ALEJANDRO ÁLVAREZ CABELLO
NIU: 1392903

FINAL DEGREE PROJECT
6TH CRIMINOLOGY + LAW
TUTOR: AINOA TORRADO SÁNCHEZ
WORDS: 9.007

UAB
Universitat Autònoma
de Barcelona

Abstract

The world has changed due to the COVID-19 pandemic, and so does cybercrime. Cybercriminals are exploiting the coronavirus scenario and as such, questions arise around how they are doing it and its impact. Coronavirus and cybercrime are relatively new topics in the scene and there are only a handful of studies that have been released. Therefore, this research tries to be an introduction to the cybercrime and phenomenon from a classic criminological perspective, to later on go on details on how COVID-19 is providing a shift in opportunities for cybercriminals and how it influences regular, old cybercrime techniques. Finally, the empirical work will try to discover if cybercrime victimization rates have increased in 2020 in lack of official records that prove so.

Key Words: COVID-19, Coronavirus, Pandemic, Cybercrime, Cyberspace, Scams, Phishing

Resumen

El mundo ha cambiado debido a la pandemia causada por el COVID-19, y también lo ha hecho la ciberdelincuencia. Los ciberdelincuentes están explotando el escenario creado por el coronavirus, lo que genera preguntas sobre su modus operandi y su impacto. Coronavirus y ciberdelincuencia son temas relativamente nuevos en la escena y es por ello que hay muy pocos estudios publicados. Por lo tanto, este trabajo trata de ser una introducción al fenómeno de la ciberdelincuencia desde la perspectiva de la criminología clásica, para luego dar detalles sobre como el COVID-19 está provocando un cambio en las oportunidades para delinquir y como éste influencia a las técnicas de ciberdelincuencia que ya estaban presentes. Finalmente, el trabajo empírico tratará de descubrir si las ratios de victimización de ciberdelincuencia han subido durante 2020 a falta de datos oficiales que lo confirme.

Palabras clave: COVID-19, Coronavirus, Pandemia, Cibercrimen, Ciberespacio, Estafas, Phishing

Acknowledgements

To my tutor, Ainoa, for her infinite patience, putting up with me and giving me a chance when I did not deserve one.

To both Aina and Mr. Felipe Z TotalSpin and their communities for helping me share and completing the online victimization survey.

To the new friends I made along the way and for those that we have lost something valuable during this pandemic.

This is for you.

INDEX

1. INTRODUCTION

Over 163.000.000 cases and 3.300.000 deaths (WHO, 2021); even to this day, COVID-19 is still going strong. What started as a few cases of an unknown disease in Wuhan back in December of 2019, it took over the world in 2020. In order to fight the pandemic, almost every country in the world had to issue lockdown measures. Confined in their homes, a critical dependency on virtual environments was born. Such surge in Internet usage did not go unnoticed though; cybercriminals were ready to exploit it.

The COVID-19 pandemic has brought to light many cybersecurity problems that have been around for years (Fontanilla, 2020). An example of this is how poorly remote work has been set up. There is also the issue of Law Enforcement Agencies lagging behind cybercrime development due to the nature of the latter, and previous year numbers and trends indicated that 2020 would be no different; cybercrime would go up; and it did (EUROPOL, 2020).

Cybercrime is continuously changing, evolving, and adapting, which is why the criminological scene must periodically study it. This paper will try to fit that criteria; it will go through a study of cybercrime literature, track down COVID-19 themed cybercrime cases and analyze why they are effective, compare 2020's vs 2019's and finally, try profiling both victims and offenders through an empirical research.

The World Health Organization, the United Nations, EUROPOL, INTERPOL and several other international organizations consider COVID-19 themed cybercrime as another type of pandemic, almost as threatening as the medical one (Wertheim, 2020). Every effort put into analyzing cybercrime might later become the key in order to prepare good prevention strategies, something that is almost intrinsic to criminology.

2. THEORETICAL FRAMEWORK

2.1. The cybercrime phenomenon

2.1.1. Defining cybercrime and cyberspace

The term *cybercrime* has been historically used interchangeably with other expressions such as cyberdelinquency, computer crimes, cybercriminality, etc. Most definitions of the term just refer to cybercrime as *"any crime that is facilitated or committed using a computer, network, or hardware device"* (Naidoo, 2020). While these kinds of definitions are not wrong and are definitely broad (taking criminology's approach to the evolution that the conception of not reflects these crimes went through. Terms such as *computer crimes* perfectly expressed the concern for a new type of crime that arose with the appearance of the first computer systems, in which they were the means or the objective of crime (Miró-Llinares, 2012). With time, the concern is focused not on the fact that the crimes are committed through these new devices, but rather the fact that such computer systems are connected in a transnational-universal communication sphere: cyberspace[1] (Wall, 2007). Hence, for the purpose of this research, Jewkes (2006) definition will be adopted:

> *"Cybercrime comprises any illegal act committed through (or with the assistance of) computer systems, digital networks, the Internet and other ICTs."*

In cyberspace's case, explanatory; it is a relational construct, devoid of physical form. It can only exist as long as there is a "spa interaction between its users (Miró-Llinares, 2011).

How does this virtual space work though? As one might guess, time and space operate differently in cyberspace due to it not being a physical location. Space gets contracted, and the notion of distance disappears. Something similar happens with time; the compression of time makes it non-linear, which means two things: firstly, contact between users is instant and, secondly, an act that in the real world would

[1] While cyberspace and the Internet are not exactly the same, for the sake of this research both terms might be used interchangeably.

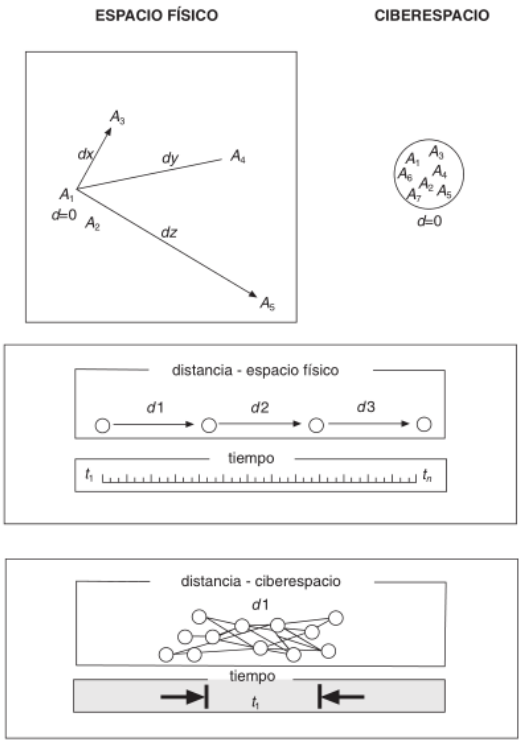
be instantaneous and deciduous, can become perennial in the virtual world. **Fig. 1** exemplifies the compression of those two elements.

There are other elements, however, that characterize cyberspace:

Cyberspace is ***transnational***. It has no physical location, which means it does not belong to any particular State, hence the inexistence of borders and hurdles in the way of communication.

Cyberspace is ***neutral***. This obeys to *Net Neutrality*, which are a set of rules that force Internet Service Providers and state legislation to treat Internet traffic as equal, regardless of its content or the means of access. In a practical sense, this means that ISPs cannot block the user's access to ce

Fig. 1. Depiction of the contraction of space and time in cyberspace.



Source: Miró-Llinares (2011).

Cyberspace is not ***centralized.*** On the Internet there is no central or superior authority that can establish any type of measures regarding the access or control of the contents on it in a systematic or general way (Casabona, 2006). Ultimately, what

this means, is that each State's law is exploited instead as applied by cybercriminals by committing offenses in other countries where they might not be prosecuted. There are, however, unique tools that the States have at their disposal in terms of cooperation, such as the European Investigation Order, mutual legal assistance and Joint Investigation Teams[2].

*Cyberspace is **anonymized**.* While it is somewhat easy for Law Enforcement Agencies to know which device is being used to access the Internet[3], it is practically impossible[4] to identify the person using said device. Adding onto this, there are also other tools to mask one's presence on cyberspace, e-mail services, *Virtual Private Networks* or even the *Dark Web* (López, 2001).

*Cyberspace is **universal***. Internet's popularity is, in an vast number of people that access the cyberspace means that there will be both a large number of potential victims and uprising offenders. This constant influx of people also means that cyberspace is **constantly evolving,** which has an important implication; the law will always trailer on its measures, many of them becoming obsolete when they come into force.

2.1.2. Criminological theories approach

As it can be seen, cyberspace presents enough peculiarities for the criminological scene to wonder if it can become a new space for criminal opportunity. Since most criminological theories were not conceived with the Internet in mind, they have had to be "updated" to try to explain cybercrime. This poses a natural question: which criminological theory suits best? While it is not a definitive answer, the Routine Activities Theory (henceforth RAT) by Cohen and Felson (1979) appears to be the one that translates the issue fairly well (Miró-Llinares, 2011). There are a few reasons behind this choice. As Yar (2016, p. 263) states:

[2] Multi-lateral agreement treaties still pose a fair share of problems though, such as time dilation and conflicts over the choice of law (Kent, 2015).
[3] The device can be geolocated through the *Internet Protocol Address* that was used to access the Internet.
[4] While identifying the person using a certain device is rather challenging, Law Enforcement Agencies could still do so through the use of specialized tools and methods, such as *honeypots* or *spyware*.

> *First, it is an established and widely mobilized theory that has been used to analyze various forms of criminal behavior […]. Second, its clear analytical schema permits relatively straightforward application across a range of scenarios. Third, it offers clear cues for policy and crime-prevention, as seen in "situational crime prevention" strategies that draw on RAT […]*

The original configuration of the theory implies that criminal activities are developed when three elements converge: a motivated offender, a suitable target and the arise of a chance to strike, that is, the absence of capable guardians against a violation. These elements however, as explained previously, must be updated and tested to see if RAT is viable in explaining cybercrime, something that has been researched several times with various degrees of success (Yar, 2016)[5].

As for the **motivated offender**, most of the differences with the physical offender that the original theory proposes stem from how time and space are perceived in cyberspace. As Brenner and Clarke (2004) point out, in the physical world, for a crime to occur, both actors must be at a close distance and together at a certain point of time; the Internet, however, as previously stated, removes that requirement. The lack of any need for physical displacement ends up lowering the costs of executing the crime.

That, in and on itself, is the main advantage that the cyberspace offers to offenders: the balance between risks/costs and reward is way too tipped in favour of the latter. As Yar (2005) states, people with less resources invested into committing an offence can still generate big profits due to the ripple effect that *ICTs* have (malware is a good example of this). There is also the fact that, due to how the Internet works, the attack can be performed from anywhere around the globe, adding onto the non-traceability of the offender.

All these factors combined lead to the disappearance of the fear of being identified and therefore, the consequent minimization of the fear of being arrested, which represent important brakes (now gone) to becoming a motivated offender.

[5] It is a comparative study that takes into account all previous researches that tried to explain the viability of understanding cybercrime through RAT.

According to RAT, the degree to which someone is a **suitable target** for a motivated offender largely explains victimization. The concept of a suitable target in cyberspace is something that has been a point of discussion among the scene. Felson (2001) alleged that a suitable target *"can be any person or property that an offender would like to take or control"*, which would mean that although not to the same degree, everyone on the Internet (and their data) are open to vulnerability. That definition, however, the conceptualization broad. As of a suitable target in RAT is itself a composite made up of a number of elements, captured in the acronym VIVA (value, inertia, visibility, and accessibility). " The challenge now lies in how these elements translate into cyberspace.

The value of the objective is pretty self-explanatory; the higher the value of the target, the greater the possibility of attack (Cohen and Felson, 1979). What might not be a valuable object by itself, can become key in cyberspace after obtaining certain information of it through other means. Take a 4 number string for example: useless on its own, but incredibly valuable after learning through *data mining* that it is associated with the "pin" concept.

The other three elements, however, hold more doubts regarding their applicability. One clear example of this is found in the element of inertia, described in the original version of theory as the physical properties of the item and the ease with which the object can be carried ". The truth is that in cyberspace the targets will generally offer little resistance, since they can be easily downloaded[6]. In that same line of thought, accessibility is defined as the offender' (Felson, et.al., 2001). Since distance is compressed in cyberspace, all objectives are, in that sense, accessible; that makes it a characteristic dependent in the offender rather than in the objective itself. As for visibility, Felson, et.al. (2010) stated that if something is not seen by the offender, it cannot become its target. That begs the question of which online activities make users suitable targets for cybercrimes. While the answer is varied depending on the type of cybercrime that is being researched (Yar, 2016), a common trait is found: more interaction (be it through

[6] Yar (2005) suggested that the inertia element could be understood as the volume of data and that large file sizes could indeed offer some resistance, but the evolution of ICTs and higher download speeds contradicts this idea (Miró-Llinares, 2011).

spending more time online or doing a wider range of activities) means that the user is most likely to become a suitable target (Miró-Llinares, 2011).

Taken that the VIVA acronym cannot be understood as it is, authors such as Miró-Llinares (2014) have chosen to use another one that is closer to the reality of cyberspace: IVI. The user or good must have been **Introduced** into cyberspace, it must have a **Value** to attract potential offenders, and the user must **Interact** online in order to make itself visible and contact may be stablished with the offender.

Last, but not least, there is the issue of the **absence of a capable guardianship**. As it has been stated, due to the nature of cyberspace, there are no central organisms that can control and oversee what is happening on a global scale, which means that there is a lack of protection for potential victims. While Law Enforcement Agencies can act on the Internet, its scope of action is quite limited.

That does not mean, however, that there cannot be guardians on the Internet. Guardianship on cyberspace can be understood in a technical, physical sense, through the use of antivirus or similar software (which would equal a security system in the real world) (Bossler & Holt, 2009), or rather, in a social sense, since having computer knowledge or interacting with acquaintances that do instead, leads to a lesser chance of becoming a victim[7].

What these guardians show though, is that they are heavily tied to the actions and initiative of the user; the victim must become its auto guardian.

[7] This is usually relevant in cybercrimes that involve malware; a user with knowledge of the dangers of the Internet is less likely to get itself infected, as it might not download a suspicious file, for example.

2.2. Cybercrime in the era of COVID-19

2.2.1. Contextualizing the COVID-19 crisis

The Severe acute respiratory syndrome coronavirus 2, also known as SARS-CoV-2, is the virus that causes coronavirus disease 2019, famously known as COVID-19[8], the respiratory illness responsible for the COVID-19 pandemic[9]. The first recorded cases of COVID-19 were identified in Wuhan, China, back in December of 2019 (hence the name). On April 8, 2020, with most countries having the strictest lockdown measures in place[10], there were already 1.353.361 confirmed cases and 79.235 deaths on a global scale (WHO, 2020). As of the writing of this (May, 2021), more than 3.300.000 people have died and there are nearly 163.000.000 confirmed cases[11].

The necessary lockdown measures forced everyone to use the Internet to cover several of our daily necessities, as stated previously in the introduction; data shows that internet traffic in Spain went up by 30% in only one month compared to 2019 (Telefónica, 2020). In relation to this, here are some numbers related to the education, work and entertainment sectors:

- Over 1.500 million students worldwide were left without classes according to UNESCO (Aretio, 2020), which represent 91% of the total academic population (as seen in **fig. 2**). In Spain's case, it is est million students were affected in the first months of the pandemic. Later on, online teaching became the norm and so did the use of apps like Zoom or Google Classroom as shown in **fig. 3**.
- Workers were in a similar situation as well, although not to the same degree. In the first months of the pandemic most businesses had to temporarily close. As such, a significant reduction in mobility to work centers was

[8] The media has interchangeably used the terms SARS-CoV-2 and coronavirus/COVID-19, even though they are not the same. While not necessarily a case of malicious conduct by the press, it goes to show that even in the most basic aspect of this crisis there has been a lot of misinformation, as it will be seen later.

[9] On the 30th of January of 2020 the World Health Organization declared the outbreak of COVID-19 to be a "Public Health Emergency of International Concern", also known as pandemic.

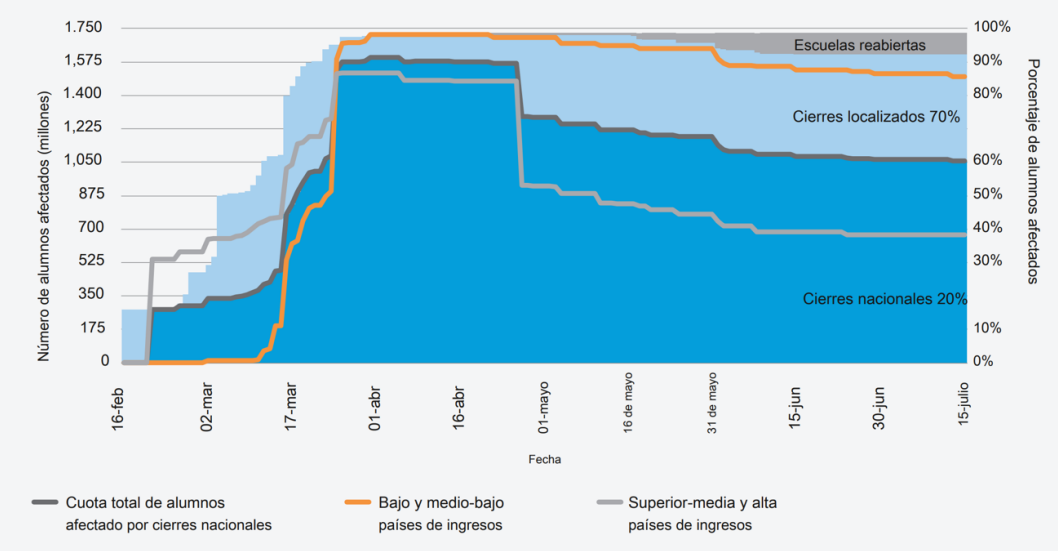
[10] For reference, the Spanish Government declared the State of Alarm on March 14, 2020.

[11] These numbers refer to the total of accumulated cases, not to the active ones.

achieved; 64% less in Spain, according to sources (Bracero, 2020). With time, more businesses chose the remote work solution, using the same apps shown in **fig. 3**, but in comparison, only a small percentage of workers ended up working from home (Lapuente, 2020). In Spa

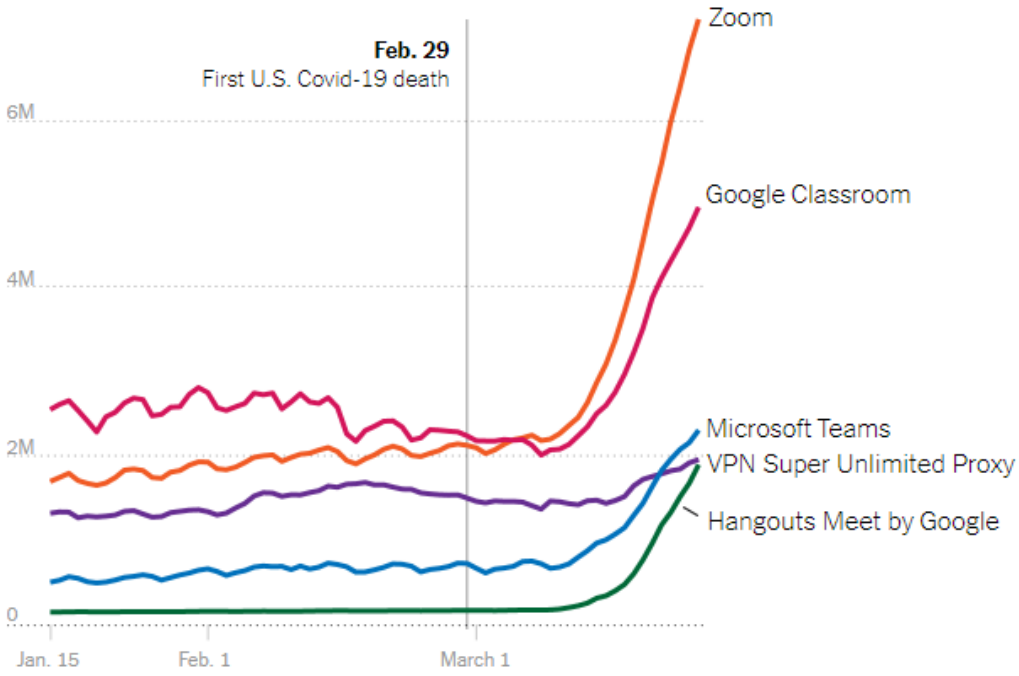
¶ Online entertainment became more relevant than ever during the pandemic. As **fig. 4** displays, streaming sites and services like Twitch.tv and Netflix saw their usage surge (so much so they had to place limitations due to bandwidth problems). Not only that, but new services were discovered and created, such as Disney+. Gaming also saw a hefty increase; the European Videogame Industry (ISFE) states that 27% of players have increased their playing time on an average of 1.5h per week (10.2h in total) (ISFE, 2020).

Fig. 2. Students affected by the COVID-19 pandemic.



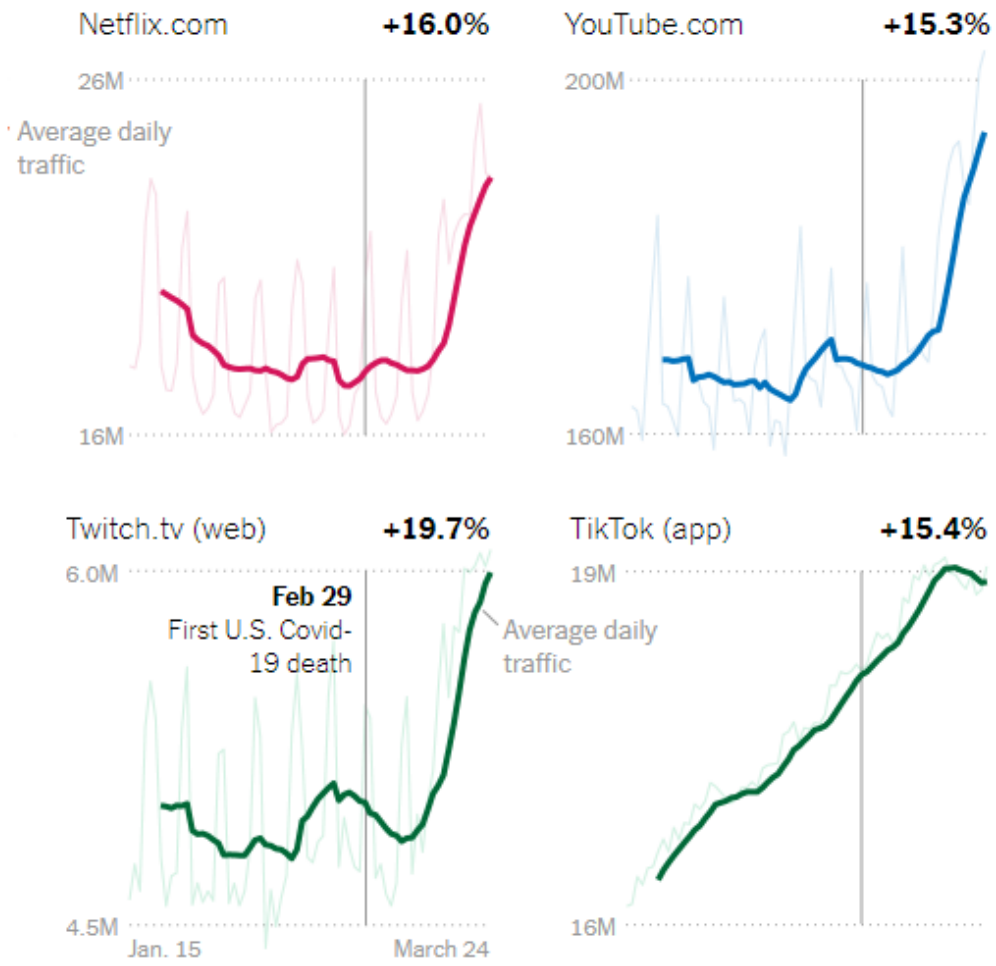
Source: Aretio (2020).

Fig. 3. Daily app sessions for popular remote work apps on March 2020.



Source: New York Times. (2020).

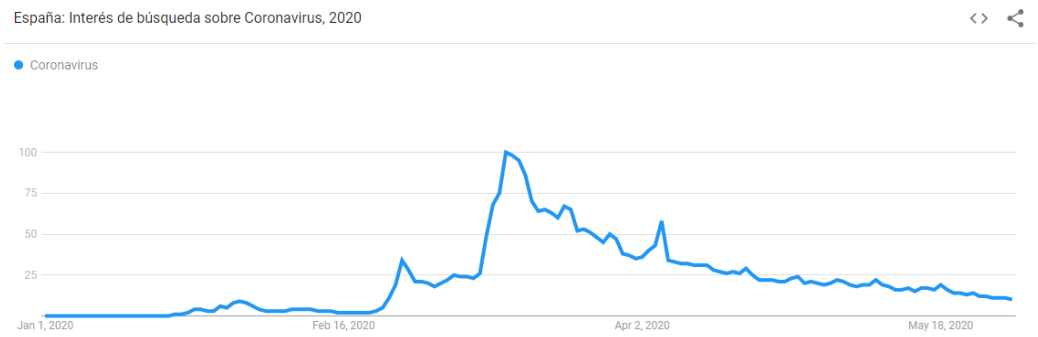
Fig. 4. Daily app sessions for popular streaming and entertainment websites on March 2019.



Source: New York Times. (2020)

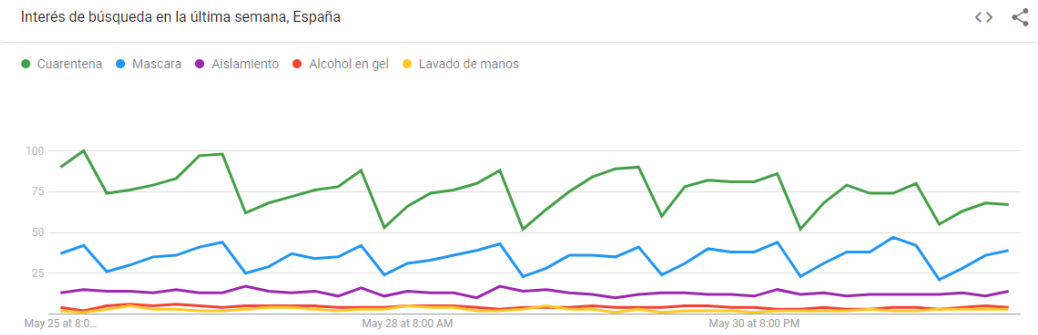
If there is one type of content that took the Internet by storm though, that was COVID-19 itself, with terms such as "coGoogle virus" search trends (displayed in **figs. 5 and 6**). Other data reports that from March 9 to April 26, 2020, 1.200.000 websites were detected to contain COVID-19 related keywords (Palo Alto, 2020).

Fig. 5. Daily Google search trends with the



Source: Google (2020).

Fig. 6. Daily Google search trends from coronavirus related terms.



Source: Google (2020).

This sudden surge of Internet usage, however, exposed old cybersecurity controversies and problems that were not yet solved (Fontanilla, 2020). On top of that, cybercriminals started following coronavirus concerns online in order to exploit them. And soon enough, this combination gave rise to the creation of COVID-19 themed cybercrime: at the peak of the outbreak, approximately one in three reported cybersecurity incidents were directly related to coronavirus[12] (Agència de Ciberseguretat de Catalunya, 2020).

[12] To add an international perspective, the FBI estimates that the number of cybercrimes has increased by 400% and that roughly 80% of them were coronavirus-related (Agència de Ciberseguretat de Catalunya, 2020).

2.2.2. COVID-19 themed cybercrime

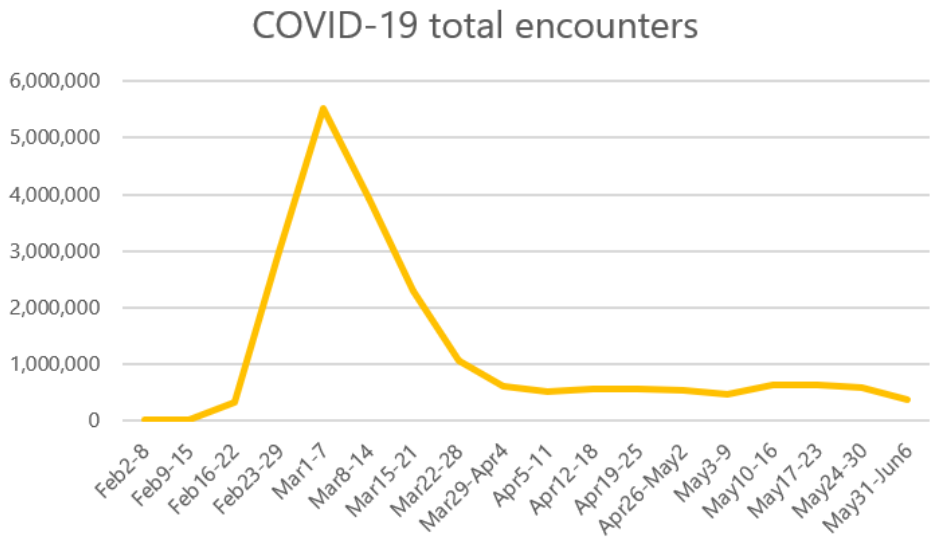
Phishing

Phishing is a fraudulent practice consisting of simulating a false identity (usually through the impersonation of a reputed source by the target) with the intent of stealing personal data from the victim. It preserves anonymity, it is easy to replicate[13], low cost and most importantly: it is effective.

With the World Health Organization (WHO) becoming the main organization in terms of delivering trusty information about COVID-19 and the state of the pandemic, it became a perfect identity for cybercriminals to impersonate (especially because it is an organization known and accepted all around the world).

To understand the magnitude of phishing attacks, it is enough to know that Google blocked 18 million phishing messages related to the coronavirus in a single day. A report from Microsoft (2020) seems to support that idea as well, as represented in **fig. 7**, having detected almost 6 million COVID-19 related phishing attacks around March.

Fig. 7. Trend of COVID-19 themed phishing attacks.

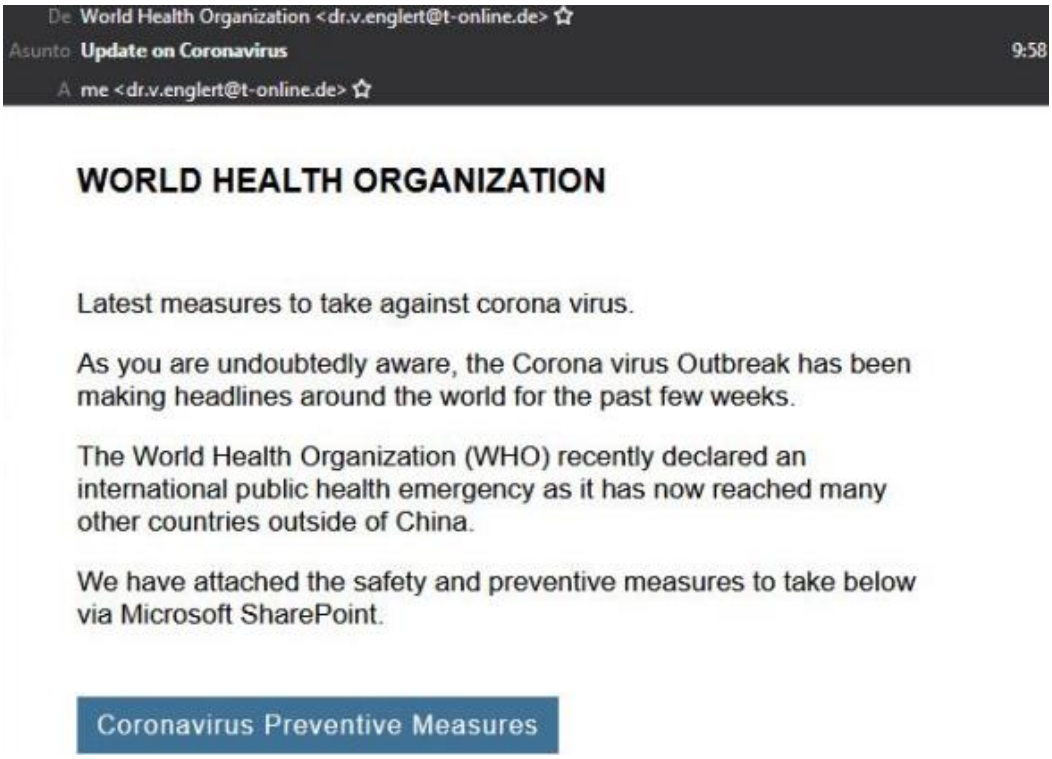


Source: Microsoft (2020).

[13] This is achieved through the use of botnets, which allows the offender to send the same e-mail to millions of people, trying to have the most answers as possible, hence increasing the effect.

While phishing is usually committed through emails (as displayed in **fig. 8**), cybercriminals have tried other approaches to exploit the pandemic context as much as possible, such as social engineering techniques, *vishing* and *smishing*, which all answer a need for higher customization in attacks as regular phishing emails started losing effectiveness.

Fig. 8. Example of a phishing email that impersonates the WHO.



Source: Grupo ICA (2020).

Vishing is phishing done through a phone call, while smishing exploits SMS and messages instead. Vishing has focused on emulating calls from local ambulatories and hospitals to obtain data under the pretext of making an appointment for PCR tests (EUROPOL, 2020).

Smishing users, on the other hand, have taken advantage of the fact that the majority of messages from official institutions have been notified via SMS. (INTERPOL, 2020). A good example of this can be found in Spain: Social Security sent messages to employees notifying the suspension of their contracts. In **fig. 9** another common use of smishing can be seen: a fake notification from a delivery service about the

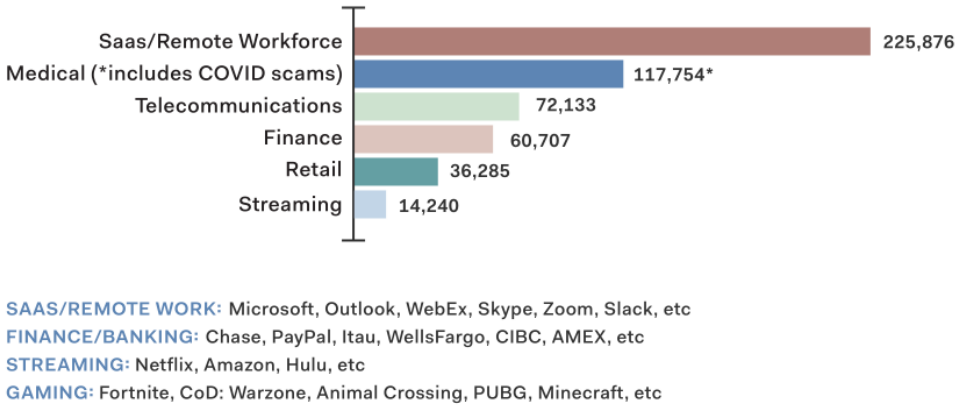
status of a shipment, relevant considering the amount of online purchases during lockdown.

Fig. 9. Example of smishing.

Source: Valero (2020).

All of the above is supported by phishing reports, as seen in **fig. 10**, with remote work and the medical industry being at the top (Bolster, 2020).

Fig. 10. Phishing by industry in Q1 2020.



Source: Bolster (2020).

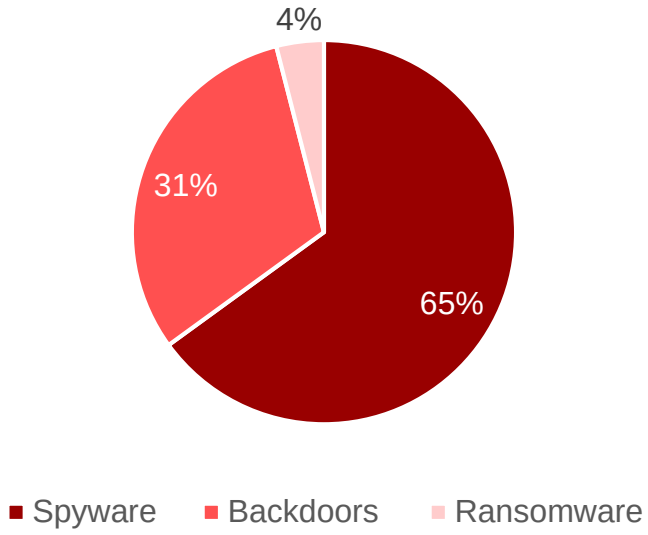
Another one of phishing's objectives is (*malware*).

Malware

Malware also had a really strong presence since the start of the outbreak. Some reports estimate a 475% overall increase (Agència de Ciberseguretat de Catalunya, 2020). Phishing, social engineering skills and fake apps related with COVID-19 topics were the main methods of malware distribution.

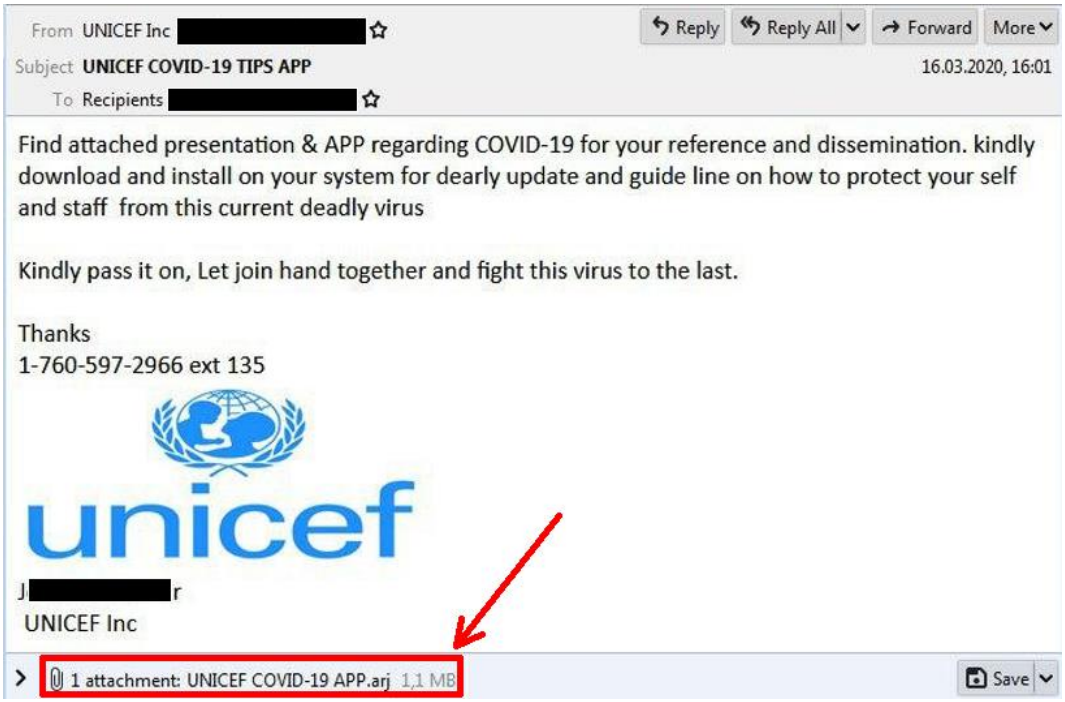
Regarding the distribution of malware through COVID-19 related phishing, 65% of them were *Spyware*, as seen in **fig. 11**, which steals personal data and credentials, something common taking into account the rise of online shopping and bank operations (an example of such is provided in **fig. 12**). In relation to this, it is estimated that during the first three months of 2020, bank Trojan detections grew by 280% compared to 2019 (CISOMAG, 2020). Spain was also the most targeted country, with 8.38% of detections, closely followed by Russia (Kaspersky, 2020).

Fig 11. Types of malware distributed in phishing attacks.



Source: Self-made from Agència de Ciberseguretat de Catalunya (2020).

Fig. 12. Example of a malicious e-mail disguised as "COVID-19 TIPS APP" with spyware in the attachment



Source: (CISOMAG, 2020).

Fake apps and software infected with malware started appearing as the pandemic advanced. Reports indicate that almost 12 million mobile devices were infected and 29.000 malicious apps were blocked (Upstream, 2020). A fair share of fake software posed as videoconference programs, with Zoom and Skype being the most affected. Kaspersky detected 120.000 of these apps only in the month of April 2020, when videoconferences were the main way to communicate due to lockdown measures (Kaspersky, 2020). The need for entertainment also exacerbated the known issue with malware-infected torrents when illegally downloading series, movies and games.

Old malware was also reused through *Malware-as-a-Service* (MaaS), i.e. selling malware in Dark Web *marketplaces* (EUROPOL, 2020).

Ransomware

Ransomware is a type of malware that threatens access to it unless a ransom is paid. Blocking the access to the files is done by

encryption. As it stands, ransomware is one of the, if not the, most dominant threat for cybersecurity, considering the scale of damage[14] that ransomware can inflict, as the IOCTA report states (EUROPOL, 2020). This is especially relevant in the context of the COVID-19 pandemic since cybercriminals have been targeting hospitals and other health organizations, administrations and supply chains, which has potentially cost lives and put many others at risks. Reports estimate that around 40 hospitals and third party providers have fallen victim to ransomware (Agència de Ciberseguretat de Catalunya, 2020). As businesses began to gradually re-open, cybercriminals started prioritizing those over hospitals again (with a big focus in tech companies).

While the pandemic context might suggest that individuals started getting more attention as suitable targets, reports say otherwise. Instead, they served as a gateway thanks to a poor remote work infrastructure (EUROPOL, 2020). The attacks also display higher skill, sophistication and adaptivity among threat actors. There is also the issue of the existence of *Ransomware-as-a-Service* in Dark Web marketplaces, which has decreased the entry barrier for those criminals that are less skilled, just as it happens with the rest of Malware-as-a-Service types.

Still, the number of effective attacks stayed relatively low: only 128 during the first half of the year (Erazo, 2020). This number might not be the real amount, since ransomware is heavily underreported, mainly due to the negative publicity and backlash that businesses would get from their clients and stakeholders. Nevertheless, such a low turnout is understandable taking into account the economic side effects of the pandemic.

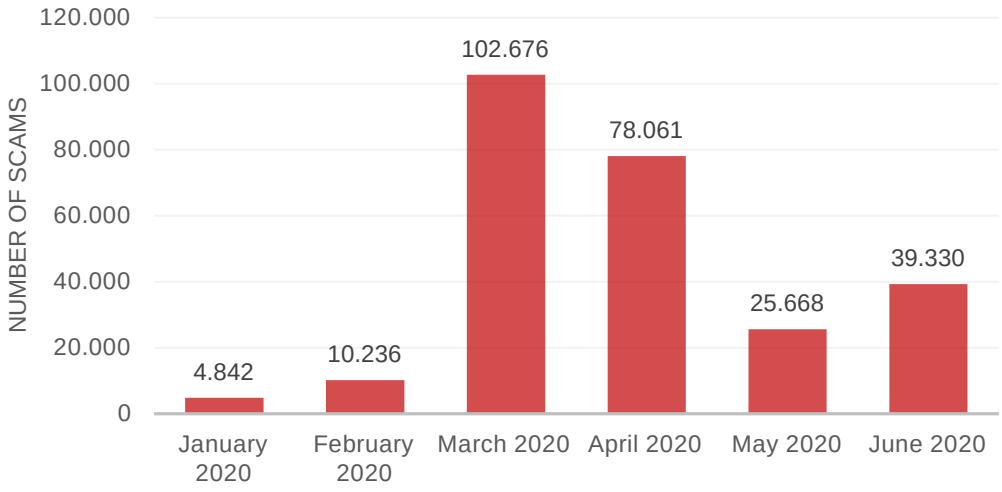
Cyber fraud and scams

The pandemic has generated a change in our necessities and consumption habits. This has been exploited by cybercriminals in order to scam both individuals and administrations. In order to quickly reach massive amounts of people so as not to lose the advantage of the surprise factor, cybercriminals resorted to phishing as the main method of initiating their scams (Agència de Ciberseguretat de Catalunya,

[14] e.g. WannaCry attack back in 2017.

2020). Most of the phishing emails had links to malicious websites and suspicious domains related with COVID-19 topics, which proliferated immediately. Out of the 1,2 million domains detected by Palo Alto that were referenced previously, 86.000 were detected to be malicious (Palo Alto, 2020). Other data such as the one displayed in **fig. 14** shows that approximately 180.000 websites between March and April were detected to hold scams related to COVID-19 as well.

Fig 14. Number of COVID-19 phishing and scams suspicious domain registrations per month.



Source: Self-made from Bolster (2020).

Fraud and scams' strategy transformed as necessities started to appear. For example, in the first stages of the outbreak there was a shortage of sanitary equipment (such as masks, gloves, disinfectants and test kits) and soon enough, the Internet became full of fraudulent offers of those items. These offers were published mostly on social networks (58%) and the rest on electronic commerce platforms (38%) (Agència de Ciberseguretat de Catalunya, 2020). Moreover, as displayed in **table 1**, over 70.000 suspicious domains with "mask" and "n95" (a type of respirator) as keywords were registered. Even governments fell victim to the mask scam due to their urgency: Germany purchased 10 million masks for the price of roughly 15 million euros; the masks, however, never arrived (INTERPOL, 2020). The shortage of materials also gave rise to activities in Dark Web marketplaces, as the IOCTA report states (EUROPOL, 2020).

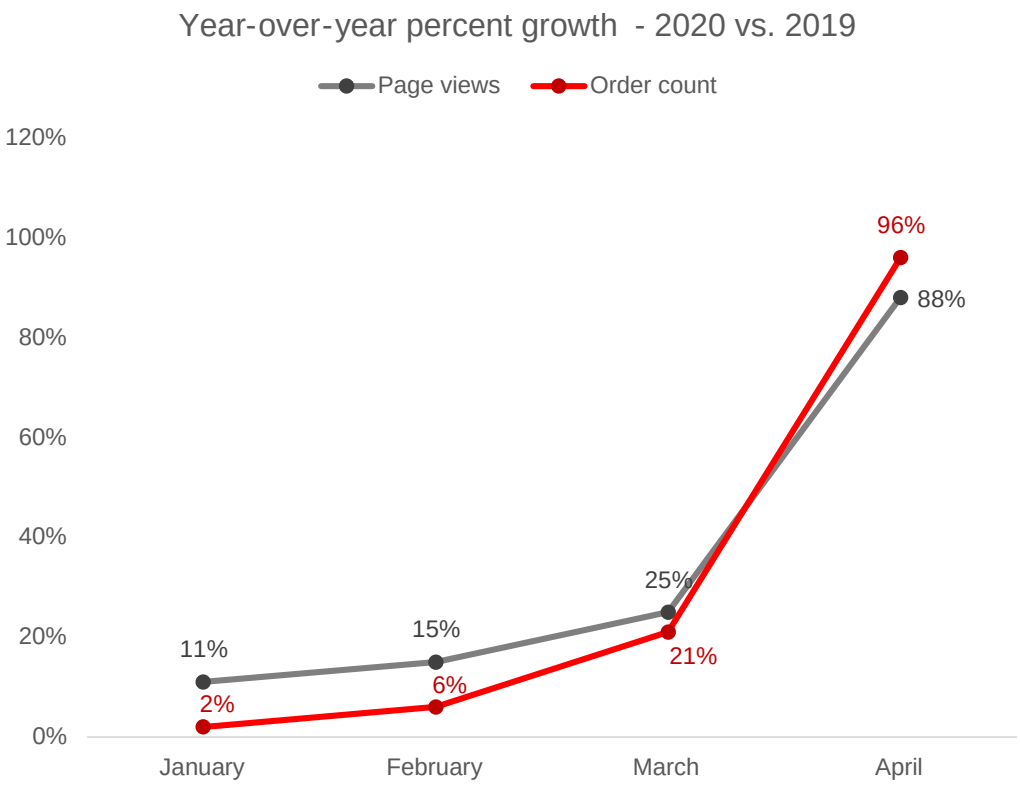
Table 1. Suspicious domain registrations per keyword.

Keyword	*March 2020*	*April 2020*	*May 2020*	*June 2020*
COVID	63.979	114.329	31.669	44.990
Corona	81.341	96.172	13.440	30.426
n95	67.891	3.121	904	976
Mask	7.203	44.659	19.751	23.627
Vaccine	6.816	2.230	887	955

Source: Self-made from Bolster (2020).

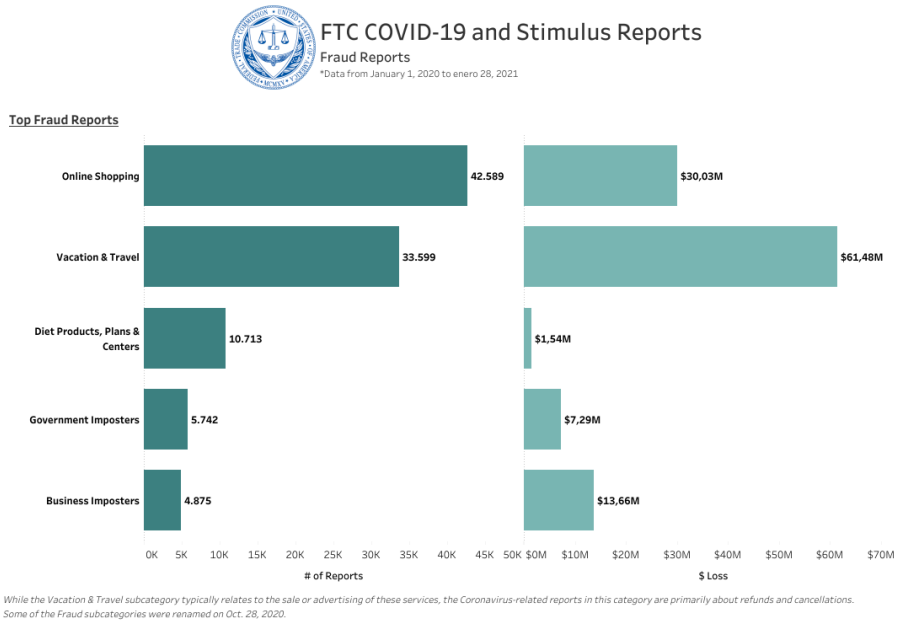
Aside from the medical equipment shortage, people started shopping online more often, mostly due to lockdown measures (with a 96% increase in orders by April in contrast to 2019, as **fig. 15** shows). Accordingly, top fraud reports saw online shopping at the top, with an approximate loss of 30 million dollars (as showcased in **fig. 16**).

Fig 15. Monthly growth of shopping activity around the world.



Source: Self-made from Agència de Ciberseguretat de Catalunya (2020).

Fig 16. Top fraud reports in the USA.



Source: Agència de Ciberseguretat de Catalunya (2020).

A combination of malware (mostly spyware) and malicious domains also had streaming services and digital banks as their focus. However, a scam that gained effectiveness later on during the pandemic was related to government aids (Agència de Ciberseguretat de Catalunya, 2020). In Spain, for example, as it can be seen in **fig. 17**, a SMS circulated offering aid between their personal data in the website listed in the message.

Fig 17. Pictures showcasing the SMS and website responsible for a popular scam in Spain.

Source: OSI (2020).

2.2.3. How do criminological theories fare against COVID-19 themed cybercrime?

As seen in the previous chapter, cybercriminals have adapted their ways to exploit the COVID-19 pandemic and some faint answers have been given on why certain things worked out for them. A deeper and proper explanation is needed, though, which is what is going to be discussed in this chapter.

How does RAT explain crime opportunities in the COVID-19 era? All three elements appear to interact with what it has been said so far:

- In regards to the **motivation of the offender**, COVID-19 cybercrime has proven to be cheap, with almost no risks for the actor (at least in phishing cases) and a big payout in terms of benefits. There is also the possibility of more people recurring to cybercrime due to their financial situation, which might have worsened due to most work contracts being either suspended or extinct (and thus end up unemployed).
- As far as the **suitable target** and **capable guardianship** goes, people's personal data and credentials surely meet the criter VIVA acronym. Such data can be more visible due to the increased time that people have been interacting in cyberspace because of lockdown measures. Moreover, it is estimated that the majority of people working remotely did not have the capacity to do so, i.e. working with their personal computer devices, without support from the IT department and no training offered (Agència de Ciberseguretat de Catalunya, 2020). That lack of security equals the absence of capable guardianship[15].

Naidoo (2020) reasons that one aspect that is frequently overlooked in cybercrime analysis are emotions; which feelings are cybercriminals appealing to the most? What makes a brand trustable to impersonate? These questions find their answer in three different theories: The Source Credibility Theory (Sussman, et.al., 2003), the Social Influence Model (Cialdini, 2001) and the Dual-Systems Model of Affect (Dillard and Peck, 2006).

The Source Credibility Theory sustains that the targeted credibility pre opinion of the organization or person being impersonated is more likely to lead to compliance.

There are, however, other influence methods that cybercriminals can use apart from impersonation to persuade their targets; the six persuasion principles of C social influence model of compliance (Cialdini, 2001). These are: authority, consistency, liking, scarcity, reciprocity and social proof (more details in **table 2**). According to Naidoo's research (2020), a

[15] Auto guardianship is not an option for the majority either.

relevant in the analysis of scams, with the top three being liking, social proof and scarcity, in that order. These seem to match characteristics of social media. During the first months of the outbreak, when uncertainty was at its peak, it was not unusual to see (and this is still true today up to some extend) videos of people impersonating frontline workers spreading misinformation about the pandemic.

Table 2. Evidence of influence techniques applied to COVID-19 crime.

Principle	Propositions	Example
Authority	People tend to comply with a request that comes from an authority figure.	The WHO serves as a respected authority on the pandemic for society.
Consistency	People, who make a commitment, tend to feel compelled to perform consistently in line with that commitment.	Completing short and easy survey commits one to disclose personal details.
Liking	People's tendency for liking another person or product affects their tendency to comply with that person's request.	Familiarity of popular banking brands. Front line healthcare worker.
Scarcity	People tend to value those opportunities that have limited availability (Cialdini 2009, p. 179).	Free groceries. COVID-19 relief funds by government agency. Credit relief by banks. Impersonating Investment company.
Reciprocity	People tend to comply to a requester who presents them with an initial favour or initial concession (Cialdini 2009, p. 38).	Fake Technology brand offers reward for completing COVID-19 survey.
Social Proof	People tend to view a particular behaviour as being more correct to the degree with which they see others in a similar situation performing the same behaviour (Cialdini 2009, p. 88).	Fake Social Media Profiles.

Source: Naidoo (2020).

And last but not least, there is the Dual-Systems Model of Affect, which emotional elements can be seen in **table 3**. As one might guess by the name, it evaluates how emotional appeals (both positive and negative) are used in cybercrime victimization. At first, due to the nature of the outbreak and general urgency of the situation one might think that cybercriminals are only using negative emotional appeals; Naidoo's research, however, says The results show that relief, fear and hope are the top three emotional principles. Misinformation campaigns played with fear while hope appeared in scams about test kits and fake coronavirus cures.

Table 3. Evidence of emotional elements employed in COVID-19 cybercrime messages.

Element	Propositions	Example
Fear/ Panic	People will tend to be persuaded by fear appeals when they feel vulnerable to an environmental threat.	Keeping informed about the local spread of the virus.
Threat/ Panic	People will tend to be persuaded by threat appeals when they feel vulnerable to an environmental threat.	Corona virus taking over the world.
Enjoyment	People will tend to be persuaded by positive appeals such as enjoyment.	Coping with lockdown and social distancing.
Relief	People will tend to be persuaded by positive appeals such as relief, when they feel they will gain a positive outcome such as gaining control over their lives.	Keeping informed about possible cure/treatment.
Hope	People will tend to be persuaded by positive appeals such as hope.	Global relief funds. National Relief Funds.
Compassion	People will tend to show compassion for others similar to them.	Empathic concern for patient.

Source: Naidoo (2020).

3. OBJECTIVES OF THE RESEARCH

The main objectives of this research are the following:

1. Build a state of the art explaining the cybercrime phenomenon and how criminological theories translate into this kind of crime through literature review.
2. Understand the COVID-19 crisis and how cybercriminals are exploiting the changes in criminal opportunity due to the pandemic by analyzing cybercrime reports and current news.
3. Discover if cybercrime victimization rates have increased in 2020 and obtain a victim profile.

4. METHODOLOGY AND HYPOTHESES

As it has just been stated, COVID-19 victimization is still a really new topic and therefore not many reports have been released yet. This also extends to official reports, so reliable data sources related to victim profiles and victimization rates are scarce. Still, taking into account the previous review of literature, the following hypotheses are raised:

H1. Cybervictimization rates during 2020 will be higher than in previous years.

H2. Changes in online activities extent are related to changes in cybervictimization rates.

In order to prove these hypothesis, the victimization rates that will be seen in the following chapter have been issued through the creation of an online victimization survey[16]. The survey features 38 questions and is heavily inspired by the empirical work done in a previous research (Hawdon, et.al., 2020). The survey has provided a total sample of 1442 respondents.

Aside from proving the hypotheses, the victimization survey results will also serve as a base to discover COVID-19 themed cybercrime victim profiles, which is one of the objectives of this research. Annual reports like the o Ministerio del Interior (2019) aim to provide additional data and comment on cybervictimization trends, which is the one that will be used later on to support the profile discussion comparison.

[16] Check Addendum 9.3. for the full survey disclosure.

5. RESULTS AND ANALYSIS

5.1. Results

In order to examine the first hypothesis, rates of cybervictimization must be investigated. In order to measure them, respondents were asked if they had fallen victim to seven different types of cybercrime during 2020 and in previous years, as shown in **table 4**. Types of victimizations tested included scams, identity theft, unknown transactions, notification from organizations about data theft, malware/viruses, online bullying and online sexual harassment[17].

Table 4. Self-reported online victimization and previous years.

Type of victimization	*During 2020*	*Previous years*	*χ2*
Lost money due to an email, website or other computer scam	56 (3,9%)	195 (13,5%)	$\chi2 = 84.314 \mid p < .001$
Had your identity used by someone else to start a bank account, credit card or loan	10 (0,7%)	8 (0,6%)	$\chi2 = 0.238 \mid p = .626$
Had unknown transactions in your bank/investment account, credit card, or other online payment system	93 (6,4%)	88 (6,1%)	$\chi2 = 0.147 \mid p = .701$
Received notification from a company or organization that your private information, such as name, social security, credit card or password, has been stolen or posted publicly	315 (21,8%)	205 (14,2%)	$\chi2 = 28.388 \mid p < .001$
Had a computer virus or malware	193 (13,4%)	630 (43,7%)	$\chi2 = 324.698 \mid p < .001$
Experienced hurtful comments, pictures or videos about you about posted online	125 (8,7%)	212 (14,7%)	$\chi2 = 25.432 \mid p < .001$
Experienced unwanted sexual comments or advances online	91 (6,3%)	111 (7,7%)	$\chi2 = 2.129 \mid p = .145$

In terms of pure count, it might seem like victimization was modestly higher in previous years rather than during 2020. Still, out of these changes, only four significant differences were found after using $\chi2$ tests: scams, notification from organizations about data theft, having a virus or malware and online bullying.

Out of these four, only data leak notifications were reported ($\chi2 = 28.388$, $p < .001$) during 2020, with 315 of the respondents (21.8%) answering affirmatively. In comparison, only 205 respondents (14.2%) were notified by a company about data loss in previous years.

[17] A summated variable of all victimization behaviors was created and tested as well, but it showed no statistical significance even at a 90% degree o the rates of specific types of victimizations are more valuable, hence its omission from the main text.

With that in mind, it is safe to say that the **first hypothesis is not supported**.

As for the second hypothesis, regarding differences in computer behaviors, it is better, for that matter, to divide it into two sub hypothesis (or two phases, if you will). The first sub hypothesis would be to examine if there are statistically relevant changes regarding the amount of time that respondents have engaged in certain online activities.

These activities include browsing social media, playing online games, reading news or other articles online, using a computer while working, shopping online and other activities. As seen in **table 5**, after performing paired t-tests between the two timeframes (2020 vs 2019), it can be stated that the extent in which the respondents have engaged in these activities is significantly higher[18] during 2020 in comparison with 2019. As such, **the first sub hypothesis is clearly supported**.

Table 5. T-tests of online activities engagement comparing 2020 and 2019.

In a typical weak how many hours do you spend	*In 2019*		*In 2020*		
	M	SD	M	SD	*t-test*
Browsing social media	4.53	2.80	5.41	2.81	-35.69 (1441) ***
Playing online games	4.96	2.87	5.72	2.99	-27.64 (1441) ***
Reading news or other articles online	1.99	2.12	2.46	2.22	-19.23 (1441) ***
Working with your computer	4.75	3.10	5.58	3.34	-32.06 (1441) ***
Shopping online	0.81	1.14	1.03	1.23	-11.593 (1441) ***
Other online activities	3.97	2.99	4.64	3.09	-27.68 (1441) ***

**p <.05, **p <.01, ***p <.001*

Now that it has been stablished that there are significant changes in the hours spent in the computer activities considered for this research, the second sub hypothesis arises: are these related to the changes in cybervictimization rates?

After crossing the online activities variables with each type of cybervictimization (since we are not interested in looking at victimization as a whole)[19], stats show that the only activities that showed any kind of significant relation were reading news or articles online, shopping online, and other online activities.

[18] All of them with a p-value of < .001.
[19] See ref. 17.

Spending more time reading news online showed to be significant in avoiding identity theft and data leak victimization (χ^2 21.49 | $p < .001$ and χ^2 31.14 | $p <$ .001 respectively), although not a strong relation overall (Cramér's V values inferior to 10% on both).

On the other hand, spending more time shopping online resulted in a significant relation in being strongly involved in identity theft and unknown transactions (χ^2 = 28.79 | $p < .001$ and χ^2 23.35 | $p < .001$ respectively and Cramér's V values superior to 30% on both).

As for the changes in the time spent on other online activities, it only had a relation with being infected with virus/malware (χ^2 16.86 | $p < .05$) with a moderate Cramér's V value of 19%.

Taking all of the above into account means that **this second sub hypothesis is not supported, so neither is the main hypothesis (H2)**.

As for other statistical testing, due to having both hypotheses not being supported, RAT variables were also tested with the previous years' victimization confirm that RAT is a valid model to analyze cybercrime (following the example of Hawdon, et.al., 2020). After performing a binomial regression test with the online activities mentioned previously plus computer self-protection behaviors, the overall model proved to be significant ($p < .001$).

On a final note regarding the demographic factors: the average age (22.63) was significantly relevant in both 2020 and pr a p-value of < .001. Gender and working status only achieved significance in 2020 total's victimization ($p < .001$ and $< .05$ respectively), while the level of studies on the other hand, only rates ($p < .001$).

5.2. Discussion and analysis

As most reports indicated an overall rise on cybervictimization behavior, both hypotheses were formulated around the idea that rates would increase during 2020. However, the results proved those assumptions to be wrong. ¿How is it possible

that these results differ so much from said reports? There are a few factors that might play a hand at that.

Let's start the analysis with malware. The low count is actually reasonable taking into account that 82.2% of the respondents used an antivirus software and 67.9% of them assured to keep it updated. There is also the fact that the WHO and other organizations have continuously warned about people exploiting the COVID-19 situation and as such have provided several recommendations on how to avoid victimization (EUROPOL, 2020). It is only natural to expect that when almost 41% of the 1442 respondents spend 7 or more hours a week on social media and almost 70% of them have dedicated 1 to 5 hours reading news or articles (both being an increment in comparison to 2019) they are informed about such dangers.

This is why scams (that, as it has been explained previously when discussing the theoretical framework, have flourished through phishing) also show such few cases. Of course, not being a victim does not mean that such as conducts did not exist or reach the participants; when asked if they had been sent a suspicious SMS, e-mail or link related with coronavirus, the majority answered affirmatively (63.25%), and as it was stated, effectivity was a constant challenge for COVID-19 cyber offenders.

Another example of self-protection measures effectively stopping victimization can be found in the high use among respondents of *2 Factor Authentication* (2FA) (80.9%), which explains why identity fraud and unknown transactions were not found to be of any significance. A point could be made that such protection measure is not under the user's choice anymore no heavily recommend it or outright enforce it, removing choice.

Talking about removing choice, and taking into account what has been discussed so far, it is not strange for data leaks to be the most reported type of cybervictimization during 2020, since as reports have stated (Agència de Ciberseguretat de Catalunya, 2020) and was discussed earlier on, people working from home had to resort to businesses rushed solutions (and in most cases the only option) for teleworking.

There is also the possibility of businesses being the main focus of offenders due to a high rate of effectivity, hence individual victimization rates being lower, but there is no way to know at the moment if such statement holds true for several reasons: no official data reports have been released as of yet, not having access to business that wanted to answer the survey, and the heavily underreported ratios of things like ransomware.

In that same line of thought, when respondents were asked if they had reported to the authorities any of the seven types of victimization in the case of having fallen victim to any of them, only 148 (10.3%) answered yes, so unrecorded cybercrime is not something exclusive to just businesses and could affect how these results are portrayed.

To close the discussion around the first hypothesis, there is one point to make regarding the last significant type of victimization: online bullying. While previous years' count is high (Miró-Llinares, et al. (2020), there's, accor is still value in observing how victimization spreads in time; there is the possibility that most of the online bullying was carried out during the months with strict lockdown measures[20] (with a reported increased time spent browsing social media) and the negativity that comes with it (Aretio, 2020 and Naidoo, 2020).

As for the second hypothesis, the results of the survey confirmed what several reports stated about the general increase in Internet use during 2020 (EUROPOL, 2020). Regarding the rebuttal of changes in cybercrime opportunities being related to the changes in Internet usage, it is to be expected taking into account that sans data leaks, every other significant change in victimization translated into fewer cases during 2020. This is based on the fact that RAT variables have, indeed, proved to be significant when associated with previ victimization rates.

There is not much to comment on the significant results obtained that has not been said already above. If anything, it would be the case of spending more time in other online activities being a risk factor in being infected by a virus/malware. It could be a result of the rampant malware infestation of most videoconference apps,

[20] This could be applied to the rest of the cybervictimization types.

downloading files from untrusted sites and Dark Web usage (Agència de Ciberseguretat de Catalunya, 2020 and EUROPOL, 2020).

Finally, in order to end up the discussion section, the demographics of the survey come into play to create a 2020 cybercrime victim profile. Taking into account the massive disproportion of gender participation in the survey (1255 male - 138 female)[21], two different profiles will be analyzed (as showcased in **table 6**):

Table 6. Victim profiling based on gender.

Gender	*Avg. Age*	*Level of studies*	*Working status*	*Main type of victimization*
Male	22.35	University studies (431 – 34.34%)	Student (775 – 61.75%)	Data leak (274 - 21.83%)
Female	24.83	University studies (56 – 40.58%)	Student (65 – 47.10%)	Online sexual harassment (34 - 24.64%)

2019's records show something totally different. Computer scams dominate cybervictimization rates for both males and females (86.73% and 84.91% respectively). As for data leaks, the most common type of victimization among our respondents, it appears that they were not really a major problem in 2019, representing only 0.68% of total victimization. These extremely low proportions can be explained with the conclusions that have already been stated from studying the ransomware phenomenon and evolution.

Regarding the average age, the 2019 report does not provide that, but gives information about age intervals instead. The most victimized group seemed to be those males and females between 26 and 40 years old, a substantial difference with our survey.

If we look at male-specific victimization, it can be seen than in comparison to our data, back in 2019 the ones that were the most affected by data leaks were men ranging from 51 to 65 years old with a total of 234 cases. Only 30 cases were reported in the 18 to 25 years old interval.

And last but not least, if the same analysis is done for female-specific victimization, it can be seen that female minors were the ones most victimized by online sexual

[21] The survey included non-binary gender options. Due to the lack of enough valuable data on Ministerio del cybercrime report (2019) to compare them to, said analysis will be omitted.

harassment with a total of 696 cases. 48 cases were reported in the 18 to 25 years old interval, which is pretty close to the numbers our survey has shown, although they are not close to being the same proportion (they only represent a 5.79% of the 2019 cases).

6. CONCLUSIONS

In attendance to the objectives of this research, a state of the art was built approaching the cybercrime phenomenon from the perspective of cyberspace and how the Routine Activities Theory is the one best suited to explain it. Then it was made clear that the COVID-19 pandemic is being heavily exploited by cybercriminals in several ways through the observation of Law Enforcement Agencies reports. Regarding the last objective, the victimization survey served its purpose on providing data to draft what the most common victim profile is and to give us some insight on how cybervictimization is measured and how circumstances created by the pandemic affect it. Only official data yet to be released will accurately show if cybercrime victimization has increased during 2020.

As the world population gets vaccinated and we return one step at a time to our normal lives, we will still have to live with coronavirus present in some way or another. It would be a mistake to assume that COVID-19 themed cybercrime is isolated in 2020 and will not continue to appear during 2021 and the years to come.

Still, the criminological scene must take up the challenge to advance deeper in cybercrime investigation and analysis, not only because it can potentially help Law Enforcement Agencies, but rather because we can still learn many lessons from it.

Yours truly has taken up the challenge and has come up with this research that tries to build upon the cybercrime phenomenon and go a little beyond of what other reports usually focus. COVID-19 is still a new topic and this is not the first research done on it, but let it be a foundation of what we can expect from the following months.

7. LIMITATIONS

There are a few limitations in the methodology area that could be fixed in later revisions of this research. For instance, since COVID-19 themed cybercrime is still a new topic, there are not many resources to study aside from LEAs reports. This also affects official data records, which have still not been released and would give us the correct hindsight on what the ideal victim profiles are.

Regarding the online victimization survey, while it had a fairly large sample, it was heavily biased both in gender and age, with 20-25-year-old males comprising most of the answers, so a more balanced sample would be ideal in a future revision. There is also the fact that yours truly does not have the means to gather data from businesses and compare it to individuals, which was one of the first ideas upon designing the research. On that same line of thought, getting the profile of a cybercriminal it is almost impossible by the reasons previously stated, so that was discarded early on as well.

Originally semi-structured interviews with experts in the field were going to be included, but time constraints due to personal problems made them ultimately impossible to be included.

8. BIBLIOGRAPHY

Agència de Ciberseguretat de Catalunya. (2020). *Informe de tendències de ciberseguretat.*

Aretio, L. G. (2020). COVID-19 y educación a distancia digital: preconfinamiento, confinamiento y posconfinamiento. *RIED. Revista Iberoamericana de Educación a Distancia*, *24*(1), 09-32.

Bolster. (2020). *State of Phishing & Online Fraud – Q1 2020 Report*. Retrieved from: bolster.ai

Bolster. (2020). *State of Phishing & Online Fraud – Q2 and Q3 2020 Report*. Retrieved from: bolster.ai

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, *3*(1).

Bracero, F. (2020). España e Italia son los que más respetan la reclusión. In *La Vanguardia.* Retrieved from: https://bit.ly/3chYWo7

Brenner, S. W., & Clarke, L. L. (2004). Distributed security: Preventing cybercrime. *J. Marshall J. Computer & Info. L.*, *23*, 659.

Bruno, D. (2020). COVID-19 and cybercrime: How rogue nations and cyber criminals are exploiting a global crisis. *Northern Policy Institute: Briefing Note*, (17), 13.

Cialdini, R. B. (2001). *Influence: Science and practice* (Vol. 4). Boston, MA: Pearson education.

Casabona, R. (2006). De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal. *El cibercrimen Nuevos retos jurídico-penales, nuevas respuestas político-criminales. Granada: Comares*.

CISOMAG. (2020). *65% of COVID-19 Phishing Campaigns Spread Spyware: Research.* Retrieved from: https://bit.ly/3pAxjuj

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, 588-608.

Dillard, J., & Peck, E. (2006). Persuasion and the structure of affect. *Human Communication Research, 27*(1), 38 -68.

Erazo, F. (2020). Successful Ransomware Attacks Decline in 2020. In *Cointelegraph*. Retrieved from: https://bit.ly/3pvsp1v

EUROPOL. (2020). *Catching the virus cybercrime, disinformation and the COVID-19 pandemic.*

EUROPOL. (2020). *Internet Organised Crime Threat Assessment Report.*

Felson, M., & Boba, R. L. (2010). *Crime and everyday life*. Sage.

Fontanilla, M. V. (2020). Cybercrime pandemic. *Eubios Journal of Asian and International Bioethics*, 30(4), 161.

Google. (2020). *Coronavirus en España.* Retrieved from: https://bit.ly/2NSp7rf

Grupo ICA. (2020). *"Aprovechando el Pánico del Coronavirus". Informe de Ciberseguridad COVID 19.* Retrieved from: https://bit.ly/39zfZQu

Hawdon, J., et.al. (2020). Cybercrime in America amid COVID-19: the Initial Results from a Natural Experiment. *American Journal of Criminal Justice*, 1-17.

INTERPOL. (2020). *COVID-19 Cybercrime Analysis Report – August 2020.*

INTERPOL. (2020). *Unmasked: International COVID-19 fraud exposed*. Retrieved from: https://bit.ly/30KLQbR

ISFE. (2020). *The impact of Covid-19 on video game play behaviors and attitudes*. Retrieved from: https://bit.ly/3t62Mq2

Jewkes, Y. (2006). *Crime online*. Routledge.

Kaspersky. (2020). *ThreatList: Skype-Themed Apps Hide a Raft of Malware*. Retrieved from: https://bit.ly/3csSI4L

Kent, G. (2015). The mutual legal assistance problem explained. *Blog Post at the Center for Internet and Society website, Stanford Law School*, *23*.

Lapuente, B. (2020). La incidencia del teletrabajo en España pasa del 5% al 34% durante la pandemia. In *El País*. Retrieved from: https://bit.ly/3pAurxx

López Ortega, J. J. (2001). Libertad de expresión y responsabilidad por los contenidos en Internet. *Cuadernos de derecho judicial*, (10), 83-126.

Microsoft. (2020). *Exploiting a crisis: How cybercriminals behaved during the outbreak*. Retrieved from: https://bit.ly/3aiYm6W

Ministerio del Interior. (2020). *Estudio sobre la cibercriminalidad en España.*

Miró-Llinares, F. (2011). La oportunidad criminal en el ciberespacio. *Revista Electrónica de Ciencia Penal y Criminología*, *7*, 1-07.

Miró-Llinares, F. (2012). El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. *Madrid, Marcial Pons*.

Miró-Llinares, F. (2014). Routine activity theory. *The encyclopedia of theoretical criminology*, 1-7.

Miró-Llinares, F., et.al. (2020). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies*, 1-13.

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*, 1-16.

New York Times. (2020). *The Virus Changed the Way We Internet.* Retrieved from: https://nyti.ms/3ta9BHk

OSI. (2020). *Identificados SMS fraudulentos con enlace a una web para solicitar una supuesta ayuda económica de entre 350 y 700 euros*. Retrieved from: https://bit.ly/3ajP1LV

Palo Alto. (2020). *COVID-19: Cloud Threat Landscape*. Retrieved from: https://bit.ly/3r3dwni

Sussman, S. W., et.al. (2003). Informational influence in organizations: An integrated approach to knowledge adoption. *Information Systems Research*, 14(1), 47 -65.

Telefónica. (2020). *Telefónica registra durante la crisis del Covid-19 un crecimiento en su tráfico de internet equivalente al de todo el año pasado*. Retrieved from: https://bit.ly/3iUYVaT

Upstream. (2020). *Upstream's Secure-D detects malware spike in Q1 2020 with 29,000 malicious Android apps at play, double 2019 figures*. Retrieved from: https://bit.ly/39x2UHB

Valero, C. (2020). *Tu envío está en camino, así te timan con un SMS de Correos.* Retrieved from: https://bit.ly/3oBc7Ti

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age* (Vol. 4). Polity.

Wertheim, S. (2020). Surviving a Pandemic in an Era of Cybercrime. *The CPA Journal*, 90(5), 64-66.

World Health Organization. (2020). *Coronavirus disease 2019 (COVID-19) Situation Report – 79.* Retrieved from: https://bit.ly/2L4b14U

World Health Organization. (2021). *Weekly epidemiological update on COVID-19 - 13 April 2021*. Retrieved from: https://bit.ly/3drlC5d

Yar, M. (2005). The Novelty of 'Cybercrim Activity Theory. *European Journal of Criminology*, *2*(4), 407-427.

Yar, M., et.al. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263-280.

9. ADDENDUMS

9.1. Terminological glossary

Term	***Definition***
2 Factor Authentication (2FA)	Two-factor authentication (2FA) is a security system that requires two distinct forms of identification in order to access something. For example, to login on Amazon, you need your password and a unique code sent to you via SMS.
Backdoors	A backdoor is a type of malware used to provide the attacker unauthorized remote access to the compromised PC by exploiting system vulnerabilities.
Data mining	Process used to extract usable data from a larger set of any raw data. This is usually done through the use of specialized kind of software that can analyze data patterns in large batches.
DDoS	DDoS stands for Distributed Denial-of-Service attack. It is a type of cyber-attack that involves sending massive amounts of requests to the targeted server, effectively flooding and overloading its systems. The attack can be sent from multiple sources, so it becomes impossible for the targeted site to properly cut off all connections.
Exploit	Security vulnerability in a system. It allows the injection of payloads.

Honeypots	A trap tool that when deployed on a network or computer is set to detect attempts at unauthorized use of information systems to later track the attacker.
ICT	Acronym that stands for Information and communications technology.
IP Address	Internet Protocol Addresses are a string of numbers that identify a device connecting to a network via any of the Internet Protocols. Internet Protocols could be defined as the channel that allows data to device to another server.
Malware:	Term used to describe any malicious program or piece of code that infects a system with the intent of harming it. It is a broad concept which includes several forms of appearances.
Malware-as-a-Service	Selling malware in Dark Web marketplaces.
Marketplace:	Any kind of trading website or forum that is hosted in the Dark Web, hence needing tools like the TOR Browser to get access to it.
Net Neutrality:	Set of rules that forces Internet Service Providers and state legislation to treat Internet traffic as equal, regardless of its content or the means of access. This means that the users cannot be charged more or less depending of the content they are accessing.

Payload	Data set to run a custom set piece of code when certain conditions apply. In the context of this work, this is the code run when a user finds an exploit.
Phishing	Act of gaining personal data or implementing malware through the impersonation of a reputed source by the target.
Ransomware	*Ransomware* is a type of malware that threatens to pub block access to it unless a ransom is paid. Blocking the access to the files is done by encryption.
Ransomware-as-a-Service	Selling ransomware in Dark Web marketplaces.
Smishing	Act of gaining personal data or implementing malware through the impersonation of a reputed source by the target via SMS.
Spyware	Type of malware designed to steal personal data and credentials.
Virtual Private Networks	Type of networks that extend a private network using public connections, which means that while the Internet connection is the same, that private network's IP mig another country, thus circumventing issues like content censuring.
Vishing	Act of gaining personal data or implementing malware through the impersonation of a reputed source by the target via voice call.

9.2. Extra information regarding COVID-19 themed cybercrime

9.2.1. Other types of cybercrime

There is the issue of what the WHO has misinformation (Fontanilla, 2020). The organization warned that misinformation about the pandemic presented a serious risk that might prove to be as dangerous as coronavirus itself. According to an INTERPOL report (2020, p. 13), the most common COVID-19 related topics that brought misinformation were the following:

- *"Public authority action;*
- *Community spread;*
- *General medical news;*
- *Prominent actors;*
- *Conspiracy theories;*
- *Virus transmission;*
- *Public preparedness;*
- *Vaccine development;"*

The sheer amount of fake news and misinformation about these topics in social media has facilitated the effectiveness o analyzed in this chapter. Cybercriminals are not the only ones who are spreading misinformation though; politicians have seen an opportunity in the pandemic as well. Bruno (2020) states that in some cases it can be the State itself the one who spreads fake news, as he calls it "Spycraft", as he calls i polemic measures that mess with the citiz nations, in pure espionage fashion.

Talking about espionage, its cyber variant has also seen an increase, especially between tech companies. Some reports even point out to the possibility that states have recurred to cyberespionage to get an advantage in the vaccine race (INTERPOL, 2020; Agència de Ciberseguretat de Catalunya, 2020).

Zoom alone has also presented a few cybersecurity issues by itself. Aside from the amount of malicious apps that tried to impersonate it, the true app had

vulnerabilities that cybercriminals exploited in several ways, such as accessing private calls and implanting *cryptomalware* (Kaspersky, 2020).

Finally, according to the IOCTA report (EUROPOL, 2020) the amount of online child sexual abuse material has continued increasing, fueled by lockdown measures and people spending more time on the Internet (hence some of them in the Dark Web). Crime in the Dark Web is already difficult to investigate on its own due to how it is set up, and with most Law Enforcement Agencies cracking down on COVID-19 related threats, less attention and resources were spent on investigating this type of content[22].

[22] This does not imply, however, that no advances were made, as the IOCTA report states. Several EUROPOL operations regarding child sexual exploitation during this year can be checked at EUROPOL's https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation

9.3. Full survey results

Both questions and answers are shown in Spanish due to the survey being presented in that language. Reader's discretion is advised.

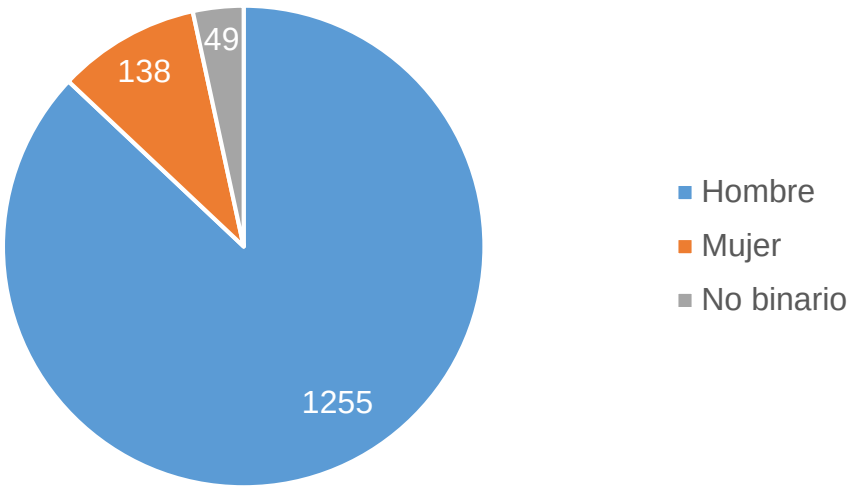
PREGUNTAS DE CONTROL

1. Edad

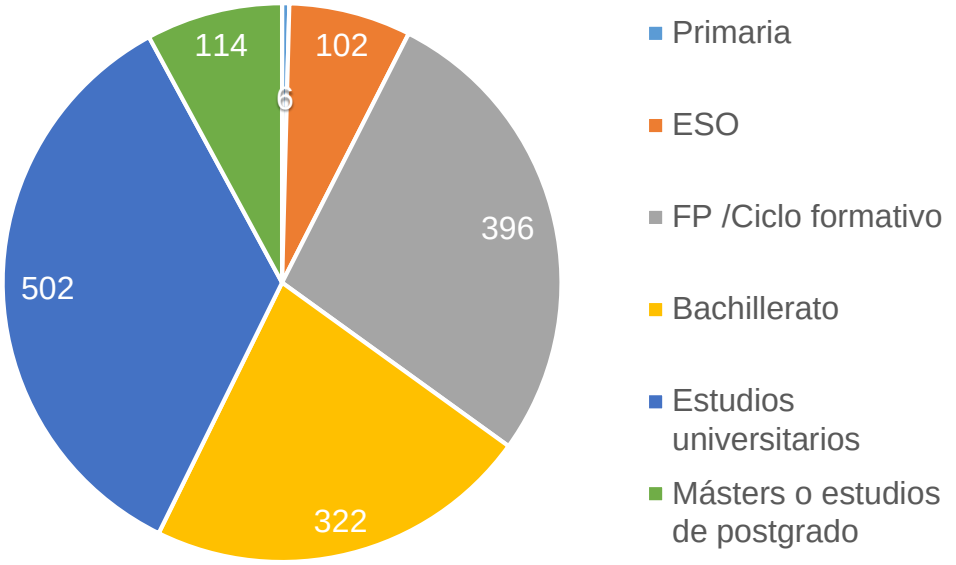
Frequencies (agegrup)

	Value	# of Cases	%	Cumulative %
1	18-23	846	58.70	58.70
2	24-29	399	27.70	86.30
3	30-39	75	5.20	91.50
4	Más de 40	11	0.80	92.30
5	Menores de edad	111	7.70	100.00

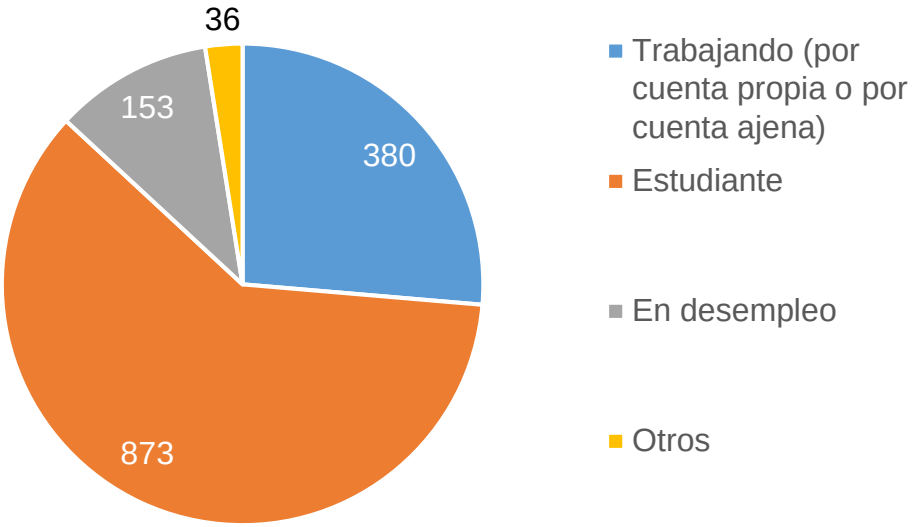
2. Género



3. Estudios

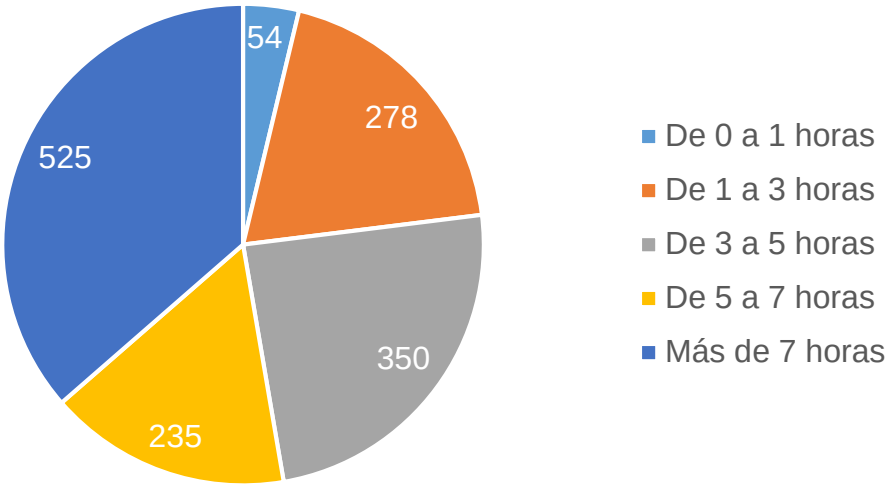


4. Situación laboral

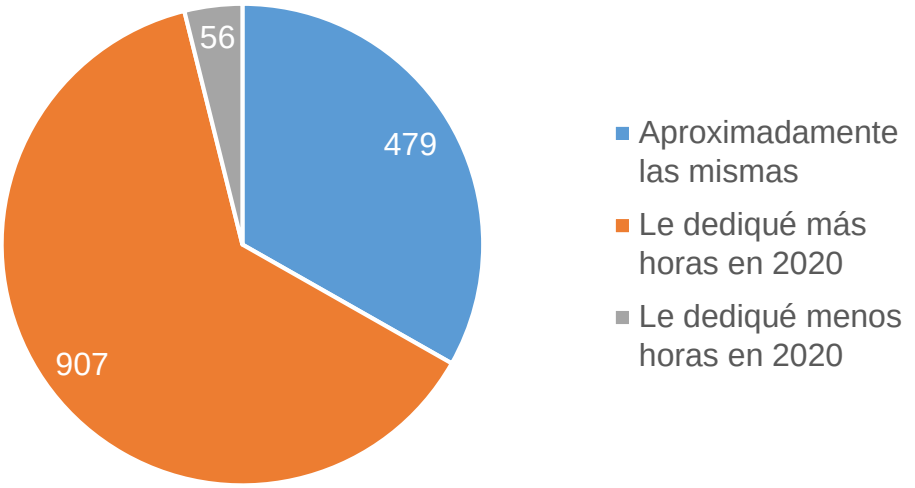


HÁBITOS DE VIDA

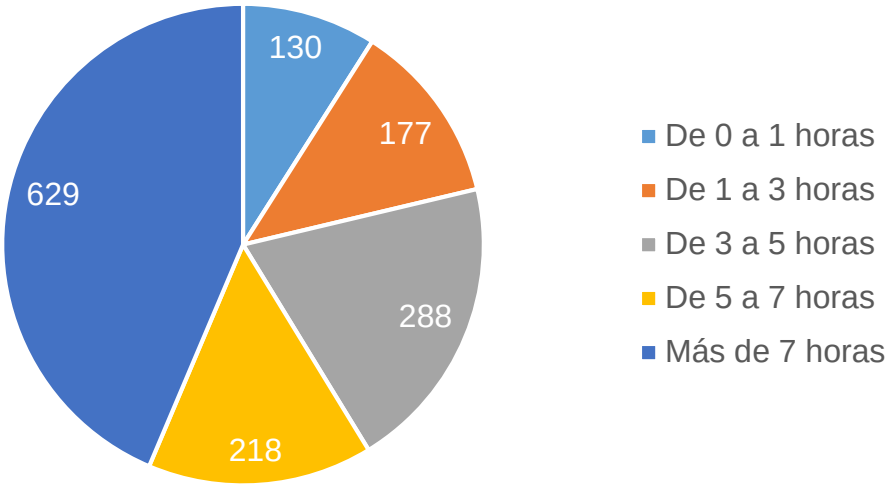
5. ¿Cuántas horas a la semana le dedicabas habitualmente a las redes sociales durante 2020?



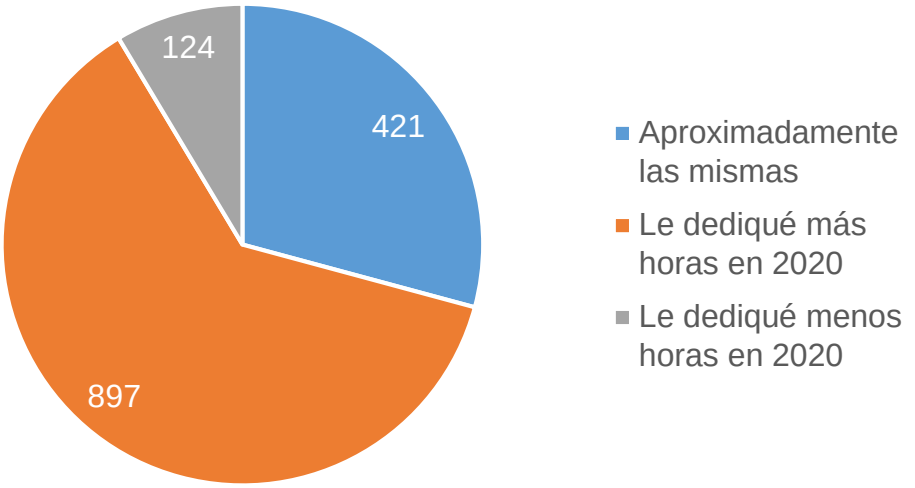
6. En comparación con 2019 ¿crees que en 2020 invertiste más tiempo a dicha actividad?



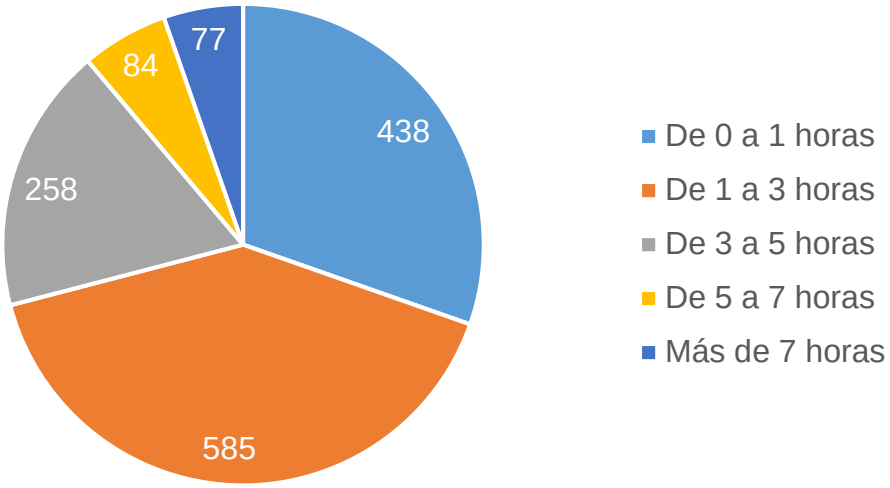
7. ¿Cuántas horas a la semana le dedicabas habitualmente a jugar online durante 2020?



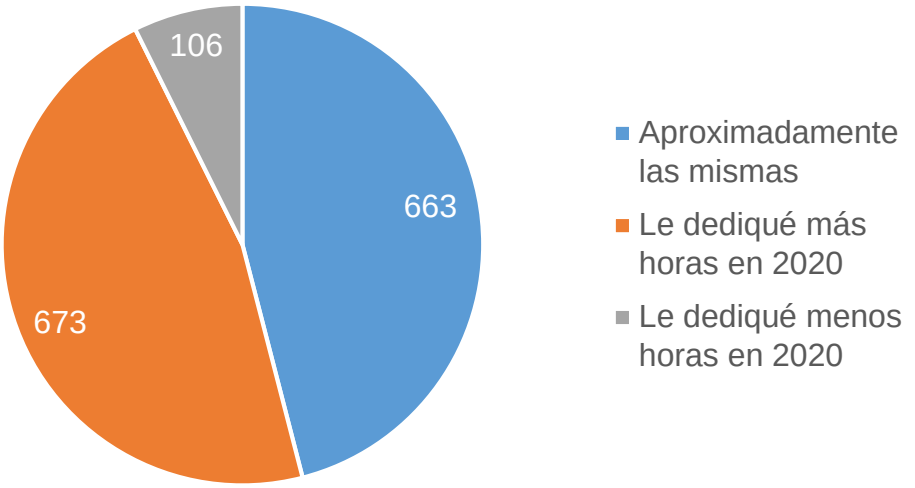
8. En comparación con 2019 ¿crees que en 2020 invertiste más tiempo a dicha actividad?



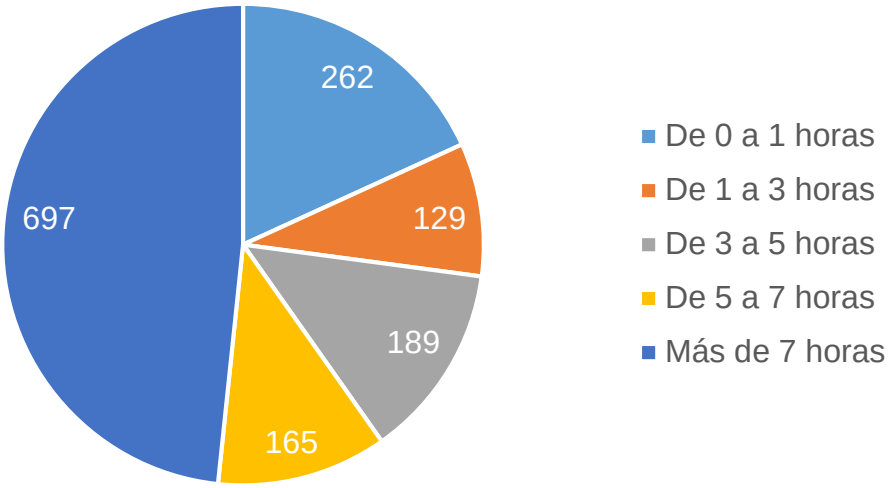
9. ¿Cuántas horas a la semana le dedicabas habitualmente a leer artículos o noticias online durante 2020?



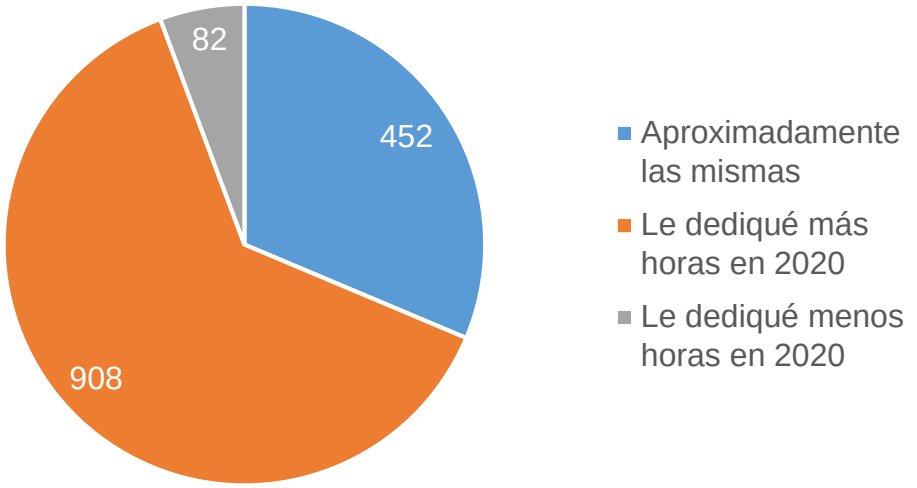
10. En comparación con 2019 ¿crees que en 2020 invertiste más tiempo a dicha actividad?



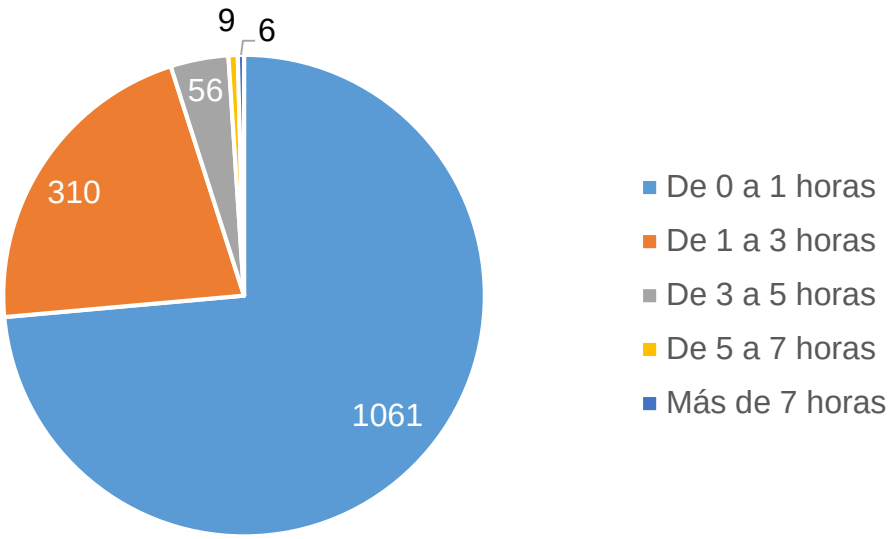
11. ¿Cuántas horas a la semana le dedicabas habitualmente a trabajar con el ordenador/teletrabajo durante 2020?



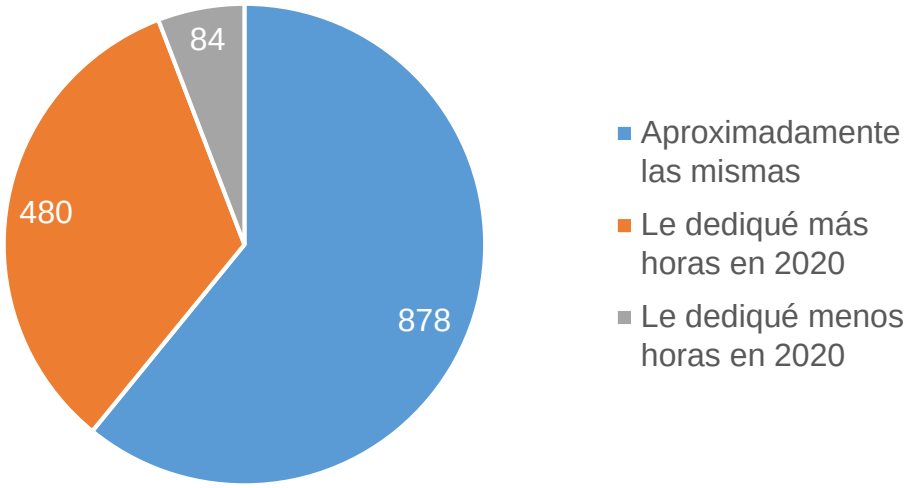
12. En comparación con 2019 ¿crees que en 2020 invertiste más tiempo a dicha actividad?



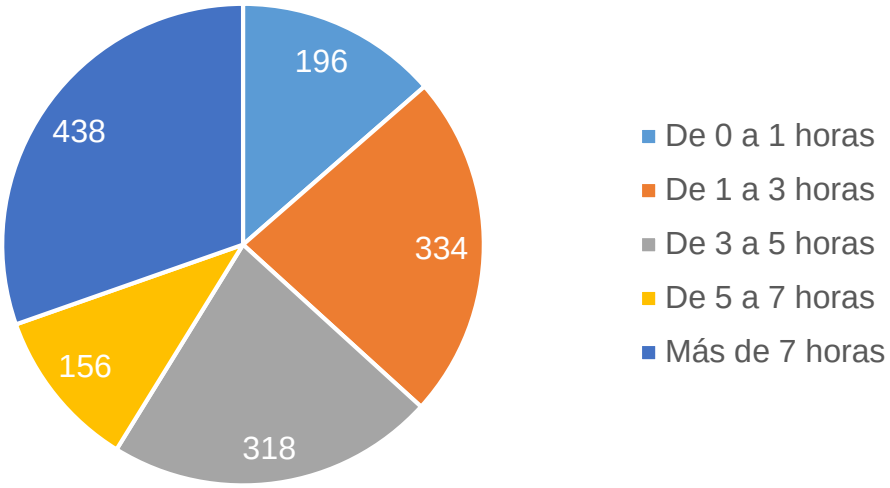
13. ¿Cuántas horas a la semana le dedicabas habitualmente a comprar online durante 2020?



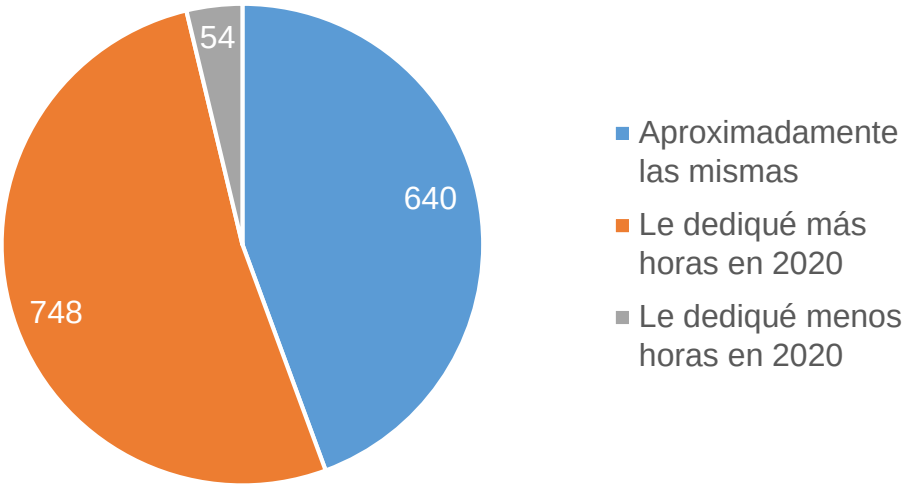
14. En comparación con 2019 ¿crees que en 2020 invertiste más tiempo a dicha actividad?



15. ¿Cuántas horas a la semana le dedicabas habitualmente a otras actividades online durante 2020?

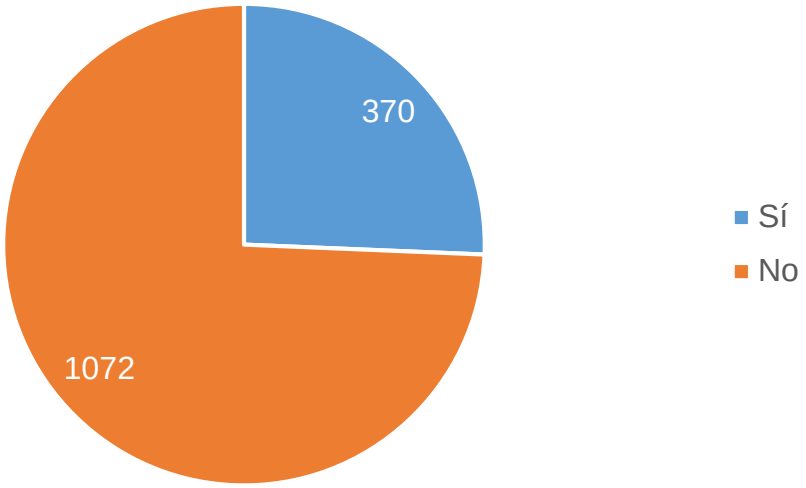


16. En comparación con 2019 ¿crees que en 2020 invertiste más tiempo a dicha actividad?

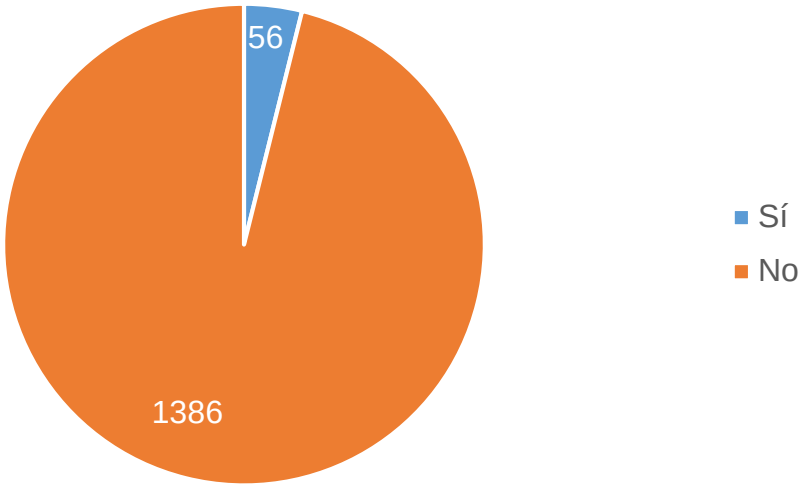


VICTIMIZACIÓN

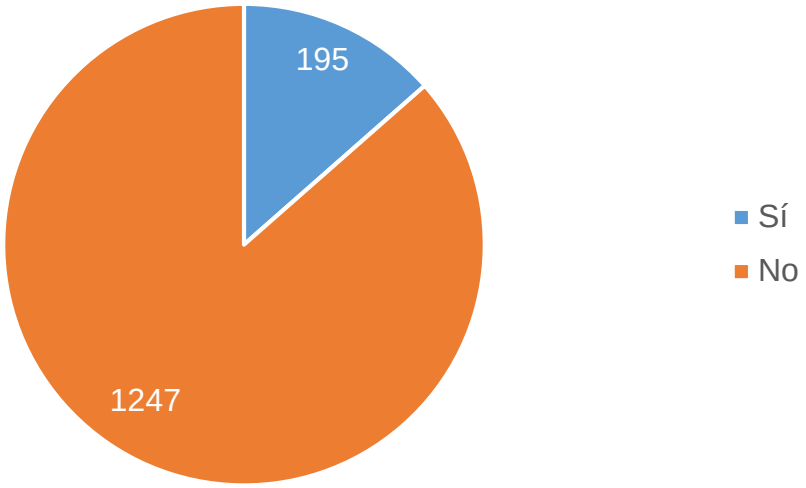
17. ¿Consideras haber sido alguna vez víctima de algún delito a través de Internet?



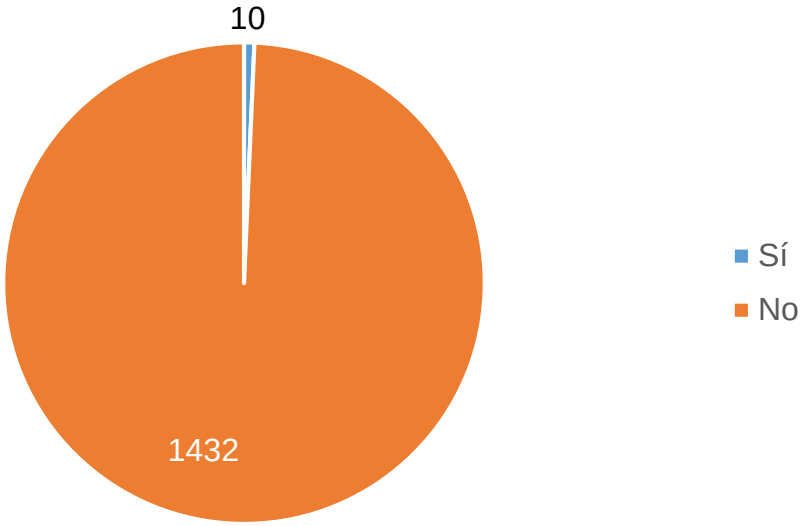
18. ¿Perdiste dinero debido a algún email, página web, SMS u otro tipo de estafa informática durante 2020?



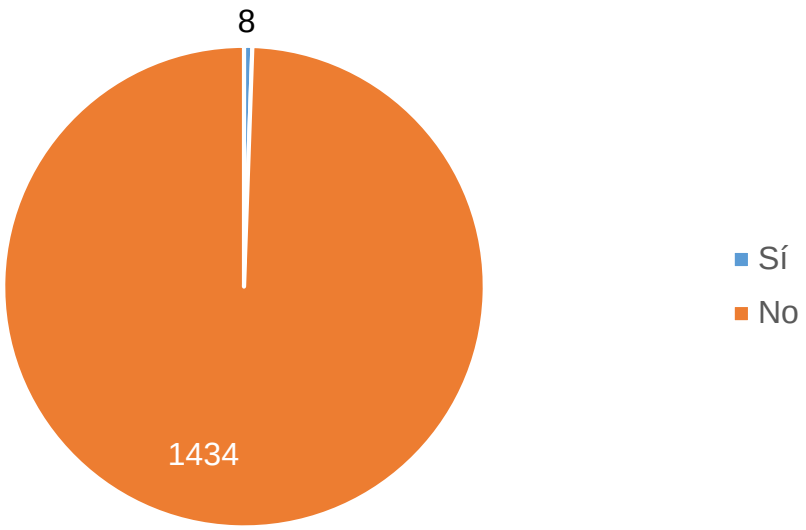
19. ¿Y durante años anteriores?



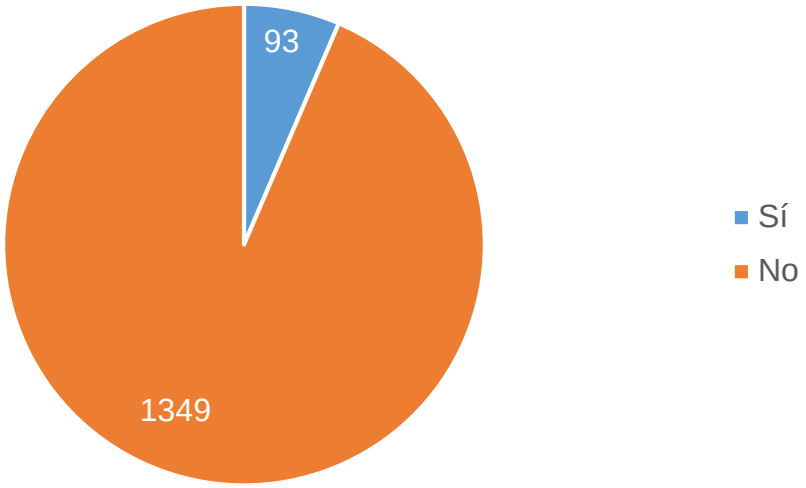
20. ¿Ha sido tu identidad suplantada por otra persona para abrir una nueva cuenta bancaria, línea de crédito o un préstamo durante 2020?



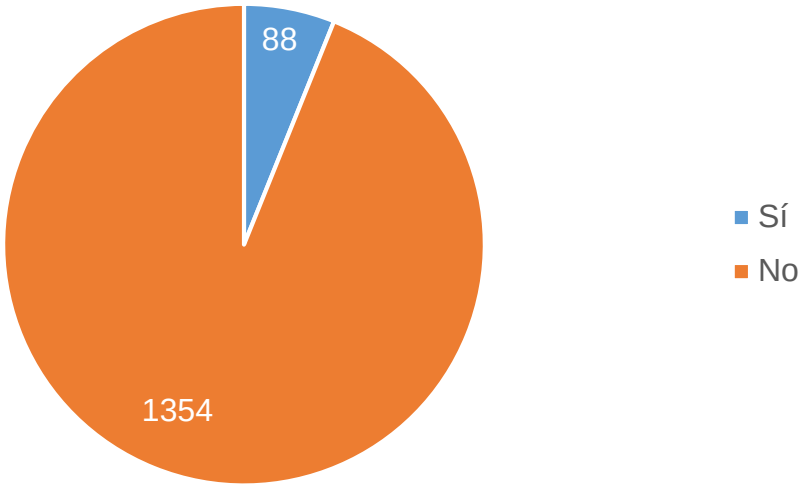
21. ¿Y durante años anteriores?



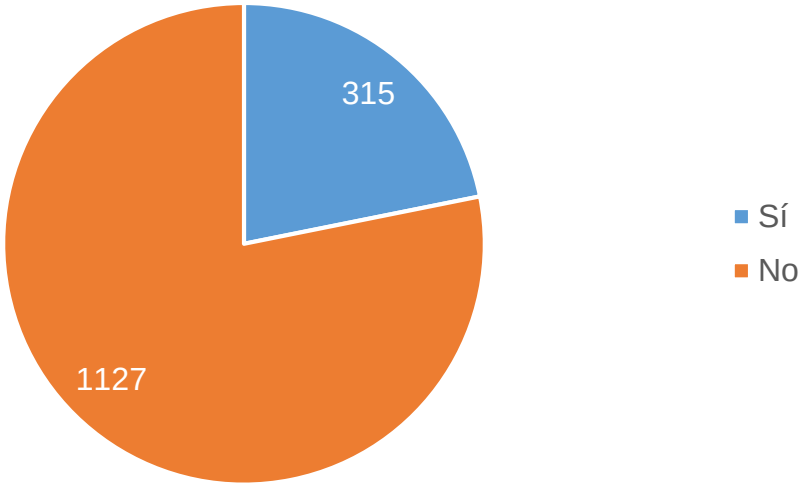
22. ¿Has tenido transacciones desconocidas en tu cuenta bancaria, tarjeta de crédito u otros sistemas de pago online durante 2020?



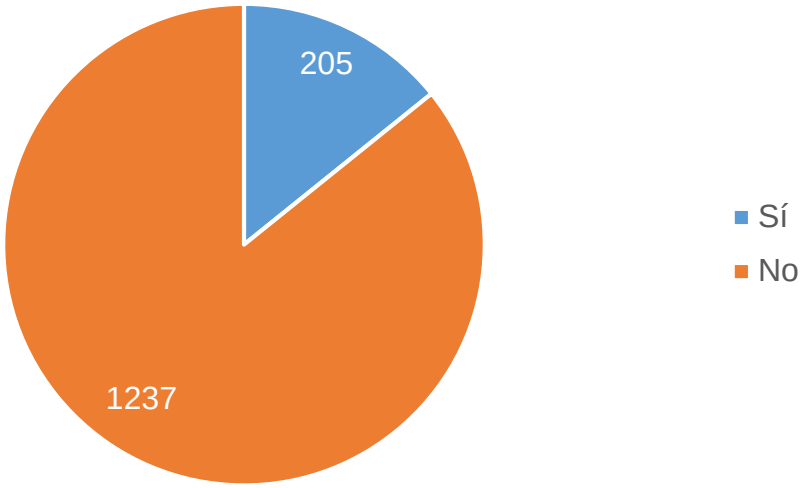
23. ¿Y durante años anteriores?



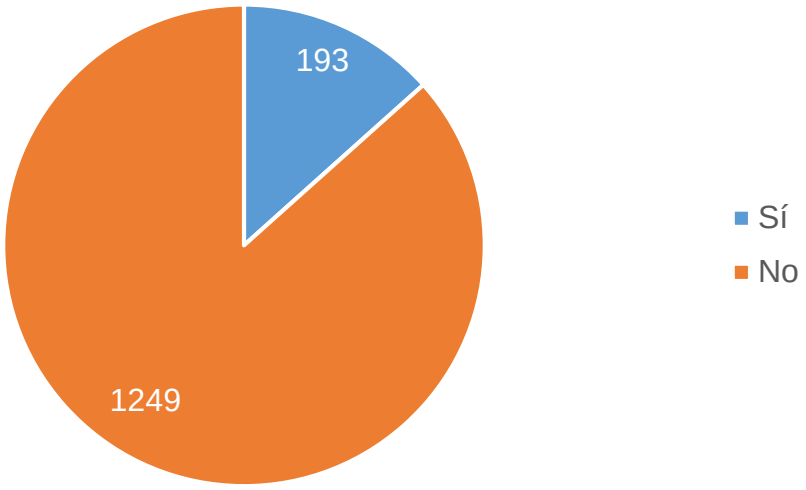
24. ¿Has recibido un mensaje por parte de alguna empresa/organización notificando que tus datos personales (como tu nombre, número de Seguridad Social, contraseña, tarjeta de crédito) han sido robados o publicados en Internet durante 2020?



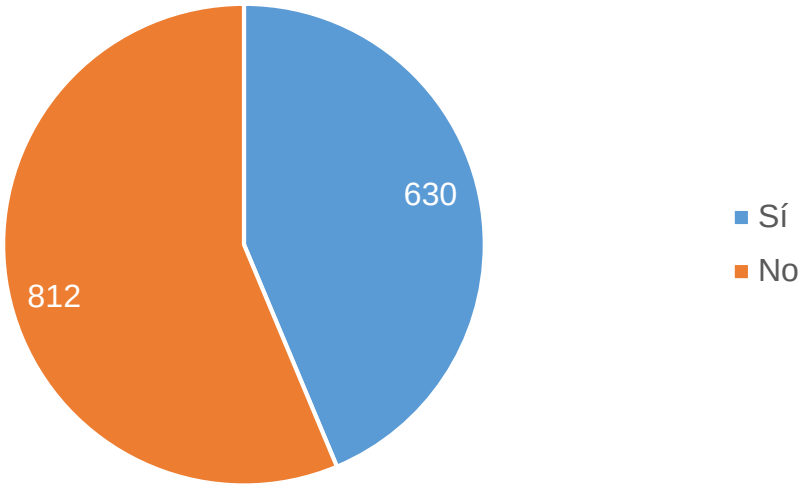
25. ¿Y durante años anteriores?



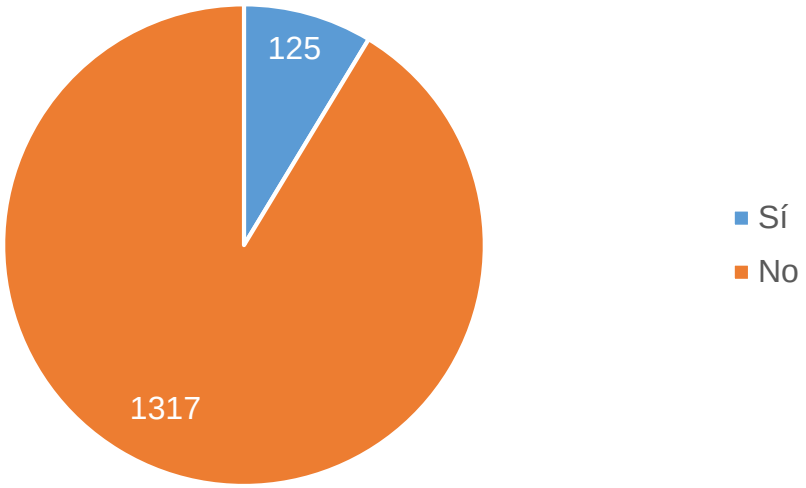
26. ¿Ha sido tu ordenador infectado por algún virus informático durante 2020?



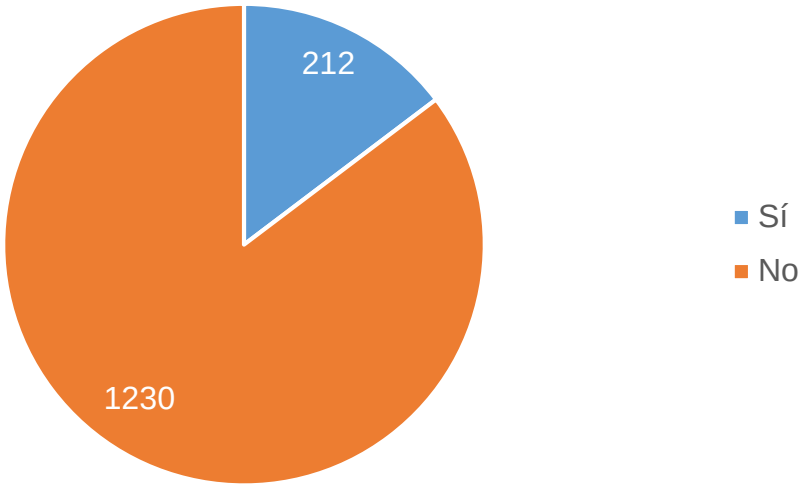
27. ¿Y durante años anteriores?



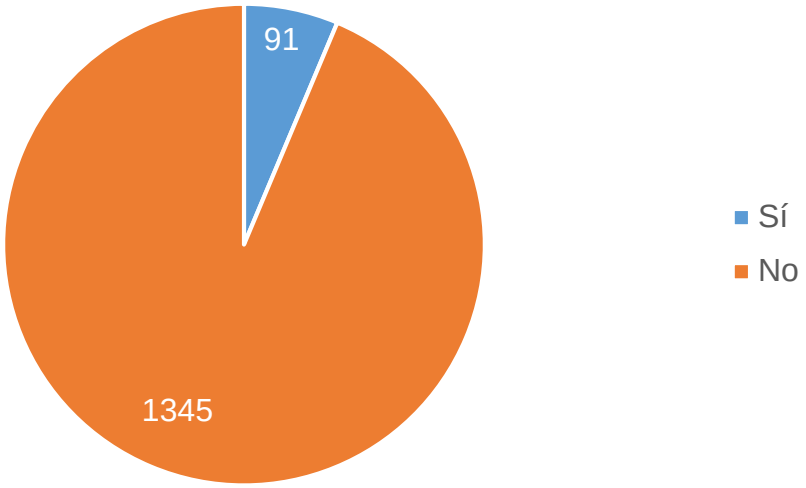
28. ¿Has sido objeto de comentarios, imágenes o videos hirientes publicados en Internet durante 2020?



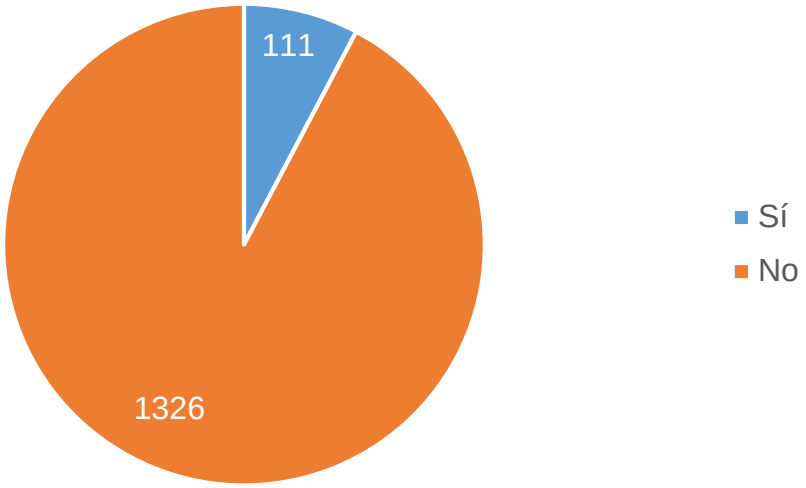
29. ¿Y durante años anteriores?



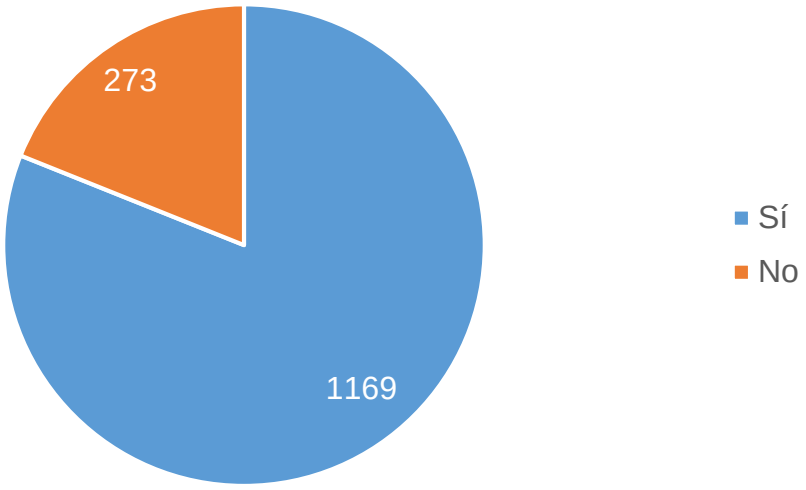
30. ¿Has sido objeto de comentarios sexuales no solicitados y/u otros tipos de acoso sexual online durante 2020?



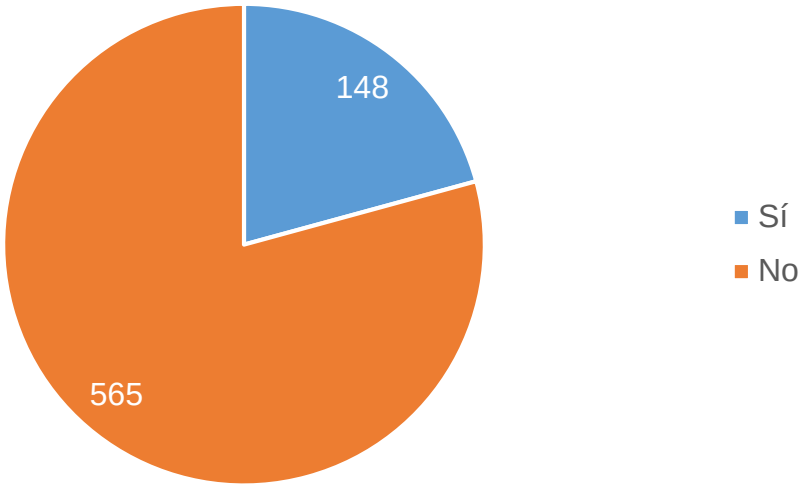
31. ¿Y durante años anteriores?



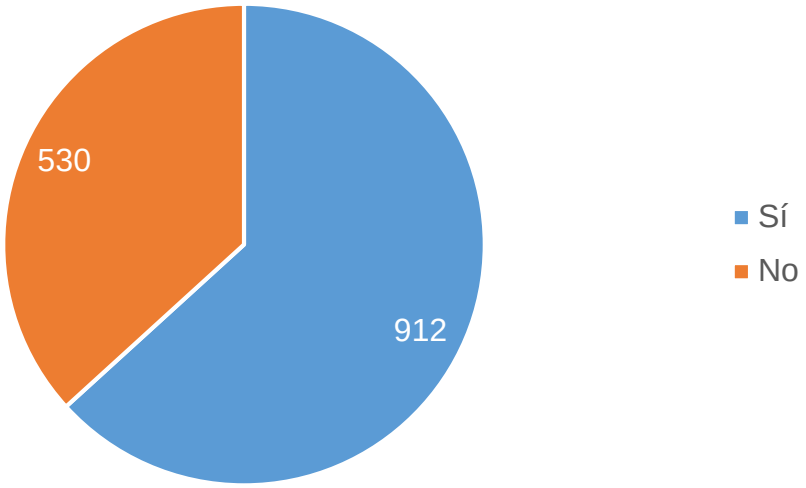
32. Si fueses víctima de algunos de los delitos previamente mencionados, ¿presentarías una denuncia?



33. En caso de haber sido víctima de algunos de los delitos previamente mencionados, ¿presentaste una denuncia?

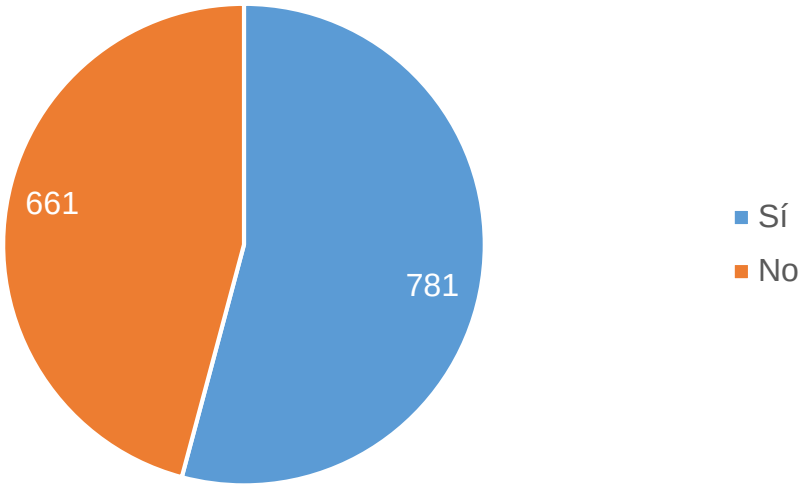


34. ¿Has recibido algún SMS, correo o link sospechoso relacionado con el coronavirus durante 2020?

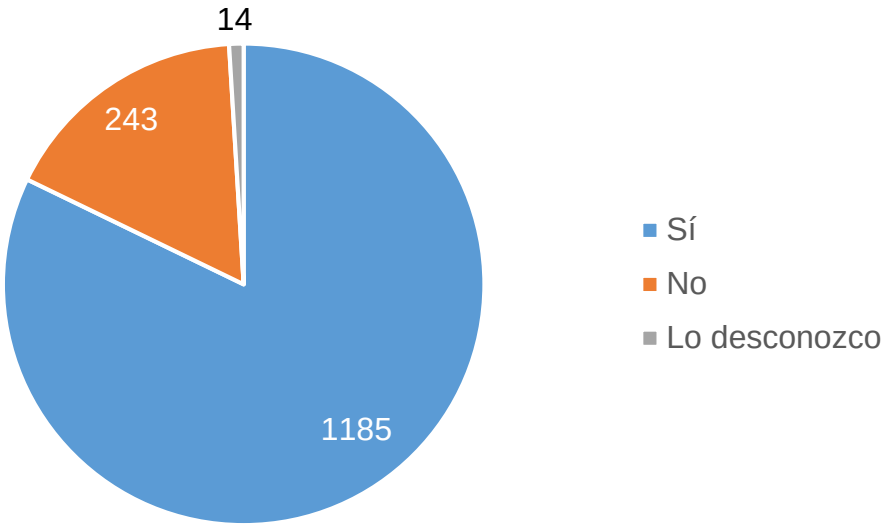


MEDIDAS DE AUTOPROTECCIÓN

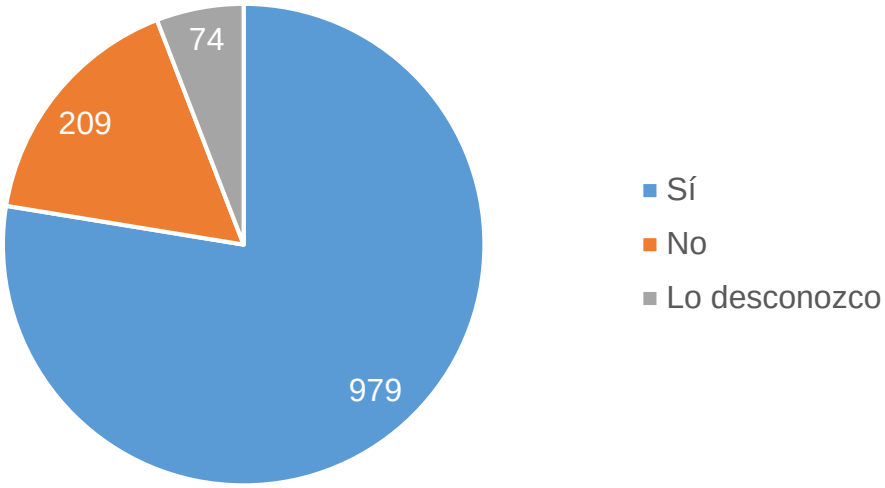
35. ¿Tapas tu webcam cuándo no la estás usando?



36. ¿Utilizas algún tipo de antivirus o software similar en tu ordenador?



37. En caso afirmativo, ¿lo mantienes actualizado con regularidad?



38. ¿Utilizas el sistema de autenticación en dos pasos cuando te conectas a alguna de tus cuentas? (Explicación: cuando para conectarte no solo te pide tu contraseña, sino otro tipo de confirmación como por ejemplo un código de seguridad que es enviado a tu número de teléfono)