



UNDERSTANDING SAFE DIGITAL SPACE:



A STUDY OF PERSPECTIVES OF YOUNG PEOPLE IN GEORGIA

AUTHORS: MARIAM TSKHOVREBASHVILI, TAMAR GAGNIASHVILI, MARIAM TSUTSKIRIDZE

The report was prepared with the financial support of **RNW MEDIA**. All opinions and views expressed in the publication belong to the author(s) of the publication and should not be taken as the position of the organization.

Understanding Safe Digital Space:

A Study of Perspectives of Young People in Georgia

Authors:

Mariam Tskhovrebashvili, Tamar Gagniashvili, Mariam Tsutskiridze

Statistical analysis and visualization of data:

Mariam Tsutskiridze

Cover:

Mariam Tskhovrebashvili

The report was prepared with the financial support of RNW MEDIA. All opinions and views expressed in the publication belong to the author(s) of the publication and should not be taken as the position of the organization.

2023

TABLE OF CONTENTS

Introduction	4
Methodology	5
Key Findings.....	11
Data Analysis	14
Conclusion.....	55
Recommendations.....	57
Appendix	59

01 INTRODUCTION

In the modern world, where young people's social life is significantly linked to online activity, digital spaces have started to occupy an essential place in their daily lives. Nonetheless, the threats and risks existing within the same digital space also produce noticeable challenges.

Studying the online platform-related perspectives and experiences of young people living in Georgia provides a general picture of their vision of the ideal and safe digital space model of the future. Besides recalling their experiences with digital threats, young people suggest preventive mechanisms and measures to make digital spaces much safer. The specific online interaction-related experiences of young people provide tangible information on how the space holding a significant part of their lives and activities can be made more comfortable and safe.

Cyber security-related studies conducted in Georgia and beyond provide a solid basis for creating security mechanisms. However, in-depth research on the experiences of young people living in Georgia, their visions, and future perspectives regarding digital spaces has not been conducted until now. Accordingly, the following study attempts to outline the experiences and perspectives of young people in Georgia regarding safe digital spaces. The findings highlighted as a result of the research aim to lay the foundation for conducting a future larger-scale research in this direction.

The research was implemented in the period of July 24 - September 15, 2023. The research report is divided into the following parts: The research methodology and key findings are presented after the introduction, followed by the data analysis part, which entails in-depth information about each research topic. The research report ends with a conclusion and lists tangible recommendations designed for all parties interested in existing or creating new, safe digital spaces for young people.

02 METHODOLOGY

Research Objectives and Goals

The primary objective of the research is to outline the understanding, experiences, and perspectives of young people in Georgia regarding safe digital spaces. The term digital space refers to all the digital platforms used by young people for various purposes, be it communication, education, creating their own content, using it for work or other purposes. The research aims to understand how young people in Georgia define the concept of a safe digital space; to understand their experiences; to understand what they think about future perspectives and challenges of the digital space. The objective of the research is to identify and explore the factors that contribute to the creation and functioning of safe digital spaces for young people in Georgia. It is essential to highlight the potential risks and challenges of what young people perceive as unsafe while interacting with the Internet. The ultimate goal of the research is to develop recommendations and guidelines tailored to the specific needs of young people in Georgia and to foster digital community development.

Main Research Topics:

- **Definition and Understanding of Digital Safe Space** - How do young people living in Georgia understand and define a digital safe space? Also, what is the role and importance of this space in their daily life?
- **Contributing factors to safe digital spaces** - What factors contribute to creating a safe online environment for young people? Including factors such as privacy, trustworthiness, support, inclusion, and freedom of expression.
- **Challenges and Opportunities** - Identifying potential risks, threats, and challenges in the digital space for young people in Georgia. Promoting opportunities for learning and positive engagement, including developing strategies to help co-create safe online digital spaces.

Research Method

Given the aim of the research to study the perceptions, experiences, and perspectives of young people in Georgia regarding safe digital spaces, qualitative research methods have been selected. This approach allows us to study all research topics important to the project comprehensively. The research methodology includes three stages. Each stage is based on three different techniques. These stages are real-time focus groups, in-depth interviews, and asynchronous focus group discussion on social media.

Respondent Sampling

Based on the objectives of the research, a model of purposive sampling was used. Purposive sampling refers to the selection of respondents based on predetermined specific characteristics, be it gender, age, social status, workplace, education level, or other criteria. **The primary criterion of sampling for our research is that all respondents are young social media users; they actively use digital spaces and have some experience in this regard.** Other criteria for the sampling of participants are as follows:

1. All respondents are in the age group of 15 to 25 years.
2. The respondents involved in the research are people with different experiences: young people with disabilities, representatives of ethnic minorities, members of the LGBTQI+ community.
3. People of all genders participate in the research.
4. All respondents of the research participate in it voluntarily.
5. Those young people who met the above criteria and were available to the researchers participated in the study.

Research Stages

Methodologically, each stage of the research differs from each other in terms of sampling of respondents and the various research techniques used in the implementation process:

1. **Stage I - In-depth Interviews** - In the first stage of the research, individual in-depth interviews were conducted with six youngsters. Among them, two interviews were conducted with young people with disabilities. (One is blind and the other is a wheelchair user). Two interviews were conducted with young people representing ethnic minorities (Armenian and Avar (Lek), and two interviews were recorded with

genderqueer youth (One identifies herself as female, and the other identifies as male). We kept gender inclusiveness, which allowed us to have interviewees beyond the gender binary. All six respondents are representatives of the 15-25 year-old age category. The interviews were recorded virtually using the Zoom platform.

- 2. Stage II - Real-time Focus Groups** - The second stage of the research includes two focus groups with young people aged 15-20 and 21-25. At this stage, half of the research participants were recruited by the psycho-social support center “Tanadgoma” through a TikTok channel. We provided information about the research and its objectives to the “Tanadgoma” TikTok channel subscribers, and they voluntarily agreed to participate. Both focus groups were conducted virtually using the Zoom platform, and six young people participated in each focus group. Their age data are as follows:

Focus group with young people in the age category of 15-20 years	Age	15	16	17	18	19	20
	Number of participants	-	1	1	2	1	1
	Gender	Female	Female	Female	Female	Female	Male

Focus group with young people in the age category of 21-25 years	Age	21	22	23	24	25
	Number of participants	2	2	1	1	1
	Gender	Female	Female	Male	Female	Female

- 3. Stage III - Asynchronous Focus Group Discussion on Social Media** - The third stage of the research includes an asynchronous discussion on social media, which was carried out in collaboration with “Tanadgoma.” The social media manager of “Tanadgoma,” along with researchers, created a special closed group for discussion on Facebook. The entire process of creating a group and conducting a discussion followed the Asynchronous Focus Group Discussion Guidelines provided by RNW MEDIA. The social media manager of “Tanadgoma” recruited young people under 25 in the group, who were given detailed information about the reason for creating the group, the research, and its objectives. Participation in the discussion was voluntary, and group members stated their positions on any question of their interest. The discussion took place for ten days



according to the researcher's questionnaire-guideline. The discussion was moderated by a social media manager of "Tanadgoma" with the supervision of the researchers. Technical details about asynchronous discussion on social media can be found in the table below.

Asynchronous Focus Group Discussion on Social Media - Technical Details	
Group name	"Collaboration"
Group type	Closed group
Number of group members	240 young people
Number of participants involved in the discussion	On average, 20-35 young people
The duration of the discussion	10 days
A tool for conducting the discussion	Questionnaire-guideline
Number of questions/posts	14 (including welcome and closing posts)
Intensity of posting questions	1 or 2 questions per day
Type of questions	Open questions Closed questions Semi-structured questions Polls
Type of respondents' activity	Commenting, expressing a reaction, filling out a poll, posting a photo/video/gif

Research Tools

Two types of instruments were created to collect data for the research - a questionnaire for in-depth interviews and focus groups and a questionnaire-guideline for asynchronous discussion on social media. Both instruments included the questions and formats to obtain the information required to achieve the research objectives. During the interview and focus group discussion, the questionnaire consisted of closed, in-depth questions and a special table created to determine priorities to obtain detailed and comprehensive information about the research issues. As for the asynchronous discussion guide questionnaire, taking into account the features of the social space, it included more diverse formats and consisted of both closed and open, semi-structured and poll-type questions. Both tools can be found in the appendix **(p.60)**

Data Collection and Analysis

To collect research data, in-depth interviews and focus group discussions were audio-recorded based on prior agreement with the respondents. The recordings took place through the [Zoom](#) platform. During the fieldwork, the online platforms [Google Docs](#) and [Poll Everywhere](#) were also used in the data collection process. After the data collection process, the data of the asynchronous discussion on social media were processed in Excel, and the audio recordings were transcribed in detail. In order to highlight the main findings, the data was categorized, and the narratives were defined according to categories. Based on the obtained results, a research report was prepared.

Ethical Aspects of the Research

Research respondents participated in interviews and discussions of their own free will. All of their personal data is confidential. The parents of the minor participants of the research (3 in total) received a consent form (written) in advance, asking for permission for their children to participate in the research. Only after receiving their consent, the minors were included in the research. Adult research participants gave verbal consent at the beginning of the interview records.

Research Limitations

The research has three limitations. The first is the small number of male respondents among the participants in the real time focus groups. The recruitment of focus group participants was carried out according to age categories, but also half of the participants were female and half were male. The date and time of the discussion was agreed upon with all possible participants in advance. However, for reasons independent of the researchers, the male participants refused to participate in the real time focus group immediately prior to the start of it due to necessity. This fact was repeated twice. That is why focus groups were conducted with the participation of all the selected respondents who were already ready to participate in the discussion. Therefore, we assume that it may cause a small change in the results of the study.

The second limitation of the research concerns the recruitment of participants for the real-time focus groups. Half of the participants of the focus groups were selected through the TikTok channel of the psycho-social support center "Tanadgoma". They might have in general higher awareness and better knowledge of digital safety/security, compared to

other young participants of research. Therefore, that might be reflected in their answers and eventually into the research findings and this factor perhaps had little effect on the final results of the research.

As for the third limitation of the research, it is related to the asynchronous focus group discussion in social media. Since the format and methodology of the discussion were significantly different from the techniques of in-depth interviews and real time focus groups, its data could not be combined with the rest and presented in a unified way. The asynchronous discussion questionnaire consisted of a different and smaller number of questions than the questionnaires used in in-depth interviews and real time focus groups. The involvement of the respondents and the format were different. Also part of the data was processed using quantitative research methods. Considering all the reasons above, in the opinion of the researchers, combining the data obtained as a result of the use of different techniques was methodologically incorrect and would make the research report chaotic. Therefore, the data analysis of the asynchronous discussion was given a separate chapter in the research report.

03 KEY FINDINGS

Definition and Understanding of Digital Safe Space

1. Young people define the term “**safe digital space**” as a space where privacy, personal data, freedom of expression, and ethical norms are protected; as well as where they feel protected from harassment, bullying, mental and emotional harm, and other cyber threats;
2. The following platforms more or less meet the criteria of safe digital spaces for young people: **YouTube, Signal, Discord, Gmail, and Instagram;**
3. Young people in the age group of 21-25 years have a particularly critical attitude towards the safety of digital spaces and do not believe in the existence of perfectly protected and safe digital spaces;

The role and importance of Digital Safe Space in young people’s daily life

1. According to the participants of the research, young people spend much of their daily social life in the digital space. Time spent in digital spaces ranges from 2 to 9 hours;
2. Young people use digital spaces mainly for three purposes: getting information, communicating with others, and entertainment.
3. **Instagram, Facebook, YouTube, TikTok, and Gmail** are the most actively used platforms.
4. All digital platforms have different functional meanings for young people, and their positioning is also different on this platform. They use different digital platforms for different activities.
5. Young people determine entrance into communication with unknown users according to the following criteria: **name and surname, age, photos, publicly posted personal information, how long ago the profile was created, mutual friends/followers, type of posted content, value congruence, and connection to common institutions;**

Contributing factors to safe digital spaces

1. An ideal digital space for group discussion for young people is characterized by the following features: **the group is closed, has internal rules, has an active moderator and has a small number of people interested in one topic;**
2. The main criteria of an ideal digital platform for young people aged 15 to 25 in the future are **privacy, personal data protection, security, a space free from hate speech and discrimination, including ethnic, religious and other types of discrimination, freedom of expression, transparency and protection from cyber crimes.**

Potential Risks, Threats and Challenges

1. Young people are worried and actively discuss the risks and dangers in the digital space. Among them, the **insecurity of personal data, harassment and psychological pressure, blackmail by disclosing personal data and correspondence, vulnerable and unsafe environment for minors and children, low standard of accessibility of websites, discrimination, and the absence of a mechanism to protect users from it, weak legal framework and legal response mechanisms;**
2. Young people named **Viber, TikTok, Facebook**, and all websites with **RU** domains as unsafe platforms;
3. The young people participating in the research are less involved in the group interaction and mostly have the role of observers. For them, being active in a group space means communicating with many unknown users, which makes them feel unsafe;
4. For security reasons, young people avoid contact and interaction with unknown users (strangers, fake accounts, trolls, bots) in the digital space. Some of them have even closed their accounts because of this reason;

Promoting Opportunities For Learning and Future Perspectives

1. The study results showed that young people generally do not possess essential or fundamental knowledge regarding media literacy, and the information they possess is based only on personal experiences;
2. Young people believe that media literacy is so critical that it should be included in the school curriculum, in addition to

- informal ways of receiving education in this direction;
3. Young people see the owners of big tech platforms (such as Meta) as important actors in the future of digital security and point out their responsibility to protect users' personal information;
 4. According to the young people participating in the research, it is crucial to raise the awareness of the users of digital spaces about their involvement and role in the process of creating safe spaces of the future;

04 DATA ANALYSIS

CHAPTER 1

The Function of the Digital Space for Young People

Based on the research objectives, data were collected about the experiences and understanding of young people aged 15 to 25 living in Georgia regarding digital spaces. According to this data, one can argue that they spend a significant part of their daily life in the digital space. More specifically, this time ranges from 2 to 9 hours, which means that a large part of the daily activities and necessities of young people are tied to digital platforms. In different cases, the forms and objectives of online activity are different. However, the digital space’s main functions for the respondents of our research can be divided into several main components. If we list these components according to priority, we get the following picture:

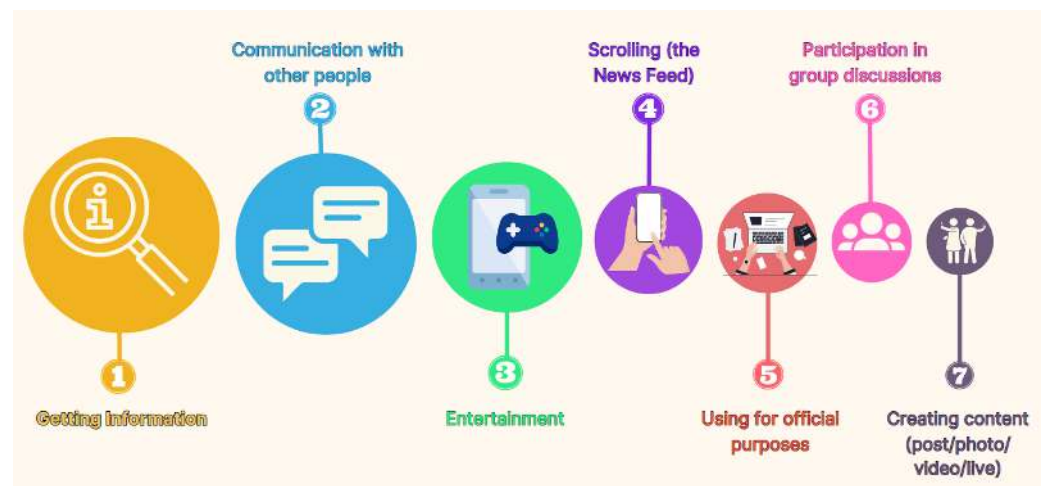


Diagram N1 - Priority Functions of Digital Spaces

Data analysis made it clear that the most important function of digital spaces for young people is receiving information. In addition to getting daily news, this process entails learning opportunities in various directions and having alternative ways of education. Getting information in the digital space is much easier and more accessible than anywhere else; however, this accessibility poses challenges for young people and the

need to develop skills to filter out unreliable and unnecessary information in the information flow. The same can be said about the ability to communicate with others, as digital means of interaction have made communication easier and faster. For some respondents, the greatest value of digital platforms is the ability to communicate with family members abroad easily. However, even in this case, along with the simplicity and efficiency, some challenges and dangers come with communicating in the digital space.

As for the use of digital platforms for official purposes, among the respondents of different age categories, this component varies in terms of priority. For 15 to 20-year-olds, using the digital space for work has the least priority, while this component is the 3rd most prioritized activity for 21 to 25-year-old respondents. The 24-year-old focus group participant works as a social media manager, and his daily work area revolves around digital platforms. Also, several participants use the online space for career purposes, to introduce their creativity to other people, and to find potential business partners. For one of the respondents, digital platforms are a space for social activism. Also, we got different results in terms of using digital platforms for entertainment in different age categories. In the 15- to 20-year-old age category of young people, this component ranks first in terms of priority, and for the 21-25-year-old age category, entertainment ranks 6th in the priority table.

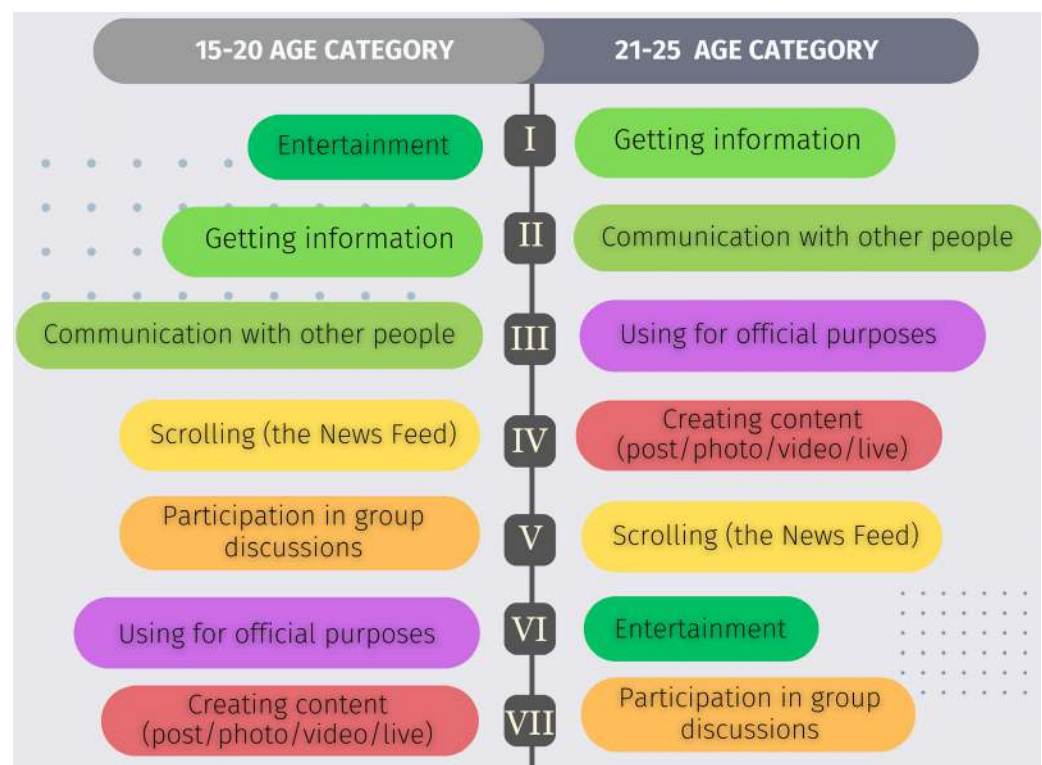


Diagram N2 -Functions of Digital Platforms According to Age Categories

Within the framework of the research, the main digital platforms used by young people living in Georgia were identified. Although young people may have personal accounts on many different digital platforms, the most actively used platforms are **Instagram, Facebook, YouTube, TikTok, and Gmail**. However, these platforms are sorted by young people according to activities, which means that all the listed platforms have different functional meanings for them, and their positioning is also different.






Digital Platform	Positioning and Functional Value
 Instagram	<ul style="list-style-type: none"> Account registration with a pseudonym Personal space Personal photos and videos Communication with friends
 Facebook	<ul style="list-style-type: none"> Account registration with own name and surname Formal and informal communication Public space Use for official purposes Education / receiving information Creating content
 Tik-Tok	<ul style="list-style-type: none"> Account registration with a pseudonym Entertainment Education
 YouTube	<ul style="list-style-type: none"> Education Entertainmen
 Gmail	<ul style="list-style-type: none"> Account registration with own name Official communication Use for official purposes Use for educational purposes

Table N1 - Functional Value of Digital Platforms for Young People

Besides the most used platforms shown in the table, young people also mention other online spaces: **Pinterest, LinkedIn, Twitter, Bereal, Messenger, WhatsApp, Signal**. Although all digital platforms have different functional meanings for young people, the degree of trust in them is also different. Security issues and the trust of personal data or private communications in the digital space are challenging for young people.

Chapter 2

Digital Interaction: Experiences and Perspectives

2.1 Individual Communication

According to the opinions and experiences of the young people participating in the research, digital interaction has a great role in their social life, and today, a large part of their social relations is carried out in the digital space. Two main types of digital interaction were identified - individual communication and participation in group discussions. Individual communication in the digital space entails several directions: communication with family members and friends, educational and work-related communication, and interaction with strangers. As it turned out, a large part of informal individual communication is with family members, friends, and acquaintances. However, young people avoid interacting with strangers. Some of the research respondents have closed their profiles on digital platforms so that strangers could not see their content and not enter into communication. If an unknown user tries to contact them in any way (friend request, follow, message), in most cases, they do not respond; they leave the request open and only respond if they notice an interest in some serious issue and can provide some help. They have their own criteria for starting communication, and according to these criteria, they decide whether to confirm friend requests/follow, or reply to a message to unknown users. The list of the most important criteria is as follows: **what kind of personal information the user has posted on their page, how they write their first and last name, whether the photo matches their name, how long ago the profile was created, whether they have mutual friends/followers, what type of content they shared and whether they have similar values or links to common institutions (for example, a university).**

“

I pay a lot of attention to this matter, and when, for example, a friend request comes from an account (or a page), or a message or an attempt to any kind of communication, I always keep an eye on personal data. I look at whether they have a photo or not, I look at mutual friends, I look at a lot of things, but I also want to point out that you can look at all this, but it is still can be a fake or an account created with someone else's name and surname or using someone else's photo; and what can I know? I think we are not safe. I don't feel safe personally.

Representative of ethnic minority_Armenian, 25 years old

”

For young people, communication in the digital space is about safety, as they try to avoid connecting to fake accounts or interacting with trolls and bots. Having real-life or mutual acquaintances during digital interactions plays an important role in terms of security, but it does not guarantee complete safety.

“

When you add a person (in your friends or follow), they see your personal page, follow you, see what you comment on, what you do, it means that they see your personal life. I definitely also pay a lot of attention if (unknown users) are from my friends, or I know them somehow in real life, or I heard about them from my friend, and so on. I don't want everyone to know about my private life and find out the details.

LGBTQ+ community member, 20 years old

”

It should be noted that, based on experience, the behavior of young people in digital interaction changes with age. Research participants remember that when they were younger and did not have much experience with digital platforms, they did not pay attention to the details as they do now. They no longer want their personal information to be available to many strangers in digital spaces, so they use the function of closing the profile and deciding the issue of starting communication with foreign users by specific criteria.

2.2 Group Interaction

First and foremost, it should be noted that **Instagram**, which has been named one of the most actively used digital platforms, does not have a group interaction function. Youngsters participating in the research use spaces for group communication mainly on the **Facebook** platform, although most of them note that they are not actively involved in group discussions. They mostly play the role of passive observers, although some find group discussion spaces a good source of information. According to some respondents - on the contrary, group discussion spaces are associated with a large flow of unnecessary and unreliable information; therefore, they either do not join groups at all or minimize the number of such spaces on their profile. In general, the young people participating in the research are not active in groups, they do not write posts/reels, do not actively participate in discussions and do not use

the function of live streaming, and they are not attracted to this type of interaction. Only a small number of respondents mentioned that they engage in discussion in some type of digital group space, with their engagement limited to posts in one case, comments in another, and engagement in a chat discussion format in a third. Other types of group interaction were not identified.

Young people join groups according to thematic interests and rational needs. For example, as it turned out, group spaces are a good way for educational institution communities, from which students can receive and share the necessary information.

Also, private groups of women and men, with topics related to sexual education, are popular among young people. They also mention groups related to their entertainment activities, such as travel, books, and movies, or rational needs, such as buy & sell groups.

Respondents mostly have the same positions regarding the issue of involvement in group discussions. They are less involved in the process of group interaction; however, different opinions and experiences are shared. One of the young people, who is most actively involved in group discussions among the respondents, says that closed and private groups are more comfortable for him. In addition, he has a space for group discussion, where he has the experience of talking about a personal problem and has received some help from other group members.

“

I would highlight the “men’s group” where there is some unprecedented solidarity towards each other, and when you post something, in a few minutes, there are already so many comments and advice that it motivates you. I also had such a case - I posted, and in a few minutes I received such comments from there that I even wrote to many people personally and thanked them.

Representative of ethnic minority_Avar Lek, 19 years old

”

In some cases, young people only post in the group space and then do not participate in the discussion. One of the research participants, an activist in the direction of rights of people with disabilities, says that she often publishes informative posts in Facebook groups related to people with disabilities, but then she no longer joins the discussion because she thinks that this is a waste of time. In the case of another respondent, the activity is limited to engaging in discussions in groups of a specific topic and format.

“

I have experience with some groups related to my hobbies. That is, such as a group of books, for example, movies, etc. And the groups that have already been mentioned, the “Women’s Group” and the “TSU” Group. There are some groups that are confidential, where information is shared anonymously, and I’m a little active there because people are asking for advice or sharing their stories. They just ask people for advice or just support. That’s why I’m active there. I mainly comment if there is an issue relevant to me.

Focus group participant, 18 years old

”

Being active in group discussions is associated with the issue of safety for young people, and they are often not active because they feel unsafe in digital spaces. For them, being active in a group space means communicating with many strangers, making them feel insecure. Facebook, which has a distinct mechanism for group interaction, is not attractive to young people mostly because of hate speech, which is difficult to control.

“

There are fights between political evils and fools in the comments. 90% of what I see is hate speech, but it’s true.

Focus group participant, 25 years old

”

In some cases, young people use the function of writing anonymously during group interactions to protect themselves from hate speech. Talking about hate speech, besides **Facebook, TikTok** is also mentioned, where it is also not possible to control hate speech and discrimination.

“

Facebook has a very good function that allows you to post anonymously. There were times, when, no matter how you wrote, you would still be criticized, and there were times when I felt insecure, and there were times of threats. That’s why I mostly comment anonymously, depending on the group and the topic.

LGBTQ+ community member, 20 years old

”

Anonymity is important for the 16-year-old young participant of the research, in whose opinion, **Discord** is the most comfortable platform for group interaction. Since **Discord** does not require registration with your first and last name and does not ask for any personal information, engaging in group discussions is much safer for him. According to the same respondent, the **Discord** group discussion space is more convenient than **Facebook** because the discussion in the chat-type space is faster and more alive, and there is no need to wait for other people's comments like on **Facebook**. For him, the involvement of many people is a precondition for an interesting discussion despite the risks of hate speech and discrimination. Other respondents note that they feel safer during a group discussion if there are few people in the group, and it is easier for them to express their opinion in such an environment.

“

The first thing that is very important to me is the name; it should be a name that makes people interested in what's going on inside. If the name is uninteresting, it doesn't matter whether the group is open or closed. Also, what I pay a lot of attention to is that I really like colorful photos in general; this colorful photo somehow makes me want to go in and say something to send a request to add to the group; it attracts my attention more. Obviously, what type of audience "follows" him is also important. I look at that too, and besides, lately, I've started to see who the admin is, how many people there are, and "follow" those admins before I send a request to join. It calms me down more, and I understand more where I am sending the request to; who is managing what I want to be a part of.

Ethnic minority representative_Avar Lek, 19 years old

”

Some of the respondents who talk about being involved in group discussions in some way do not mention specific topics that they might talk about or enter into discussions. In one case, it was revealed that if the group space is connected to the community of an educational institution, where topics related to the learning process are discussed, young people may engage in this type of interaction based on practical goals and it is not unsafe for them. Besides, the respondents mentioned 'Women's' and 'Men's' groups, in which the topic of sexual education is mainly discussed. However, in order to enter the discussion in such topic groups, it is important for them that the group is closed and has specific rules for safety. However, they did not specify the specific topics in which they discussed.

When imagining an ideal digital space for group discussion where they would be willing to participate in the discussion, the youngsters named several features. Besides the **number of people** in the group, it is important for them that the group has **rules** and the **moderator controls** the adherence to them. The group should be **closed** so that not everyone can join, and only people interested in one topic should be members. Nonetheless, young people still do not think that they will feel safe even if all the criteria mentioned by them are met. Although group interaction platforms are still considered one of the necessary components of the digital space.

Chapter 3

Safe Digital Space

3.1 Definitions, Criteria, Mechanisms, Experiences

One of the main objectives of the research was to find out how young people aged 15-25 understand and interpret the term “safe digital space.” Respondents of the research offered a number of definitions of the term. Based on the obtained results, we can conclude that a safe digital space for young people is a space in which:

- User privacy is protected; (This criterion is especially relevant for members of the LGBTQ+ community)
- Offensive comments can be avoided;
- Personal information of users is protected;
- Personal data is not available to other persons without permission;
- Users have the ability to decide whom to share their content with;
- There are internal protection mechanisms and hacking is not easy;
- The age limit is respected and inappropriate information is not available for the minors;
- There are no trolls or bots;
- It is not possible to spread disinformation and fake news;
- Freedom of expression and ethical norms are protected;
- It is possible to control and prevent cybercrime;
- People are protected from harassment, bullying, mental and emotional harm; (This criterion is especially important for a person with a disability and a representative of an ethnic minority)
- There are defense mechanisms against phishing, viruses and other types of threats;

All participants agree that in this century, when the use of digital spaces is an integral part of human daily life, due to the high publicity of these spaces, it is impossible to name any of them as a completely safe platform. The issue of personal data protection remains an important dilemma in digital spaces, and young people find it almost impossible to resolve this topic fully. Young people aged 21-25 years have a particularly

critical attitude in this regard. While defining the term, they said there are simply no safe digital spaces; they do not name the specific definitions of the term and underline the fact that they can never feel safe in the digital space. According to the representatives of this age group, there are specific mechanisms for defense, but they cannot provide guaranteed protection. Therefore, it is difficult for them to name a platform where they feel safe and secure. It is also difficult for other age categories of young people to point out such platforms. However, they still identify some digital spaces that more or less meet their criteria for a safe digital space. The results according to age categories are available in the table below:

	“We can’t be 100% safe anywhere... But I think a platform where people are less active is more secure. I never had the fear that someone would disclose my personal information on YouTube.” (Focus group participant, 20 years old)
	“Now I think Signal is a safe space; for now, I use this.” (Ethnic minority - Avar Lek, 19 years old)
	“Facebook is safe, but only my friends are there, very close ones, who I trust 100%. It’s the only space where I feel safe.” (LGBTQ+ community, 25 years old)
	“Discord is the safest for me because it doesn’t ask for my real name, it doesn’t ask for my address, it doesn’t ask for my real age...it actually doesn’t have information that this company can use for bad purposes and hurt you.” (Person with disability - wheelchair user, 16 years old)
	“I feel safe on both Facebook and Instagram because I know how to look after myself in that space. But, I am saying that none of the social networks nowadays is so perfect that it was protected from everything”. (Focus group participant, 18 years old)
	“In my opinion, email is safer than other digital spaces... I also use YouTube, of course, if that counts.” (Ethnic minority_Armenian, 25 years old)
	“I don’t know if you know an application like Signal; I used it for a while; I can say that it is less dangerous. There’s also some other app for sending photos, I can’t remember the name exactly, where you feel safe.” (LGBTQ+ community member, 20 years old)
	“I think Gmail is the most secure I can remember... WhatsApp is the most unsafe for me.” (Person with disability, 21 years old)

Table N2 - Safe and Secure Digital Spaces for Young People

Security Mechanisms and Functions of Digital Platforms

During the research process, young people talked not only about the criteria of a safe digital space and safe platforms but also about the functions and mechanisms of digital spaces that give their users a certain sense of security. Young people have highlighted features that different platforms have and are actively using them to protect their personal accounts. For some participants, having information about defense mechanisms provides a sense of security on digital platforms, as they use these mechanisms to create their own safe space. The list of defense mechanisms and functions of digital spaces named by young people is quite diverse and mostly of a technical nature.

- 1. The function of controlling the publicity of personal information** - users can decide whether to share personal data with other people. Name, surname, age, date of birth, photos, or other types of content that they share on digital platforms.
- 2. The function of choosing the type of personal account** - users can choose whether they will have an open or closed account. Instagram is mentioned as a good model of such a platform.
- 3. A mechanism that allows the user to find out if someone records a private message or makes a screenshot of the photo** - Examples of digital spaces with this mechanism are **Instagram** and **Snapchat**.
- 4. Mechanism of control of access to the personal account** - On certain platforms, users can see if another person has logged into his personal account. Users use the double protection mechanism to protect their accounts. Respondents mentioned **Facebook** and **Instagram** as platforms that have such mechanisms.
- 5. The function of detecting and “reporting” fake accounts on digital platforms** - users can identify fake accounts and contact the platform administration for some measure.
- 6. A function that allows you to find out if someone creates a fake analogue of your account (Cloning a user account)** - on **Instagram**, you can try to log into that account several times, and the platform will show you the first letters of its data.

7. **Verified account function** - there are platforms where the users pay a certain amount, give their account a verification mark, and thus protect themselves from fake duplicates. According to the respondents, this mechanism is mostly used by famous people, but any other user can do the same.
8. **Automatic deletion of messages** - On certain digital platforms, users can set a time in advance when a message they have sent to another person will be deleted.

Experiences - The discussion about defense mechanisms and functions of digital spaces showed that young people aged 21-25 are well aware of specific mechanisms of digital spaces and platforms. They also analyzed well what a safe digital space should be; however, they have never tried to create it themselves. Most of the participants only had experience in creating common “chats.” Only a few respondents talked about the experience of creating specific groups on social platforms. One of them, a 18-year-old respondent, had an attempt to create a group based on inclusive goals; however, the group was soon canceled due to the lack of human resources. Nevertheless, she says that even for a short period of time, with the help of active moderators, rules, and regulations, the group functioned quite efficiently and did not face any particular challenges:

“

I was trying to create a group for those students who faced some obstacle in the university space. They had to provide this information through the group, and then specific people would talk about it publicly. It could have been accessibility problems and others. Several people were very active, including the moderator, who filtered the posts and comments. People could post anonymously. Of course, there were rules, but not all of them adhered to these rules, and that's why we had the verification. We have always been careful about this.

Focus group participant, 18 years old

”

One of the respondents, a young person with a disability, also mentioned her own experience of creating space on one of the digital platforms. She often creates these kinds of spaces mostly for professional purposes, and has had quite a few cases. According to her, such groups are mostly closed; she also uses the internal rules of the group, which she considers to be one of the mechanisms of security protection:

“

I created a lot of groups because sometimes when we do projects, we need something for communication and... in many cases, it is closed groups because later on, photos of the project are uploaded or something like that, and maybe someone doesn't want to, somehow this information spread outside the group... I also pay a lot of attention to the rules; it is very important to keep something neutral, and so on. Also, we don't discuss any off-topic topics in the group. It is also related to security that the topic should be discussed, around which topic these people united.

Person with disability_blind, 21 years old

”

A 25-year-old respondent representative of the LGBTQ+ community also spoke about his own experience of creating a group. He emphasizes predetermined rules and a small number of people in the group as the main criteria of the safe space he created:

“

I created a group with my friends, but it was a few years ago; we were posting for a while. We had predetermined rules that said no obscene language in this group. There were somewhere around 60-70 people, but then it got passive, we didn't pay attention anymore... It was like that - we were uploading funny pictures, everyone was laughing, and we really didn't have any bad cases or obstacles.”

LGBTQ+ community member, 25 years old

”

3.2 Threats, Risks, Platforms, Emotional Experiences

The young people participating in the research talk a lot about the risks and threats in the digital space. Almost all of them have a negative experience in this regard. In this table, you will find detailed information about the threats mentioned by young people, the platforms containing risks, their negative experiences and emotional memories related to specific threats.

Threats and Risks	Personal Experiences of Young People
<p>1. Threats and attempts to hack personal accounts</p>	<p>A member of the LGBTQ+ community, 20 years old: "It was a personal attack; a specific person wanted to hack my Facebook... I avoided it; I had a very long password, and it would be difficult to hack it without hackers. There have been many attempts, and I have received a notification from Facebook that someone is trying to log into your Facebook; I also received a password reset email that someone is trying to reset your password".</p>
<p>2. Harassment and psychological pressure</p>	<p>Focus group participant, 18 years old: "There was one such case. For example, a friend of mine on social network had a case where he was harassed by a very bad person. In the end, the parents got involved and solved it. We couldn't involve the police in the process because we might've gotten hurt again because we didn't have any supporting documents. Thus, the intervention of the parents and then the intervention of someone from the parents produced some results.</p>
<p>3. Insecure environment for minors and children</p>	<p>Focus group participant, 18 years old: "There was a page created at school, where they wrote very bad things about children and mostly lied. When people started to find out who created this page, they put my name and surname as if I did it, but I really didn't. So far, I have not been able to prove that I didn't do it because a 9-year-old can't deal with such things. This story stopped by itself then, but to this day, everyone thinks that I was that "account" and I wrote all that, and I can't prove it.</p>
<p>4. Blackmail by disclosing personal data and correspondence</p>	<p>Focus group participant, 19 years old: "There have been moments of spreading things on social networks, blackmails, a lot of things, and these people have not been punished to this day... They can even get your personal photos, even correspondence and things and publish them on different pages".</p>

5. Cloning a user account	Focus group participant, 19 years old: "I had a case when my "fake account" was created. At that time, I was too young to take it a little more seriously, that it is punishable, that it cannot be done, and that is, when I found out, I was probably 12-13 years old at that time, and at least I still haven't found out who was doing these thing".
6. The risk of easy access to personal data	Focus group participant_Sandro, 20 years old: "I had an experience when I was 15 years old; someone posted my Facebook profile in an online game, somehow a complete stranger found me, even a foreigner, he was not Georgian, and somehow he found me..."
7. Risk of viruses, phishing, scams, and other threats	Person with disability_wheelchair user, 16 years old: "First there are threats of discrimination, bullying, which can cause problems, then there are hacker threats such as phishing, hacker attacks, as well as when they can steal your credit card information, hack your accounts and so on, that's why there are so many danger in social media."
8. Digital environment not adapted for people with disabilities - low accessibility standard of websites	Person with disability_blind, 21 years old: "One of the most unsafe things for me personally, from my point of view, is that I can't see a photo and I can't look at a person, it's very important. It is very difficult to get the information you need only from what people write. Maybe someone will ask me for help, who does not need it at all. By the way, I have lost my desire in this direction, because I don't know what kind of person is asking me, who are they, I can't see an elementary photo, I can't look at the photos to somehow understand that someone really needs help".
9. Bullying in the online space	Member of the LGBTQ+ community, 20 years old: "Bullying is such a topic... Yes, I experienced it from my older classmates. Because of the LGBT issue, of course, the way I dress, and so on. Also, there were questions about who I was hanging out with and so on. It doesn't matter to pay attention to it, it's probably better to ignore it.."
10. Threats for expressing a different opinion	Focus group participant, 20 years old: "I had an experience with a parallel classmate who threatened to beat me. ..I just made a joke, and he didn't like my joke."

11. Threats related to Artificial Intelligence (AI)	Focus group participant, 21 years old: "After the recent news in this direction, new threats have appeared - they can take your face and use artificial intelligence to do something. According to this logic, you should not publish anything personal anywhere. Thanks to this artificial intelligence, you can find yourself on a video or a post that you can't imagine at all and say or do something like that"... (Deefake).
12. Lack of awareness of common responsibility from users and a superficial attitude towards the threats in the digital space	Focus group participant, 25 years old: "For example, if someone hacked my account on any platform, they also could find my job by email, then go to my job page... I mean, it's a very big chain, and this security means that everyone works from a computer... this security, it's not just ours and it's personal."
13. High risk of spreading disinformation and fake news	Ethnic Minority_Armenian, 25 years old: "There is disinformation. For example, some facts happened, but someone may use these situations for other purposes."
14. Discrimination and lack of user protection mechanisms	<p>Ethnic minority_Avar_Lek, 19 years old: "Sometimes they can tell me about my name and surname that you are not Georgian, you are Armenian, and so on. That is the main argument. I don't know why, but that is how they most often express their displeasure towards me".</p> <p>A member of the LGBTQ+ community, 25 years old: "Yes, there have been many times on Facebook, they have insulted me because of my dress, for example - what do you look like, are you a girl or are you a boy and so on... more often it is about my appearance."</p> <p>Ethnic minority_Armenian, 25 years old: "I remember some Armenophobic statuses. There was something about me, now I remember exactly, I won in some competition of the conference, and someone there wrote - there were no Georgians? Why did Armenians win?"</p>

15. Artificially creating virtual reality using trolls and bots and influencing people's views	Ethnic minority_Avar Lek, 19 years old: "The main threat is that some virtual reality is created at some point. We think those 2-3 posts we see in our feed are the opinion of the masses. This very real perception of virtual reality is my main problem today. I have this problem, even though I understand that there is a problem, I still have this problem that even the comments affect your psychological state, for example... For example, in the case of Facebook, they create an artificial reality with bots and trolls, which for me is a real problem that needs to be solved."
16. Weak legal framework and response mechanisms	Focus group participant, 21 years old: "My relative had a case where they made an account with her name and surname, put someone's photos on it, and when she applied to the police, it was pointless, because they couldn't do anything."
17. The risk of unauthorized access to personal data placed in digital space by the state	Ethnic minority_Avar Lek, 19 years old: "The problem in our case is surveillance by the state using social networks." The state manages to obtain the personal information of people in the digital space, very illegally or legally, without asking a person. This is a problem with that social network because it is not well protected, obviously because it can be accessed by a third party. Therefore, let's say that these social networks should take responsibility for their users and their security".
18. The risk of sharing information about user behavior between different digital platforms	Focus group participant, 21 years old: "In my opinion, when you do something and even think of something and enter any social network and all the posts are about it. As long as it is like that, nothing can make you feel safe and secure."

Unsecured Platforms	Experiences of Young People
1. Viber	Person with disability_blind, 21 years old: "Viber is the most vulnerable in my opinion because very often strangers write to you and may even call you. They can get access to your phone if you click on some link and so on. That's why I don't like Viber, and I always delete."
2. Facebook	Person with disability _ wheelchair user, 16 years old: "Facebook is mostly full of various phishing links, that's why you can never be safe. I never click links on Facebook. Many times, I had a case where someone hacked my friend's Facebook and then they sent me links, but I knew that my friend would not send me these links".
3. Online application with phone number recognition database	Ethnic minority_Avar Lek, 19 years old: "Phone numbers database" You probably know that this application exists, and a friend told me that having this application on the phone is not safe, because the State Security Service controls this database."
4. Instagram and TikTok	Member of the LGBTQ+ community_20 years old: "Instagram, you can't copy a photo on Instagram, but you can take a screenshot. On TikTok, all are under risk."
5. Sites with RU domain - Russian sites	Person with disability_blind, 21 years old: "I don't trust any site with RU domain, i.e. Russian sites. I don't even risk logging in because I think I'll get a virus or they'll have access to my information."

Feelings and Emotions Caused by Digital Threats	Emotional Experiences of Young People
<p>Anger</p> <p>Unpleasant feelings</p>	<p>Ethnic minority_Avar Lek, 19 years old: "I feel so unpleasant when they emphasize my name and surname and ethnic origin and think that because of my ethnicity, I have no right to say anything. In that situation, I just feel bad because I don't understand what to say to that person; I don't have an argument.."</p>
<p>Fear</p> <p>Panic</p> <p>Pain</p> <p>Crying</p>	<p>Focus group participant, 18 years old: "My friend had a case on social networks that she was harassed by a very bad person. For six months, ten of us cried every day because of it, and we couldn't get rid of this person. This person threatened us, and there was even talk about suicide. Both my friend and us were in great danger. At first, my friend responded to the message, and at the beginning, it was a very normal correspondence, but at some stage, we realized that it was not safe. This person knew the address, phone numbers, knew everything, and was already scaring my friend with everything. It was such a situation that not only my friend but we were all at a big risk. We were all very worried about it. I took it as my personal experience because I was just as scared as my friend was".</p>
<p>A sense of injustice</p> <p>Feeling insecure</p>	<p>Focus group participant, 18 years old: "I had a feeling of injustice because I was being blamed for something I didn't do, and I couldn't prove it. If it happened to me now, I would do something, but before, I was so vulnerable and such a child that I didn't know what to do. I just sat and watched how the situation was developing, and I had a feeling of injustice."</p>
<p>The feeling of weakness</p> <p>Emotional imprinting in the mind</p>	<p>Focus group participant, 18 years old: "I had health problems when I was a schoolchild, that's why I didn't go to school, and at that time I heard that one of my friends was sharing our personal correspondence in his friend's chat, and then they discussed all this. When I found out about it, I was in a very difficult situation emotionally because I couldn't physically go to school. I was not very young, and it affected me so well that it was emotionally imprinted in my mind".</p>

Chapter 4

Educational Function of Digital Space

15 to 25-year-old youngsters who participated in the research consider receiving information and using it for educational purposes as one of the most important functions of the digital space. According to young people, it is possible to find almost any type of information in the digital space, and it is easy to get an education in different areas, although the main challenge is trustworthiness. Respondents say that any digital platform can have an educational function, but the most important thing is that users can identify and filter correct and verified information. The skills with which they can identify trustworthy digital spaces are based mainly on experience and not on any fundamental theoretical knowledge. When talking about reliability features, some respondents focus on technical details, such as the popularity of a particular website or channel, the number of subscribers, constant updating, and content views. The content shared should exhibit thematic consistency and be authored by individuals possessing adequate qualifications. Notably, one of the respondents underscores the significance of attending to safety parameters and adhering to accessibility standards. This is particularly significant because incorporating accessibility standards within web platforms plays a pivotal role in enhancing the inclusivity of the digital landscape for individuals with disabilities.

“

If accessibility standards are met on a website, it means it's done by responsible people. If there is this privacy policy at the bottom, that link may not open and in that case it is not reliable and the information obtained from this site may not be relevant for me. I pay a lot of attention to it because a lot of information may be related to employment and you may find yourself in a very bad situation, it is very important to pay attention to it.

Person with disabilities, 21 years old

”

When characterizing educational digital spaces, young people participating in the research also pay attention to who recommends a particular website or channel and only then observe the quality thematically. For example, if the topic is about digital technologies, the content itself must be provided with high quality; otherwise, there is a reason for suspicion. If

the topic is medical, young people observe who is providing the information, whether they are a doctor, what competencies and regalia they have, and so on. After receiving information from a new channel, young people think that this information should be verified through several sources. If the credibility is confirmed, this already provides the basis for trusting the channel as a whole.

“

For example, now my friend and I are members of one of the channels on TikTok; we are interns or something like that; we help the admin of the channel in posting some videos related to sexual education. The criteria we use to post these videos is that we always talk about the same topic on our channel. If someone goes to our page, they will understand that this is a reliable page because we have specified the sources, we are always talking about the same topic; we have specified dates, numbers, studies, sites as a source. From a lot of details, you can understand whether a certain page is reliable or not, and whether it all has a certain appearance.

Focus group participant, 18 years old

”

The digital platforms most often used by young research respondents are **YouTube, academic scientific online bases linked to official institutions**, some **Facebook and Instagram pages** or groups, some **TikTok channels**, and **Google**. YouTube has been mentioned many times, where they have clear criteria to determine credibility; for example, the number of views of a video is one of the most important and apparent criteria. Besides, it should be noted that TikTok has been cited as one of the better sources for education, especially since TikTok added a new update and made it possible to stream Steam videos.

“

*As it used to be “Googling” something, then I used to search it on **YouTube** - how to do something, but now I can search it on **TikTok** if it's something elementary, and I know that the answer to a similar topic will be on TikTok. I sometimes divide the platforms according to the information I'm looking for; for example, I look for one type of information on YouTube and search for other things on **Google**. Sometimes I know something, that there will definitely be an answer to it in some Facebook group, or a question will be written, and I will definitely find the answer, so I search for it in the Facebook group. I don't have only one social network for this, I trust all social networks, but I don't trust all users, I don't trust everyone who posts, and I sort all this myself.*

Focus group participant, 18 years old

”

Chapter 5

Media Literacy

In the framework of the research several questions related to finding out what information young people had about safety of digital spaces, from which sources they got this information and whether they generally considered media literacy as necessary for young people. The questions were also about finding out how they would like to receive information and knowledge about safety digital spaces in the future. In the table below, the views of the young people participating in the research on this topic are described in detail.

Topic	Results	Quotes
<p>Prior knowledge in terms of media literacy</p>	<p>The results of the research showed that young people do not have significant or fundamental knowledge in terms of media literacy.</p> <p>Their knowledge is mostly based on their experiences on digital platforms, and they have difficulty specifying sources from which they get this type of information.</p> <p>Only few of the research participants so far have had the experience of getting this type of knowledge theoretically, out of their own interest.</p> <p>The information that young people possess is mostly related to the protection of personal data, accounts and cyber security.</p>	<p>Member of the LGBTQ+ community, 25 years old: "I know there are these types of videos on YouTube, but I haven't watched them. I had to open the virus link once and learned from my own experience."</p> <p>Focus group participant, 24 years old: "If you don't search it at least once, it's very rare that you get such information. I mostly try to cope with such situations on my own. I didn't get any education with videos and training."</p>

The source of information

Two respondents remembered that their school held cybersecurity meetings, where they acquired some information.

One of the research participants was interested in programming and was actively exposed to cybersecurity topics on various platforms, mainly on YouTube.

Two research participants had training in terms of disinformation and media literacy.

Other young people participating in the research emphasize YouTube as the primary source of information.

Focus group participant, 17 years old: I didn't find it personally, but there was a period when special people came to school and held educational meetings in the direction of cybersecurity. I remember well, I was somewhere in tenth or eleventh grade at that time".

Ethnic minority_Armenian, 25 years old: "I have completed two training sessions regarding disinformation. "One was a Rondeli Foundation program, which was for ethnic minorities, focused on raising awareness... and I was at another camp by CENN, which also had different topics, and one of the sessions was on media literacy."

Person with disability_blind, 21 years old: "IREX had these media literacy training and I got involved there. It was very interesting, by the way, then we conducted it ourselves. It was training of trainers, and by the way, I also have a certificate and can conduct training on this topic."

Person with disability_wheelchair user, 16 years old: "Computers and programming have always been my hobby, so I was always interested in cyber space and always learning things... Because of this knowledge, it became very easy to avoid all dangers in cyberspace. This kind of stuff has mostly always come from social media. For example, I use YouTube and there are a lot of free things about cyber security".

The need for this type of knowledge in the future

All research respondents understand and agree on the need for knowledge regarding media literacy.

Young people note that currently, the methods of defense they use in the digital space are weak, which is caused by the lack of education.

For some participants, the feeling of insecurity in the digital space convinces them of the need for this type of knowledge.

A young person representing an ethnic minority community believes that in the future, the importance of this type of information will be even greater for future generations, and they must face the increased opportunities and threats of the digital space with appropriate knowledge.

Focus group participant, 22 years old: "I don't have exact information about how these social networks are managed in the internal system, and it causes discomfort. That's why I have this attitude... As for self-defense, I can say that I defend myself weakly, although I don't have more opportunities in terms of knowledge."

Ethnic minority_Avar Lek, 19 years old: "I think that it is very important because as time passes and something, for example, now that my brother is growing up, this stage of social networks will also enter his life and it will obviously take a bigger role; it can be seen, that is a trend. Therefore, knowing how to deal with, let's say, how to protect yourself there will be very important. Or, how to protect his personal data, his social network from being hacked, etc. A person should know this, and now I can't tell him; I can't teach him because I don't know it myself."

Preferred ways of acquiring knowledge

The youngsters aged 15-25 participating in the research emphasize a number of methods and ways in which the users of digital spaces can acquire appropriate knowledge in the direction of cyber security and media literacy in the future:

Informational video blogs should be posted on social networks that people use;

Create training and video blogs for parents who do not know the dangers of the digital space for their children. Parents' awareness should be raised.

Some time should be devoted to teaching digital safety (media literacy) issues in the school from the fifth grade.

Sponsored videos should be placed on the social network, which will appear on everyone's account, regardless of whether a person is interested in this topic and searches for it or not.

When registering on digital platforms, initial information about defense functions should be provided to all users through small tips.

Create paid and free training about real situations in the digital space with practical advice - how to avoid unknown users' interaction, whether to reply or not, how to react to feedback on our posts, etc.

Courses of lectures and seminars should be planned, where, along with theory, practical, simulated situations will be discussed.

To inform and raise the awareness of young people so that they understand the necessity of getting an education to protect themselves from the threats in the digital space.

It is possible to create a specific platform that will be directly focused on cybersecurity and media literacy issues.

Focus group participant, 18 years old: I think it would be very good if parents and even the previous generation of parents, who do not have much information in this matter. First of all, what dangers it contains and then how to protect yourself from these dangers, and it will be important to make such information more accessible to them. They don't know that their children could be on these platforms or what the dangers might be, and it's very important to educate them.

Person with disability blind, 21 years old: "I think that issues of media literacy should be taught at school. If we're studying human rights and so on, it's such an important topic today, and we're so often exposed to social media that media literacy is very important. Schoolchildren must know... I think it would be much more productive if it was a separate course."

Focus group participant, 18 years old: I think that in addition to schools and trainings, the social network where you register should also have some primary information, for example, you can delete your birthday or, I don't know, elementary "tips," let's say, during registration in the application itself, or in the form of a video, or something that people will pay attention to from the beginning."

Ethnic minority _ Avar Lek, 19 years old: "When my friends and I found out that Signal was a relatively safe space, it happened that we moved everything from Messenger there and our chats are created in Signal, and we write to each other there. This gives me a reason to say that if there is some relatively protected space, even safer, naturally, there will be a desire to go to it, and we will move there. That feeling of security is very important. Therefore, I think that we will follow what they call protected spaces".

Chapter 6

Future Perspectives of Digital Security

As a result of collecting the experiences and views of the research participants, it is possible to create a complex approach to how the security of the digital space can be increased and protected in the future. The respondents talk about what a more secure and comfortable digital environment would look like for them in the future. Each participant's vision in this direction is determined by their own experience. There are concurrence of opinions and differences between the participants' views. These differences are observed both between age categories and among members of ethnic minorities, persons with disabilities, and the LGBTQ+ community. In particular, while defining the future perspective of the digital space, we asked the research participants to talk about the specific criteria, as well as the measures and mechanisms that will allow stakeholders to create an ideal digital platform model for the 15- to 25-year-old youth. The main criteria include **privacy, personal data protection, security, space free from hate speech and discrimination, including ethnic, religious and other types of discrimination, freedom of expression, transparency and protection from cybercrimes.**

“

Where there is no offensive environment, where there is no discrimination, be it ethnic, religious or any other kind of discrimination and a person can express their opinion freely. And besides, there are high safety standards. Protected from cyber crimes...

Ethnic minority - Armenian, 25 years old

”

Notably, a significant difference between age categories can be observed regarding the protection of the digital space in the future. On the one hand, everyone points out that the digital space will never be completely protected from threats; however, the 21-25-year-olds participating in the research show a particularly skeptical attitude in this regard. They critically evaluate the future perspective of digital spaces. They don't talk much about specific criteria or measures to make digital spaces safer in the future because they don't believe in it. For example, one of the participants of the focus group, a 22-year-

old, believes that the only thing that can be done to increase the security of digital spaces in the future is to narrow them down more. She believes the solution is to create spaces with few users, and not everyone will have access to them.

“

If there will be a specific space where specific people will be, for example 500-600, and not global, it will be better.

Focus group participant, 22 years old.

”

Some 21-25-year-old youngsters realize that the future without digital spaces is unimaginable, and they will have to live with these spaces; however, they say they will never feel safe in this space. Some even consider minimizing the use of digital spaces and believe they can be used only in case of specific needs. For example, a 22-year-old respondent uses online platforms only to communicate with her mother abroad.

“

The only good thing about the social space is that you can contact other people abroad. I wouldn't have Instagram or Facebook if my mother wasn't abroad. It will be very difficult for a person to turn around and trust some social network.

Focus group participant, 22 years old.

”

Young people in the age group of 15-20 participating in the research evaluate the perspectives of future development of digital spaces more positively and have several opinions regarding the measures and mechanisms that will make these spaces better in the future. The first consideration they offer is the integration of defense mechanisms in digital spaces. Namely, putting all defense mechanisms characteristic to each application or digital platform together. The second consideration concerns informing users registered on digital platforms regarding security mechanisms. Some participants think that users should be provided with this information directly by a particular platform's official page and management. Most people do not know the mechanisms and functions of protecting their accounts or personal data in the digital spaces they use. The young people participating in the research consider the information the official website provides more reliable and effective. It is also possible to have a foreword

during registration in this space, informing users of the possible risks and ways to protect themselves from them.

As we mentioned above, when discussing the future of digital spaces, young people pay special attention to privacy and personal data protection. In this regard, two respondents should be mentioned: a person with a disability and a member of the LGBTQ+ community. A 21-year-old person with a disability believes that one of the important mechanisms to defend privacy, for instance, posting anonymously, lacks effectiveness because the administrator or moderator of that space can see the author of the posts. Therefore, she thinks it would be good if, in the future, there was a mechanism that would keep the post author anonymous, even for the group admins, when someone secretly decides to leave a comment in the group. Regarding security, in her opinion, it would also be good to add functions such as “fingerprint” and “face recognition” to digital platforms in the authentication process. In this case, strangers cannot access the other person’s account even if they have access to their phone.

“

I think it is very important if we add some functions; for example, when I open Facebook with my phone, it opens with Face recognition or fingerprint, something that only I have and no one else has access to.” It is very important in my opinion. First of all, this one is very convenient because you can unlock it with Face recognition or fingerprint, because even if someone takes your phone, they still won’t be able to unlock it.

Person with disability_blind, 21 years old

”

The second participant of the research, a 25-year-old member of the LGBTQ+ community, would like to disable or cancel the sharing function of closed groups of digital spaces in the future. It would further limit the removal of information from the group in order to protect privacy. Besides, in his opinion, it would be good for groups to have an authentication function so that unauthorized persons cannot gain access to the information in the closed space with fake accounts.

“

I would turn off the sharing feature from the group to keep all of this out of the group, when a group is a closed space, that means nothing should go out, so I turned it off. Also, I would add an authentication function to add real people.

LGBTQ+ community member, 25 years old

”

Since the 15-25-year-olds participating in the research represent the generation that had access to digital spaces from a young age, based on their own experience, they definitely consider the presence of age restrictions on digital platforms and a mechanism for filtering age-appropriate information. Some of the participants share the idea of the necessity of age restriction; however, the other part does not agree with the imposition of such a restriction and believes there are many ways to avoid this restriction. Therefore, they consider it necessary for digital platforms to have functions that filter information based on age, set hourly limits, or some other mechanism to control this issue.

When young people talk about the future of digital security, they directly consider the owners of digital platforms as important actors in this process and talk about their responsibility. They focus on the question of the good faith of the owners of digital spaces regarding the use of the personal information of their users for other purposes. The transparency of this process and the consent of users to the use of personal information by the platform is mentioned as an important aspect of safe digital spaces in the future. Young people are concerned that their personal information may be transferred from online networks to third parties without their permission and would like effective mechanisms to control this in the future.

“

It is also important that the person who is the head of these social networks feels responsible for their users and protects them. I understand that absolute protection from state intervention will be difficult and it may be necessary in special cases, but the necessity must be justified.

Ethnic minority_Avar Lek, 19 years old

”

“

Transparency isn't just about knowing who's accessing your account, it's about knowing how my information is being used on a digital platform and having full control over it.

Focus group participant, 20 years old

”

According to the young people participating in the research, the involvement of users of digital spaces and their role in creating safe digital spaces of the future is essential. They consider that one thing is the issue of the functioning of online spaces from the point of view of security, and the other is the responsibility, awareness, and behavior in the virtual space. Some participants believe that the main threats in the digital space are created by people, which no platform can regulate and eliminate if there is no direct will of users in the process. Digital spaces can inform them of common threats and defense mechanisms against them, but people must share a joint responsibility in the digital space.

“

In general, the understanding should be formed that what happens on the social network is not separated from real life, and real laws apply here, and other users are also real people.

Focus group participant, 20 years old

”

Chapter 7

Asynchronous Focus Group Discussion in the Social Network - Data Analysis

7.1 Safe Digital Space - Definition of the Term, Platforms and Criteria

An asynchronous focus group discussion with young people on social networks started with the definition of the term - "safe digital space." They had to write all the words that came to mind in the post's comments around this term. As the results showed, they mainly describe the safe digital space with the following words: Confidentiality, personal data protection, security defense mechanisms, hate speech free space, trustworthy space, freedom of expression, protection of privacy.



The participants agree that all the listed criteria are important; however, the most important among them are confidentiality, personal data protection, and security defense mechanisms.

“

Participant of asynchronous discussion: “I don't know how correct it is, but for me a safe digital space is associated with having 100% privacy protection.”

Participant of asynchronous discussion: “A safe space for me is associated with a place where I expect my data to be safe.”

Participant of asynchronous discussion: “The fact that no one can use your private conversation, correspondence as a compromise against your will.”

”

Some participants in the discussion also noted that when talking about the criteria of safe digital spaces, the existence of a regulatory mechanism and inclusiveness also play an important role.



Diagram N4. - Criteria of Safe Digital Space - Poll results

Most of the young people who were members of the asynchronous discussion group “Collaboration” found it difficult to name a specific platform where they feel safe and which meets the criteria they listed. In their opinion, there are no completely safe and secure digital spaces. The list of these platforms, which some of them named, is available on Diagram N5.

Among the named platforms, Signal and Telegram are considered the most secure.

As one young participant in the discussion points out, Signal is characterized by high mechanisms of personal data protection, while another participant prefers Telegram and likes that it does not oblige its users to disclose personal information to other people.



Diagram N5. - The most secure digital platforms



“And Telegram is convenient because it is not necessary to share a personal phone number to communicate with strangers. Only the user’s name is enough, which can be any comfortable and pleasant word for me”.



“Signal, for example, because if a person registers with my number on any other device, the signal will start using the platform from scratch and all old correspondence, files, and voice messages will disappear. That is, the information is only in my device and does not go anywhere”.

During the discussion, we asked the group members in one of the posts to mark all the platforms on which they have an account through a poll. As it turned out, most of them have accounts on such digital platforms as: **Facebook, Instagram, Telegram, YouTube, and Mail**. A smaller number of discussion participants account for the following platforms: **TikTok, WhatsApp, and Viber**. And the smallest number of young people participating in the research were registered on **Twitter and Signal**.

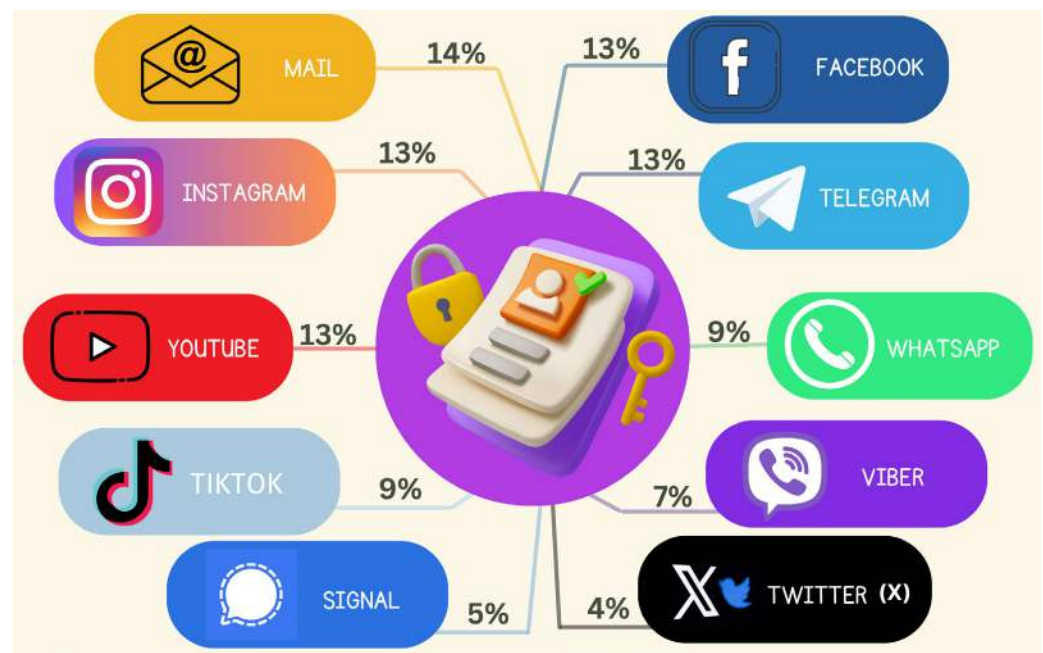


Diagram N6 - Most usable platforms for young people

This question had two goals, on the one hand, it was supposed to identify the digital platforms on which the group members were registered and then to classify which of the named platforms the young people consider safe and which are dangerous. They considered Telegram, Signal, and WhatsApp to be the safest, Mail, Twitter, and YouTube were the least safe, and young people of the group considered Facebook, Instagram, and TikTok the most dangerous.

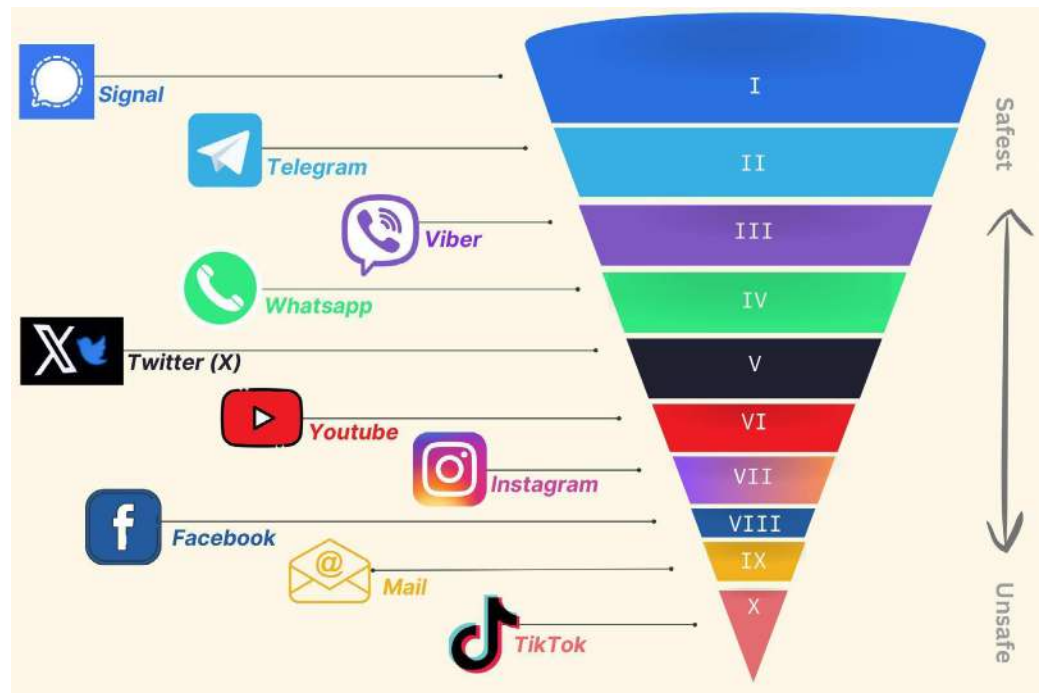


Diagram N 7. The Safest and Unsafe Online Platforms

7.2 Security Functions, Mechanisms, Criteria

For young people participating in asynchronous discussions, safety in the digital space is associated with an environment of confidentiality, and privacy protection, which is free from hate speech. Also, they consider controlling cyberbullying and age control as necessary measures to feel comfortable and safe in the digital space.

“
 Maximum secure platforms in the online space, should control the presence of children in inappropriate spaces and also the protection of the personal rights of each individual.
 Participant in asynchronous discussion
 ”

The answers revealed that the protection of children’s rights is important for the participants of the discussion, and for this, they consider the restriction of 18+ content and the control of pedophile content as relevant measures.

“
First of all, protection from bullying and filtering of comments or posts containing similar content. Age control, as we know, many minors use the online space, therefore there are some things that should not be available for some age category. Of course, this list is not complete, but it will help us create a more comfortable and safe space.
 ”

Participant of asynchronous discussion



Diagram N 8. - Specific Defense Mechanisms in the Digital Space

Young people participating in the discussion also offer more specific defense mechanisms. It is important for them to feel safe during group interaction in the digital space, and this can be achieved by developing group protection mechanisms on online platforms. First of all, it should be noted that closed groups are more acceptable for group discussions, where comments and posts are filtered, the moderator is actively involved in the discussion process and filters fake accounts in the group. Also, using the anonymity feature when active in groups is an important defense mechanism for some respondents. In addition, participants name specific technical functions.

“
 For me personally, safe digital space is associated with double protection when you receive a code on your mobile phone or email, and the secret conversation function is also convenient, as is the private profile function.
 ”

Participant of asynchronous discussion

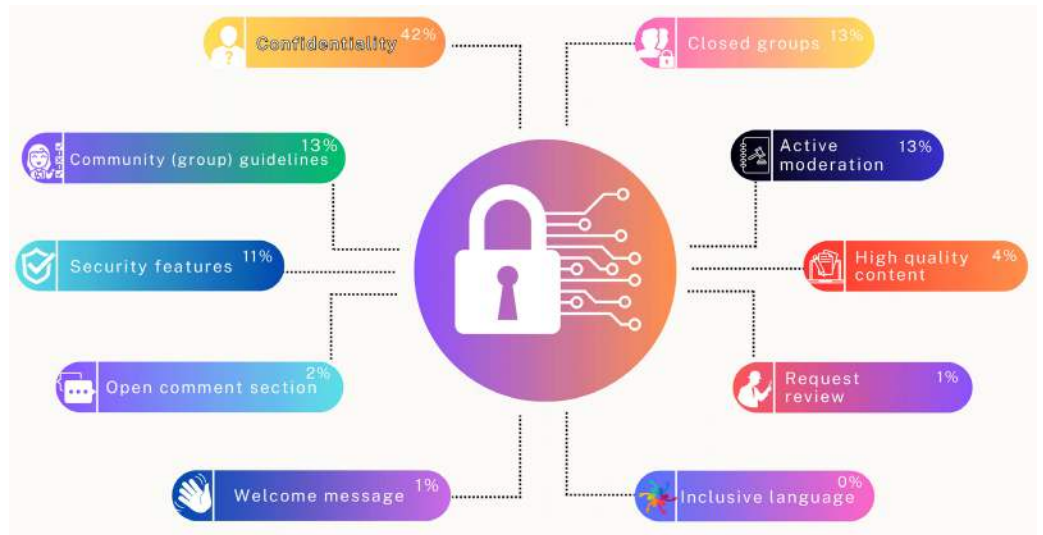


Diagram N9. Forms and Functions for Securing Digital Spaces

In the characterization of specific platforms, specific features were also highlighted, for example, Signal and Telegram were considered secure platforms due to the features through which the user remains confidential and correspondence is protected at a high level.

The young people involved in the discussion are skeptical about the existence of a perfectly protected, safe digital space in the future. They believe that they can never feel completely safe on online platforms, even with the use of several defense mechanisms at the same time. However, some specific criteria are formulated on the question of what mechanisms should be used to create a safe and secure digital space for young people.

The presence of security protection mechanisms in the digital space is an important factor for them, as well as age restrictions and user customization. In addition, the ideal digital spaces of the future are expected by young people to be constantly updated based on user opinion research.



Diagram N 10. - Criteria for the Digital Safe Space

7.3 Threats, Risks, Challenges in the Digital Space



Young people identify cyberstalking, cyberbullying, and scammers as the main threats in the digital space. Ignoring cases of bullying in the digital space creates discomfort for young people involved in the discussion, and in their opinion, activating the internal regulation mechanisms of digital platforms in this direction will be the first step toward prevention.

Diagram N 11. - Threats in the Digital Space

“
A dangerous social network involves weak security (log in) insecure chat as well as ignoring bullying comments and anyone registering or joining a group.
 Participant of asynchronous discussion
 ”



GIFs Expressing Respondents' Emotions Regarding Digital Threats

According to the current reality, young people often feel completely unsafe in digital spaces. We asked discussion participants to describe unsafe digital spaces and their emotions when they meet such spaces. They shared their emotional experiences with us using gifs. Young people believe that their personal data is not protected on any digital platform they register and share any information with because, under some circumstances, the platforms may release the collected personal information. During the discussion, the young people also remembered the cases when they felt the most unsafe and insecure in the digital space.

- “There was such a case when I was doing some work and during a break I opened TikTok and the first video was exactly what I was doing.”
- “And again, when I was talking about dogs, and then soon I came across the video on Tiktok again and again.”
- “Yes, I had a similar case and I thought that the device was clearly listening. In other words, we are deciphered.”
- “I have had it and, by the way, very often. A case like this sometimes makes me think and doubt. I believe that it cannot be a simple coincidence.”

7.4 The Need for Cyber Security Education

Young people participating in asynchronous discussions consider it necessary to receive information about digital security in the future. Towards the end of the discussion, we asked them to name the preferred ways in which they would like to obtain this type of knowledge. The post listed several options, and participants could suggest their version in the comments. As it turned out, the majority of them consider training and the existence of a platform that would meet the security criteria as a way to get information in the direction of media literacy. A cycle of lectures was also named as a possible form of receiving information.



Diagram N 12. - Ways to Get Information in the Direction of Digital Security

Since the members of the group actively supported the existence of a secure digital platform and named it as the preferred version of receiving information about digital security, in the last question, we asked them to offer ideas on what they would call an ideal safe and comfortable platform in the future. The list of suggested names:

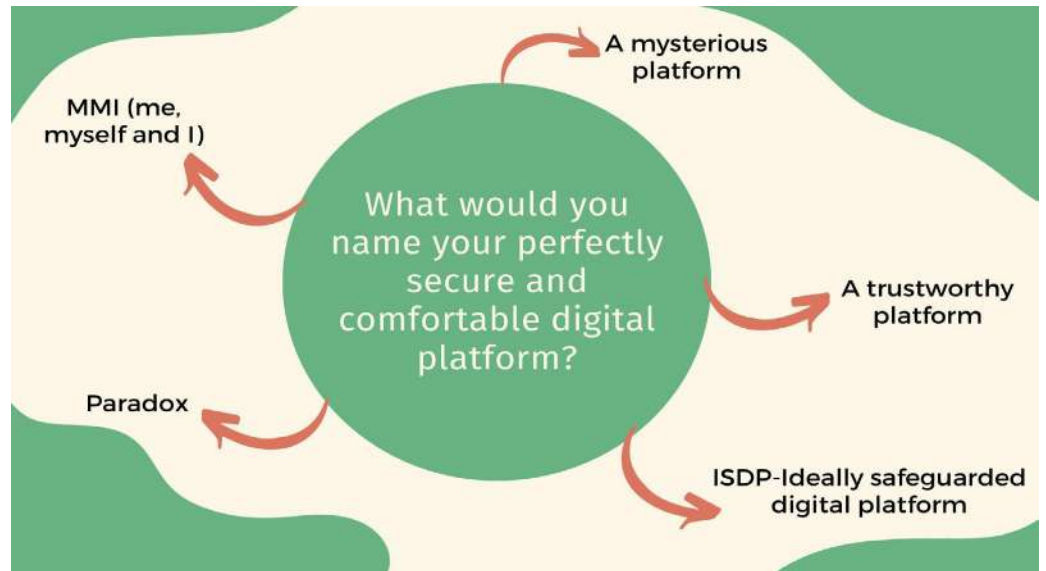


Diagram N 13. - What would you call a perfectly protected digital platform for you?

05 CONCLUSION

Based on the research results, one can argue that digital spaces play a significant role in the social life of 15-25-year-old youngsters living in Georgia. Their experiences with digital spaces show that young people actively use digital platforms and various forms of online interaction in their daily lives. For them, learning, entertainment, work, formal and informal communication are impossible without digital activity. One of the most important functions of digital spaces for young people is communication. They actively use digital platforms in their everyday life for **formal and informal communication**. Besides communication, online spaces for young people have an informative and educational function because they receive **daily information** digitally, and online platforms play an important role in the process of receiving **education**. The experience of the young people involved in the research shows that they use various online platforms for their educational needs, where they can find competent and reliable information.

In the process of getting information, the biggest challenge is determining the received information's **reliability**. Young people already have experiential skills to **filter the information** they receive and sort it through verification for reliability and appropriateness. It is also essential for young people to keep **private correspondence** safe as they use digital platforms for both informal and formal communication. Young people consider group interaction as one of the forms of online communication, which is useful for them in many cases. Therefore, young people choose spaces for group discussions that are as **secure and private** as possible while being **controlled by a moderator**, and the community gathered in the group is acceptable.

Young people use digital platforms with different frequencies and different purposes every day. Therefore, the threats and risks that exist in the digital space create significant challenges for them. In order to connect a large part of their activities and daily lives to digital platforms, young people have to share some of their **personal data** with the online platforms they have an account on. They see this as one of the most important threats and note that improving **security protection mechanisms** is especially necessary in this direction. According to young people, even accessing the personal data of one individual may lead to a chain of threats to other individuals and institutions













connected to that person. This puts users of digital platforms at risk of **cyber attacks, scammers**, and other **cyber crimes**. However, it was found that there are more risks in the direction of group discussions, as engaging in group discussions involves interacting with many unknown users. Based on the experiences of young people, we can say that it is often dangerous - there are risks of **unpleasant communication, cyber-attacks, discrimination**, and **cyber-bullying**. In this process, the biggest challenge is determining the received information's reliability. Young people already have experiential skills to **filter the information** they receive and sort it through verification for reliability and appropriateness.

Since young people's daily activities are significantly related to digital spaces, and they have to deal with the risks and dangers that exist in the digital world every day, they consider **media literacy** very important. Most respondents do not have theoretical knowledge or education from formal sources about digital security. Their knowledge in this direction is mainly based on personal experiences. That is why all respondents point out that it is necessary for all people to have at least some level of education about digital security, and in the modern world, everyone needs media literacy. Some respondents see media literacy as an important component of the **school curriculum** in the future.

Young people believe that the role of digital platforms in human social life will increase even more in the future, and the risks will increase accordingly. Some respondents are skeptical about the existence of perfectly protected and safe digital spaces in the future. For them, the feeling of security in the digital space brings more narrowness, closedness, and confinement, where they only communicate with close people, share very little personal information, and communicate only without important information. Some of the respondents believe that the improvement in the existing security mechanisms, as well as the creation and development of new ones, would allow the creation of comfortable and protected digital spaces. In addition, the future safety of young people in the digital space is also related to legislative-level control, as they believe that the existing legal framework cannot fully respond to real cyber threats.

06 RECOMMENDATIONS

Type of recommendation	For stakeholders, Organizations and/or interested actors	For Legislators	For tech platforms and their owners
Organizations working on cyber security issues and/or stakeholders of the topic should plan and implement an information campaign to provide the right information to young people on the importance of the topic.	✓		
Organizations working on media literacy issues and/or interested actors in the topic should prepare training and/or lecture courses primarily to raise the awareness of minor users of digital spaces about the risks and threats in the online space.	✓		
Interested actors in providing educational information to young people in online spaces should be guided by the criteria listed in their characterization of such spaces.	✓		
On the part of relevant institutions and stakeholders, digital security issues should be discussed at the legislative level, and the existing legislative base should be expanded in this direction.	✓	✓	
Educational institutions and relevant state structures should ensure the inclusion of media literacy and cyber security issues (subject) in the educational curriculum.		✓	
At the very first stage of registration on the digital platform, users should be informed about the risks and threats in this space;			✓
Expand privacy protection functions and mechanisms on digital platforms. Among them, one of the important mechanisms can be that when someone talks about sensitive topics during a group discussion, even the group admin or moderator does not have the opportunity to see the post's author;			✓

<p>Create specific rules for users registered on these digital platforms;</p>		
<p>Discrimination and hate speech should be controlled on the platforms, and freedom of expression should be protected.</p>		
<p>For young people, it is essential for the digital platform to have a privacy protection function when talking about sensitive topics; even the administrator or moderator of that space will not know the identity of the author of the post.</p>		
<p>Establish age control on the platforms and the content posted there.</p>		
<p>Owners of already existing digital spaces and/or parties interested in creating a safe digital platform in the future should ensure the development and improvement of accessibility standards of websites on these platforms, creating an environment adapted for people with disabilities.</p>		
<p>Owners of existing digital spaces and/or parties interested in creating a secure digital platform in the future should consider young people's opinions about combining the protection functions of other digital platforms to create a complex defense mechanism against digital threats.</p>		
<p>Owners of existing digital spaces and/or parties interested in creating a safe digital platform in the future should consider young people's view of social networks as a kind of narrowness. (The future of safe digital spaces for young people is directly related to the small number of users on it).</p>		
<p>Owners of existing digital spaces and/or parties interested in creating a secure digital platform in the future should inform users when they need to transfer their data to third parties (including the state).</p>		

07 APPENDIX

List of charts

1. Diagram N1 - Priority Functions of Digital Spaces
2. Diagram N2 - Functions of Digital Platforms According to Age Categories
3. Diagram N3 - Safe Digital Space - Definition of the Term
4. Diagram N4 - Criteria of Safe Digital Space
5. Diagram N5 - The most secure digital platforms
6. Diagram N6 - Most usable platforms for young people
7. Diagram N7 The Safest and Unsafe Online Platforms
8. Diagram N8 - Specific Defense Mechanisms in the Digital Space
9. Diagram N9 - Forms and Functions for Securing Digital Spaces
10. Diagram N10 - Criteria for the Digital Safe Space
11. Diagram N11 - Threats in the Digital Space
12. Diagram N 12 - Ways to Get Information in the Direction of Digital Security
13. Diagram N 13 - What would you call a perfectly protected digital platform for you?
14. GIFs Expressing Respondents' Emotions Regarding Digital Threats

List of tables

1. Table N1 - Functional Value of Digital Platforms for Young People
2. Table N2 - Safe and Secure Digital Spaces for Young People
3. Table N3 - Threats, Risks, Platforms, Emotional Experiences
4. Table N4 - Unsecured Platforms
5. Table N5 - Feelings and Emotions Caused by Digital Threats
6. Table N6 - Media Literacy

Research tools

1. Questionnaire for in-depth interviews
2. Questionnaire for focus groups
3. Questionnaire-guideline - asynchronous focus group discussion in the social media