STUDY ON CYBERSECURITY AND TRUST IN SPANISH HOUSEHOLDS

n.1 SECURITY MEASURES

n.2 BEHAVIOUR HABITS IN BROWSING AND INTERNET USE

n.3 SECURITY INCIDENTS

n.4 CONSEQUENCES OF SECURITY INCIDENTS AND USER REACTIONS

n.5 TRUST IN THE DIGITAL ENVIRONMENT IN SPANISH HOUSEHOLDS

1. STUDY ON CYBERSECURITY AND TRUST IN SPANISH HOUSEHOLDS

Red.es, in collaboration with Hispasec Systems 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 improve their habits 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.

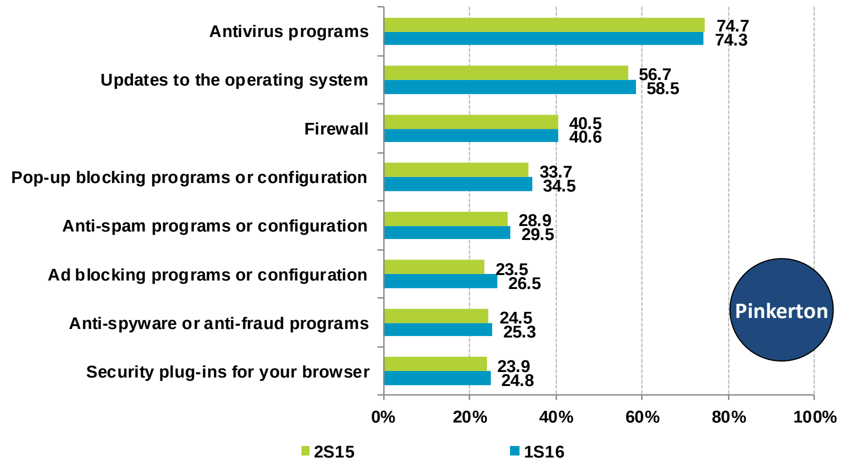
The data reported were obtained from online surveys given to households included in the study sample, while the real data was obtained using Pinkerton software to analyse their systems, collecting data about the operating systems being run and their update status, and which security tools were currently installed. Pinkerton also detects the presence of malware on computers and mobile devices by using a combination of 50 antivirus engines.

1.1 Security measures

The presence of security measures on computers and devices (home computers and Android devices) is one of the basic pillars of information security.

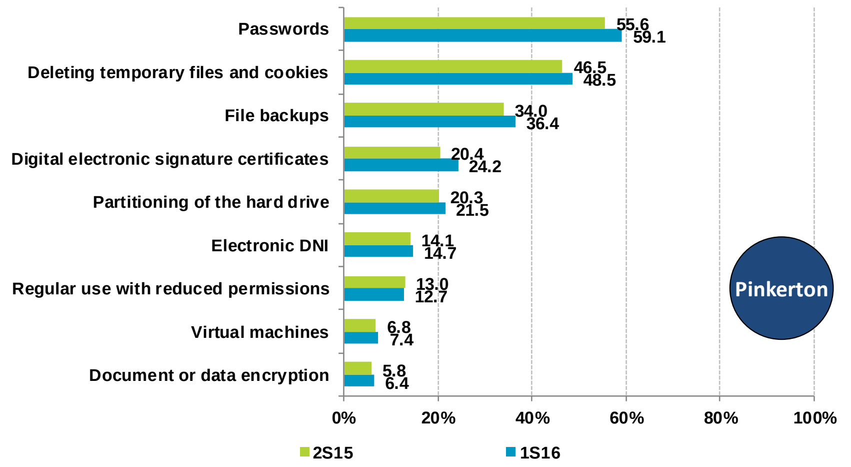
The usage trends for security measures on home computers that had been observed in the previous analyses were confirmed for the period of January to June 2016.

FIGURE 1. EVOLUTION OF REPORTED USE OF AUTOMATABLE SECURITY MEASURES ON THE HOUSEHOLD COMPUTER (%)



Base: PC users
Source: Household panel, ONTSI

FIGURE 2. EVOLUTION OF REPORTED USE OF NON-AUTOMATABLE SECURITY MEASURES ON THE HOUSEHOLD COMPUTER (%)



Base: PC users
Source: Household panel, ONTSI

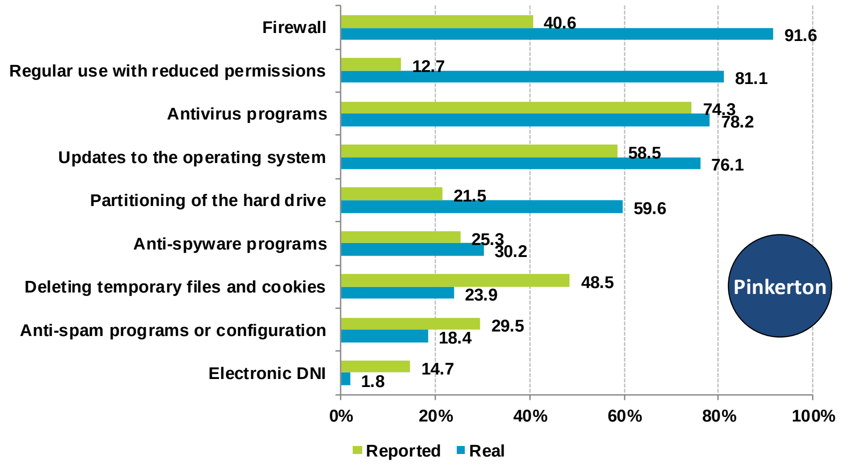
Thus, the main reported security measures are using antivirus software and a firewall and updating the operating system, among automatable measures, and using passwords and deleting temporary files and cookies, among the non-automatable ones.

In the current period a slight increase in the reported use of security measures can be seen. This is mainly in the use of electronic signature certificates (+3.8 percentage points), passwords (+3.5 p.p.), backup copies and deleting temporary files (+2 p.p.).

There is also an almost negligible decrease in the use of antivirus software (-0.4 p.p.) and the use of a user account with reduced permissions (-0.3 p.p.).

The greatest disparities between actual data and those reported by users are in the regular use of user accounts with reduced permissions, use of firewall software, and in the hard disk partition.

FIGURE 3. REPORTED VS REAL USE OF SECURITY MEASURES ON THE HOUSEHOLD COMPUTER (%)



Base: PC users
Source: Household panel, ONTSI

The main security measures, according to actual use detected by Pinkerton, are firewalls (91.6%), the regular use of the computer with a user account with reduced permissions (81.1%) and antivirus software (78.2%).

Large contrasts regarding use reported by users can be seen. In most cases, as can be seen, they are positive since the actual presence of such security measures is higher than that reported by the user.

Such is the case with firewalls, possibly due to the inclusion of these solutions in operating systems and security suites[1], as a result of which the existence of this tool goes unnoticed by a large number of users (reported usage is 51% below real use).

The same occurs with regular computer use with a user account with reduced permissions: Pinkerton detects real usage at 81.1% while only 12.7% of Internet users report it. The latest operating system versions establish a user with limited permissions by default, and these 68 percentage points of difference confirm that the user does not usually realise this since it is not necessary to have administrator permissions for the normal use of a computer.

Continuing with these reasons, the discrepancy in the data concerning partitioning hard disk space can be seen as positive. It is common for computers sold with a preinstalled operating system to include a hidden recovery partition. This, although it has no direct impact on user data, can be a great help when restoring or reinstalling the operating system. This is one reason why it can not be considered positive that 38 p.p. of users are unaware of its existence.

Also to be considered are the inclusion of security measures in the

USE OF SECURITY MEASURES ON THE HOUSEHOLD COMPUTER (REAL DATA)

91.6%

WITH FIREWALL SOFTWARE

81.1%

WITH REDUCED PERMISSIONS

78.2%

WITH ANTIVIRUS SOFTWARE

[1] A security suite is a set of security-related programs that, along with traditional antivirus software, can include firewalls, anti-spam tools, anti-spyware tools, parental control, etc.

newest versions of operating systems and the increased use of online or cloud services, in many cases as a replacement for traditional tools (anti-spam filters of main e-mail service providers, ad blockers and fraudulent website blockers on browsers, etc.).

REGULAR USE WITH REDUCED PRIVILEGES (REAL DATA)

99.7%

WITH REDUCED PERMISSIONS IN WINDOWS 8

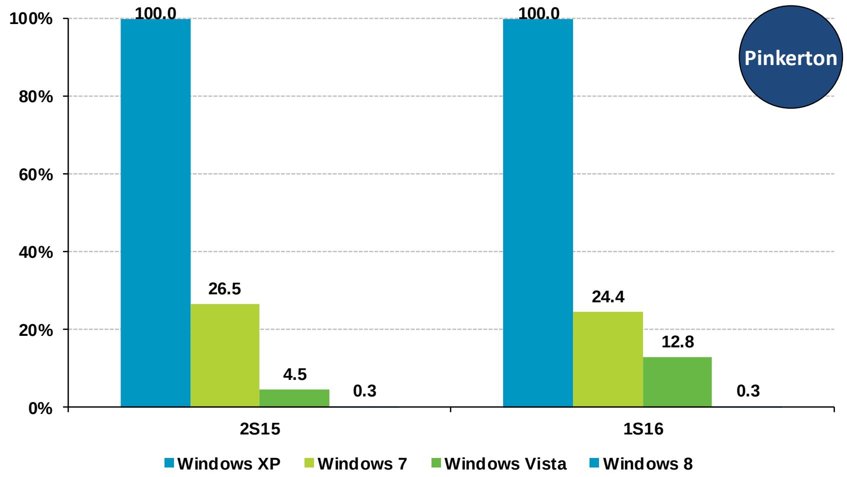
75.6%

WITH REDUCED PERMISSIONS IN WINDOWS 7

87.2%

WITH REDUCED PERMISSIONS IN WINDOWS VISTA

FIGURE 4. EVOLUTION OF ACTUAL ADMINISTRATOR PROFILE USE IN MICROSOFT WINDOWS OPERATING SYSTEMS (%)



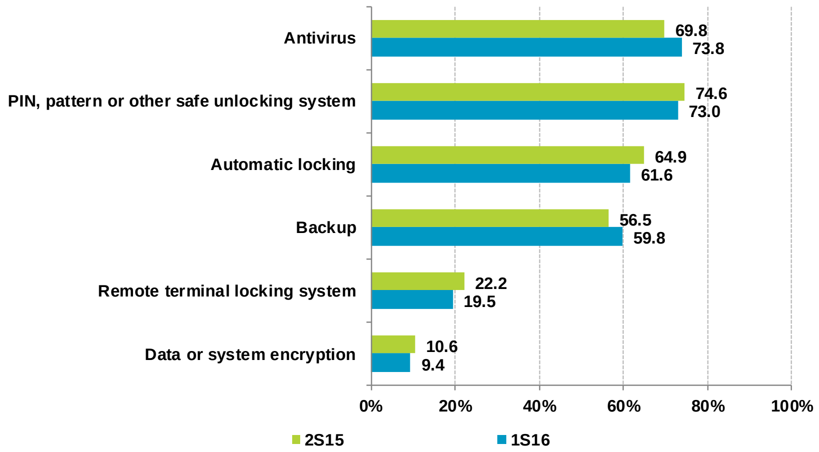
Base: Microsoft Windows users
Source: Household panel, ONTSI

As previously mentioned, by default Microsoft establishes a user account with reduced permissions in the latest versions of its operating system.

This security measure can be seen in the data obtained by Pinkerton regarding the real level of privileges of user accounts on analysed computers. Thus, a large majority of users surveyed regularly use an account with reduced permissions in Windows Vista (87.2%), Windows 7 (75.6%) and Windows 8 (99.7%).

In view of the previous results we should explain that some Windows 10 operating systems may have been identified as previous versions. This is due to Microsoft's updating process, which allows Windows 10 to be installed over a version of Windows 7, 8, or 8.1, keeping files from the previous version of the operating system in order to facilitate a possible roll-back to the previous version.

FIGURE 5. EVOLUTION OF SECURITY MEASURES ON ANDROID DEVICES (%)

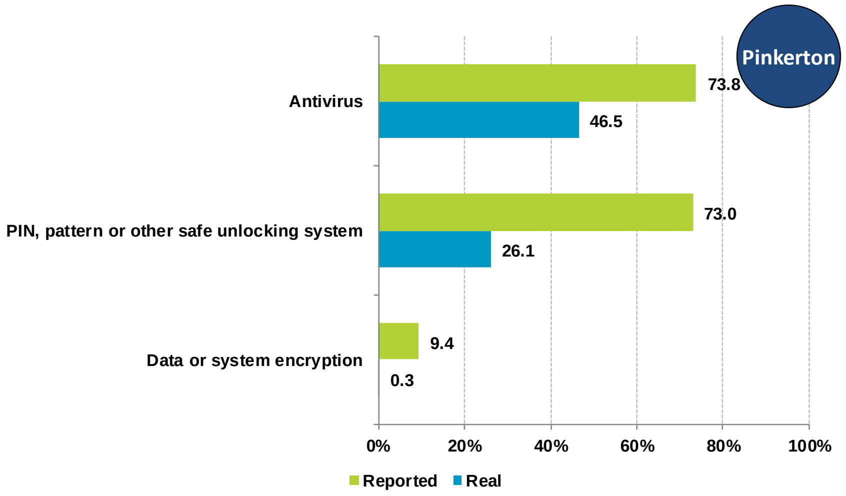


Base: Android device users
Source: Household panel, ONTSI

The security measures most used on Android devices, according to user statements, are antivirus software (73.8%), secure unlocking systems via PIN codes, patterns, fingerprint detection, etc. (73%), and automatic locking of devices after a period of inactivity (61.6%). The use of antivirus software (+4 p.p.) and backup copies (+3.3 p.p.) has also increased during this period.

However, encryption software is being used less and less, with only 9.4% (-1.2 p.p. with respect to the previous period). This tool may prevent third parties from accessing the data on the device in the event of loss or theft.

FIGURE 6. REPORTED VS REAL USE OF SECURITY MEASURES ON ANDROID DEVICES (%)



Base: Android device users
Source: Household panel, ONTSI

On the other hand, the real data obtained with Pinkerton once again reveals discrepancies regarding the reported data.

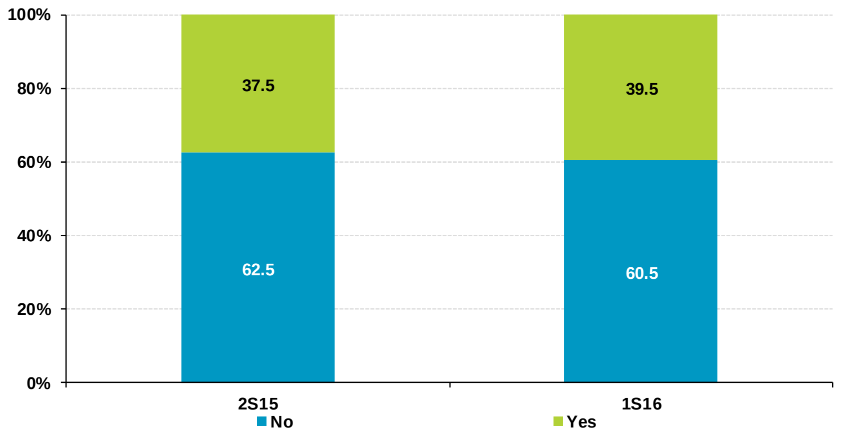
The most notable difference is in the Android device's secure unlocking systems, of which 73% of users claim to use, while Pinkerton finds that only 26.1% of the devices analysed have a system of this type activated. It can be concluded from this data that the user believes any unlocking system to be secure. However, for an unlocking system to be secure it must require a password, numerical code (PIN), swipe pattern, or use a sensor to detect some biometric parameter (fingerprints, for instance), etc. so that only someone who knows the password, or who has the unique physical characteristics required by the biometric sensor, can access the device. Other unlocking systems such as the ones based on a simple swipe across the screen (slider) or pushing a button are not secure, as they allow anyone with access to the device to unlock it.

Another important difference of 27.3 p.p. can be seen in the use of antivirus software. Only 46.5% of the devices analysed by Pinkerton have this type of software installed, while 73.8% of users claim to have antivirus software on their Android device. This entails a large number of users who trust that this protection is present, exposing them to malware threats.

1.2 Behaviour habits in browsing and Internet use

The behaviour and security habits adopted by Spanish users when they access the Internet are indicative of their level of caution regarding the dangers of the digital world.

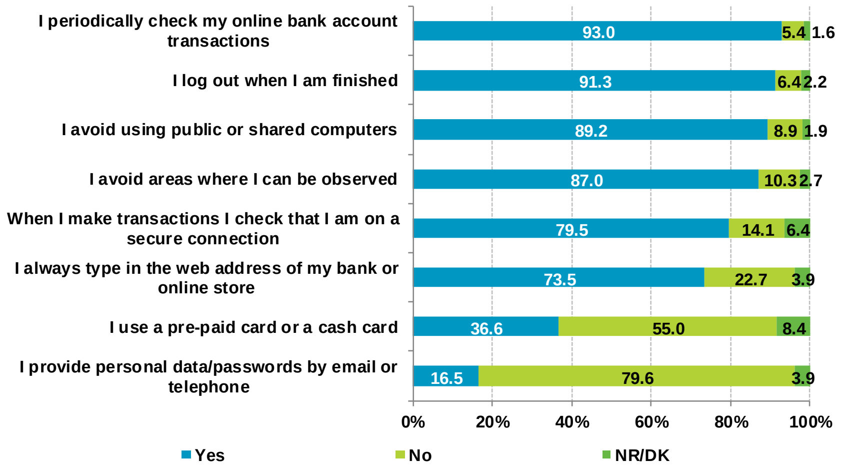
FIGURE 7. EVOLUTION OF THE KNOWING ADOPTION OF RISKY BEHAVIOURS (%)



Base: all users
Source: Household panel, ONTSI

During the first half of 2016 the number of Internet users reporting that at times they knowingly engage in behaviour that entails security risks while browsing or using Internet services increased by 39.5% (+2 p.p.). This fact can be very relevant to, if not decisive in, the occurrence of security incidents.

FIGURE 8. CAUTIOUS BEHAVIOUR RELATED TO ONLINE BANKING AND E-COMMERCE (%)



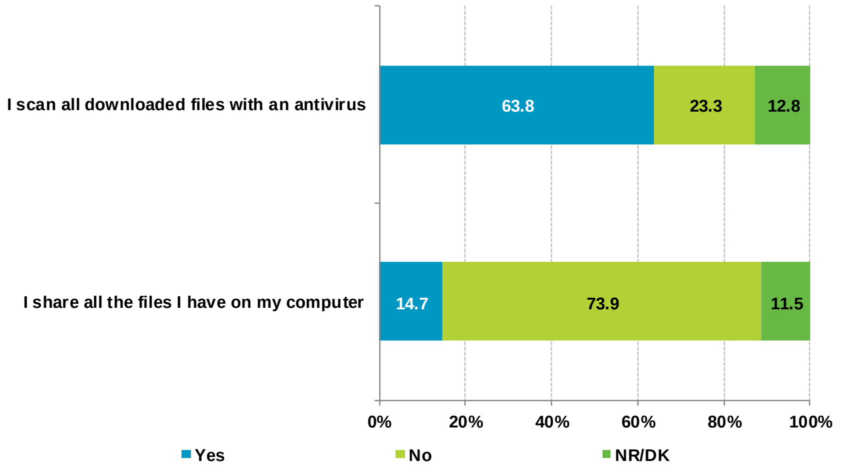
Base: users of online banking and/or e-commerce
Source: Household panel, ONTSI

One in three users takes advantage of prepaid cards or cash cards offered by banks as a security measure to make online purchases.

This is not true in the context of online banking services and e-commerce, where most users are cautious and report good usage habits. This was generally observed to be the case for more than 73% of Internet users.

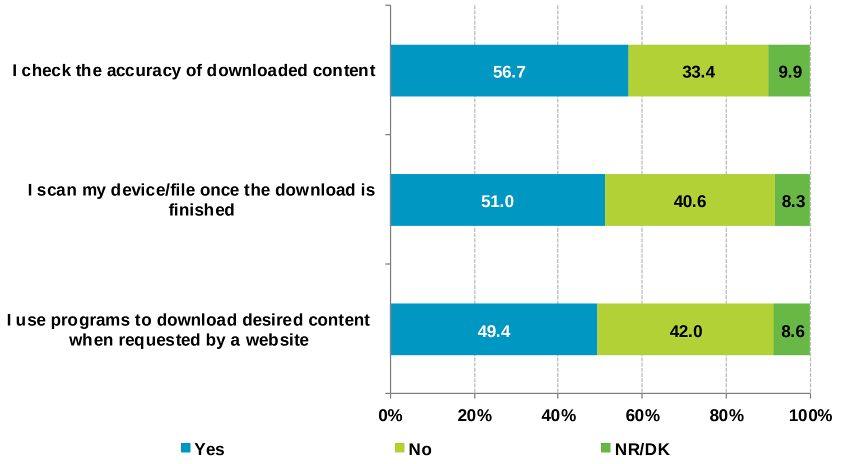
Only the use of prepaid or e-purse cards to make payments online has a lower acceptance rate among Spanish users. Only 36.6% consider this option despite the fact that most banks offer them among their products. However, this is a highly recommended measure that protects the user in several ways. It helps prevent real banking data from being compromised when the card is used for online transactions. In addition, if you become a fraud victim from an online payment, you can minimise the possible economic impact by having a limited balance (it is advisable to only top up with the amount needed to make the payment).

FIGURE 9. P2P NETWORK DOWNLOADS (%)



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

FIGURE 10. INTERNET DOWNLOADS (%)



Base: all users
Source: Household panel, ONTSI

Internet downloads are one of the main ways computers and devices get infected. Although malware is usually hidden in file launchers, cracks, serial number generators, etc.[2], it also often

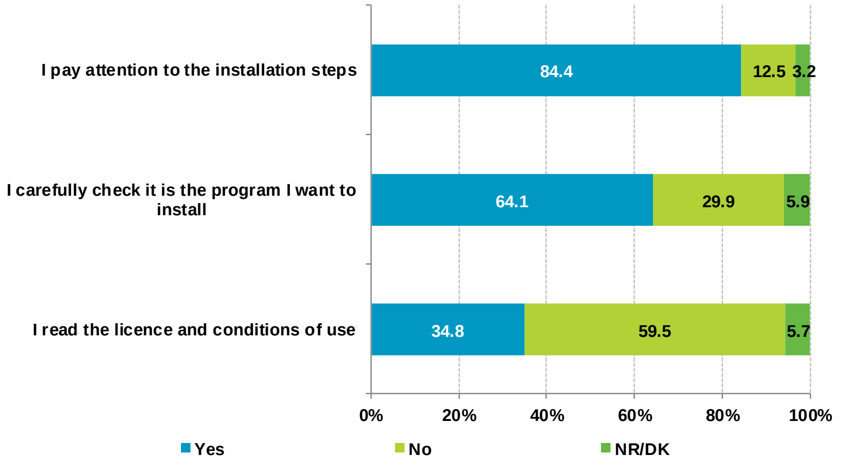
[2] Activators and cracks are programs used to modify files (usually to run legitimate software or register an operating system), the reason why antivirus software marks them as potentially dangerous. This means that the user who

simulates other known software, multimedia files (videos and photos), or any other type of harmless visible file in order to spark user interest to get the user to open or run the file, thus unleashing the infection on the machine.

Many users are aware of this fact, evident from their good habits when downloading files from the Internet. Nearly 64% of users of P2P networks do not open downloaded files if they are not sure they have been scanned, just like half (51%) of users do for files that they download directly. Also, 56.7% of users report checking the accuracy of downloaded content (download site, file type, hash[3], etc.) before opening it.

Another danger, which sometimes goes unnoticed, is the dissemination of information and data of a private nature. In many cases it is the users themselves who reveal it or facilitate access to it, for example, by publishing it on social networks or sharing all the files of their computer through P2P networks (as reported by 14.7 % of panellists).

FIGURE 11. INSTALLATION OF PROGRAMS ON THE HOUSEHOLD COMPUTER (%)



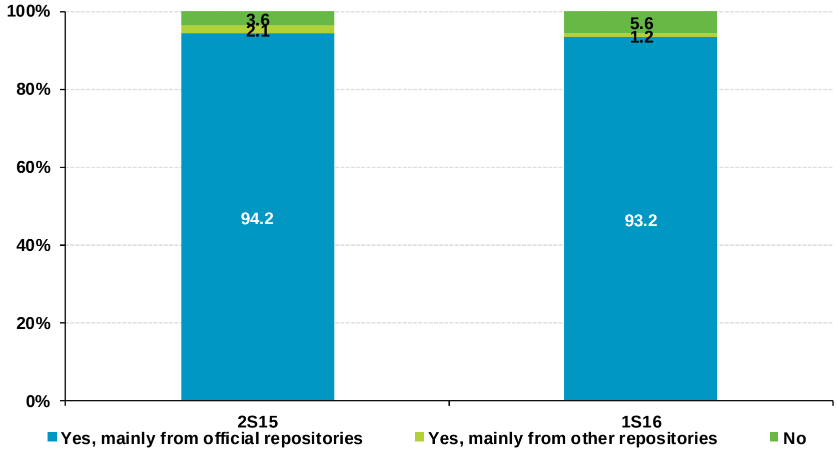
Base: all users
Source: Household panel, ONTSI

Before installing a program or application on the computer, 64.1% of users report carrying out a thorough check to make sure that it is the desired program. Once the process has started, 84.4% said they pay attention to the steps of the installation, although only one in three Spaniards read the license sheet and the conditions of use.

uses such programs to run a copy of non-legitimate software without restrictions ignores the antivirus warnings or even disables the software if it blocks the application. In addition, it is the users themselves who want to run these programs, without the need for deception or persuasion by third parties. Malware developers are aware of this so they often hide their malicious code in such programs.

[3] The hash of a file is an alphanumeric string of normally fixed length that represents a summary of all the information contained in said file. It is used to check the integrity of the files since a change in a simple character implies obtaining a completely different hash.

FIGURE 12. EVOLUTION OF APPLICATION DOWNLOADS ON ANDROID DEVICES (%)



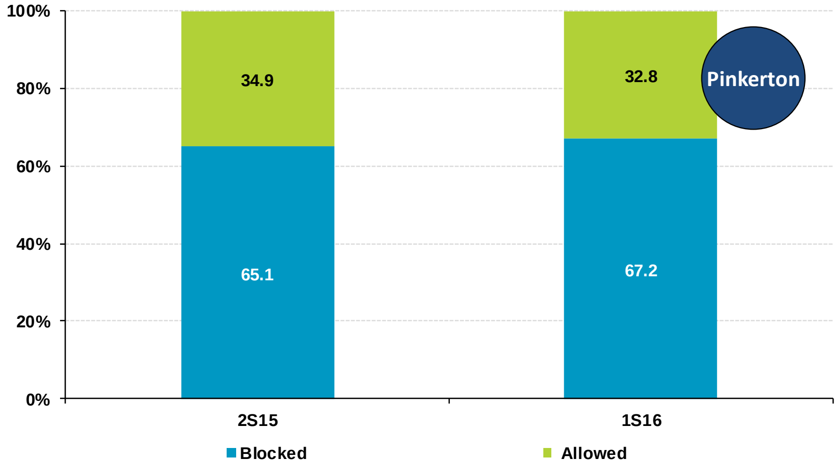
Base: Android device users
Source: Household panel, ONTSI

Although it has decreased by 1 p.p., the vast majority of Android device users (93.2%) state that they mainly use official repositories to download applications.

There are many alternative markets that allow the free download of applications. However, we are concerned with analysing the applications that are uploaded to their systems, to detect fake applications or those containing malware.

Therefore, using official markets or repositories is a good cautious habit among users to avoid problems of malware or security on their mobile devices.

FIGURE 13. EVOLUTION OF THE STATUS OF UNKNOWN SOURCES (%)



Base: Android device users
Source: Household panel, ONTSI

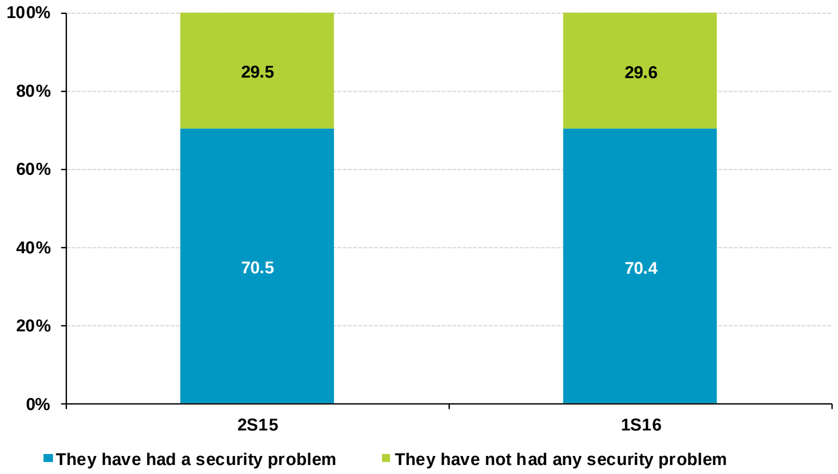
Android devices whose analysis reveals that they are configured to block the installation of applications from unknown sources has increased by 2 p.p.

On the other hand, it was observed that despite mainly preferring to use official repositories, almost one third of users could have downloaded and installed applications from third-party sources on some occasion, with the potential risk this entails.

1.3 Security incidents

This section analyses which security incidents occurred and to what degree among Spanish users, both on their home computers and Android devices.

FIGURE 14. EVOLUTION OF SECURITY INCIDENTS (%)



Base: all users
Source: Household panel, ONTSI

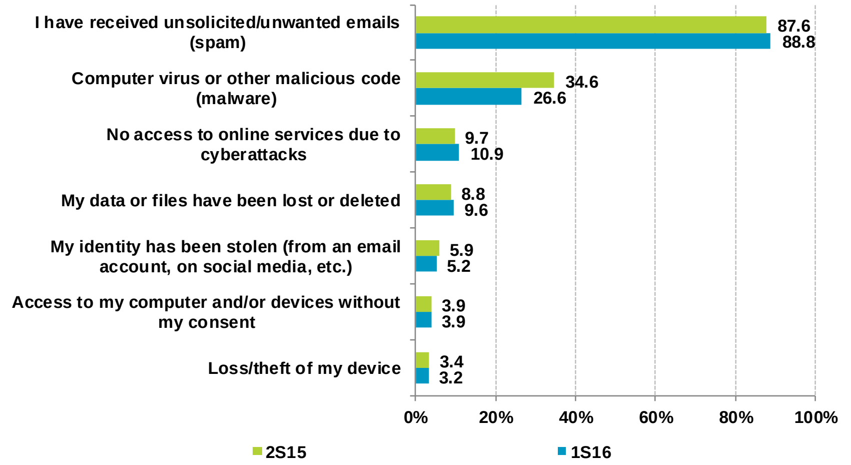
Security systems are constantly evolving towards more robust and effective models. However, we must understand that they are not infallible or impassable and ultimately depend on the user, who could neglect the necessary updates, warnings or security alerts, and even disable them to perform specific actions that these systems block. For these reasons there is always a possibility of incidents occurring despite security measures being applied to the system and good careful usage habits.

Thus, in the first half of 2016, 70.4% of users report having experienced some kind of security incident. This value has remained consistent since the last half of 2015.

Malware is the name for any malicious program that aims to infiltrate computer equipment 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.

FIGURE 15. EVOLUTION OF CLASSIFICATION OF SECURITY INCIDENTS (%)



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

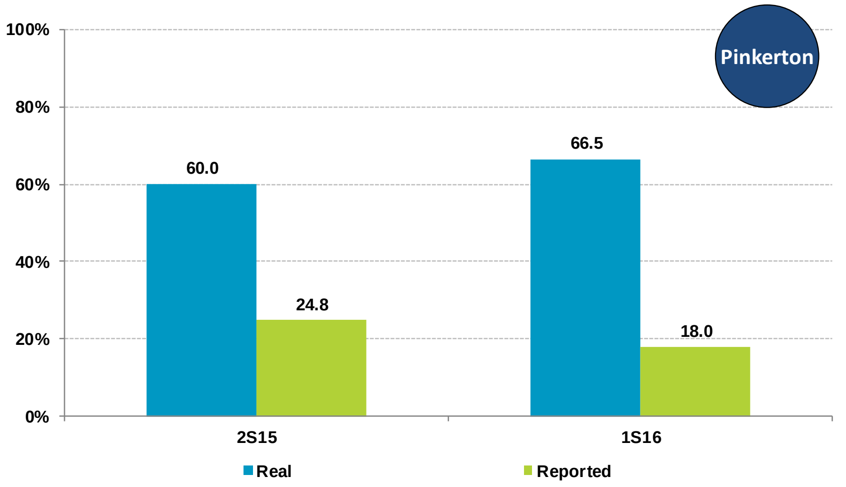
Spam campaigns continue to rank first in the list of incidents perceived by users (88.8%). It is quite logical since the main objective of these e-mails is to get the attention of users.

Malware and virus incidents have significantly decreased (8 p.p.) during the first half of 2016. An explanation can be found in the fact that the goal of many types of malware is to go undetected by both antivirus software and the user.

Furthermore, it is interesting to note that, as seen below, the number of actual infections increases both on home computers and among Android devices.

Let us first look at the contrast between the actual presence of malware detected by Pinkerton and the statements by the Internet users surveyed.

FIGURE 16. EVOLUTION OF MALWARE INCIDENTS (REPORTED VS REAL) ON HOME COMPUTERS (%)



Base: PC users
Source: Household panel, ONTSI

COMPUTERS HOSTING MALWARE (REAL DATA VS PERCEPTION)

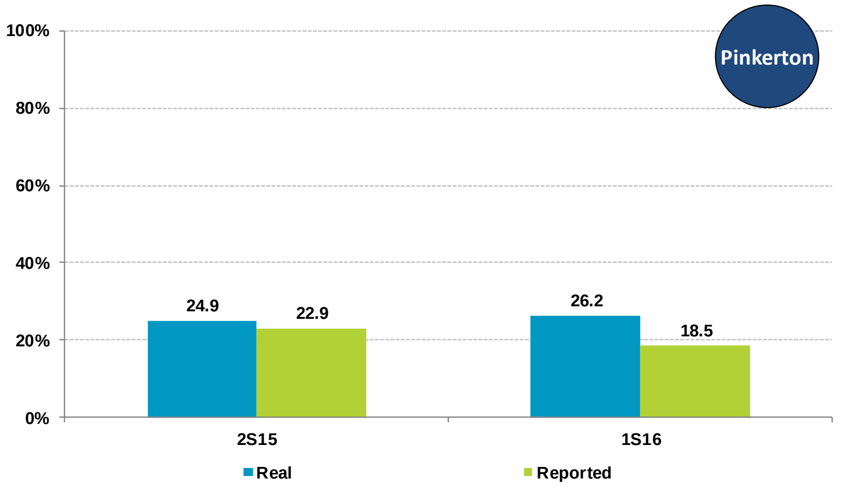
66.5%

OF COMPUTERS SCANNED WITH PINKERTON HOST MALWARE

18.0%

OF USERS NOTICE MALWARE ON THEIR PERSONAL COMPUTERS

FIGURE 17. EVOLUTION OF MALWARE INCIDENTS (REPORTED VS REAL) ON ANDROID DEVICES (%)



Base: Android device users
Source: Household panel, ONTSI

ANDROID DEVICES HOSTING MALWARE (REAL DATA VS PERCEPTION)

26.2%

OF ANDROID DEVICES SCANNED WITH PINKERTON HOST MALWARE

18.5%

OF USERS NOTICE MALWARE ON THEIR ANDROID DEVICES

It can be noted that fewer than one in five respondents are aware of malware infections on their personal computer (18%) or on their Android device (18.5%). Meanwhile, the real data collected by Pinkerton puts the presence of malware in a greater number of computers: 66.5% of personal computers and 26.2% of Android devices.

Although the gap between the user's perception and the actual computer state has increased considerably since the last period analysed, it is also important to note that this perception has decreased (-6.8 p.p. among personal computer users and -4.4 p.p. among Android device users) while the number of infections has been increasing (+6.5 p.p. and +1.3 p.p. respectively). This data could be indicative of a false sense of security contrary to reality on the part of the user.

So far the data have been analysed on a global scale. But, does the perception of each user, according to their statements, match the real state of their computer? It is important to know the answer to this question as there may be situations that lead to erroneous conclusions. For example, users who report detecting a malware incident and who had eliminated their computer's virus prior to Pinkerton's analysis.

The following tables break down both user responses and the data obtained from scanning their devices with Pinkerton with the goal of contrasting them.

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

They reported having malware on PC	Their PC had malware		
	Yes	No	Total
Yes	12.2	5.8	18.0
No	54.3	27.8	82.0
Total	66.5	33.5	100.0

Base: PC users
Source: Household panel, ONTSI

TABLE 2. MALWARE INCIDENTS ON ANDROID DEVICES (%)

They reported having malware on Android	Their Android had malware		
	Yes	No	Tota
Yes	6.0	12.5	18.5
No	20.1	61.4	81.5
Total	26.1	73.9	100.0

Pinkerton

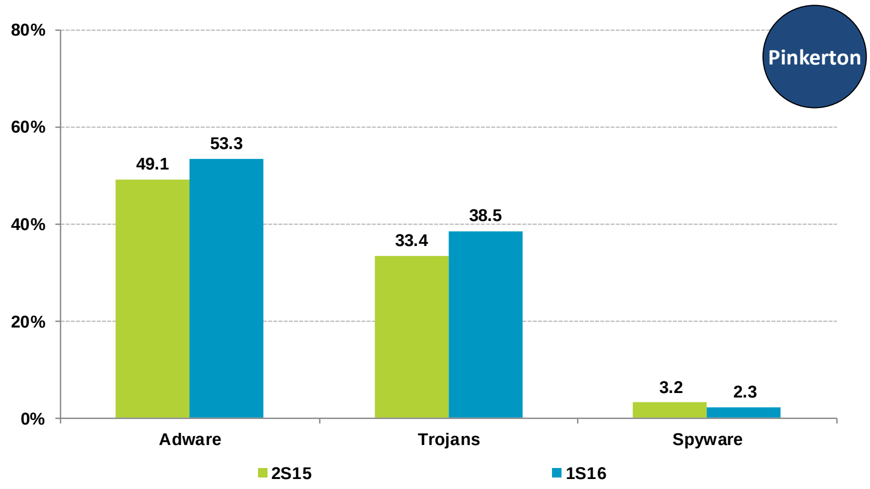
Base: Android device users
Source: Household panel, ONTSI

Some 54.3% of PC users who report not having experienced malware incidents actually have an infection on their computer. The same is true for one in five (20.1%) Android devices. In examining the results it can be confirmed that the gap between user perception and the reality of the computers and devices is much wider than expected.

It is clear that malware achieves its goal and a large percentage of users do not detect its presence despite the widespread acceptance of antivirus software use, and the good habits reported.

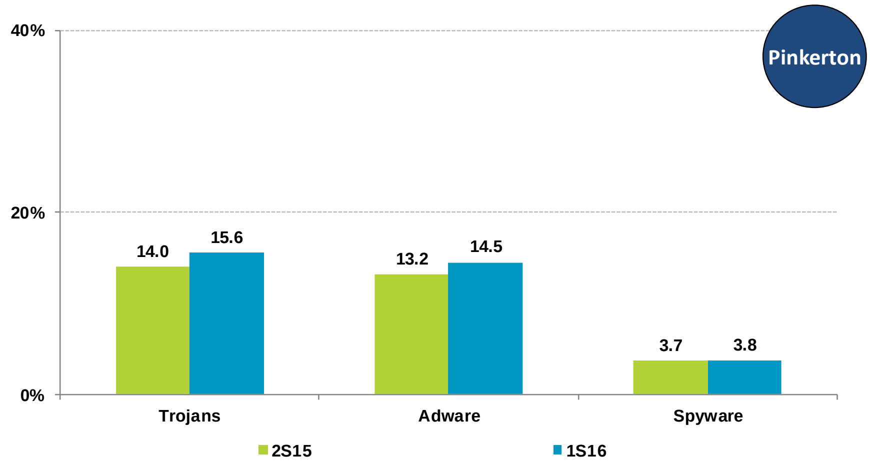
Below the type of malware detected by Pinkerton is analysed in order to confirm if this gap really corresponds to the reasons previously mentioned, meaning, the intention of the malware to go unnoticed.

FIGURE 18. EVOLUTION OF MALWARE ON THE HOUSEHOLD COMPUTER (%)



Base: All computers
Source: Household panel, ONTSI

FIGURE 19. EVOLUTION OF MALWARE ON ANDROID DEVICES (%)



Base: All Android devices
Source: Household panel, ONTSI

In analysing the types of malware detected on the computers of respondents according to detection by the Pinkerton tool, adware (present in 53.3% of computers) and Trojan horses (38.5%) stand out.

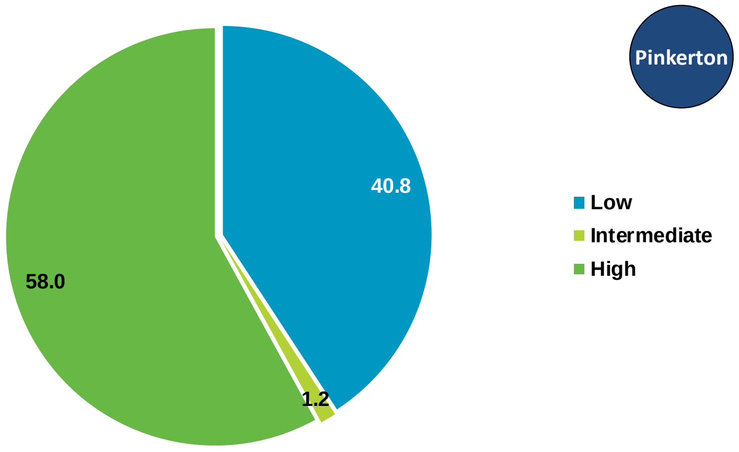
This data contrasts with the previous findings as adware is a type of malware whose purpose is to financially benefit its creator by including advertising in pop-up windows, installing a toolbar on the computer or in the browser, changing the default browser, etc. In other words, it is not hidden from the user, but is in fact visible, even though the user seems to be so accustomed to the constant bombardment of advertisements that they do not detect these incidents. However, adware also collects user data, information regarding the computer, websites visited, search patterns, and so on.

Adware, like all other malware, can take advantage of vulnerabilities and install itself on a computer, but it is often included with free programs which give the option to not install it during the installation process. It is also interesting to note that it is one of the most common types even though 84.4% of Internet users claim to pay attention to the steps of installing software on their computers.

On Android devices the results are similar: Trojan horses are found in 15.6% of devices and adware in 14.5%. Although the percentage of infections on Android devices is much lower than on personal computers, the numbers continue to grow in 2016.

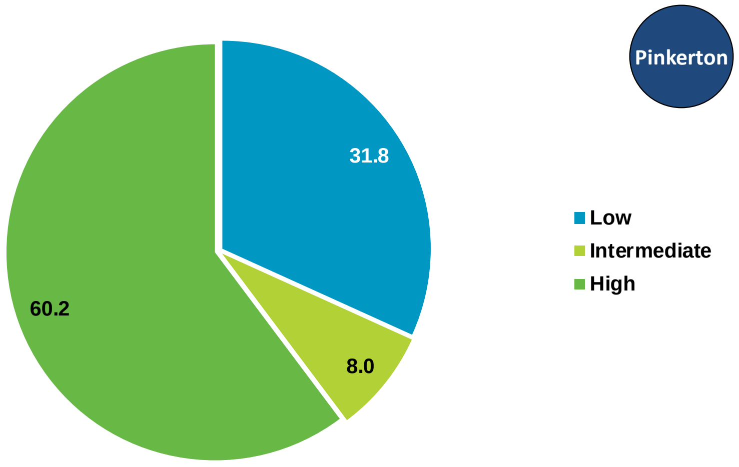
More than half of the computers infected by malware are at a high risk level.

FIGURE 20. RISK LEVEL ON THE HOUSEHOLD COMPUTER (%)



Base: PCs hosting malware
Source: Household panel, ONTSI

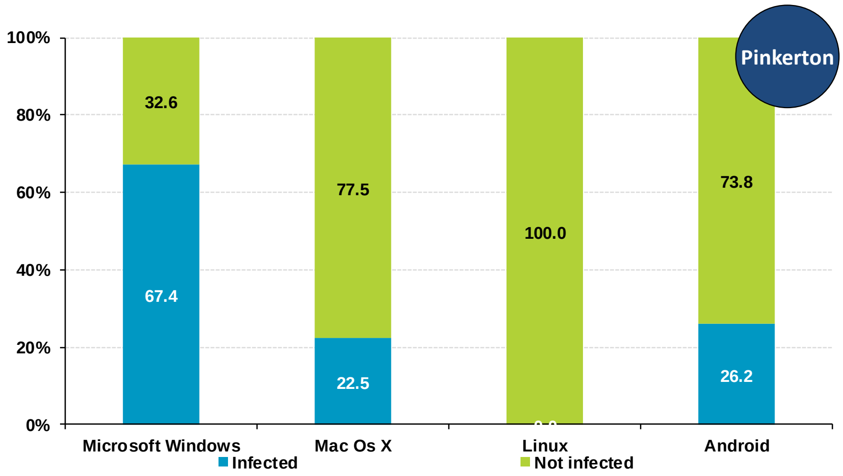
FIGURE 21. RISK LEVEL ON ANDROID DEVICES (%)



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

Based on the malware samples detected by the Pinkerton software and their level of dangerousness, a risk level was determined for each unit scanned, classifying them into three levels: low, medium and high. It is estimated that 58% of personal computers and 60.2% of Android devices that are infected by malware are at a high risk level due to the dangerous nature of the malware.

FIGURE 22. MALWARE BY OPERATING SYSTEM (%)



Base: All computers
Source: Household panel, ONTSI

The analysis of malware detection by different operating systems and/or platforms reveals that Microsoft Windows systems are most commonly affected by this type of incident. This situation can be explained mainly on the basis of the following hypotheses:

- The main use of the Windows operating system on personal computers. Developers of malicious codes attempt to reach the maximum number of possible targets, and they can do so by developing malware for those operating systems that are most widely used by users.

- The use of unauthorised or illegitimate software and cracks, serial number generators, unofficial patches or modified binaries, and other "tools" for illicit operation. Malware developers include malware in this type of software to get users to install and run it on their computer or device. This way, even security warnings are usually ignored in anticipation of having the software installed on the computer or device.

- User trust is taken advantage of with the inclusion of certain types of malware in programs, usually those which are free or trial versions. During the installation process a check box (checked by default) is displayed that allows the user to stop their installation on the computer or device; however, the user does not usually notice this option, meaning the malware is installed after "acceptance" or "approval".

- The security update cycle. Microsoft has a security update program that runs on a calendar (except in exceptional cases). This way, patches to correct a security problem are released on the second Tuesday of each month. This can be considered an advantage, as a user doesn't have to be constantly looking out for updates to be installed. However, when there is a vulnerability being exploited, any temporary window is a risk preferably avoided.

  Furthermore, the Windows XP operating system life cycle ended in April 2015. This means that Microsoft stopped giving support for this operating system and releasing security updates for it. Thus, Windows XP is in an obsolete and potentially vulnerable system that nevertheless maintains a significant usage rate.

It should be noted that this does not mean that other operating systems and/or platforms are free from malware, as can be seen in the graphic. However, in these cases the methods described above are not usually a means of infection. For example, Mac OS and GNU/Linux programs are usually installed through the official store or packages downloaded from official repositories and/or sources that are included in the operating systems by default. Similarly, it is common for security updates to be released as soon as possible for these operating systems.

On the other hand it can be seen that malware is still not as common on the Android platform as it is on Microsoft systems. Pinkerton has found infections on one in four (26.2%) scanned devices, although the existence of malware for this platform continues to grow. This fact can be explained on the basis of the following hypotheses:

- The usage rate of the Android operating system on mobile devices. As discussed previously, malware developers are interested in those systems most used by users with the goal of reaching as many objectives as possible.

- The use of mobile devices for handling sensitive information. Beginning some years ago, the trend for users is to use smartphones and mobile devices as a replacement for personal computers on both a personal and professional level. Therefore, it is more and more frequent to access e-mail, use social networks, make purchases online, check the status of bank accounts, etc. from mobile devices.

- Not checking the permissions granted to applications. Many applications request an excessive number of permissions that give them access to different system functionalities. In a high percentage of cases, the requested permissions are completely unnecessary for the functioning of the application, and may be indicative of its real intent. When in doubt, it is recommended to look for an official application for the same purpose from a trusted source, or one that requests fewer permissions.

- The update status of devices. Although Google releases security updates for Android fairly frequently, updating the operating systems of most Android devices depends not on the user but on the device manufacturers or operators. They take much longer to release updates, or in the case of some devices, simply never do so. This implies that there are a large number of potentially vulnerable devices and that malware developers can take advantage of this route of infection.

- Downloading applications from unknown sources. Official app stores are concerned with security and control the applications offered to prevent malware from spreading to users, but unofficial app stores do not. Unofficial stores focus on offering the largest number of applications in order to be attractive to and draw users, so they allow anybody to send apps that are not subjected to any analysis or checks. Moreover, black markets often offer free downloads of paid applications. Installing these applications entails a security risk to the Android device as they may be false or have been modified to conceal malware, and are offered in this way as bait so that users will want to install them.

There is also another type of application known as a downloader that covertly downloads and installs other malicious apps from unofficial servers. This can obviously only be carried out on devices that are configured to allow applications to be downloaded from unknown sources.

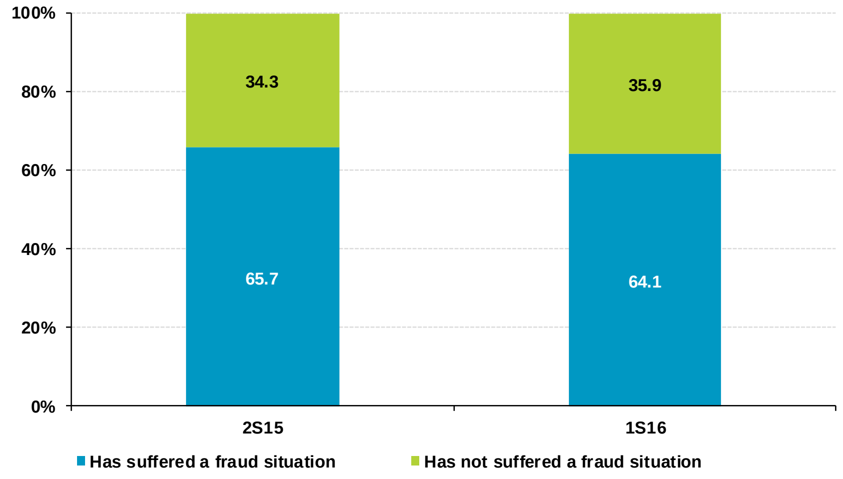
- Ignorance of users to the dangers lurking on mobile devices. While the threat of malware is well known to personal computer users, on other platforms there is a great lack of awareness that involves a high risk for users, who may have a false sense of security.

1.4 Consequences of security incidents and user reactions

This section examines the consequences of security incidents and reactions involving changes to adopted cautious behaviour and the security measures applied in order to avoid further security incidents.

Two out of three Spaniards have been exposed to attempted online fraud.

FIGURE 23. EVOLUTION OF ONLINE FRAUD ATTEMPTS (%)

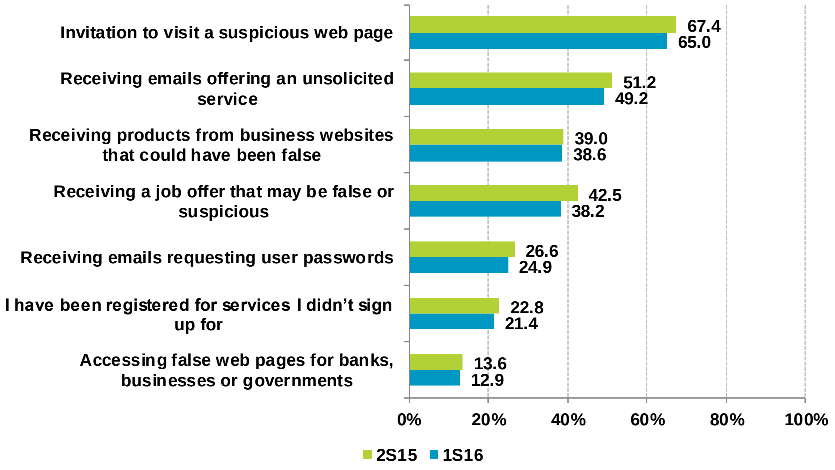


Base: All users
Source: Household panel, ONTSI

The occurrence of fraud situations (consummated or not) among Spanish Internet users has remained virtually unchanged during the first half of 2016. Therefore, almost two out of three Internet users interviewed (64.1%) reported having been involved in some kind of online fraud situation.

Such fraud situations can be presented in very different ways, with the intention of deceiving the user and making them believe that it is a normal and innocuous situation. The analysis of the following graphic reveals the most frequently perceived fraud situations by users.

FIGURE 24. EVOLUTION OF THE MANIFESTATION OF ONLINE FRAUD ATTEMPTS (%)



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

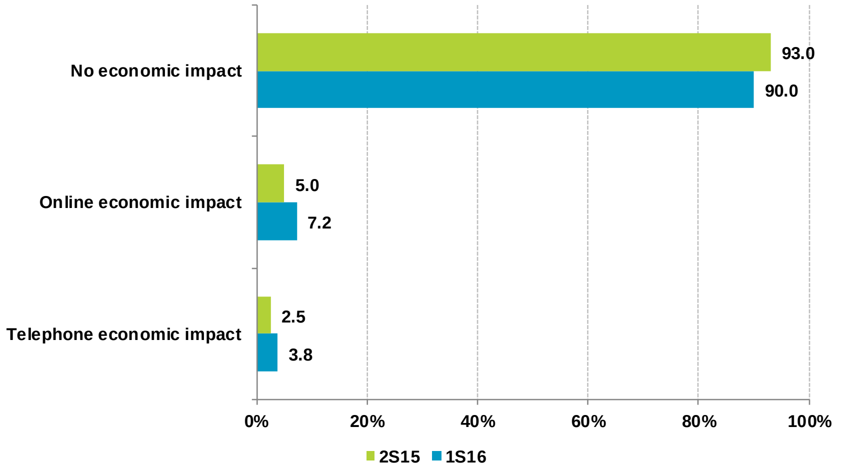
Generally speaking, there has been a reduction in the perceived occurrences of different types of online fraud attempts. The most common fraud attempts continue to manifest themselves through invitations to visit suspicious websites (65%) or via an e-mail offering unsolicited services (49.2%).

The most striking decrease (-4.3 p.p.) can be seen in the manifestation of fraud through fake or suspicious job offers because, due to the current situation, there is a high number of citizens actively seeking out employment. It seems that much care is put into these fake offers and therefore they are not being detected as such.

One in five panellists (21.4%) is affected by attempted fraud stemming from registration for a service to which they have not subscribed. This reported fraud includes subscription to SMS Premium services that entail a certain cost for each SMS message received, among other services.

The least perceived form among users who have experienced attempted fraud (with only 12.9% of reports) is the request for access to fake websites that try to supplant banking entities, online shops or governments for the purpose of deceiving the user and obtaining their credentials to perform operations without their knowledge or consent.

FIGURE 25. EVOLUTION OF THE ECONOMIC IMPACT OF FRAUD (%)



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

ECONOMIC DAMAGE DUE TO FRAUD

7.2%
OF ONLINE FRAUD

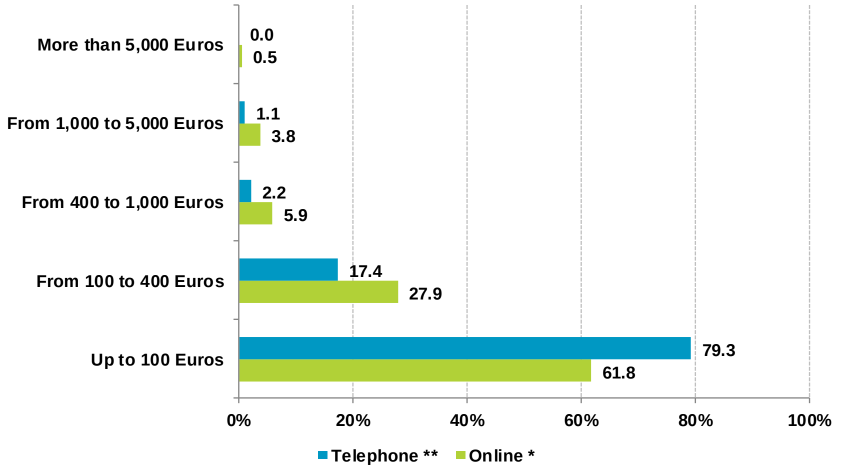
3.8%
OF TELEPHONE FRAUD

It has been seen that two out of every three users are affected by a situation of attempted fraud, but the frequency in which they are successful and imply an economic impact for the victim is quite low: only 7.2% of Internet fraud attempts and 3.8% of telephone fraud attempts are successful.

Fraud campaigns generally use e-mail as a means of dissemination. This is due to the ease, speed and low cost of mass mailing messages and the immediacy of receiving them. This means a longer window for action until the fraud campaign is detected and deactivated. Also through this medium, the attacker can take advantage of both the trust of the receiver and the urgency of decision making, since there is no two-way communication through which they can request more information for fear of suffering the consequences specified in the e-mail; however, in a telephone conversation it can be more difficult to convince the interlocutor and clarify all their doubts without suspicion.

Another difficulty involved in using the telephone is the language barrier. This implies that the fraud must be more localised and be carried out by individuals with a good command of the language in order to answer questions that may be posed by potential victims.

FIGURE 26. EVOLUTION OF THE DISTRIBUTION OF THE ECONOMIC IMPACT OF FRAUD (%)



Base: Users who have suffered economic damage as a consequence of online / telephone fraud
Source: Household panel, ONTSI

The Spanish Penal Code establishes a limit on the monetary amount to classify the severity of the crimes. This limit, which is at 400 euros, has great importance regarding fraud attempts.

It can be observed that among consummated fraud attempts those that have caused an economic impact inferior to this amount stand out: 89.7% (61.8 + 27.9) of telephone fraud and 96.7% (79.3 + 17.4) of online fraud.

In breaking down these values, 61.8% of online fraud cases and 79.3% of telephone fraud cases have an impact of below 100 euros, while in 27.9% and 17.4% of cases (respectively) the amount is between 100 and 400 euros.

It can also be observed that as the monetary amount increases, there is a tendency to use telephone contact to the detriment of e-mail, although fraud with monetary objectives of more than 400 euros have merely a nominal occurrence. This way the attacker avoids taking greater risks, as an e-mail provides more evidence and can be more easily traced than a telephone conversation.

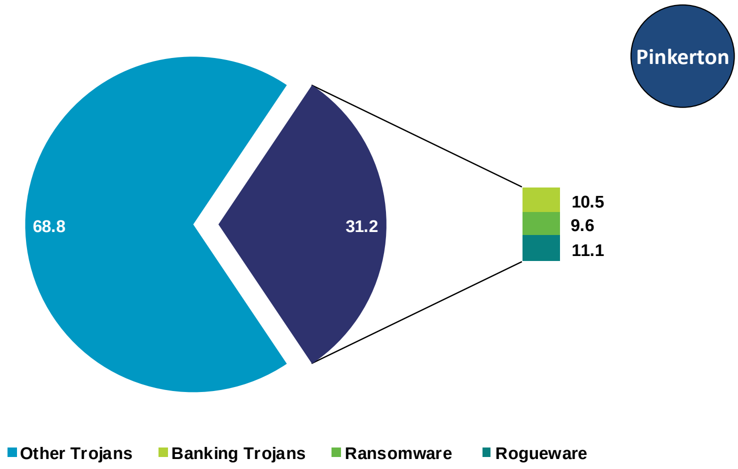
Another possible way to consummate attempted fraud is through malware. The purpose of malware like banking Trojans, rogueware and ransomware is to try to cause economic damage to affected users and, in the case of banking Trojans, to go unnoticed by the user.

Actually, the fact that a computer or device hosts malware does not mean that it will end up experiencing a situation of successful fraud, considering a series of requirements and circumstances that would allow such a situation must be fulfilled. For example, in the case of a banking trojan: malware must infect the user's computer, be directed to the user's bank, the user must use electronic banking and log on to the system from the computer, and the additional data requested by the malware must be filled in without suspicion.

Type of malware analysed

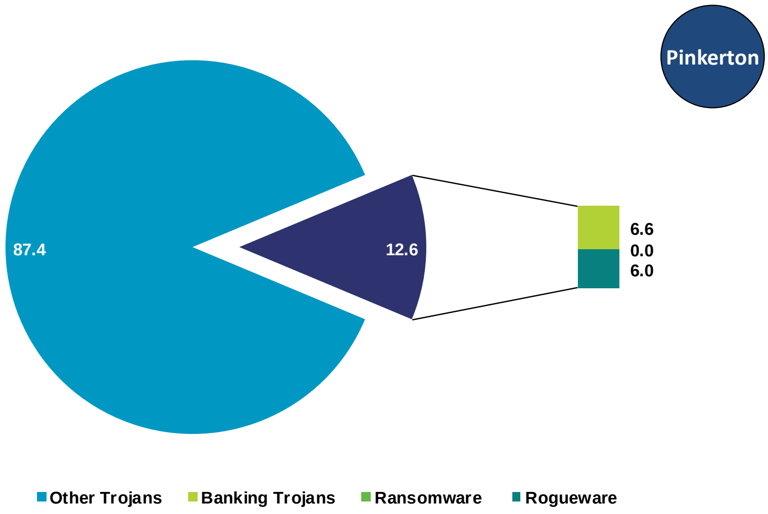
- Banking Trojan: malware that steals confidential information from customers of banks and/or online payment platforms.
- Rogueware or rogue: malware that makes victims think they have been infected by some kind of virus, getting them to pay a certain sum of money to remove it. The user is usually asked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

FIGURE 27. BANKING TROJANS, RANSOMWARE AND ROGUEWARE ON THE HOUSEHOLD COMPUTER (%)



Base: Total Trojans detected on PC
Source: Household panel, ONTSI

FIGURE 28. BANKING TROJANS, RANSOMWARE AND ROGUEWARE ON ANDROID DEVICES (%)



Base: Total Trojans detected on Android devices
Source: Household panel, ONTSI

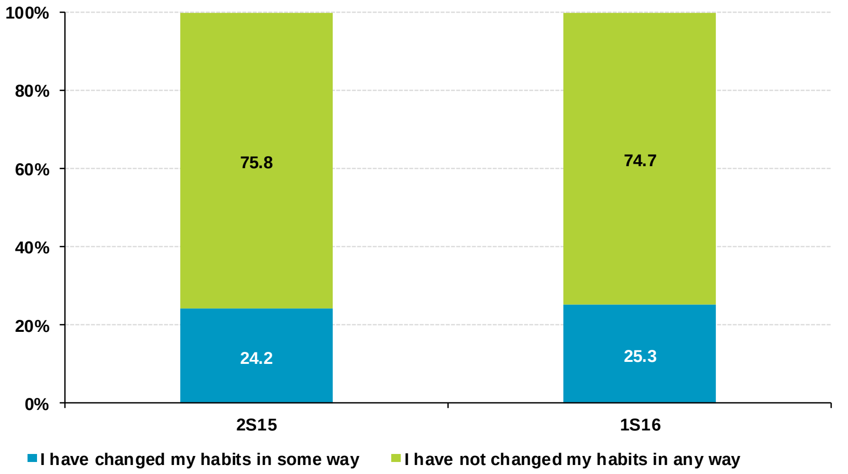
These graphs describe the Trojan types mentioned above from the samples obtained from the analysis carried out by Pinkerton. It is evident that 31.2% of the Trojans found in the computers of Spanish households belong to one of these subcategories: 10.5% are banking Trojans, 11.1% are rogueware, and 9.6% are ransomware.

Among the Android devices analysed by Pinkerton, the presence of these types of Trojans is significantly lower: 12.6%. They are distributed between banking Trojans (6%) and rogueware (6.6%).

In the current period, no sample of the ransomware type was detected among the Android devices analysed. This does not mean that there haven't been incidents related to this type of malware since the user could have removed it from the system. It is important to remember that the way ransomware acts is by installing itself on the system and taking it hostage, blocking it and preventing the user from using the computer in a normal manner. Therefore it is quite plausible that in such a scenario, a user may choose to restore an older version or backup of the system, or install a new ROM in their device. In this way, the malware would be removed and Pinkerton would not be able to detect it.

Only one in four Spanish Internet users modify their habits after suffering a situation of attempted online fraud.

FIGURE 29. EVOLUTION OF REACTIONS AFTER HAVING EXPERIENCED A SECURITY INCIDENT (%)

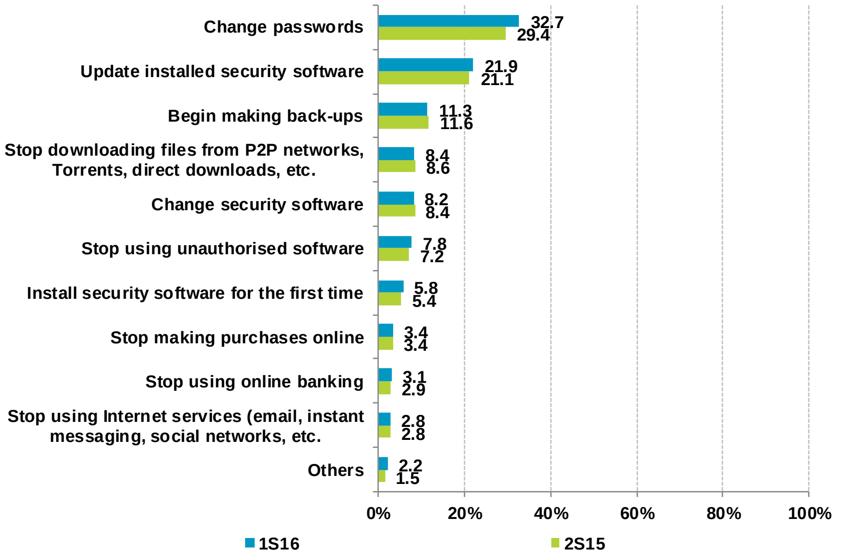


Base: Users that have suffered a security incident
Source: Household panel, ONTSI

After experiencing a security incident, users may decide to modify their behavioural habits and security measures, take on new ones, and even use the different services offered on the Internet to try to prevent new incidents from happening in the future, or if they do happen, to minimise their consequences.

One in four (25.3%) users claim to take these decisions after suffering a security incident. But what are these reactions? Which changes do Spaniards adopt to try to protect themselves against future incidents?

FIGURE 30. 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

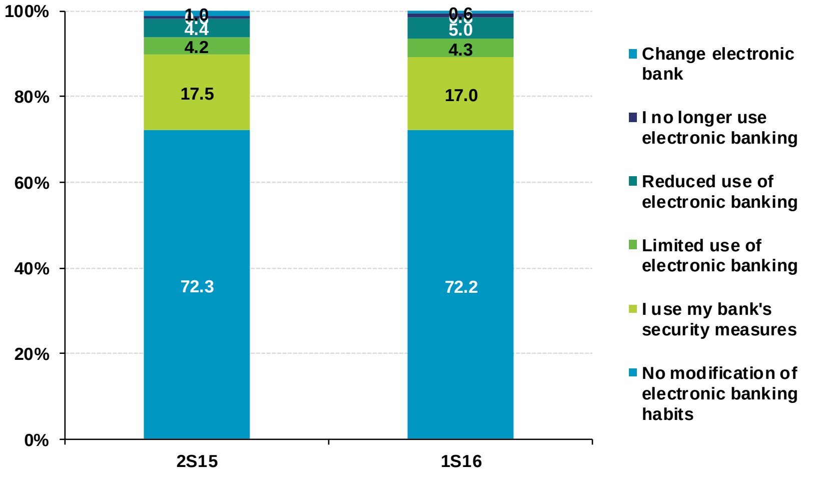
According to the responses provided by users, there is no change in the trend that typical user reactions follow.

The main options considered by users after the occurrence of a security incident are changing passwords (performed by 32.7%) in the case that they could have been compromised and updating already-installed security tools (21.9 %). Both experienced slight growth during the current analysis.

Likewise, less seen reactions continue to be stopping use of online banking, e-commerce, and Internet services such as e-mail and instant messaging. These are done by less than 3.4% of Internet users, which is an indication of the trust placed in these services.

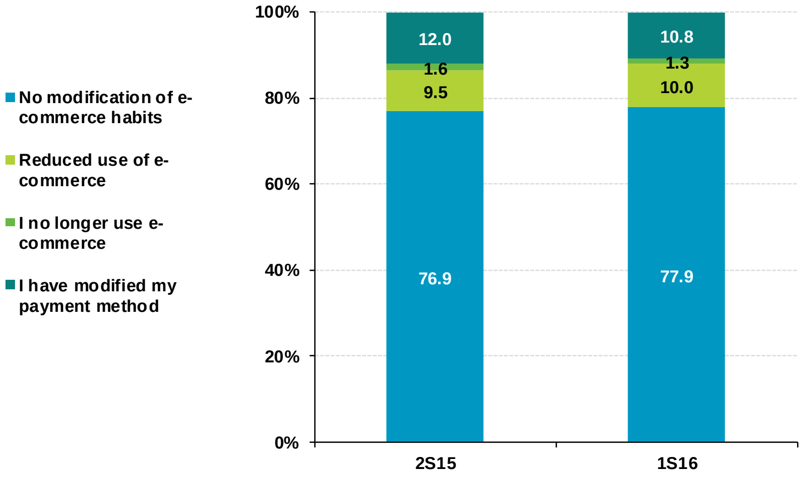
It must be noted that continuing to use a service does not mean not modifying any of the habits related to it in order to avoid future situations of attempted fraud. Below the changes regarding habits adopted by users in the field of online banking and e-commerce are analysed.

FIGURE 31. EVOLUTION OF MODIFYING BEHAVIOUR CONCERNING ONLINE BANKING AFTER HAVING EXPERIENCED A FRAUD ATTEMPT (%)



Base: Users of online banking / e-commerce who have experienced attempted fraud
Source: Household panel, ONTSI

FIGURE 32. EVOLUTION OF MODIFYING BEHAVIOUR CONCERNING E-COMMERCE AFTER HAVING EXPERIENCED A FRAUD ATTEMPT (%)



Base: Users of online banking / e-commerce who have experienced attempted fraud
Source: Household panel, ONTSI

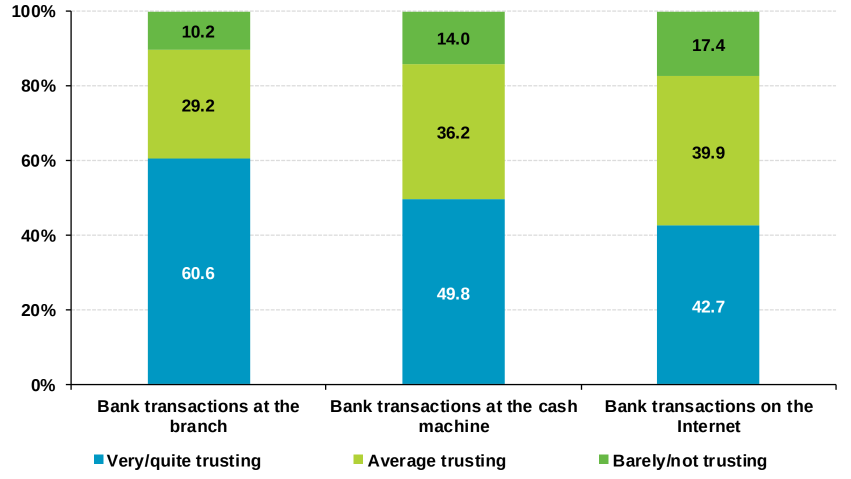
The existence of a high level of trust by the user in banking and e-commerce services is confirmed. Approximately three out of four Spanish users do not change their usage habits at all.

The main changes are the use of security systems offered by the bank itself (17.0%) and changing the payment method (10.8%) in online stores.

1.5 Trust in the digital environment in Spanish households

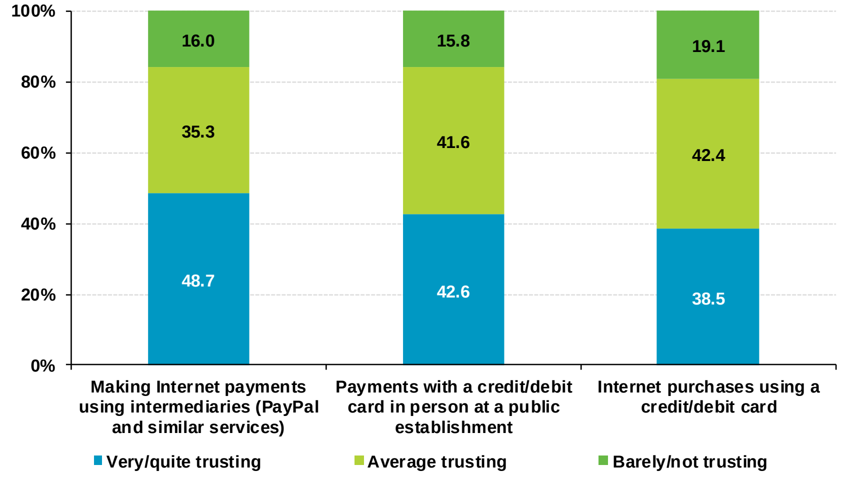
To complete the study, an analysis of users' opinions regarding the state of protection of their devices, trust in the services used, perception of the risks and dangers found on the Internet, and considerations about their own responsibility in terms of security has been performed.

FIGURE 33. LEVEL OF TRUST IN BANK TRANSACTIONS (%)



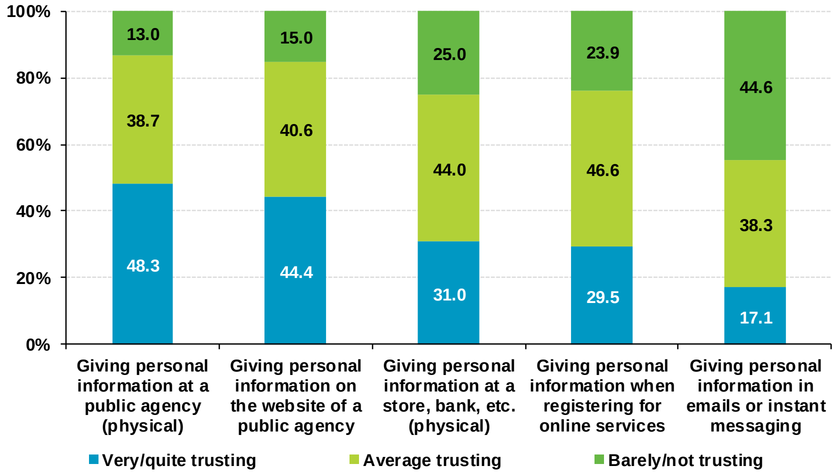
Base: users of online banking
Source: Household panel, ONTSI

FIGURE 34. LEVEL OF TRUST IN E-COMMERCE OPERATIONS (%)



Base: users of e-commerce
Source: Household panel, ONTSI

FIGURE 35. LEVEL OF TRUST IN PROVIDING PERSONAL DATA (%)



Base: all users
Source: Household panel, ONTSI

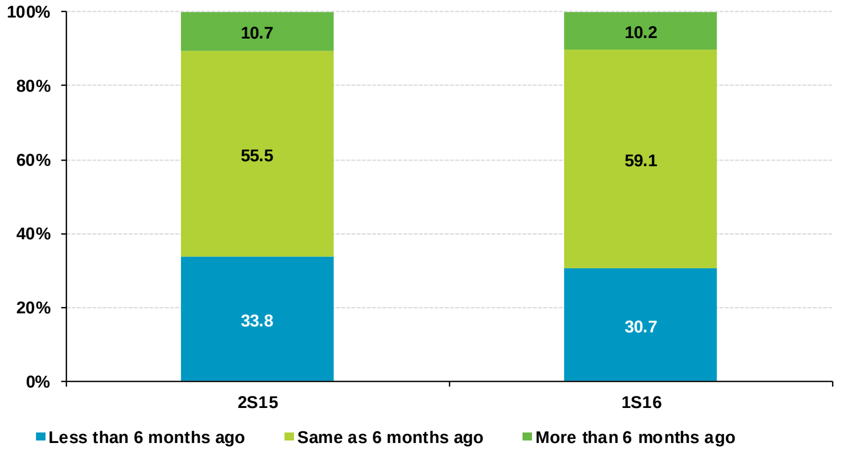
As it might be expected, the physical services with which the user can interact in the real world inspire a higher level of trust than their digital counterparts and, likewise, those in which they interact with another person provide greater trust than those made through a machine.

Thus, Spanish users rely mainly on banking transactions carried out in a branch (60.6%), while the number falls to 49.8% in the case of ATMs, and to 42.7% for online banking transactions. The gap between trust in a physical and online service is around 18 p.p.

The trust that Spanish Internet users put in intermediaries such as PayPal to carry out transactions via the Internet (48.7%) should be noted, as it is even higher than that generated by payments with a credit/debit card in a public establishment (42.6%). The option to use a credit/debit card directly for online payments is the least trusted method by users (10.2 p.p. below the intermediary option).

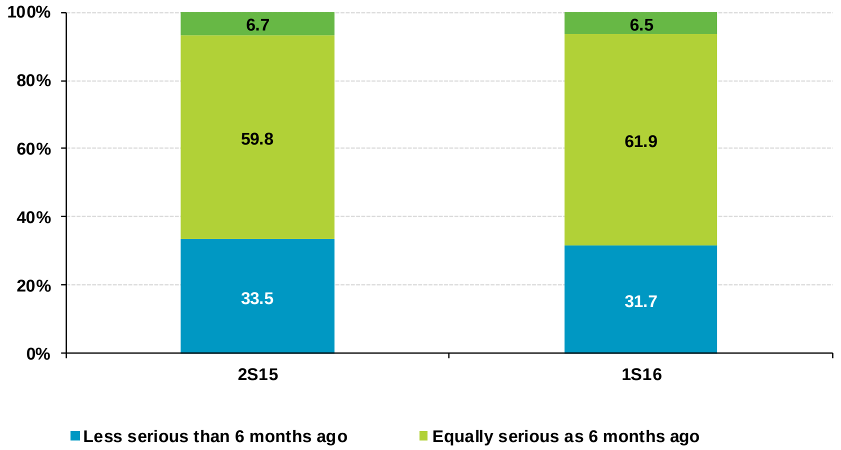
Regarding the provision of personal data, there seems to be less concern among users, since less than half (44.6% and down from the previous period) of Spaniards are suspicious when providing this type of information when it is requested of them through e-mails or instant messaging. However, it is necessary to emphasise that this medium is often used to solicit user-sensitive information under the guise of contests, sweepstakes, discount coupons, prizes, and so on, with different objectives such as collecting information, registering the user in Premium SMS services, using social engineering to gain access to user services, etc.

FIGURE 36. EVOLUTION OF THE PERCEPTION OF THE NUMBER OF SECURITY INCIDENTS (%)



Base: all users
Source: Household panel, ONTSI

FIGURE 37. EVOLUTION OF THE PERCEPTION OF THE SEVERITY OF SECURITY INCIDENTS (%)

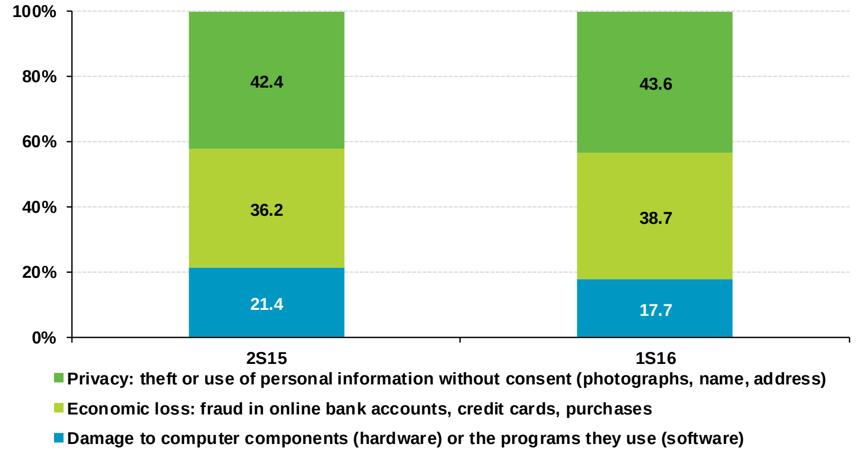


Base: all users
Source: Household panel, ONTSI

Approximately three out of five users perceive that the number of security incidents over the last three months is similar to those observed in previous months (59.1%) and their severity is similar (61.9%).

One in three users even believed that both the number of incidents and their severity decreased during the last three months.

FIGURE 38. EVOLUTION OF THE PERCEPTION OF RISKS ON THE INTERNET (%)

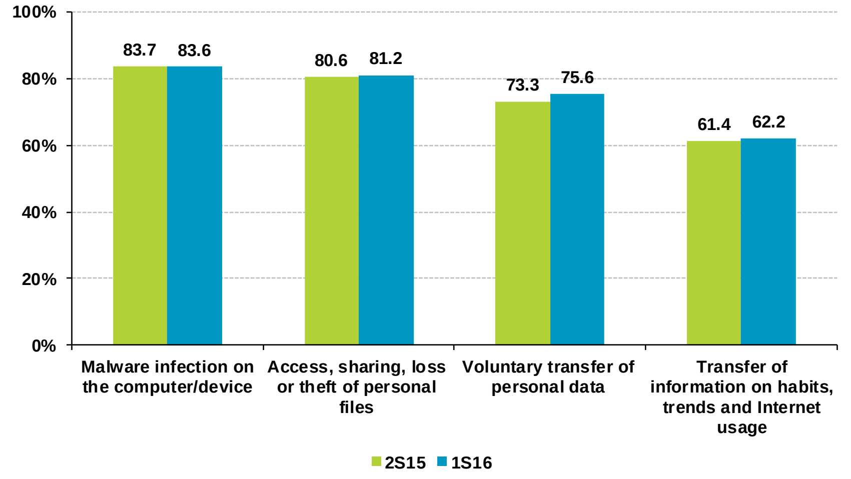


Base: all users
Source: Household panel, ONTSI

Despite what was previously observed in terms of low levels of concern regarding the provision of personal data through e-mails or instant messaging, users surveyed place the loss of privacy and its consequences (theft and use of personal information without consent or knowledge of the user) as the main risk on the Internet (43.6%).

The second-placed threat hidden on the Internet is economic damage stemming from online fraud attempts. This was reported by 38.7% of users.

FIGURE 39. EVOLUTION OF THE ASSESSMENT OF DANGERS POSED BY THE INTERNET (%)

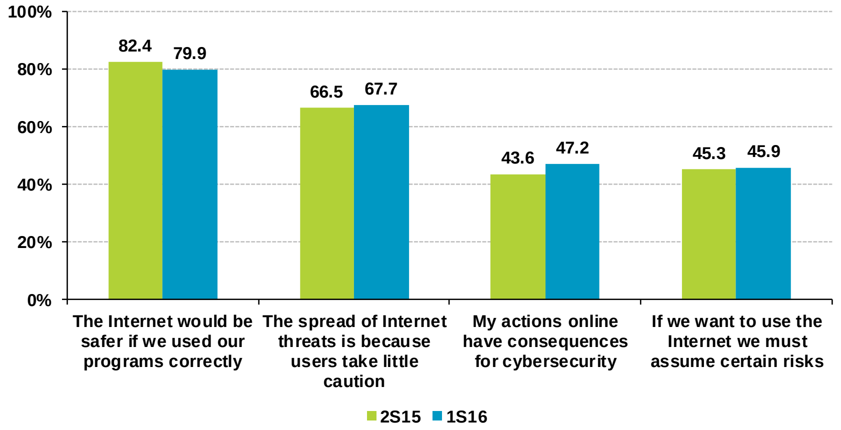


Base: all users
Source: Household panel, ONTSI

An analysis is made of the importance that the users give to the different dangers of the Internet. Again, it should be pointed out that privacy-related dangers are relegated to third and fourth place, those being the transfer of personal data (75.6%) and information regarding habits, tendencies and use of the Internet (62.2%).

Malware is considered the most dangerous (83.6%). Despite this, only a minority (7.8%) would consider stopping using unauthorised or illegitimate software after suffering a security incident, with cracks, serial number generators, unofficial patches, modified binaries, etc. being some of the main vectors of infection.

FIGURE 40. EVOLUTION OF RESPONSIBILITY IN TERMS OF INTERNET SECURITY (%)



Base: all users
Source: Household panel, ONTSI

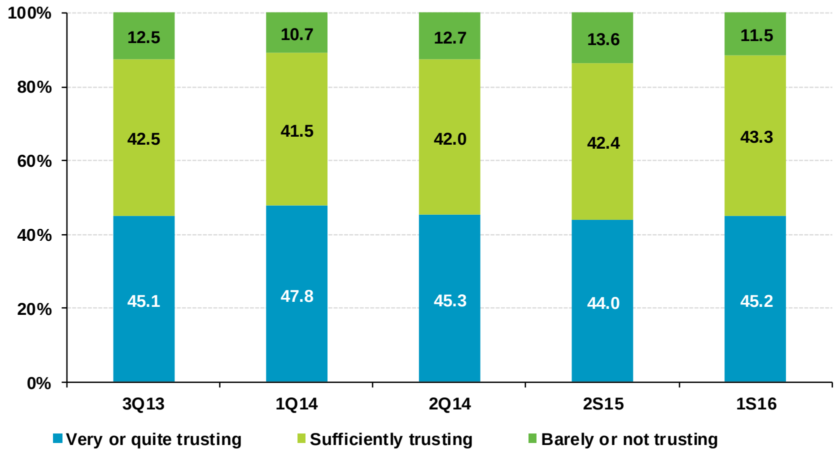
Being aware of the repercussions that one’s actions may have on Internet security can positively influence a user's cautious habits, the use of security measures, and the adoption of risky behaviour, in such a way that it can be key in avoiding security incidents.

But less than half (47.2%) of users believe that their online actions can have some kind of cybersecurity consequence. In addition, a similar number of Internet users (45.9%) think that in order to enjoy the Internet, certain risks must be assumed. Because of this, more than half of users expose both their computer or device as well as their personal and private information to the previously analysed dangers.

On the other hand, two out of every three statements correspond to the claim that the spread of threats over the Internet is due to the low level of caution shown by the users themselves. And, a high number (practically 80%) believe that the Internet could be safer if users make adequate use of the tools and programs at their disposal.

In analysing all these responses globally, there seem to be users who -despite understanding that a low level of caution when browsing the Internet favours the possible occurrence of security incidents- think that these are not caused by their own online actions (but by those of other users), and even that certain risks must be taken for a better online experience. This could explain the high rate of reported security incidents as well as the number of infected computers and devices.

FIGURE 41. EVOLUTION OF THE LEVEL OF TRUST ON THE INTERNET (%)



Base: all users
Source: Household panel, ONTSI

Generally speaking, the levels of trust that users have in the Internet remain at similar levels to those observed in previous analyses. 45.2% say they trust the internet to a great degree, 43.3% sufficiently trust it, and only 1 in 10 shows little or no trust in the Internet.

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:

ontsi

Management: Alberto Urueña López
Technical team:
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. Spain

Tel.: 91 212 76 20 / 25
Fax: 91 212 76 35
www.red.es