REPORT
on a midterm study on target groups' awareness of the main aspects of cybersecurity

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

May 2023

Table of Contents

Abbreviations

CAPI	computer assisted personal interview
CATI	computer assisted telephone interview
IDI	in-depth interviews
IDP	internally displaced people
FGD	focus group discussion
NA	no answer
TG	target group

I Key Results

Pressure of cyber threats.

We have recorded the increasing pressure on the teenage group. The share of teenagers who have experienced cyber threats has increased due to both personal and friends' experiences. At the same time, the level of personal experience of cyber threats among adults has hardly changed since 2021, while the share of elderly people with experience of cyber threats has decreased.

The most common cyber threats among teenagers are theft (hacking) of accounts on social networks (the share of teenagers who have had this experience or heard about it from friends has increased from 28% in 2021 to 41% in 2023) and theft of game accounts in computer games (increased from 19% to 38%). However, a purely personal experience of cyber threats among teenagers remains the lowest: only 11% and 12% of them have personally faced threat of theft (hacking) of accounts in social networks and computer games, respectively.

Among young people aged 18-25, the biggest threat is theft (hacking) of accounts in social networks: 21% of respondents personally faced this (compared to 2021, the indicator decreased by 8 p.p.). Among adults aged 26 and over, the biggest threat faced by about one in four respondents is the extortion of bank details, passwords and access to accounts of mobile banking applications and bank accounts (unchanged compared to 2021).

Cybersecurity rules.

Most respondents have a general understanding of cybersecurity - from 44% to 55% in different groups. Young people aged 18-25 are the most knowledgeable: 29% stated they were very familiar with the concept of cybersecurity (compared to 18% in 2021). Teenagers took second place: 23% of them are familiar with the concept of cybersecurity. Among the adults aged 26-59, 18% are well aware of cybersecurity, while only 7% of elderly respondents are well informed.

In contrast to general knowledge of cybersecurity, self-reported knowledge of cyber hygiene rules has increased in all target groups. The largest share of people familiar with cyber hygiene rules, at least in general, is reported in the group of young people aged 18-25 (62%), the smallest - among the elderly aged 60 and over (42%).

The older audience demonstrated an increase in compliance with the rule *"In case of any suspicion of infecting your device or compromising data, immediately notify the relevant authorities: Cyber Police of Ukraine, your children and family"* (from 37% in 2021 to 43% in 2023). Adherence to *"If possible, use two-factor authentication"* rule has also increased among youth aged 18-25 (from 38% to 49%) and adults aged 26-59 (from 28% to 42%).

The general trend of knowledge and use of cyber hygiene rules is controversial. Level of knowledge has increased among adults aged 25-59 and elderly people, while compliance with the rules has

decreased among teenagers. However, teenagers remain the most knowledgeable audience as for cybersecurity rules.

Ability to detect risky situations.

Not all audiences can distinguish between situations of real cyber threats. For example, most respondents regard the situation when *"A friend went to a cafe for "free Wi-Fi to transfer money to parents via online banking"* as normal and not risky. On the other hand, many people regard VPN use or automatic software update risky.

A total of 71% of respondents can correctly identify five or more situations (out of ten) related to cybersecurity. This indicator is the highest among young people aged 18-25 (90%). Adults aged 25-59 are in second place with 72%. Teenagers are in third place (64%), while the lowest indicator is reported among elderly people (47%). It must be pointed out that *CRDF Global* training program participants can determine risky situations better than all other audiences - for them, the indicator reached 96%.

II. Study Goal and Methodology

Recognizing the risks associated with the increasingly digitized world, *CRDF Global* launched a cybersecurity improvement program in Ukraine, Moldova, and the Western Balkans in 2019. This program is aimed at prevention of cyber-attacks through building a strong cyber infrastructure and cybersecurity strengthening. This program is supported by the Department of State's Office of the Coordinator of U.S. Assistance to Europe and Eurasia.

Cybersecurity Information campaign is a part of *CRDF Global* Cybersecurity Program, and the main goal of the project is to improve awareness of cybersecurity threats among the general public of Ukraine.

A basic study (I wave of the study) on target groups' awareness of the main aspects of cybersecurity and cyber hygiene rules was conducted in August-September 2021.

The current interim study (II wave) conducted in March 2023 presents interim results and aims to analyze the dynamics of indicators.

The survey is to evaluate the following:

- levels of target groups' awareness of cyber threats and cybersecurity;
- levels of awareness of basic rules of cyber hygiene and their application in everyday life;
- latest (recent months) personal experience of users as for cyber-hackers, cyber-crimes, cyber-attacks, and cyber threats;
- ability to detect potentially threatening situations from the point of view of cybersecurity

The target audience of the main study is citizens of Ukraine using 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
- Elderly people aged 60+:

The main method of conducting the study is a **quantitative survey** based on a structured questionnaire.

Geography of the study: all of Ukraine, including villages, with the exception of the Autonomous Republic of Crimea and territories not controlled by the Ukrainian authorities.

The total number of the main survey respondents: 1,224.

Number of respondents by target groups:

- Teenagers aged 11-17: 315 respondents;
- Young people aged 18-25: 314 respondents;
- Adults aged 26-59: 354 respondents;
- Elderly people aged 60+: 241 respondents;

It was previously planned to conduct an equal number of interviews with representatives of all target groups (300 interviews in each group). However, during the survey, the researchers encountered very limited use of Internet in the oldest target group (elderly people aged 60+). This taken into consideration, it was decided to reduce the target number of interviews in this group to 241 by increasing the target number of interviews in the 26-59 age group to 354 interviews.

Survey method:

- for target group "Teenagers" - personal interview at the respondent's home with the help of a computer (CAPI - computer assisted personal interview);
- for the rest of the target groups — computer assisted telephone interview (CATI).

The sample is random with quota control by sex, age, region and size of the inhabited locality. Within each target group, the sample is representative, its structure corresponds to the structure of Internet users by gender, age, region and size of the inhabited locality.

For the general analysis of the sample, weighting was applied, which brought the sample structure into compliance with the structure of the population of Ukraine by age.

The maximum statistical sampling error is:

- Sample in general: 2,8% with a probability of 95%;
- Teenagers aged 11-17: 5,5% with a probability of 95%;

- Young people aged 18-25: 5,2% with a probability of 95%;

- Adults aged 26-59: 4,6% with a probability of 95%;

- Elderly people aged 60+: 6,3% with a probability of 95%.

In addition, **quantitative and qualitative survey of the control group** was conducted:

- People who took *CRDF Global* courses: 305 respondents.

Quantitative survey method: online interview. The link to the survey was sent by specialists of the *CRDF Global* Representative Office in Ukraine.

The quantitative survey was conducted on a basis of a structured questionnaire (see Appendix 2) containing five- and ten-point scales. From the analytical point of view, a score of 4 or 5 on a five-point scale and 9 or 10 on a ten-point scale is regarded as positive.

Qualitative research method: focus group discussions (FGDs) and in-depth interviews. In particular, the following was carried out:

- 2 online FGDs with students and young people who have attended CDRF *Global* cybersecurity courses. 4-6 respondents from different cities, part of whom are IDPs, took part in each FGD;

- 3 mini FGDs with representatives of local authorities and public officers, who have attended *CDRF Global* cybersecurity courses. Each FGS included 3 respondents living and working in different regions of Ukraine;

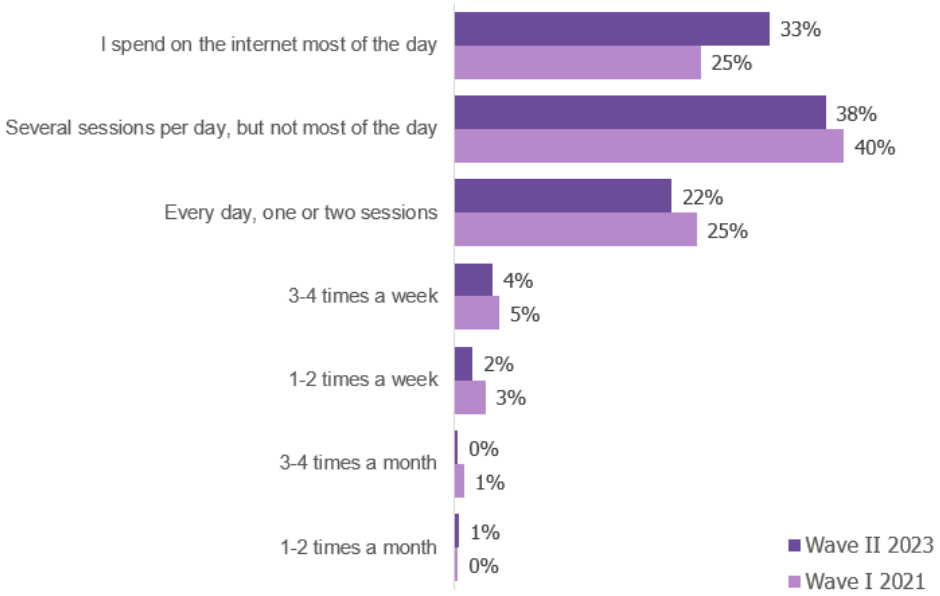
- 3 in-depth interviews with school teachers of computer science who have attended *CDRF Global* cyber security courses. Teachers also represented different regions of Ukraine.

III Study Results

Behavior in Internet

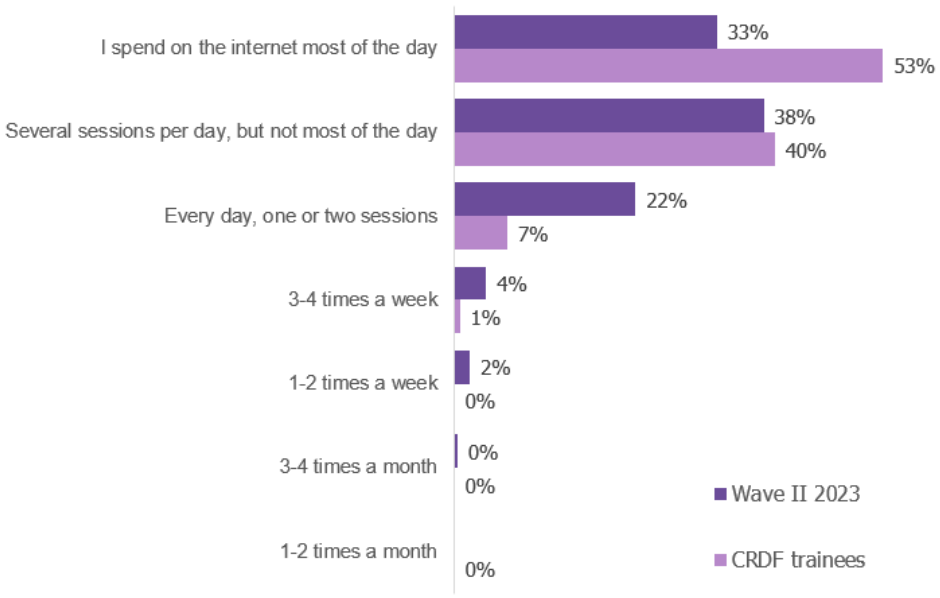
People using Internet at least once a month were invited to participate in the survey, similarly to the previous study wave. Most of 2023 wave II survey respondents are using Internet daily - 93% compared to 90% of 2021 wave I survey. The increase in daily Internet use level was significant: 33% vs. 25%. It could be due to COVID-19 pandemic (shifting to remote work) and results of a full-scale invasion (current news monitoring) (see Chart 1).

Chart 1. How often do you use the Internet, for example, visit websites, social networks, use applications, messengers? (% of responses by wave I and II respondents)



For Internet behavior comparison, respondents who had attended *CRDF Global* training events were interviewed - this group of respondents uses Internet on a daily basis more often and more than half of them spend most of the day on the Internet (see Chart 2).

Chart 2. How often do you use Internet, for example, visit websites, social networks, use applications, messengers? (% of responses by wave II respondents and CRDF Global course attendees)



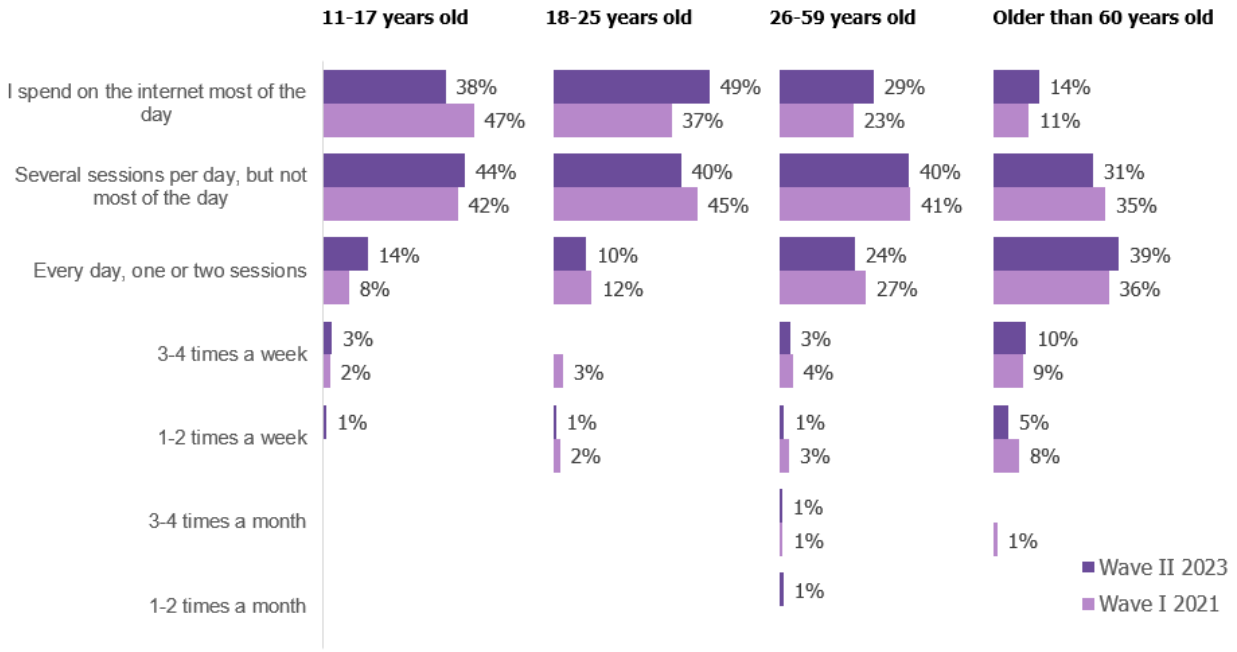
The older the respondents are, the less time they spend on the Internet. This tendency was recorded in 2021 wave I, and it remains unchanged in 2023.

In 2023, respondents aged 18-59 started to spend more time on the Internet, while Internet time of teenagers aged 11-17 has slightly reduced.

Thus, among the youngest group (teenagers aged 11-17), 38% of the respondents (compared to 47% in 2021 wave I) spend most of the day on the Internet. Among young people aged 18-25, almost half of the respondents (49%) spend most of the day on the Internet (vs. 37% in wave I). Among adults and elderly people, the share of those spending most of the day on the Internet has also increased, but this increase is not as significant. The share of the respondents aged 26-59 spending on the Internet most of the day was 29%, among elderly people - 14% (compared to 23% and 11% in 2021, respectively) (see Chart 3).

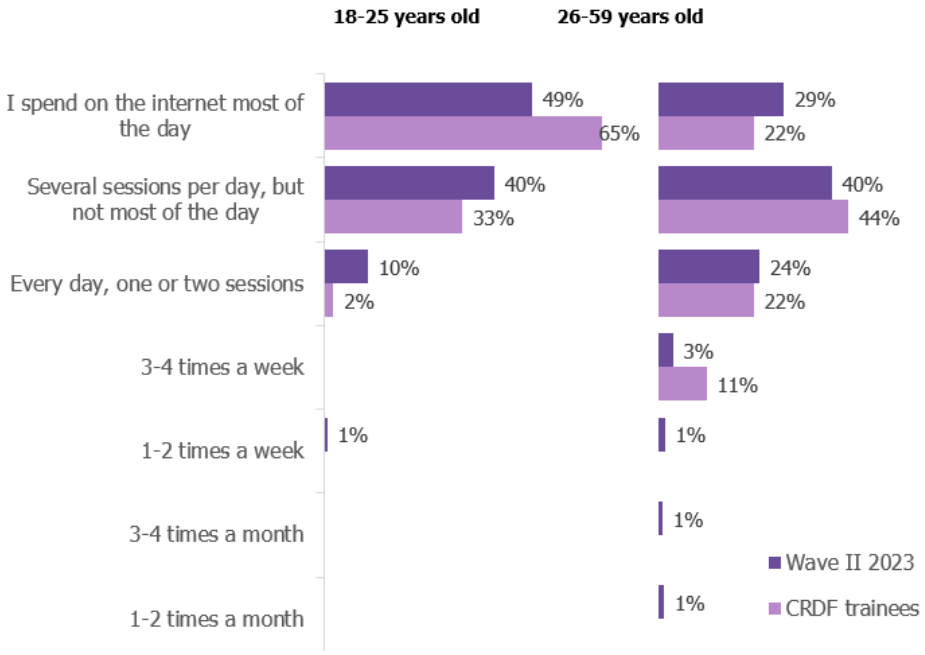
Thus, people with access to the Internet tend to use it daily, but while elderly people are, for the most part, limited to 1-2 sessions of communication per day, young people spend on the Internet most of the day.

Chart 3. How often do you use Internet, for example, visit websites, social networks, use applications, messengers? Distribution by target groups
(% of responses by waves I and II respondents)



Comparing answers by *CRDF Global* training attendees with those of the corresponding target groups of the main survey, it can be stated that among the former the young people aged 18-25 also spend on the Internet most of the day - 65% (see Chart 4).

***Chart** 1. How often do you use Internet, for example, visit websites, social networks, use applications, messengers? Distribution by target groups*
(% of responses by wave II respondents and CRDF Global course attendees)



Awareness of notions «cybersecurity» and «cyber hygiene rules»

The indicator of awareness of Ukrainians of such concepts as "cybersecurity" and "cyber hygiene rules" is measured for the second wave in a row via a direct question. However, checking the extent to which declarative knowledge corresponds to the real one is not one of research goals.

In general, the level of awareness of "cybersecurity" and "cyber hygiene rules" concepts has increased compared to the data of 2021 wave I. Thus, the answer "I know it very well and can explain it to others" was chosen by 19% and 14%, respectively for the concepts of "cybersecurity" and "cyber hygiene rules".

Ukrainians have better awareness of "cybersecurity" concept. 69% of the respondents have a general idea [1] about it, while 55% have at leasta general idea about the "rules of cyber hygiene". However, for both concepts, the decrease in the share of answers "I hear for the first time" is quite noticeable, with a corresponding increase in the share of answers "I have a general idea, without details." This may indicate the growing attention to "cyber hygiene rules" (see Chart 5).

It is quite obvious that there is a large gap in the level of awareness of "cyber hygiene rules" and "cybersecurity" concepts between 2023 wave II respondents and *CRDF Global* training attendees. Thus, 50% of training attendees "know it very well and can explain it to others" about the concept of "cybersecurity" and 49% "have a general idea, without details." Consequently, 52% of training

[1] The total of responses «I know it very well…» and «I have a general idea…»

attendees "know it very well and can explain it to others" about "cyber hygiene rules" and 46% of them "have a general idea, without details" (see Chart 6).

Chart 2. Tell me, please, how familiar are you with "cybersecurity" and "cyber hygiene rules" concepts? (% of responses by waves I and II respondents)

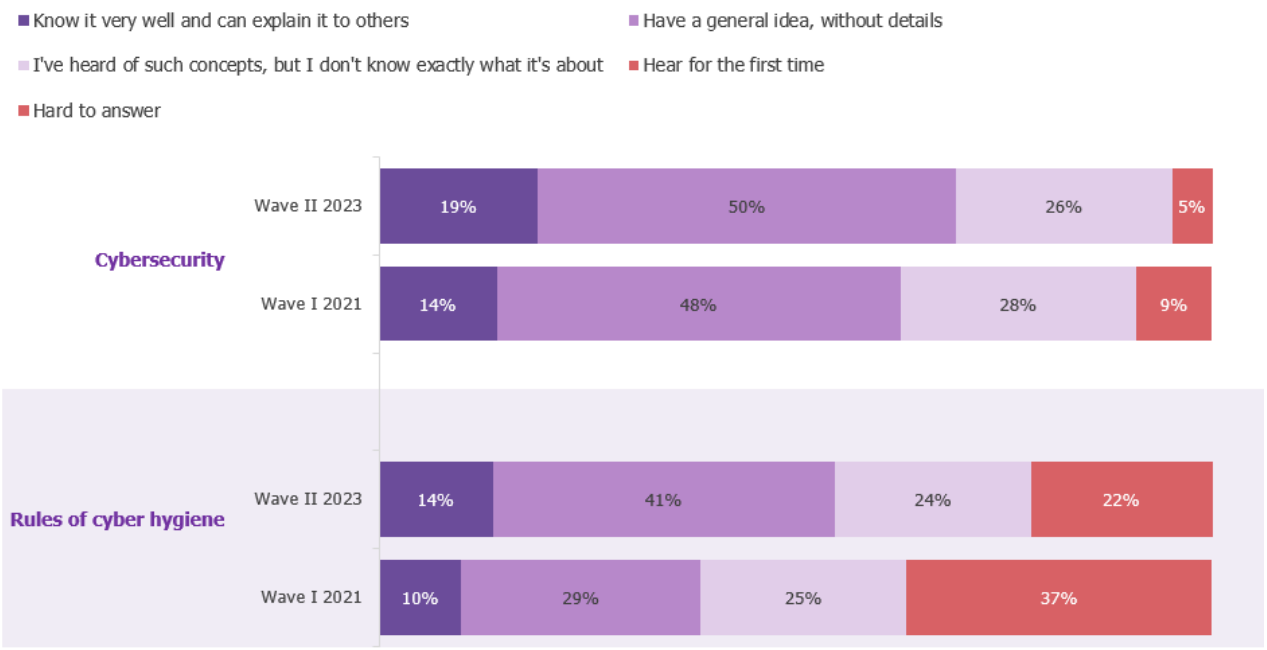
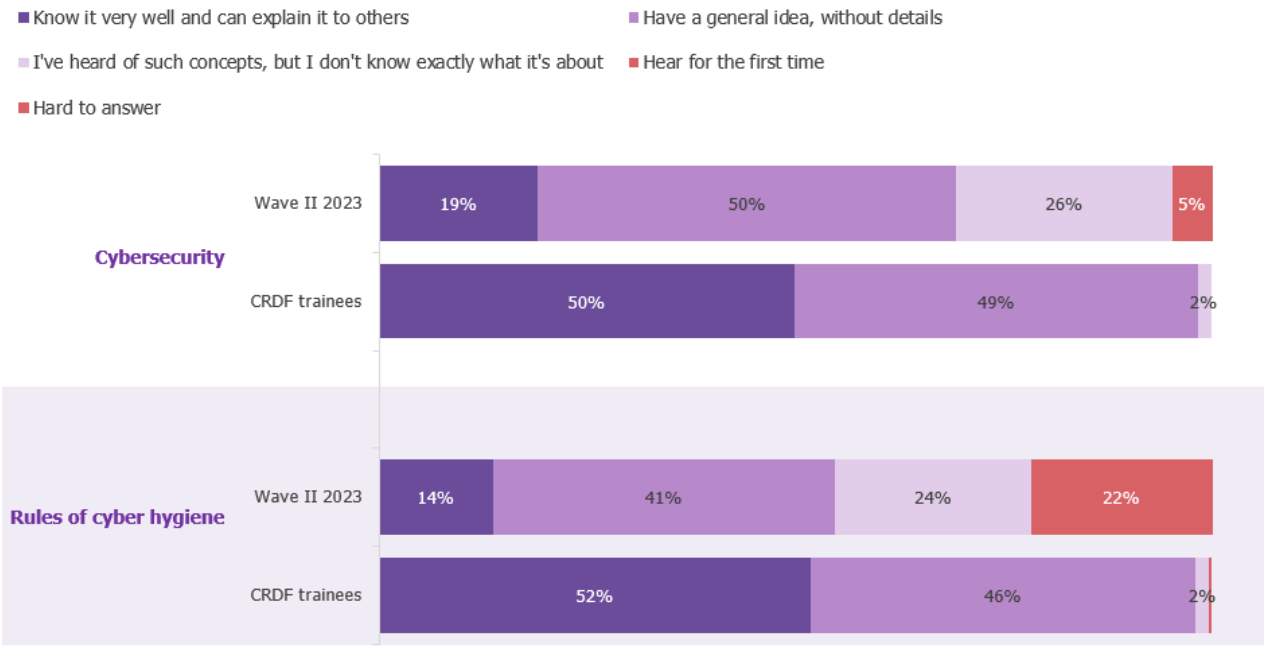


Chart 3. Tell me, please, how familiar are you with "cybersecurity" and "cyber hygiene rules" concepts? (% of responses by wave II respondents and CRDF Global training attendees)



A picture remains similar when division is made by age: indicators for general public and training attendees differ by 2-3-fold (see Chart 7).

Chart 7. Tell me, please, how familiar are you with "cybersecurity" and "cyber hygiene rules" concepts? Distribution by target groups (% of responses by wave II respondents and CRDF Global training attendees)

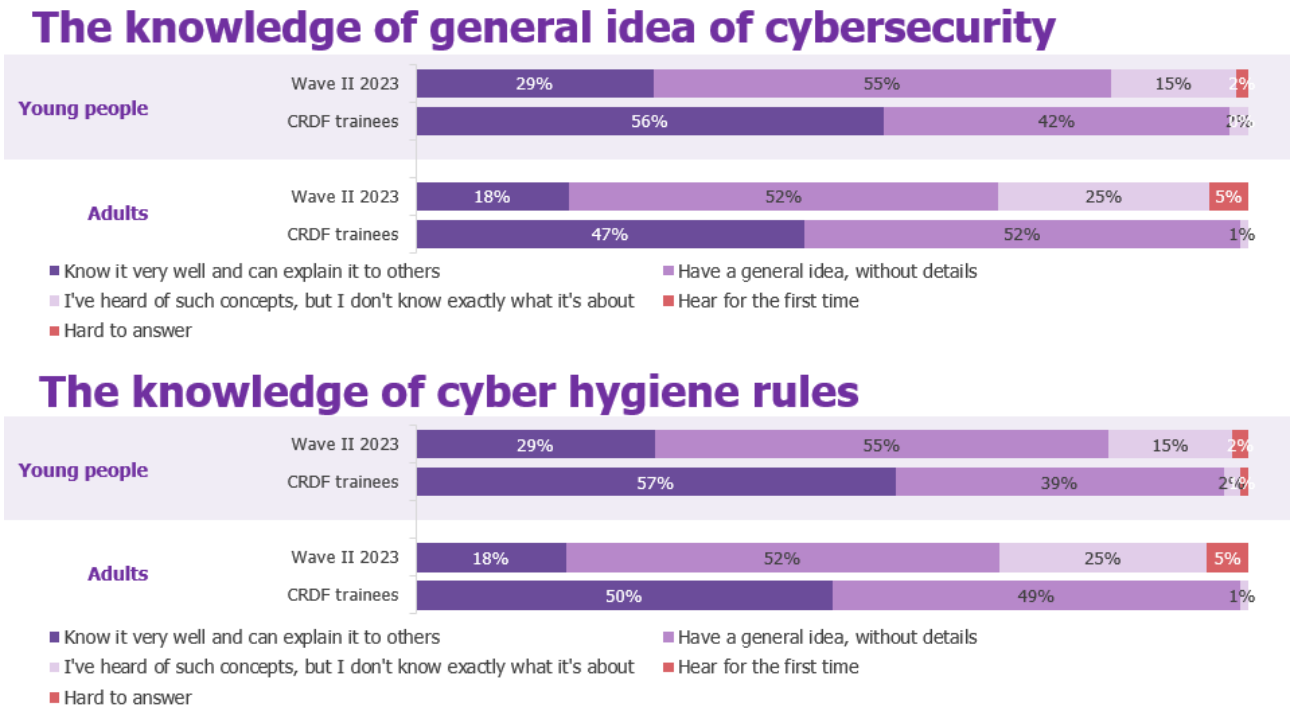
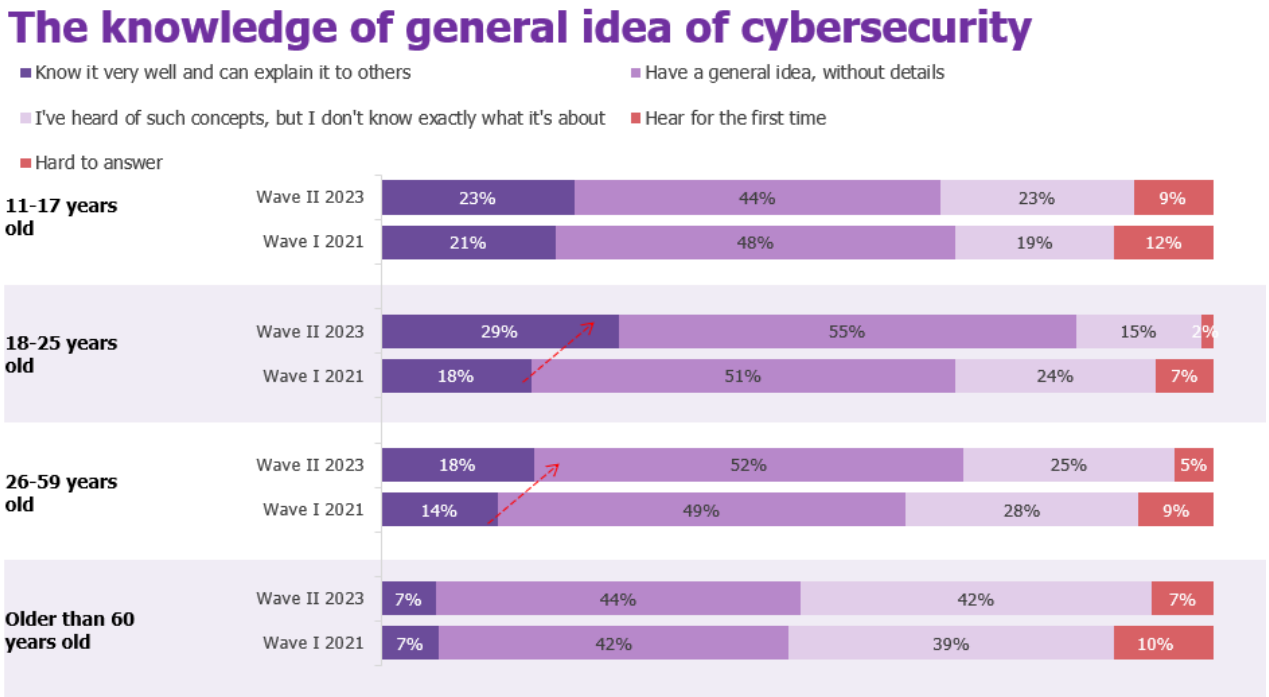
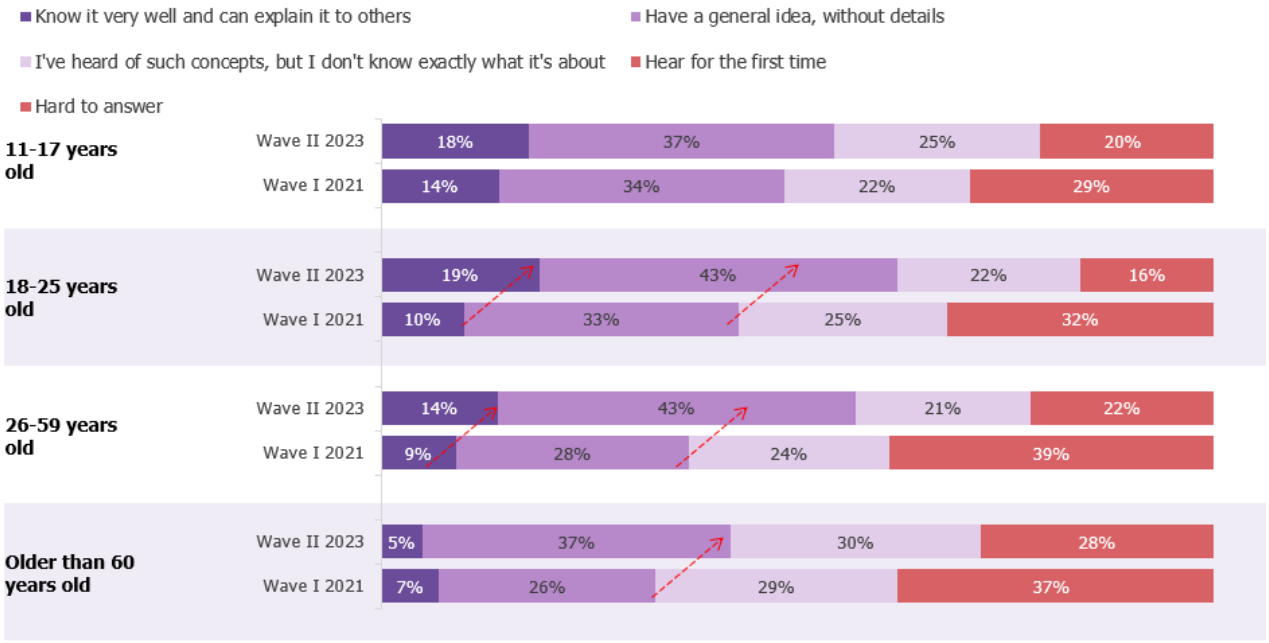


Chart 8. Tell me, please, how familiar are you with "cybersecurity" and "cyber hygiene rules" concepts? Distribution by target groups (% of responses by waves I and II respondents)



The knowledge of cyber hygiene rules



According to 2 waves' survey results, cybersecurity awareness indicators for age groups of 11-17 and elderly people aged 60+ do not vary much, although a slight increase in the share of "I have heard of such concepts" response is noticeable. At the same time, as for 18-25 and 26-59 age groups, the share of answers "I know it very well and can explain it to others" has increased (from 18% to 29% and from 14% to 18% respectively). "Cyber hygiene rules" knowledge has improved in all age groups, except for elderly people aged 60+ (see Chart 8).

FGD respondents also indicated that knowledge of cybersecurity and cyber hygiene is necessary for any user of digital devices and that this knowledge is as important as that of traffic regulations. Students and teachers talked about the getting basic knowledge at school, starting from the elementary level - from the time when a child starts using a phone.

"There is a total digitization of the society and the entire document management; all documents are available in electronic form. … certain rules must be followed in order to protect this information. And therefore, the rules of cyber hygiene must be followed. …in order not to lose your data or let them fall into the hands of people who can use it against you or against your interests." (female student)

"... we receive letters that have already been checked by the Department of Cybersecurity. Because such informational attacks have become more frequent now. ...now the topic is very important and should be the talk of the town." (Public sector employee, chief medical officer)

"I spent all my time introducing information culture and digital culture to my colleagues, i.e. managers of institutions, heads of district, community, and also taught computer science to children. Starting even from elementary school age, children already have a certain understanding of cybersecurity. They are already more or less aware of these dangers and rules. They are trying to secure a certain level of their privacy. But at the same time, there is an actual disregard for those rules, because they think, "who would be interested in us?" (Teacher)

Risky behavior

Within the framework of this study, it was proposed to evaluate several patterns of risky behavior on the Internet. Respondents answered how similar these behavioral patterns were to their own behavior. Comparing the results of 2021 wave I and current 2023 wave II, three patterns of risky behavior are all-time leaders:

- Absence of backup copies of documents and data (44% do not make them)

- Failure to use two-factor authentication (44% do not do this)

- Confidence that the user is not of interest to Internet scammers (64% are at least partially sure of this, 24% are sure) (see Chart 9).

Comparing answers of *CRDF Global* course attendees with those of 2023 wave II respondents, it is possible to state that course attendees are more likely to avoid risky behavior on the Internet and are aware of the dangers that may await them. Nevertheless, interviewed *CRDF Global* training attendees marked the following situations as "partially about me":

- Absence of backup copies of documents and data - 55%

- Confidence that the user is not of interest to Internet scammers - 44%

- Failure to use two-factor authentication – 37%

The comparison of answers to the question "I visit Russian sites" is interesting. 29% of the surveyed training attendees indicate that this is "definitely not about me" and "partially about me", while only 18% of 2023 wave II respondents indicate the same.

As for the question "I can insert someone else's flash drive or an unfamiliar flash drive into my computer", the gap between the answers "definitely about me" and "partially about me" by training attendees and 2023 wave II respondents is two-fold (47% and 24%, respectively) (see Charter 10).

Teachers and students note that the use of Russian websites, including for educational purposes, was widespread among young people and schoolchildren. Due to the full-scale invasion, the use of Russian resources, as well as Russian language, has sharply decreased among young people and schoolchildren - opposition to everything Russian is a mass trend. Civil servants and representatives of local government authorities note that even before the invasion they were seldom using Russian, except for downloading the necessary, often unlicensed, software, which they are now trying to minimize.

"I am not on Russian social networks. Even before the full-scale invasion, I sometimes went to Russian websites solely to find the necessary literature, because it was practically unavailable in Ukrainian. And access to everything in English is closed, and commercial subscription is needed. And Russian stuff was free. But now I do put a lot of effort into searching in French or English, that's all. And I don't go to .ru anymore." (Female student)

"Unfortunately, we have a lot of outdated equipment, so there is a need for some drivers and so on. And I have to download it all from Russian resources... I use a VPN server, and, accordingly, through a VPN server, I localize myself as a user, presumably, from Russian Federation. And then I download the necessary content." (Local government authority employee)

Chart 4. I will read several statements. Let me know how they relate to you.
(% of responses by waves I and II respondents)

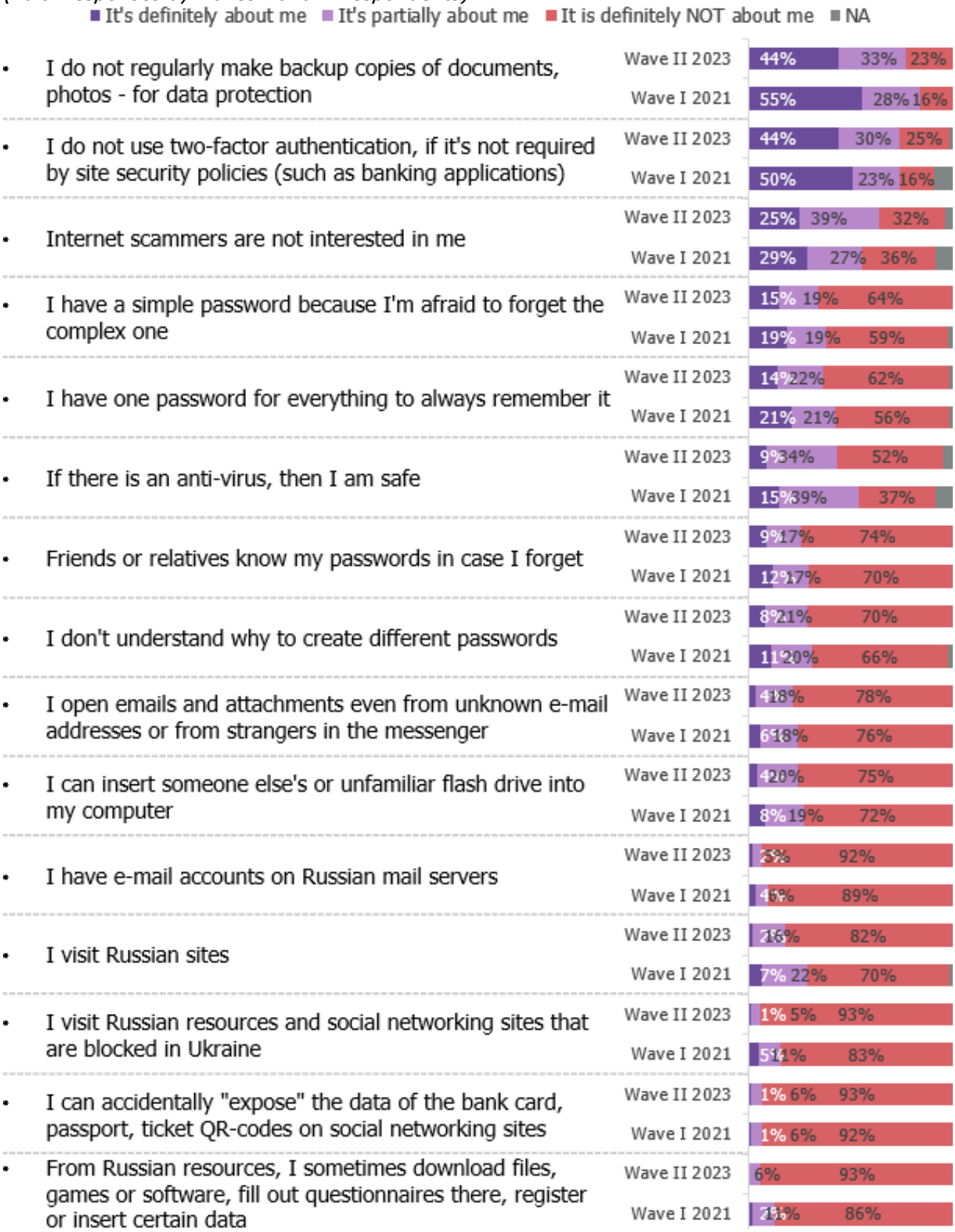
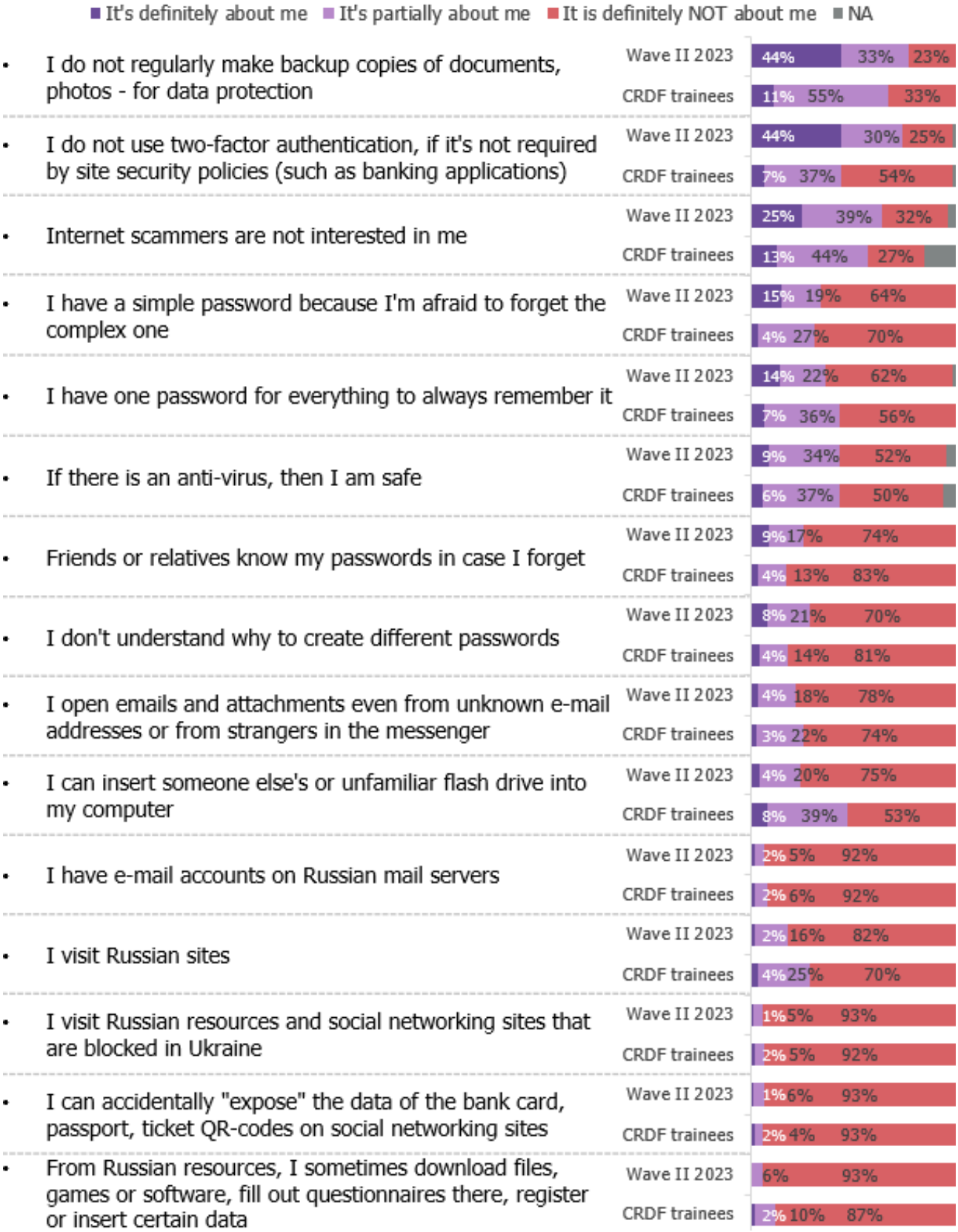


Chart 5. I will read several statements. Let me know how they relate to you.
(% responses by wave II respondents and CRDF Global course attendees)



Failure to use backup copies and two-factor authentication remain the main risk behavior patterns for all age groups. Teenagers are more confident, than the rest of the audience, that they are of no interest to Internet scammers: 38% are sure of this, while another 28% are partially sure (for comparison: in wave I study, these indicators were at the level of 45% and 27 % respectively).

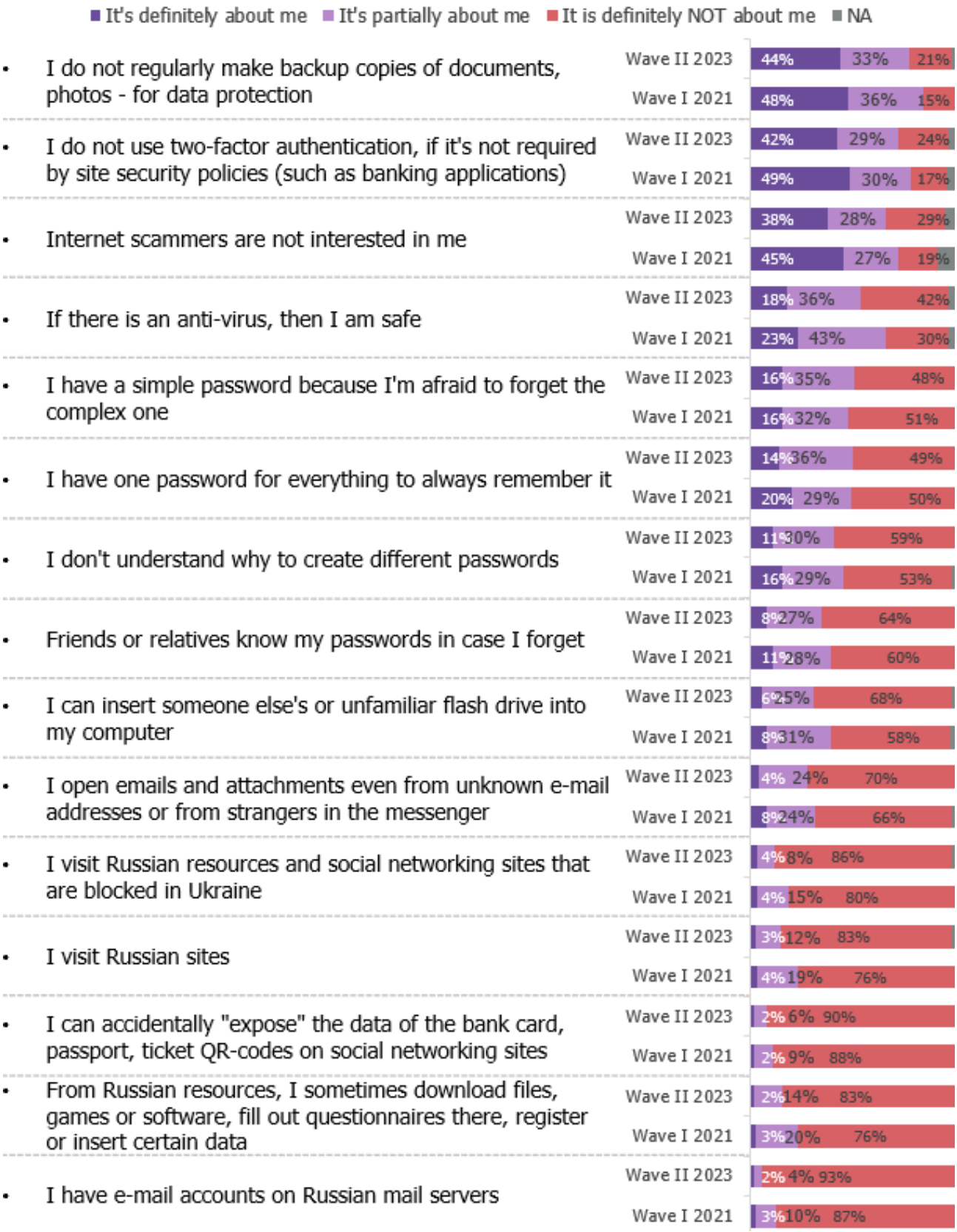
Also, to a greater extent than other respondents, teenagers are sure that antivirus provides full protection.

The indicator of using one single password for all occasions remains higher among teenagers than in the sample in general: 14% reported that this behavior pattern completely matches theirs (9% in the sample in general). (see Chart 11).

Teachers confirm that the younger the children are, the simpler their passwords are, and there is also a tendency to create one password for different accounts. Passwords of younger children can be known by their parents and they can also pass them on to friends. Older children are more concerned about privacy issues, and high school students demonstrate more serious attitude to cybersecurity rules. In general, there is a common perception among children that cyber-scammers are not interested in them because they do not have bank accounts or financial assets.

"One single password is the dominant password behavior pattern. One password for everything is their rule. The only ray of light here is the fact that children invent such a password that requires good finger skills - up to 11, 12 or more characters, but one for everything." (Teacher)

Chart 6. I will read several statements. Let me know how they relate to you. Distribution by target groups – 11-17 years old. (% of responses by waves I and II respondents)



Young people aged 18-25 remain the most cautious target group among others: they use two-factor authentication more regularly and make backup copies of documents and data (and the share of those who do not do this is almost half of that of the sample in general). The important change reported is the increase of two-factor authentication use indicator in this age group by 6 p.p. compared to 2021 wave I.

Also, young people less frequently agree that they are of no interest to Internet scammers (18% strongly agree vs. 25% of the sample in general) (see Chart 12).

"I believe that there are simply no uninteresting people to Internet scammers. They will still be able to use, for example, your page in social networks in any way. Friends also had a case when their page was simply hacked and used for advertising. Therefore, I am 100% sure that I am of interest to everyone." (Student)

Although this age group visits Russian sites most often, a noticeable two-fold decrease in the indicator of these visits - from 40% of wave I respondents to 22% at the moment – is reported, and this fact is of great importance. As for teenagers, this indicator is now 15% vs. 23% (wave 1), for adults - 19 vs. 28%, for elderly people – 12 vs. 24%.

Analyzing risky behavior indicators of 18-25-year-old course attendees, attention should be drawn to the fact that although 10% of them replied "I do not make backup copies of documents, photos - for data protection" - "it is definitely not about me", but, at the same time, 62% stated that it was "partially about me". (see Chart 13).

It can also be said that *CRDF Global* course attendees aged 18 - 25 do not pay enough attention to passwords. Thus, 58% of them use one and the same password in one way or another (28% of the corresponding age category of wave II respondents) in order to always remember it. 39% of attendees have a simple password because they are afraid to forget a complex one (16% of wave II respondents).

"I know I have a problem with passwords. I have a very similar or completely identical passwords for almost all accounts, which is incorrect. Since I often forget them and it takes a long time to renew everything, I made it the same for everything. Sometimes, when I really need to find some information, but it is available on the site with insecure connection, I can turn off the antivirus. Although I know that it shouldn't be done." (Female student)

Chart. I will read several statements. Let me know how they relate to you. Distribution by target groups – 18-25 years old. (% of responses by wave I and II respondents)

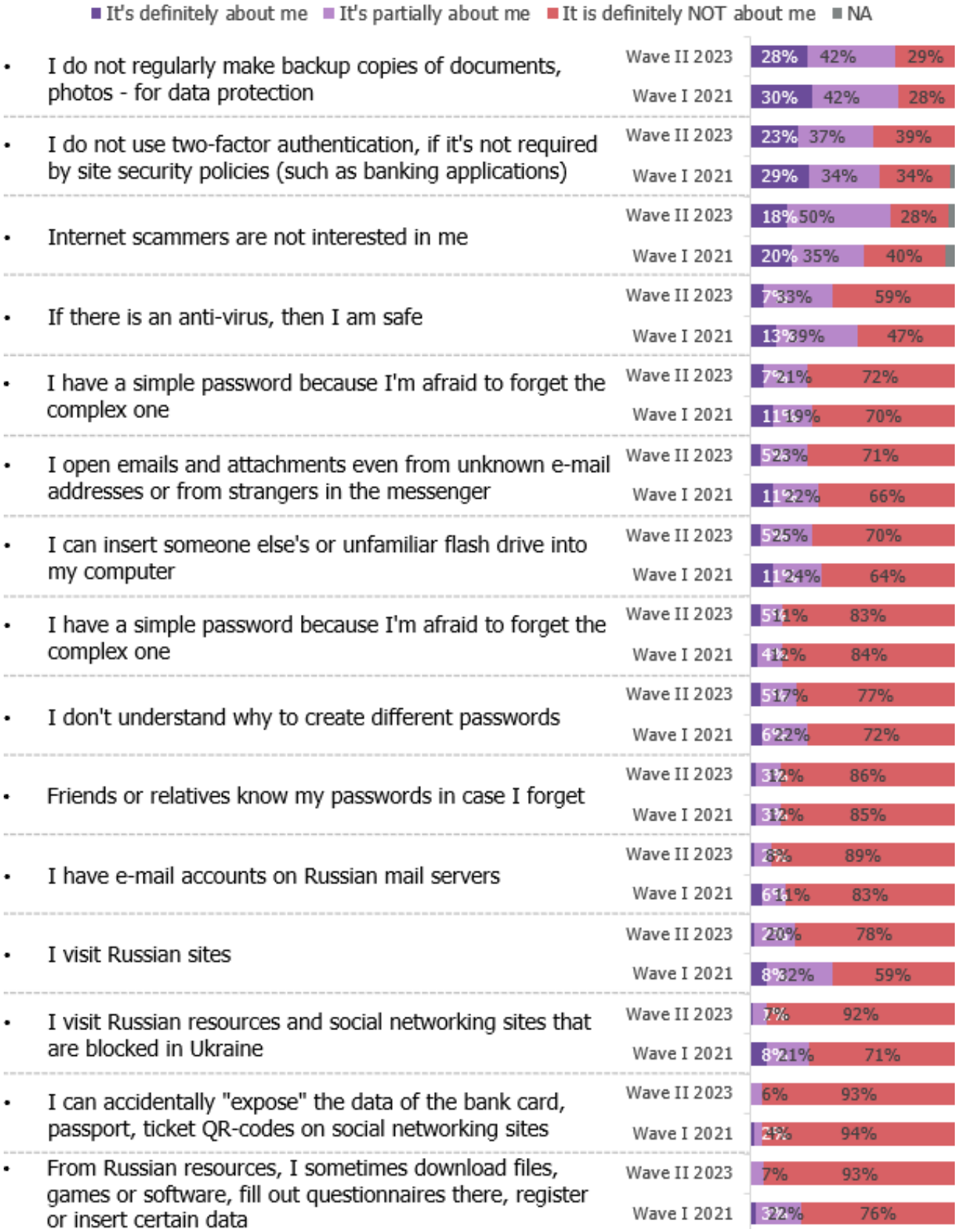
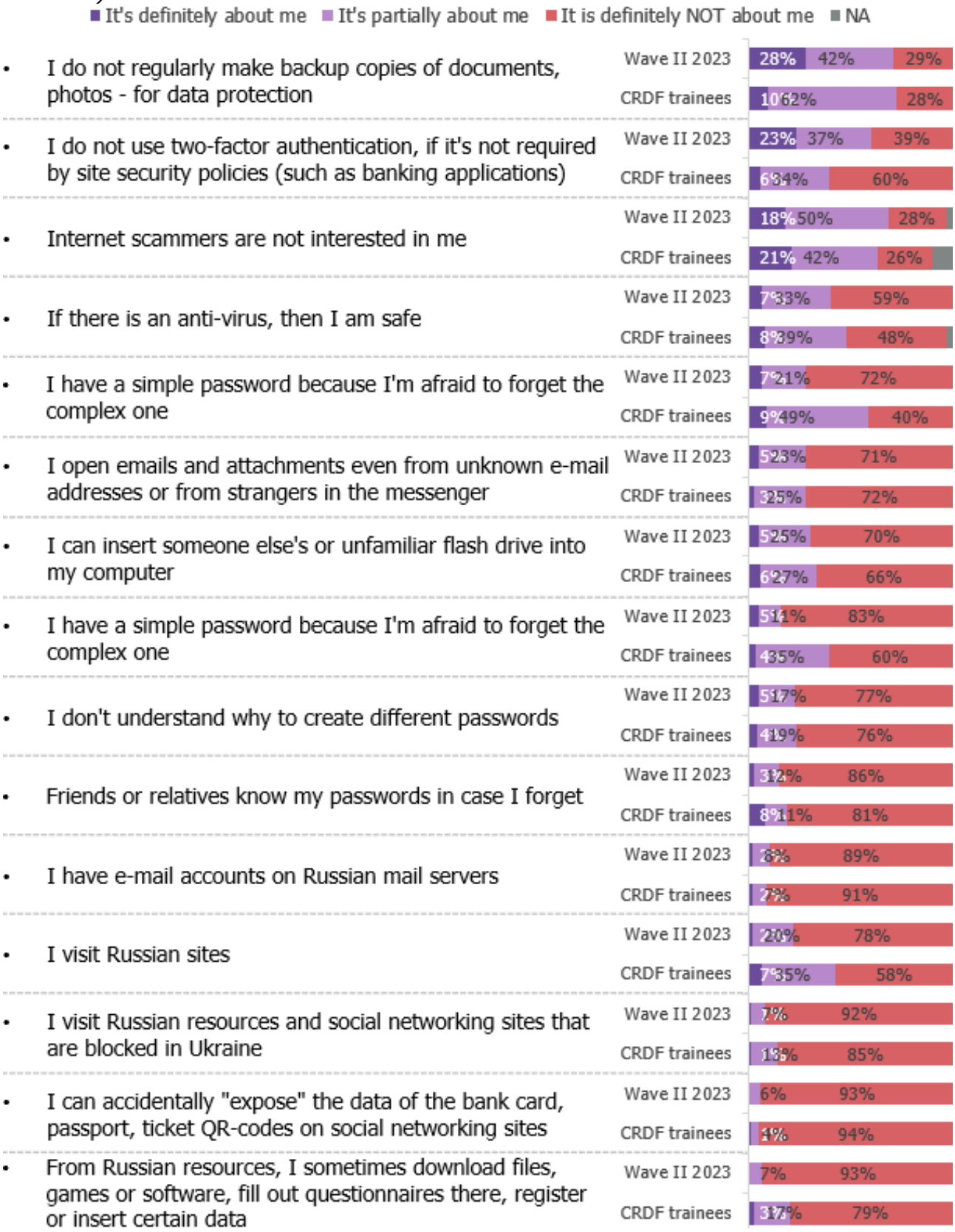


Chart 7. I will read several statements. Let me know how they relate to you. Distribution by target groups – 18-25 years old. (% of responses by wave I respondents and CRDF Global course attendees)



Among adults aged 26-59, more than half of 2021 wave I respondents (57%) did not make backup copies of documents and photos for data protection. In 2023, this indicator has decreased by 13 p.p. to 44%.

"I don't make backup copies regularly, but I do them partially. ...there is a lot of business information, single copy documents, and now I am actively using Google Drive. …if something happens to my computer, I will still have a document in the cloud. Therefore, it is convenient to work with cloud technologies. However, people seldom do this and some still save information on pin drives and even on CDs, which are not reliable media. (Local self-government authority employee)

Almost half of the respondents in this age group (40%) do not use two-factor authentication unless required by the site's security policy, but overall this indicator has decreased by 8 p.p. As for passwords, 14% of the respondents have a simple one fearing to forget a complex one, and 12% use one password for everything for convenience reasons (for comparison, in 2021, these indicators were 19% and 20%, respectively) (see Chart 14).

"...some of my passwords are the same, the ones to not very important resources. But after all, this is my flaw ... a habit and, after all, it is more convenient." (Local self-government authority employee)

Notable is the fact that the vast majority (56%) of *CDRF Global* course attendees belonging to this age group "can insert someone else's or unfamiliar flash drive into their computer," while only 26% of wave II respondents of this age group (see Chart 15).

During focus group discussions, public sector workers indicated that they were continuing using flash drives quite often and that the use of other people's flash drives was possible and quite common. Another violation reported is digital signature data transfer to colleagues in order to shorten processing procedure for certain documents.

"It is a common situation when people think that these flash drives are friends' and colleagues', but they are other people's pin drives. And you don't know where this pin drive has been before. And the problem is not deliberate infection of the computer. A person could insert her pin drive into an infected computer and bring you the virus ...we don't always do what's right. I avoid it, but it is common among colleagues." (Educational authority employee)

Failure to use a two-factor authentication remains the most widespread risky behavior pattern among elderly people (60+) in comparison with other age groups: 77% of the respondents do not use this protection method. It is noteworthy that this indicator has increased by 7% compared to the previous wave of study. Also, elderly people more often than the general audience use one simple password and/or have one password to remember.

Like teenagers, elderly people often (34%) say that they are of no interest to Internet scammers. They also more often (than other age groups) lack understanding of the need for complex passwords (15% compared to 9% of the sample in general). It should be pointed out that this indicator is decreasing (19% in wave I group of elderly people and 12% in the sample in general), therefore the trend is positive.

Elderly people more often share their passwords with friends or relatives: 21% fully support this behavioral pattern, 16% partially support it (for comparison, in the sample in general, these indicators are 12% and 17%, respectively) (see Chart 16).

Chart 8. I will read several statements. Let me know how they relate to you. Distribution by target groups – 25-69 years old. (% of responses by wave I and II respondents)

Chart 9. I will read several statements. Let me know how they relate to you. Distribution by target groups – 25-69 years old. (% of responses by wave II respondents and CRDF Global course attendees)

Chart 10. I will read several statements. Let me know how they relate to you. Distribution by target groups – elderly people aged 60+ years old. (% of responses by wave I and II respondents)

Respondents who participated in FGD and IDI also confirmed that they often have access to the accounts and devices of their older relatives, because they take care of security and can help them with one or another issue. In addition, the respondents set passwords on the device, therefore they have this information.

Undoubtedly, use of Russian mailboxes, visiting Russian resources and social networks blocked in Ukraine, as well as visiting Russian sites and performing certain actions on them, such as downloading files, filling out questionnaires, registration, especially in the context of current situation, remains a separate risky behavior pattern.

Currently, there is a noticeable decrease in visits to Russian sites. At the moment, 18% of the respondents follow such practices, while in the previous wave of the study, this indicator was at the level of 30%. Russian sites visiting indicators by age group compared to the previous wave are as follows:

- 15% among teenagers 11-17 (wave I - 23%);
- 22% among young people aged 18-25 (wave I - 40%);
- 19% among adults 26-59 (wave I - 28%);
- 12% among elderly people aged 60+ (wave I - 24%).

However, it can be assumed that two-fold decrease in the level of use among the elderly people can be explained by the fact that Russian resources and sites are currently blocked, and they have not learned how to use VPN service allowing access to Russian domains.

Also, visits to Russian resources and social networks blocked in Ukraine has significantly decreased among the young people aged 18-25 (more than three-fold, from 29% to 8%) and among adults aged 26-59 (more than two-fold, from 15% to 7%).

Teenagers download files and programs from Russian resources as well as register in them more often than other groups. The share of the respondents with this behavior pattern among this group is 16%; the rest of the groups – young people, adults and elderly people demonstrate this behavior pattern two times less often (7%, 6% and 4%, respectively).

Currently, there is an obvious decrease in Russian mailboxes availability indicator among respondents aged 18-25 (from 17% in 2021 to 10% in 2023) and teenagers aged 11-17 (from 13% in 2021 to 6% in 2023).

Experience of Encountering Cyber-Threats

The respondents were asked to rate their experience of encountering cyber threats in order to monitor the situation and conduct a comparative analysis with the data from the previous study wave in 2021. 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 had happened to them personally, their real or virtual acquaintances.

The situation when cybercriminals' extortion of bank card details, passwords and access to mobile application accounts is currently the top in the sample in general. Second place belongs to the situation that was the leader last time - extortion of money using social engineering techniques (manipulation, threats, blackmail), as well as personal and family data (via phone and messengers). The first situation was evaluated by adults aged 26-59 and elderly people aged 60+, and the second situation was evaluated only by elderly people (see Chart 17).

As for *CRDF Global* training attendees, the TOP-3 situations that have happened to them or to their acquaintances are the following (see Chart 18):

- Theft (hacking) of accounts on social networking sites;
- Theft (hacking) of game accounts in computer games;

Focus group participants know a little about the mechanisms of such hacks:

"No one will write to you "give me your e-mail address" because such person will be immediately blocked. But they use some manipulations first in order to gain a certain authority and ask for your data after that. Some of my acquaintances, who have found themselves in such a situation, due to imprudence, did provide these data... more advanced ones ask for a mail. And after that, the password is guessed, almost everything is now done via mail. Then they download the password database and select it. …it is very important not to transfer passwords in any case, and to create a complex password that takes a long time to guess." (Female student)

Chart 11. I will read a list of the main threats that can be encountered by the Internet user and you, please, tell whether you personally or your friends have encountered such situation. (% of responses by waves I and II respondents)

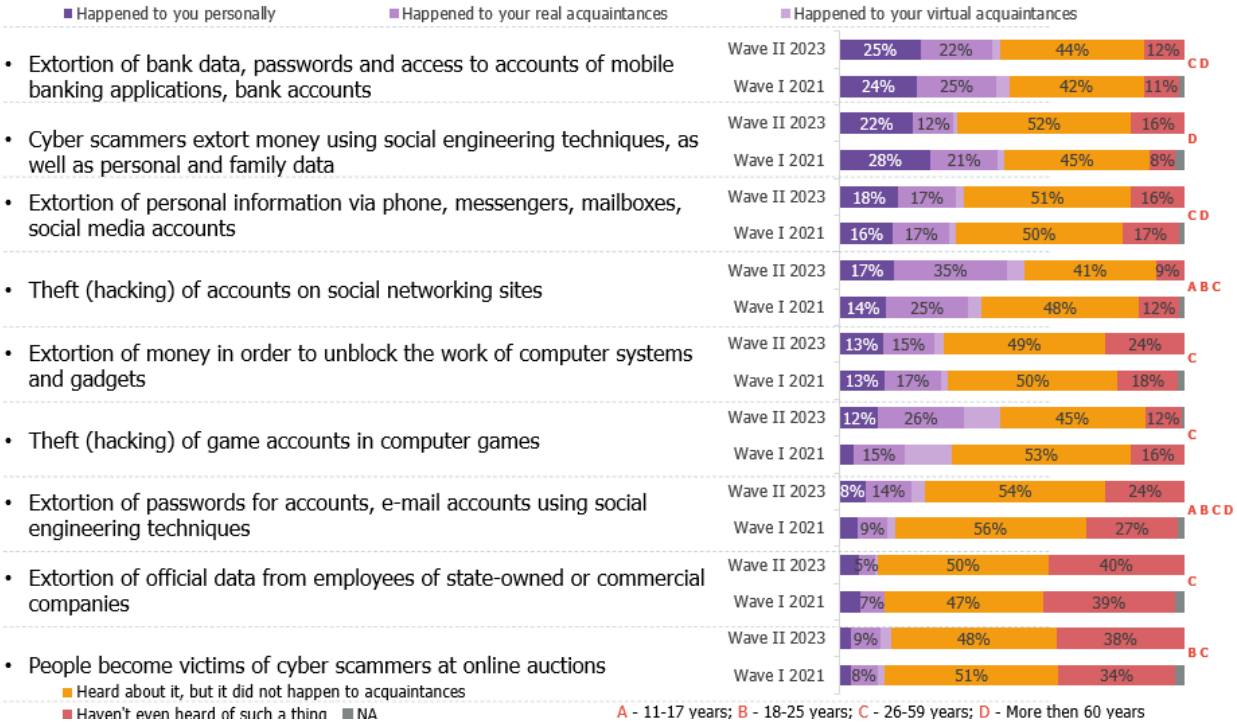
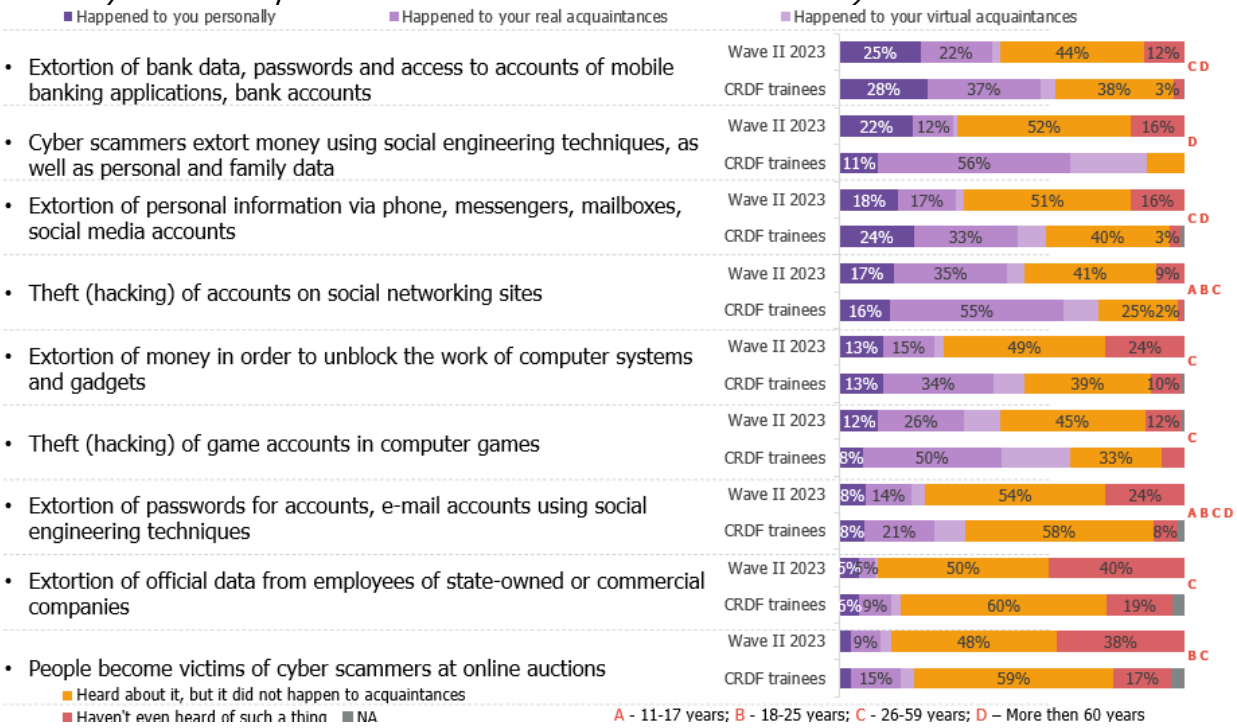


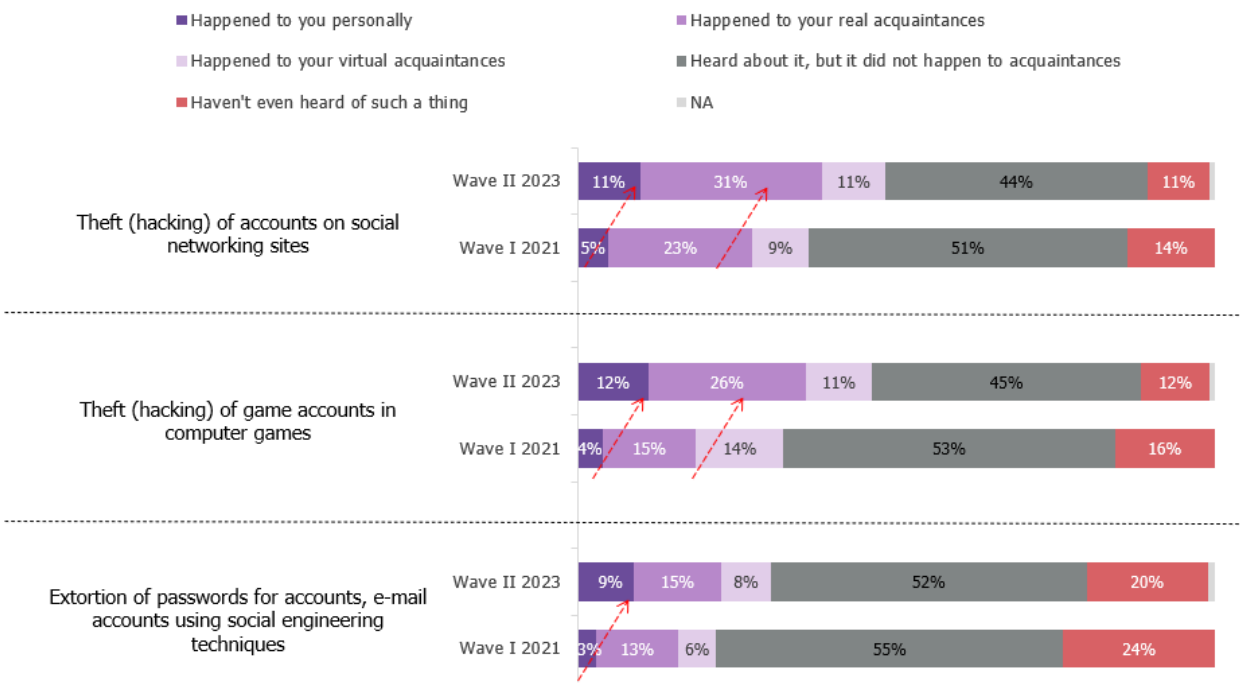
Chart 12. I will read a list of the main threats that can be encountered by the Internet user and you, please, tell whether you personally or your friends have encountered such situation. (% of responses by wave II respondents and CRDF Global course attendees)



Currently, teenagers most often encounter theft of game accounts in computer games. This indicator has generally increased by 15 p.p. if compared with wave I and taking into account the situations that have happened not only to the study participants but also to their acquaintances. Taking into account the general picture for this age group, it can be seen that all the situations relate more to the surveyed respondents (see Chart 19).

"...from what I see, most often these are hacks of social networks, children's own accounts. Next - hacks of cheap game accounts. In other words, children often buy a "cool" account with alleged bonuses at a very cheap price to play later on the network and so on. This is what is happening to my son - his accounts are hacked every few days because he buys cheap accounts in some games" (Teacher)

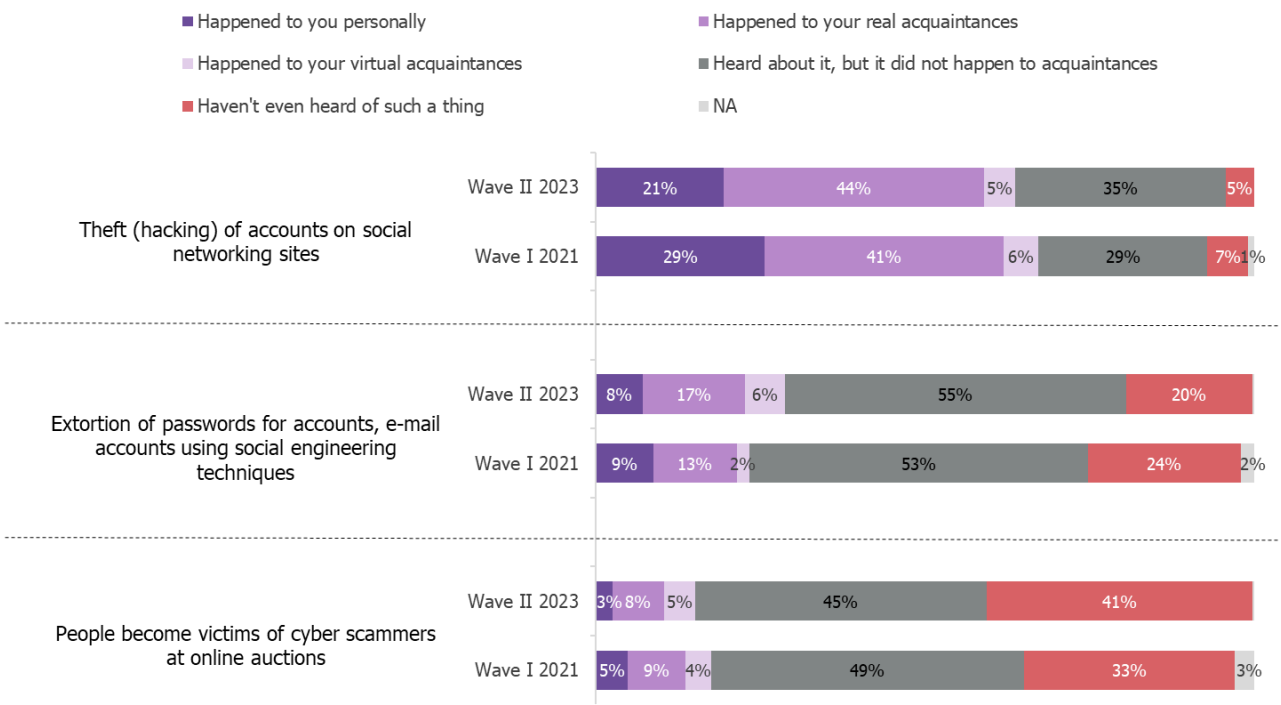
Charter 13. I will read a list of the main threats that can be encountered by the Internet user and you, please, tell whether you personally or your friends have encountered such situation.
Distribution by target groups – 11-17 years old (% of responses by waves I and II respondents)



However, young people aged 18-25 continue facing theft of accounts on social networking sites more often than all other target groups. This indicator, although reduced from 29% to 21%, remains the highest among other age groups (see Chart 20).

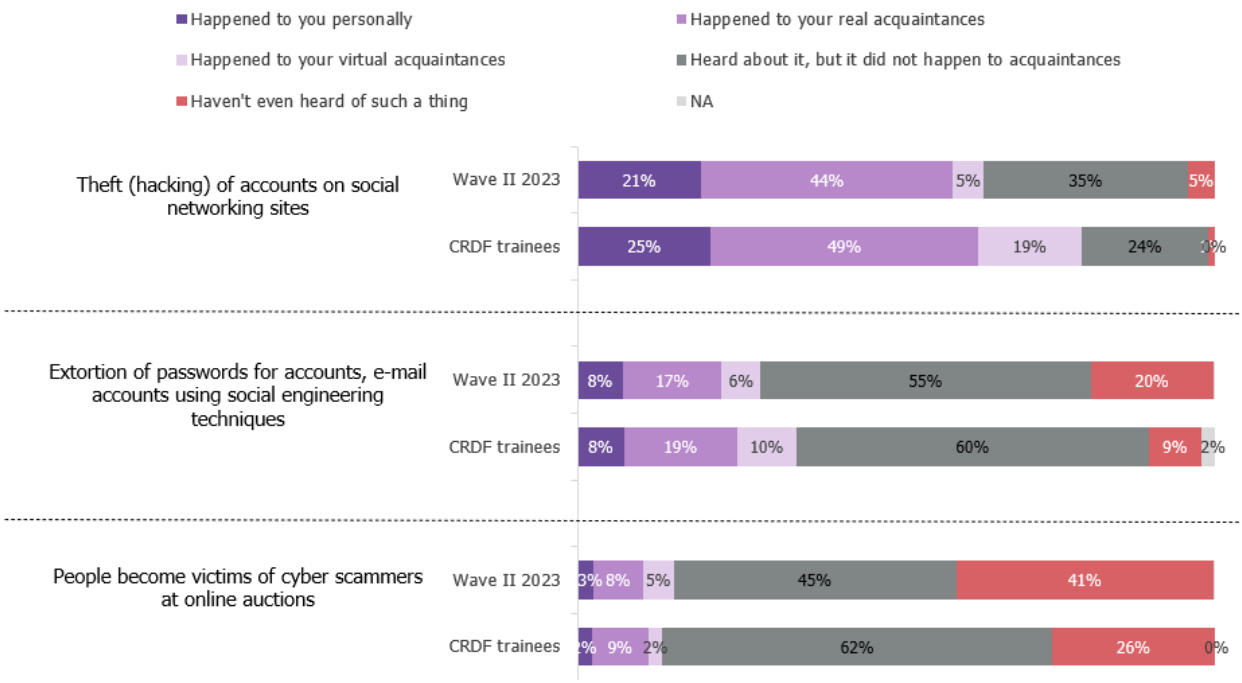
"For the most part, I follow almost all cyber hygiene rules because I had a very negative experience. ...there was such a situation that I just barely managed to intercept access to my Google account, so after that I completely changed all my passwords." (Student)

Charter 14. I will read a list of the main threats that can be encountered by the Internet user and you, please, tell whether you personally or your friends have encountered such situation. Distribution by target groups – 18-25 years old (% of responses by waves I and II respondents)



Respondents of this age group who have attended *CRDF Global* course have encountered cyber threats as often as wave II respondents (see Chart 21).

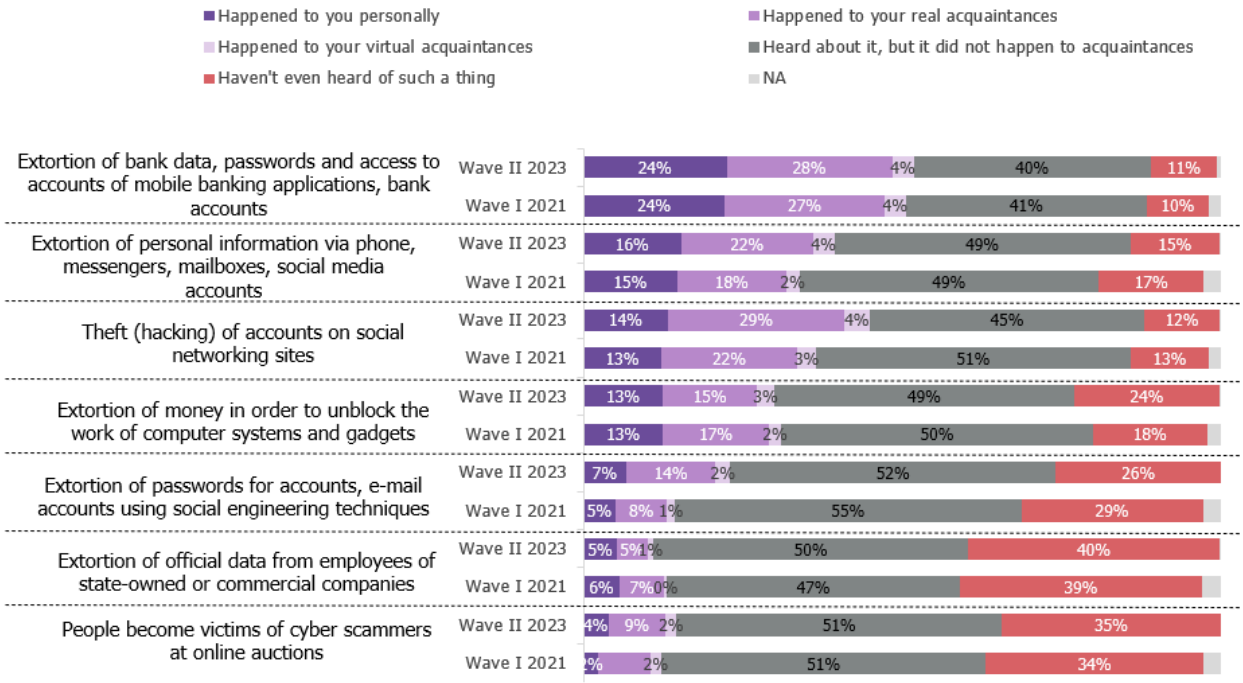
Charter 15. I will read a list of the main threats that can be encountered by the Internet user and you, please, tell whether you personally or your friends have encountered such situation. Distribution by target groups – 18-25 years old (% of responses by waves II respondents and CRDF Global course attendees)



For the adults aged 26-59, the most widespread threat is extortion of bank data, passwords and access to accounts of mobile banking applications, bank accounts (including via phone, messengers): one in four has encountered this personally, 28% know about such cases from the acquaintances. Cases of personal information extortion, hacking of accounts on social networking sites and extortion of money in order to unlock the work of computer systems also remain common (the share of the respondents who have encountered such situations personally is 16%, 14% and 13%, respectively). The prevalence of these cyber threats has remained largely unchanged since 2021 (see Chart 22).

"I personally have not encountered any cases of scam, but my friends had their Facebook page hacked. ... there was also a mailing, a message that money is needed and request to wire it… There were also calls from scammers who introduced themselves as bank employees, but did not specify the name of the bank and asked to provide the card data." (Local self-government employee)

Chart 16. I will read a list of the main threats that can be encountered by the Internet user and you, please, tell whether you personally or your friends have encountered such situation. Distribution by target groups – 26-59 years old (% of responses by waves I and II respondents)

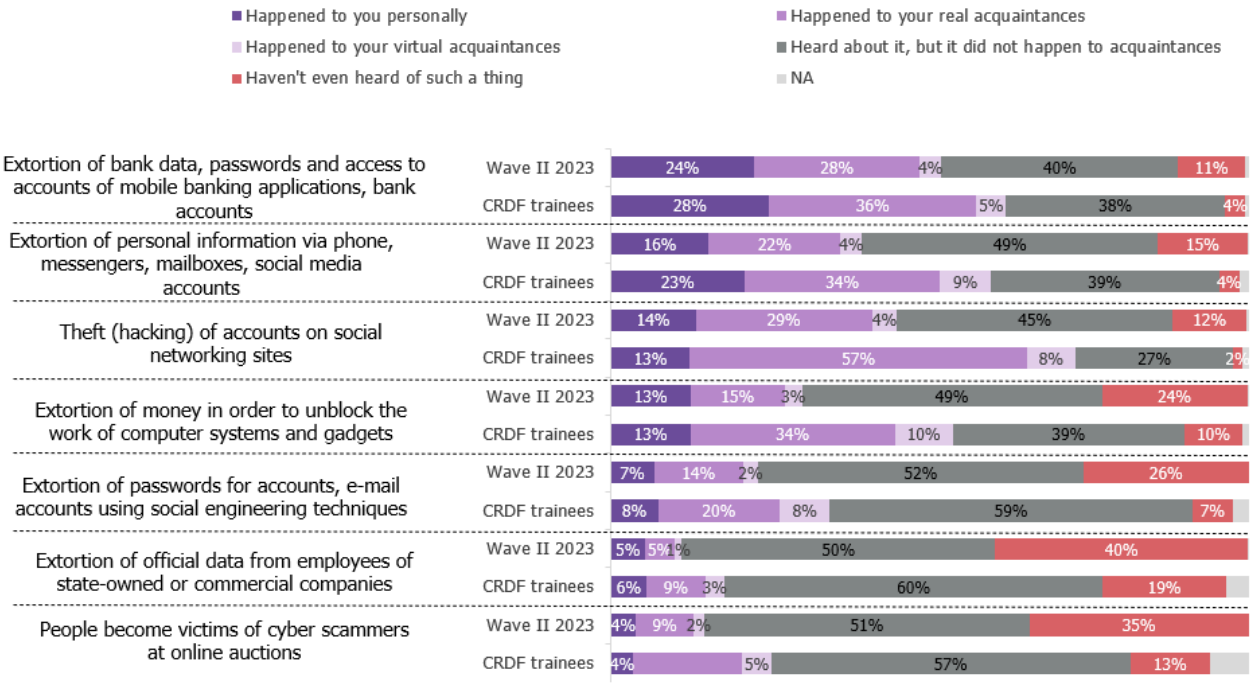


Analysis of responses by CRDF Global course attendees demonstrates a significant difference: there are more such situations among the "virtual acquaintances" of the interviewed respondents than among the acquaintances of wave II respondents. In particular, this applies to the following situations (see Chart 23):

- Theft (hacking) of accounts on social networking sites – 57%
- Extortion of bank data, passwords and access to accounts of mobile banking applications, bank accounts - 36%
- Extortion of personal information via phone, messengers, mailboxes, social media accounts - 34%
- Extortion of money in order to unlock the work of computer systems and gadgets - 34%

A possible explanation of the above may be the fact that training attendees possibly pay more attention to such situations and discuss them more often with acquaintances.

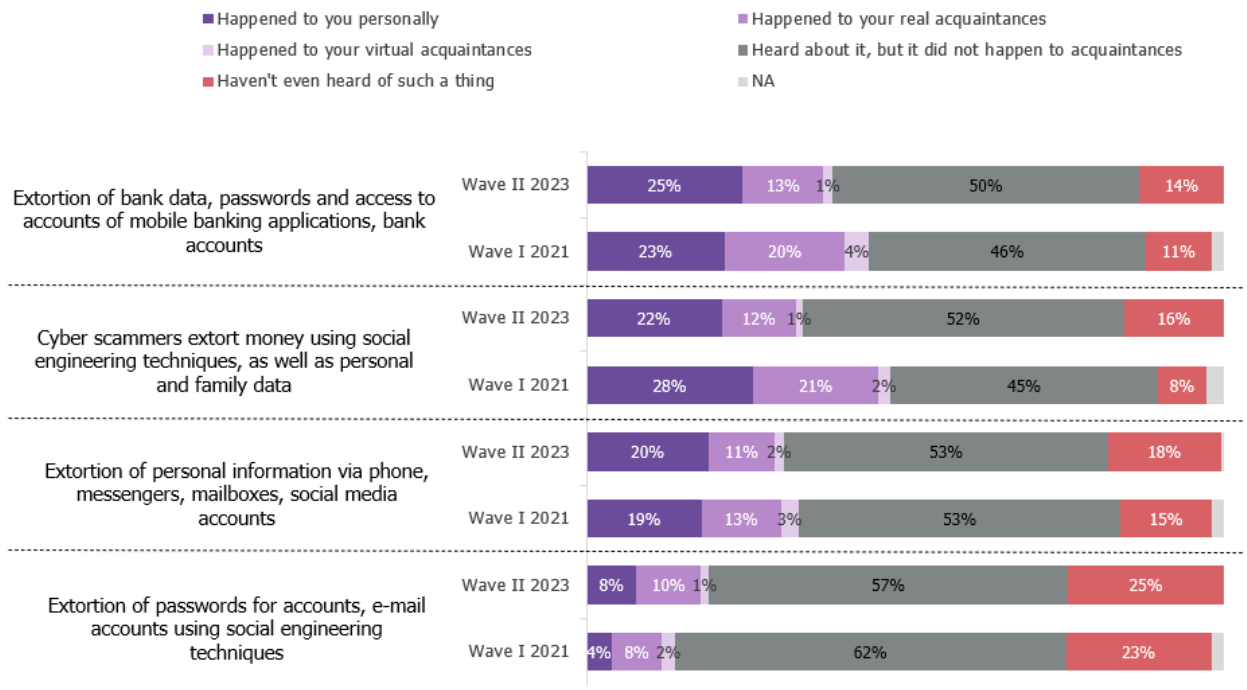
Charter 17. I will read a list of the main threats that can be encountered by the Internet user and you, please, tell whether you personally or your friends have encountered such situation. Distribution by target groups – 26-59 years old (% of responses by waves II respondents and CRDF Global course attendees)



Elderly people continue facing cyber threats more often than other groups. For example, 25% of the respondents from this age group have personally encountered extortions of bank data, passwords, and access to accounts of mobile banking applications and bank accounts. Situations where cyber scammers extort money using social engineering techniques (manipulation, threats, blackmail), as well as personal and family data (via phone and messengers) were personally experienced by 22% of the respondents (see Chart 24).

"They extorted money from my parents at night for releasing me from the police. This is a very common scam when elderly people are phoned and told that something has happened to their child. My parents thought that the voice was similar to mine, but they called me back anyway, but it happens that people transfer funds. (Local self-government employee)

Chart 18. I will read a list of the main threats that can be encountered by the Internet user and you, please, tell whether you personally or your friends have encountered such situation. Distribution by target groups – over 60 years old (% of responses by waves I and II respondents)



Awareness of Cybersecurity Rules

Within the frameworks of this study, issues related to basic rules of cyber hygiene have also been raised. Target groups were given the opportunity to assess attitudes towards basic rules of cyber hygiene in order to monitor the situation and track trends. Among the TOP-3 most complied with basic rules of cyber hygiene remain:

- Do not send photos and scans of bank cards and personal documents to strangers and dubious organizations (89%);
- Do not leave your device unattended, especially when operated in public places (86%);
- Do not send your contact phone numbers and personal photos to strangers, especially those asking for nude photos (83%)

The respondents are aware of most of the rules (see Chart 25).

CRDF Global course attendees are familiar with all cybersecurity rules better than the general population of Ukraine. However, they do not follow all the rules, in particular:

- Do not connect to public, unknown, or unprotected Wi-Fi networks
- In case of any suspicion of infecting your device or compromising data, IMMEDIATELY notify the relative authorities: Cyber Police of Ukraine etc. (see Chart 26).

IDI and FGD respondents mentioned that they do not believe in cyber police actions effectiveness, therefore they often do not consider the option of contacting the relevant authorities in case of violations. All the respondents know that cyber police does exist, but, for the most part, do not consider it necessary to contact them in case of minor scams, such as account hacking or calls from scammers. Some respondents indicated that they had had negative experience with cyber police when their application had not been considered. At the same time, the respondents pointed out that there were cases of successful investigations, which, however, were worked on under considerable pressure and in the focus of attention of people who have contacted the authorities. Respondents from the public sector believe that the cyber police are gradually gaining experience in confronting various attacks and scams and learning to investigate such cases, and at the time of war and cyber threats coming from the Russian Federation this is of paramount importance.

"...the police told me that they had more important things do to. I had such a terrible disappointment, because they actually talk about terrible things here and it is not known what is behind it, maybe people are caught and killed there on the air; it is a closed group and, for some reason, I received that invitation. I felt so responsible that I should report it. As a result, they made it look like I don't know what." (Female student)

"It was a case of tough persecution. Then it turned out that this swindler had already committed two similar crimes. There was an investigation and I observed it. But when it came to solving the problem, it took so long and at such a low level, that life protection from cyber-crimes and - it is not about this ... my personal opinion is that, God forbid, but I would hardly turn to them as the only authority that can help. Maybe now, at this stage, when there is an ongoing war, when they are brought to their knees, these authorities, maybe they will be a little faster." (Teacher)

"Of course, I heard about Cyber Police. ...when I was a public servant, we were checked by SSU and State Special Communications Service – they checked compliance with cybersecurity requirements. I personally was not checked, but there was a person - system administrator. But I do know about these inspections. Therefore, I think that the relevant authorities are working and now they have more work to do. However, whether a layman can contact them about the issues we have discussed and whether there will be a reaction to such an application is a whole other story." (Local self-government employee)

Chart 19. I will read several basic rules of cyber hygiene and you, please, specify to what extent you personally are aware of this rule. (% of responses by waves I and II respondents)
(A – 11-17 y.o. B – 18-25 y.o. C – 26-59 y.o. D – 60+ y.o.)

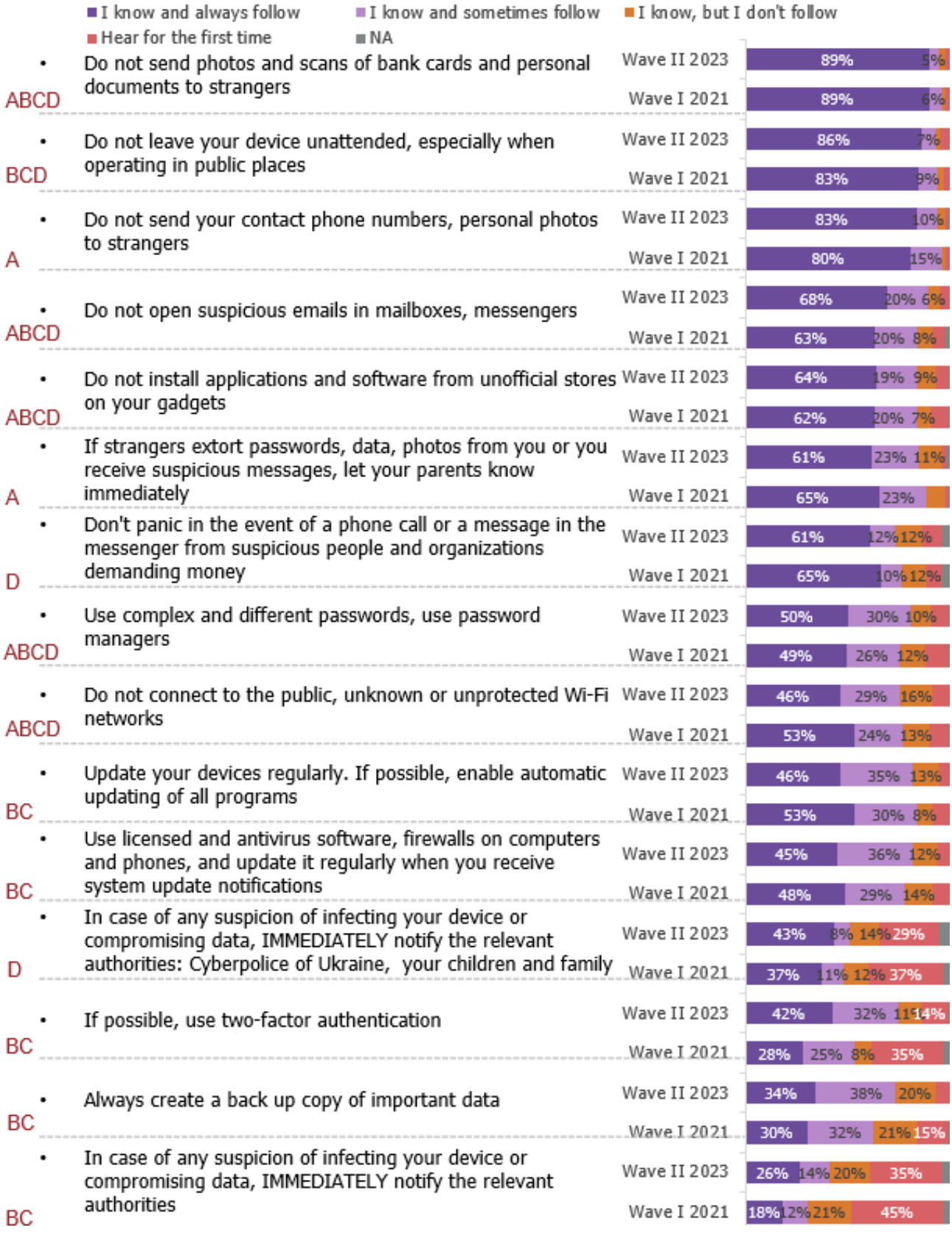
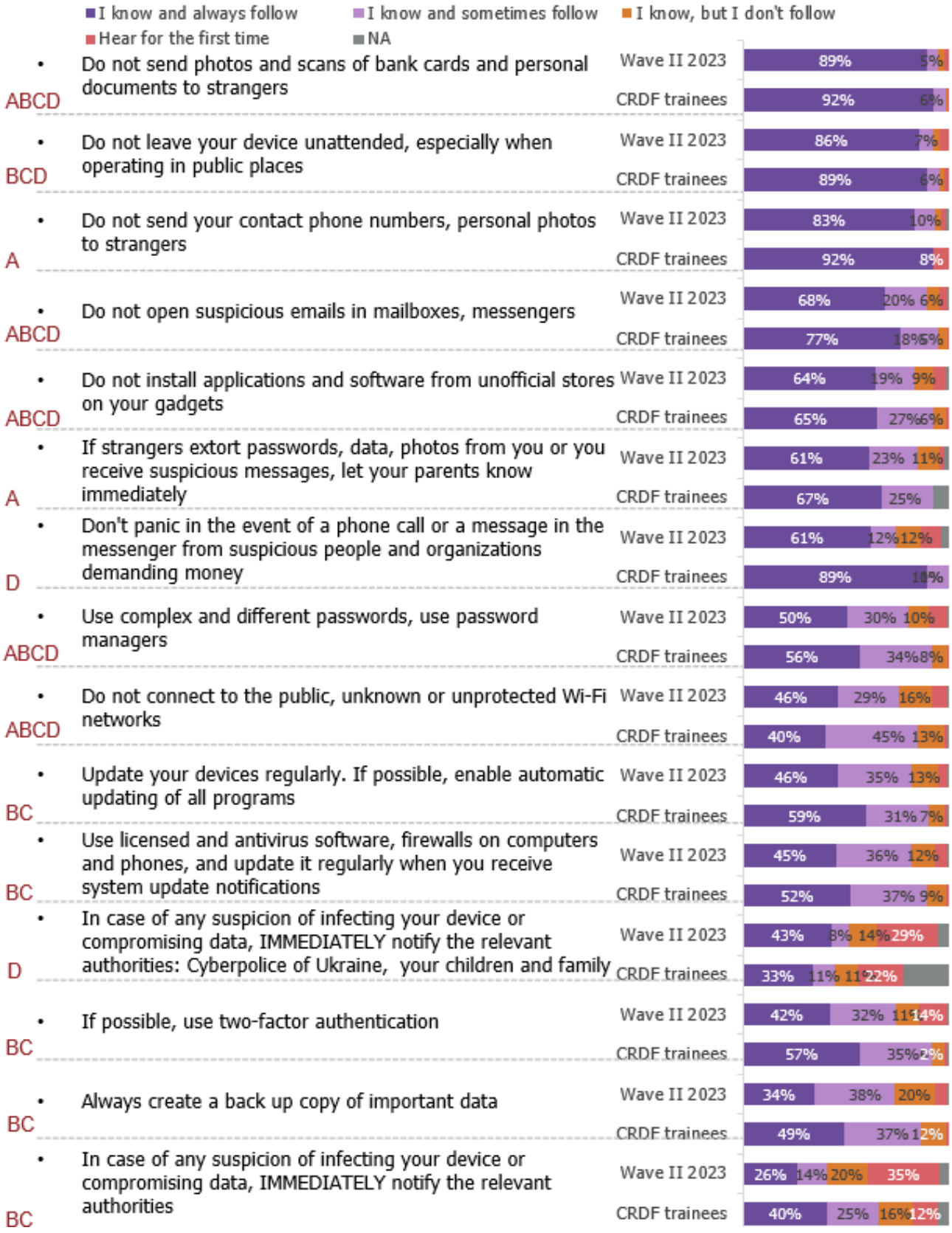


Chart 20. I will read several basic rules of cyber hygiene and you, please, specify to what extent you personally are aware of this rule. (% of responses by wave II respondents and CRDF Global course attendees)
(A – 11-17 y.o. B – 18-25 y.o. C – 26-59 y.o. D – 60+ y.o.)



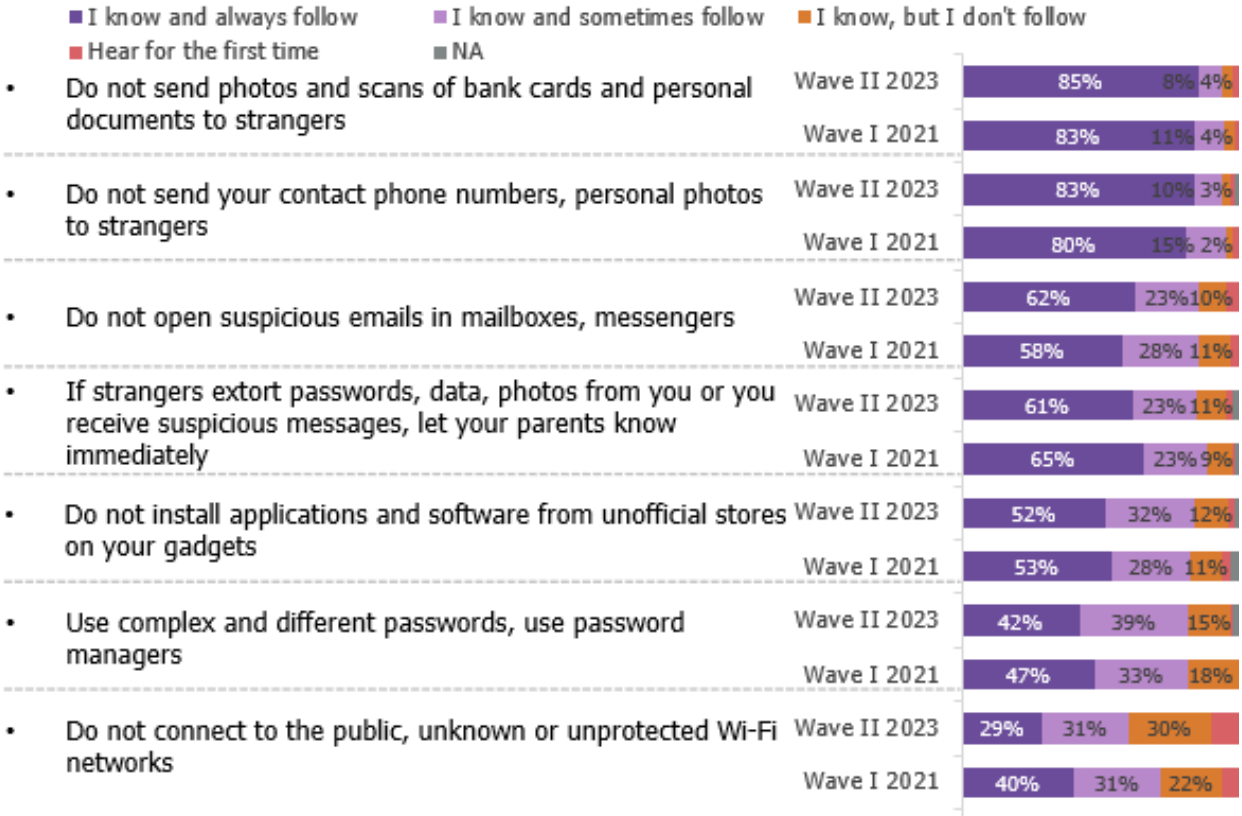
Teenagers know all the rules quite well. The share of this group respondents knowing every rule and always complying with them exceeds 50% for all rules, except for following two:

• Using complex and different passwords for registration on online resources, banking systems, etc. - 42% reported they know and follow the rules

• Don't connect to the public, unknown or unprotected Wi-Fi networks – 29% reported they know and follow the rules.

"It is very difficult for children and elderly people of my age to stop using the free services. Do you know the saying about the free cheese in the mousetrap? It is very common, even in our small town there are many opportunities to use the free VI-WI and people are using it without thinking about the risks." (Teacher)

Chart 21. I will read several basic rules of cyber hygiene and you, please, specify to what extent you personally are aware of this rule. Distribution by target groups - 11-17 y.o. (% of responses by wave I and II respondents)



Young people aged 18-25 are also quite aware of most of the proposed rules, although they have a slightly lower level of awareness of the six last-ranked rules than teenagers. The rule about the need to notify the relevant authorities about suspicion of infection or compromising data was not very familiar to respondents: 36% said it was the first time they heard about such a rule (for comparison: in the previous wave, this indicator was 42%). The second lowest awareness level was reported for the two-factor authentication rule, with 5% hearing about it for the first time (in the previous wave of study, this indicator was 15%).

Undoubtedly, young people aged 18-25 have become more aware and always follow the rule not to open suspicious letters in e-mail boxes and messengers; this is evidenced by indicator increase by 13 percentage points, up to 70% (see Chart 28).

"In the fall of 2021, I just entered the university. And then strange mails started to arrive to corporate email addresses of all the students - some kind of letter with some link. Some clicked on the link, and then something began to break. And then, after some time, and it all happened very quickly, a letter came from the administration with the request not to open unfamiliar letters because something had been hacked and defective letters were sent. And that's why you understand that you can't trust even the corporate mail. Although it could seem to be the safest resource." (Female student)

"...I was receiving emails with real abracadabra for a long time. Just some set of incomprehensible symbols, and they were coming literally every day. I couldn't throw them into spam because there were different sources. I don't understand at all what this was done for and who needed it. But there was such a case – I obviously have left my mails somewhere and someone decided to take advantage of it. But I never opened it anyway." (Female student)

91% of the respondents know the rule about using complex and different passwords quite well, but only 56% always follow it, which is 8 p.p. less than in the previous wave of study. However, this indicator is paradoxically higher when compared to that by CRDF Global course attendees of this age group (see Chart 29).

More than half of the young people aged 26-59 also know and always follow the rule about complex passwords. This indicator is higher for the sample in general than in wave I, but lower compared to CRDF Global course attendees' (see Chart 30) (see Chart 31).

Chart 22. I will read several basic rules of cyber hygiene and you, please, specify to what extent you personally are aware of this rule. Distribution by target groups - 18-25 y.o. (% of responses by wave I and II respondents)

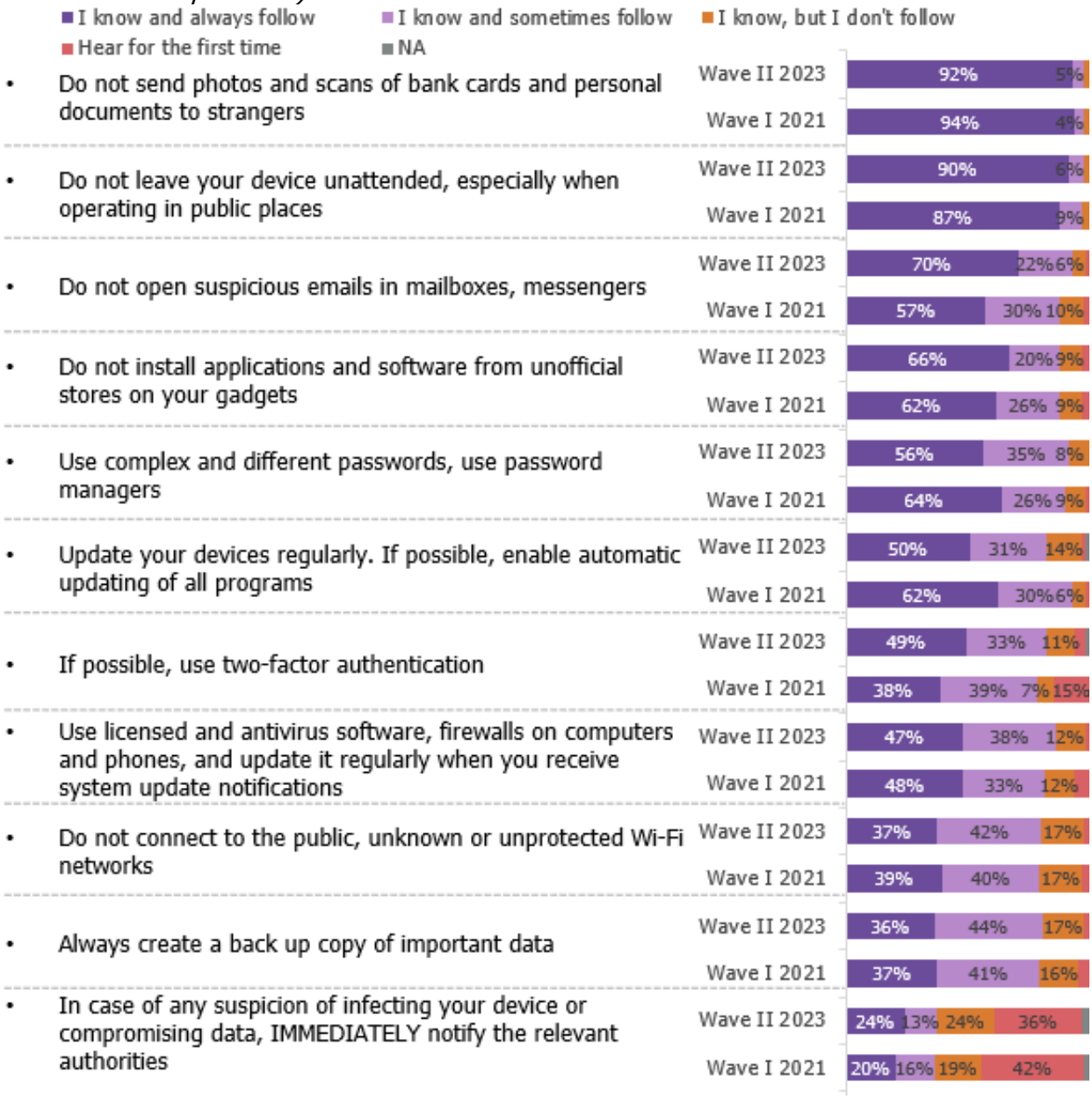


Chart 23. I will read several basic rules of cyber hygiene and you, please, specify to what extent you personally are aware of this rule. Distribution by target groups - 18-25 y.o. (% of responses by wave II respondents and CRDF Global course attendees)

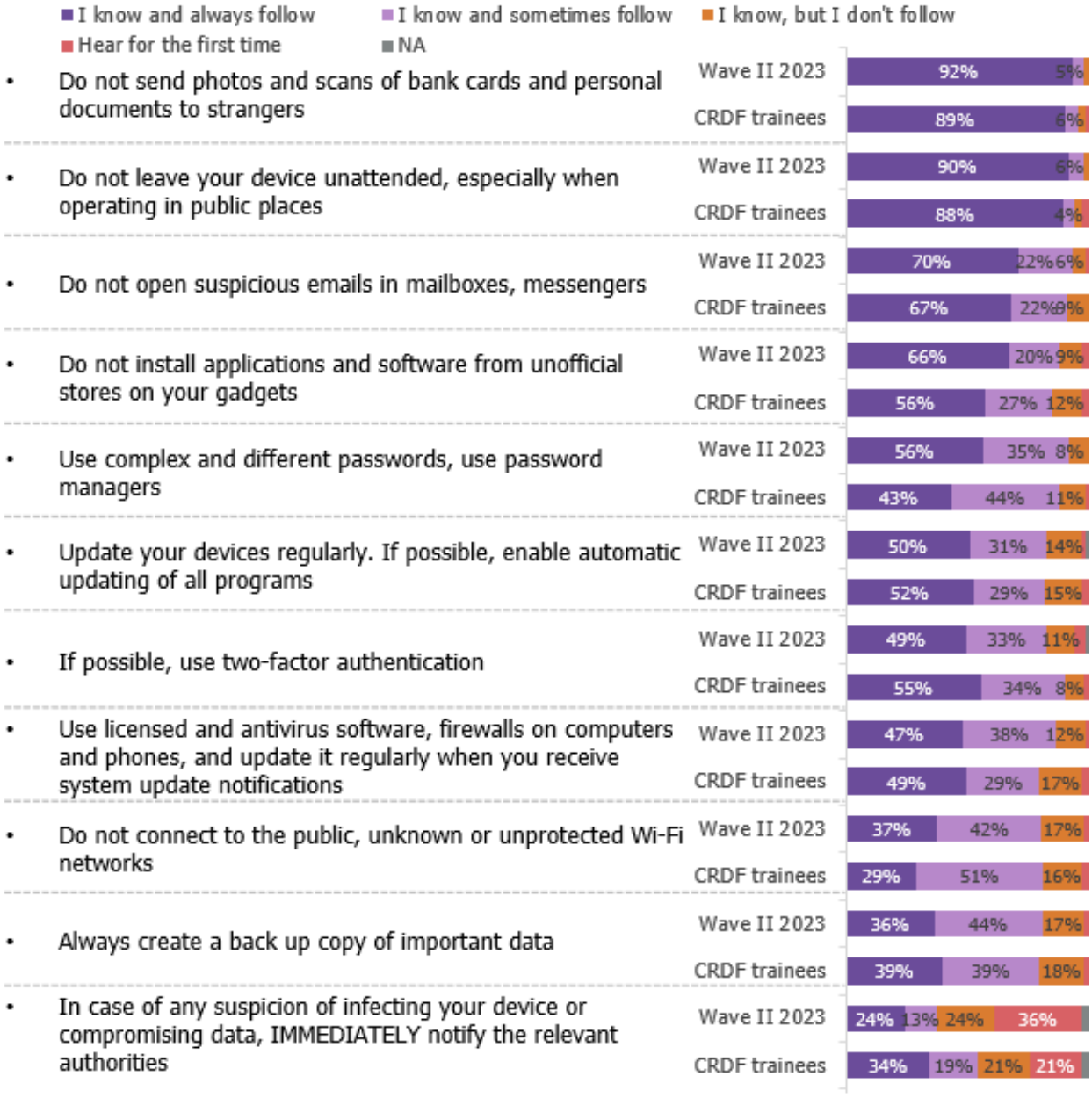
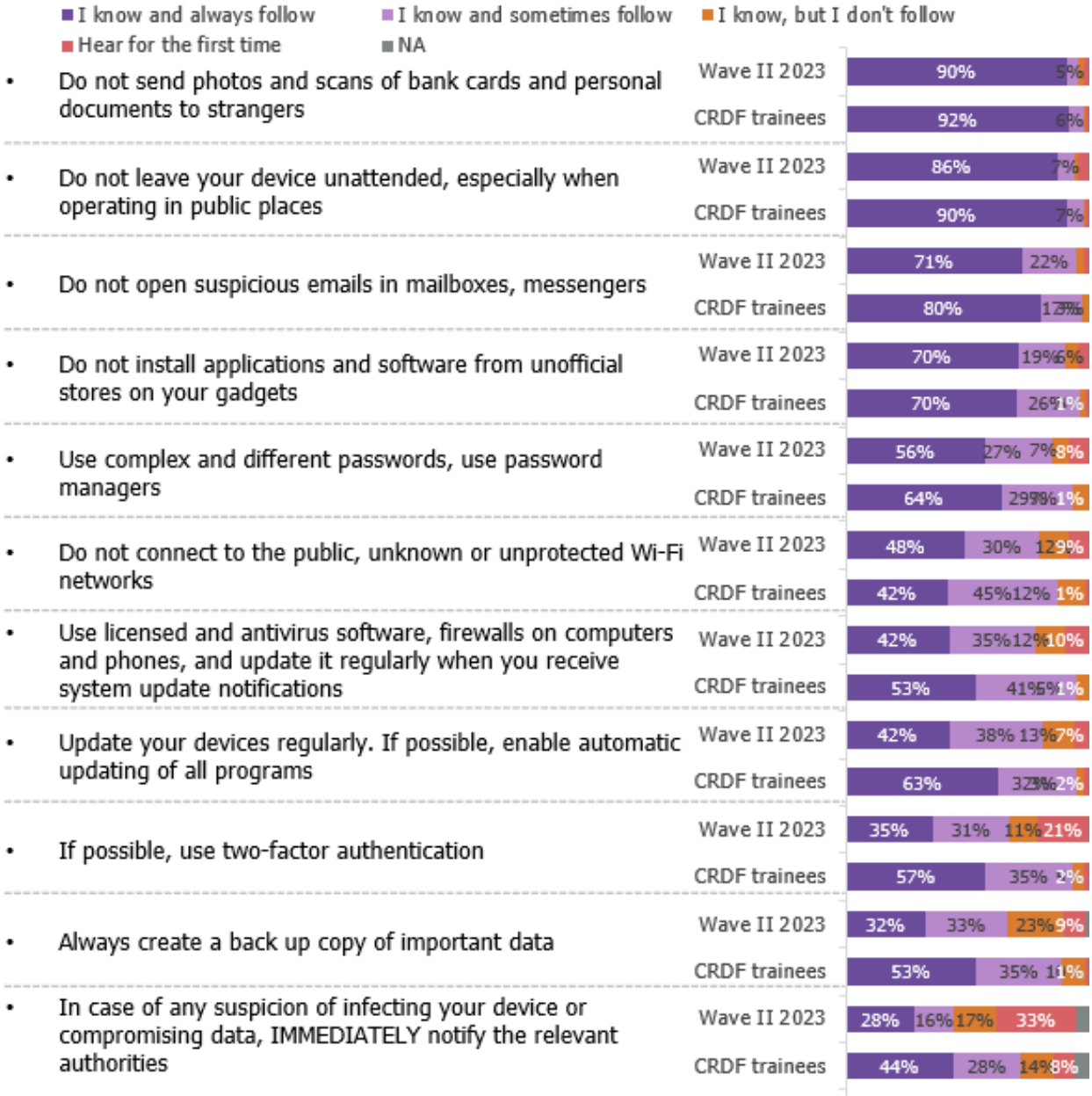


Chart 24. I will read several basic rules of cyber hygiene and you, please, specify to what extent you personally are aware of this rule. Distribution by target groups - 26-59 y.o. (% of responses by wave I and II respondents)

Chart 25. I will read several basic rules of cyber hygiene and you, please, specify to what extent you personally are aware of this rule. Distribution by target groups - 26-59 y.o. (% of responses by wave II respondents and CRDF Global course attendees)



The oldest respondents remain as attentive and cautious as ever. They are aware of the dangers of sending photos and scans of bank cards or documents to strangers (89% follow the rule not to do this), 79% do not leave the device unattended (see Chart 32).

However, the oldest respondents often (26%) do not even know about password safety rule, as evidenced by an increase in the share of the answer "hear it for the first time" and a decrease in the share of answers "I know and always follow" by 3 and 5 p.p. respectively.

Chart 26. I will read several basic rules of cyber hygiene and you, please, specify to what extent you personally are aware of this rule. Distribution by target groups – 60+ y.o. (% of responses by wave I and II respondents)

In order to compare how much each age group knows and follows a number of cybersecurity rules and how these indicators have changed over time, we have calculated several integral indicators:

- Know all cybersecurity rules;
- Follow all cybersecurity rules at least sometimes;
- Always follow all cybersecurity rules.

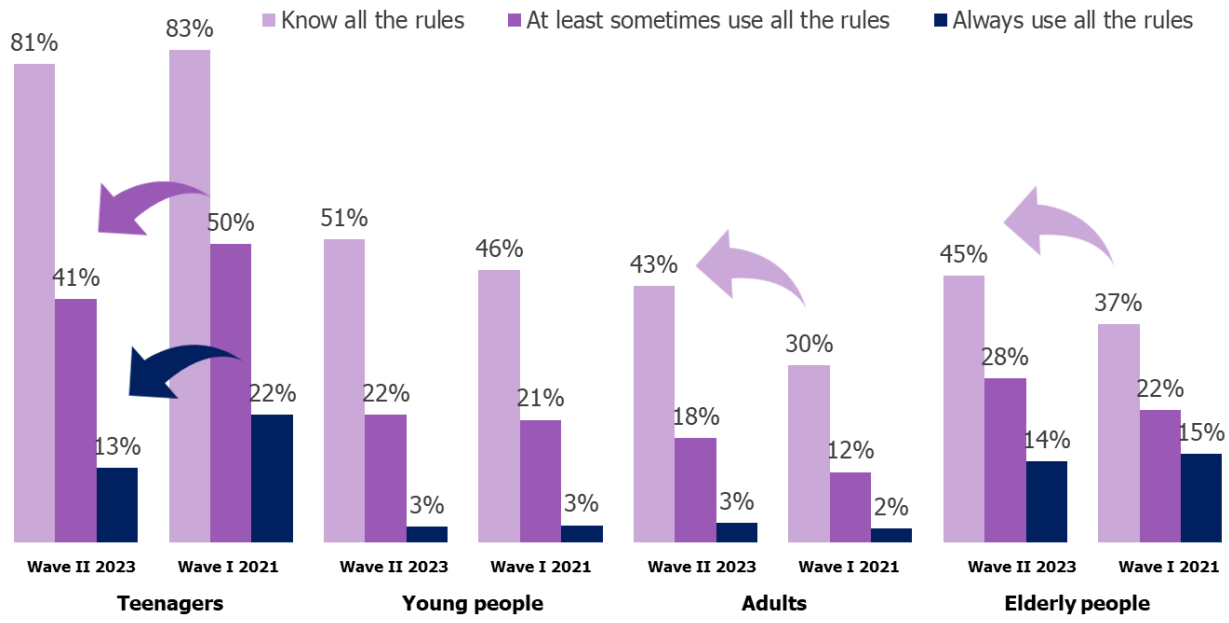
According to the results of the analysis of these integral indicators, teenagers aged 11-17 remain the group with the highest awareness level: 81% of them know all the rules of cybersecurity. However, only 41% follow all the rules at least sometimes, and only 13% always follow all the rules.

Moreover, as for the last two indicators, a noticeable decline of about 10 p.p. was recorded in comparison with the previous wave. Nevertheless, indicators of compliance with the rules in the group of teenagers remain the highest among the rest of target groups: among young people aged 18-25 years, 22% follow the rules at least sometimes, among adults aged 25-59 years – 18%, and among the oldest respondents aged 60+ years old – almost a third - 28%.

Among all age groups, a noticeable increase in cybersecurity rules knowledge is the most significant in the group of adults aged 26-59 (by 13 p.p.) and in the elderly aged 60+ (by 8 p.p). Indicator of following the rules has increased by 6 p.p. in both groups.

The oldest group of respondents remains the most responsible: the share of those who always follow all the rules is 14% (see Chart 33).

Chart 27. Knowledge and compliance with cybersecurity rules. Distribution by target groups (% of responses by wave I and II respondents)



Safety Behavior in Internet

For self-assessment of their own safety on the Internet, respondents were offered a 10-point scale where 1 means "very unsafe" and 10 means "completely safe." Based on this scale, the following behavior patterns were identified:

- Very unsafe (1-6)
- Moderately safe (7-8)
- Completely safe (9-10)

As for safety behavior on the Internet of the sample in general, it is possible to state that the level of its perception has remained almost unchanged (a slight decrease from 27% to 25% was recorded), while perception of one's behavior as moderately safe has increased by 12 p.p. - from 41% to 53%. The share of those regarding their behavior as completely unsafe is 20% (29% in wave I) (see Chart 34). There is significant difference in the assessment of one's safety behavior on the Internet among wave II respondents and *CRDF Global* course attendees (see Chart 35) (see Chart 37).

Chart 284. How safe is your Internet behavior in general? (% of responses by wave I and II respondents)

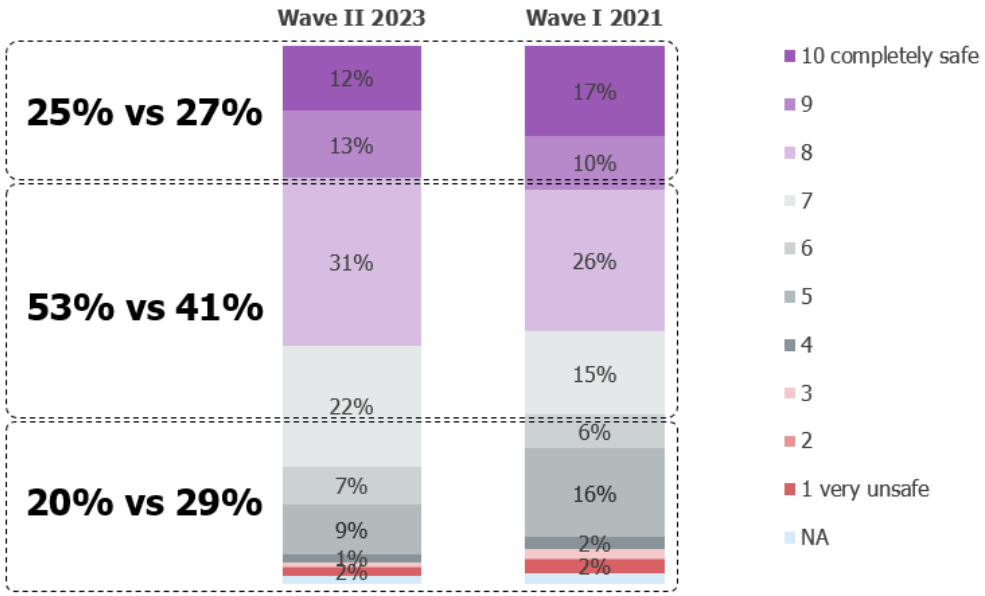
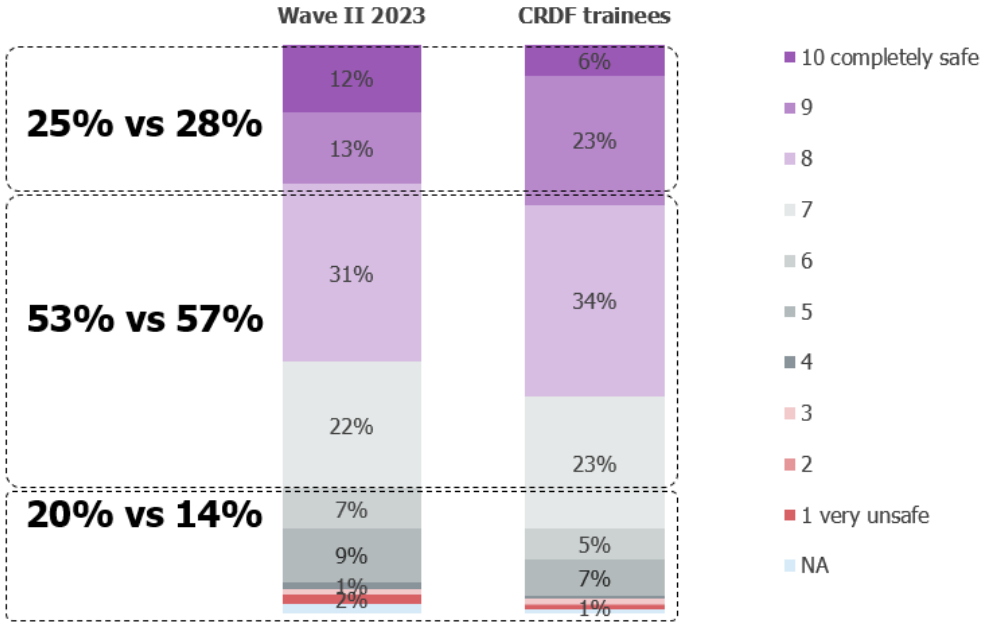


Chart 295. How safe is your Internet behavior in general? (% of responses by wave II respondents and CRDF Global course attendees)



Personal safety assessment varies significantly with age: for example, among teenagers (11-17 years old) and young people (18-25 years old) there are fewer of those who regard their behavior as unsafe (20% and 12% respectively), while in the group of respondents over 25 there are more of those considering their behavior on Internet unsafe.

The largest share of those regarding their behavior as completely safely (28%) is reported among teenagers, while in other age groups this share is, though insignificantly, but smaller.

In general, among young people under the age of 25, the share of those regarding their behavior as safe is greater than that of those considering it unsafe (see Chart 36).

Chart 306. How safe is your Internet behavior in general? Distribution by target groups (% of responses by wave I and II respondents)

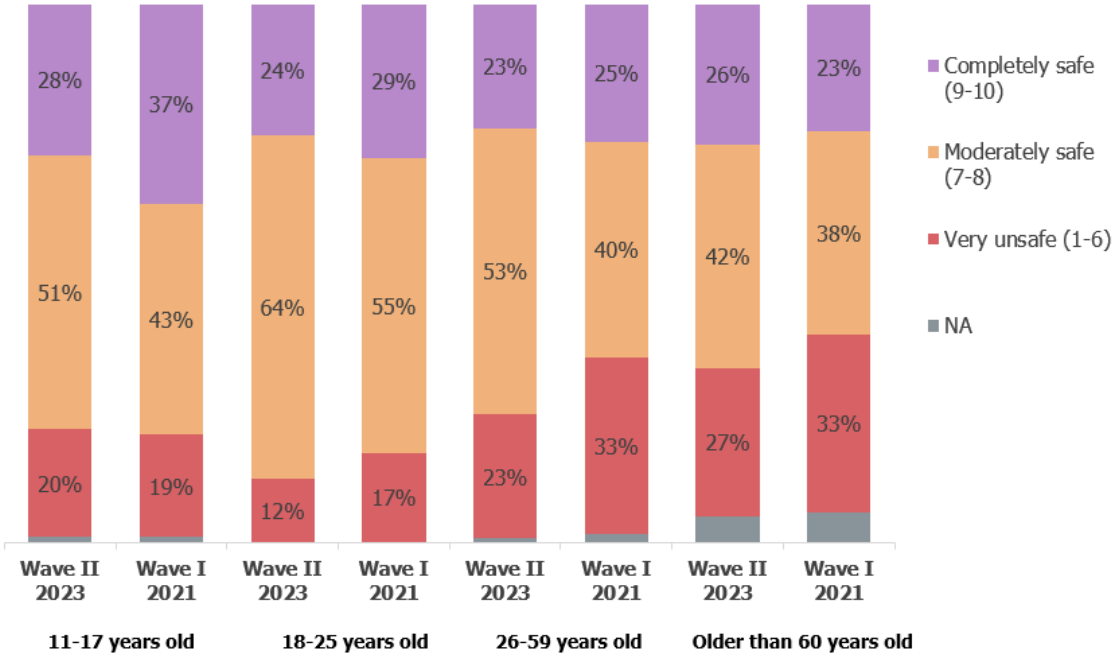
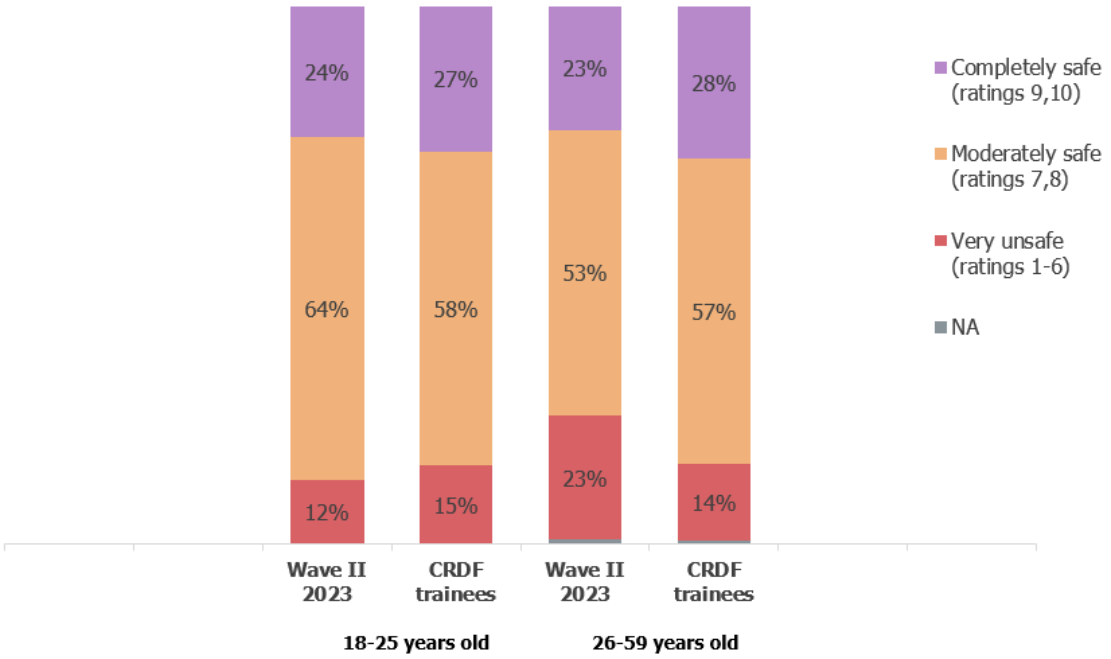


Chart 317. How safe is your Internet behavior in general? Distribution by target groups (% of responses by wave II respondents and CRDF Global course attendees)



Self-assessment of behavior on the Internet depends on knowledge and compliance with cybersecurity rules: the higher behavior safety evaluation is given, the better knowledge and more frequent compliance with cybersecurity rules is demonstrated. This correlation applies to all age groups.

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

The most elderly group (60+ years old) of respondents rating their behavior as safe, is the most conscientious group in terms of compliance with cybersecurity rules: if a person knows a rule, s/he strictly follows it.

However, the fact that partial compliance with some rules also gives a sense of security is also rather significative: this is especially noticeable in 18 – 59 group: among those who regard their behavior as completely safe, only 2% follow all the rules (see Chart 38).

CRDF Global training positively impacts on behavior safety assessment, increasing it, by an average, 1.5-2-fold (see Chart 39).

Chart 328. Knowledge of cybersecurity rules and compliance with them by the level of self-assessment of safety behavior on Internet.

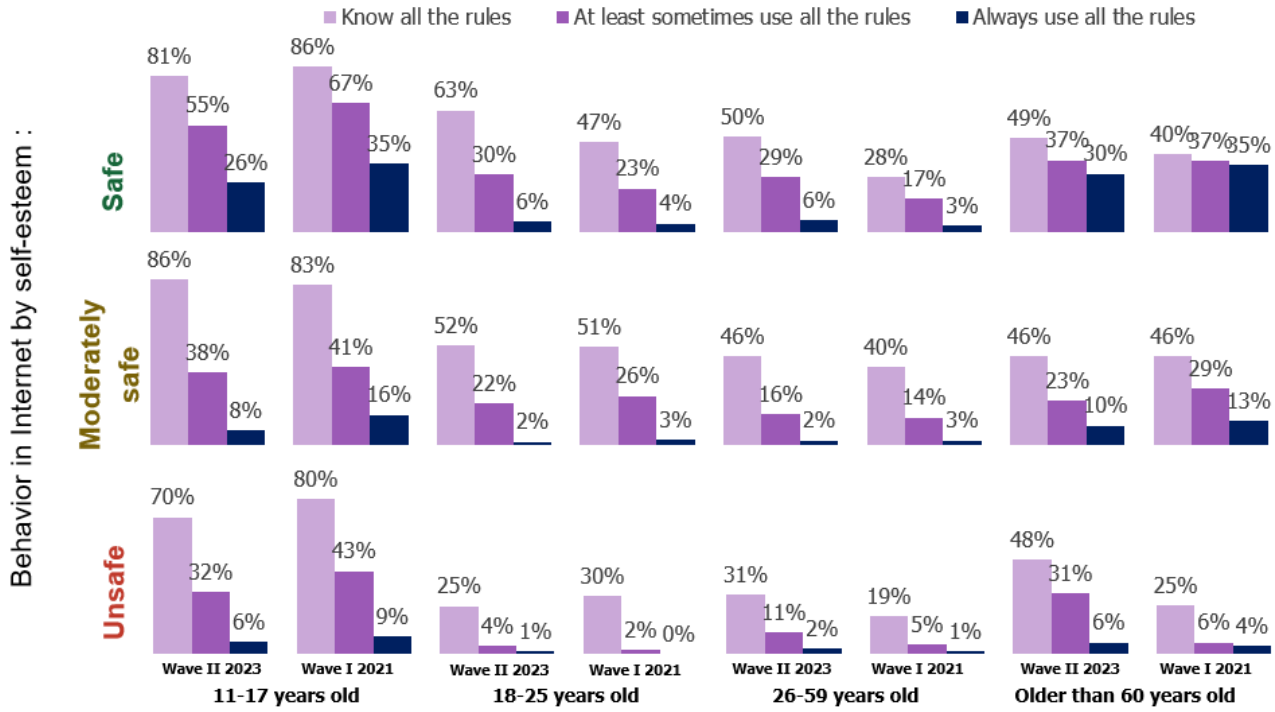
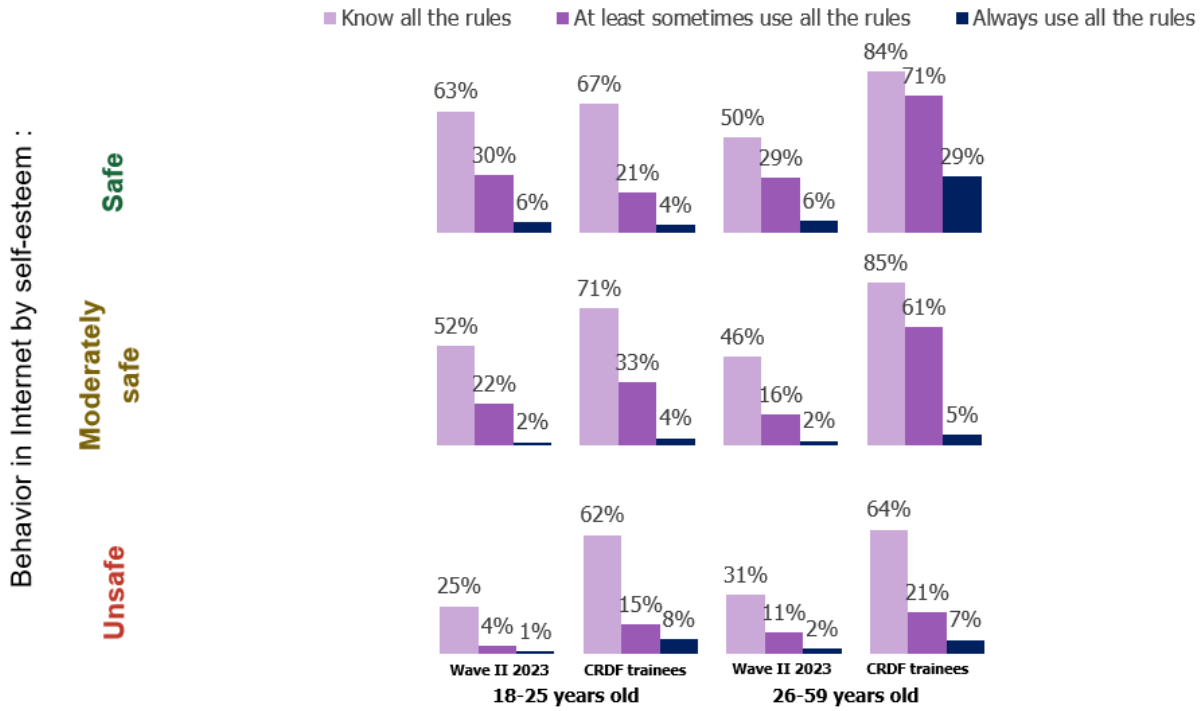


Chart 33. Knowledge of cybersecurity rules and compliance with them. Distribution by target groups (% of responses by wave II respondents and CRDF Global course attendees)



At the time of IDI and FGD, respondents fully agreed that knowledge of the rule does not mean compliance with it. Sometimes violations occur due to the lack of attention, sometimes - due to lack of time, certain mistakes can be made automatically when a person is busy with several things at the same time or tired. Respondents mostly rated safety of their behavior on the Internet, on an average, at 6-8 points out of 10.

For the most part, IDI and FGD respondents openly indicated that they are aware of the danger of a certain behavior when certain rules are not followed, such as use of licensed programs, antivirus, creation of complex and not the same passwords for different accounts, use of two-factor authentication, etc.

"I had a case when I opened a letter from an unfamiliar mail simply automatically. In the same way, someone can ask for data in a messenger, and you can send a photo of a card - there are cases when a person does not think because of being tired or inattentive. It can happen to me."
(Female student)

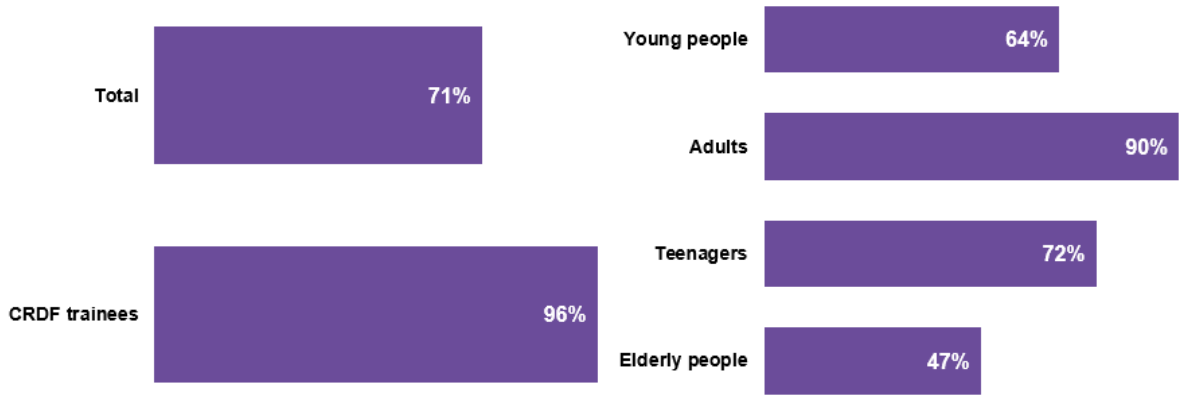
Ability to detect risky situations

The ability to clearly detect risky situations is an important factor for Internet security improving. Without such skills, a person can either consider Internet to be a completely safe place and ignore safety rules, or, on the contrary, believe that danger awaits everywhere and that there is no protection.

In order to assess how well the respondents are capable of detection of risky situations, they were offered ten projective situations, five of which, according to *CRDF Global* experts, are safe and five are unsafe. The indicator of the ability to detect risky situations is the proportion of respondents capable of correct distinguishing between five or more situations (in other words, correct detection of unsafe and safe situations).

The results of the analysis are shown in Chart 40.

Chart 40. Ability to detect risky situations (share of respondents who succeeded to detect 5 and more situations)



The best results were demonstrated by a group "youth" respondents (18-25 years old), as well CRDF Global course attendees - more than 90% of these respondents have correctly identified more than 5 situations (it should be pointed out that the share of the respondents who have correctly identified all 10 situations is 1,5% among CRDF Global course attendees, and close to 0 for other age groups).

Elderly people (47%) and, unexpectedly, teenagers (64%) have demonstrated the worst ability to detect risky situations. At the same time, it is quite typical for all the groups to mark as "risky" those situations which are, in fact, safe.

Extortion money from an "alleged" friend on social networks is the best detectable situation by all the groups of respondents - it was detected as risky by the largest share of the respondents - 88% among teenagers and from 90% among all groups of the respondents over 18 years old (See Charts 41-44).

Respondents of all age groups believe that reading emails that end up in spam can be risky for older people, although simply reading such emails does not carry any risk. 68% of teenagers and young people, as well as more than 75% of the respondents aged 26-59 and over 60, mistakenly regard this situation as risky.

Among the situations that are also mistakenly classified as unsafe, there is also a situation when a person forgets complex passwords. A significant proportion of the respondents from all age groups believe that recovering passwords poses a risk: 58% of teenagers, 40% of young people under 25, 47% of adults aged 26-59 and 66% of elderly respondents are of this opinion.

On the contrary, connection to public Wi-Fi networks for carrying out bank operations, is the "leader" among unsafe situations that are mistakenly regarded as safe. 54% of teenagers, 44% of young people, 55% of adults and 35% of elderly people do not see any danger in it.

Also, a significant share of the respondents mistakenly regards the use of VPNs and automatic application updates as dangerous. The share of the respondents considering VPN use dangerous varies from 32% among teenagers to 52% among adults.

Automatic update of applications on a smartphone is regarded as risky behavior by about a third of teenagers and young people and about half of adults and elderly respondents.

Also worthy of attention is the situation when two-factor authentication does not work, for example, SMS messages do not arrive due to bad connection. While the majority of the respondents consider opting out two-factor authentication for these reasons to be risky behavior, a significant share of respondents (from a quarter to a third) believe that opting out two-factor authentication is a normal practice when connection is bad.

CRDF Global course attendees demonstrated a better ability to distinguish between risky and safe situations (Chart 45). They are the only group that has considered situations in general more dangerous than safe situations. However, even these respondents, for the most part (83%), believe that grandmothers' reading e-mail spam is risky, therefor this situation can become a subject for discussion.

Chart 41. Detection of risky situations. Distribution by target group - 11-17 years old (% of responses)

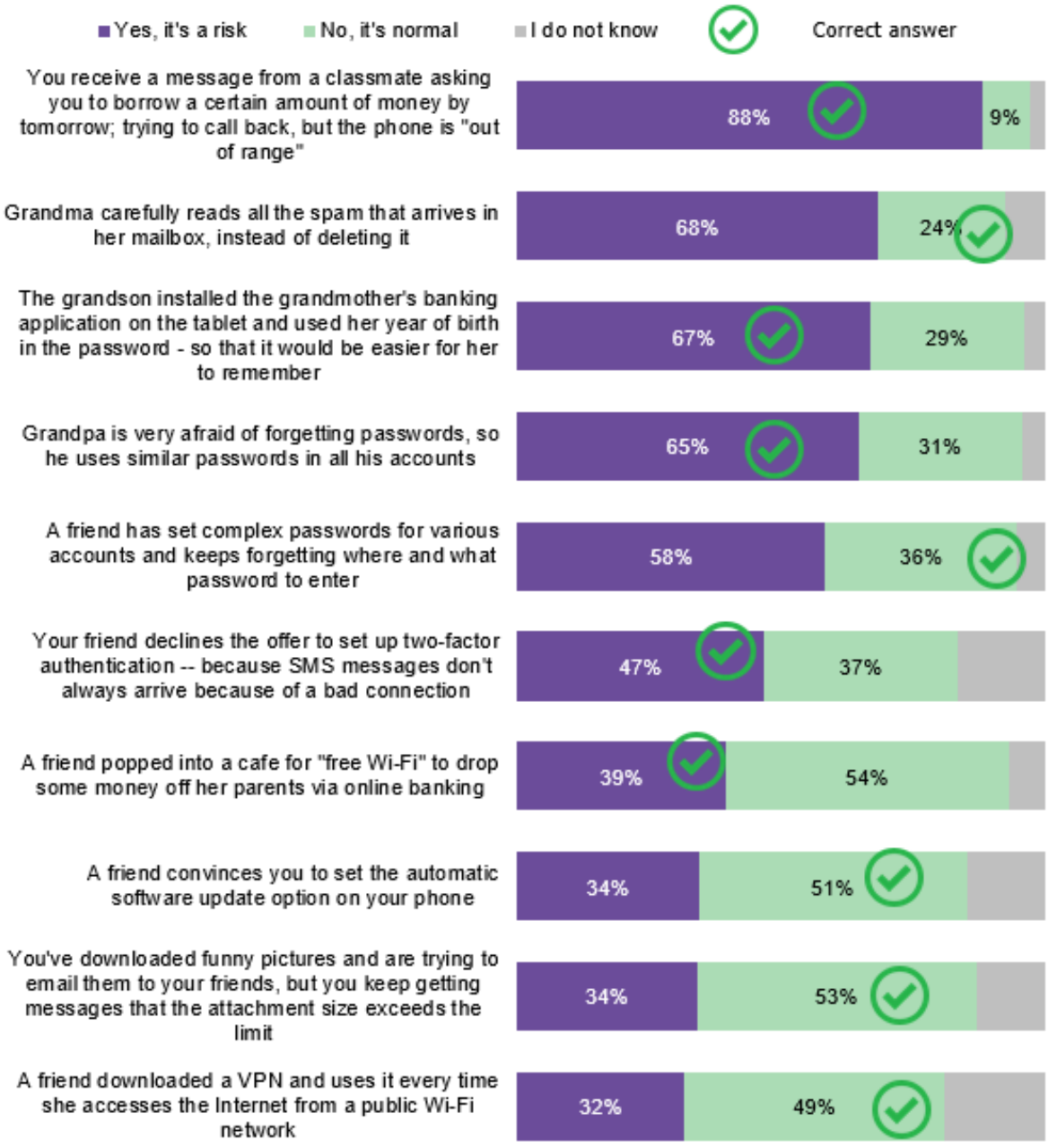


Chart 42. Detection of risky situations. Distribution by target group - 18-25 years old (% of responses)

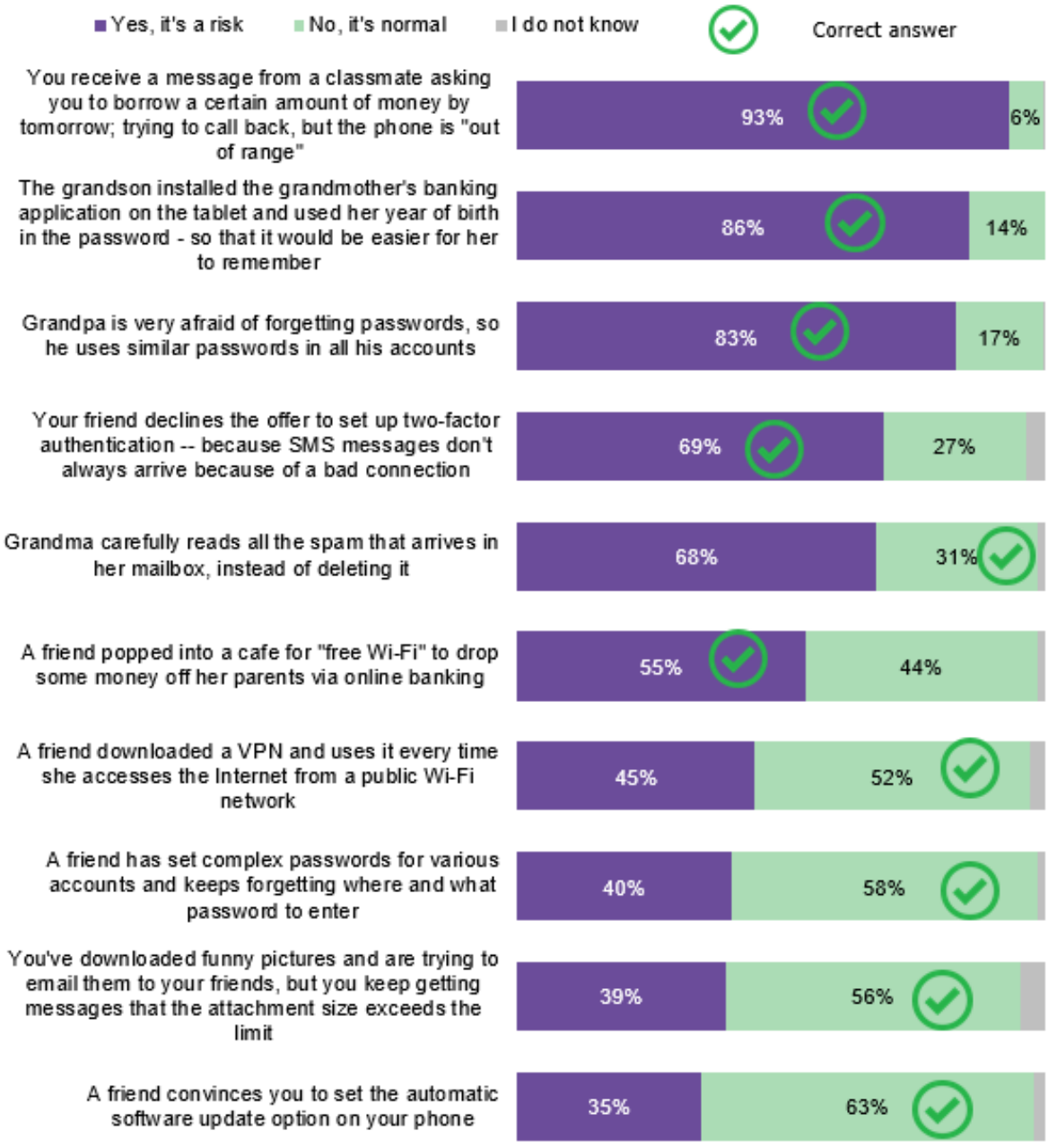


Chart 43. Detection of risky situations. Distribution by target group - 26-59 years old (% of responses)

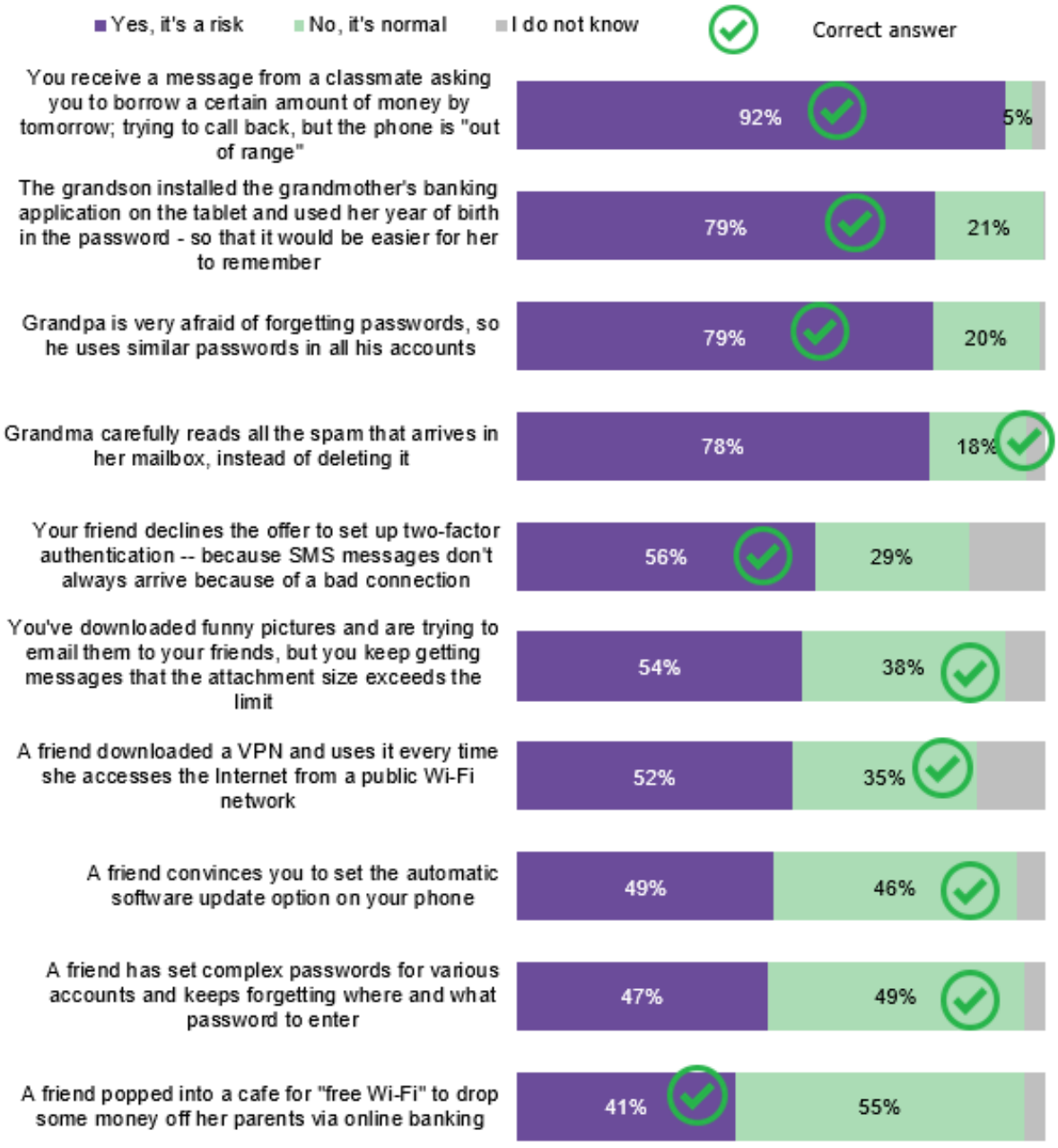


Chart 44. Detection of risky situations. Distribution by target group – 60+ years old (% of responses)

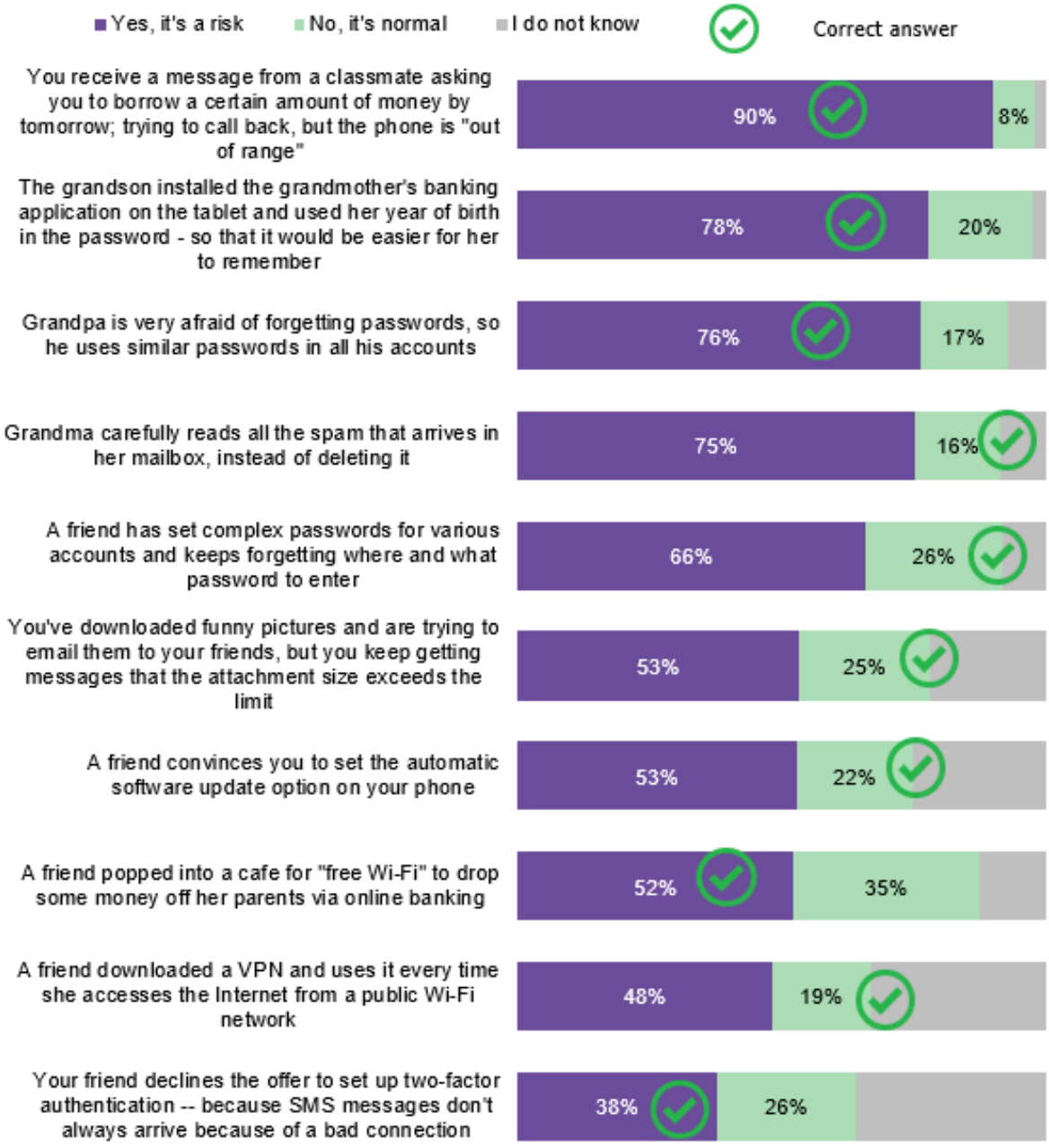
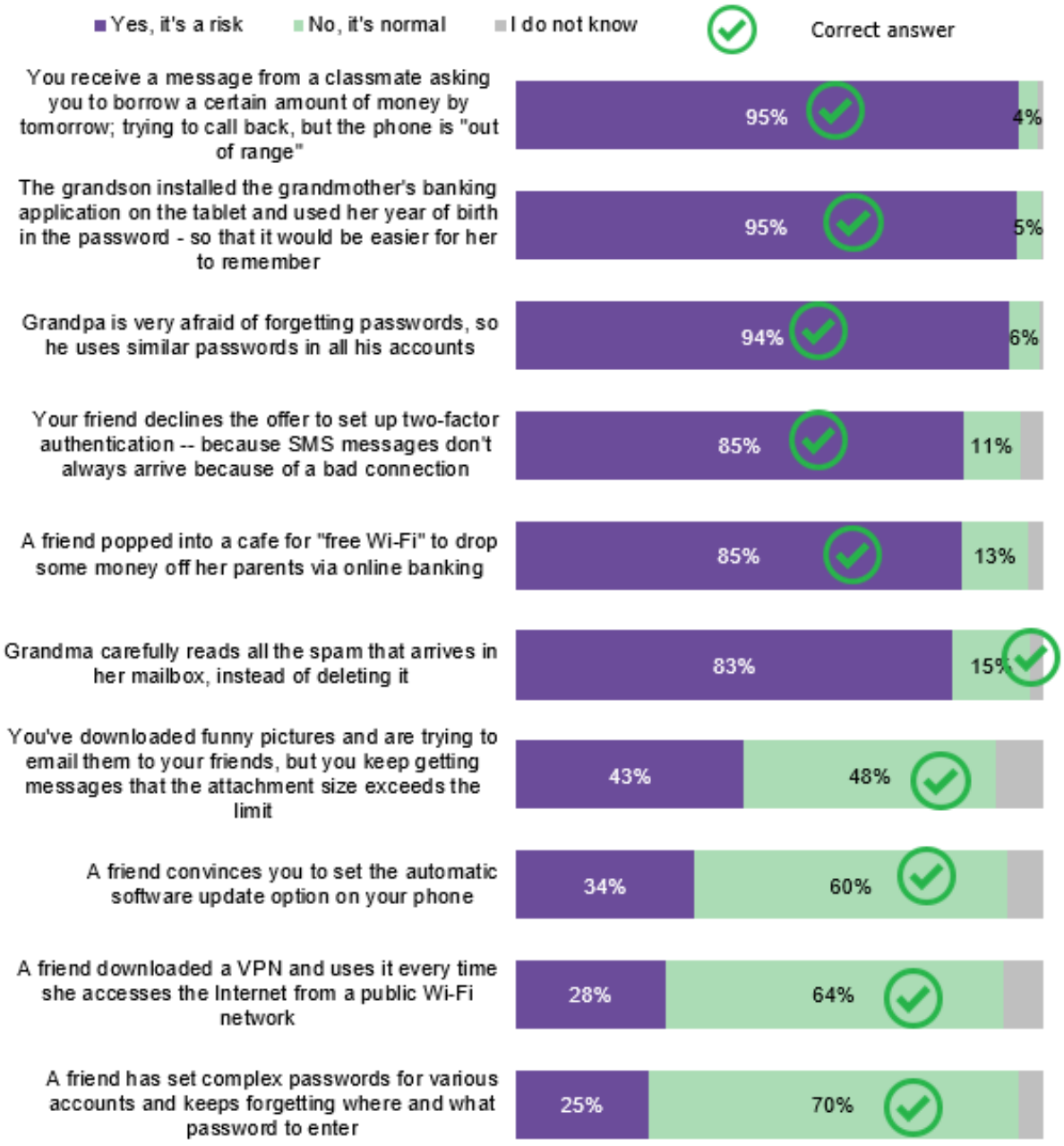


Chart 45. Detection of risky situations. Distribution by target group – CRDF Global course attendees (% of responses)



Reviews about *CRDF Global*

During FGD and IDI, the respondents were asked about their impression about the course. Some of the respondents attended the course several years ago, so they could not provide much details. At the same time, not all the respondents were able to recall which course it was about, as they have attended several similar courses; not all the respondents were able to recognized CRDF Global name and logo.

"I also attended it, but long time ago, several years ago. I don't remember much of it now. But visually I remember, I recall that it was easy to perceive this information and easy to answer questions. That is, I didn't have any objections at that time and I don't have them now either." (Female student)

Teachers, representatives of public sector and local self-government authorities who have attended it offline could, of course, recall more. For teachers, the course is more recognizable as they motivate children to attend cybersecurity trainings for school students and get certified. Also, teachers regularly work with course materials that are convenient for teaching their students. Teachers say that the materials are well structured, uncomplicated, presented in a clear way, have good design and animation. According to teachers, even children who are skeptical of the program at the beginning, later become enthusiastic about the learning process.

In all target groups, respondents said that they occasionally attend cybersecurity courses and search for information on the Internet. In particular, public officials are obliged to undergo cybersecurity trainings on regular basis. Respondents mentioned digital literacy course from the Ministry of Digital Transformation, students also have cybersecurity courses in their educational institutions, younger participants recall cybersecurity lessons at school.

"...in November of last year, there was a workshop on cybersecurity for the employees of public and self-government authorities. Throughout the day, we talked about cybersecurity. Then I attended the course for the employees of public authorities mentioned today. And I also started, but haven't yet completed, the course on cybersecurity basics from the company "Cisco" – a free one on Skill School platform. Also, there is a course called "Attention! Cyber Scammers" on Diya Education platform. It is like a short educational sitcom, and I completed it too. (Educational sector employee, Teacher)

"The Ministry of Education offers NUS [New Ukrainian School] in Computer Science or a general course of Computer Science. …and it contains a lot of materials on cybersecurity. There are also courses for teachers, when workshops on Computer Science are prepared." (Teacher)

According to the respondents, there is a lot of information on cybersecurity on the Internet now. After all, the topic is extremely relevant: scammers are creative, so regular monitoring of new threats and security rules is necessary. Because of this, authors of the materials or course organizers are not always remembered.

Respondents who remembered the course well and could identify the organizers had the best impressions about the content, speakers, data presentation and visual design. No significant comments regarding the course improvement were given by the attendees. Specialists expressed the desire for more offline courses because online information is not perceived so deeply and with

such attention. One IT specialist from the local self-government authority commented that the course, as it seemed to him, was designed for non-specialists, so information was somewhat general, but still interesting.

"I liked data presentation and its being visual and very close. Video characters were showing what shouldn't be done. And these characters were, like, about the same age as us. It was easy to memorize." (Female student)

"...it wasn't just a hard-to-understand text or the one you don't want to read at all. It was very easy to understand. There was some kind of interactivity, and this kind of presentation makes it easier to understand and you also have a desire to understand it." (Student)

"The presentation itself is very cool. I, unfortunately, have to read a lot of text. And such visual design is at least easily perceived. The information is presented in such a way that it is easy to memorize. And the most important aspects and general rules are highlighted. It is not difficult to simply follow them. And they are presented in a very interesting format. Therefore, visual design plays a very important role. Besides, if it is compared with the video, then it is just fascinating. Because it is not necessary to concentrate at reading the course text, but, for example, watch and perceive such information while having tea or coffee. So, it's very, very cool." (Female student)

"Actually, courses help to structure information. And my impression is that this course is designed for a bit older people. Well, at the beginning the process was very slow. I wished it to be faster, more intensively, to be more precise. And I know this, and too many details are provided about that. But in general, the course was very useful." (Local self-government authority employee)

Recommendations for cybersecurity knowledge improvement for different TGs

The respondents regard cybersecurity as a very topical issue, therefore any information campaigns in mass media, social advertising on the Internet and in mass media, as well as outdoor advertising, TV programs about possible scams and security rules would be relevant. Less digitally literate elderly people aged 50+ are more vulnerable. Children are more careless, but they are continuously receiving information about risks and rules at school, therefore they are less vulnerable as compared to the above group.

"As for adults, it is possible, for example, to provide information on news channels, the ones they are watching now, or on the Internet where they are looking for the news; experts can describe certain facts, provide certain recommendations about the rules of Internet use. And as for younger audience, in my opinion, it would be interesting for them to take part in some quests on the subject of cybersecurity, information security, information hygiene. ... some animation formats." (Female student)

In their own opinion, students have sufficient knowledge in the field of cybersecurity and have no significant problems with access to information. However, knowledge must be continuously

maintained and updated and, among other things, it is necessary to be disciplined enough to follow all the rules and recommendations. According to the respondents, courses like those offered by CRDF Global help to refresh knowledge and help to form the necessary motivation to comply with safety rules. Therefore, regular training and self-education are necessary, and any educational opportunities are openly and gladly accepted by the respondents, especially if the content is interesting and creative.

"Knowledge must be updated, this is a very dynamic field, and there are many new risks, while the rules could be forgotten. Therefore, new courses are useful, and it is necessary to study all the time. And it's great if a course is presented in an easy, interesting and pleasant format" (Student)

Employees of local self-government authorities, public sector and public officers pointed out that outdated equipment, retirement age and low digital literacy of specialists, use of unlicensed software are a significant problem. Most often, there are no funds for solving these problems, and, at least until the end of the war, there will be no significant changes. There are small rural and urban communities where budgets have never been large, therefore there are no funds for equipment and data protection. Quite often, the communities do not even have professionals performing the role of system administrators - everything is handled by either the head of the community or his/her deputy, who are not professionals. According to the respondents, situation with equipment and software might somewhat change with assistance of Western partners, donors and grant funds.

"We are discussing problems with the professionals, and at the moment neither local budgets nor central budget suffices for systemic solutions to the problems of digital threats in the public sector. So far, we are operating in such conditions - far from the ideal. This problem can be partially solved with the help of grants, therefore assistance is necessary not only in the field of education and specialists' digital literacy buildup, but also in solving problems with equipment and software. (Local self-government employee)

There is a need to increase digital literacy level of public sector specialists, thus trainings must be mandatory and certificates - registered. It would be great to offer some kind of a reward or motivation for taking the course, or at least allow an employee to undergo training during working hours, which is also a motivation. If training takes place outside of working hours, it is more likely to be not highly effective.

"Employees do not always have an opportunity to find time for studies, therefore special timing for this is needed, preferably during work hours. An employee is to receive a personal certificate upon training completion, participation is to be mandatory and there should be certain motivation to take part in this. Offline format of trainings offers more advantages." (Local self-government employee)

The teachers' problem is that although children are aware about the risks and safety rules, they can ignore them. However, the teachers are optimistic and they believe that during school study time the topic of cybersecurity is constantly discussed in various classes, therefore the children do have basic knowledge. The effect of educational programs like *CDRF Global* ones is positive and teachers welcome any initiatives creating an interesting educational content, and the most attractive is game content in the form of quests, computer games or simulations. Content for senior students is needed more, while more interesting content for younger children is available. Visits of cyber police

professionals to schools and their explanations about the main risks in the field of cybersecurity, cyber hygiene rules, as well as about the specifics of work of professionals of specialized law enforcement agencies would be very useful.

"... cool idea about games and quests. Quests are about life, but someone is needed to design them. And a game can be designed for a phone or a tablet, because all parents give their children a phone or a tablet from an early age." (Student)

"We need practical things. There should be some platforms designed so that children, students and others - the younger generation - could test them and see what ignoring cybersecurity might result in. So that there are such programs, platforms, a virtual computer. When a person ignores certain cybersecurity rules, what danger can this person face? So, the programs should simulate a trouble a person can get into. ... to introduce fundamental platforms, software products, simulators. I do understand that this project is quite costly, but this should be done at the state level and such good projects are needed. It's not simply publishing a textbook; it will be more expensive. But it should be completed – fully implemented in life. So that the children have the opportunity to learn about modern problems on modern platforms. Systemically, not occasionally... As far as the ministry is concerned. The Ministry is a certain state structure that, since it is entrusted with education and science tasks, must coordinate this thing. Of course, by investing and bringing into its circle all these structures, both private and public, that are doing this at the professional level. Perhaps such global projects should be handled by the organization we have discussed." (Teacher)

IV Appendix 1. Questionnaire

Questionnaire for the Interview

Greeting

Good afternoon, CRDF Global Representative Office in Ukraine is conducting a survey of our educational program attendees about Internet behavior safety. Your answers shell be kept strictly confidential, we will not ask about your passwords or websites you are visiting. The survey will last 20 minutes and we will be happy if you are able to answer our questions.

Respondent's Choice

S1. Please, tell your age in years

Note _____ and encode

0	> 10 y.o.	END
1	11-17 y.o.	
2	18-25 y.o.	
3	26-59 y.o.	
4	60+ y.o.	
5	Refusal	END

S2. **Your sex** *One answer only*

1	Male	
2	Female	

S3. How often do you use Internet, for example, visit websites, social networks, use applications, messengers? One answer only

1	I spend on the Internet most of the day	
2	Several sessions per day, but not most of the day	
3	1-2 sessions daily	
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 Internet at all	END
99	Hard to say	END

MAIN Questionnaire

A1. 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

A2. Some types of behavior on the Internet can be risky and lead to negative consequences. I'll read out different situations that other people find themselves in, and you tell me whether you think that situation is risky or normal:

Programmer, random order of statements!	**Yes, it's a risk**	**No, it's normal**	**I do not know**
The grandson installed the grandmother's banking application on the tablet and used her year of birth in the password - so that it would be easier for her to remember	1	2	99
Your friend declines the offer to set up two-factor authentication -- because SMS messages don't always arrive because of a bad connection	1	2	99
A friend popped into a cafe for "free Wi-Fi" to drop some money off her parents via online banking	1	2	99
You receive a message from a classmate asking you to borrow a certain amount of money by tomorrow; trying to call back, but the phone is "out of range"	1	2	99
Grandpa is very afraid of forgetting passwords, so he uses similar passwords in all his accounts	1	2	99
A friend convinces you to set the automatic software update option on your phone	1	2	99
A friend downloaded a VPN and uses it every time she accesses the Internet from a public Wi-Fi network	1	2	99
Grandma carefully reads all the spam that arrives in her mailbox, instead of deleting it	1	2	99

A friend has set complex passwords for various accounts and keeps forgetting where and what password to enter	1	2	99
You've downloaded funny pictures and are trying to email them to your friends, but you keep getting messages that the attachment size exceeds the limit	1	2	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 per line.

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.Я зачитаю списки основних загроз, які можуть спіткати користувача інтернету, а ви скажіть, чи стикалися ви особисто або ваші знайомі з такою ситуацією?

Multiple answers.

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 acquaintances	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. 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".

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	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

A6.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

DEMOGRAPHICS

D1. Please, specify your main occupation. *One answer only*

1	Employee
2	Registered private entrepreneur
3	Self-employed
4	Student
5	Housewife
6	Retired
7	Temporarily unemployed, but looking for a job
98	Other

D2. [If D1= 1] Where exactly are you studying? *One answer only*

1	School
2	Vocational school
3	College
4	Higher educational institution
98	Other

D3. What is your educational level? *One answer only*

1	No elementary education
2	Elementary education
3	Basic secondary education
4	Full secondary education
5	Secondary professional education
5	Incomplete/undergraduate higher education
6	Higher education, Bachelor's Degree
7	Higher education, Master's Degree
99	Hard to answer

D4. What can you tell about your family's financial status? *Read, only answer only*

1	Have to save on food
2	Need to save or borrow in order to purchase clothes and shoes
3	Need to save or borrow in order to purchase such items as a nice suite, cell phone etc.
4	Need to save or borrow in order to buy expensive goods
5	Need to save or borrow in order to buy a car or an apartment
5	Capable of buying whatever is necessary anytime
99	Hard to answer

These are all the questions.

Thank the respondent for participation in the survey!

V Appendix 2. Respondent's Portrait

		TOTAL		TOTAL		Respondent's Age							
						11-17 y.o.				18-25 y.o.			
		Wave 2, 2023		Wave 1, 2021		Wave 2, 2023		Wave 1, 2021		Wave 2, 2023		Wave 1, 2021	
		Count	Col%	Count	Col%	Count	Col%	Count	Col%	Count	Col%	Count	Col%
Sex	Male	685	47.40%	570	47.47%	162	51.38%	154	51.38%	201	51.55%	159	52.94%
	Female	760	52.60%	630	52.53%	153	48.62%	146	48.62%	189	48.45%	141	47.06%
	TOTAL	1445	100.00%	1200	100.00%	315	100.00%	300	100.00%	390	100.00%	300	100.00%
Region	Kyiv	116	8.03%	98	8.20%	27	8.45%	22	7.42%	31	7.95%	24	8.00%
	North	243	16.82%	162	13.46%	94	29.95%	38	12.78%	49	12.56%	39	13.00%
	West	313	21.66%	295	24.55%	32	10.01%	84	27.89%	110	28.21%	83	27.67%
	Center	325	22.49%	290	24.14%	45	14.18%	73	24.37%	92	23.59%	71	23.67%
	South	246	17.02%	206	17.19%	63	20.15%	49	16.34%	61	15.64%	50	16.67%
	East	202	13.98%	149	12.45%	54	17.27%	34	11.19%	47	12.05%	33	11.00%
	TOTAL	1445	100.00%	1200	100.00%	315	100.00%	300	100.00%	390	100.00%	300	100.00%
Population of the inhabited locality (thousand people)	Village	488	33.77%	352	29.29%	112	35.54%	102	34.07%	139	35.64%	102	34.03%
	0-50	311	21.52%	247	20.61%	67	21.36%	63	21.11%	81	20.77%	58	19.04%
	51-500	318	22.01%	299	24.91%	64	20.19%	64	21.41%	82	21.03%	68	22.79%
	500+	328	22.70%	302	25.19%	72	22.91%	70	23.41%	88	22.56%	72	24.14%
	TOTAL	1445	100.00%	1200	100.00%	315	100.00%	300	100.00%	390	100.00%	300	100.00%

		TOTAL		TOTAL		Respondent's Age							
						26-59 y.o.				60+y.o.			
		Wave 2, 2023		Wave 1, 2021		Wave 2, 2023		Wave 1, 2021		Wave 2, 2023		Wave 1, 2021	
		Count	Col%	Count	Col%	Count	Col%	Count	Col%	Count	Col%	Count	Col%
Sex	Male	685	47.40%	570	47.47%	214	48.68%	212	47.02%	108	36.01%	65	43.17%
	Female	760	52.60%	630	52.53%	226	51.32%	238	52.98%	192	63.99%	85	56.83%
	TOTAL	1445	100.00%	1200	100.00%	440	100.00%	450	100.00%	300	100.00%	150	100.00%
Region	Kyiv	116	8.03%	98	8.20%	36	8.18%	38	8.44%	22	7.33%	12	8.07%
	North	243	16.82%	162	13.46%	59	13.41%	64	14.22%	41	13.67%	18	12.02%
	West	313	21.66%	295	24.55%	106	24.09%	105	23.33%	65	21.67%	37	24.77%
	Center	325	22.49%	290	24.14%	110	25.00%	108	24.00%	78	26.00%	37	24.35%
	South	246	17.02%	206	17.19%	72	16.36%	80	17.78%	50	16.67%	24	16.22%
	East	202	13.98%	149	12.45%	57	12.95%	55	12.22%	44	14.67%	22	14.56%
	TOTAL	1445	100.00%	1200	100.00%	440	100.00%	450	100.00%	300	100.00%	150	100.00%
Population of the inhabited locality (thousand people)	Village	488	33.77%	352	29.29%	137	31.14%	128	28.45%	100	33.33%	40	26.67%
	0-50	311	21.52%	247	20.61%	98	22.27%	94	20.90%	65	21.67%	30	20.00%
	51-500	318	22.01%	299	24.91%	103	23.41%	111	24.75%	69	23.00%	43	28.67%
	500+	328	22.70%	302	25.19%	102	23.18%	117	25.90%	66	22.00%	37	24.67%
	TOTAL	1445	100.00%	1200	100.00%	440	100.00%	450	100.00%	300	100.00%	150	100.00%

		TOTAL		TOTAL		Respondent's Age							
						11-17 y.o.				18-25 y.o.			
		Wave 2, 2023		Wave 1, 2021		Wave 2, 2023		Wave 1, 2021		Wave 2, 2023		Wave 1, 2021	
		Count	Col%	Count	Col%	Count	Col%	Count	Col%	Count	Col%	Count	Col%
Main occupation	Employee	380	26.30%	445	37.04%	3	0.96%	0	0.00%	127	32.61%	103	34.25%
	Registered private entrepreneur	70	4.84%	82	6.81%	0	0.00%	0	0.00%	27	6.82%	25	8.20%
	Self-employed	57	3.94%	58	4.82%	2	0.73%	0	0.00%	25	6.35%	20	6.66%
	Student	403	27.89%	176	14.68%	299	94.95%	299	99.63%	100	25.63%	74	24.68%
	Housewife	84	5.81%	111	9.25%	0	0.00%	1	0.37%	16	4.08%	33	10.94%
	Retired	263	18.20%	225	18.73%	1	0.38%	0	0.00%	0	0.00%	3	1.10%
	Temporarily unemployed, but looking for a job	105	7.27%	94	7.82%	3	0.92%	0	0.00%	53	13.94%	38	12.50%
	Other	83	5.74%	4	0.30%	6	2.05%	0	0.00%	41	10.56%	1	0.49%
	Hard to say	0	0.00%	7	0.56%	0	0.00%	0	0.00%	0	0.00%	4	1.18%
	TOTAL	1445	100.00%	1200	100.00%	315	100.00%	300	100.00%	390	100.00%	300	100.00%
Educational institutions	School	259	64.27%	120	67.96%	259	86.47%	251	84.08%	0	0.00%	0	0.00%
	Vocational school	17	4.22%	8	4.27%	15	4.86%	12	3.91%	1	1.46%	5	6.10%
	College	37	9.18%	14	7.69%	18	6.15%	18	5.91%	19	18.84%	12	15.94%
	Higher educational institution	88	21.84%	35	20.08%	6	2.10%	18	6.11%	79	78.68%	58	77.96%
	Other	2	0.50%	0	0.00%	1	0.42%	0	0.00%	1	1.03%	0	0.00%
	TOTAL	403	100.00%	176	100.00%	299	100.00%	299	100.00%	100	100.00%	74	100.00%

		TOTAL		TOTAL		Respondent's Age							
						26-59 y.o.				60+ y.o.			
		Wave 2, 2023		Wave 1, 2021		Wave 2, 2023		Wave 1, 2021		Wave 2, 2023		Wave 1, 2021	
		Count	Col%	Count	Col%	Count	Col%	Count	Col%	Count	Col%	Count	Col%
Main occupation	Employee	380	26.30%	445	37.04%	200	45.34%	233	51.68%	50	16.54%	24	16.07%
	Registered private entrepreneur	70	4.84%	82	6.81%	41	9.19%	40	8.97%	2	0.69%	5	3.50%
	Self-employed	57	3.94%	58	4.82%	29	6.68%	28	6.17%	1	0.25%	4	2.54%
	Student	403	27.89%	176	14.68%	4	0.88%	1	0.23%	0	0.00%	0	0.00%
	Housewife	84	5.81%	111	9.25%	64	14.55%	59	13.03%	4	1.31%	3	1.97%
	Retired	263	18.20%	225	18.73%	25	5.57%	36	8.06%	237	78.96%	112	74.96%
	Temporarily unemployed, but looking for a job	105	7.27%	94	7.82%	47	10.76%	48	10.71%	2	0.52%	1	0.96%
	Other	83	5.74%	4	0.30%	31	7.04%	2	0.41%	5	1.73%	0	0.00%
	Hard to say	0	0.00%	7	0.56%	0	0.00%	3	0.73%	0	0.00%	0	0.00%
	TOTAL	1445	100.00%	1200	100.00%	440	100.00%	450	100.00%	300	100.00%	150	100.00%
Educational institutions	School	259	64.27%	120	67.96%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
	Vocational school	17	4.22%	8	4.27%	1	30.98%	0	0.00%	0	0.00%	0	0.00%
	College	37	9.18%	14	7.69%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
	Higher educational institution	88	21.84%	35	20.08%	3	69.02%	1	100.00%	0	0.00%	0	0.00%
	Other	2	0.50%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
	TOTAL	403	100.00%	176	100.00%	4	100.00%	1	100.00%	0	0.00%	0	0.00%

		TOTAL		TOTAL		Respondent's Age							
						11-17 y.o.				18-25 y.o.			
		Wave 2, 2023		Wave 1, 2021		Wave 2, 2023		Wave 1, 2021		Wave 2, 2023		Wave 1, 2021	
		Count	Col%	Count	Col%	Count	Col%	Count	Col%	Count	Col%	Count	Col%
Educational level	No elementary education	7	0.48%	1	0.08%	7	2.27%	2	0.71%	0	0.00%	0	0.00%
	Elementary education	160	11.07%	80	6.65%	159	50.37%	159	53.07%	0	0.00%	1	0.23%
	Basic secondary education	156	10.80%	82	6.83%	120	37.99%	105	35.03%	12	3.13%	10	3.22%
	Full secondary education	171	11.83%	129	10.78%	18	5.72%	16	5.37%	58	14.91%	41	13.62%
	Secondary professional education	321	22.21%	311	25.94%	2	0.61%	5	1.58%	73	18.75%	61	20.30%
	Incomplete/undergraduate higher education	102	7.06%	61	5.09%	5	1.44%	13	4.25%	65	16.66%	51	16.87%
	Higher education, Bachelor's Degree	158	10.93%	124	10.31%	0	0.00%	0	0.00%	77	19.70%	82	27.20%
	Higher education, Master's Degree	362	25.05%	407	33.91%	0	0.00%	0	0.00%	101	26.17%	52	17.37%
	Hard to answer	10	0.69%	5	0.39%	5	1.59%	0	0.00%	3	0.68%	4	1.18%
	TOTAL	1445	100.00%	1200	100.00%	315	100.00%	300	100.00%	390	100.00%	300	100.00%
Family's financial status	Have to save on food	142	9.83%	119	9.94%	8	2.44%	1	0.49%	8	1.97%	17	5.61%
	Need to save or borrow in order to purchase clothes and shoes	266	18.41%	218	18.15%	36	11.49%	18	5.92%	51	13.06%	29	9.62%
	Need to save or borrow in order to purchase such items as a nice suite, cell phone etc.	373	25.81%	266	22.18%	114	36.16%	133	44.18%	104	26.74%	69	23.14%
	Need to save or borrow in order to buy expensive goods	330	22.84%	280	23.37%	77	24.45%	66	21.99%	112	29.00%	71	23.56%
	Need to save or borrow in order to buy a car or an apartment	177	12.25%	189	15.78%	34	10.84%	38	12.79%	78	20.09%	63	20.99%
	Capable of buying whatever is necessary anytime	67	4.64%	52	4.31%	15	4.73%	5	1.52%	21	5.49%	29	9.58%
	Hard to answer	88	6.09%	75	6.28%	31	9.88%	39	13.12%	14	3.65%	23	7.50%
	TOTAL	1445	100.00%	1200	100.00%	315	100.00%	300	100.00%	390	100.00%	300	100.00%

		TOTAL		TOTAL		Respondent's Age							
						26-59 y.o.				60+ y.o.			
		Wave 2, 2023		Wave 1, 2021		Wave 2, 2023		Wave 1, 2021		Wave 2, 2023		Wave 1, 2021	
		Count	Col%	Count	Col%	Count	Col%	Count	Col%	Count	Col%	Count	Col%
Educational level	No elementary education	7	0.48%	1	0.08%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
	Elementary education	160	11.07%	80	6.65%	1	0.22%	2	0.33%	0	0.00%	1	0.58%
	Basic secondary education	156	10.80%	82	6.83%	22	4.91%	17	3.69%	2	0.64%	1	0.74%
	Full secondary education	171	11.83%	129	10.78%	45	10.29%	57	12.68%	50	16.83%	10	6.59%
	Secondary professional education	321	22.21%	311	25.94%	134	30.31%	128	28.52%	112	37.45%	55	36.76%
	Incomplete/undergraduate higher education	102	7.06%	61	5.09%	14	3.08%	16	3.66%	18	5.88%	5	3.26%
	Higher education, Bachelor's Degree	158	10.93%	124	10.31%	50	11.40%	46	10.20%	31	10.35%	11	7.39%
	Higher education, Master's Degree	362	25.05%	407	33.91%	174	39.41%	183	40.64%	87	28.85%	66	44.10%
	Hard to answer	10	0.69%	5	0.39%	2	0.38%	1	0.27%	0	0.00%	1	0.58%
	TOTAL	1445	100.00%	1200	100.00%	440	100.00%	450	100.00%	300	100.00%	150	100.00%
Family's financial status	Have to save on food	142	9.83%	119	9.94%	58	13.18%	43	9.50%	68	22.69%	30	19.94%
	Need to save or borrow in order to purchase clothes and shoes	266	18.41%	218	18.15%	92	20.90%	83	18.39%	87	28.89%	45	30.23%
	Need to save or borrow in order to purchase such items as a nice suite, cell phone etc.	373	25.81%	266	22.18%	83	18.90%	87	19.22%	72	23.98%	25	16.84%
	Need to save or borrow in order to buy expensive goods	330	22.84%	280	23.37%	113	25.71%	122	27.10%	28	9.35%	18	12.32%
	Need to save or borrow in order to buy a car or an apartment	177	12.25%	189	15.78%	46	10.50%	72	15.95%	19	6.47%	21	14.14%
	Capable of buying whatever is necessary anytime	67	4.64%	52	4.31%	26	5.91%	21	4.64%	5	1.70%	3	1.95%
	Hard to answer	88	6.09%	75	6.28%	22	4.90%	23	5.20%	21	6.92%	7	4.58%
	TOTAL	1445	100.00%	1200	100.00%	440	100.00%	450	100.00%	300	100.00%	150	100.00%