KASPERSKY lab

ARE YOU CYBER SAVVY?

RESEARCH SUMMARY

September, 2015

Contents

Introduction	2
Main findings	4
Section 1. Safe web surfing	5
Section 2. Digital identity protection	7
Section 3. Privacy protection	10
Section 4. Data protection	12
Section 5. Money protection	15
Section 6. Social media activity	17
Section 7. Applications usage	19
Section 8. Self–protection	21
Conclusion	24
Appendix 1	25

INTRODUCTION

On the Internet, like in the real world, habits can be either dangerous or safe. For example, it is safe to cross the road on the zebra crossing when the green light is on, but it is risky to count large sums of cash in the middle of a bar in a red-light district. However, dangers are lying in wait for us online as well as in physical reality.

Unfortunately, not everyone knows the rules of safe online behavior. Meanwhile, our inability to recognize a potential Internet threat may lead to consequences that are as unpleasant as in the real world – the loss of money or valuable things, an interference with privacy, etc.

With this in mind we carried out testing in the form of an online survey to check how cyber savvy over 18,000 Internet users are. Respondents were all over 18 years old from 16 countries around the world. The aim was to learn what their online habits were, whether they could make the right decisions about their cyber security and whether they could recognize a threat when they encountered one.

Figure 1. The geographical distribution and the number of users surveyed

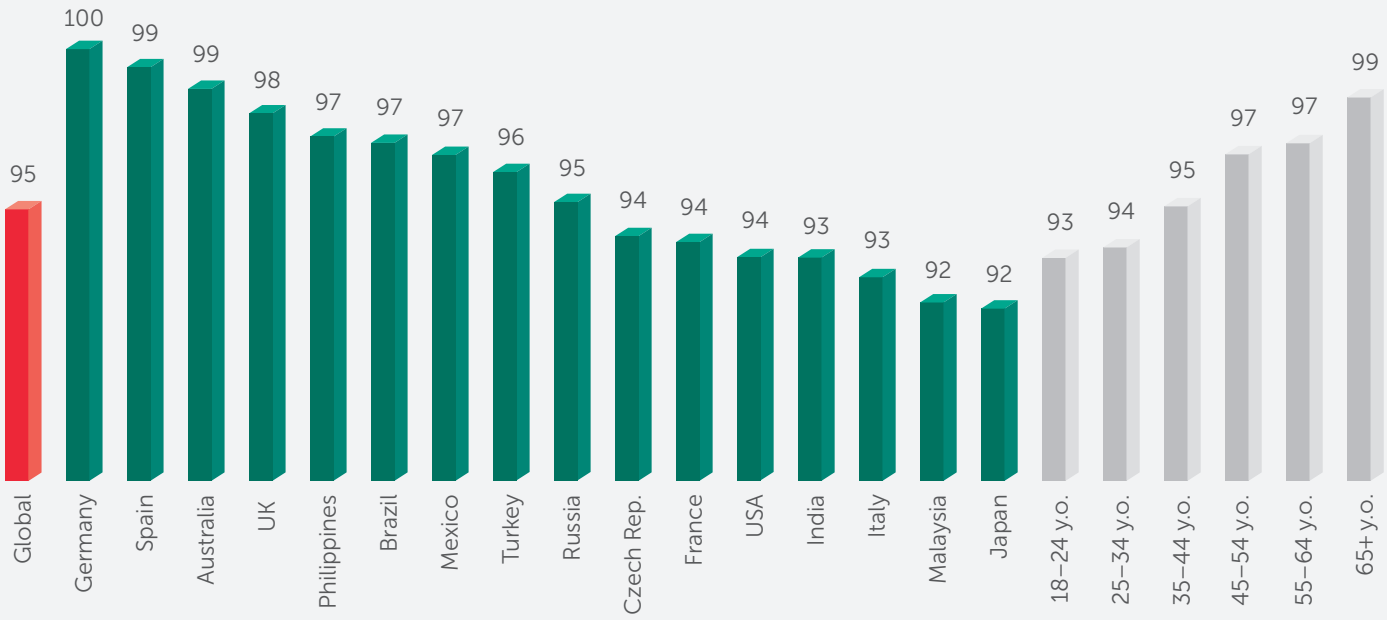
The respondents were asked to consider several potentially dangerous situations, which often occur on the Internet while users are, for example, web surfing, downloading files or using social networks (in total there were eight scenarios, which are all dealt with in this report).

Each scenario had several answers. Depending on the possible negative consequences, each answer was given a certain score – the safer the user's choice, the higher their score, and vice versa. The maximum score that the user could get was 150.

After passing the test, the users learnt their final score and thus the level of danger to which they expose themselves if they continue to adhere to this current line of behavior. Final scores were categorized based on Kaspersky Lab's experience in combating cyber threats:

- Scores over 137 — an excellent result, the lowest level of risk. The user knows the rules of safe behaviour on the Internet and makes the right decisions.
- 113–137 scores — a good result. The user makes some dangerous mistakes on the Internet but in general he or she behaves carefully and safely.
- 75–113 scores — the average level of risk. The user is able to identify only half the cyberthreats he or she encounters which means that for him or her the level of risk is high.
- Scores lower that 75 — very dangerous online behavior. The user is not able to recognize cyberthreats, he or she could not protect himself and his data from these threats and/or did not attach enough importance to this issue.

Figure 2. The distribution of the average number of scores by country and by age



The testing also included several social–demographic questions to monitor the differences in the respondents' answers related to the following factors: year of birth, gender, the device most commonly used by the respondent to access the Internet.

MAIN FINDINGS

A significant number of users were unable to identify a cyberthreat...

- only **24%** of users could identify an original webpage without selecting a fake webpage as well
- **34%** of users, instead of an audio file, were ready to download a file with an exe. extension, i.e. most likely, a malicious program

...or protect themselves...

- When generating a password, only **38%** of users thought of a new and more difficult password while **14%** of those surveyed always use only one password
- **35%** of respondents continued private correspondence in all applications available; **13%** of them did this from any available device
- only **37%** of users carefully read the license agreement before installing software; **9%** of those surveyed never read it

...being overly confident in their security.

- **29%** of respondents believe that no precaution measures are necessary when buying online, as the websites of major companies are well protected
- **12%** of users are ready to add friends on social networking sites indiscriminately, and **26%** of respondents click on the link received from a friend with no question
- **19%** of respondents would prefer to disable antivirus software if it prevents them from installing a program

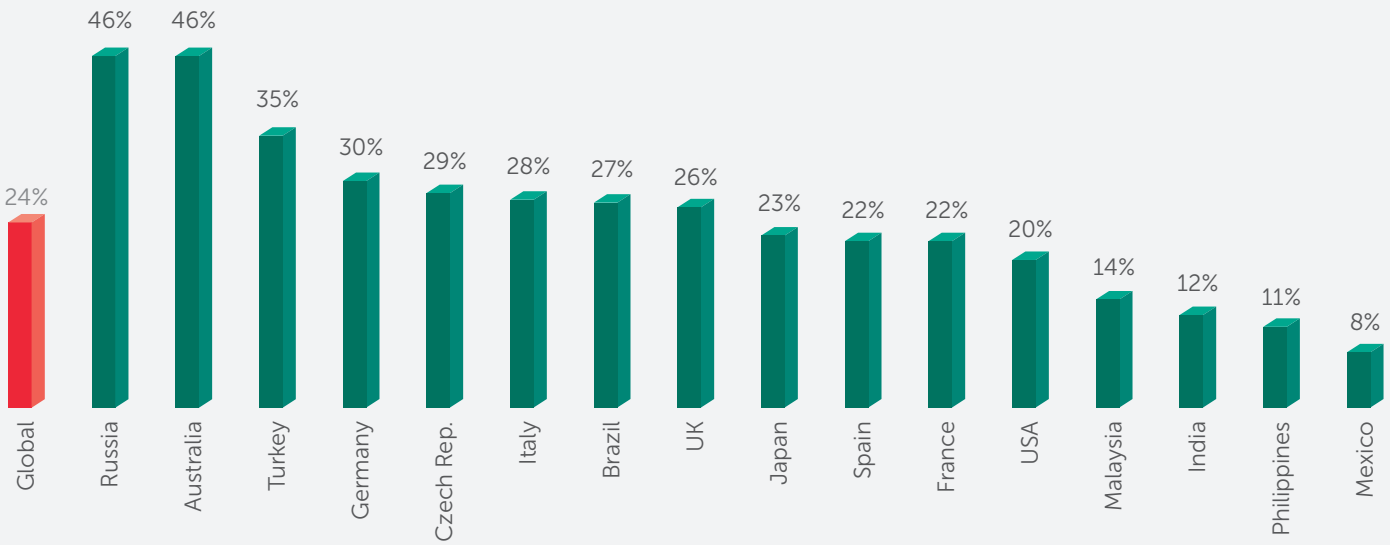
SECTION 1. SAFE WEB SURFING

Web surfing is one of the users' main activities on the Internet. However, in order to avoid falling victim to cybercriminals, the user must be sure he only opens safe pages and files.

To find out whether users can distinguish between a fake and a genuine page, we asked the respondents to choose one of four offered web pages on which they would freely enter their personal information. For each country, special samples were selected (see Appendix 1). The respondents could choose more than one page. But in fact, three out of four pages were screenshots of phishing pages detected by Kaspersky Lab experts on the Internet.

Only 24% of users could recognize the genuine page without choosing a phishing page as well. That is, only 1 out of 4 Internet users surveyed could recognize the remaining pages as hazardous. Moreover, while specifying the web pages on which they were ready to enter their data, 58% of users only named fake sites.

Figure 3. The proportion of respondents who only selected a genuine page

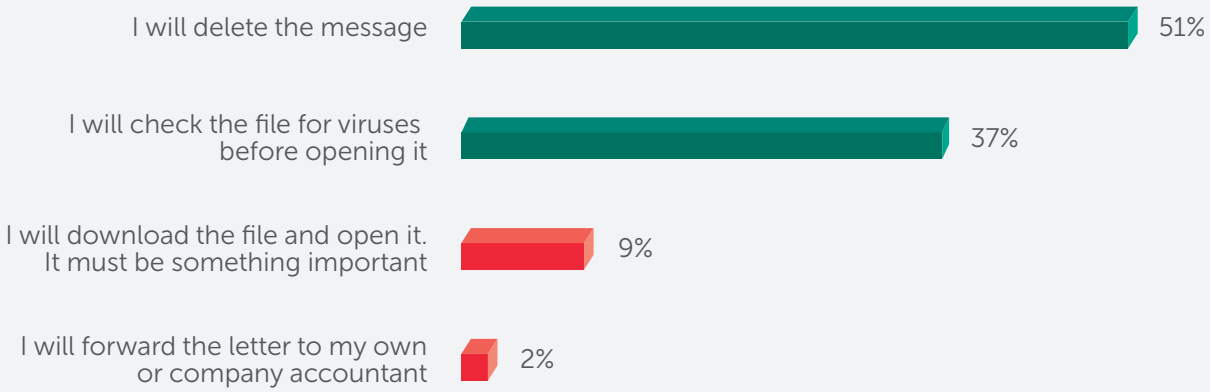


It should be noted that all phishing samples were easy to identify — in the address bar, one could easily see significant differences from the standard address which is often the most evident sign of a fake page. However, it appears that the majority of users did not have the instinct to look at the address bar when facing the web page samples.

The second task for the respondents was to select what they would do if they received an email from the 'tax office' with the attached Word document "Information about your unpaid fines." Such frightening or arresting emails often contain malware masked under common harmless formats like the text format.

The majority of users did not fall for this trick — 89% of respondents made the right decision to remove the email or check the attached file with the help of a protection product. At the same time **9% of those surveyed decided to open the attached file without checking, and yet a small portion (2%) forwarded it** to their accountant thereby expanding the range of possible infection. Interestingly, these figures were slightly higher among younger users (aged 18–24) — 12% and 3% respectively.

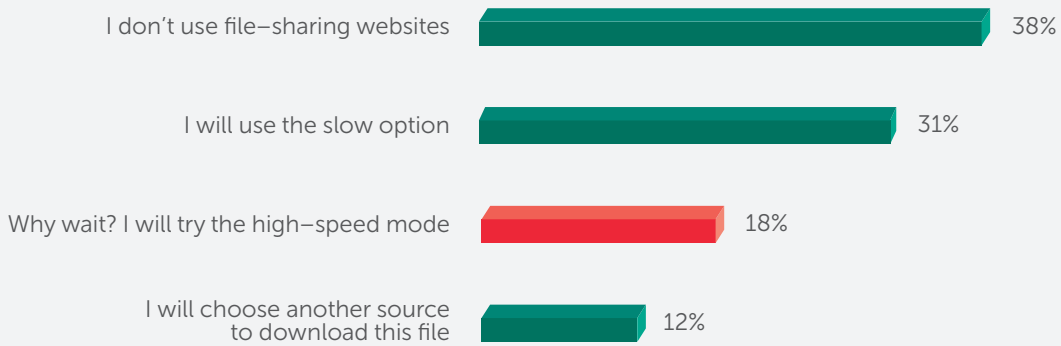
Figure 4. The variants of actions with the phishing email



The third situation was related to file sharing services, the sites which allow users to upload and download files. Many file sharing services offer the user a choice of whether to download the necessary file slowly or select the quick download mode. When choosing the second option, the user is often asked to click on an advertising link or enter his phone number or perform similar actions that carry the potential risk of infecting a device or losing sensitive data.

Almost one in five (18%) respondents preferred a quick but risky download. Young people under the age of 24 were most prevalent here: 22% of them voted for this variant.

Figure 5. The variants of respondents' actions when downloading files from file sharing services



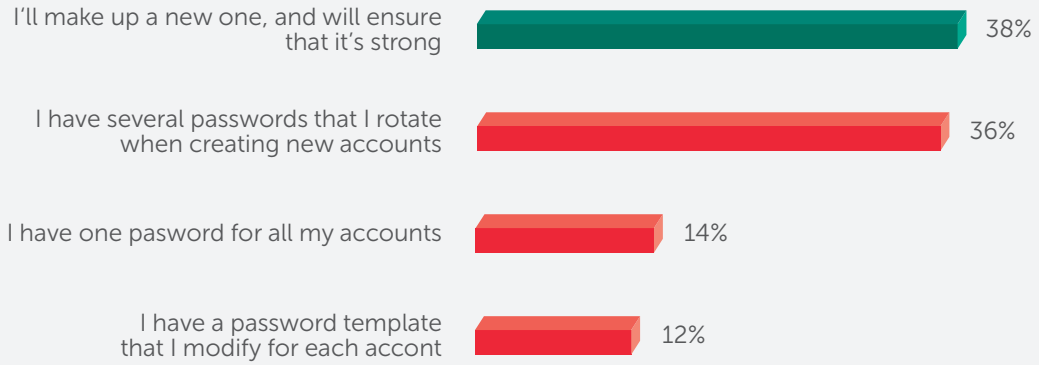
As we see from this section, in general, users demonstrate quite a good level of cyber-savvyness when dealing with e–mails and file downloads. However, when it comes to the ability to differentiate the phishing web page from the genuine page, the average user does not perform well at all. Users need to avoid falling victim, by learning to improve their instincts in this respect. If they do not, there will still be room for fraudsters to exploit the users' lack of social engineering resilience. As the list of Internet activities continues to expand, people will stray further away from their traditional domains and their safety instincts will fail them more and more often.

SECTION 2. DIGITAL IDENTITY PROTECTION

Like in the real world, you should always be yourself on the Internet. It means we must be able to protect our virtual "self", our credentials for the different services such as e–mail, IM or social networking sites from being used by someone else.

According to the results of the test, while choosing a password for a new account, **only 38% of respondents thought of a new and more complicated combination.** At the same time, 36% of those surveyed used a limited number of passwords; 12% of people use variations of one password pattern to create a new password while **14% of users admitted that they had one password for all occasions.** Thus, 62% of respondents are at risk: the leak of one password may lead to the simultaneous crack of several accounts.

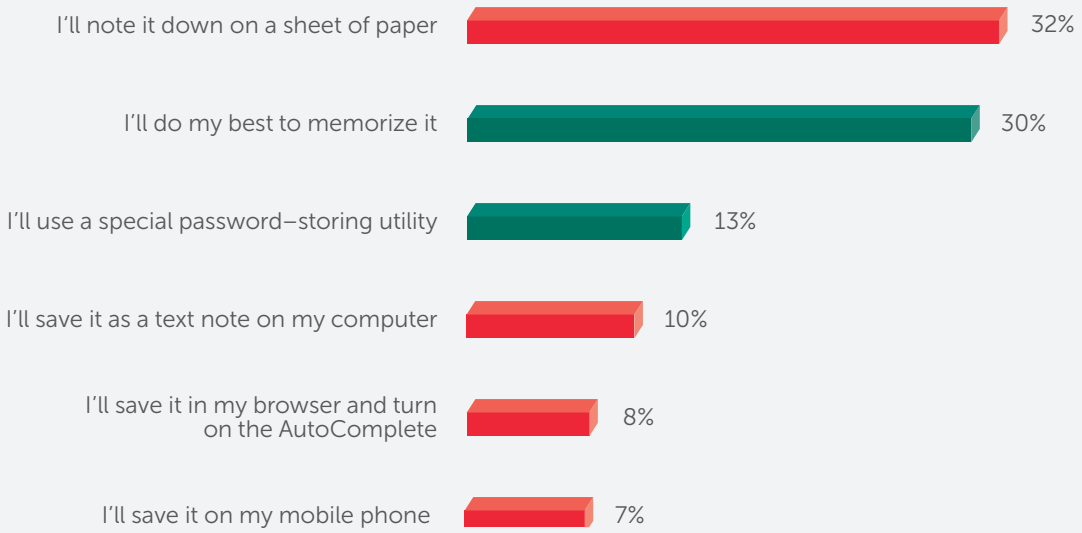
Figure 6. Principles of generating passwords for new accounts



Interestingly, the older the respondent, the greater the willingness to create a new and complicated password. Only a third of young people are ready to come up with a more complex password while among older users this figure exceeds half.

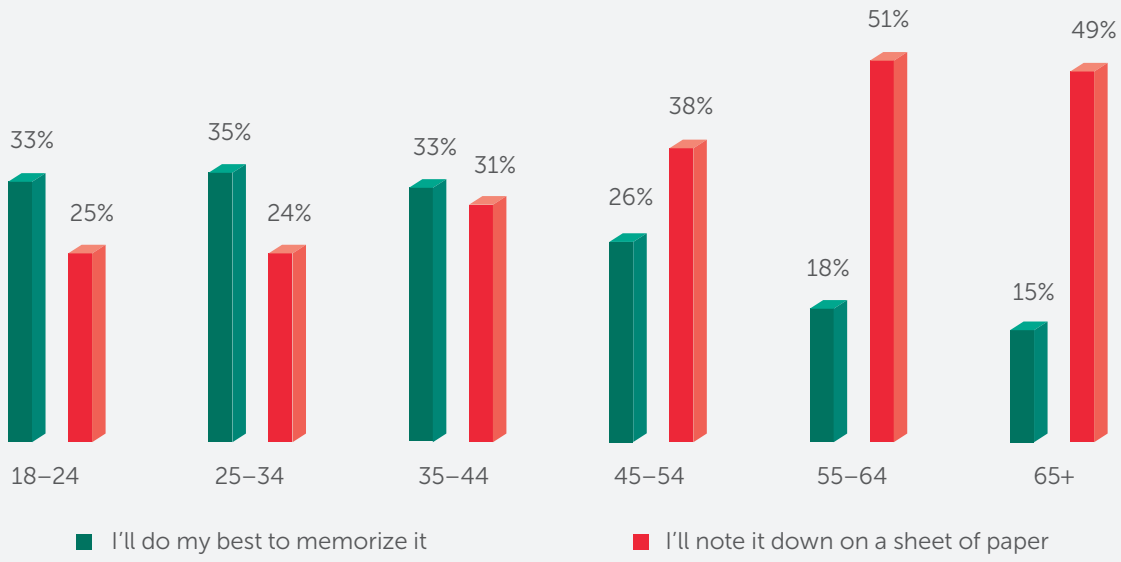
In addition, 57% of respondents choose insecure methods of storing passwords, and put them at risk by writing them on paper, saving them in the browser or on their mobile phone, etc.

Figure 7. Ways of storing passwords



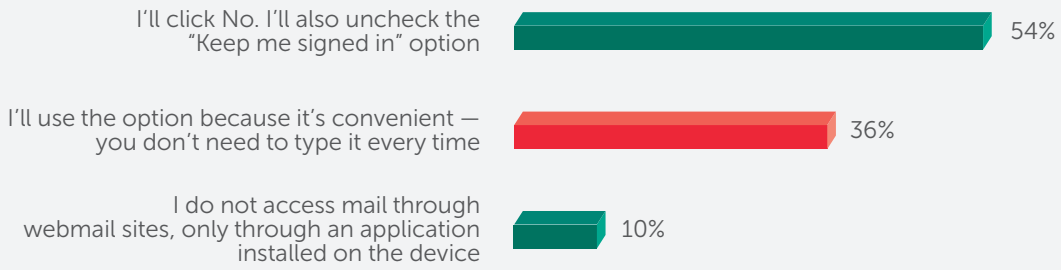
Despite the fact that older users tend to create complex passwords, they rely less on their memory and often choose the simplest and most unsafe methods of storing them.

Figure 8. Ways of storing passwords by age



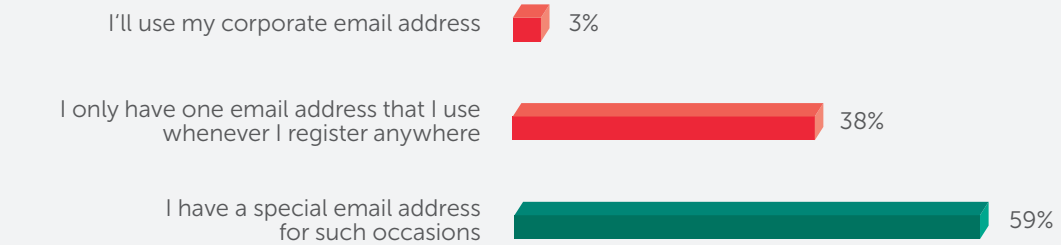
If the browser offers the respondent the chance to save their login and password, 36% will agree, thus playing into the hands of cybercriminals or dishonorable people who could get access to their device.

Figure 9. Automatic account specifications selected for the browser



38% of respondents use one email address for all occasions, even for a temporary registration, for example, on the site of a pizza delivery service, as proposed in the framework of this test. The majority of those surveyed (59%) protect themselves by creating a special address for such cases while 3% of users are ready to specify their corporate email address for this purpose.

Figure 10. The readiness to specify email address for temporary registration



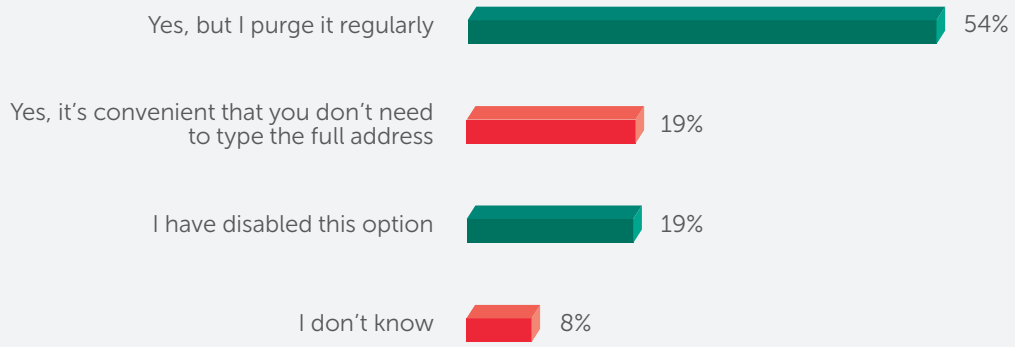
The testing has shown that many Internet users do not effectively protect their accounts from unauthorized access. Choosing complex passwords and reliable ways of storing them is a contribution of cyber savvy users both to their own and to their friends' security. Stolen profiles can be used to track users, to steal their data, to send spam and malicious files.

SECTION 3. PRIVACY PROTECTION

With the development of the Internet, the concept of privacy protection has an expanded reach. Now, what the user does, what he or he is interested in, who and what he or she communicates, i.e. his personal life, has been entrusted to digital technology. The ability to protect your privacy is a special skill that every Internet user should master.

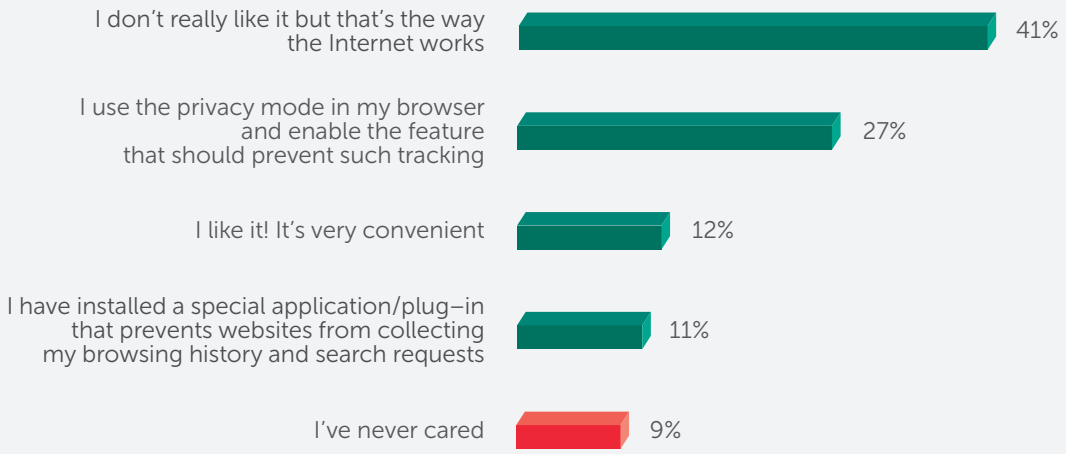
For example, **8% of respondents do not even know whether the browser stores their history of visiting web pages.** Meanwhile, this information can be used to spy on the user.

Figure 11. Storing the history in the browser



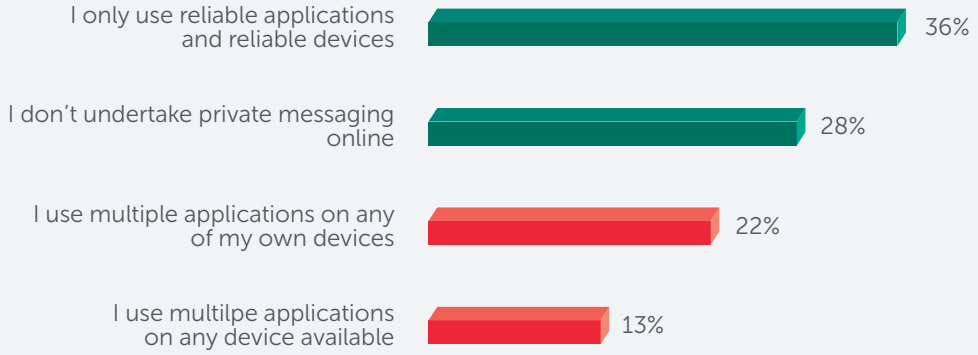
This test also shows that 9% of users have never thought about the fact that the sites they visit not only automatically determine their location but also offer advertising based on what sites they visit and what words they are looking for in the search engines. While 12% of respondents find this practice convenient, **41% of those surveyed are not satisfied but do nothing to protect their privacy** because "that's how the Internet works".

Figure 12. The attitude of users to tracking by web sites



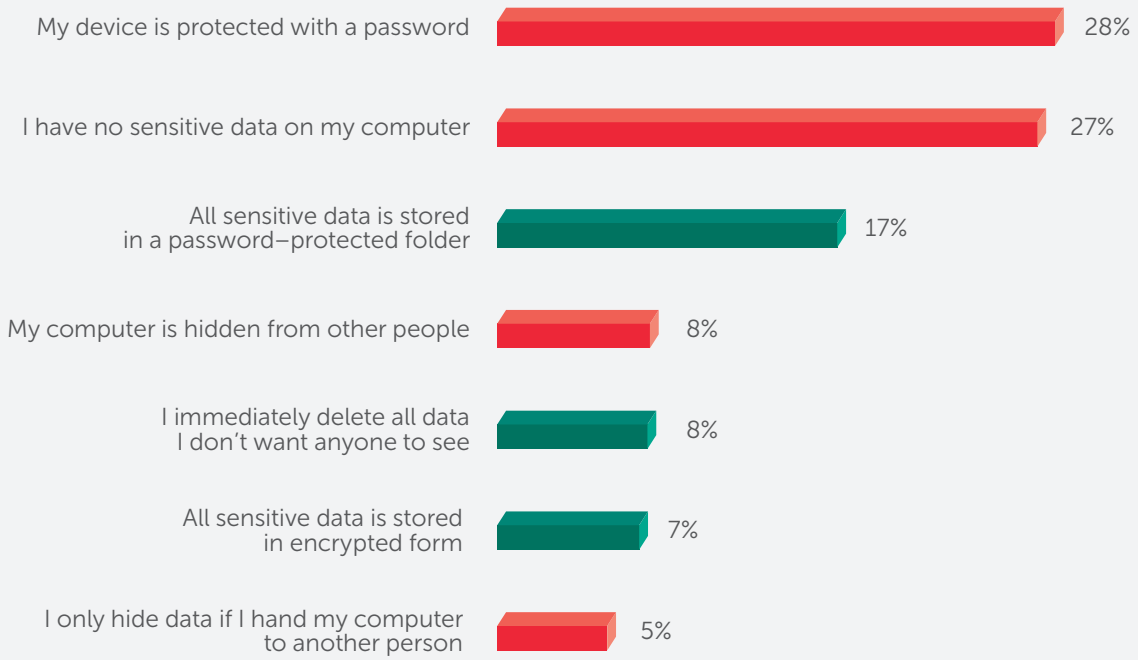
35% of respondents carry on private correspondence in all available applications and 13% of them do it from any available device, not just from their personal one. And less than one–third (28%) of users are aware that these communication channels may be vulnerable to interception and do not discuss personal matters online at all.

Figure 13. Applications used for private correspondence



Every Internet user is the owner of confidential information about himself – the history of their online activities, personal contacts, files, passwords, and so forth. All of this data requires additional protection from possible access by other people or cybercriminals. However, **27% of users believe that their computers have no confidential information.**

Figure 14. The answers to the question "How is the information that you would not want to share with anyone stored on your computer?"



Unfortunately, neither protecting the device with a password (selected by 28% of users) nor hiding the device from other people (8%) can secure your data from intrusion using digital techniques — Wi–Fi traffic interception, malware implementation, etc. can all play a part here. More reliable methods include the removal of all data not intended for prying eyes (8%) as well as the creation of password–protected (17%) or encrypted (7%) folders.

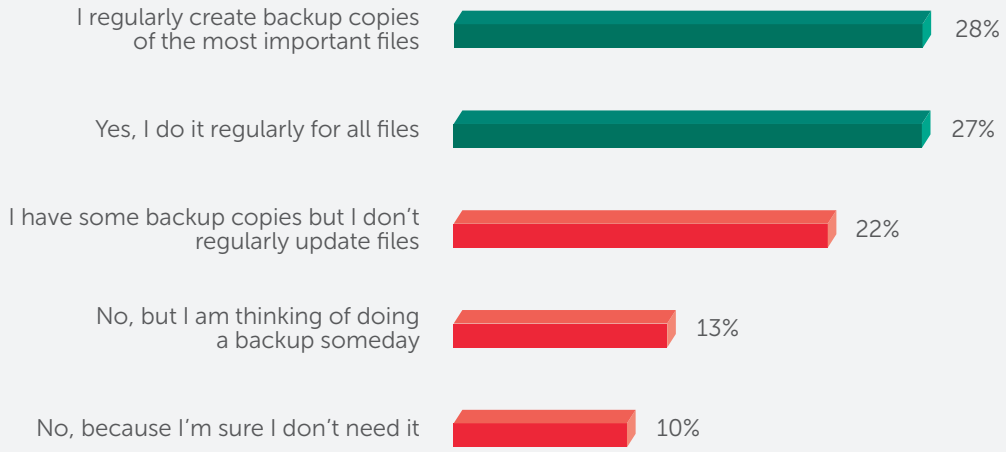
Today, we each create a digital shadow, which contains information about who we are. This shadow includes our online credentials, accounts, logins and passwords, where we are, what we have done, and who we have communicated with and how. Although users show an overall understanding that this data exists, they tend to underestimate its value to third parties, such as advertisers or criminals. It is vital that we learn to protect our digital shadow with cyber–savvyness and specialist tools. This is a skill that all Internet users should master, although it is currently strikingly low among users.

SECTION 4. DATA PROTECTION

Currently people are creating more digital content than ever. Terabytes of new data fill the Internet every minute. Photos, documents, notes, video and audio files of various types are stored on the devices of Internet users. But the digital world is unstable — devices break down, cybercriminals encrypt user files for ransom or steal them for the further use, and all these threats require certain protection skills from the users.

We asked the respondents whether they back up their files in case their device is lost. The survey shows that **23% of users do not make backup copies at all and one in ten respondents do not consider it necessary.**

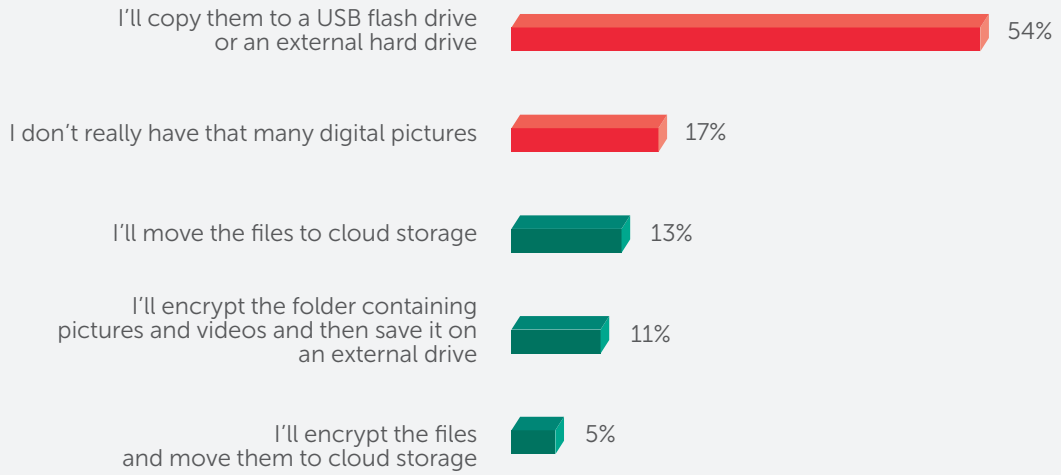
Figure 15. Backup copying



In a hypothetical situation, when there is lack of space on a device for photographs and video, **half of the users (54%) will prefer to copy them to external media.** However, this method can hardly be considered the most reliable as external drives are often lost or broken. If the disk is lost, the user's data is at risk of falling into the wrong hands. To avoid this, 11% of respondents encrypt their data before copying it to the disc.

Moreover, 17% of users believe that copying backups is not necessary because they have few photos. However, the devices on which these photos are stored are as vulnerable as external drives. The best solution in this case is to make a backup copy in the cloud – cloud services usually have a more reliable storage system. However, depending on the cloud service, data encryption may also be useful. This variant was only selected by 5% of respondents.

Figure 16. The solution for the problem with the large number of photos and video files



The respondents were also asked which sources they use for downloading files — programs, movies, books, games, etc. It was found out that **one in five (21%) users download files from a variety of sources running the risk of encountering an unconscionable supplier.**

Figure 17. Sources for downloading files

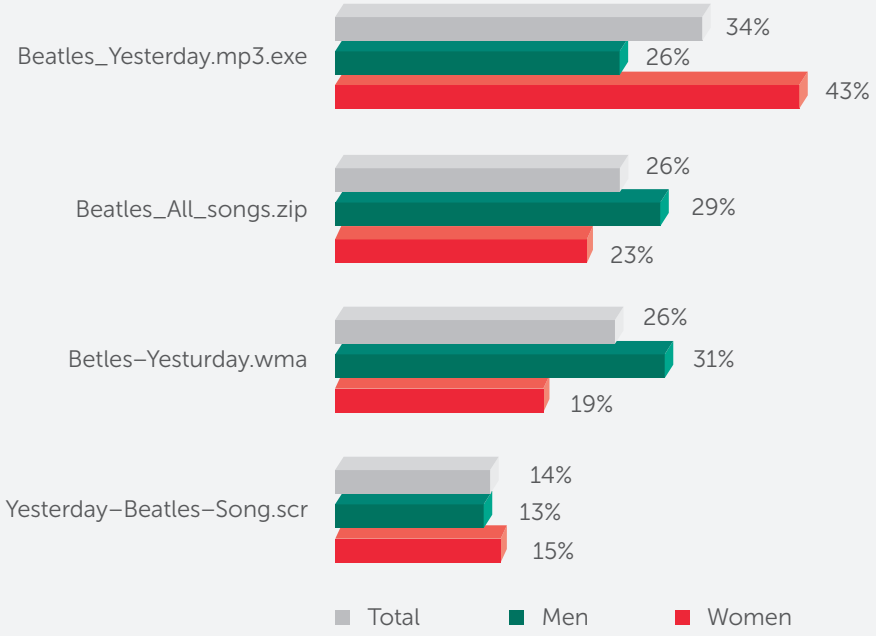
Interestingly, men make backup copies and select reliable methods of storage more often than women. At the same time they are less careful about the sources from which they download files (25% of men vs.17% of women). The trend shows that the younger the respondent the more often he or she downloads files from any resource: 31% of users under 24 vs 6% of those aged 65+.

The respondents were also asked to test themselves by downloading one of the versions of the Beatles' song "Yesterday," allegedly found on the Internet on their devices. Only one out of four files had the secure extension while the remaining three files could hide dangerous content instead of the well-known song. The task was to detect the safe file evading the tricks of a potential fraudster. The task was complicated by writing the only safe file with misprints while the most dangerous file contained the popular mp3. extension in its name.

As a result, only 26% of participants could choose the right file – the one with the wma extension (Windows Media). Another 26% of respondents preferred the archived zip folder which, in addition to audio recordings, could contain unpleasant surprises. 14% of those surveyed chose the file with the scr extension (i.e. the screen saver rather than the audio recording), which is yet another file format used by cyber criminals to deliver malicious software to a user device.

The most dangerous thing is that **instead of music the majority (34%) of the respondents were ready to download the file with the exe extension, i.e. the executable file that is most probably a dangerous program.** This variant is preferred mostly by women. The files with the scr and exe extension were chosen by the older respondents while the younger participants tended to choose the zip and wma files.

Figure 18. The variants of the song for downloading



Although there is a noticeable group of users that are totally careless about their digital memories, the majority of respondents do understand the unreliability of digital storage media and recognize the need to backing up at least the most important files from time to time. However, when we test the users in scenarios when they are offered the chance to download a file, they demonstrate that their level of cyber threat awareness is much lower – this means that there is a significant risk of them losing their digital moments forever.

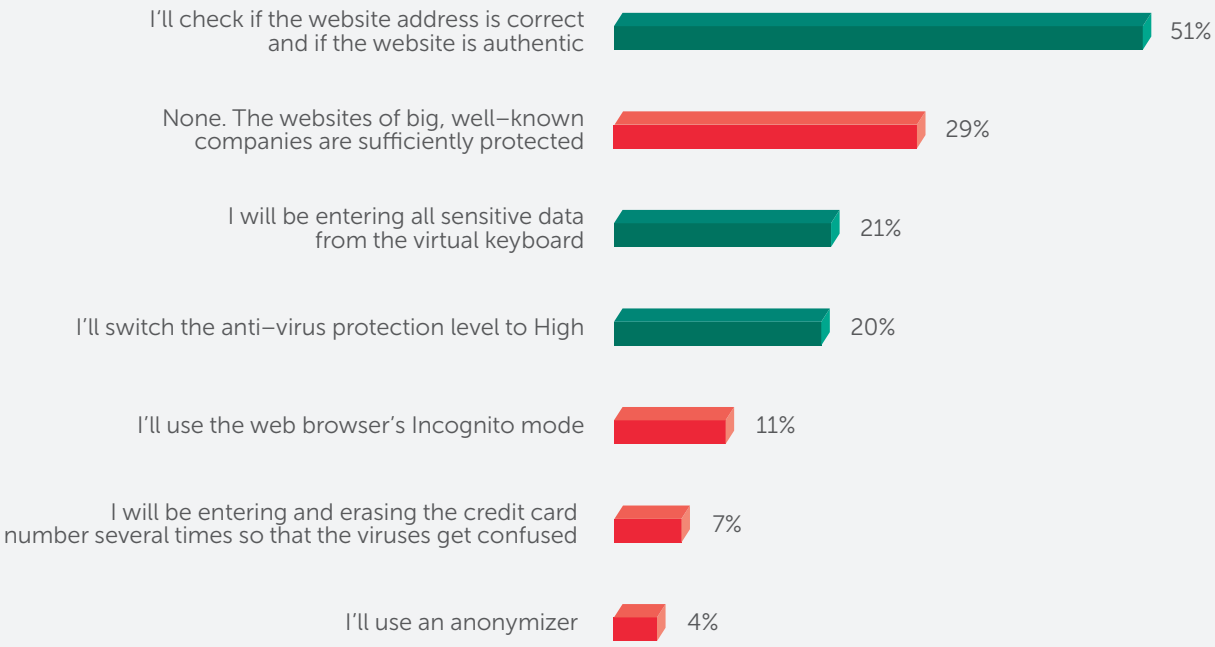
SECTION 5. MONEY PROTECTION

As it turned out during testing, **the majority of respondents (86%) from time to time make online purchases paying for goods and services via the Internet.** At the same time, nowadays the theft of money by means of digital technologies is not an episode of the science fiction movie but a harsh reality. To protect their bank accounts from fraudsters, users should both use safety solutions while making financial transactions and be able to identify a potential threat.

For example, 86% of those surveyed were asked to choose the precautions they would take when entering the bank card data while making an online purchase. They could choose several options. According to their answers, half of the users (51%) thoroughly inspect the site — this is the right decision. Only 21% of respondents will enter the data from a virtual keyboard that avoids interception by special malware if the computer is infected. Another 20% of users will make sure that the security solution is enabled to protect them.

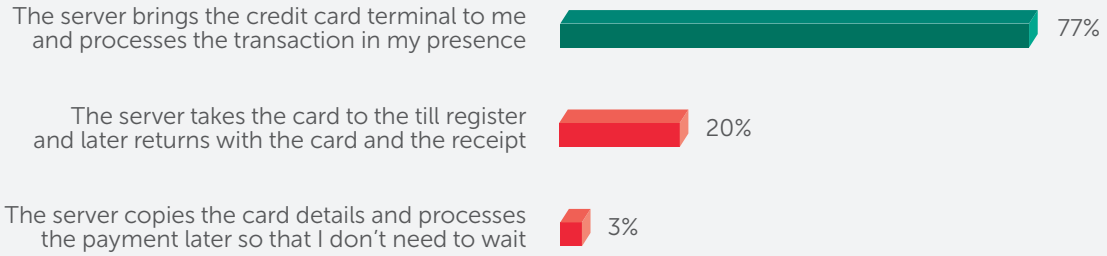
29% of respondents believe that no precautions are required when making e–payments, as the websites of major companies are well protected. However, a protected site does not guarantee that the data will not be intercepted on the compromised device of a user. 11% of users are plan to use the "incognito" mode in the browser, and 4% of respondents think of the anonymizer, although these measures cannot help protect financial data from either interception or malware. 7% of those surveyed chose a humorous version — attempting to confuse viruses by entering numbers several times.

Figure 19. Precaution measures taken while making an online purchase



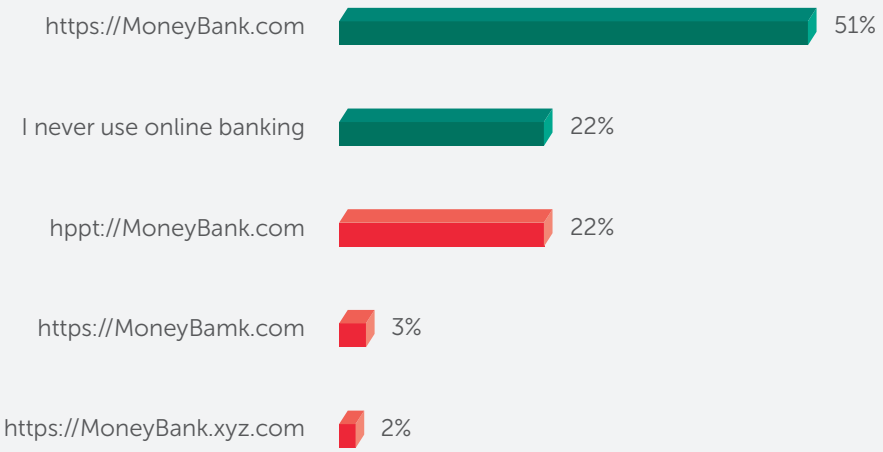
Yet another common method of financial fraud is the illegal creation of a credit card copy. Fortunately, the majority of users (77%) do not want to lose sight of their credit card and in a hypothetical situation of paying by credit card in a café, they expect the waiter/waitress to bring the credit card terminal to them, so that they can process the transaction in their presence, rather than taking the card to the till register. However, 20% of respondents do not mind such a scenario, and 3% of users will share a copy of their financial data with the waiter/waitress.

Figure 20. Preferred way of paying by credit card in a cafe



The respondents were also asked to enter their data on the site of an imaginary bank called the Money Bank by selecting an appropriate web page. The safest variant with the correct address and the encryption necessary in such cases (the https prefix instead of http) was chosen by 51% of respondents. At the same time, **one in five (22%) of respondents chose the page with unencrypted traffic,** a page potentially vulnerable to interception. Another 5% of respondents chose a fake page with the distorted address.

Figure 21. Variants of a hypothetic bank page



Online banking, online shopping and financial transactions are becoming part of daily life for many people and this is making us careless. We trust the websites as we trust the high street store, and that trust can be exploited by others. Most of us see what we expect to see, assume that we could not possibly be a target or that someone else will pick up the tab if we are.

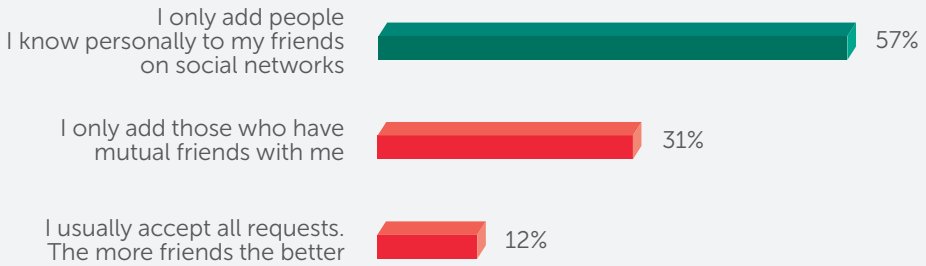
As these results show, a significant percentage of users trust the Internet more than they should. The inability or unwillingness to choose a safe site for financial transactions as well as an unreadiness to use effective tools to protect them makes users vulnerable to cybercriminals.

SECTION 6. SOCIAL MEDIA ACTIVITY

Social networks today are more than entertainment or web surfing. A page on a social networking site is the official representation of an individual Internet user, a huge storage of personal information. **78% of the «Are you cyber savvy?» test respondents use social networks.** However, a social network does not only unite and inform, it is also be a useful tool for cybercriminals.

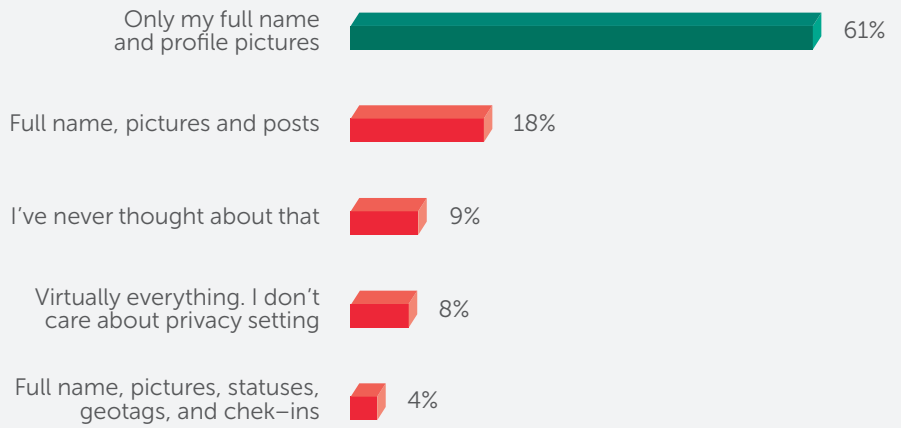
For example, **12% of those having a page on a social networking site are ready to add almost everyone as friends, and another 31% of respondents will add strangers as friends if they have friends in common.** These friends in common could also accept an invitation from a stranger. Only slightly more than half (57%) of users are careful about who they add as friends. Moreover, with age, this percentage increases to 52% among the youngest respondents and to 77% among the oldest.

Figure 22. Adding friends in social networking sites



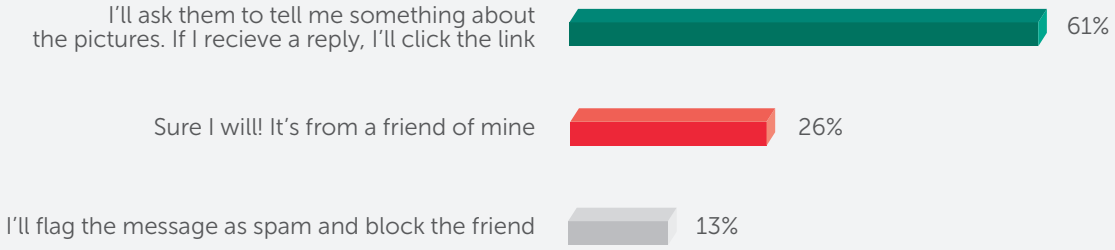
About the same number of cautious users (61%) open only the name and the profile photo of people for public viewing. **30% of page owners are ready to share their posts, location, etc., that is, the information about their private life, with everyone.** Moreover, 9% of respondents do not even wonder about what others see on their page; the percentage of older users sharing this approach accounts for 14%.

Figure 23. The information on social networking sites that is open for public viewing



Having received a link from a friend asking to view some photos, one in four (26%) respondents will click on the link without any doubt. So, if their friend's page is compromised, these 26% of users will follow a malicious link and most probably get their device infected. Only 61% of those surveyed will make sure that it is not spam, while 13% of respondents will solve the problem radically and block such a friend.

Figure 24. The reaction of a user to his social networking friend's request to click on a link and Like a photo



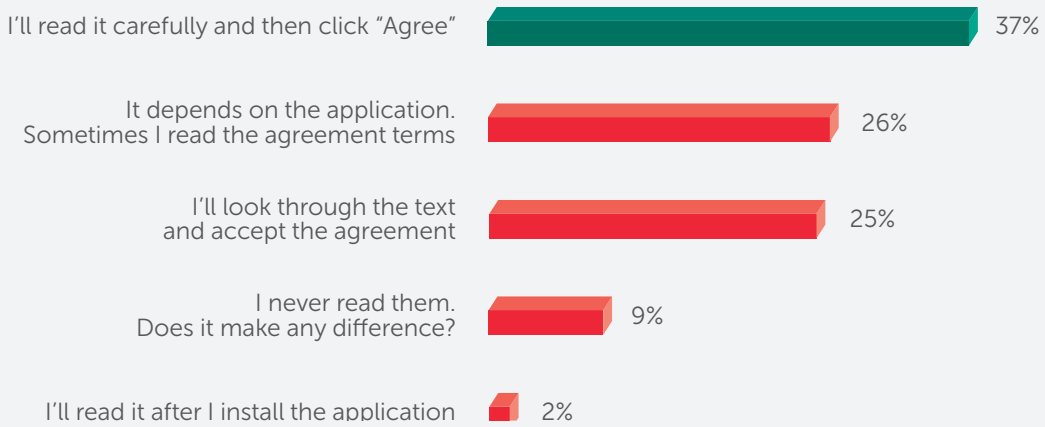
Social networking sites are where we leave information about ourselves — our digital shadow. Once they have cracked a user's page, cybercriminals get the chance to publish advertisements on his behalf, send malicious links to his friends, or use his personal information for their own purposes. Each user of a social networking site should be ready for this and follow some simple rules: for example, not add to friends all in a row, not disclose too much personal information and not to click on all links received from his friends.

SECTION 7. APPLICATIONS USAGE

Sometimes, an application does not need to be hidden malware to create problems to Internet users. Even relatively legitimate applications may collect information about their owners, change the settings without their awareness or show unexpected adverts. However, a user can reduce the probability of such actions if he is careful while installing applications on his device.

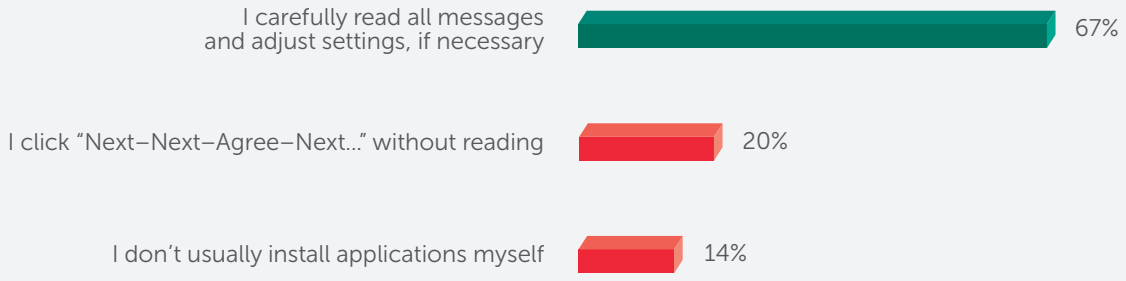
For example, **only 37% of users carefully read the license agreement before installing software.** One in ten (9%) respondents never reads them because he finds no sense in it. The younger the respondent the more he is inclined to agree with this statement and reads the license agreement less.

Figure 25. Reading license agreements



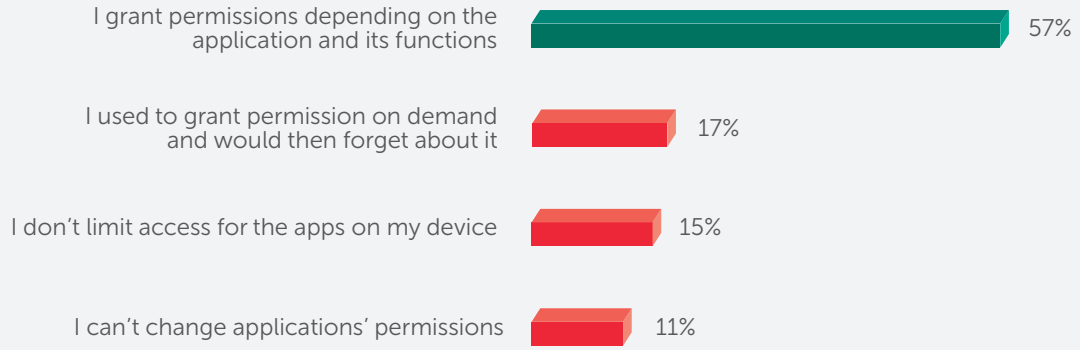
20% of users do not carefully read the content of the installation window during the installation of applications; they just click "Next — Next — Agree — Next". Only 67% of respondents read carefully and adjust settings if necessary, avoiding the installation of unnecessary additional applications from the manufacturer or an unauthorized change to the operating system settings.

Figure 26. Check of settings during the installation of the application



While answering the question about the permissions they grant to applications on their devices, **17% of users admit that they grant access on demand, and then forget about it; and 15% of respondents never restrict access for the applications on their devices.** Only 57% of those surveyed allow applications to access particular information or perform certain functions depending on their intended purpose. Interestingly, the younger respondents are more often ready to provide the applications with the freedom of action while the older generation is more often sure they cannot change the permissions at their own discretion.

Figure 27. The permissions granted to applications



When it comes to an application that was once installed but turned out to be unnecessary, **37% of users are ready to leave it on the device just in case is could be useful some time** while 63% of respondents will remove it and download it again when needed. The latter is the right choice because old, not updated programs can serve as a "front door" for malicious applications that exploit vulnerabilities in the software to seamlessly penetrate to your computer.

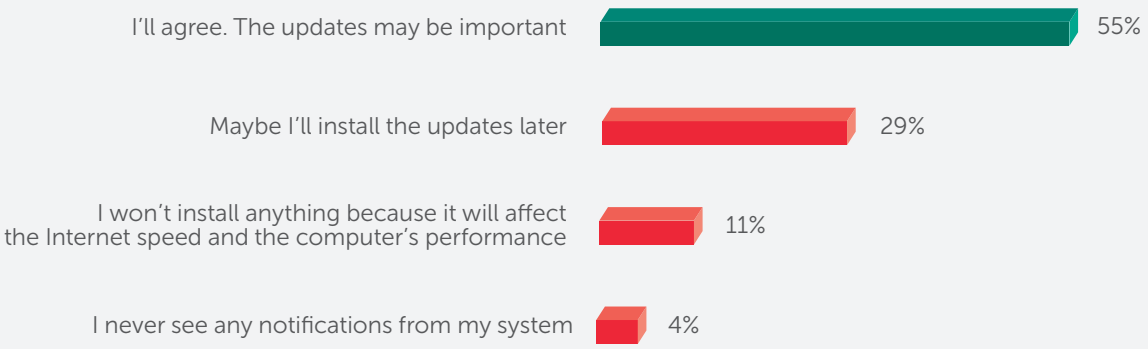
By not reading license agreements and granting unlimited access to applications, the Internet user is unaware about what the applications are doing. It is easy to forget that the device, and its applications, can look in as well as out. For example the camera function we use to take pictures of the world can take pictures of our world. In the wrong hands, the Internet can invade the most private corners of our lives; and a device that was our friend can become our enemy. Cyber–savvy users, on the other hand, are eager to control what is happening on the device to which the user trusts his life.

SECTION 8. SELF–PROTECTION

In previous sections we have gained an overall picture of how well Internet users have adapted to the ever–growing range of opportunities they get from the Net. In this section we will concentrate on how attentive humans are to their digital helpers. Being cyber savvy involves using the right digital tools too, so it is important to take proper care of them.

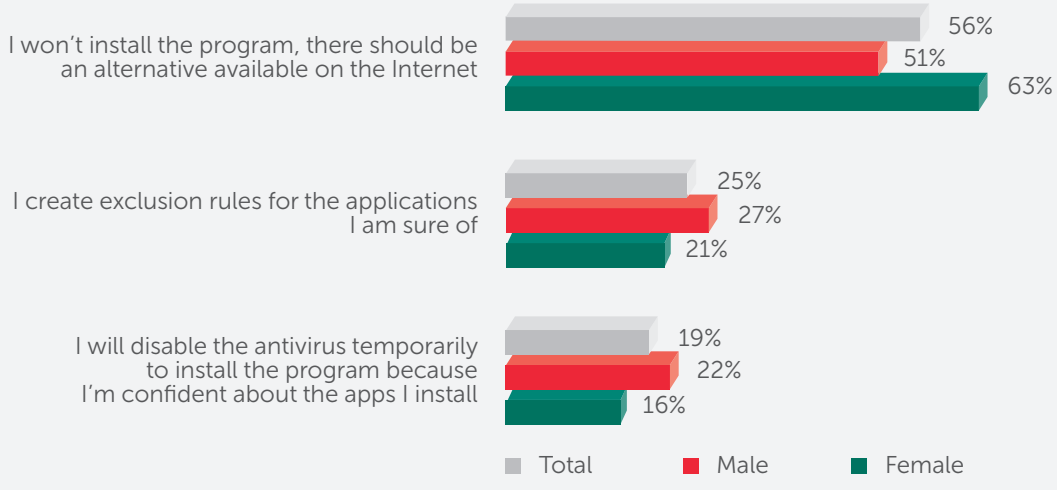
For example, when the operating system prompts you to install important updates, it makes sense to agree. However, only 55% of users are ready to do it immediately; 29% of respondents will consider the proposal later, and **11% of those surveyed won't install updates until it affects their device's performance.**

Figure 28. The agreement to install OS updates



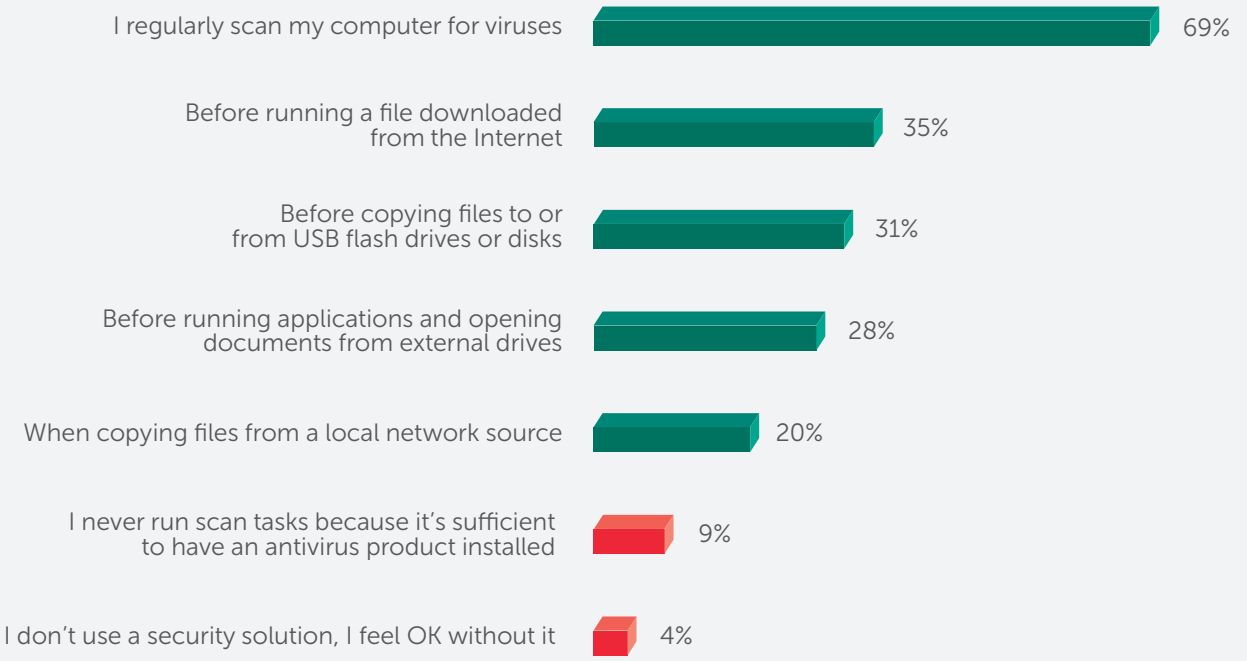
If the security solution attempts to prevent the installation of a program, **19% of respondents would prefer to disable antivirus software and install the program** although it might be dangerous. The younger the users, the more confident they are and the more often they disable antivirus software in such situations, or set up exclusion rules for these programs. This step is more typical for men than women.

Figure 29. Users' actions when a security solution prevents the installation program



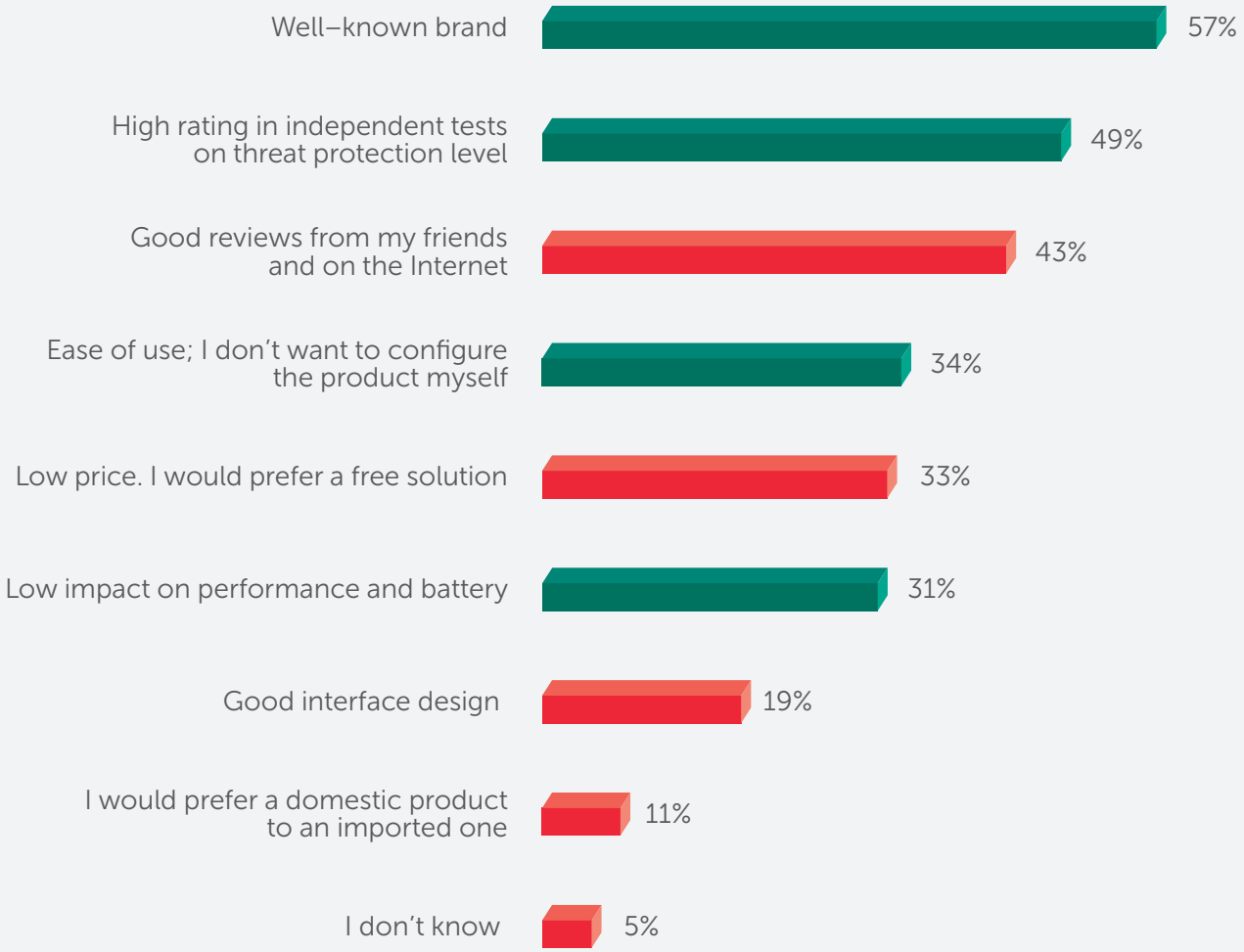
9% of respondents believe that it is not necessary to scan the computer because an installed security solution is enough; 4% of users feel safe without any security solution at all and 69% of that surveyed regularly scan their device for threats — a good result.

Figure 30. Scanning the device for cyber threats



When choosing a security solution and having the ability to specify multiple criteria simultaneously, 33% of respondents would prefer low price and 19% of users will vote for the design (13% women vs. 23% men). Young people are more likely to rely on their friends' opinion and online reviews (51% of respondents under 24) while older people would prefer a product made in their own country (27% of respondents over 65).

Figure 31. Criteria that are important when choosing a security solution



It is worrying to see that a significant portion of users tend to treat digital tools with a "fire and forget" attitude. Moreover, in some cases, if they see an obstacle to a "here and now" scenario in the Internet security solution, they are ready to ignore it and go ahead. The consequences of this attitude can be really disastrous when we remember that in the cyber world conventional security instincts often fail.

CONCLUSION

The instinct of self–defense is inherent in any person. However, this instinct often does not work when the virtual rather than the real world is at issue. Many people are careless about their devices and the data stored on them: they enter their personal information on phishing pages, choose passwords that are too easy, follow any proposed links, download and install unchecked software... All this makes them vulnerable and easy targets for fraudsters, criminals and tricksters.

Being cyber savvy is a skill that in the current digital world should be imparted to people from childhood. At the time when the child first takes his father's tablet to play or watch cartoons, he should be warned and protected.

Cyber savvy people know that they are responsible for their safety. They understand what's inside the Internet, where their weaknesses are and how they can reduce the probability of encountering a threat to a minimum. They know that their accounts and files stored on their device are no less valuable than the passport data, the wallet or other things in the real world. They tend to know or learn how to identify a fake website, to detect malware, to protect their data from loss or theft and to choose a security solution that helps protect against threats that are invisible to the eye.

Cyber savvy is a new instinct of self–defense. As this test shows, at the moment it is possessed by the overwhelming minority of Internet users. However, that cannot remain the case if we are to protect ourselves and each other. As a society of Internet users, we need to develop a new type of protective instinct — a digital instinct that kicks in when we go online.

Check for yourself: https://blog.kaspersky.com/cyber-savvy-quiz/

APPENDIX 1

The phishing samples used:

Australia	CommonwealthBank
Brazil	Itau
Czech Rep.	Facebook (English language)
France	Orange
Germany	Sparkasse
Great Britain	Facebook
India	Facebook
Italy	CartaSi
Japan	GameCity
Malaysia	Facebook
Mexico	Banamex
Philippines	Facebook
Russia	Vkontakte
Spain	Banko Popular
Turkey	Facebook
United States	Facebook

KASPERSKY lab