Study on Cybersecurity and trust in spanish households

July – December 2016 Series

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

ontsi observatorio nacional de las telecomunicaciones y de la SI

March 2017

CONTENT

Introduction to the study

1. **Presentation**
2. **Objectives**

Presentation

The National Telecommunications and Information Society Observatory (ONTSI) of Red.es has designed and promoted the:

Study on Cybersecurity and Trust in Spanish households

This research is a benchmark in diagnosing the status of cybersecurity in Spanish digital households. It analyses security measures adopted and the rate of situations that can entail security risks, as well as the level of trust that Spanish households place in the Information Society.

The data presented in this report have been extracted using different methodologies:

- Reported data: Obtained from online surveys conducted among 3,516 households in the study sample.
- Real data: We used **Pinkerton** software developed by Hispasec Sistemas, which analyses the systems by gathering data from the operating system, its update status and the security tools installed. **Pinkerton** also detects the presence of malware on computers and mobile devices by using a combination of 50 antivirus engines. The data extracted this way are shown in this report with the following label:

The data reflected in **this report cover analysis from July to December 2016.**

Presentation

This report includes information on the data presented during studies previously conducted on cybersecurity and trust in Spanish households.

The objective is to be able to contrast this information with that obtained in this study, and thus be able to determine the evolution in the field of cybersecurity and digital trust.

We have used the following names for each study:

- **1Q14**, study conducted during the first quarter of 2014 (February - March).
- **2Q14**, study conducted during the second quarter of 2014 (April - June).
- **2H15**, study conducted during the second half of 2015 (July - December).
- **1H16**, study conducted during the first half of 2016 (January - June).
- **2H16**, study conducted during the second half of 2016 (July - December).

Objectives

1

The **overall objective** of this study is to **analyse the real status** of **cybersecurity and digital trust** among Spanish Internet users and, at the same time, compare the real level of incidents suffered by computers and mobile devices with user perception, and show the evolution over time of these indicators.

We also want to **foster specialised and useful knowledge** of **cybersecurity and privacy** to improve the implementation of measures by users

The objective is also to reinforce the **implementation of policies and measures** by the Government, directing public initiatives and policies to generate trust in the Information Society and to improve individual security, based on a realistic perception of their benefits and risks.

Security measures

1. Definition and classification of security measures
2. Use of security measures on the household computer
3. Security measures used on wireless Wi-Fi networks
4. Use of security measures on Android devices
5. Reasons for not using security measures

Definition and classification of security measures

Security measures[1]

They are programs or actions used by the user to protect the computer and the data on it. These tools and actions can be used with direct user intervention **(automatable and non-automatable)** and they can also be measures before or after a security incident **(proactive, reactive or both).**

Automatable measures

Are those **passive** measures that generally do not require **any action from the user**, or whose configuration allows automatic implementation.

Non-automatable measures

Are those **active** measures that generally **require a specific action by the user** for correct operation.

Proactive measures

Are those measures used to **prevent and avoid**, as much as possible, security incidents occurring and to minimise possible **unknown and known threats**.

Reactive measures

Are those measures used to **correct** security incidents, in other works, they are the measures used to eliminate **known threats and/or incidents occurred**.

Tools that will help you protect your devices: https://www.osi.es/herramientas

[1] There are security measures that can be classified in various categories, e.g. antivirus programs and their updates, or operating system measures. Due to its nature, an antivirus program can detect existing threats on the computer and threats that try to enter it.

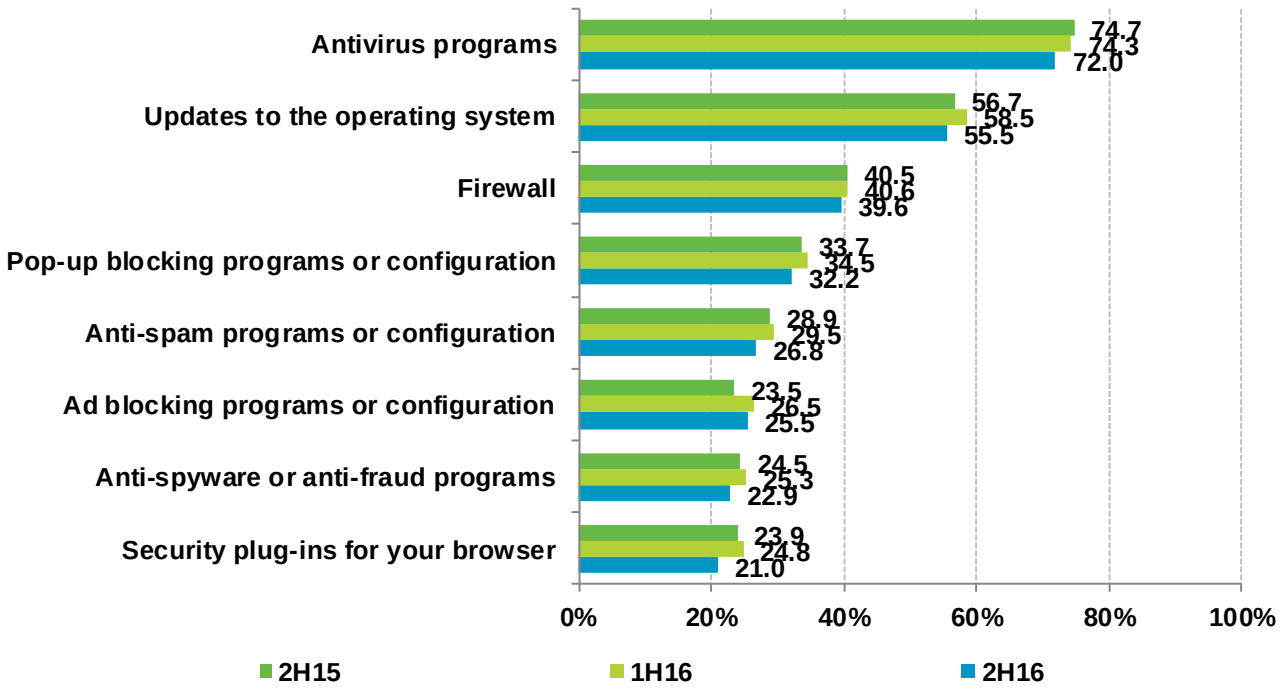
Definition and classification of security measures

	Automatable measures	Non-automatable measures
Proactive	• Firewall	• Passwords • File backups • Partitioning of the hard drive • Digital electronic signature certificates • Regular use with reduced permissions • Electronic DNI • Document or data encryption • Use of virtual machines
Proactive and reactive	• Antivirus program • Updates to the operating system and programs • Antivirus updates	
Reactive	• Browser plug-ins • Pop-up window blocking programs • Banner blocking programs • Anti-spam programs • Anti-fraud programs.	• Deleting temporary files or cookies.

Use of security measures on the household computer

Automatable security measures

There is a downward trend in the use of automatable security measures compared to the previous study. The main measures are **antivirus software** (**72.0%**) and **updates to the operating system** (**55.5%**).



Antivirus program functions are only limited to eliminating malware on the computer. Their most important task is to prevent and avoid malware infections.

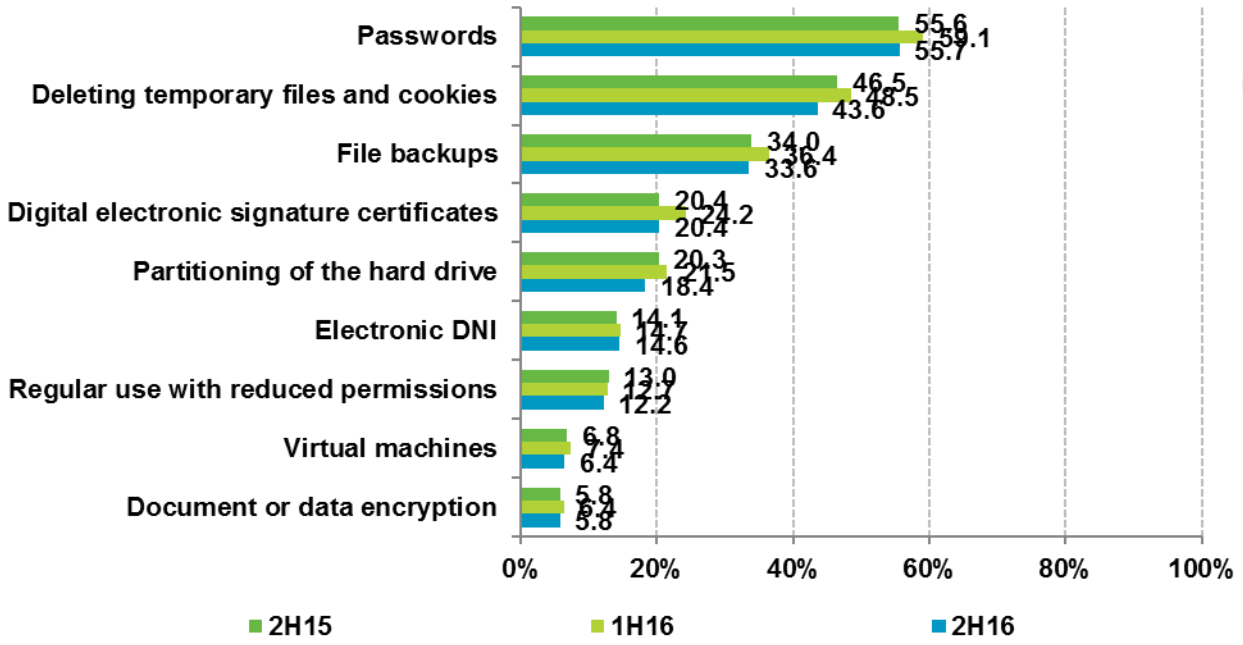
https://www.osi.es/contra-virus

BASE: PC Users

Use of security measures on the household computer

Non-automatable or active security measures

There is a decrease in use of practically all active or non-automatable security measures.



Active security tools are the most secure layer offered by systems.

They are the main measures in terms of physical security when automatable measures are avoided.

BASE: PC Users

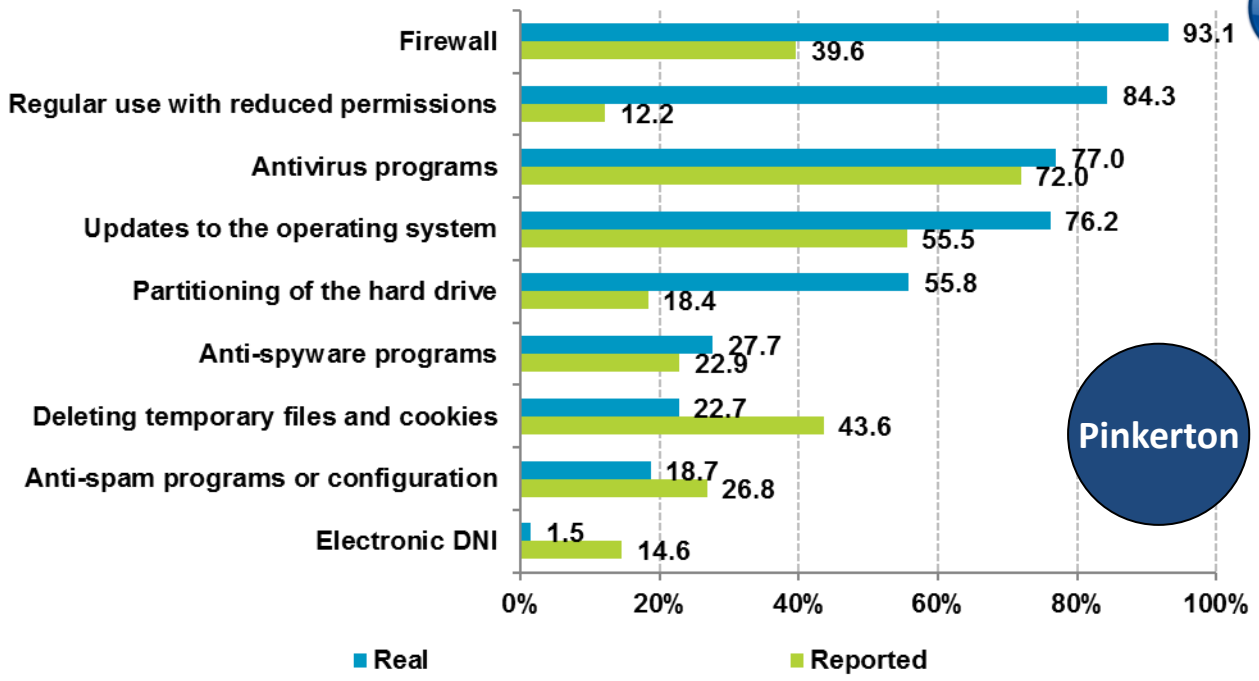
It is extremely important to use passwords etc. correctly, and create backups of the data we want to save. For more information on these tasks:

- ✓ **Passwords:** https://www.osi.es/contrasenas
- ✓ **Backups:** https://www.osi.es/copias-de-seguridad-cifrado

Use of security measures on the household computer

Reported vs real use of security measures

Less than **40%** of the Internet users report using **firewall** software on their computers. However, the data obtained with Pinkerton reveals that this type of program is <u>really</u> found on **93.1%** of the computers scanned.



BASE: PC Users

Malware is all the programs and malicious code whose purpose is to infiltrate a computer without the user's consent.

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

https://www.osi.es/es/actualidad/blog/2014/07/18/fauna-y-flora-del-mundo-de-los-virus

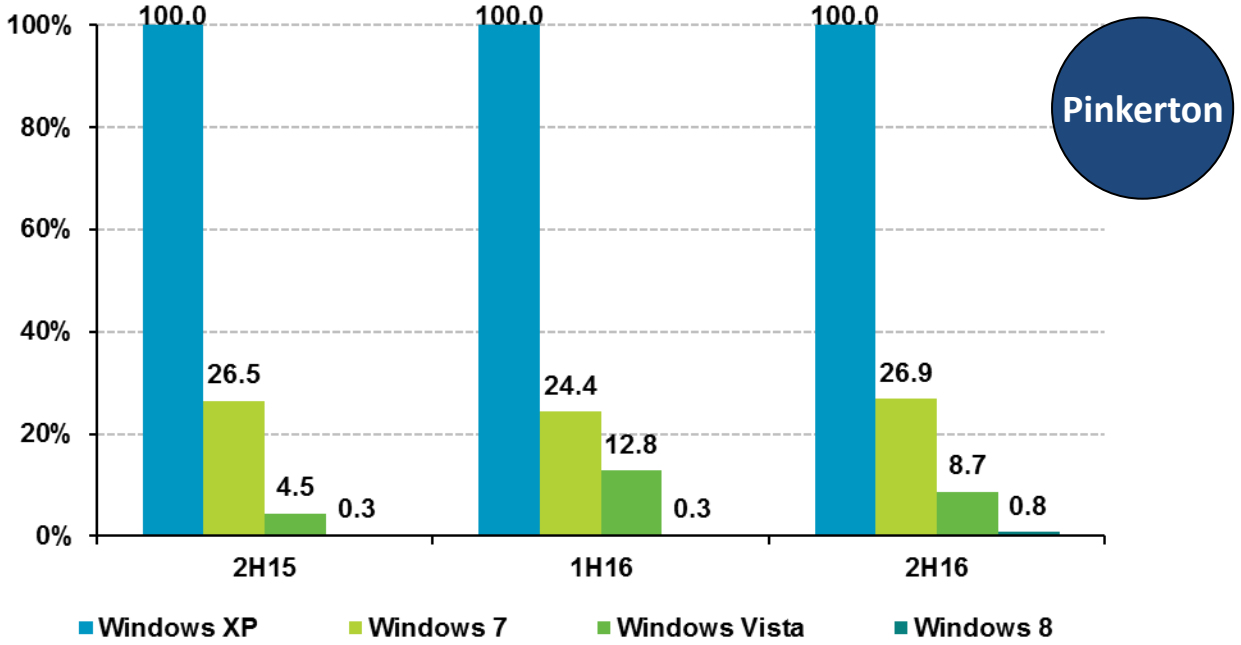
To obtain the real data, we used **Pinkerton** software developed by Hispasec Sistemas. This scans the systems and the presence of malware on computers using a series of 50 antivirus engines. **Pinkerton** is installed on the computers and scans them, detecting the malware on them and collecting data from the operating system, its update status and the security tools installed.

Use of security measures on the household computer

Real use of profiles with administrator privileges on Microsoft Windows

Use the standard user account for daily computer use. Use the administrator account only when strictly necessary. More information on user accounts and how to configure them: https://www.osi.es/cuentas-de-usuario

The difference between the level of privileges used in the different Windows versions must be configured by default applied to the user account.

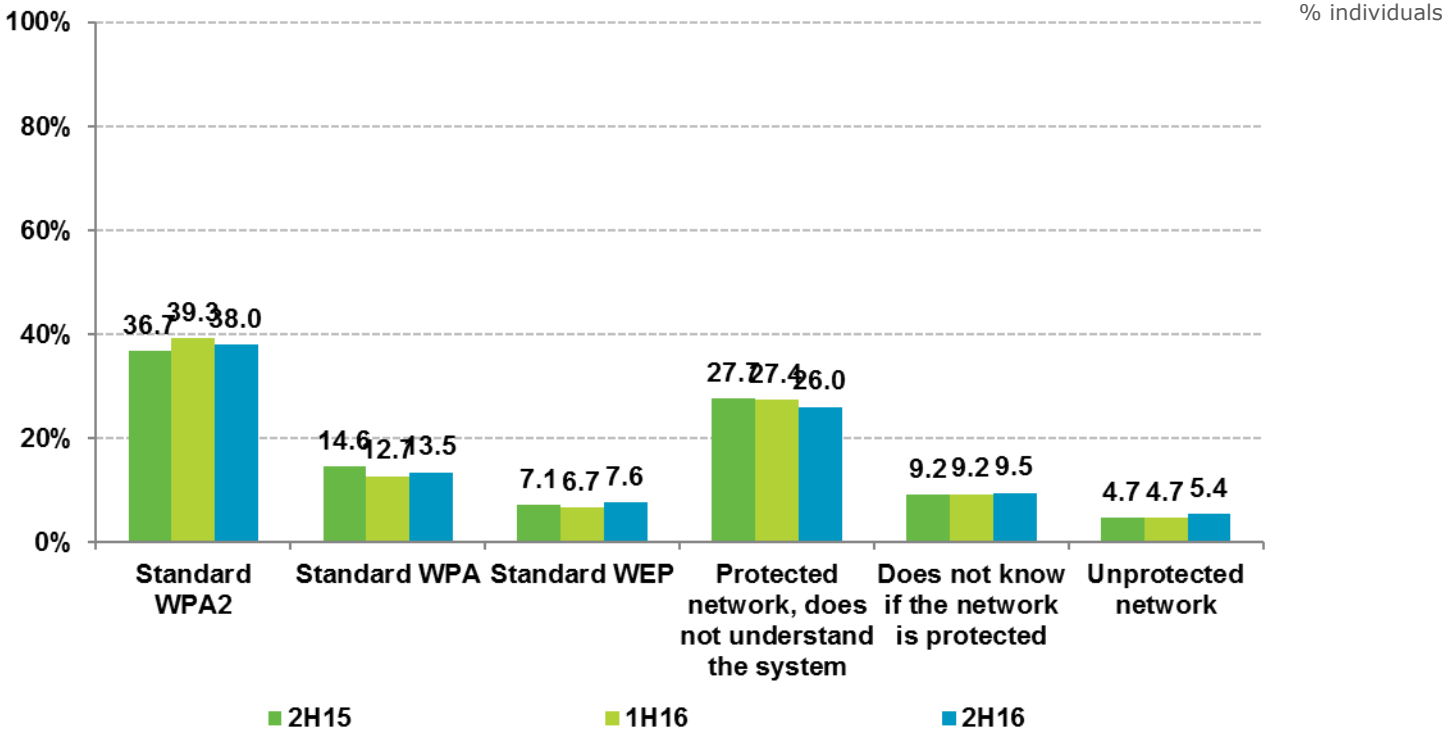


BASE: Microsoft Windows users

There may be Windows 10 operating systems 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.

Security measures used on wireless Wi-Fi networks

Over half (**51.5%**) use **WPA** and **WPA2**. **14.9%** of users leave their wireless Wi-Fi network **unprotected** and/or **do not know** its status.

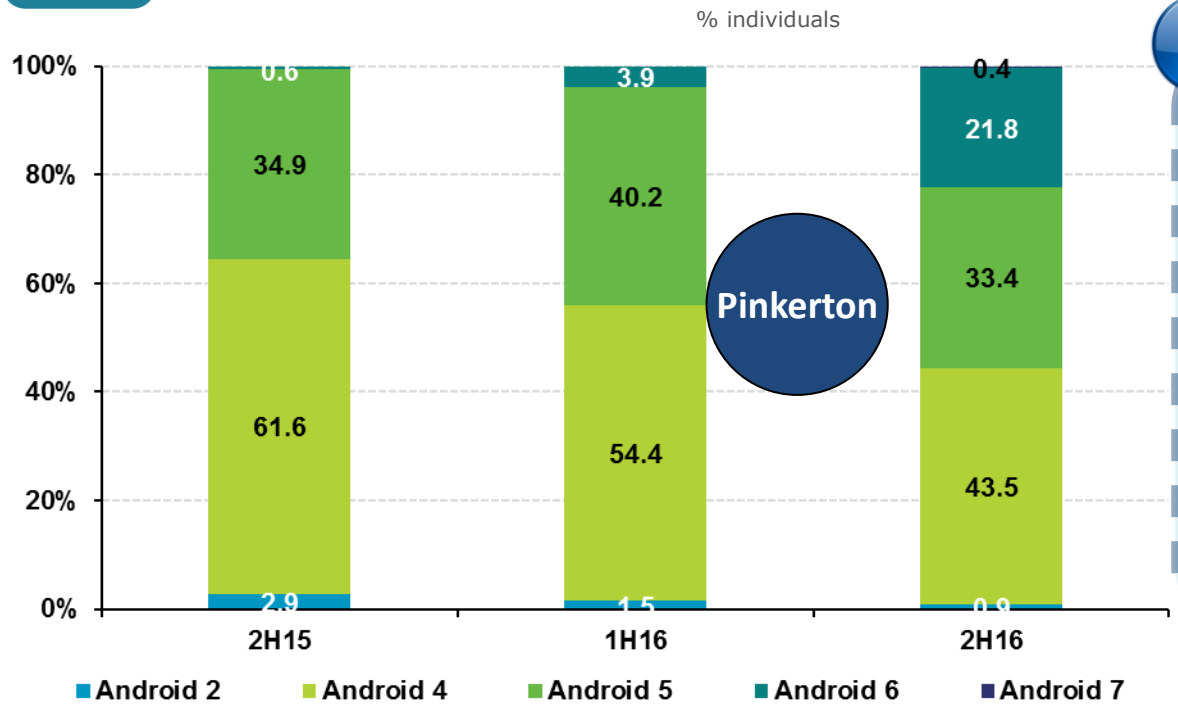


How to securely configure your Wi-Fi network: https://www.osi.es/protege-tu-wifi

BASE: Users with their own Wi-Fi connection

Operating system version on Android devices

Android 4 is still the most used version on smartphones and tablets (**43.5%**). Meanwhile, Android 6 has experienced a major increase (**+17.9 p.p.**) since the last period analysed.



It is highly recommendable to maintain the operating system updated to the latest version available to prevent the device being vulnerable or affected by problems or errors known and corrected in the latest Android versions.

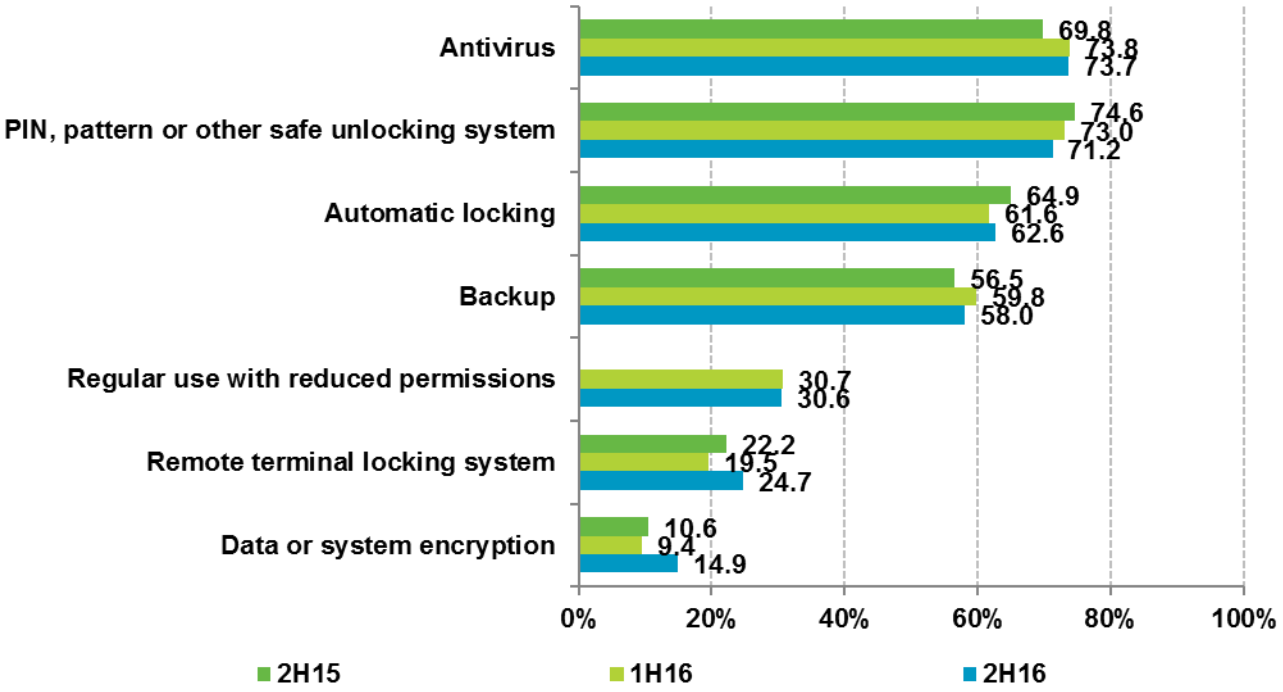
Remember that the 4.x Android version is not supported.

BASE: Users with an Android device

The official list on Android distributions confirms that version 4 is the most used: **Android Develop dashboard:** https://developer.android.com/about/dashboards/index.html

Use of security measures on Android devices

The main security measures reported by mobile device users are **antivirus software** (**73.7%**), the use of **secure unblocking systems** using PINs or patterns (**71.2%**) and **automatic device blocking** after a period of inactivity (**62.6%**).



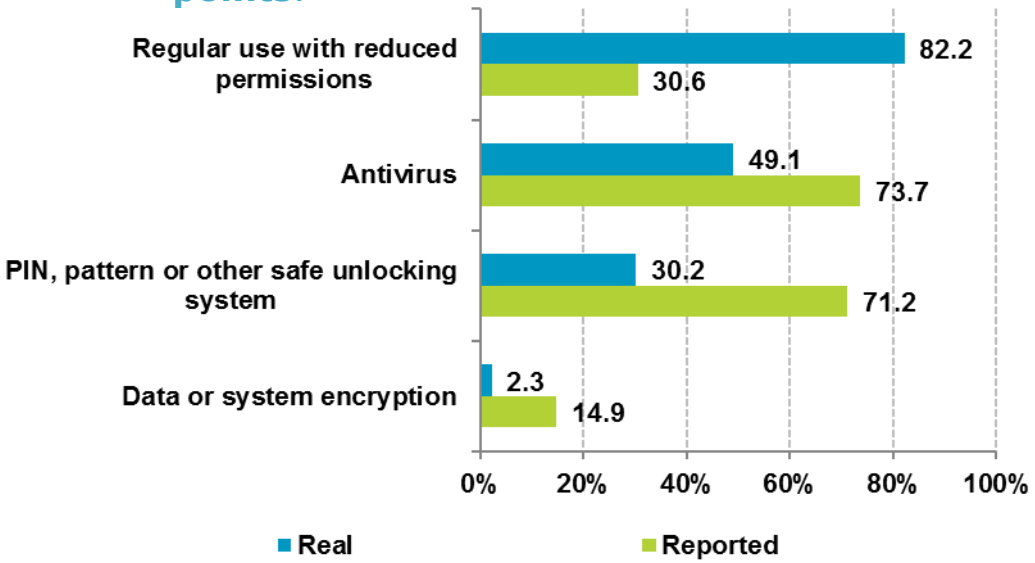
BASE: Users with an Android device

Use of security measures on Android devices

Reported vs real use of security measures

73.7% of users say they use an **antivirus** program on their mobile device, but the real data provided by **Pinkerton** reveals that they are only found on **49.1%** of devices scanned.

The **PIN, pattern or other secure unblocking system** is the measure that shows the **most distance between real and reported use**, standing at **41 percentage points**.



Pinkerton

The use of a secure unblocking system using a **pattern, PIN, biometric systems**, etc., is a simple way to prevent **unauthorised or undesired access** to the mobile device and its content, **protecting the user's privacy**.

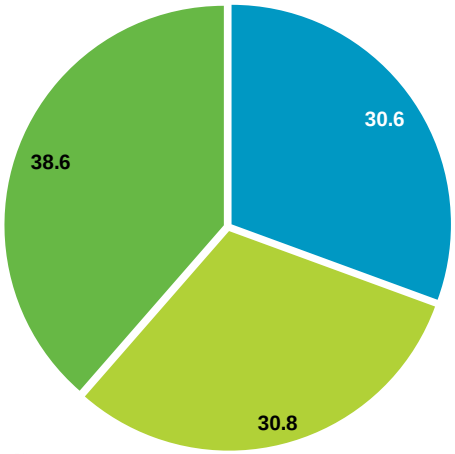
BASE: Users with an Android device

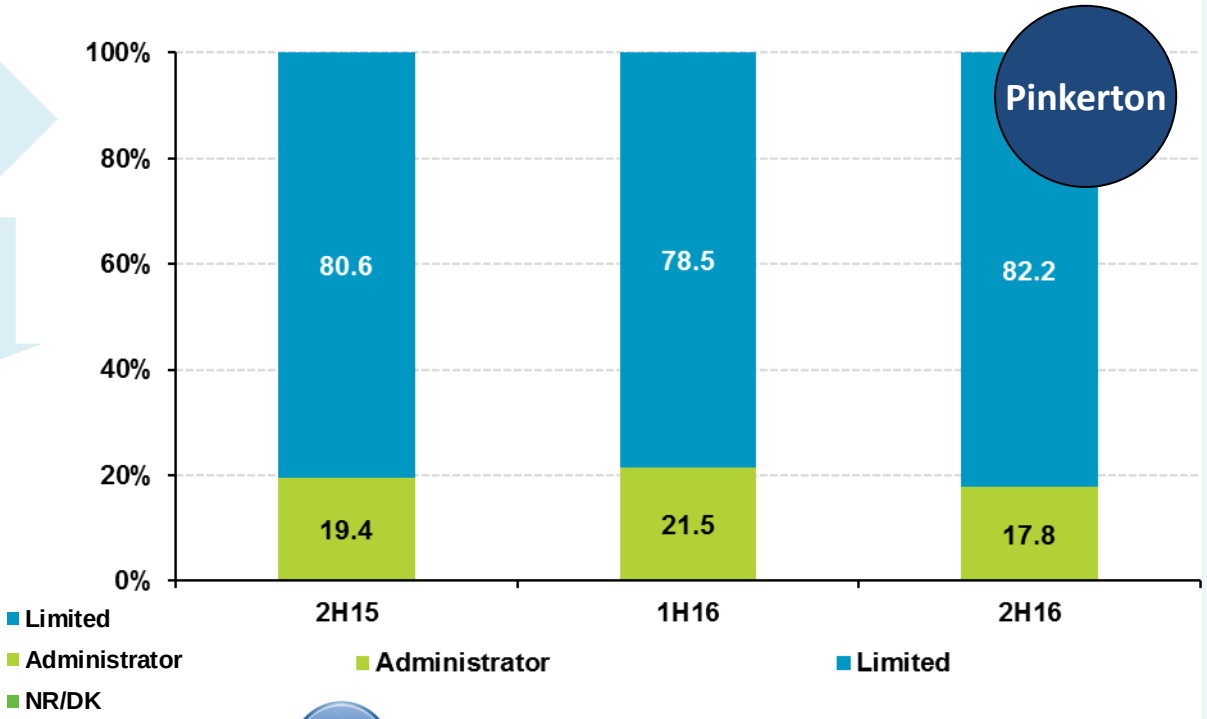
Data or system **encrypting** or **coding** allows you to store the content of the coded device so that it can only be accessed if you know the encryption key (PIN, pattern, or password) to decode it. This maintains data safe in case of theft or loss of the mobile device.

Use of security measures on Android devices

Real data

Reported data (2H16)





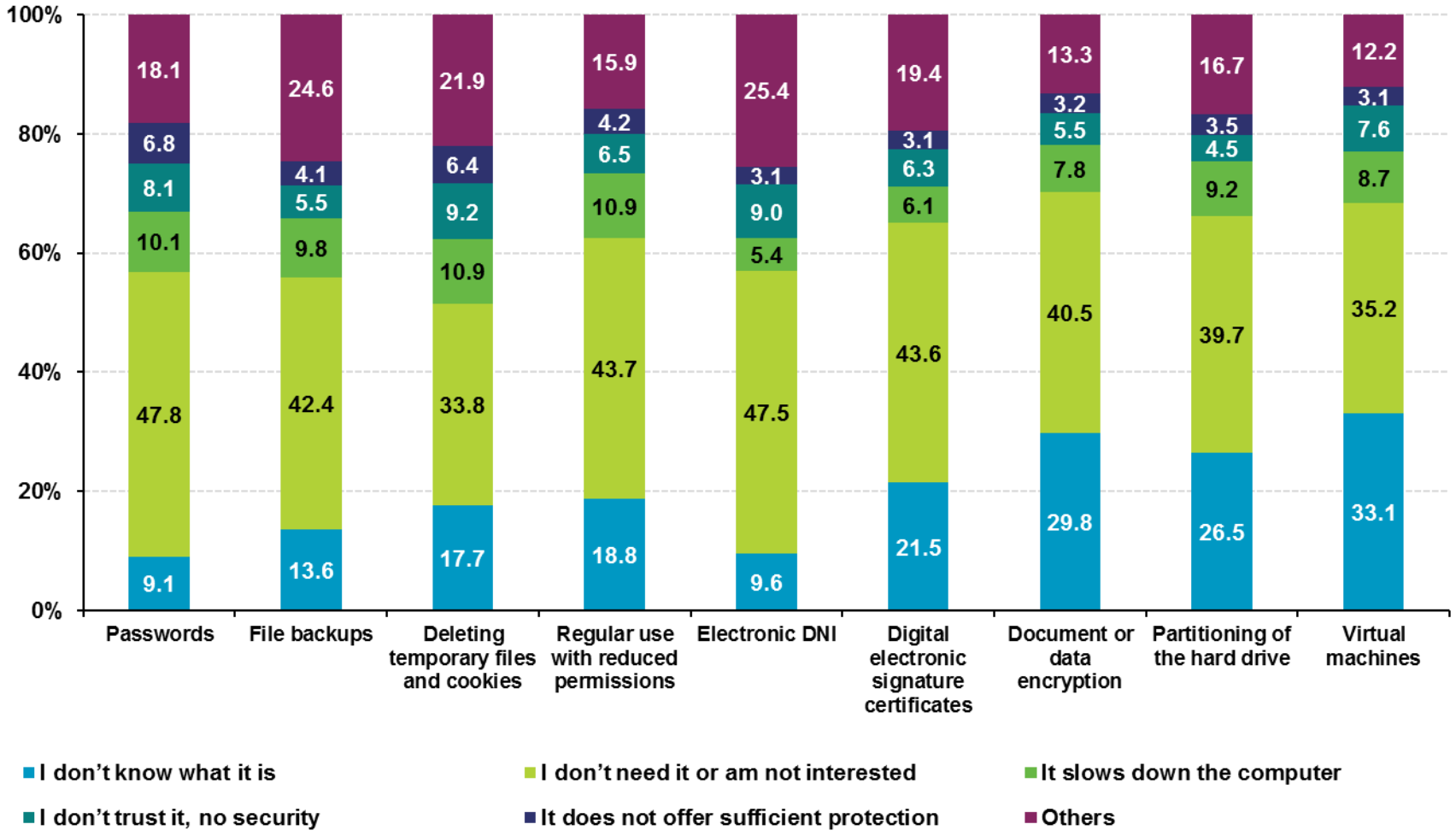
Pinkerton uses indirect methods to obtain information on the administrator privileges of the Android device.

Obtaining **administrator privileges** (root) is known as **"rooting"**. This enables the user to **access and modify any aspect of the operating system**. But there are also risks as **the malware can use this** to obtain greater control and/or access to the device.

BASE: Users with an Android device

Reasons for not using security measures

The main reason reported by Spanish Internet users for not using non-automatable security measures is that they **do not need them or are not interested in them.**



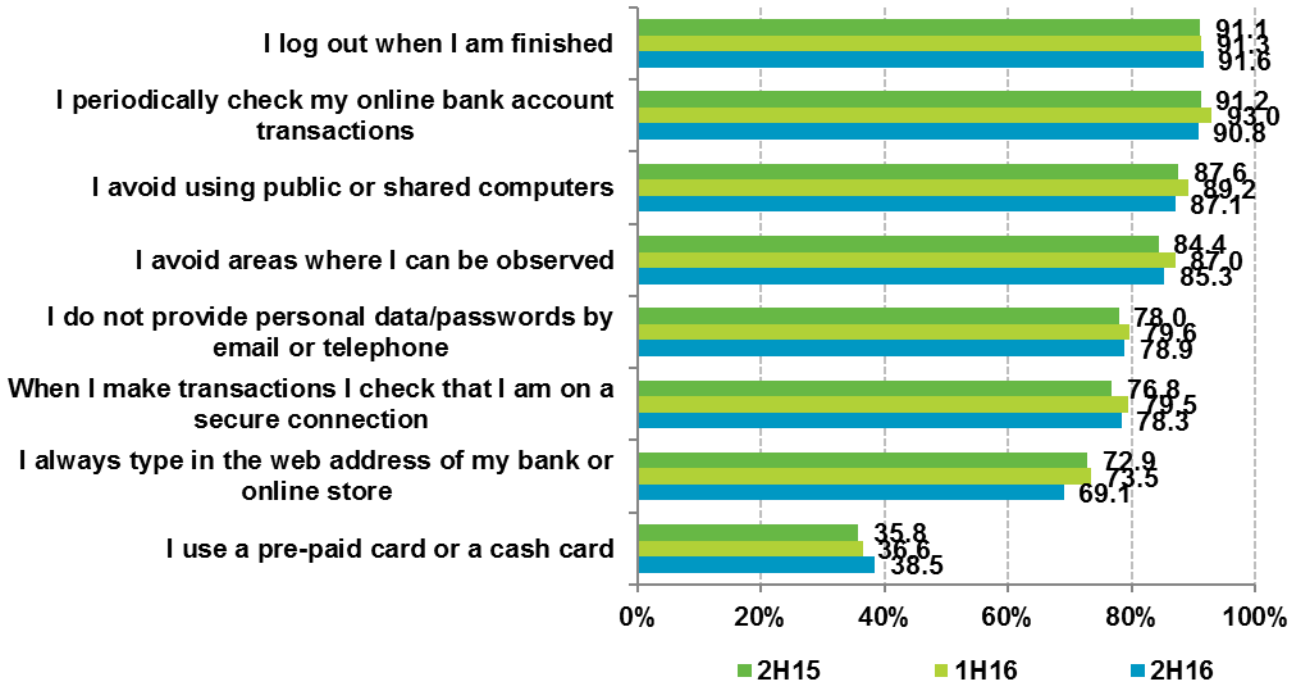
BASE: Users who do not use any of the security measures

Behaviour habits in browsing and Internet use

1. Online banking and e-Commerce
2. Internet downloads
3. Registering with Internet services
4. Social networks
5. Habits of wireless Wi-Fi network use
6. Habits of Android device use

Online banking and e-Commerce

Users of **online banking and commerce services** generally maintain good behaviour habits. **Prepaid cards or wallets** are the least used measure, by **38.5%** of the users of said services.



Banks never request data and passwords from users. This information is confidential and must only be known by the user.

Banks normally have a warning to alert their customers of these practices. The purpose is to avoid online and/or telephone fraud seeking to obtain user credentials and access their accounts.

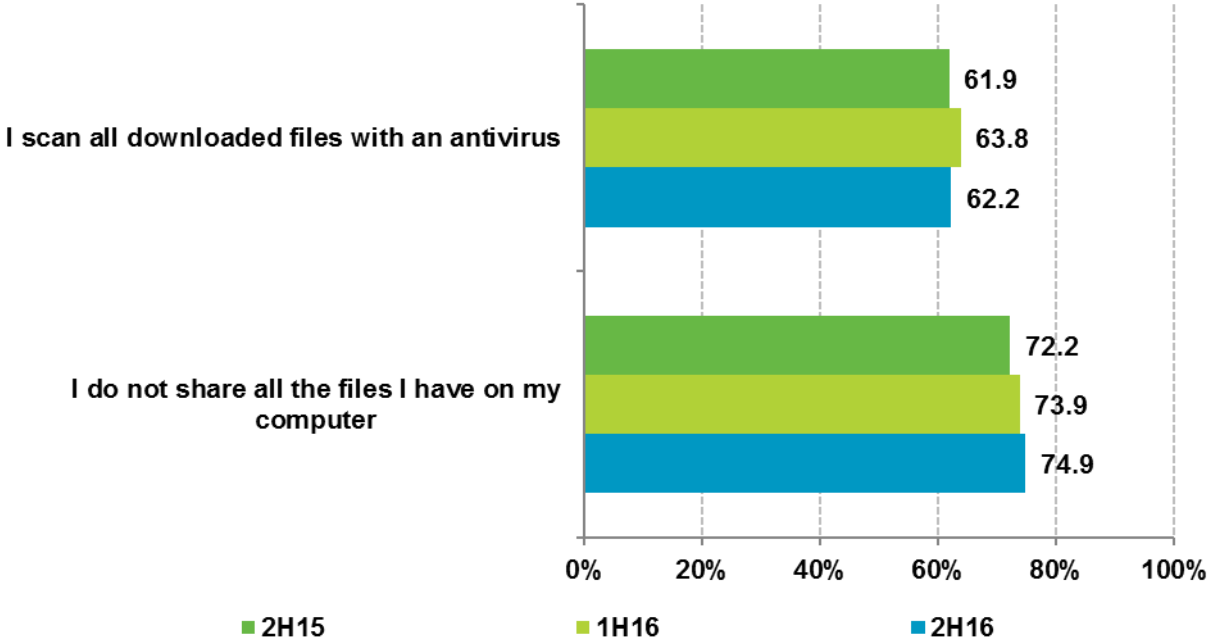
BASE: Users of online banking and/or e-Commerce

Measures to protect yourself during online processes: https://www.osi.es/pagos-online

How to detect false bank emails online: https://www.osi.es/es/banca-electronica

P2P networks

Three in four users (**74.9%**) say they **do not share <u>all</u> files** on their computer on P2P networks, avoiding exposing their private information to any user of these download networks. Furthermore, **62.2%** of users report that they do not open any downloaded file if they are not certain that it is has been **analysed by an antivirus**



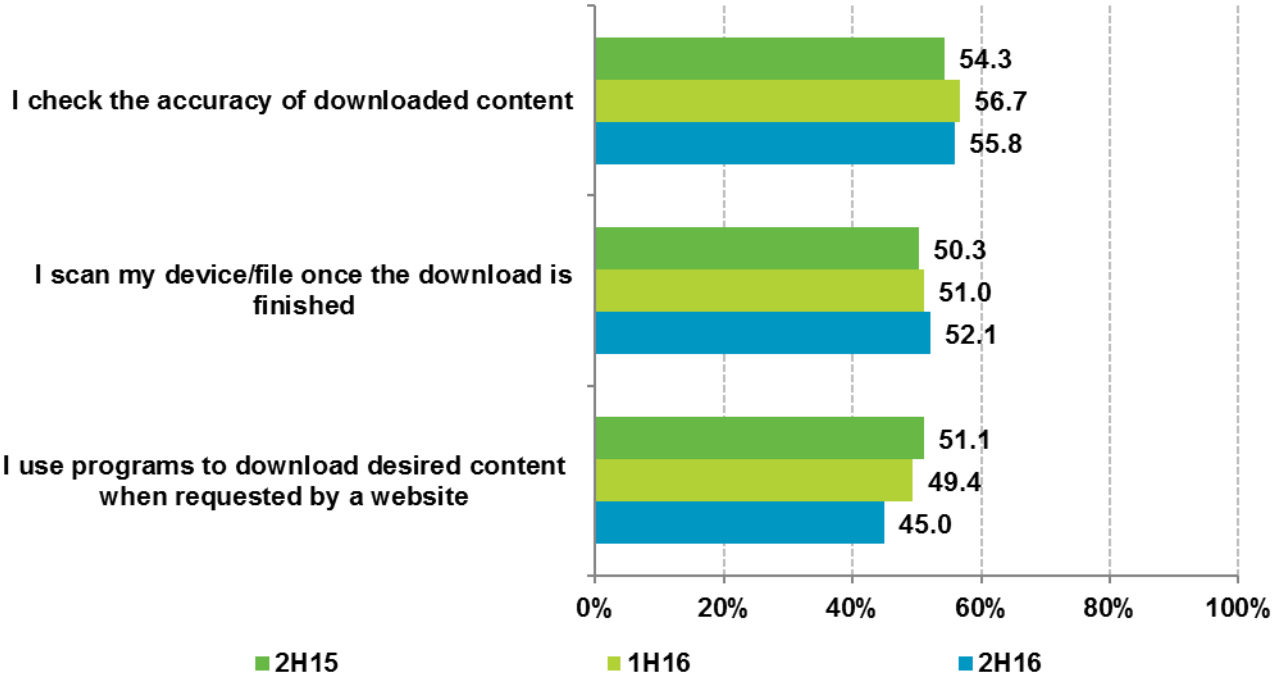
Internet downloads are a source of infection widely used by malware developers. Using malicious codes camouflaged in files that catch the interest of the user (for example the latest software, films, music, etc.) they infect the computer of incautious users.

BASE: Users of P2P networks

Direct download

According to reports, panellists **check the accuracy of downloaded content** (download site, file type, hash, etc.) before opening it (**55.8%**), and **they analyse the device or file once the download is completed** (**52.1%**).

On the other hand, **45%** say they **use programs to download content requested by the website**, exposing their computer to malware infections.

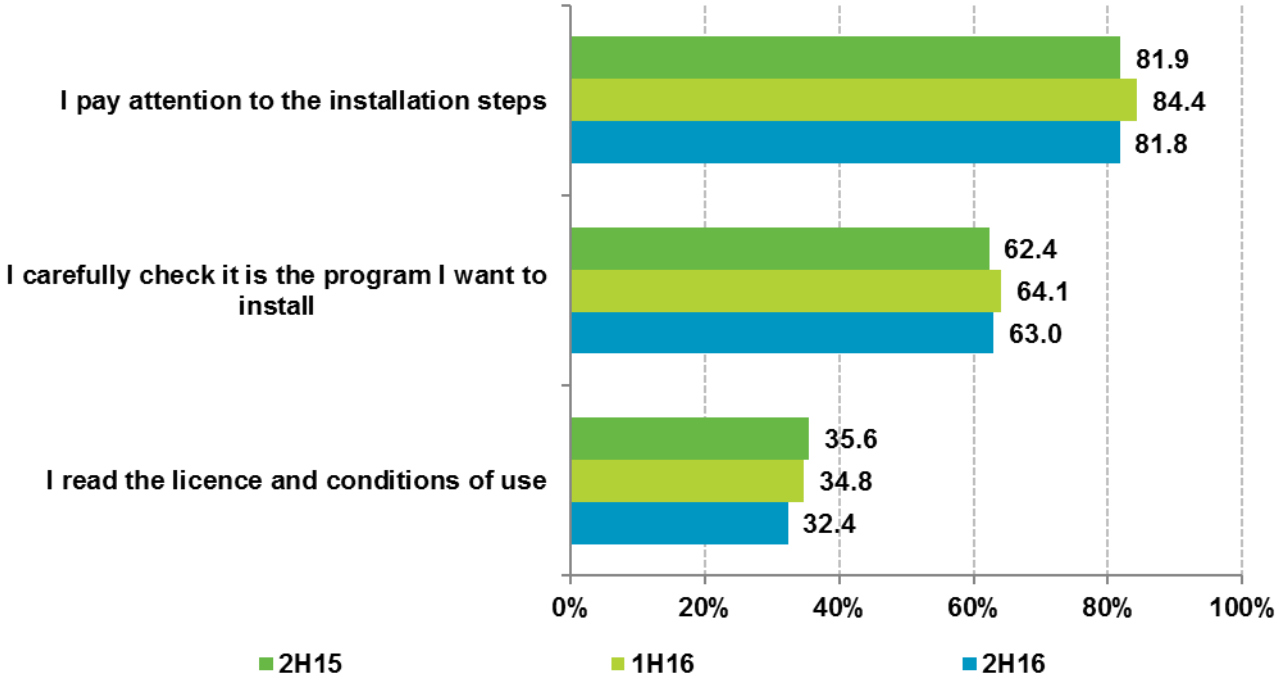


BASE: All users

Installing downloaded software

Most panellists (**81.8%**) report they **pay attention to the steps to install software**, although only two thirds (**63%**) run a **detailed check to ensure that the program is the one they want to install**.

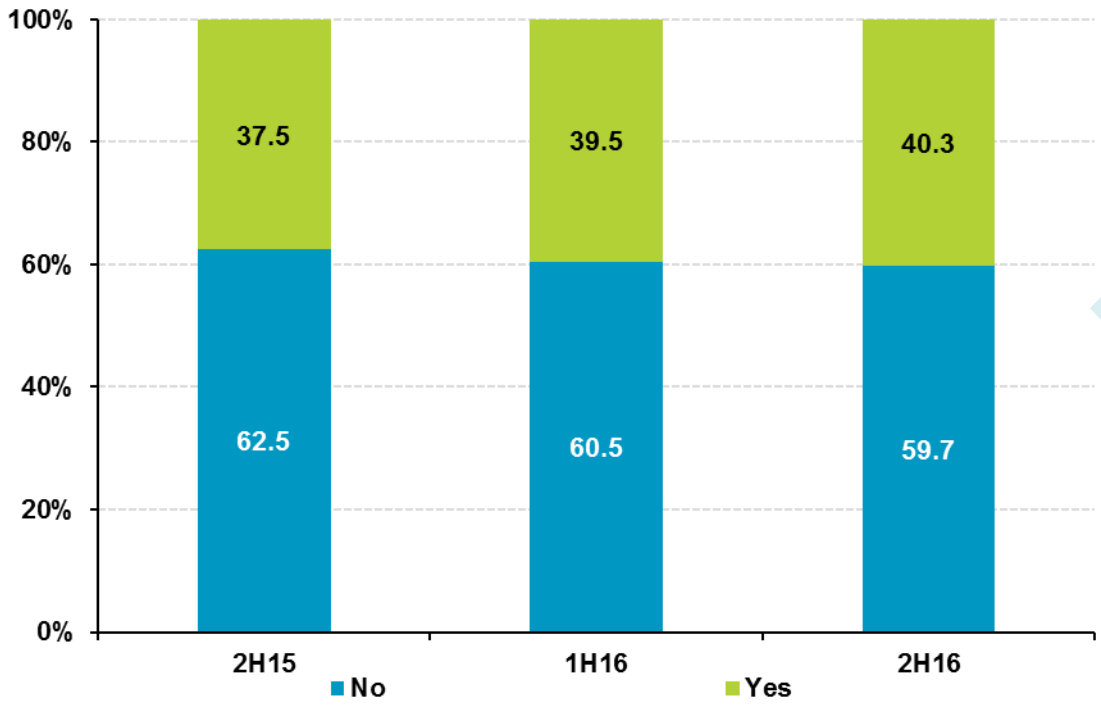
Only **1 in 3** users **read the licences and/or conditions of use** when installing a program.



BASE: PC Users

Registering with Internet services

Over half of users (**56.5%**) **do not read the legal terms and information before accepting them when they register with Internet service providers** (for example social networks, e-commerce, email, etc.)



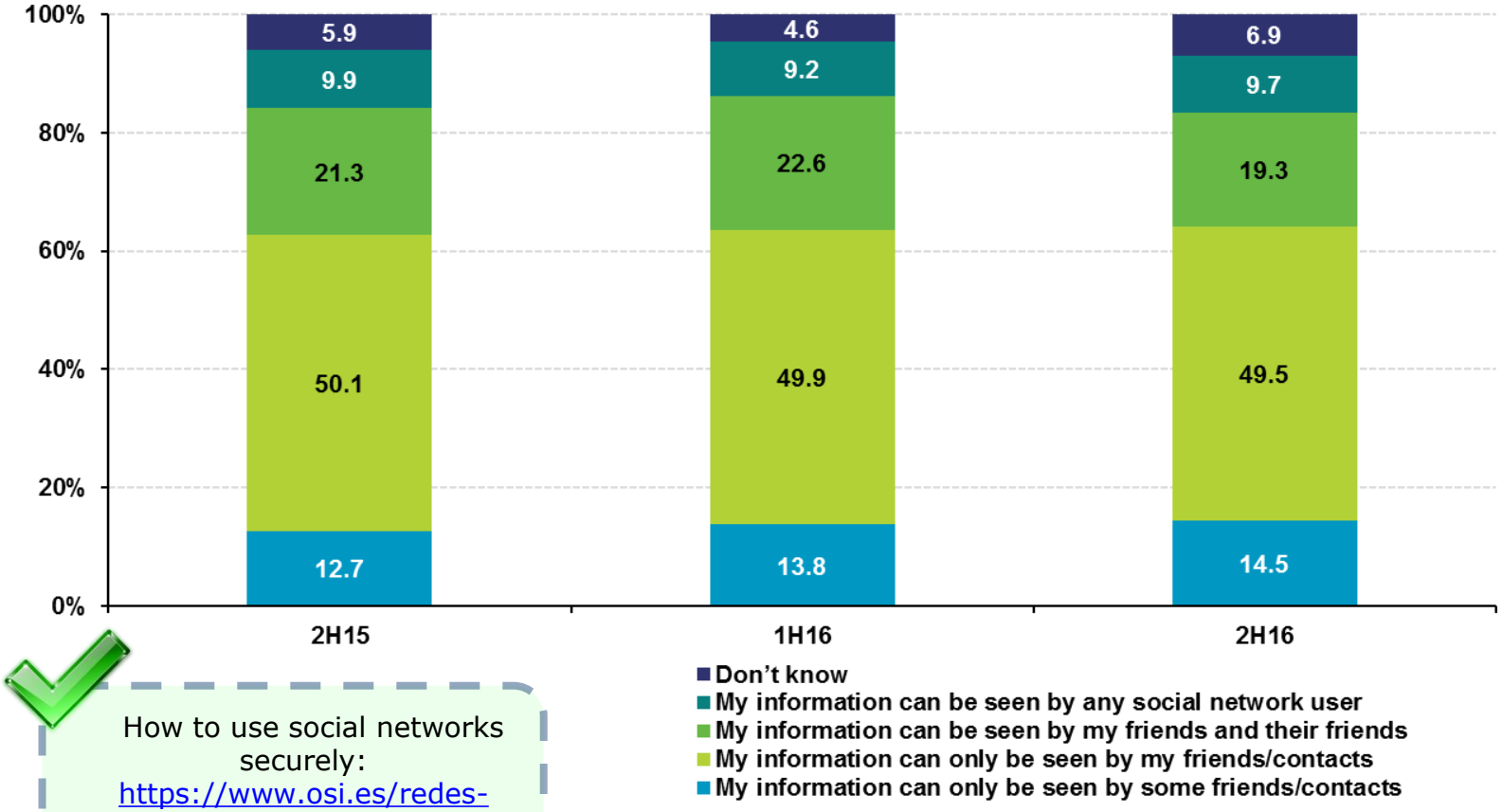
% individuals

Reading and accepting legal information when registering with Internet service providers (social networks, e-Commerce, etc.)

BASE: All users

Social networks

64% (49.5 + 14.5) of social network users configure their profile so that it can only be accessed by their friends and contacts. However, **29%** (19.3 + 9.7) **expose the data** published on their profile to **third and/or unknown parties**, and even **6.9%** of those consulted report that they **do not know** their profile privacy level.



How to use social networks securely: https://www.osi.es/redes-sociales

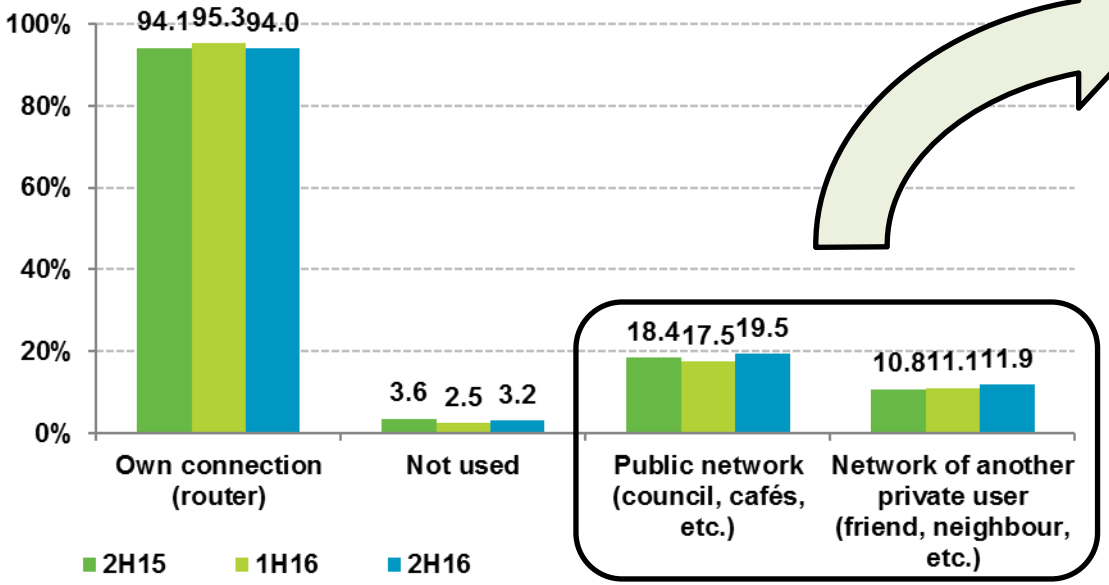
BASE: Social network users

% individuals

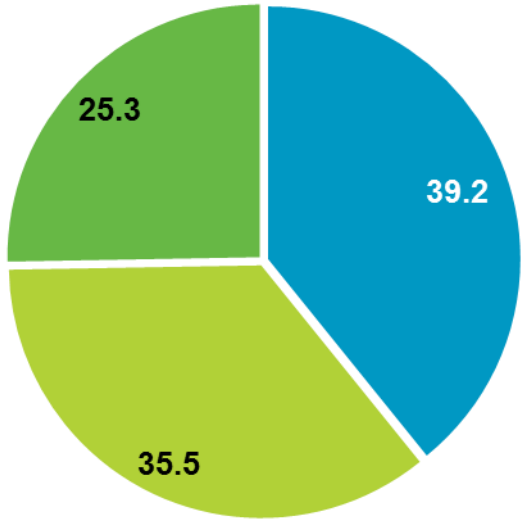
Habits of wireless Wi-Fi network use

Internet access point using wireless Wi-Fi networks

Multiple response



BASE: All users



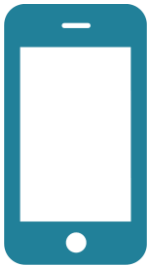
% individuals

BASE: Users who connect to a public Wi-Fi network or another user's network

39.2% of users who connect to a public wireless Wi-Fi network do so **whenever they need to** and **anywhere**, exposing the confidentiality and integrity of their data.

How to connect to public Wi-Fi networks securely: https://www.osi.es/wifi-publica

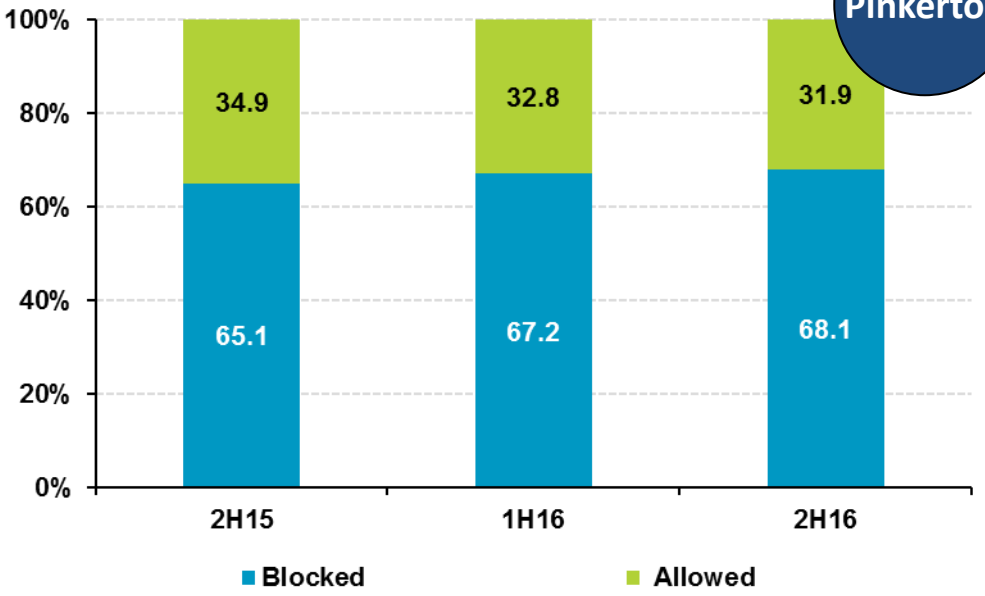
Habits of Android device use



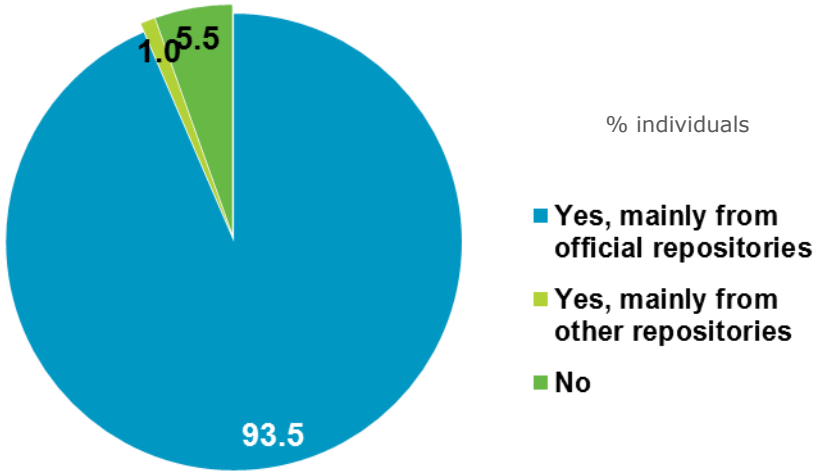
Executing or using programs and/or files from doubtful sources can pose **security problems** and the installation of any type of **malware** on the mobile device.

Downloads from unknown sources

Pinkerton



Downloading programs or applications on a mobile



Most (**93.5%**) Android smartphone and tablet users report they download applications from **official repositories.**

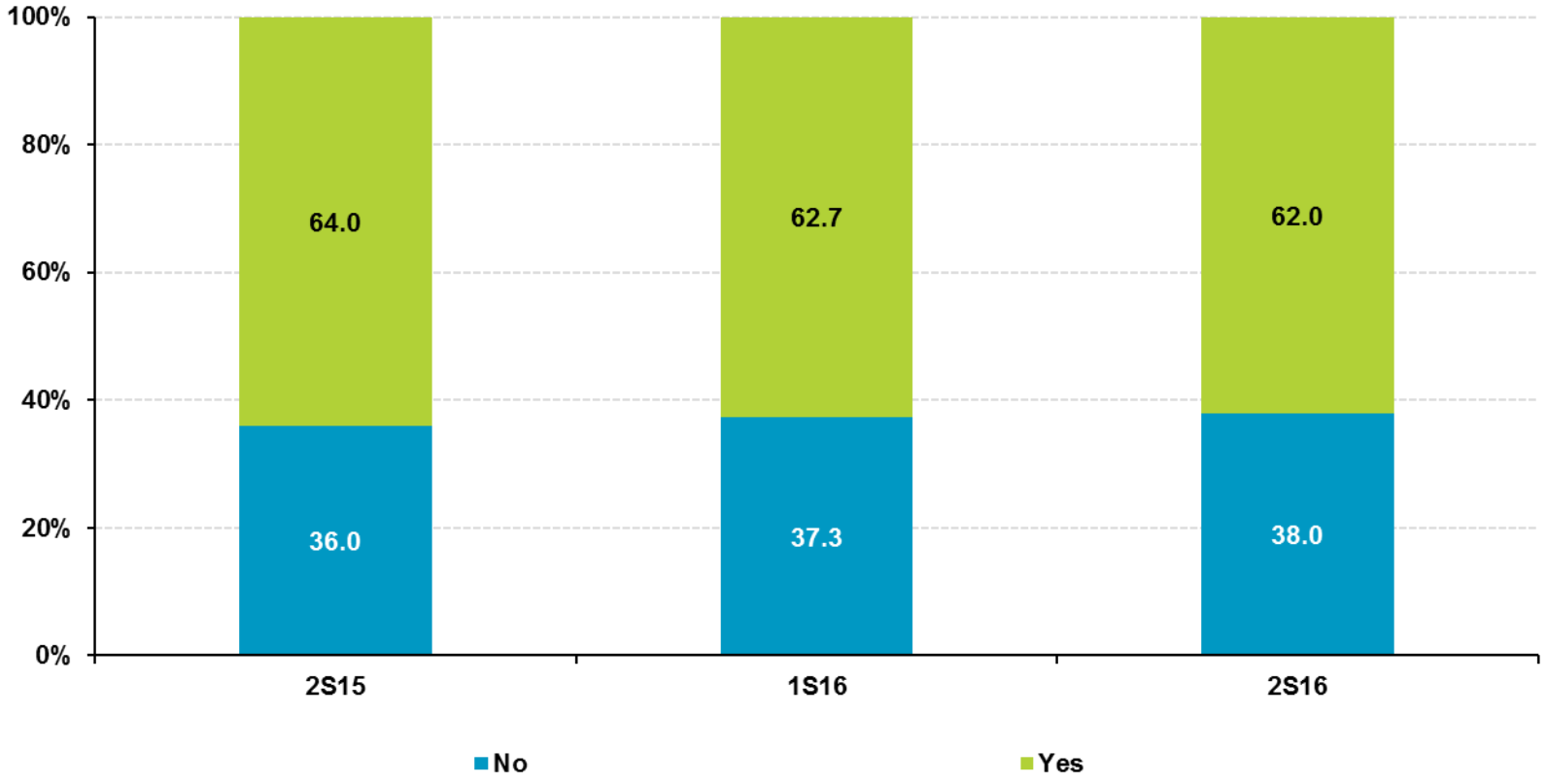
However, on almost **one third** (**31.9%**) of the Android devices scanned, the default configuration had been modified to allow applications to be installed from **unknown sources.**

BASE: Users with an Android device

Habits of Android device use

Checking permits when installing an application

% individuals



BASE: Android device users who download applications

Security incidents

Types of malware

Malware is all the programs and malicious codes whose purpose is to infiltrate a computer/laptop or mobile device (tablet, smartphone, smartwatch, etc.) without the owner's consent. They are commonly known as viruses, in reality it is a much broader term that encompasses other types.

Trojans or Trojan horses. Bankers, Backdoors, Keyloggers, Diallers, Rogueware

Adware

Intrusion tools

Virus

Suspicious files detected heuristically. Technique used by antivirus programs to recognise malicious code not found in the antivirus database.

Spyware

Worm

Others. Exploit, Rootkits, *Scripts, Lockers*, Scareware or Jokes

More information: https://www.incibe.es/glossary/empresas/diccionario/

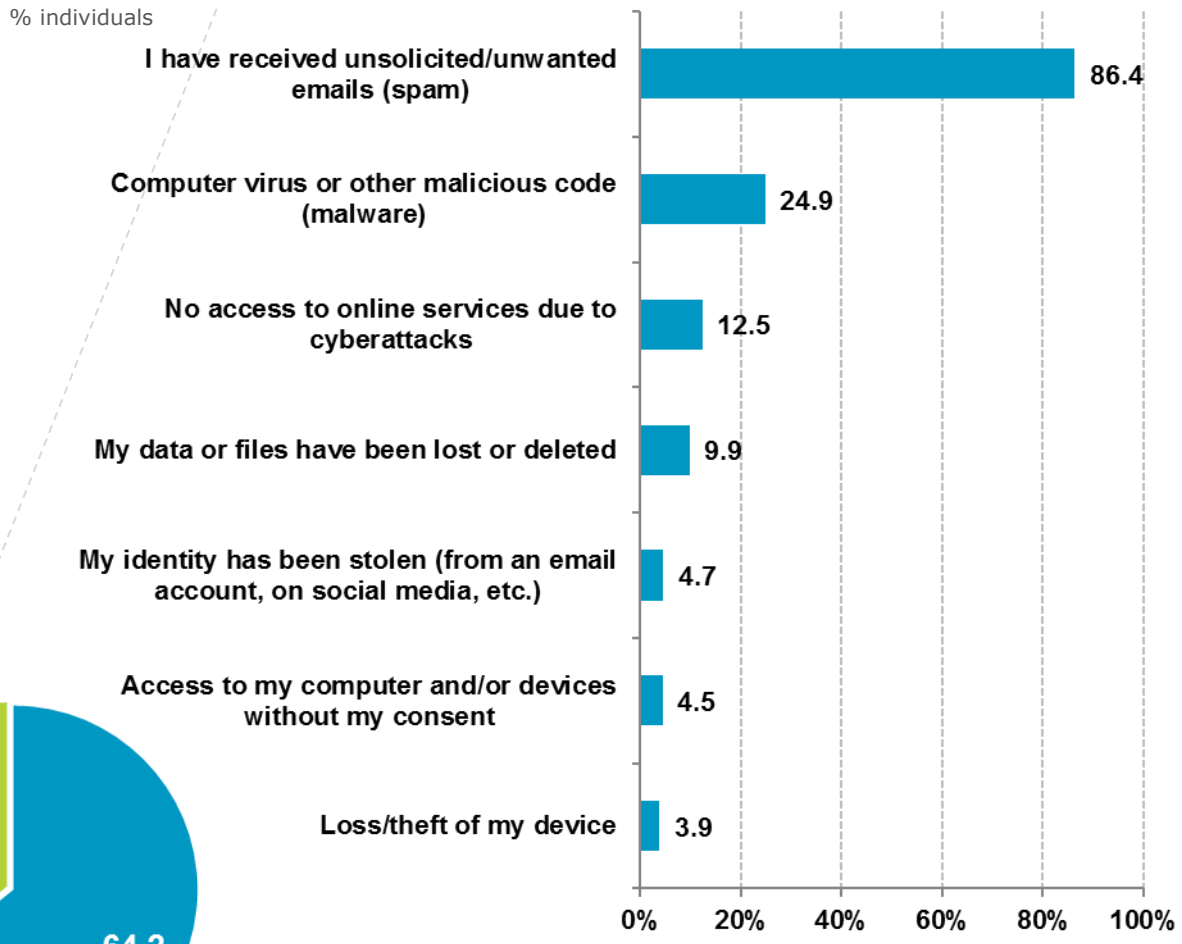
Security incidents

Malware is all the programs and malicious code whose purpose is to infiltrate a computer without the owner's consent.

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

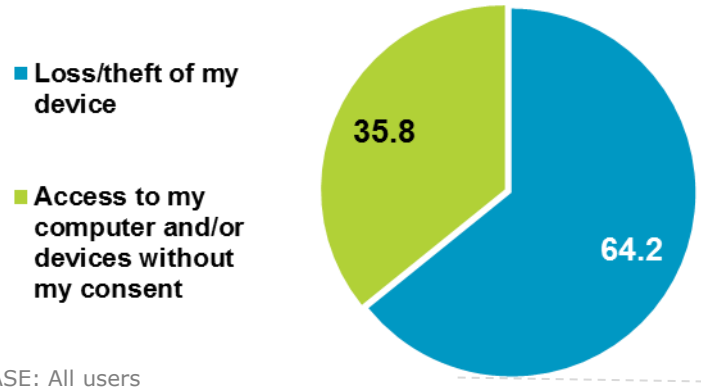
Incidents suffered:

Multiple response



BASE: Users who have experienced a security incident

Affected:



BASE: All users

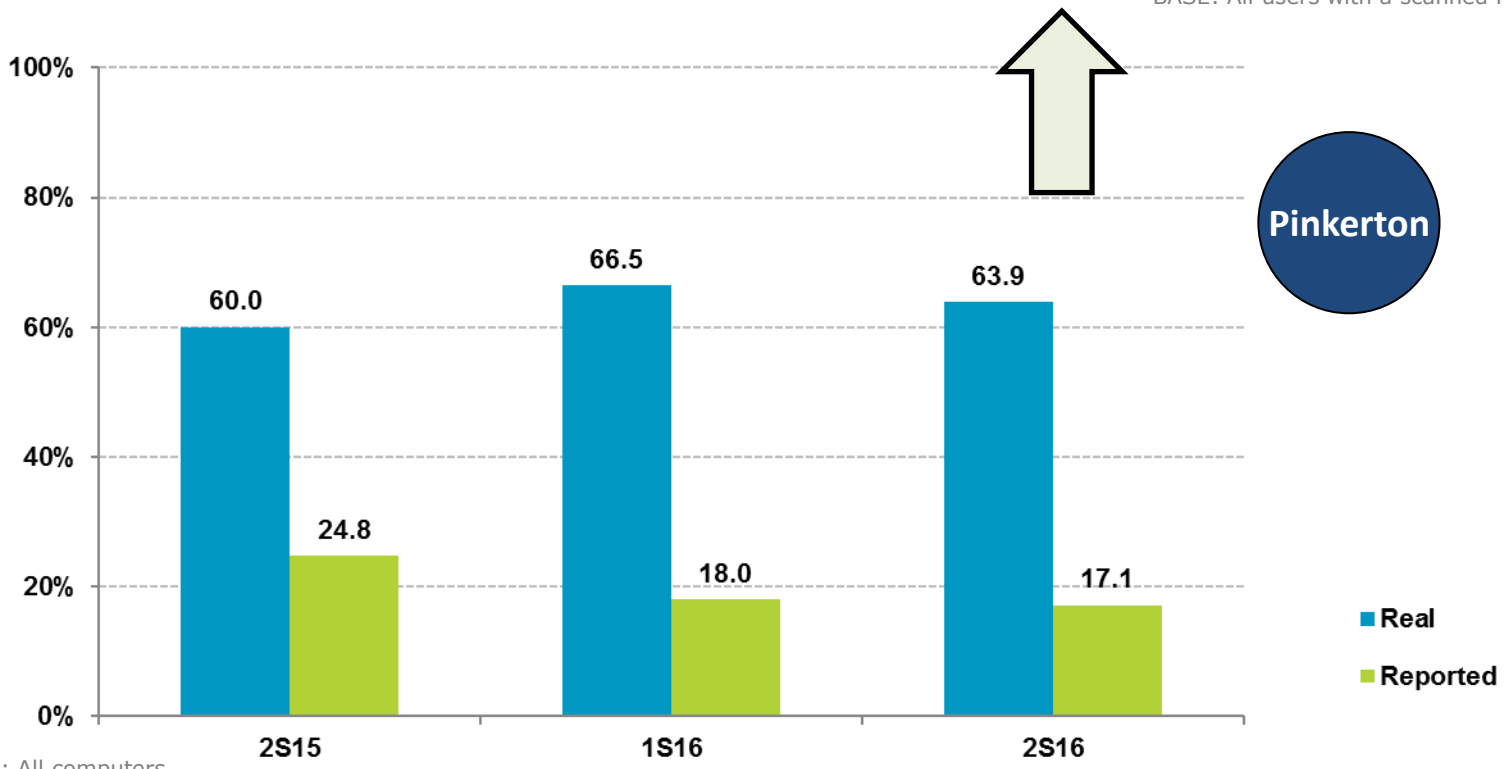
Malware incidents

Household computer

Of the computers analysed, **53.7% had a virus and their users had not noticed**.

They reported having malware on PC	Their PC had malware		
	Yes	No	Total
Yes	10.2	7.0	17.2
No	53.7	29.1	82.8
Total	64.0	36.0	100.0

BASE: All users with a scanned PC



BASE: All computers

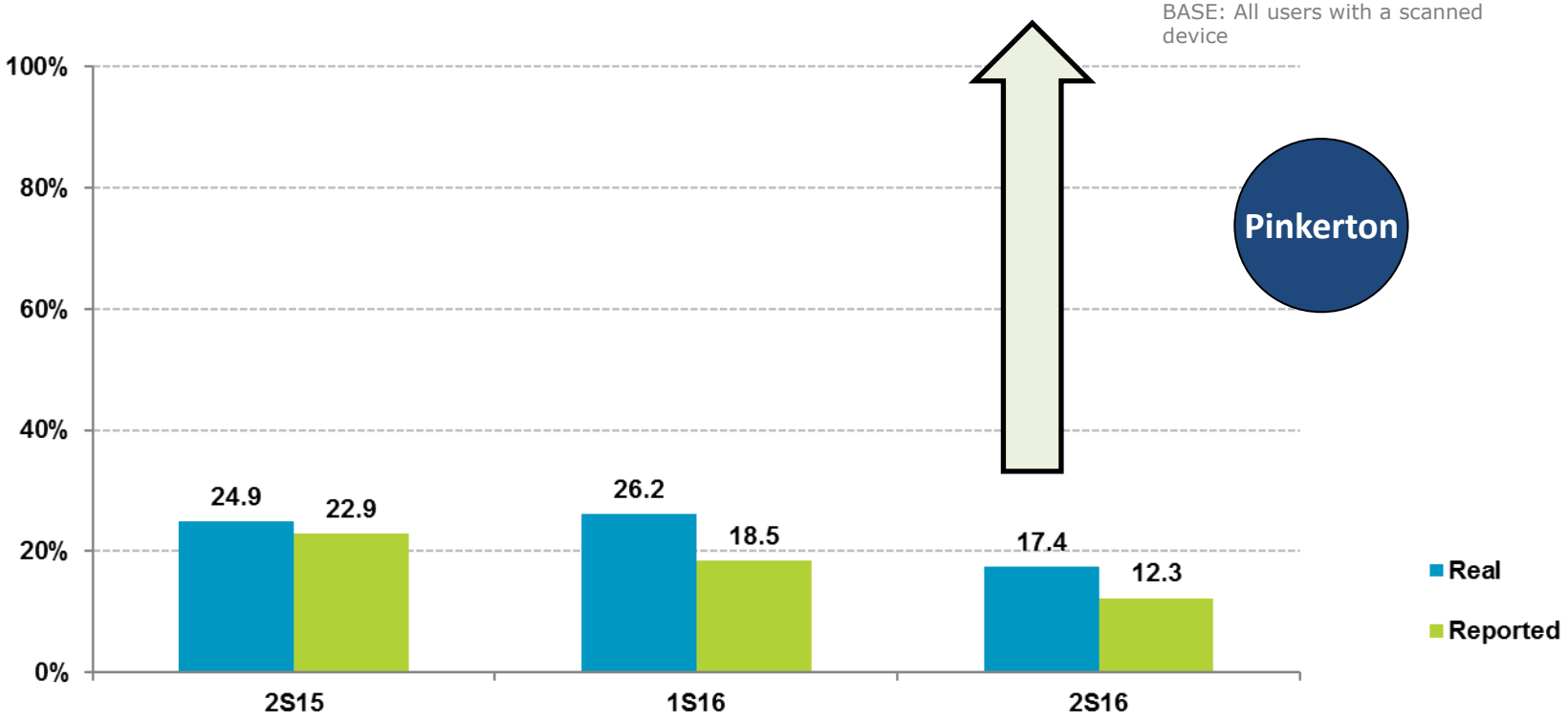
Malware incidents

Android Devices

This gap is smaller on Android devices: users did **not notice the presence of malware** on **14.6%** of the devices on which **Pinkerton found infections**.

They reported having malware on Android	Their Android had malware		
	Yes	No	Total
Yes	2.8	9.4	12.1
No	14.6	73.2	87.9
Total	17.4	82.6	100.0

BASE: All users with a scanned device



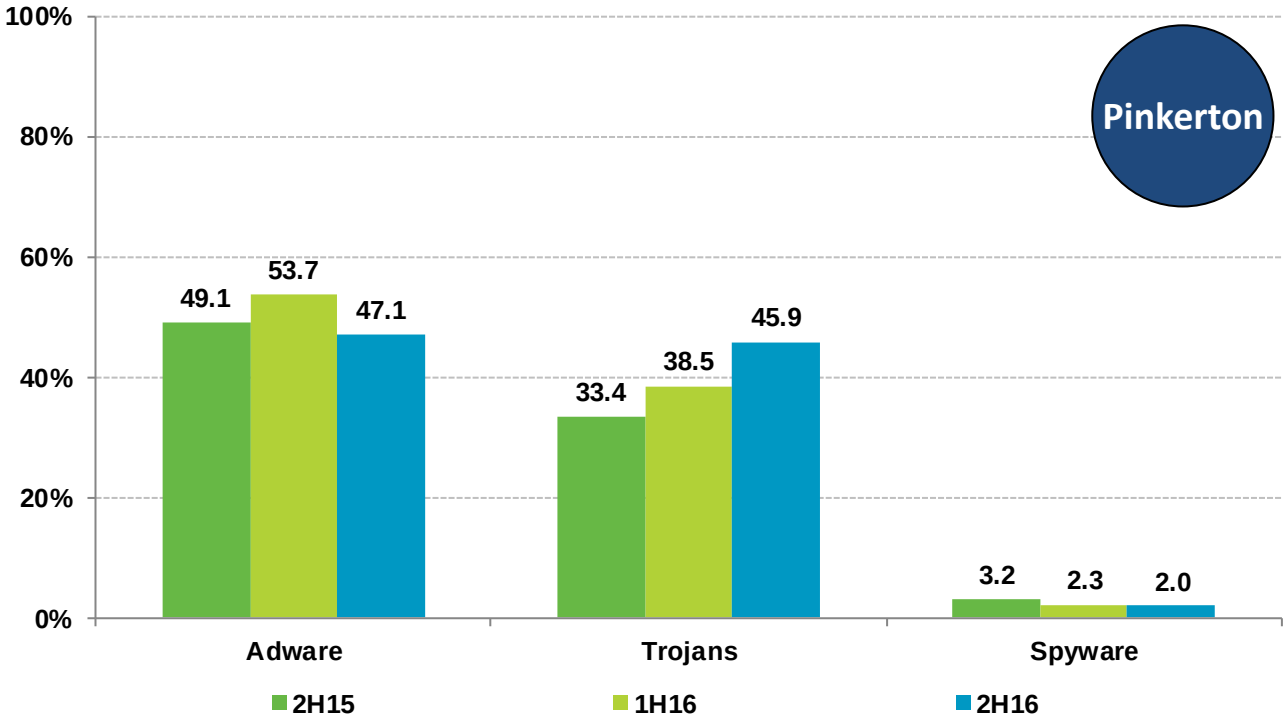
BASE: Users with an Android device

Type of malware detected on PC

Household computer

The malware most found on computers are those intended to gain economic benefits: **adware (47.1%)** and **Trojans (45.9%)**. While **adware falls 6.5 p.p.**, **Trojan rise by 7.4 p.p.** compared to the previous analysis.

Computers hosting malware according to type



Types of malware: https://www.osi.es/actualidad/blog/2014/07/18/fauna-y-flora-del-mundo-de-los-virus

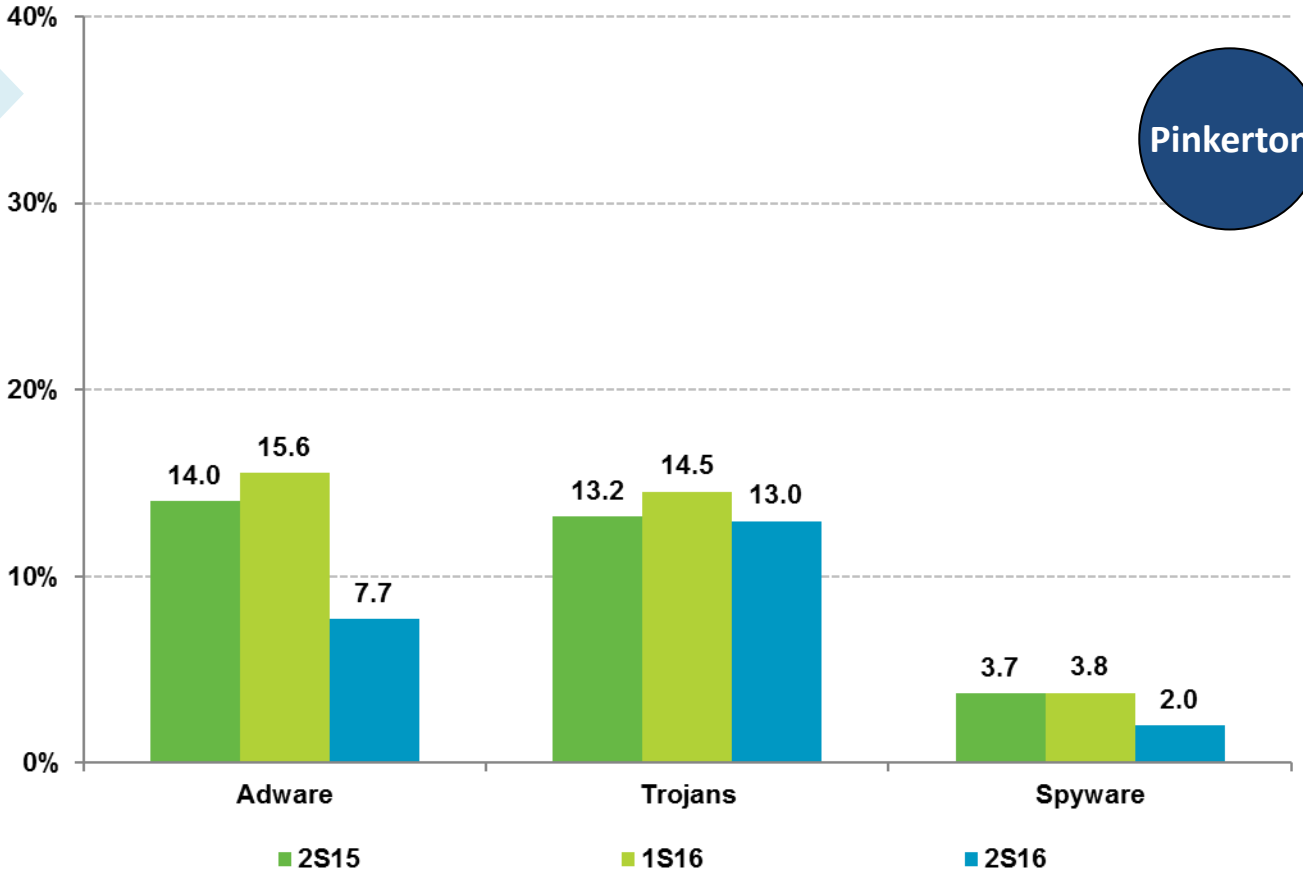
BASE: All computers

Type of malware detected on Android

Android Devices

On Android devices, **Trojans** and **adware** are also the main types of malware detected. However, on these devices there is a fall in both categories (**-7.9 p.p.** and **-1.5 p.p.** respectively).

Computers hosting malware according to type



BASE: Users with an Android device

Danger of malicious code and computer risks

To determine the level of risk[3] of the computers analysed, the danger of malware detected is set according to the possible consequences suffered.

They are classified according to the following criteria:

High risk: this category includes specimens that potentially: allow an attacker remote access to the victim's system; can cause economic loss to the user; facilitate the capture of the victim's confidential or sensitive information; are used as gateways to attack other computers (which may have legal consequences for the victim); or undermine system performance and functionality, whether by deleting files, slowing the computer down, closing windows, etc.

Medium risk: this includes examples that, although they have an undesired impact on the system: do not noticeably affect their performance; open undesired windows when browsing; embed advertising on legitimate websites that do not contain advertising; or facilitate the capture of the victim's non-sensitive information (for example, browsing patterns to create targeted advertising profiles, etc.).

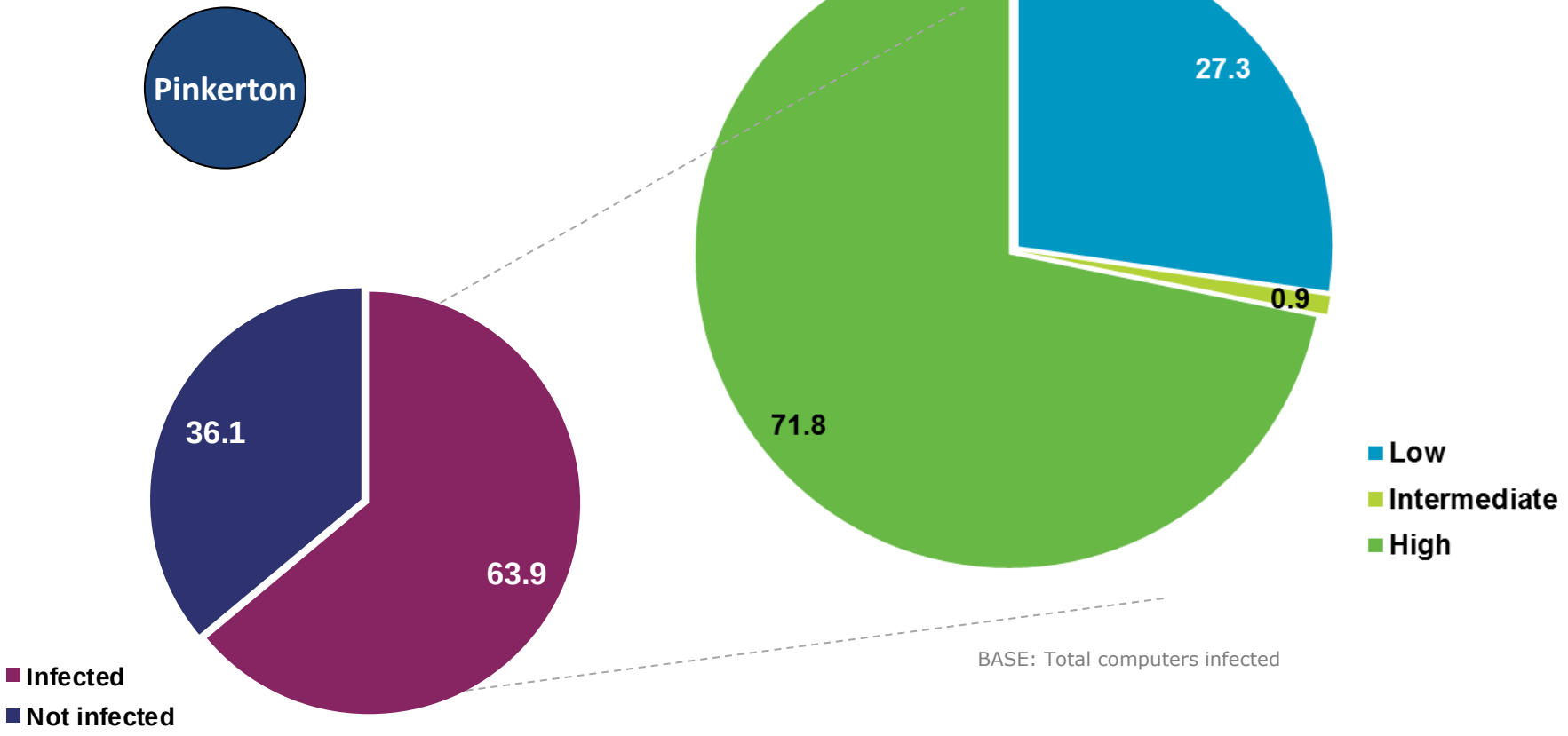
Low risk: encompasses manifestations that have a lesser effect on computers. These are tools used for hacking (scanning ports, ethernet address modifiers, hacking tools, etc.). In most cases they are tools installed by the user intentionally, to list and complete processes, or connect remotely to their computer, etc. On the other hand, "joke" programs are also considered low risk specimens (for example those that deploy a window that moves and is impossible to close with the mouse) and viruses exclusively for mobile platforms, as they cannot run on user computers.

[3] The risk level of each computer is established as that of the highest level of malware hosted. In other words, a computer that is detected to have high risk malware and another medium risk malware will always be included in the group of high risk computers.

Danger of malicious code and computer risks

Household computer

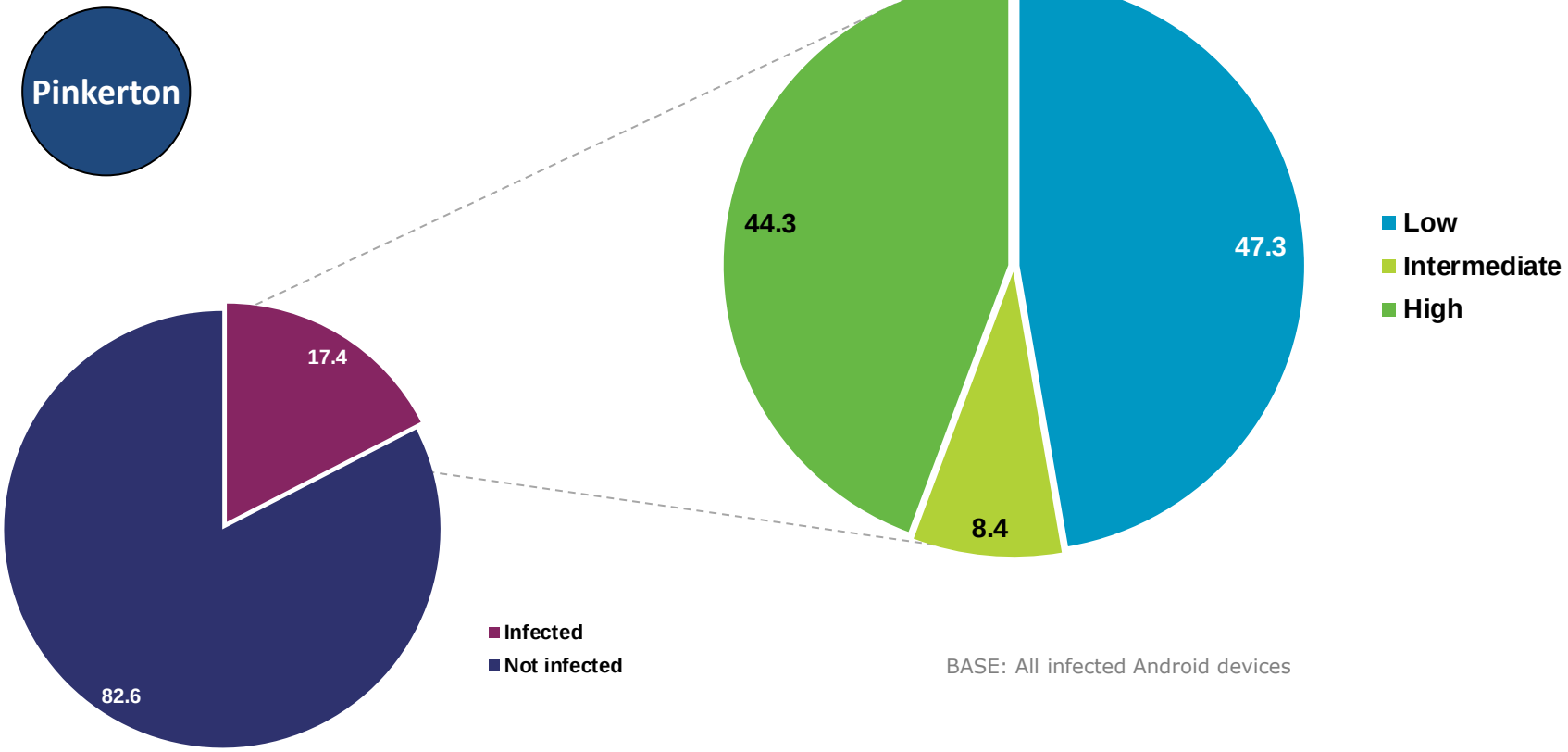
Almost two thirds (**63.9%**) of Spanish household computers analysed with Pinkerton are infected with at least one example of known malware. Of these, **71.8%** are **high risk** due to the potential danger of the malicious files found.



Danger of malicious code and computer risks

Android Devices

17.4% of the Android devices analysed with Pinkerton are infected with at least one example of known malware, of which **44.3%** are of **high risk**.



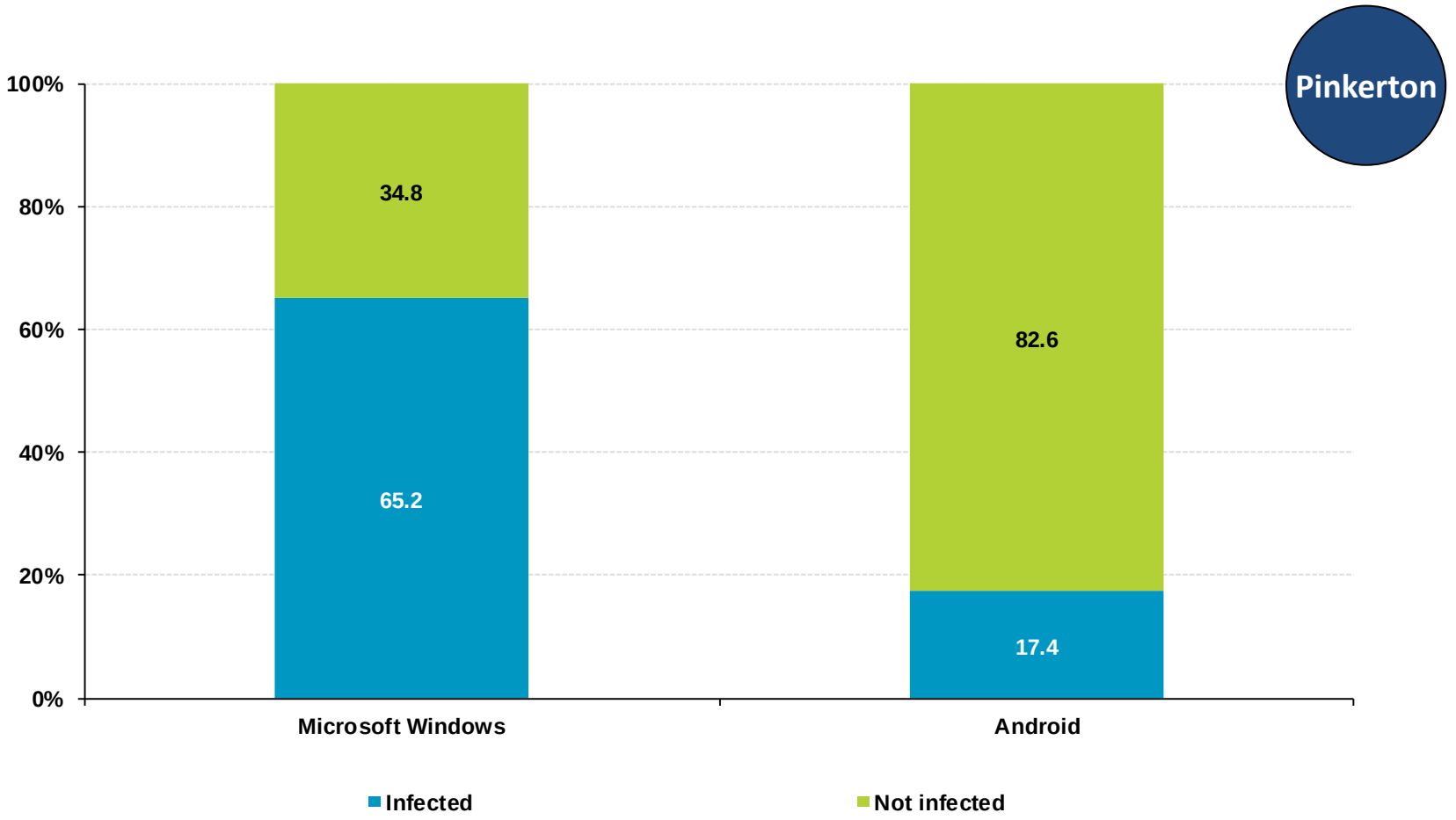
BASE: All Android devices

BASE: All infected Android devices

Malware vs operating system

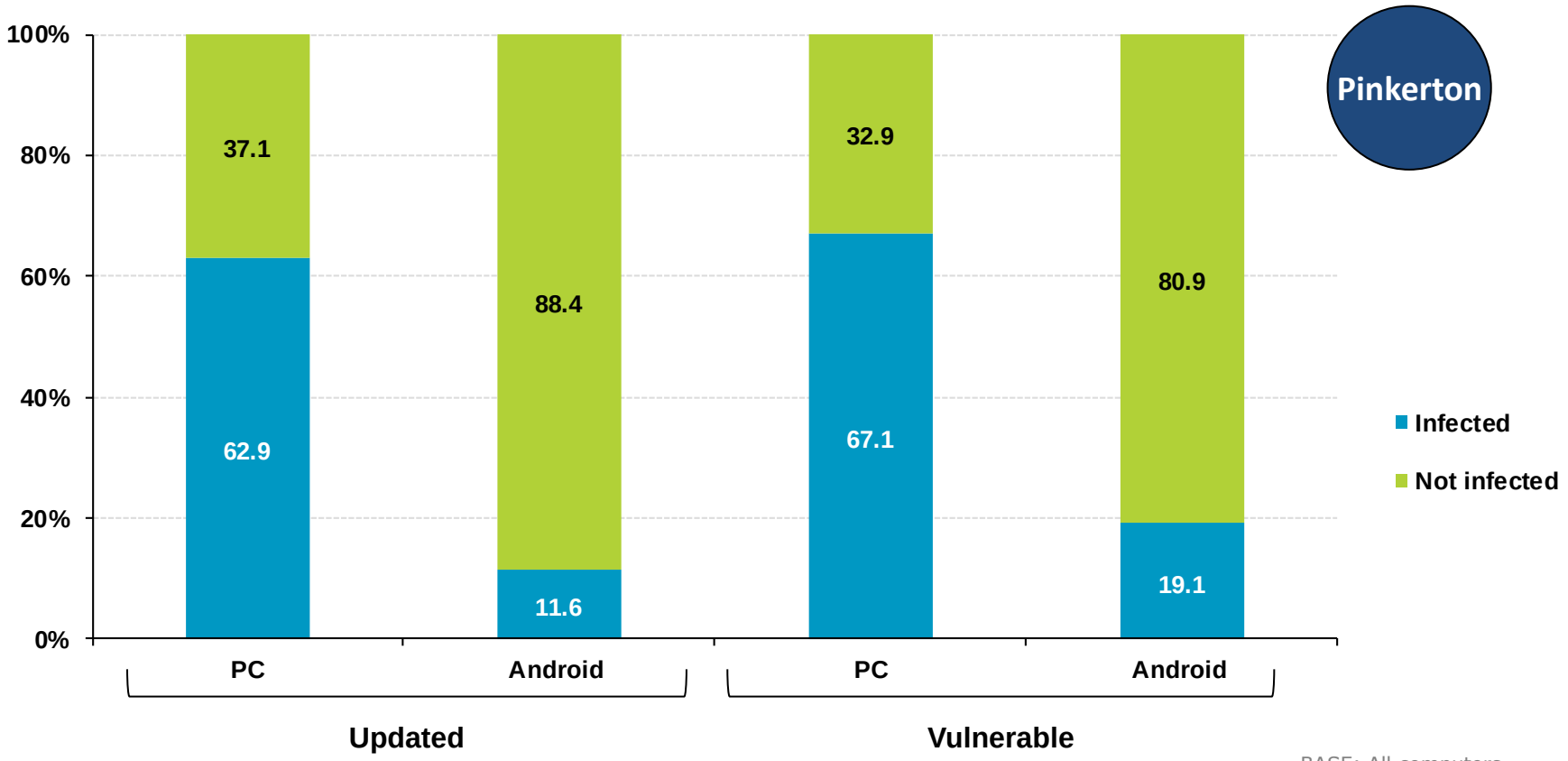
Pinkerton detects malware on two in three (**65.2%**) computers with a **Microsoft Windows** operating system.

On **17.4%** of **Android** devices some type of known malware is detected.



BASE: All computers

Malware vs system updates

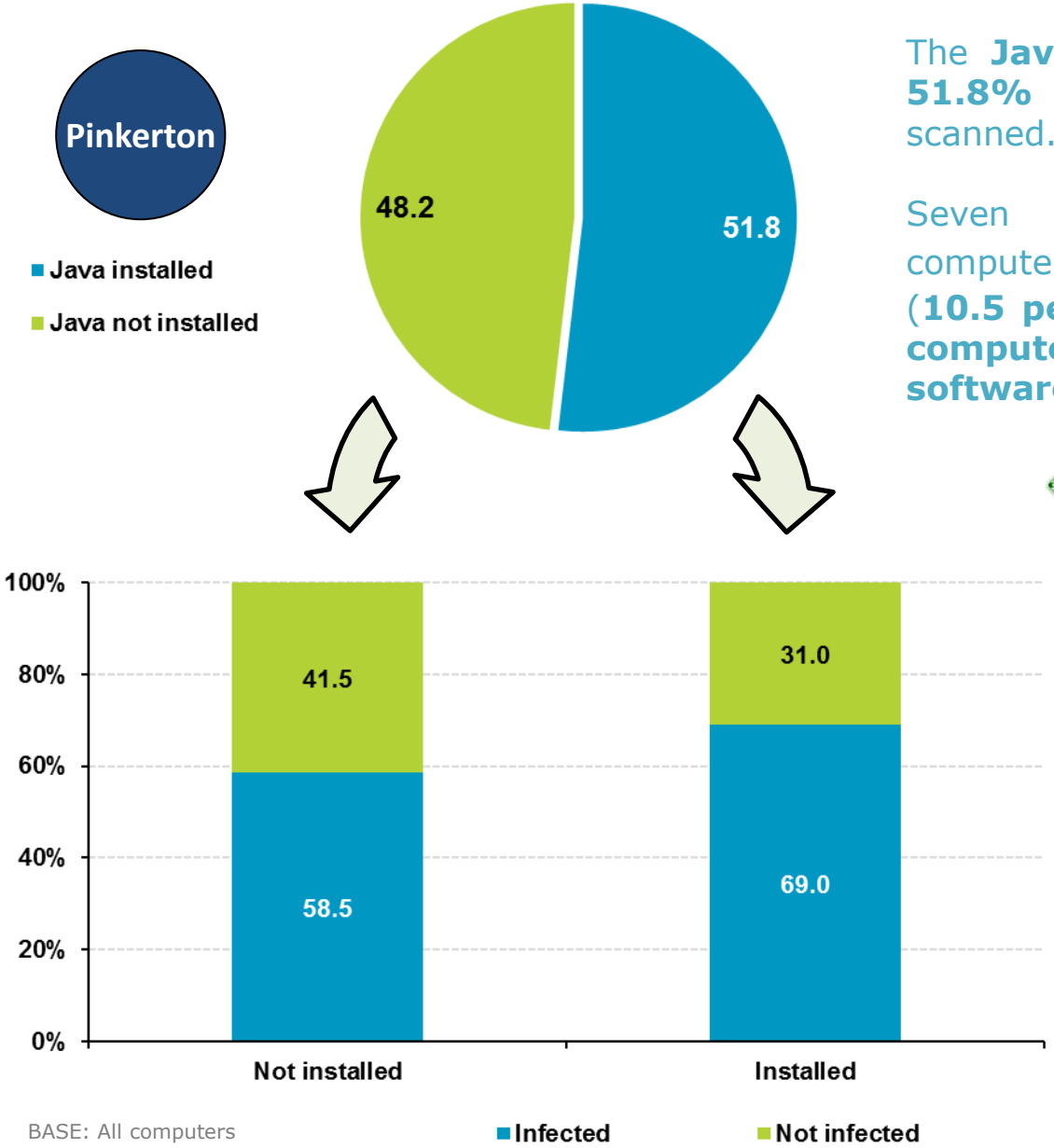


BASE: All computers

Regarding infections, it can be observed that there is a difference of **7.5 percentage points** in favour of updated systems on Android devices. Among desktop systems this difference is **4.2 p.p.**

There is greater penetration of malware on devices that are not updated, which proves that the infection process takes advantage of vulnerabilities.

Malware vs Java on PC



BASE: All computers

The **Java** environment is present on **51.8%** of the household computers scanned.

Seven in ten (**69%**) of these computers are affected by malware (**10.5 percentage points above the computers that do not have this software installed**).

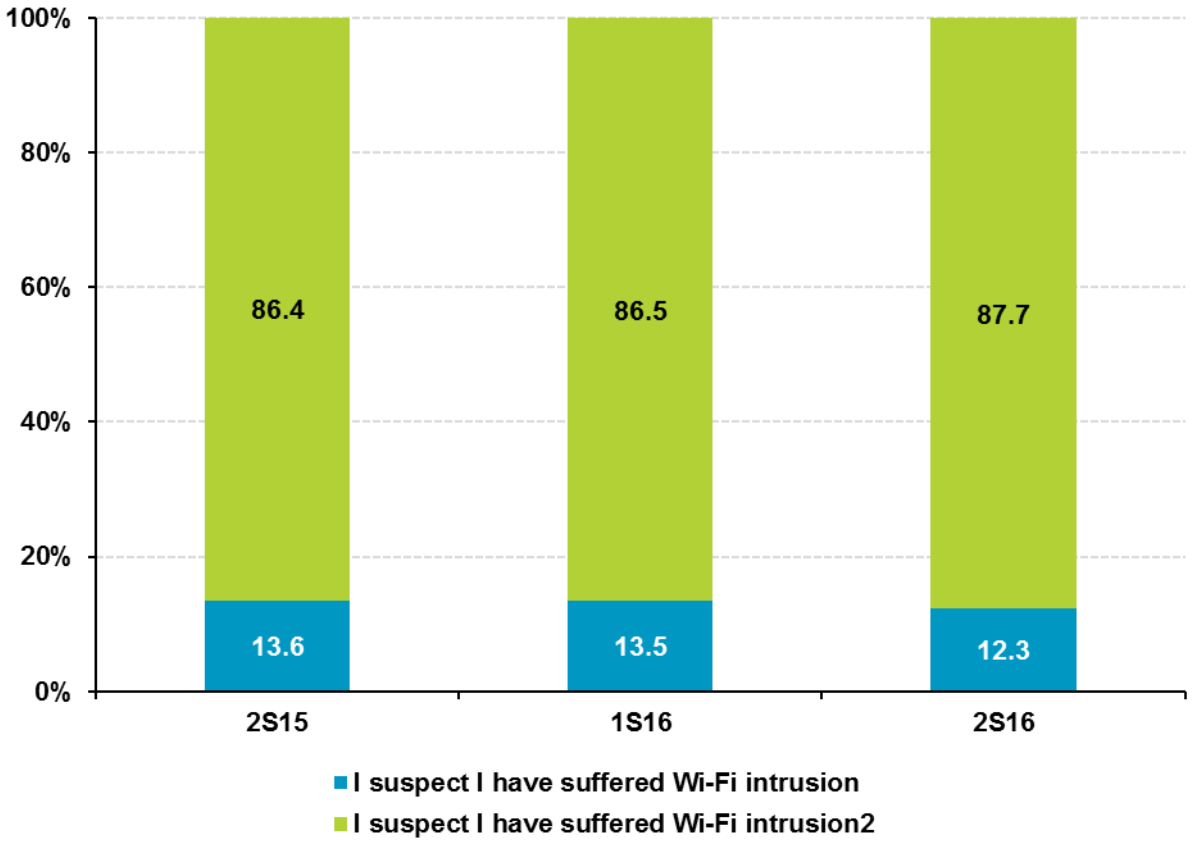
Java security alerts in July 2016: http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html#AppendixJAVA

In recent years, taking advantage and exploiting vulnerabilities in Java has been one of the entry vectors most used by malware to infect computers with an outdated version of this software.

Security incidents with wireless Wi-Fi networks

12.3% of panellists *suspect* that they may have suffered **intrusion into the wireless Wi-Fi network** of their home.

% individuals



Do you know how to find out if someone is connected to your home's wireless Wi-Fi network?

https://www.osi.es/protege-tu-wifi

BASE: Users with their own Wi-Fi connection

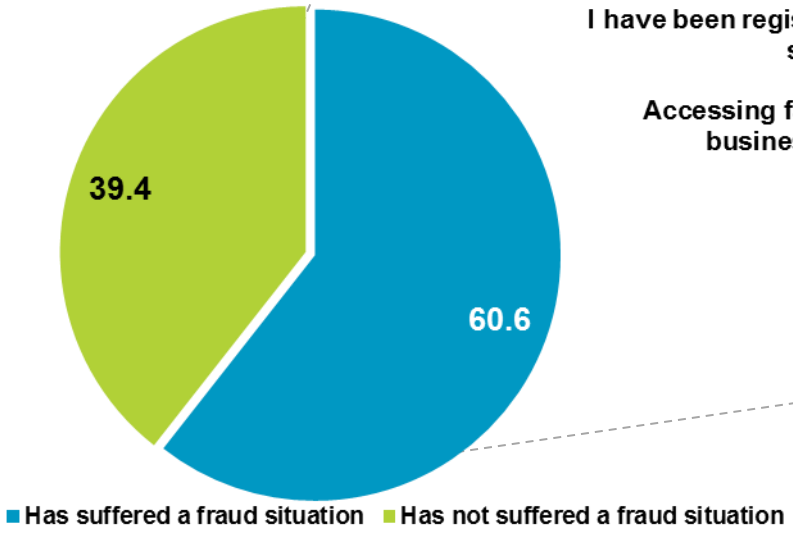
Consequences of security incidents and user reactions

1. **Online fraud attempt and manifestations**
2. **Security and fraud**
3. **Changes made after a security incident**

5

Online fraud attempt and manifestations

Online fraud attempt:

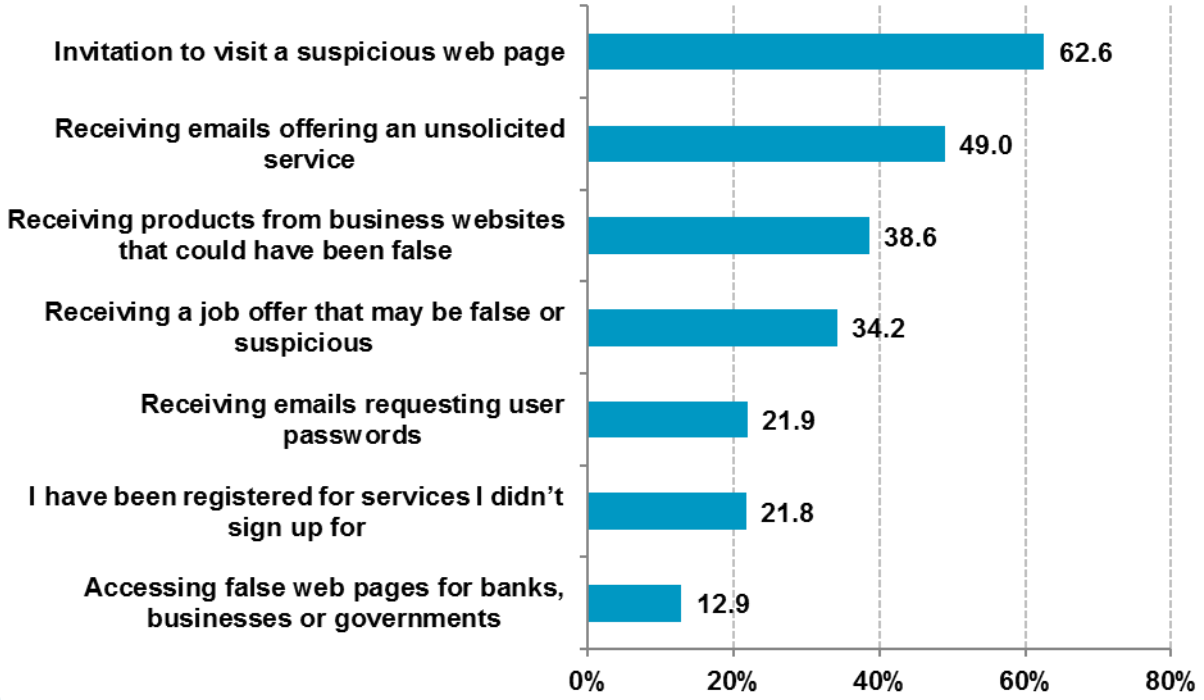


BASE: All users

Manifestation of the online fraud attempt:

Multiple response

% individuals



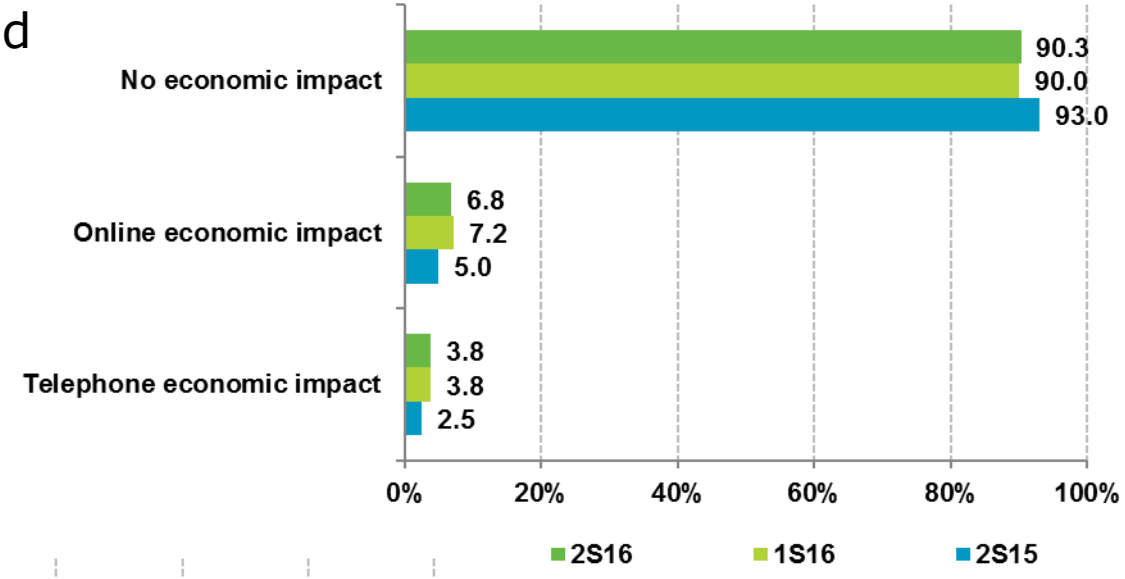
BASE: Users who have experienced attempted fraud

Find out more about online fraud:
https://www.osi.es/fraude-online

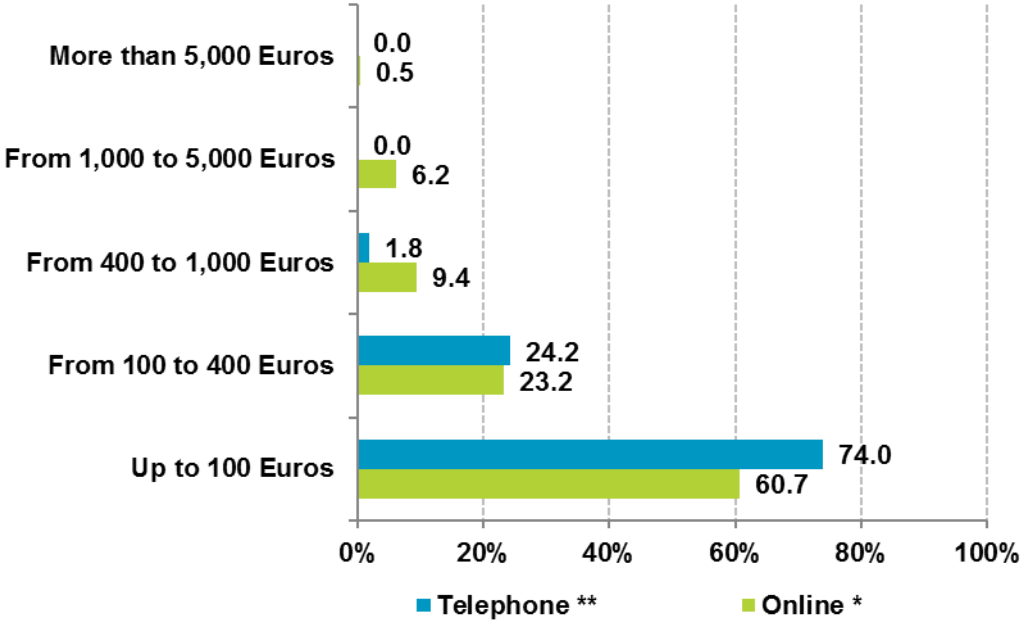
Online fraud attempt and manifestations

Economic impact of fraud

The percentage of fraud attempts that end in an **economic loss** for the victim remains at the same levels as the previous periods analysed.



BASE: Users who have experienced attempted fraud



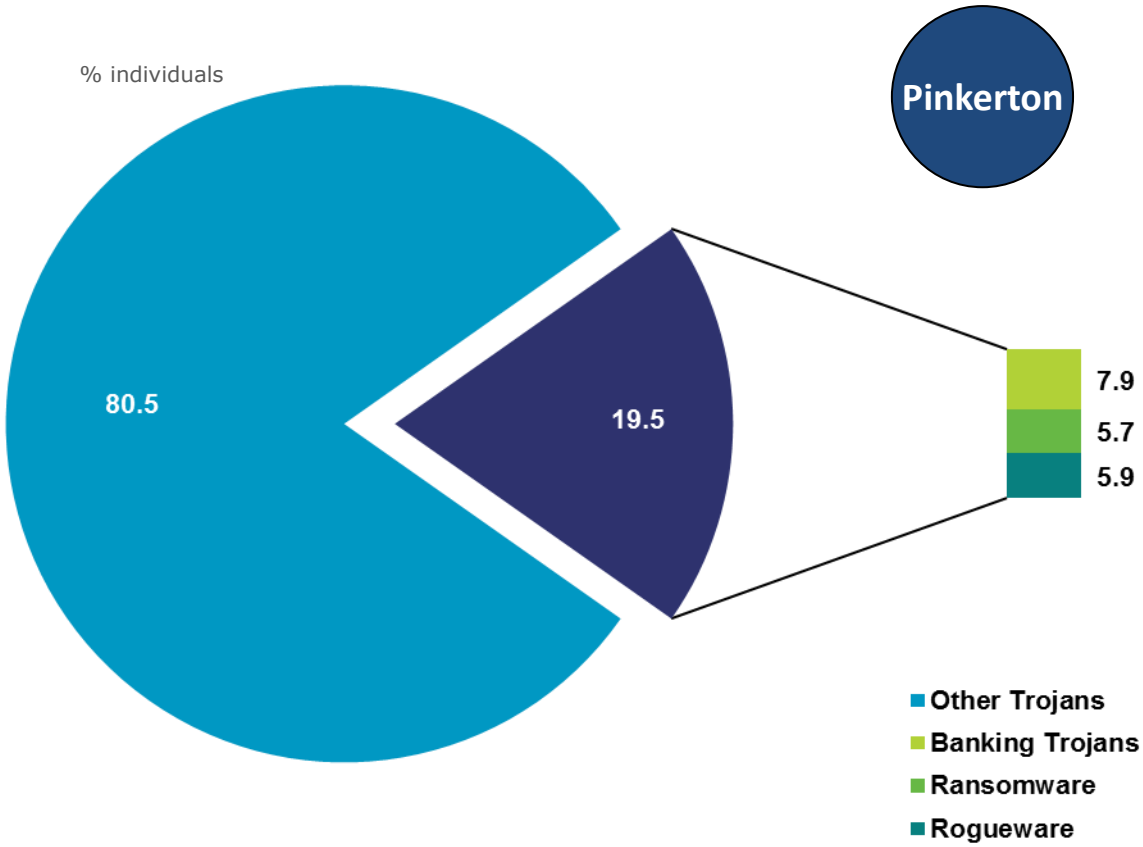
Distribution of the economic impact of fraud

* BASE: Users who have suffered economic damage as a consequence of online fraud

** BASE: Users who have suffered economic damage as a consequence of telephone fraud

Fraud and malware on a computer

During the second half of 2016 the number of **banking Trojans**, **ransomware** and **rogueware** detected on Spanish household computers fell.



Type of malware analysed

✓ Banking Trojans:
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.

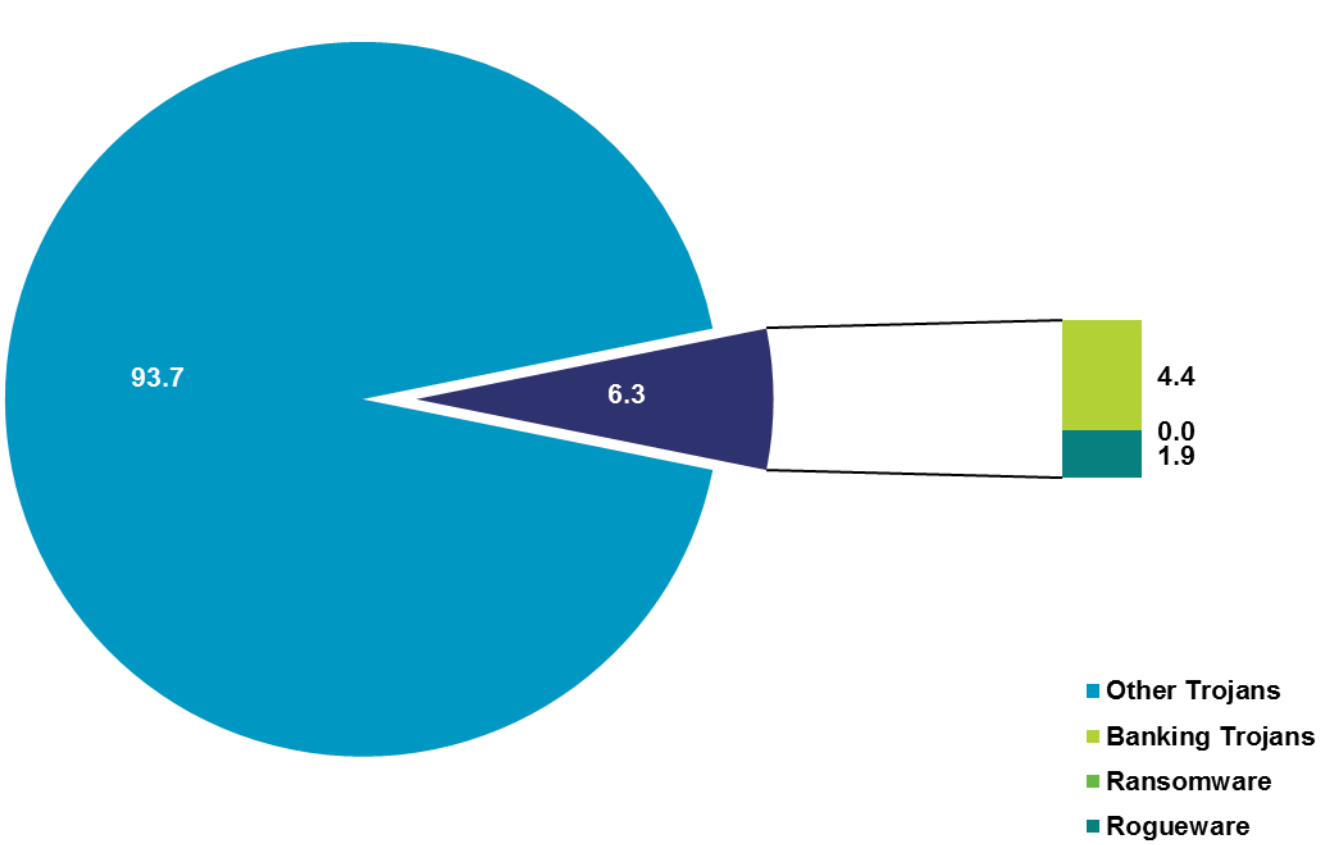
✓ Ransomware:
malware that installs itself in the system and takes it "hostage", then asks the user to pay a monetary amount as a ransom in exchange for disinfection.

BASE: Total Trojans detected on PC

Security and fraud

Fraud and malware on mobile devices

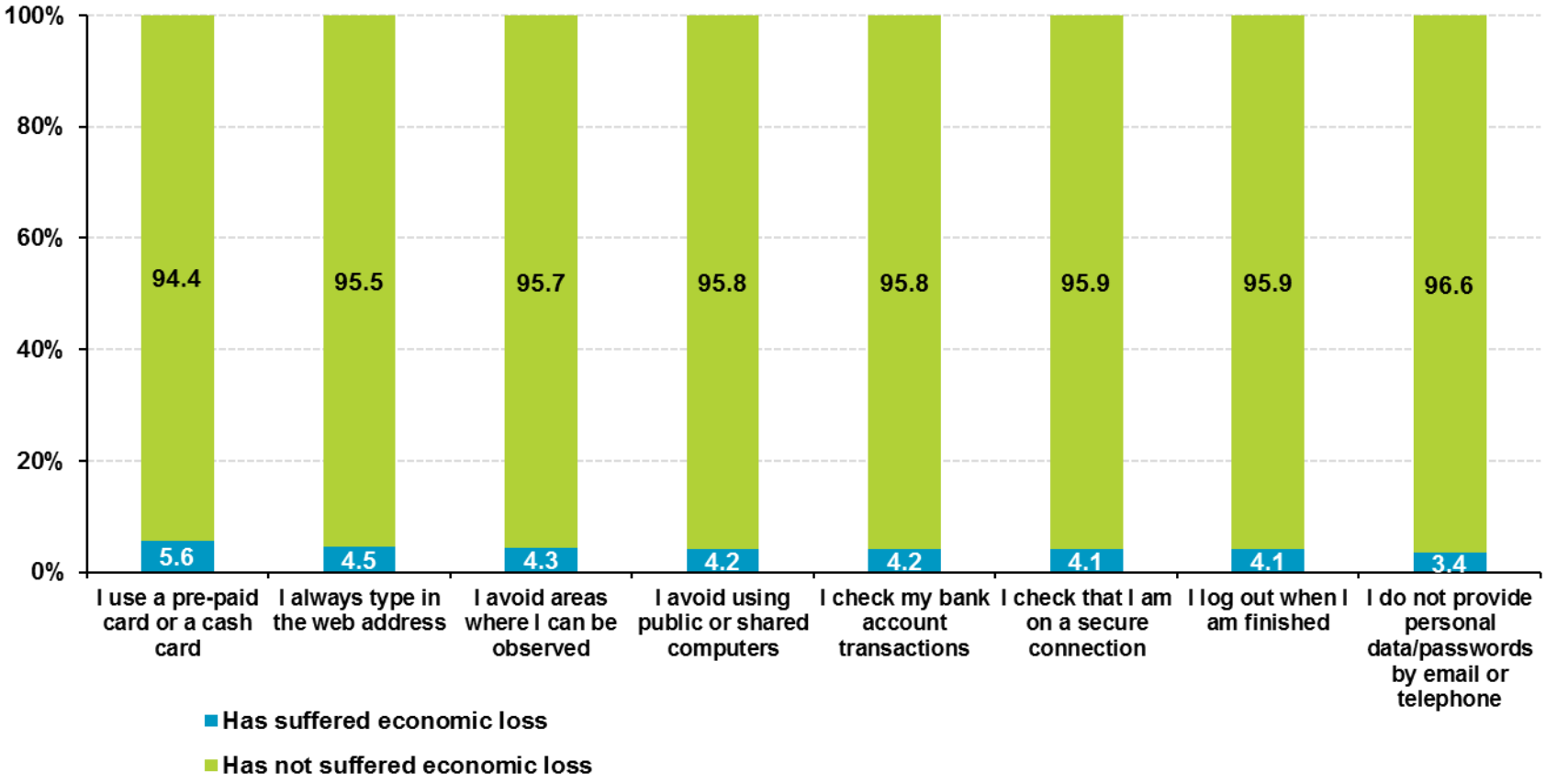
The presence of **banking Trojans** and **rogueware** on the Android devices analysed with **Pinkerton** also fell during the second half of 2016.



BASE: Total Trojans detected on Android devices

Successful fraud attempt according to prudent habits

Using prudent habits **minimises** the risk of the fraud attempt being successful. In all cases, a percentage over **94.4%** of users with good habits suffered NO economic loss as a result of online or telephone fraud.

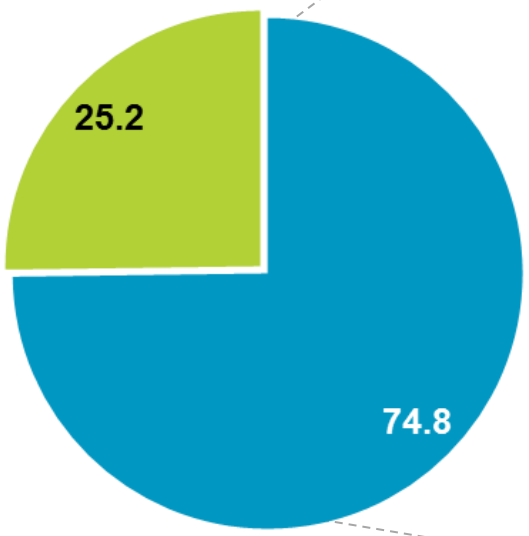


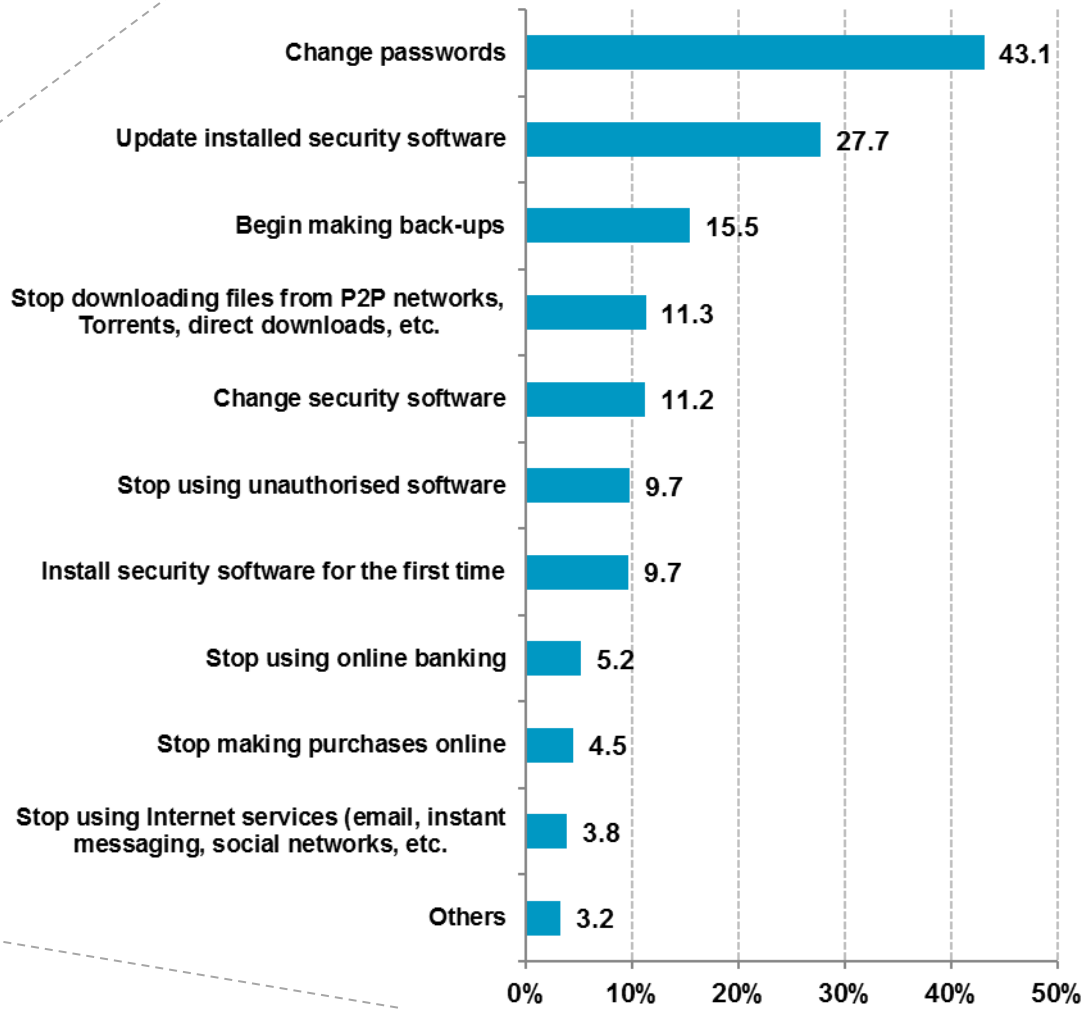
BASE: Online banking users

Changes made after a security incident

Changes made: **Multiple response**

% individuals





I have changed my habits in some way
I have not changed my habits in any way

BASE: All users who experienced an incident

BASE: Users who experienced an incident and made a change

5

Changes made after a security incident

Changes in security habits and measures according to type of incident

Of users who experienced a security incident related to **stolen identify,** a **change of password** is the main change in habit (**61.5%**).

Incident (%)	Change in habits					
	Change passwords	Update tools	Make backup	Change security programs	No longer using unauthorised software	Install tools for the 1st time
Malware	39.6	31.7	17.9	15.7	12.2	13.0
Loss of files or data	44.4	31.8	26.8	18.0	16.6	15.0
Spam	32.5	21.1	10.4	7.7	6.9	6.1
Stolen identity	**61.5**	35.6	25.8	25.3	23.8	21.0
Wi-Fi intrusion	48.6	**36.3**	**29.8**	**27.0**	17.6	**25.7**
Loss of device	49.3	25.7	21.1	24.0	**24.1**	19.0
Services inaccessible due to cyberattacks	45.7	32.6	23.0	18.2	13.4	16.3

BASE: Users who have experienced each of the security incidents

Changes made after a security incident

Changes in use of Internet services according to type of incident

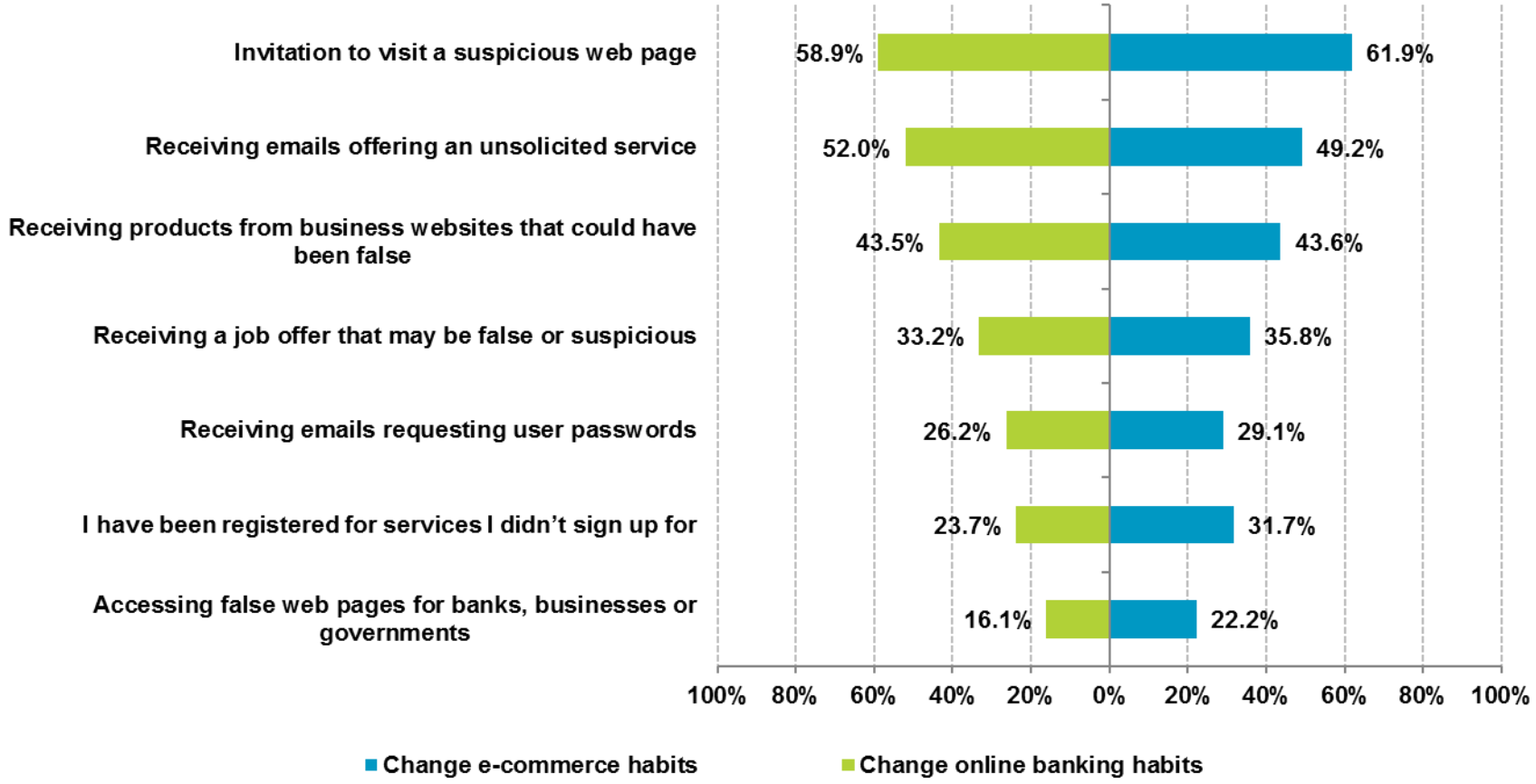
Incident (%)	Change in use of services			
	Stop using Internet services	Stop using online banking	Stop using e-Commerce	Stop downloading
Malware	5.6	6.2	6.3	14.3
Loss of files or data	12.2	12.7	14.3	12.3
Spam	1.7	2.5	2.3	7.7
Stolen identity	9.4	21.2	12.4	22.4
Wi-Fi intrusion	**18.7**	16.9	16.0	19.5
Loss of device	14.9	**28.4**	**17.9**	**28.5**
Services inaccessible due to cyberattacks	7.3	12.3	10.2	15.4

BASE: Users who have experienced each of the security incidents

Changes made after a security incident

Impact of the fraud attempt on online banking and e-Commerce services

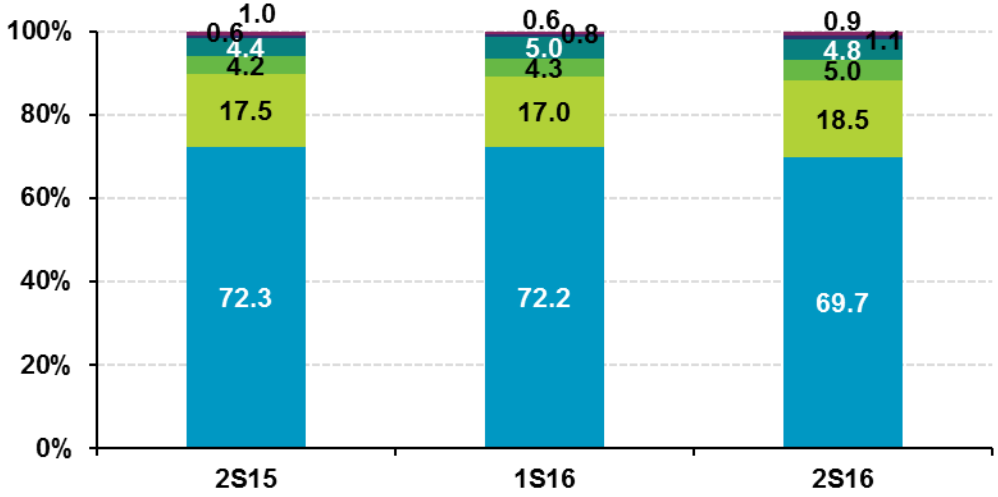
58.9% of online banking users and **61.9%** of e-Commerce users change their habits after receiving an **invitation to visit a suspicious website**.



BASE: Users who have experienced attempted fraud

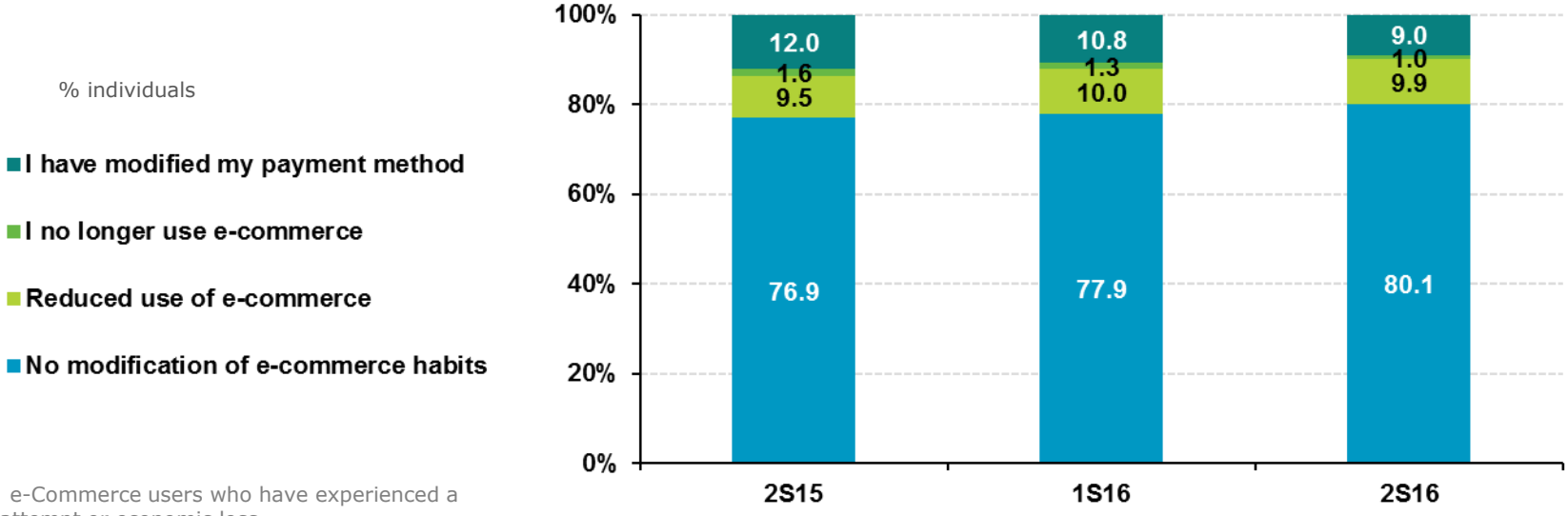
Changes made after a security incident

Modification of prudent habits related to online banking and e-Commerce services after experiencing attempted fraud



BASE: Online banking users who have experienced a fraud attempt or economic loss

% individuals



BASE: e-Commerce users who have experienced a fraud attempt or economic loss

Trust in the digital environment in Spanish households

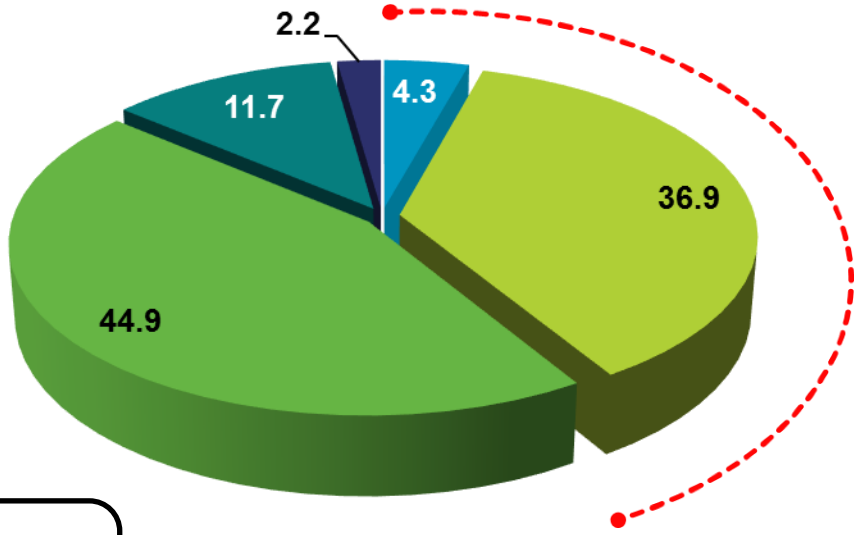
1. e-Trust and limits to the Information Society
2. User perception on the evolution of security
3. Assessment of the dangers of the Internet
4. Responsibility for Internet security

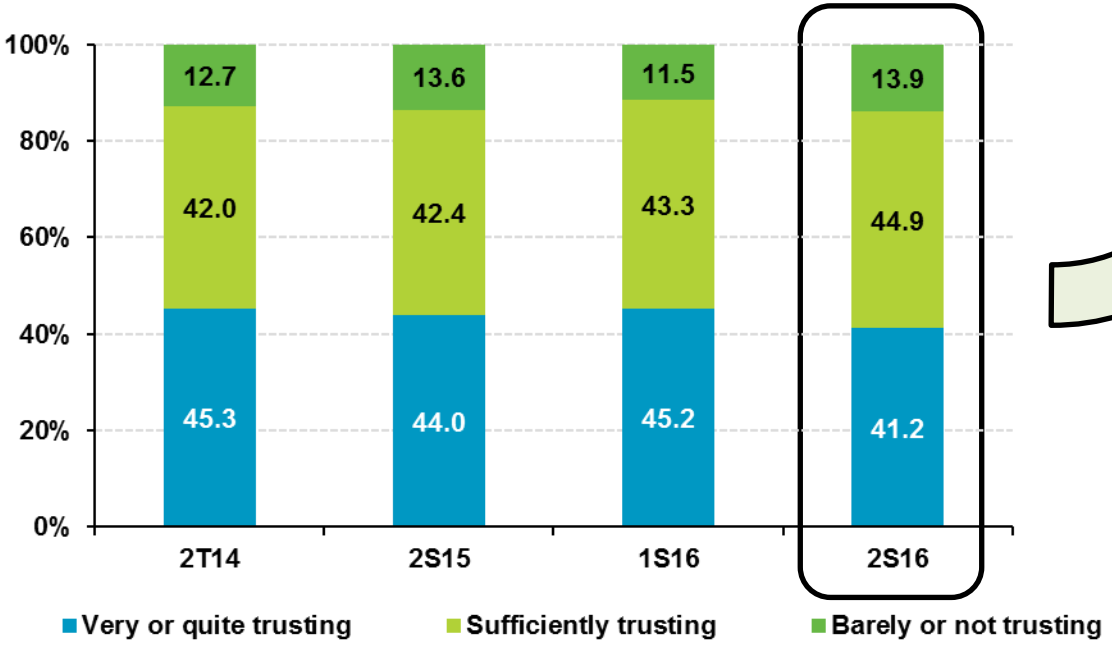
6

Level of trust in the Internet

Over **41.2%** of the users surveyed are quite or very **trusting** in the Internet.

Barely **2.2%** of the Spanish population **do not trust** the Internet.



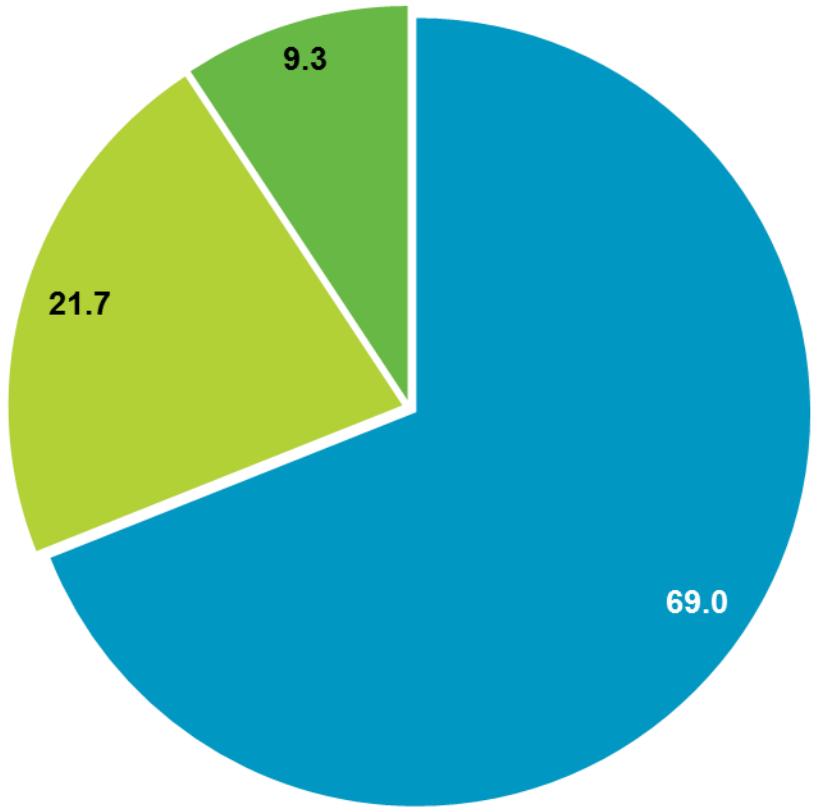


% individuals

BASE: All users

Assessment of the reasonably protected personal computer and/or mobile device

% individuals



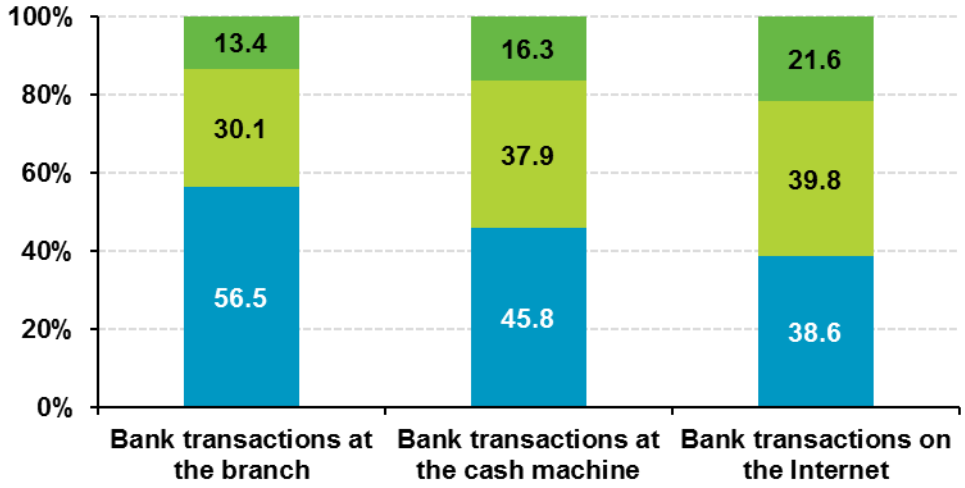
69% of the Internet users surveyed consider that their **computer** or **mobile device is reasonably protected** against potential Internet threats.

6

BASE: All users

e-Trust and limits to the Information Society

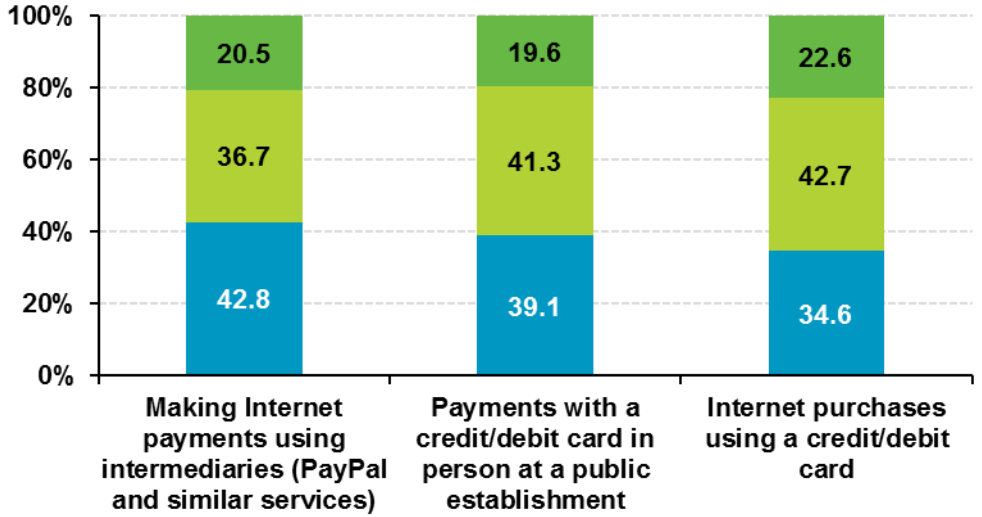
Online trust vs offline trust



Level of trust in bank transactions

% individuals

Level of trust in e-Commerce operations

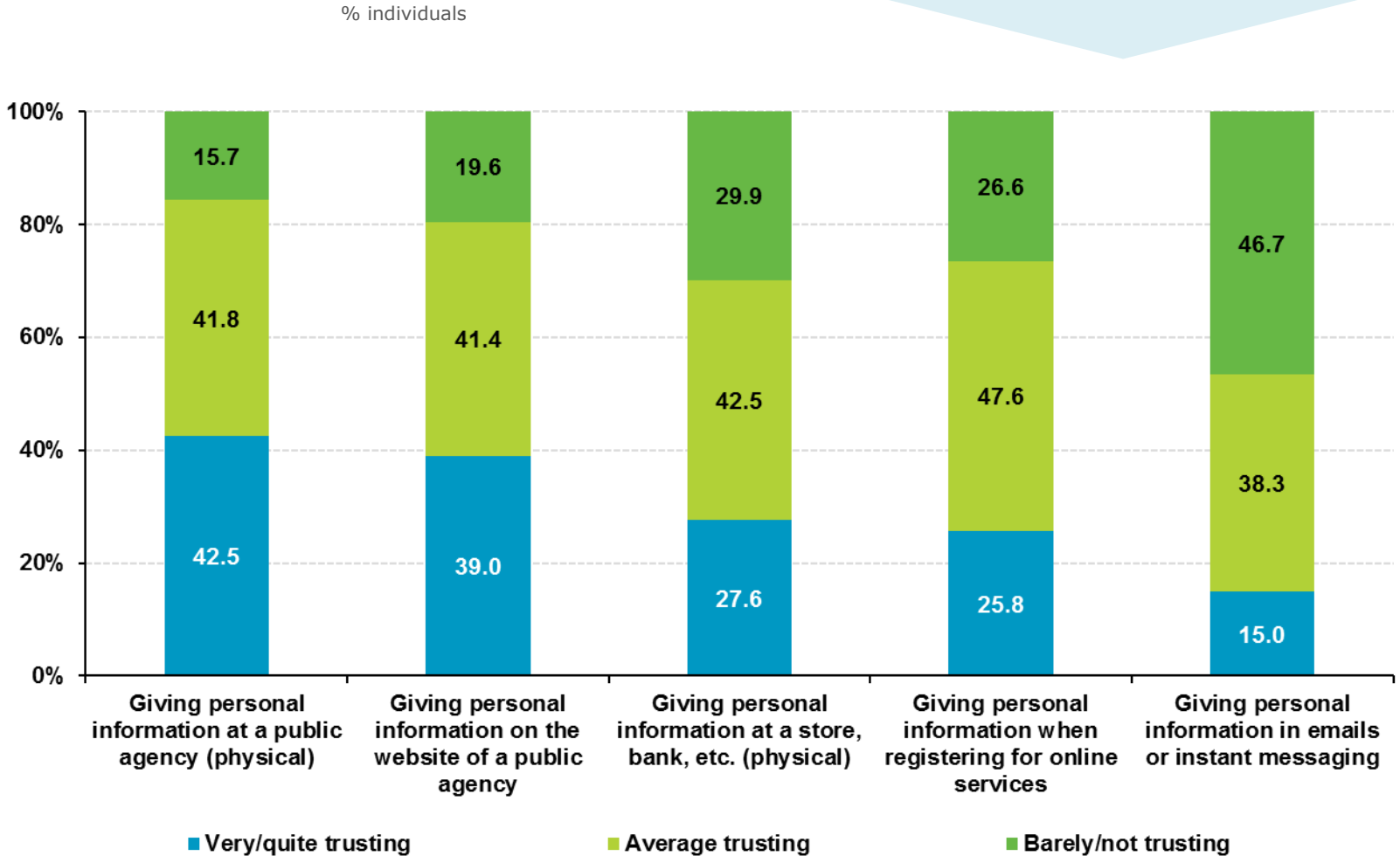


- Very/quite trusting
- Average trusting
- Barely/not trusting

BASE: All users

Online trust vs offline trust

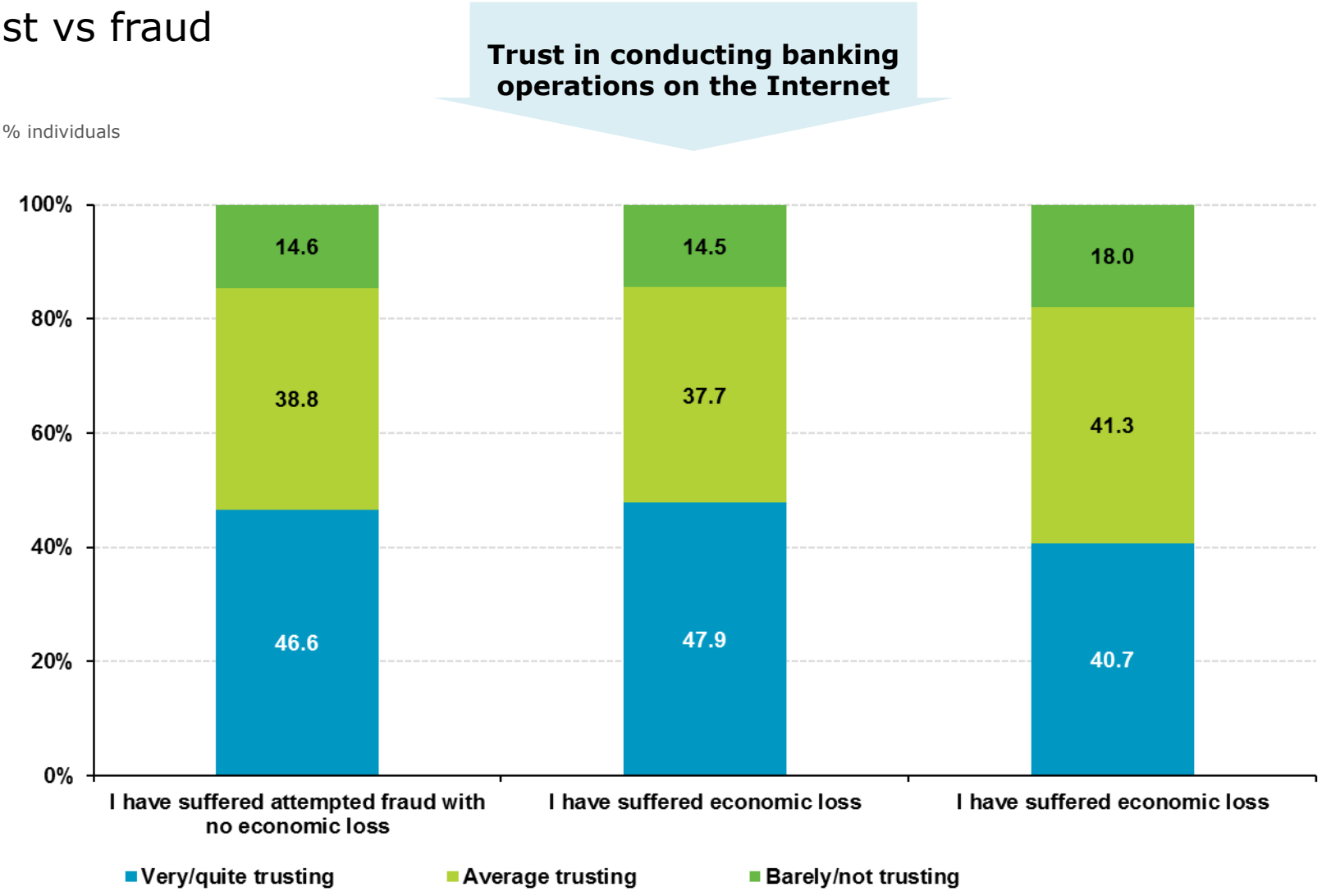
Level of trust in providing personal data



BASE: All users

e-Trust and limits to the Information Society

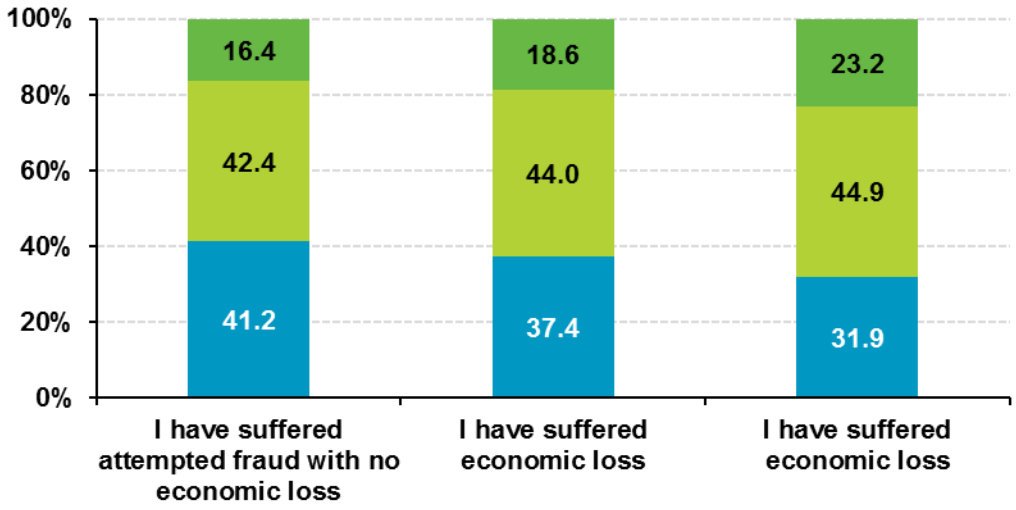
Trust vs fraud



BASE: Online banking users

e-Trust and limits to the Information Society

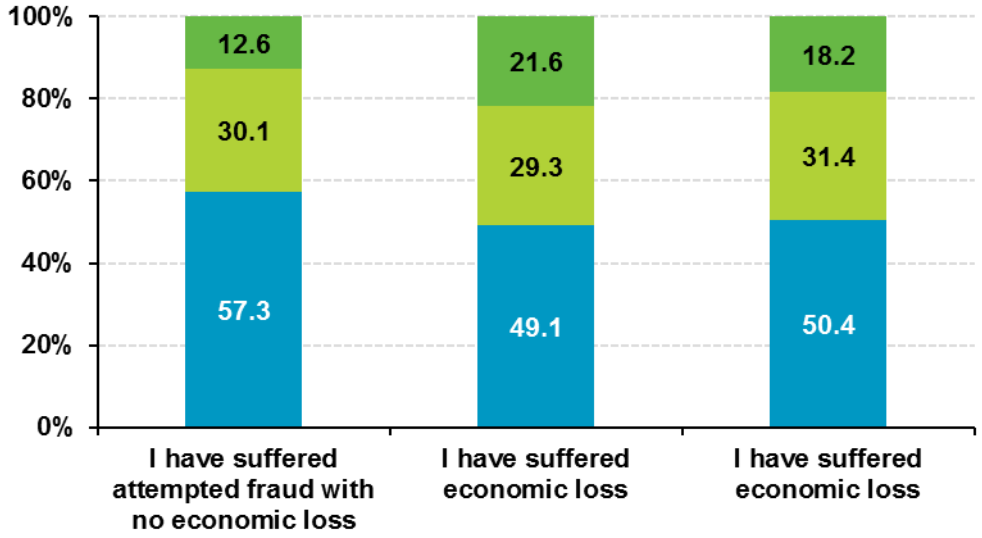
Trust vs fraud



Trust in Internet purchases using a credit/debit card

% individuals

Trust in Internet purchases <u>WITHOUT</u> using a credit/debit card



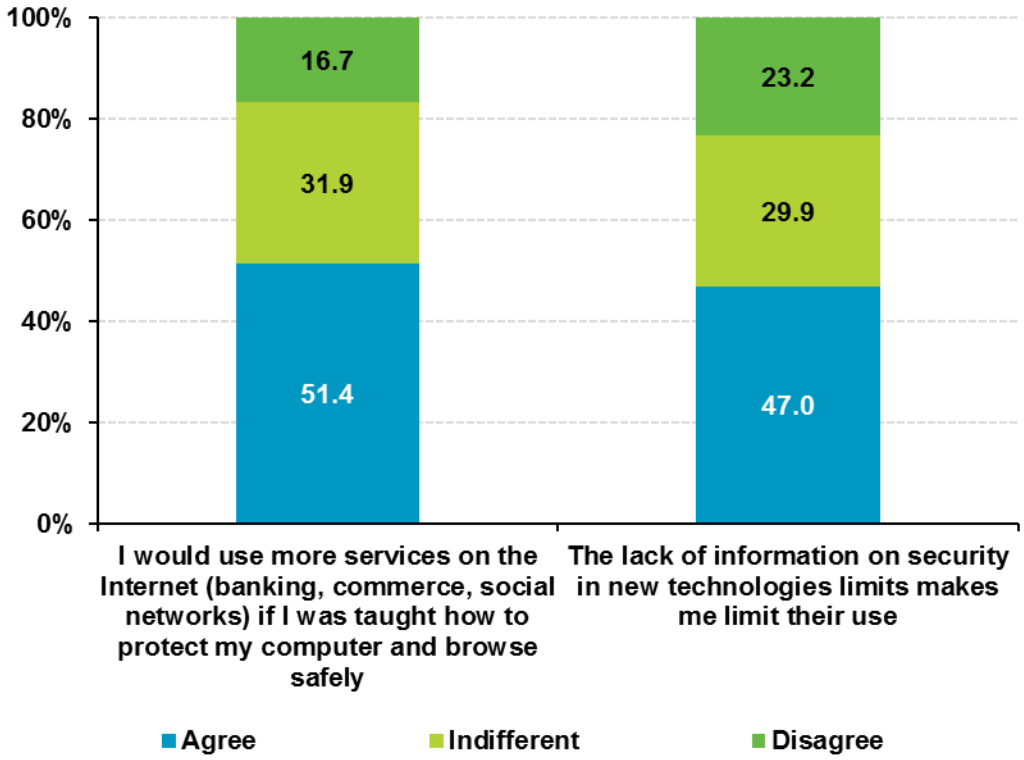
Very/quite trusting
Average trusting
Barely/not trusting

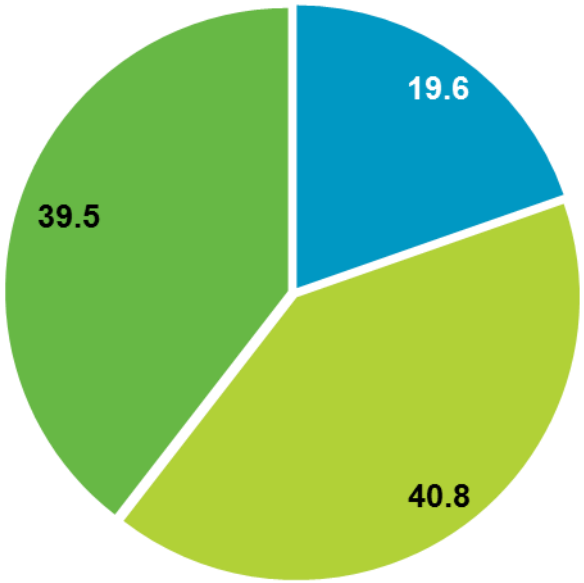
BASE: e-Commerce users

e-Trust and limits to the Information Society

Limitation caused by security problems

Security as a limiting factor in the use of new services





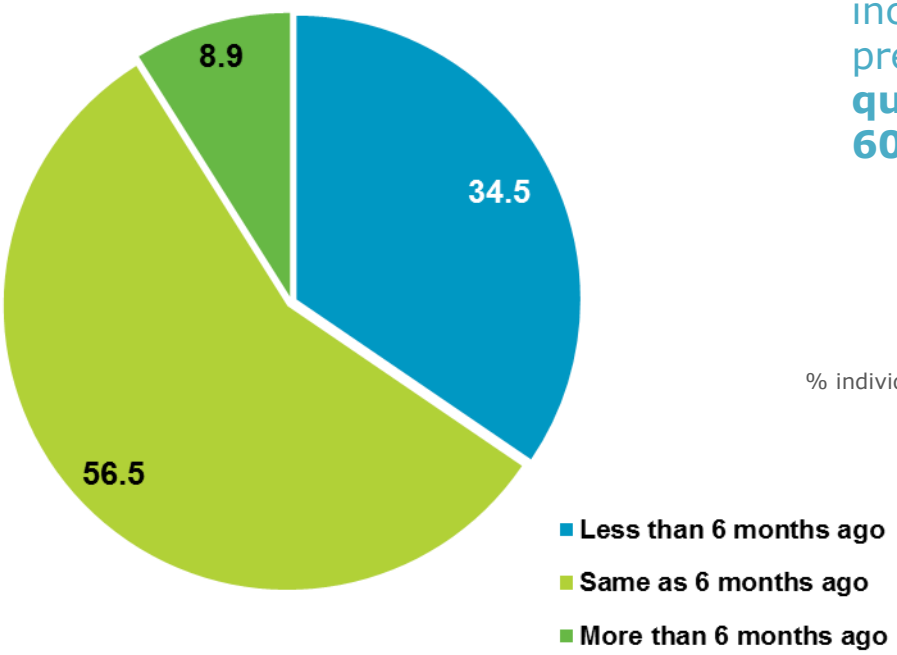
% individuals

Limitations in the use of Internet

6

User perception on the evolution of security

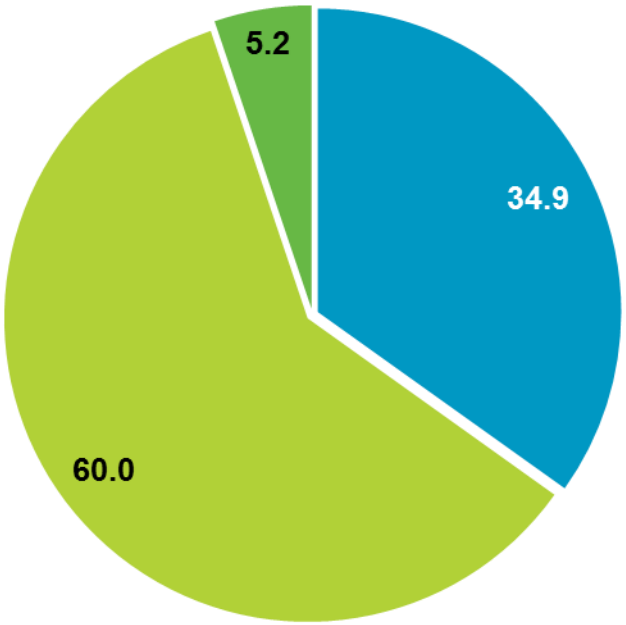
Number of incidents



Most of the users surveyed perceive that incidents in the last 3 months compared to previous months are **similar in terms of quantity and seriousness** (**56.5%** and **60%**, respectively).

Seriousness of incidents

% individuals



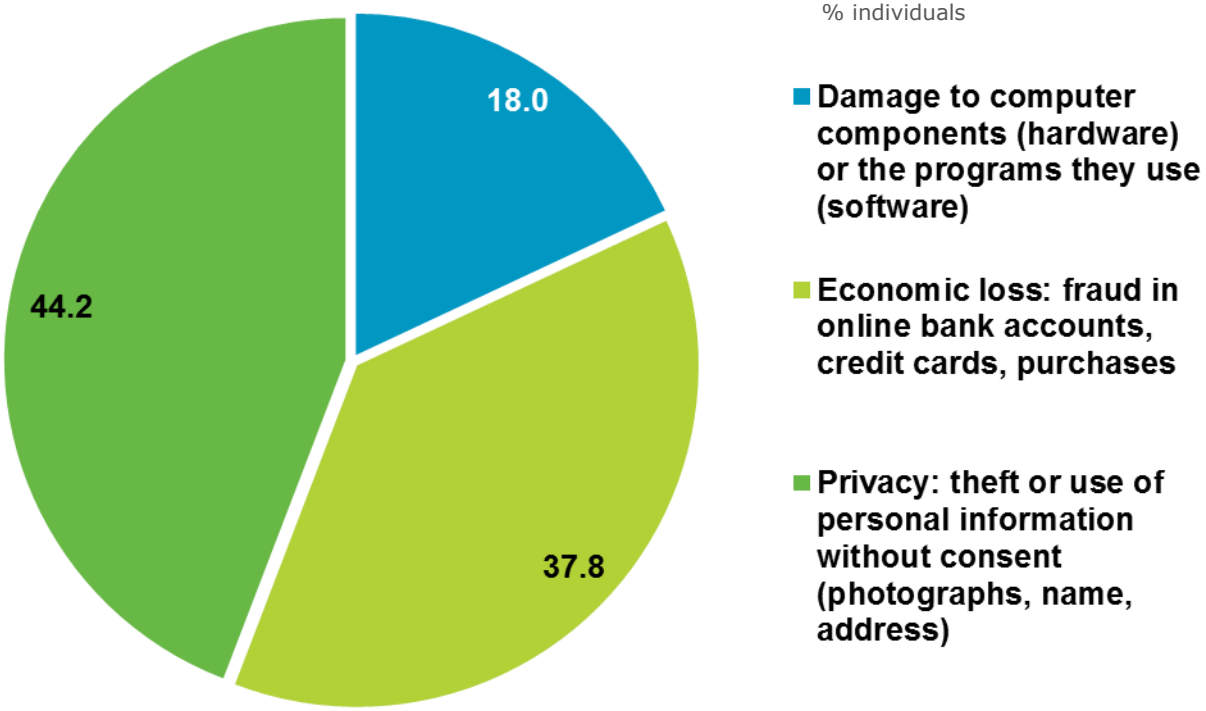
More than one third perceive a **lower number** of incidents in the last 3 months (**34.5%**) and also consider them to be **less serious** (**34.9%**).

BASE: All users

User perception on the evolution of security

Perception of risks on the Internet

Theft and use of personal information (**44.2%**) without the user's consent and the **economic loss** (**37.8%**) from fraud are the main risks on the Internet perceived by users.

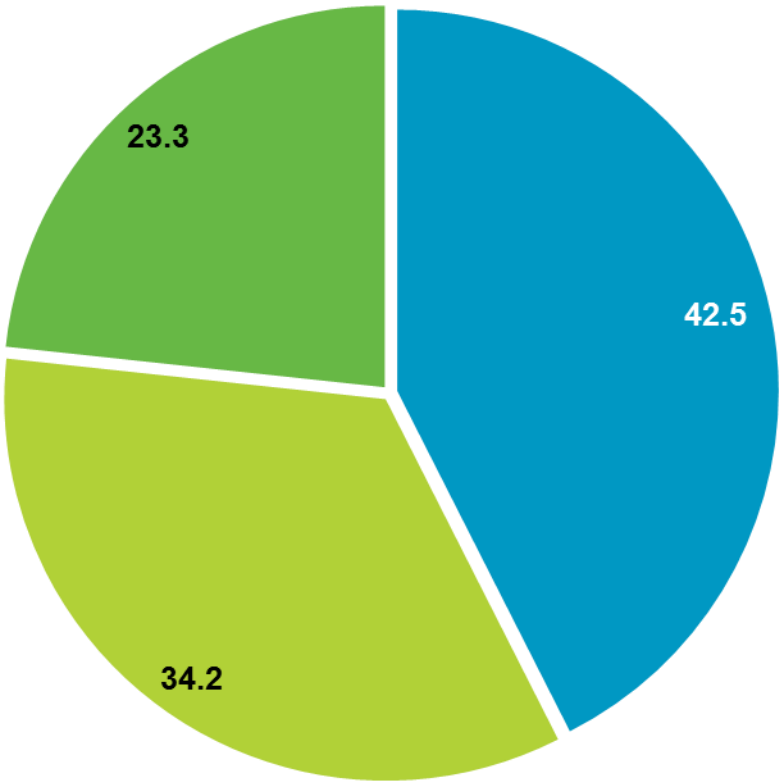


BASE: All users

User perception on the evolution of security

Assessment of the Internet as increasingly safer

% individuals



42.5% of Spanish users perceive the **Internet as increasingly safer**.

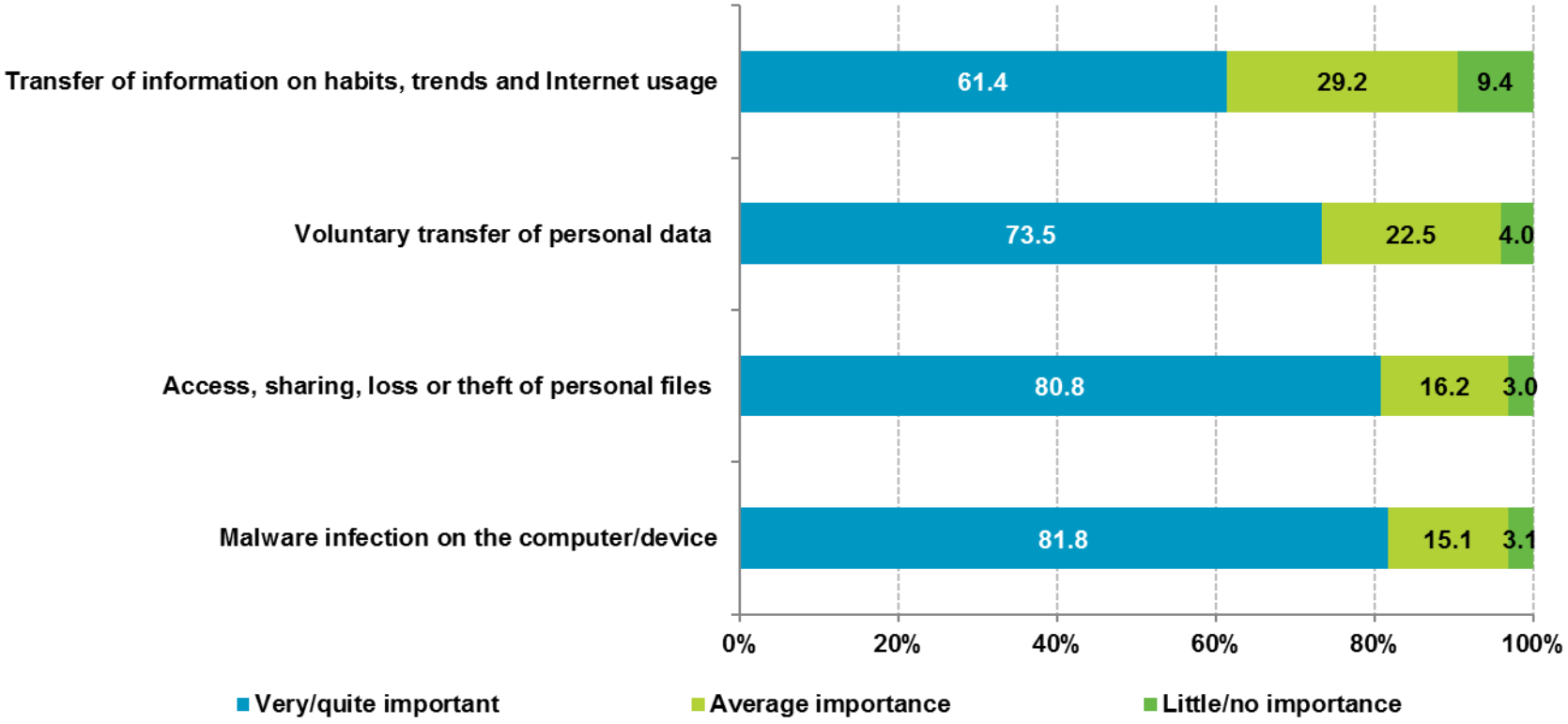
6

BASE: All users

Assessment of the dangers of the Internet

The dangers most valued by panellists are **malware infection on their computer/device (81.8%)**, and **access, sharing, loss or theft of personal files** (**80.8%**).

On the other hand, **transferring information on Internet habits, trends and use** (**61.4%**) is the danger Spanish Internet users give least importance to.



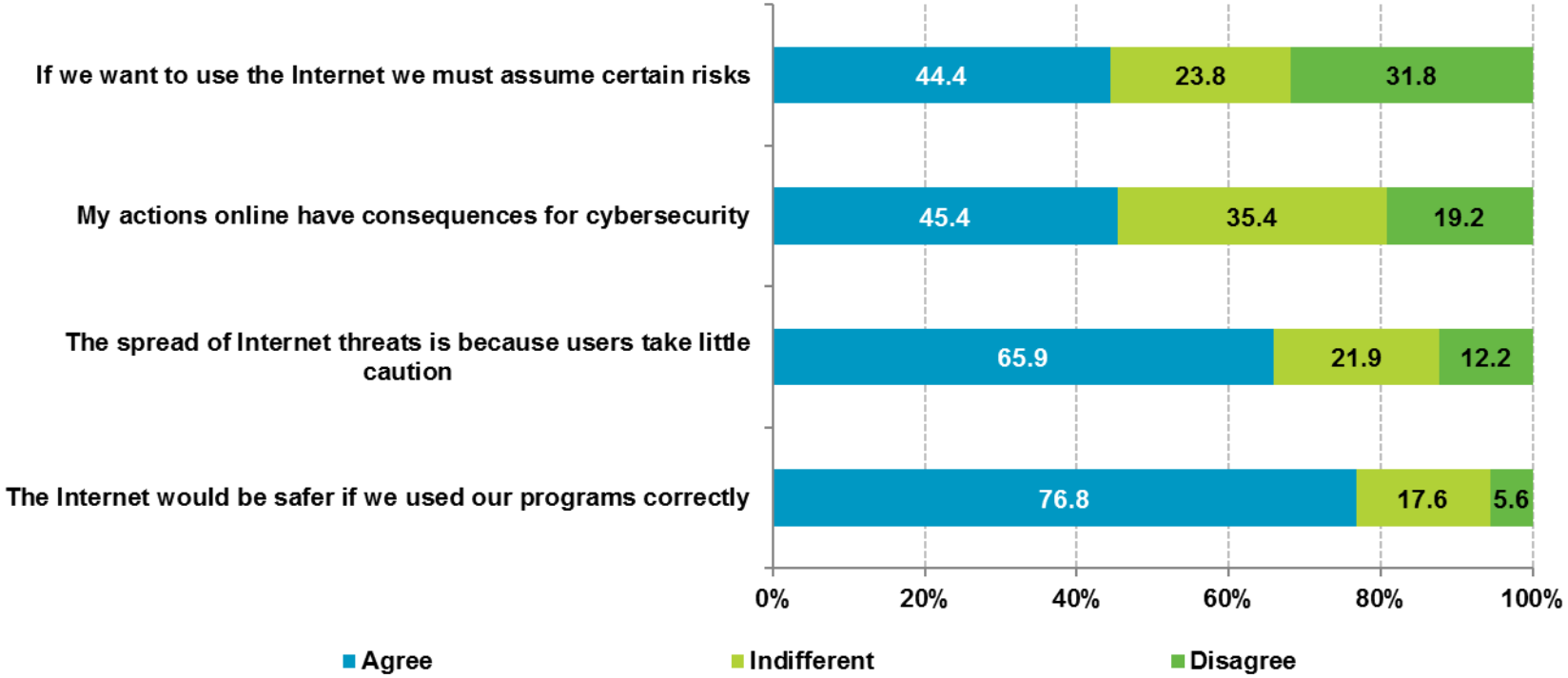
BASE: All users

Responsibility for Internet security

Role of the user

Three in four users (**76.8%**) consider that they do **not use the software available properly**, and **two thirds** (**65.9%**) believe that **threats spread due to the lack of caution of users**. Furthermore, **45.4%** of the panellists believe that **their actions affect cybersecurity**.

However, **44.4%** report that **certain risks must be assumed to enjoy the Internet**.



6

BASE: All users

Conclusions

Conclusions

Conclusions

Wi-Fi networks have become a daily element for any user. However, many of them are not aware of the risks[1] involved in connecting to an insecure or misconfigured network. 22.5% of Spanish Wi-Fi networks are insecure as they use WEP encryption (obsolete and vulnerable), or because the user is unaware of its status (5.4%, 7.6% and 9.5% respectively). This means that these Wi-Fi networks could suffer an intrusion, and even allow access to sensitive data stored on the computers and devices that connect to it.

But they are not only a risk for the owners of these wireless networks, the potential threats also affect users who connect to them: for example, others could connect in order to capture interesting data[2,3] transmitted on the networks; or they could even be false access points configured to appear like public networks in order to capture data.

Nevertheless, two in five (39.2%) users who connect to a public or third party Wi-Fi network do so whenever they need to and in any location, without checking the security offered, or considering the nature and degree of sensitivity of the data transmitted on it. In this way, they check their email, go on social networks, use online banking, purchase items, or even send and receive business information[4,5], exposing the confidentiality and integrity of all these sensitive data and information.

[1] https://www.kaspersky.com/about/press-releases/2016_1-in-4-wi-fi-hotspots-just-waiting-to-be-hacked-kaspersky-lab-stats-show

[2] https://www.slideshare.net/NortonSecurity/norton-wifi-risk-report-global

[3] https://www.infosecurity-magazine.com/news/kaspersky-lab-quarter-of-wi-fi

[4] https://blog.kaspersky.es/kaspersky-secure-connection/9160/

[5] https://blog.kaspersky.com/kaspersky-lab-international-travel-report/12429/

Conclusions

Malware also takes advantage of Wi-Fi networks[6]. Such is the case of a *"Switcher Trojan"*, which infects Android devices and then attempts to access Wi-Fi routers, taking advantage of their vulnerabilities or the default access credentials. Once it has accessed the network, it modifies the default addresses of the DNS servers for malicious addresses, so that when the user tries to access a legitimate page they are really forwarded to a fraudulent page.

Malware is constantly evolving and its developers search for and design new methods to infect and spread malware, as proven by *"Svpeng"*. This banking Trojan used *Google Adsense*, the largest advertising network in the world, to infect Android devices from the ads and banners published on legitimate websites trusted by users[7].

But this is not the only case of malware taking advantage of the trust of users. *"Guerrilla"*, another malware for Android, attempts to steal *Google Play*[8] credentials, using the store API to download, buy, rate and comment applications in the user's name without their knowledge or consent. This strategy of manipulating market APP opinions and ratings conditions the trusting user who makes decisions based on the ratings and comments of others

[6] https://blog.kaspersky.es/switcher-trojan-attacks-routers/9808/

[7] https://blog.kaspersky.es/advertising-svpeng/9511/

[8] https://securelist.com/blog/research/75894/how-trojans-manipulate-google-play/

Conclusions

they know. Because although they are included in an official repository, and despite all the measures used to avoid it, these applications could be malicious[9]. This could also put at risk all the users (93.5%) who mainly download applications from official repositories to avoid security problems.

In these cases, the presence of an antivirus software that detects potential threats can be decisive. However, only 49.1% of the devices scanned with Pinkerton have this type of solution.

Malware can even request collaboration from victims[10] to spread even faster. After infecting a computer, the ransomware *"Popcorn Time"* encrypts all its content and gives the victim the option of paying a ransom to recover their data, or it infects their contacts by sharing the link to download the malware with them. In this way it avoids the good habit of not opening emails or clicking on links sent by an unknown source.

The above examples should not be seen as isolated cases: the average number of new samples of malware detected during the second half of 2016 stands at 200,000 a day[11,12] and, as mentioned above, they are constantly evolving to avoid detection, dodge new security measures, take advantage of vulnerabilities, etc.

[9] http://blog.checkpoint.com/2016/08/31/dresscode-android-malware-discovered-on-google-play/

[10] https://www.wired.com/2016/12/popcorn-time-ransomware/

[11] http://resources.pandasecurity.com/newhome2016/microsite AD/resources/Pandalabs/Pandalabs-2016-Q2-es.pdf

[12] http://resources.pandasecurity.com/newhome2016/microsite AD/resources/Pandalabs/Pandalabs-2016-Q3-es.pdf

Conclusions

As an example, the banking Trojan *"Gugi"* which, given the increased use of Android 6 (+17.9 p.p. in the last six months), has been updated to avoid some security measures implemented in that version[13]: permissions to superimpose applications and perform actions such as sending SMS messages.

The situation is more serious in household computers. While 69% of Internet users consider their computer to be protected, malware was found in 63.9% of the computers scanned, and in 53.7% of the cases the user thought that their computer was not infected. Also, according to the nature of the malware found, we can conclude that 71.8% of the computers are infected at a high risk level.

Returning to the issue of antivirus software, considering that 77% of PC users and 49.1% of Android users use this security measure, we must ask how such a number of infections is possible. One possible reason is that antivirus software is not infallible and malware always seeks new ways of avoiding detection, but this is not the only reason. According to reports by Internet users, a significant percentage does not analyse files downloaded from P2P networks (37.8%) or by direct download (47.9%). Users also consider that security tools are not used correctly (76.8%), that users themselves must be more cautious (65.9%), and that risks must be taken to enjoy the Internet experience (44.4%).

These declarations could be a key to the number of infections: misuse of this type of tool, ignoring security alerts, disabling them to browse untrusted sites, installing illegitimate programs with patches/cracks, etc.

[13] https://securelist.lat/blog/moviles/83840/banking-trojan-gugi-evolves-to-bypass-android-6-protection/

Conclusions

We must understand that an antivirus software is not a reactive tool (used only to correct a security problem that has already arisen). It is actually proactive, as it can prevent and avoid these security incidents.

Therefore it is advisable to use this security tool properly because, as shown in the above examples, malware can use extremely varied techniques to deceive users and take advantage of their trust for its own benefit.

Scope of the study

Scope of the study

Scope of the study

The *"Study on Cybersecurity and Trust in Spanish households"* is conducted using a dedicated online panel methodology comprising households with Internet connection around the country.

The data extracted from the survey, conducted every six months, allow us to ascertain the users' perception of Internet security and level of e-Trust.

Data sheet

Universe: Spanish Internet users over 15 who frequently access Internet from the home (at least once a month).

Sample Size: 3,516 households surveyed and their computers/Android devices scanned (software installed on 2,667 PCs, and 831 Android smartphones and 18 Android tablets).

Scope: Peninsula, Balearic Islands and Canary Islands

Sample Design: For every Autonomous Region, proportional stratification by type of home, with quotas per social segment and number of people in the household.

Fieldwork: Fieldwork was conducted between July and December 2016 with online surveys conducted on a panel of Internet users.

Sample Error: Assuming simple random sampling criteria for dichotomous variables in which p=q=0.5, and for a level of trust of 95.0%, the sample size of n=3,516 is established an estimated sample error equal to ±1,65%.

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

Thanks for collaborating in this study goes to:

HISPASEC

GfK

Thanks as well to the following individuals for their collaboration:

INSTITUTO NACIONAL DE CIBERSEGURIDAD

ISSN 2386-3684

All rights reserved. Copying and distributing via any media is permitted as long as the authors are credited, no commercial use is made of the work, and no modifications are made.

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