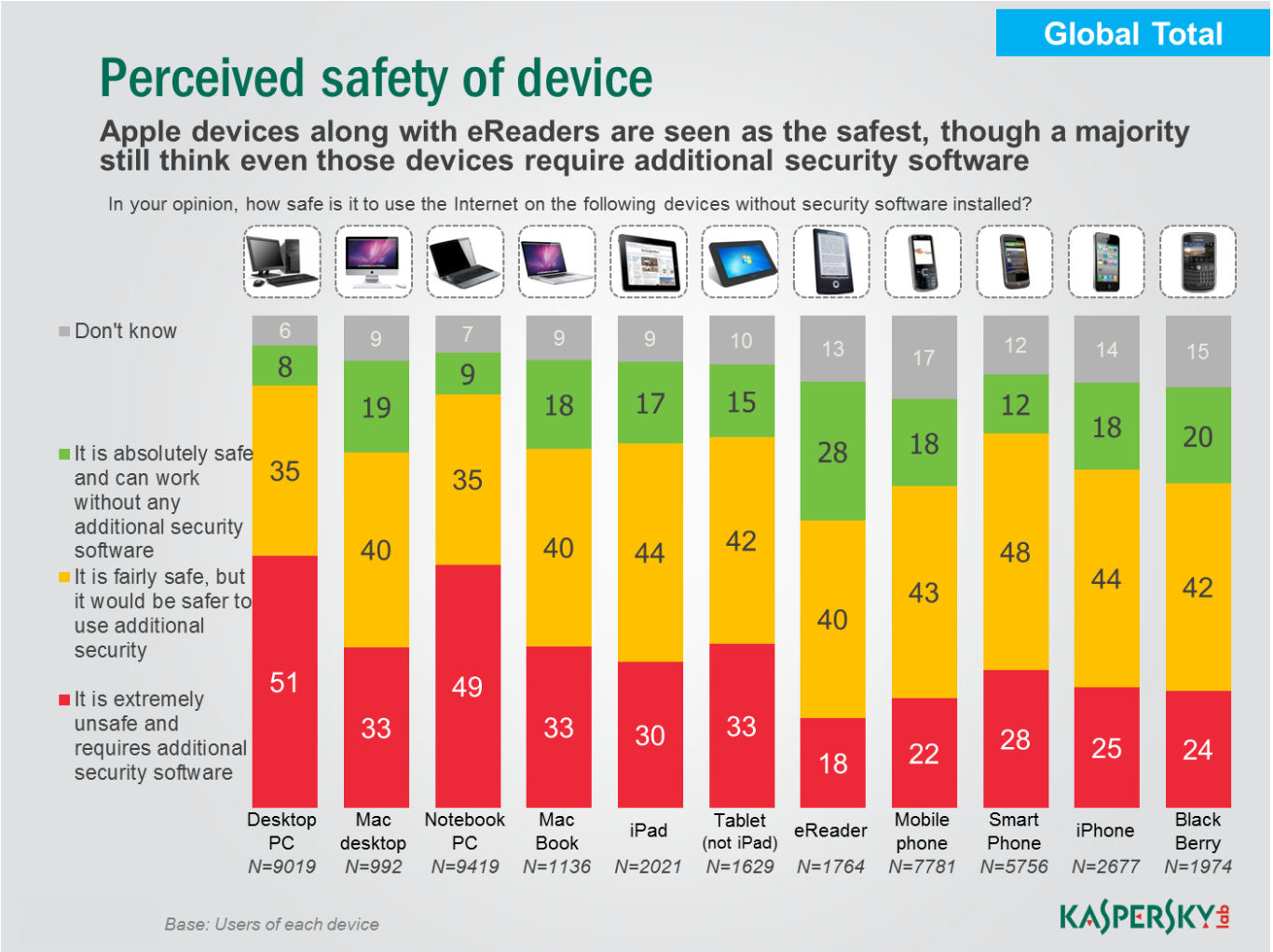
Perception and knowledge of IT threats: the consumer's point of view

It's hard to imagine life without digital devices, be it a large desktop computer or a smartphone. Modern users are storing some of their most valuable information in digital format and hoping their data is securely protected from prying eyes. In order to develop security solutions that most closely meet the needs of users, Kaspersky Lab conducts regular surveys focusing on the key issues facing IT security.

In the latest research, carried out in collaboration with O+K Research, we attempted to find out how people from all over the world use their digital devices, whether they trust social networks and cloud storage systems, how informed they are about the latest threats and how they protect their most valuable data from theft or loss. In particular, we wanted to know what type of information users considered most valuable. Throughout the course of the survey we polled over 11,000 users living in Latin and North America, Europe, the Middle East, Asia and Africa. All the participants were aged 16 or over and had access to the Internet, with over 90% of them going online every day. Both experienced and novice computer users took part in the survey.

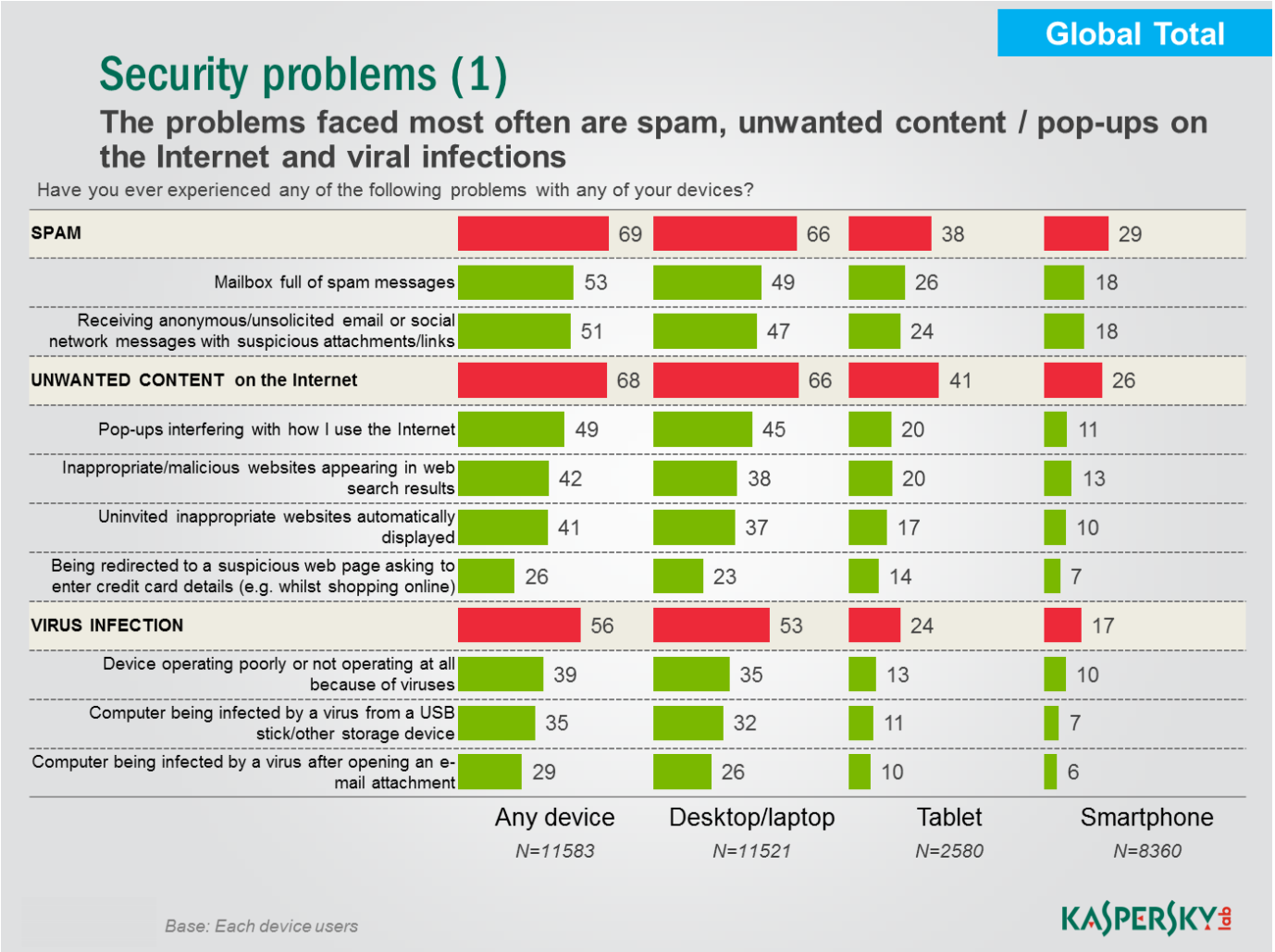
Perception of security



Approximately half of the Windows desktop and laptop users surveyed believe it is unsafe to use their computers without additional security software; only 8 and 9% of users respectively consider them to be completely safe. Contrary to common belief, owners of Apple devices are under no illusions when it comes to the security – just 19% of Mac users and 17% of iPad users think their devices do not require protection. These figures are still significantly higher than the corresponding figures for users of Windows desktops and laptops.

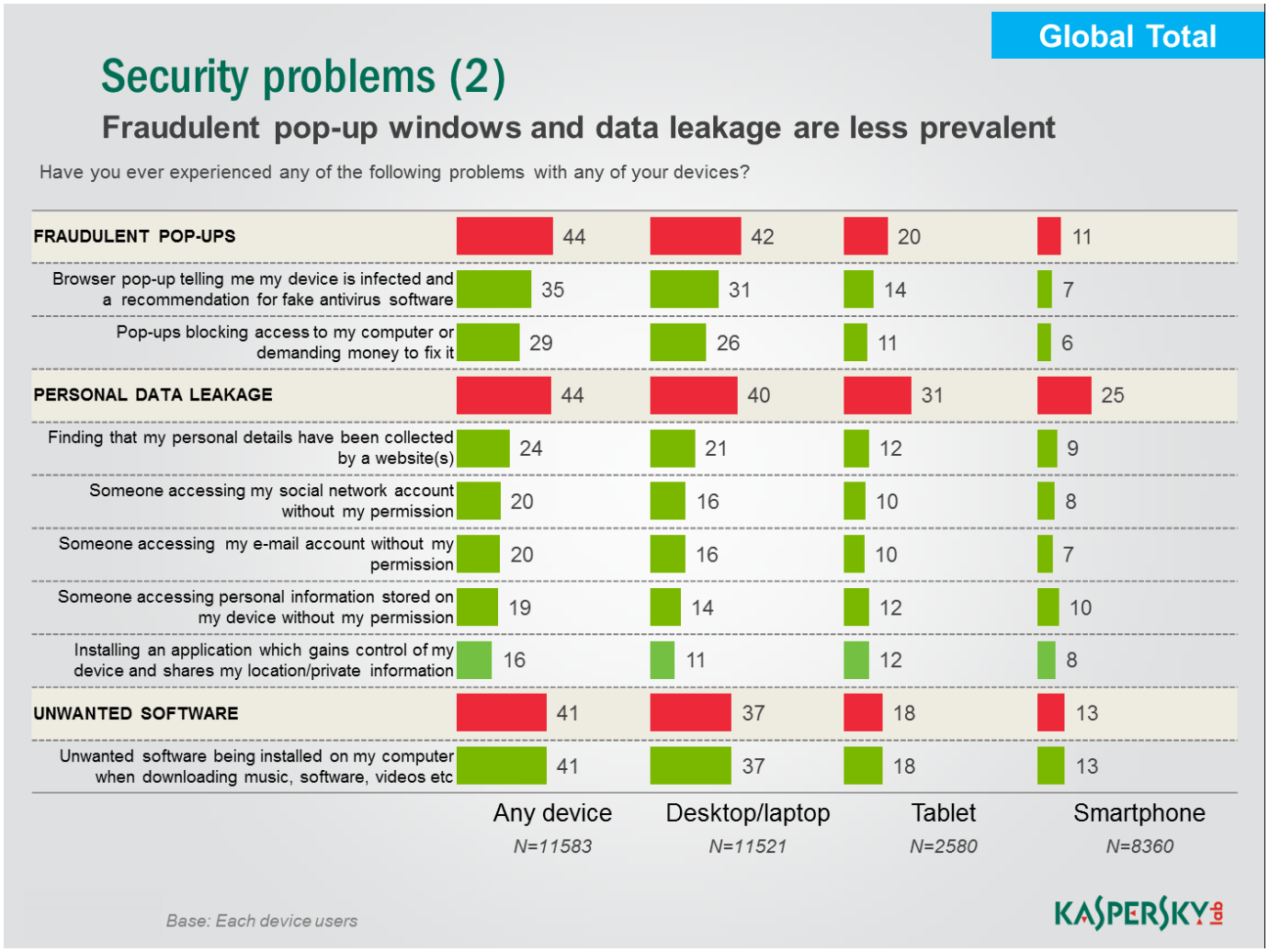
KASPERSKY lab

Current threats: spam, malware and personal data theft

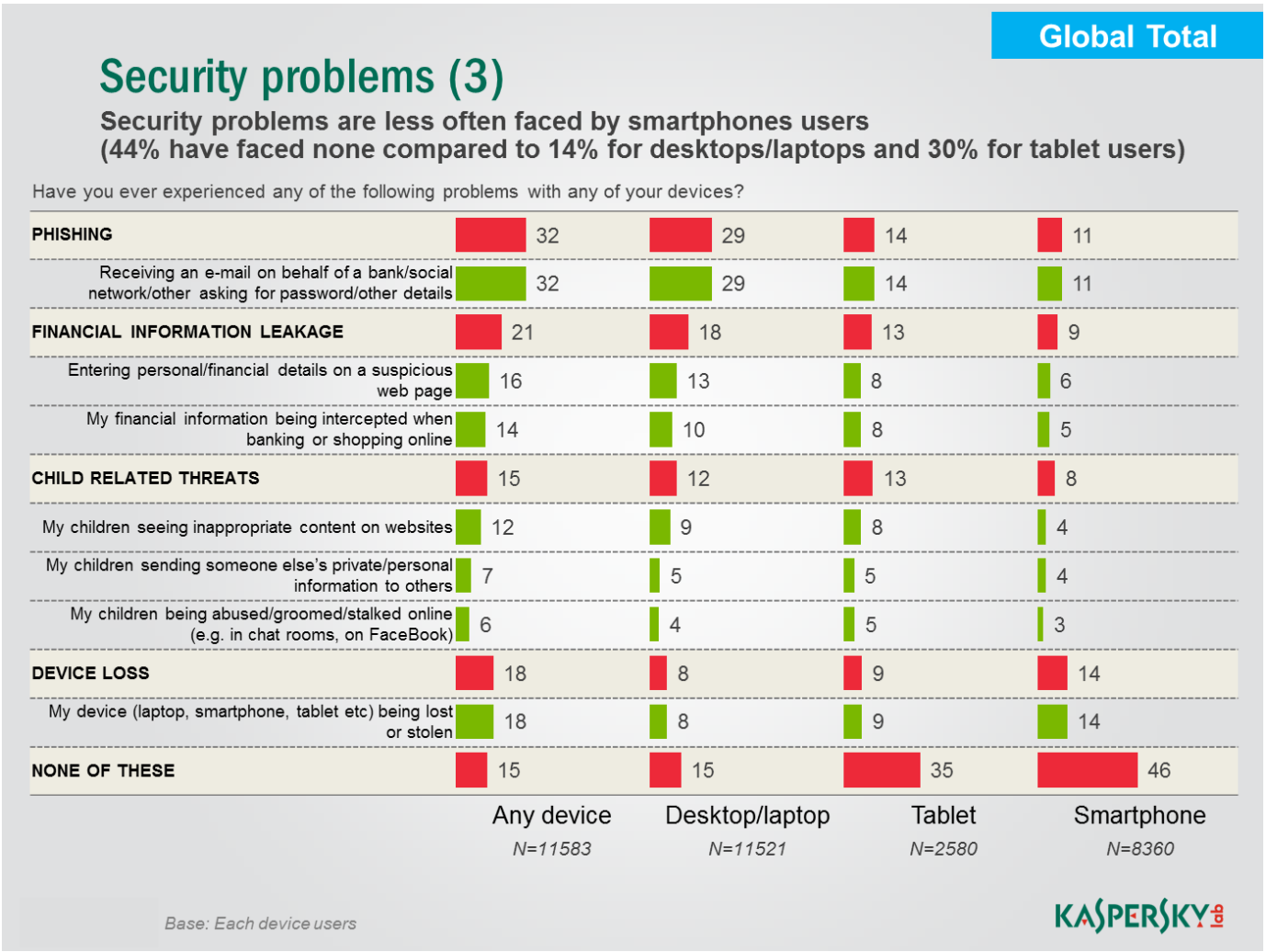


The most prevalent problem facing users remains spam, with 69% of respondents having been affected, regardless of the device they use. It includes such things as relatively harmless emails or instant messages containing suspicious links which, if clicked, can result in a device being infected. Malicious programs are another major problem that affected 56% of users, while 13% of tablet owners and 10% of smartphone owners reported that their device had not worked properly at some point due to malware.

KASPERSKY lab

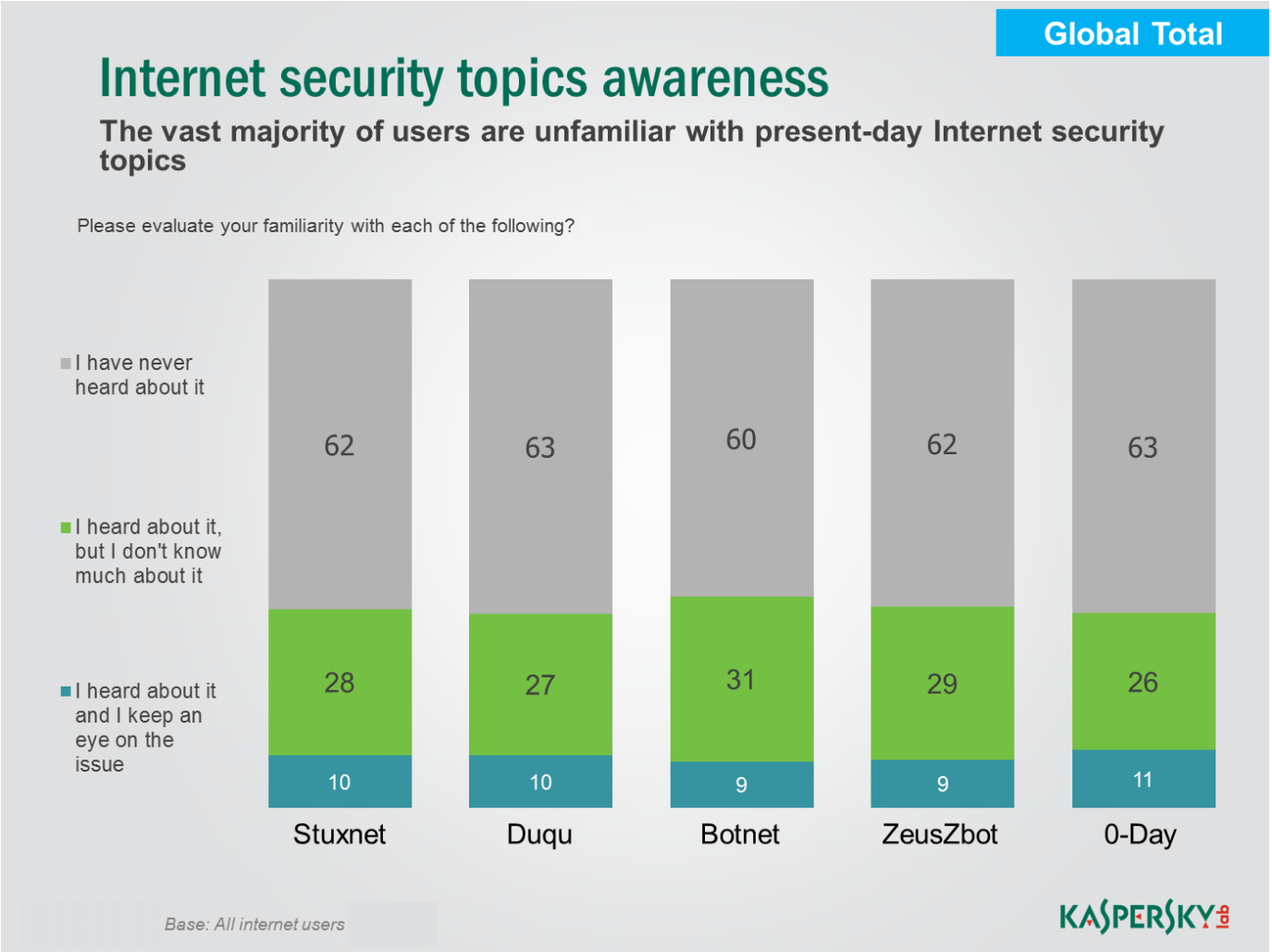


Trojan ransomware affected 29% of the respondents, mostly PC users. Another 35% encountered pop-up windows that warned them about an alleged infection on their devices and suggested installing fake antivirus solutions. Another significant threat, personal data leaks, affected 44% of respondents. The gap here between PC users and mobile device owners is not as substantial as is the case for pop-up windows. For instance, 16% of PC users and 10% of tablet owners reported unauthorized access to their social network or email accounts.



Phishing messages were encountered by about a third of respondents. 11% of smartphone users and 14% of tablet users were targeted by cybercriminals, indicating that mobile users are no longer safe from phishing scams. The vitally important issue of financial data loss affected 21% of respondents. Interestingly, a significant share of PC (13%), tablet (8%) and smartphone users (6%) admit they entered their personal data on suspicious looking websites.

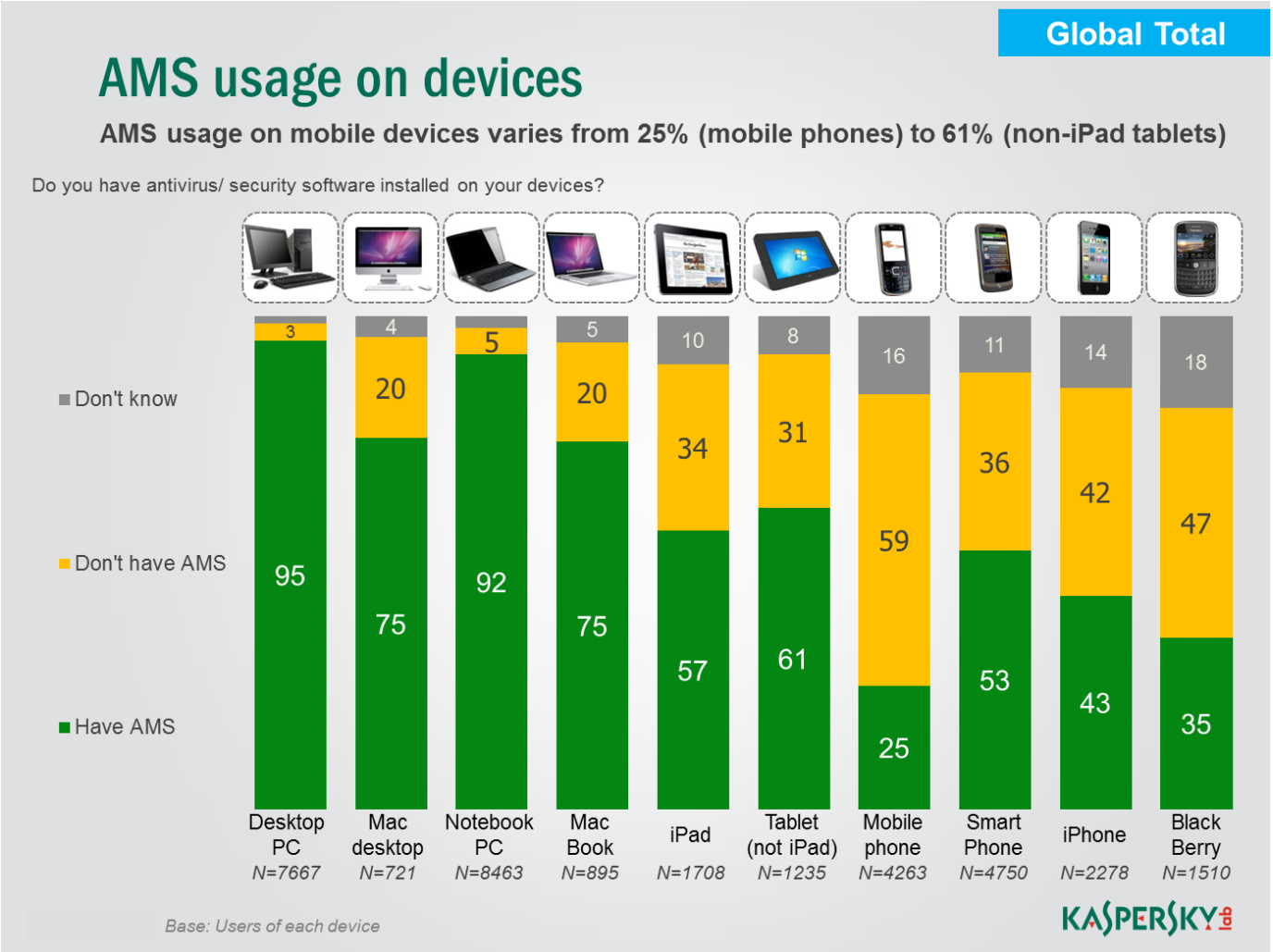
Lack of awareness about the most dangerous threats



Despite all the media coverage, almost two-thirds of respondents have never heard of such notorious malware as Stuxnet, Duqu and Zeus. Unfortunately, this also applies to today's other current threats: only 9% of respondents follow news about botnets, while just 11% look out for stories about 0-day threats. 31% and 26% of respondents respectively have heard of these two threats, but don't know much about them.

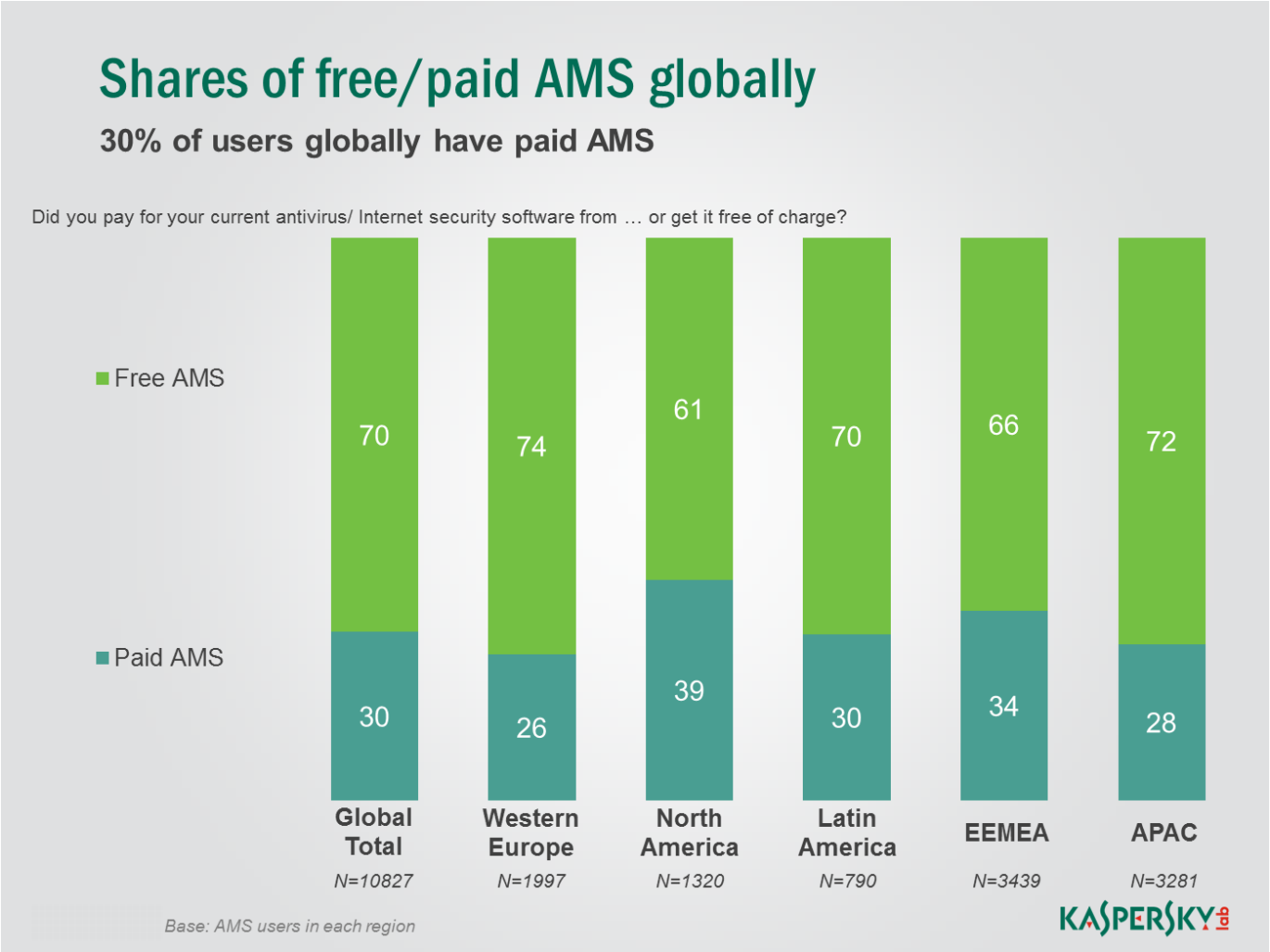
KASPERSKY lab

Usage of security software: high on desktops, low on smartphones



The overwhelming majority of Windows desktop (95%) and laptop (92%) users have an antivirus program installed on their computers – ranging from basic solutions to Total Security products. The figure for Mac desktop users is 75%. The level of security software use on mobile devices, however, is worrying: 36% of smartphone users (except iPhone and BlackBerry) and 31% of tablet owners (except iPad) do not use antivirus software. 43% of iPhone users claim to have security software on their devices, but specific features of the platform make it is impossible to create a fully functional security system.

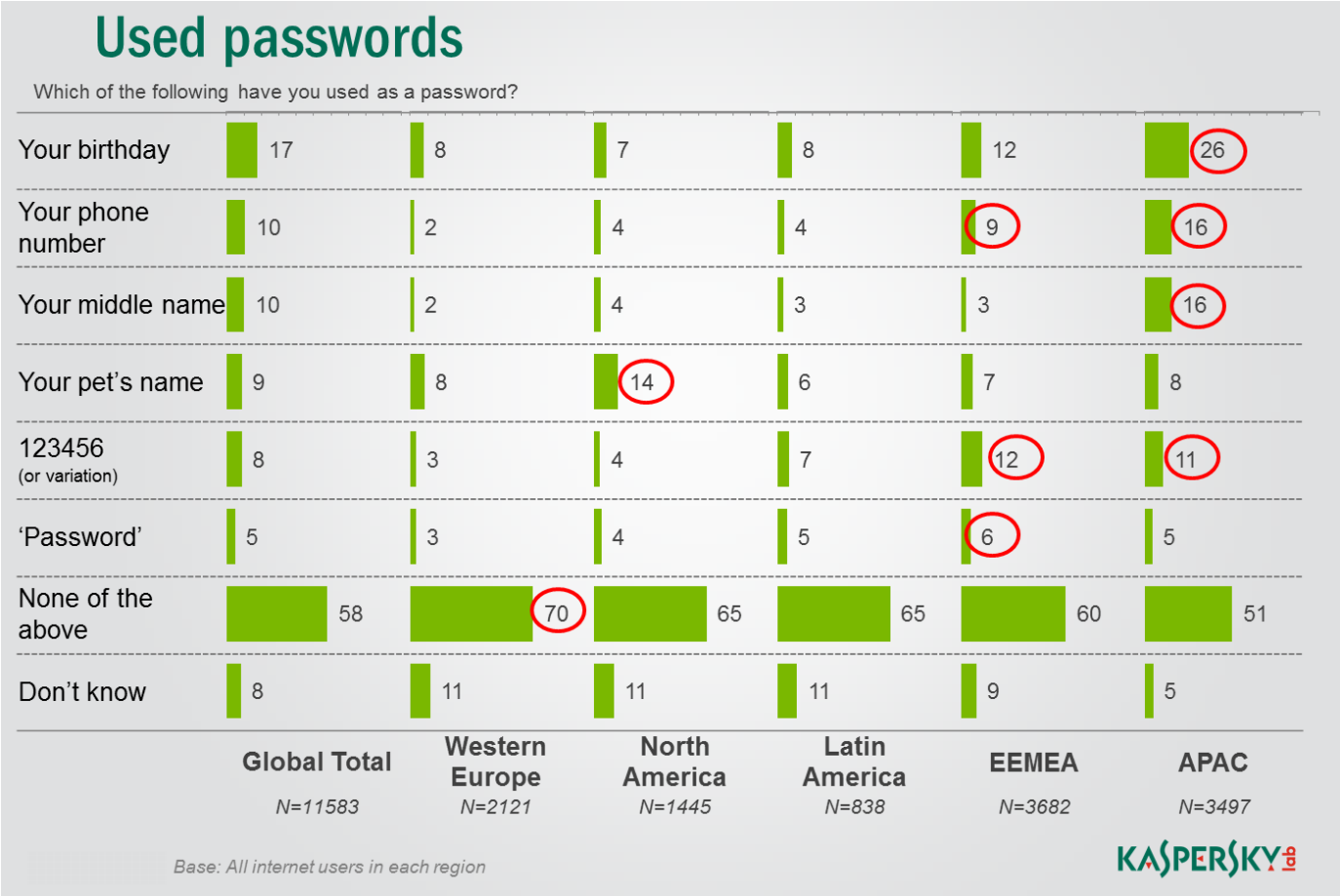
Trial and error



Despite the fact that today's Internet Security solutions are relatively inexpensive, free antivirus solutions are still very popular. According to the research, free antivirus programs are used by two thirds of users around the globe. Though the majority of free solutions provide only basic security and are incapable of blocking the most dangerous threats, a considerable amount of users think they provide sufficient security.

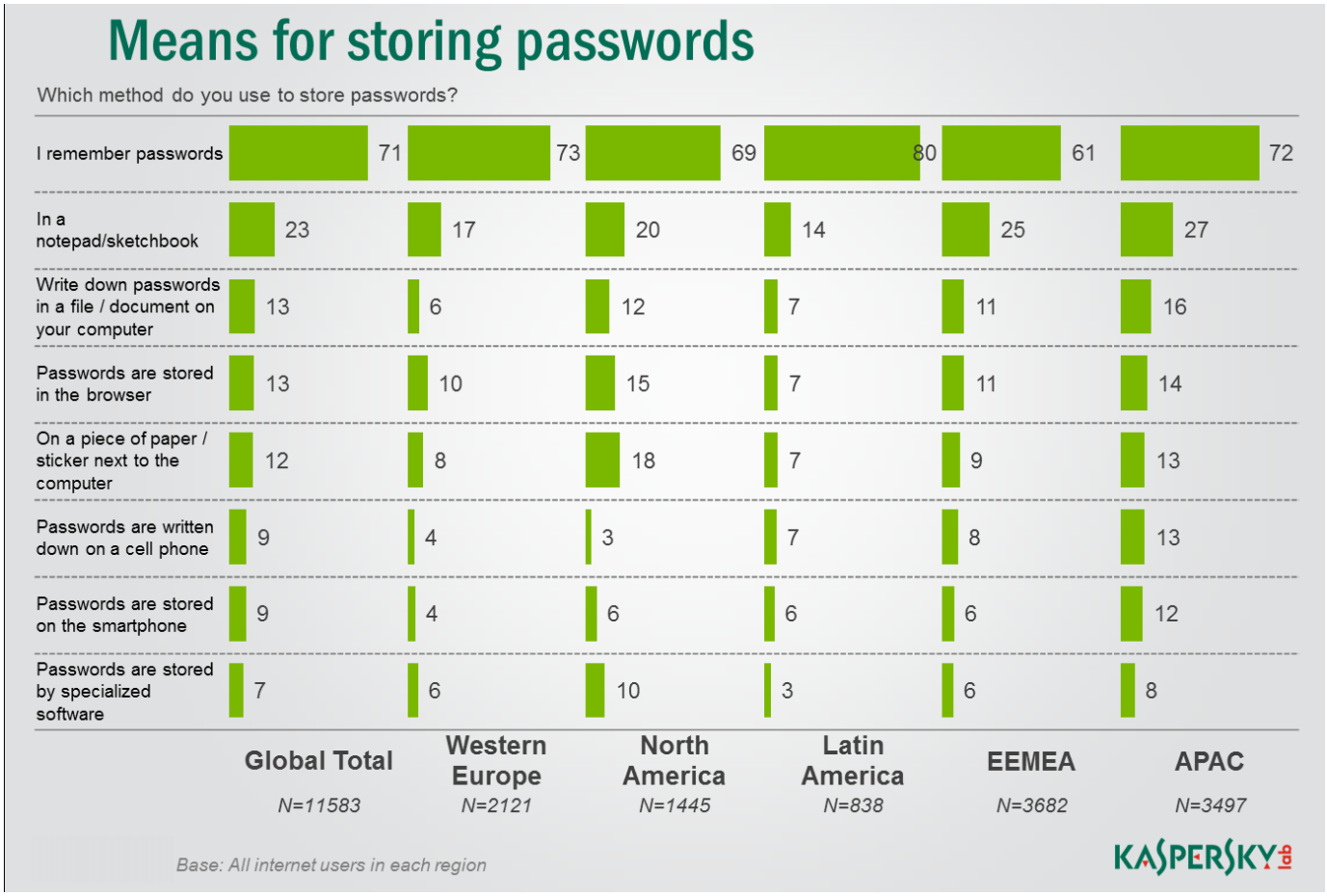
Many computers and laptops are sold with a pre-installed trial version of an antivirus program, usually of the Internet Security class. About 60% of respondents made use of these programs, but after the trial period was over only 13% purchased the license, while 30% installed a different antivirus product. On average, 2% of users take no action at the end of the trial period, i.e. their computers are left unprotected.

123456 is not the worst password



Passwords are the primary security measure for safeguarding user accounts, e.g. email. Sometimes users themselves can be guilty of extreme carelessness: 34% of those surveyed, for instance, use obvious, simple passwords. Some of them can be found on social networks, e.g. date of birth (used by 17%) or a pet's name (9%). Others use '123456' and other similar variations (8%) or 'Password' (5%), which are fairly simple to crack. Weak passwords are one of the most obvious gaps when it comes to securing user data.

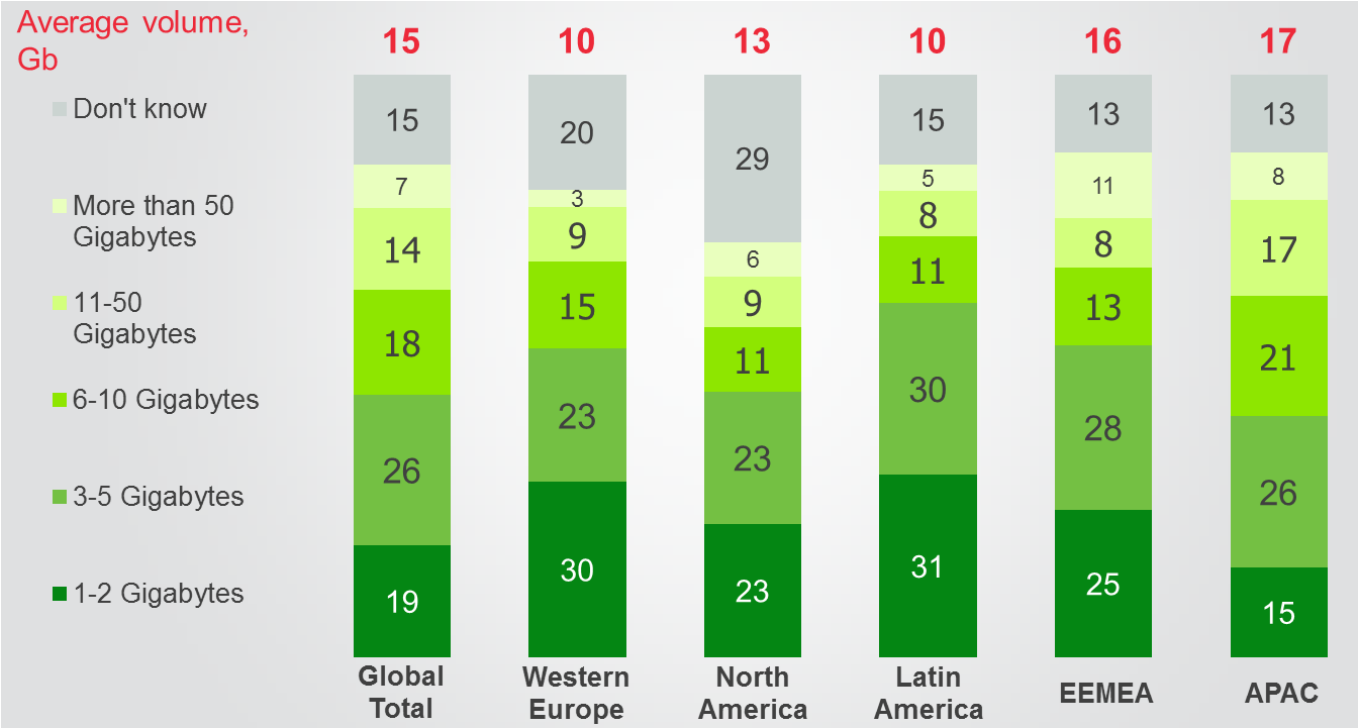
Forgot your password? Some things shouldn't be left to memory



How passwords are stored can play an important role in keeping personal information secure. The majority of users consider the most reliable method is to keep passwords in your head – this is how 71% of those surveyed store their passwords. This would appear to be the most obvious method, but it is difficult to remember a variety of passwords for different resources, and using the same password for several online services is downright dangerous. All it takes is for a cybercriminal to crack or steal the password to a single service in order to gain access to all of a user's information stored in the cloud.

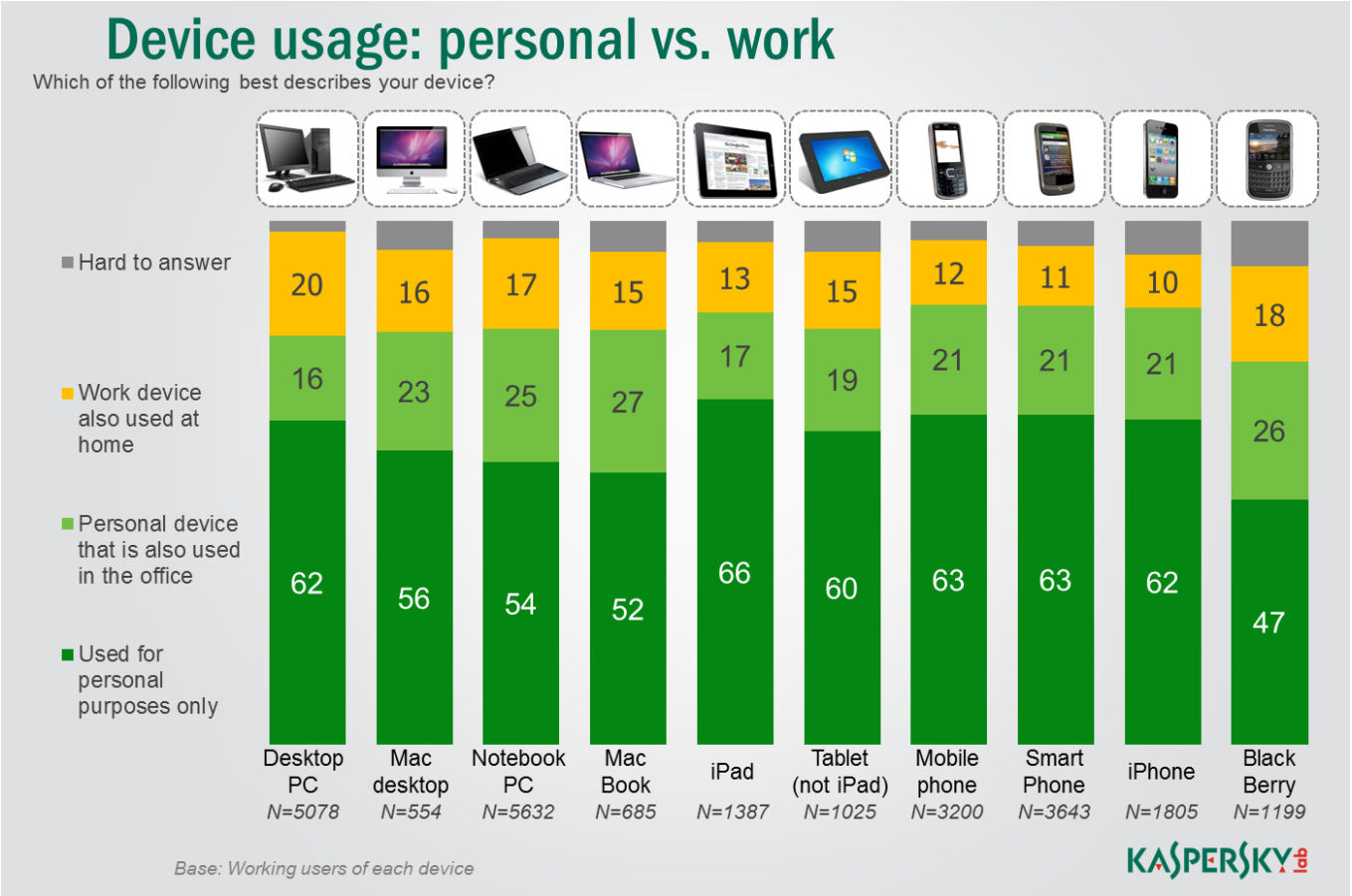
The statistics justify these fears. 34% of the respondents make use of simple, obvious passwords, and 31% prefer to use just one or two passwords for all their accounts. As a result, the level of data protection plummets. Many of those surveyed write down their passwords and keep them in easily accessible places: 12% leave bits of paper such as Post-It notes on or near their computer monitors, and 13% create a text document on the hard drive. Dedicated software for secure password storage is used only by 7%, though these solutions are capable of providing easy access to various online services and significantly enhance data security.

Cloud storage: almost as popular as email



The diversity of devices used to store personal data is supplemented with various cloud-based storage services. As it turns out, cloud storage is used quite heavily by the majority of users, with the average volume of data stored going up to 15 GB. For 45% of users surveyed, 5 GB of data is enough, although this is still a significant amount, possibly containing very sensitive information. Such active use of cloud services raises a number of questions about the security of data stored remotely. The most significant potential threats include access credentials for cloud storage being stolen and potential security issues with the cloud services themselves. Both problems can be solved by using some form of encryption, like that included in Total Security solutions.

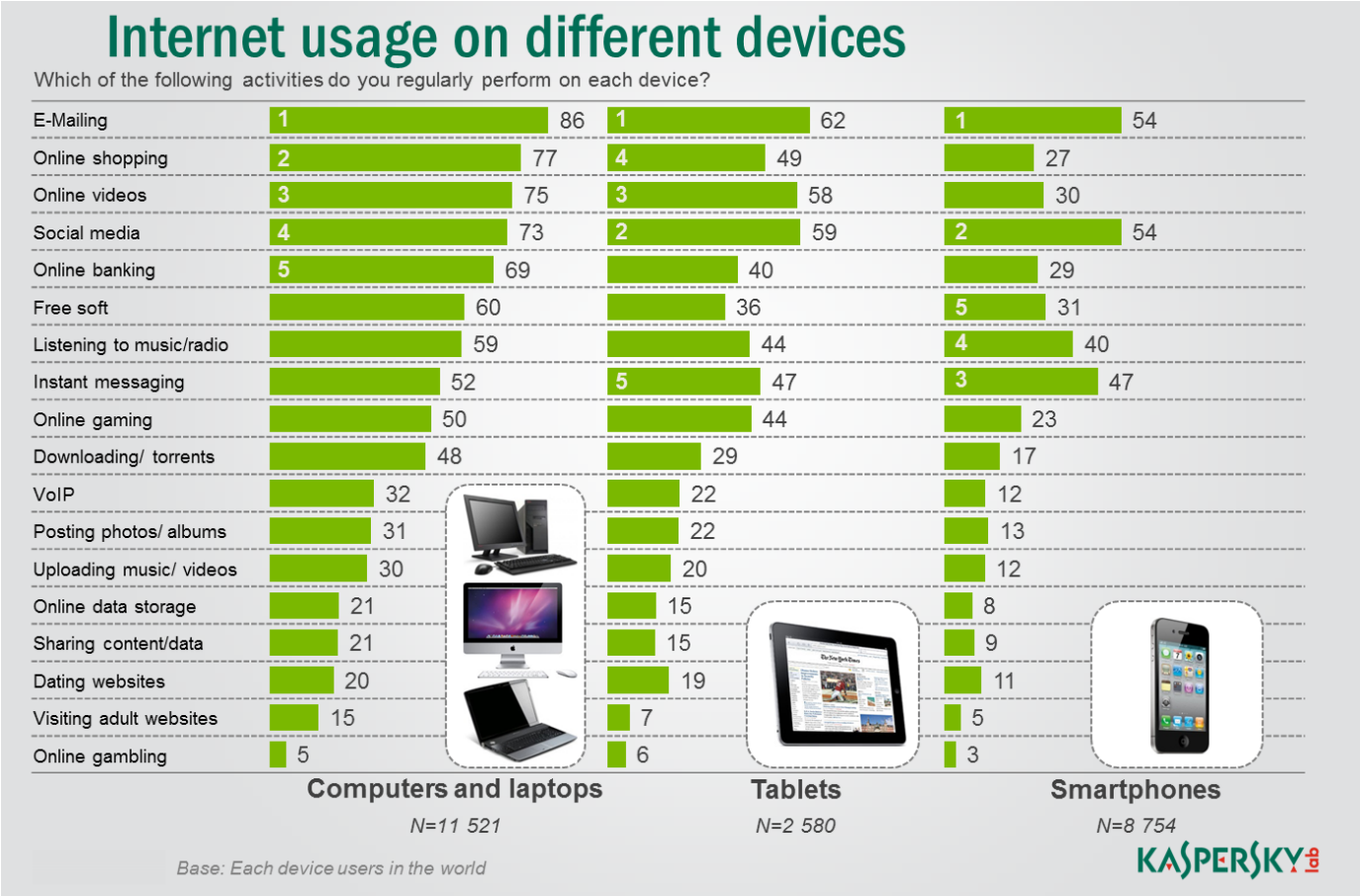
Thin line between work and entertainment



Another major security issue is the use of personal devices for work purposes and, vice versa, corporate devices for personal use. The theft of corporate data is the primary threat (if the personal device is not protected in accordance with corporate standards) as well as personal details falling into the wrong hands, e.g. if the device is sold or lost.

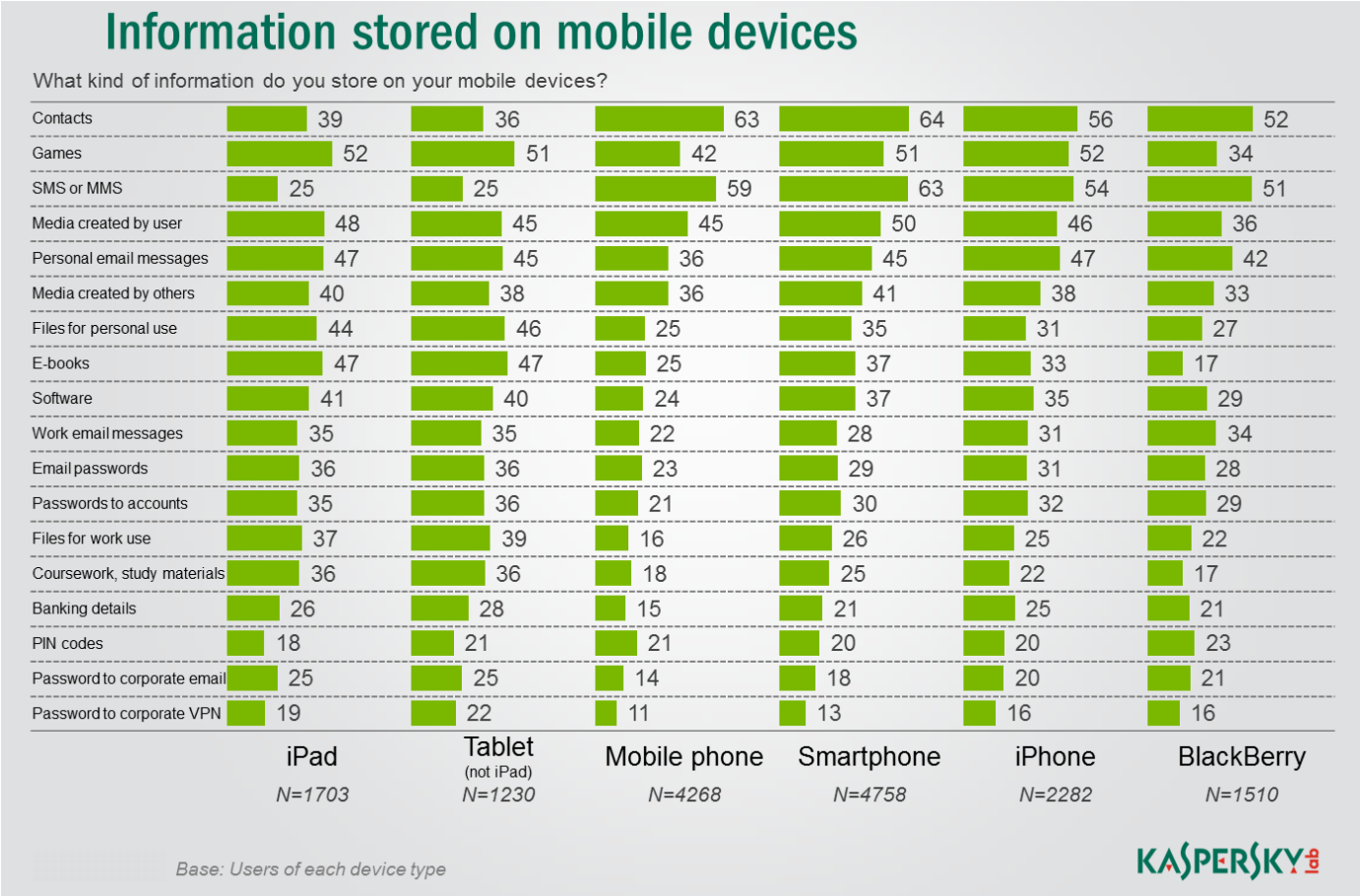
A number of users acknowledged that they store both personal and work-related data on a single device. The figure was 36% for owners of Windows desktops, while the list was headed by Mac Book owners (42%). The survey results also demonstrate that a wide range of devices – from laptops to mobile phones – are used for work-related tasks.

Online banking is on the rise, even on mobiles



Online banking (69%) and shopping online (77%) are already among the five most popular activities for desktop and laptop owners, which means we can expect to see even more banking Trojans and attempts to steal financial information in the future. Mobile device users are still lagging behind in this respect, preferring instead to use them primarily for communicating. For instance, email is used by 62% of tablet and 54% of smartphone owners, with social networks coming a close second – 59% and 54% accordingly.

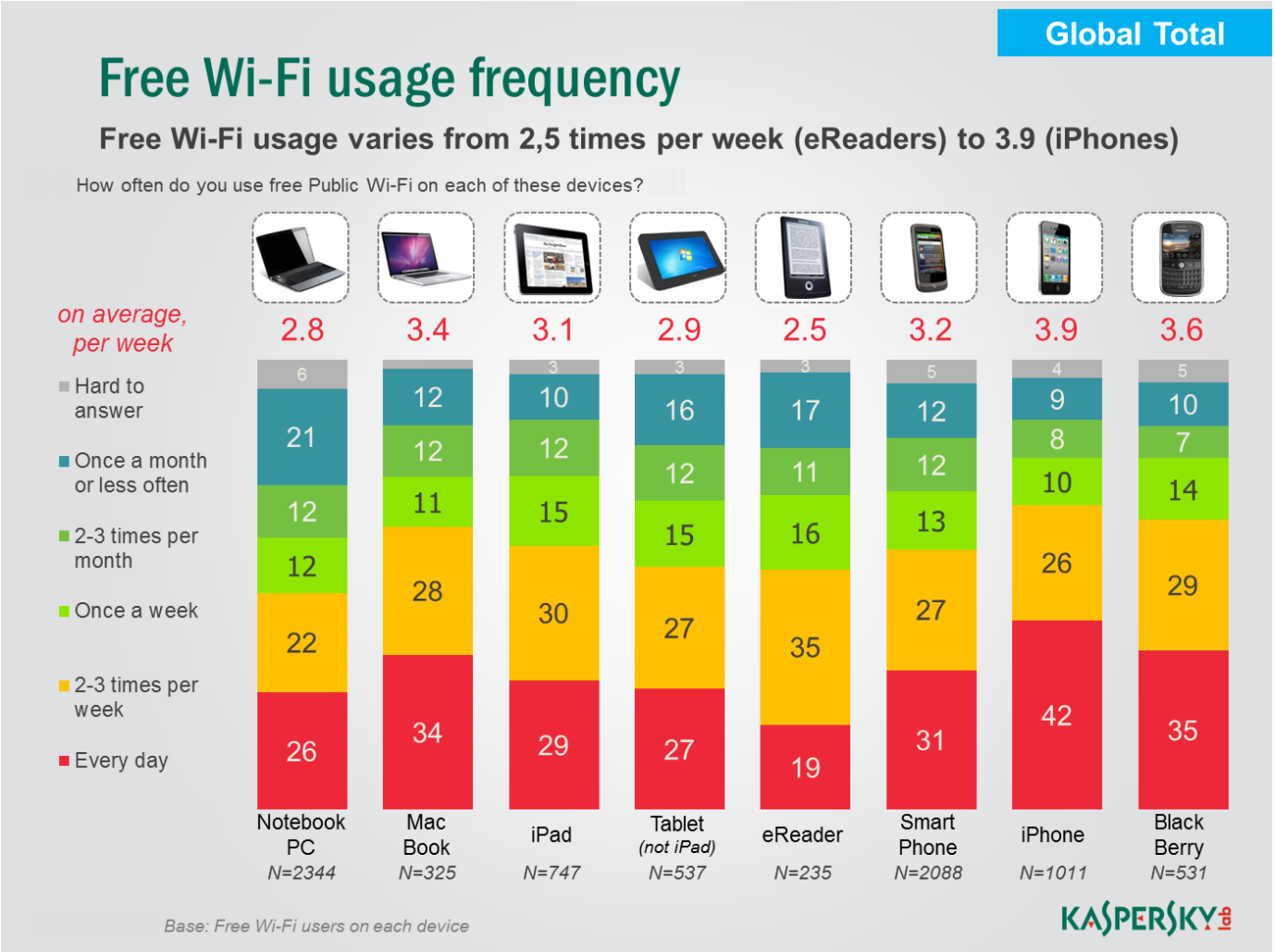
Contacts, messages and games: what's stored on mobile devices?



A significant proportion of users store sensitive data, including corporate data, on their mobile devices. 16% of iPhone and BlackBerry users and 13% of other smartphone owners store data for accessing their corporate network on their devices. Twice as many users do the same with corporate correspondence. The personal data stored on these devices often includes passwords, with a little under a third of respondents saving them to their devices – 21% of mobile owners and 36% of tablet users (except iPad). Compared to the total amount of critical data that is stored on the hard drives of desktops and laptops, these figures may seem insignificant. However, now is the time to start thinking about security software, because the amount of data on mobile devices is set to grow.

KASPERSKY lab

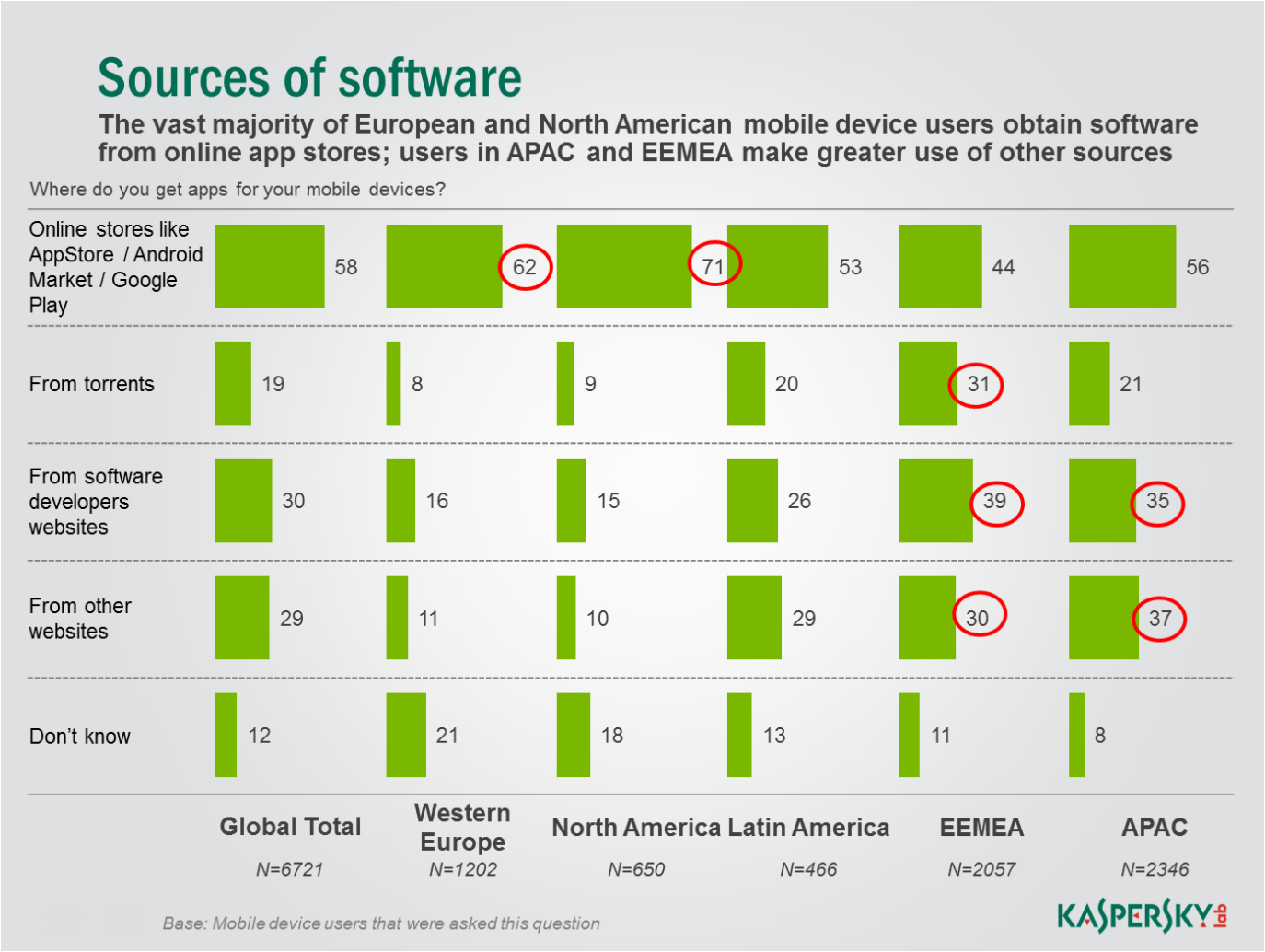
Free Wi-Fi: lax security



Wireless networks are popular throughout the world, with most Wi-Fi users (73%) accessing the Internet at home via their own personal Wi-Fi network. Public hot-spots are the second most popular, with 45% of respondents preferring free public Wi-Fi networks that often are poorly secured if at all. Moreover, on average more than a quarter of mobile device owners use these networks every day, with iPhone users (42%) leading the way. This means almost half of mobile users expose their personal data on a regular basis.

KASPERSKY lab

Sources of mobile malware: torrents and dubious distributors



Installation of software downloaded from untrustworthy sources is one of the primary causes of mobile infections. According to the survey, only 58% of users get applications from official online stores – AppStore and Google Play. An almost equal percentage of respondents use software from the developers' official sites (30%) and third-party websites. 19% of users prefer downloading software from torrent networks, exposing the data stored on their devices if they are not secured by antivirus software.

KASPERSKY lab

Conclusions

The survey shows that more and more users around the globe are aware of the benefits of antivirus software, including for mobile devices. However, knowledge of current threats leaves much to be desired. Here are the most important findings to come out of the research:

- Today's users are active online shoppers and regularly use online banking systems. The proportion of PC users performing financial transactions of one sort or another is almost equal to that of social network fans, and mobile device users are catching up fast. Therefore, both the amount of sensitive data on the Internet and the risk of data theft are increasing.

- Most users realize it is necessary to use antivirus software either as the main protection or as an extra later of security. However, almost two thirds of respondents prefer antivirus solutions that provide insufficient security. A significant number of users have bought a computer with a pre-installed trial version of a paid antivirus, but only 13% have extended the license. The situation with mobile security is far from ideal.

- The majority of respondents are careless when it comes to protecting their private data. In particular, at least a third of them use passwords that are easy to crack. Another alarming tendency is the frequent (in fact, daily) use of unsecured public Wi-Fi networks – it is the second most popular method of wireless connection, though it is the most dangerous from the point of view of security.

- Few users have a clear understanding of the dangers posed by botnets and 0-day threats. Around half of all those surveyed had been affected directly by these threats – either losing sensitive data or suffering the effects of malware.

- The research shows that users are interested in using new devices and technologies. 85% of respondents use cloud storage systems. People actively use mobile devices both for communication and for work, store important data on them and think about security. Therefore, one of the most likely prospects for the future of security solutions is the development of integrated products capable of simultaneously protecting personal data on a wide range of devices.