Study on Cybersecurity and Trust in Spanish households

January – June 2019 Series

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA Y EMPRESA

ontsi observatorio nacional de las telecomunicaciones y de la SI

red.es

October 2019

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 the adopted security measures 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 3.619 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 that are 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 the analysis from **January to June 2019**.

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:

- **1H17**, study conducted during the first half of 2017 (January - June).
- **2H17**, study conducted during the second half of 2017 (July - December).
- **1H18**, study conducted during the first half of 2018 (January - June).
- **2H18**, study conducted during the second half of 2018 (July - December).
- **1H19**, study conducted during the first half of 2019 (January - June).

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

Definition and classification of security measures

Security measures[1]

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

Automatable measures

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

Non-automatable measures

Active measures that generally **require a specific action by the user** for correct operation.

Proactive measures

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

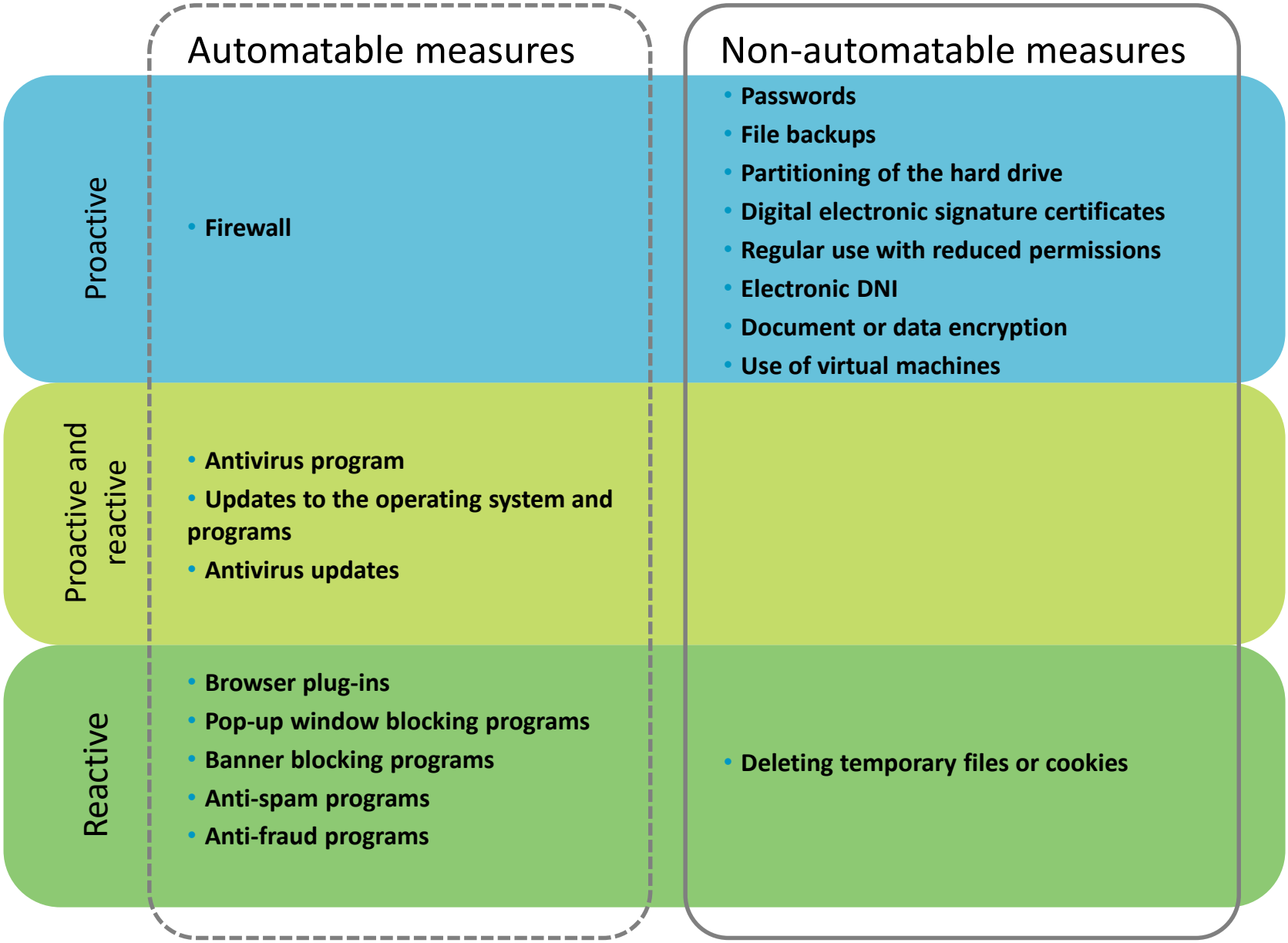
Reactive measures

Measures used to **correct** security incidents, in other words, 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 those that try to enter it.

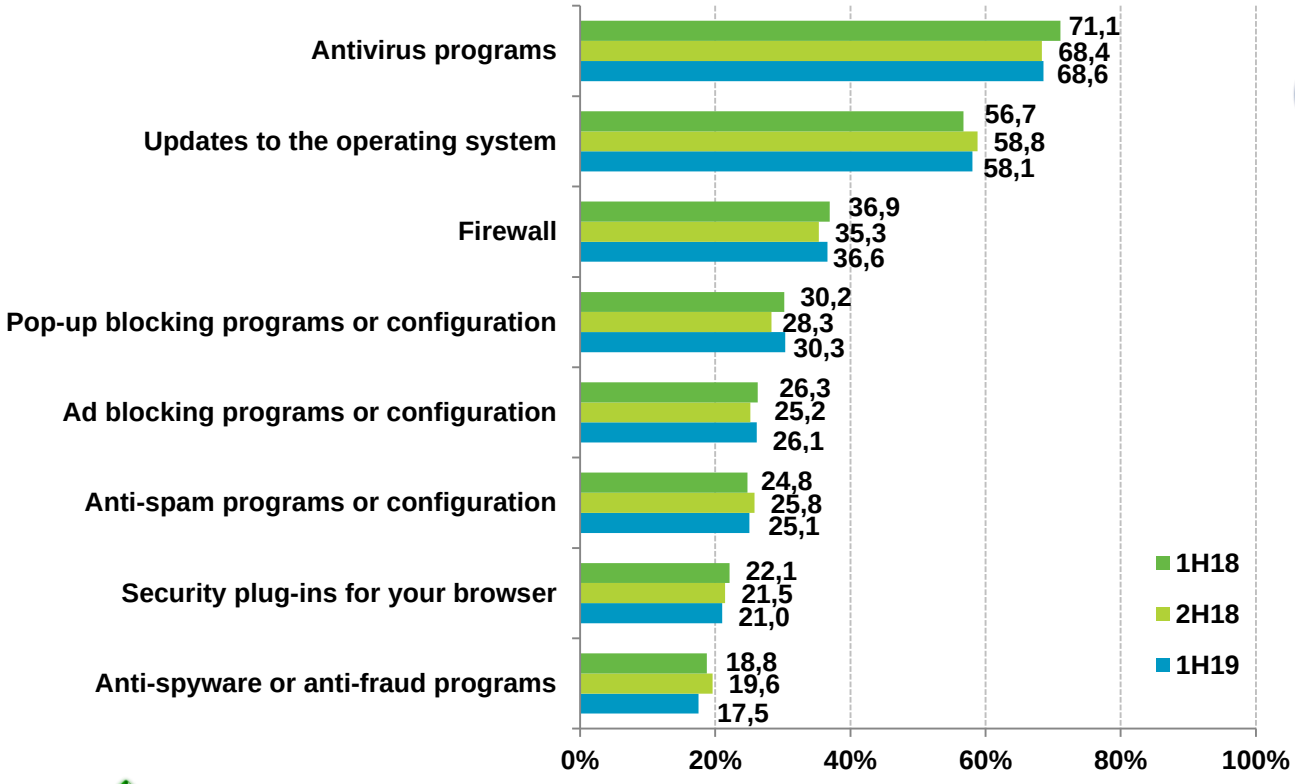
Definition and classification of security measures



Use of security measures on the household computer

Automatable security measures

The use of **antivirus programs** (**68.6%**) and **OS updates** (**58.1%**) keeps stable.



Antivirus programs do not only eliminate malware on the computer. Their most important task is to prevent and avoid malware infections.

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

BASE: PC Users

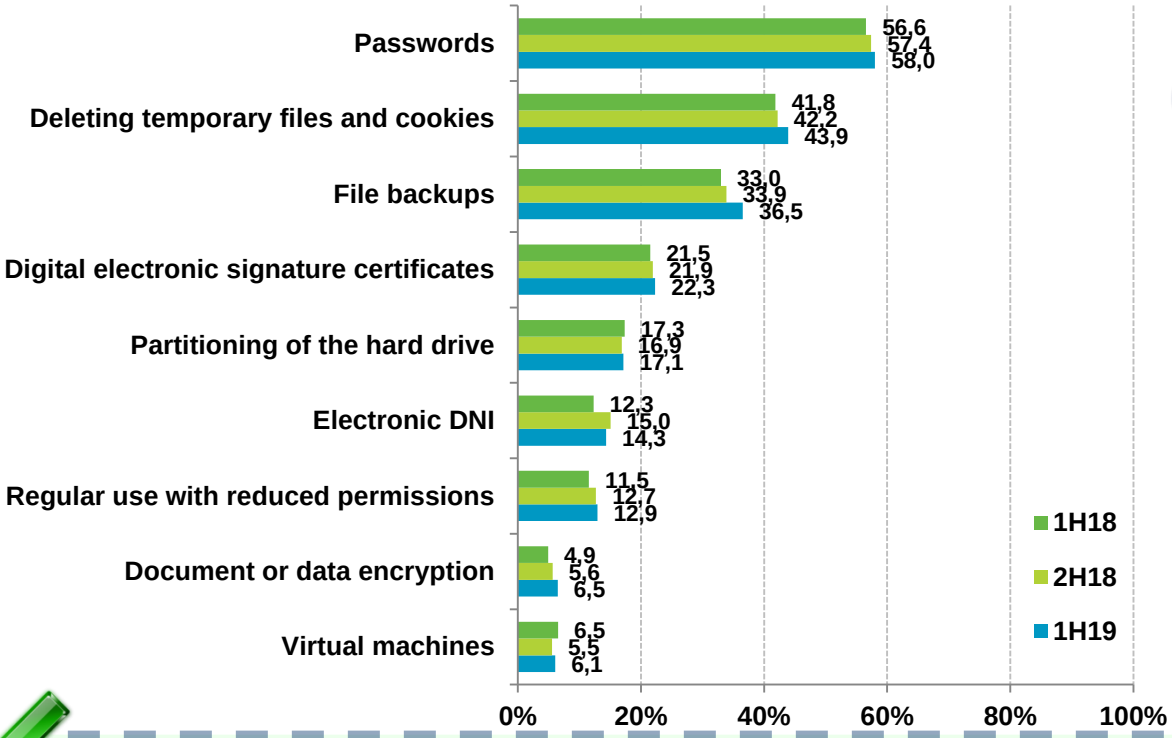
Do you know why security updates are important?

https://www.osi.es/es/actualizaciones-de-seguridad

Use of security measures on the household computer

Non-automatable or active security measures

Active security measures tend to continue growing, particularly **file backups** (**36.5%**) along with **deleting temporary files and cookies** (**43.9%**)



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

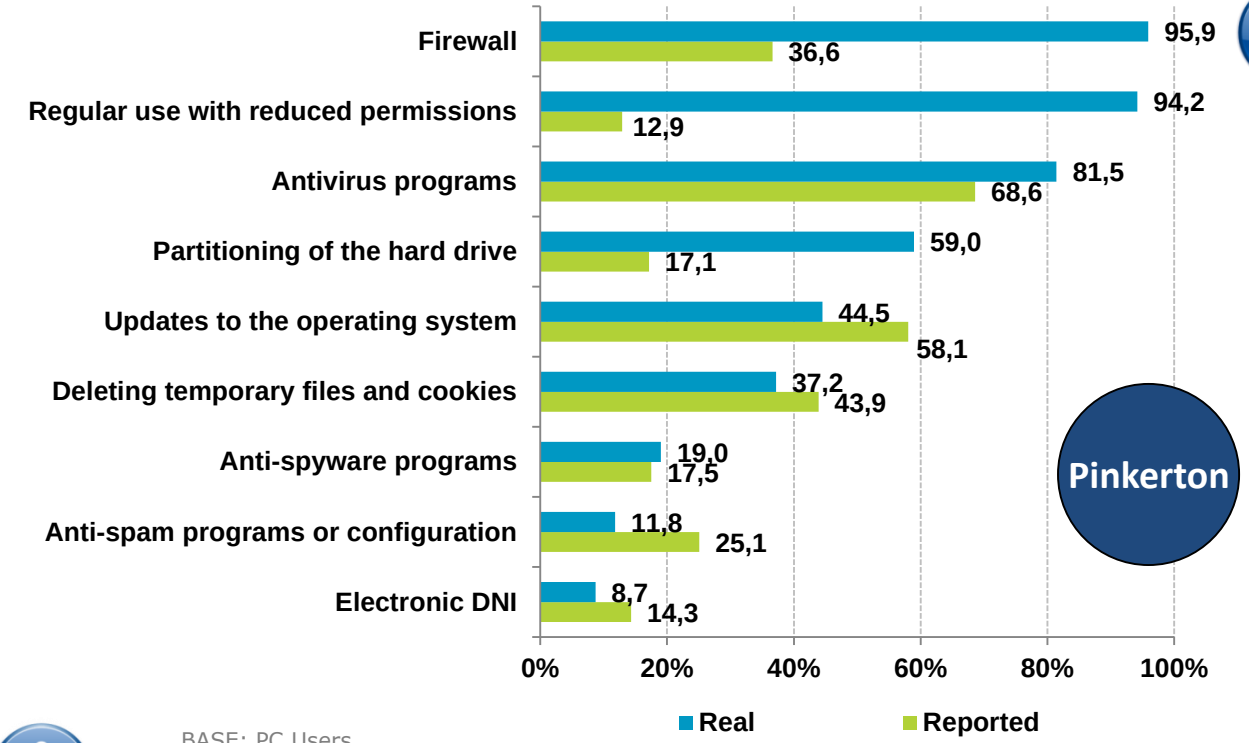
It is extremely important to use passwords, etc., correctly, and create backups of the data we want to save. For more information on these tasks:

- ✓ **Passwords:** https://www.osi.es/es/campanas/contrasenas-seguras
- ✓ **Backups:** https://www.osi.es/es/campanas/copias-cifrado-informacion

Use of security measures on the household computer

Reported vs real use of security measures

There is still a remarkable gap between the reported and the real use of security measures, specially regarding the **regular use with reduced permissions** (**81.3 p.p.**) and the use of **firewall** (**59.3 p.p.**).



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 of malicious programs.

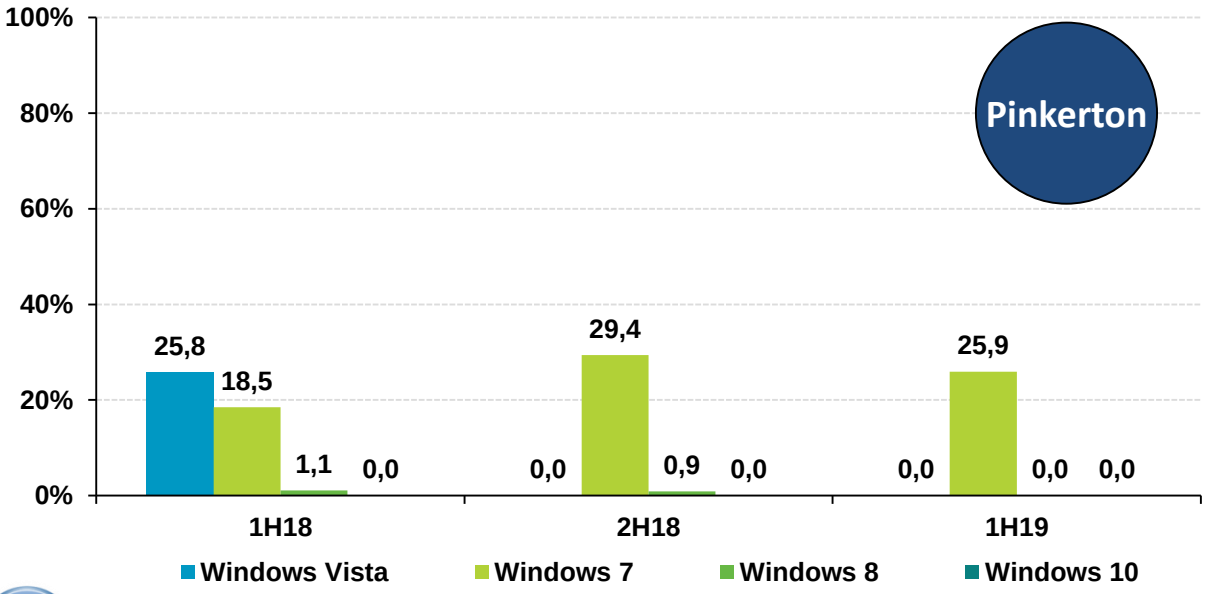
https://www.osi.es/es/actualidad/blog/2014/07/18/fauna-y-flora-del-mundo-de-los-virus

To obtain the real data, we used **Pinkerton** software developed by Hispasec Sistemas. This program 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



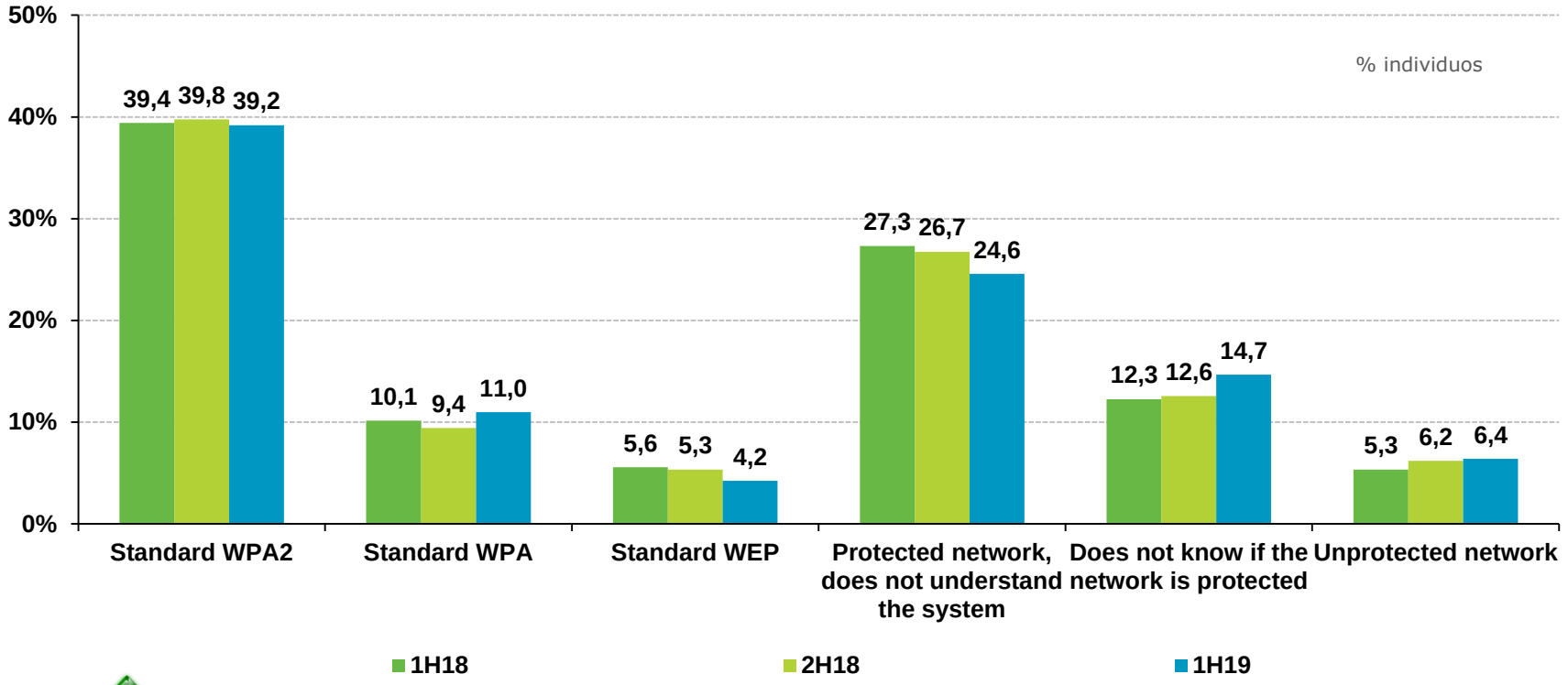
The difference between the level of privileges used in the different Windows versions must be configured by default applied to the user account.

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

The volume of **networks with unknown security level or completely unprotected networks** is still very high (24.6% + 14.7% + 6.4%). Also, the use of the **standard WEP** keeps decreasing compared to the results of the last version of this study **(-1.1 p.p.)**.

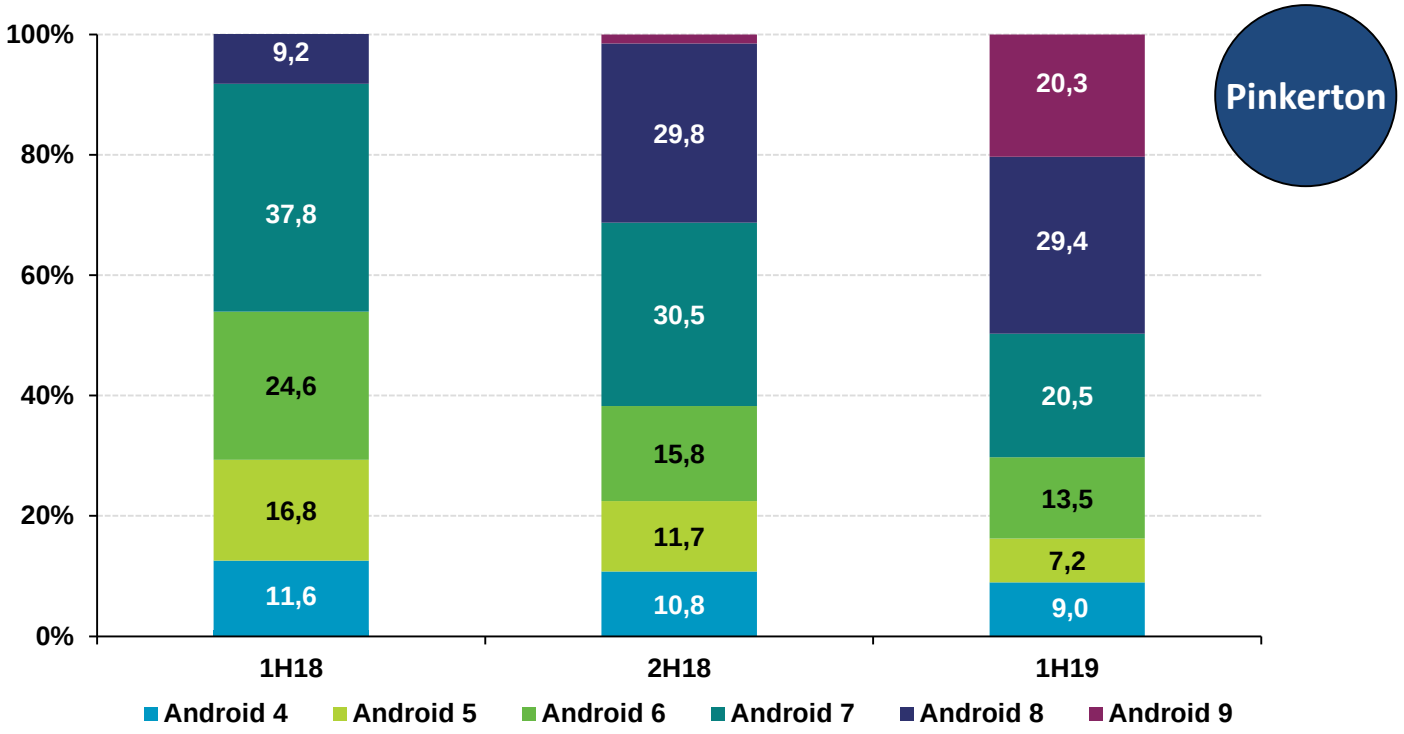


How to securely configure your Wi-Fi network: https://www.osi.es/protege-tu-wifi

BASE: Users with their own Wi-Fi connection

Operating system version on Android devices

Android 9 has reached the same market share as **Android 7** (around **20%**). The use of **Android 8** maintains stable (**29.4%**).

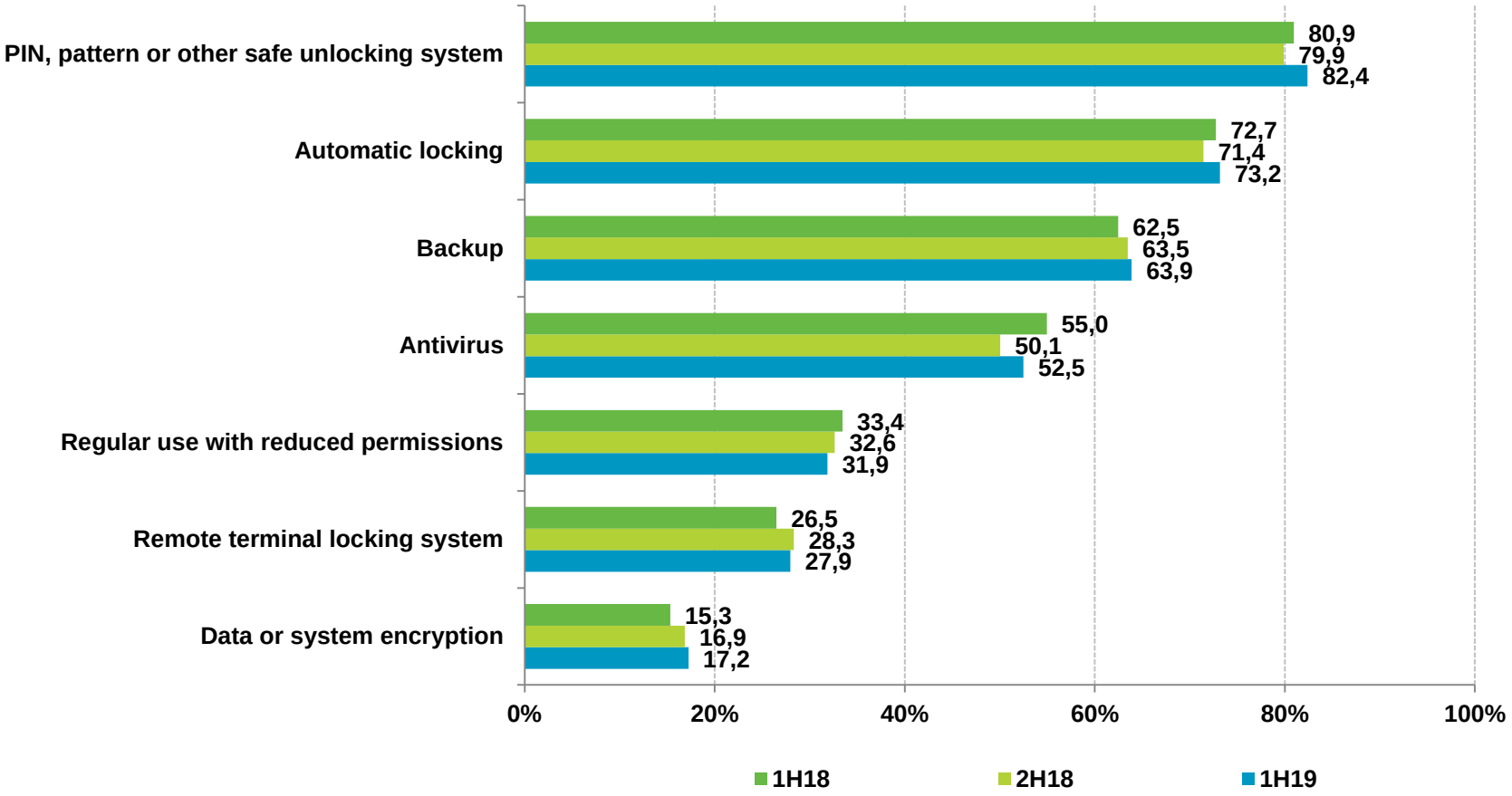


BASE: Users with an Android device

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

Use of security measures on Android devices

The use of **secure locking systems** (**+2.5 p.p.**) and **automatic locking** (**+1.8 p.p.**) shows the greatest increase and they continue to be the most frequently used security measures according to users' report.

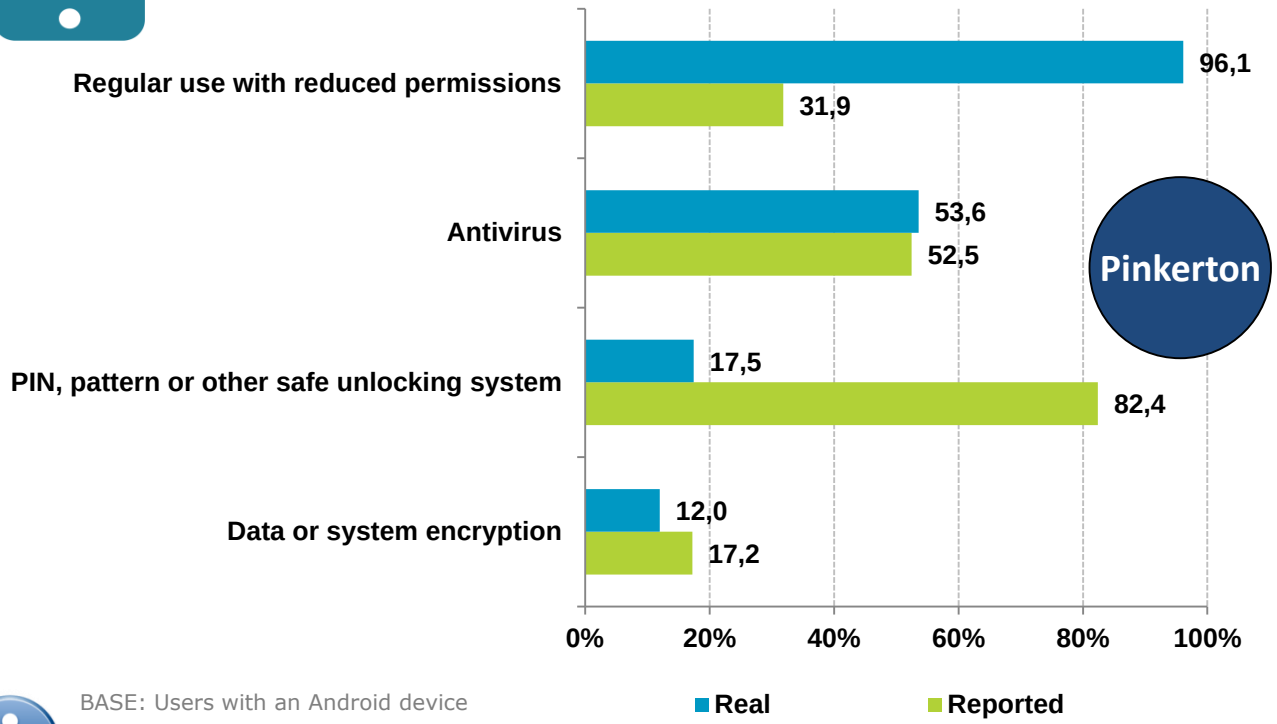


BASE: Users with an Android device

Use of security measures on Android devices

Reported vs real use of security measures

Real **regular use with reduced permissions** shows a growing tendency, reaching up to **96.1%** during the first semester of 2019, which accounts for a difference of **64.2 p.p.** compared to the reported data.



BASE: Users with an Android device

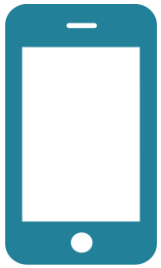
The use of a secure locking system using a **pattern, PIN, biometric systems**, etc., is a simple way to prevent **unauthorised or undesired access** to the mobile device and its content, **protecting the user's privacy.**

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.

✓ **Encrypting:** https://www.osi.es/es/actualidad/blog/2019/04/10/no-pierdas-nada-protege-la-informacion-de-tu-dispositivo

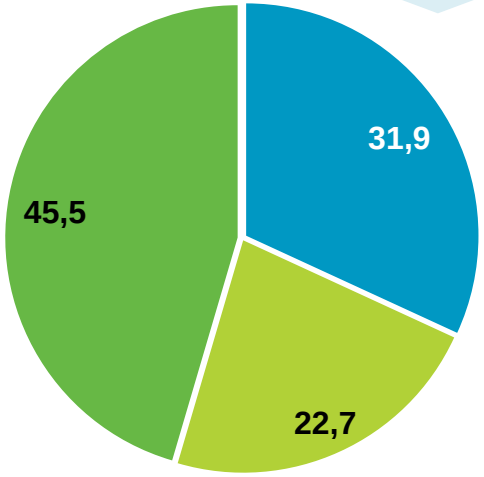
Use of security measures on Android devices

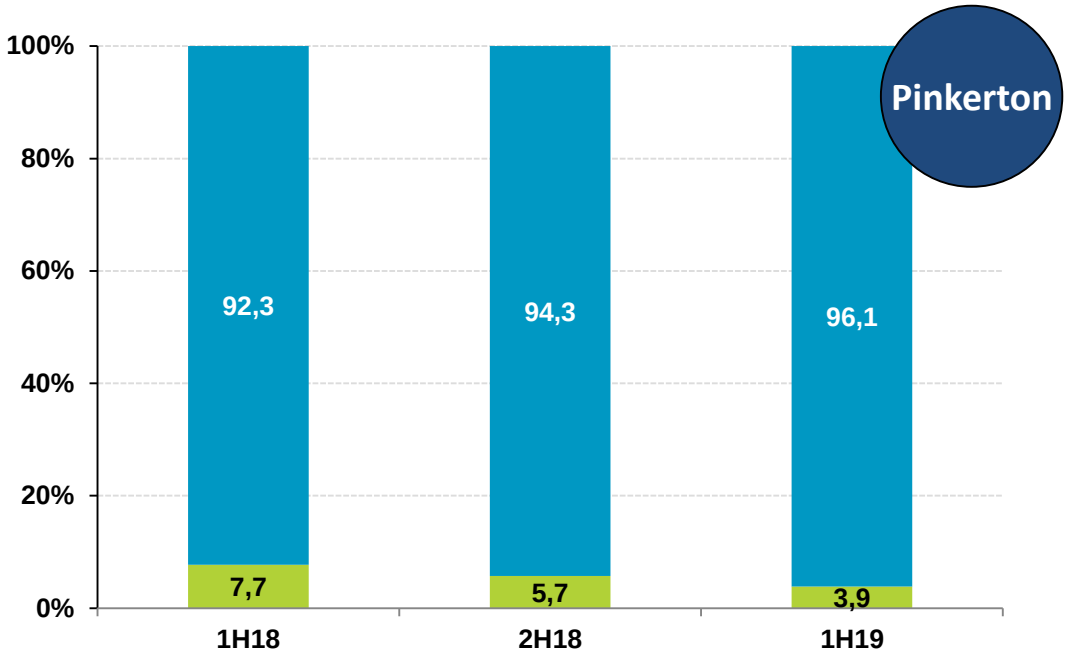
Administrator permissions



Real data

Reported data (1H19)





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

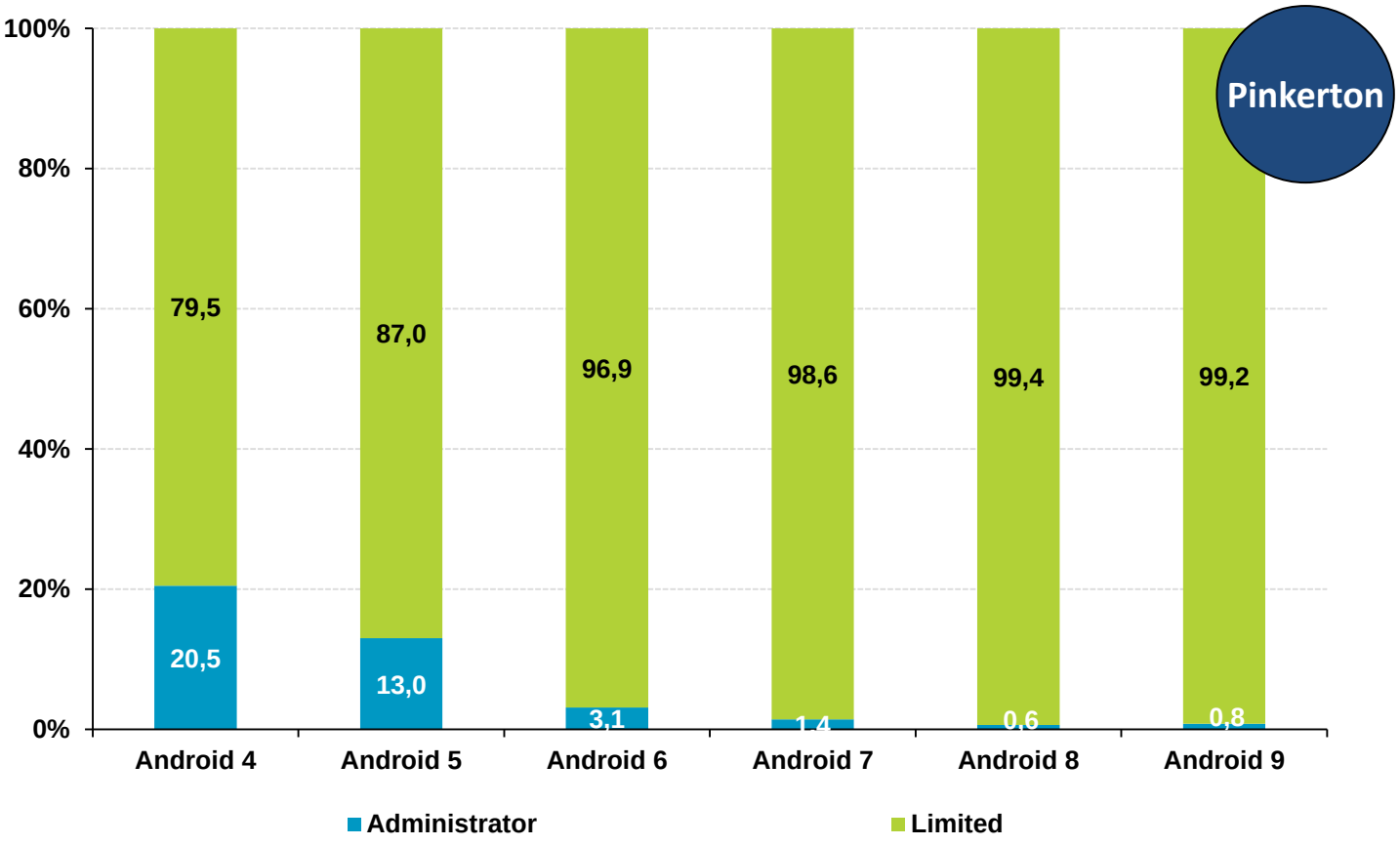
BASE: Users with an Android device

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.

✓ **Rooting:** https://www.osi.es/es/actualidad/blog/2019/04/24/conocias-el-termino-jailbreaking-o-rooting

Use of security measures on Android devices

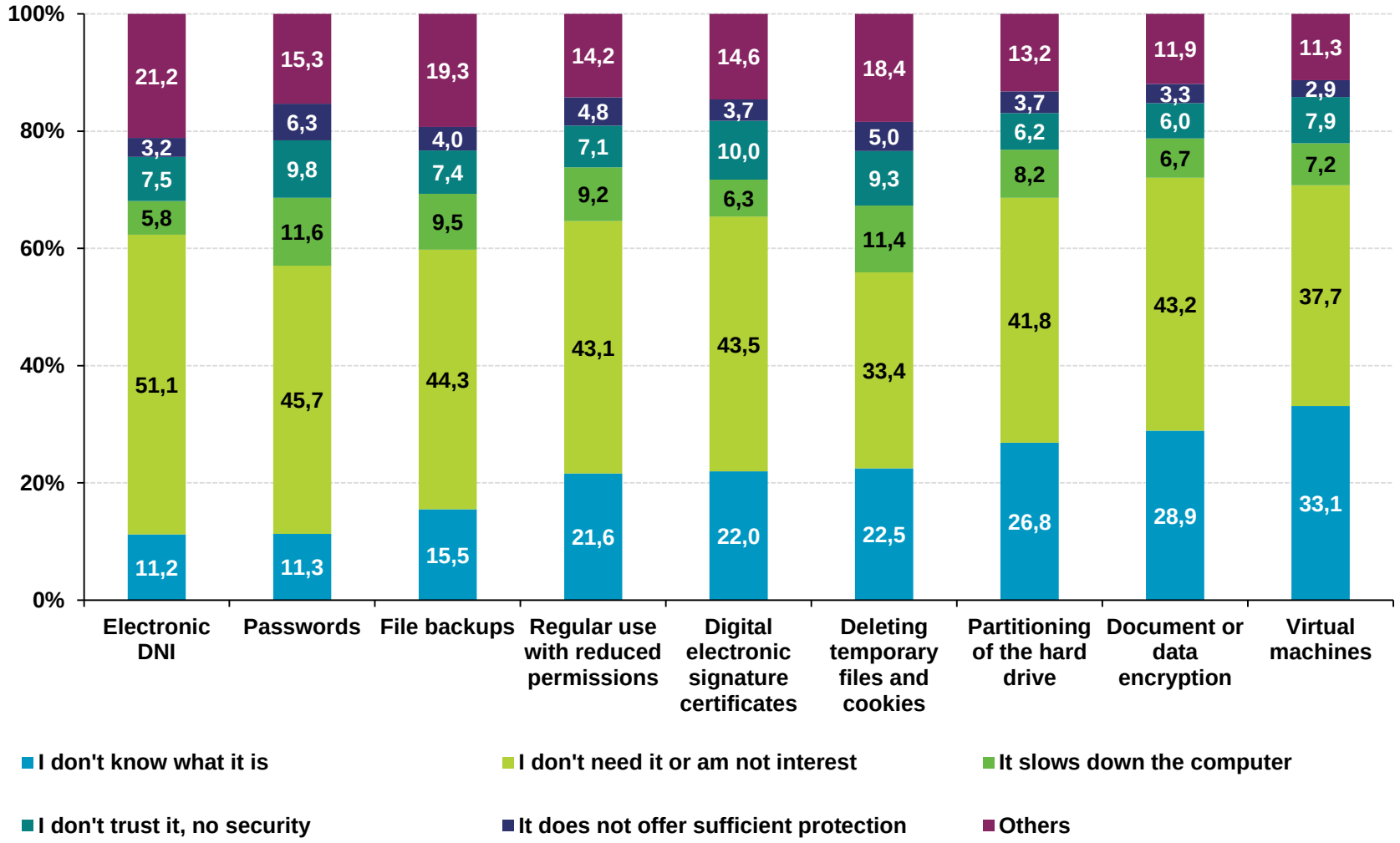
Devices with older versions of Android still tend to be '*rooted*', which is probably related to the necessity of escalating privileges in order to keep the device updated once the software manufacturer stops providing support for a given version.



BASE: Users with an Android device

Reasons for not using security measures

The main reasons given for not using certain security measures are still that there is **no need or interest** and **a lack of knowledge about the measure**.

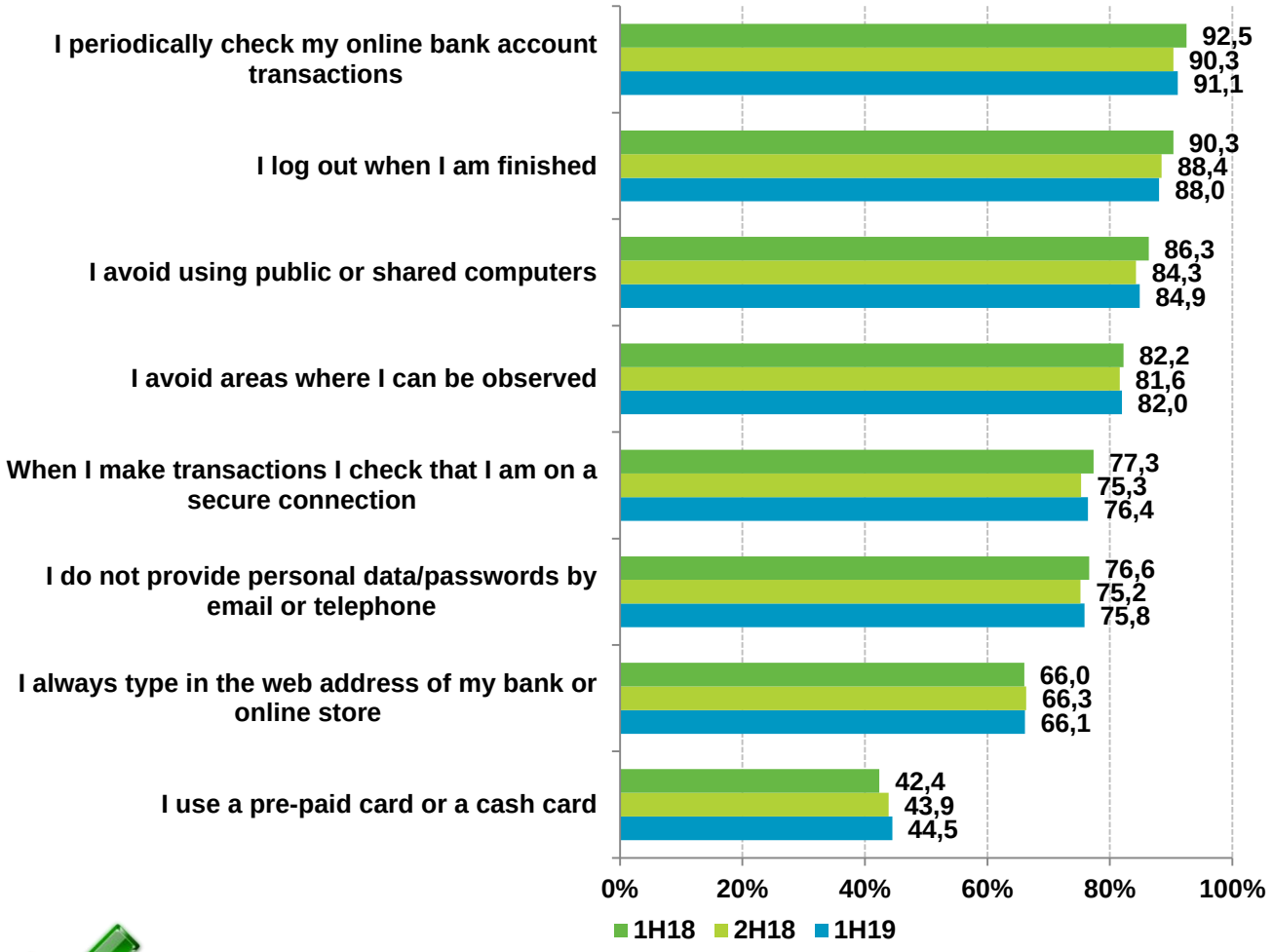


BASE: Users who do not use any of the security measures

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**
7. **Knowingly adopting risky behaviours**

Online banking and e-Commerce



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

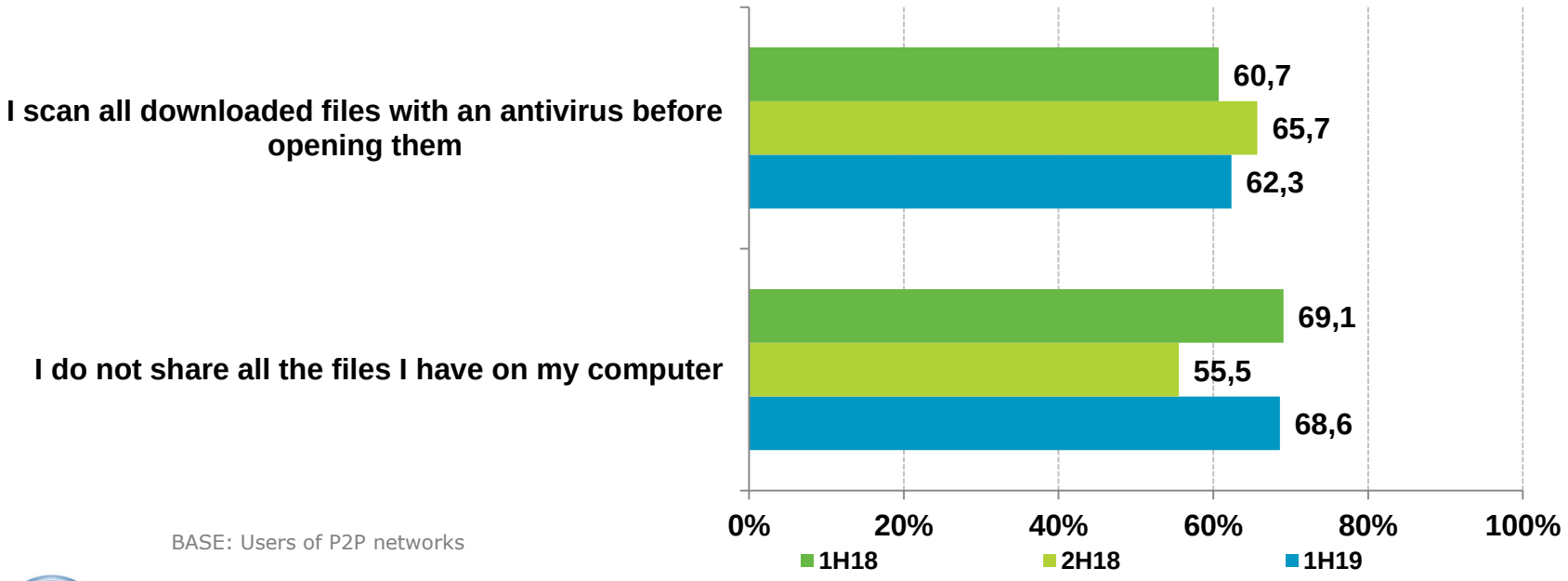
Banks normally have a warning to alert their customers of these practices. The purpose is to avoid online and/or telephone fraud seeking to obtain user credentials and access their accounts.

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

There is an increase in the number of users who limit the amount of **files shared on P2P networks** (**68.6%**), thus reaching similar values to those obtained a year ago.



BASE: Users of P2P networks

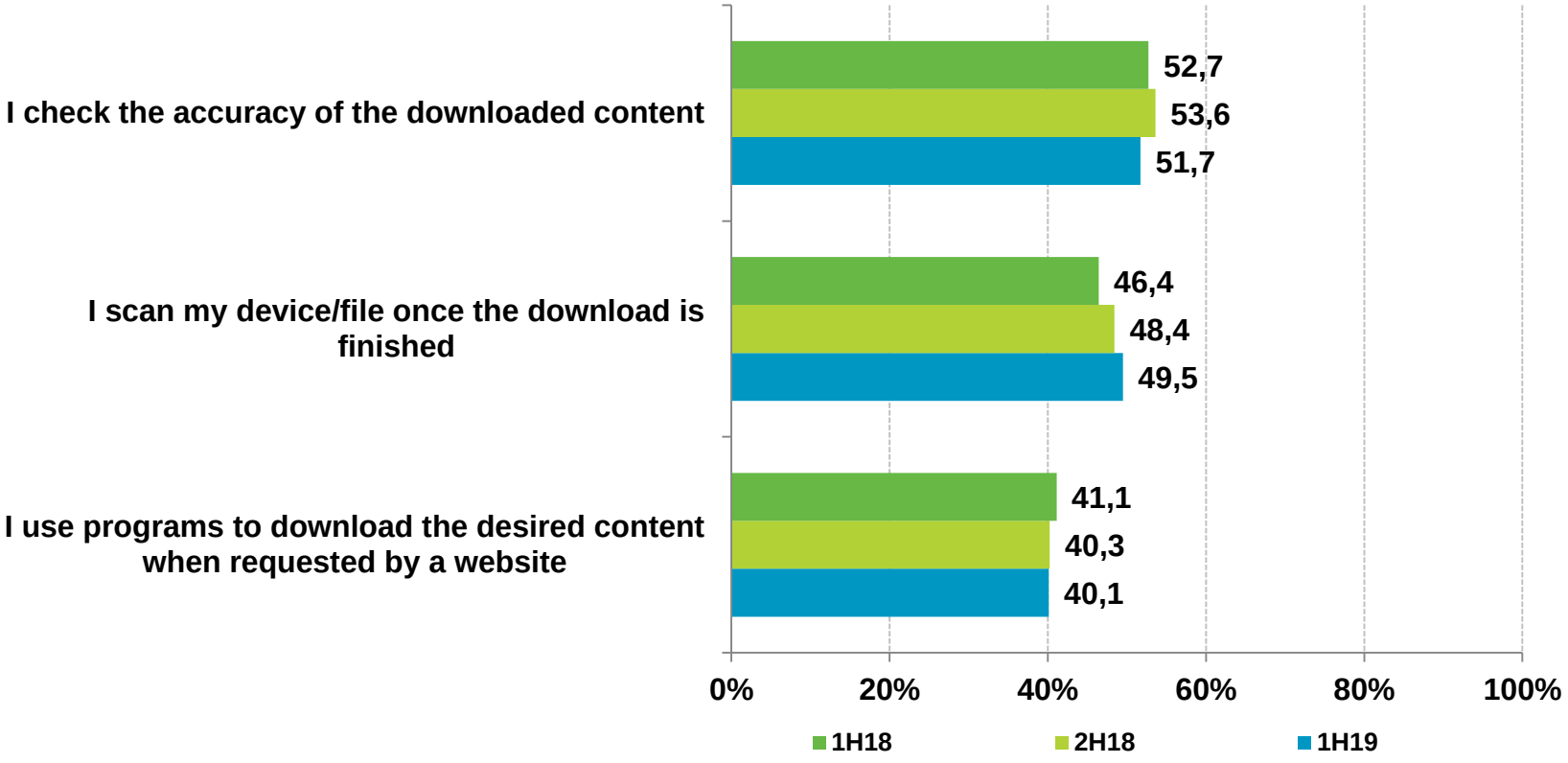
Internet downloads are a source of infection widely used by malware developers. Using malicious codes camouflaged in files that catch the interest of the user (for example the latest software, films, music, etc.) they infect the computer of incautious users.

✓ **Downloads:** https://www.osi.es/es/webs-de-descarga

Direct download

Habits regarding prevention related to **direct downloads** of files maintain around 50%.

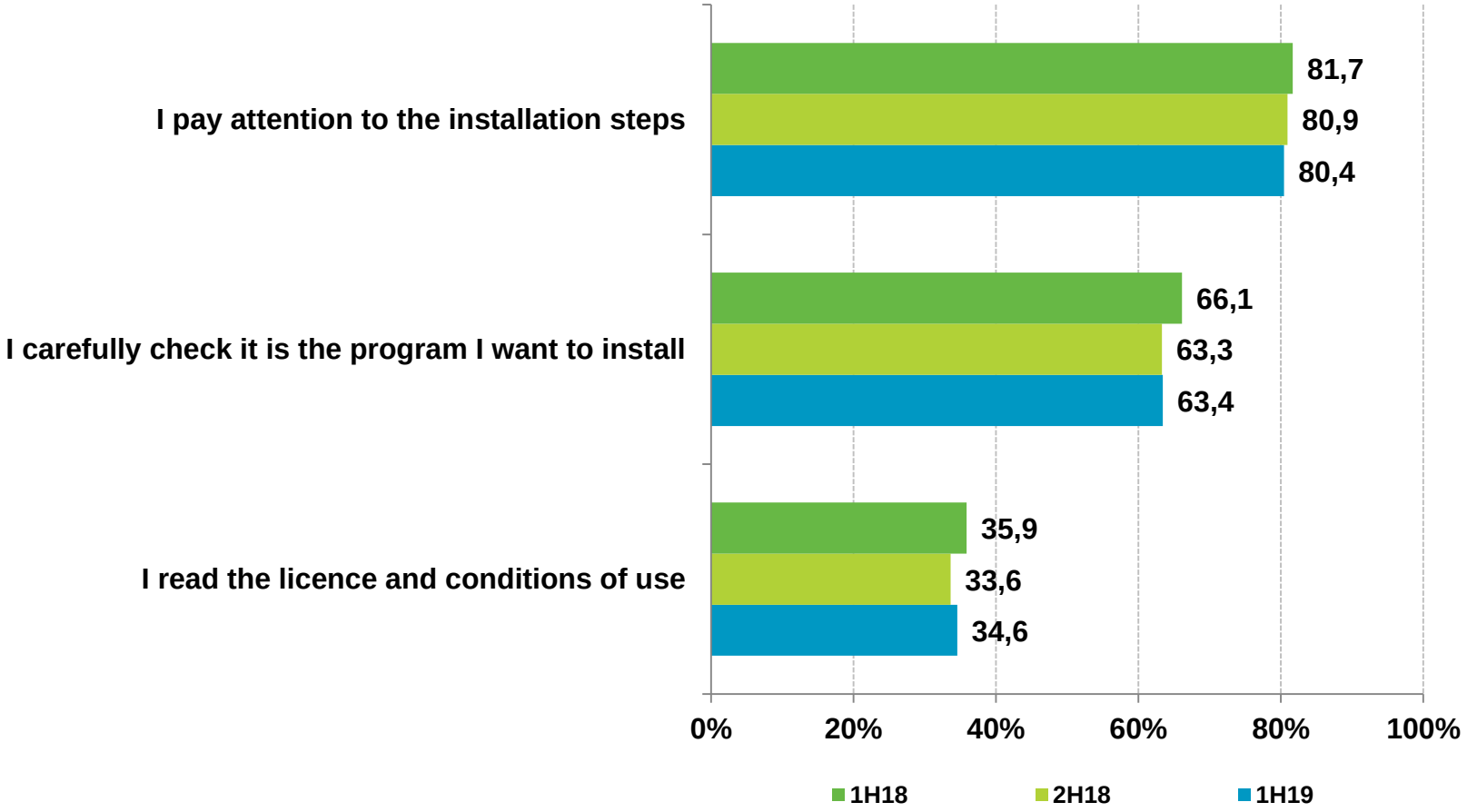
In addition, 2 out of 5 users (**40.1%**) install programs when requested by the website in order to download the file(s).



BASE: All users

Installing downloaded software

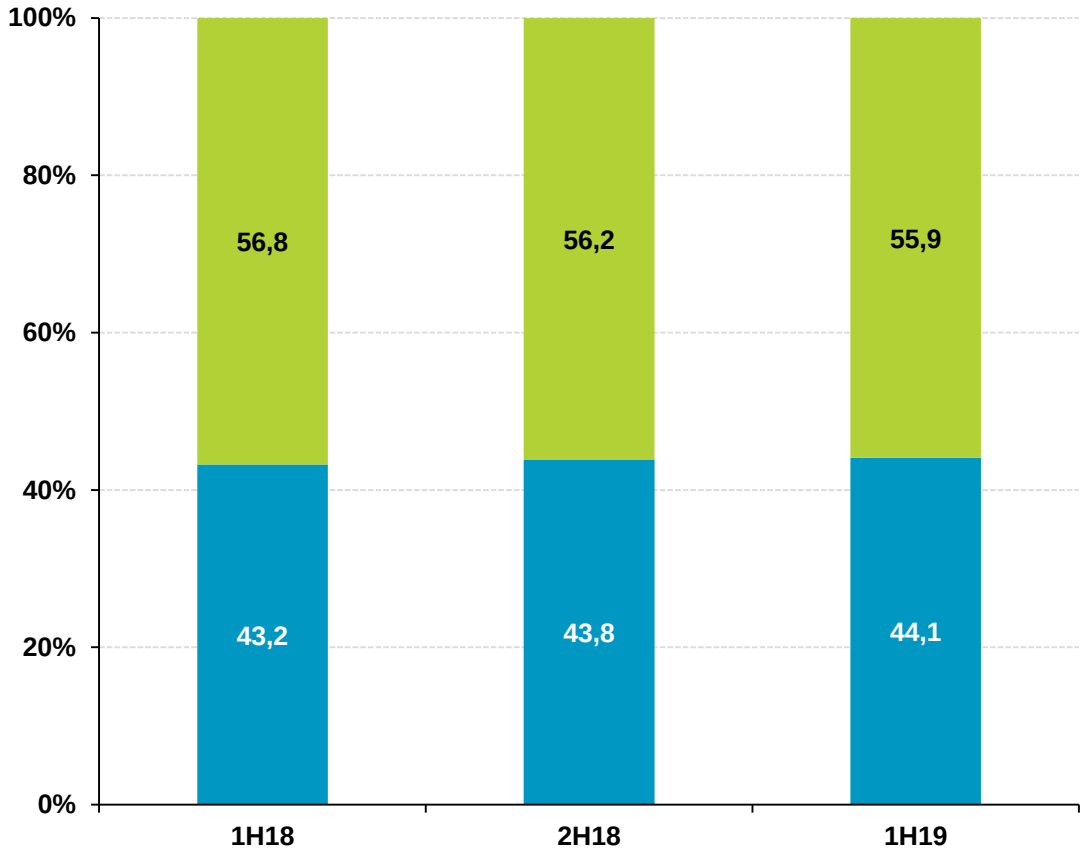
The number of users who **read the licence and conditions of use of the downloaded software** remains below **35%**, although over **80%** declares **paying attention to the installation steps**.



BASE: PC Users

Registering with Internet services

The volumen of Spanish Internet users who claim they **do not read the terms and conditions and legal information before accepting them** is still over half the Spanish population (**55.9%**).



%
individuals

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

Yes

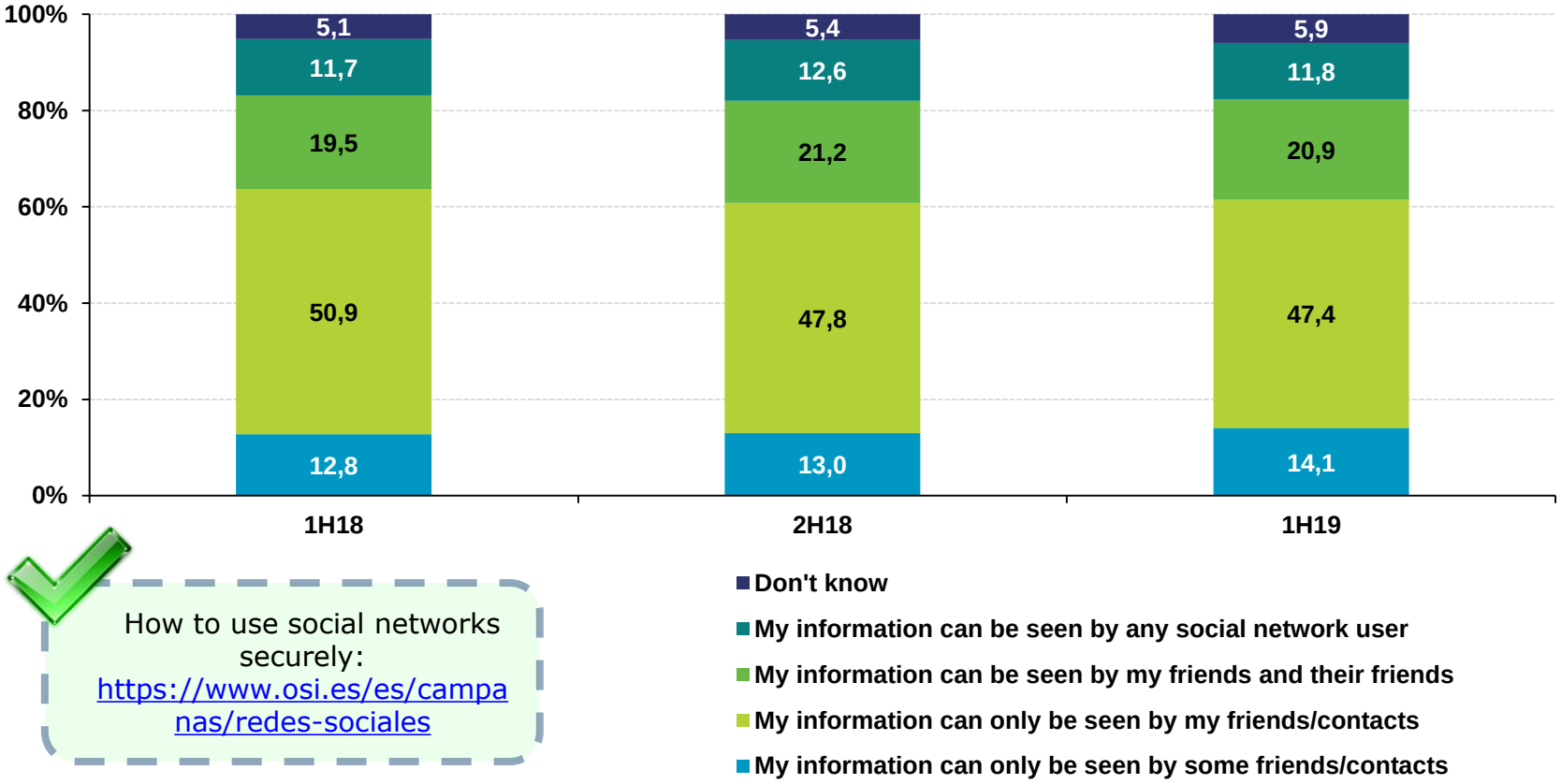
No

BASE: All users

Social networks

A significant percentage of social networks users **keep their posts on social media private** so just friends have access to their data (**61.5%**) (14.1% + 47.4%).

A reduced amount of users claim they **do not know their social network profile privacy levels** (**5.9%**), and an additional **11.8%** of users consulted **expose the data** published on their profile to **third and/or unknown parties**.



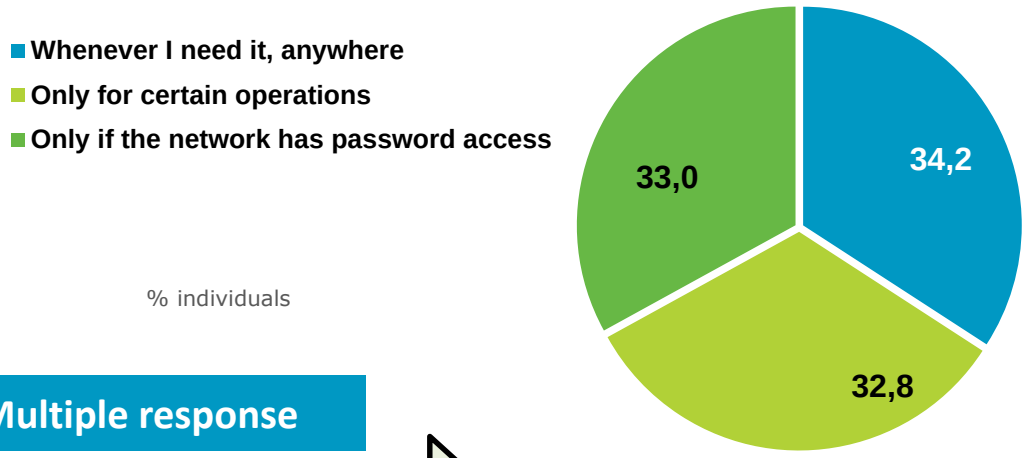
How to use social networks securely: https://www.osi.es/es/campanas/redes-sociales

BASE: Social network users

% individuals

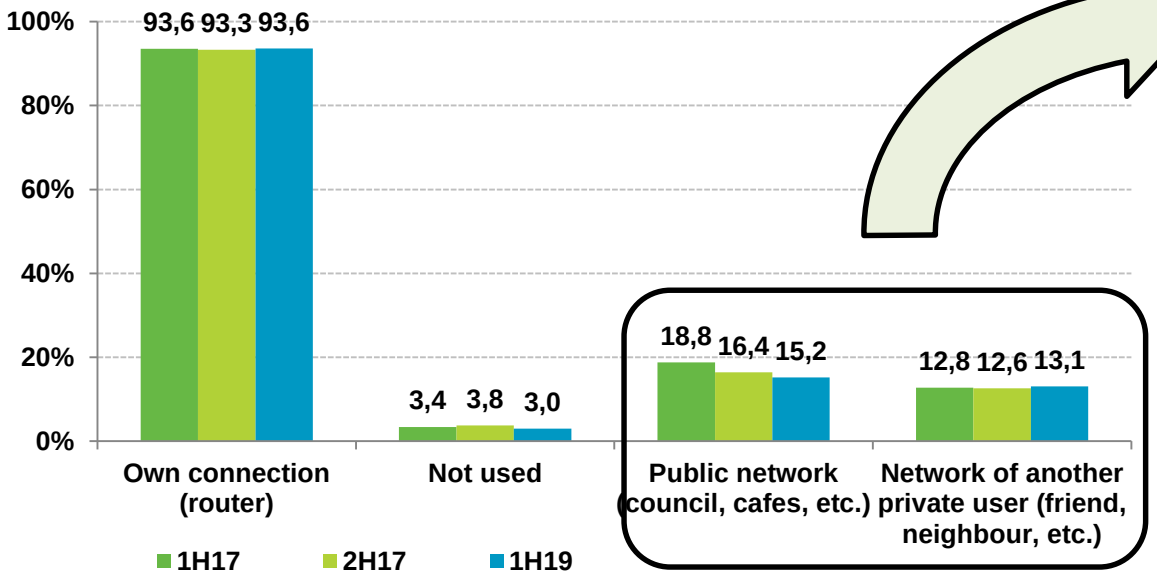
Habits of wireless Wi-Fi network use

Internet access point using wireless Wi-Fi networks



% individuals

Multiple response



BASE: All users

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

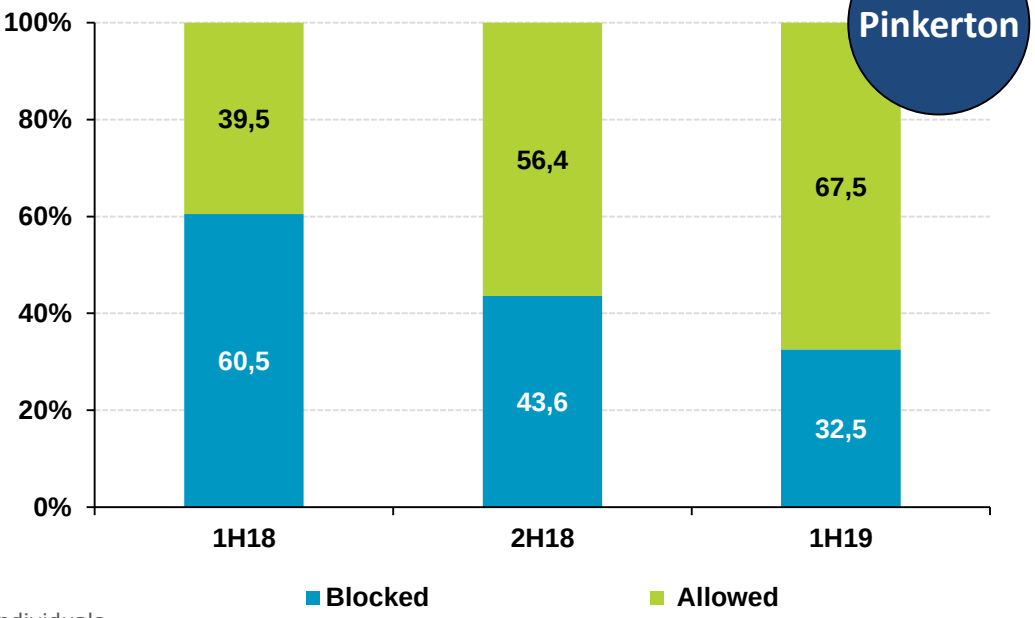
The volume of users who connect to public Wi-Fi networks continues to decrease **(-1.2 p.p.)**. But among these users there is still a high percentage that do not pay attention to the level of security of the network and **connect to this kind of networks whenever and anywhere they need it** (**34.2%**).

How to connect to public Wi-Fi networks securely:
https://www.osi.es/es/actualidad/blog/2019/05/02/conexion-gratis-la-vista-conecto-mi-movil

Habits of Android device use

The use of applications from doubtful sources can pose **security problems** and the installation of any type of **malware** on a mobile device.

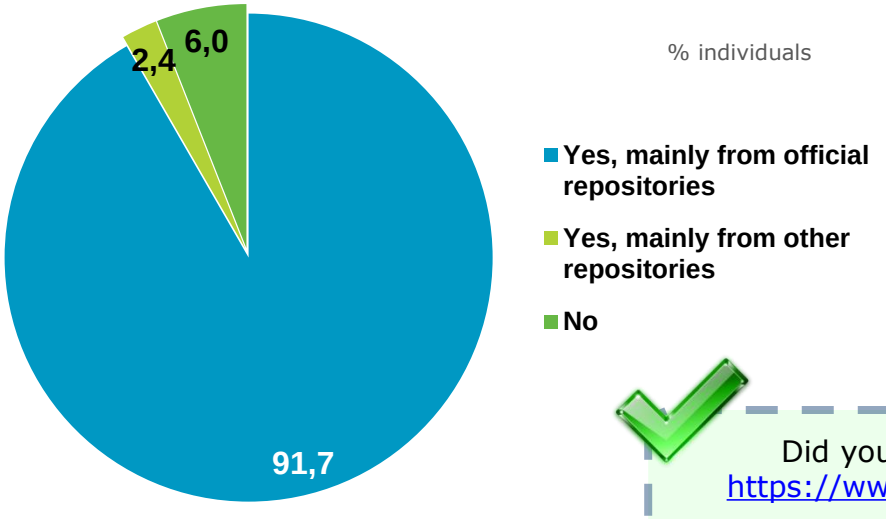
Downloads from unknown sources



% individuals

The number of users **allowing the installation of software from unknown sources** continues to grow (**+11.1 p.p.**) according to the data collected by Pinkerton. However, in contrast to this, most users (**91.7%**) report that they **mainly install applications from official repositories**.

Downloading programs or applications on a mobile

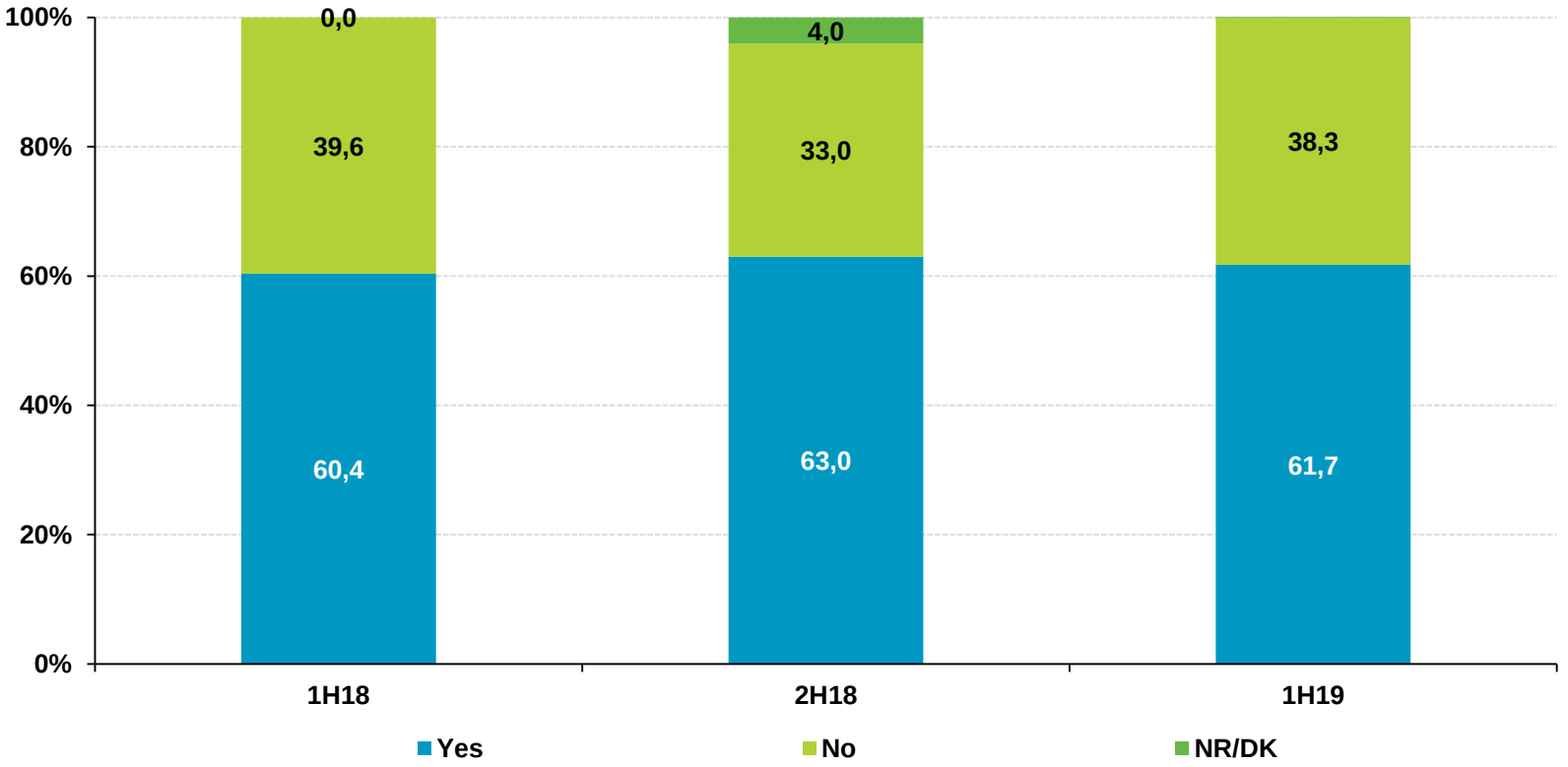


Did you know that this APP can steal your information?
https://www.osi.es/es/campanas/dispositivos-moviles/instale-app-no-fiable

BASE: Users with an Android device

Habits of Android device use

Checking permits when installing an application



BASE: Users with an Android device and who download applications

Cheking aplications' permits: https://www.osi.es/es/campanas/dispositivos-moviles/acepto-no-acepto

Knowingly adopting risky behaviours

Users **knowingly adopting risky behaviours** decreased **-2.4 p.p.** compared to previous studies, reaching lower values than those observed a year ago.

BASE: All users

Security Incidents

1. Types of malware
2. Security incidents
3. Malware incidents
4. Type of malware detected
5. Danger of malicious code and computer risks
6. Malware vs operating system
7. Malware vs system updates
8. Malware vs Java on PC
9. Malware vs origin of APPs on Android
10. Security incidents with wireless Wi-Fi networks

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. Commonly known as viruses, in reality 'malware' is a much broader term that encompasses other types of malicious progams.

Trojans or Trojan horses. Bankers, backdoors, keyloggers, dialers, 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* o *scareware*, *jokes.*

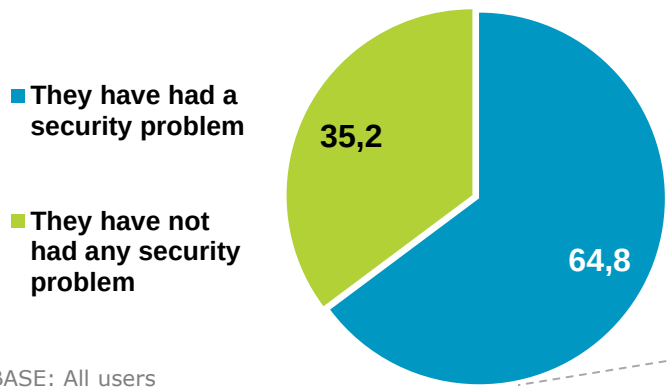
More information: https://www.incibe.es/glossary/empresas/diccionario/

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 of malicious programs.

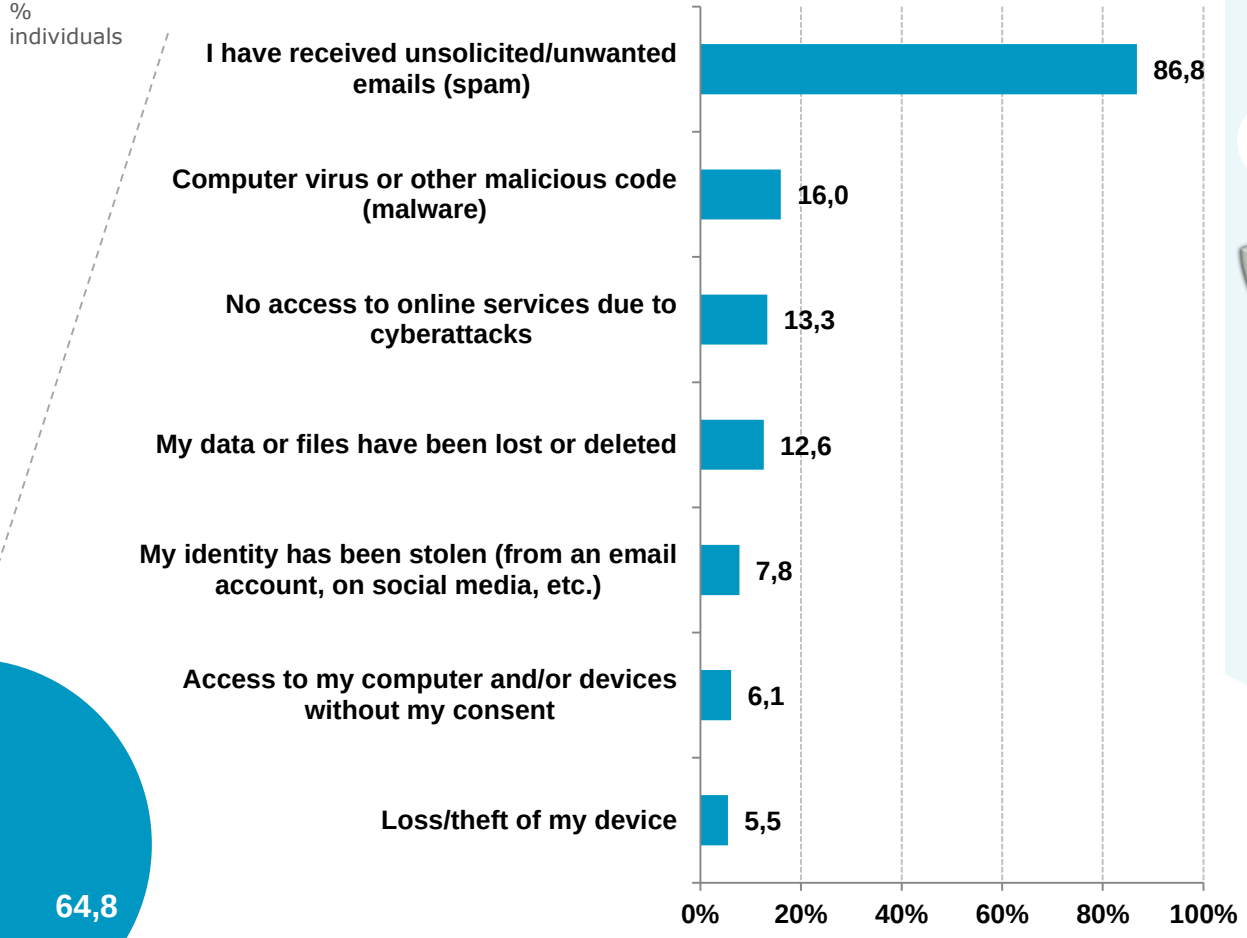
Affected:



BASE: All users

Incidents suffered:

Multiple response



BASE: Users who have experienced a security incident

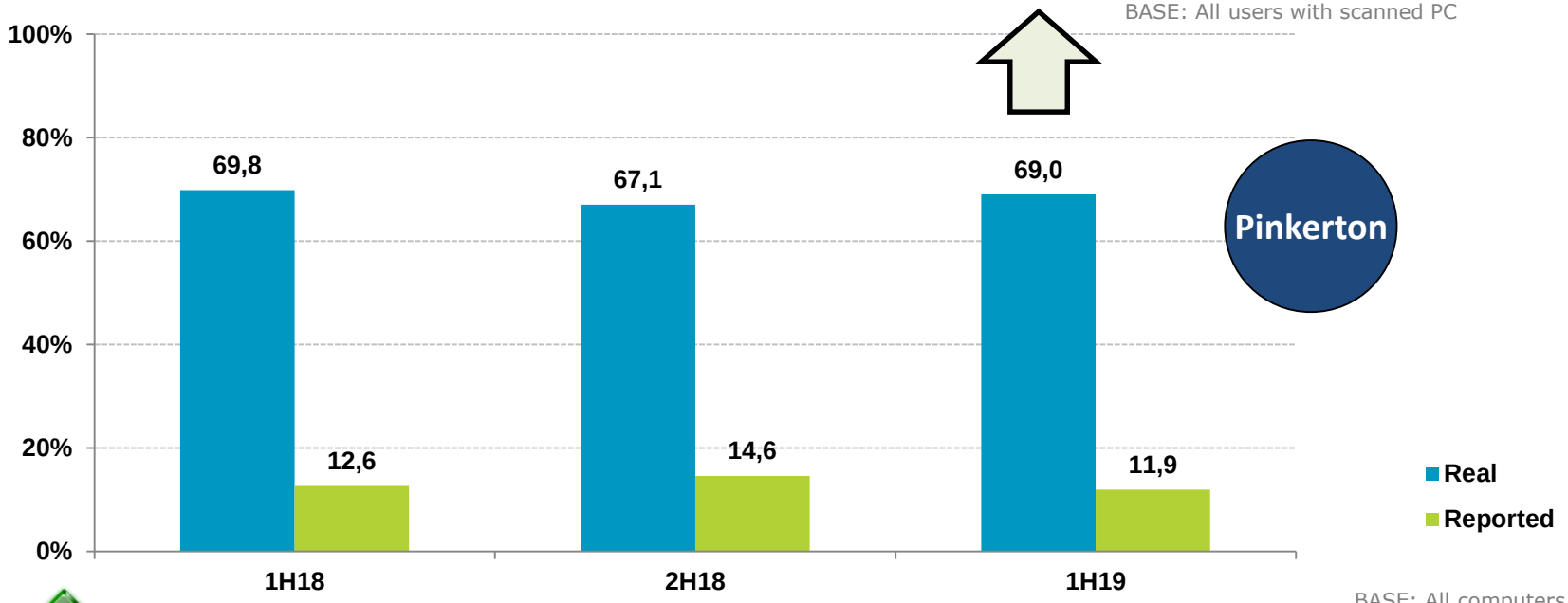
Malware incidents

Household computer

60.9% of the computers analysed are **infected by some form of malware even though their users think they are not**.

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

BASE: All users with scanned PC



BASE: All computers

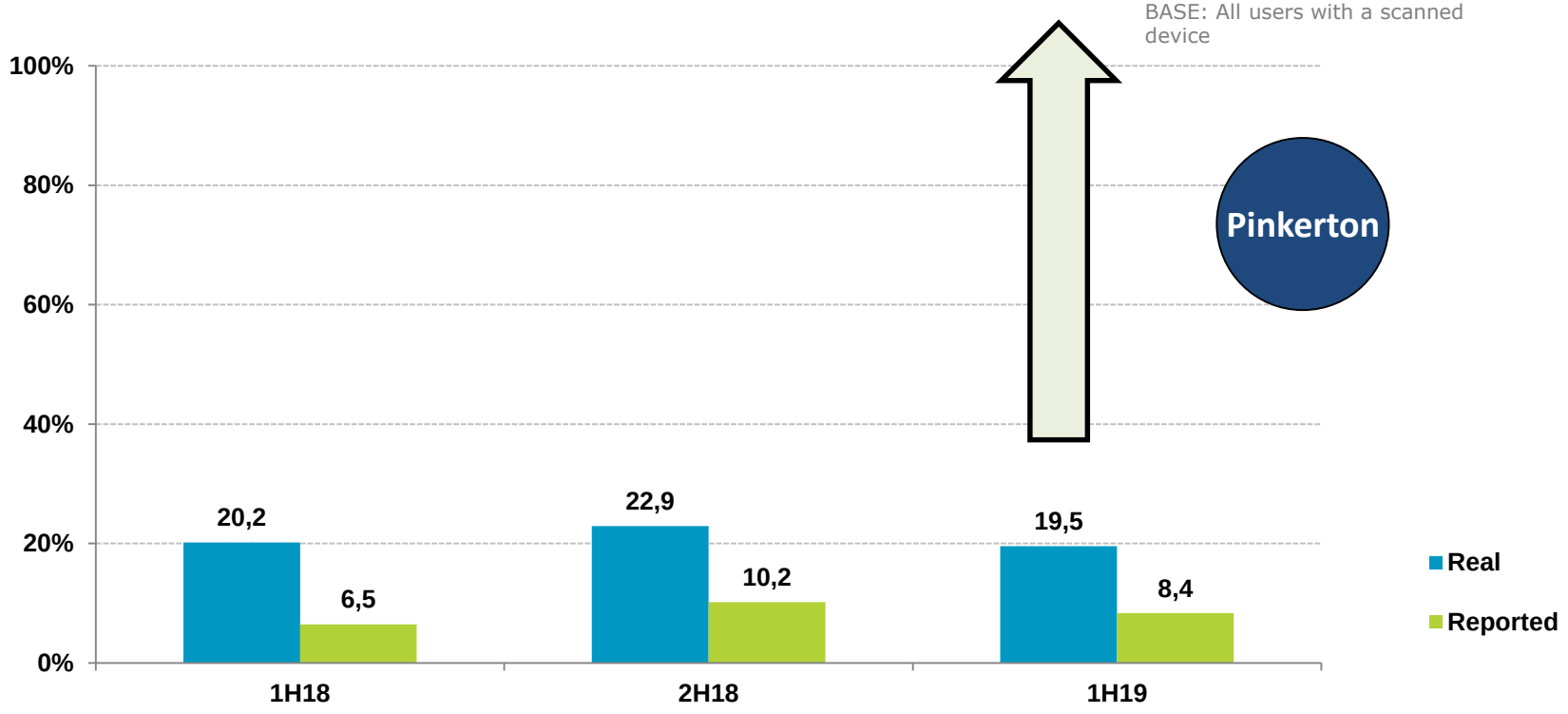
Learn the steps you need to take to remove viruses from your computer:
https://www.osi.es/es/desinfecta-tu-ordenador

Android Devices

Although there is a lower level of malware infection on Android devices (**19.5%**), still **18.4%** of users with infected devices did not notice the presence of malware.

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

BASE: All users with a scanned device



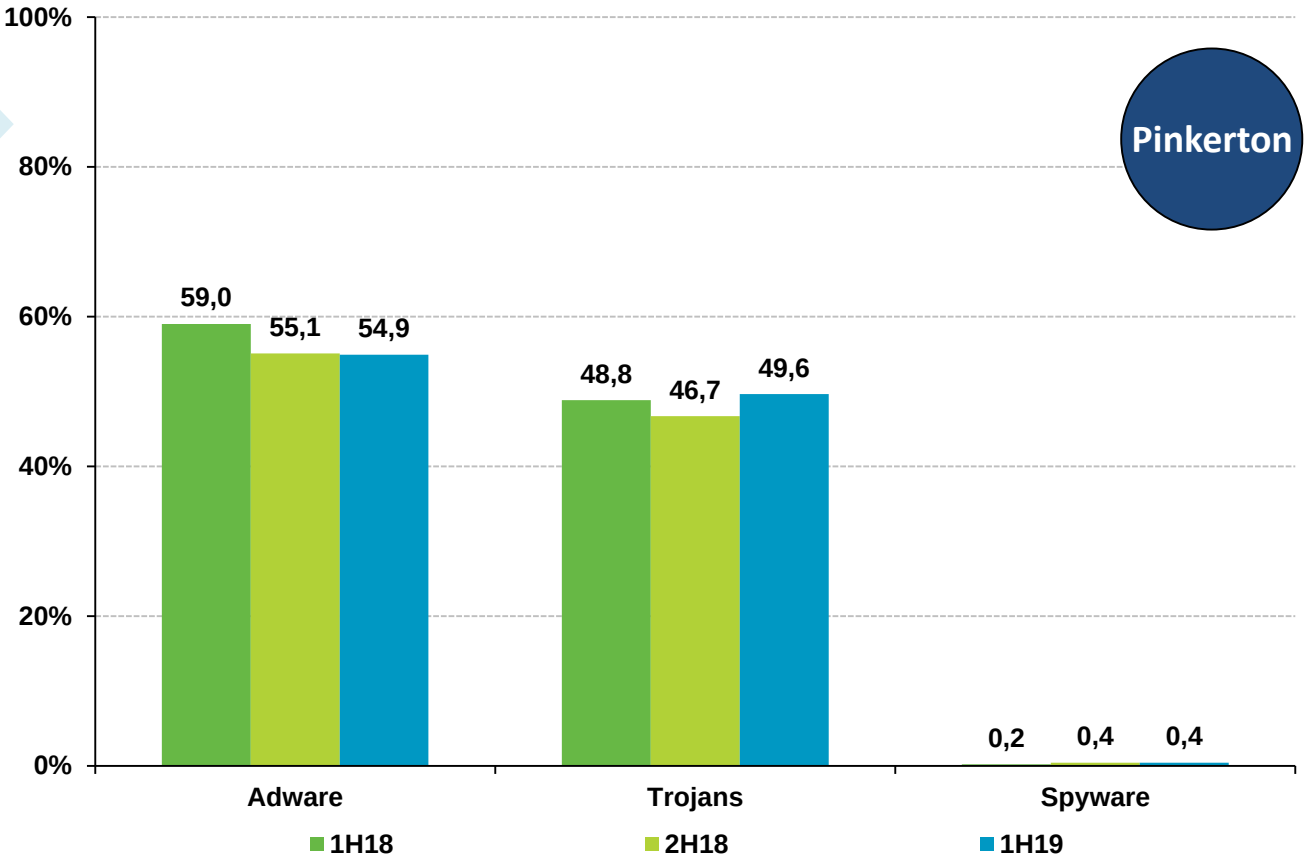
BASE: All Android devices

Type of malware detected on PC

Household computer

The presence of **Adware** remains stable (**54.9%**) on Spanish computers. Meanwhile, **Trojans** show a rebound (**2.9 p.p.**).

Computers hosting malware according to type



Pinkerton

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

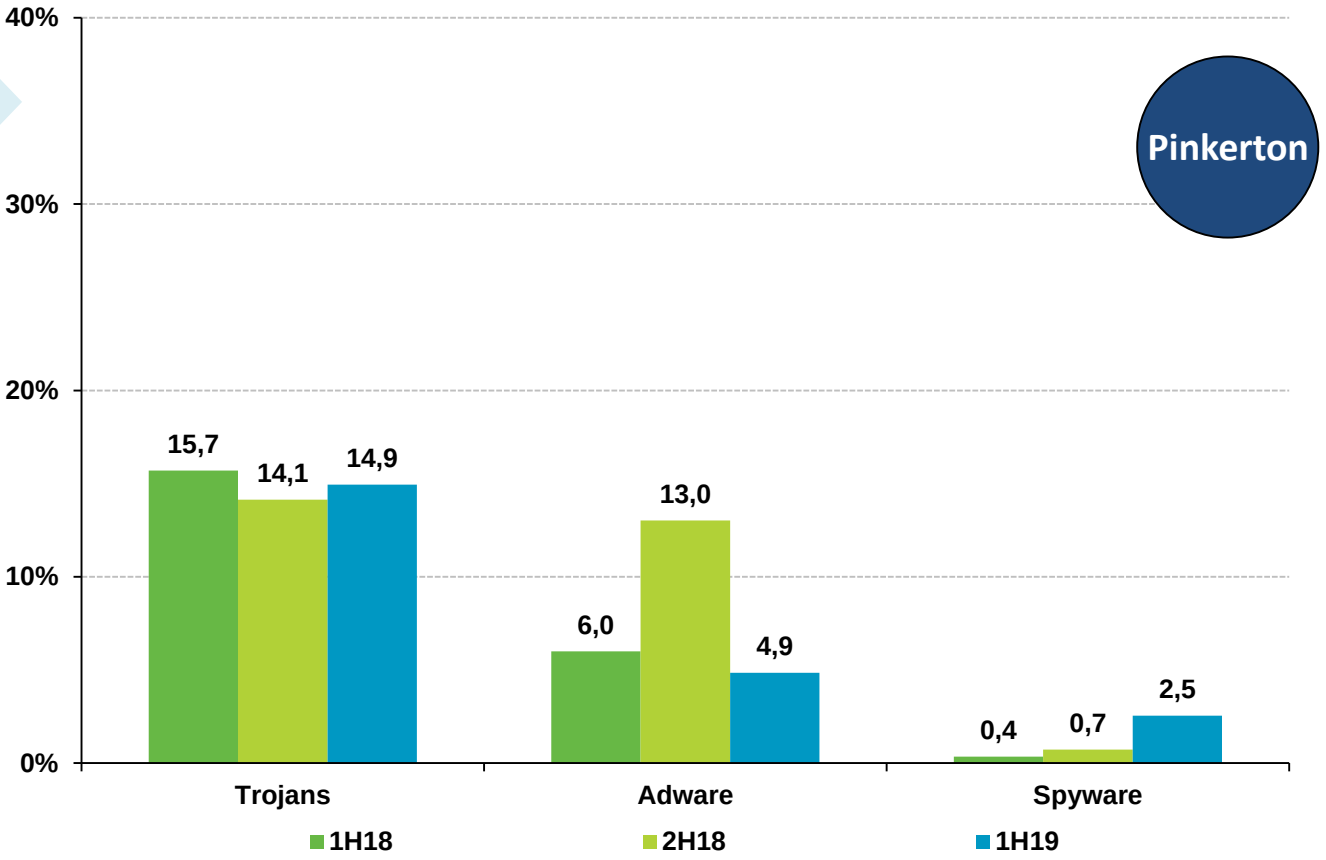
BASE: All computers

Type of malware detected on Android

Android Devices

Trojan infections on Android reach up to 15% again, and, on the other hand, **Adware** experiences a fall of **8.1 p.p.**

Devices hosting malware according to type



BASE: All Android devices

Danger of malicious code and computer risks

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

They are classified according to the following criteria:

High risk: this category includes specimens that potenttially: 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.

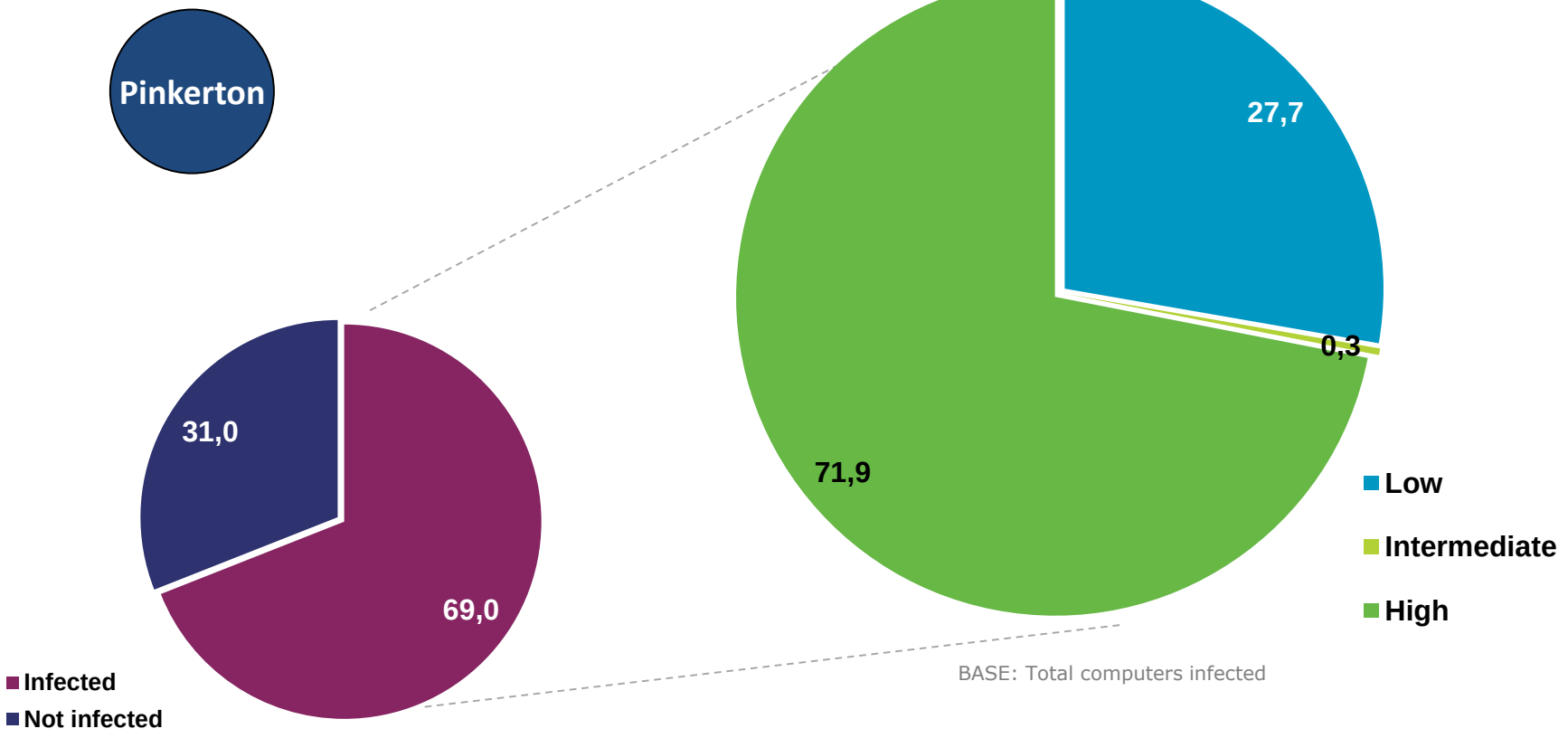
Medium risk: this includes examples that, although they have an undesired impact on the system: do not noticeably affect its performance; open undesired windows when browsing; embed advertising on legitimate websites that do not contain advertising originally; or facilitate the capture of the victim's 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 médium risk malware will always be included in the group of high risk computers.

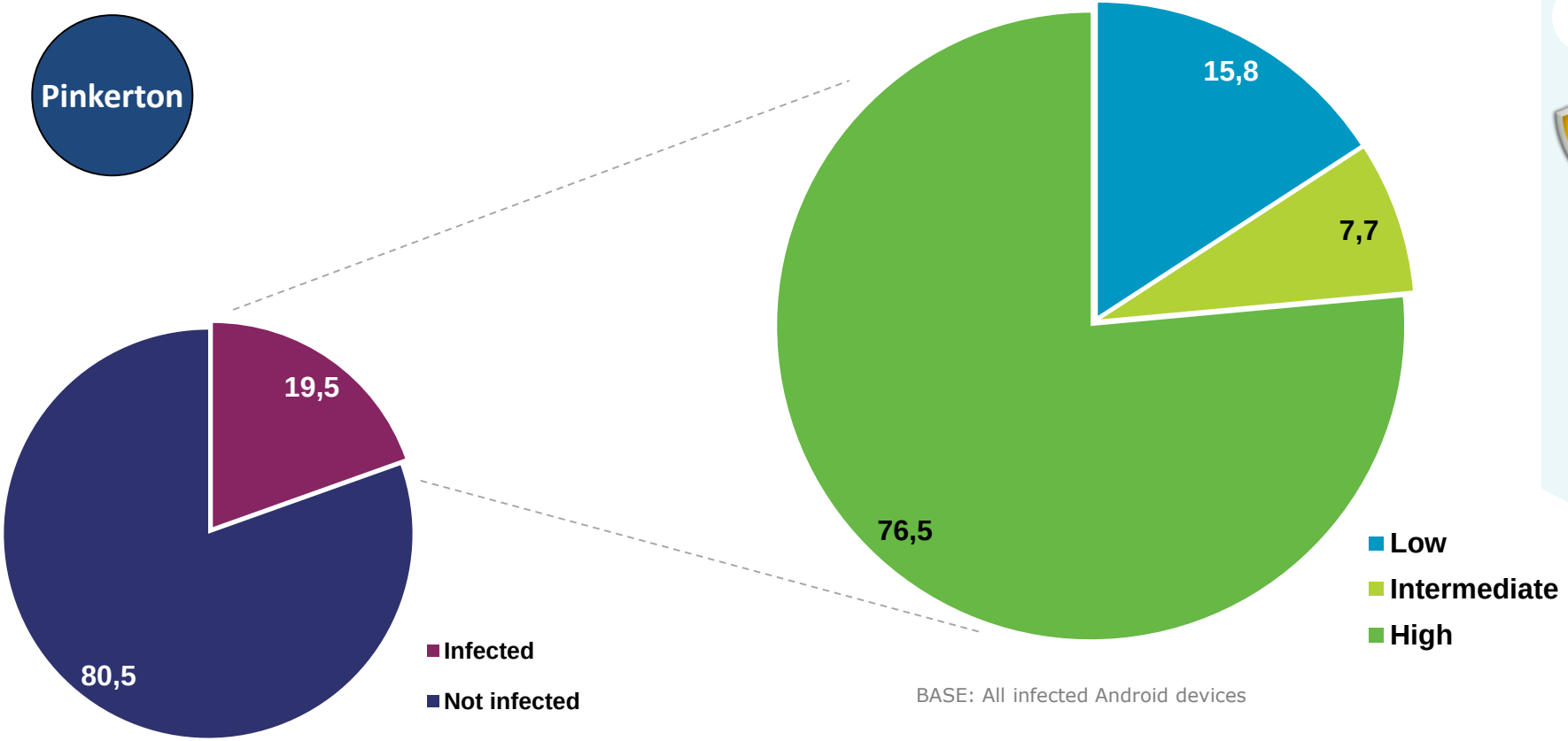
Household computer

The number of household computers analysed by Pinkerton that are **infected by some type of malware** is still high (**69%**), and, among these, **71.9%** are classified as **high risk**.



Android devices

The volume of Android users with infected devices is significantly lower than the volume of infected computers (**19.5%**), although the proportion of malware samples detected and classified as **high risk** is much higher (**76.5%**).

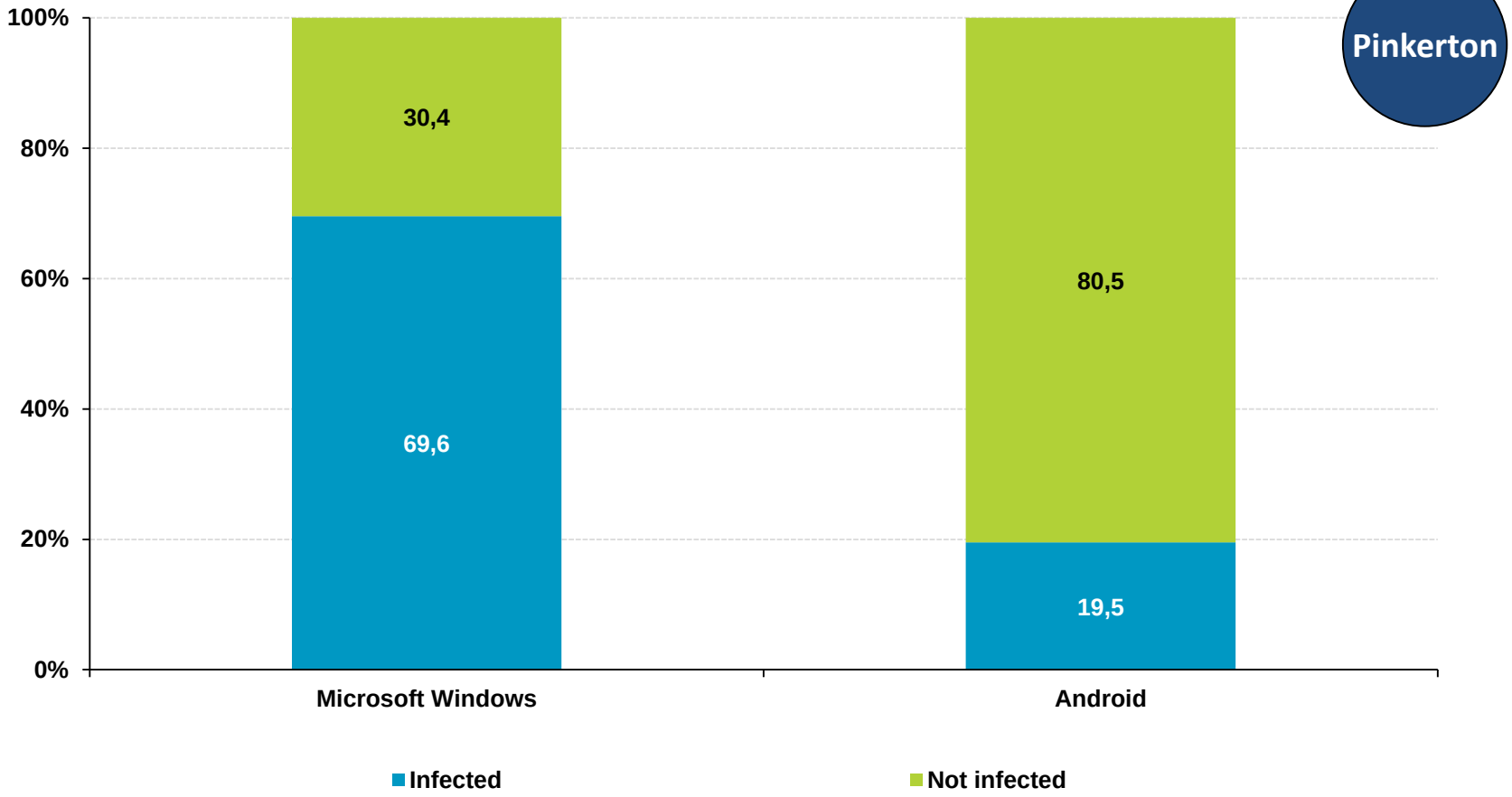


BASE: All Android devices

BASE: All infected Android devices

Malware vs operating system

The presence of malware continues to be significantly higher on household computers with a version of Microsoft Windows (**69.6%**) than on Android devices (**19.5%**).

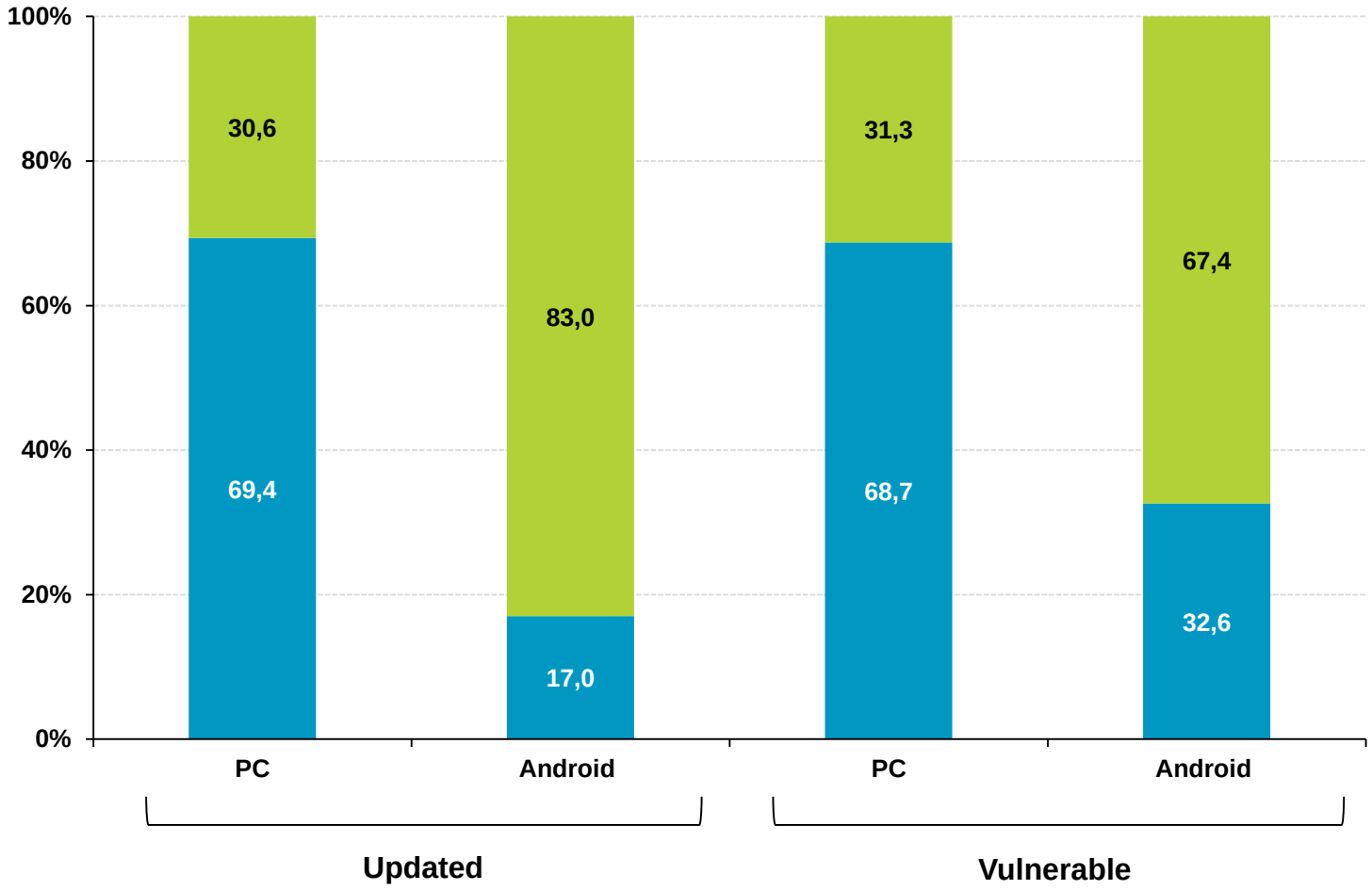


Pinkerton

4

BASE: All computers

Malware vs system updates



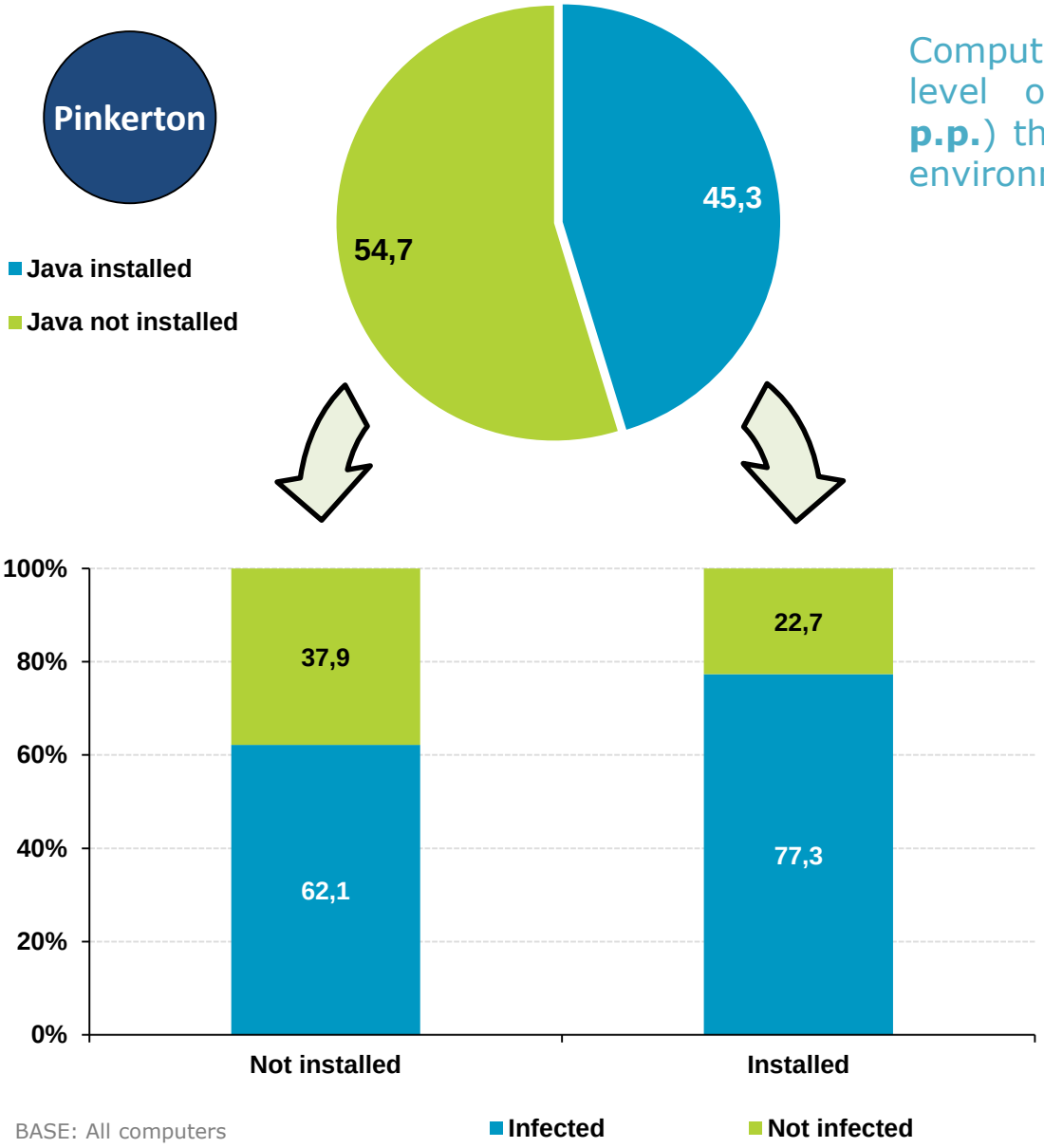
Pinkerton

4

Outdated Android devices are still affected more by malware (**+9.3 p.p.**), whereas in the case of computers, the numbers are almost equal.

BASE: All computers

Malware vs Java on PC



BASE: All computers

Computers with Java have a higher level of malware infection (**+15.2 p.p.**) than those that do not have this environment installed.

Java security alerts in July and October 2018:

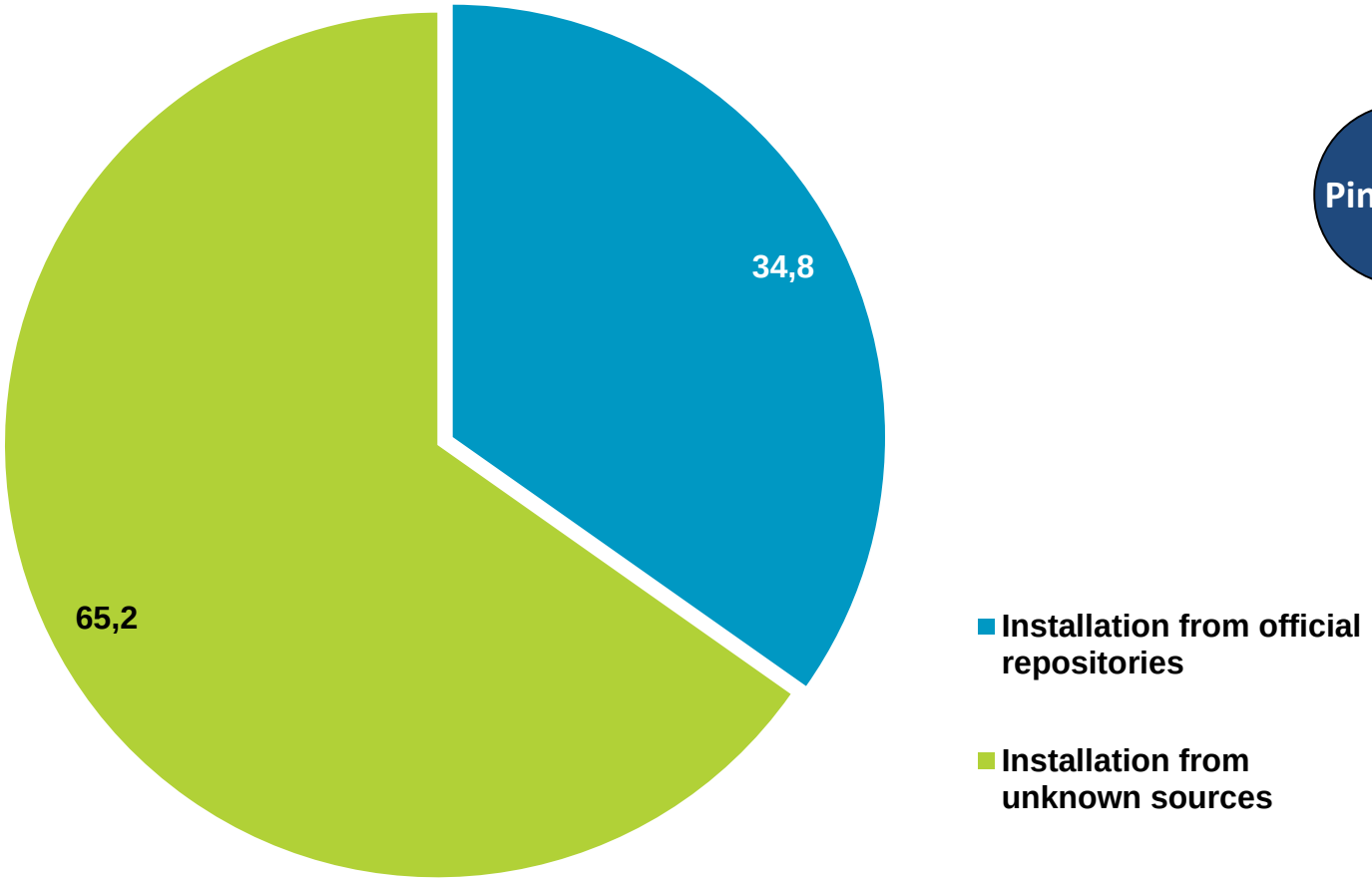
https://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html#AppendixJAVA

https://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.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.

Malware vs origin of APPs on Android

Although the option to **allow the installation of applications from unknown sources** is deactivated by deafult due to security reasons, almost two-thirds (**65.2%**) of the analysed devices that happen to be infected have this option active.



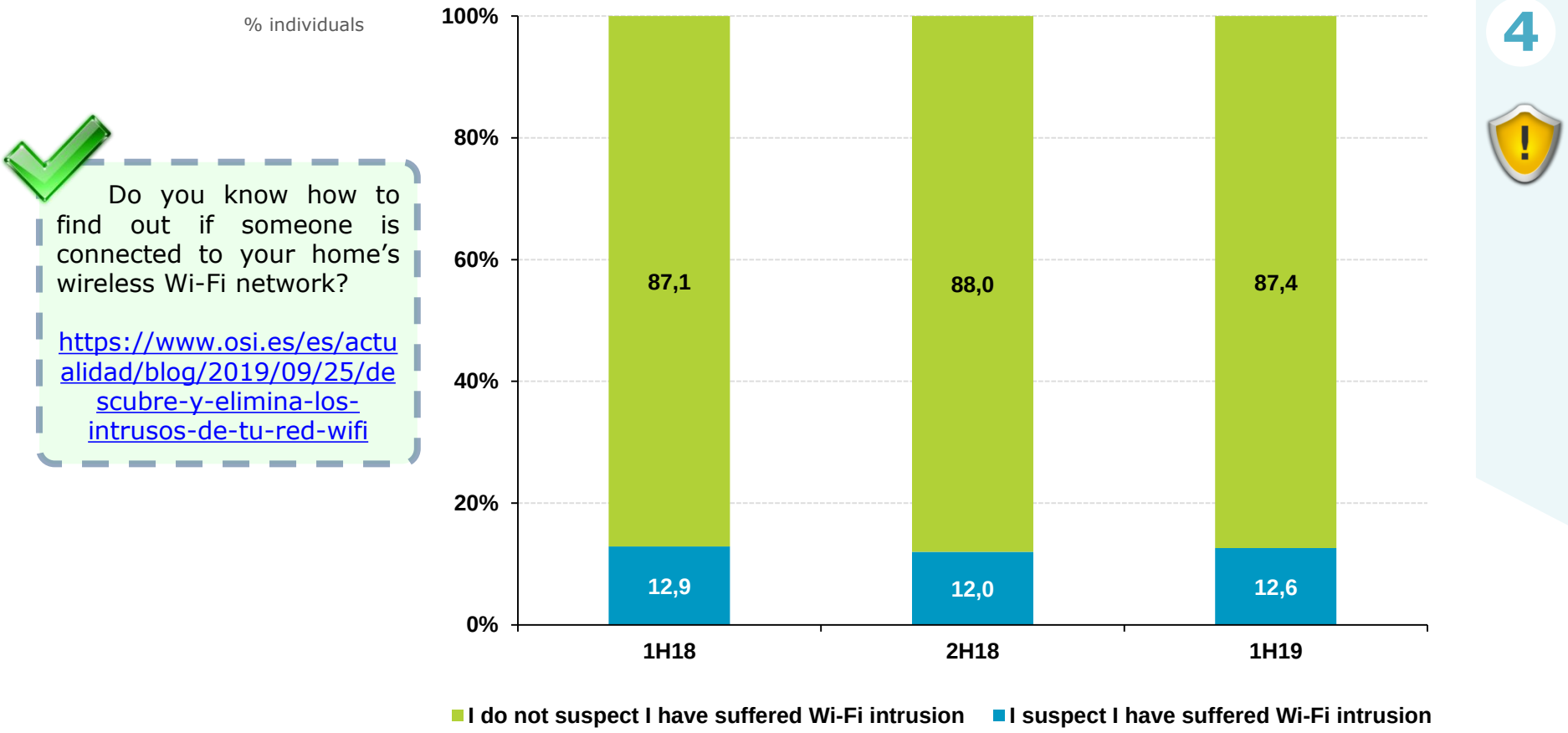
Pinkerton

4

BASE: All infected Android devices

Security incidents with wireless Wi-Fi networks

The percentage of users who ***suspect*** **that they have suffered intrusion into the wireless Wi-Fi network** of their home is still relatively low (**12.6%**).



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

https://www.osi.es/es/actualidad/blog/2019/09/25/descubre-y-elimina-los-intrusos-de-tu-red-wifi

BASE: Users with their own Wi-Fi connection

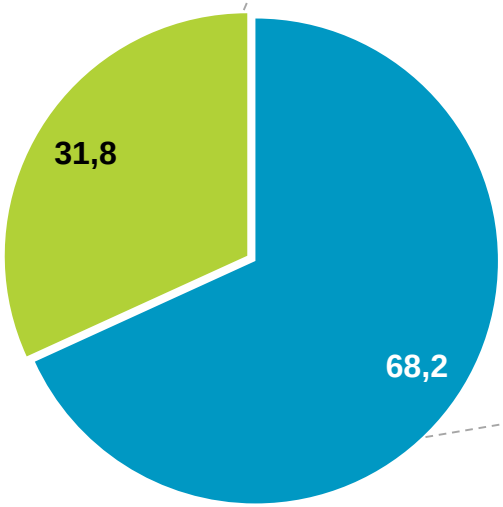
Consequences of security incidents and user reactions

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:

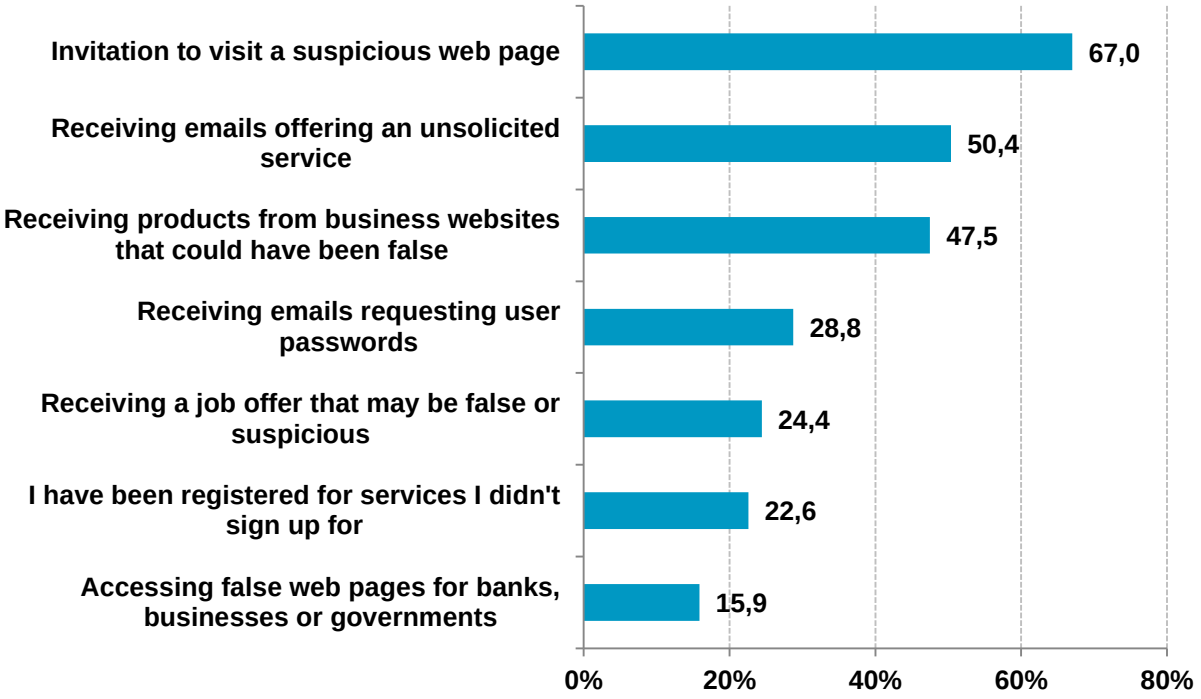


BASE: All users

Manifestation of the online fraud attempt:

Multiple response

% individuals



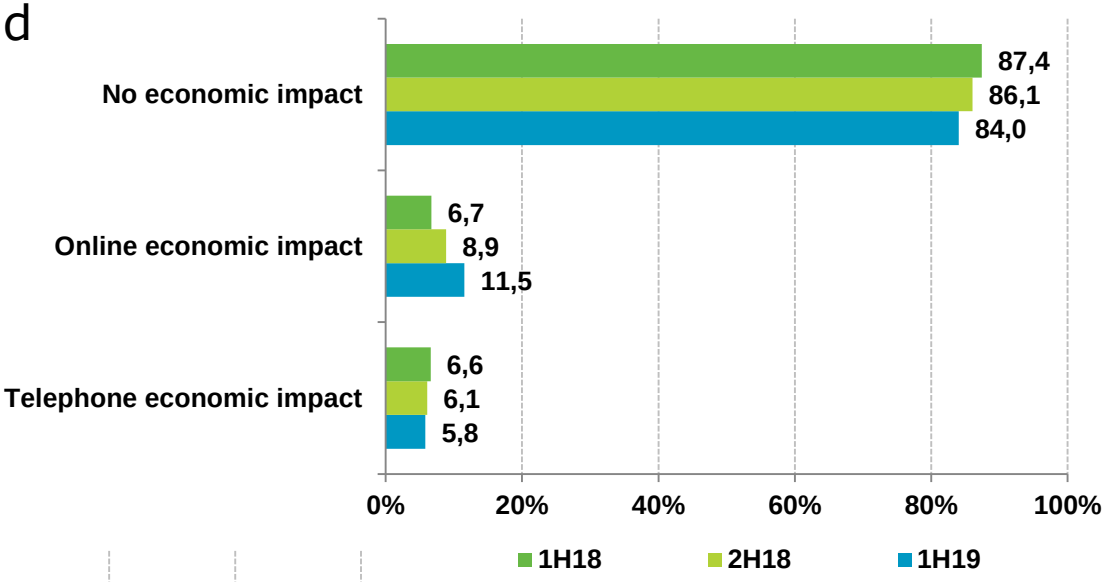
BASE: Users who have experienced attempted fraud

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

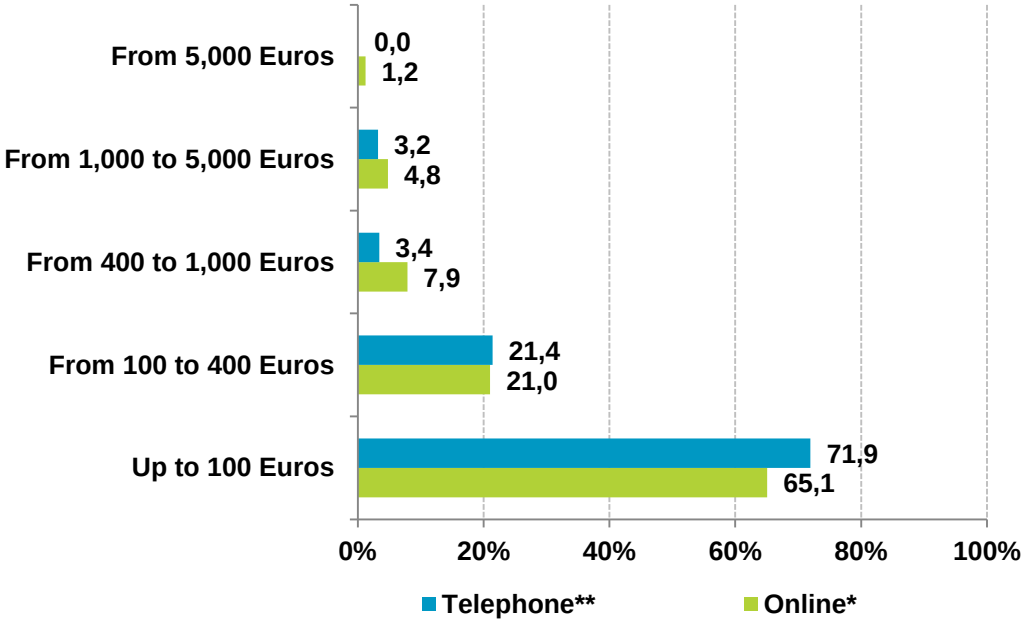
Online fraud attempt and manifestations

Economic impact of fraud

Online fraud attempts that cause an **economic loss** to the victim have increased up to **11.5%**.



BASE: Users who have experienced attempted fraud



Distribution of the economic impact of fraud

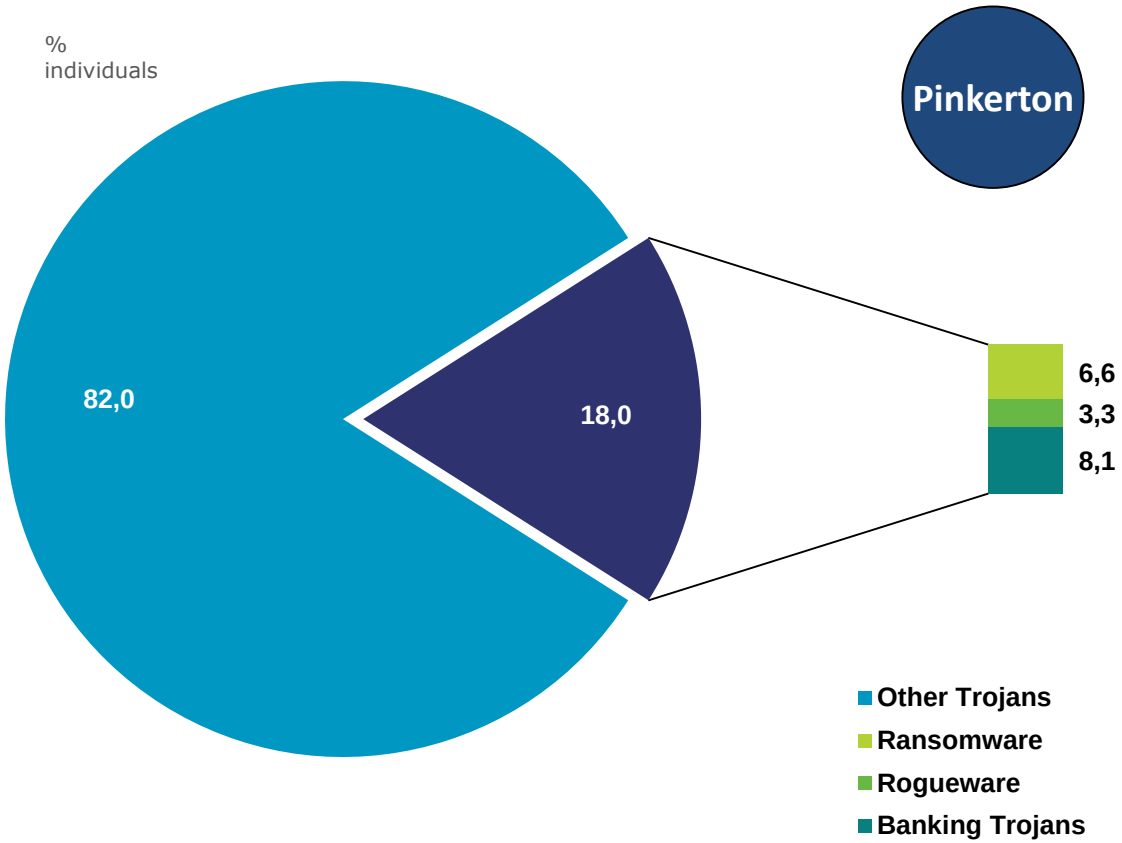
* BASE: Users who have suffered economic damage as a consequence of online fraud

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

Security and fraud

Fraud and malware on a computer

Figures for the presence of **banking Trojans** and **ransomware** on Spanish household computers stand at 6 - 8%.



Types of malware that have been analysed

✓ Banking Trojans: malware that steals confidential information from customers of banks and/or online payment platforms.

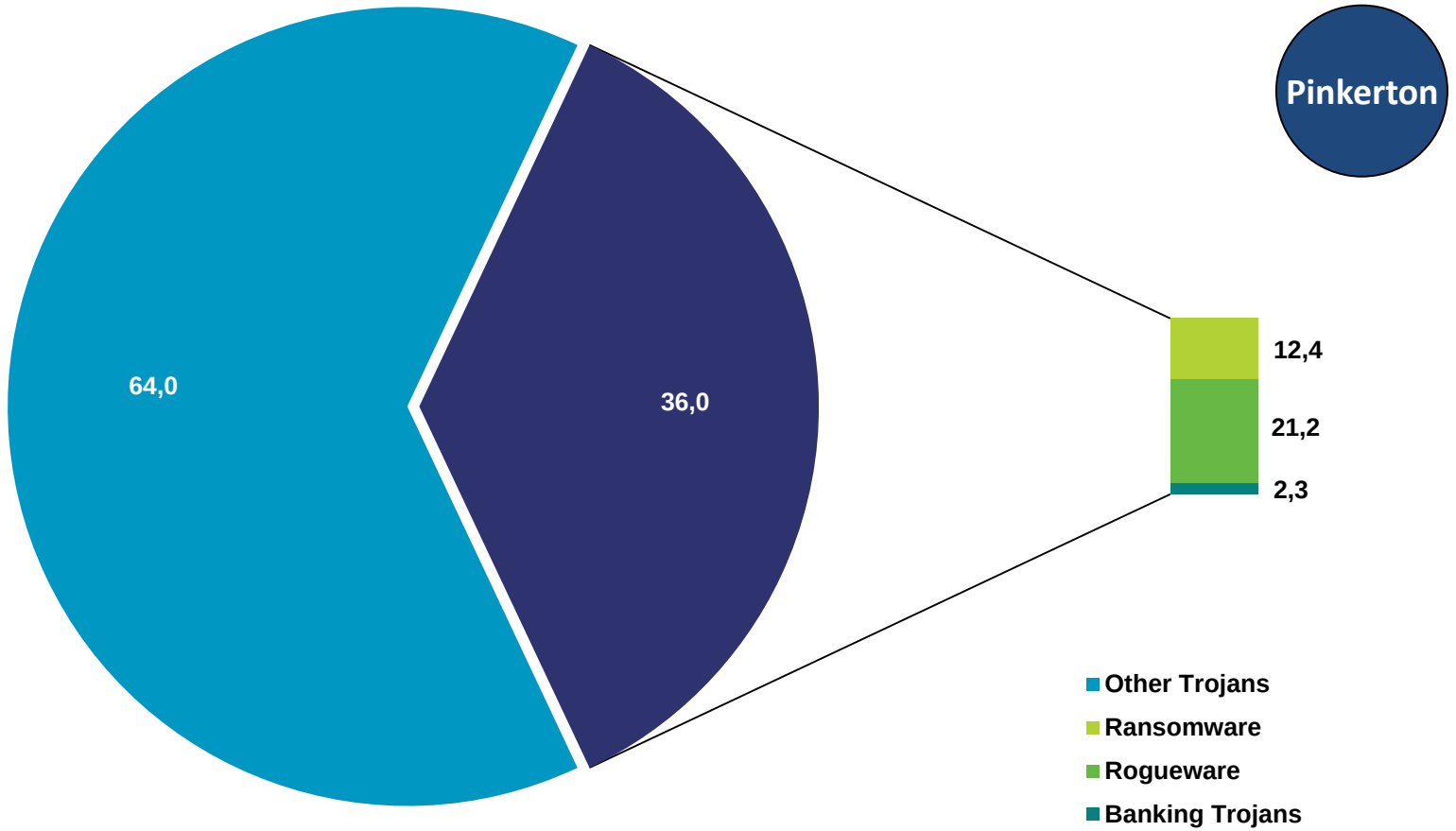
✓ Rogueware:
malware that makes victims think they have been infected by some kind of virus, getting them to pay a certain sum of money to remove it. The user is usually asked to purchase a false antivirus program, which turns out to be the malware itself.

✓ 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 the removal of the malware.

BASE: Computers with Trojans detected

Fraud and malware on mobile devices

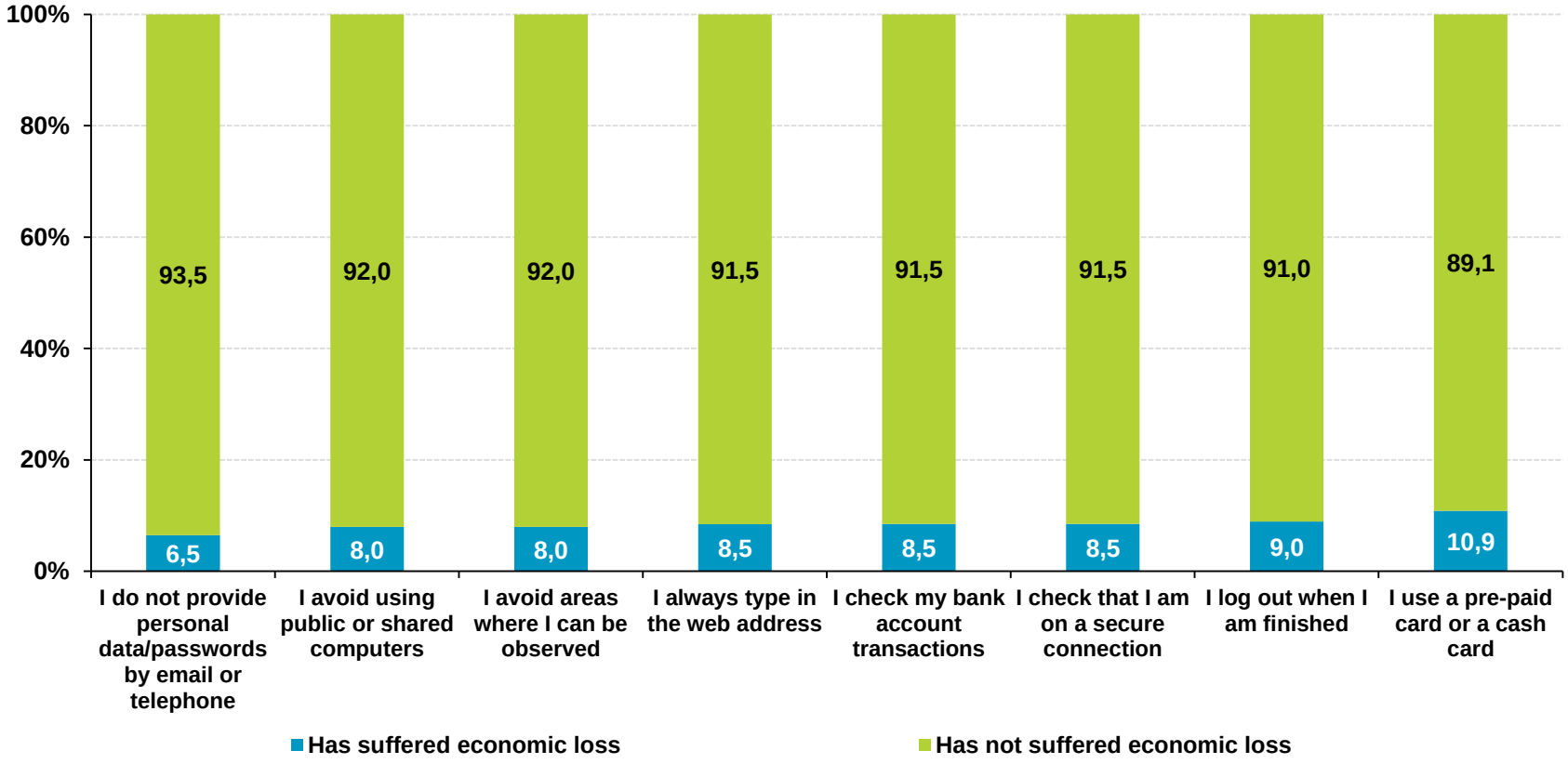
Rogueware is the Trojan subcategory most detected on Android devices (**21.2%**).



BASE: Android devices with Trojans detected

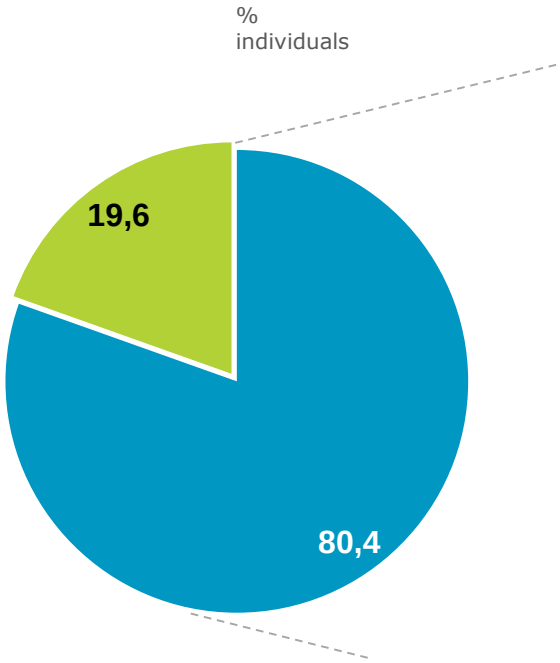
Succesful fraud attempt according to prudent habits

Prudent habits browsing the Internet and using the computer or mobile device **minimise** the risk of the fraud attempt being successful. In all cases, a percentage under **11%** of users with good habits have NOT suffered economic loss stemming from a fraud attempt.



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

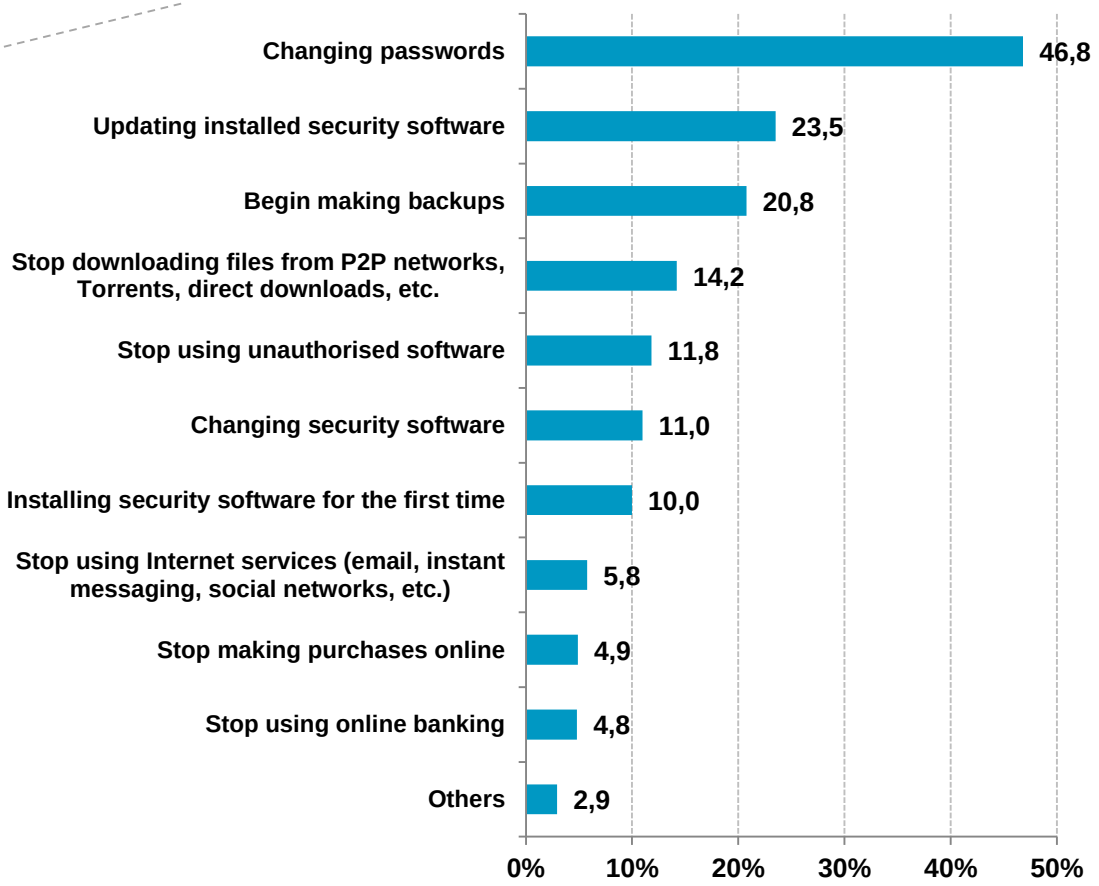
Changes made after a security incident



BASE: Users who experienced an incident

Changes made:

Multiple response



BASE: Users who experienced an incident and made a change

5

Don't wait until you have a problem to create backups:

https://www.osi.es/es/campanas/copias-cifrado-informacion/5-razones-por-las-que-hacer-copias-de-seguridad

Changes made after a security incident

Changes in security habits and measures according to the type of incident

Wi-Fi intrusion is the incident that most affects a change in different user habits (between **23%** and **48.4%** depending on the habit that suffered a change).

Incident (%)	Changes in habits					
	Changing passwords	Updating tools	Making files backups	Changing security programs	Stop using unauthorised software	Installing security tools for the 1st time
Malware	44,5	29,4	26,2	21,4	18,1	16,8
Loss of files or data	44,0	23,8	32,7	17,4	18,7	18,0
Spam	39,2	18,6	16,3	8,0	9,0	6,9
Identity theft	45,6	30,2	27,9	26,1	19,6	21,5
Wi-Fi intrusion	**48,4**	**34,2**	**34,1**	**33,8**	**23,6**	**23,0**
Loss of device	41,8	16,5	22,7	26,0	14,7	18,8
Inaccessible services due to cyberattacks	46,7	31,8	28,1	12,2	19,7	17,0

BASE: Users who have experienced each of the security incident

Changes made after a security incident

Changes in use of Internet services according to type of incident

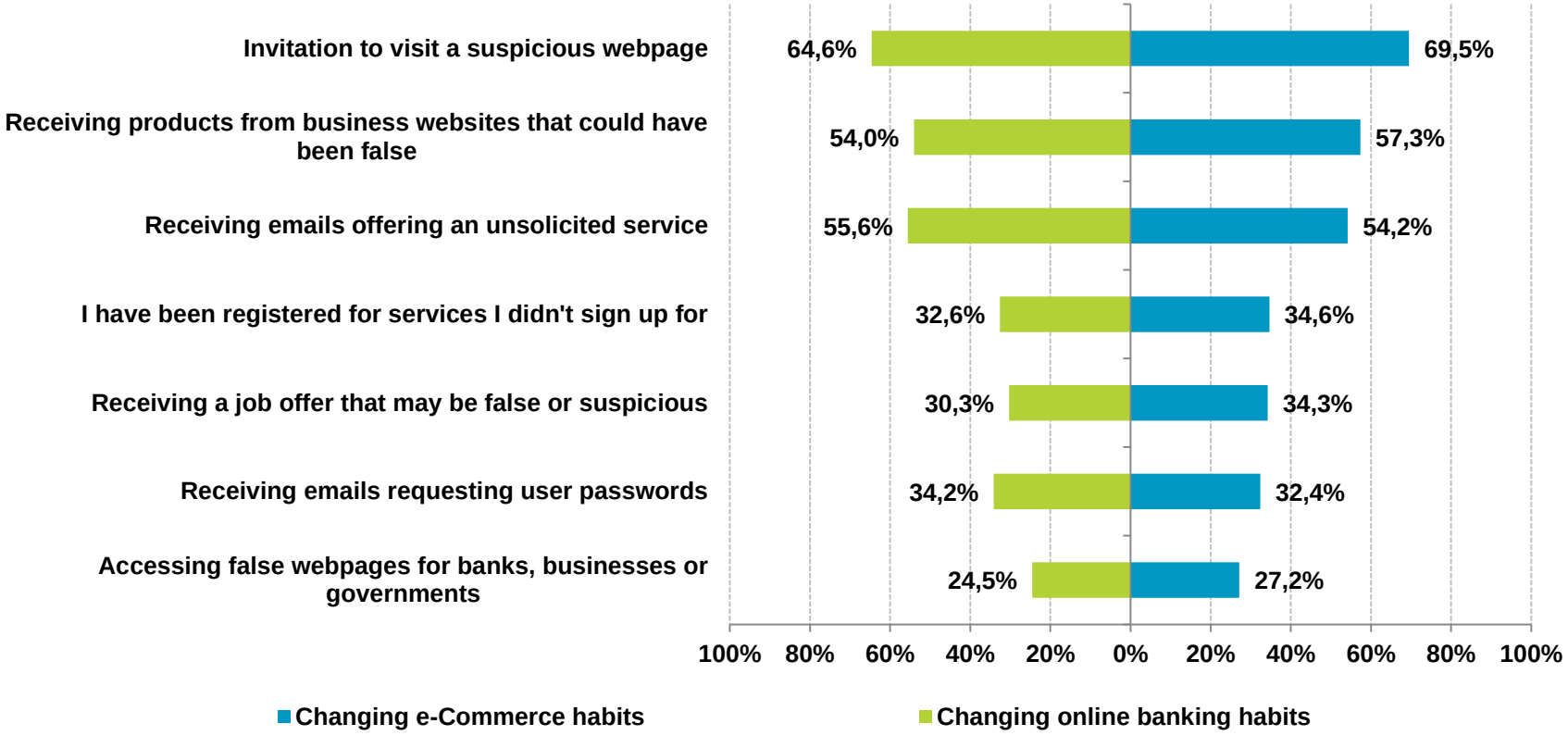
Incident (%)	Stop using Internet services	Stop using online banking	Stop using e-Commerce	Stop downloading files, software, etc.
Malware	9,5	9,6	8,1	21,8
Loss of files or data	10,7	10,9	9,7	20,4
Spam	2,5	3,1	3,6	10,4
Identity theft	15,6	10,8	**16,4**	**24,1**
Wi-Fi intrusion	16,7	**13,2**	15,7	22,3
Loss of device	**27,3**	13,0	10,7	20,7
Inaccesible services due to cyberattacks	10,1	8,9	9,5	19,2

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

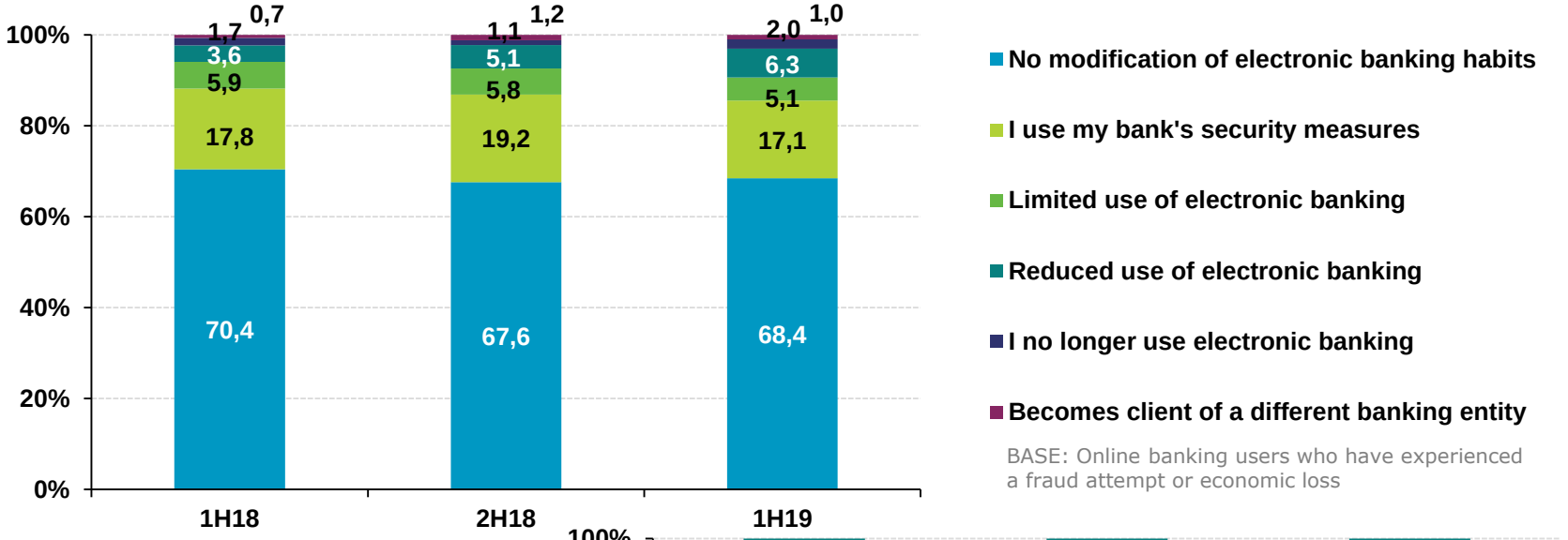
Receiving an **invitation to visit a suspicious website** is still a great influence for users in terms of changing prudent online banking (**64.6%**) and e-Commerce (**69.5%**) habits.



BASE: Online banking and/or e-Commerce users who have experienced attempted fraud

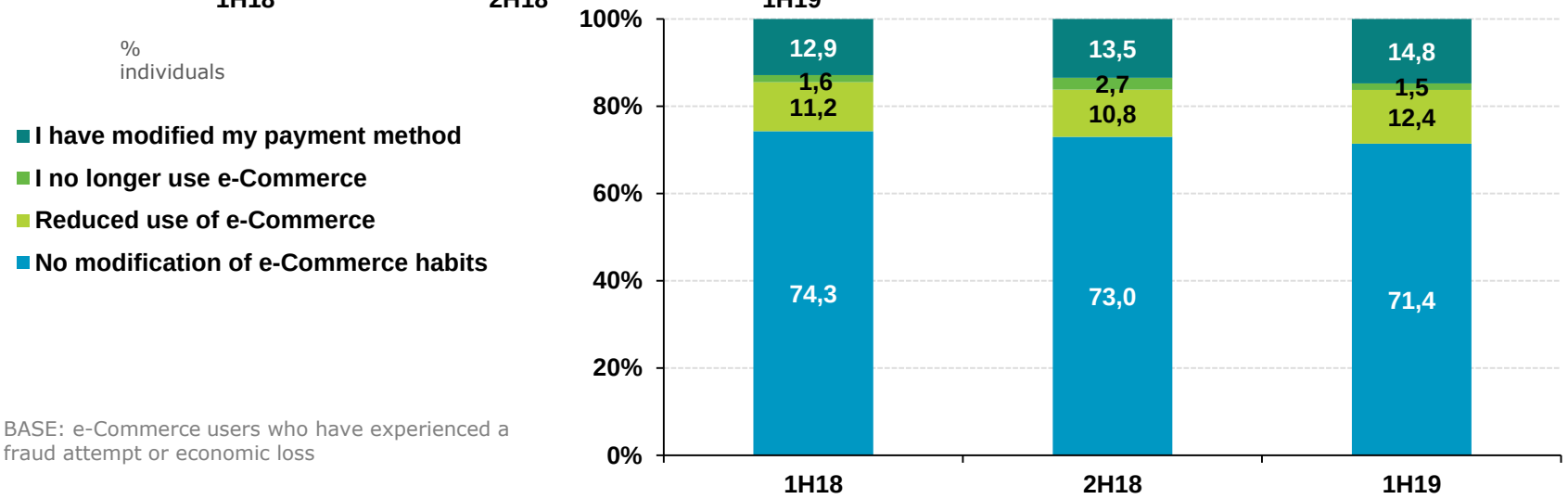
Changes made after a security incident

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



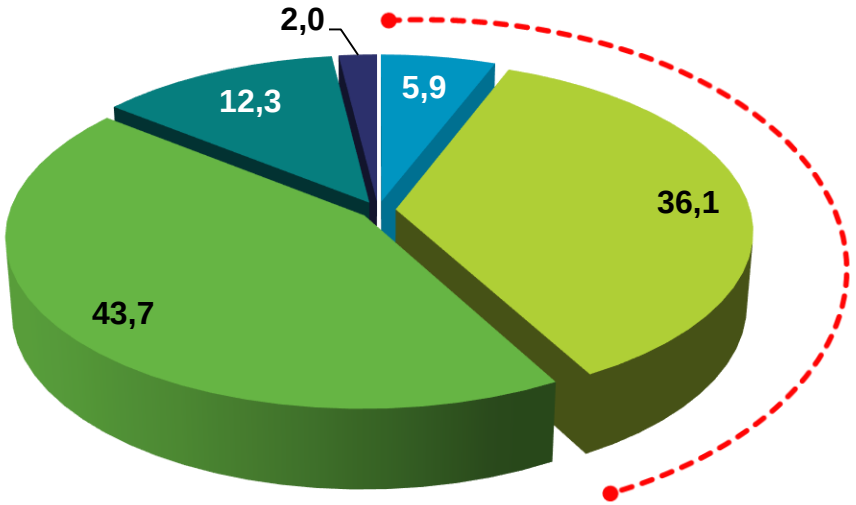
BASE: e-Commerce users who have experienced a fraud attempt or economic loss

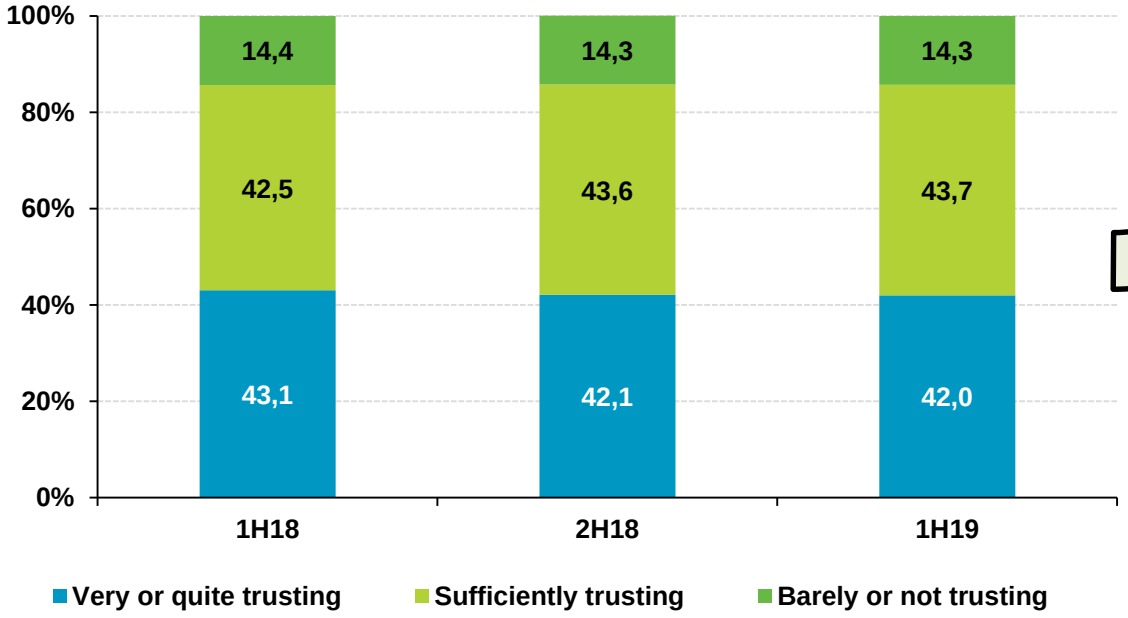
1. e-Trust and limits to the Information Society
2. User perception on the evolution of security
3. Assessment of the dangers of the Internet
4. Responsibility for Internet security

6

Level of trust in the Internet

The **level of trust in the Internet** remains constant since the second half of 2018.



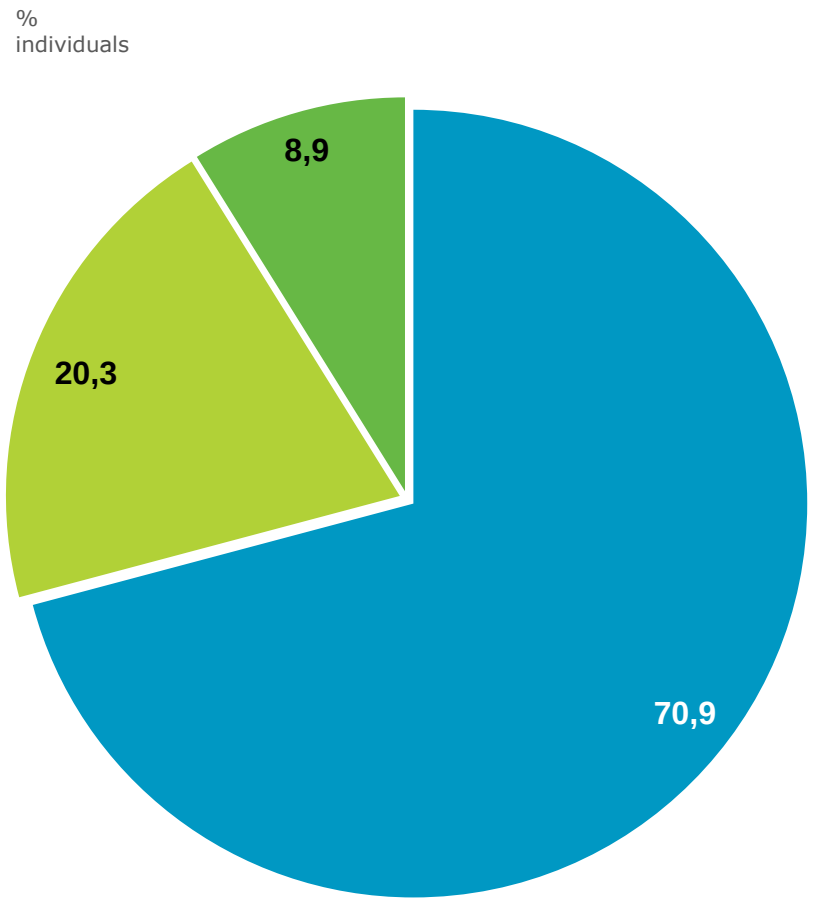


Very trusting
Quite trusting
Sufficiently trusting
Barely trusting
Not trusting

% individuals

BASE: All users

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

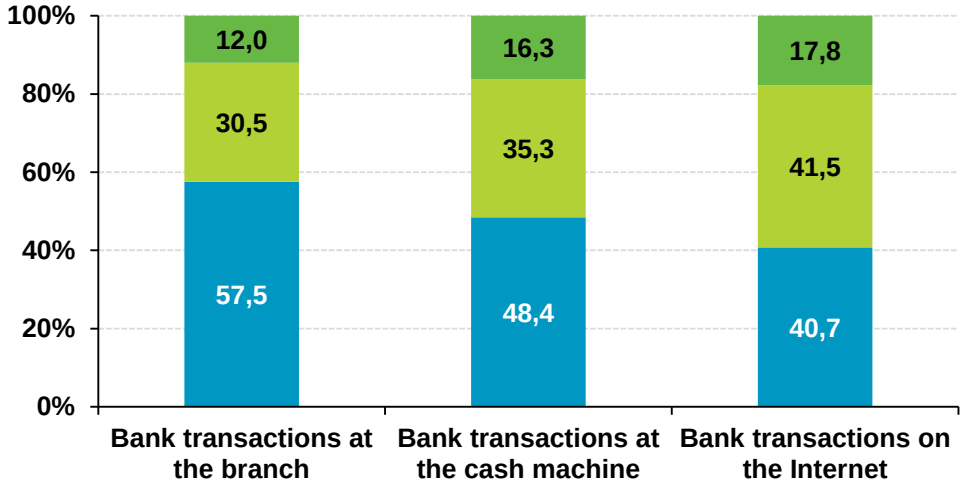


Most users (**70.9%**) consider that their personal computer or mobile device is **reasonably protected** against Internet threats.

6

BASE: All users

Online trust vs offline trust



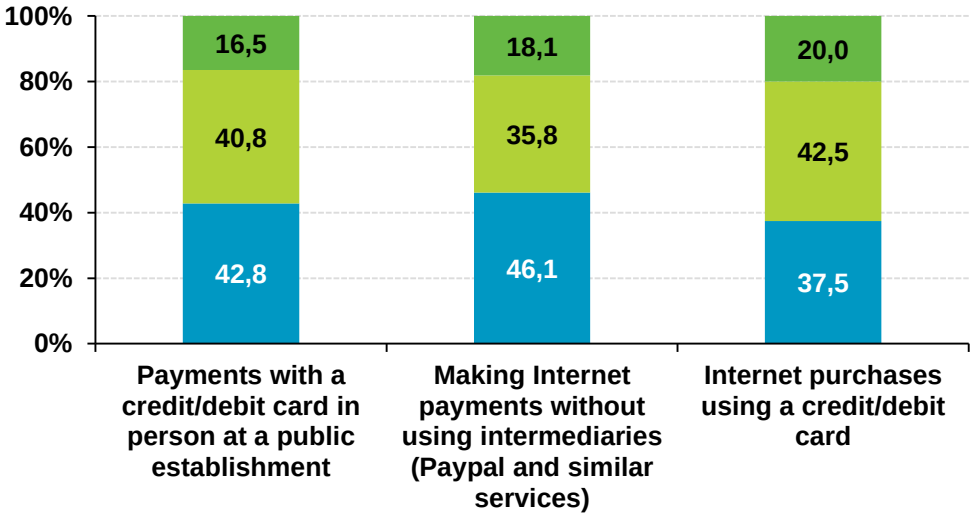
Level of trust in bank transactions

% individuals

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

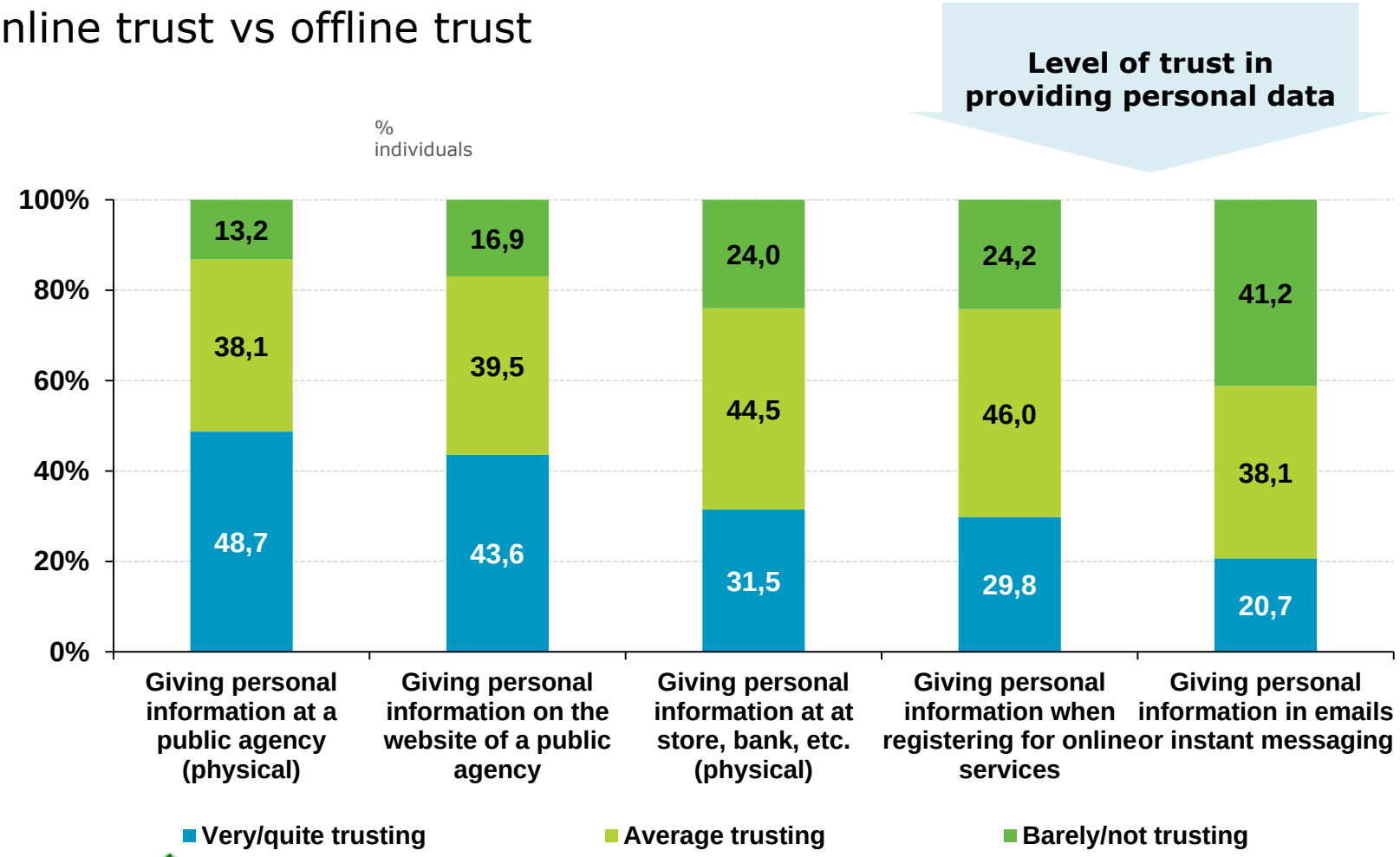
Level of trust in e-Commerce operations

Users prefer carrying out bank transactions at the branch (**57.5%**), and payments on the Internet using an intermediary, avoiding the use of credit/debit cards (**46.1%**).



BASE: All users

Online trust vs offline trust



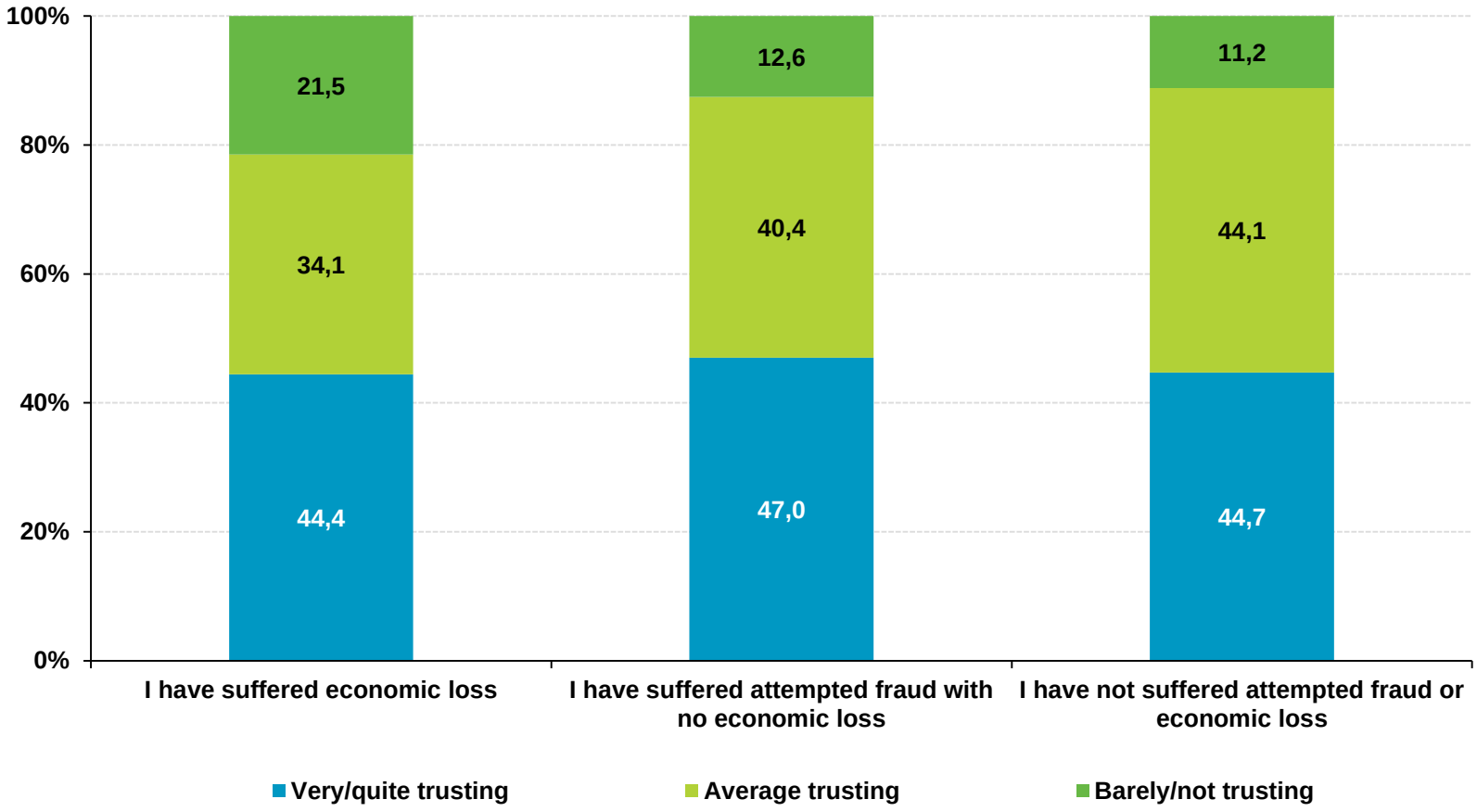
Am I obliged to provide my personal information/data when asked?

https://www.osi.es/sites/default/files/docs/datospersonales.pdf

BASE: All users

Trust vs fraud

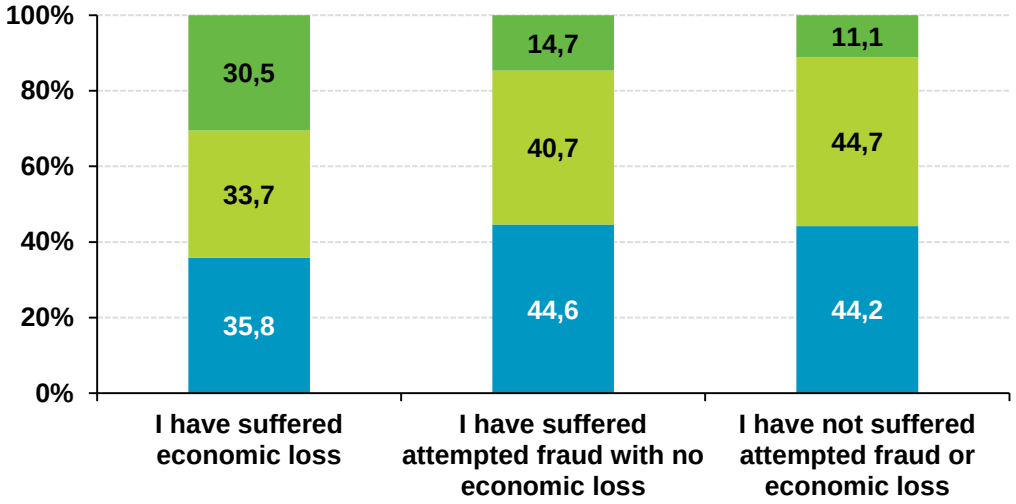
Trust in conducting banking operations on the Internet



BASE: Online banking users

e-Trust and limits to the Information Society

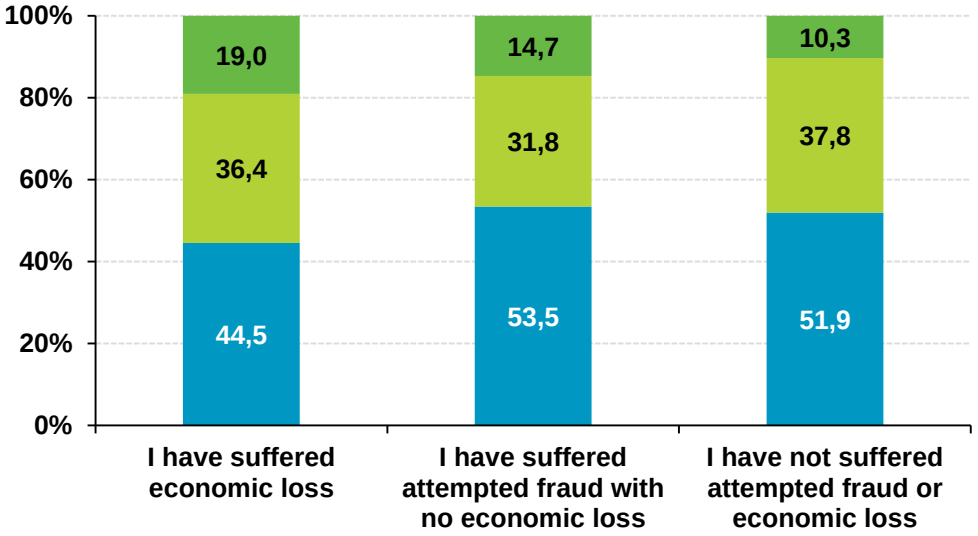
Trust vs fraud



Trust in Internet purchases using a credit/debit card

% individuals

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



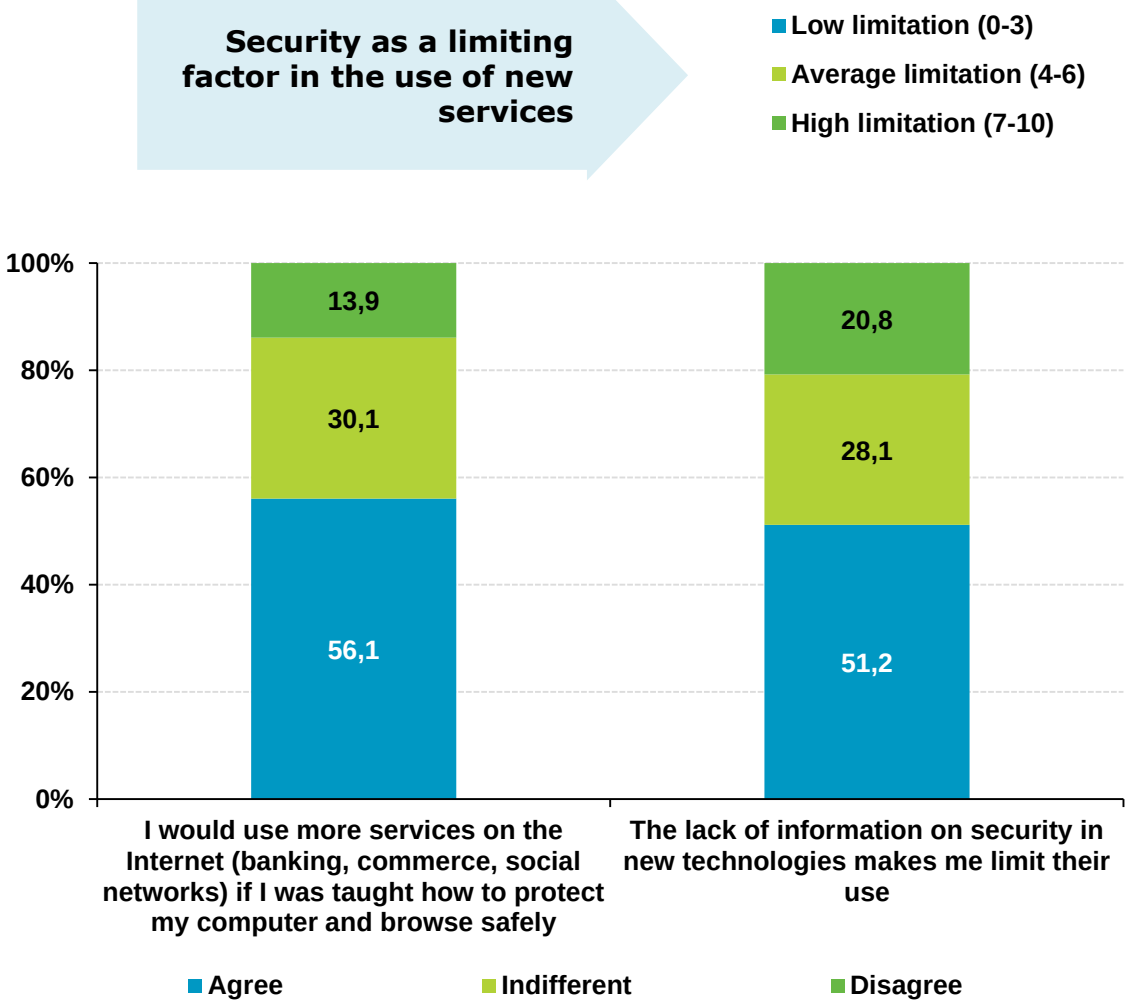
Very/quite trusting
Average trusting
Barely/not trusting

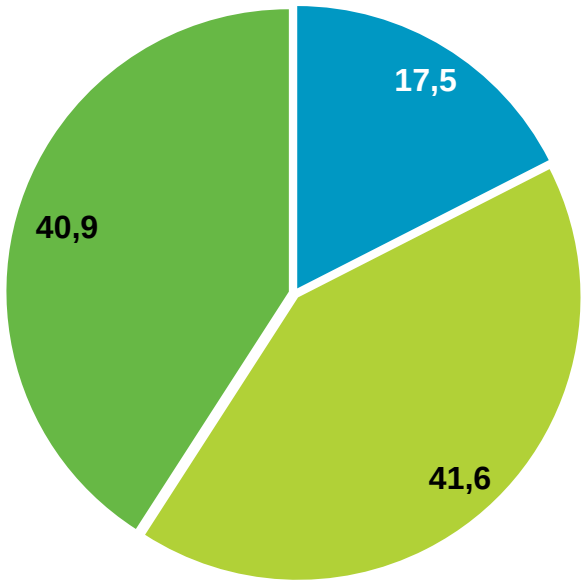
BASE: e-Commerce users

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

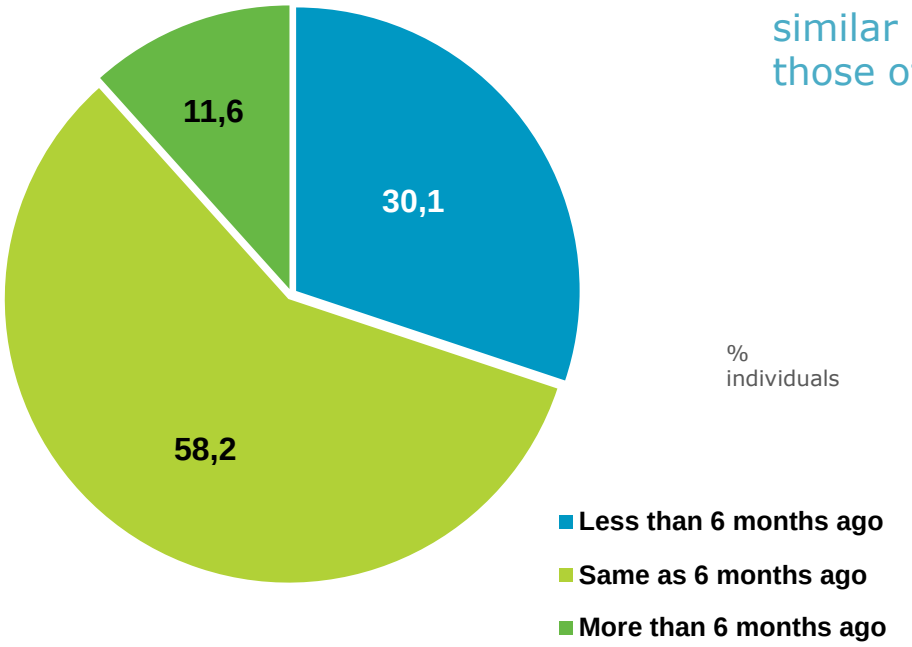
Limitations in the use of Internet

6

BASE: All users

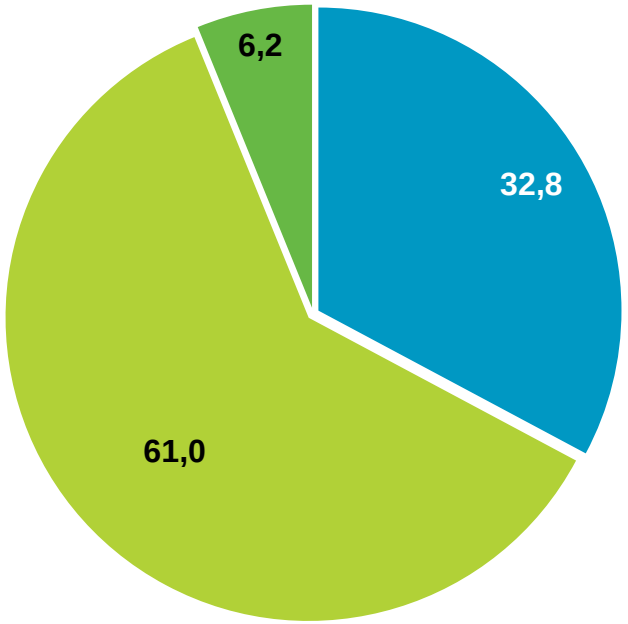
User perception on the evolution of security

Number of incidents



Approximately 3 out of 5 users consider that incidents in the last 6 months are similar in terms of quantity and severity to those of the previous semester.

Seriousness of incidents

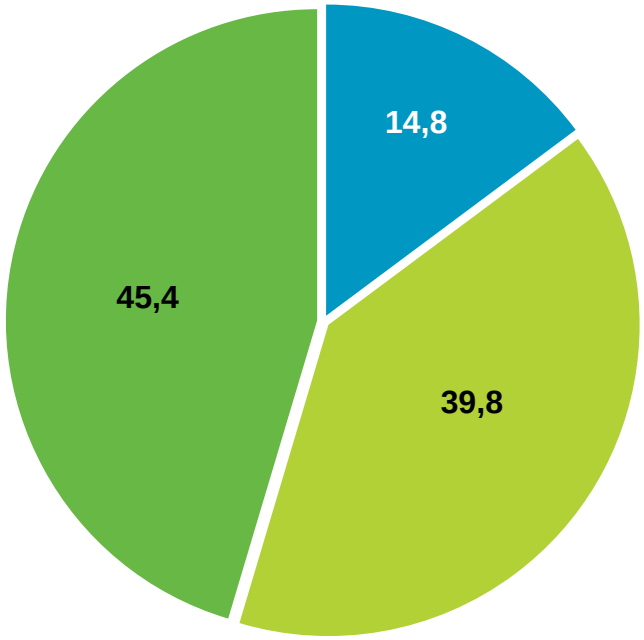


Almost **one third** perceived a **lower number** of incidents in the last 6 months (**30.1%**) and also considered them to be **less serious** (**32.8%**).

BASE: All users

Perception of risks on the Internet

Perception of risks on the Internet is still led by the **theft and use of personal information** (**45.2%**) and **economic loss** (**39.8%**).



%
individuals

Do you know how to protect your privacy on the Internet and your data in the cloud?

✓ **Privacy:** https://www.osi.es/es/tu-informacion-personal

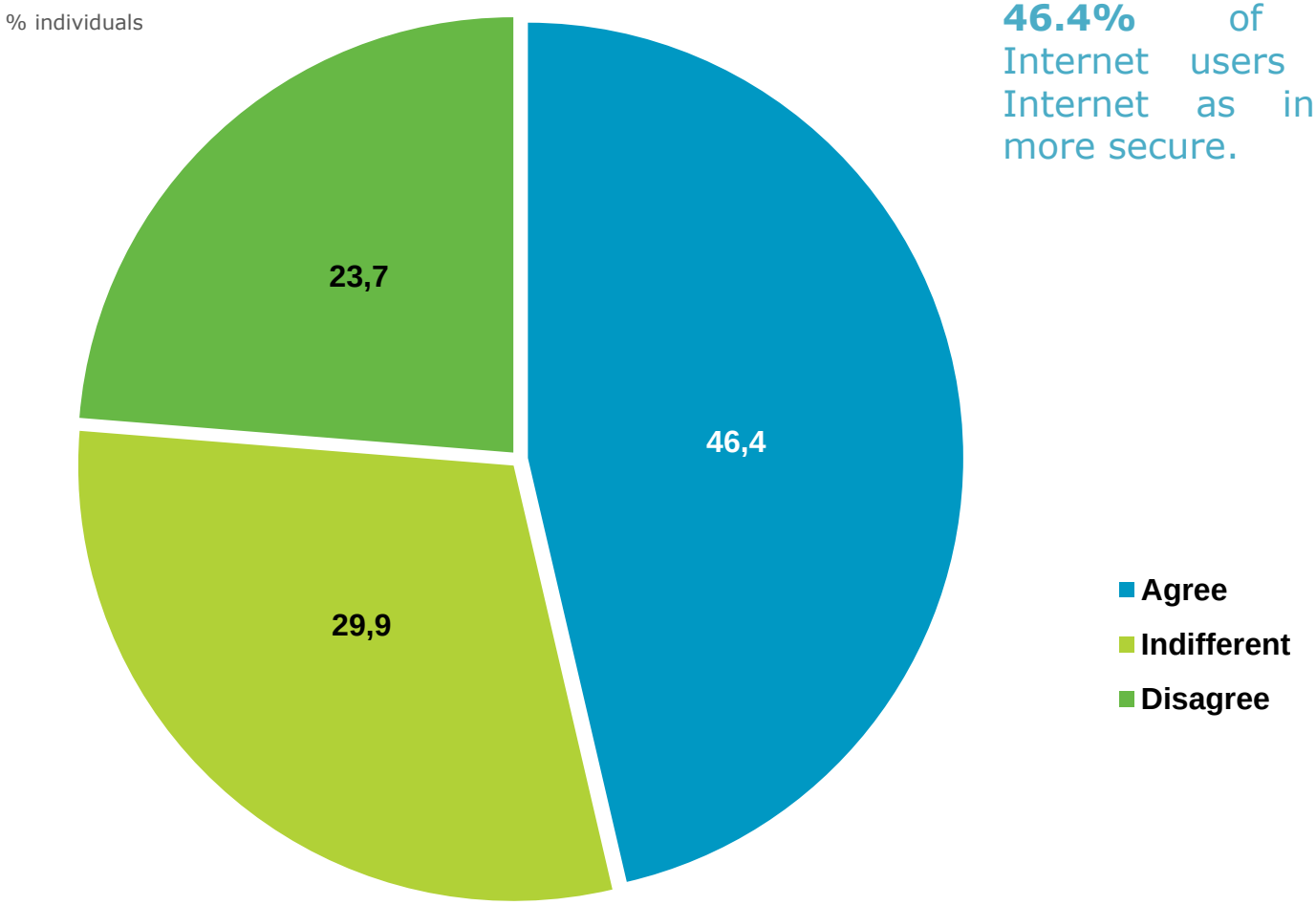
✓ **Data in the cloud:** https://www.osi.es/es/tu-informacion-en-la-nube

6

- **Damage to computer components (hardware) or the programs they use (software)**
- **Economic loss: fraud in online bank accounts, credit cards, purchases**
- **Privacy: theft or use of personal information without consent (photographs, name, address)**

BASE: All users

Assessment of the Internet as increasingly safer



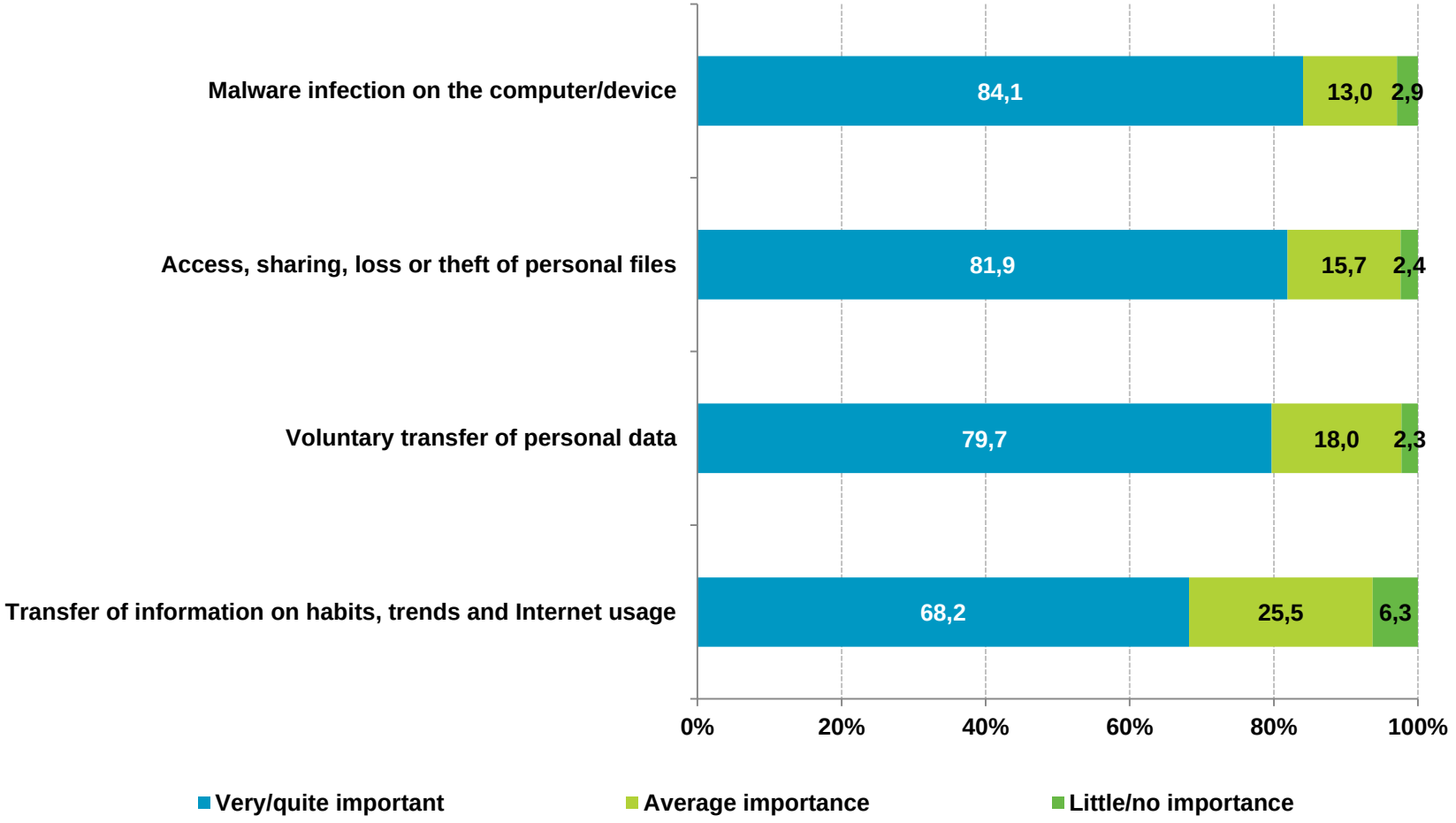
46.4% of Spanish Internet users rate the Internet as increasingly more secure.

6

BASE: All users

Assessment of the dangers of the Internet

The dangers most valued by panellists are still **malware infection** (**84.9%**) and **personal files security** (**81.9%**).

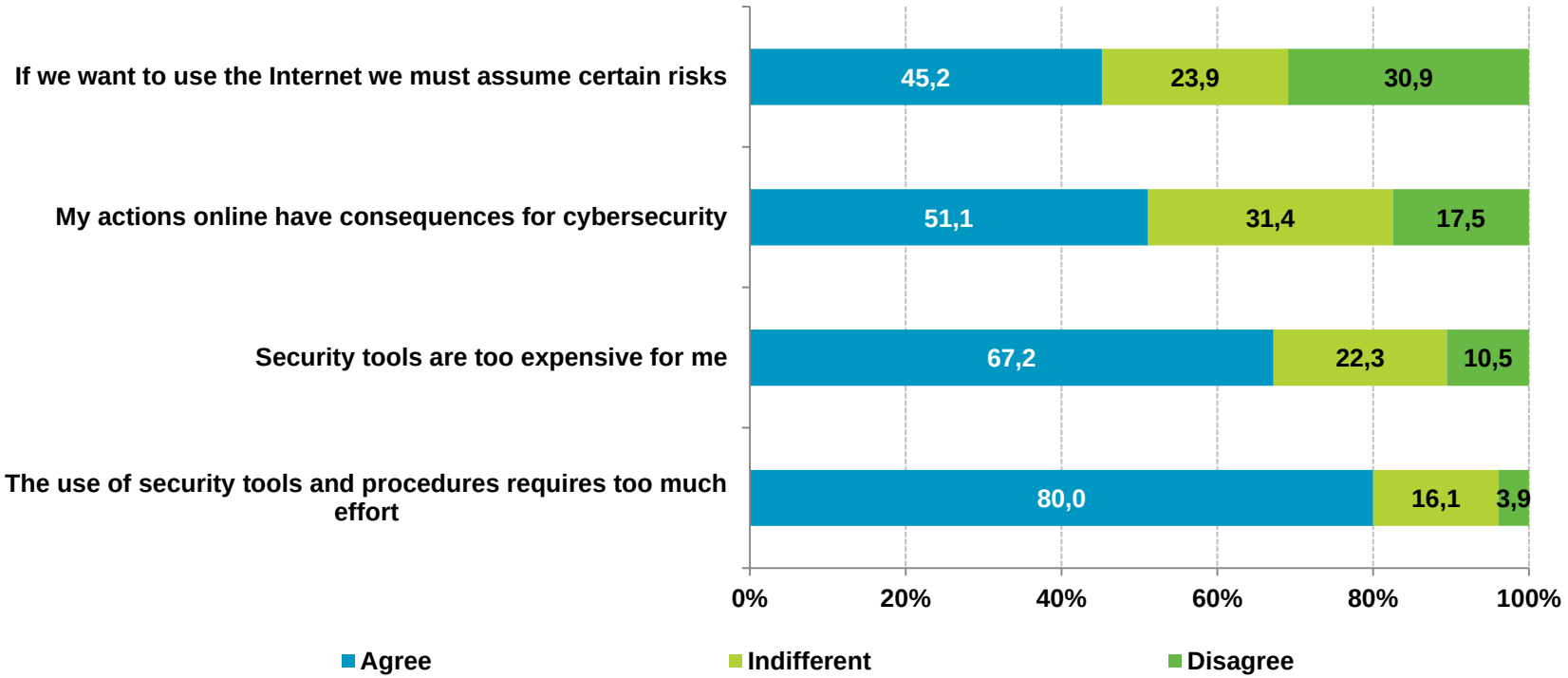


BASE: All users

Role of the user

Half of the Internet users believe that **their actions have consequences for cybersecurity** (**51.1%**).

Meanwhile, almost half (**45.2%**) consider that **they must assume certain risks to enjoy the Internet**, two-thirds (**67.2%**) that **security tools are too expensive**, and four out of five (**80%**) that **the use of security tools and procedures requires too much effort**.



BASE: All users

Conclusions

Conclusions

Spanish Internet users worry the most about theft and unauthorised use of their personal information (45.4%), voluntary transfer of personal data (79.7%) and transfer of information on habits, trends and Internet usage (68.2%).

In this regard, cloud services security has some deficiencies: in 2018, Bitglass released a report warning about the lack of protection of personal data on cloud services [1]. In 2019, Facebook recognised that millions of users' credentials had been stored on its platform in a non-secure manner [2].

Although awareness about the possible privacy loss due to the use of social networks is rising –four out of ten Spanish users claim they would be willing to completely stop using this kind of services if by doing so they could regain control over their personal data [3]- there are still users who do not implement or do not know the available privacy options on social networks (5.59%) and/or leave their information public for third parties to have access to it (11.8%).

[1] https://www.bitglass.com/press-releases/bitglass-2018-report-cloud-security-adoption-trails-usage

[2] https://www.infotechnology.com/online/Error-de-seguridad-de-Facebook-expone-millones-de-contrasenas-de-Instagram-20190419-0001.html

[3] https://www.eleconomista.com.mx/finanzaspersonales/Por-privacidad-internautas-dejarian-sus-redes-Kaspersky-20190707-0090.html

Conclusions

Almost 40% of European IT experts [4] believe the legislation regulating data protection needs to be significantly improved, particularly its correct implementation, in order to effectively asure the security of users' data privacy.

These data could be exacerbated if attention is paid to the fact that most Spanish users do not really know what kind of information is considered to be private. For instance, Vida Digital (CPP Group) released a study [5] informing that a quarter of Spanish people do not think about their email address or personal photos as personal information. And according to Kaspersky Lab, one out of five users would be willing to give up their privacy in exchange for a free service [6].

Users still have dangerous habits such as connecting to public Wi-Fi or third party networks (28.3%), and not changing the default settings of their smartphones to allow the installation of apps from unknown sources (67.5%). These are security gaps that could allow the access to private information, thus increasing the risk of cyberbullying and cyberviolence due to the lack of protection of personal data.

[4] https://mktg.forrester.com/predictions-2019

[5] https://blog.segurostv.es/ciberacoso-principal-problema-de-la-vida-digital-para-las-familias/

[6] https://www.pinoybisnes.com/news-release/38-would-give-up-social-media-to-guarantee-lifetime-data-privacy-kasperskys-study-says/

Conclusions

A research carried out by Kingston [7] reveals that 73% of Spanish users do not make security backups of their personal data regularly. This, in accordance with the data collected from the Panel (63.5%), shows an inherent risk associated with loss of information and personal data if a security incident or failure of the system happens.

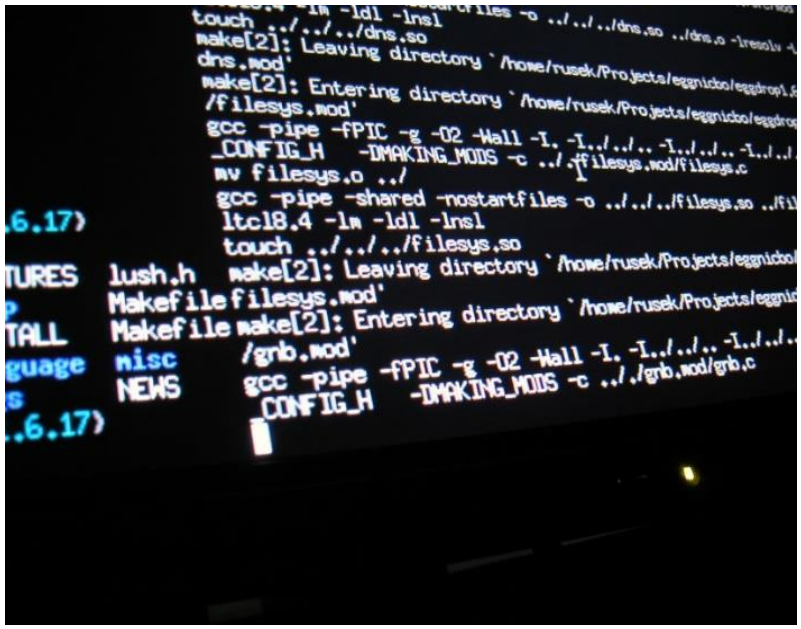
Although users worry about non-authorised access and sharing personal data and the theft of the latter (81.9%), there is simply a slight increase (+2.6 p.p.) in the number of users who began making security backups compared to the second half of 2018.

This can be extrapolated to companies that, according to the cybersecurity survey carried out by Forbes Insights [8], also need to improve their strategy by using better and updated security tools.

[7] https://www.kaspersky.com/about/press-releases/2019_a-shift-from-quantity-to-quality-2018-saw-cybercriminals-dropping-basic-ddos-operations

[8] https://www.vmware.com/radius/forbes-insights-cybersecurity-strategy-report/

Conclusions



The most reported security incident this semester by Spanish Internet users continues to be spam (86.8%). Unsolicited email entails multiple dangers since this practice is one of the main vectors (because of their reach and cost) used by cybercriminals to distribute malware, carry out phishing campaigns and online frauds.

The number of phishing attacks detected by Kaspersky Lab [9] in 2018 increased up to almost 500 millions, a twofold increase compared with last year, thus reaching over 44%. These attacks targeted banks, payment systems and e-Commerce.

In the case of Spanish companies, according to Proofpoint [10], approximately 70% of IBEX35 companies are potential victims of impersonation in this kind of attacks due to the lack of defense mechanisms such as DMARC verification system, which is implementend only in 31% of Spanish companies.

Even though, only a quarter of Spanish Internet users repot using anti-spam programs/settings in order to avoid this kind of incidents.

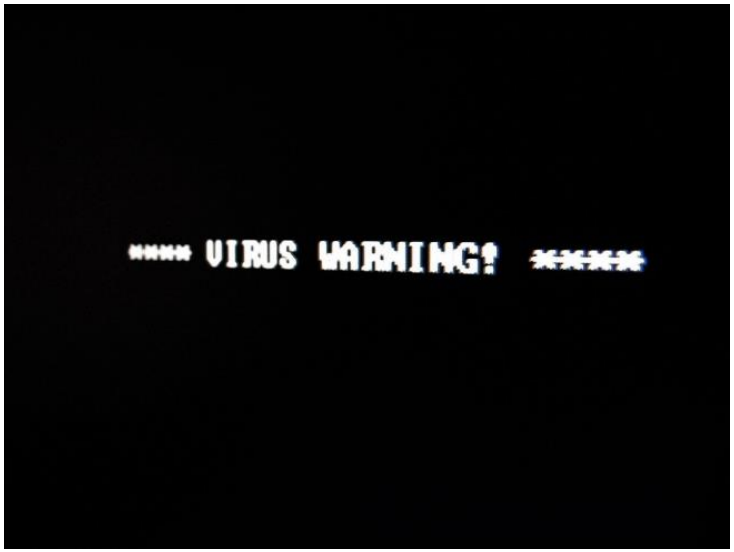
[9] https://www.kaspersky.es/about/press-releases/2019_los-ataques-de-phishing-crecen-m-s-del-doble-en-2018-llegando-casi-a-500-millones

[10] https://www.proofpoint.com/es/newsroom/press-releases/el-70-de-las-companias-del-ibex-35-esta-en-riesgo-de-que-suplanten-su

Conclusions

The new strategies used for the distribution of malware, such as the use of Trojan-droppers, have significantly increased the number of infected smartphones throughout last year [13]; this situation is exacerbated by risky habits adopted by users.

For example, barely half of Android users have some kind of antivirus installed on their devices, whereas over two-thirds of users allow the download of applications from unkwon sources.



However, not even Google Play can escape malicious applications [14]. The latter sometimes get through the security filters of Google Play with the intention to take advantage from the trust users have in the content downloaded from an official market in order to carry out the infection of the device succesfully. Over 200 applications uploaded to that market, with a total of almost 150 millions downloads, were detected as being hosts to the malware 'SimBad', which allowed adware, phishing and sharing data with other applications.

Given such a situation it is clear that there is a need for the user to take part more actively in cybersecurity, improving its non-risky habits and broadening the use of security tools with the intention to prevent all of these online threats.

[13] https://www.europapress.es/portaltic/ciberseguridad/noticia-nuevas-estrategias-distribucion-malware-movil-afectan-cerca-10-millones-usuarios-2018-20190329160305.html

[14] https://www.checkpoint.com/es/press/2019/mas-de-200-aplicaciones-de-google-play-infectadas-por-la-vulnerabilidad-simbad/

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, allows 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 their homes (at least once a month).

Sample Size: 3.619 households surveyed and their computers/Android devices scanned (software installed on 1.950 PCs, and 1.910 Android smartphones y 241 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.

Filedwork: fieldwork was conducted between January and July 2019 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 estimated sample error of the sample (size n=3.619) is equal to ±1,62%.

The '*Study on Cybersecurity and Trust in Spanish households*' was prepared by the following team of 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

Thanks for collaborating in this study goes to:

Thanks as well to the following individuals for their collaboration:

ISSN 2386-3684
doi: 10.30923/2386-3684-29

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

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