandemic was the amount of Phishing attacks that are usually detained two or three dozen people a year, but in the face of the pandemic. This social engineering attack, as we can see from the figures described above, has been highly used and efficiently.

Phishing is nothing more than a fraudulent attempt to acquire the other persons data by means of a disguise, which means trying to pass yourself off as a trustworthy person or entity, so that the person to be attacked has no problem in providing any kind of personal data due to their legitimate appearance.

This attack takes place mostly in the form of a message through e-mail forgeries or even through instant messaging if the hacker already has the persons phone number. As a rule, this attack always has a reliable format as legitimate looking websites, offers not to be missed or even pretending to be a non-profit company to make the person feel in the scope of help.

Table 2. There have been numerous cases in which the intruders pretend to be from legit organizations such as WHO. They use domain spoofing to fool the victim that the email is coming from WHO and ask them to donate in bitcoins. For instance, the end of the email address normally ends with the organizations website, and people can know from there whether they are communicating with the right person or organization. The intruders use an email such as coronavirusfund@who.org. The WHO official website www.who.int ends with "int" and not with "org." Any user who did not confirm this email may become a victim [7].

3.5 Malicious Social Media Messaging

Nowadays, social media is very common and is almost in the reach of every individual. Hackers find it a great opportunity and tend towards the various social media platforms such as Facebook and WhatsApp. The attempts to obtain confidential information through fraudulent messages), spam (unsolicited email) and targeted attacks on social networking platforms. The scams typically lure victims into free subscriptions such as Netflix premium free account. When the victim clicks on the link, it redirects them to their social media phishing website. In some cases, it may ask to enter the credentials of their accounts.

From what has been described we can see that during the pandemic this was one of the most used attacks and with great efficiency, however, how to prevent such attacks. Unfortunately, we cannot simply install a software program or have the usual antivirus for prevention. Because we live in an age where there is great social exposure it is very easy for anyone or hacker to get their email, name, mobile phone. Because of this it is inevitable not to receive phishing emails.

The new pandemic landscape has shown that several companies have been forced to accelerate digital transformation processes. Digital transformation brings with its security considerations regardless of flexibility. Most users were working remotely as a result of the pandemic and it was also noted that the company, they were working for did not provide the necessary security tools to do the work remotely.

Although some companies had already adopted mechanisms to carry out the digital transformation process, many others ignored the three basic pillars for saying that a computer system is secure that it is: Confidentiality, Integrity and availability. But it is not the companies fault either because of the comfort of the home, some people ignored some care that we would have in the workplace. As a result, some workers pay less attention to cyber-security issues.

One of the big reasons for this is because employees use their own home equipment as a working tool. Working from home made it sound like a nice idea to many people, but it might bring some problems for companies because of Security. People have ended up neglecting security measures, which leads to compromising sensitive company data. From another point of view, it is reported that because there is more pressure on telework, employees ignore the recommended security measures.

4 Possible attack prevention

Companies and organizations need to prepare for the risks of cyber security. In recent months the threat called "sars-cov2" has made the area of security difficult due to the need to spread as much information about the virus as possible which has caused phishing emails to grow.

In this area it is necessary to understand the main risks that need to be faced and measures that we can take to ensure the privacy of companies and hacker personnel trying to take advantage of the vulnerabilities in this sector.

With the implementation of containment there was the idea of teleworking as mentioned above in this paper, companies enabled employees to take equipment that was in a business environment home. This led to a great danger of integrity due to the fact that most homes did not have a secure network. A recommendation in this environment will be to protect this equipment with data encryption, strong passwords so that it cannot be accessed by third parties and good practices of use such as blocking / logging out.

Another important measure will be the investment of a separate camera from the device and of good quality. With the containment the participation of teleconferences and video calls became important. However, it is need to be aware of the attacks that can be made these days. It is easy for a hacker or even an ordinary person to "hack" a camera and in order to be able to prevent this kind of attacks we should cover the camera whenever we are not using it and if the camera is separated from the device simply disconnect it.

Another procedure to keep in mind is the use of a VPN if employees need to access the companys internal network. It is recommended to do it inside the company or that the IT team creates a VPN so that employees at home can access the necessary resources in a secure way. This measure is quite clever as it ensures the privacy of any remote worker including this method ensures strong authentication and high encryption methods.

A good practice and investment will be in protecting the home network that ensures enhanced protection when working at home. Some methods to increase the security of the home network would be:

1. Create a unique strong password.
2. Changing the SSID name.
3. Limit MAC address access
4. Update the firmware

Companies should implement training to inform company employees of the dangers of cybersecurity is to conduct awareness campaigns to help combat cybercriminals who often try to exploit vulnerabilities.

In order to avoid this kind of attacks we must be careful with e-mails to which we are asked for personal data, usually reputable companies and banks do not make this information requirements of personal data.

We should try to avoid opening embedded attachments or links, as they may be loaded with malware. Usually, this kind of attacks may have unmissable offers and grammatical errors and when we receive e-mails of this kind, we should be cautious and check if we are dealing with a legitimate company and if the link redirects us to a real link, one way to understand if we are in the presence of a real link is to pass the cursor on that same link and see the information in the bottom left corner that will show the real link. Unfortunately, in the face of the pandemic the great volume of attacks was not only phishing.

With the changes caused by the pandemic, hackers have adjusted new strategies so that they can profit from radical changes in the lives of people and companies.

5 Conclusion

In conclusion, we can see that the scenario is not at all favorable, either from a health point of view or from a safety perspective. If we think about the future in a positive way, people and companies may now pay more attention to safety and the risks behind it. That said, users are now more aware and aware of security risks and companies will be better prepared for when it is necessary to go back to remote work. With the recent outbreak of the coronavirus pandemic, there have been

A huge increase in the number of users interacting with each others working online. Taking advantage of the situation, the hackers IT is increasing daily, with the same ratio, there is an increasing cyber-security threats and privacy issues as well. There has been a considerable increase in the record of malicious attacks, websites, and spam e-mails. Intruders are targeting individuals, government officials and even doctors and health care workers care systems. This paper presented what happened during the pandemic and how people and businesses adapted to the new lifestyle derived from Covid-19 as well as the most commonly used hacking links. These cyber-security threats have led to some serious questions and concerns about personal data and the future of telework.

6 References

1. The official annual cybercrime report 2020. Herjavic Group. 2020. URL: https://tinyurl.com/y56trmgv
2. Naidoo R. Um modelo de influência de vários níveis do cibercrime com o tema COVID-19. Eur J Inf Syst 2020: 306-321. [CrossRef]
3. The WHO reports a five-fold increase in cyber attacks, calling for vigilance. World Health Organization. 2020 April 23. URL: https:. / / Www who.int/ fourth news / detail / 23-04-2020-which-reports-quintuple-in-ciber-attacks-impulses-surveillance

10.11228/dpsc.03.01.002

4. N. A. Khan, S. N. Brohi, and Jhanjhi. NZ, “UAV’s Applications Architecture Security issues and Attack Scenarios: A Survey,” in 1st International Conference on Technology Innovation and Data Sciences (ICTIDS) 2019, 2019
5. https://www.researchgate.net/publication/341324576_Ten_Deadly_Cyber_Security_Threats_Amid_COVID-19_Pandemic
6. S. Stein and J. Jacobs, “Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak,” 2020. [Online]. Available: https://www.bloomberg.com/news/articles/2020-03-16/u-s-healthagency-suffers-cyber-attack-during-covid-19-response
7. Interpol,” Covid-19 cyberthreats, “2020.: https://www.interpol.int/en/Crimes/Cybercrime/COVID-19- cyberthreats.
8. 25-WHO, “Beware of criminals pretending to be WHO,” 2020. [Online]. Available: https://www.who.int/about/communications/cybersecurity.