NOVA IMS Information Management School

MGI

Mestrado em Gestão de Informação
Master Program in Information Management

# Cybersecurity in Social Networks

Ricardo Jorge Girante Gonçalves

Dissertation report presented as partial requirement for obtaining the Master's degree in Information Management

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

**NOVA Information Management School**
**Instituto Superior de Estatística e Gestão de Informação**
Universidade Nova de Lisboa

# CYBERSECURITY IN SOCIAL NETWORKS

by

Ricardo Jorge Girante Gonçalves

Dissertation report presented as partial requirement for obtaining the Master's degree in Information Management, with a specialization in Business Intelligence.

**Advisor:** *Prof.* Dr. Vítor Duarte dos Santos

JULY 2021

# ACKNOWLEDGEMENTS

I would like to leave here a word of appreciation to all those who contributed directly or indirectly to the preparation of this Master's thesis. In particular, to the supervisor of this dissertation, Professor Vitor Duarte dos Santos, who was always exceptional. Thank you very much for all your support, understanding, help, encouragement, and availability to guide me throughout this journey. I must also thank

I must also thank Nova IMS for the opportunity to integrate this master's degree and be able to learn and develop more skills. Thank you to all the teaching and non-teaching staff for the learning and support throughout this time. To all the people who completed the survey, who were essential for the preparation of this Master's thesis.

To all my colleagues who along this path also helped me to bring this master's degree to a successful conclusion. To my wife, for her unconditional support, help and understanding that were essential to finish my Master's thesis. And finally, to my family and friends who support me unconditionally in everything I do.

A big **THANK YOU** to everyone once again!

# ABSTRACT

In recent years, the use of social networks has been increasing substantially. As we know, platforms such as Facebook, Twitter, Google +, Pinterest, LinkedIn or Instagram allow millions of individuals to create online profiles and share personal information with several friends through social networks – and, often, it's possible to do the same with a large amount of strangers.

By itself, social networks should not be considered a cyber threat. However, there are several issues related to maintaining the user's data security and privacy, especially when they upload personal information, photos and / or videos. The large majority of users ignores the security best practices, which sometimes facilitates the hackers' attacks.

The main goal of this research is to understand patterns of information that are revealed on online social networks and their privacy implications. The goal is to map people behaviour on social networks and understand if they care about the security of their data exposed on the Internet. This research also aims to understand the impact of cybersecurity in social networks and a comparison of which social network is most concerned with the exposure of its user. It will be also addressed the current defence solutions that can protect social network users from these kinds of threats.

## KEYWORDS:

Social Networks, Security Best Practices, User Behavior, Cybersecurity, Defense Solutions.

# INDEX

# LIST OF FIGURES



# LIST OF GRAPHICS

# 1. INTRODUCTION

This research aims to contribute to a better understanding of users' behaviour on social networks. The world's best-known social networks are investing in cybersecurity, especially now with the entry of the General Data Protection Regulation (GDPR), which is a new European reference text on the protection of personal data, that aims to "give back to the citizens the control of their data while simplifying the regulatory environment of companies" (Union, 2018).

The goal is to analyse the user's behaviour and create a model/ list of best practices that can contribute to better use of the social networks.

Cybersecurity in social networks has already been studied, especial by the biggest platforms, such as Facebook and Google. Although most recently, Mark Zuckerberg, Facebook's chairman and chief executive officer, was involved in legal issues when the Cambridge Analytica company utilized the users' data of their social networks without their consent.

What happened to Facebook is just a small example of what is happening worldwide, many people still use social networks to share everything about their lives and it is necessary to study in detail all the promises that lead people to do such things.

## 1.1. BACKGROUND AND PROBLEM IDENTIFICATION

In the actual world or better digital world, social networks have become part of our daily life. Every day all of us post something on LinkedIn, Facebook, or Twitter and we are sharing our personal information with our friends and with persons that are strangers to us.

In the article by Parker (2017), all email users are well-informed about how to handle email security issues, especially the people who deal with work emails every day. For instance, we cannot open emails that seem strange to us and click on unknown links. The malicious methods that are used in emails can also be used in social networks to infect people's computers and smart devices.

Once a single user is infected successfully, the message can be sent back to all that person's contacts. For example, a link shared by a friend on the social network are more expected to be trusted, but when someone clicks on it there is a high probability that it will be redirected to a malicious website.

A recent Symantec's (cybersecurity firm) research indicates that 65 per cent of spear-phishing emails were used by all of the known groups carrying out targeted cyber-attacks. And 96% of the targeted attacks are carried out for the purpose of intelligence gathering (Symantec, 2019).

According to the Benevenuto, Rodrigues et al. (2009), the majority of online video at social networks, such as the world's most popular – YouTube – that allow users to post videos gives the opportunity to introduce reliable content or even poor-quality content.

For instance, when a viral message is spread on WhatsApp, YouTube, Facebook, among others, it can be seen by thousands of people, which can open the "doors" to spammers access to our data. "Content pollution may jeopardize the trust of users on the system, thus compromising its

success in promoting social interactions. Despite that, the available literature is very limited in providing a deep understanding of this problem" (Benevenuto, Rodrigues et al., 2009).

A normal social media user does not care about the security of their data exposed on the Internet. On these days, we need to be more careful about what we post on the Internet. "Malicious users may post video response spam for several reason, including increase the popularity of a video, marketing advertisements, distribute pornography, or simply pollute the system" (Benevenuto et al., 2008).

With the emergence of the General Data Protection Regulation – GDPR (2018), social networks must review and adapt measures to protect their users' privacy. But in reality, it's not enough, as the vast majority of users may not be prepared to defend themselves against constant cyber-attacks.

## 1.2. Research Motivation – Why we should care about this "big" problem?

Before we go further, and in order to answer that question, we have to think about why this is a "big" problem, and to do so, we need to answer these two big questions of this research: "Do users rely on cybersecurity?" and "How concerned are users about the exposure of their data on social networks?". These questions are important, because nowadays everyone exposes their data and probably they don't know how to protect themselves from social network threats.

From the most varied studies that exist nowadays, there is no one that makes a comparison of which social network cares most about its user as well as provide a "guide" of the best cybersecurity practices, so that the user can protect himself from all the threats that may arise during their presence in social networks.

## 1.3. Study Objectives

We all know that social networks are susceptible to cyber-attacks. And with this, it is necessary to examine the social networks and identify network metrics and processes associated with security vulnerabilities. The analysis of the "cybersecurity in social networks" will provide valuable insights into users' behaviour in social networks.

It will be also possible to understand the key factors that lead people to expose their data on the Internet in the way they compromise themselves.

The study will also identify patterns of attacks in different categories and which social network is the most vulnerable. This will be particularly important in understanding the most common social networking issues and how to avoid them so that people can deal with very specific cases.

Besides that, it will be possible to perceive if social network users really trust on cybersecurity and whether they are willing to pay for software to be more secure on their electronic devices.

All these research questions are based on the following:

- Are there social mechanisms to improve network security?
- Are there different security and privacy threats in social network platforms?
- Which social network provides the best data security?
- How concerned are users about the exposure of their data on social networks?
- Do users trust in cybersecurity?

## 1.4. STUDY RELEVANCE AND IMPORTANCE

Social networks are extremely popular in today's world. Thousands of people use social networks, for example, Facebook was the first social network to surpass 1 thousand million registered accounts and currently sits at 2.79 thousand million monthly active users (Statista, 2021).

A recent study by Global Social Media Stats (n.d.), shows that as of early January 2021 there are 4.33 thousand million social media users around the world which represents more than 55 per cent of the total global population.

Social networks allow individuals to connect with unknown people, friends, family and share their private information. However, the sharing of information can bring some problems to maintaining privacy. The shared content carries information that can be transmitted in a viral and almost instantaneous way.

This shared content can be problematic in the sense that user's private data is exposed to the Internet, and this can have serious consequences. For instance, this may open the "door" for hackers to access our private information and to use our data in its benefits, such as using our bank details to do online purchases, or even know where we live.

In this research, it will be present a comprehensive survey of different security and privacy threats that target every user of the social networking platform. In addition, it will be discussed current defence solutions (cybersecurity) that can protect social networks users from these threats and if there are better defence solutions than the worldwide best-known antivirus, as well as users' behaviour in dealing with these issues and if they care about the exposure of their data on the Internet.

As it is well known, in large industrial organizations, the Cybersecurity of Industrial Control Systems (ICS) does not always get the same level of attention and protection as a corporate infrastructure.

Nowadays, there are still organizations that may also show a lack of useful and specific knowledge regarding the cybersecurity of operational technology (OT), even containing experts who perceive corporate cybersecurity.

## 2. METHODOLOGY

The Research Design approach to the topic of the master thesis will be based on the mix of two methods: Quantitative and Qualitative methods. Those methods will answer the five questions presented in the "study objectives" topic.

The Quantitative Method will be the major focus of the research with the analysis of data provided by the social networks regarding the information on what type of attacks exist in social networks (Hackers, Phishing, Malware, etc.), and how to avoid such problems.

In the Qualitative method, it will be presented a sample of 170 people randomly chosen and for this purpose will be used a survey to perceive the users' behaviour about the constant threats of the social networks. The research also aims to understand if they are concerned with their exposed data on the Internet and what they do to get around these daily threats in their online accounts, such as if they trust in cybersecurity mechanisms.

As it shown in Figure 1, the research is distributed into 8 steps.

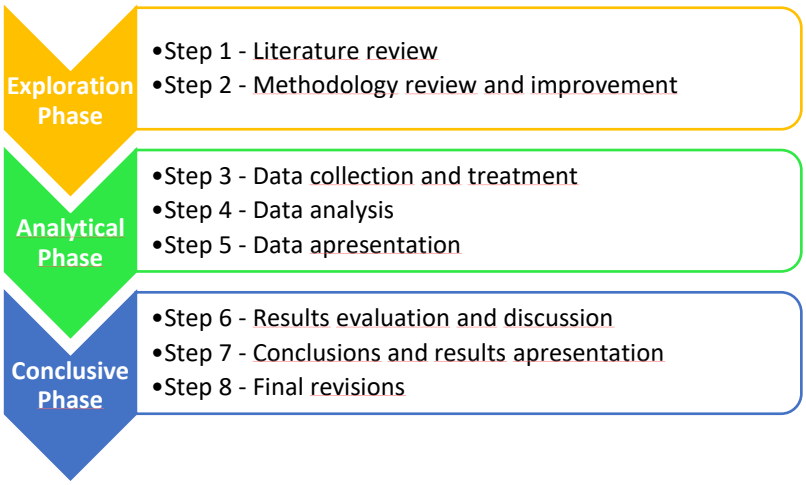



Figure 1 – Research steps

In the first step, a literature review is done, which is divided into two parts.

- The first part talks about what social networks are, what their purpose is and how they work, as well as their advantages and disadvantages.
- In the second part, a review of the computer security literature is made. Where the subject of cybersecurity is addressed, when it emerged, what is its concept and what types of viruses exist. However, the focus of this work is on cybersecurity in social networks.

At steps 3, 4, 5, all the collected data will be processed and analysed with an algorithm that will provide inputs that will allow answering the research questions. Moreover, it will be done a search about privacy, security, people behaviour, among others, so that it can be demonstrated in the research the best practices of protection against cyber-attacks.

Steps 6 and 7 will discuss the results of the analysis made in step 5 and finally will show the recommendations so that users can be more aware of cybercrime and also change their behaviour on social networks. Lastly, in step 8 will be discussed the conclusion, limitations, and future work.

# 3. LITERATURE REVIEW

In this topic, a systematic review of the literature will be made, to make known what social media is and its derivatives (Social Networks, Social Communities, types of social networks), as well as its advantages and disadvantages. The topic of computer security will also be addressed with the following topics: Cybersecurity, concepts, threats, and cybersecurity in social networks.

## 3.1. SOCIAL MEDIA

The concept of social media refers to several online communications channels dedicated to interaction, content sharing and collaboration with other users in real-time. In fact, social media tools started with computers, lately, they were expanded to other devices, like smartphones and tablets.

Social Media transformed the way we live today because we can buy something on the Internet, we can share photos, events, white papers, our localization in real-time to generate engagement with our fans and followers and wait for their interaction.

One of the world's most respected analysts and award-winning author, keynote speaker Brian Solis, in 2008 had decided to categorize social sites and services into various types of social media by creating a social media chart, called "The Conversion Prism", as shown below.

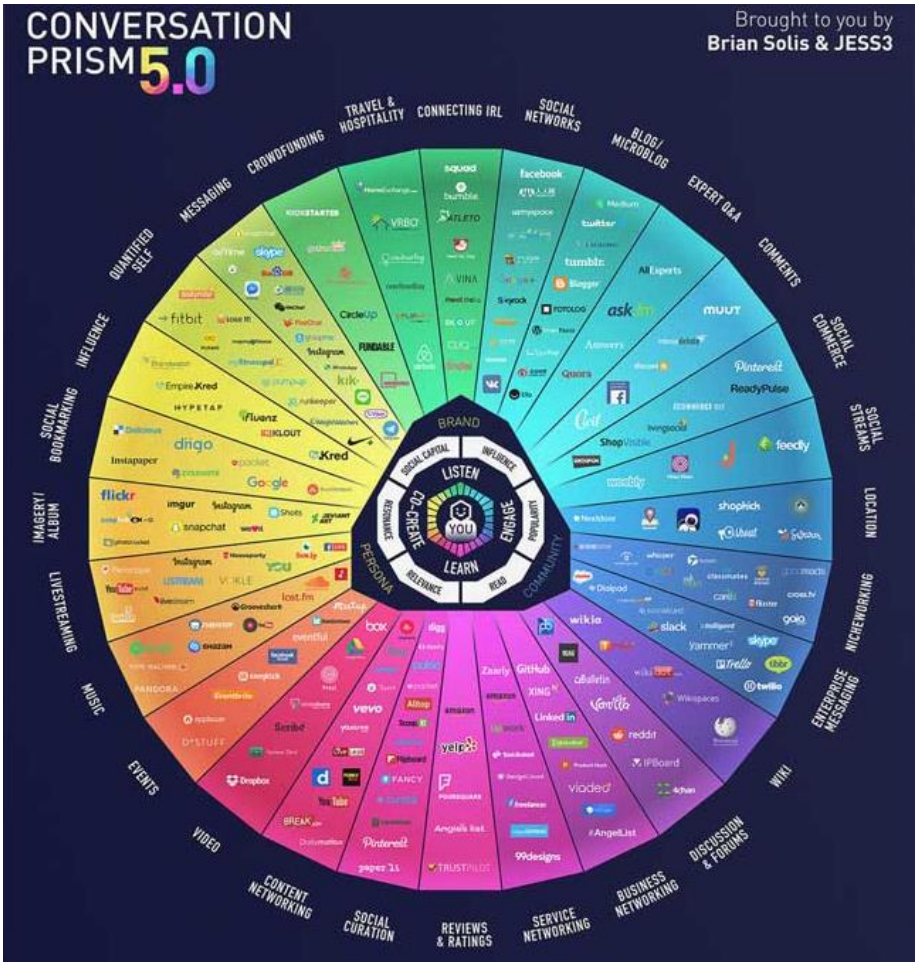



Figure 2 – The Conversion Prism

“The Conversation Prism is meant to help viewers better understand and appreciate the state of ‘the statusphere’, and how it’s evolving, so that they may play a productive and defining role in shaping how businesses, educational organizations, governments, and everyday people engage, communicate and build mutually-beneficial communities.” (Solis, 2017).

The Social Media concept includes social networks, apps, forums, and websites with reviews, among other social communities online. For this research, the focus will be Social Networks that is referred to the creation and maintenance of personal and/ or business online relationships.

### 3.1.1. Social Networks/ Social Communities

#### 3.1.1.1. Social Networks

According to Samur (2018), the idea of social networks appeared in the 1990s. The first social network to be created was Six Degrees (1997-2001), its users could create their profile and add other users, reaching around 3.5 million users. Nowadays and as the site Datareportal (2020) indicates, in 2020 there are about 3.80 thousand million people active on social networks.

“Social networks, such as Facebook or Twitter, are currently the applications with the greatest contribution to the digital footprint of Internet users”, (Antunes & Rodrigues, 2018). As mentioned by the two authors, these two social networks are the most widely used today, since their main objective is to establish and strengthen “social relations” between people with common interests.

The main purpose of social networks is to connect people to each other, whether they are known to one another or not, and as time went by and already in the new millennium, user-oriented sites started to appear, among them Myspace, Orkut, hi5, LinkedIn, among others. No one would believe that Social Networks would remain until today because the vast majority of social networks cannot keep their user for too long.

The emergence of social networks has enabled users to establish virtual relationships with other users, from whom they have an affinity.

For each user, these networks store a set of information, such as their personal data, messages, multimedia contents, that has been produced over time, stored in chronological order and it is possible to obtain information at any time through the digital footprint produced by each user.

As it is well known, there are several motivations for the use of social networks by companies or individuals, and individuals emphasize the need to have a network of “virtual friends” with whom they can share their interests, answer questions, comment on publications and talk in real-time with through messages.

Concerning companies, their main goal is to promote their services/ products together with a large number of customers or potential clients using the same social networks. To set the example companies have begun to turn more to digital marketing to advertise their products/ services to their customers through strategies on social networks.

With the emergence of social networks some new terms also appeared according to the application.

To start, when a user registers in any social network automatically becomes a **member** and has an associated **profile**, and from that moment the member of the social network will have the **page** with his information made available to the other members that can do it a **request for friendship** (Antunes & Rodrigues, 2018).

The member has a list of **friends** who may or may not grow over time, you can also **post** posts at your page that can be commented or shared. Each member linked with another user receives all the updates of the posts of each other, ordered chronologically, that is a **feed**.

Members can also identify their **friends**/ **links** in their posts. In social networks, there is also the possibility to create **groups**/ **channels** according to their interests.

In each type of social network, we can verify there are at least one of the three options:

**Friendship –** This type of relationship is done by sending a request for friendship, and the information shared will become available in the feed of both members.

**Fan –** This type of relationship is most commonly used between members and the pages of brands and/ or companies. The member subscribes the page and has access to the content published by the companies through its feed.

**Follower –** In this case, the member can only choose to follow another member, as is the case of Twitter that allows you to follow personalities. It does not imply to send and accept a friend request. It is a unilateral relationship in which the follower does not receive content published by his followers in his feed.

The vast majority of social networks have adopted these terminologies, but for example, in the case of Twitter posts, are considered tweets and have a maximum of 140 characters and are classified by several words preceded by a hashtag (#) and republishing a post is called a retweet.

### 3.1.1.2. *Social Network Organization*

Conceptually, a social network is seen as a set of bidirectionally related “members”, according to figure (3). Each of the members is connected directly to others and this link corresponds to a friendship between the two users (Antunes & Rodrigues, 2018).

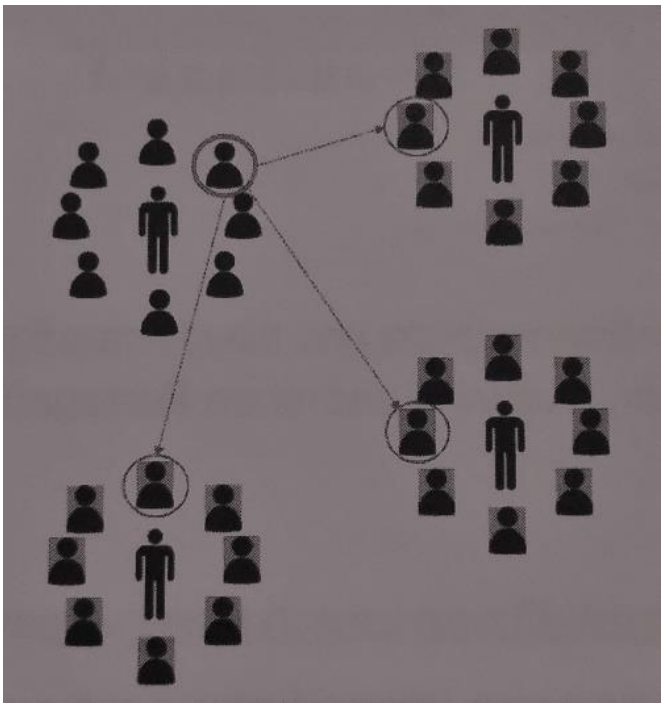


Figure 3 – Social Networks organization.

### 3.1.1.3. *Social Network Contents*

Social networks can cover the most varied formats of content that essentially depend on a set of publication rules defined by each type of social network and the type of content is authorized. As well as the features that are available also vary between each type of network. To illustrate this, below we ca see two images of publications made in two of the most used networks in the world, Facebook and Twitter.

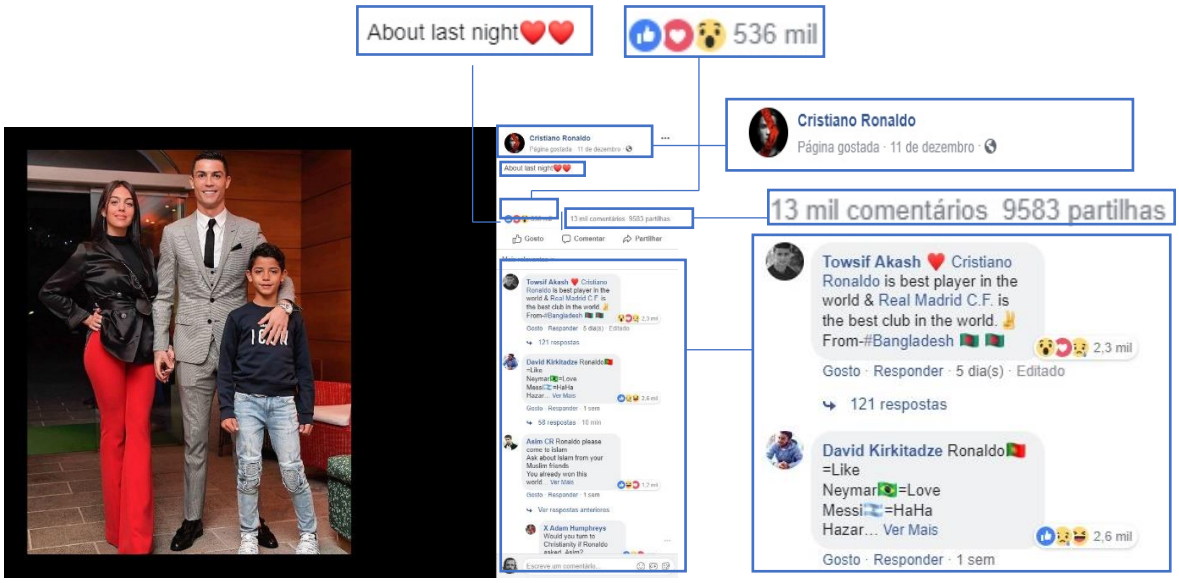



Figure 4 – Facebook Post

As shown in the figure above, we can observe that a post is divided into the following elements:

- Content – Text message and a photograph.
- User identification – The post was placed by the user “Cristiano Ronaldo”.
- Comments – This post has 13 thousand comments.
- Emotions – This post obtained three types of manifestations from 536 thousand users.
- Shares – The post in question was shared 9583 times.


Figure 5 – Twitter Post

The above image is from Twitter. In this case, the publication has the name of tweet, and we can identify:

- User identification – The post was placed by the user "La Liga".
- Hashtag – The hashtag is "#LevanteBarça".
- Content – The content consists of a short text message.
- Retweets – Retweets indicate the number of times this tweet was shared; in this case it was shared only 19 times. Each time you retweet it, it is possible to see the message that accompanies it.
- Emotions – This post obtained 74 emotions.

#### 3.1.1.4. *Social Communities*

A Social Community or online community is not built or befriended, but it is a group of people with something in common, where they can share experiences, ideas, goals, shared interests, thoughts, and solutions (usually these networks are non-profit) (Bond, 2020).

There are several tools to bring together communities for discussion on topics that a community or network finds mutually interesting or beneficial. "Stack overflow" and "Zwame" are an example of a social community where we can share our doubts, ideas, and solutions for other people.

Social communities are online communities that use social platforms, they can include personal communities and communities as they are built using tools such as LinkedIn.

As said before an online community it's a group of people based on proximity and with something in common, like experiences, ideals, goals, or profiles.

In some communities, its users are “invisible”, such as a community that accompanies a blog. In the community that accompanies the blog there is always a central community of believers/ fans of a specific blog and other people who are only interested in a specific subject of that same blog that continue to frequent the site. But most of them will not make any kind of commentary on the published articles.

As a way to identify who does not make comments the author of the blog can create forms and mechanisms to offer a voucher, or even a discount on any article in order to retain people to your site.

In other communities, it is easier to identify users because they are built on the profile of each user’s interests.

In the image below we can see how the inspired vision of an engagement funnel (different types of communities) shows how users interact with brands (Aboulhosn, 2020).

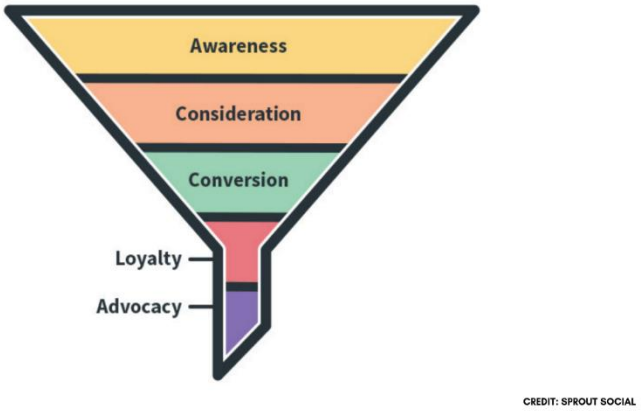



Figure 6 – Social Media Engagement Funnel.

According to Bradley and McDonald (2011), the Gartner group has created six basic principles of community involvement for a social community to succeed and enjoy the participation of its users, as mentioned below (figure 7):

1. **Participation**

    a. Some companies see social networking as a good opportunity to release some information to focus on the user’s attention.
    b. The design of social networks becomes the main focus of companies and with this, they sometimes lose the notion that they should focus more on “please” the customer.

2. **Collective**

    a. It's so easy to get people to join a community and contribute to their growth.
    b. A plan must be created to be able to "reach" the target audience.

3. **Transparency**

    a. Successful communities allow users to see the participation of other users, generating mutual knowledge.
    b. For this purpose, community network managers provide the means for their followers to evaluate other users' posts, for example by rating the post of other users with stars or allowing feedback from the post to improve communication.

4. **Independence**

    a. In social communities, there has to be dependency so that anyone can participate, but for this, the moderator and/ or certain mechanisms can filter which types of users can participate in their sites to avoid generating conflicts.

5. **Persistence**

    a. Other great features of community networks are the ability to retain information and interactions among their users.

6. **Emergency**

    a. The fact that there is a giant collaboration on the part of its followers also causes certain behaviours to appear gradually as an interaction exists. These behaviours must be regulated but so that the communities themselves have the autonomy to manage themselves by creating productivity.

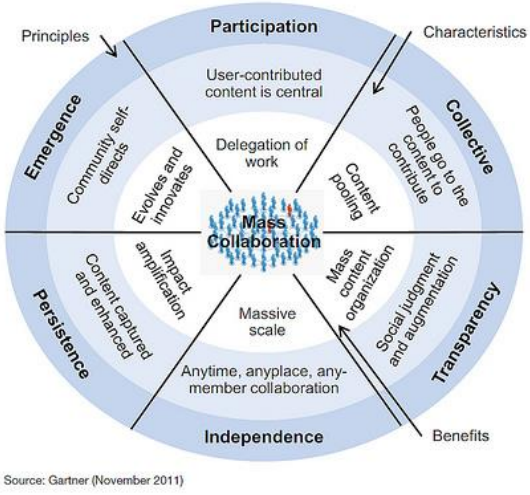



Figure 7 – Six core principles of community participation according to Gartner.

### 3.1.2. Typologies

There are several types of social networks, divided into different types and according to their purpose, that will be demonstrated below:

#### 3.1.2.1. Social Networks

According to Antunes and Rodrigues (2018), social networks are divided into five categories:

- **Generalists**
    - Relationship Social Network: This kind of social networking is meant to connect people from all over the world. In fact, the biggest goal of social networks is to create a relationship between users. Among them, there are LinkedIn, Google+, etc.
    - Professional Social Network: They are social networks that aim to generate professional relationships with other users, by exposing their curriculum and skills, getting leads, jobs etc. As an example, we have the social network LinkedIn the best-know and the most used around the world.
    - Niche Social Network: Targeting a specific audience, be it a professional category or people who have a specific common interest. The best-known case is TripAdvisor, where users give ratings to places related to the gastronomy and tourism industry.

- **Multimedia**
    - Entertainment Social Network (Multimedia): The focus of these social networks is not to create relationships between their users, as seen in the point above, their main goal is content consumption. The biggest example of such social networks is YouTube, being the largest video distribution platform in the world, where the goal is to publish and watch videos.

- **Microblogging**
    - The microblogs provide the origin of blogs, where it is nothing more than a mini version of the original blog, but with fewer features and interface options. These blogs have an average character size of 120-180 per post, not exceeding three lines. As an example, the most popular service in the category is microblogging Twitter with the slogan “What are you doing?”.

- **Messaging**
    - The Messaging Social Networks are platforms that enable messaging, many of which started around social networking platforms, like Facebook. Facebook Messenger and WhatsApp are the best-known platforms that enable the user to interact with everyone that is on their network.

- **Games**
    - Like the Messaging Social Network, in this one (Game Social Network) user has the games he bought, and he can chat with anyone on their network. Steam and Origin are the best-known platforms that enable us to play multiplayer games and chat with other users.

### 3.1.3. Vantages and disadvantages

Social networks and social communities are already part of people's routines. This “fashion” has made brands and companies also begin to use and interact with their prospects and customers, bringing some advantages and disadvantages to society, such as:

#### 3.1.3.1. *Vantages*

1. Social networks provide us with great ease of communication, they allow connections with a lot of people, regardless of their location.
2. The search for old friends, family, etc. The social network gives us the possibility to find people who have moved from a long time ago, colleagues and even relatives.
3. Due to a large number of users, social networks provide the possibility that all members discover friends according to their interests and hobbies.
4. Social networks can be well used as Internet ads and, looking at the number of visitors, to very effective ads, bringing incredible possibilities to find good job offers.
5. Being able to participate in discussion groups is another positive aspect of social networks. Some groups gather people interested in exchanging information on a range of subjects, such as illnesses, doubts, courses, books, etc.
6. Companies can have a much more personalized and direct relationship with each client or possible client, since you can contact each one, either to solve problems or give new information.
7. Be able to know more about each of your customers: people share their likes, desires, and other information that can be valuable to businesses when it comes to getting close to their target audience.
8. Real-time information: Social networks allow you to communicate urgent brand messages on an official channel.

#### 3.1.3.2. *Disadvantages*

1. The information provided in social networks can be used by anyone without the users having any knowledge about it.
2. Contact information can be used for spam.
3. sometimes social networks can even harm families, and users who are very interested in social networks, because they spend all their free time online and do not pay attention to the people around them.

4. Parents should monitor what their children are doing in order to prevent them from being victims of malicious people, such as paedophiles.
5. A large number of people cannot spend a day or even a few hours without visiting the social network. The vice of people and the absence of the Internet becomes a disaster and people do not know what to do when cannot access online communication.
6. Dissemination of false information is another problem that occurs in social networks. The spread of false information leads to gigantic proportions, even seriously damaging the victims of such lies.
7. Most people demonstrate their lives on social networks, that is, they tell where they live, to where they travel, where their children study, etc. This information is a gateway to the wrong people who can use this information to plan robberies, kidnappings, etc.

## 3.2. COMPUTER SECURITY

### 3.2.1. Cybersecurity

With the emergence of social networks and the advancement of technology, it was necessary to create something that would allow the safeguarding of users of social networks, so, in the 80's, emerged the concept of cybersecurity (Academy, 2021).

According to Shea (n.d.), "Cybersecurity is the protection of Internet-connected systems such as hardware, software and data from cyberthreats. The practice is used by individuals and enterprises to protect them against unauthorized access to data centers and other computerized systems". Cybersecurity consists of a set of technologies, designed to protect networks, data, and systems against cyber-attacks.

Some people consider the emergence of cyber-security as the third industrial revolution, where the presence of large-scale information and communication technologies, involved in various areas of human activity, is observed, and has the capacity to reduce the risk of attack and protect against the unauthorized entry of third parties into the systems.

### 3.2.2. Concepts

In order to have a successful cyber-security system, it is necessary to fulfil three great characteristics, known as the Triad CIA (Walkowski, 2019), a concept without whom it would not be possible to implement any kind of cybersecurity. And the three big requirements are:

1. **Confidentiality**
    - There can be no access to information to unauthorized users or systems. In other words, only users and systems with the appropriate privileges (legitimate entities) can have access to information. With the guarantee of confidentiality, third parties who obtain information between a sender and a recipient will not be able to extract comprehensible content from it.
2. **Integrity**
    - Integrity is related to confidence in the information obtained, that is, the information in question cannot be altered by unauthorized parties.
    - If there is a break in the integrity of the information, it can only be resettled if you change the information content or even the structures that support the storage of the content.
    - Confidentiality and integrity are ultimately dependent on each other, if confidential information is lost, integrity mechanisms are at risk of being disabled and the basis for confidentiality is not at all reliable.
3. **Availability**
    - Availability ensures that authorized users have access to certain types of services/ features whenever access is requested.


Figure 8 – Triad CIA.

### 3.2.3. Treats

In recent years, cyber threats have increased in severity, as the tendency of certain types of users to attempt to expose flaws in security systems in order to compromise the infrastructures of companies and individuals. Every day, a new virus is placed on the web and these security breaches cost companies several million of euros.

Although security is continually moving forward to combat new threats from hackers, human behaviour changes very slowly and as such, unauthorized third-party entries and privacy breaches continue to occur very frequently. The biggest threat is not whoever tries to enter the network, but whoever leaves a "door" open to a threat.

According to IBM's report (IBM 2015 Cyber Security Intelligence Index) "Human error is almost always a factor in breaches," although data show that about 23.5% of the attacks are conducted inexorably and 31.5% have been malicious, most of the problems/ violations, about 95%, come from someone who makes a mistake and leaves a breach to anyone else. Threats can arise from any part of a company, and users who have more permissions are sometimes the ones that leave more holes in the computer networks.

In this chapter we will discuss in general what types of threats exist on the web:

1. **Nonrepudiation:**
    - Through the non-repudiation technique, although it is not easy to know who had access to the page, it is possible to keep track of who caused the threat. For example, if a user sends a message and says he did not do it, nowadays it is possible to check whether he did it or not through, by analysing the weblogs (Finjan Team, 2017).
2. **Authentication Violation:**
    - Most of the time, users use passwords relatively easy to remember, such as password 123456, and this facilitates theft and allows unauthorized access to their account
3. **Trojan Horses and Virus:**
    - These are malicious programs that provoke various kinds of attacks, in which, for example, viruses spread from machine to machine, if they are connected to the same network and delete important files. Trojan horses may leak information to a low level (University Information Technology Services, 2021).

4. **Phishing:**
    - Phishing is a way for the hacker to introduce himself as a trusted person to any entity, through email, or other communication channels, to distribute malicious links or attachments, to defraud anyone who opens the emails or attachments. This action is done by extracting the access credentials to the machines.
5. **Malware:**
    - Malware is malicious software that includes ransomware, viruses, worms, and spyware. This threat enters the network through a vulnerability, usually when the user clicks on a dangerous link or opens an attachment in an email and installs malicious software. As malware enters the network, access to the main components of the network (ransomware) installs additional malicious software and obtains all the information available on the network without the user being aware of what is happening.
6. **Zero-day attack:**
    - Zero-day attacks occur as soon as a vulnerability appears, long before any solution or patch that solves the breach is installed. Hackers try to exploit the breach during the vulnerability.
7. **SQL injection:**
    - SQL injection occur when the attacker inserts malicious code on a SQL server and forces the server to reveal all its information.

### 3.2.4. Cybersecurity in Social Networks

As previously stated, the main purpose of social networks is to connect people and organizations. Social networking has not only brought significant changes to the way people communicate, but also to everyday concerns about user privacy and security.

Social networking security focuses on malware detection, as it can come from a "trusted" contact and users click on what has been made available by that contact. However, the misuse of social networks can compromise all personal and financial information exposed, so it is necessary to adjust some precautions, so that the user is not caught by surprise.

According to Antunes and Rodrigues (2018), Both cybercriminals and malicious software are always lurking in a loophole to be able to extract some information to gain access to all user accounts, and this brings several problems, such as:

- **Social Engineering:**
    - It aims to obtain private information. This technique is most often used by users who resort to fake profiles to obtain information that allows them to inflict some harm on the victim. The most commonly used social engineering techniques in social networks stand out as follows:
    - The attacker attempts to obtain personal and confidential information (telephone, address, passwords) from the victim through a false profile.
    - Through a fake profile, an attacker can use a phishing attack, athwart of sharing a credible link in order to obtain personal information.
    - If the attacker obtains the password to access the victim's social networks, the victim may share fake content with the victim's contacts. Through this technique, the aggressor can promote a digital "persecution", through the actions that other users subsequently generate in their shares.
- **Content Sharing:**
    - Sharing content with other users is one of the main reasons for using social networks. The wide range of possible content to share ranges from files to posts, and multimedia content, but there are precautions that must be considered when they are published on social networks. Among them are:
        - The sharing of personal information, such as bank accounts and passwords, involves some risks, as the data is sent over the

Internet and, in certain cases, through unprotected networks, which could lead to its theft.

- Sharing of multimedia content can provoke defamatory reactions and comments that are very harmful to people who post certain content.
- Geo-referencing stores the geographic coordinates of the user's location which, in turn, can make it easier to share the location of the photos that are posted and can make another user recognize the location, so that the location of the person who shared the location be robbed.

- **Cyberbullying:**
  - Cyberbullying can be considered one of the main threats hanging over social networks. Like bullying, cyberbullying is a threat that aims to inflict psychological damage on victims by spreading content that compromises them.
  - When this practice is carried out and, most often, leads to digital harassment, either for inappropriate messages or comments, unfortunately, many of these cases have a tragic end to the victims who cannot get rid of the aggressors and end up committing suicide.
- **Legal Issues:**
  - There are legal risks associated with the use of social networks, that if any user posts content that is offensive to a community or country, they may face sanctions for their actions.
- **Privacy of Data:**
  - Users sharing their personal information on the Internet may cause privacy vulnerabilities unless they act appropriately on computer security.

# 4. STUDY

In this chapter, the description of the study is presented in three phases. Section 4.1 discusses the conceptualization and design of the survey, showing how it was developed.

Section 4.2, divided into three parts, is where the analysis of the survey is made. Finally, in the third part, an analysis of the results obtained in the survey is made and recommendations are also presented for users to know how to protect themselves from cybercrime.

The study main goal is to understand how people behave online and then to recommend best practices to protect themselves from threats on social networks.

## 4.1. CONCEPTUALIZATION & DESIGN

In order to understand what people's behaviour is, and how they protect themselves from cyber-attacks on their social networks it was built a survey. Survey questions are answered with the support of literature reviews.

The structured survey is made up of three parts. The first one (Section A) aims to characterize the respondents, through gender, age, education, and occupation. The second part (Section B) of the survey is where we will understand how people behave on social networks and what they think about them is composed of 9 multiple-choice questions. Lastly, the third part (Section C) of the survey is where we will notice people's behaviour in cybersecurity is composed of 8 multiple-choice questions.

Information related to social media, identification of the Social Networks/ Social Communities, its typologies, advantages and disadvantages were addressed in section B, using the following questions:

- How much time do you spend on social media per day?
- Which of the following social networks do you use?
- What are you looking for in Social Networks?
- Which are the most negative factors in the use of Social Networks?
- Which are the most positive factors in the use of Social Networks?
- What goal did you achieve on Social Networks?
- In your opinion, in which area do Social Networks makes the most impact?
- Which device do you prefer to access Social Networks?
- How many friends do you currently have on your Social Networks?

Information related to computer security, cybersecurity, their concepts, treats and cybersecurity in social networks were addressed in section C, using the following questions:

- Do you keep the passwords saved in the browser?
- Which social network provides the best data security?
- Do you trust in cybersecurity?
- How well informed do you feel about cybercrime risk?
- Do you agree or disagree with the following statements?
    - I avoid revealing my personal information.
    - The risk of being a cybercrime victim is increasing.
    - I'm concerned that my personal information isn't secure on the websites.
    - I'm concerned that my personal information isn't protected the public authorities.
    - A protection tool, like an antivirus, will protect me from cybercrime?
- Cybercrimes include many types of criminal activities. How concerned are you, personally, about experiencing or being a victim of the following situations?
    - Device infection with malicious software (malware, etc.).
    - Identity theft (someone that steals your personal information).
    - Bank card or online banking fraud.
    - Hacking your social networks or email account.
    - Online material that promotes racial or religious extremism.
    - Cyber-attacks that prevent you from accessing online services, such as your bank account.
    - Payment request in exchange for regaining control over your device.
    - Online fraud in which purchased products are not delivered, counterfeit or do not correspond to the advertised.
- In your opinion, which of these situations represents a very serious, reasonably serious, minor crime or is it not even a crime?
    - Infection of devices with malicious software (malware, etc.).
    - Identity theft (someone that steals your personal information).
    - Bank card or online banking fraud.
    - Hacking your social networks or email account.
    - Online material that promotes racial or religious extremism.

- Cyber-attacks that prevent you from accessing online services, such as your bank account.
- Payment request in exchange for regaining control over your device.
- Online fraud in which purchased products are not delivered, counterfeit or do not correspond to the advertised

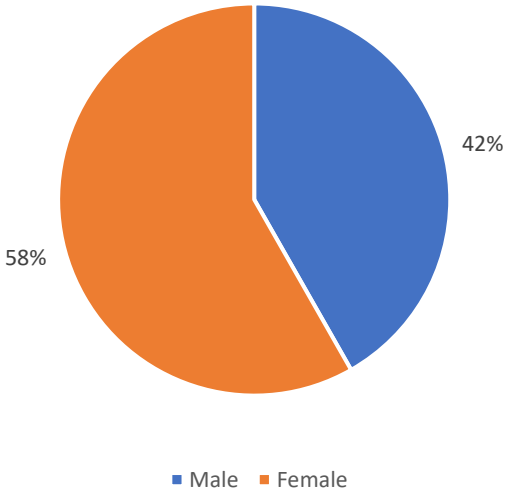
- What would you do in the following situations if you had been a cybercrime victim?
  - Discover malicious software on your device (virus, etc.).
  - Identity theft (someone that steals your data).
  - Being a victim of online bank or bank card fraud.
  - Find online child pornography.
  - Hacking your social networks or email account.
  - Finding online material that promotes racial or religious extremism.
  - Payment request in exchange for regaining control over your device.
  - Receive fraudulent e-mails or phone calls asking for your personal information (e.g., login, computer access, fraudulent payments, or your bank information).
  - Online fraud in which purchased products are not delivered, counterfeit or do not correspond to the advertised.

The structured survey is available in the annexes, in order to facilitate the analysis of the questions proposed to the respondents.

## 4.2. SURVEY

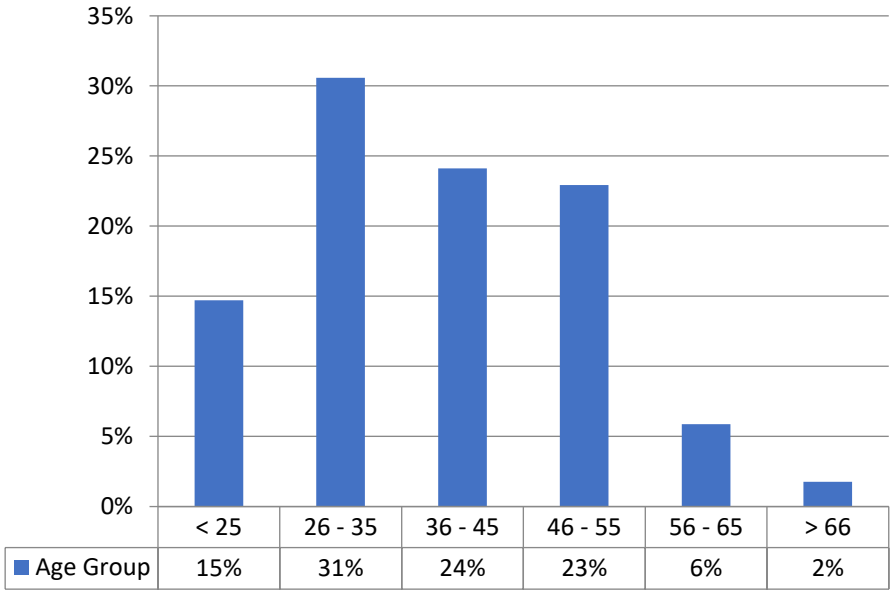
After the creation of the structured survey, it was made available online, on Facebook, LinkedIn, and email platforms, obtaining a total of 170 final responses.

### 4.2.1. Part A – Characterization of respondents



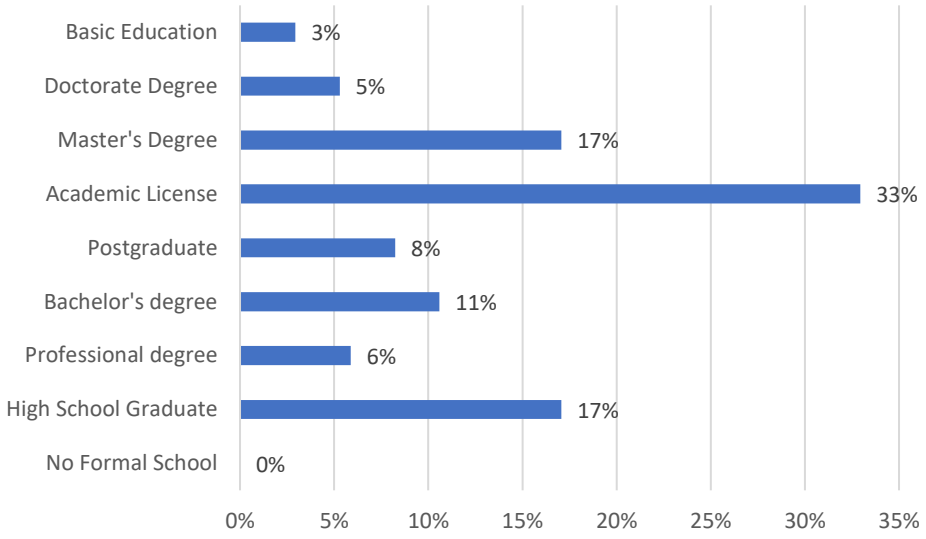

Graphic 1 – Gender of Respondents.

Of the 170 respondents, 99 (58%) are female and 71 (42%) are male.



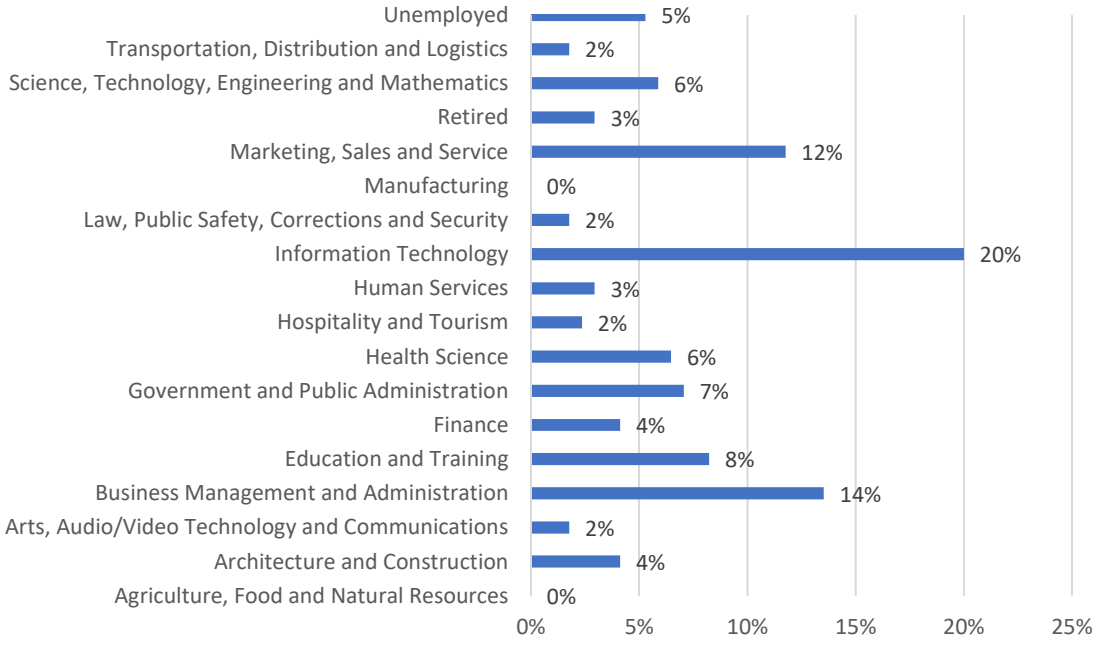

Graphic 2 – Age of Respondents.

We can see that the majority of answers correspond to ages between 26 - 35 (31%), followed by the 36 to 45 age group with 24%.




Graphic 3 – Education of Respondents.

Most respondents have an academic degree (33%), 17% of them have a master's and high school graduate.




Graphic 4 – Occupation of Respondents.

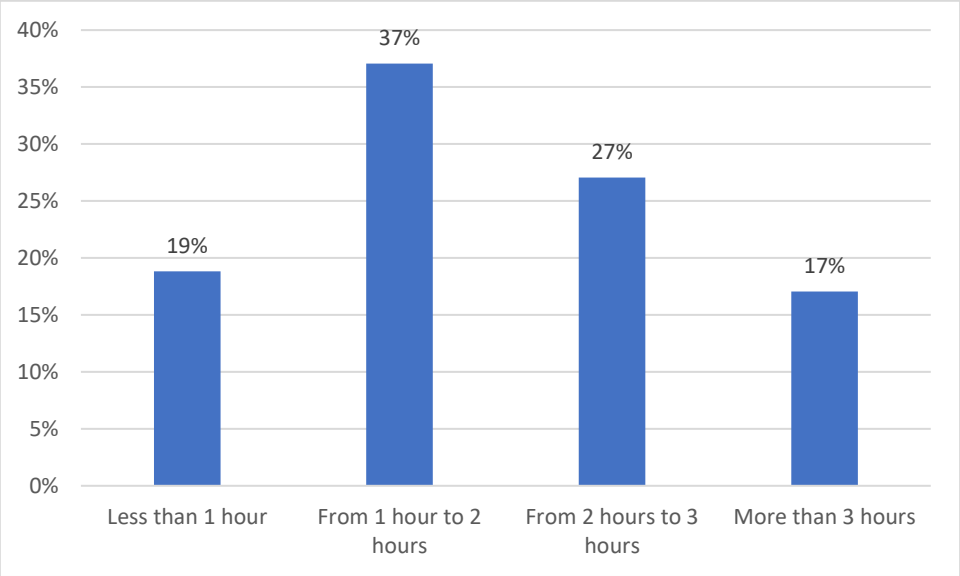
According to the graph above, we can see that 20% of respondents work in information technology and only 1% in transport, distribution and logistics.

### 4.2.2. Analysis of Respondents' Responses

Next, the results and respective analyses of the answers given in the online survey will be presented. In the first section, will be shown the results of the analysis of the second part of the survey related to social media. In the second section will be shown the results of the cybersecurity analysis (Part C).

#### 4.2.2.1. *Part B*

1. How much time do you spend on social media per day?

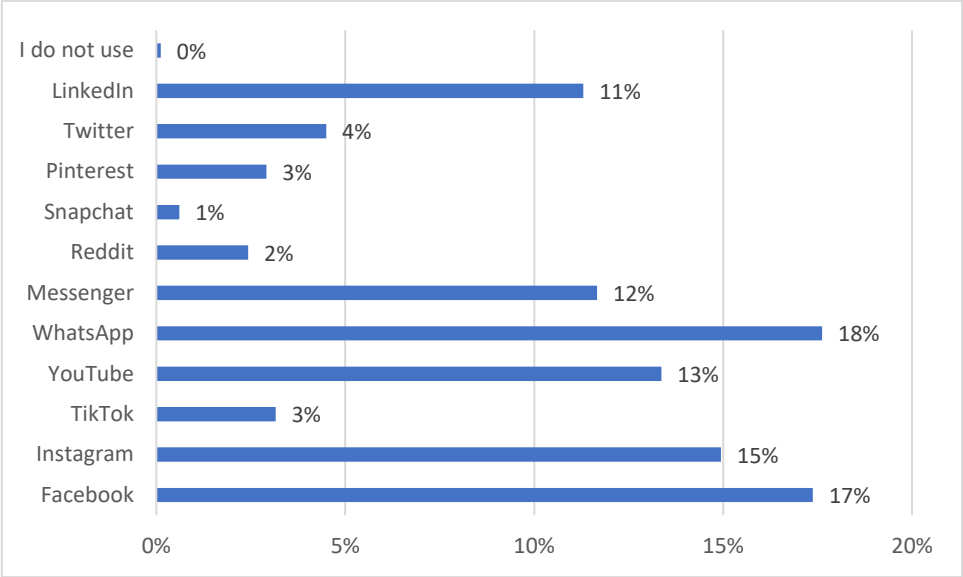



Graphic 5 – Analisis of Question 1.

In graph 5, we can see that 37% of respondents spend between 1 and 2 hours a day on social networks.

It should be noted that only 17% of respondents spend more than 3 hours on social networks.

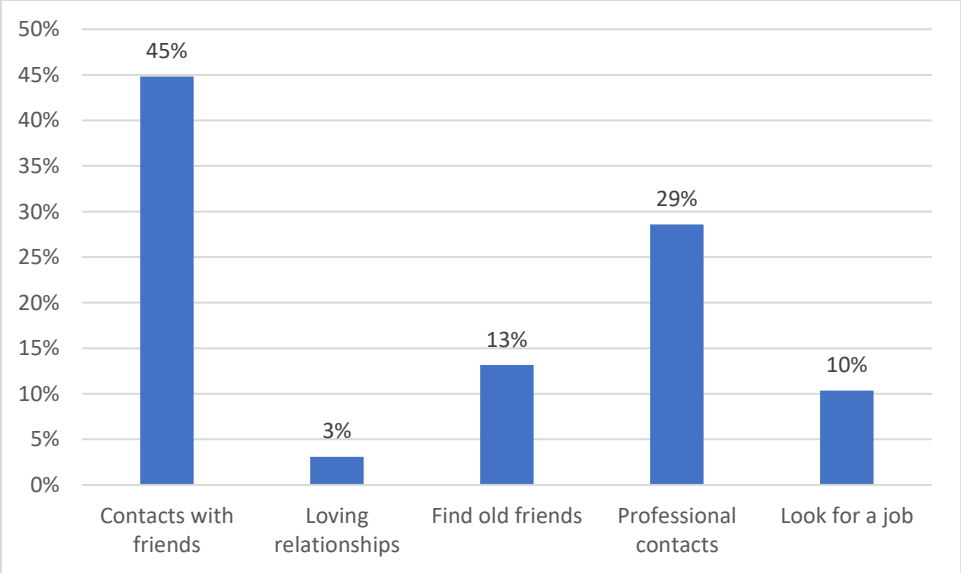
2. Which of the following social networks do you use?




Graphic 6 – Analysis of Question 2.

In the chart above the vast majority of respondents use WhatsApp (18%) and then Facebook, with 17% of responses. It should be noted that only 1% of respondents use Snapchat and 3% use both Pinterest and TikTok.

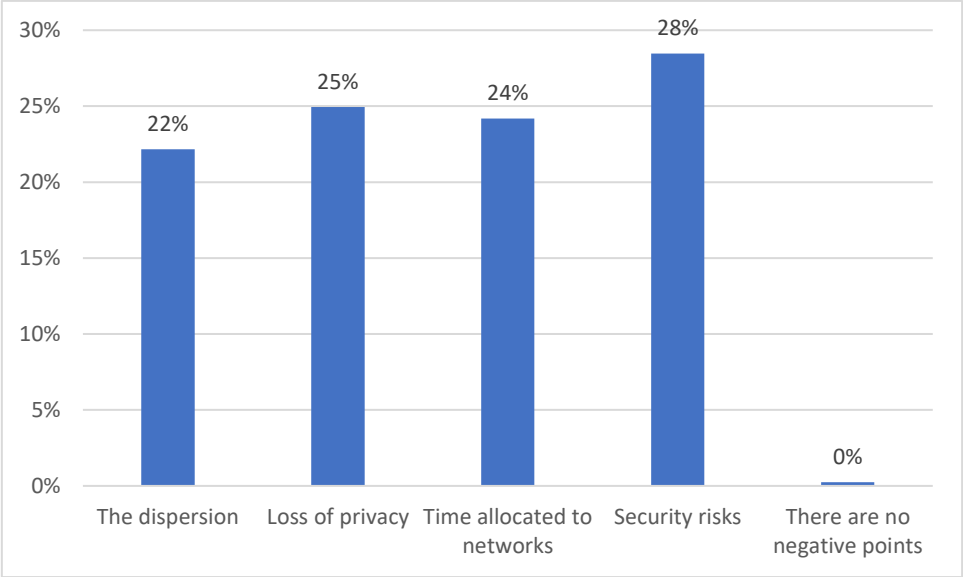
3. What are you looking for in Social Networks?




Graphic 7 – Analysis of Question 3.

We can see that in graph 7, 45% of respondents use social networks to keep in touch with their friends. It can also be seen that 29% use the networks for professional contacts, and 13% to find old friends.

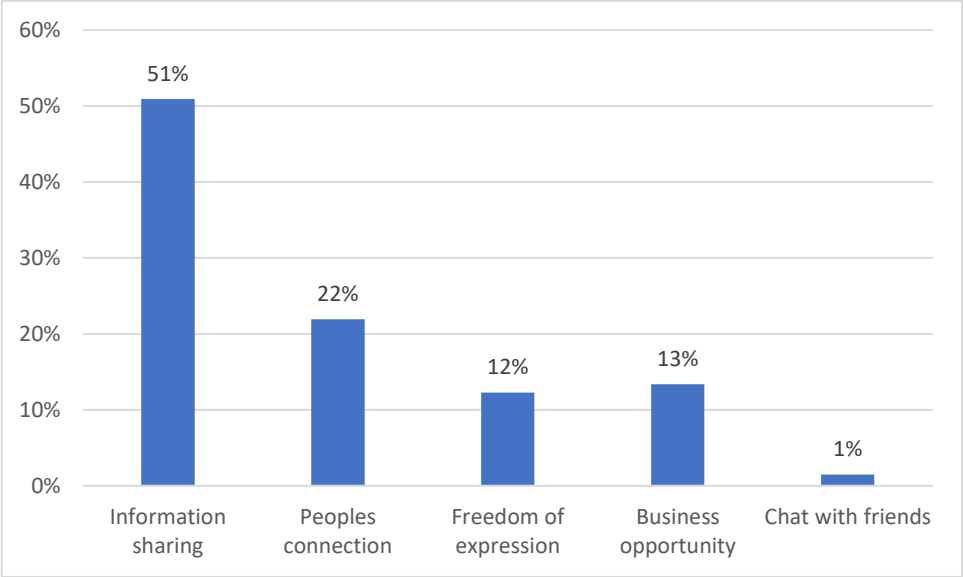
4. Which are the most negative factors in the use of Social Networks?




Graphic 8 – Analysis of Question 4.

In the eighth graph, 28% of respondents think that the biggest negative factor is security risks. Already 25% indicate that it is the loss of privacy.

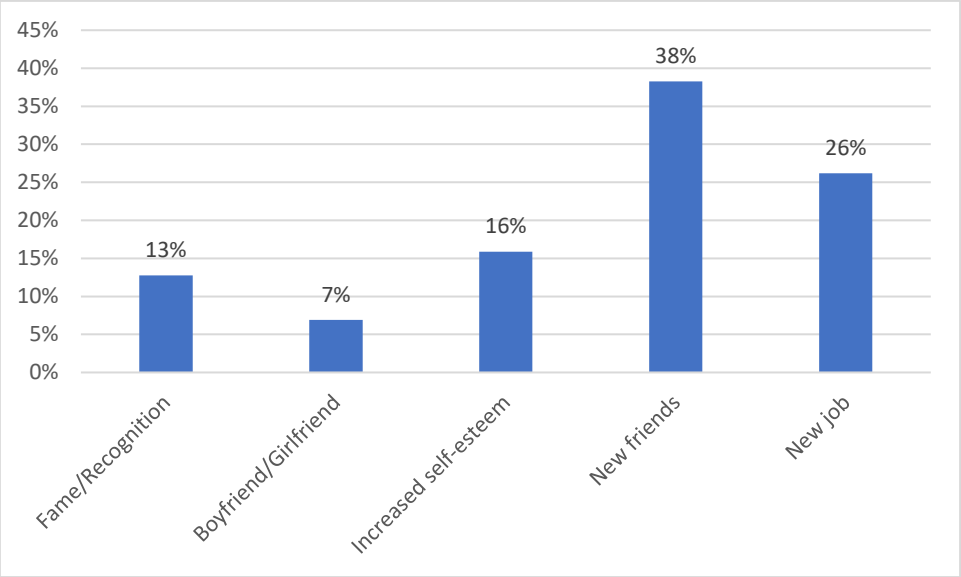
5. Which are the most positive factors in the use of Social Networks?




Graphic 9 – Analysis of Question 5.

In the chart above, we can see that 51% of respondents indicate that one of the positive factors is sharing information. 22% of respondents refer that another positive factor is connecting with people. It should be noted that only 1% think that it is talking with friends.

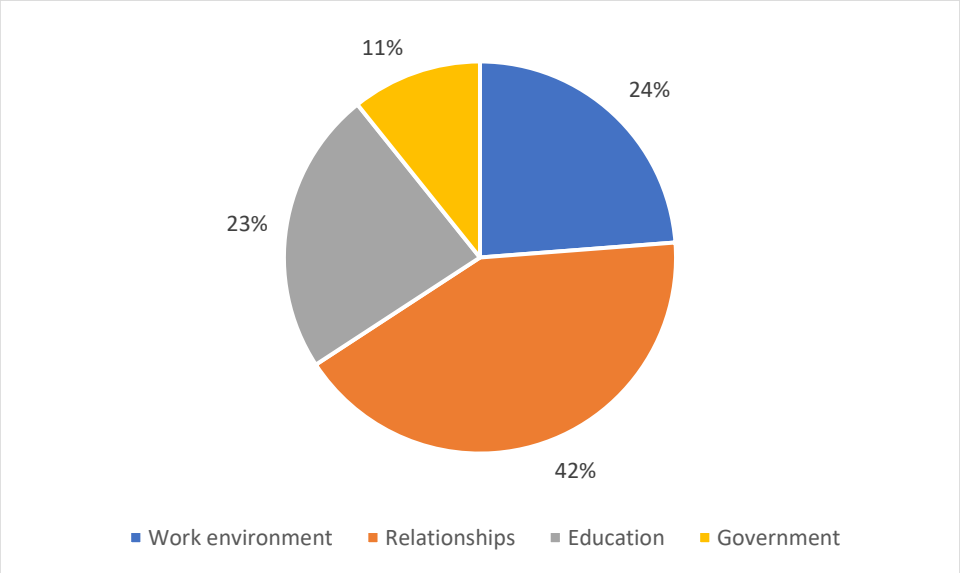
6. What goal did you achieve on Social Networks?




Graphic 10 – Analysis of Question 6.

In graph 10, we can see that 38% of respondents were able to create new friendships and 26% a new job. Another interesting point is that 16% of the respondents had an increase in self-esteem.

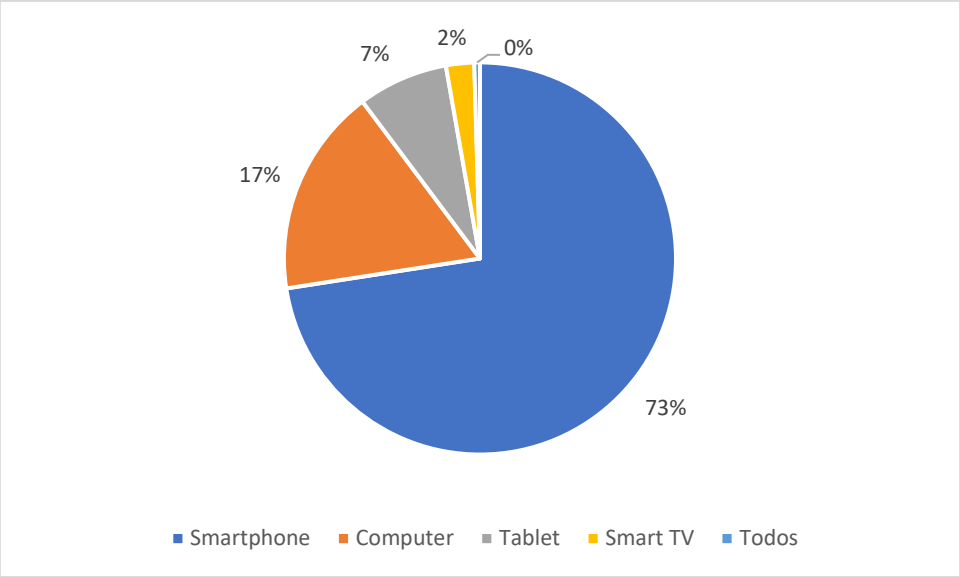
7. In your opinion, in which area do Social Networks makes the most impact?




Graphic 11 – Analysis of Question 7.

In the respondents' opinion, the area where social media impacts the most are in relationships (40%) and also in the work environment (24%), it can also be seen that 23% indicate that it also impacts on education and 11% on government.

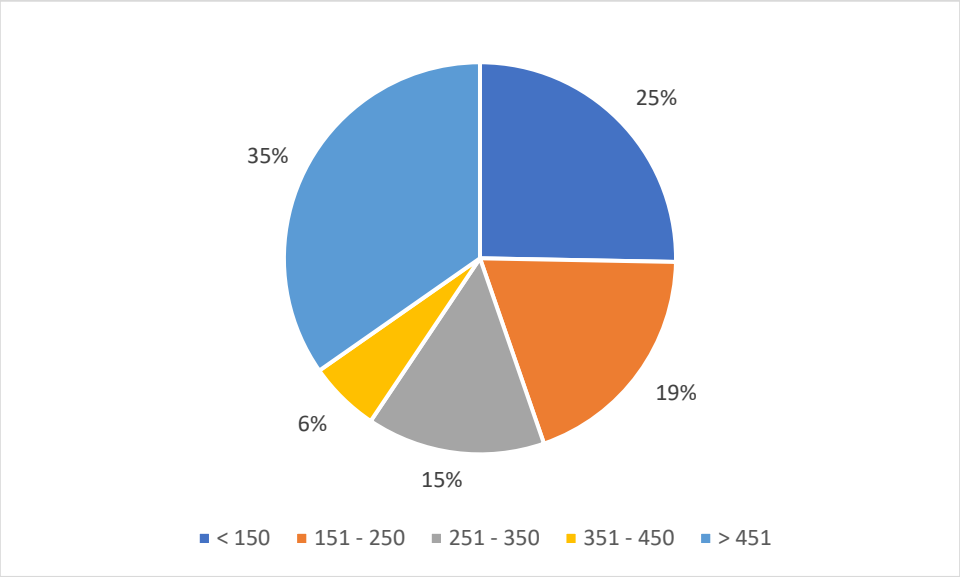
8. Which device do you prefer to access Social Networks?




Graphic 12 – Analysis of Question 8.

The vast majority of respondents use smartphones to access social networks (73%), while 2% use a smart TV.

9. How many friends do you currently have on your Social Networks?

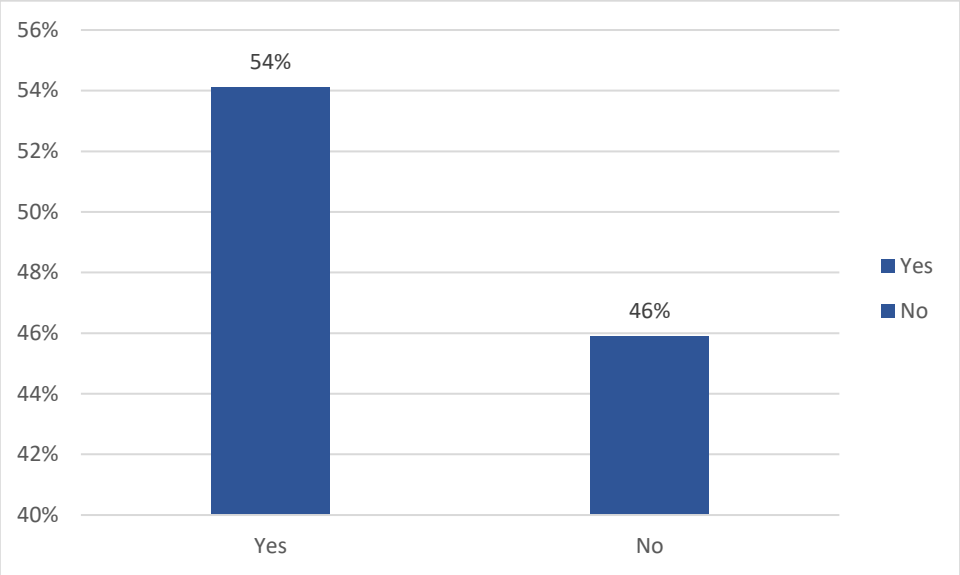



Graphic 13 – Analysis of Question 9.

In graph 13 it is achieved that 35% of the respondents have more than 450 friends on social networks and 25% below 150. It should be noted that only 6% of respondents have between 350 and 450 contacts on social networks.

#### 4.2.2.2. *Part C*

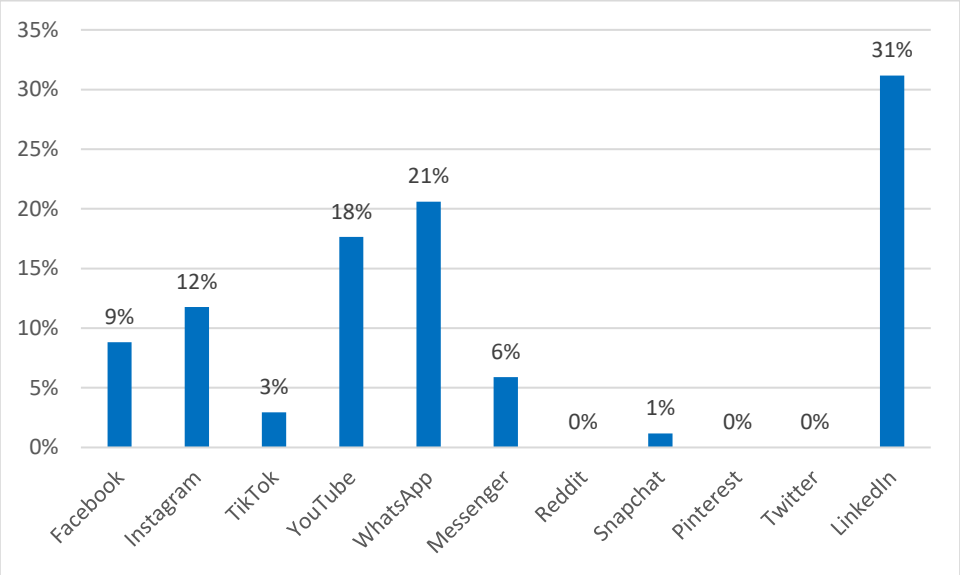
1. Do you keep the passwords saved in the browser?




Graphic 14 – Analysis of Question 1.

It should be noted that in the graph above, 54% of respondents keep their passwords in their browsers. The remaining respondents (46%) do not store passwords in their browsers.

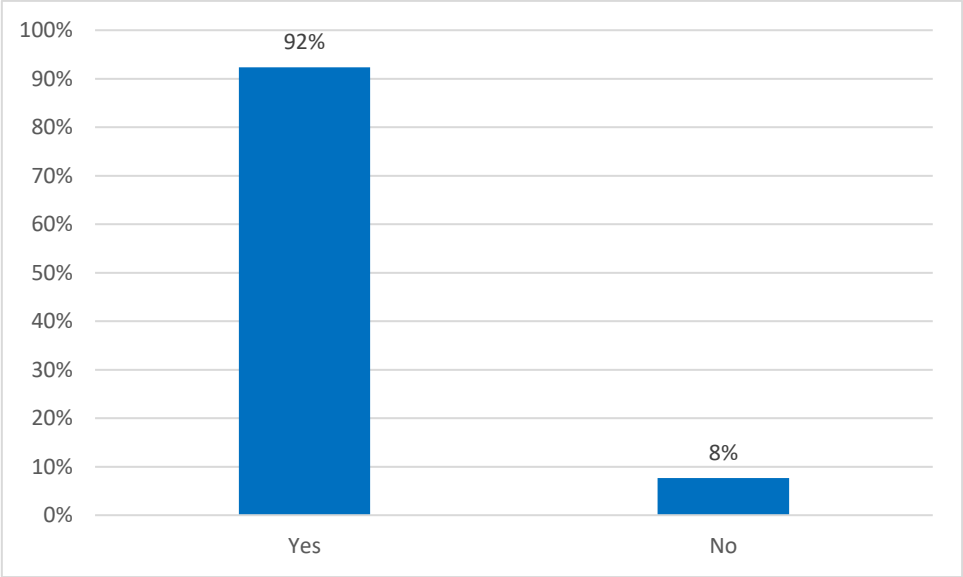
2. Which social network provides the best data security?




Graphic 15 – Analysis of Question 2.

In graph 15, it is achieved that 31% of the respondents trust in LinkedIn, 21% in WhatsApp and 18% on YouTube.

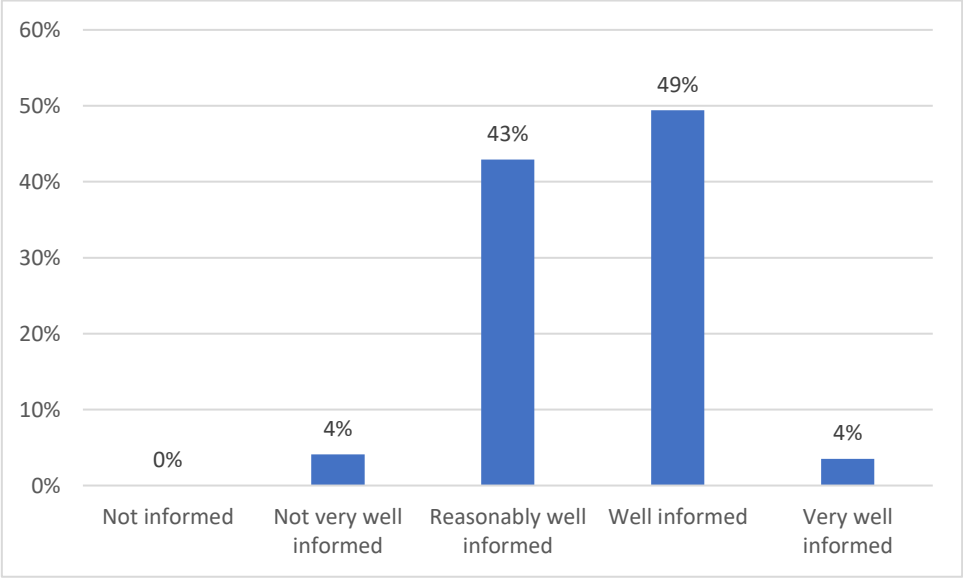
3. Do you trust in cybersecurity?




Graphic 16 – Analysis of Question 3.

In chart 16, 92% of the respondents' trust in cybersecurity and 8% don't trust in cybersecurity.

4. How well informed do you feel about cybercrime risk?



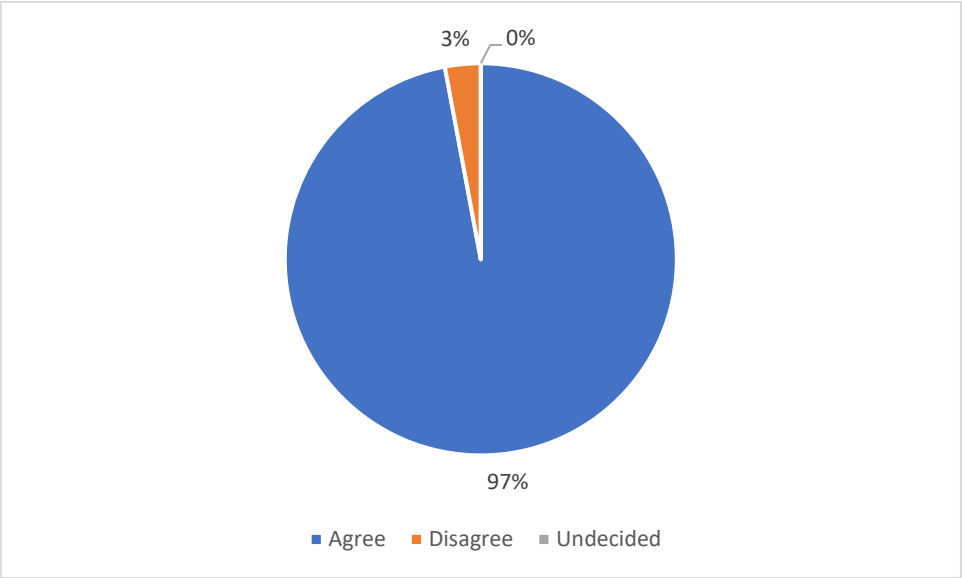

Graphic 17 – Analysis of Question 4.

In the chart above, 49% of respondents'are well informed and 23% are shallowly informed about cybercrime.

An interesting point is that only 4% of people are not well informed and also another 4% are very well informed about cybercrime.

5. Do you agree or disagree with the following statements?

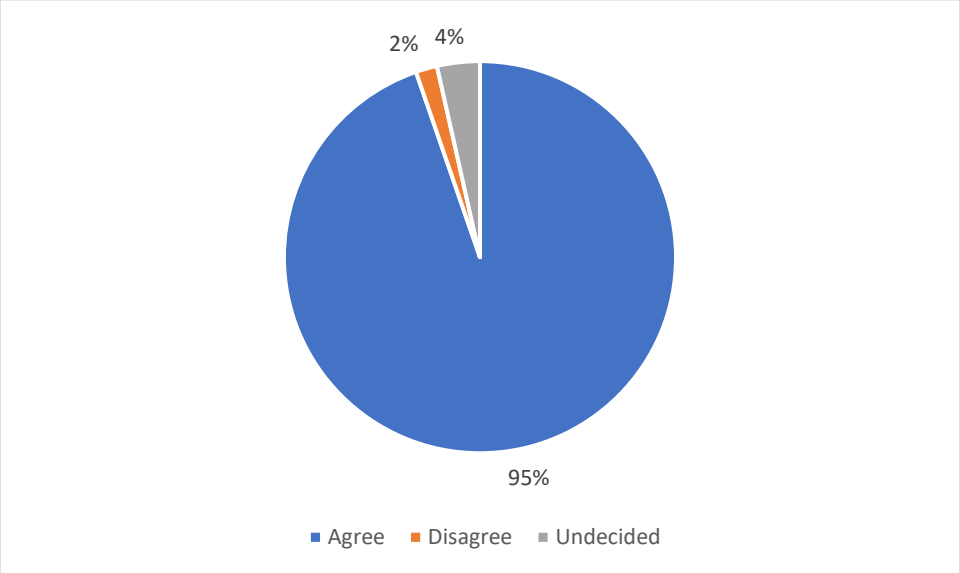
5.1. I Avoid revealing my personal information




Graphic 18 – Analysis of Question 5.1.

In graph 18, it is noted that 97% of respondents agree that disclosing their personal information should be avoided and only 3% are not concerned that they may disclose their data.

5.2. The risk of being a cybercrime victim is increasing.

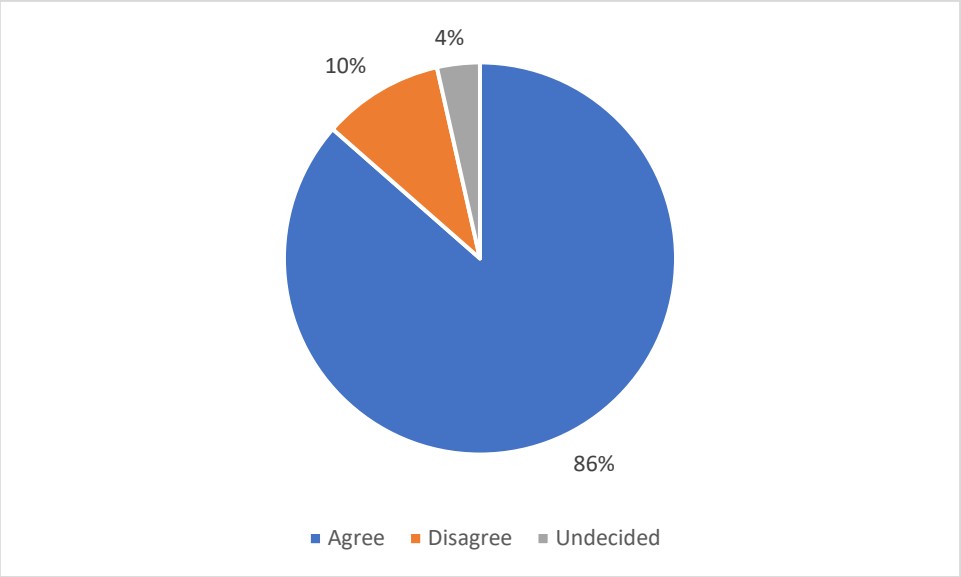



Graphic 19 – Analysis of Question 5.2.

In the above graph, 95% of respondents agree that the risk of being a victim of cybercrime is increasing.

It can also be seen that 4% are undecided and 2% of respondents do not agree that the risk of being a victim of cyber-attacks is increasing.

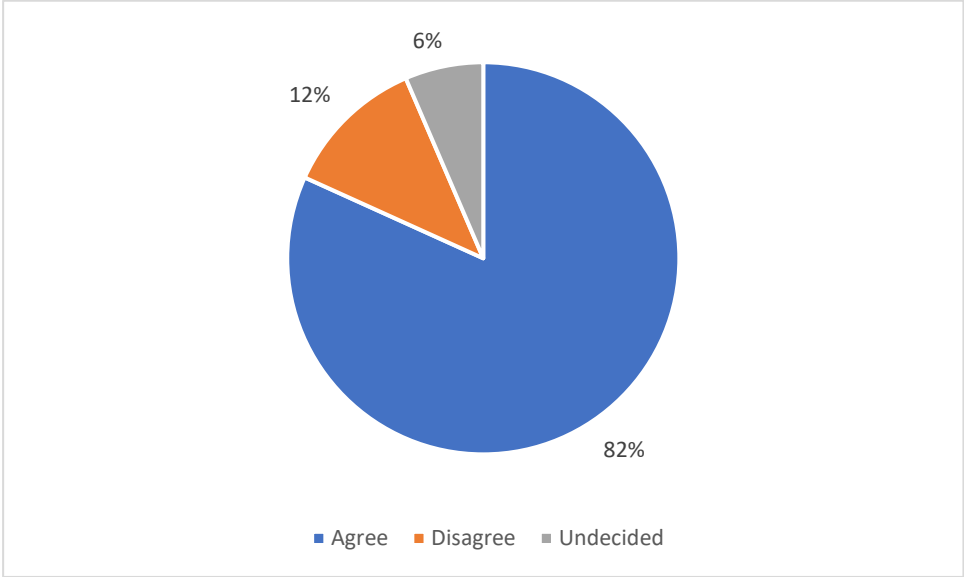
5.3. I'm concerned that my personal information isn't secure on the websites.




Graphic 20 – Analysis of Question 5.3.

In graph 20, 86% of respondents agree that personal data is not secure on websites, 10% disagree and only 4% are undecided.

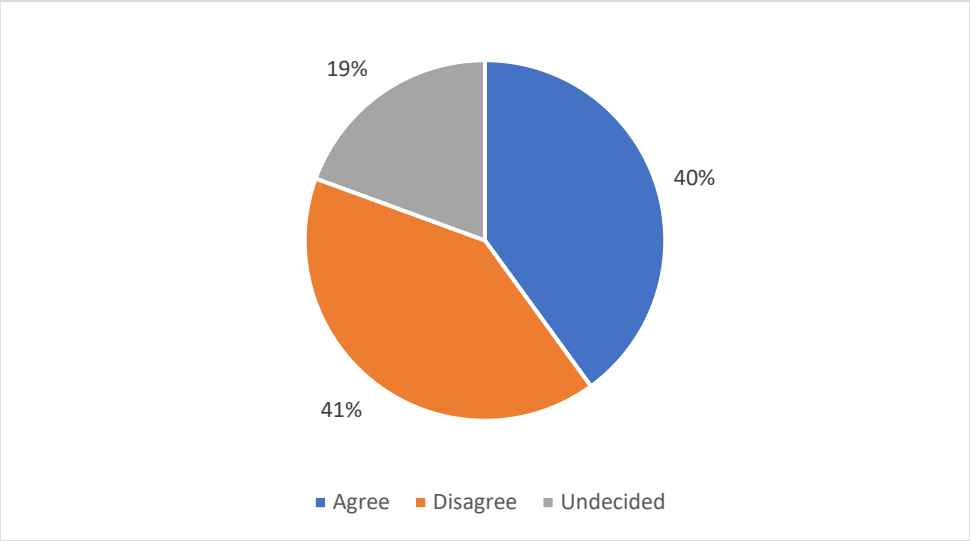
5.4. I'm concerned that my personal information isn't protected by public authorities.




Graphic 21 – Analysis of Question 5.4.

In the chart above, 82% of respondents agree that personal information is not protected by public authorities, 12% disagree and 6% are undecided.

5.5. A protection tool, like an antivirus, will protect me from cybercrime.



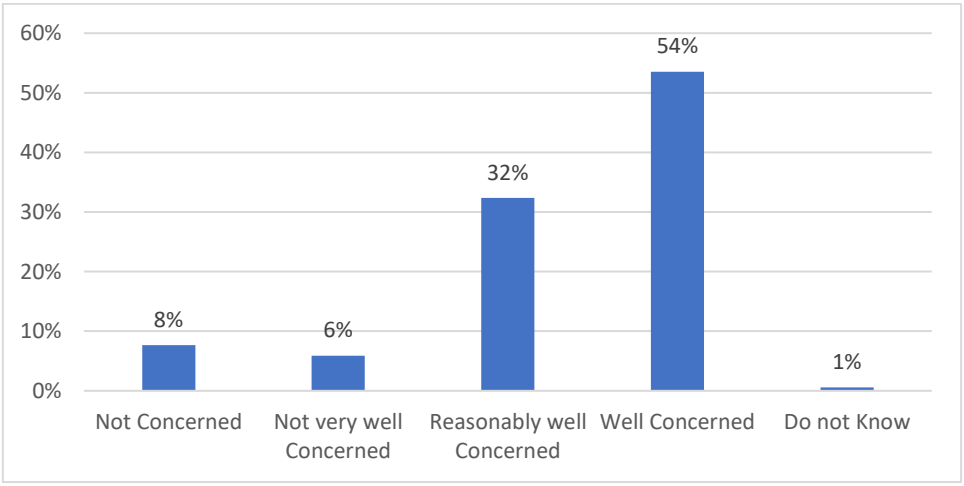

Graphic 22 – Analysis of Question 5.5.

In the chart above, we can see that 41% of respondents disagree a protection tool such as an antivirus does not protect against cybercrime.

We can also see that 40% of people surveyed agree that a protection tool, can protect against cybercrime. Also, 19% of the respondents are undecided on this subject.

6. Cybercrimes include many types of criminal activities. How concerned are you, personally, about experiencing or being a victim of the following situations?

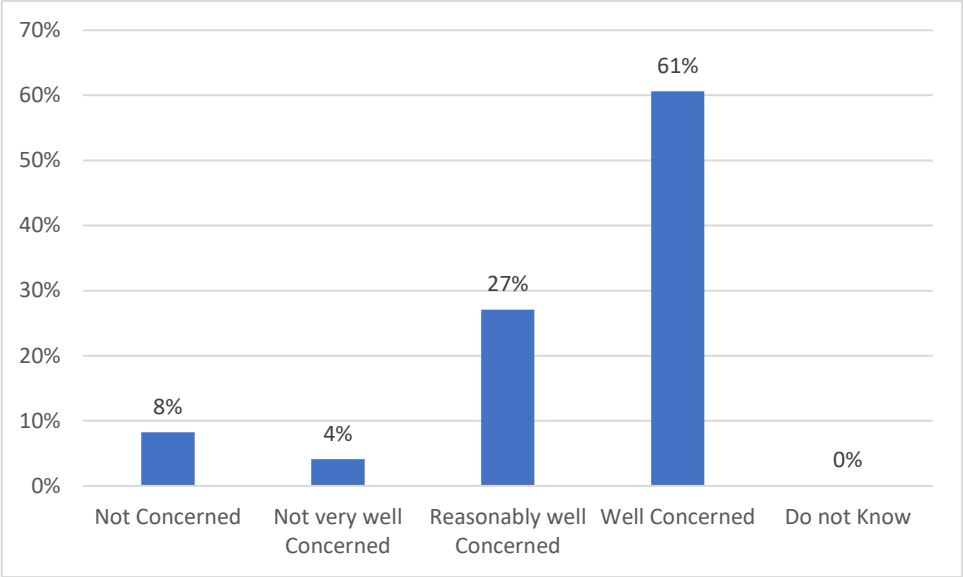
6.1. Device infection with malicious software (malware, etc.).




Graphic 23 – Analysis of Question 6.1.

In graph 23, it can be seen that the great majority of respondents are well concerned about being a victim of the infection of devices with malicious software (54%). Also, we can see that 32% of the respondents are reasonably well concerned that the malicious software could affect their devices. It is worth noting that 8% is not concerned and 6% are also not very well concerned.

6.2. Identity theft (someone that steals your personal information).

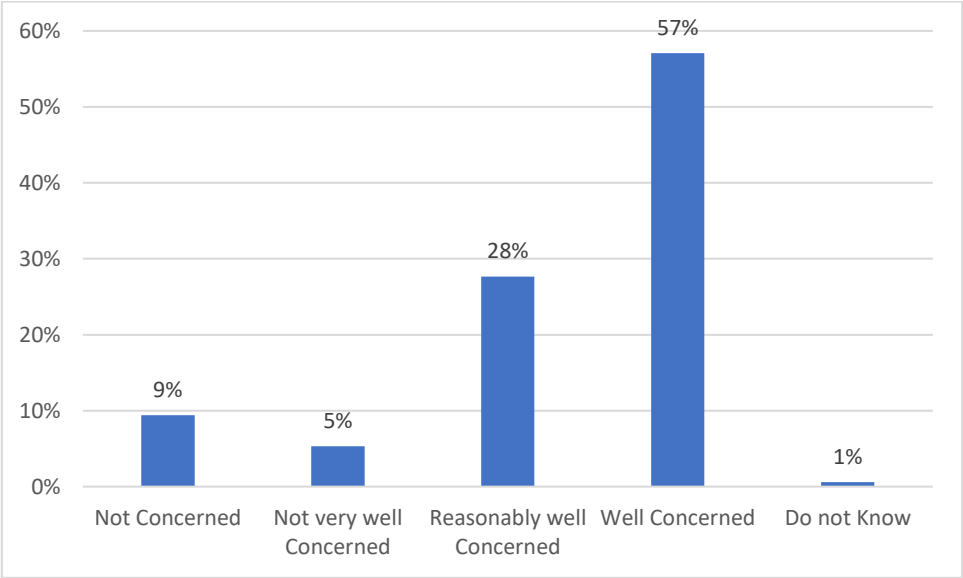



Graphic 24 – Analysis of Question 6.2.

In the chart above, we can see that a large proportion of respondents (61%) are very concerned about being a victim of theft, and 27% are reasonably concerned.

Also, we can see that 8% of the respondents are not concerned about being a victim of theft.

6.3. Bank card or online banking fraud.

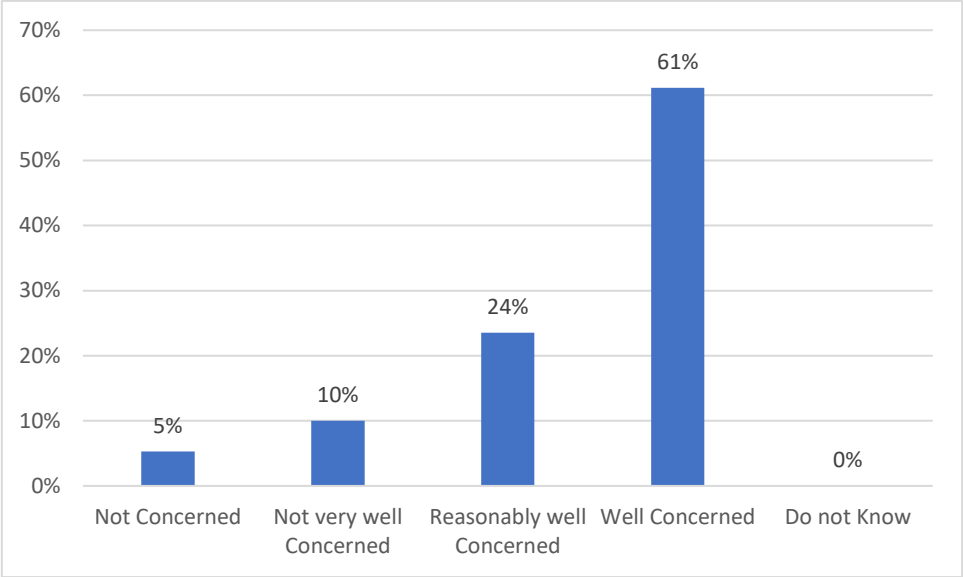



Graphic 25 – Analysis of Question 6.3.

In graph 25, 57% of respondents are very worried about being a victim of bank card or online banking fraud and 28% are reasonably well concerned.Also, we can see that 9% of the respondents are not concerned about being a victim of bank cards or online banking fraud.

it is worth noting that only 1% do not know whether or not they are worried about being a victim of online banking or bank card fraud.

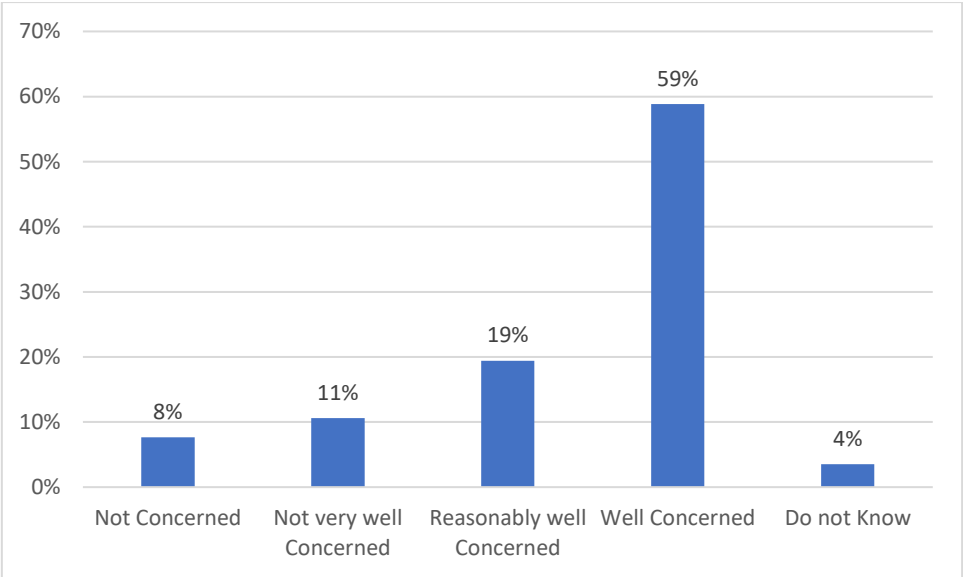
6.4. Hacking your social networks or email account.




Graphic 26 – Analysis of Question 6.4.

In chart above, it can be seen that 61% of respondents are well concerned that they may fall victim to the hacking of their social media or email account, 24% are reasonably well concerned and 10% are not very well concerned about being a victim. Also, we can see that 5% of the respondents are not concerned.

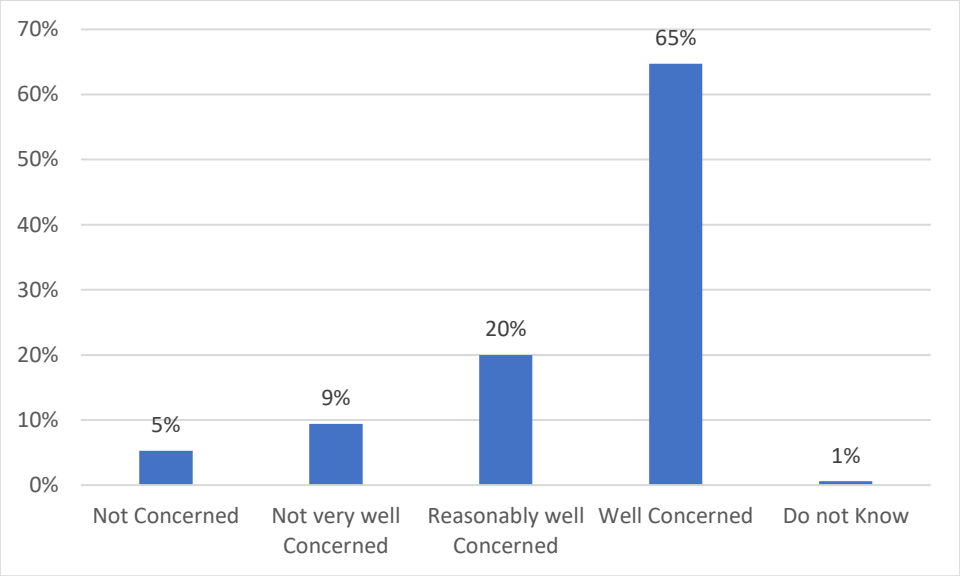
6.5. Online material that promotes racial or religious extremism.




Graphic 27 – Analysis of Question 6.5.

In Graph 27, it is noted that the majority (59%) of respondents are well concerned that they may be victims of online material that promotes racial or religious extremism, 19% consider to be reasonably well concerned and 11% are not very well concerned. It should be noted that 8% of the respondents are not concerned about being a victim of racial or religious extremism.

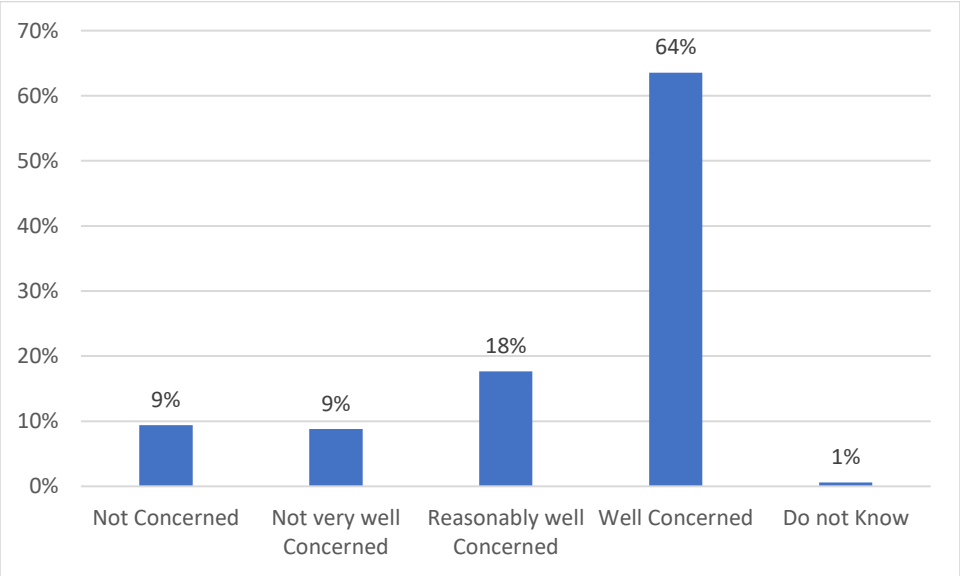
6.6. Cyber-attacks that prevent you from accessing online services, such as your bank account.




Graphic 28 – Analysis of Question 6.6.

In the graph above, 65% of respondents are well concerned that they could be a victim of a cyber-attack that prevent them from accessing their online services, as well 20% is reasonably concerned.Also, it can be seen that 5% is not concerned and 9% are not very well concerned about being a victim of a cyber-attack where they cannot access their online services.

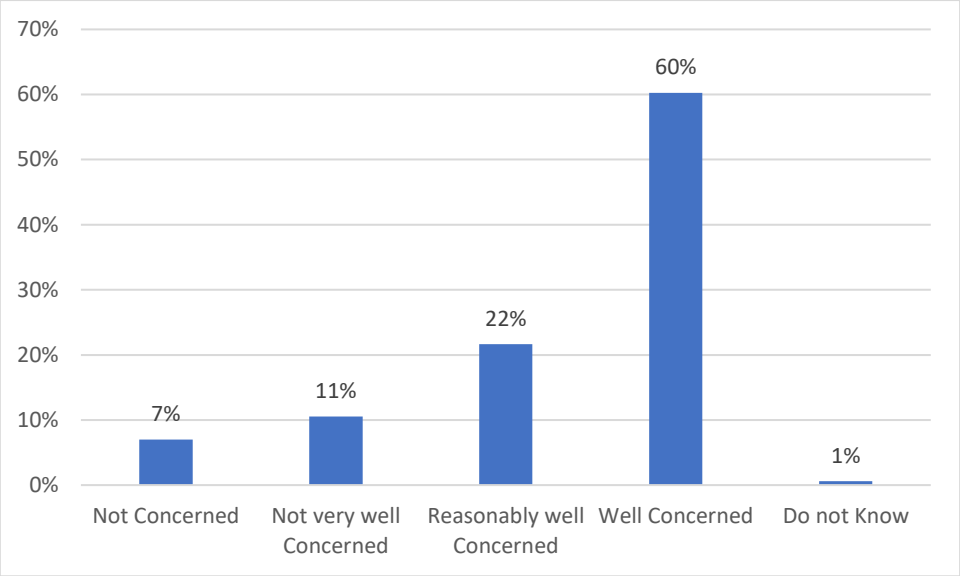
6.7. Payment request in exchange for regaining control over your device.




Graphic 29 – Analysis of Question 6.7.

In Chart 29, the vast majority of respondents are very concerned that they may be the victim of demands for payment in exchange for regaining control over their devices. As for 18% are reasonably well concerned and 9% are not very well concerned and 9% are not concerned at all.

6.8. Online fraud in which purchased products are not delivered, counterfeit or do not correspond to the advertised.



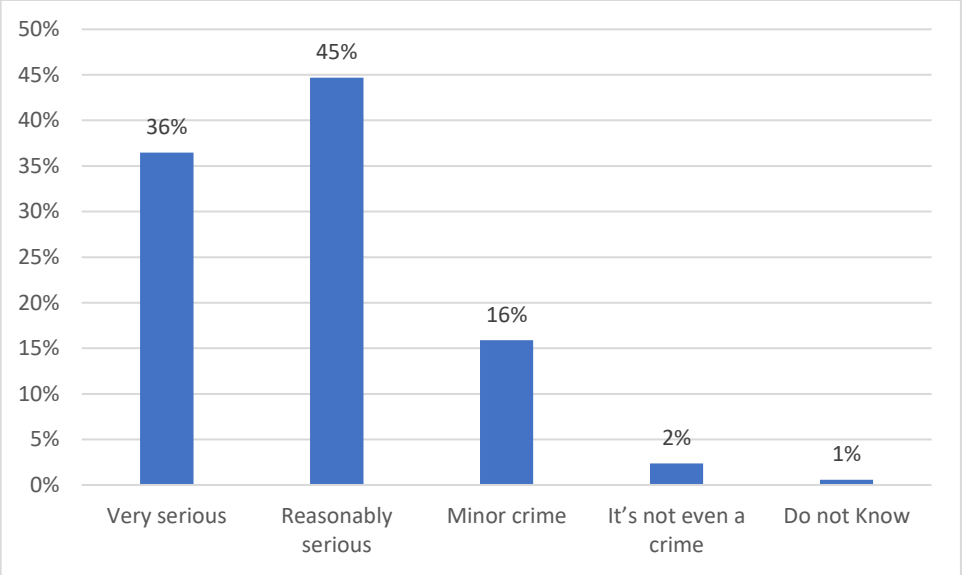

Graphic 30 – Analysis of Question 6.8.

In the chart above, it can be seen that 60% of respondents are very concerned about falling victim to online fraud where purchased products are not delivered, counterfeit or not real. It can also be seen that 22% of people are reasonably well concerned and 11% are not very well concerned.

It should also be noted that 7% are not concerned about being a victim of online fraud.

7. In your opinion, which of these situations represents a very serious, reasonably serious, minor crime or is it not even a crime?

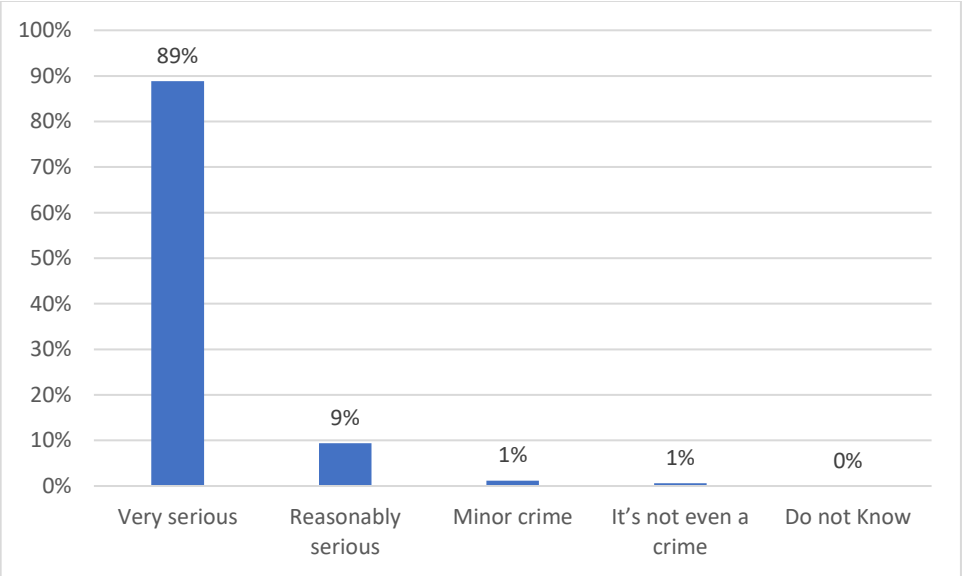
7.1. Infection of devices with malicious software (malware, etc.).




Graphic 31 – Analysis of Question 7.1.

In graph 31, 45% of respondents consider that infecting devices with malicious software is a reasonably serious crime, and 36% of them consider it a very serious crime. It should be noted that 16% consider a minor crime and 2% thinks that it's not even a crime.

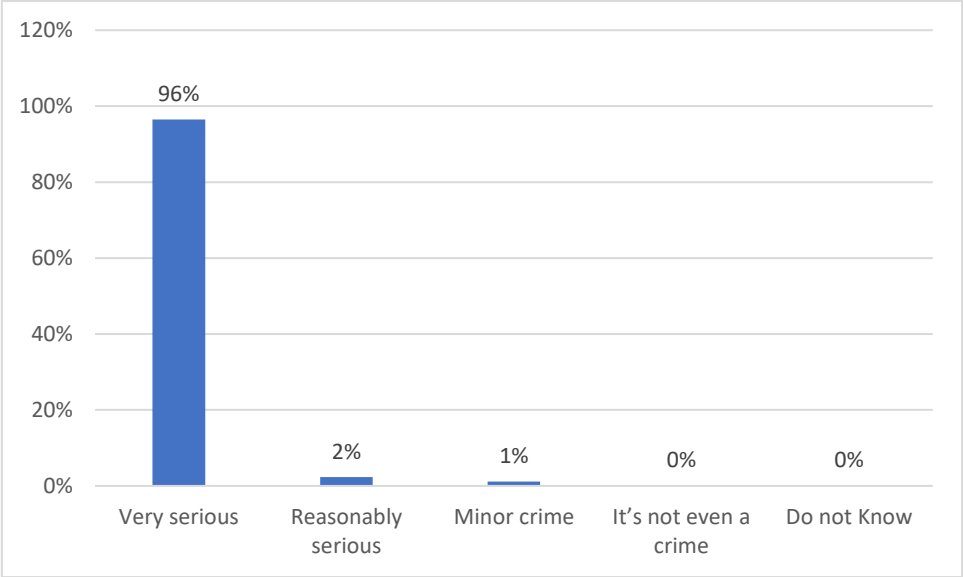
7.2. Identity theft (someone that steals your personal information).




Graphic 32 – Analysis of Question 7.2.

In the chart above, the majority of respondents (89%), consider identity theft to be a very serious crime and only 9% consider it to be a reasonably serious crime.

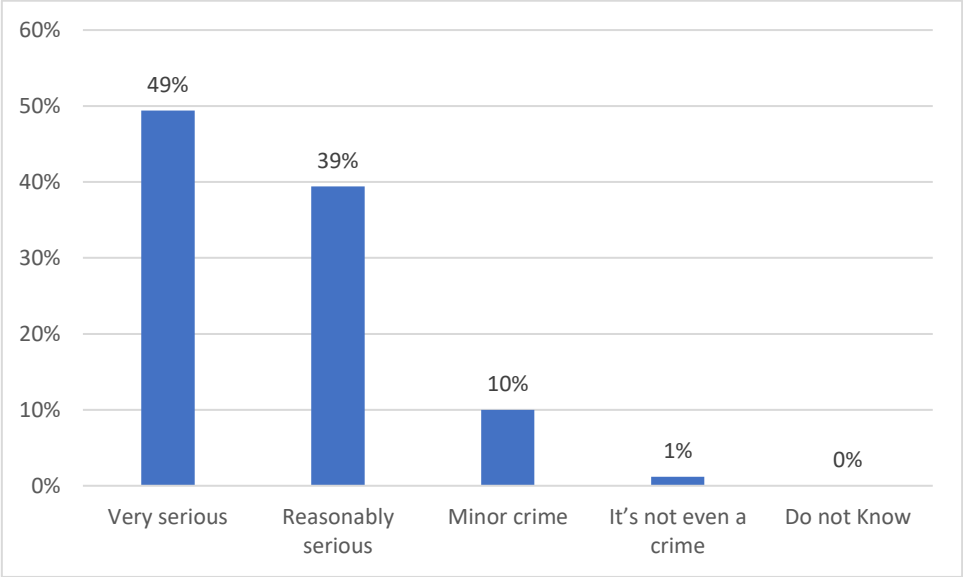
7.3. Bank card or online banking fraud.




Graphic 33 – Analysis of Question 7.3.

In Chart 33, the majority of respondents (96%), consider online banking fraud or bank card theft to be a very serious crime and only 2% consider it to be a reasonably serious crime.

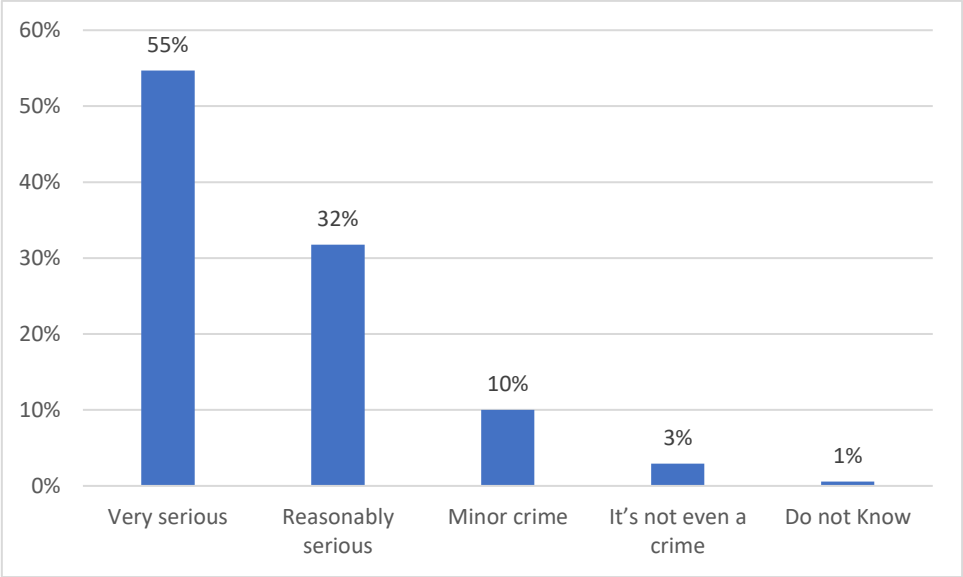
7.4. Hacking your social networks or email account.




Graphic 34 – Analysis of Question 7.4.

In Chart 34, 49% of respondents considered hacking into their social networks or email to be a very serious crime and 39% considered it to be a reasonably serious crime and 19% considered it to be a minor crime.

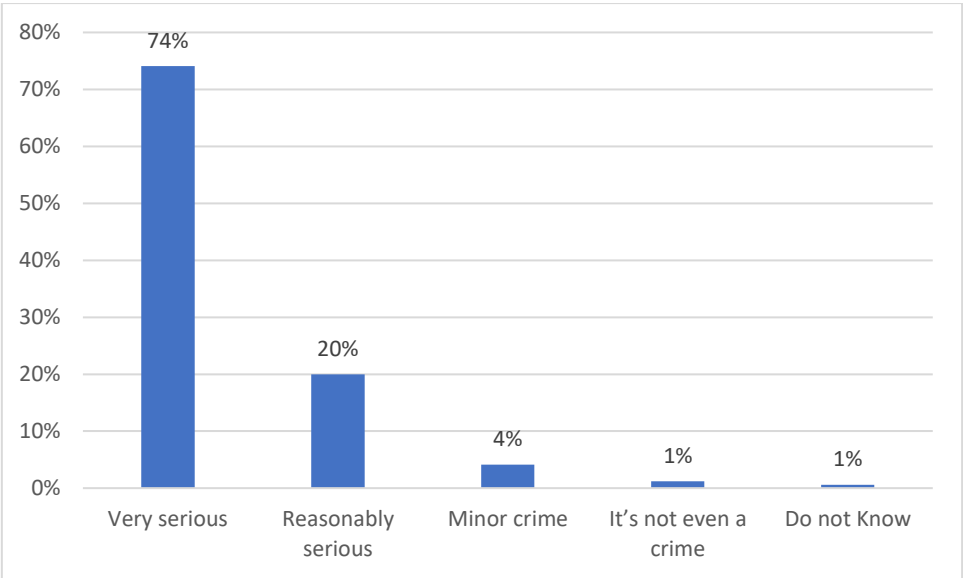
7.5. Online material that promotes racial or religious extremism.




Graphic 35 – Analysis of Question 7.5.

In Chart 35, 55% of respondents consider racism or religious extremism a very serious crime and 32% consider it a reasonably serious crime, 10% consider it a minor crime and 3% do not consider it a crime.

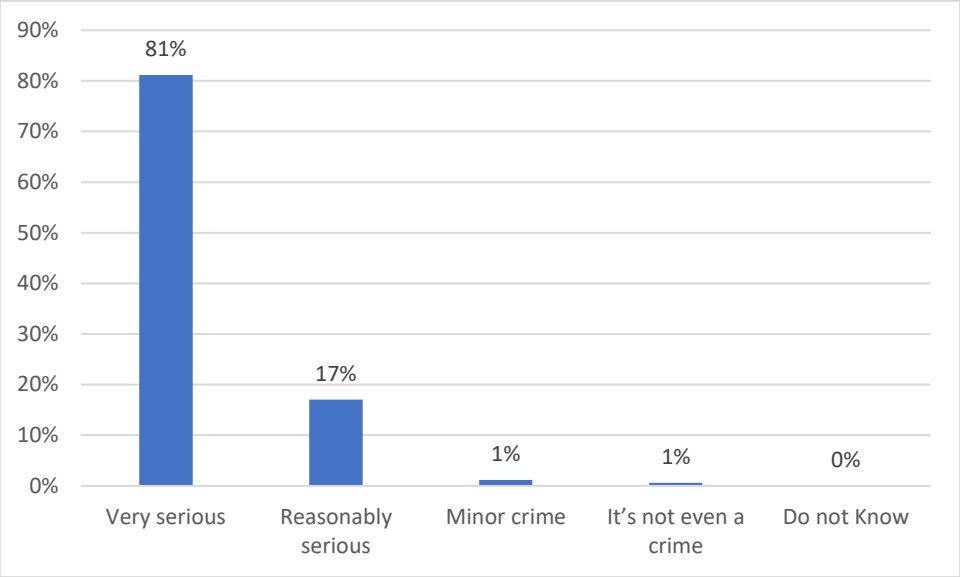
7.6. Cyber-attacks that prevent you from accessing online services, such as your bank account.




Graphic 36 – Analysis of Question 7.6.

In the graph above, 74% of respondents, consider that cyber-attacks that prevent them from accessing their online services is a very serious crime and 20% consider it a reasonably serious crime. Also, 4% of the respondents consider it a minor crime and 1% do not consider it a crime.

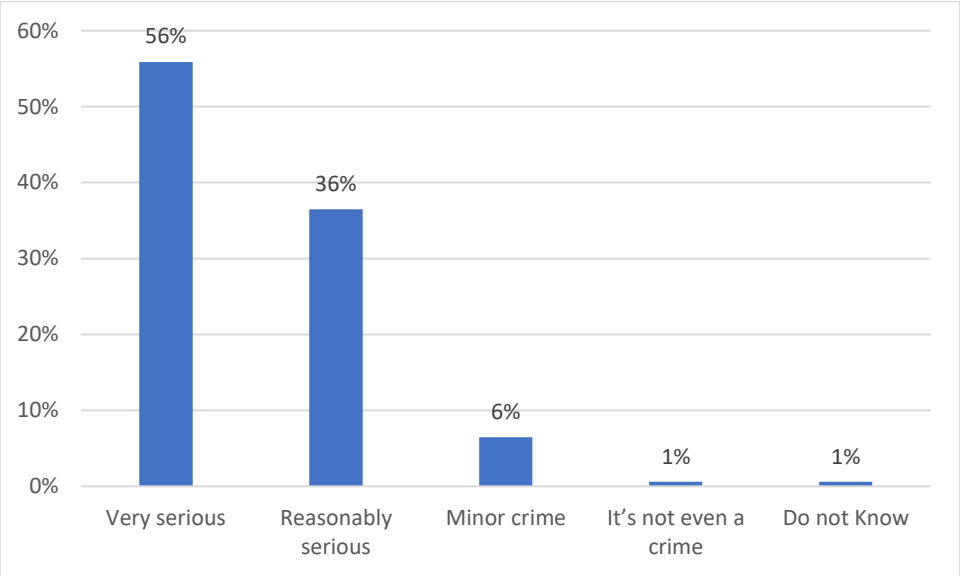
7.7. Payment request in exchange for regaining control over your device.




Graphic 37 – Analysis of Question 7.7.

In the above graph, the vast majority of respondents (81%), consider that requesting payment in exchange for being able to access their devices is a very serious crime. It is also noted that 20% consider it a reasonably serious crime, 1% consider it a minor crime also 1% do not consider it a crime.

7.8. Online fraud in which purchased products are not delivered, counterfeit or do not correspond to the advertised.

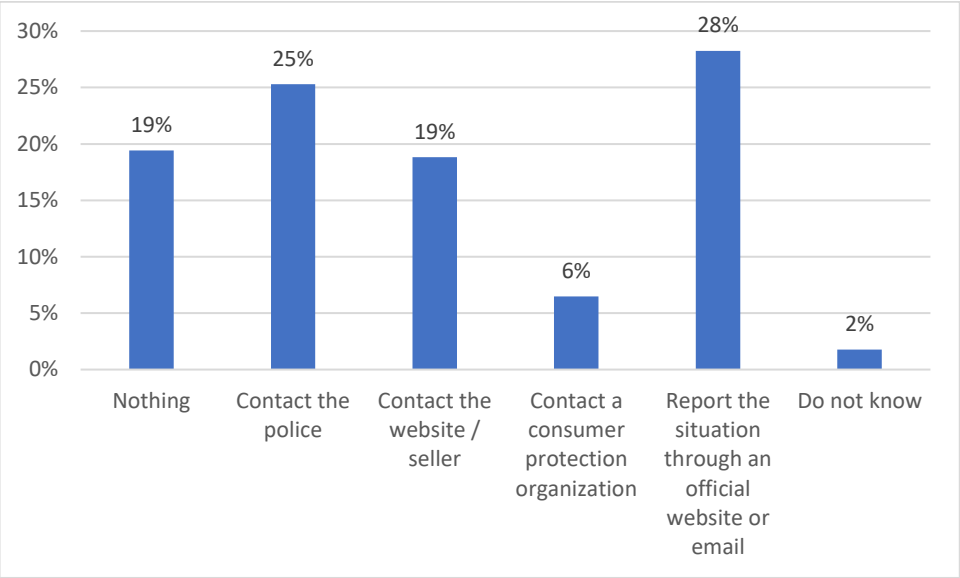



Graphic 38 – Analysis of Question 7.8.

In Chart 38, 56% of respondents consider online fraud in which the products purchased do not match the advertisement, are not delivered or are counterfeited to be a very serious crime. It should also be noted that 36% consider it to be a reasonably serious crime, 6% consider it to be a minor crime and 1% do not consider it to be a crime.

8. What would you do in the following situations if you had been a cybercrime victim?

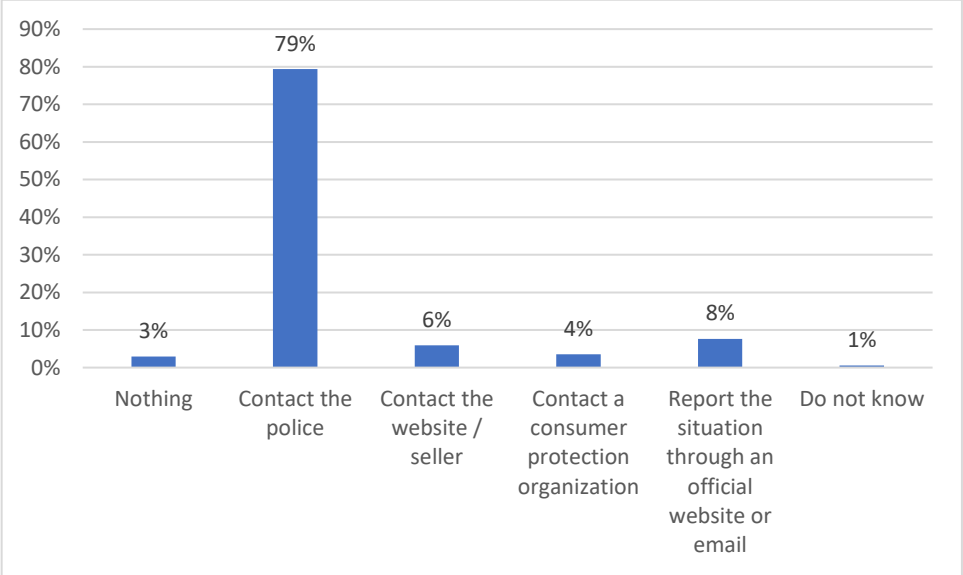
8.1. Discover malicious software on your device (virus, etc.).




Graphic 39 – Analysis of Question 8.1.

In the graph above, it can be seen that 28% of respondents if they were a victim of cybercrime would report the situation through official websites or email. As also next 25% would contact the police, 19% would contact the website/seller, another 19% would do nothing.

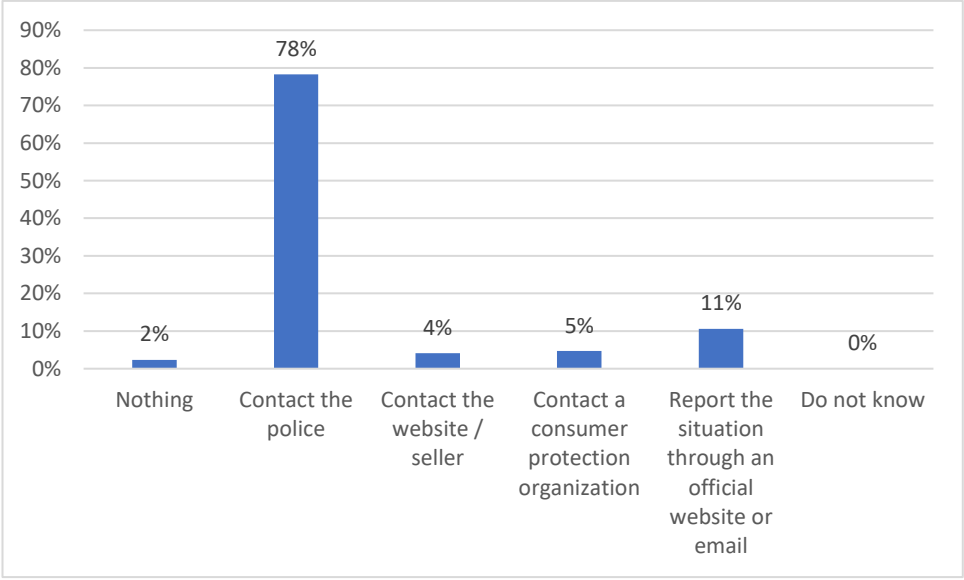
8.2. Identity theft (someone that steals your data).




Graphic 40 – Analysis of Question 8.2.

In graph 40, most of the respondents (79%) if they were a victim of cybercrime by identity theft would contact the police. Also, 8% would report the situation through an official website, 6% would contact the website/ vendor, 4% would contact the consumer protection organisation.

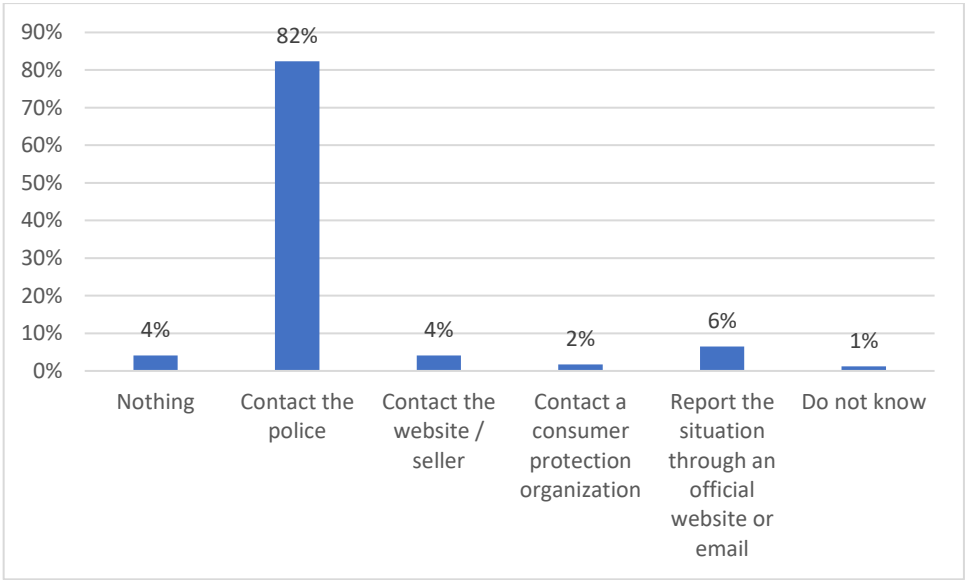
8.3. Being a victim of online bank or bank card fraud.




Graphic 41 – Analysis of Question 8.3.

According to the graph above, most of the respondents (78%) if they were a victim of cybercrime for bank fraud, would contact the police. It can also be seen that 11% would report the situation through an official website, 4% would contact the website/ vendor, 5% would contact the consumer protection organization. It is noteworthy that 2% would do nothing in this situation.

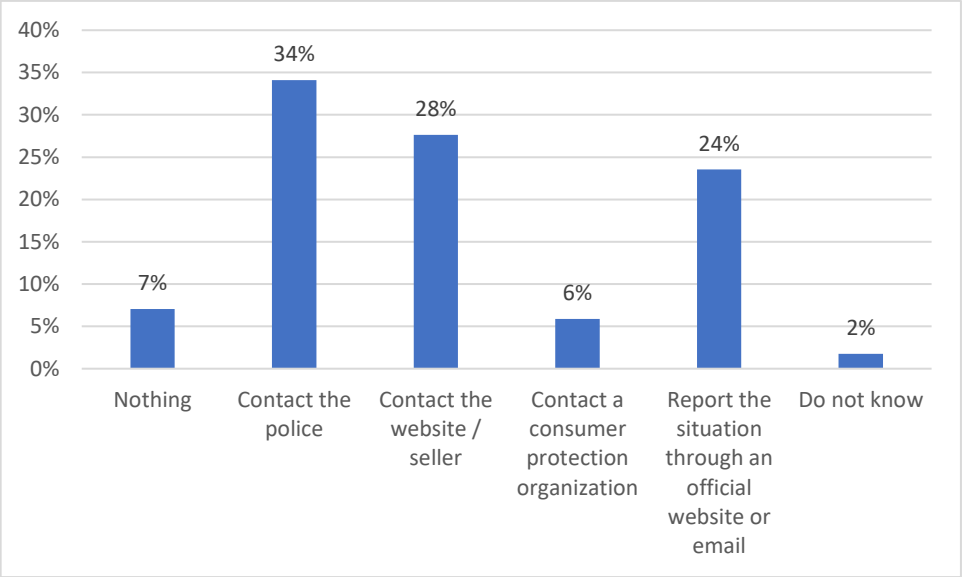
8.4. Find online child pornography.




Graphic 42 – Analysis of Question 8.4.

As graph 42 indicates, 82% of the respondents, if they found child online pornography, would contact the police. It is also noted that 6% would report the situation through an official website, 4% would contact the website/ dealer, 5% would contact a consumer protection organization and it should be noted that 4% would do nothing about the situation.

8.5. Hacking your social networks or email account.

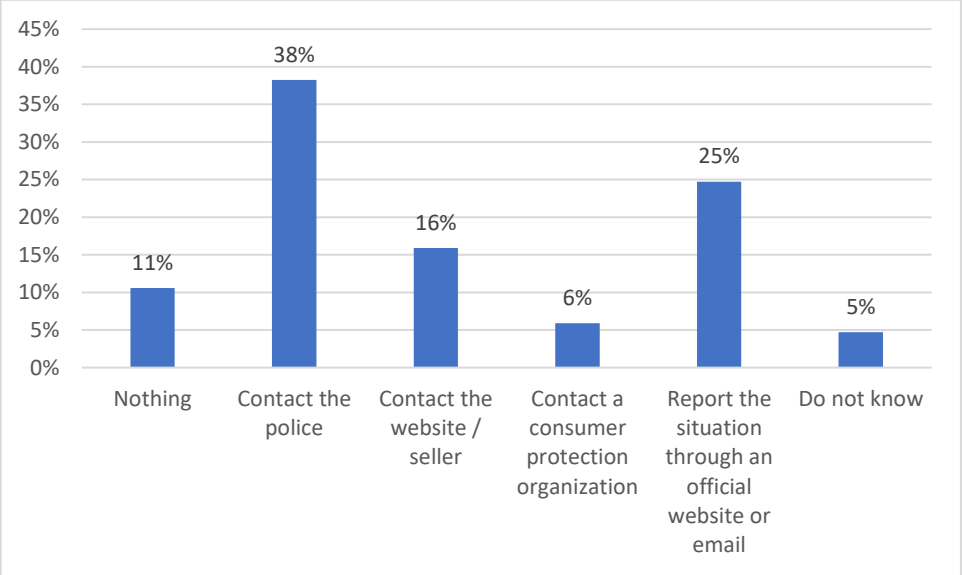



Graphic 43 – Analysis of Question 8.5.

Graph 43 shows that 34% of respondents if they were victims of cybercrime by hacking their social networks or email, would contact the police.

It should also be noted that 28% would contact the website/ vendor and 24% would report the situation via an official website.

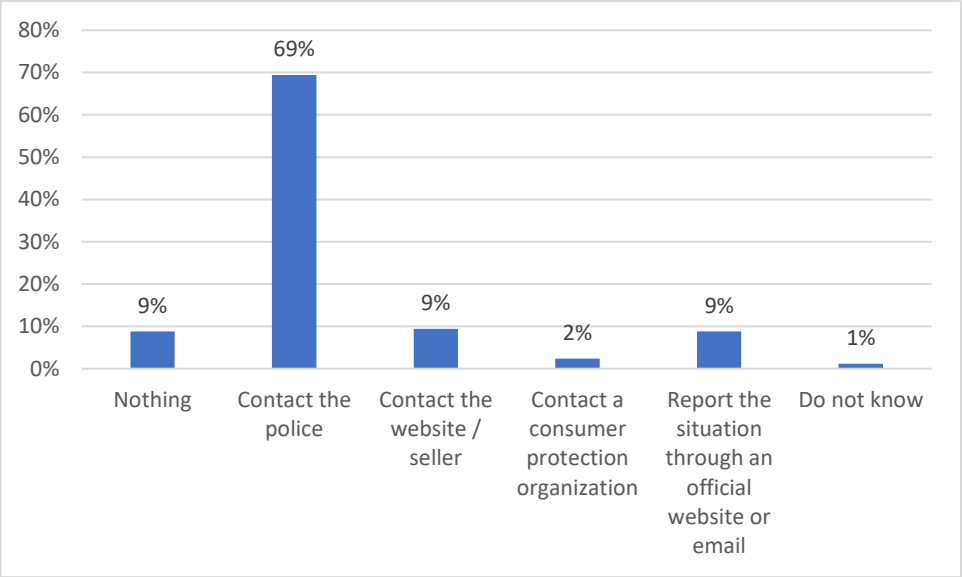
8.6. Finding online material that promotes racial or religious extremism.




Graphic 44 – Analysis of Question 8.6.

According to the graph above it shows that 38% of respondents if they found racist or extremist material would contact the police, 25% would report it through an official website, 16% would contact the website/ vendor and 11% would do nothing.

8.7. Payment request in exchange for regaining control over your device.

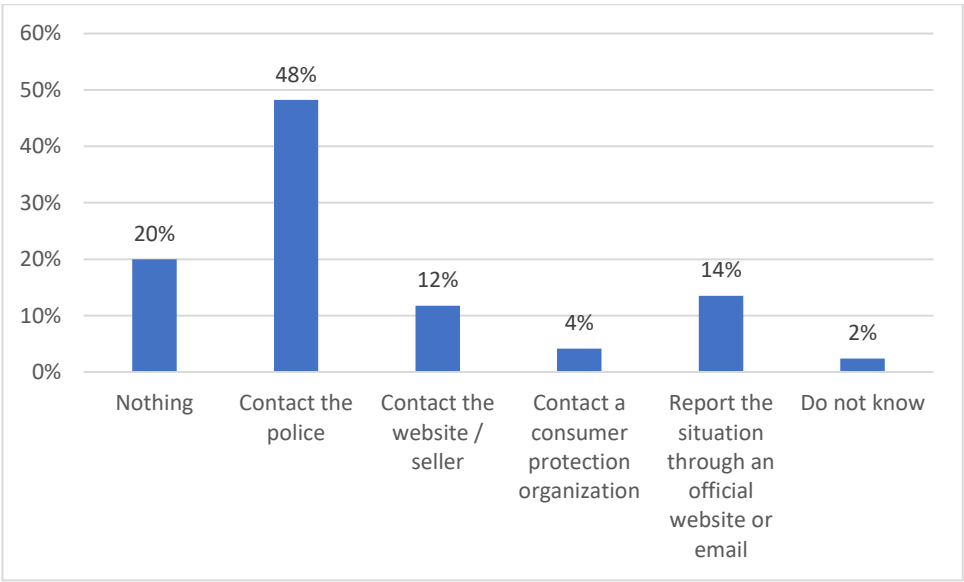



Graphic 45 – Analysis of Question 8.7.

The above graph shows that most of the respondents (69%), if they were a victim of cybercrime by requesting payment in exchange for access to their devices would contact the police.

Also, we can verify that 9% would report the situation through an official website, another 9% would contact the website/ vendor and 2% would contact the consumer protection organisation.

8.8. Receive fraudulent e-mails or phone calls asking for your personal information (e.g., login, computer access, fraudulent payments or your bank information).

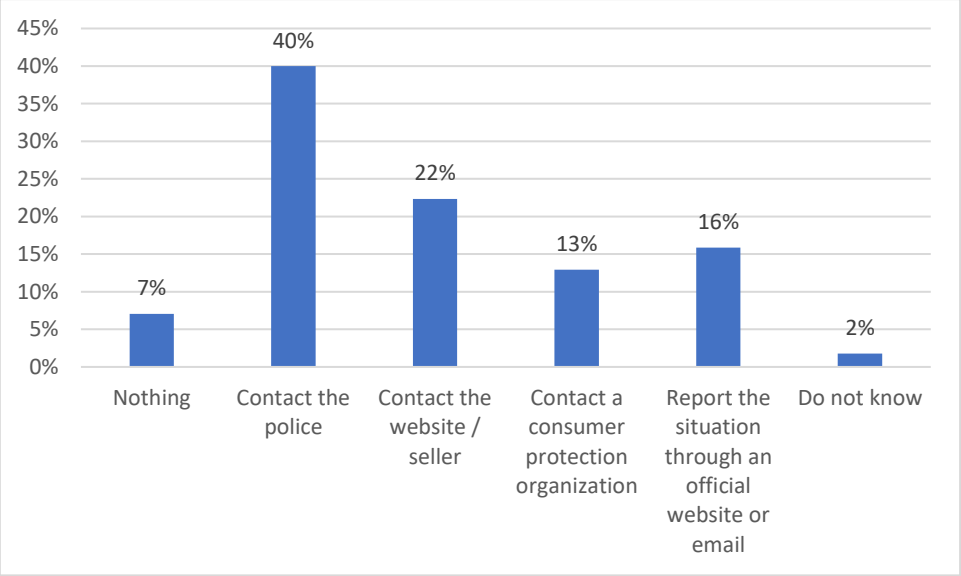



Graphic 46 – Analysis of Question 8.8.

Chart 46 indicates that 48% of respondents would contact the police, if they received fraudulent emails or phone calls asking for their personal information. According to the same chart, 20%

would not, 14% would report the situation through an official website, 12% would contact the website/ vendor and 4% would contact the consumer protection organisation.

8.9. Online fraud in which purchased products are not delivered, counterfeit or do not correspond to the advertised.




Graphic 47 – Analysis of Question 8.9.

The chart above indicates that 40% of respondents would contact the police if they received online fraud where the purchase of an item does not correspond to the advertisement or is counterfeit.

It is also possible to verify that 22% would contact the website/ seller, 16% would report the situation through an official website, 12% and 13% would contact a consumer protection organisation.

## 4.3. DISCUSSION AND RECOMMENDATIONS

Social networks like Facebook, Instagram, YouTube are part of our daily lives. Not a day goes by without anyone accessing social media, whether on a smartphone, tablet, or PC. However, we never think about the risks involved and how we can avoid them. So for this reason, it is necessary to answer some questions, such as:

- Are social mechanisms to improve network security?
- Are there different security and privacy threats in social network platforms?
- Which social network provides the best data security?
- How concerned are users about the exposure of their data on social networks?
- Do users trust in cybersecurity?

### 4.3.1. Discussion

According to the survey's analysis, most respondents leave their passwords stored in the browser, and they are well informed about cybercrime (49%). In 2020, around 164 million people were affected by data breaches. These negative factors that social networks entail, such as security risks, loss of privacy, among others, make respondents worried about their exposure on social networks.

With the number of devices that are connected to the Internet and with the possibility of accessing the most popular services, be they Facebook, WhatsApp, Instagram, etc., human beings want to access their social networks from anywhere, quickly and easily, doing it, most of the time, through your smartphone (73% - Graph 12).

The fact that they want to have immediate access to their services means that they spend more time immersed in social networks, as shown in graph 2 of the previous topic, in which 37% of the respondents spend between 1 and 2 hours a day on their social networks, which leads to other negative factors, such as dispersion and the time they allocate to social media. And, according to some studies, it is indicated that a average user spends on average around 2h24m on social networks. This does not escape the result of the analysis made to respondents.

But on the other hand, as we know, technologies have made the world easier and this has brought some advantages for personal and professional development. And although, sometimes, it has a negative and/ or positive impact on relationships (42%), education (23%), or even increase the number of friends on social networks. When sharing information and being in constant contact with friends, finding new friends or enriching the network of professional contacts to create good job opportunities, human beings need to be increasingly connected to what is happening around them to meet your needs.

While cybercrime is on the rise by the day, leaving people worried about providing personal information on websites (86%), of the 170 people surveyed, 165 avoid revealing their personal information on social networks to protect themselves from cybercrime.

Still, according to 31% of respondents, the social network that brings them more security is LinkedIn. LinkedIn is an active job search platform, where our curriculum vitae is exposed only to those we intend, in this case, the interviewers.

As it is known, the topic of cybersecurity is much debated nowadays, with public authorities trying to find ways to fight cybercrime. However, even so and despite the existence of several solutions, people remain concerned that, often, public authorities or even antiviruses fail to fight cybercrime. Despite all the difficulties that social networks go through and the challenges that present themselves daily, 92% of respondents trust cybersecurity.

When we talk about cybercrime, we know that there are different types of criminal activities. Among these crimes, we have, for example, infection by malicious software, which lead to fraud, identity theft and, as can be seen in the analysis made in point 4, most respondents are very concerned about the fact that they can go through these situations.

In addition to the aforementioned situations being worrisome cybercrimes, they represent crimes for society. For most respondents, if they are infected with malicious software, this is considered a reasonably serious crime. However, if there is an identity theft and they suffer fraud or find material that promotes racial/ religious extremism, they consider it a very serious crime. (Identifying video spammers in online social networks)

In conclusion, if respondents were to suffer from any of the crimes, they would take some steps in order to try to protect themselves against cybercrime. In case they were victims of identity theft, fraud or found child pornography, they contacted the police.

Since there are several ways to suffer a cyber-attack that can harm our lives, whether in relationships or even as individuals, it is necessary that in these situations we are all aware and know when to act to avoid major problems.

### 4.3.2. Recommendations

According to the analysis made to 170 people surveyed, they were able to understand there are mechanisms that can improve Internet security and, for this, the agencies responsible for information security (police, consumer protection agency) must act. Here are some examples that can be applied even by a simple user:

**Passwords –** Cybercriminals are always looking for ways to log into the accounts of home users who use easy-to-remember passwords, such as 123456 or QWERTY. To fight cybercrime, it is best to create passwords made up of special characters, capital letters and numbers (Agarwal, 2021).

**Be able to find threats effectively –** Every day we are impacted by emails and advertisements that seem to us to be trustworthy. However, you must be aware of its origin, if it is an email, pay attention to the sender's email, if it is an advertisement, check if the company in question exists and/ or if we are not referred to malicious websites (Stealth Labs, 2020).

**Antivirus/ Firewalls –** Some companies specialize in home and professional security that help protect networks. Purchasing an antivirus or a firewall helps the security of our machines, thus keeping cybercriminals away (TSR – The Software Report, 2020).

**Suspicious software –** There are some software, namely browser plugins that are malicious and have stolen personal information from users. The best way to combat this is to check the rating that other users give to plugins and choose those from well-known companies (Olzak, 2021).

**Clicking on social media links –** When we are browsing our social networks sometimes some posts have curious stories. Our curiosity to click on posts opens a door for cybercriminals to capture our data (Girolamo, 2019).

**Keep software up to date –** According to the website "Get Cyber Safe" (2020), it is important to keep the operating system up to date as this includes software security services and this helps the system to be always protected.

If we keep an eye on our surroundings and in conjunction with the options presented above, users can have a more relaxed life when it comes to network security. Furthermore, as demonstrated in the study, the concerns of users of social networks have increased over the years.

As it is known, companies that manage social networks collect daily billions of data. Since there aren't many government regulations to manage all these companies, cybercriminals take advantage of every loophole to commit any crime.

If personal data ends up in the hands of cybercriminals, the consequences can be very damaging, for example, if personal information has been stolen it can be redirected to malware sites, among others. And with constant attacks or even warnings that are published by the media, users are forced to change certain behaviours, so as not to expose their personal information.

Any social media user can be tricked by a cybercriminal so that they hand over all their data without realizing it. For this to happen, what are the most common threats?

**Phishing –** According to Ivan Belcic (2021), it is the oldest one, and the most used way by cybercriminals, where they try to get the information of social network users. Usually, criminals use email, text messages in which they present themselves as a legitimate company. Another example is posts on social networks such as "look what they're saying about you...". Either emails, messages or social media posts induce people to share their private data. To get around this, the best protection is not to click on the links, delete the messages, block third-party access to accounts or even use two-factor authentication.

**Bot Attacks (Botnet Attacks) –** Social media bots are automated accounts created to capture user data without users realizing it. These bots not only create posts like a regular user but can also follow your every move. To avoid being caught off guard, it is best to read the post or messages carefully to avoid clicking on links that appear to be fraudulent, such as messages or videos created by the bots (CDNetworks, 2021).

**Malware –** Malware is designed to directly access computers. Once installed on the computer, malware can steal personal information (spyware) or lock the PC, and the user is forced to pay a monetary ransom to access your machine (ransomware). Or even Adware, the famous pop-ups that appear on browsers, serve as a gateway to various other malware. To avoid getting infected with malware, it is best to check if the websites you browse are safe (if they have an SSL security certificate – Secret Socket Layer) and use ad blockers (Regan, 2019).

When it comes to social networks, you know the risks involved, and none offers enough security, our protection depends only on ourselves. One of the great, very recent, examples is the 2016 US presidential elections, when over 50 million Facebook users' private information was exposed (Cadwalladr & Graham-Harrison, 2018). This event, by itself, destroyed all the trust social networks had until then.

Each new policy implemented brings new challenges to social networks in the fight against cybercrime. Of the 170 respondents, 53 indicated that the social network that offers the most security is LinkedIn, but in 2012 the company was forced to create and change protocols to bring more security to users and to be able to forget what happened (Andy, 2017). In this same situation, Twitter had 0% of respondents, although it is a social network with some growth, it still has little expression in Portugal. Twitter is a platform that uses many bots, and is trying to protect the integrity of the platform by reducing the number of bots present on the social network (Roth & Pickles, 2020).

None of the social networks, despite the daily fighting against cybercrime, offers much security. Or rather, they sometimes offer a false sense of security, as criminals always find ways to bypass social media platforms. It is best to follow the recommendations of each of the social networks. Although some recommendations are not easy to understand or are a bit boring (e.g., changing your password frequently), about 90 per cent of cyber-attacks are caused by human error (Bisson, 2020). For this reason, it is important to trust the recommendations as it will increases our confidence in cybersecurity.

# 5. CONCLUSION

The first part of this chapter contains the conclusions that were reached on the work developed as the literature and data analysis. The second part contains the limitations of the research and the third and last part of this chapter contains suggestions for future works.

## 5.1. SYNTHESIS OF THE DEVELOPED WORK

With the entry of the 21st century, social networks and the Internet developed very quickly. And with this, the interaction between users on social networks is improving every day, but as technologies evolved, threats also increased. These threats are causing a lot of problems for common social networks users.

The main goal of this research is to create a theoretical model that will allow social network users to protect online their privacy. Furthermore, this study allows us to understand if users of social networks adopt security measures to protect their personal information and if they know the best security practices. The research questions were:

- Are there social mechanisms to improve network security?
- Are there are different security and privacy threats in social network platforms?
- Which social network provides the best data security?
- How concerned are users about the exposure of their data on social networks?
- Do users trust in cybersecurity?

To answer these questions, a survey was applied to do the research. The overall conclusion is that most respondents have basic knowledge about cybersecurity, but even so it still compromises their protection on social networks, mainly by leaving the password recorded in the browser.

Through this study of cybersecurity on social media networks, it was possible to discuss the different types of threats that users face every day on social networks. These threats concern the sharing of our personal information, the posts we make, the messages that are exchanged, and the shared links that are clicked.

Security policies existing in different organizations are constantly revised. The best practical solution to end the problem of users being victims of social media threats is end-user awareness. This work was developed in-depth and gave several points about which the 170 respondents and the other users should be informed.

## 5.2. RESEARCH LIMITATIONS

The biggest limitation of this research was the data used. the first moment starts with the survey that was sent to the respondents, as it is worrying that some of them may have provided wrong answers or false data. In fact, this is because the survey was online, both on Facebook and LinkedIn and was sent by email, it was a bit long and there was no compensation for respondents.

Another limitation was the time restriction. The survey was carried out within a stipulated deadline, however, there were some delays, especially in the delivery of data by respondents. As the survey was online, users were free to fill it at any time or day.

There were also other challenges beyond this research, such as balancing work for the master's degree and my daily work. Therefore, as I was limited in terms of time, I took advantage of all the free time I had to be able to dedicate myself to this research. As there were also monetary constraints, data analysis was not done through premium tools. The main data collection tool to lower research cost.

The selected sample was also a limitation, as it was very difficult to find respondents who would make available part of their time to answer the survey. Initially, when the survey was made available on social networks, not all volunteers filled in and sent back their answers. However, even with all these limitations, a significant number of responses were obtained, enough to extract the necessary information from them.

And, finally the biggest limitation found in this research was writing. To carry out this research and presenting the problems objectively seems to be an easy thing to do. However, once the information becomes available and new discoveries are made, research development becomes more challenging.

## 5.3. FUTURE WORK

By analysing the most diverse works in the existing literature on the subject, this research sought to address the main threats to privacy and security in social media. This has been outlined by earlier researchers in their works. For this reason, this research aims to present some areas for future researchers to deepen and, probably, bring more knowledge on the subject.

One of the topics that future researchers will be able to address is to thoroughly research and analyse how applications are collecting all users' information and how access to personal information can be limited. Another point that can be addressed in future research is how social networks and governments can collaborate together to fight cybercrime, which increases day by day, to avoid bigger problems.

A third point that could also be addressed is the legislation that governments are or should be drafting to protect their citizens and how they can ensure their privacy. It would also be interesting to make the survey available by different parts of the world and also by different age groups, in order to gain more knowledge about how people are informed about the exposure of their data on online platforms and how they protect themselves.

## BIBLIOGRAPHY


Aboulhosn, S. (2020, February 19). How to build a social media marketing funnel that converts. Retrieved from Sproutsocial: https://sproutsocial.com/insights/social-media-marketing-funnel/

Academy, E. F. (2021, January 25). A Decade-by-Decade History of Cybersecurity. Retrieved from Eleven Fifty Academy: https://elevenfifty.org/blog/a-decade-by-decade-history-of-cybersecurity/

Agarwal, K. (2021, March 03). 10 Ways to Improve Data Security. Retrieved from Lepide: https://www.lepide.com/blog/ten-ways-to-improve-data-security/

Alliance, N. C. (n.d.). Social Media. Retrieved from Stay Safe Online: https://staysafeonline.org/stay-safe-online/securing-key-accounts-devices/social-media/

Antunes, M., & Rodrigues, B. (2018). *Introdução à Cibersegurança: A Internet, os aspetos legais e a análise digital forense.* Lisboa: FCA – Editora de Informática.

B., A. (2017, June 28). National Cybersecurity Centre. Retrieved from LinkedIn 2012 hack: what you need to know: https://www.ncsc.gov.uk/blog-post/linkedin-2012-hack-what-you-need-know

Banerjee, S. (2017, September 19). The Cyber Security Risks On Social Media – Learn From Case Studies. Retrieved from RS Websols: https://www.rswebsols.com/tutorials/internet/cyber-security-risks-social-media

Belcic, I. (2021, May 19). O guia essencial sobre phishing: Como funciona e como se proteger. Retrieved from Avast Academy: https://www.avast.com/pt-br/c-phishing#topic-7

Benevenuto, F., Rodrigues, T., Almeida, V., Almeida, J., & Gonçalves, M. (2009, July 19). Detecting spammers and content promoters in online video social networks. Retrieved from ACM Digital Library: https://dl.acm.org/citation.cfm?id=1572047

Benevenuto, F., Rodrigues, T., Almeida, V., Almeida, J., Zhang, C., & Ross, K. (2008, April 22). Identifying video spammers in online social networks. Retrieved from ACM Digital Library: https://dl.acm.org/citation.cfm?id=1451996

Bisson, D. (2020, October 15). 7 Data Breaches Caused by Human Error: Did Encryption Play a Role? Retrieved from Venafi: https://www.venafi.com/blog/7-data-breaches-caused-human-error-did-encryption-play-role

Bond, M. (2020, December 16). What is an Online Community? The Basics & Benefits. Retrieved from Higer Logic: https://www.higherlogic.com/blog/what-is-an-online-community/

Bradley, A. J., & McDonald, M. P. (2011). *The Social Organization - How to use social media to tap the collective genius of your customers and employees.* Boston, Massachusets: Gartner Inc.

Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. Retrieved from The

Guardian: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Castillo, C., Mendoza, M., & Poblete, B. (2011, March 28). Information credibility on twitter. Retrieved from ACM Digital Library: https://dl.acm.org/citation.cfm?id=1963500

Cavelty , M. D. (2007). *Cyber-Security and Threat Politics: Us Efforts To Secure The Information Age.* Taylor & Francis LTD.

CDNetworks. (2021, May 17). Botnet Attacks – Everything you need to know. Retrieved from CDNetworks: https://www.cdnetworks.com/cloud-security-blog/botnet-attacks/

Cyber Security Information Portal. (n.d.). Learning Centre: Safe Social Networking. Retrieved from Cyber Security Information Portal: https://www.cybersecurity.hk/en/learning-social-networking.php#slide-1

Datareportal. (n.d.). Global Social Media Stats. Retrieved from Datareportal: https://datareportal.com/social-media-users

Finjan Team. (2017, February 27). Finjan Cybersecurity. Retrieved from What is Non-Repudiation? A Closer Look at the Principles, Techniques and Best Practices: https://blog.finjan.com/what-is-non-repudiation/

Get Cyber Safe. (2020, January 15). Software updates: Why they matter for cyber security. Retrieved from Government of Canada: https://www.getcybersafe.gc.ca/en/blogs/software-updates-why-they-matter-cyber-security

Ghosh, S. (2011, January 28). Seven social media security best practices. Retrieved from ComputerWeekly.com: https://www.computerweekly.com/tip/Seven-social-media-security-best-practices

Girolamo, R. D. (2019, October 02). Never Click and Tell: Staying Safe on Social Media. Retrieved from Connected: https://community.connection.com/never-click-and-tell-staying-safe-on-social-media/

Grundy, W. (n.d.). Cyber Security Risk in a Social Media World. Retrieved from Cyber Risk & Insurance Forum: http://www.cyberriskinsuranceforum.com/content/cyber-security-risk-social-media-world

Hayes, N. (20016, June 09). Why Social Media Sites Are The New Cyber Weapons Of Choice. Retrieved from Dark Reading: https://www.darkreading.com/attacks-breaches/why-social-media-sites-are-the-new-cyber-weapons-of-choice/a/d-id/1326802

IBM Corporation. (2015). IBM 2015 Cyber Security Intelligence Index. USA: IBM. Retrieved from https://essextec.com/wp-content/uploads/2015/09/IBM-2015-Cyber-Security-Intelligence-Index_FULL-REPORT.pdf

Jabee, R., & Afshar, A. (2016, June). Issues and Challenges of Cyber Security for Social Networking Sites (Facebook). Retrieved from Researchgate: https://www.researchgate.net/publication/304066517_Issues_and_Challenges_of_Cyber_Security_for_Social_Networking_Sites_Facebook

Kemp, S. (2020, January 30). Digital 2020: Global Digital Overview. Retrieved from Datareportal: https://datareportal.com/reports/digital-2020-global-digital-overview

Olzak, T. (2021, March 8). Malicious Browser Extensions: Why they could be the next big cybersecurity headache. Retrieved from Toolbox: https://www.toolbox.com/it-security/vulnerability-management/articles/malicious-browser-extensions/

Parker, S. (2017, Jully 31). Cyber Security Risks in the Social World. Retrieved from The State of Security: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/cyber-security-risks-social-world/

Parker, S. (2017, June 06). Cyber Security Risks On Social Media: 5 Ways Users Are Vulnerable. Retrieved from SAC - The Security Awareness Company: https://www.thesecurityawarenesscompany.com/2017/06/06/cyber-security-risks-social-media-5-ways-users-vulnerable/

Patel, F., Koreh, R., Levingson-Waldman, R., & DenUyl, S. (2019, May 22). Social Media Monitoring. Retrieved from Brennan Center For Justice: https://www.brennancenter.org/our-work/research-reports/social-media-monitoring

Peters, J. (2018, March 31). Weekly Cyber Risk Roundup: Myfitnesspal breach, carbanak leader arrested. Retrieved from Cyber in Sight: https://blog.surfwatchlabs.com/2018/03/31/weekly-cyber-risk-roundup-myfitnesspal-breach-carbanak-leader-arrested/

Peters, J. (2018, March 24). Weekly Cyber Risk Roundup: Orbitz breach, Facebook Privacy Fallout. Retrieved from Cyber in Sight: https://blog.surfwatchlabs.com/2018/03/24/weekly-cyber-risk-roundup-orbitz-breach-facebook-privacy-fallout/

Poremba, S. (2017, December 21). Prediction: Social Impact of Cybersecurity Breakdowns. Retrieved from IT Business Edge: https://www.itbusinessedge.com/blogs/data-security/prediction-social-impact-of-cybersecurity-breakdowns.html

Rathore, S., Sharma, P. K., Loia, V., Jeong, Y.-S., & Park, J. H. (2017, August 23). Social network security: Issues, challenges, threats, and solutions. Retrieved from ScienceDirect: https://www.sciencedirect.com/science/article/pii/S0020025517309106

Regan, J. (2019, July 10). O que é malware? Como malwares funcionam e como se livrar deles. Retrieved from AVG: https://www.avg.com/pt/signal/what-is-malware

Rita, P. (2018, February 19). Research Design. Universidade Nova Information Management School.

Roth, Y., & Pickles, N. (2020, May 18). Bot or not? The facts about platform manipulation on Twitter. Retrieved from Twitter: https://blog.twitter.com/en_us/topics/company/2020/bot-or-not

Salam, M., Panda, M., Elbarawy, Y., Hassanien, A. E., & Abraham, A. (2012, June 20). Computational Social Networks: Security and Privacy. Retrieved from Springer Link: https://link.springer.com/chapter/10.1007%2F978-1-4471-4051-1_1

Samur, A. (2018, November 22). The History of Social Media: 29+ Key Moments. Retrieved from Hottsuite: https://blog.hootsuite.com/history-social-media/

SBA – U.S. Small Business Administration. (n.d.). Cyber-attacks are a growing concern for small businesses. Learn about the threats and how to protect yourself. Retrieved from Stay safe from cybersecurity threats: https://www.sba.gov/managing-business/cybersecurity/social-media-cyber-vandalism-toolkit

Shea, S., Gillis, A., & Clark, C. (n.d.). Cybersecurity. Retrieved from Searchsecurity: https://searchsecurity.techtarget.com/definition/cybersecurity

Solis, B. (2017, July 24). The 2017 Social Media Universe in One Infographic: Introducing The Conversation Prism 5.0. Retrieved from LinkedIn: https://www.linkedin.com/pulse/2017-social-media-universe-one-infographic-prism-50-brian-solis/

Statista. (2021). Number of monthly active Facebook users worldwide as 1st quarter 2021 (in millions). Retrieved from Statista: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

Stealth Labs. (2020, December 04). *Cyber Security Threats and Attacks: All You Need to Know*. Retrieved from Stealth Labs: https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/

Symantec. (2019). ISTR – Internet Security Threat Report. United Stated of America: Symantec. Retrieved from https://docs.broadcom.com/doc/istr-24-2019-en

Terrill, C. (2017, April 28). What You Need To Know Now About Cybersecurity And Social Media. Retrieved from Forbes: https://www.forbes.com/sites/christieterrill/2017/04/28/what-you-need-to-know-now-about-cybersecurity-and-social-media/#1ea936543a16

Trend Micro. (2016, May 18). 2012 Linkedin Breach had 117 Million Emails and Passwords Stolen, Not 6.5M. Retrieved from Trend Micro: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/2012-linkedin-breach-117-million-emails-and-passwords-stolen-not-6-5m

Trend Micro. (2018, May 04). Change Your Passwords: Twitter Bug Exposes User Passwords. Retrieved from Trend Micro: https://www.trendmicro.com/vinfo/us/security/news/online-privacy/change-your-passwords-twitter-bug-exposes-user-passwords

Trend Micro. (2019, June 30). Hunting Threats on Twitter. Retrieved from Trend Micro: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hunting-threats-on-twitter

TSR – The Software Report. (2020, December 22). *The Top 25 Cybersecurity Companies Of 2020*. Retrieved from TSR – The Software Report: https://www.thesoftwarereport.com/the-top-25-cybersecurity-companies-of-2020/

Union, E. (2018). The GDPR: new opportunities, new obligations. Luxembourg: Publications Office of the European Union. Retrieved from https://ec.europa.eu/info/sites/default/files/data-protection-factsheet-sme-obligations_en.pdf

University Information Technology Services. (2021, March 16). About viruses, worms, and Trojan horses. Retrieved from University Information Technology Services: https://kb.iu.edu/d/aehm

Walkowski, D. (2019, July 09). What Is the CIA Triad? Retrieved from F5 Labs Application Threat Intelligence: https://www.f5.com/labs/articles/education/what-is-the-cia-triad

Yang, C., Harkreader, R., Zhang, J., Shin, S., & Gu, G. (2012, April 16). Analyzing spammers' social networks for fun and profit: a case study of cyber criminal ecosystem on twitter. Retrieved from ACM Digital Library: https://dl.acm.org/citation.cfm?id=2187847

# Cybersecurity on Social Networks

This survey aims to characterize and assess your concern with cybersecurity issues on social networks. The information collected will be treated with the utmost respect for the confidentiality of respondents.

**Part A**

**Age**

☐ <25 ☐ 26 – 35 ☐ 36 – 45 ☐ 46 – 55 ☐ 56 – 65 ☐ > 66

**Gender:**

☐ Male ☐ Female ☐ Other

**Education:**

☐ No Formal School
☐ High School Graduate
☐ Professional degree
☐ Bachelor's degree
☐ Postgraduate
☐ Academic License
☐ Master's Degree
☐ Doctorate Degree

**Occupation:**

☐ Agriculture, Food and Natural Resources
☐ Architecture and Construction
☐ Arts, Audio/ Video Technology and Communications
☐ Business Management and Administration
☐ Education and Training
☐ Finance
☐ Government and Public Administration
☐ Health Science
☐ Hospitality and Tourism
☐ Human Services
☐ Law, Public Safety, Corrections and Security
☐ Information Technology
☐ Marketing, Sales and Service
☐ Manufacturing

☐ Transportation, Distribution and Logistics
☐ Science, Technology, Engineering and Mathematics
☐ Unemployed
☐ Retired
☐ Other

**Part B**

1. **How much time do you spend on social media per day?**

☐ Less than 1 hour
☐ From 1 hour to 2 hours
☐ From 2 hours to 3 hours
☐ More than 3 hours
☐ None

2. **Which of the following social networks do you use?**

☐ Facebook
☐ Instagram
☐ TikTok
☐ YouTube
☐ WhatsApp
☐ Messenger
☐ Reddit
☐ Snapchat
☐ Pinterest
☐ Twitter
☐ LinkedIn
☐ I do not use

3. **What are you looking for in Social Networks?**

☐ Contacts with friends
☐ Loving relationships
☐ Find old friends
☐ Professional contacts
☐ Look for a job

4. **Which are the most negative factors in the use of Social Networks?**

   ☐ The dispersion
   ☐ Loss of privacy
   ☐ Time allocated to networks
   ☐ Security risks
   ☐ There are no negative points

5. **Which are the most positive factors in the use of Social Networks?**

   ☐ Information sharing
   ☐ Peoples connection
   ☐ Freedom of expression
   ☐ Business opportunity
   ☐ Chat with friends

6. **What goal did you achieve on Social Networks?**

   ☐ Fame/ Recognition
   ☐ Boyfriend/ Girlfriend
   ☐ Increased self-esteem
   ☐ New friends
   ☐ New job

7. **In your opinion, in which area do Social Networks makes the most impact?**

   ☐ Work environment
   ☐ Relationships
   ☐ Education
   ☐ Government

8. **Which device do you prefer to access Social Networks?**

   ☐ Smartphone
   ☐ Computer
   ☐ Tablet

9. **How many friends do you currently have on your Social Networks?**

   ☐ < 150
   ☐ 151-250
   ☐ 251-350
   ☐ 351-450
   ☐ 151-250
   ☐ > 451

**Part C**

1. **Do you keep the passwords saved in the browser?**

   ☐ Yes
   ☐ No

2. **Which social network provides the best data security?**

   ☐ Facebook
   ☐ Instagram
   ☐ TikTok
   ☐ YouTube
   ☐ WhatsApp
   ☐ Messenger
   ☐ Reddit
   ☐ Snapchat
   ☐ Pinterest
   ☐ Twitter
   ☐ LinkedIn

3. **Do you trust in cybersecurity?**

   ☐ Yes
   ☐ No

4. **How well informed do you feel about cybercrime risk?**

   ☐ Not informed
   ☐ Not very well informed
   ☐ Reasonably well informed
   ☐ Well informed
   ☐ Very well informed

**5. Do you agree or disagree with the following statements?**

| Statements | Agree | Disagree | Undecided |
|---|---|---|---|
| Avoiding revealing your personal information. | | | |
| Do you believe that the risk of being a cybercrime victim is increasing? | | | |
| Are you concerned that your personal information isn't secure on the websites? | | | |
| Are you concerned that your personal information isn’t protected by the public authorities? | | | |
| Do you think that a protection tool, like an antivirus, will protect you from cybercrime? | | | |

6. **Cybercrimes include many types of criminal activities. How concerned are you, personally, about experiencing or being a victim of the following situations?**

| Situations | Not Concerned | Not very well Concerned | Reasonably well Concerned | Well Concerned | Do not Know |
|---|---|---|---|---|---|
| Device infection with malicious software (malware, etc.). | | | | | |
| Identity theft (someone that steals your personal information). | | | | | |
| Hacking your social networks or email account. | | | | | |
| Online material that promotes racial or religious extremism. | | | | | |
| Cyber-attacks that prevent you from accessing online services, such as your bank account. | | | | | |
| Payment request in exchange for regaining control over your device. | | | | | |
| Online fraud in which purchased products are not delivered, counterfeit or do not correspond to the advertised. | | | | | |

**7. In your opinion, which of these situations represents a very serious, reasonably serious, minor crime or is it not even a crime?**

| Situations | Very serious | Reasonably serious | Minor crime | It's not even a crime | Do not know |
|---|---|---|---|---|---|
| Infection of devices with malicious software (malware, etc.). | | | | | |
| Identity theft (someone that steals your personal information). | | | | | |
| Bank card or online banking fraud. | | | | | |
| Hacking your social networks or email account. | | | | | |
| Online material that promotes racial or religious extremism. | | | | | |
| Cyber-attacks that prevent you from accessing online services, such as your bank account. | | | | | |
| Payment request in exchange for regaining control over your device. | | | | | |
| Online fraud in which purchased products are not delivered, counterfeit or do not correspond to the advertised. | | | | | |

**8. What would you do in the following situations, if you had been a cybercrime victim?**

| Situations | Nothing | Contact the police | Contact the website / seller | Contact a consumer protection organization | Report the situation through an official website or email | Do not know |
|---|---|---|---|---|---|---|
| Discover malicious software on your device (virus, etc.). | | | | | | |
| Identity theft (someone that steals your data). | | | | | | |
| Being a victim of online bank or bank card fraud. | | | | | | |
| Find online child pornography. | | | | | | |
| Hacking your social networks or the email account. | | | | | | |
| Finding online material that promotes racial or religious extremism. | | | | | | |
| Payment request in exchange for regaining control over your device. | | | | | | |
| Receive fraudulent e-mails or phone calls asking for your personal information (e.g., login, computer access, fraudulent payments, or your bank information). | | | | | | |
| Online fraud in which purchased products are not delivered, counterfeit or do not correspond to the advertised. | | | | | | |