ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1570

Cyber Threats in the Health Sector in the DRC: Risks, Opportunities, Consequences and Preventive Measures

Ruben Kanku[1]; Hervé Kinkete Mfumabi (Assistant and Research)[2]; Michel Kabeya Kadima (Lecturer)[3]
Anderson Malanda Landu Kuyi (Lecturer)[4]; Pathy Nkayilu Wabaluku[5]
Bruno Luwa Muanda (Lecturer)[6]; Hugor Bolompata[7]
Information Technology Expert, Governorate of KASAI (DR Congo), & University of Kinshasa

Abstract:- While hackers ravage the world, social media, banking and other accounts are hacked every day, but cyber threats in DRC are not taken very seriously. There is a total negligence on the part of the country's authorities and hospital managers and human lives are in danger. one of the large hospitals of Kinshasa HJ Hospital has always been faced with multiple problems concerning its system. Once I left to get tested, I found a crowd waiting for the results because their system was blocked. It took almost a week to find a solution to this problem. But no statement has been released regarding this issue. lives are in danger; personal data is not protected and no one is complaining. We encounter many diverse cases across the country. With a country of more than 100 million inhabitants, the country cannot escape this scourge. As in many other countries, healthcare facilities in the DRC are increasingly dependent on IT systems to manage patient records, appointments, medical prescriptions and other critical aspects of their operation.

However, this increased reliance on information and communications technology (ICT) also exposes healthcare organizations to various online threats, such as cyberattacks, malware, ransomware, and data theft. These threats can have serious consequences, including disruption of healthcare services, disclosure of confidential patient data and even endangering lives.

To combat these threats, it is crucial that healthcare facilities in the DRC implement robust cybersecurity measures. This includes raising staff awareness of IT security practices, implementing effective firewalls and antivirus software, regularly backing up data, and training and educating users on how to recognize and report malware. suspicious online activities.

Additionally, close collaboration between health authorities, regulators, healthcare providers and cybersecurity experts is essential to develop effective policies and protocols to protect healthcare infrastructure and data from cyber threats. constantly evolving.

We decided to put together this article to be able to enlighten the entire Congolese community, more specifically health establishments, and warn them about the dangers and risks of technology.

Keywords:- *ICT, Cybersecurity, Cyber Threats DRC, Malware, Virus, OS, DoS.*

I. INTRODUCTION

Technology has made the world too small, reduced distances and removed borders. Access to information becomes very simple: just click on a button to record, delete and save. New technologies have changed the way we work, communicate and spend our free time.

According to predictions for 2020, there will be more than a billion connected objects in the world in 2022[1]: from cell phones to wearables, from refrigerators to coffee makers, almost anything that can be connected to the internet will be. Unfortunately, this development also brings many problems. The facility with which we connect our devices and share our data can increase risks to our privacy.

The Democratic Republic of Congo (DRC), one of the largest and popular countries in the world with more than 100 million inhabitants where almost half of the population is connected thanks to their telephone, computer or television, has not been left behind. Hospitals want to take advantage of this progress to improve healthcare delivery and facility management.

Some hospitals in the DRC are integrating technology into their medical practices to improve the efficiency, accuracy and quality of healthcare. However, much remains to be done to make the use of technology widespread across all healthcare facilities across the country.

➢ *Here are some examples:*

- Monkole Hospital Center (Kinshasa): has an electronic medical record system to track patients' medical histories and manage appointments.

[1] Published by Maxime Gautier, December 13 2023

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1570

- Bukavu Provincial General Reference Hospital (Bukavu): This hospital also uses computer systems for the management of medical records and appointments, which helps improve the efficiency and precision of care.
- Kananga General Reference Hospital (Kananga): Located in the Kasai-Central province, this hospital uses technologies such as scanners and medical imaging equipment for the diagnosis and treatment of patients.
- Kisangani Provincial General Reference Hospital (Kisangani): This facility also uses modern medical technologies to provide advanced healthcare, including medical imaging equipment and medical monitoring devices.
- Cinquantenaire Hospital (Kinshasa): As one of the largest hospitals in Kinshasa, it has gradually adopted modern technologies to improve patient management and quality of care.
- HJ Hospital: has a website and an electronic medical record system to track patients' medical histories and manage appointments.

But how does technology affect the healthcare sector (staff and their patients)? Although technology has many advantages and everyone is running to avoid finding themselves obsolete, the biggest question remains security. Accidents resulting in personal data breaches can have serious consequences for patients, staff members and the hospital itself. How can healthcare organizations protect themselves, their staff and their patients against these growing threats? And how can health professionals contribute to this process?

In this article, we will examine the concept of cybersecurity in the health sector in DR Congo, why, its importance, its advantages and opportunities. We will also talk about the challenges of digitizing healthcare, human behavior like weak jersey, social media usage, types of malware and how to detect them.

II. METHODOLOGY

The study used quantitative and qualitative methods. The case study design is applied when data has been collected using documentary analyzes and discussions with health personnel in Kinshasa. Thus, the qualitative approach was used to provide reliable answers to the research questions and, in return, to propose a framework to combat cyber-attack.

➢ *Definition and why Cybersecurity?*

Many have contributed to the evolution of this discipline so there are several definitions. We choose the simplest definition that fits with our vision.

"The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this." (Oxford University Press, 2014).

➢ *Cybersecurity Issues in Healthcare*

The healthcare sector is a big target for cybercriminals because they store precious and large amounts of sensitive data. [3].

The health sector in the Democratic Republic of Congo (DRC) faces several cybersecurity challenges. These challenges include:

- Negligence, Lack of user awareness and training: Healthcare professionals in the DRC are unaware of cybersecurity risks and best practices to mitigate them. Threat awareness and training is necessary.
- Outdated infrastructure: Many health facilities in the DRC use outdated IT systems and free software, making them vulnerable to attacks.
- Lack of investment in IT security: Due to budgetary constraints and other priorities, healthcare facilities in the DRC may not invest enough in IT security, leaving their systems vulnerable to attacks.

We have all heard about the WannaCry ransomware, this example could help health specialists in my country not to neglect the IT security aspect, because what happened can still happen. The DRC being one of the most populous in the world and currently the population depends much more on technology in their daily lives, patient attendance is increasing more and more in modern hospitals. Let's imagine that if such a scenario occurred, there would be serious damage. So we must take preventive measures seriously.

➢ *What really Happened?*

"*The patient lying on the emergency room table in front of Paul Pugsley was having a stroke. Time was running out. Pugsley, an emergency medicine resident at Maricopa Medical Center, knew he had to send the patient for a CT scan. But when Pugsley looked at the computer screen on the side of the room, he saw a pop-up message demanding payment in bitcoins. Minutes later, he was told that the same message had stopped the scanner, it should help the patient without knowing whether the stroke was caused by bleeding or a clot, information that is usually vital to the course of treatment.*

After a few minutes of frantic running around, the patient was carried out of the room (prognosis: survival, but severe brain damage). The flashing ransom note was part of a simulation, designed to expose doctors like Pugsley to the very real threat of cyberattacks on their hospitals.

Reports show that ransomware and other cyberattacks are on the rise , and healthcare is one of the top targets . Just this week, researchers in Israel announced that they had created a computer virus capable of adding tumors to CT and MRI scans, malware designed to trick doctors into doing bad things . diagnosing high-profile patients, reports Kim Zetter for the Washington Post . Despite the growing threat, the vast majority of hospitals and doctors are unprepared to deal with cybersecurity threats, even though they pose a major public health problem.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1570

A week after the attack, researchers have a better understanding of how the WannaCry ransomware spread so quickly and have judged by the initial numbers that the story appears to be almost entirely about Windows 7. According to data released today by Kaspersky Lab, About 98% of computers hit by ransomware were running some version of Windows 7, and fewer than one in a thousand computers were running Windows XP. R2 2008 server clients were also hit hard, accounting for just over 1% of infections [7].

Windows 7 remains by far the most common version of Windows, running on approximately four times as many computers as Windows 10 worldwide. Since newer versions of Windows are not vulnerable to WannaCry, it makes sense that most infections affect computers running version 7. Nonetheless, the stark disparity highlights the small role that Windows XP appears to have played in the spread of infection, despite early concerns about the infection. outdated operating system.

The healthcare industry increasingly relies on Internet-connected technology: from patient records and laboratory results to X-ray equipment and hospital elevators. This is good for patient care because it facilitates data integration, patient engagement, and clinical support. On the other hand, these technologies are often vulnerable to cyberattacks, which can siphon patient data, hijack drug infusion devices to mine cryptocurrency, or shut down an entire hospital until a ransom is paid.

"If systems are disrupted over the Internet, by an adversary or an accident, it can have a profound impact on patient care," says Beau Woods, cybersecurity advocate and cybersecurity innovation researcher at the Atlantic Council.

Fig 1 A Screenshot of Wanna Cry Ransomware. Image: Secure List / AO Kaspersky Lab

III. STATE OF PLACE

To effectively protect our hospitals against cyber risks and future threats, we must first assess the current situation and possible threats. It is not a question of circumscribing with precision of the risks incurred by hospitals, but to strategically integrate the importance of different threats and to anticipate their solutions.

A. Challenges and Opportunities for Healthcare

The mobile phone has become an essential tool for communication in the Democratic Republic of Congo (DRC), with an increasing number of users over the years. However, accurate data on the precise number of mobile phone users in the DRC may be difficult to obtain due to various factors, such as the lack of reliable data collection infrastructure and the prevalence of mobile phone use. unregistered or prepaid.

Nevertheless, the penetration rate of mobile phones in the DRC is estimated to have increased significantly over the past decade, due to the increasing availability of mobile devices at affordable prices and the expansion of telecommunications networks in the country.

According to the DESKECO report of May 27, 2024, 56.26 million mobile phone subscriptions recorded at the end of 2023. The main trends for 2023 in mobile telephony in the Democratic Republic of Congo are:

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1570

- Active subscriptions: stability and growth of telecoms subscriptions in the DRC despite the electoral period: a marginal increase of 0.15% was observed, with the number of active subscriptions increasing from 56.18 million to 56.26 million. The mobile penetration rate stagnates at 59%.
- Mobile Internet: The mobile Internet segment recorded a notable growth of 3.69% in terms of subscriptions, from 28.91 million to 29.98 million. The penetration rate reached 31.5%.
- Mobile money: a booming tool for financial inclusion: mobile money services also saw a 2.35% increase in active users, from 21.67 million to 22.18 million for a rate of penetration of 23.3%.

A large portion of the Congolese population uses cell phones for a variety of activities, including voice communication, text messaging, Internet access, mobile financial services, and other applications. Mobile phones also play a crucial role in providing health and information services in regions where traditional communications infrastructure is limited. Although there are no precise figures on the number of mobile phone users in the DRC, it is undeniable that their use is widespread and continues to grow, contributing to connectivity and socio-economic development. from the country. In summary: the mobile operator market in the 1st Quarter of 2023

INDICATORS	Q4-2022	Q1-2023	Variation
Total subscriptions	**49,844,134**	**53,674,957**	**7.69%**
Penetration rate	52.35%	56.38%	4.02%
Global revenue (voice+SMS+data) (USD)	**528 857 518**	**458 652 569**	**-13.27%**
Global ARPU (USD)	3.57	2.88	-19.47%
Revenue Data (USD)	**160 604 133**	**167,788,912**	**4.47%**
ARPUdata (USD)	2.05	**2.13**	**3.81%**
Turnover on payment of commissions by SFMs to MNOs in USD 4	-	2,167,416	-
MFS turnover on mobile money transactions in USD5	**66,447,539**	**69,785,918**	**5.02%**
Voice traffic (minutes)	4,106,875,472	3,855,164,818	-6.13%
SMS traffic (number)	15,255,213,919	15,122,392,323	-0.87%
MoU (minutes)	27.8	24.2	-12.83%
Mobile Internet subscription	25,935,100	28,188,471	8.69%
Mobile Internet penetration rate	**27.24%**	**29.61%**	**2.37%**
Mobile Internet traffic (megabytes)	**142 115 039 096**	**150 222 233 560**	**5.70%**
Mobile money subscription	13,825,882	18,206,633	31.69%
Mobile money penetration rate	14.52%	19.12%	4.60%
IHH Market Concentration Index (IHH Market Concentration Index) Herfindahl-Hirschmann)	**> 2500**	**> 2500**	
Population of the DRC (x)	**95,207,000**		

Fig 2 Estimates Central Bank of Congo “Condensed Statistical Information Report n°24/2022” P2

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1570

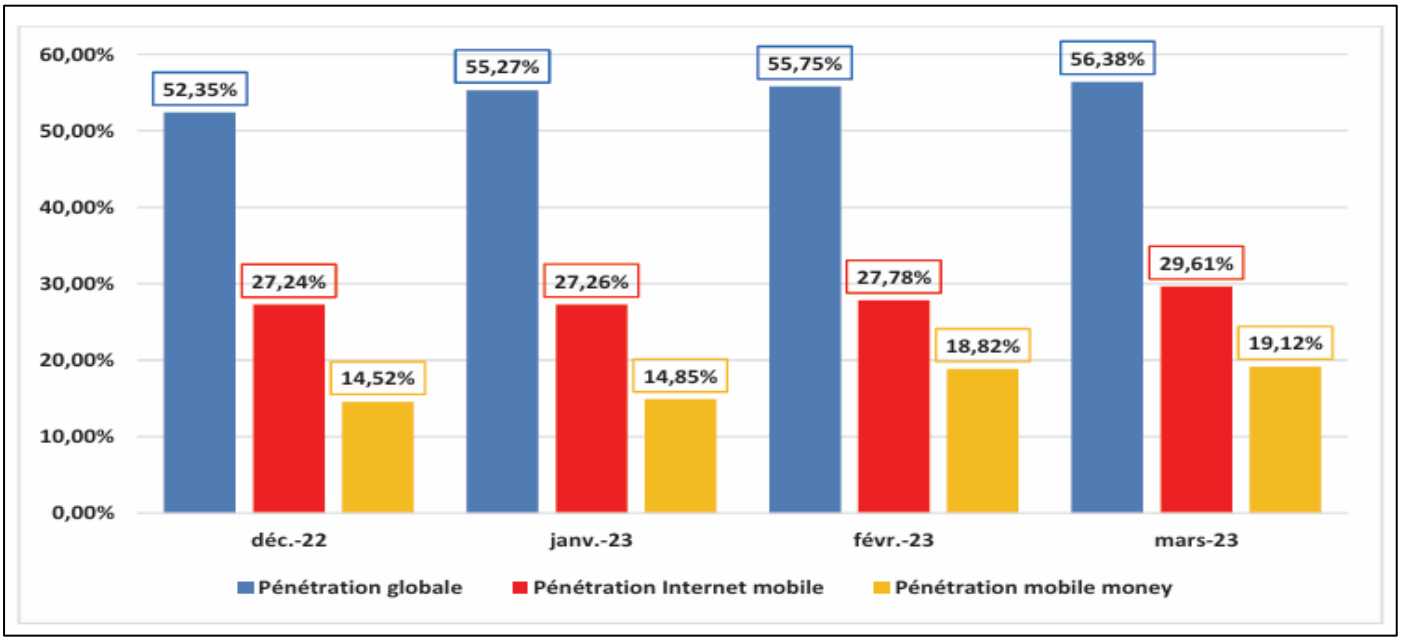

Fig 3 Monthly Evolution of the Penetration rate of Mobile Services in DRC

The health sector in the DRC is starting to transform its processes to communicate easily and effectively with people (marketing via SMS, making appointments with a doctor, receiving results by WhatsApp...etc). As long as the rate increases and cybersecurity therefore remains an unresolved problem in the health sector in the DRC, an environment where the consequences for patients can be fatal. Cybersecurity is therefore still an unsolved problem in the healthcare sector, an environment where the consequences for patients can be fatal.

Disclosed patient information may be used for identity theft, fraud, and other financial gain. Here are some of the key challenges and opportunities:

➢ *As Challenges:*

- Medical data protection: Patient medical data, such as medical records, personal information, and test results, are potential targets for cybercriminals. Protecting this data from unauthorized access, leaks and privacy violations is a major challenge.
- Vulnerability of IT systems: Hospitals and health establishments in the DRC are very exposed and vulnerable to cyberattacks due to outdated IT systems, obsolete software, untrained and unprofessional staff.
- Lack of awareness and training: Medical staff in the DRC are not well aware and trained to deal with cyber-attack, which is a great practical risk to protect health systems and data from cyber threats.
- Low investment in cybersecurity: Due to budget constraints, lack of will and other priorities, health facilities in the DRC do not invest sufficiently in cybersecurity, leaving their IT systems vulnerable to attacks.

➢ *As Opportunities:*

- medical staff need to be trained on cybersecurity risks in healthcare, as well as protective measures and best practices to prevent cyberattacks.
- We must invest in system security: Although it is expensive, a proverb of Laurence Hartmann says: “Health is priceless, but it has a cost”. By investing in modern, secure IT infrastructure and robust security software, healthcare organizations can strengthen the protection of their systems against cyber threats.
- Use of innovative security technologies: Technologies such as cryptography, biometrics and multi-factor authentication can be used to strengthen the security of medical data and limit unauthorized access to IT systems.
- Collaboration and sharing of best practices: By collaborating with other health facilities, government agencies, cybersecurity experts and international partners, health facilities in the DRC can share best practices, advice and resources to improve their cybersecurity posture. In summary, although the challenges of cybersecurity in healthcare in the DRC are significant, there are opportunities to strengthen the protection of medical data and ensure the security of IT systems by investing in awareness, training, innovative technologies and collaboration.

B. Types of Data in Healthcare

Health data is very sensitive data that is valuable in the eyes of cybercriminals. Due to this sensitivity, their computerized processing and use is subject to the laws. health data is so-called personal data,

Health data is all information relating to a person’s state of health. This includes not only medical data, such as data relating to physical and mental health, but also financial and administrative data related to the provision of healthcare (Simoncini, 2017).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1570

➢ *According to Victoria Hordern, Personal Data Concerning Health also Includes:*

- Information about a person's registration for healthcare services
- Any number or symbol that uniquely identifies an individual for health purposes
- Information from tests or medical examinations, as well as
- Information on a disease, disability or disease risk, medical history and clinical treatment.

C. Processing of Health Data and General Data Protection Regulation ("GDPR")

Under the EU's General Data Protection Regulation ("GDPR"), the use of personal data is only permitted where there is a "lawful basis" for doing so. There are many articles but, in this work, we take only Article 6(1).

➢ *Article 6(1): Processing shall be Lawful only if and to the Extent that at Least one of the following Applies:*

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- Processing is necessary for compliance with a legal obligation to which the controller is subject;
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

➢ *Checklist for Collecting and Processing Health Data*

The following list contains useful questions for people who collect and/or process medical data (Simoncini, 2017):

- Is the data directly relevant to medical treatment?
- Is the patient informed about what information is being processed and why?
- Is the patient aware of his right to access his medical file to verify or correct information?
- Is the access request procedure known to him?
- Is data retained for an appropriate period?
- Are the data processed by health professionals bound by medical confidentiality?
- Are the data processed by administrative staff who have signed a specific confidentiality declaration?
- Has a risk assessment been carried out and appropriate security measures put in place?

D. Human Behavior and Cybersecurity in Health and Social Service Organizations

A common belief in the cybersecurity field is that the human factor is the weakest link in the cybersecurity chain. This seems to be true because IT sector is the most neglected sector in hospital's sector in DR Congo. The staff being ignorant and their behavior poses the greatest risk to maintaining cybersecurity. they make bad decisions, ignore warning signs, or don't care about cybersecurity at all. So, they are not made aware and trained. This is why they are considered the weak link.

IV. SOCIAL ENGINEERING AND THE DIFFERENT TYPES OF ATTACKS

➢ *We may have Heard of Social Engineering before. But what is it and how does it Work?*

Any professional may have already received phone calls or emails from people offering you offers. They try to take their targets into confidence and make them pay a large sum to claim the offers. There are testimonies everywhere in DR Congo, people receive emails and text messages via their mobiles from hospitals but in reality, this is false. This is what we call fraud. This is an example of social engineering.

The objective of social engineering is not only financial. It can also be used for other purposes, such as collecting personal information from people. Today social engineers are everywhere. Even among our close friends. There are many social engineering tactics depending on the medium used to implement it. It could be email, website, phone, USB, or something else.

➢ *So here are the Different Types of Popular Social Engineering Attacks:*

- Phishing: Phishing is the most common type of social engineering attack. Here's how it works; the criminal recreates the hospital's website and sends the link to targets via emails or social media platforms. Being ignorant, people end up registering and giving out their personal information and even their credit card details. To prevent phishing emails, use spam filters in your email accounts. These days, most email providers do this by default. Also, do not open emails from an untrusted source or you find them suspicious.
- Voice Phishing or Vishing: this technique is currently at the top in DR Congo. Imposters or social engineers use the telephone. They recreate a company's IVR (Interactive Voice Response) system or look for a number similar to the company's and contact people. Most people don't think twice before giving away confidential information or even paying for it.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1570

- **Pretending**: Pretending is another example of social engineering you may have encountered. An attacker can pretend to be another person or a known person to extract information by tricking people. Another example of pretense can be fake emails, fake Facebook accounts, X, Linkdin and others that you receive from your distant friends who need money. Probably, someone hacked their account or created a fake one.
- **Baiting** : is one of the social engineering techniques people use. Attackers leave USB sticks, memory cards and the like in public places in the hope that someone will pick them up out of curiosity and use them on their devices. A more modern example of baiting can be found on the web. Various download links, mostly containing malware, are thrown in front of random people in the hope that someone will click on them. As a tip, don't click on just any file.
- **Tailgating**: Likewise, there are other social engineering techniques, such as tailgating, in which a person requests help from an authorized person to gain access to restricted areas where authentication or other electronic barrier is present. And you receive an email and a text message asking you to enter the code or change your password. once you enter your information your account will be hacked.
- Quid pro quo: Another method of social engineering, **Quid pro quo** , involves passing people off as technical support. They make random calls to a company's employees pretending they are contacting them about a problem. Sometimes these people have the ability to make the victim do what they want. It can also be used for common people. The misunderstanding involves an exchange of something with the target, for example, the attacker trying to solve a victim's real problem. The exchange may include material things such as a gift in exchange for the information.

➢ *How to Defend yourself against Social Engineers?*
To fight against attack:

- Any professional must be careful, especially when someone asks you to provide your information or when an unknown person gives you something for free (a service, a USB key, computer equipment).
- Improve your emotional intelligence: don't be open to those who try to give you emotional comfort.
- Think before you act and Also pay attention to the web pages you visit or files you download. They may contain malicious tools to harvest your information.
- Protect your accounts and devices: It is therefore important to protect your smartphones, PCs and online accounts by adding strong passwords and other methods such as two-factor authentication. Take appropriate security measures such as antivirus software, firewalls, etc. This is the least you can do. Also make sure that you are not in the habit of writing down passwords and financial details.

Despite the elements cited above, the best method according to my own understanding, for dealing with attacks remains staff training. prepared to deal with such situations.

V. USE OF SOCIAL MEDIA

Social networks remain the most used communication channel in the DRC. There is even a Congolese expression which says "Missing everything except mobile data". Facebook, Twitter, LinkedIn, YouTube, Instagram, WhatsApp and TikTok are part of the daily life of the Congolese. These networks help us connect, communicate, exchange and share information, messages, photos, videos with people around the world at low cost. Given this popularity, companies are now using social media to communicate, strengthen their brand awareness, their public relations, their marketing and their customer service.

Health establishments in the DRC also took advantage of this opportunity to stay in daily contact with patients and staff, offering online services, sharing results and relevant information.

But the biggest problem in use remains security. The risks associated with the use of social networks for the health sector in the DRC are too high, a country where half of the population uses Facebook, Whatsaap and Tiktok and where account hacking is wreaking havoc.

Thus, users of social networks and doctors must be aware of their role as health professionals and maintain a professional relationship with patients online. Social media should be used ethically and respectfully to communicate useful and accurate health information. Physicians have a responsibility to protect patient confidentiality and maintain high ethical standards online, to ensure a trusting relationship with patients and protect their professional reputation.

A. Data Breach

➢ *We often hear about Data Breaches and Credit Card Hacks. do you really know what that means?*
A data breach occurs when unauthorized people or software infiltrate computer systems, networks or databases to access confidential information. The consequences of a data breach can be serious: financial losses, reputational damage, legal implications and potential harm to victims.

The goal of hacking these systems is to use this breached information for identity theft and fraud.

There are several types of data breaches. A data breach is intended to damage your personal image and that of your company. The most common types of data breach and malware are:

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1570

- Information theft: often information theft comes from human errors and these errors cost the company too much. an employee may leave a computer, phone or file in a place where they should not have left it and have it stolen. This can compromise not only the new prototypes you are trying to keep confidential, but also customer or patient information. larger companies like Apple have experienced these kinds of problems
- Ransomware
- Password deduction: This is the theft of passwords. many falls victim to hacking simply because their password is too simple or too easy to guess;
- Recording of keystrokes: A professional should avoid downloading files from the internet, clicking any files and opening emails from questionable sources. Malware called keyloggers can record what you type on your computer. The data is then passed to hackers and used to access sensitive data.
- Phishing: Here hackers create or duplicate sites that appear incredibly authentic to the businesses. For example, they can create a site that perfectly copies that of the HJ hospital and ask you to log in. As soon as you log in without realizing that the site is fraudulent, you directly give your password to the hacker.
- Malware or viruses: Aim to delete all data from a computer. For example, if a virus is sent to a hospital, it will delete the data of thousands of patients and healthcare workers. the organization of the hospital will be disrupted, medical examinations, treatment, operations and results will be delayed. This leads to a very serious situation, even the death of certain patients in the hospital.
- Distributed Denial of Service (DDoS): this attack targets large companies to prevent them from working.
- Worms: the worm is more dangerous than the virus. it spreads quickly without the end user. Viruses require an end user to at least trigger them before they can attempt to infect.
- Trojan horses: Trojans appear to be legitimate programs, but they contain malicious instructions. this is the type most used today by pirates. Trojan horses generally arrive by email or are transmitted to users when they visit infected websites (porn, free software and games download sites...etc. here is a clear example of a Trojan horse, a message appears abruptly asking you to scan and restart your computer once click yes, you are caught and infected.
- Malicious advertising: Malicious advertising pays to place its advertisements and advertisements on legitimate social networks and websites. When a user clicks on the ad, the ad code redirects them to a malicious website or installs malware on their computer.

Most hacks fail too. It's like a thief who plans his theft, he attacks houses where the security is not at the top.

So what businesses can do to strengthen their security and to prevent these attacks. as long as technology advances, so do hackers in their strategies and people and companies will always be at risk. Here are some ways to protect your identity in the event of a breach:

- Use strong passwords: combinations of numbers, letters and symbols. a password that is difficult to remember.
- check your accounts regularly to detect any unusual activity because currently with two-factor authentication, any movement in your accounts is reported;
- Take action: When you notice suspicious or unrecognized activity on your accounts,
- Use secure URLs: Only use sites starting with https://. The “s” is essential to know that you have a reputable site.
- Use PayPal: Using PayPal can prevent your credit card information from being sent to the wrong source. PayPal will pay it from your account for you without having to enter any sensitive information;
- Avoid sharing too much online: Don't post sensitive information that could be used to hack your accounts.
- Implement high-quality security software that protects against attacks. For example, anti-virus software like Avast. Not the free version.

B. How to Detect and Remove Malware

Malware first infects your computer, collects personal data in order to prevent your computer from functioning properly and efficiently.

Here are the signs to recognize that your computer has been infected and the steps you can take to detect and remove all malware from your computer:

➢ *Use Microsoft Defender Antivirus*

Most health establishments in the DRC use Windows as their operating system, for Mac environment, Malwarebytes is a power tool to check for and remove malware. According to me, Microsoft Defender Antivirus is a very powerful tool for searching and removing malware in windows environment. It is free software and included in each version of Windows. It often requires updates to strengthen security and it is necessary to do so to be up to date and ready against attacks. Here's how to use it on Windows 10 or 11.

Before launching it, make sure to save all open files and close applications and programs. The example bellow show how to open and scan with Microsoft defender.

- Open Windows Security Settings and Select Virus & Threat Protection/ Scanning Options.
- Select Microsoft Defender Antivirus, then select Scan now.
- It takes several minutes to run the Microsoft Defender offline scan, then your PC will restart.
- View your analysis results and Open your Windows Security settings.
- Select Virus & Threat Protection / Protection History.
- Microsoft Defender Offline Scanning will detect and automatically remove or quarantine malware.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1570

Fig 4 The Windows Security Interface: Microsoft Defender

➢ *Check if Your Operating System is up-to-Date.*

Updating your operating system can be tiring, because almost every week Windows fixes and places new rules to strengthen security. The first step to defeating malware is to do regular updates.

➢ *To Update Windows:*

- Click on update & Security" in the Windows Settings.
- On Mac, click on System Preferences in the Apple Menu, and then clicking Software Update.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1570

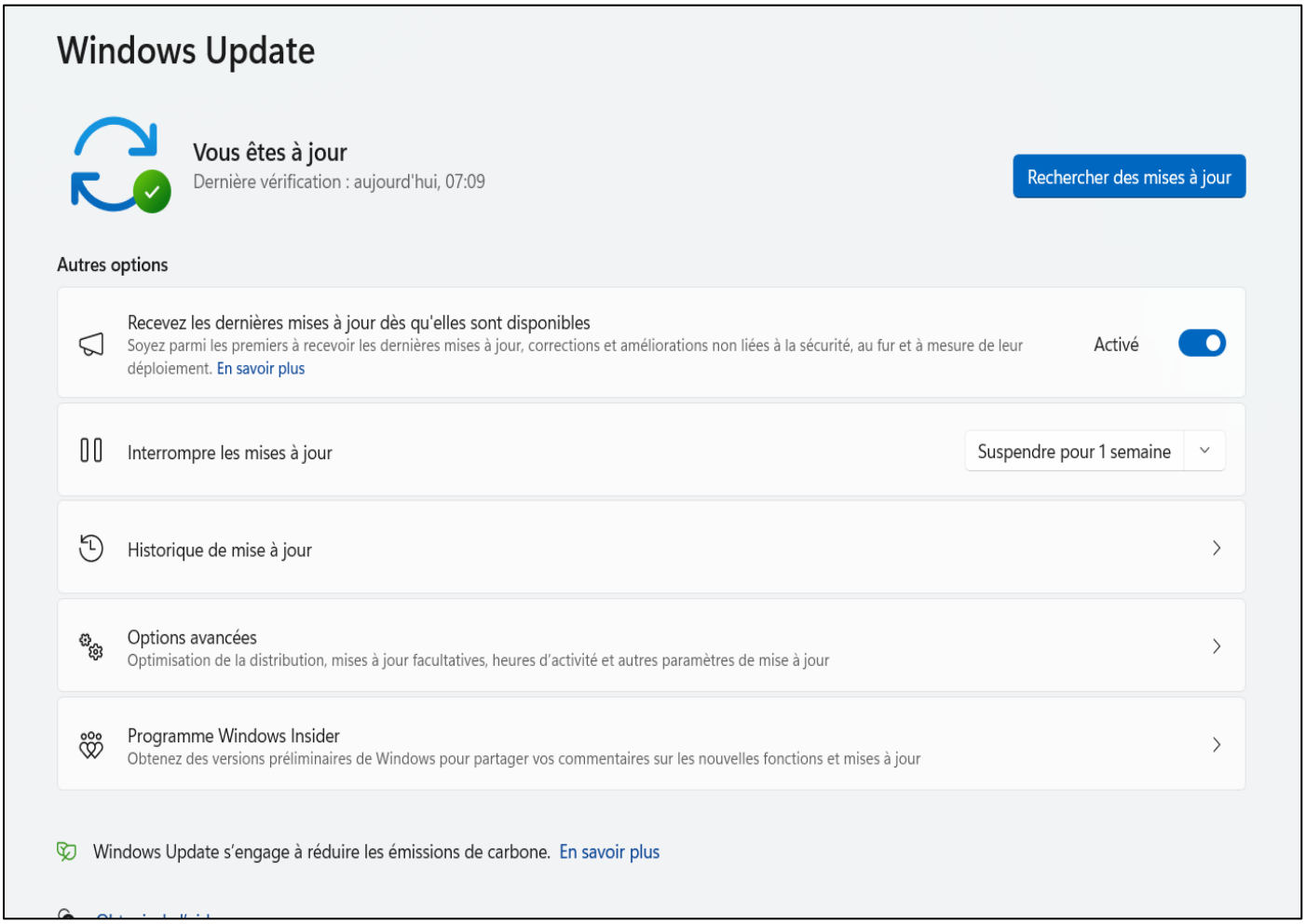

Fig 5 The Windows Update Interface

➢ *Check if you are getting a lot of pop-ups.*

When we use YouTube, Facebook, Google, we see all kinds of advertising windows suddenly appear. Never click or download any software advertised through an ad, even if it is antivirus software. Always download software from trusted websites.

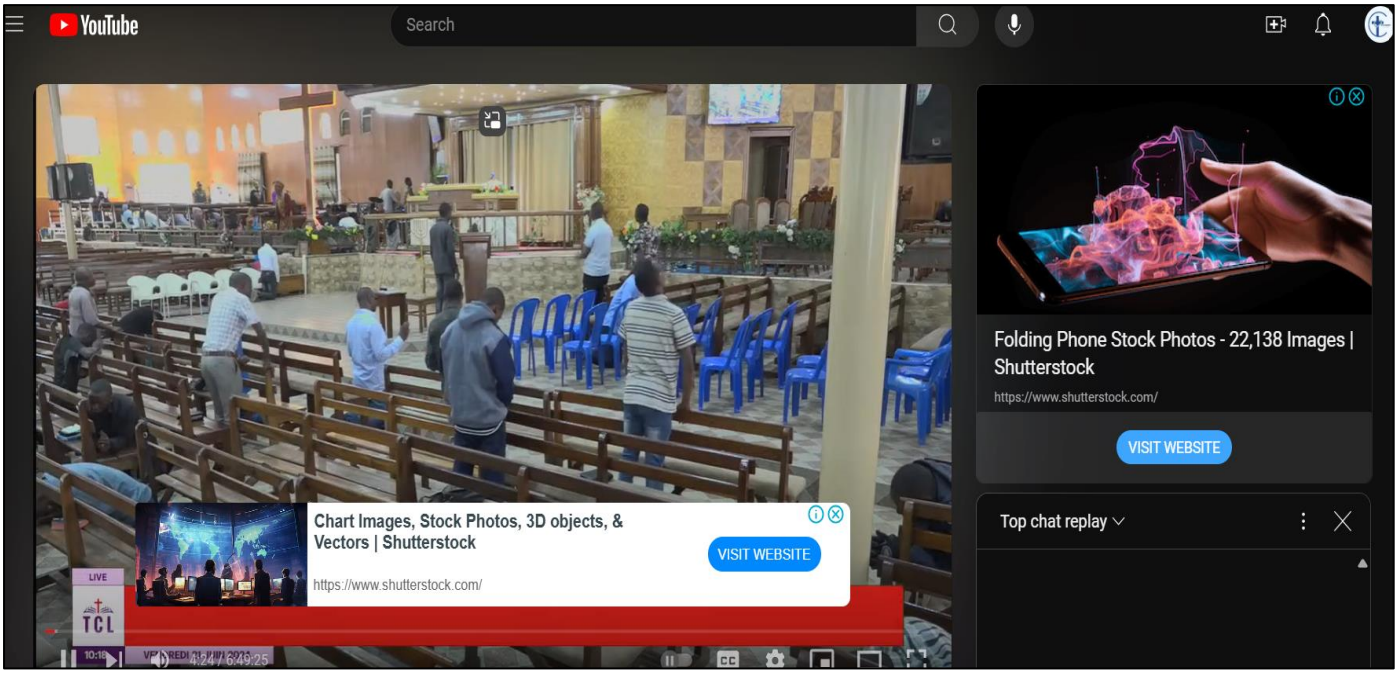

Fig 6 Pop-up Message when using Youtube

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1570

➢ *Be careful if you are being redirected to unexpected web pages.*
If your web browser redirects you to unknown pages on the Internet, your computer may be infected with malware

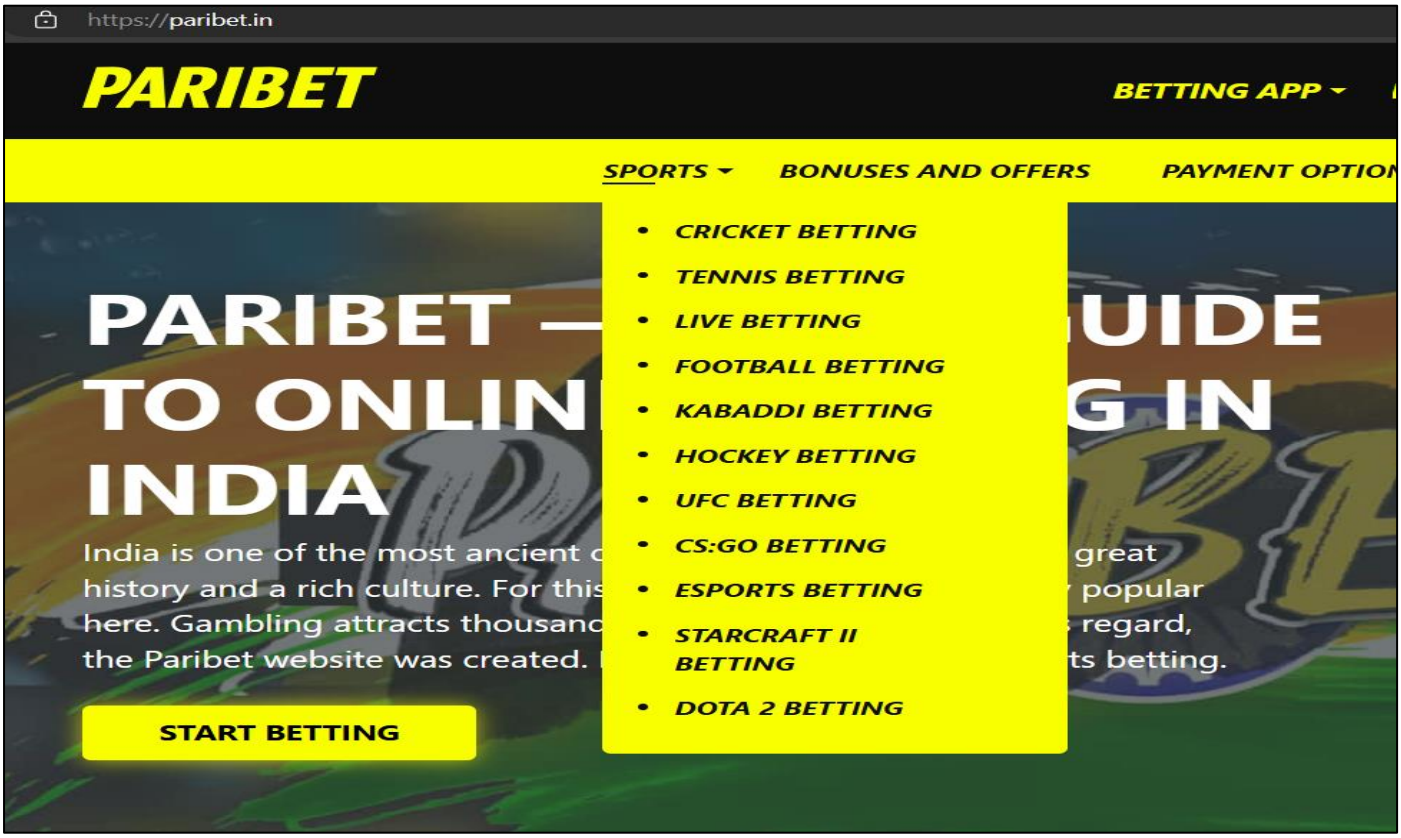

Fig 7 Redirected to Unexpected Web Pages

➢ *Is your Computer Running Slower than usual?*
If you notice this, your computer may be infected with malware that is running tasks in the background and consuming a higher percentage of your computer's resources.

To check resource consumption and stop certain possible tasks, open your task manager by pressing CTRL+ALT+DELETE

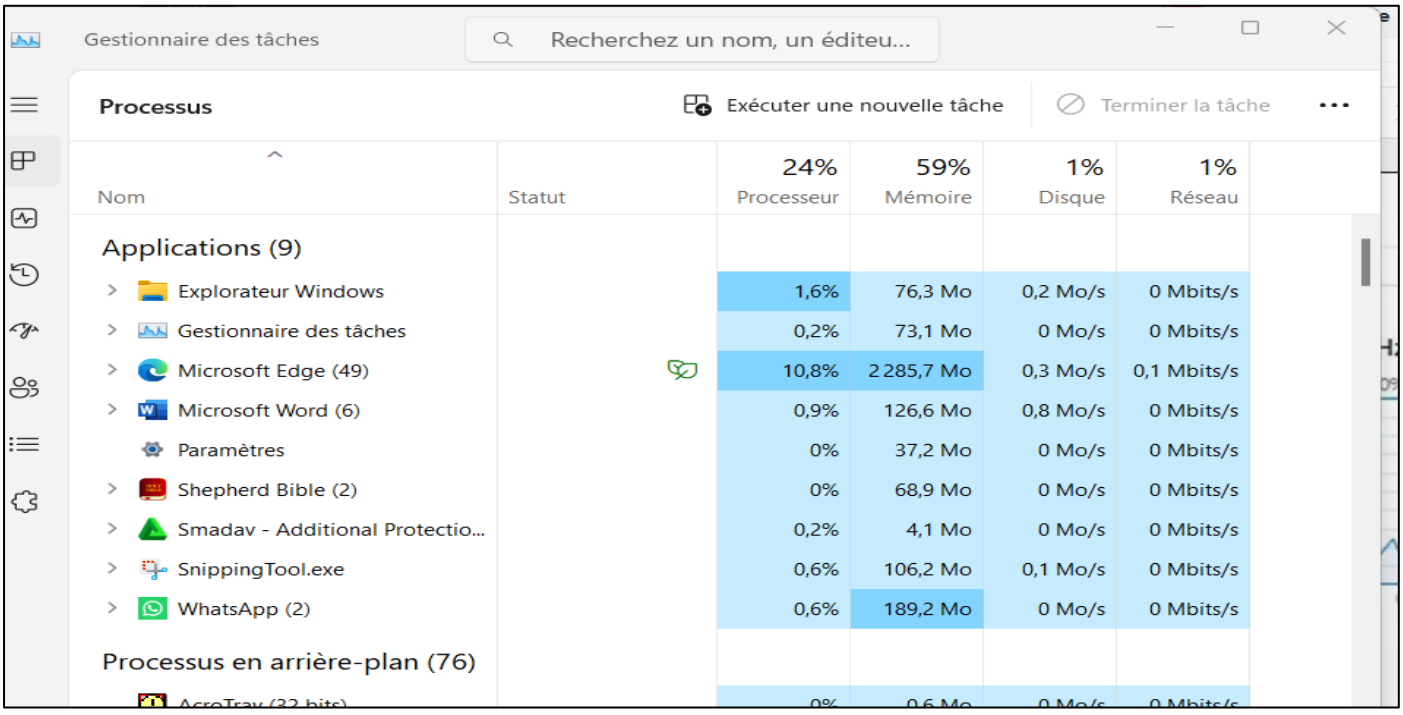

Fig 8 Check Resource Consumption and Stop Certain Possible Tasks

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1570

- *Make it a Habit to always Check if Microsoft Defender and Firewall has been Disabled*

Because some malware has the ability to temporarily disable your computer's antivirus software and firewalls

- *Observe and Trace any unusual Error Messages you may have Received.*

Sometimes malware corrupts your computer and causes it to display strange or unusual error messages when you try to use or access certain programs. Frequent error messages may indicate that your computer is infected with malware.

Fig 9 Unusual Error Messages you may have Received

- *Check your Personal Email and Social Media Accounts Often.*

If you notice strange emails in your outbox that you never composed or sent or if you post and send direct messages on your social media accounts that you did not personally send, your system has may have been infected with malware.

- *Block Notification Messages and Website Location.*

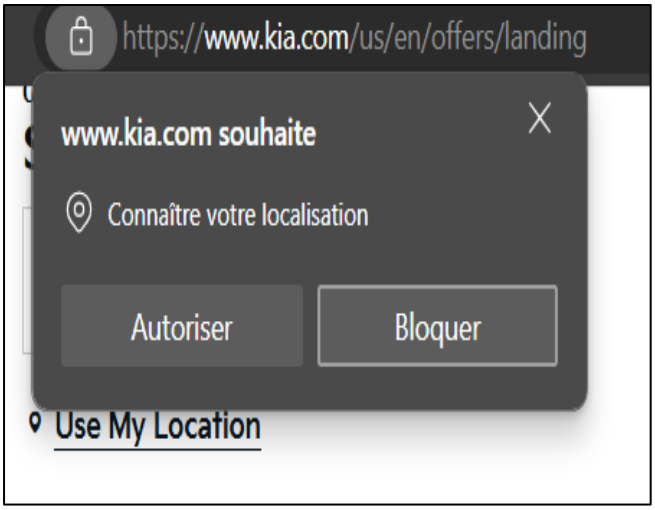

Fig 10 Do not allow notifications and message location

VI. CONCLUSION

We hope that with this article healthcare organizations in the Democratic Republic of Congo will be prepared to face cybersecurity issues and skillful in helping to create a more cybersecurity focused culture within their own organization.

Cybersecurity is a healthcare issue that requires ongoing training and learning and to which everyone must contribute. This article will help apply certain knowledge, tips and tricks to the daily work of healthcare professionals.

If you are interested in learning more about cybersecurity and its implications for healthcare organizations and healthcare practices. Many resources are available. Remember that to properly care for patients, you have to take care of data.

REFERENCES

[1]. https://www.zotero.org/groups/2280149/securehospitals/library
[2]. https://www.onelogin.com/fr-fr/learn/what-is-cyber-security
[3]. https://www.ipac-traductions.com/blog/la-cybersecurite-dans-le-secteur-de-la-sante-quels-sont lesenjeux/#:~:text=Si%20la%20cybers%C3%A9curit%C3%A9%20dans%20le,D%C3%A9programmation%20ou%20report%20des%20interventions.
[4]. https://healthitsecurity.com/news/healthcare-industry-takes-brunt-of-ransonware-attacks
[5]. https://www.arxiv.org/abs/1901.03597
[6]. Brandom, R. (2017, May 19). Almost all WannaCry victims were using Windows 7. Accessed September 26, 2019, from The Verge website
[7]. https://www.theverge.com/2017/5/19/15665488/wannacry-windows-7-version- xp-patched-victim-statistics
[8]. http://www.springer.com/series/5576
[9]. Marco, G, (2014, November). Understanding cybercrime: phenomenon, difficulties and legal responses

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1570

[10]. David, T. (September 28, 2014) Cybersecurity and SMEs. 2014. ffhal-01781568
[11]. Ali, D., Mauro, C., Tooska, D. ( ) Cyber Threat Intelligence- Advances in Information Security 70 (2018)
[12]. Field, M. (2018, October 11). The WannaCry cyberattack cost the NHS £92 million as 19,000 appointments were cancelled. The Telegraph. Retrieved from https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/