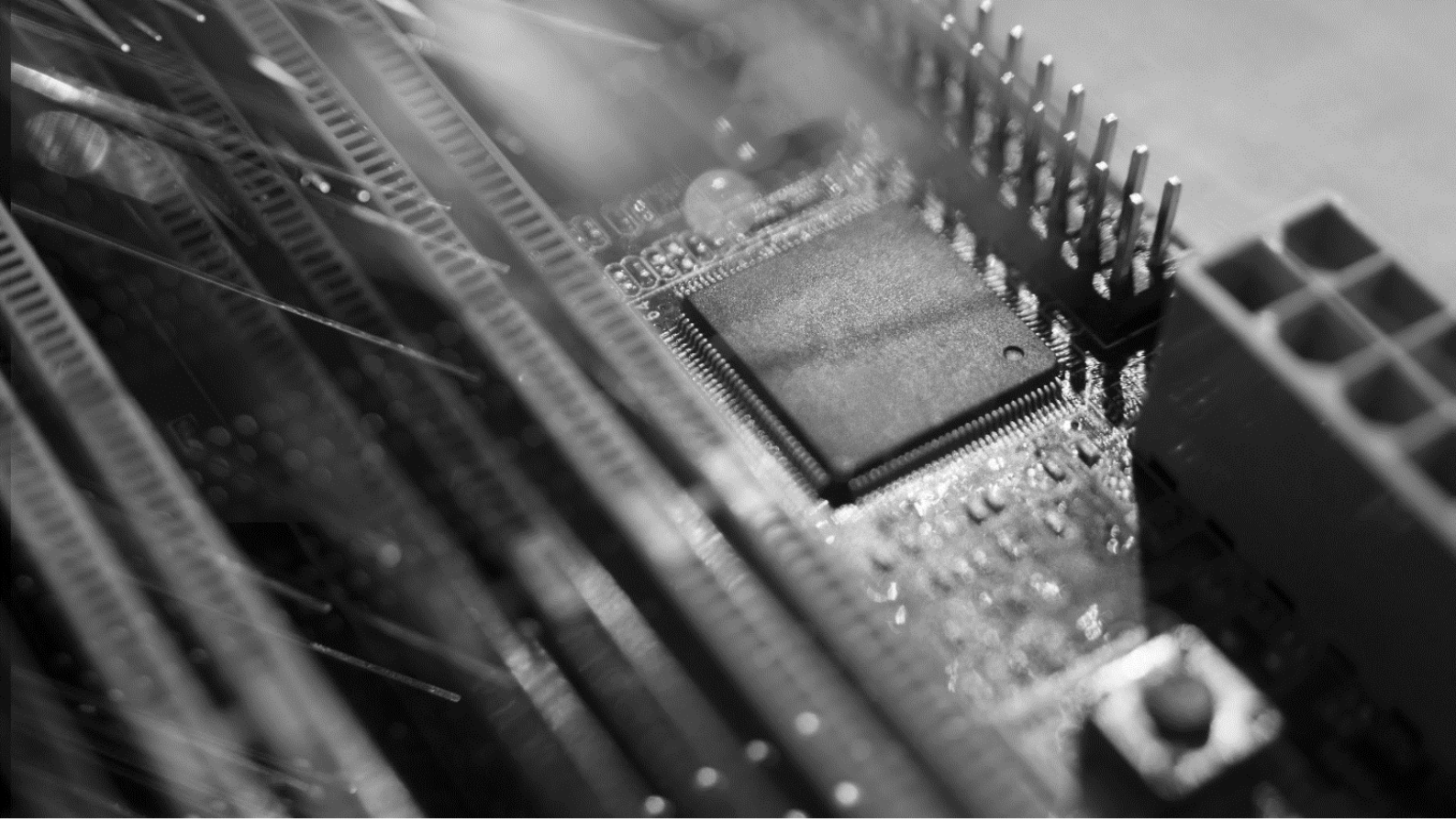


STUDY ON CYBERSECURITY AND TRUST IN SPANISH HOUSEHOLDS

January - June 2019

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA Y EMPRESA
ontsi observatorio nacional de las telecomunicaciones y de la SI
red.es

CONTENT

1. STUDY ON CYBERSECURITY AND TRUST IN SPANISH HOUSEHOLDS

Red.es, in collaboration with Hispasec Sistemas and GFK, has conducted a study to analyse the adoption of security measures and evaluate the occurrence of situations that could constitute security risks, as well as the degree of trust that Spanish households place in using new information technologies.

The objective of this study is to analyse Spanish households using security indicators that are based on users' perception of security as well as their level of trust in Internet security and how it has evolved over time, comparing this with users' real level of security on computers and Android devices.

The aim is to promote the understanding and monitoring of the main indicators as well as public policies related to information security and e-trust. Thus, among other aims, the report seeks to provide information on safe and private behaviours and use of new technologies and serve as a tool to help users solve incidents and for governments to adopt security measures.

The study was conducted via two channels: an analysis of the real security of computers and Android devices via scans with Pinkerton software; and an analysis of statements provided by surveyed Internet users.

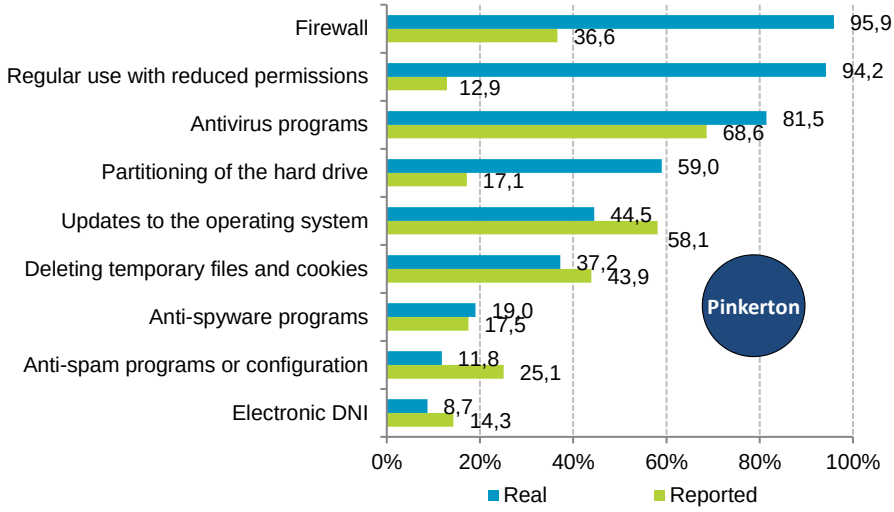
The data reported were obtained from online surveys given to households included in the study sample, while the real data was obtained using Pinkerton software. This software analyses the systems by gathering data from the operating system, its update status and the security tolos installed and detects the presence of malware on computers and mobile devices by using a combination of 50 antivirus engines.

1.1 Security measures

The use of passive and active security measures is one of the essential pillars of information security. Passive security measures are those which do not require the user's intervention in order to be implemented. On the other hand, active security measures are those that must be directly executed by the user.

The following results regarding security measures come from the statements of Spanish users and from data collected by analysing their systems (household computers and mobile devices) with the Pinkerton tool. Here, passive security measures as well as active security measures are included.

FIGURE 1. REPORTED VS REAL USE OF SECURITY MEASURES ON THE HOUSEHOLD COMPUTER (%)



Base: PC users
Source: Panel hogares, ONTSI

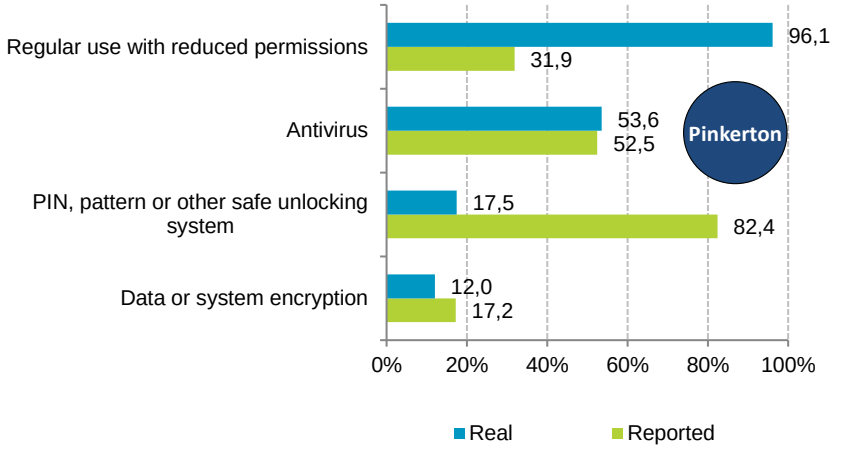
The use of firewall and the use of devices with reduced permissions are the most widespread security measures, with a small rise in both of them (about 95%) compared with the last semester. Antivirus protection is still a popular security measure among users (81.5%), followed by partitioning of the hard drive (59.0%).

The use of electronic DNI remains below 10%, which makes it the least implemented security measure by Spanish Internet users. This indicates that its popularity among Spanish people has not increased.

Nonetheless, the data obtained using the Pinkerton software evince great differences when compared with users' statements. The highest variations are shown in the use of firewall (59.3 p.p.), the use of devices with reduced permissions (81.3 p.p.) and the use of partitioning of the hard drive (41.9 p.p.). One possible explanation for these differences could be the lack of user knowledge about these security measures that are implemented by default on the operating system of their computers.

Most operating systems nowadays include firewall software, create users without administrator permissions by default, and when the OS is already installed on the device, it usually has a hidden partition for recovery. In addition to this, the latest versions of Microsoft operating systems create a low capacity boot partition that is also inaccessible to the user. Given users are not aware of all these default features, when they start their computers they will have limited privileges on the system, the firewall will remain active, and they will work on the system partition and its data unknowingly.

FIGURE 2. REPORTED VS REAL USE OF SECURITY MEASURES ON ANDROID DEVICES (%)



Base: Android device users
Source: Household panel, ONTSI

The most widely used security measure on mobile devices is the regular use with reduced permissions (96.1%), followed at great distance by antivirus (53.6%). Data or system encryption is barely used (12.0%); and there is a notable discrepancy between reported (82.4%) and real (17.5%) use of a safe unlocking system.

Regarding the use of antivirus and data encryption, there is not a high deviation among the information obtained using Pinkerton tool and what users reported.

However, Pinkerton shows that a much higher percentage of users than what was reported make regular use of their devices with reduced permissions (65.2 p.p.). This could be so because a significant proportion of users are not aware that they are not using their terminals as a 'root' user. In order to be able to execute admin tasks, the system requires the special intervention of the user so privileges can be escalated. This escalation of privileges can be quite difficult for the average user, and it might lead to the loss of the manufacturer warranty due to a significant alteration of the product. In other cases the process of privileges escalation might entail damage risk for the device.

Another discrepancy between user reponses and real data obtained with Pinkerton lies in the use of a secure unlocking system (82.4% reported use and 17.5% real use). This gap (64.9 p.p.) could be due to most users' lack of knowledge regarding the correct use of a safe unlocking system such as a PIN number, a pattern or byometric systems. Thus, people might answer 'yes' to this question when in reality most of them are using an insecure locking system such as suspending the terminal, which can be reactivated by simply pressing the on button or swiping the screen.

REGULAR USE WITH REDUCED PRIVILEGES IN WINDOWS (REAL DATA)[1]

100.0%
WITH REDUCED PERMISSIONS IN WINDOWS 10

100.0%
WITH REDUCED PERMISSIONS IN WINDOWS 8

74.1%
WITH REDUCED PERMISSIONS IN WINDOWS 7

REGULAR USE WITH REDUCED PRIVILEGES IN ANDROID (REAL DATA)

99.2%
WITH REDUCED PERMISSIONS IN ANDROID 9

99.4%
WITH REDUCED PERMISSIONS IN ANDROID 8

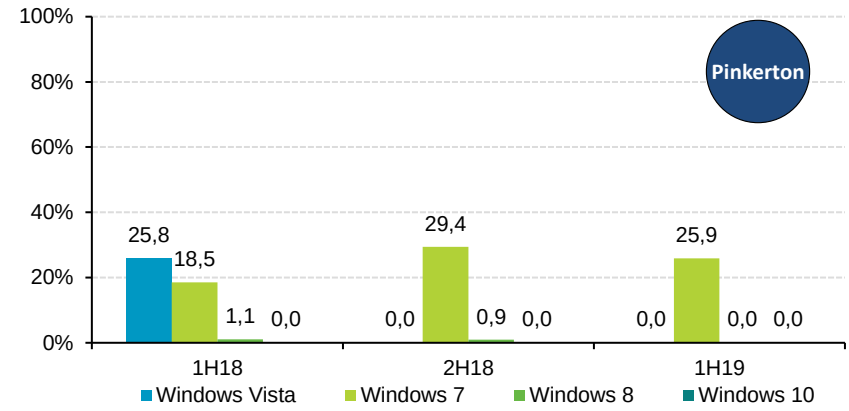
98.6%
WITH REDUCED PERMISSIONS IN ANDROID 7

96.9%
WITH REDUCED PERMISSIONS IN ANDROID 6

87.0%
WITH REDUCED PERMISSIONS IN ANDROID 5

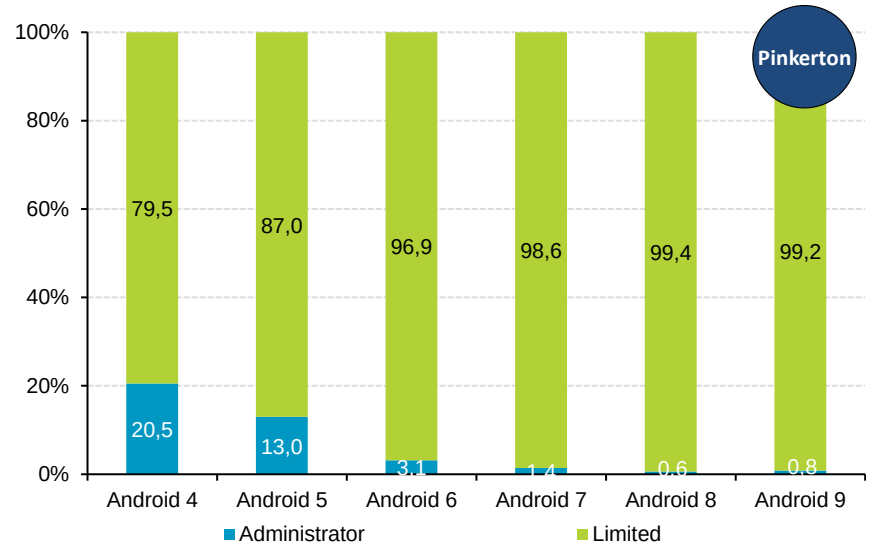
79.5%
WITH REDUCED PERMISSIONS IN ANDROID 4

FIGURE 3. EVOLUTION OF ACTUAL ADMINISTRATOR PROFILE USE IN MICROSOFT WINDOWS OPERATING SYSTEM (%)[1]



Base: Microsoft Windows Users
Source: Household panel, ONTSI

FIGURE 4. REAL USE OF ADMINISTRATOR PROFILES ON ANDROID DEVICES (%)



Base: Android device users
Source: Household panel, ONTSI

Figure 3 shows that the use of administrator profile on Windows operating systems is limited to Windows 7 version (25.9%), compared with around 0% in the rest. In the latest versions of Windows 8 and Windos 10, it is a strengthened habit because an account with limited privileges is created by default.

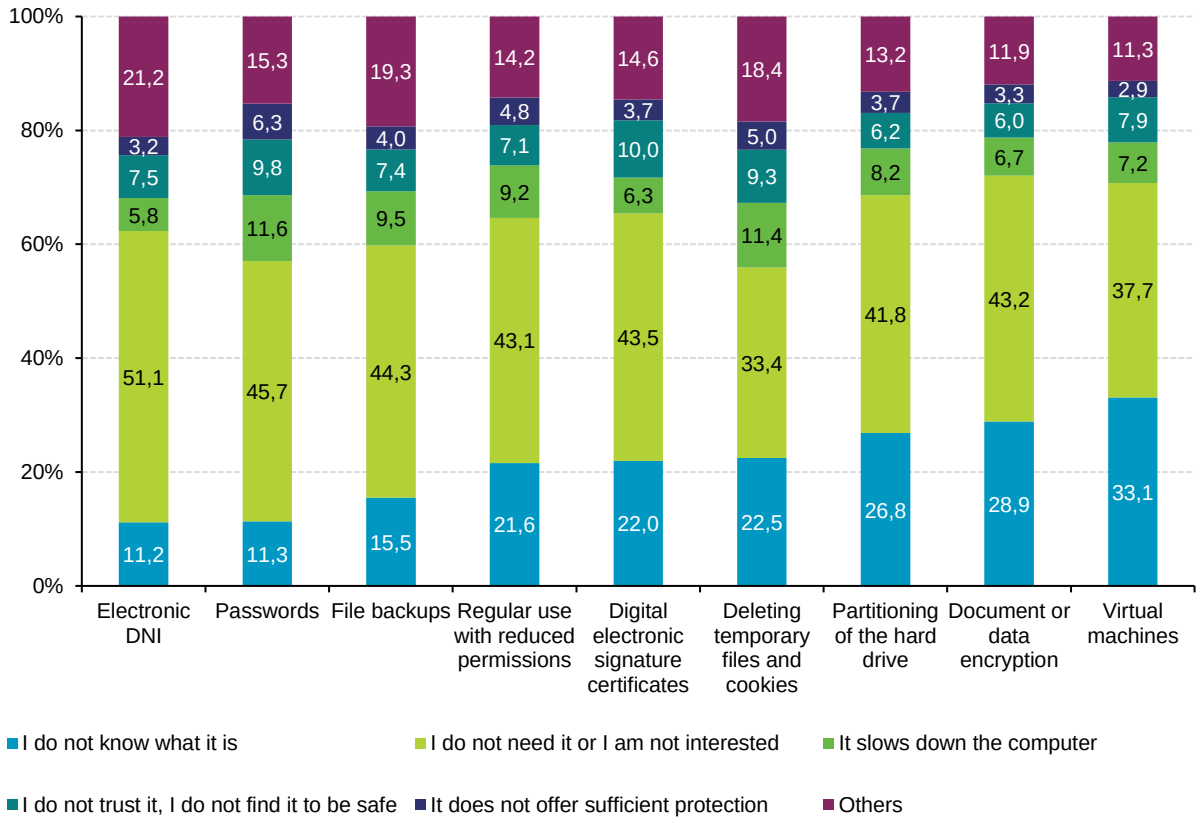
We must highlight a substantial decrease in the use of devices with administrator privileges as the Android version is more recent. The usage of th is feature rests below 2% for Android 7 and 9.

In spite of the statement on the last paragraph, in the case of Android 4, 20.5% of users usually make use of their devices with administrator privileges, whereas this percentage is reduced to 13.0% with the introduction of Android 5. The trend of manipulating older terminals may be due to the end of the device warranty period

[1] Since the second semester of 2018 until the present day, the use of Microsoft Windows Vista operating system has been essentially symbolic among panelists so data on this system should not be considered.

and the end of oficial support from the manufacturer, so the user is 'forced' to search for alternatives in order to continue using the terminal with an updated operating system or to be able to install more modern applications.

FIGURE 5. REASONS FOR NOT USING SECURITY MEASURES (%)



Base: users who do not use any of the security measures
Source: Household panel, ONTSI

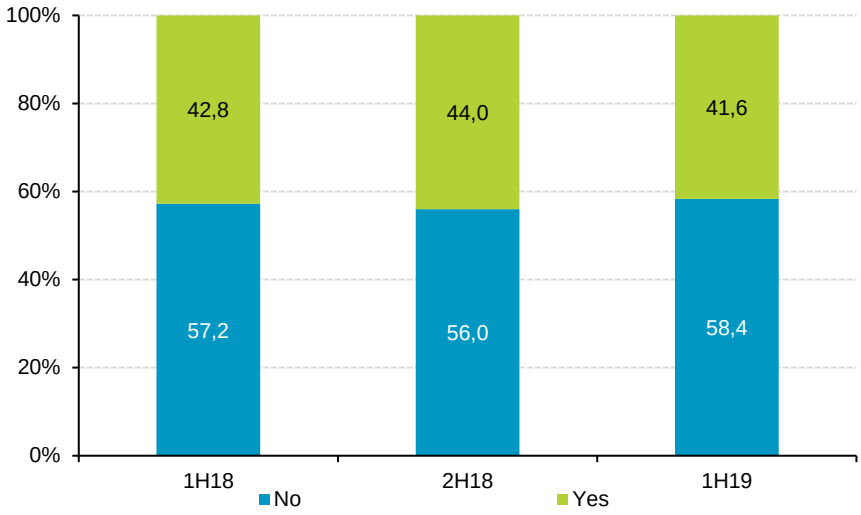
According to users' responses, the main reason for not using security measures is that these are considered unnecessary (between 33.4% and 51.1% depending on the security measure). The least interesting measure for Internet users is the use of electronic DNI (51.1%), followed by the use of secure passwords (45.7%).

The least known measures that users do not adopt because of their lack of knowledge regarding their functioning mechanisms are virtual machines (33.1%), document or data encryption (28.9%) and partitioning of the hard drive (26.8%).

1.2 Behaviour habits in browsing and Internet use

During this semester there has been a downturn in the percentage of users who admit to knowingly having risky behaviours (2.4 p.p.). We could infer that raising of awareness regarding the importance of safe habits on the Internet to prevent problematic and/or dangerous situations is growing.

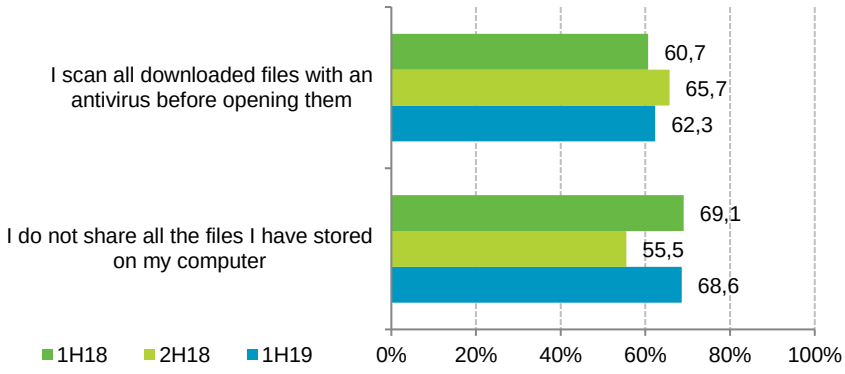
FIGURE 6. EVOLUTION OF THE KNOWING ADOPTION OF RISKY BEHAVIOURS (%)



Base: all users
Source: Household panel, ONTSI

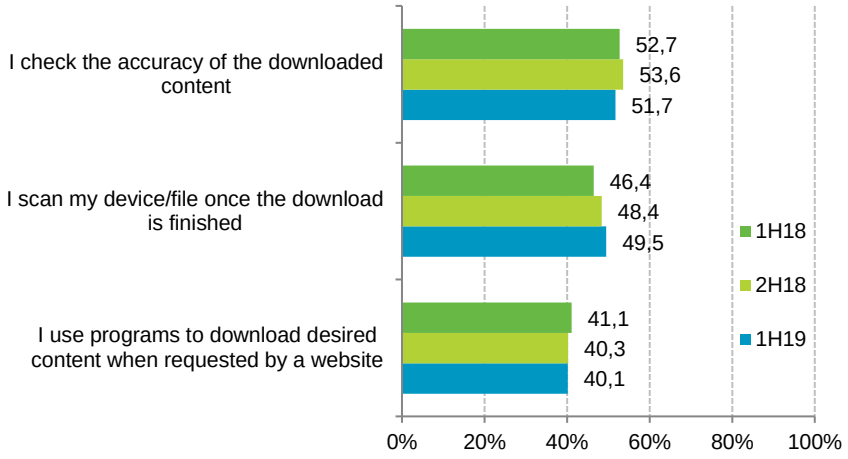
During the last semester the use of security measures has increased, which might be associated to a higher awareness of the necessity to use the Internet in a responsible way and with proper and safe consumption habits. Nonetheless, the aforementioned increment of the implementation of security measures and the number of users who declare not adopting risky habits is still moderate.

FIGURE 7. P2P NETWORK DOWNLOADS (%)



Base: users of P2P networks
Source: Household panel, ONTSI

FIGURE 8. INTERNET DOWNLOADS (%)



Base: all users
Source: Household panel, ONTSI

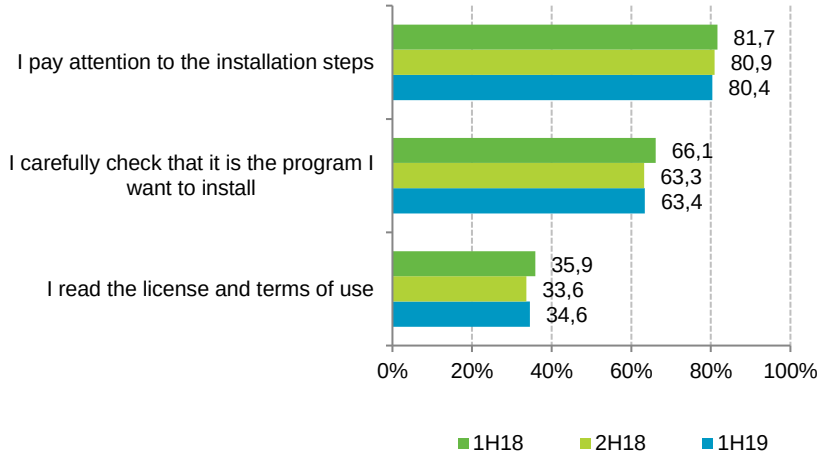
After analysing the data obtained pertaining the downloads from P2P networks and direct downloads from the Internet, a slight decline can be seen in **FIGURE 6** regarding the use of security measures. This decline, aside from the use of antivirus engines to scan the downloaded files (-3.4 p.p.), cannot be considered significant compared to the data obtained last semester.

The most meaningful variation regarding the adopted security measures when downloading files can be observed in the configuration of shared folders in P2P download networks, where 68.6% of users declare not sharing the totality of the files stored in their computers. Thus, we observe similar values to those obtained in the beginning of 2018, after the sudden drop during the last semester of that same year.

Despite the surge in the number of users restricting shared folders on P2P networks, the results obtained regarding safe habits when conducting this kind of actions can be considered alarming since approximately half of the users do not seem to pay enough attention to the security risks attached to files downloaded from the Internet (regardless of whether these files are downloaded directly from the Internet or from P2P networks). These files are not vouched by any organisation, therefore they are likely to contain malware, being damaged (unusable or at risk of endangering the system security), or even incorporate different content from what was expected by the user as well as content not suitable for children.

Also, free downloads sites usually resort to a wide range of strategies in order to obtain benefits, as might be the use of fake additional download buttons or the inclussion of adware and/or other kind of unwanted software, among other similar practices.

FIGURE 9. INSTALLATION OF PROGRAMS ON THE HOUSEHOLD COMPUTER (%)



Base: all users
Source: Household panel, ONTSI

An elevated percentage of the surveyed users report paying attention to the installation steps, although as shown in Figure 9, this percentage maintains a lessening tendency compared to previous semesters. This apparent sense of security that increasingly emerges among users may be the result of the official markets for computers (such as Microsoft Store for Windows, Software Manager for Linux, and App Store for iOS), where it is assumed that the offered applications undergo strict quality controls and are free of potential threats for the user's computer.

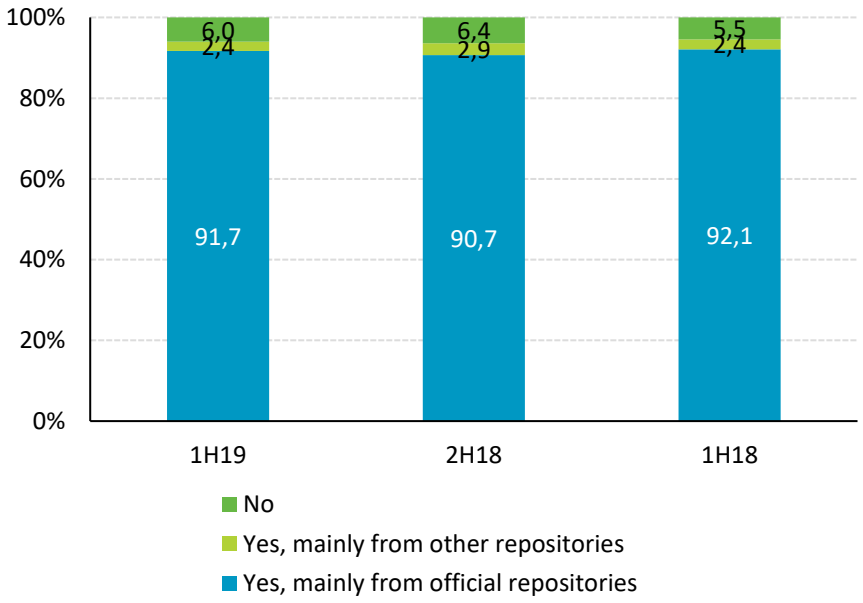
The percentage of users who carefully verify a program before installing it has not changed very much in comparison to the last semester, something that could be considered worrisome since this percentage is down almot 3 p.p. from the first semester of 2018. This might demonstrate a seemingly ongoing increase in the deceptive sense of security among users during a time when uncountable and very diverse attacks are constantly taking place on the Internet.

This decrease on the rate of verification of the installed programs might also be a consequence of the apathy of the user when facing the installation process, since for those with reduced technical knowledge it can become tedious. This is related as well to the recommended reading of the license and the terms of use included with every software that the user installs on their computers. Reading these documents is something that people rarely do, particularly home users. However, it must be highlighted that compared with the second semester of 2018, this percentage has increased 1 p.p., which could mean that the general public is becoming aware of the importance of taking security measures when using the Internet. Users seem to be more concerned about the terms of use they accept when installing and using a program.

During the installation process, freeware and shareware applications normally request the user's permission to install the software of third parties that sponsor their services; sometimes, the installation of this third-parties' software is not even requested but directly installed on the user's computer. For this reason, if sufficient attention is not payed during the installation process, the

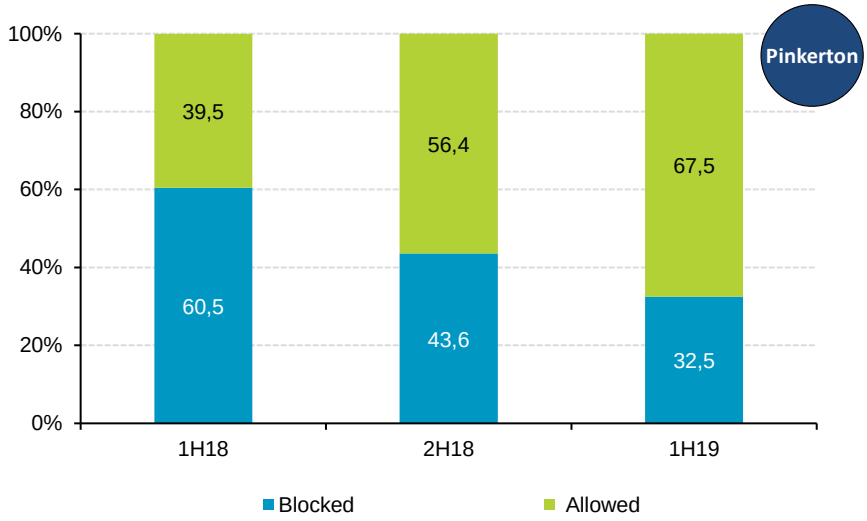
user might end up installing adware or even malware on their device.

FIGURE 10. EVOLUTION OF APPLICATION DOWNLOADS ON ANDROID DEVICES (%)



Base: Android device users
Source: Household panel, ONTSI

FIGURE 11. EVOLUTION OF THE STATUS OF UNKNOWN SOURCES (%)



Base: Android device users
Source: Household panel, ONTSI

As reported by Android users, 91.7% of them download apps mainly from official repositories / official markets, which may be due to the integration of these official repositories with the system and the user-friendliness they provide, rather than because of a security matter.

Real data obtained by means of Pinkerton tool reveal that users are increasingly taking more risks when installing applications on their Android devices, and that they have modified the default settings to allow the installation of applications downloaded from unknown sources. This percentage has risen 28 p.p. during the last year.

Thus, the results obtained in the first semester of 2019 are opposite to those of previous versions of this study (2015-2016).

Installing mobile applications from unknown markets involves high risk for the security of the device, since these repositories do not implement analysis measures nor do they detect stored fraudulent applications. In the same way they do not control the source these applications come from. The main feature offered by these unknown markets that attracts the user's attention is granting paid content for free.

It is important to mention the existence of *droppers* –malware whose function is downloading other malicious content to install it on the infected system-. These suppose high additional risk for all devices in which the installation of applications from unknown markets is allowed.

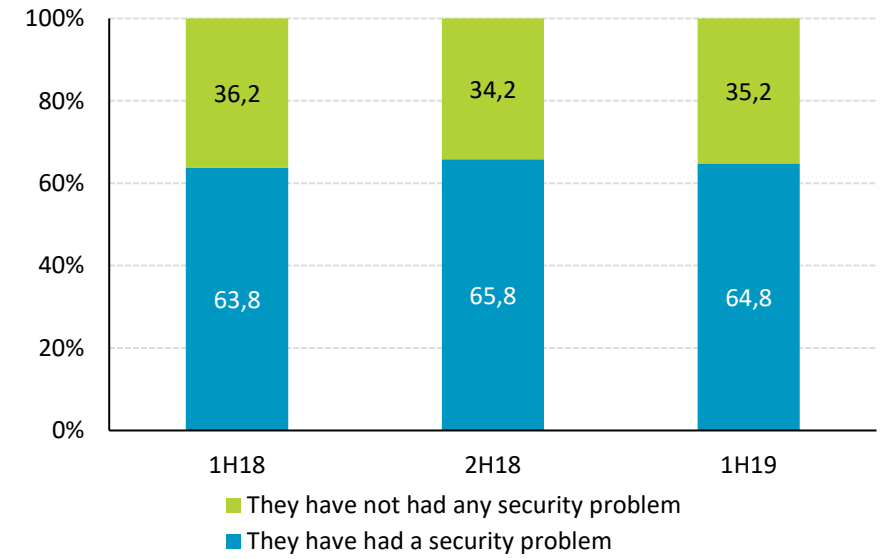
1.3 Security incidents

Cyberthreats are continuously evolving and trying to avoid all security measures taken by the user as well as those implemented on the system itself, and even antivirus engines, which makes it impossible to have sure-fire ways to avoid security incidents.

This means that the use of different security measures and the implementation of safe habits on the Internet will reduce the risk of becoming a victim, but this risk will always be present.

In this section security incidents suffered by surveyed users during January and June, 2019, will be analysed.

FIGURE 12. EVOLUTION OF SECURITY INCIDENTS (%)

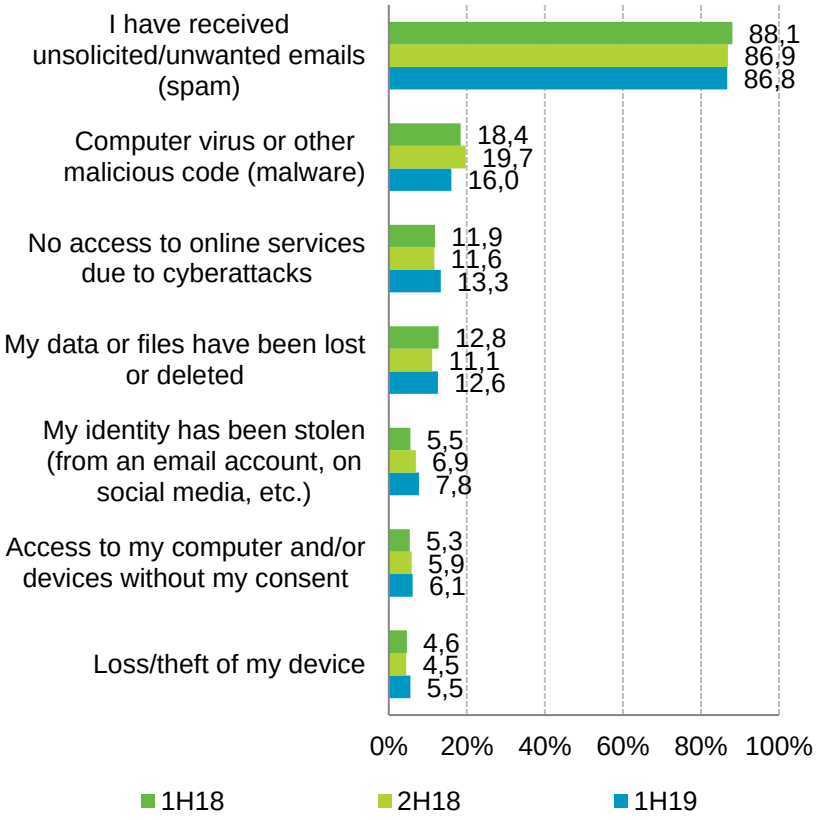


Base: all users
Source: Household panel, ONTSI

A decrease of 1 p.p. over all users reporting a security-related incident during this semester can be observed in Figure 12. This figure also shows that 35.2% of them did not have any security problem, or that they are not aware of having been a victim, compared to almost two-thirds of affected users. These data show

a strong correlation with the data regarding the conscious adoption of risky habits shown on **FIGURE 6**.

FIGURE 13. EVOLUTION OF CLASSIFICATION OF SECURITY INCIDENTS (%)



Base: users who have experienced a security incident
Source: Household panel, ONTSI

As expected, the receipt of unwanted emails (SPAM campaigns) leads the list with 86.8% of the reported incidents, a much higher value than the rest of the reported security incidents. There are no significant changes compared to the last version of this study. However, a decrease of -1.3 p.p. since last year must be highlighted.

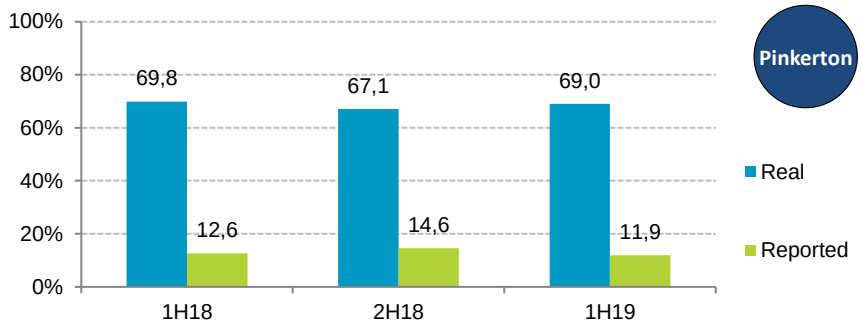
Users perceive that malware-related incidents have significantly diminished, which has led to a decrease of affirmative answers since the publication of the last report (-3.7 p.p.), thus presenting a substantial improvement compared with the left options.

The following figures will show a deeper analysis of malware incidents with the intention to determine whether users' perception matches reality or malwares are a hidden threat that still goes unnoticed for most Internet users.

Malware is the name for any malicious program that aims to infiltrate a computer and take action without the owner's consent.

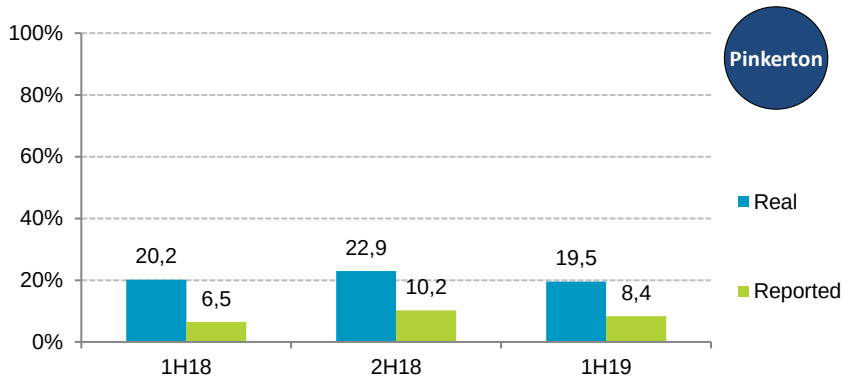
They are commonly known as viruses, although in reality malware is a much broader term that encompasses many other types of malicious programs.

FIGURE 14. EVOLUTION OF MALWARE INCIDENTS (REPORTED VS REAL) ON HOME COMPUTERS (%)



Base: PC users
Source: Household panel, ONTSI

FIGURE 15. EVOLUTION OF MALWARE INCIDENTS (REPORTED VS REAL) ON ANDROID DEVICES (%)



Base: Android device users
Source: Household panel, ONTSI

COMPUTERS HOSTING MALWARE (REAL DATA VS PERCEPTION)

69.0%
OF COMPUTERS SCANNED WITH PINKERTON HOST MALWARE

11.9%
OF USERS NOTICE MALWARE ON THEIR PERSONAL COMPUTERS

Data obtained with Pinkerton tool differs substantially from what has been reported by users.

Although the current situation might seem worrisome because 69% of household computers are host to some kind of malicious software, this number is still lower than the data obtained during the second semester of 2017 and the first semester of 2018.

Nonetheless, there is still a great gap between reality and what is reported by users, which becomes one of the most worrying aspects of this study, particularly if we take into account that the statements provided by users in this regard have kept a lessening tendency since the year 2016 (**FIGURE 13** and **FIGURE 14**).

In the case of Android devices, the number of malware cases detected by users as well as by Pinkerton tool has decreased (-1.8 p.p and -3.4 p.p respectively).

ANDROID DEVICES HOSTING MALWARE (REAL DATA VS PERCEPTION)

19.5%
OF ANDROID DEVICES SCANNED WITH PINKERTON HOST MALWARE

8.4%
OF USERS NOTICE MALWARE ON THEIR ANDROID DEVICES

TABLE 1. MALWARE INCIDENTS ON THE HOUSEHOLD COMPUTERS (%)

They reported having malware on PC	Their PC had malware (Pinkerton)		
	Yes	No	Total
Yes	8,1	2,3	10,4
No	60,9	28,7	89,6
Total	69,1	30,9	100

Base: PC users
Source: Household panel, ONTSI

TABLE 2. MALWARE INCIDENTS ON ANDROID DEVICES (%)

They reported having malware on Android	Their Android had malware (Pinkerton)		
	Yes	No	Total
Yes	1,2	5,2	6,4
No	18,4	75,2	93,6
Total	19,6	80,4	100

Base: Android device users
Source: Household panel, ONTSI

In the previous pair of tables data reported by users and real data have been compared for each scanned device in order to emphasise the existing gap between the obtained data. This will allow us to dismiss wrong conclusions that might be given by posible technical problems on the devices, which are not caused by malicious software but by an incorrect configuration.

A small group of users were aware that their computers had been infected (8.1%) as well as other devices (1.2%). Also, these users had not taken any measures to solve this situation –due to lack of knowledge about the available solutions to the problem, because they were waiting for technical support, or even because they did not consider the issue to be important enough- at least up to the moment the analysis by the Pinkerton tool was carried out.

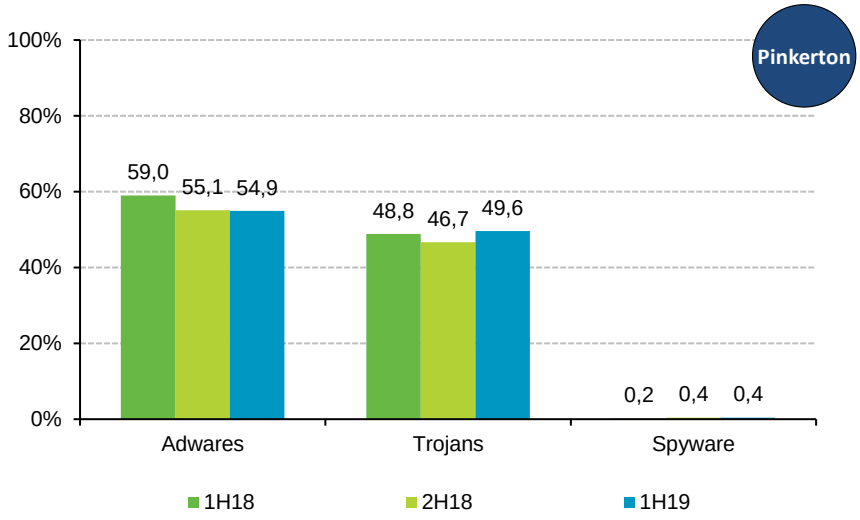
On the other hand, we can find users who detected the malware infection and knew what to do in order to solve the problem, or that identified what seemed to be a strange behaviour of their devices and considered a virus to be the cause of the abnormality. This group is comprised of users who declared that their computers (2.3%) or their Android device (5.2%) were infected by malware, although Pinkerton tool did not find any traces of a threat of this nature.

In spite of the detected improvements, the most outstanding result is, once again, the amount of users who report not having suffered any malware-related incident when, in fact, their devices have been compromised. It has been found that 60.9% of household computers and 18.4% Android devices analised by Pinkerton are actually affected by malware.

As it has been shown, we face a particularly troubling situation, not only because of the malware-related incidents themselves, but also due to the lack of awareness of users.

The only real improvement compared with the last version of this study is found among Android users who declare not being victims of malicious software incidents in spite of their devices showing some kind of malware-related problem; this percentage has fallen -3 p.p.

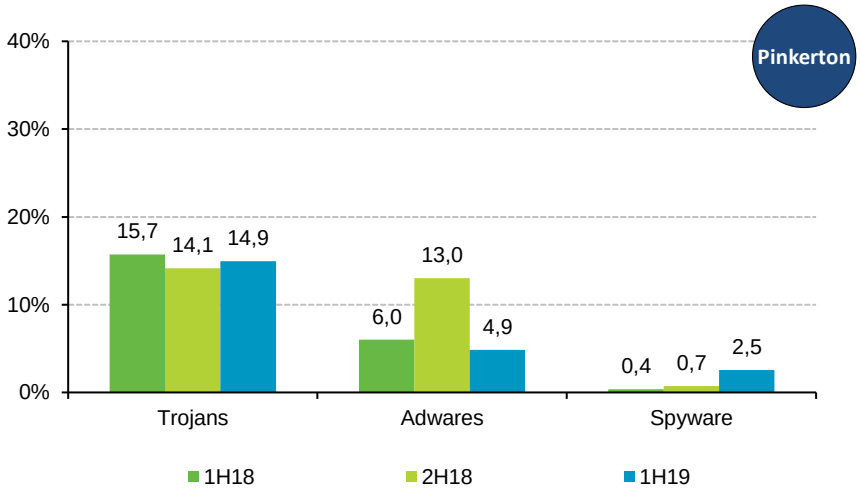
FIGURE 16. EVOLUTION OF MALWARE ON THE HOUSEHOLD COMPUTER (%)



Base: All computers
Source: Household panel, ONTSI

Household computers are mainly infected by adware and Trojans

FIGURE 17. EVOLUTION OF MALWARE ON ANDROID DEVICES (%)



Base: All Android devices
Fuente: Household panel, ONTSI

Attackers use two different strategies to develop the malicious software aimed at infecting the victim with the intention to achieve their goals.

One of these strategies is based on hiding the malware in plain sight on the PC or Android device of the victim in order to obtain monetary benefits from adwares shown in the device without the person's authorisation, the addition of web browser adds, or asking

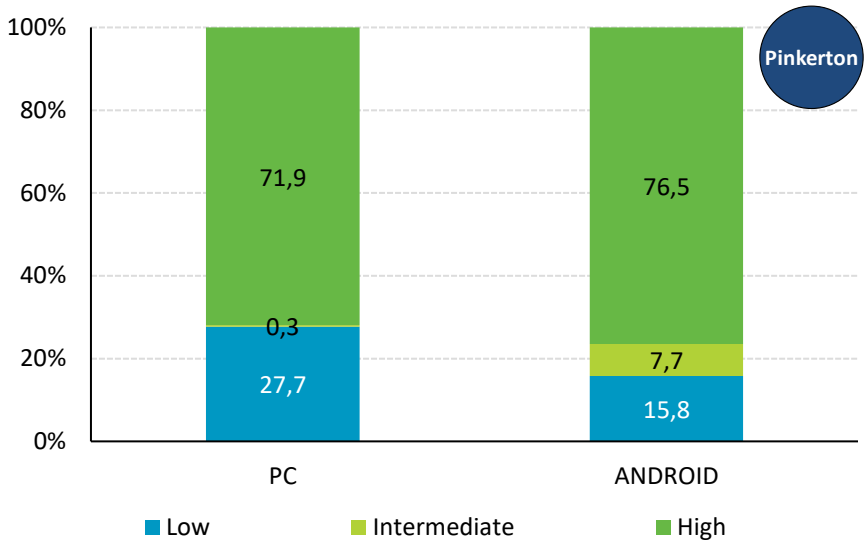
the victim for a rescue to be able to recover the files that have been encrypted by the malicious software (ransomware). The second strategy involves making the malware go unnoticed by solutions such as antivirus engines and even the user itself. This way, the malware achieves its purpose, i.e. obtaining banking credentials, email accounts, or any other information that may allow the attacker to get money from the victim.

Figure 16 shows how the presence of malware on personal computers increases in the case of Trojans (+2.9 p.p.), which becomes the highest value compared with the last two versions of this study. In the case of spywares, the number of affected users is mereley 0.4%, therefore it could be considered almost non-existing. Lastly, the amount of users infected by adware (the prefered method by attackers) is almost the same as the obtained results for the last version of this study.

71.9% of comptuers and 76.5% of Android devices infected with malware are at high risk level

Regarding Android devices infected with malware, data in Figure 17 shows a higher presence of Trojans compared with adware, but still the amount of Android devices affected by malware is much smaller than the number of affected personal computers. Despite the growth of adware campaigns detected during the conducted research for the last version of this study, its level of incidence goes down once again, thereby falling below the results in the first semester of 2018 (-1.1 p.p).

FIGURE 18. RISK LEVEL ON THE HOUSEHOLD COMPUTER AND ANDROID DEVICES (%)



Base: PCs and Android devices hosting malware
Source: Household panel, ONTSI

According to the estimated level of risk for the different types of malware detected on the computers analysed by Pinkerton, the level of risk observed is high for 71.9% of PCs and 76.5% of Android devices. This shows an increase of +2.9 p.p. for PCs.

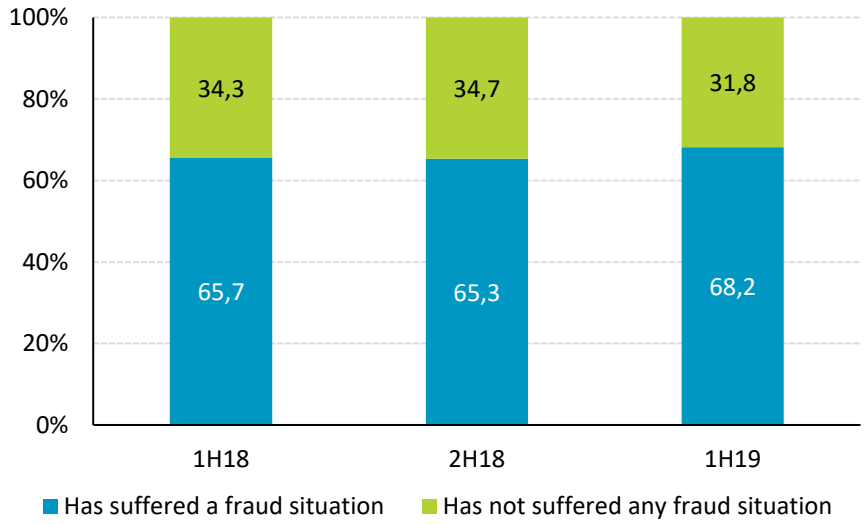
These data increments even more the current concern due to the hidden threat presented by malware (**FIGURE 13**, **TABLE 1** and **TABLE 2**).

1.4 Consequences of security incidents and user reactions

After suffering the consequences of a cybersecurity incident, users normally react showing willingness to learn how to prevent similar situations in the future. This involves introducing certain changes in their behaviour and adopting safer habits when browsing the Internet, as well as increasing the number of implemented security measures.

These changes on users' habits on the Internet after suffering a cybersecurity incident will be analysed in this section of the study.

FIGURE 19. EVOLUTION OF ONLINE FRAUD ATTEMPTS (%)



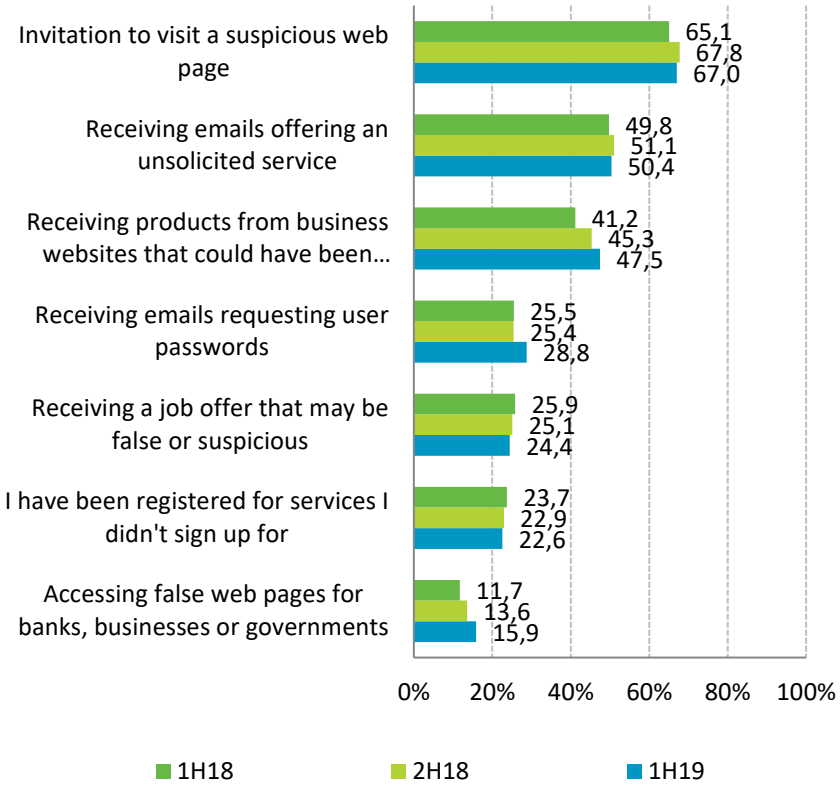
Base: All users
Source: Household panel, ONTSI

The percentage of Internet users who report having suffered some type of online fraud is over two thirds (68.2%) –whether effective or not- during the first semester of 2019. A rise of 2.9 p.p. is perceived when compared with the last version of this study.

It must be noted that the high effect of online fraud attempts is not only due to the lack of caution and/or knowledge of users, but also it must be taken into consideration that the technical aspects of the methods used by attackers are continuously evolving very fast, and so are social engineering campaigns (based on exploiting the lack of knowledge of the users and their excessive trust and interest), two points that make it difficult to implement protection measures and gain awareness regarding every single type of fraud that is being carried out on the Internet.

Fraud campaigns can adopt very different forms in order to achieve their goal and deceive their victims. The following figure will show the results of the study committed to analyse the main fraud campaigns according to Spanish Internet users.

FIGURE 20. EVOLUTION OF THE MANIFESTATION OF ONLINE FRAUD ATTEMPTS (%)



Base: Users who have experienced attempted fraud
Source: Household panel, ONTSI

The percentage of malicious intents to make users visit websites with potential malicious content (67%) and the receipt of unsolicited email or SPAM (50.4%) are still the most utilised means of online fraud attempt.

In the same way it is remarkable the raising tendency of the receipt of products from e-Commerce websites that could potentially be fraudulent sites (+2.2 p.p.), the access to banking/commerce/official administration entities phishing sites (+2.3 p.p.), and the receipt of emails requesting user passwords (+3.4 p.p.).

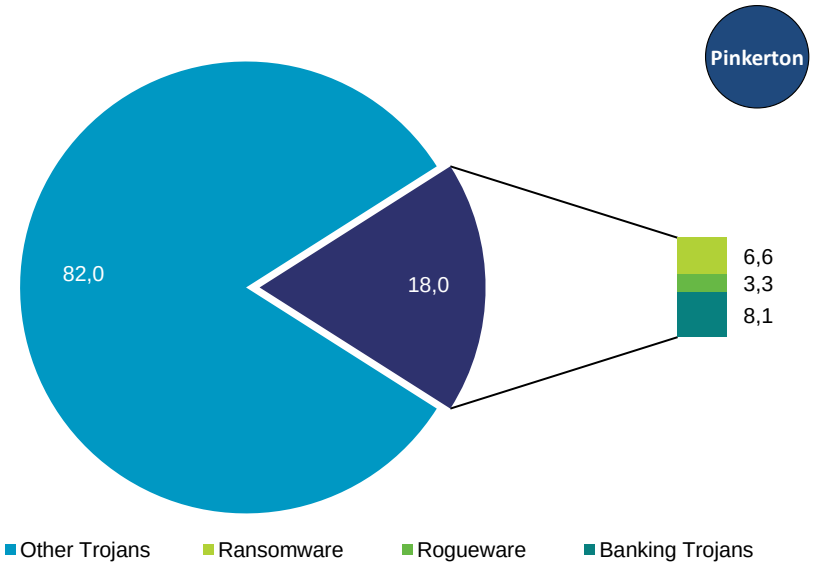
Most fraudulent websites are sent to the final user via the above-mentioned unsolicited emails or SMAP (**FIGURE 13**), although they can also reach the victim on social media or via SMS. Many of these fraud campaigns might be stopped by the security measures implemented by default on email and social media services, which explains that fake websites impersonating banking entities and e-Commerce sites (also known as phishing) lag behind other and more effective online fraud strategies. However, phishing could also be a threat that goes unnoticed for the user when the attacker achieves a perfect copy of the original website.

Attempts to deceive the user with surveys, fake prizes, discount coupons, gift vouchers, or any other ruse to steal the identity of a well-known brand or chain continue to be a successful means of attack. Victims usually facilitate personal information and are unaware that they are being subscribed to unsolicited offers and various services (50.4%), undesired publicity (SPAM), unwanted Premium SMS services (22.6%), installing unofficial and therefore non-secure –and potentially malicious- application, etc.

Type of malware analysed

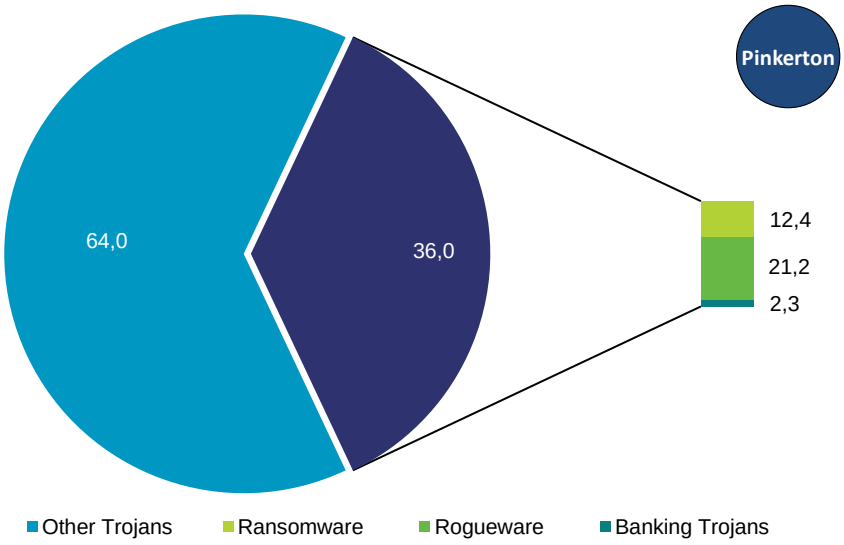
- Banking Trojans: malware that steals confidential information from customers of banks and/or online payment platforms.
- Rogueware: malware that makes victims think they have been infected by some kind of virus, getting them to pay a certain amount of money to remove it. The user is usually asked to purchase a false antivirus program, which turns out to be the malware itself.
- Ransomware: malware that installs itself on the system and takes it 'hostage', then asks the user to pay a monetary amount as a ransom.

FIGURE 21. BANKING TROJANS, RANSOMWARE AND ROGUEWARE ON THE HOUSEHOLD COMPUTER (%)



Base: Computers with Trojans detected on PC
Source: Household panel, ONTSI

FIGURE 22. BANKING TROJANS, RANSOMWARE AND ROGUEWARE ON ANDROID DEVICES (%)



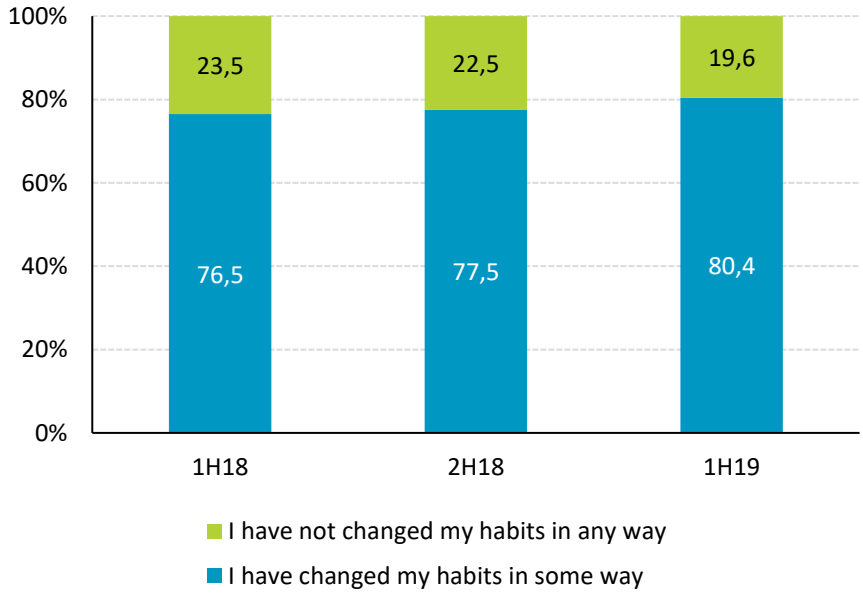
Base: Android devices with Trojans detected
Source: Household panel, ONTSI

Household computers are much more vulnerable to banking Trojan. The fact that malware developers are following this trend might be related to the old habit of using personal computers to buy things online, adminístrate banking accounts, as well as other online monetary operations, although mobile devices are gaining popularity for this kind of activities at the expense of PC use. Besides, multiple members of the family usually use the same computer –sometimes even an administrator account- instead of creating different profiles for each user. This could be considered a particularly dangerous habit since each of these users has different risky habits on the Internet that go unnoticed for the rest of them, which means those who don't know about the risky behaviours adopted by someone else do not take any precautions when using the device.

Rogueware is the prefered attack in the case of Android devices (21.2%). This kind of malware tries to deceive victims into thinking that they have been infected by some kind of virus and making them install a malicious application that turns out to be the malware itself.

FIGURE 23. EVOLUTION OF REACTIONS AFTER HAVING EXPERIENCED A SECURITY INCIDENT (%)

Four out of five Spanish Internet users change their prudent habits after experiencing a security incident

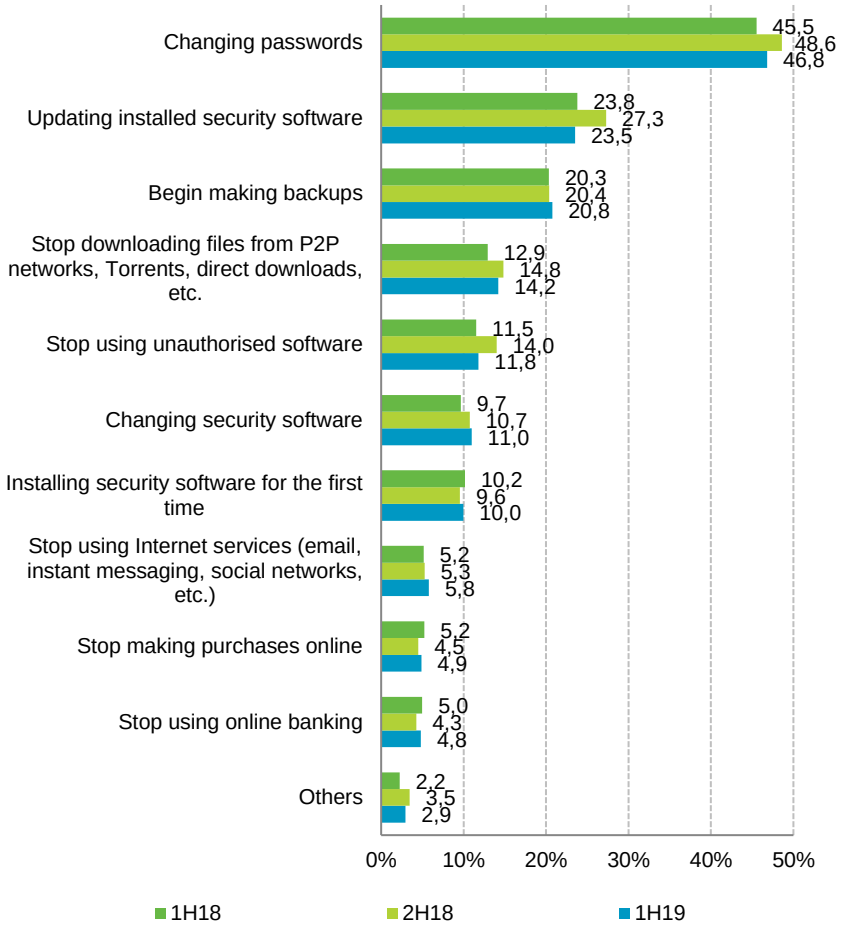


Base: Users who have experienced a security incident
Source: Household panel, ONTSI

During the first half of 2019, data show a new increase and a positive growth in the adoption and modification of safe habits by users and a new tendency to use security measures after having experienced a security incident (+2.9 p.p. compared with 2S18).

However, in spite of the progressive increment in the number of people using safer habits when browsing the Internet after becoming the victim of a cybersecurity incident, efforts should focus on making Internet users opt to implement secure habits that prevent them from becoming a target of cyberattacks, instead of the individual gaining awareness about the problem only after the negative consequences have occurred.

FIGURE 24. EVOLUTION OF CHANGES IN HABITS AFTER HAVING EXPERIENCED A SECURITY INCIDENT (%)



Base: Users who change their habits after experiencing a security incident
Source: Household panel, ONTSI

During the first semester of 2019 a small decrease in the habit of changing passwords was detected (-1.8 p.p). During the research carried out for the last version of this study there was an increse in the number of users who reported having updated their passwords, which could be a consequence of the multiple information leaks that took place throughout that period of time. These leaks were reported on the news and social media, thus getting the information to the general public and raising awareness. Having changed their passwords not long ago could be a possible explanation of the previously mentioned decrease in the habit of changing passwords, since users might have considered it not to be necessary at the moment of taking the survey. However, it is important to remember that changing passwords periodically –regardless of whether the user has been a victim or not of a cyberattack- and to not use the same password for different Internet services are key habits in order to keep our personal data and information safe.

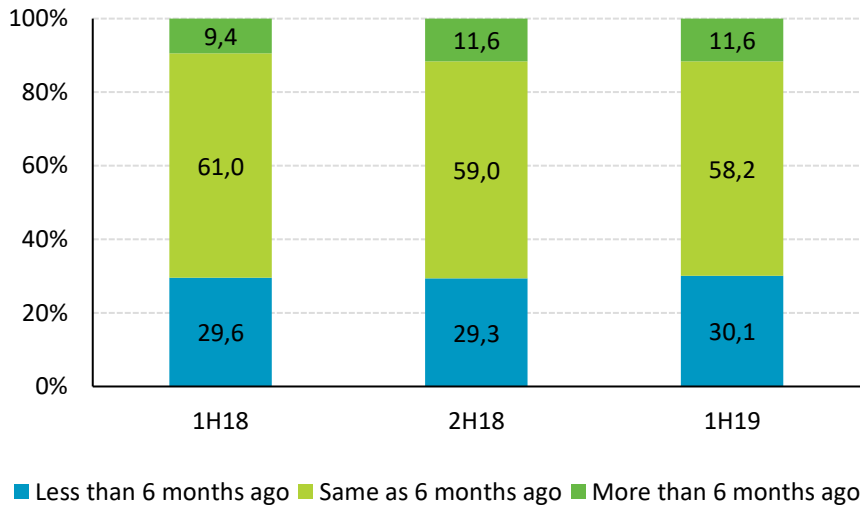
In the second place there is the updating of the already installed security software (23.5%), which is a particularly important habit if the user aims to keep all devices free from malwares, since the latter are under continuous development. Despite the importance of this habit, it has experienced a rather significant downturn that could lead to new security breaches.

The data related to making backups of the system have kept stable (20.8%), although this practice seems to be steadily increasing. However, although it is highly recommended to make security backups from time to time in order to prevent data loss in the case of a security incident, barely 1 in every 5 users actually makes security backups after suffering a cybersecurity incident (44.3% of users consider security backups an unnecessary practice (**FIGURE 5**).

1.5 Trust in the digital environment in Spanish households

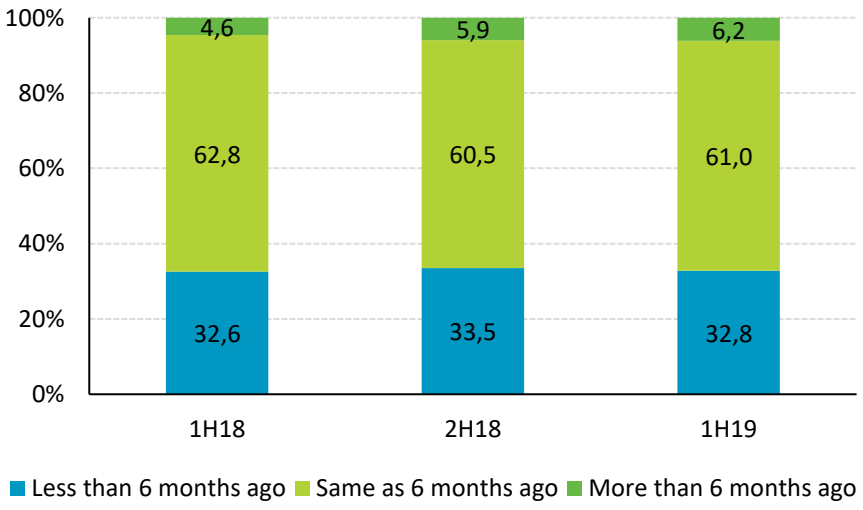
The last part of the study focuses on how users assess the risks and dangers of the Internet, their opinions and considerations on their own responsibility for security, and overall trust in the Internt.

FIGURE 25. EVOLUTION OF THE PERCEPTION OF THE NUMBER OF SECURITY INCIDENTS (%)



Base: all users
Fuente: Household panel, ONTSI

FIGURE 26. EVOLUTION OF THE PERCEPTION OF THE SEVERITY OF SECURITY INCIDENTS (%)

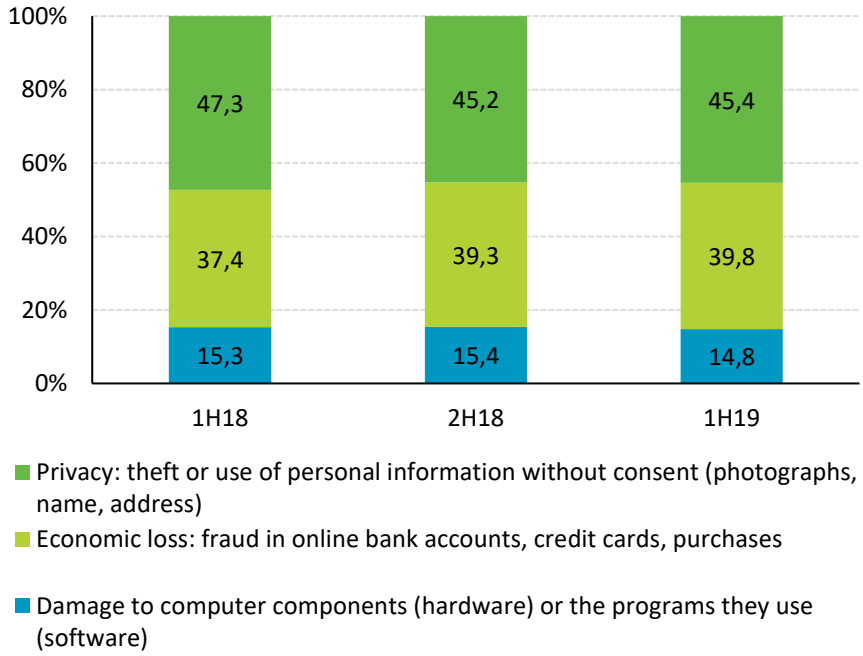


Base: all users
Fuente: Household panel, ONTSI

Data has not varied much compared to previous versions of this study, which means that surveyed Internet users consider that the perceived number of incidents and their severity are similar. Among surveyed users, 11.6% believe that the number of incidents has increased, and, as for perception of the seriousness of the incidents, 6.2% believe that it has lessened.

However, these data do not turn out to be possitive when compared with the obtained data regarding the real state of the devices in relation to malware (**FIGURE 14** and **FIGURE 15**), the level of risks of these devices (**FIGURE 18**) and the lack of awareness of users regarding this kind of incidents (**TABLE 1** and **TABLE 2**).

FIGURE 277. EVOLUTION OF THE PERCEPTION OF RISKS ON THE INTERNET (%)



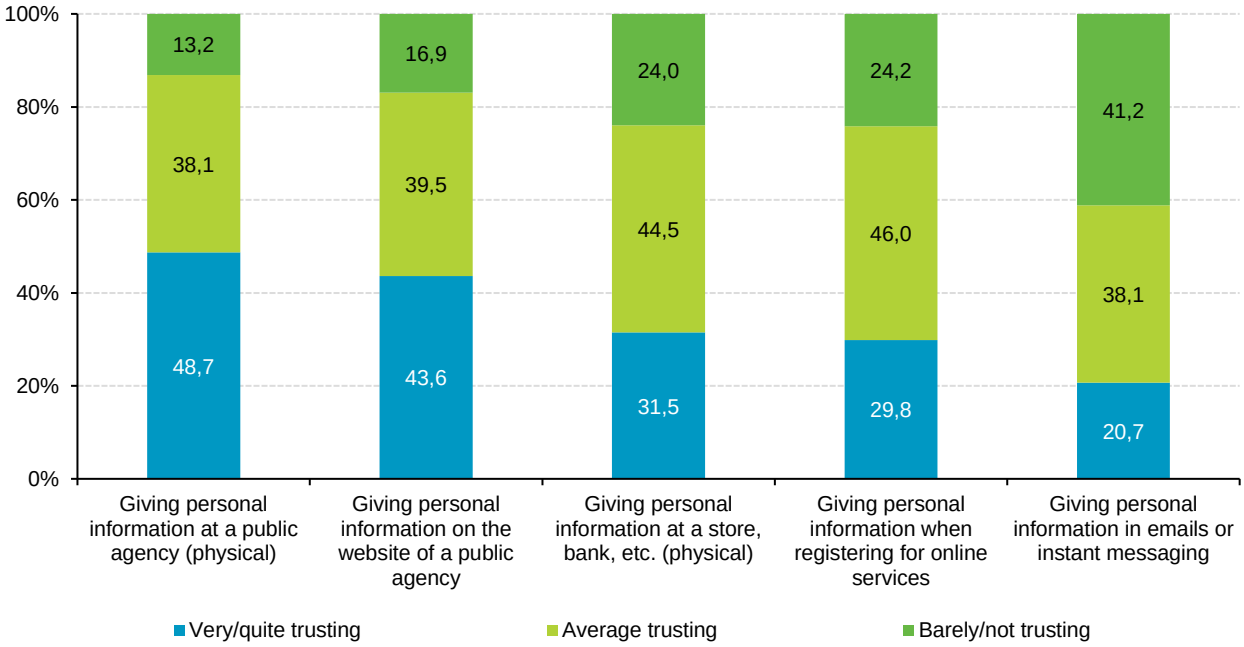
Base: all users
Source: Household panel, ONTSI

Figure 27 shows that users still believe that the most dangerous risk of the Internet is the loss of privacy due to theft or unauthorised use of personal information, followed by economic loss caused by an online banking service fraud, credit cards, online purchases, etc.

The perception of risks on the Internet has mostly remained consistent throughout the year.

To delve deeper into this aspect, below we analyse the trust generated in the user by providing personal data in different situations.

FIGURE 28. LEVEL OF TRUST IN PROVIDING PERSONAL DATA (%)

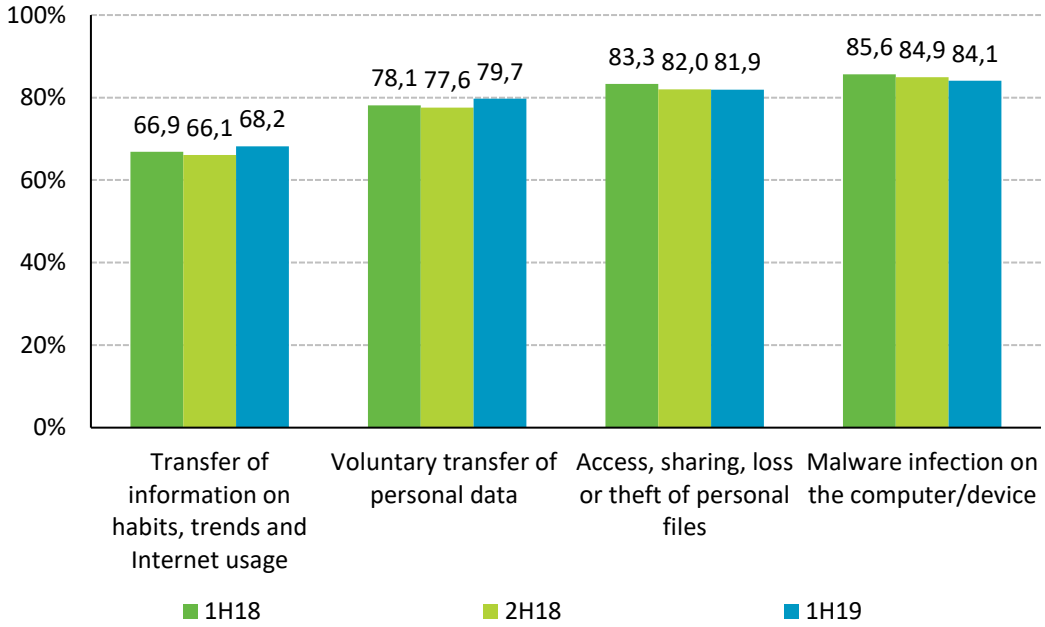


Base: all users
Source: Household panel, ONTSI

Despite numerous efforts made by attackers to collect personal and/or private information from Internet users, 41.2% of the latter group are very suspicious when asked for this kind of information on an email or instant messaging services. However, the percentage of users who do not trust giving private information when registering for online services is significantly lower (24.2%).

On the other hand, it should be noted the high percentage of users who trust public bodies when giving personal information, with a relatively small difference between physical offices (48.7%) and e-Offices (43.6%). The similarity between the percentages of users who trust giving personal information at a physical office and e-Offices is caused by how much time users save by using online services, since e-Offices are much more convenient than personally going to the physical office.

FIGURE 29. EVOLUTION OF THE ASSESSMENT OF DANGERS POSED BY THE INTERNET (%)



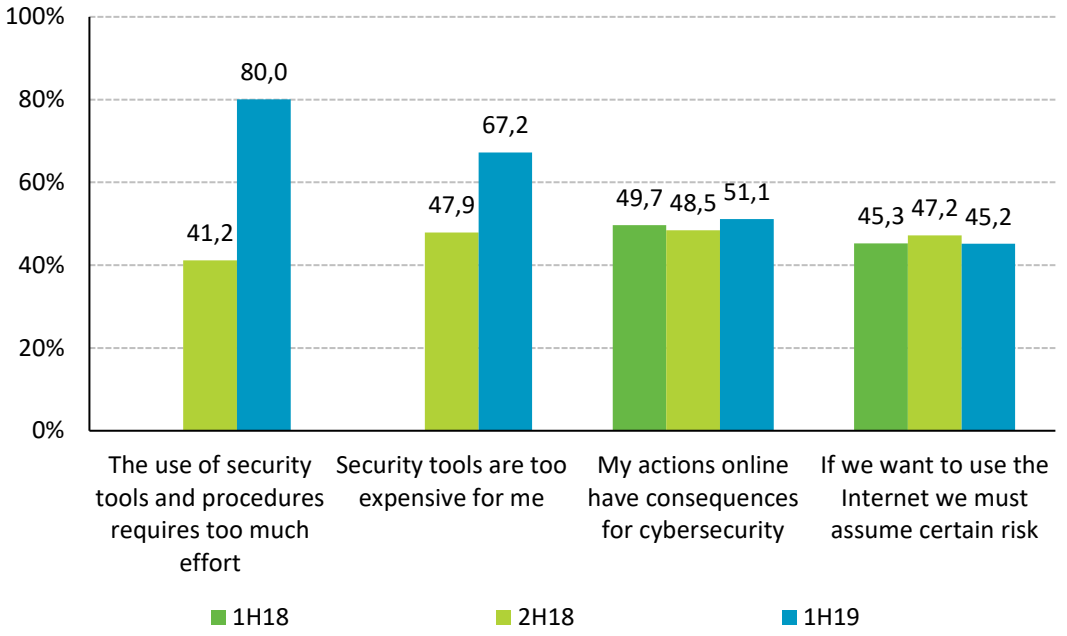
Base: all users
Source: Household panel, ONTSI

Spanish Internet users believe that the risk associated with transferring information on habits, trends and Internet usage is higher than in previous studies (+2.1 p.p.). Thus, it could be inferred that users are more worried about the data use and the possibility of theft of personal data as a consequence of a cyberattack to the organisation storing those data. On the other hand, users continue to give the risk of malware infection the first position among their worries, although after establishing a comparison between this and previous semesters data, a slight decrease in the number of users worried about this kind of risk can be appreciated (-0.8 p.p.).

Given the general perception of users regarding the different types of risks associated to Internet use laid out in this study is a round 80% for most of them (except for giving information about habits, trends and Internet use, a risk that ranks approximately 10 p.p. below the others) it could be stated that the general awareness is high.

A significant amount of users are aware of the risks they take when using the Internet and of the consequences surrounding the implementation of security measures to prevent those risks.

FIGURE 30. EVOLUTION OF RESPONSIBILITY IN TERMS OF INTERNET SECURITY (%)[2]



Base: all users
Fuente: Household panel, ONTSI

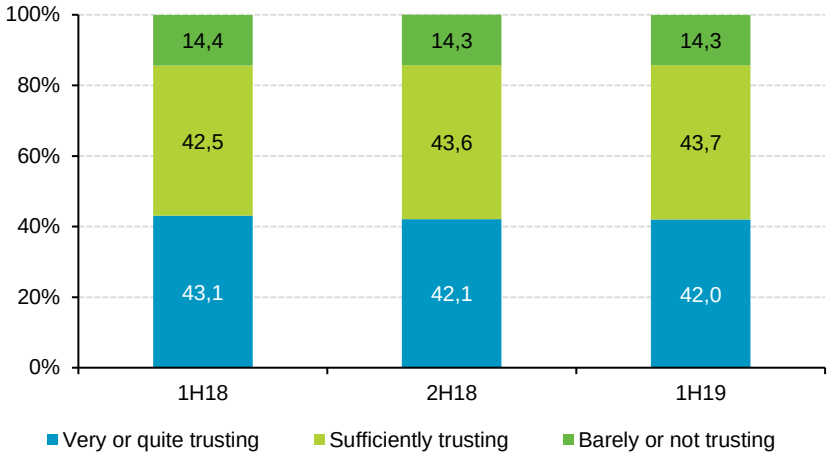
Among surveyed users, 51.1% report being aware of the importance and consequences their actions have on cybersecurity, a modest increase that points to an acquisition of good habits already shown on **FIGURE 24**. Also, among these Internet users 45.2% of them accept taking some risks in order to fully enjoy Internet services. This percentage has decreased -2 p.p. compared with the last semester.

Also, users have significantly changed the way they think about the costs of security tools (67.2% of them considered these tools to be too expensive) and how difficult it is to use them (4 out of 5 users believe these tools to require too much effort in order to use them correctly). However, this is a preconceived and mistaken idea since there are plenty of free security tools that offer good protection. In addition to this, lots of these tools usually include a *wizard* (an assistant feature) that provides information or even a guided process for the correct installation and configuration of the software.

These data, along with those referring to the reasons why users do not implement security measures –thinking of them as non-necessary, as well as the lack of knowledge about them- (**FIGURE 5**) presents a rather worrisome landscape which is strengthened by the level of risk faced by users' devices (**FIGURE 18**).

[2] Options "The use of security tools and procedures requires too much effort" and "Security tools are too expensive for me" are analysed for the first time in the second half of 2018.

FIGURE 31. EVOLUTION OF THE LEVEL OF TRUST ON THE INTERNET (%)



Base: all users
Fuente: Household panel, ONTSI

Figure 31 shows that from the first semester of 2018 to the second half of 2019, the percentage of users who are very or quite trusting when using the Internet has slightly decreased (-1.1 p.p.). This is not something negative but it must be analysed along with previously explained data, thus confirming the rendered conclusions of **FIGURE 14** and **FIGURE 15**: as users perceive a higher risk derived from Internet use, distrust rises too.

Consciousness-raising and risks assesment by Internet users are variables showing positive data regarding cybersecurity. However, there are still critical weak points, such as the ability to recognise the threats.

The "*Study on Cybersecurity and Trust of Spanish households*" was prepared by the following team of the Spanish National Observatory of Telecommunications and the Information Society (ONTSI) of Red.es:

Management: Alberto Urueña López
Equipo técnico:
Raquel Castro García-Muñoz
Santiago Cadenas Villaverde
Jose Antonio Seco Arnegas

Thanks for collaborating in this study goes to:

HISPASEC

GfK

Thanks as well to the following individuals for their collaboration:

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Edificio Bronce
Plaza Manuel Gómez Moreno s/n
28020 Madrid. España

Tel.: 91 212 76 20 / 25
Twitter: @ONTSI
www.red.es