Study on cibersecurity and trust in spanish households

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

ontsi observatorio nacional de las telecomunicaciones y de la SI

STUDY ON CYBERSECURITY AND TRUST 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

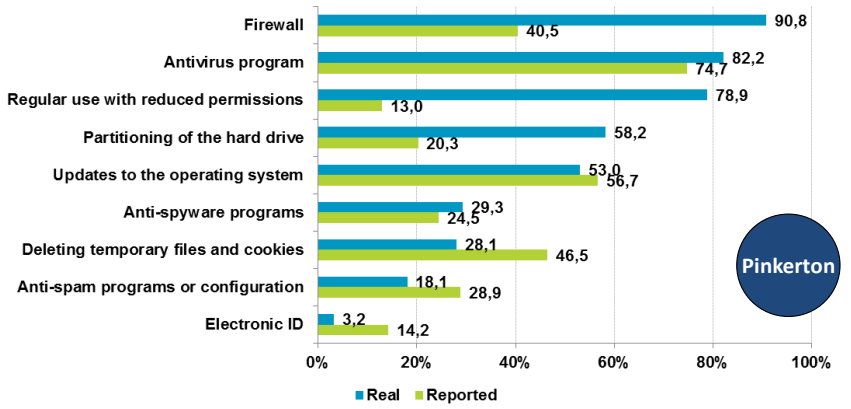
The presence of security measures on computers and devices (home computers and Android devices) is one of the basic pillars of information security.

The usage trends for security measures on home computers that had been observed in the previous analyses were confirmed for the period of July to December 2015.

These trends comprise the inclusion of security measures in the newest versions of operating systems and the increased use of cloud services, in many cases as a replacement for traditional tools (anti-spam filters of the main email service providers, inclusion of ad blockers and fraudulent website blockers on browsers, etc.). This explains the discrepancies between the real data obtained by Pinkerton and user statements about using these types of tools.

The greatest disparities between the real data and user statements are related to the use of firewall software and the regular use of user accounts with reduced permissions.

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



Base: PC users
Source: Household panel, ONTSI

The primary security measures, according to the real use detected by Pinkerton, are firewalls (90.8%) and antivirus software (82.2%). However, we can note a discrepancy in the stated responses, mainly due to the inclusion of these firewall solutions in operating systems and security suites, as a result of which their existence goes unnoticed by a large number of users (reported usage is 50% below real use).

The same occurs for the data for regular computer use with a user account with reduced permissions: Pinkerton detects real usage of 78.9% while only 13% of Internet users report it. This difference of nearly 66 percentage points confirms the degree to which users do not know their privilege level on their computers, and of not needing to have high privileges to be able to use the system normally.

Regardless of the discrepancies between the real and stated values, the data above are a positive sign given that the presence of these security measures is higher than what is perceived by users.

However, there is also a negative counterpoint: the differences between reality and the statements regarding deleting temporary browser files and cookies (over 18 percentage points) and running an updated version of the operating system (in this case under 4 percentage points). The lack of running updated versions highlights the risk of these computers and devices being vulnerable to malware that takes advantage of unaddressed security issues to infect the system.

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

90.8%
WITH FIREWALL SOFTWARE

82.2%
WITH ANTIVIRUS SOFTWARE

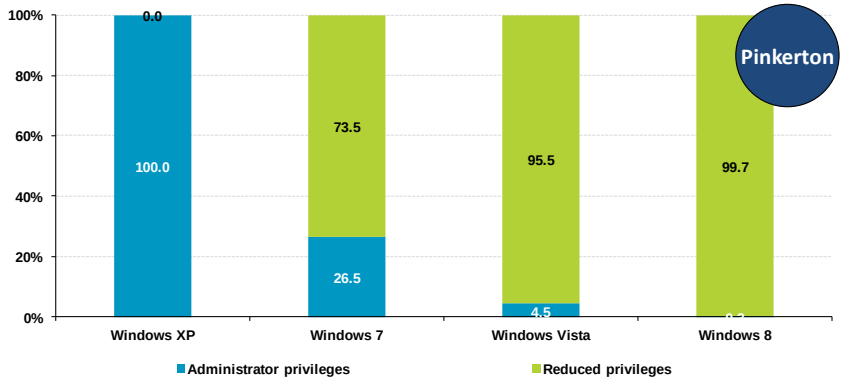
REGULAR USE WITH REDUCED PRIVILEGES (REAL DATA)

99.7%
WITH REDUCED PERMISSIONS IN WINDOWS 8

73.5%
WITH REDUCED PERMISSIONS IN WINDOWS 7

95.5%
WITH REDUCED PERMISSIONS IN WINDOWS VISTA

FIGURE 2. REAL USE OF PROFILES BY PRIVILEGE LEVEL ON MICROSOFT WINDOWS OPERATING SYSTEMS (%)

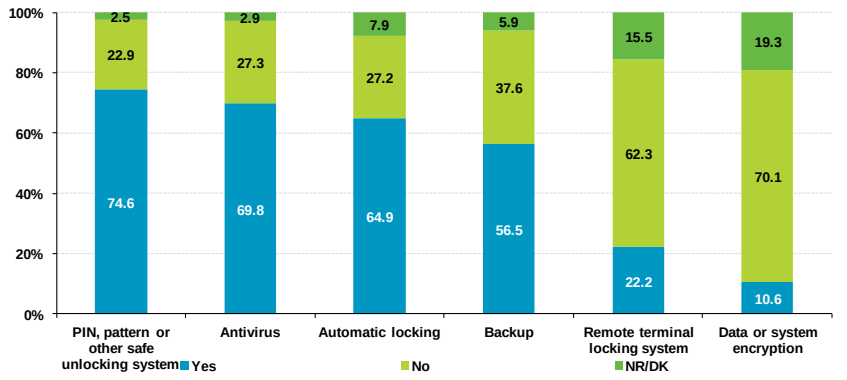


Base: Microsoft Windows users
Source: Household panel, ONTSI

Microsoft sets up a standard user account, or one with reduced permissions, by default in the latest versions of its operating system. This security measure can be noted in the data obtained by Pinkerton regarding the real level of privileges of user accounts on computers and devices. Thus, a large majority of users surveyed regularly use an account with reduced permissions in Windows Vista (95.5%), Windows 7 (73.5%) and Windows 8 (99.7%).

In view of the previous results we should explain that there may be Windows 10 operating systems that are 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 3. SECURITY MEASURES ON ANDROID DEVICES (%)



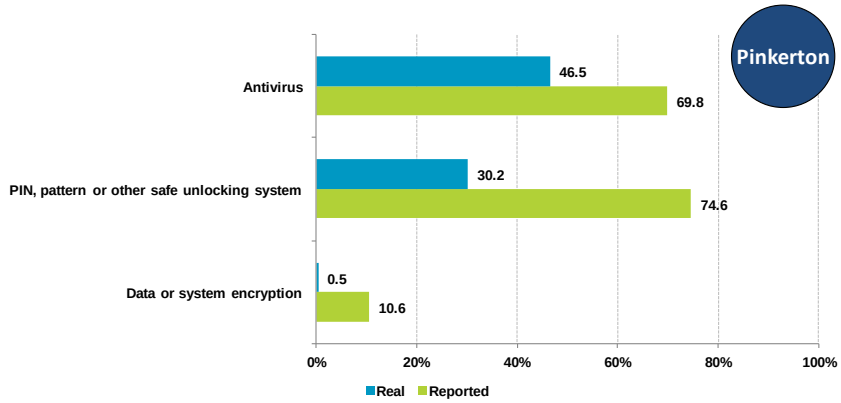
Base: Android device users
Source: Household panel, ONTSI

The security measures most used on Android devices, according to user statements, are secure unlocking systems via PIN codes, patterns, fingerprint detection, etc. (74.6%), antivirus software (69.8%), and automatic locking of devices after a period of inactivity (64.9%).

However, only 10.6% use encryption software to prevent third parties from accessing the data on the device in case of loss or

theft. Additionally, 22.2% have a remote locking system set up to prevent the device from being used in case of loss or theft.

FIGURE 4. REPORTED VS. REAL USE OF SECURITY MEASURES ON ANDROID DEVICES (%)



Base: Android device users
Source: Household panel, ONTSI

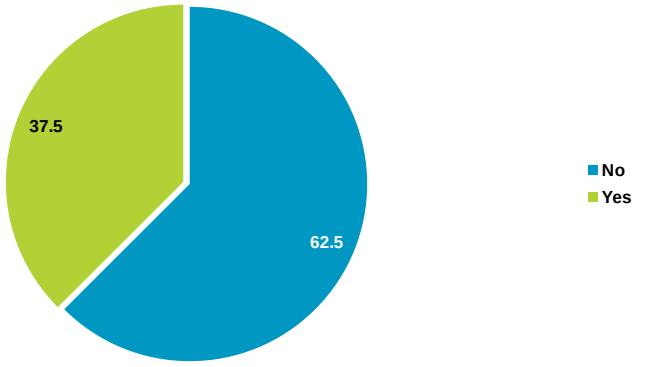
The real data obtained via Pinkerton reveals that there are also some discrepancies with the reported data. One major difference is in the case of antivirus software installed on the device: the real data shows that it is present in under 23% of cases, indicating that there are a large number of users of Android devices who are under a false layer of security and who think they are protected from malware threats even though that is not the case.

Equally significant is the case of unlocking systems on Android devices, where the user perception is that their unlocking systems are secure when actually they are not. A secure unlocking system is one that requires a password, numerical code (PIN) or swipe pattern, or that uses 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 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.

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 5. KNOWING ADOPTION OF RISKY BEHAVIOURS (%)

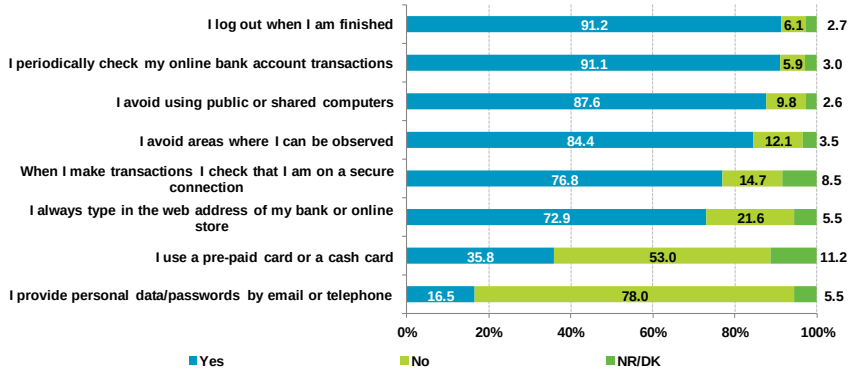


Base: all users
Source: Household panel, ONTSI

Some 37.5% of Internet users report that at times they knowingly engage in behaviours that entail security risks while they browse or use Internet services.

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

FIGURE 6. PRUDENT HABITS RELATED TO ONLINE BANKING AND E-COMMERCE (%)

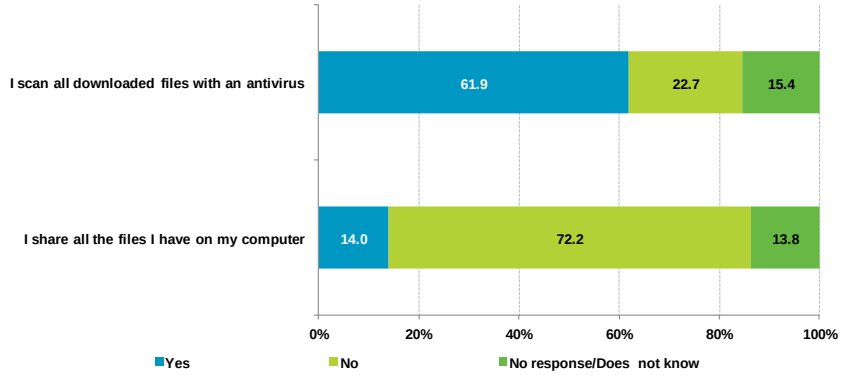


Base: users of online banking and/or e-commerce
Source: Household panel, ONTSI

However, in the context of online banking services and e-commerce, most users are cautious and report good usage habits. This was generally observed to be the case for more than 73% of Internet users.

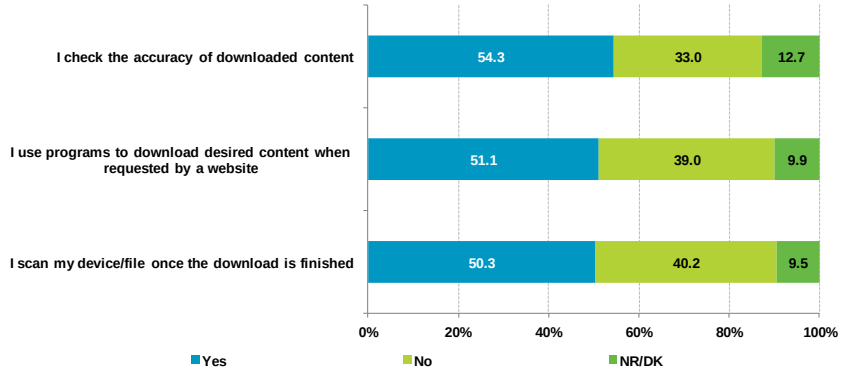
Only the use of prepaid cards and cash cards to make online payments is less widespread, by just one in three users, despite most banks offering them. Despite this weak level of adoption, it is a highly recommended measure that prevents real bank account information from being compromised. Moreover, as these cards carry a limited balance, they minimise the possible economic impact in the event of becoming a victim of fraud when making payments on the Internet.

FIGURE 7. P2P NETWORK DOWNLOADS (%)



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

FIGURE 8. INTERNET DOWNLOADS (%)



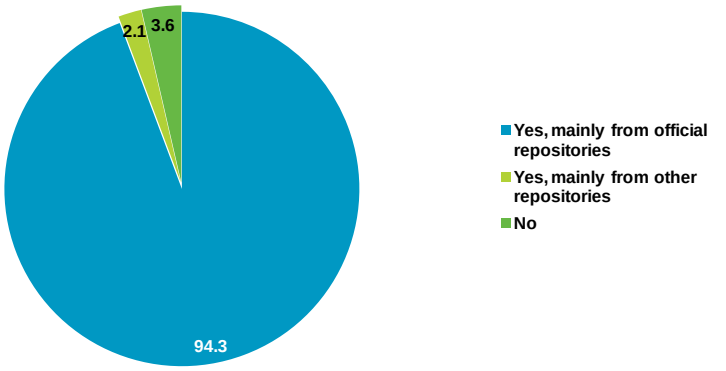
Base: all users
Source: Household panel, ONTSI

Internet downloads are one of the main ways computers and devices get infected. Although malware usually shows up in file launchers, cracks, serial number generators, etc., it also often simulates other known software, multimedia files (videos and photos), or any other type of harmless file in order to spark user interest and get the user to open or run the file and thus unleash the infection on the machine.

Many users are aware of this fact, evident from their good habits when downloading files from the Internet. Nearly 62% of users of P2P networks do not open downloaded files if they are not sure they have been scanned, just like half (50.3%) of users do for files that they download directly.

Another good habit is adopted by 54.3% of users, who report checking the accuracy of downloaded content before opening it (download site, file type, hash, etc.).

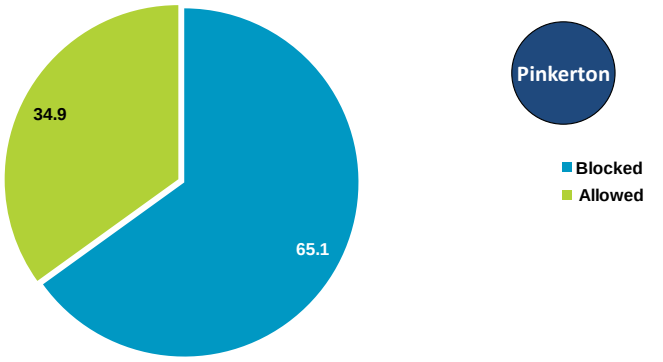
FIGURE 9. APPLICATION DOWNLOADS ON ANDROID DEVICES (%)



Base: Android device users
Source: Household panel, ONTSI

Most users of Android devices (94.2%) download applications primarily from official repositories. This is a prudent user habit, because running or using programmes and/or files from suspicious sources could lead to the installation of malware on the mobile device or other security issues.

FIGURE 10. UNKNOWN SOURCES (%)



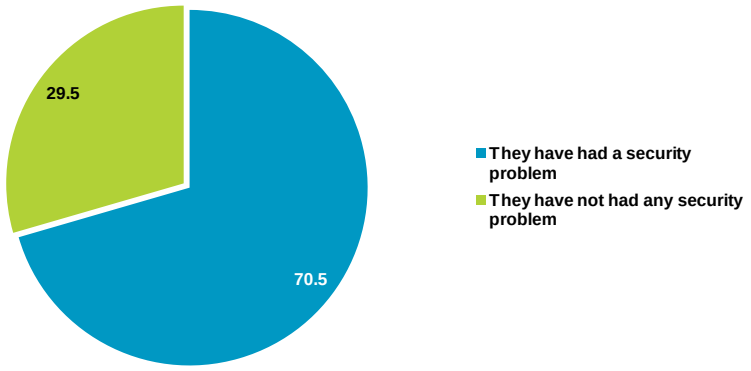
Base: Android device users
Source: Household panel, ONTSI

However, the analysis performed with the Pinkerton tool reveals that more than a third (34.9%) of Android devices are configured to allow the installation of applications from unknown sources. It was observed that despite preferring to use official repositories, many users could have downloaded and installed applications from third-party sources on some occasion, with the potential risk entailed.

1.3 Security incidents

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

FIGURE 11. SECURITY INCIDENTS (%)

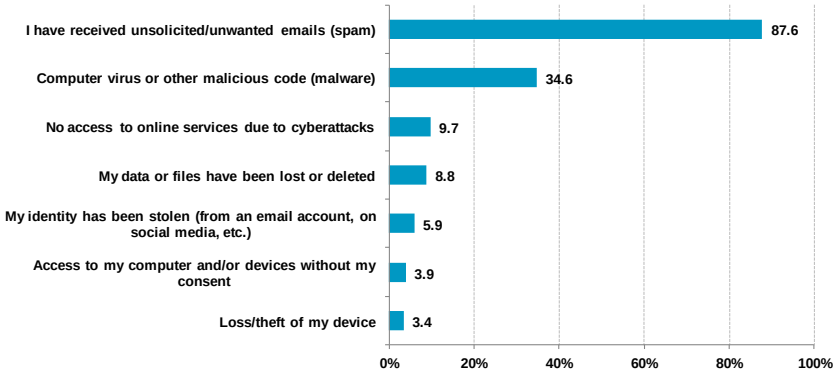


Base: all users
Source: Household panel, ONTSI

Although security systems are constantly evolving towards more robust models, we should understand that they are not infallible nor impenetrable. For that reason there is always a possibility of security incidents occurring despite measures in place and good careful usage habits.

Thus, between July and December 2015, 70.5% of users report having experienced some kind of security incident.

FIGURE 12. CLASSIFICATION OF SECURITY INCIDENTS (%)



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

Malware is the name for any malicious programme that aims to infiltrate computer equipment and take actions without the owner's consent.

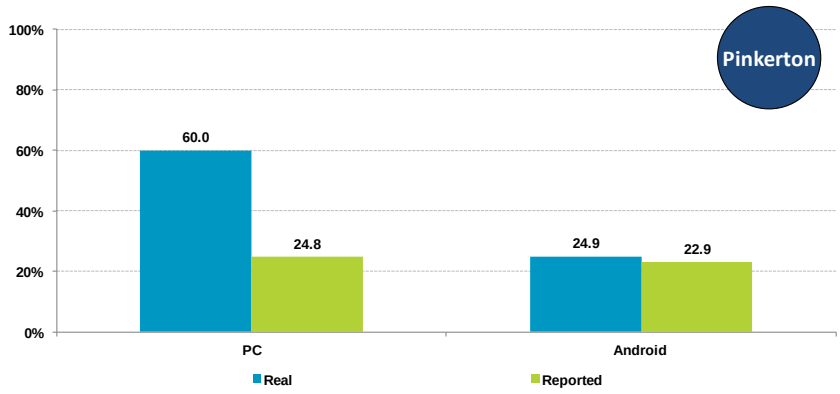
They are commonly known as viruses, although in reality malware is a much broader term that encompasses many other types.

The primary incident perceived by users is spam or unwanted emails (87.6%), which aims to capture users' attention.

Incidents related to viruses and malware (34.6%) are in second place. Unlike with spam, the goal of many types of malware is to go undetected by both antivirus software and the user.

This fact is explored below by analysing the real malware infections existing on computers and devices (both personal computers and Android devices) compared to the statements made by Internet users surveyed.

FIGURE 13. MALWARE INCIDENTS (REPORTED VS. REAL) (%)



Base: all users
Source: Household panel, ONTSI

COMPUTERS HOSTING MALWARE (REAL DATA VS. PERCEPTION)

24.8%
OF USERS NOTICE MALWARE ON THEIR PERSONAL COMPUTERS

60.0%
OF COMPUTERS SCANNED WITH PINKERTON HOST MALWARE

Approximately one in four people interviewed reported having detected malware on their personal computers. However, the real data obtained through the Pinkerton scans of computers detected a much higher number of infections: around 60%.

In the case of Android devices, user perception is much closer to reality. Here, Pinkerton found infections on nearly 25% of the devices analysed, while 23% of users perceived an incident of this type. But do these perceptions match the reality of the equipment analysed? The following tables compare user responses with the data obtained by scanning their devices with Pinkerton.

TABLE 1. MALWARE INCIDENTS ON PERSONAL COMPUTERS (%)

Pinkerton

Reported having malware	They have malware in their PC		
	Yes	No	Total
Yes	15.2	8.9	24.1*
No	44.8	31.1	75.9
Total	60.0	40.0	100.0

Base: PC users
Source: Household panel, ONTSI
** The 24.1% refers to users who reported having malware and whose PCs were scanned*

TABLE 2. MALWARE INCIDENTS ON ANDROID DEVICES (%)

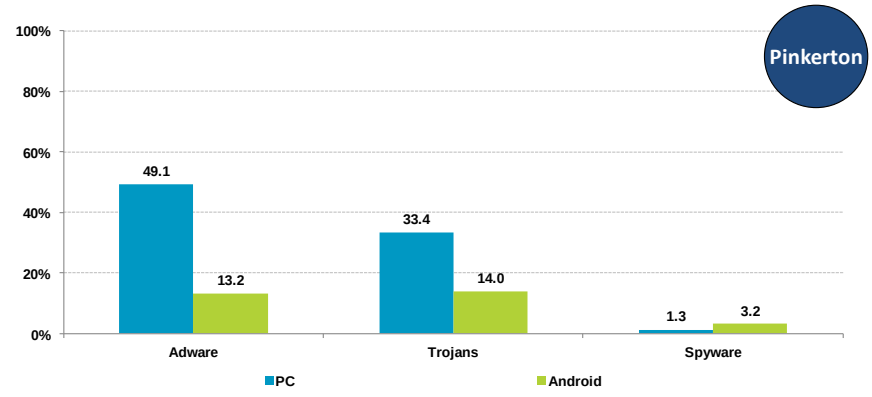
Reported having malware	They have malware in their Andro		
	Yes	No	Total
Yes	4.9	18.2	23.1*
No	20.0	56.9	76.9
Total	24.9	75.1	100.0

Base: Android device users
Source: Household panel, ONTSI
** The 23.1% refers to users who reported having malware and whose Android devices were scanned*

Some 44.8% of PC users who report not having experienced malware incidents really have an infection on their computer. The same is true for one in five Android devices. In other words, the gap between user perception and the reality of the computers and devices is much wider than expected.

These data confirm the conclusion presented above: malware is a veiled threat that is very commonly present on user computers and devices. Malware incidents are much more common than perceived by users, revealing the intentions of those who develop malicious code to prevent it from being discovered by users and evade detection by antivirus programmes.

FIGURE 14. COMPUTERS HOSTING MALWARE ACCORDING TO TYPE (%)

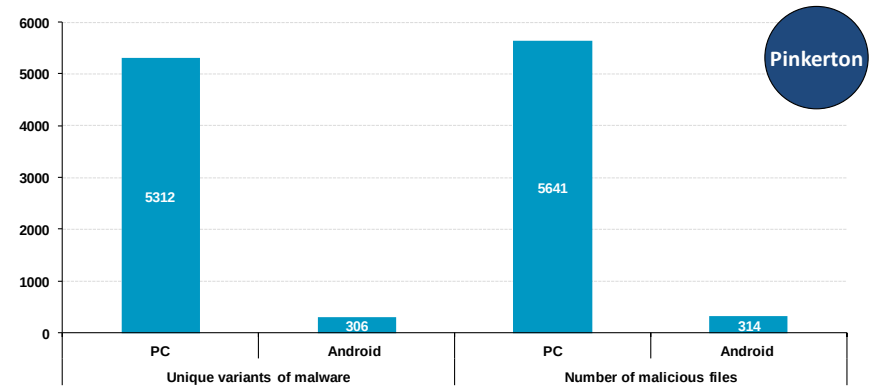


Base: all users
Source: Household panel, ONTSI

When analysing the type of malware detected on the computers and devices of those interviewed based on what was detected by the Pinkerton software, most was malware that aims to economically benefit its creators. Thus, the types of malware most present on personal computers are adware (49.1%) and Trojans (33.4%). On Android devices we see the same types, but at lower rates: 13.2% and 14%, respectively.

This reveals the true motives of the developers: to prevent the malware from being detected, because if it goes unnoticed there is great potential for economic gain.

FIGURE 15. DIVERSIFICATION OF DETECTED MALWARE (%)



Base: Computers hosting malware
Source: Household panel, ONTSI

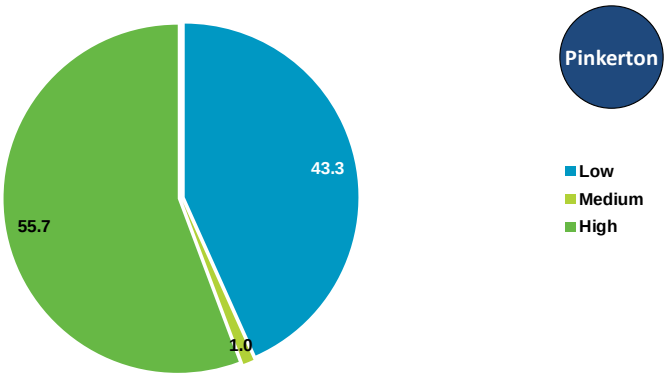
A unique variant of malware is each of the different samples detected, regardless of the number of times they appear on scanned equipment.

Some 94.1% of malicious files detected on personal computers and some 97.4% of those detected on Android devices were unique variants.

This new data highlights another of the guidelines followed by malware programmers. They are increasingly focusing their efforts on developing new variants of their codes, and even personalising malware when it infects a system so that it can only be executed on that system. In this way they can get practically every sample to be unique. The reason for this is once again to prevent detection by antivirus engines.

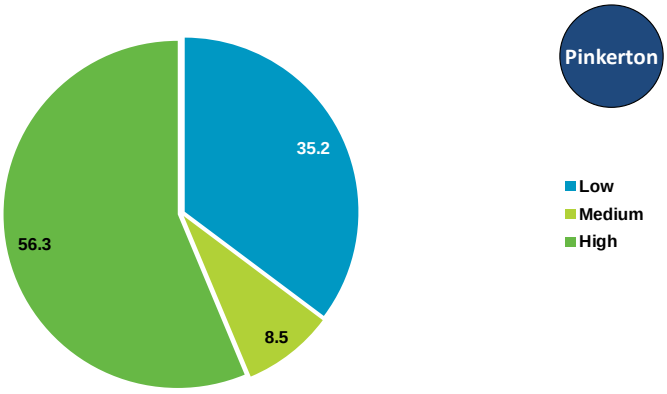
FIGURE 16. RISK LEVEL ON PERSONAL COMPUTERS (%)

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



Base: PCs hosting malware
Source: Household panel, ONTSI

FIGURE 17. RISK LEVEL ON ANDROID DEVICES (%)

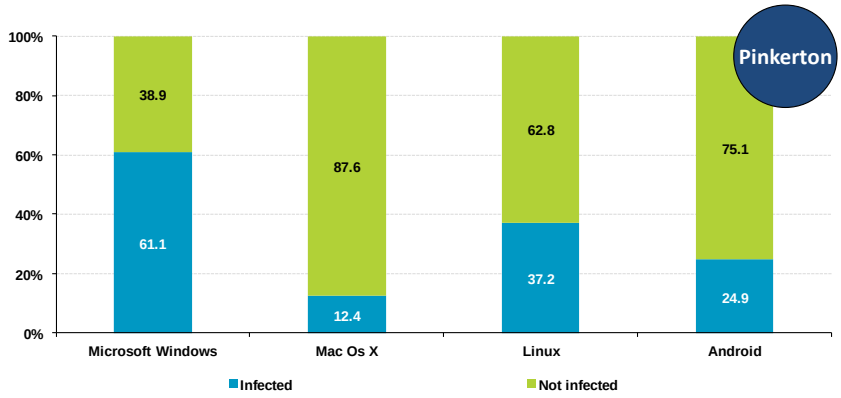


Base: Android devices hosting malware
Source: Household panel, ONTSI

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.

According to this classification, around 56% of the personal computers and Android devices that are infected by malware are at a high risk level due to the dangerousness of the malware.

FIGURE 18. 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 incidents: up to four times more than other platforms.

This fact can be explained using three main hypotheses:

- The greater use of Windows operating systems compared to Mac OS and GNU/Linux by users. Developers of malicious code attempt to hit the maximum number of possible targets, and they can do so by developing malware for the operating systems that are most widely used by users.

- The use of unauthorised 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 in order to get users to install it on their equipment. Moreover, in this case even security warnings are ignored in anticipation of having the software installed on the computer or device.

- Taking advantage of user trust by including a certain type of malware in programmes that are normally free, or test versions, for which the installation process includes a verification window, checked by default, that allows them to be installed on computer equipment with user "acceptance."

What's more, the Windows XP life cycle came to an end in April 2015. This means that Microsoft no longer provides support for this operating system and has stopped releasing security updates for it, making it an obsolete and potentially vulnerable system. However, it continues to be used by a significant number of users.

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, in Mac OS and GNU/Linux programmes 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.

In terms of the Android platform, malware is still not as widespread as on computers and servers. Still, one in four devices came back with positive results in the Pinkerton scan. Just as with PCs with Windows operating systems, this can be explained using the following hypotheses:

- The usage rate of the Android system on mobile devices. As mentioned above, malware developers focus on the most widely-used systems. Moreover, smartphones and mobile devices are increasingly being used as a replacement for personal computers on both a personal and professional level. So the interest in these devices is hardly a surprise.

- 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.

1.4 Consequences of security incidents and user reactions

This section will determine the consequences of the security incidents that have occurred as well as user reactions and prudent security measures and habits adopted and/or modified in order to prevent them from happening again.

Practically two out of three Internet users interviewed reported having been involved in some kind of online fraud situation.

But which types of fraud situations are perceived by users?

To answer this question we must analyse the following graphic.

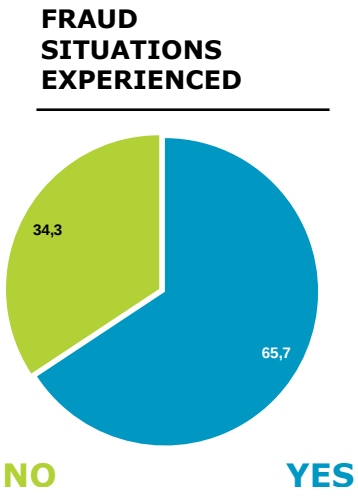
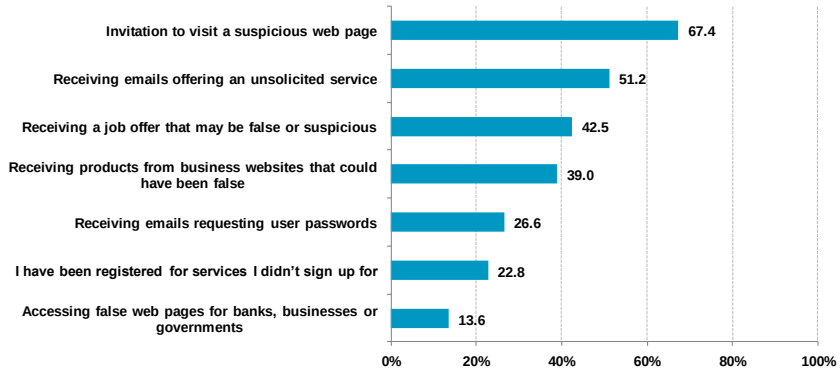


FIGURE 19. MANIFESTATION OF INTENT (NOT CONSUMMATED) TO COMMIT ONLINE FRAUD (%)



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

The most common occurrence of attempted fraud of all those perceived by Spanish Internet users who have experienced attempted fraud is an invitation to visit a suspicious web page (67.4%).

In half of the cases (51.2%), the attempted fraud reaches the user in the form of an offer for non-solicited services and, in 42.5% of cases it is in the form of a false or suspicious job offer, taking advantage of the current economic situation.

More than one in four panellists were registered for services they did not sign up for. This reported fraud includes subscription to SMS Premium services that entail a certain cost for each SMS message received, among other services.

The form of attempted fraud that was perceived the least, by only 13.6% of users who reported having experienced attempted fraud, are false web pages (phishing) that attempt to impersonate banks, online stores or governments in order to trick users and obtain their credentials, and then operate in their name.

Online fraud campaigns generally use email as a means of propagation, mainly because it is easy, quick and cheap to send mass messages, which are received immediately. In addition to convincing users to perform actions to consummate the fraud, the sender often tries to conceal themselves by impersonating a trusted entity that brings some reliability to the communication established. The following table shows the entities most impersonated for each type of communication suspected of being fraudulent.

TABLE 3. METHODS USED BY THE SENDER BY TYPE OF SUSPICIOUS COMMUNICATION (%)

Manifestation of fraud	Form taken by the sender of the communication (%)											
	Bank	E-commerce	Payment methods	Social networks	Government authorities	Telecommunications	NGOs and foundations	Auctions	Lottery	Security forces	Individual	Other
Receipt of email requesting login details	**54.2**	35.1	32.2	33.5	13.5	26.4	15.3	23.8	35.6	15.9	31.2	7.2
Receipt of email offering an unsolicited service	34.0	**42.5**	20.6	28.4	8.3	31.7	14.4	24.5	41.5	11.1	31.9	12.7
Receipt of email with invitation to visit a suspicious website	33.5	**35.6**	20.3	27.5	8.8	24.4	12.7	20.9	35.0	8.8	28.9	14.5
Receipt of a job offer online that may have been false or suspicious	35.8	35.2	23.3	29.5	10.6	26.0	14.0	22.1	35.2	11.9	**42.0**	14.4
Receipt of products from e-commerce pages that may have been false	35.7	43.5	25.0	32.6	10.3	30.2	16.1	28.9	**43.5**	12.4	34.0	10.6
Access to false banking, e-commerce or Government authority websites	**53.1**	32.3	33.1	28.4	21.9	30.7	20.5	25.0	39.0	25.4	29.8	7.9
I have been registered for services I didn't sign up for	32.1	**45.1**	26.4	33.3	10.5	37.7	18.2	25.1	40.2	10.5	31.6	14.1

Base: Users who have experienced each specific type of attempted fraud
Source: Household panel, INCIBE, ONTSI

The main method used by senders is to impersonate banks and attempt to request user passwords (54.2%), or false web pages (*phishing*) for banks, e-commerce, etc. (53.1%).

On the other hand, e-commerce entities are preferred for registering users for services they have not signed up for (45.1%), receiving products from suspicious e-commerce pages (43.5%), and offering unsolicited services (42.5%).

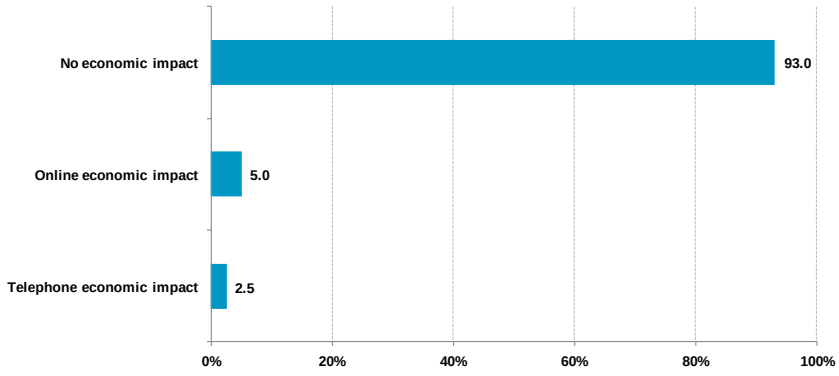
We can also note that the image of social networks is used as a sender in practically one of every three cases to spread fraud attempts.

ECONOMIC DAMAGE DUE TO FRAUD

5.0%
OF ONLINE FRAUD

2.5%
OF TELEPHONE FRAUD

FIGURE 20. ECONOMIC IMPACT OF FRAUD (%)



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

As we have seen, attempted fraud situations occur very regularly, and have been experienced by two out of three Internet users. But the percentage of fraud that is consummated and has economic repercussions for the victim is actually low: 5% of fraud

attempts on the Internet and 2.5% of fraud attempts by telephone.

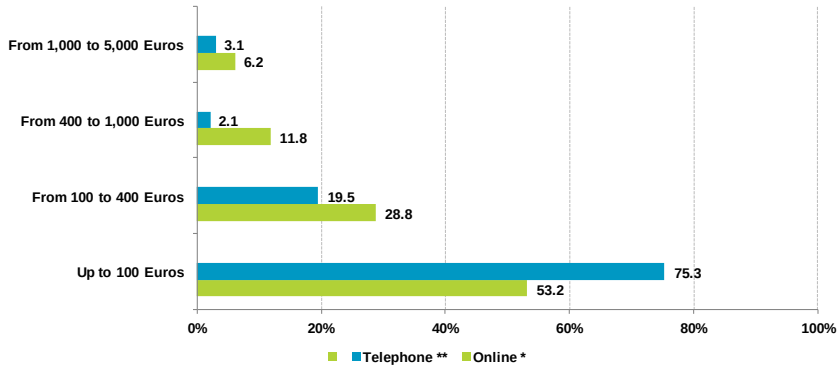
This difference, although small, lies in the preference for email over the telephone as a means of attempted fraud. One of the main reasons is related to the economic cost and time involved in making telephone calls and/or sending text messages to all the potential victims, compared with the ease, speed and low cost of sending mass emails.

Another reason is the immediacy of email, which can reach a large number of users practically instantaneously. This maximises the time window for consummating the fraud before being detected.

Email takes advantage of the trust of the recipient as there is no two-way communication to request more information, while in a telephone conversation there is an exchange of information.

Even the language barrier constitutes an obstacle to attempted telephone fraud, as it must be more localised and perpetuated by people with a good command of the language in order to be able to improvise responses to questions from potential victims.

FIGURE 21. 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 economic limit of 400 Euros set by the Spanish Penal Code to distinguish between felony and misdemeanour has an enormous impact on fraud attempts.

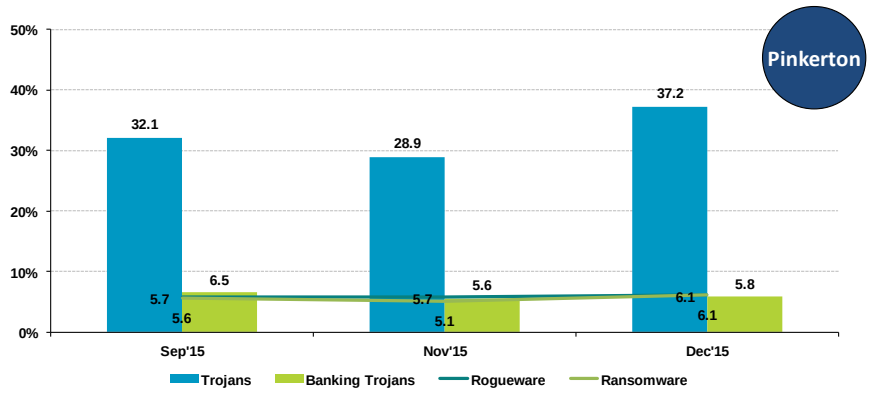
Thus, most consummated frauds have an economic impact below this limit: 53.2% of online fraud cases and 75.3% of telephone fraud cases have an impact of below 100 Euros, while in 28.8% and 19.5% of cases (respectively) the impact is between 100 and 400 Euros.

In this way, to avoid taking larger risks, fraud attempts that entail economic damage above this limit occur only occasionally.

Type of malware scanned

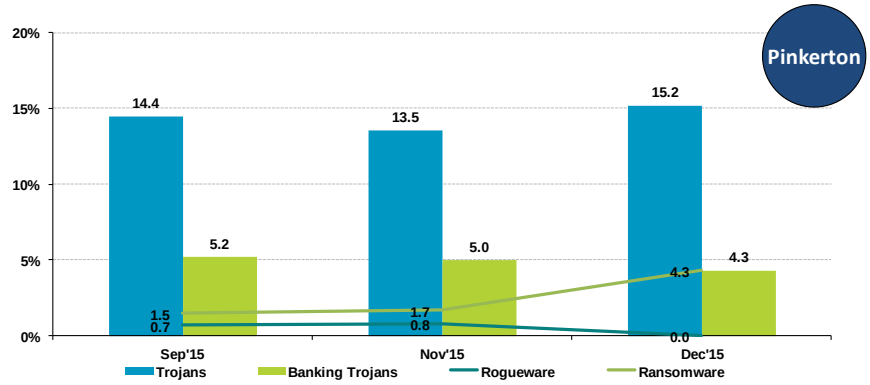
- Banking Trojan: malware that steals confidential information from customers of banks and/or online payment platforms.
- Rogueware or rogue: malware that makes victims think they have been infected by some kind of virus, getting them to pay a certain sum of money to remove it. The user is usually asked to purchase a false antivirus programme, 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 22. BANKING TROJANS AND ROGUEWARE ON PERSONAL COMPUTERS(%)



Base: All computers
Source: Household panel, ONTSI

FIGURE 23. BANKING TROJANS AND ROGUEWARE ON ANDROID DEVICES (%)



Base: All Android devices
Source: Household panel, ONTSI

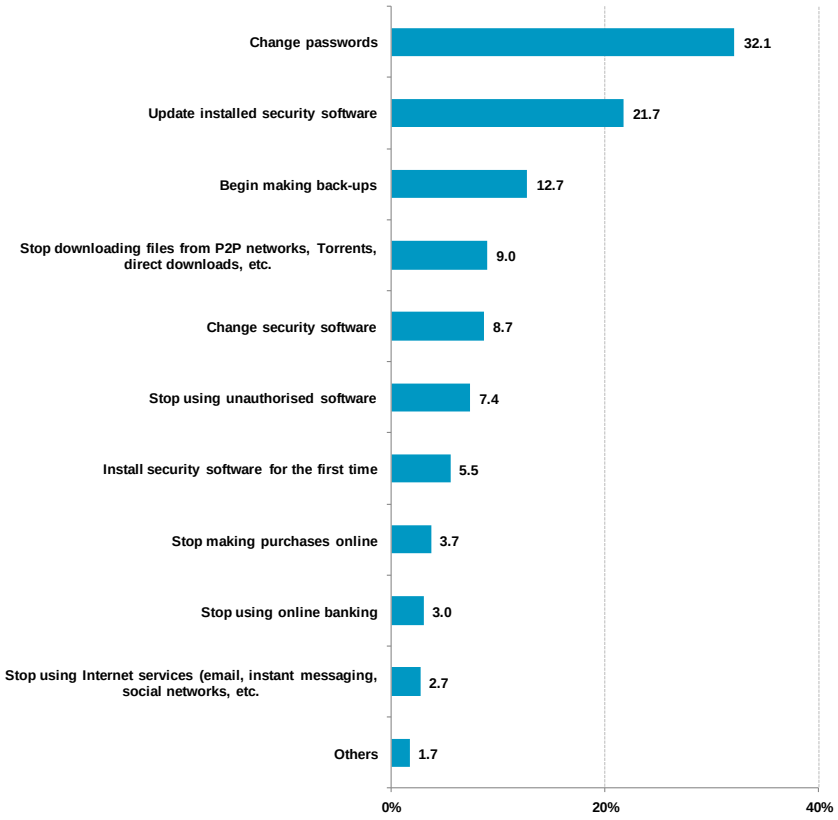
Another way for fraud to be carried out is through malware: banking Trojans, rogueware and ransomware. The purpose of these types of malware is to try to cause economic damage to affected users and, in the case of the first two, to go unnoticed by the user.

Yet not all computers and devices that host banking Trojans necessarily end up experiencing a fraud situation. A series of requirements must be met for a fraud to be consummated using these methods, for instance: infecting the user's computer or device, affecting the user's bank, the user must log onto the electronic banking system and fill in the additional data that the malware is seeking without suspecting anything.

The analysis of the malware samples detected by Pinkerton during the second half of 2015 shows that between 5% and 6% of computers in Spanish households are infected by some banking Trojan, rogueware or ransomware.

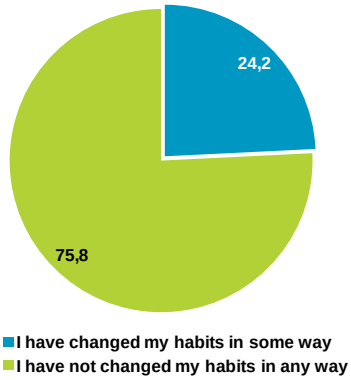
Among the Android devices analysed by Pinkerton the presence of Trojans is significantly lower than on personal computers, however the proportion of banking Trojans is similar to those on personal computers: around 5% of devices. The appearance of rogueware and ransomware on these devices is much lower.

FIGURE 24. REACTIONS AFTER HAVING EXPERIENCED A SECURITY INCIDENT (%)



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

MODIFICATION OF HABITS



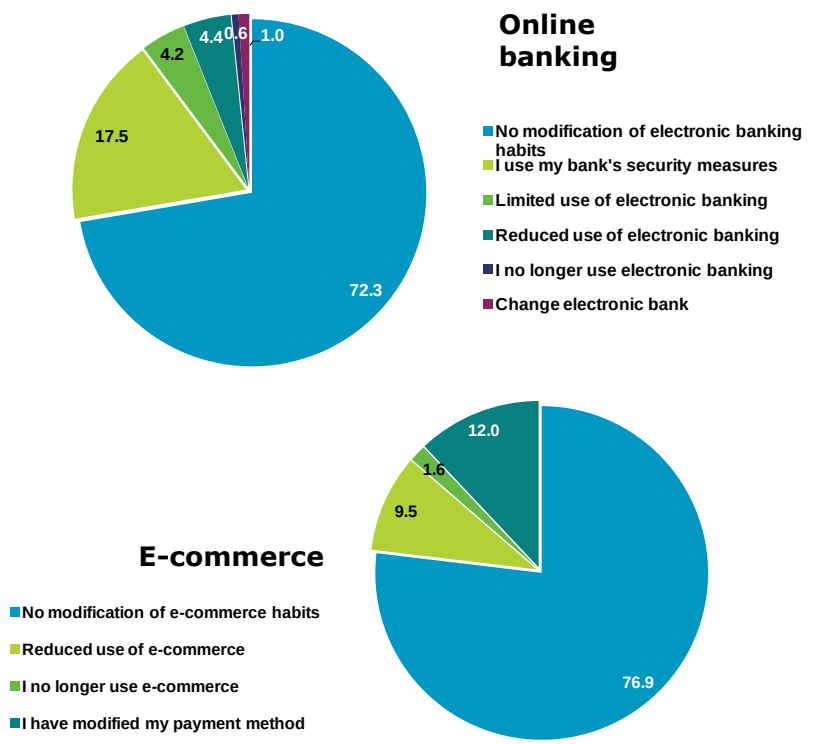
After experiencing a security incident, users decide to modify their behaviour habits and security measures, take new ones, and even use the different services offered on the Internet to try to prevent new incidents from happening in the future, or if they do happen, to minimise their consequences. This is done by 24.2% of users

According to responses provided by users, the main reaction following a security incident is to change passwords (done by 32.1%) if they could have been compromised. Updating security software that is already installed (21.7%) is another of the most frequent reactions to security incidents.

Less common reactions are to stop using the online bank, e-commerce site or other Internet services. These is done by less than 3.7% of Internet users, which is an indication of the trust placed in these services.

However, continuing to use a service does not mean not modifying any of the habits related to it after experiencing attempted fraud. Below we analyse the modification of habits related to online banking and e-commerce.

FIGURE 25. MODIFICATION OF HABITS RELATED TO ONLINE BANKING AND E-COMMERCE AFTER EXPERIENCING ATTEMPTED FRAUD (%)



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

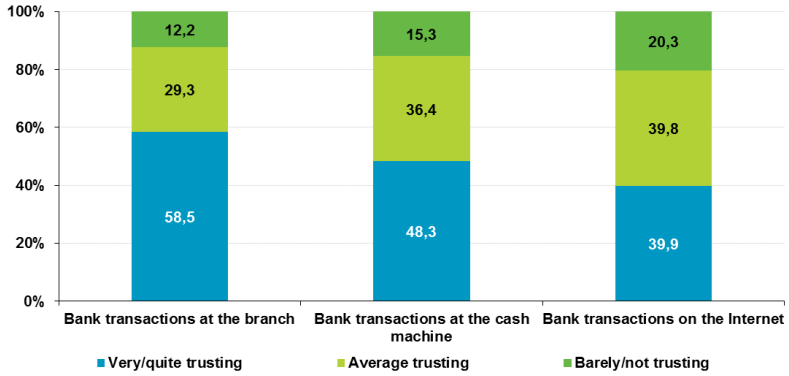
We can confirm that the level of trust in online banking and e-commerce services is high among Spanish users, given that approximately three out of four do not alter their usage habits whatsoever.

The most common changes are the use of security measures offered by the bank itself (17.5%) and changing the payment method (12%) on online stores.

1.5 Trust in the digital environment in Spanish households

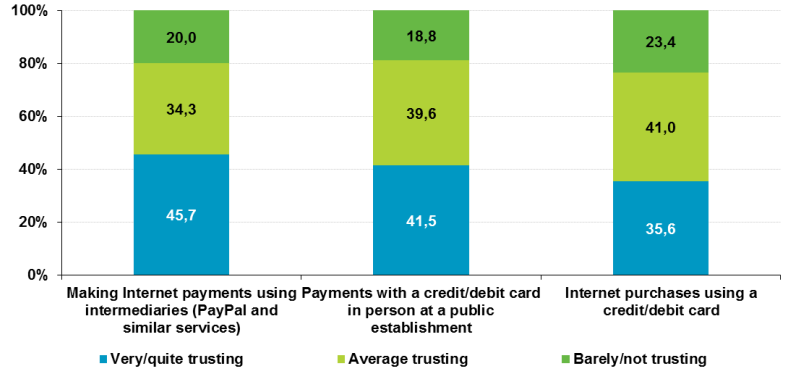
The study concludes with an analysis of the level of trust in Spanish users.

FIGURE 26. LEVEL OF TRUST IN BANK TRANSACTIONS (%)



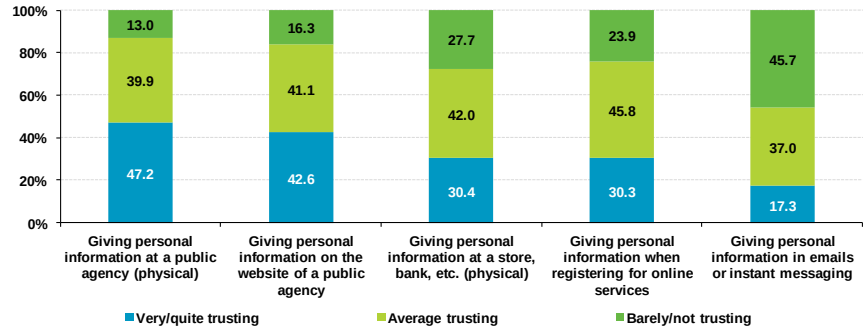
Base: users of online banking
Source: Household panel, ONTSI

FIGURE 27. LEVEL OF TRUST IN E-COMMERCE OPERATIONS (%)



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

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



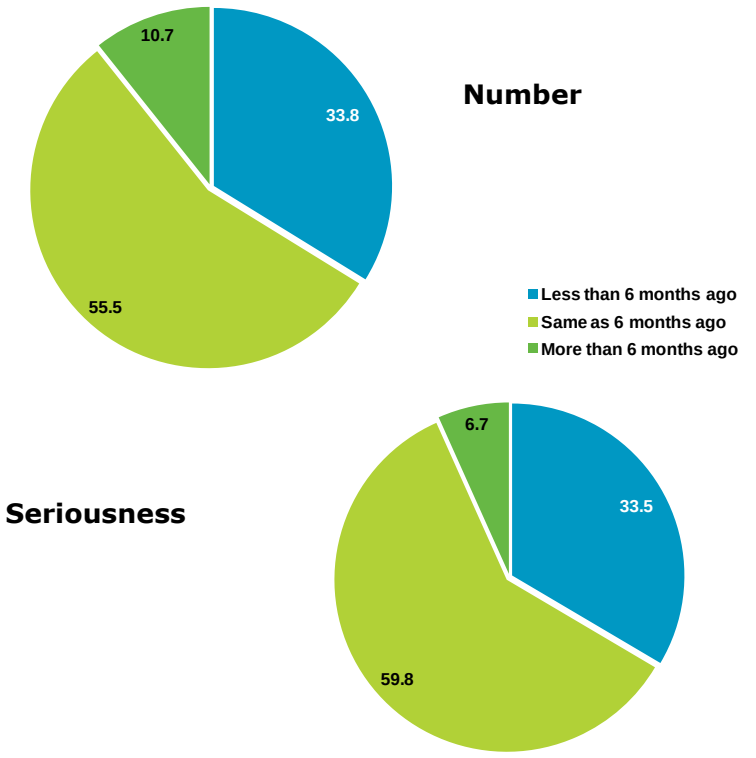
Base: all users
Source: Household panel, ONTSI

In general, physical services inspire a higher level of trust in users than their digital counterparts. In this context, the largest gap between a physical and online service is noted for bank transactions (over 18 percentage points).

It is worth noting that Internet users place greater trust in intermediaries like PayPal for making online transfers than in payments made using a credit/debit card in a public establishment (45.7% and 41.5%, respectively).

However, there seems to be less concern with regard to providing personal data: fewer than half (45.7%) of Spaniards are distrustful when providing this information by email or instant messages.

FIGURE 29. PERCEPTION OF THE NUMBER AND SERIOUSNESS OF SECURITY INCIDENTS (%)

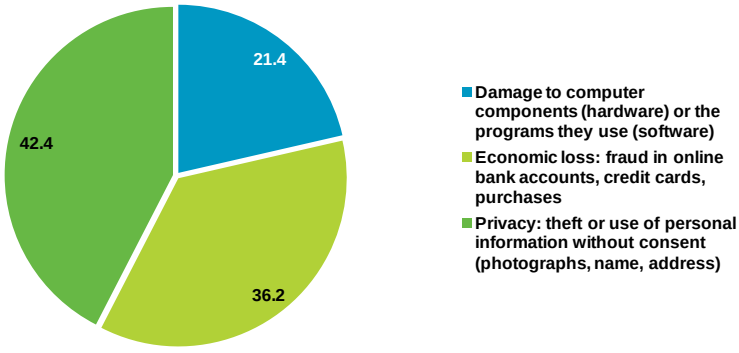


Base: all users
Source: Household panel, ONTSI

According to the perception of Internet users, the number of security incidents that occurred during the last three months is similar to those observed in the previous months for more than half of those surveyed (55.5%). In terms of the seriousness of these incidents, nearly 60% of panellists consider it to have stayed the same.

A third of users even believed that both the number of incidents and their seriousness decreased during this period.

FIGURE 30. PERCEPTION OF RISKS ON THE INTERNET (%)

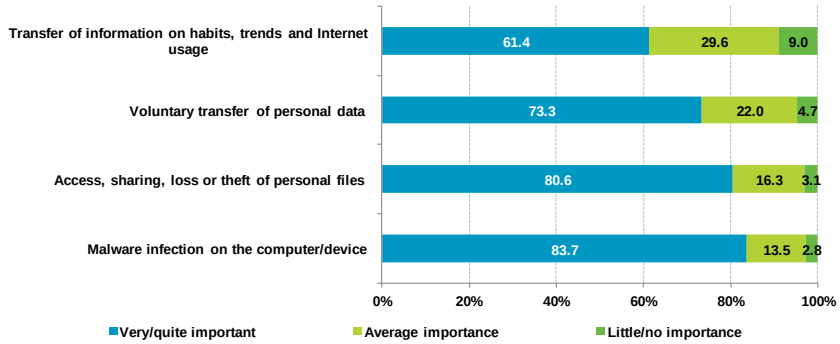


Base: all users
Source: Household panel, ONTSI

Spanish Internet users think that the main risk of using the Internet concerns privacy violations. For 42.4% of them, the most frequent threat is the theft and use of personal information (name, address, photographs, etc.) without user consent.

They believe the second greatest threat to be economic damage derived from attempted fraud via the Internet, based on the statements of 36.2% of the panellists.

FIGURE 31. ASSESSMENT OF THE DANGERS OF THE INTERNET (%)

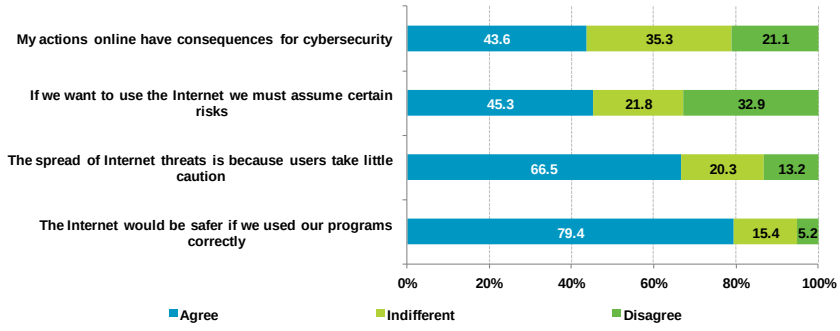


Base: all users
Source: Household panel, ONTSI

It is interesting to see the level of importance known risks spark in users. The responses from panellists show that the importance accorded to privacy -it is worth recalling that this is the main risk perceived by Internet users- is relegated to third and fourth place, depending on whether it is the transfer of personal data (73.3%) or information about Internet habits, trends and usage (61.4%), respectively.

At the top of the list is malware infection (83.7%) and access, loss or theft of personal files stored on the computer or mobile device (80.6%).

FIGURE 32. RESPONSIBILITY FOR INTERNET SECURITY (%)



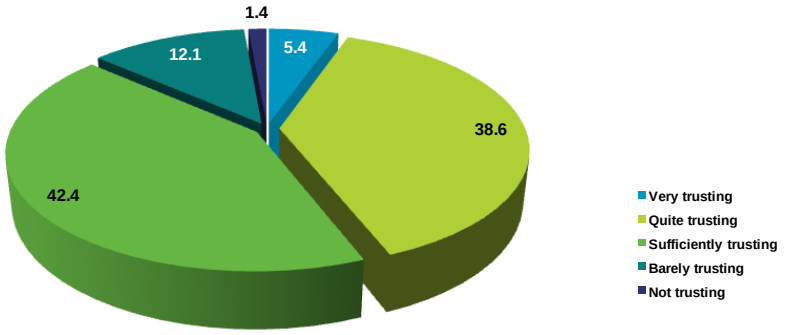
Base: all users
Source: Household panel, ONTSI

Being aware of the repercussions that one's actions have on Internet security can have a positive influence on prudent habits, the use of security measures, and risky behaviour, in such a way that it can translate into a decrease in security incidents. Some 43.6% of Spanish Internet users are aware of their responsibility for Internet security and the consequences of their online actions.

Moreover, two out of three think that the propagation of threats online is mainly due to the lack of caution shown by users themselves. And they even think that the Internet would be more secure if the programmes and tools available to users were used correctly, according to 80% of respondents.

However, nearly half agree that is necessary to take risks -putting both their computers or devices and their information in danger- in order to fully enjoy the Internet experience.

FIGURE 33. LEVEL OF TRUST IN THE INTERNET (%)



Base: all users
Source: Household panel, ONTSI

Some 44% of Internet users report being very or quite trustful online. The Internet inspires little trust for 9.9% of the Spanish population, while 0.9% report having no trust in it.

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
Technical team:
Raquel Castro García-Muñoz
Santiago Cadenas Villaverde
Jose Antonio Seco Arnegas

ISSN 2386-3684

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