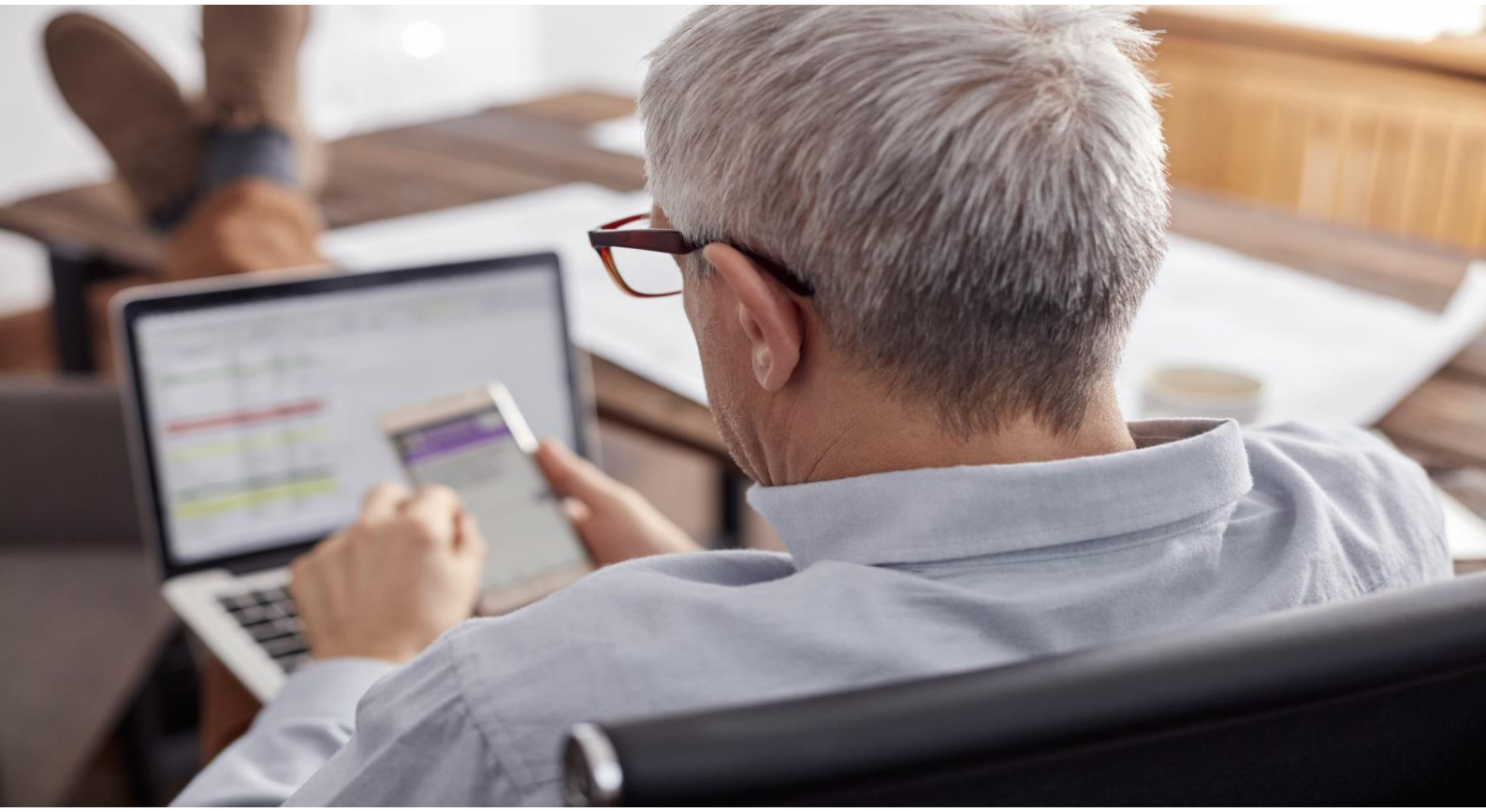
Baseline Research Report on Target Audiences Awareness of Key Aspects of Cybersecurity



Conducted for CRDF GLOBAL

The study was supported by the US State Department Office of the US Assistance Coordinator for Europe and Eurasia

Content

Table of figures

Table of tables

I Summary

Activities in the Internet

For all age groups, the most popular daily activity in the Internet is using messengers (Viber, Telegram, WhatsApp, Facebook), while passive use of social networks (visiting, reading) ranks second.

Second-order activities:

- For teenagers – games, content downloading and posts in social networks
- For the rest of responders – e-mail, internet banking

Popularity of content downloading fades with age: only 4% of teenagers don't do this, while among the oldest responders this number is 58%. However, teenagers are the ones downloading content from official sources (or such reliability of which they are sure of), while the rest of responders most often don't check source reliability at all.

Teenagers also use public wi-fi networks more actively than other groups.

Awareness of the concepts of "cybersecurity" and "cyber hygiene"

The concept of "cybersecurity" is regarded as quite familiar in all age groups: frequency of "hear for the first time" ranges from 7% to 12%, while relative majority have replied "have a general idea, without details" (from 42% to 51%). Respondents are less familiar with the concept of "cyber hygiene": frequency of "hear for the first time" is 4-fold higher: from 29% in teenagers to 32% - 39% in the rest of age groups.

Unsafe behavior in the Internet

As for unsafe behavior patterns demonstrated by respondents, the most popular one for all age groups is not making backup copies of the data. Next one is not turning two-factor authentication on. The most careful about these issues is the group aged 18-25, while the most careless is the group of 60+.

The idea that internet scammers are not interested in a "simple person" is also quite widespread – it is shared by every second respondent over 18 years old and approximately by three out of four teenagers.

Respondents are also quite careless about passwords: most responders (around 40% in the mean) confess about using one and the same password for everything and also that this password is quite simple. The most responsible behavior is demonstrated by the group of youth aged 18-25 where unsafe behavior is less common than in other groups.

A separate type of unsafe behavior is actions in the Russian segment of the Internet. Such actions are not very common, especially in comparison with other types of unsafe behavior. Ukrainians practice (in descending order of frequency): visiting Russian websites (29%); visiting Russian

resources and social networks blocked in Ukraine (16%); downloading files from Russian websites, filling out questionnaires, registration, etc. (13%); using of Russian mailboxes (10%).

In terms of actions in the Russian segment, the most vulnerable group is young people aged 18-25: such users most often visit Russian websites (40%) and resources blocked in Ukraine (29%), download files, programs from Russian resources, register (25%), have mailboxes on Russian servers (17%). In second place in the prevalence of such behavior - adolescents aged 11-17 years old. The oldest age group resorts to such actions the least. However, there is a suspicion that respondents of this age (over 60 years old) may not be aware of which segment of the Internet they are in.

Experience of cyber threats

In total, 41% of users in the sample encountered at least one type of cyber fraud. The largest share falls on the group aged 25-59 years. Almost every second person has personal experience there (47%). Among young people aged 18-25 this share is 37%, and among the elderly over 60 - 43%. Adolescents were the luckiest - only 7% faced cyber fraud in person. More cautious behavior of youth (18-25 years old) in terms of passwords, the habit of backing up and using two-factor authentication can be explained by the fact that representatives of this group are the ones facing hacked passwords more often: for instance, 60% of respondents from this group reported that hacking of social network account had happened to their real acquaintances, and it also happened to a half of them personally. For the rest of age groups, this number is 1,5-2-fold lower.

Number one cyber threat for people aged from 26 years old is extortion of bank data, passwords, and access to accounts of mobile banking, bank accounts (including by phone and messengers). 44% of middle-aged people (26-59) and 37% of seniors (60+) either encountered it personally or it happened to their real acquaintances, and the share of personal experience is pretty much the same – 23-24%. Most seniors (28% of respondents aged 60+) had personal experience when, using social engineering methods (manipulations, threats, blackmail), cyber scammers extorted money as well as personal and family data (via phone and messengers), and 42% of them reported that this situation was encountered by their real acquaintances.

A state of security in the Internet

Depending on the age group and situation, 49% - 75% of people feel vulnerable or don't always feel safeguarded/protected. The biggest concern of users is hacking of passwords and accounts in social networks: 75% of respondents aged 26-59 do not feel completely secured against this cyber threat. About all types of threats, teenagers and young people under 25 feel more secure in comparison with older respondents.

At the same time, teenagers and young people regard their behavior in the Internet safer than other age groups. 37% consider the behavior completely safe (in the age groups 18-25, 26-59 and 60+ years old this figure is 29%, 25% and 23% respectively).

Among users over the age of 25, one in three believes that he or she behaves recklessly in the Internet.

Cybersecurity rules

As for principal cybersecurity rules, most respondents (97%) know that they shouldn't send out photos or scans of their bank cards and personal documents (this figure is stable and does not vary with age), while 83-90% of respondents follow this rule depending on age. Respondents are also .well aware that the device should not be left unattended or unlocked (81-87% know this and follow this rule). Smaller part of respondents know that suspicious letters should not be opened: 57-58% of respondents under 25 follow this rule; in groups aged 26-59 and over 60 years this number is higher – 65% and 64% accordingly. Regular updating of devices is performed, on avarage, by a little more than a half of respondents. Complex and different passwords are used, on average, by a little bit less than a half of respondents (18-25 years old – 64%, other age groups – 45-48%).

Creation of backup copies of important data and obligatory use of two-factor authentication declare 30% and 28% of respondents respectively, these two rules are followed less often than others. Young people aged 18-25 declare compliance with these rules more often than the age group 25-59 years (for other age groups, the rule was not proposed).

In general, teenagers aged 11-17 are the most aware group about cybersecurity rules: 83% know all the rules. However, only 50% of teenagers follow all the rules at least sometimes, and only 22% constantly follow all the rules. However, compliance with the rules in the group of teenagers is the highest among other target groups: among young people aged 18-25 at least 21% follow the rules sometimes, among adults aged 25-59 - 12%, and among the oldest respondents over 60 - 22%.

The oldest group of respondents is the least aware: only 37% know about all cybersecurity rules for this group. But also these respondents are the most conscious: if an older person knows the rule, he or she is more likely to follow it.

Self-assessment of use of the Internet depends on knowledge and compliance with the rules of cybersecurity: the higher a person evaluates the security of their behavior, the better he or she knows and more often follows the rules of cybersecurity. This correlation is observed for all age groups. Users who rate their behavior as unsafe either do not know the rules or know but ignore them.

However, declaring compliance with cybersecurity rules does not mean genuine compliance with those rules. We analyzed the responses of respondents who stated that they follow a certain rule, and looked at how unsafe their behavior is due to non-compliance with this rule. It turned out that among those who declared compliance with the password rule, only approximately ¾ actually behave in this way; only half of those who declare compliance with the two-factor authentication rule actually use it, and one in five do not use it at all; among those who know and, according to them, always follow the rules of backup, less than half do declare such behavior, and one in three says they do not.

Information sources

As for information sources about safe behavior in the Internet, the first and second place for all age groups are «word of mouth» (friends, relatives and acquaintances familiar with the topic) and people respondents regard as specialists (for instance, system administrator at work, school or university). At the same time, word of mouth is in the lead by a wide margin for the youngest (11-17 years old) and the oldest (60+ years old) groups. Consequently, these are the most trusted sources.

For other sources, they vary with age. Yes, the oldest group uses almost no sources other than friends and familiar experts. Teenagers are more likely to turn to social networks; youth (18-25 years) and the adults (26-59 years) use the Internet (apart from social networks) and special sources, websites, forums more often. Traditional media, external advertising and bloggers are not regarded as relevant sources of information about safe behavior in the Internet for all age groups.

II Conclusions

Most users spend part of the day on the Internet every day using a personal device. Therefore, users are personally responsible for their own safety.

The use of messengers and social networks is the most common type of activity in the Internet, so the main threats face users here. However, it is also possible to recommend the use of these sources to disseminate knowledge about cybersecurity and basic cyber hygiene rules.

The first priority for the information campaign is to promote the rules of cyber hygiene. After all, 62% of users either have not heard of such a concept, or have heard but do not know what it is. Only one in ten is so confident in their knowledge that they can explain it to others.

This situation is threatening, as the sources of information about cybersecurity are dominated by "friends, acquaintances and relatives" who can explain in their own words what and how to work to secure themselves from threats. Namely, with this source there is an obvious failure. This is why myths spread among users, which reinforce unsafe behavior.

One of the most common myths is the statement "Internet scammers are not interested in me " - more than half of respondents are inclined to this opinion (the most vulnerable group - teenagers aged 11-17, 72% of whom agree with this opinion). The second equally common myth is "if there is an antivirus, then I'm safe" (the most vulnerable groups are teenagers aged 11-17 and the oldest people over the age of 60).

Armed with these ideas, users feel more or less confident in the Internet (teenagers are the most confident group), at least about two out of three do not consider their behavior unsafe. But with regard to external threats that do not depend on their own behavior, users often feel vulnerable.

In particular, users often feel insecure in situations where attackers steal accounts on social networks (76%), cybercriminals demand money from older people using social engineering methods (manipulation, threats, blackmail), as well as personal and family data (through phone and messengers) (74%). It is significant that these cyber threats are one of the most common: at least 80% of users have heard about hacking accounts on social networks (and among young people aged 28-26 every third person has experienced it), among the elderly 90% know about extortion (28% know it from personal experience).

People who feel insecure mostly (three out of four) declare their readiness to follow the rules. The problem is that the most relevant (and least intuitive) rules are known to a small number of users. Yes, almost everyone knows the rule about the inadmissibility of sending photos of bank cards and documents to strangers, and almost everyone follows them. But the rules for using two-factor authentication or backing up important documents are known and at least sometimes followed by only 53% and 62% respectively (however, as the analysis showed, declaring the rule and the actual use of this rule in everyday life can be twice as different).

Users are the least aware of the rule of notifying the relevant authorities about gadget having malicious software or data compromise: almost half of users aged 18-59 hear about it for the first

time. Older people are encouraged to report to the Cyberpolice as well as children and loved ones - due to the latest knowledge of this rule a little higher. However, as we remember, among children and relatives the level of awareness about the rules of cyber hygiene is generally about 10%.

Given that Ukrainians are increasingly faced with cyber threats in their own experience (41%), the issue of an educational information campaign is becoming increasingly important. After all, it is the knowledge and use of cyber hygiene rules that is a factor in safe behavior in the Internet, and users are aware of this.

Such campaign can be aimed both at disseminating information on where to get support in a critical situation (Cyberpolice, other relevant authorities) and at disseminating expertise in an accessible format. It is also important to explain why it is necessary to resort to certain actions that are not always clear to the average user, but require some effort (two-factor authentication, strong passwords, backups, etc.). The rules, which are intuitive at the household level (report the cyber incident to parents or adult children, do not panic, etc., the level of knowledge of which is already quite high), can not be explained in detail, but provide a level of support.

The campaign can have a prolonged effect due to the so-called "word of mouth" - people who have acquired knowledge through the campaign will be able to seek advice from their relatives and acquaintances.

III Methodology

Recognizing the risks associated with the increasing digitalization of the world, CRDF Global in 2019 launched a program to improve cybersecurity in Ukraine, Moldova and the Western Balkans. The program is dedicated to preventing cyber attacks by building a strong cyber infrastructure and strengthening cybersecurity. This program is supported by the US State Department Office of the US Assistance Coordinator for Europe and Eurasia.

«The Cyber Security Information» campaign project is part of the CRDF Global Cybersecurity program, and the main goal of the project is to raise awareness of cybersecurity threats among the general public in Ukraine.

Given the lack of data on the level of public awareness about cybersecurity threats, it was decided to conduct a baseline study on the awareness of target audiences on the main aspects of cybersecurity and cyber hygiene rules.

The survey aims to assess:

- the level of awareness of target audiences about cyber threats to cybersecurity;
- level of awareness of the basic cyber hygiene rules and their use in everyday life;
- personal experience of users in recent months on cyber hackers, cybercrimes, cyber attacks, cyber threats;
- sources of information on cybersecurity, cyber attacks, cyber hygiene;

The target audience of the research is citizens of Ukraine who use the Internet at least several times a month.

Target groups of respondents:

- Teenagers, 11-17 years old;
- Young people, 18-25 years old;
- Adults, 26-59 years old
- People older than 60 years old.

The research method is a quantitative survey based on a structured questionnaire.

Geography of the research: all of Ukraine, including villages, except for the Autonomous Republic of Crimea and some districts of Donetsk and Luhansk regions temporarily not controlled by the Ukrainian government. The survey was conducted in all regions of Ukraine, in particular, 296 respondents were interviewed in cities with a population of over 500,000; 287 respondents - in cities with a population of over 50 thousand (the list of cities is given in Annex 1); 245 respondents - in smaller towns and urban-type settlements, and 372 respondents were interviewed in villages.

Total number of respondents: 1,200.

Number of respondents by target groups:

- Teenagers, 11-17 years old: 300 respondents;
- Young people, 18-25 years old: 300 respondents;
- Adults, 26-59 years old: 450 respondents;
- People older than 60 years old: 150 respondents.

It was previously planned to conduct an equal number of interviews with all target groups (300 interviews each). However, during the survey, researchers encountered very low Internet penetration for the oldest target group (people over the age of 60). According to the Omnibus of Info Sapiens, the level of Internet penetration is 99% among the audience aged 11-25, 90% among the audience aged 26-59 and only 38% among the audience over 60.

In view of the low penetration of the Internet among the oldest age group, it was decided to reduce the target number of interviews to 150 by increasing the target number of interviews for groups aged 26-59 to 450 interviews.

Survey method:

- for the target group "Teenagers" - a personal survey at the respondent's home using a computer (CAPI - computer assisted personal interview);
- for other target groups - computer assisted telephone interview (CATI).

Sampling is random with the control of quotas by sex, age, region and size of settlement. The sample is representative within each target group, the structure corresponds to the structure of Internet users by gender, age, region and size of the settlement.

Weighting was used for the analysis of the sample as a whole, which brought the structure of the sample in line with the structure of the population of Ukraine by age.

The maximum statistical sampling error is:

- Sampling overall: 2.8% with probability of 95%;
- Teenagers, 11-17 years old: 5.7% with probability of 95%;
- Young people, 18-25 years old: 5.7% with probability of 95%;
- Adults, 26-59 years old: 4.6% with probability of 95%;
- People older than 60 years old: 8.0% with probability of 95%.

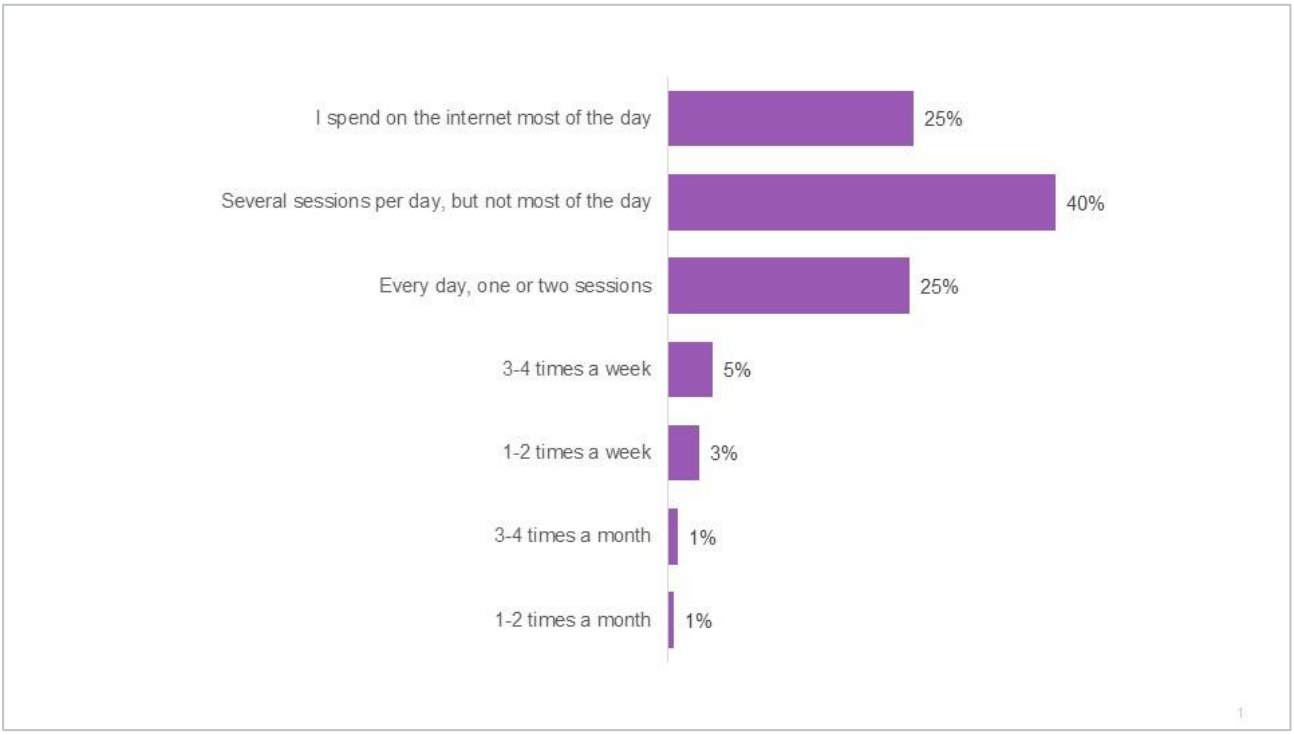
The survey was conducted on a structured questionnaire (see Annex 2). In the questionnaire, in particular, were included five-point and ten-point scales. From the point of view of analysis, a positive grade is 4 or 5 on a five-point scale, and 9 or 10 on a ten-point scale.

IV Research results

Use of the Internet

People who use the Internet at least once a month were invited to participate in the survey, but the majority of respondents (90%) use the Internet daily. A quarter of them spend most of the day online (see Figure 1).

Figure 1. How often do you use the Internet, for example, visit websites, social networks, use applications, messengers? (% of answers, all respondents)

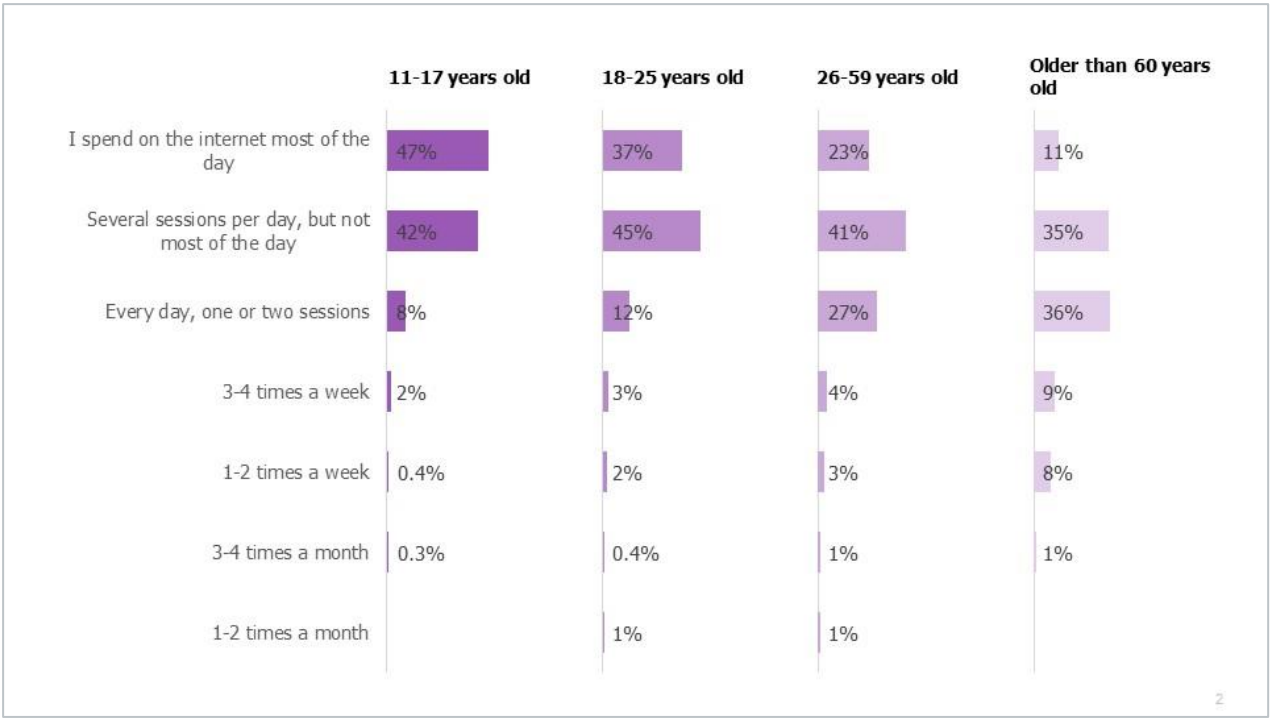


The proportion of people who spend most of the day on the Internet decreases with the age of the respondents. Thus, there is almost half of such respondents (47%) among the youngest group - teenagers of 11-17 years old, 37% spend most of the day on the Internet among young people of 18-25 years old, almost one in four (23%) among adults of 25-59 years old, and only 13% among the elderly.

However, the frequency of daily use decreases with age much more slowly: the share of people who go online daily is significantly lower than the general figure only for the elderly (82% of respondents over 60 years old), and for other age groups it exceeds 90%, 94% and 91% for teenagers, young people and adults, respectively).

Thus, people with access to the Internet tend to use the Internet on a daily basis, but older people are mostly limited to 1-2 communication sessions, while young people spend most of the day on the Internet (see Figure 2).

Figure 2. How often do you use the Internet, for example, visit websites, social networks, use applications, messengers? Distribution by target groups (% of answers, all respondents)



As for the devices via which respondents access the Internet, the undisputed leader is the smartphone: in general, 89% of respondents use this device and 76% consider it the main device to access the Internet (see Figure 3, Figure 4).

Figure 3. Via which devices do you access the Internet? (% of answers, all respondents)

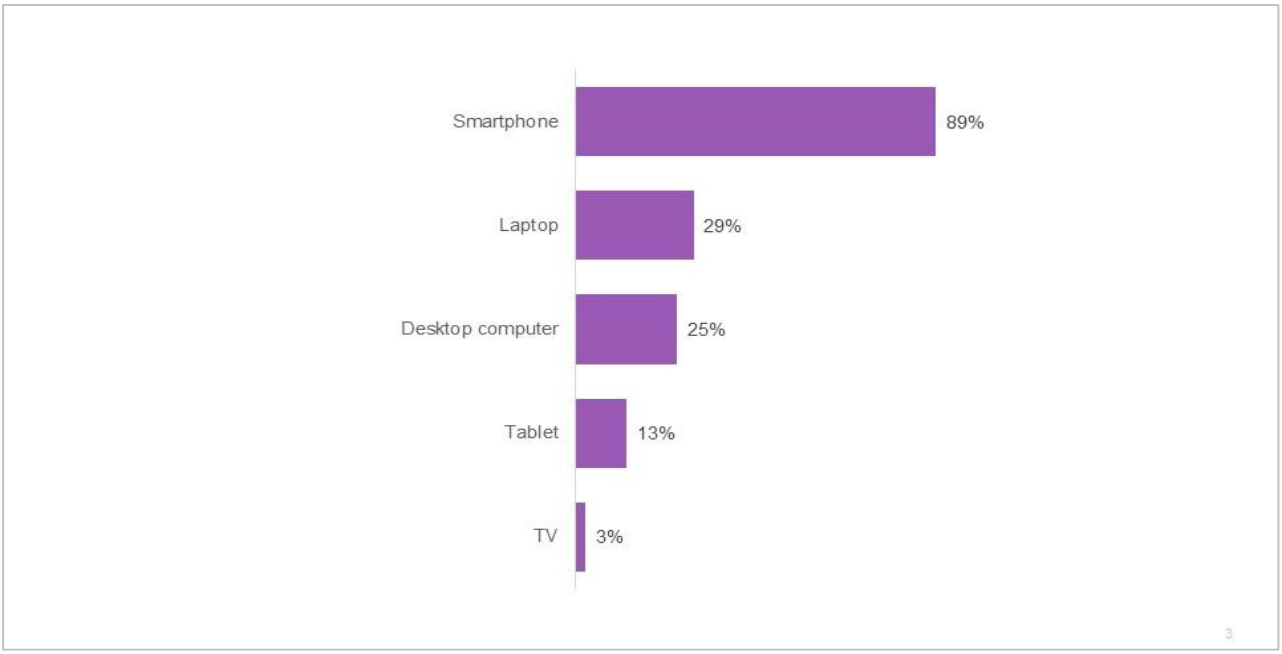
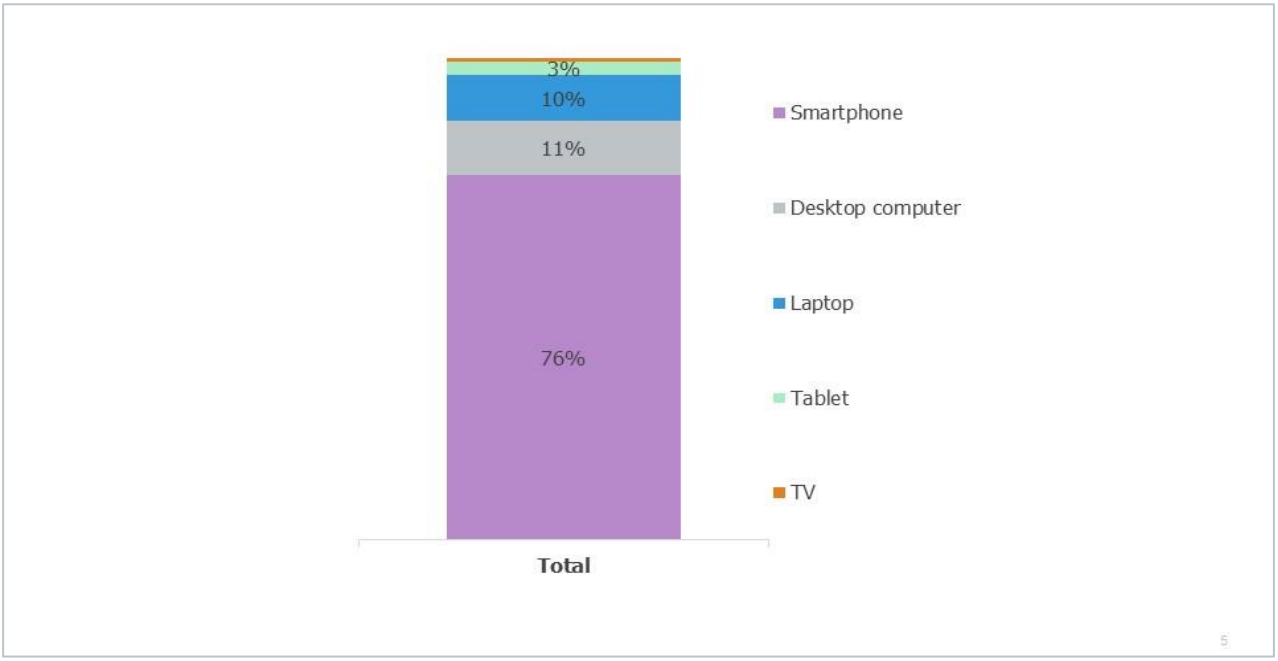
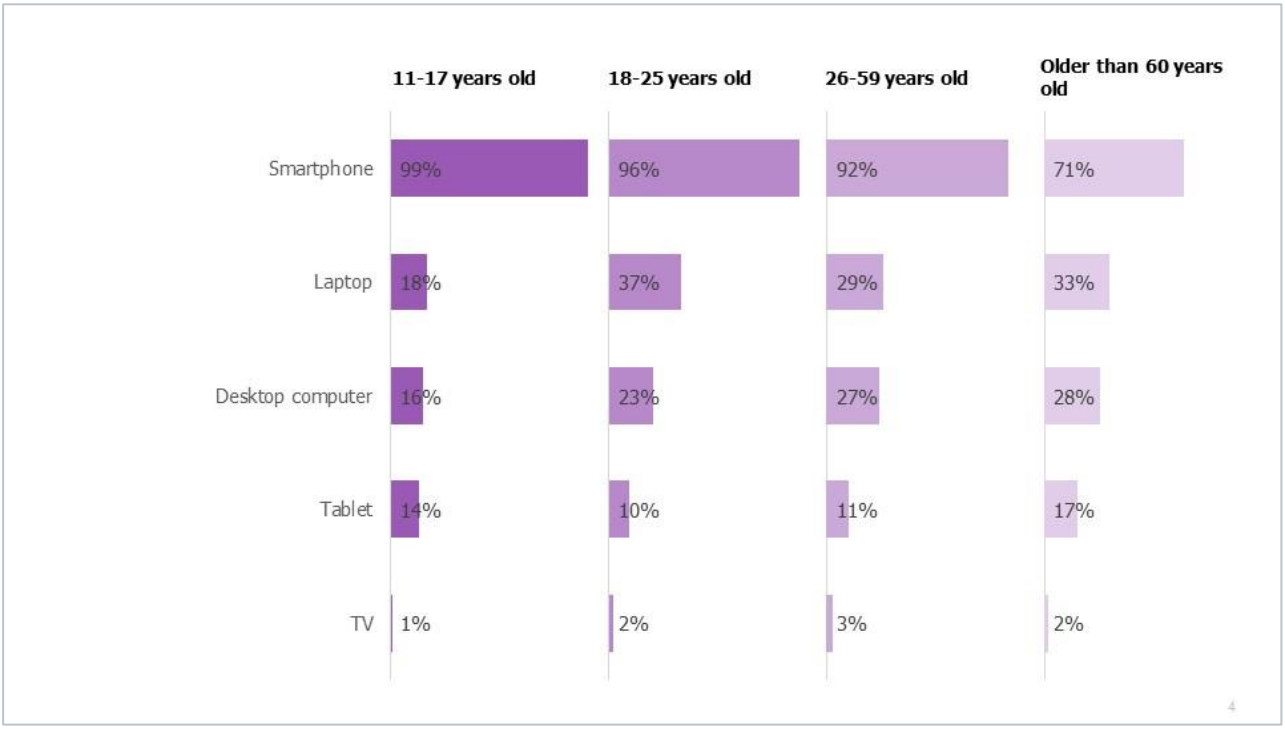


Figure 4. Via which device do you access the Internet most often? (% of answers, all respondents)



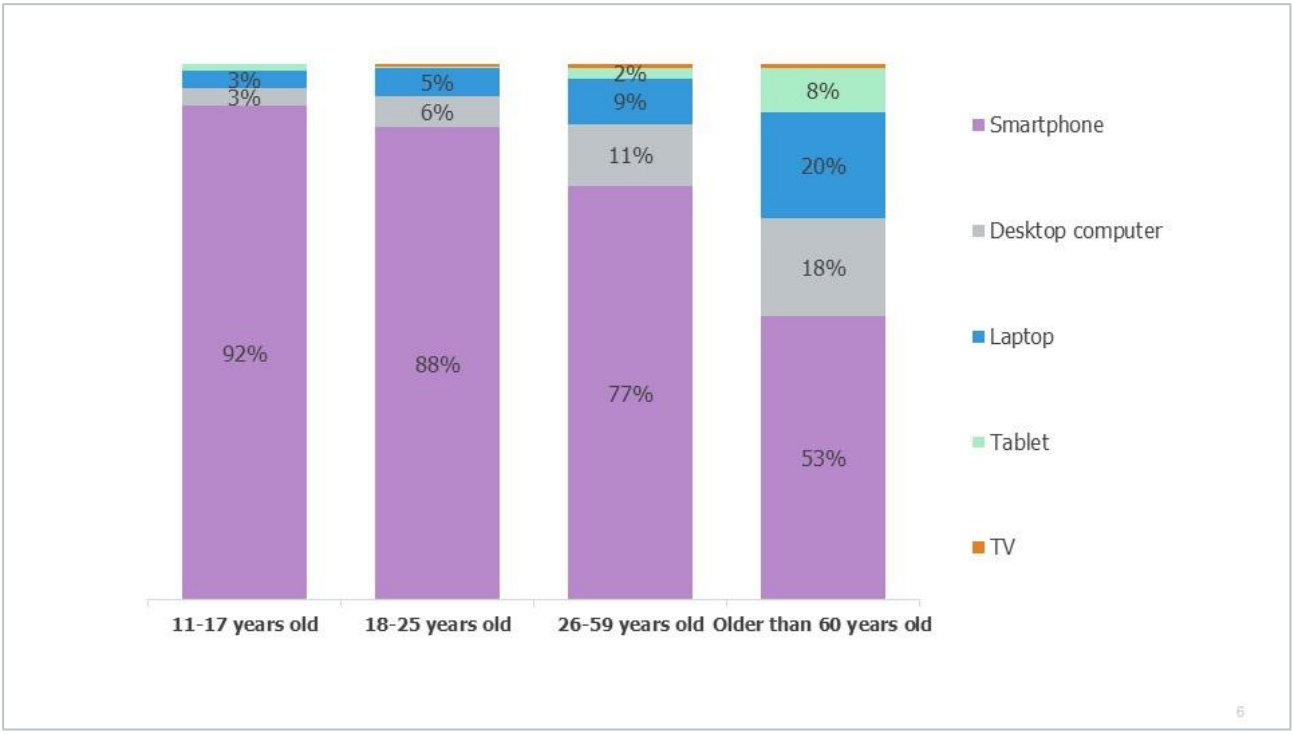
The share of smartphone use is the highest among teenagers (99%) and decreases significantly for the oldest audience (71%). For young and adult respondents, the share of smartphone users is 96% and 92%, respectively (see Figure 5, Figure 6)

Figure 5. Via which devices do you access the Internet? Distribution by target groups (% of answers, all respondents)



For respondents of all target groups, the smartphone is the main device for Internet communication, although a significant proportion of respondents most often use laptops (20%) and desktops (18%) among the older audience (see Figure 6).

Figure 6. Via which device do you access the Internet most often? Distribution by target groups (% of answers, all respondents)



If a smartphone is unquestionably a personal device, laptops and desktops can be shared. We asked respondents who most often access the Internet via a computer or laptop if the device belongs to them personally.

The majority of the audience (55%) does not share a computer or laptop with family or colleagues, but one in four uses family equipment with other family members, and one in five uses corporate equipment (see Figure 7).

The share of respondents who use corporate devices is the largest in the group of respondents of 26-59 years of age (29%). Teenagers often do not have their own computer and are forced to share equipment with their families (48% of those who access the Internet from a computer or laptop, and only 6% of the total sample).

Older people, who most often access the Internet via computer or laptop (38% of them in the general sample), also often have their own equipment - 70% said they use a personal device and only 26% share the equipment with other family members (see Figure 8).

Thus, most of the access to the Internet comes via a personal device, which is in individual use.

Figure 7. Please specify, does this computer / laptop belong to you personally? (% of answers, respondents who visit the Internet more often via a computer / laptop)

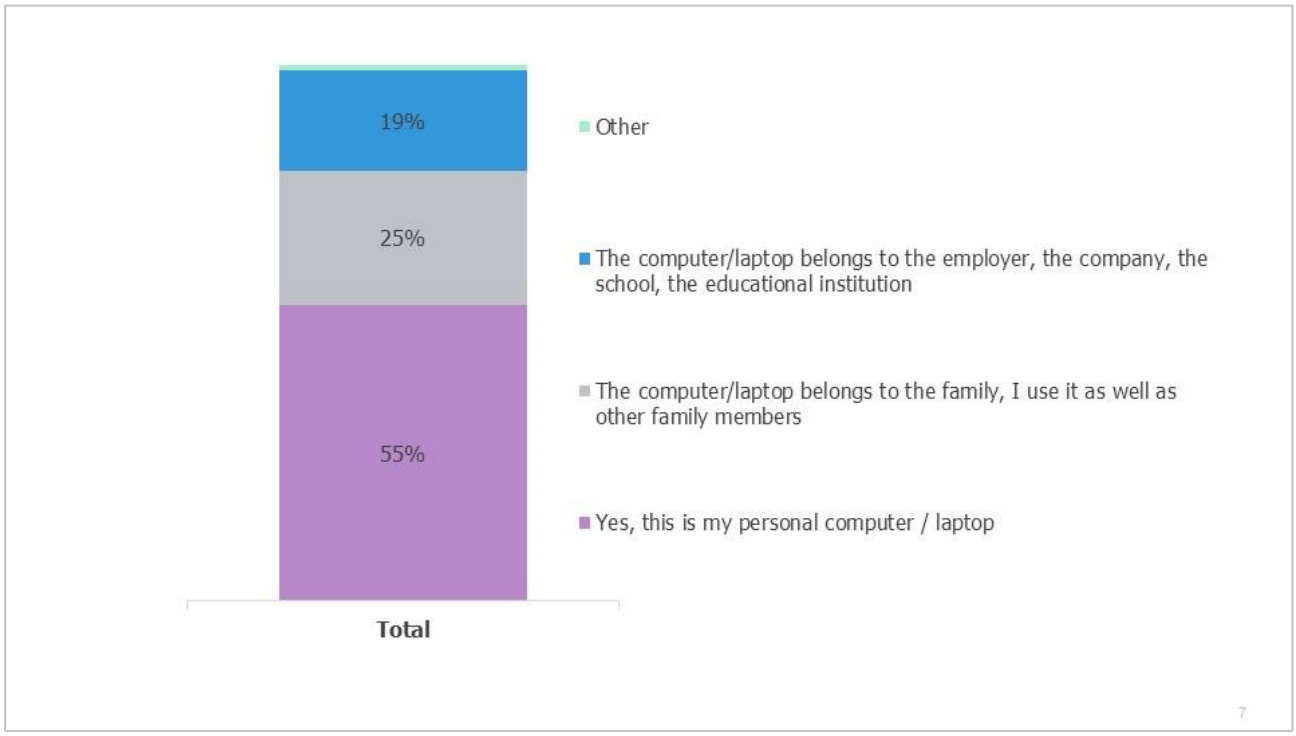
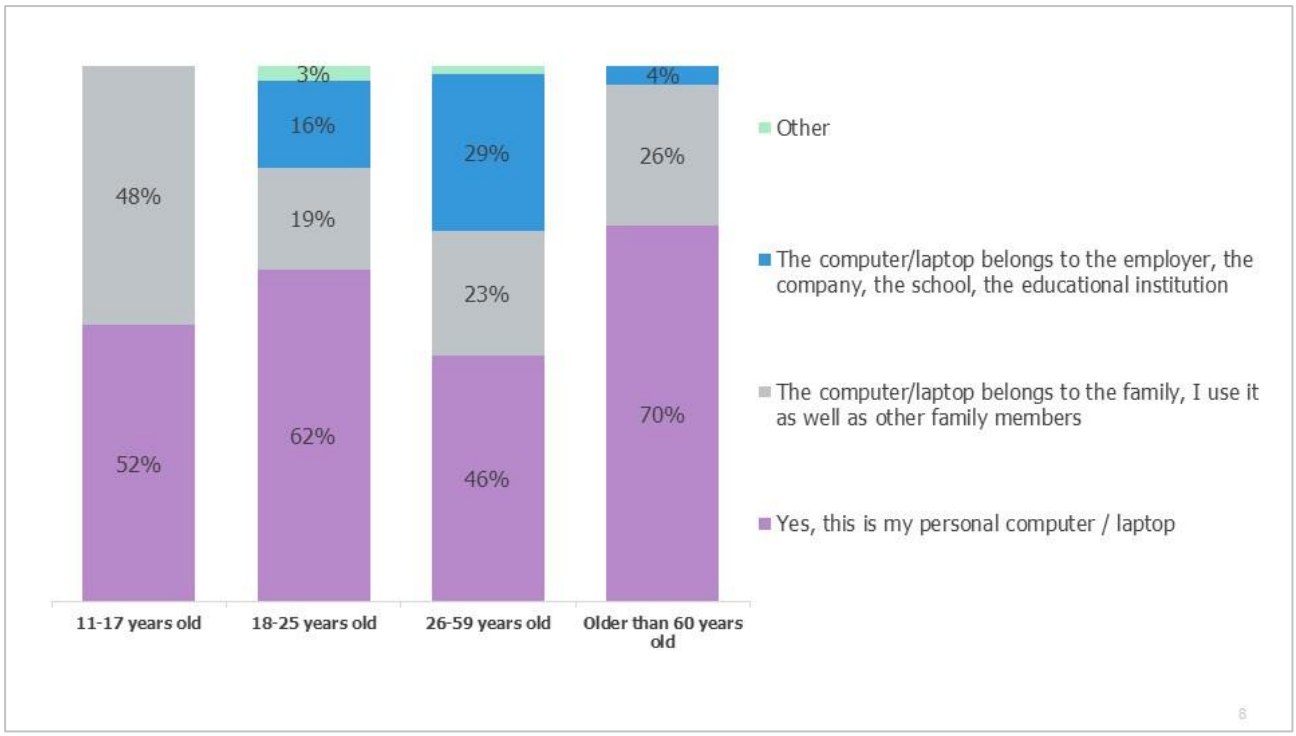
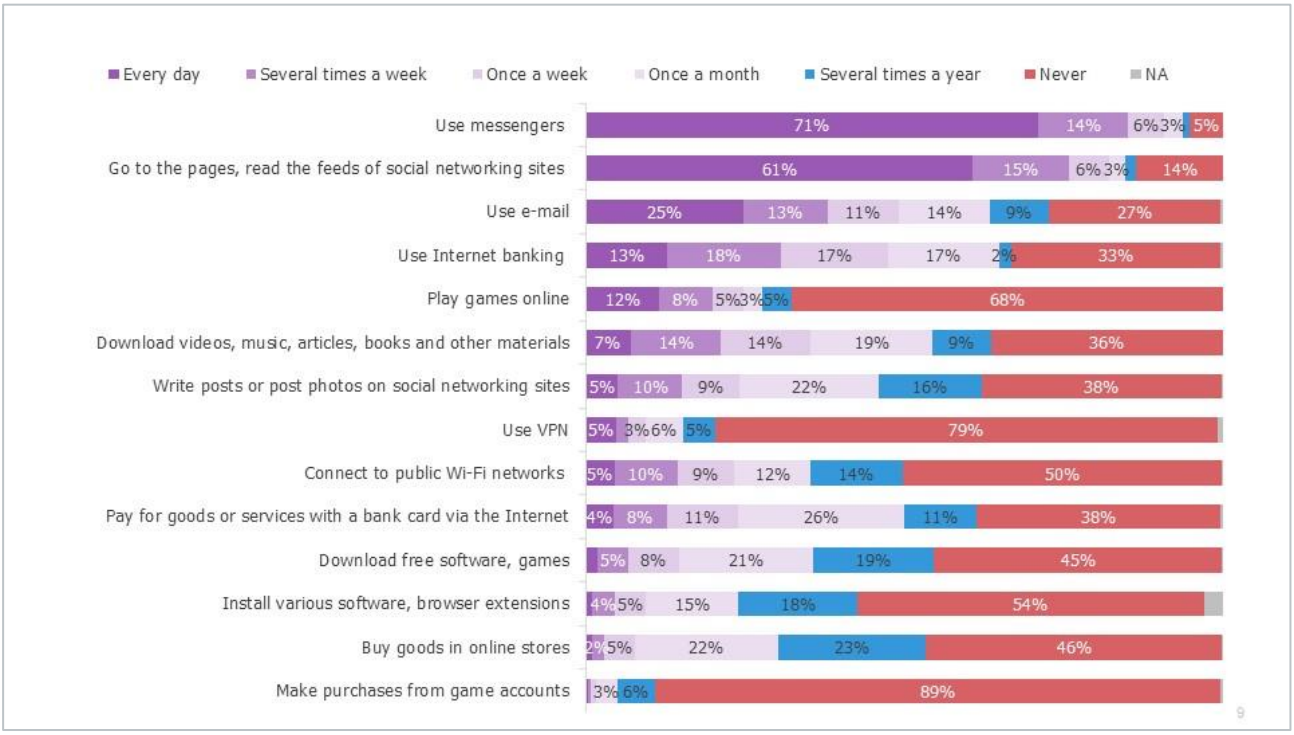


Figure 8. Please specify, does this computer / laptop belong to you personally? Distribution by target groups (% of answers, respondents who visit the Internet more often via a computer / laptop)



Among the actions that users do on the Internet, unquestionable leadership belongs to messengers (a total of 71% of respondents use them daily, and another 14% - several times a week). In second place - the use of social networks (61% daily, 15% - several times a week). Email closes the top three - every fourth respondent uses email every day, another 13% - several times a week (see Figure 9).

Figure 9. Do you perform the following actions on the Internet and how often? (% of answers, all respondents)



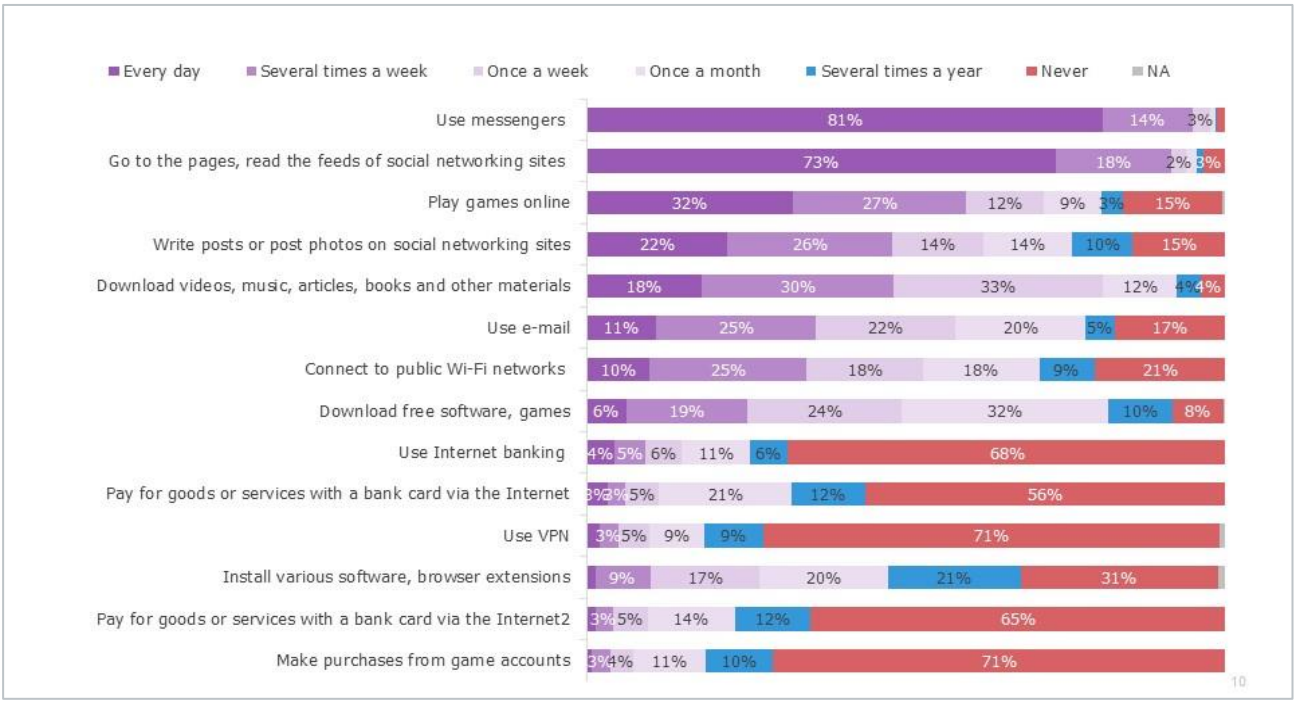
However, while instant messaging and social media scrolling are the leaders in frequency of use in all age groups, the frequencies of other online activities vary with age.

Thus, for teenagers, online games are in third place in terms of frequency: almost every third (32%) plays every day, and another 27% - several times a week. In general, only 15% of respondents in the youngest group do not play online games.

Teenagers are also the most active group in posting content on social networks: almost half make posts or post photos at least a few times a week, with 22% doing so daily.

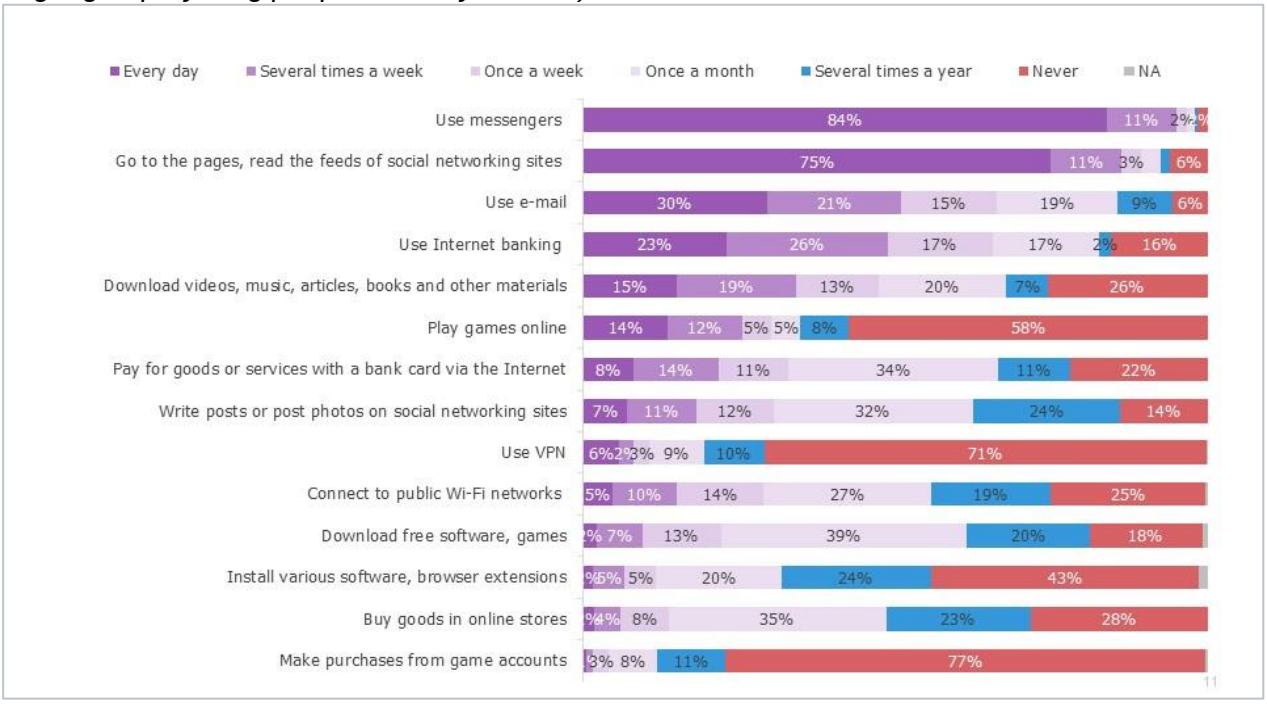
Also, half of the youngest respondents download materials (music, videos, etc.) from the Internet at least several times a week, and only 4% never do so (see Figure 10).

Figure 10. Do you perform the following actions on the Internet and how often? (% of responses, target group - teenagers, 11-17 years old)



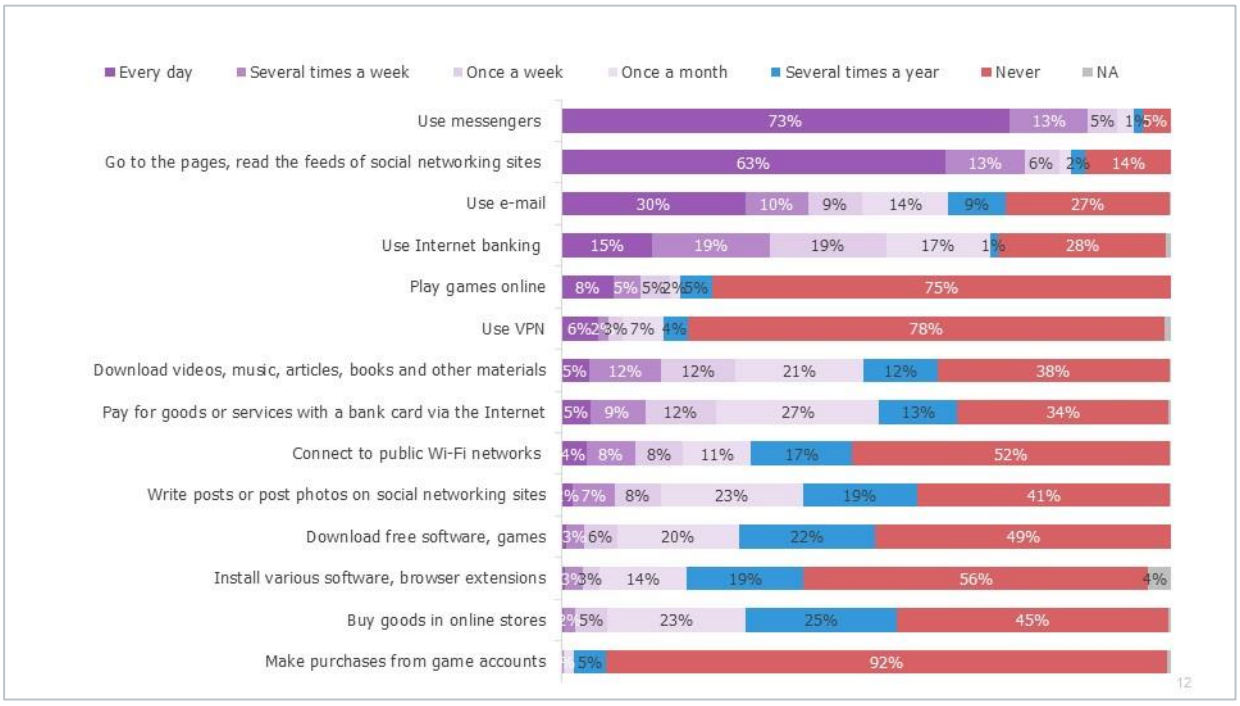
For young people of 18-25 years of age, the third and fourth most frequent are e-mail and Internet banking - about half of respondents turn to these activities at least a few times a week (see Figure 11).

Figure 11. Do you perform the following actions on the Internet and how often? (% of answers, target group - young people, 18-25 years old)



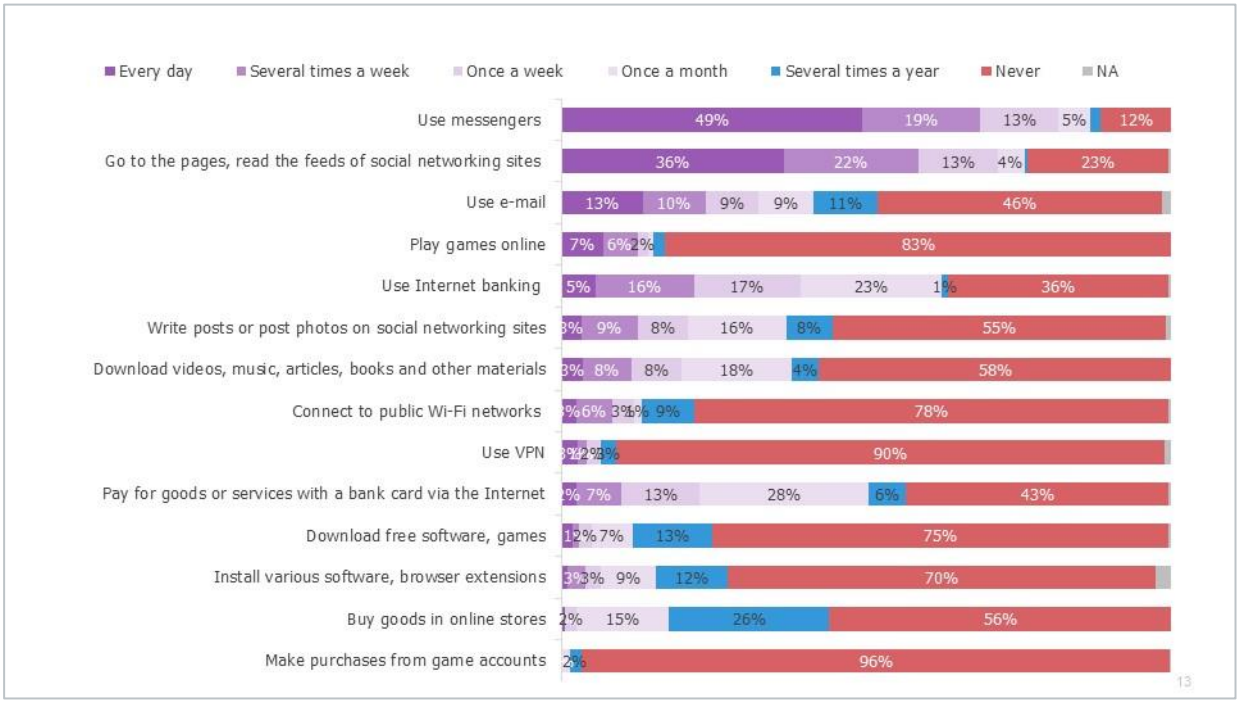
Adult respondents aged 25-59 also frequently use e-mail and Internet banking, but the frequency is slightly lower than among young people (see Figure 12).

Figure 12. Do you perform the following actions on the Internet and how often? (% of responses, target group - adults, 26-59 years)



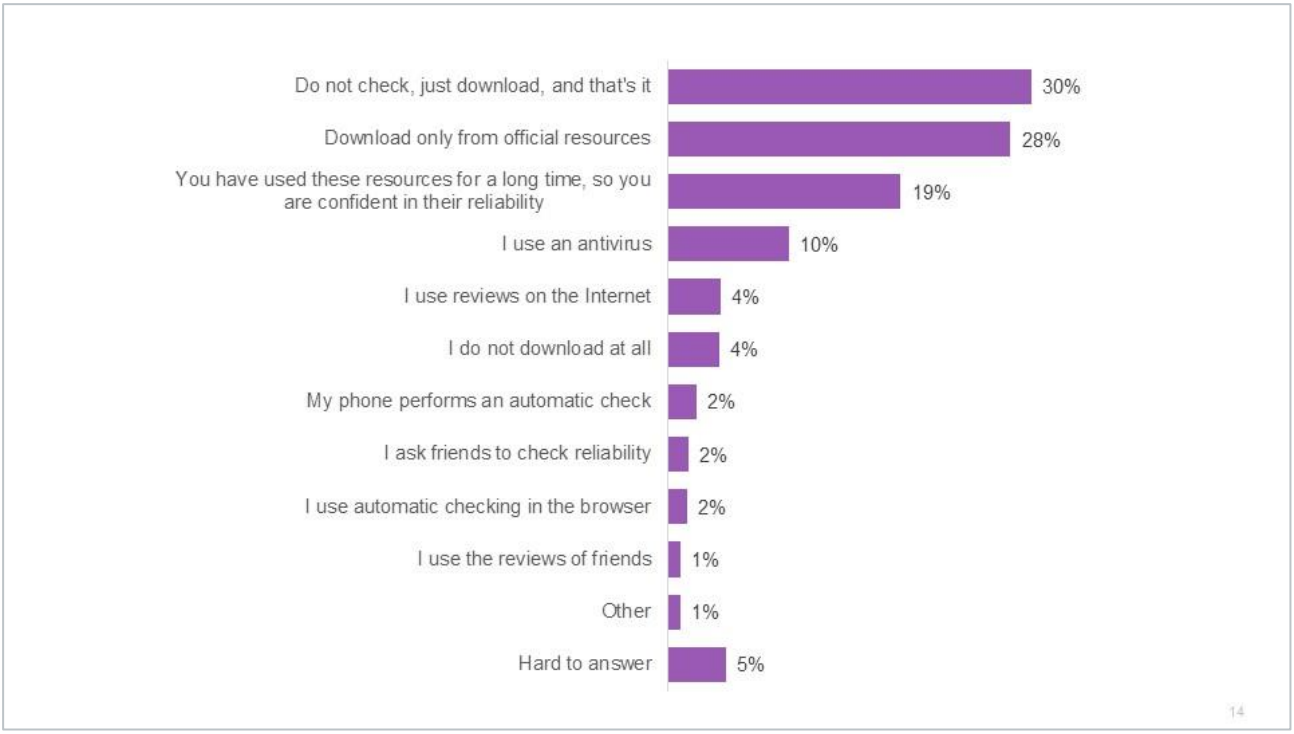
Older respondents are less likely to engage in all types of online activities (see Figure 13)

Figure 13. Do you perform the following actions on the Internet and how often? (% of responses, target group - people over 60 years old)



Thus, among those who download materials, programs, games from the Internet, young people predominate. We asked such respondents if they check the reliability of the resource. In general, according to the sample, almost equal shares of respondents answered that they either do not check reliability at all, or are confident in reliability, because they download from official resources (30% and 28%, respectively). Another 19% believe in the reliability of resources due to long experience and 10% believe that the antivirus program will warn them of the danger (see Figure 14).

Figure 14. When you download materials, programs, games, how do you check if a resource is reliable? (% of answers, respondents who download materials, programs, etc.)

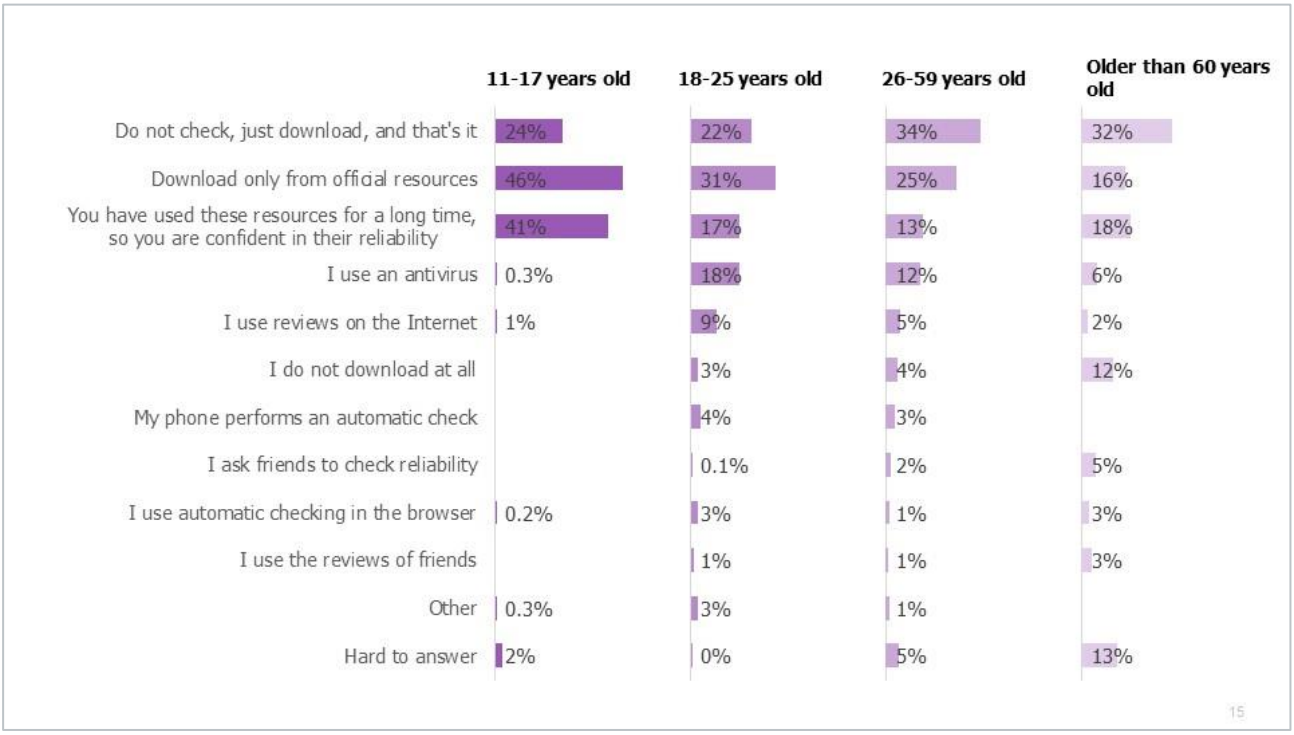


However, the proportion of these most common responses varies considerably across age groups. Yes, teenagers almost do not use antivirus, but most often use official resources (46%). Young people aged 18-25 also often turn to official resources (31%), but 22% do not check the reliability of the resource, and a significant proportion rely on antivirus (18%).

Among middle-aged (26-59 years) and older (over 60 years) respondents, the share of those who do not check the reliability of the resource increases to 34% and 32%, respectively.

Among older respondents, the share of those who use official resources is the lowest, at only 16% (see Figure 15).

Figure 15. When you download materials, programs, games, how do you check if a resource is reliable? By target groups (% of answers, respondents who download materials, programs, etc)



Awareness of the concepts of "cybersecurity" and "rules of cyber hygiene"

We asked the respondents how familiar they are with the concepts of "cybersecurity" and "cyber hygiene rules". However, the verification, of what exactly the respondents who chose the answer "I know very well and can explain to others" mean, wasn't conducted. 14% of respondents know very well what cybersecurity is and 10% know what cyber hygiene rules are.

In total, 9% of the sample hear about the concept of "cybersecurity" for the first time and 37% hear about the existence of "cyber hygiene rules" for the first time. About half of the respondents have a general concept of "cybersecurity", but do not know the details. Only 29% of respondents chose the same answer regarding "cyber hygiene rules" (see Figure 16).

It is noteworthy that these indicators of knowledge do not vary much with age (see Figure 17): for almost all age groups, the share of "first time" responses is comparable, and all age groups are more familiar with the concept of "cybersecurity" than "cyber hygiene rules". Young people feel more aware of both concepts (the answer "I know very well" was chosen by 21% and 14% of teenagers, respectively). For the older audience, the same indicators constitute 7% for both questions, which is three to two times less.

Figure 16. How familiar are you with the concepts of "cybersecurity" and "cyber hygiene rules"? (% of answers, all respondents)

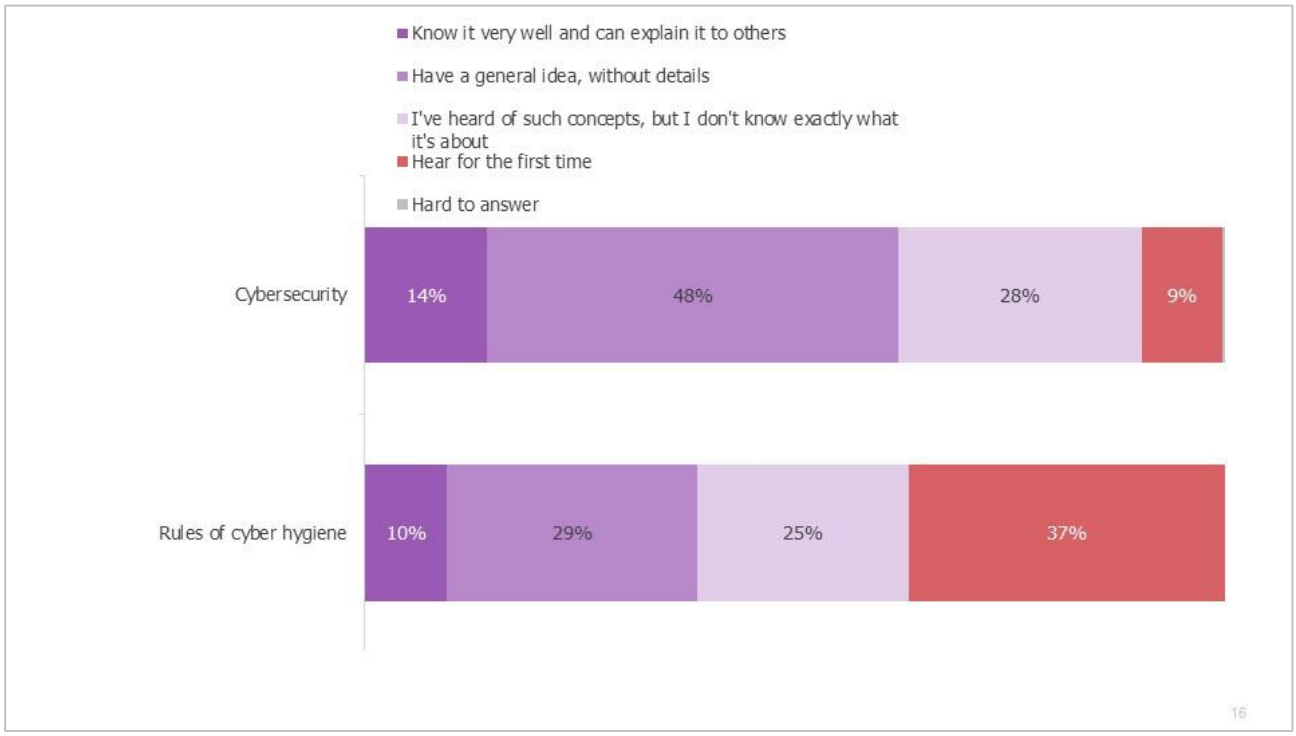
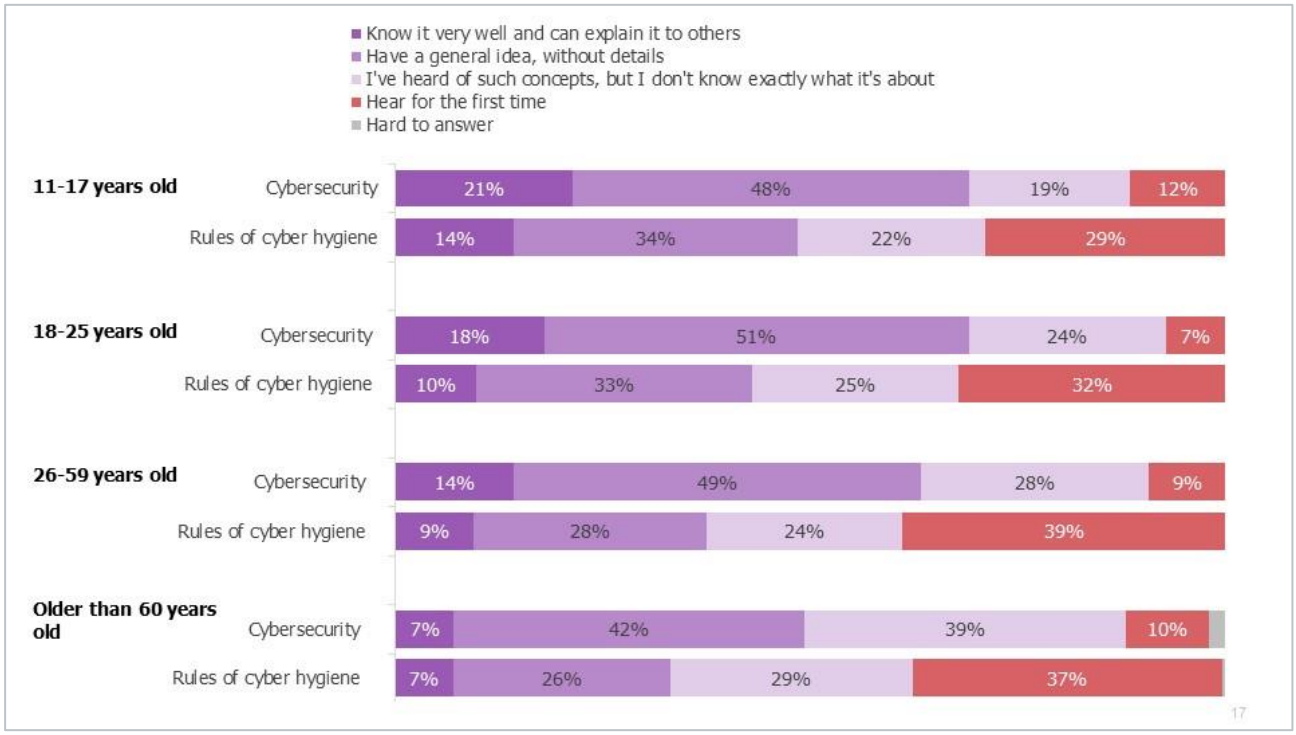


Figure 17. How familiar are you with the concepts of "cybersecurity" and "cyber hygiene rules"? By target groups (% of answers, all respondents)



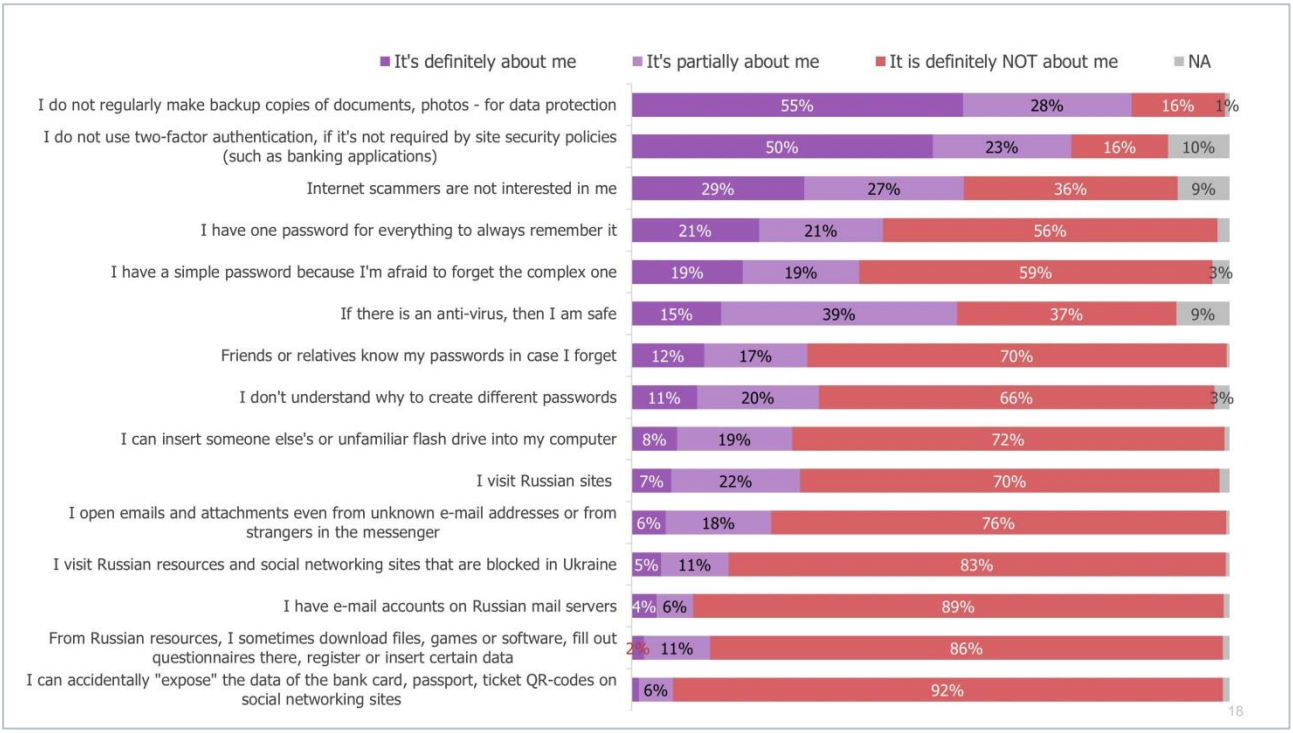
Unsafe behavior

We asked respondents to evaluate several options for unsafe use of the Internet, how similar these behavioral patterns are to their own behavior. Leaders of unsafe behavior are three patterns:

- Lack of backups of documents and data (55% do not do them)
- Failure to use two-factor authentication (50% do not do it)
- Confidence that the user is not interesting to Internet fraudsters (54% are convinced of this at least partially, 29% are sure).

It is also widely believed that use of an antivirus guarantees security against threats (15% are sure, another 39% are partially sure) (see Figure 18.).

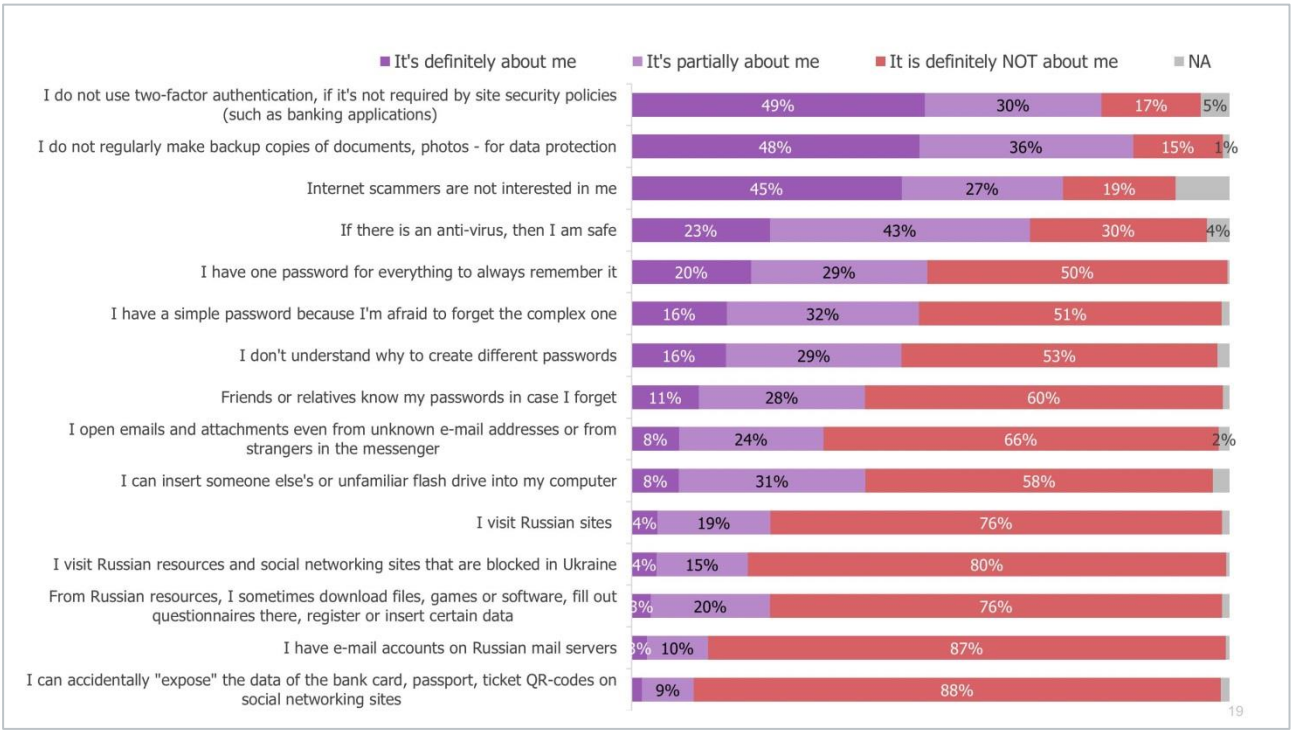
Figure 18. I will read some statements. To what extent do they describe you? (% of answers, all respondents)



Non-use of backups and two-factor authentication are the main patterns of unsafe behavior for all age groups. Teenagers are characterized by the belief that they are not interesting to Internet fraudsters (45% believe this, another 27% are partially sure). Also, teenagers are more convinced than the Internet audience in general, that antivirus provides full security (23% are sure, another 43% are partially sure).

The level of use of a single password for all cases among teenagers is even higher than in the sample as a whole: 20% said that this pattern of behavior completely coincides with theirs (21% in the sample as a whole), another 29% said that the pattern partially coincides with theirs (21% in the sample as a whole) (see Figure 19).

Figure 19. I will read some statements. To what extent do they describe you? (% of responses, target group - teenagers, 11-17 years old)



Young people aged 18-25 are the most cautious target group among others: they use two-factor authentication more regularly and back up documents and data (and the share of those who do not do so is almost twice less than in the sample as a whole).

They also to a lesser extent agree that they are not interesting to Internet fraudsters (20% absolutely agree compared to 29% in the sample as a whole).

However, 40% of this group visit Russian websites - the highest rate among other age groups (among teenagers - 23%, among adults - 28%, among older respondents - 24%) (see Figure 20).

Adults aged 26-59 are also confident that they are not interesting to Internet scammers (26% are sure, another 28% are partially confident and believe in the power of antivirus (13% rely entirely on antivirus, 39% rely partially). Non-use of backups and two-factor authentication are the main patterns of unsafe behavior for this group (see Figure 21).

Figure 20. I will read some statements. To what extent do they describe you? (% of answers, target group - young people, 18-25 years old)

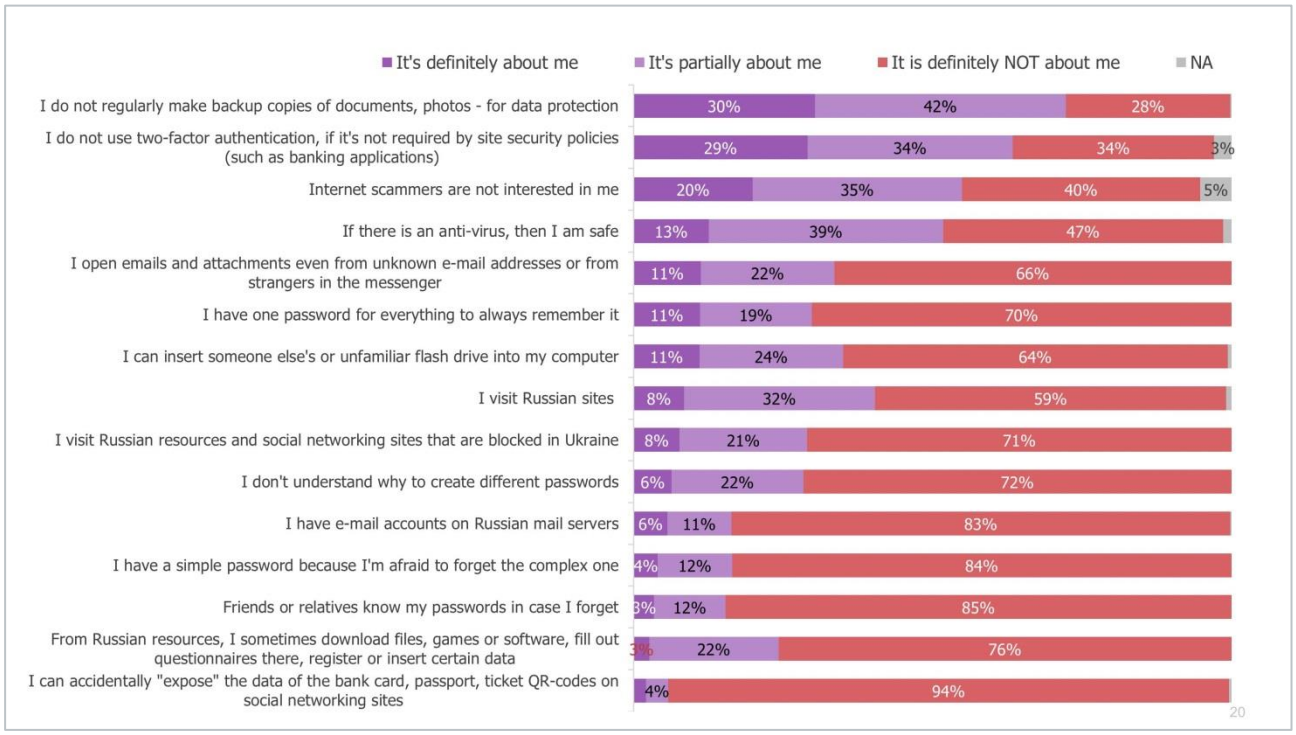
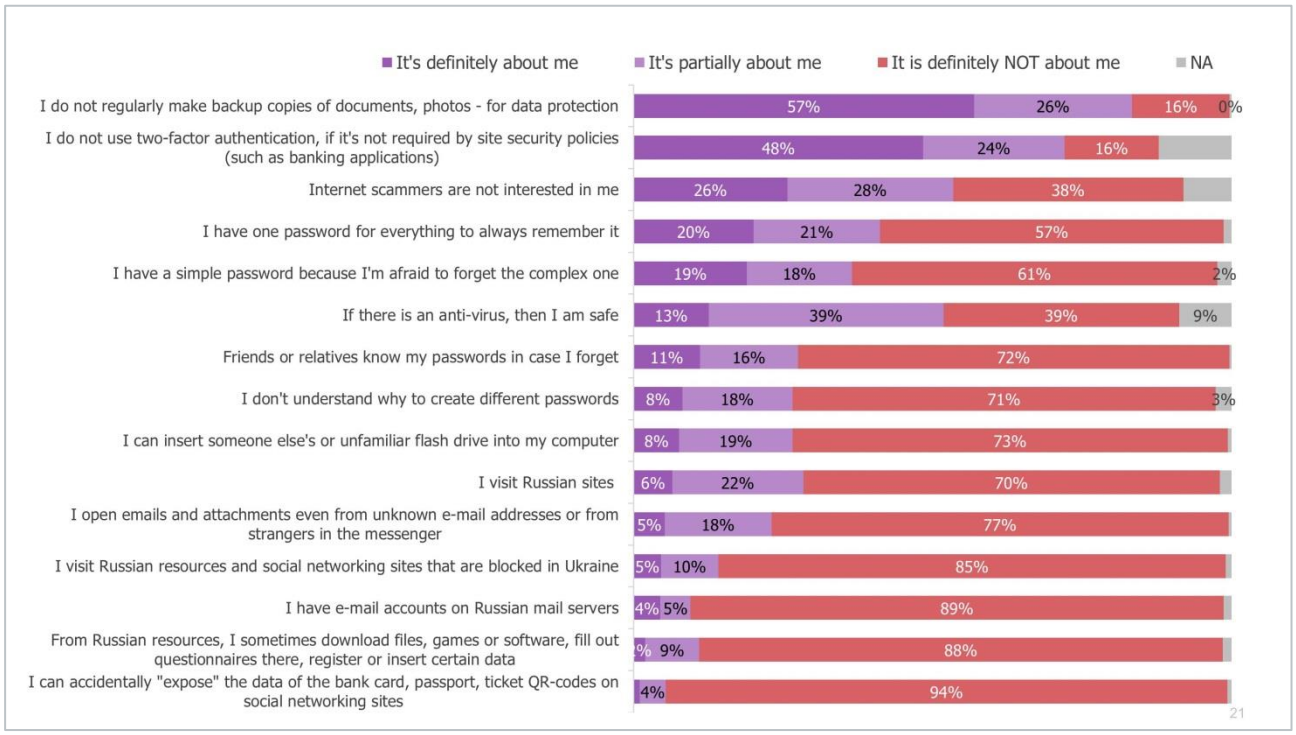


Figure 21. I will read some statements. To what extent do they describe you? (% of responses, target group - adults, 26-59 years old)

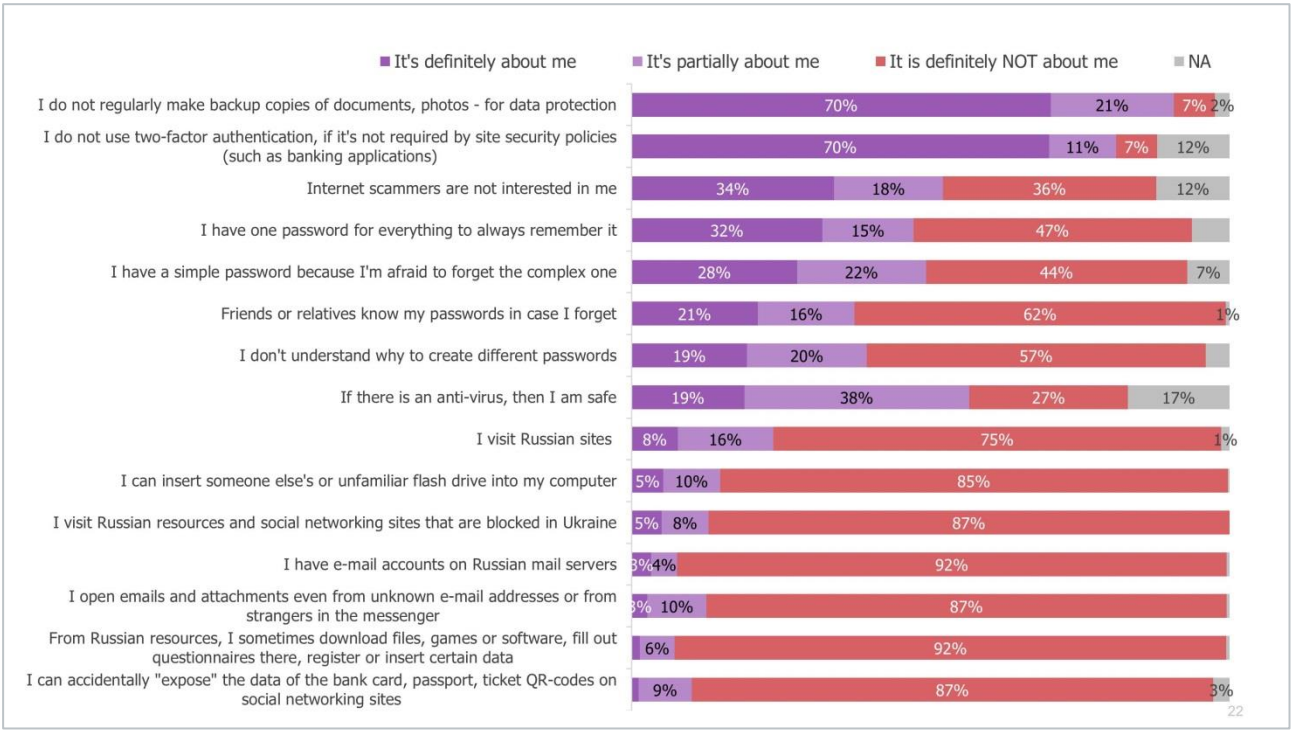


Non-use of backups and two-factor authentication among the oldest audience (over 60 years) is most common for other age groups: 70% of respondents do not do this. Also older people use one simple password more often than the general audience (32% have one password, 28% have a simple password in order not to forget it).

Also, 19% of this group do not understand why they need to create strong passwords (this figure is 11% in the sample as a whole).

Also, older people are more likely to share their passwords with friends or family (21% fully support this behavioral pattern, 16% partially support it, while in the sample as a whole these figures are 12% and 17% respectively) (see Figure 22).

Figure 22. I will read some statements. To what extent do they describe you? (% of responses, target group - people over 60 years old)



A separate type of unsafe behavior may be the use of Russian mailboxes, visiting Russian resources and social networks blocked in Ukraine, as well as visiting Russian websites and performing certain actions there, such as downloading files, filling out questionnaires, registration, etc.

In general, the most common action is visiting Russian websites, 30% of the audience said they do it. The largest share of respondents with such behavior is among young people aged 18-25 (40%), and the smallest - among the oldest audience over 60 years (24%). However, there is a hypothesis that the oldest respondents do not always pay attention to the domain name of the website and may not know which website they are on.

Young people aged 18-25 are also more likely to visit blocked resources in Ukraine than other groups - this behavior was recognized by 29% of this target group (this is almost twice as much as in the sample as a whole, 16%).

Young people (18-25 years old) and teenagers (11-17 years old) also more often than other groups download files from Russian resources, programs, register. The share of respondents with such behavior among these groups is 24% and 23%, respectively. Among the target group of 25-59 years, such behavior is twice less common (11%), and among the oldest respondents - three times less often (8%).

Russian mailboxes are most often used by respondents aged 18-25, 17% are registered on Russian mail servers. In second place in the prevalence of such behavior - teenagers 11-17 years, 13% of them have Russian mailboxes. Older audiences use Russian mail servers less often: among the group aged 26-59 9%, and among the group over 60 - 7%.

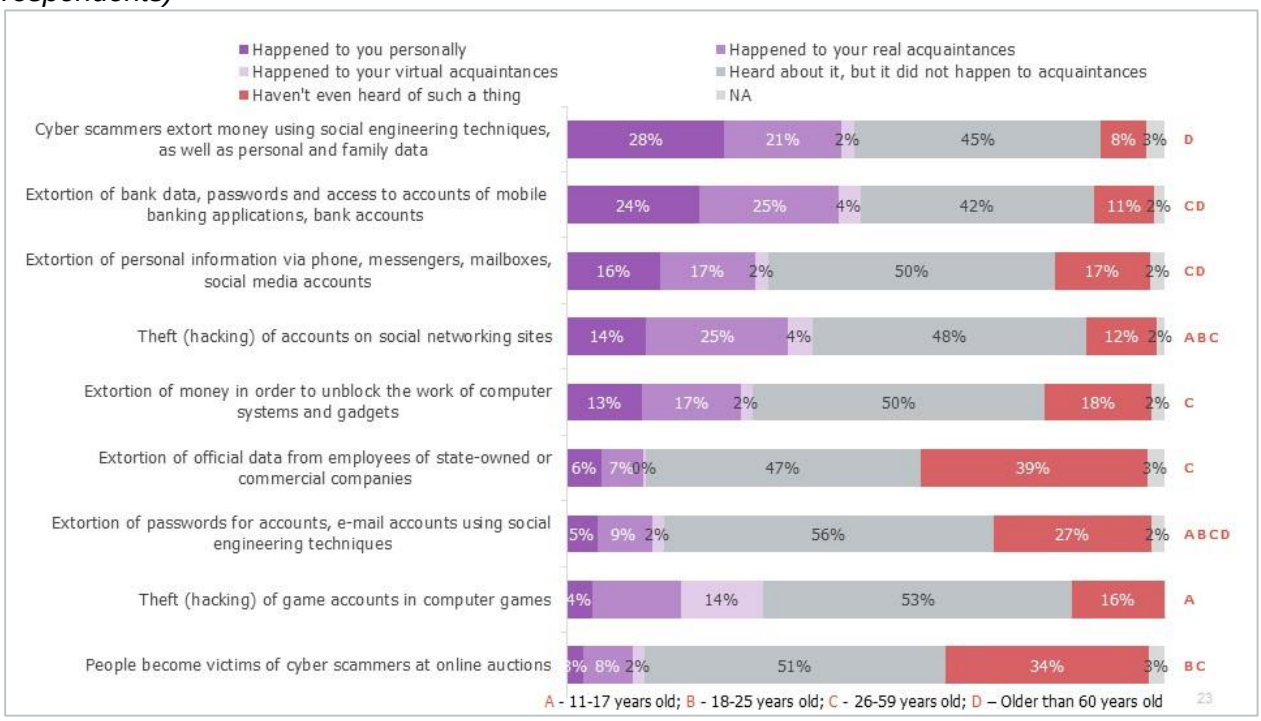
Experience in encountering cyber threats

We asked respondents to rate their experience of dealing with cyber threats. Each target group was offered its own list of cyber threats, which, according to experts, are specific to this age group; for each cyber threat, respondents could indicate whether such a situation occurred with them personally, with their real or virtual acquaintances.

In total, 41% of users in the sample encountered at least one type of cyber fraud. The largest share falls on the group aged 25-59 years, almost every second person has personal experience here (47%). Among young people aged 18-25 this share is 37%, and among the elderly over 60 - 43%. Teenagers were the luckiest - only 7% experienced cyber fraud in person.

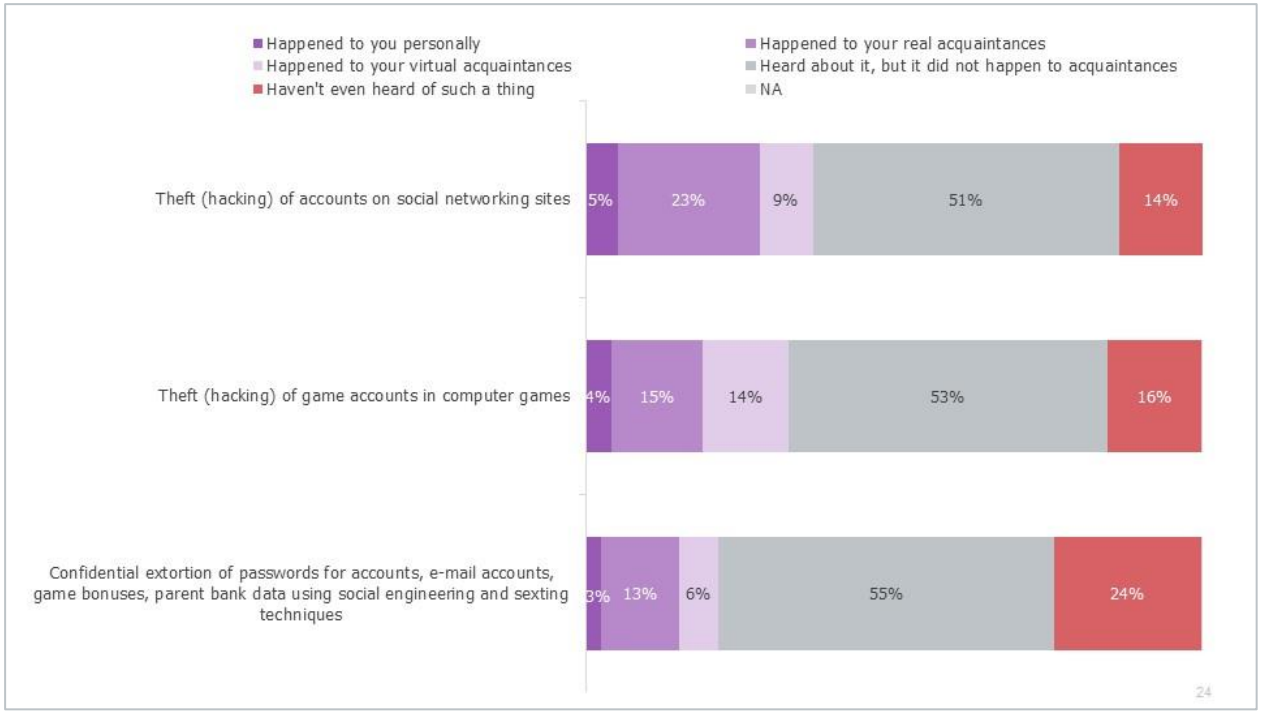
The first place in the sample was taken by the situation when cybercriminals demand money using social engineering methods (manipulation, threats, blackmail), as well as personal and family data (via phone and messengers). This situation was assessed only by the elderly (over 60 years of age), and almost one in three (28%) faced this situation personally. 21% had heard of similar situations from acquaintances (see Figure 23).

Figure 23. I will read the lists of the main threats that the Internet user can face, and you'll tell me if you personally or your acquaintances had encountered this situation? (% of answers, all respondents)



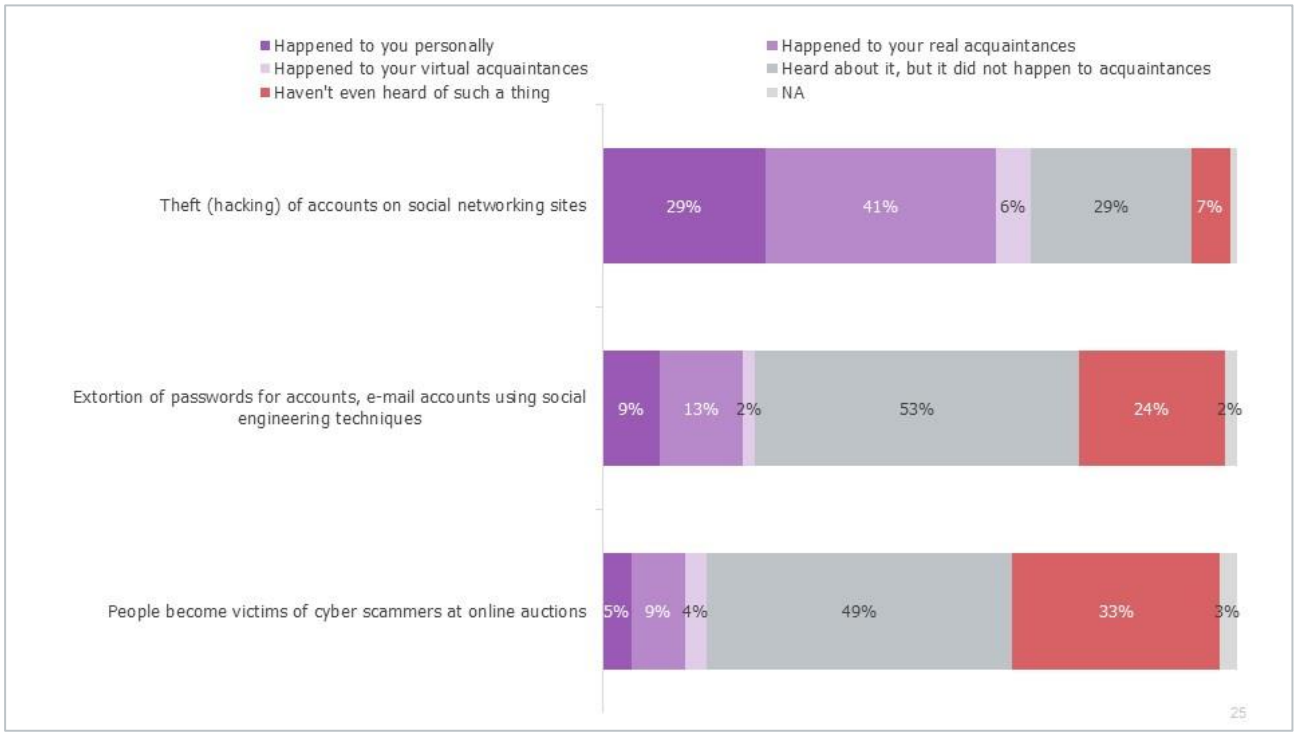
Teenagers encounter account hacking most often (see Figure 24).

Figure 24. I will read the lists of the main threats that the Internet user can face, and you'll tell me if you personally or your acquaintances had encountered this situation? (% of responses, target group - teenagers, 11-17 years old)



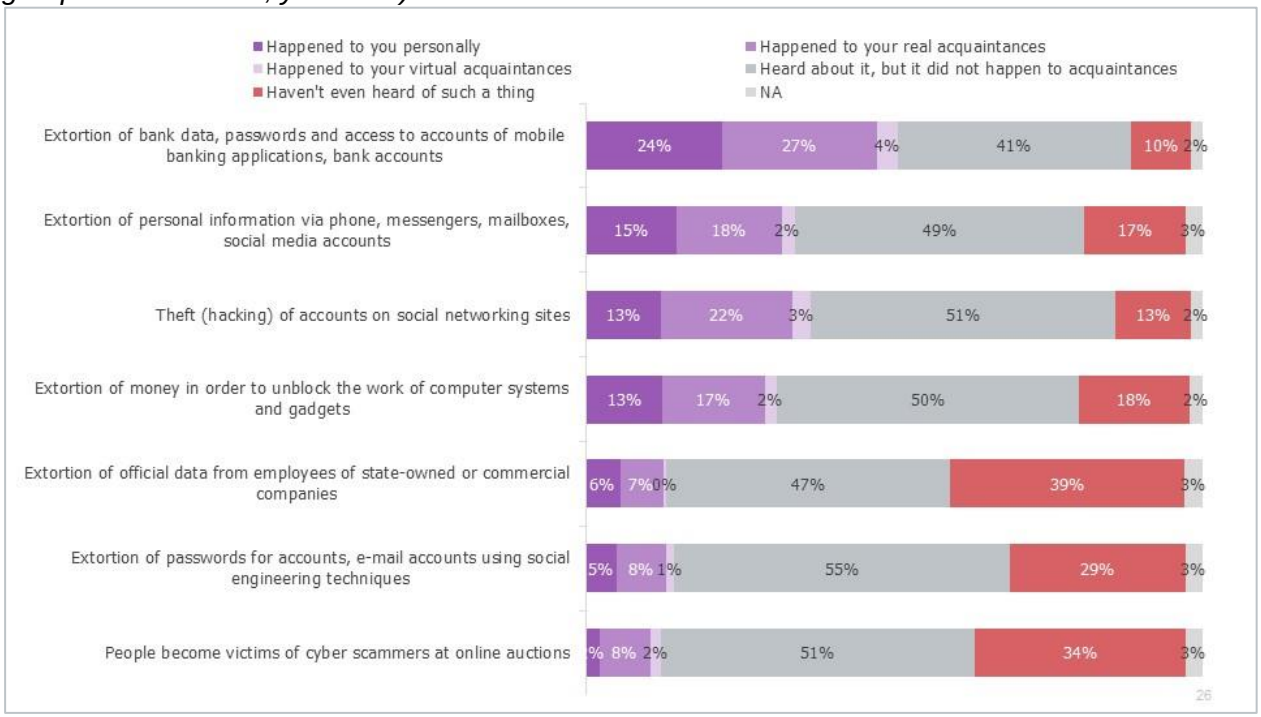
However, young people aged 18-25 encounter the social media account hacking most often compared to other audiences: almost every third (29%) has encountered this in person, 41% know about such cases from acquaintances. And every tenth had personal experience and knows about the experience of friends. In general, 60% of respondents faced account breakage in person or in a friendly circle. Young people face password extortion three times less often (see Figure 25).

Figure 25. I will read the lists of the main threats that the Internet user can face, and you'll tell me if you personally or your acquaintances had encountered this situation? (% of answers, target group - young people, 18-25 years old)



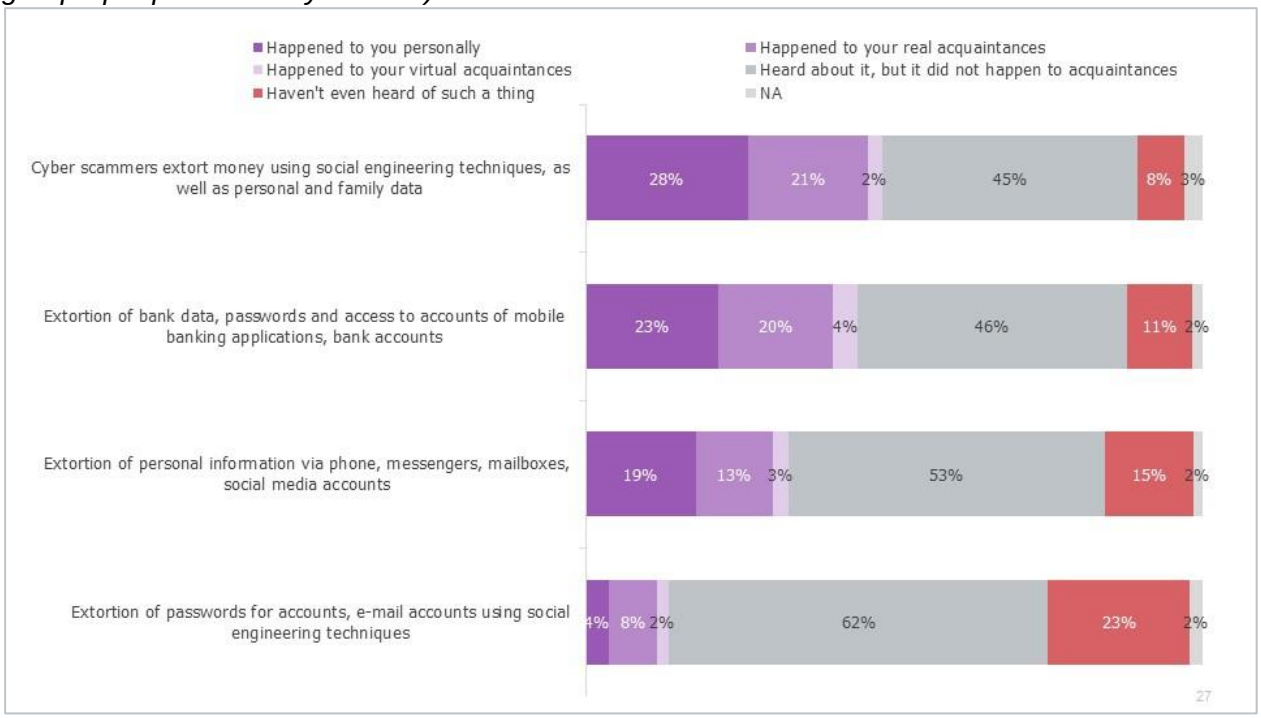
For the adult audience aged 26-59, the most common threat is extortion of bank data, passwords and access to bank mobile application accounts, bank accounts (including via phone, messengers): every fourth person faces this personally, 27% know about such cases from acquaintances. Also common, but less common, are cases of extortion of personal data, hacking of social media accounts and extortion of money to unlock computer systems (the share of the audience who encountered these situations personally is 15%, 13% and 13% respectively) (see Figure 26).

Figure 26. I will read the lists of the main threats that the Internet user can face, and you'll tell me if you personally or your acquaintances had encountered this situation? (% of responses, target group - adults 26-59, years old)



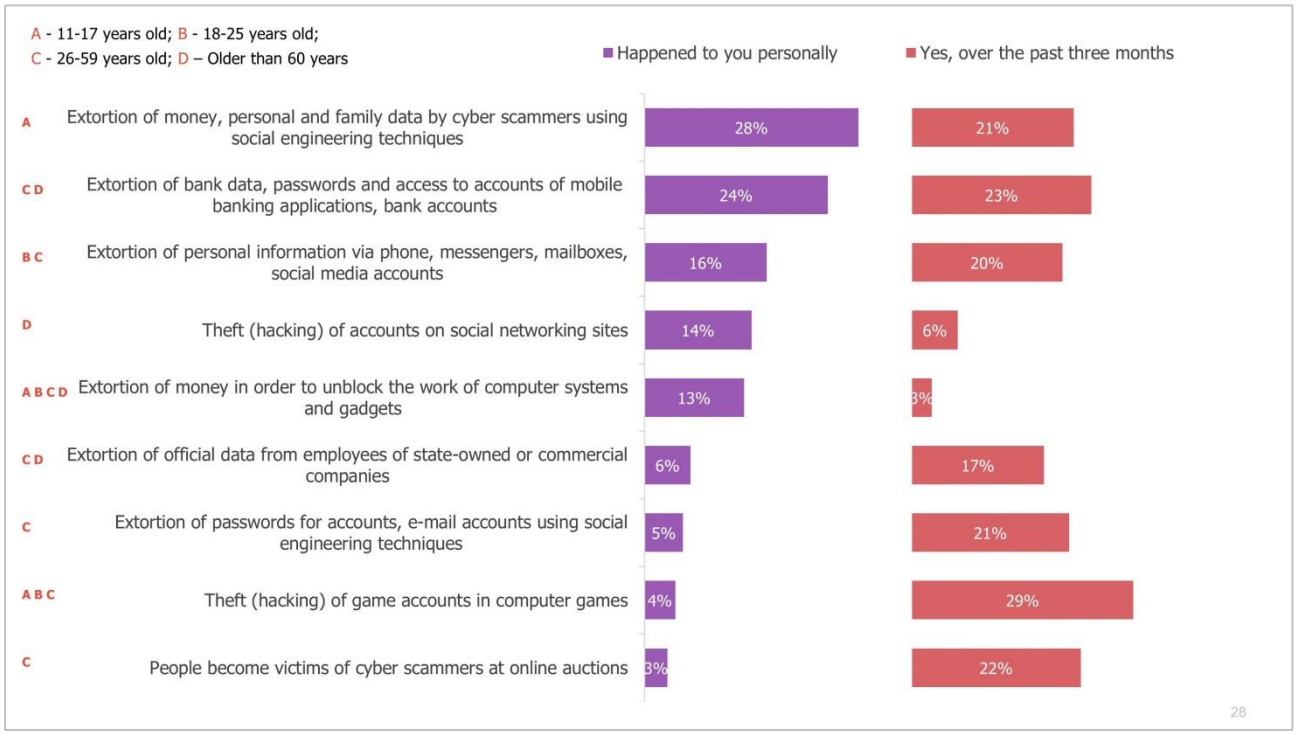
Elderly people face cyber threats more often than other audiences: 28%, 23% and 19%, respectively, faced extortion of money, bank and personal data (see Figure 27).

Figure 27. I will read the lists of the main threats that the Internet user can face, and you'll tell me if you personally or your acquaintances had encountered this situation? (% of responses, target group - people over 60 years old)



A significant proportion of situations that occurred to respondents personally occurred during the last 3 months (see Figure 28).

Figure 28. You said that some threatening situations had happened to you personally. Please, specify when exactly this happened last time? (% of responses, respondents who faced threats personally)



41% of teenagers who have encountered trust password extortion have had this experience over the last three months. Attacks on gaming accounts and social media accounts have also occurred recently (29% and 23% of those who have encountered this situation have encountered it in the last 3 months) (see Figure 29).

Attacks on older audiences (young people aged 18-25) are less common: only 4% of those who have experienced account hacking (and this is the most common cyber fraud in this age group) have encountered this situation over the last three months and almost half (48%) encountered it more than a year ago (see Figure 30).

Respondents of the adult (26-59 years) group face threats a little more often than young people: 24% of those who have faced extortion of bank data have experienced this negative experience in the last 3 months. Only 2% were victims of cyber-fraud in online auctions, but 27% have been in recent months (see Figure 31).

Among the older group, one in five extortions of money or bank details occurred over the last three months (see Figure 32).

Figure 29. You said that some threatening situations had happened to you personally. Please, specify when exactly this happened last time? (% of responses, respondents who faced threats personally, target group - teenagers, 11-17 years)

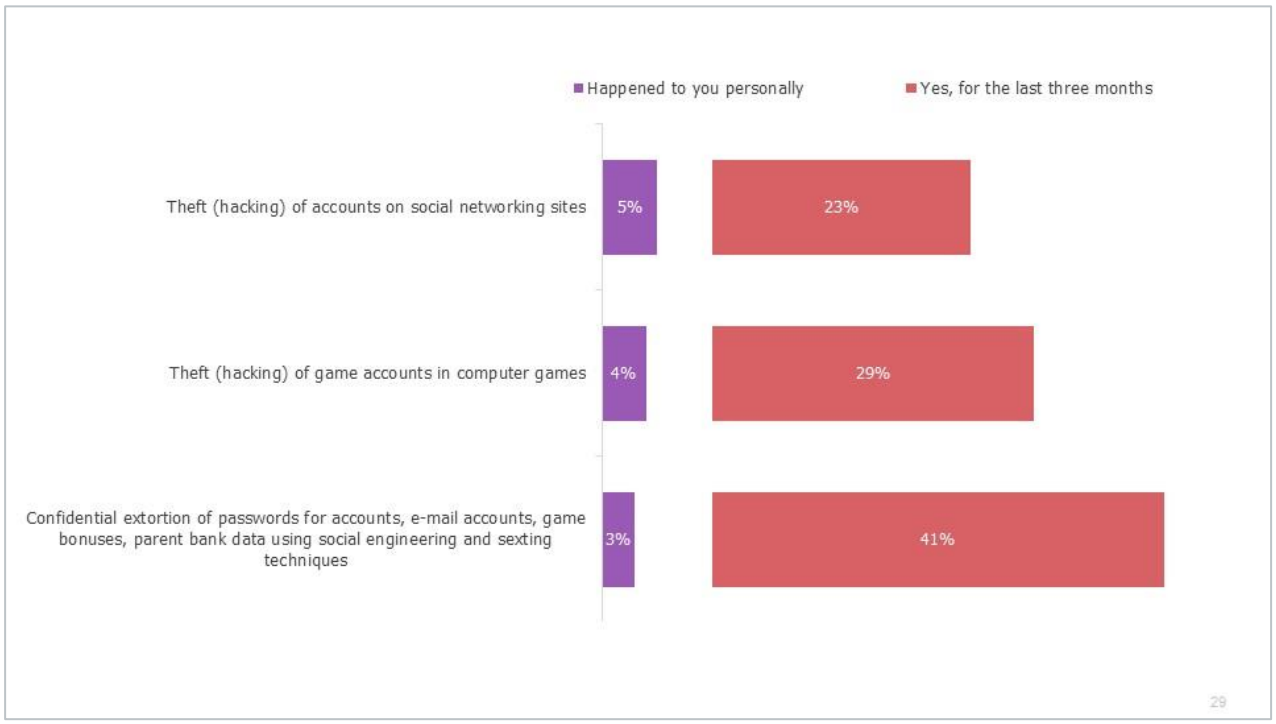


Figure 30. You said that some threatening situations had happened to you personally. Please, specify when exactly this happened last time? (% of responses, respondents who faced threats personally, target group - young people,18-25 years old)

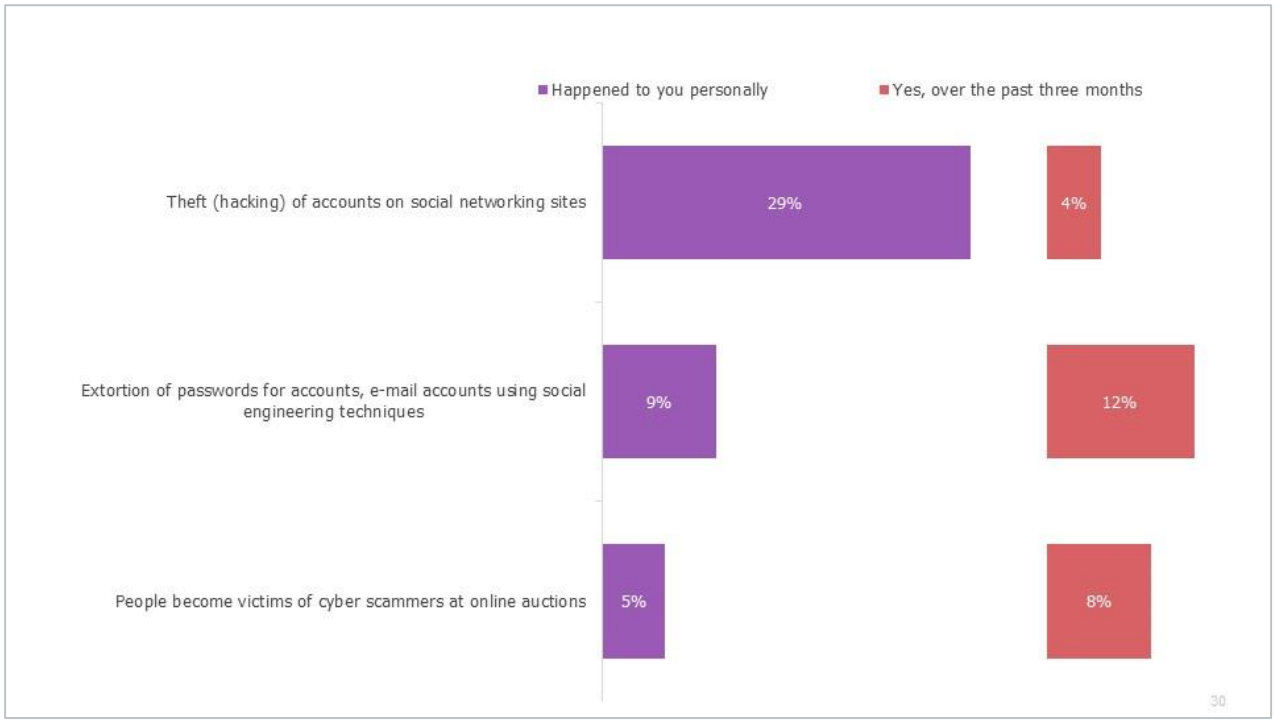


Figure 31. You said that some threatening situations had happened to you personally. Please, specify when exactly this happened last time? (% of responses, respondents who faced threats personally, target group, adults - 26-59 years old)

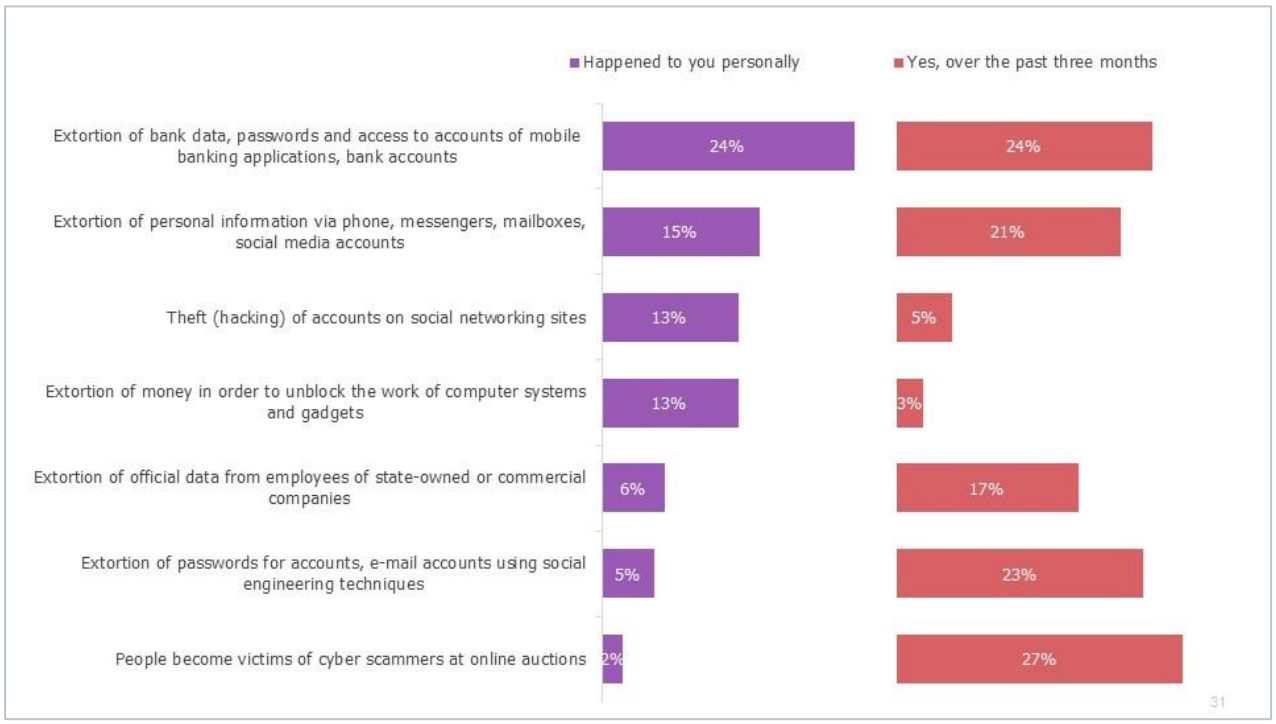
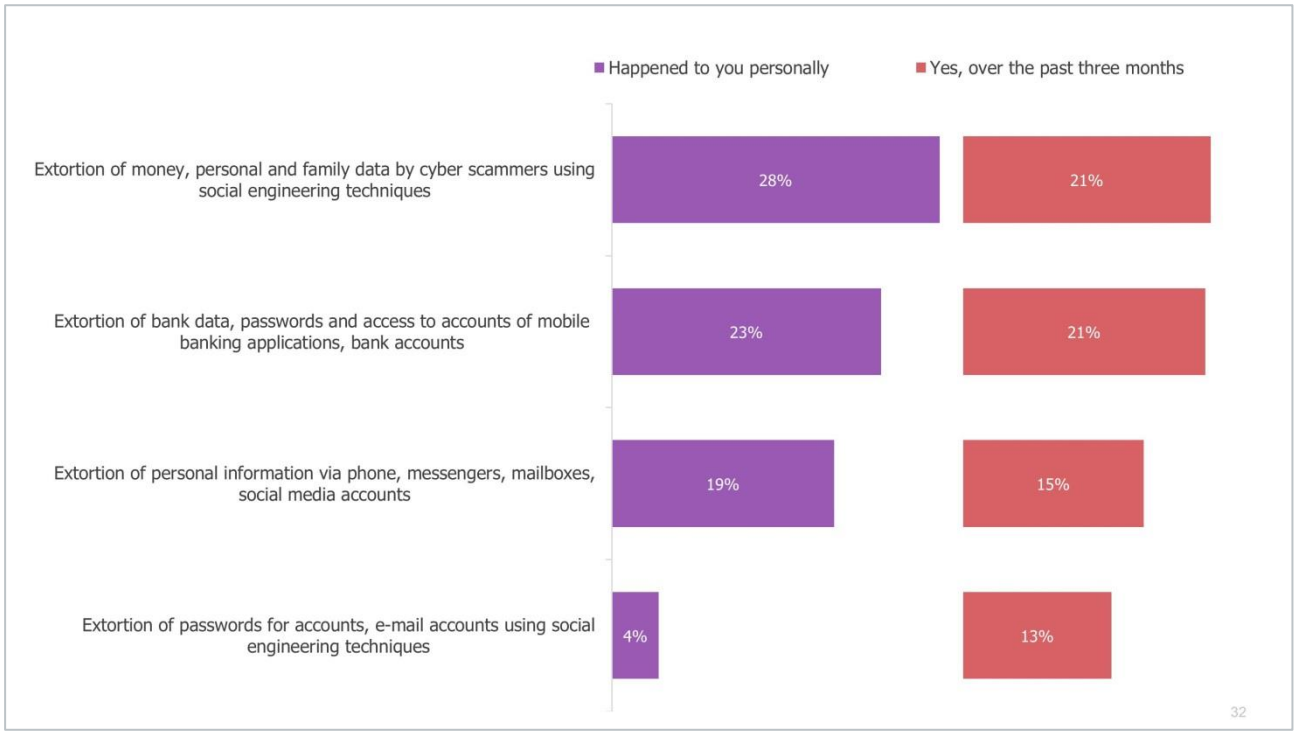


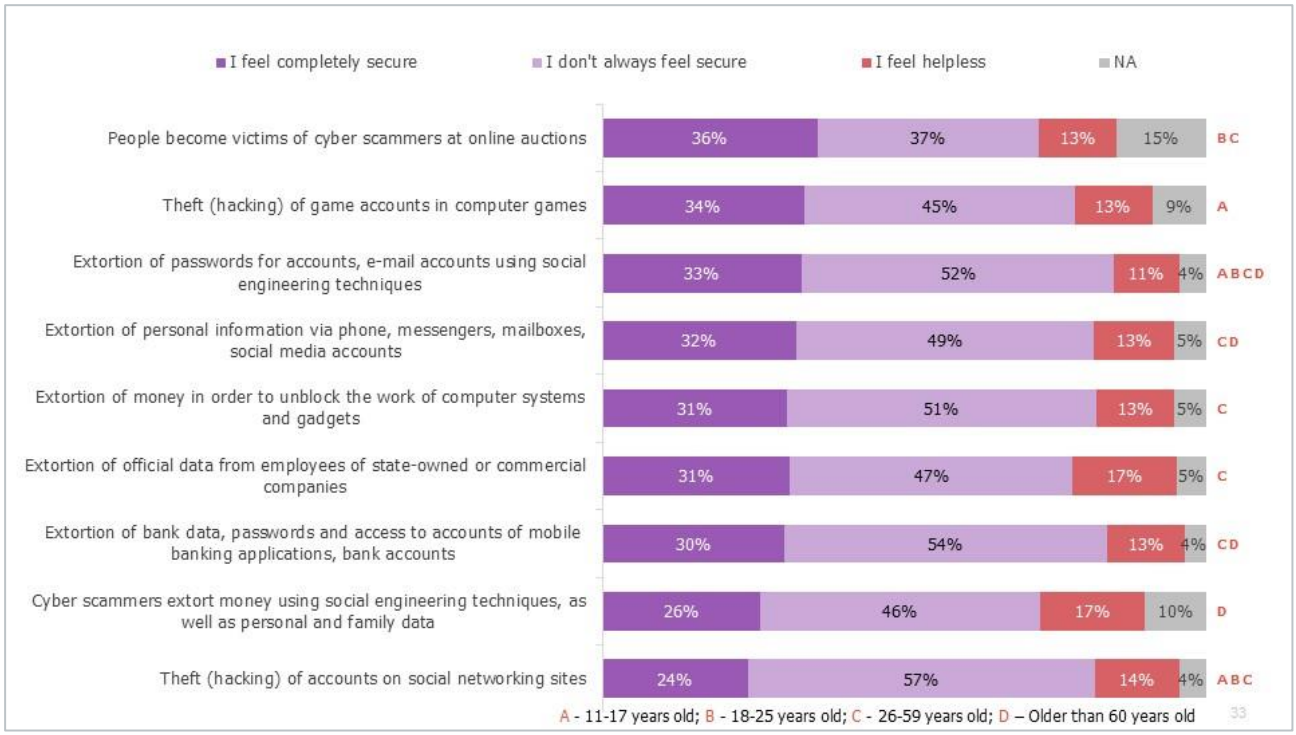
Figure 32. You said that some threatening situations had happened to you personally. Please, specify when exactly this happened last time? (% of responses, respondents who faced threats personally, target group - people over 60 years old)



Despite all cases of threats, respondents rarely feel completely vulnerable in such situations: the share of such responses varies from 11 to 17% depending on the threat. Older people often feel completely defenseless in cases where fraudsters demand money using social engineering methods.

The most common answer for all types of threats is the answer "I do not always feel secure" - it was chosen by 37% to 57% of respondents depending on the threat. However, about a third of respondents feel completely secure from most threats, with the lowest proportion of "feel completely secure" responses as for the threat of hacking social media accounts (24%) (see Figure 33).

Figure 33. How secure do you feel about certain threats? (% of responses, respondents who faced threats)



- Teenagers are a fairly self-confident group of Internet users - 34% to 43% of those who face threats feel completely secure (see Figure 34).
- Young people are less confident about account hacking (31% feel completely secure) and more confident about password protection (43% feel completely secure) (see Figure 35).
- The adult audience is also the least confident about account hacking (21% feel completely secure), with 30% to 34% fully secure for the rest of the threats (see Figure 36).
- Almost all older respondents do not differ from the general audience in terms of the level of security: 26% - 32% feel completely secure, and 12% - 17% feel vulnerable, depending on the type of threat (see Figure 37).

Figure 34. How secure do you feel about certain threats? (% of responses, respondents who faced threats, target group - teenagers, 11-17 years old)

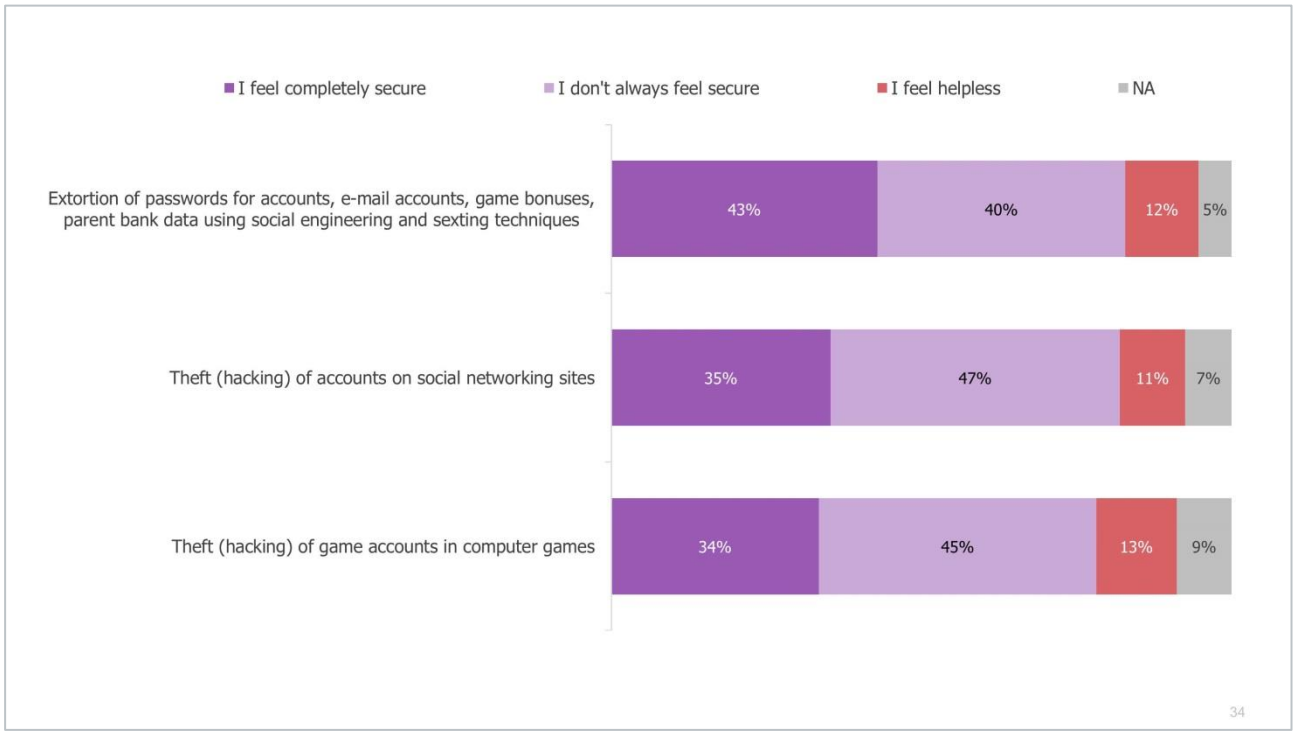


Figure 35. How secure do you feel about certain threats? (% of responses, respondents who faced threats, target group - young people, 18-25 years old)

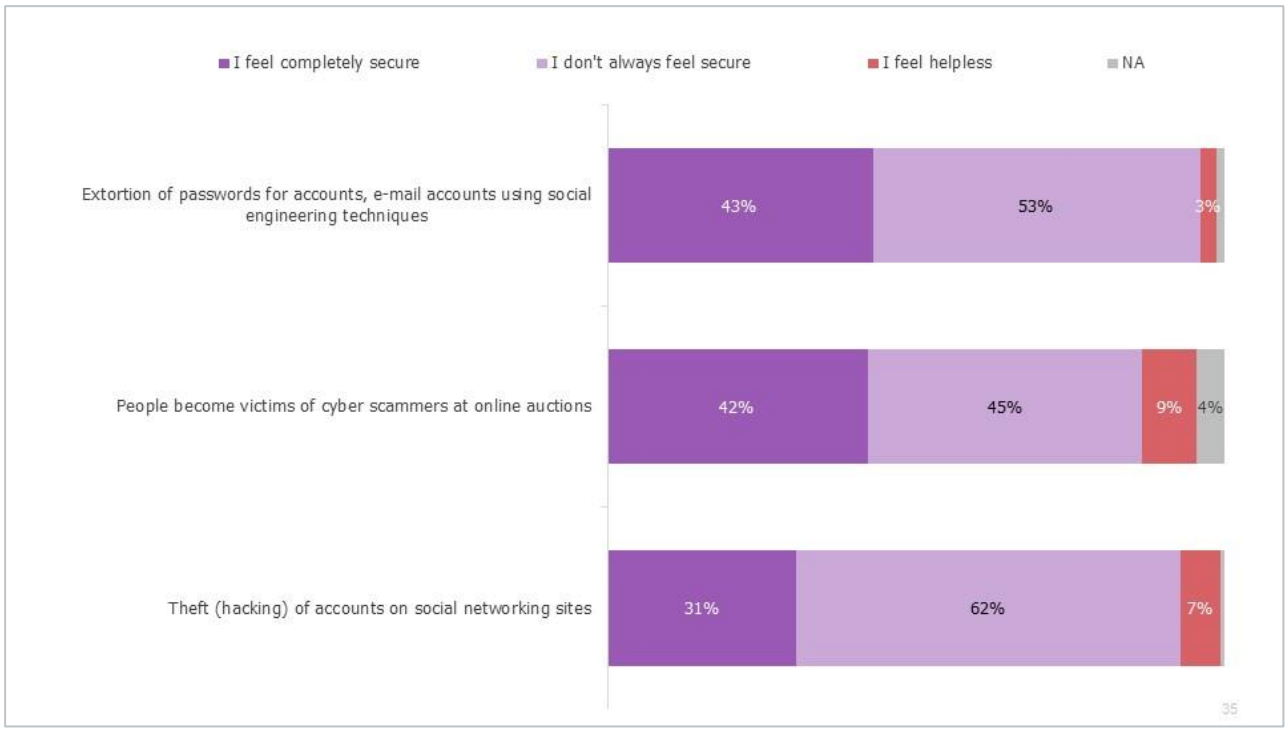


Figure 36. How secure do you feel about certain threats? (% of responses, respondents who faced threats, target group - adults, 26-59 years old)

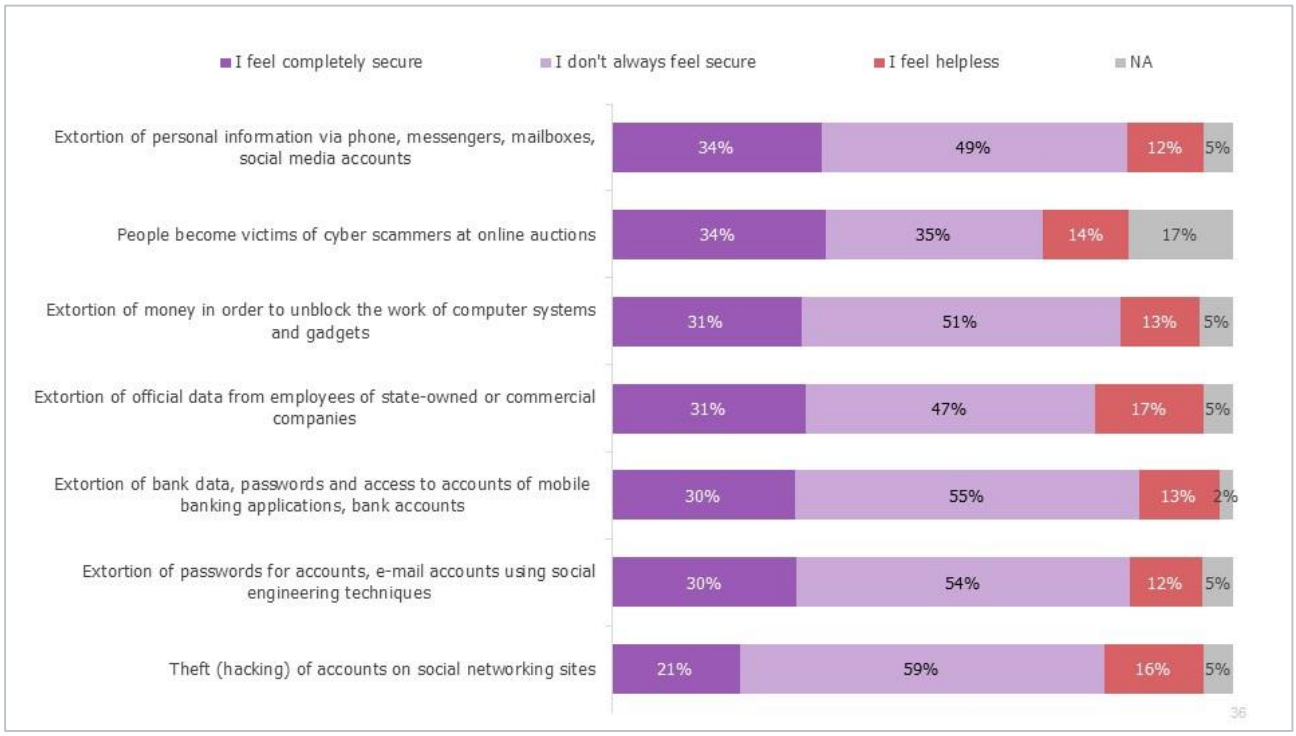
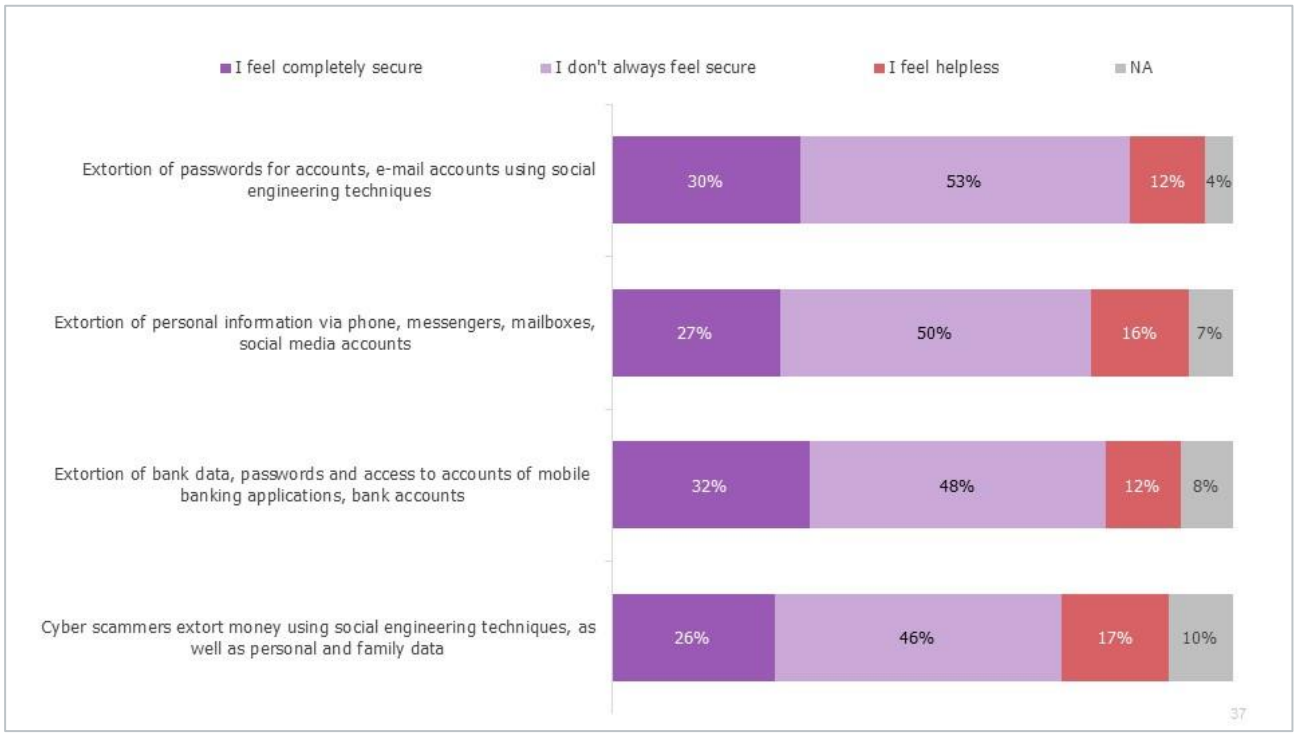


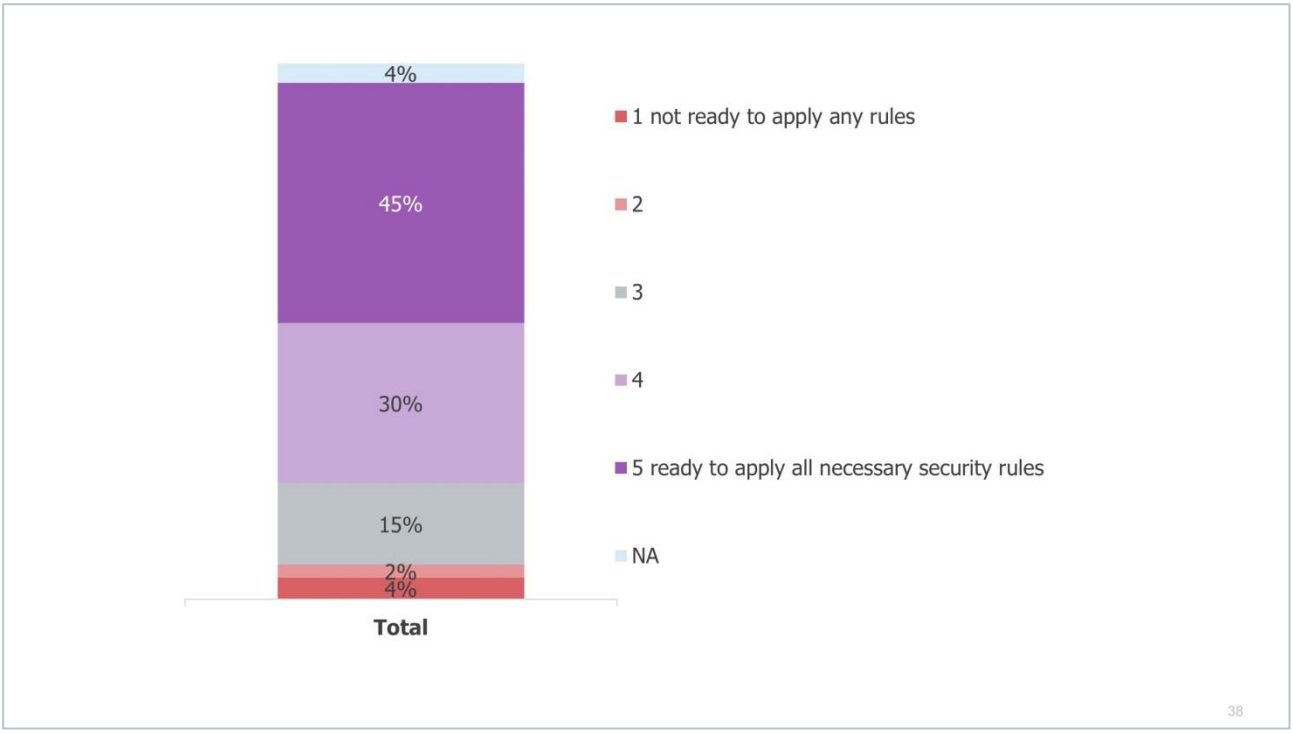
Figure 37. How secure do you feel about certain threats? (% of responses, respondents who faced threats, target group - people over 60 years old)



Awareness of cybersecurity rules

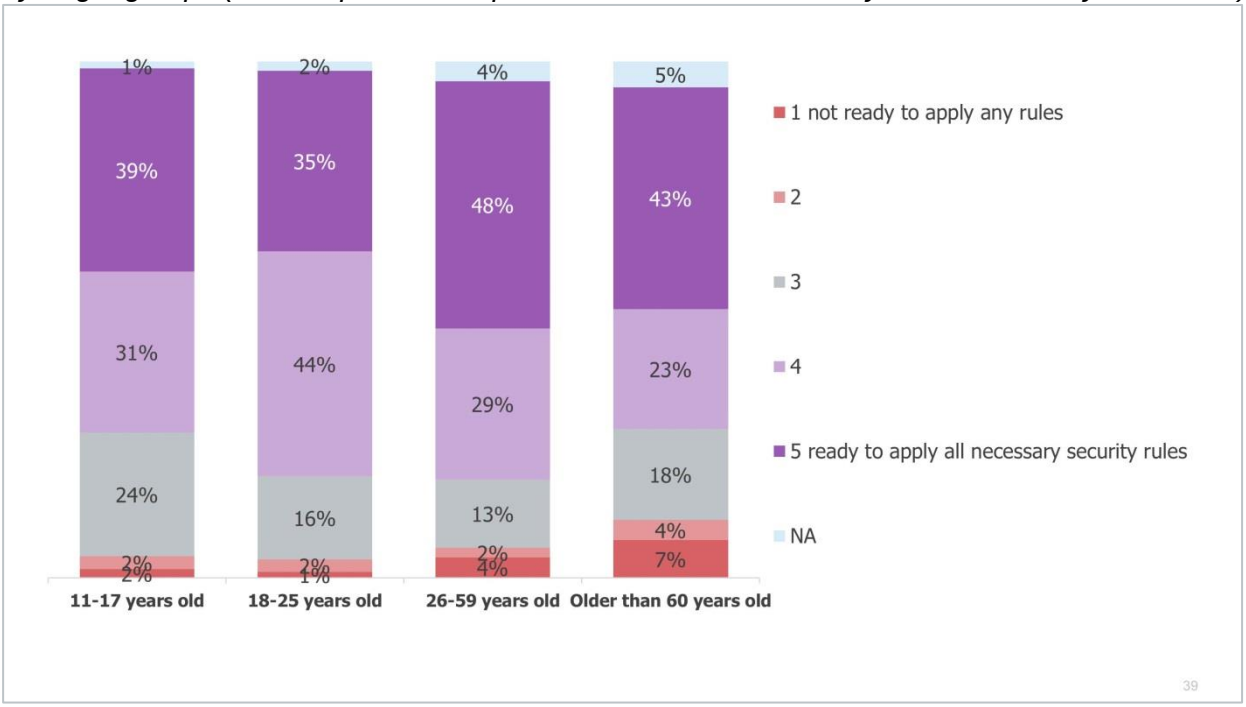
Despite a fairly high level of feeling of security, most respondents are willing to apply security rules: 45% of the sample are generally willing, and 30% are mostly willing to apply all necessary security rules (or at least declare such readiness) (see Figure 38).

Figure 38. How willing are you to apply cyber hygiene rules to secure yourself from these threats? (% of responses, respondents who do not feel fully secured from cyber threats)



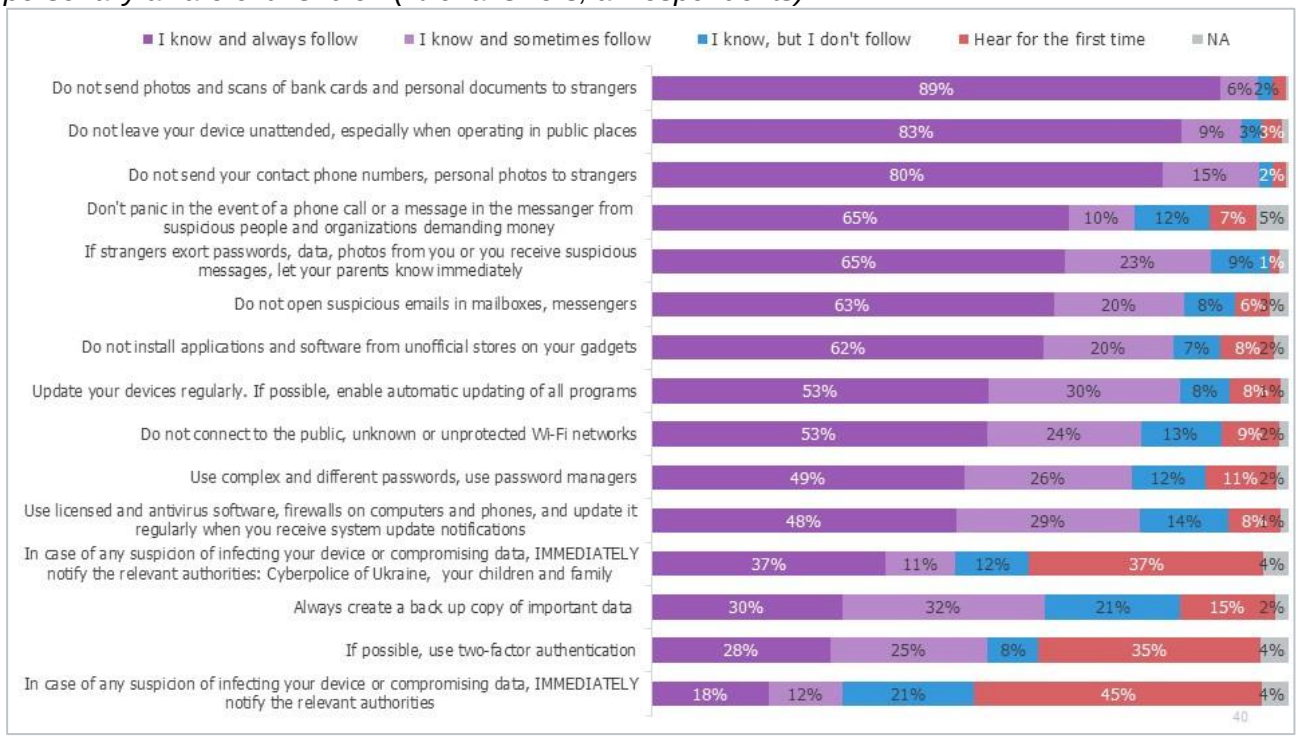
The target groups "young people" and "adults" show the greatest readiness to use the security rules - 79% and 77% of respondents respectively declare their readiness to use all necessary security rules (the sum of scores "4" and "5" on a five-point scale), whereas in the "adults" group unquestioning willingness to follow the rules (score "5") is 48% - this is the highest rate among all groups. According to this indicator, the second place is taken by older people (over 60 years old) - 45% of them declare their readiness to follow all necessary security rules. However, it is in this group that there is the highest level of resistance to following security rules: 7% are not ready to follow any rules (score "1"), another 4% - rather not ready to follow (score "2") (see Figure 39).

Figure 39. How willing are you to apply cyber hygiene rules to secure yourself from these threats? By target groups (% of responses, respondents who do not feel fully secured from cyber threats)



We gave the audience the opportunity to assess the attitude to the basic rules of cyber hygiene. The audience is at least familiar with most of the rules: only 5 rules received a share of "first time" responses of more than 10% (see Figure 40). However, awareness of the rules varies considerably with age.

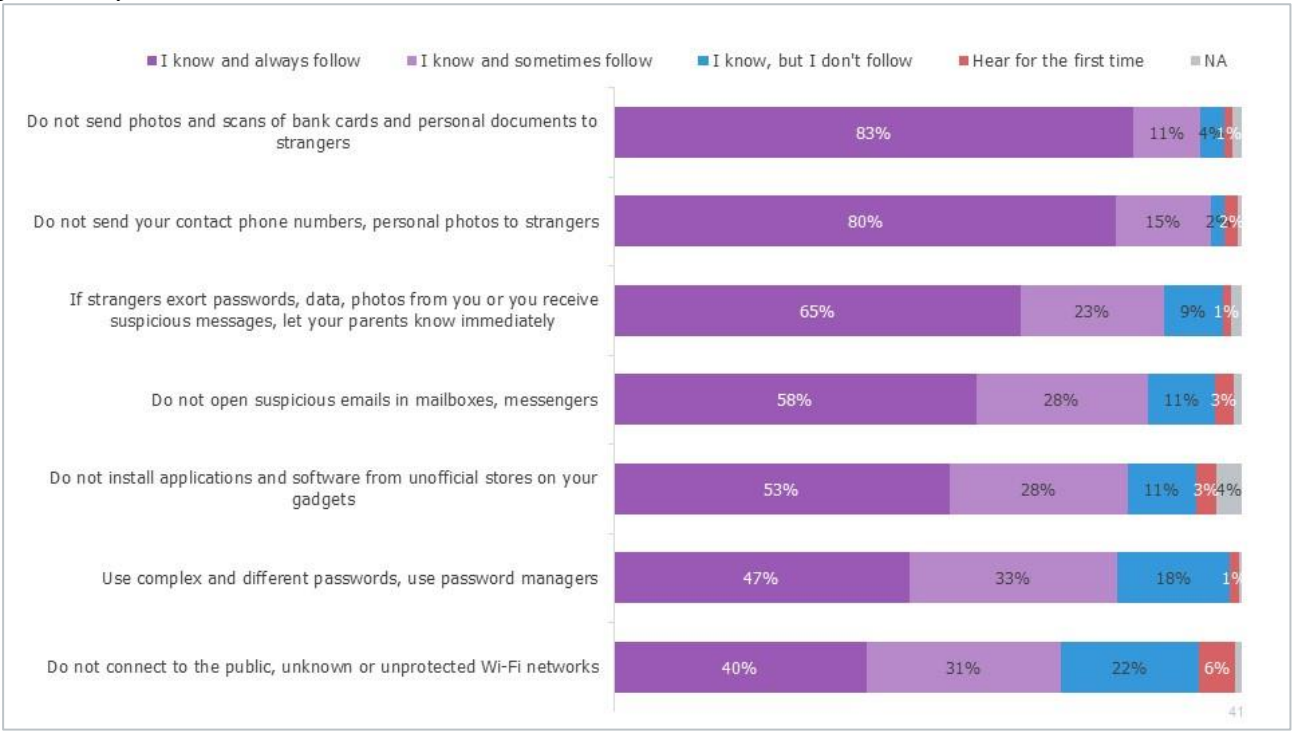
Figure 40. I will read some basic rules of cyber hygiene, and you tell me to what extent are you personally aware of this rule? (% of answers, all respondents)



Yes, teenagers are fairly familiar with all the rules, the share of respondents who know each rule exceeds 90%. The least known are the rules "Do not install applications from unofficial stores" (92% know) and "Do not connect to public Wi-Fi networks" (93% know). An even larger proportion of respondents know the rest of the rules. However, not all of them are followed: yes, the rule on refraining from connecting to public Wi-Fi networks is always followed by 40% of respondents, and not followed by 22%.

Teenagers most often follow the rules prohibiting sending scans of bank cards or documents and contact details or photos - 83% and 80%, respectively, declare strict compliance with these rules (see Figure 41).

Figure 41. I will read some basic rules of cyber hygiene, and you tell me to what extent are you personally aware of this rule? (% of answers, all respondents, target group - teenagers, 11-17 years old)



Young people are also well acquainted with most of the proposed rules. Only one rule turned out to be unfamiliar to respondents: 42% said it was the first time they had heard of reports of suspicions of infection or data compromise. The second place by the level of poor awareness is taken by the rule of using two-factor authentication: 15% hear about it for the first time.

The two rules that young respondents follow best are "do not send photos and scans of bank cards" and "do not leave the device unattended" - 94% and 87% of respondents, respectively, declare compliance with these rules (see Figure 42).

The same two rules are most often followed by adult respondents (89% and 83%, respectively). Adult respondents, as well as young people, are relatively poorly acquainted with the rules on the necessity to notify the relevant authorities in case of suspicion of infection or data compromise (42% hear for the first time) and the use of two-factor authentication (39% hear for the first

time). Also, this group is less aware than younger groups of the need to make regular backups (17% hear for the first time) (see Figure 43).

Figure 42. I will read some basic rules of cyber hygiene, and you tell me to what extent are you personally aware of this rule? (% of answers, all respondents, target group - young people, 18-25 years old)

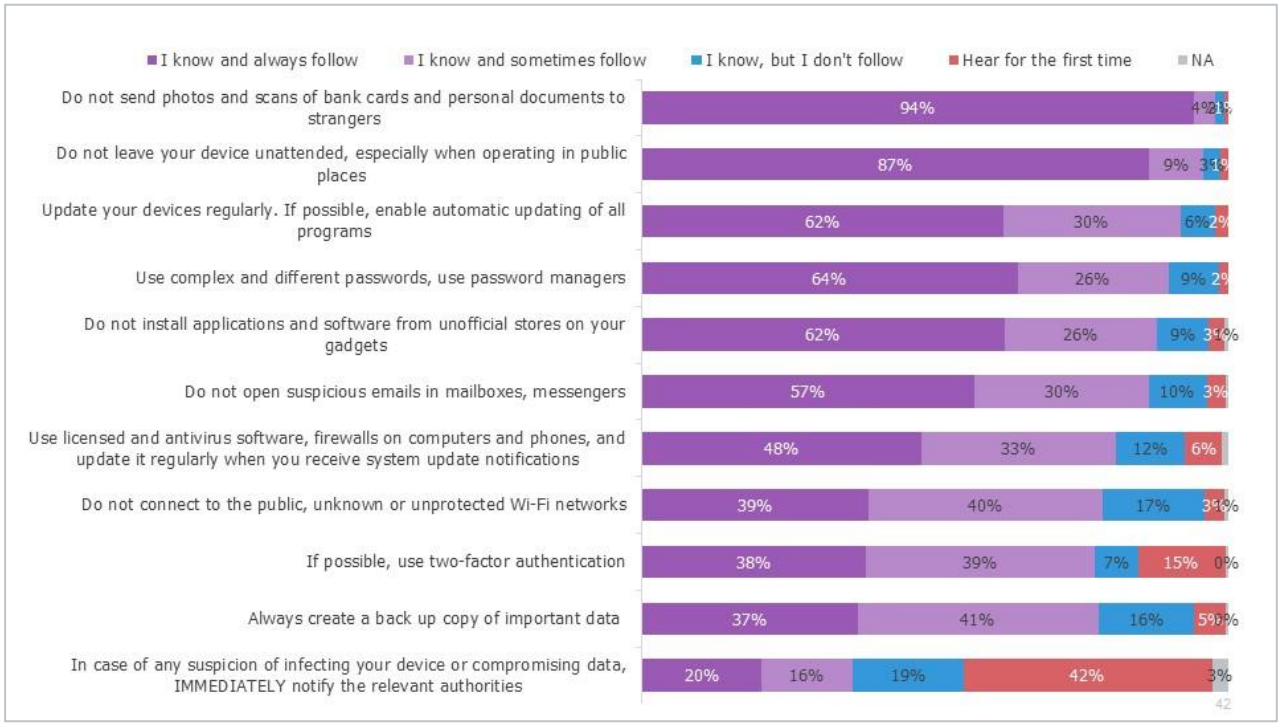
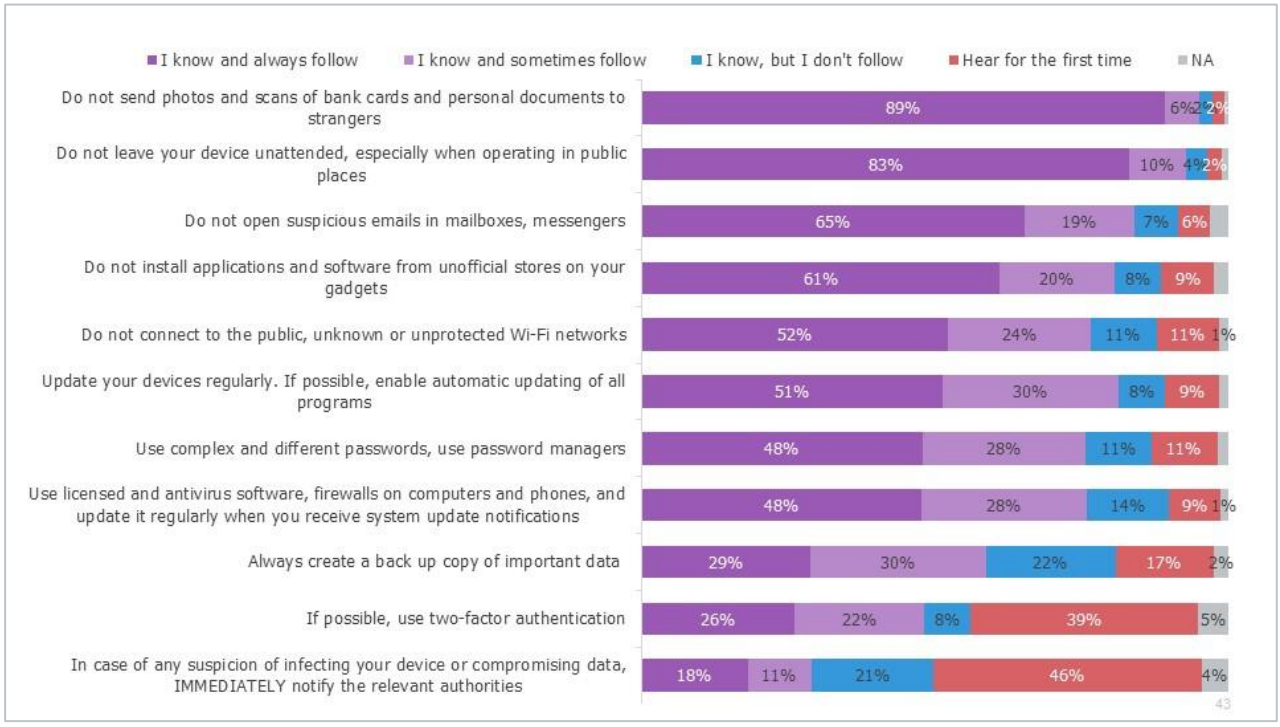


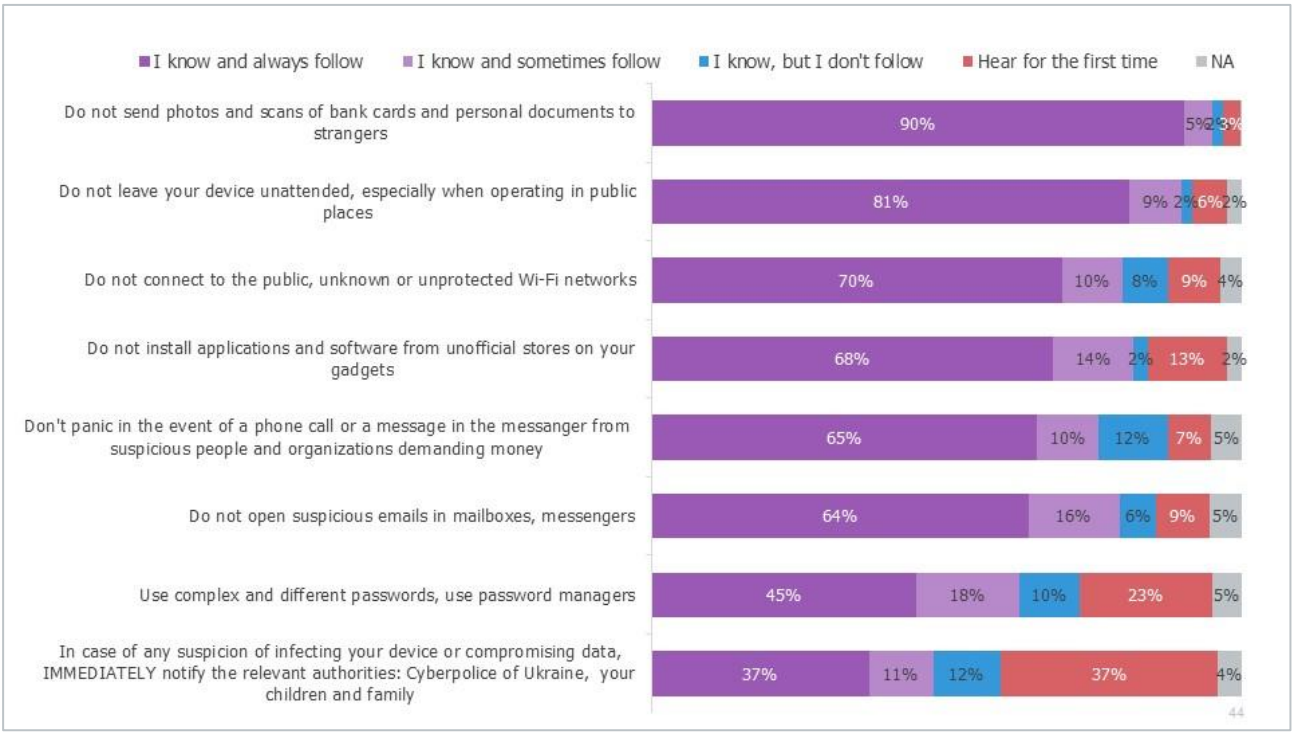
Figure 43. I will read some basic rules of cyber hygiene, and you tell, how much you are personally aware of this rule? (% of answers, all respondents, target group - adults, 26-59 years old)



Older respondents, like other groups, are aware of the danger of not sending photos and scans of bank cards or documents to strangers (90% follow the rule not to do so). 81% do not leave the device unattended.

Only 45% of older respondents use complex and different passwords. This share is comparable to the corresponding indicator in the group of adult respondents (48%). But if the 26-59 age group is aware of the necessity to use complex and different passwords, and deliberately does not do so, older respondents often (23%) are not even aware of such a security rule (see Figure 44).

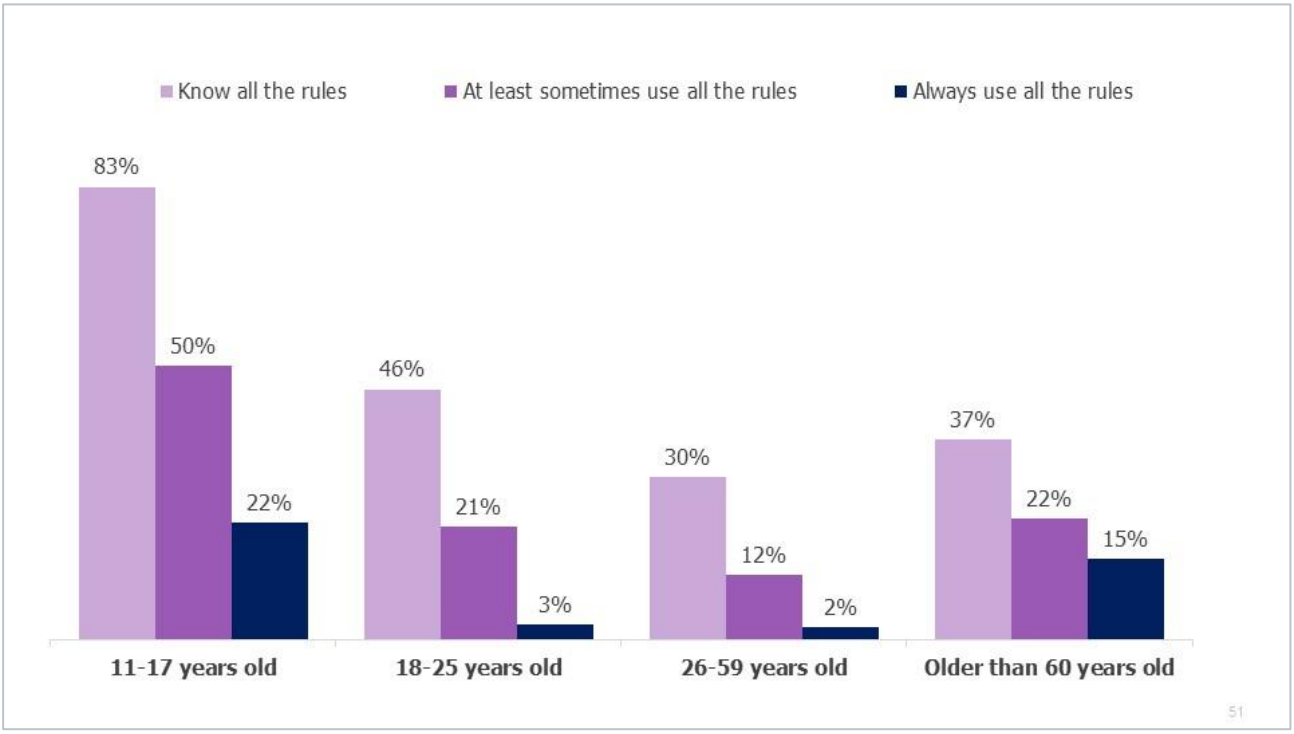
Figure 44. I will read some basic rules of cyber hygiene, and you tell me to what extent are you personally aware of this rule?? (% of answers, all respondents, target group - people over 60 years old)



We analyzed the extent to which each age group knows and follows a number of cybersecurity rules in general. Yes, teenagers aged 11-17 are the most knowledgeable group: 83% know all the rules of cybersecurity. However, only 50% follow all the rules at least sometimes, and only 22% constantly follow all the rules. However, compliance with the rules in the group of teenagers is also the highest among other target groups: among young people aged 18-25 at least sometimes follow the rules 21%, among adults aged 25-59 - 12%, and among the oldest respondents over 60 - 22 %.

The oldest group of respondents is the least aware: only 37% know about all cybersecurity rules for this group. But also these respondents are the most conscious: the share of those who follow all the rules, among those who are familiar with them, for the oldest audience is 40%. This is the highest rate among other groups: for teenagers it is 26%, and for young people 18-25 years and adults 26-59 years - only 6% and 8%, respectively (see Figure 45).

Figure 1. Knowledge and implementation of cybersecurity rules in general



Internet safety

We asked respondents to rate the safety of their own use of the Internet on a scale of 1 to 10, where 1 means "very unsafe" and 10 - "completely safe". In general, slightly more than half of the respondents rate their own use of the Internet as completely or fairly safe (scores "9" or "10" on a 10-point scale). The proportion of those who believe that they are behaving unsafely (scores from 1 to 6) is 30% (see **Error! Reference source not found.**).

These estimates vary considerably with age: yes, among teenagers (11-17 years) and young people (18-25 years) a share of those who believe that they behave unsafely (19% and 17%, respectively) is smaller, while among people over 25 years, one in three considers behavior as unsafe.

Among teenagers the largest share is among those who believe that they behave completely safely (37%), while among other age groups this share is significantly lower.

In general, the proportion of young people under the age of 25 who consider their behavior safe is higher than the proportion of those who consider their behavior as unsafe. Among respondents over the age of 25, the proportion of those who are aware of the dangers of behavior is higher than the proportion of those who think they are behaving safely (see Figure 47).

Figure 46. In general, how safe do you consider your own use of the Internet? By target groups (% of answers, all respondents)

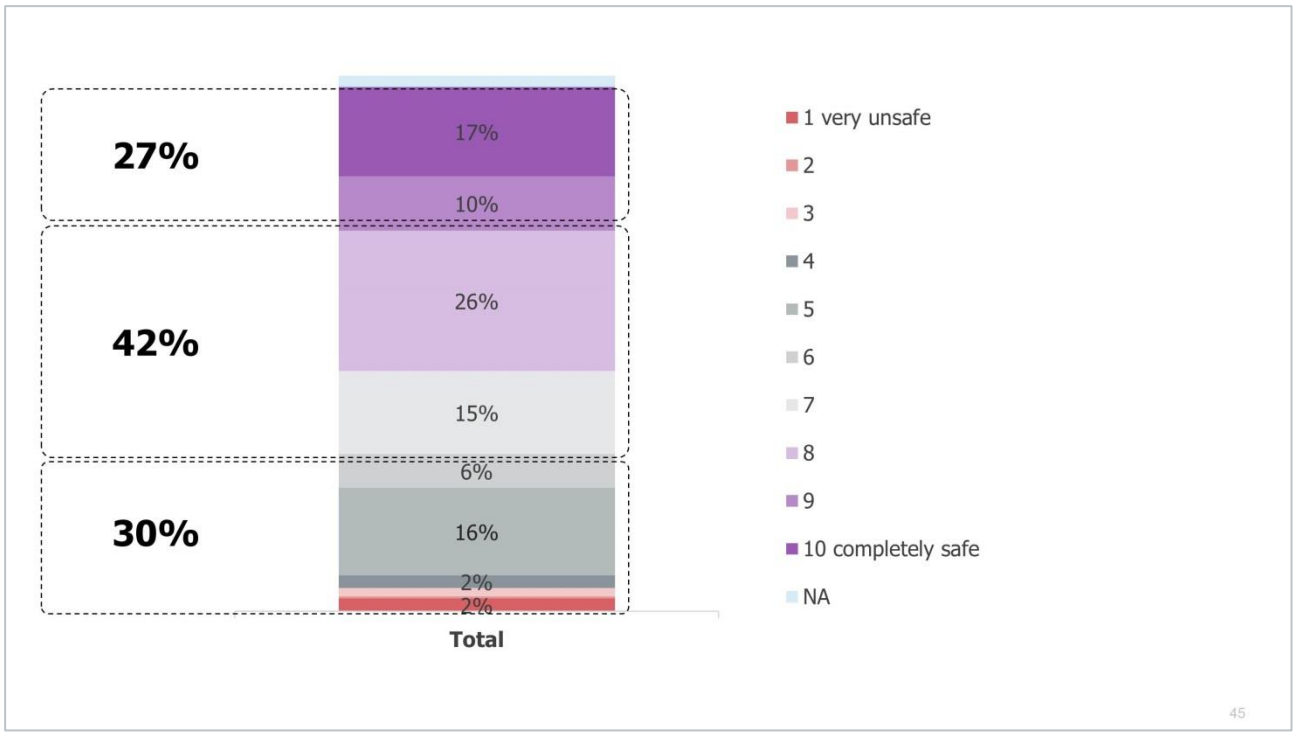
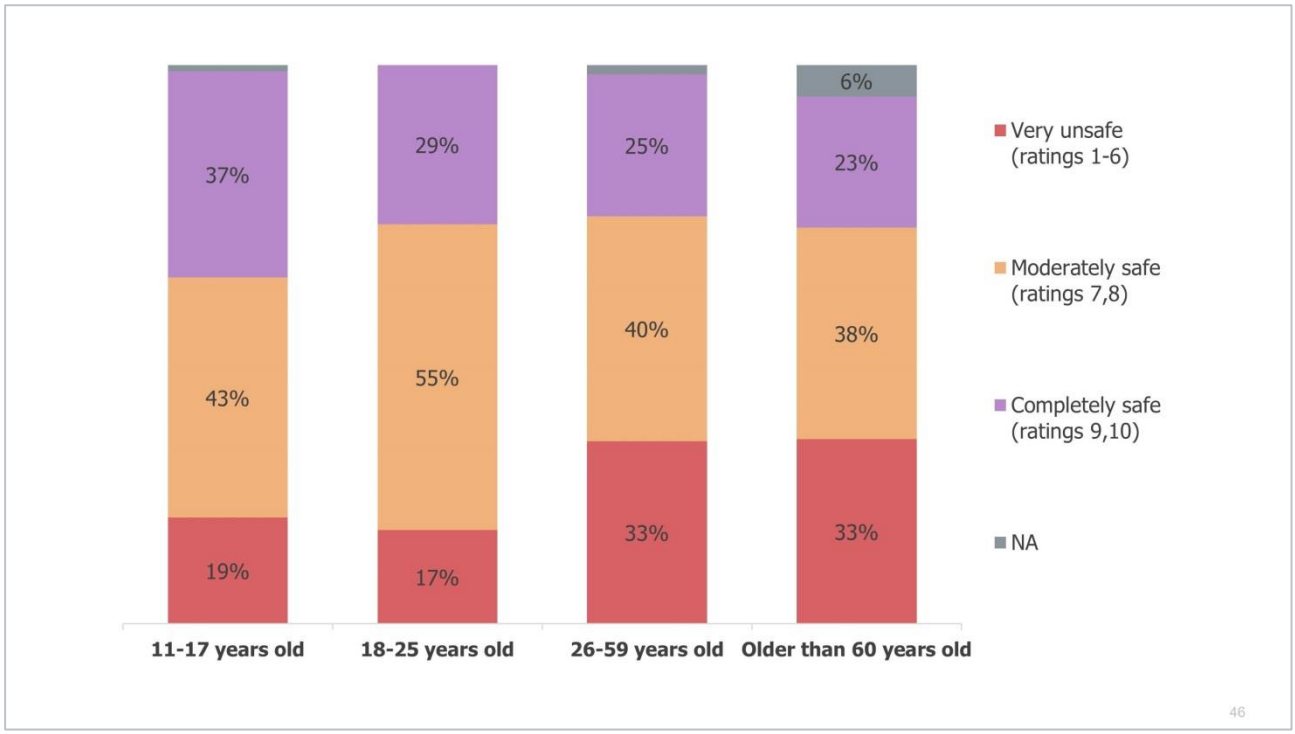


Figure 2. In general, how safe do you consider your own use of the Internet? By target groups (% of answers, all respondents)



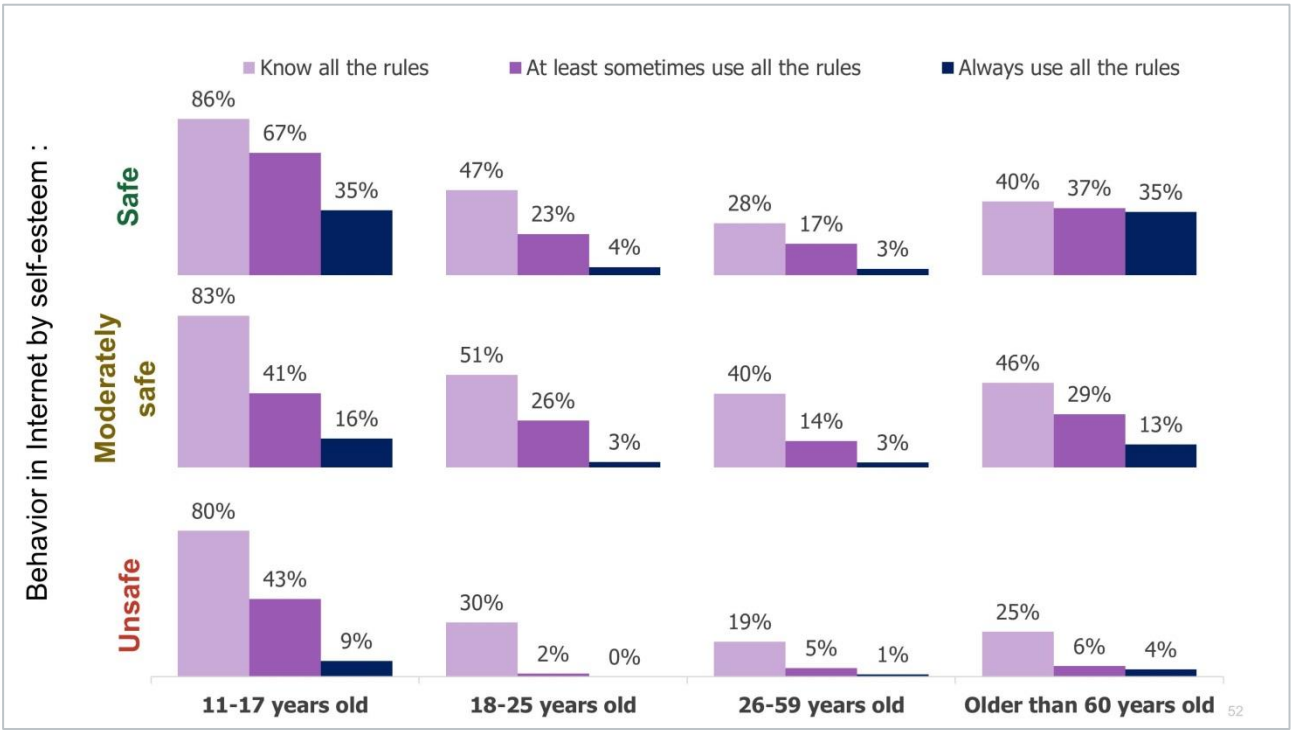
Self-assessment of use of the Internet depends on knowledge and compliance with the rules of cybersecurity: the higher a person evaluates the security of their behavior, the better he/she knows and more often follows the rules of cybersecurity. This correlation is observed for all age groups. Yes, those who assess their behavior as unsafe either do not know the rules or know but ignore them.

Teenagers, as the most knowledgeable group, evaluate their behavior by the level of compliance. For the rest of the age groups, self-assessment of safety correlates primarily with the level of knowledge.

The group of the oldest respondents (over 60 years old) who assess their behavior as safe is the most conscientious group in terms of cybersecurity: if a person knows the rule, he strictly follows it.

However, it is significant that the partial implementation of some rules also gives a sense of security: this is especially noticeable in the segment of respondents aged 18 to 59: among those who consider their behavior completely safe, only 3-4% follow all the rules (see Figure 3).

Figure 3. Knowledge and implementation of cybersecurity rules by the level of self-assessment of security behavior in the Internet



However, declaring compliance with cybersecurity rules does not mean genuine compliance with those rules. Yes, we analyzed the responses of respondents who stated that they follow a certain rule, and looked at how unsafe behavior associated with non-compliance with this rule is inherent in them.

For example, among those who have declared compliance with the rule «*Use strong passwords and do not use the same passwords to register on online resources, social networks and mobile games, get used to password managers*», only about ¾ really behave this way (see Table 1).

Table 1. Actual behavior regarding passwords among those who declare the use of the relevant rule

Respondents who said they always follow the rule: *«Use strong passwords and do not use the same passwords to register on online resources, social networks and mobile game applications, get used to using password managers» (49% of respondents)*	It's definitely about me	It's partially about me	It is definitely NOT about me	NA
I have a simple password because I'm afraid to forget the complex one	9%	13%	77%	1%
I have one password for everything to always remember it	12%	13%	74%	1%
I don't understand why to create different passwords	8%	17%	73%	2%

The situation with two-factor authentication is significantly worse: only half of those who declare compliance with this rule actually do so, and one in five do not do so at all (see Table 2).

Table 2. Actual behavior regarding the use of two-factor authentication among those who declare the use of the relevant rule

Respondents who said they always follow the rule: *«If possible, use two-factor authentication» (28% of respondents)*	It's definitely about me	It's partially about me	It is definitely NOT about me	NA
I use two-factor authentication, even if it's not required by site security policies (such as banking applications)	49%	28%	20%	3%

The situation with backup is even worse: among those who know and, according to them, always follow the rule «*Always back up important data on a separate local device or cloud storage*'», less than half do declare such behavior, and one in three say that does not do so (see Table 3).

Table 3. Actual behavior regarding the use of backup among those who declare the use of the relevant rule

Respondents who said they always follow the rule: *«If possible, use two-factor authentication» (30% of respondents)*	It's definitely about me	It's partially about me	It is definitely NOT about me	NA
I regularly make backup copies of documents, photos - for data protection	44%	21%	35%	0%

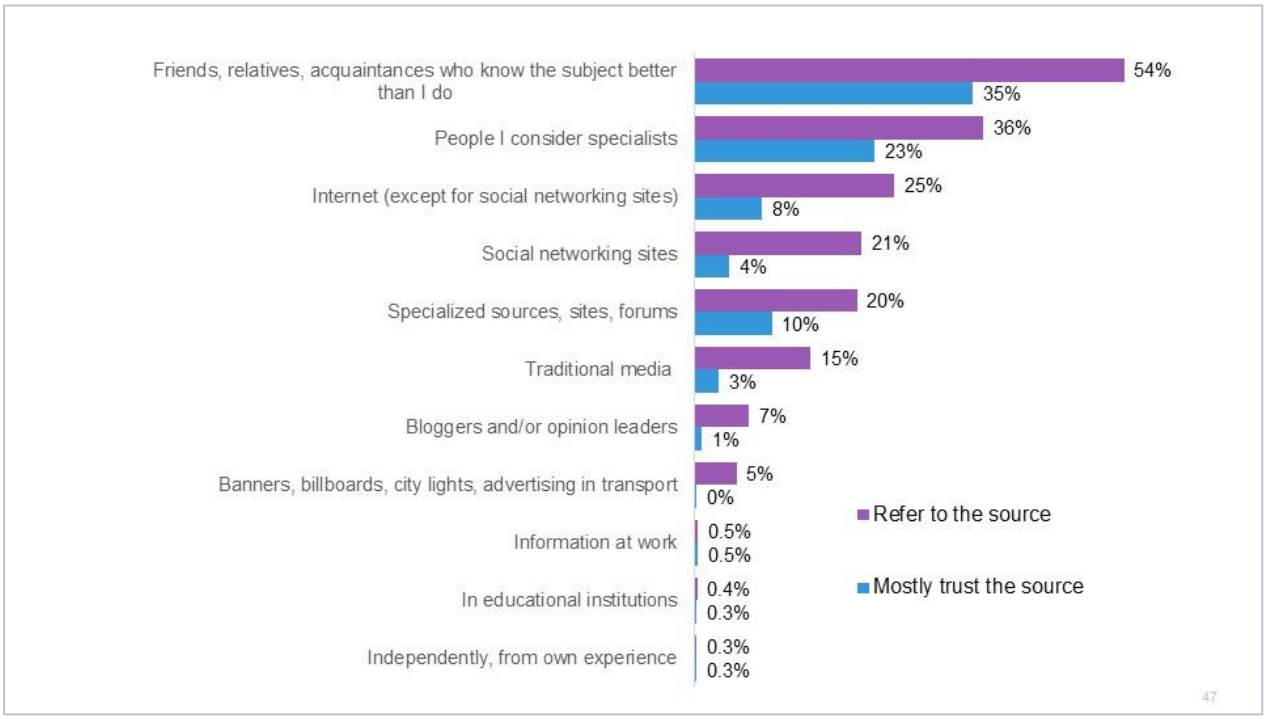
Situations where declaring compliance with the rule and actual behavior coincide are about a ban on sending strangers photos and scans of bank cards and personal documents (it is significant that this rule is intuitively followed even by those who do not formally know about it), as well as warnings against opening questionable letters (94% of those who know and follow this rule actually said that they do not open letters and attachments from unknown e-mail addresses or from strangers in the messenger).

Sources of information about the rules of safe use of the Internet

More than half (54%) of the respondents in the sample generally learn about the rules of safe use of the Internet from friends and acquaintances. In second place - people whom respondents consider experts (36% turn to this source). From 20 to 25% of respondents turn to the Internet in one way or another (websites, social networks, forums).

According to the indicator of trust in sources, the first places are also taken by friends, relatives, acquaintances (35%) and people whom respondents consider experts (23%). A very small proportion of respondents receive information from the place of work or study (0.5% and 0.4%, respectively), but those who use these sources consider them to be the most reliable and trustworthy (see Figure 49).

Figure 49. What sources of information do you use to learn about the rules of safe use of the Internet? Which of these sources of information do you trust the most? (% of answers, all respondents)



The sources of information used and trusted by the respondents vary considerably by target groups. Thus, for teenagers, the second place in the list of sources is shared by social networks and people whom respondents consider experts (however, they trust social networks less). For

young people, the first place went to people whom respondents consider experts (38% turn to this source and 24% trust it the most). Adults aged 26-59 most often turn to acquaintances and (51%), but the level of trust in experts is higher. Older people are more likely than others to turn to friends or relatives (68%) and trust this source the most (55%) (see Figure 50, Figure 51).

Figure 50. What sources of information do you use to learn about the rules of safe use of the Internet? By target groups (% of answers, all respondents)

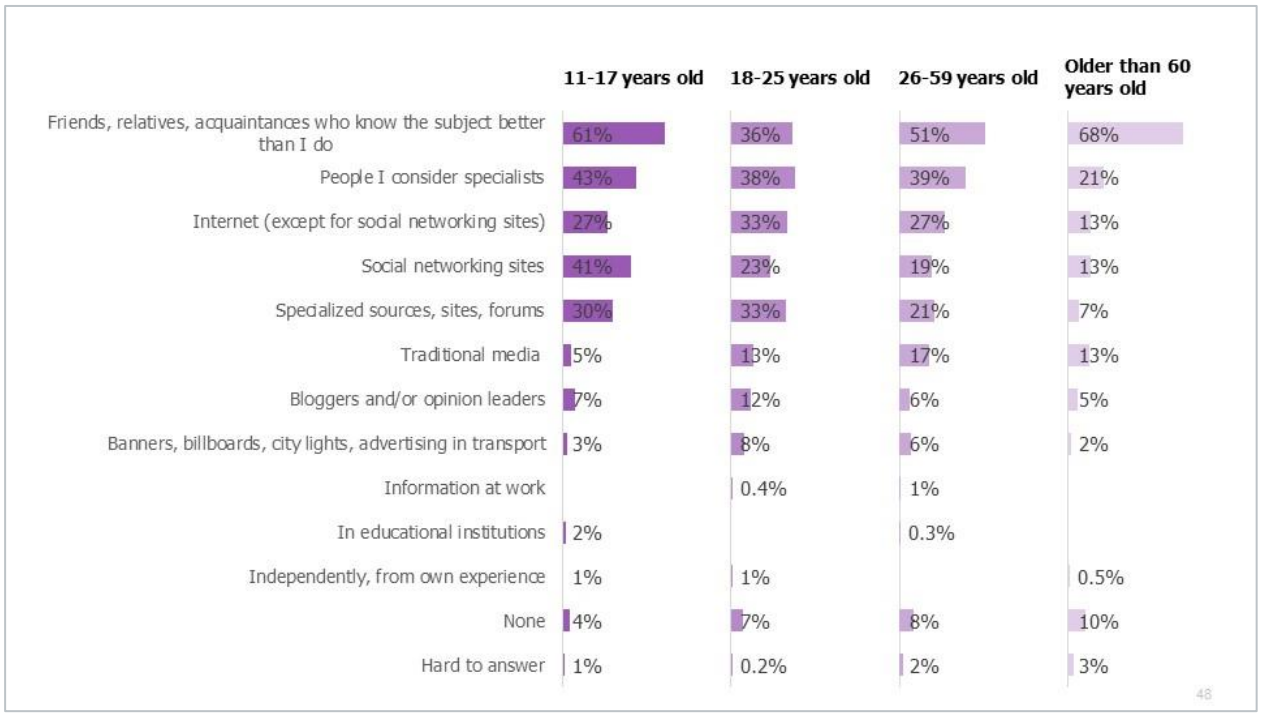
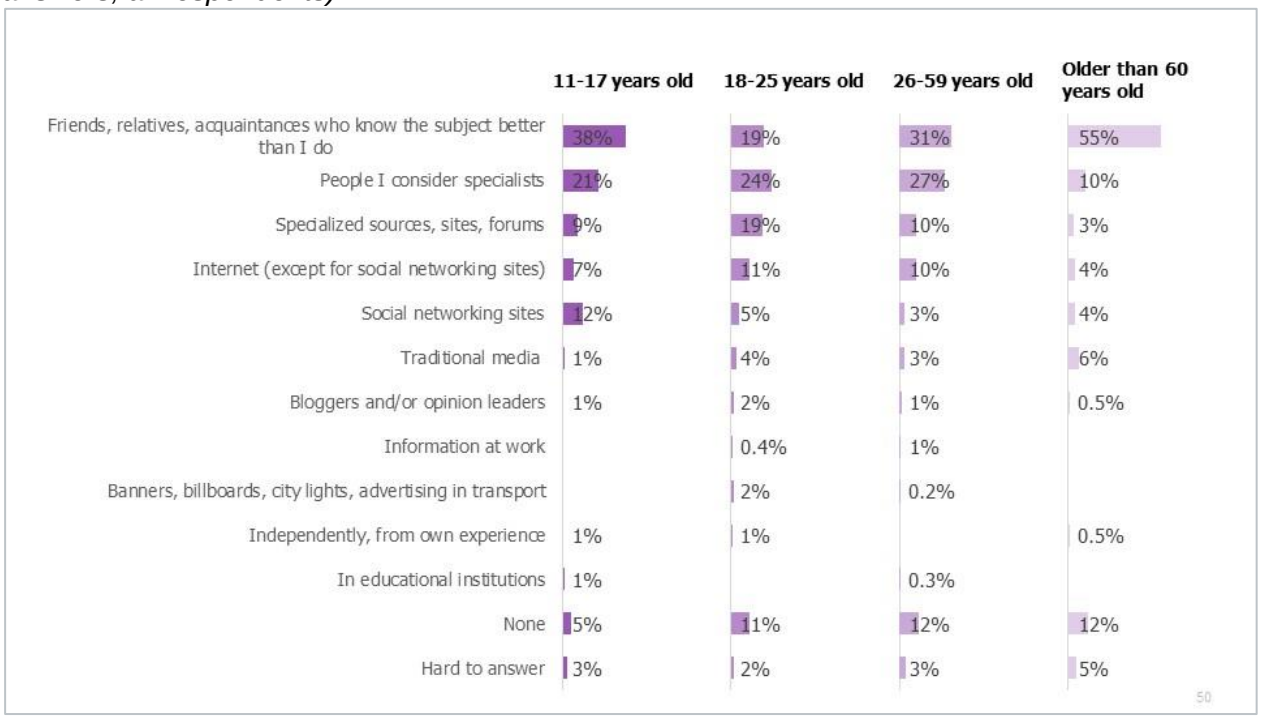


Figure 51. Which of these sources of information do you trust the most? By target groups (% of answers, all respondents)



V Appendix 1. Cities 50+, where the survey was conducted

Bakhmut (formerly Artemivsk)
Berdychiv
Berdyansk
Bila Tserkva
Boryspil
Brovary
Dnipro (formerly Dnipropetrovsk)
Drogobych
Energodar
Zhytomyr
Zaporizhzhia
Ivano-Frankivsk
Izmail
Irpin
Kamyanske (formerly Dniprodzerzhynsk)
Kamianets-Podilskyi
Kyiv
Kovel
Kolomyia
Konotop
Konstantinovka
Kramatorsk
Kremenchuk
Krivyi Rig
Kropyvnytskyi (formerly Kirovohrad)
Lysychansk
Lozova
Lutsk
Lviv
Mariupol
Melitopol
Mykolayiv
Mukacheve
Nizhyn
Nikopol
Novovolynsk
Novograd-Volynsky
Novomoskovsk
Odesa
Olexandria
Pavlograd
Pokrovsk (formerly Krasnoarmeysk)
Poltava
Rivne
Rubizhne
Severodonetsk
Slovyansk
Smila
Sumy
Ternopil
Uzhhorod
Uman
Kharkiv
Kherson
Khmelnytskyi
Cherkasy
Chernivtsi
Chernihiv
Chernomorsk (formerly Illichivsk)
Shostka

VI Appendix 2. Questionnaire

Greeting

Hello, my name is _____, I represent Info Sapiens. We conduct public opinion polls on various topics. We are currently conducting a survey on the safety of online behavior. Your answers are strictly confidential, we will not ask about your passwords or sites you visit. The survey will last up to 20 minutes, we will be grateful if you can answer our questions.

Selection of the respondent

S1. Please tell, how old are you?

Write_____ and encode

0	Less than 10 years	END
1	11-17 years	➔ Continue, QUOTA N = 300 (F2F)
2	18-25 years	➔ Continue, QUOTA N = 300 (CATI)
3	26-59 years	➔ Continue, QUOTA N = 450 (CATI)
4	More than 60 years	➔ Continue, QUOTA N = 150 (CATI)
5	Refuse to answer	END

S2. Mark sex of respondent

One answer, don't read

1	Male	Quota control within the age penalty
2	Female	Quota control within the age penalty

S3. **How often do you use the Internet, for example, visit sites, social networking sites, use applications, messengers?**

One answer, read out

1	I spend on the internet most of the day	
2	Several sessions per day, but not most of the day	
3	Every day, one or two sessions	
4	3-4 times a week	
5	1-2 times a week	
6	3-4 times a month	
7	1-2 times a month	
8	Less than once a month	END
9	I do not use the Internet at all	END
99	Hard to answer	END

S4. Which devices do you use to access the Internet?

Few answers, read out

S5. [If more than one device is mentioned in S4, otherwise move the answer]
Which devices do you use to access the Internet most often?

One answer, from those mentioned in S4.

	S4.	S5.
Desktop computer	1	1
Laptop	2	2
Tablet	3	3
Smartphone (if necessary, explain: phone, where you can install applications, specifically for Internet access)	4	4
Other	5	5
Hard to answer	99 → END	99 → END

S6. [If S5 =1 or 2]

Could you specify, is it your personal computer/laptop?

One answer, read out if needed

1	Yes, this is my personal computer / laptop (I only use it)
2	The computer/laptop belongs to the family, I use it as well as other family members
3	The computer/laptop belongs to the employer, the company, the school, the educational institution
4	Other: write down _____
99	Hard to answer (do not read out!) → END

MAIN QUESTIONNAIRE

A1. Do you follow these steps online and how often?

Read alternatives. One answer per line.

Programmer: ROW ROTATION		Every day	Several times a week	Once a week	Once a month	Several times a year	Never	NA (do not read out)
1	Go to the pages, read the feeds of social networking sites (such as Tik Tok, Facebook, Instagram)	1	2	3	4	5	6	99
2	Write posts or post photos on social networking sites	1	2	3	4	5	6	99
3	Buy goods in online stores (including social networking sites such as Facebook, Instagram)	1	2	3	4	5	6	99
4	Pay for goods or services with a bank card via the Internet	1	2	3	4	5	6	99
5	Use Internet banking (transfer funds, view account balance, manage accounts)	1	2	3	4	5	6	99
6	Download videos, music, articles, books and other materials	1	2	3	4	5	6	99
7	Connect to public Wi-Fi networks (in cafes, public places)	1	2	3	4	5	6	99

8	Use e-mail	1	2	3	4	5	6	99
9	Use messengers (Viber, Telegram, WhatsApp, Facebook)	1	2	3	4	5	6	99
10	Use VPN (for example, to access sites that are blocked)	1	2	3	4	5	6	99
11	Play games online	1	2	3	4	5	6	99
12	Make purchases from game accounts	1	2	3	4	5	6	99
13	Download free software, games	1	2	3	4	5	6	99
14	Install various software, browser extensions	1	2	3	4	5	6	99

A1.2 **[If the answers "1..4" are selected for the following statements in A1: 6, 13, 14]**

When you download materials, software, games, how do you check that the resource is reliable?

Do not read out! There are several possible answers

1	Do not check, just download, and that's it
2	Download only from official resources
3	You have used these resources for a long time, so you are confident in their reliability
4	Other: write down_____
99	Hard to answer (do not read out!)

A2. The main topic of our conversation is cybersecurity and the rules of cyber hygiene. Please tell me, how familiar are you with these concepts? Choose the answer: "Know it very well and can explain it to others", " Have a general idea, without details", " I've heard of such concepts, but I don't know exactly what it's about" or " Hear for the first time".

One answer in the column.

	cybersecurity	**rules of cyber hygiene**
Know it very well and can explain it to others	1	1
Have a general idea, without details	2	2
I've heard of such concepts, but I don't know exactly what it's about	3	3
Hear for the first time	4	4
Hard to answer (do not read out!)	99	99

A3. I will read a few statements. Answer please how true is it about you. You can say " It's definitely about me", " It's partially about me" or " It is definitely NOT about me".
One answer.

Programmer: ROW ROTATION		It's definitely about me	It's partially about me	It is definitely NOT about me	NA (do not read out)
1	I have a simple password because I'm afraid to forget the complex one	1	2	3	99
2	I have one password for everything to always remember it	1	2	3	99
3	Friends or relatives know my passwords in case I forget	1	2	3	99
4	I don't understand why to create different passwords	1	2	3	99
5	Internet scammers are not interested in me	1	2	3	99
6	If there is an anti-virus, then I am safe	1	2	3	99
7	I open emails and attachments even from unknown e-mail addresses or from strangers in the messenger	1	2	3	99
8	I can insert someone else's or unfamiliar flash drive into my computer	1	2	3	99
9	I can accidentally "expose" the data of the bank card, passport, ticket QR-codes on social networking sites	1	2	3	99
10	I use two-factor authentication, even if it's not required by site security policies (such as banking applications)	1	2	3	99
11	I regularly make backup copies of documents, photos - for data protection	1	2	3	99
12	I visit Russian sites (ending in "dot RU")	1	2	3	99
13	I have e-mail accounts on Russian mail servers	1	2	3	99
14	I visit Russian resources and social networking sites that are blocked in Ukraine (such as Yandex, Vkontakte)	1	2	3	99
15	From Russian resources (dot RU), I sometimes download files, games or software, fill out questionnaires there, register or insert certain data	1	2	3	99

A4. I will read the lists of the main threats that can befall the Internet user, and you tell me, have you personally or your acquaintances encountered such a situation?

Programmer: ROW ROTATION		Happened to you personally	Happened to your real acquaintances	Happened to your virtual acquaintances	Heard about it, but it did not happen to	Haven't even heard of such a thing	NA (do not read out)	Display alternatives according to age groups **S1 = …**			
								1	2	3	4
1	Theft (hacking) of accounts on social networking sites	1	2	3	4	5	99	x	x	x	
2	Theft (hacking) of game accounts in computer games	1	2	3	4	5	99	x			
3	**[The wording for S1 =1]** Extortion of passwords for accounts, e-mail accounts, game bonuses, parent bank data using social engineering and sexting techniques (messages of a sexual nature) **[The wording for S1 =2,3,4]** Extortion of passwords for accounts, e-mail accounts using social engineering techniques (manipulations, threats, blackmail)	1	2	3	4	5	99	x	x	x	x
4	People become victims of cyber scammers at online auctions	1	2	3	4	5	99		x	x	
5	Extortion of personal information via phone, messengers, mailboxes, social media accounts	1	2	3	4	5	99			x	x
6	Extortion of bank data, passwords and access to accounts of mobile banking applications, bank accounts (including by phone, messengers)	1	2	3	4	5	99			x	x
7	Extortion of money in order to unblock the work of computer systems and gadgets (electronic devices)	1	2	3	4	5	99			x	
8	Extortion of official data from employees of state-owned or commercial companies	1	2	3	4	5	99			x	
9	Cyber scammers extort money using social engineering techniques (manipulation, threats, blackmail), as well as personal and family data (via phone and messengers)	1	2	3	4	5	99				x

A5. Have you ever had a situation where you thought you had encountered malicious activity while using digital devices, but you can't say for sure what it was?

1	No	
2	Yes, over the past three months	→ Please clarify: _____
3	Yes, in the past	
99	NA (do not read out)	

A6. You said that some threatening situations happen to you personally. Please specify when did it happen for the last time for sure?

Read alternatives. One answer per line.

	Programmer: ROW ROTATION	Over the past 3 months	Within a year, but more than 3 months ago	More than a year ago	NA (do not read out)
1	Attention, programmer: Output alternatives for which **0 =1**	1	2	3	99
2		1	2	3	99
…		1	2	3	99

A7. How secure do you feel about some threats? You can answer " I feel completely secure"; " I don't always feel secure" or " I feel helpless."

Read alternatives. One answer per line.

Programmer: ROW ROTATION		I feel completely secure	I don't always feel secure	I feel helpless	NA (do not read out)
1	Attention, programmer: Output alternatives for which 0={1..4}	1	2	3	99
2		1	2	3	99
..		1	2	3	99

0.1 [If A7 has answers 2 or 3] You've said that sometimes you do not feel completely secure about cyber threats. How willing are you to apply rules of cyber hygiene to secure yourself from these threats? Score on a scale from 1 to 5, where 1 - "not ready to apply any rules", and 5 - "ready to apply all necessary security rules "

1	2	3	4	5	NA=99

A8. I will read some basic rules of cyber hygiene and you tell me how well are you personally aware of this rule. You can choose the answer " Hear for the first time", " I know, but I don't follow", " I know and sometimes follow" or " I know and always follow".

Read alternatives. One answer per line.

Programmer: ROW ROTATION		Hear for the first time	I know, but I don't follow	I know and sometimes	I know and always follow	NA (do not read out)	Attention, programmer: Display alternatives according to age groups **S1 =**			
							1	2	3	4
1	**[The wording for S1 =1]** Use strong passwords and do not use the same passwords to register on online resources, social networks and mobile game applications, get used to using password managers **[The wording for S1 =2,3,4]** Use strong passwords and do not use the same passwords to register on online resources, in banking systems, etc., get used to using password managers.	1	2	3	4	99	x	x	x	x

2	[The wording for S1 =1] Do not send photos and scans of bank cards and personal documents of yourself and parents to strangers and dubious organizations [The wording for S1 =2,3,4] Do not send photos and scans of your bank cards and personal documents to strangers and dubious organizations	1	2	3	4	99	x	x	x	x
3	[The wording for S1 =1] Don't open questionable emails in your mailboxes, messengers or game accounts [The wording for S1 =2,3,4] Do not open suspicious emails in your mailboxes, messengers	1	2	3	4	99	x	x	x	x
4	Do not send your contact phone numbers, personal photos to strangers, especially those who ask for nude photos	1	2	3	4	99	x			
5	Do not install applications and software from unofficial stores on your gadgets	1	2	3	4	99	x	x	x	x
6	Do not connect to the public, unknown or non-secure Wi-Fi networks	1	2	3	4	99	x	x	x	x
7	If strangers exort passwords, data, photos from you or you receive suspicious messages, let your parents know immediately	1	2	3	4	99	x			
8	If possible, enable automatic updating of all programs	1	2	3	4	99		x	x	
9	Use licensed and antivirus software, firewalls on computers and phones, and update it regularly when you receive system update notifications	1	2	3	4	99		x	x	
10	Always create a back up copy of important data on a separate local device or cloud storage	1	2	3	4	99		x	x	
11	If possible, use two-factor authentication	1	2	3	4	99		x	x	
12	Do not leave your device unattended, especially when operating in public places	1	2	3	4	99		x	x	x
13	In case of any suspicion of infecting your device or compromising data, IMMEDIATELY notify the relevant authorities: Government Computer Emergency Response Team of Ukraine, National Coor	1	2	3	4	99		x	x	
14	Don't panic in the event of a phone call or a message in the messanger from suspicious people and organizations demanding money from you to save your family, pet or loved one. Immediately notify the relevant authorities or your relatives in the event of such a call	1	2	3	4	99				x
15	In case of any suspicion of infecting your device or compromising data, IMMEDIATELY notify the relevant authorities: Cyberpolice of Ukraine (tel. 0 800 505 170) and your children or family	1	2	3	4	99				x

A9. In general, how safe do you find your own use of the Internet? Rate on a scale of 1 to 10, where 1 means "very unsafe" and 10 means "completely safe".

1	2	3	4	5	6	7	8	9	10	NA=99

A10. What sources of the information do you use to learn about the security rules of use of the Internet?

A11. [If more than one source is mentioned in A10] Which of these sources of information do you trust the most?

If necessary, read one of the answers mentioned in A10

	A10	A11
Specialized sources, sites, forums	1	1
People I consider specialists (for example, system administrator at work, at school, at university)	2	2
Friends, relatives, acquaintances who know the subject better than I do	3	3
Social networking sites	4	4
Internet (except for social networking sites)	5	5
Traditional media (television, newspapers, radio)	6	6
Bloggers and/or opinion leaders	7	7
None	8	8
Banners, billboards, city lights, advertising in transport	9	9
Other (write down _____)	98	98
Hard to answer (do not read out!)	99	99

A12. [If A10 = 7] What bloggers and/or opinion leaders do you consider a source of information about safe use of the Internet?

Write down: _____

DEMOGRAPHY

D1. Please indicate your main occupation.

Read out, one answer

1	Employed
2	Registered private entrepreneur
3	Self-employed
4	Student/school student
5	Running a household
6	Retired
7	Temporarily unemployed but looking for a new job
98	Other (write down)

D2. [If D1= 1] Where exactly do you study?

One answer

1	School
2	Vocational school
3	College
4	Higher educational institution
98	Other (write down)

D3. What is the highest level of education that you have completed?

Read out, one answer

1	No primary education
2	Primary secondary education (specify if necessary: graduated from 4 classes of secondary school)
3	Secondary Basic (specify if necessary: graduated from 9 classes of secondary school)
4	Secondary Complete (specify if necessary: graduated from 12 classes of secondary school)
5	Secondary Vocational (specify if necessary: graduated from vocational school, college)
5	Unfinished Higher/Higher (specify if necessary: completed 1-3 years of higher educational institution)
6	Higher, bachelor's degree
7	Higher, master's degree (specialist)
99	Hard to answer (do not read out!)

D4. Which of the following statements describes the financial status of your family in the best way?

Read out, one answer

1	We have to save on food
2	We have enough money for food, but we have to borrow or save money to buy clothes and footwear
3	We have enough money for food and necessary clothes and footwear, but we have to borrow or save money to buy such things as good suit, mobile phone, vacuum cleaner and the like
4	We have enough money for food, clothes, footwear and other purchases but we have to borrow or save money to buy expensive goods (such as TV-set, refrigerator and the like)
5	We have enough money for food, clothes, footwear and expensive purchases, but have to borrow or save money to buy car or flat
5	We can make any purchases at any time
99	Hard to answer (do not read out!)

These are all questions.

Thank the respondent for participating in the survey

VII Appendix 3. Portrait of the respondent

		TOTAL		Age of the respondent							
				11-17 years old		18-25 years old		26-59 years old		Over 60 years old	
		Count	%	Count	%	Count	%	Count	%	Count	%
Sex	Male	570	47.47%	154	51.38%	159	52.94%	212	47.02%	65	43.17%
	Female	630	52.53%	146	48.62%	141	47.06%	238	52.98%	85	56.83%
	TOTAL	1,200	100%	300	100%	300	100%	450	100%	150	100%
Region	Kyiv	98	8.20%	22	7.42%	24	8.04%	38	8.43%	12	8.07%
	North	162	13.46%	38	12.78%	39	13.12%	64	14.11%	18	12.02%
	West	295	24.55%	84	27.89%	83	27.54%	105	23.25%	37	24.77%
	Center	290	24.14%	73	24.37%	71	23.63%	109	24.12%	37	24.35%
	South	206	17.19%	49	16.34%	50	16.58%	80	17.79%	24	16.22%
	East	149	12.45%	34	11.19%	33	11.08%	55	12.30%	22	14.56%
	TOTAL	1,200	100%	300	100%	300	100%	450	100%	150	100%
Size of the settlement (thousand inhabitants)	Village	352	29.29%	102	34.07%	102	34.03%	128	28.45%	39	26.11%
	0-50	247	20.61%	63	21.11%	57	19.04%	94	20.90%	30	20.30%
	51-500	299	24.91%	64	21.41%	68	22.79%	111	24.76%	43	28.89%
	500+	302	25.19%	70	23.41%	72	24.14%	117	25.90%	37	24.70%
	TOTAL	1,200	100%	300	100%	300	100%	450	100%	150	100%

		TOTAL		Age of the respondent							
				11-17 year old		18-25 years old		26-59 years old		Over 60 years old	
		Count	%	Count	%	Count	%	Count	%	Count	%
The main occupation	I work for hire	445	37.04%	0	0.00%	103	34.25%	233	51.68%	24	16.07%
	Registered private entrepreneur	82	6.81%	0	0.00%	25	8.20%	40	8.97%	5	3.50%
	Self-employed	58	4.82%	0	0.00%	20	6.66%	28	6.17%	4	2.54%
	Student	176	14.68%	299	99.63%	74	24.68%	1	0.23%	0	0.00%
	I run the household	111	9.25%	1	0.37%	33	10.94%	59	13.03%	3	1.97%
	Retiree	225	18.73%	0	0.00%	3	1.10%	36	8.06%	112	74.96%
	Temporarily unemployed, but I am looking for a job	94	7.82%	0	0.00%	38	12.50%	48	10.71%	1	0.96%
	Other	4	0.30%	0	0.00%	1	0.49%	2	0.41%	0	0.00%
	Hard to tell	7	0.56%	0	0.00%	4	1.18%	3	0.73%	0	0.00%
	TOTAL	1,200	100%	300	100%	300	100%	450	100%	150	100%
Place of study	At school	120	67.96%	251	84.08%	0	0.00%	0	0.00%	0	0.00%
	In a vocational school	8	4.27%	12	3.91%	5	6.10%	0	0.00%	0	0.00%
	In college	14	7.69%	18	5.91%	12	15.94%	0	0.00%	0	0.00%
	In an institution of higher education	35	20.08%	18	6.11%	58	77.96%	1	100%	0	0.00%
	Other	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
	TOTAL	176	100%	299	100%	74	100%	1	100%	0	0.00%

		TOTAL		Age of the respondent							
				11-17 years		18-25 year		26-59 year		Over 60 year	
		Count	%	Count	%	Count	%	Count	%	Count	%
Educational level	No primary education	1	0.08%	2	0.71%	0	0.00%	0	0.00%	0	0.00%
	Primary secondary education	80	6.65%	159	53.07%	1	0.23%	2	0.33%	1	0.58%
	Basic secondary education	82	6.83%	105	35.03%	10	3.22%	17	3.69%	1	0.74%
	Complete secondary education	129	10.78%	16	5.37%	41	13.62%	57	12.68%	10	6.59%
	Specialized secondary education	311	25.94%	5	1.58%	61	20.30%	128	28.52%	55	36.76%
	Incomplete higher education / initial higher education	61	5.09%	13	4.25%	51	16.87%	16	3.66%	5	3.26%
	Higher education, bachelor's degree	124	10.31%	0	0.00%	82	27.20%	46	10.20%	11	7.39%
	Higher education, master's degree	407	33.91%	0	0.00%	52	17.37%	183	40.64%	66	44.10%
	Hard to tell	5	0.39%	0	0.00%	4	1.18%	1	0.27%	1	0.58%
	TOTAL	1,200	100%	300	100%	300	100%	450	100%	150	100%
Financial situation of the family	Forced to save on food	119	9.94%	1	0.49%	17	5.61%	43	9.50%	30	19.94%
	Need to save or borrow to buy clothes, shoes	218	18.15%	18	5.92%	29	9.62%	83	18.39%	45	30.23%
	Need to save or borrow for purchases such as a fancy suit, mobile phone	266	22.18%	133	44.18%	69	23.14%	87	19.22%	25	16.84%
	Need to save or borrow to buy expensive things	280	23.37%	66	21.99%	71	23.56%	122	27.10%	18	12.32%
	Need to save or borrow for purchases such as a car, an apartment	189	15.78%	38	12.79%	63	20.99%	72	15.95%	21	14.14%
	Able to make any necessary purchases at any time	52	4.31%	5	1.52%	29	9.58%	21	4.64%	3	1.95%
	Hard to tell	75	6.28%	39	13.12%	23	7.50%	23	5.20%	7	4.58%
	TOTAL	1,200	100%	300	100%	300	100%	450	100%	150	100%