



# Digital Security Among Palestinian Youth:

*A Study on Threats and Challenges  
in Light of the War on Gaza*

*(West Bank and Jerusalem)*

August 2024

7amleh- the Arab Center for the Advancement of Social Media

**Digital Security Among Palestinian Youth: A Study on Threats and Challenges in Light of the War on Gaza**

Analytical Survey Study (West Bank and Jerusalem)

Author: Dr. Saeed Abu Ma'ala

Edited by: Inas Khatib

Focus group coordination: Sura Abu al-Rub

Project coordinator: Mahdi Kurzum

Survey Execution: Mina Analytics

Design: Amal Shoufany

Translated by: DarLaila Publishing

This version is licensed under the following International License: Attribution-NonCommercial-NoDerivs 4.0 International

To view a copy of the license, please visit the following link:

<https://creativecommons.org/licenses/by-nc-nd/4.0>

Contact Us:

info@7amleh.org | [www.7amleh.org](http://www.7amleh.org)

Tel: +972 (0)774020670

Find us on Social Media: **7amleh**



# Table of Contents

<b>Executive Summary .....</b>	<b>4</b>
<b>Chapter One .....</b>	<b>6</b>
Introduction .....	6
<b>Chapter Two .....</b>	<b>16</b>
Literature Review .....	16
<b>Part Three .....</b>	<b>19</b>
Research Methodology .....	19
<b>Chapter Four .....</b>	<b>48</b>
Analytical Study Results .....	48
Conclusions and Recommendations .....	49

## Executive Summary:

This study sheds light on the digital security landscape in the West Bank and Jerusalem by tracing the experiences of Palestinian youth aged 15-30. This study comes at an extremely sensitive, turbulent, and transformative stage. The war on the Gaza Strip prevented Gazans from being included in the study. To draw credible conclusions, the study used two methods of data collection: focus groups (5 groups with 35 participants) and field survey (a survey of 449 respondents), along with a literature review on digital security and digital rights.

The questionnaire contained 31 questions distributed into six axes: characteristics of respondents; characteristics of Internet use among respondents; knowledge of digital security and the extent of awareness of digital risks; digital attacks and violations and the extent of exposure to them; interrogation and investigation by security authorities (Israeli and Palestinian) for reasons related to digital activism; the impact of social media policies on the activism of Palestinian youth during the war on the Gaza Strip. Here are the indications concluded after analyzing the data from the survey and interviews:

- **86%** of respondents use the internet at home.
- **67%** of respondents spend at least 7 hours daily using the internet.
- Respondents use a wide range of applications and social networks, most notably **WhatsApp (95%), Facebook (91%), Instagram (78%), TikTok (71%), and Telegram (66.6%).**
- **68%** of respondents said they know or have heard about network-related electronic device spyware.
- The source of information of **47%** of those who know about spyware is derived from family or friends.
- **43%** of respondents have never changed their password.
- **56%** of respondents have security settings activated.
- **37%** of respondents do not accept friend requests from strangers, and the rest do so divergently.
- **42%** of respondents often or always share photos and personal matters online.
- **47%** of respondents are unaware of security programs.

- **66%** of respondents do not use security software.
- **59%** of respondents do not use any digital security software.
- **43%** of respondents ignore messages from anonymous sources.
- **30%** of respondents use GEO location.
- **20%** of respondents have been attacked or assaulted digitally.
- **42%** of respondents said they felt scared and anxious after the attack or assault.
- **74%** of respondents said they had been attacked or assaulted by individuals (55% were strangers and 19% were acquaintances.)
- **30%** of respondents resort to relevant authorities (police, digital experts) when exposed to a digital attack or assault.
- **50%** of respondents have been attacked or assaulted by identity theft.
- **55%** of respondents have been attacked or assaulted by harassment and cyber surveillance.
- **50%** of respondents were personally questioned or know someone who had been questioned and interrogated by the Israeli authorities.
- **38%** of respondents were personally questioned or knew someone who had been questioned and interrogated by the Palestinian security authorities.
- **39%** of respondents were pressured by social circles to delete their posts.
- **14%** of respondents were pressured by Israeli security sources to delete their posts.
- **60%** of respondents said they self-censor their digital activity.
- **50%** of respondents said that policies restricting publishing have reduced their digital activity.

Discussions with focus groups reflected a decline in Internet users' trust in official authorities) police (.The personal experience of being attacked or assaulted is the primary source of awareness regarding knowledge of digital security issues .All young participants view the Internet as an unsafe place ,given their personal and traumatic experience ,which requires them to educate themselves and their families without moving away from the Internet.

## Part One

### Introduction

Since the Internet entered the occupied Palestinian territories, Israel has imposed control and censorship over Palestinian digital rights and fought them in numerous ways. As researchers in this field have shown, Israeli practices confirm that land occupation and digital occupation cannot be separated. Palestinian activists are engaged in a multi-level struggle in digital spaces, both locally and globally, as they confront the practices of the Israeli occupation and the consequently complex geographical divisions and fragmentation of the Palestinian presence on the ground. These challenges are processes that form due to realities on the ground and in the digital space, in parallel and simultaneously. Researchers coined a new term for this landscape, *Cyber Colonialism*, considering the impossibility of separating the concepts of colonialism on the ground and colonialism in digital spaces.<sup>1</sup>

Just like the daily lives of Palestinians are subject to military occupation measures and permanent surveillance through the latest technology at military surveillance centers and checkpoints, the virtual space is also subject to collective surveillance policies using the latest technologies. In the Palestinian context, Israel controls and monitors any personal, public, or human rights content. Additionally, social media platforms, to a large extent, have been involved in, or complicit to, violations of Palestinian digital rights,<sup>2</sup> which increased after October 7th, 2023.

Since the start of the war on the Gaza Strip (October 2023), Palestinian youth have been going through a fateful stage in everything related to the Internet. Due to the growing policies of digital repression and their growing sense of insecurity considering these policies that violate their digital rights, Palestinian youth are stuck in a space that has become more dangerous than ever before. For example, network users are exposed to diverse types of digital attacks and violations originating from priers and *hackers*, such as *identity theft*, *cyber harassment*, *Cyberstalking*, or *spyware attacks* such as Pegasus, as well as the use of bots, phishing, and revenge pornography. These attacks differ in terms of the attackers' identity, the targets, the results, and their impact on victims, thus creating a digital environment that lacks the most basic elements of security.

---

1. Tawil-Souri, Helga & Aouragh, Miriyam. (2014). Intifada 3.0? Cyber colonialism and Palestinian resistance. *Arab Studies Journal*. Pp. 103-120.

2. Taha, Suhail. (2020). The Cyber Occupation of Palestine; Suppressing Digital Activism and Shrinking the Virtual Sphere. [Global Campus Arab World, Policy Briefs](#). Pp. 3-4.

A study conducted years ago by 7amleh<sup>3</sup> revealed that the digital security of Palestinian youth suffers from an "alarming institutional vacuum" in addition to social media allowing privacy compromise, which has created new challenges for users. Studies revealed that about 58% of youth are unaware of their digital rights, with more than 85% of them needing to know how to protect their privacy and personal data, and more than 93% of the respondents need to acquire digital protection skills for their mobile phones.

On the other hand, Palestinian youth increasingly feel that their relationship with the Internet has become solid and cannot stop, as they consider it a life parallel to their original lives. The Palestinian official statistics issued by the Palestinian Central Bureau of Statistics show a steady annual increase in the use of everything related to the infrastructure and technology of Internet connectivity, such as fixed lines and smart mobile devices. Statistics show that the expansion of fixed telecommunications network infrastructure coincided with the increase in the use of these associated services by households and institutions, particularly the Internet,<sup>4</sup> which means an increase in the number of users exposed to digital threats and attacks.

This disturbing duality, which deepened during the war on the Gaza Strip, reinforces the need to know the real state of digital security and the digital risks of using the Internet according to the experiences of Palestinian youth, which have become a worrying moment in their relationship with the Internet.

This study aims to extract tools to enhance the protection of digital rights among youth by providing up-to-date scientific data on the nature and characteristics of Palestinian youth's use of the Internet and reveal the nature of youth's knowledge of digital safety concepts and awareness of the digital risks that they may face. The study also aims to reveal the extent to which respondents are exposed to digital attacks and violations and illuminate the reality of interrogation and investigation by security authorities for reasons related to digital activism, and the impact of platform policies on the activity of Palestinian youth since the start of the war on the Gaza Strip in October 2023.

Furthermore, the study aims to identify the challenges, threats, and key opportunities available to Palestinian youth in the West Bank and East Jerusalem concerning protecting their digital rights. It also aims to empower youth and the institutions related to digital safety awareness, hoping to contribute to enhancing digital rights protection, engaging in strategic advocacy, and addressing violations of digital safety and security.

---

3. 7amleh Center. (2017, May). [The concept of digital safety among Palestinian youth, a survey.](#)

4. Palestinian Central Bureau of Statistics and Ministry of Telecommunication and Digital Economy. [Joint Information Statement.](#) Accessed: 16.3.2024.

## Part Two

### Literature review

#### The Internet and the birth of digital rights

Since the emergence, spread, and expansion of Internet use, there has been a debate over the impact, scope, and mechanism of the expansion of the information society. As a result, divergent opinions and different visions emerged regarding the future trends of the online information society.<sup>5</sup> In this regard, researchers and experts are divided into different teams. Some researchers are heralds of digital change and are optimistic about the possibilities the Internet provides. These researchers believe that the development of the Internet will significantly reduce the information gap between groups in society and reduce traditional class dissimilarities concerning the right to access information. On the other hand, there is a group of researchers that looks pessimistically to the reality of digital technology development, claiming that it reproduces the social and political complexities that exist on the ground, and reuses them online, creating a new type of favoritism, namely digital and information favoritism. According to the second team of researchers, social and political activism via the Internet often fails to integrate marginalized groups in society or groups that do not have political inclinations or a desire for political and social activity.<sup>6</sup> From a more moderate and objective point of view without being overly optimistic or pessimistic, digital technology has created a space that can adapt to and be influenced by existing social and political systems. At the same time, however, digital technology is changing traditional political stereotypes by shifting the balance of knowledge resources in political institutions. For example, digital technology reduces the cost of accessing and collecting information. This shift is in favor of small or marginalized political groups and the most vulnerable activists. Moreover, digital technology has created new and unconventional lifestyles and interests in societies. It has historically revolutionized the knowledge and information economy by shifting the balance of resources from investing in land and capital towards investing in digital skills, expertise, and informatics knowledge.<sup>7</sup>

---

5. Norris, Pippa” .(2001) .Understanding the Digital Divide “.In *Digital Divide :Civic Engagement, Information Poverty ,and the Internet Worldwide* .Pp .235-238 ,26 „Cambridge University Press.

6. Ibid

7. Norris, Pippa. (2001). [Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide](#). Pp. 26, 235-238. Cambridge University Press.



With the spread of the Internet worldwide, digital politics has become a domain that can potentially be used to strengthen national democracies that are struggling to empower their political systems. The spread of the Internet in civil society has contributed to strengthening the democratic process by improving communication mechanisms and the flow of information.<sup>8</sup> With the profound impact of digital development on social, political, and economic transformations, this development was bound to set off an intellectual and philosophical debate about the relationship of users with this newly born space, which revealed many challenges that expand in parallel with the growth of the digital society and the deep penetration of digital technology into the productive activity and daily lives of users, despite its positive change and impact. In the context of political and social activism in digital spaces, it must be said that the spread of digital technology has not only created new patterns of political and social participation and action but has also sparked a new debate regarding the political and civil rights of users about this new space. It was clear that the revolution brought about by digital technology changed all traditional concepts and systems, including the traditional discourse of human rights, leading to the emergence of new categories and concepts related to human rights and the emergence of the term digital rights.<sup>9</sup>

As digital technology has forever changed the ways and means of learning, working, and communicating, Kay Mathiesen argues that there is an urgent need to examine how concepts of human rights and the achievement of justice are reflected in digital environments.<sup>10</sup> Mathiesen believes there is an urgent need for a digital declaration of human rights, similar to the Universal Declaration of Human Rights. In addition, Mathiesen believes that considering technological development, it is necessary to build on existing human rights charters and treaties and review and study them to learn how to apply them in digital spaces, because digital development has created a special environment that differs from the environment we live in real life.<sup>11</sup>

Amid the rapid technological development in digital environments, the United Nations has begun to act to ensure respect for human rights in these environments by issuing general comments related to the Universal Declaration of Human Rights

8. Ibid, pp. 239-240.

9. Borjigin, Namulun. (2023). Systemic Dilemmas and Practical Responses of Digital Human Rights Theory in the Context of Smart Society: A Literature Review. [Advances in Education, Humanities and Social Science Research](#), 5(1). p. 461.

10. Mathiesen, Kay. (2014). Human Rights for the Digital Age. [Journal of Mass Media Ethics](#), 29(1). Pp. 2-18.

11. Ibid, p. 7.

to add provisions for specification and clarification in the context of specific rights. For example, in 2011, the Human Rights Committee issued General Comment No. 34 on Article 19 of the Universal Declaration of Human Rights on the rights to freedom of expression and access to information. General Comment No. 34 sets out the type of means that people are entitled to use to express and access to information, including oral and written language, sign language, and non-verbal expression such as images and artistic materials, including means of expression such as books, newspapers, pamphlets, posters, banners, and legal memoranda. It also includes all forms of audiovisual expressions and electronic and Internet-based means of expression.<sup>12</sup> The general comment on the right to privacy – the Universal Declaration of Human Rights, Article 17 – specifies that the collection and retention of private information and data on computers, databases, or any other devices, whether by public authorities or individuals and private entities, must be implemented by law.<sup>13</sup> Although these general comments are example of attempts to adapt international agreements, conventions to ensure the application of recognized human rights in digital environments, the complexities of digital technology and the specificity and rapid development of the digital environment often place these attempts to fall short, and make them unable to keep pace with the rapid progress and continuous change that has become characteristic of the digital environment.

The impact of these profound and ongoing changes in digital and virtual environments on fundamental human rights, such as the right to privacy and the right to freedom of expression, remains an open question. Although the Internet and related telecommunication technologies have created opportunities and areas that promote fundamental human rights – such as the right to free expression – they have simultaneously imposed new challenges, risks and threats to the same fundamental rights and imposed a new reality on the relationship of these rights to various issues, such as the concept of transparency. UNESCO's 2016 Privacy, Freedom of Expression and Transparency report notes that the right to privacy, defined in the report as "the right of users and individuals to maintain the privacy of their information and data on the Internet," is subject to continuous violations. On the one hand, there is a noticeable increase in the use of privacy-invading technologies, which have

---

12. UN Human Rights Committee (UNHRC). (2011, September 12). **General comment no. 34, Article 19: Freedoms of opinion and expression.** [CCPR/C/GC/34](#). Retrieved February 2, 2023

13. UN Human Rights Committee (UNHRC). (1988, April 8). [CCPR general comment no. 16: Article 17 \(right to privacy\).](#) **The right to respect of privacy, family, home and correspondence, and protection of honour and reputation.** Retrieved February 2, 2023

contributed to a gradual collapse in the traditional communal boundaries,<sup>14</sup> which were formed in the pre-digital age with classical concepts and tools, such as law, moral, and social norms, physical and technical barriers, and geographical barriers, resulting in violations of users' privacy boundaries on a global scale. On the other hand, due to the rise of the information economy, the control of users' data and privacy has become an extremely sensitive topic, which can affect individuals' dignity, independence, and freedom.<sup>15</sup>

This report highlights another critical issue related to investment in and abuse of the right to freedom of expression. The desire of different communication platforms to make the most of user data has led to the use of technologies that allow many avenues of expression, enabling individuals to access and share more information on a global level. However, the abuse of this fundamental right has led to a violation of the rights of others, for example, smear campaigns, cyberbullying, harassment, hate speech, etc.<sup>16</sup>

A serious practice that threatens both the right to privacy and the right to freedom of expression is mass surveillance by governments and regimes over individuals. In this regard, the interests of social networks and the information economy intersect with those of governments. While social networks invest in user data and exploit it in ways that are often far from transparent and clear, governments seek to employ the development of network and information technology to censor and restrict dissenting content.<sup>17</sup>

---

14. (UNESCO). "Privacy, Free Expression and Transparency: Redefining Their New Boundaries in the Digital Age." *UNESDOC Digital Library*. United Nations Educational, Scientific and Cultural Organization (UNESCO), 2016. <https://unesdoc.unesco.org/ark:/48223/pf0000246610>

15. Cannataci, J. A., Zhao, B., Torres Vives, G., Monteleone, S., Bonnici, J. M., & Moyakine, E. (2016). **Privacy, free expression and transparency: redefining their new boundaries in the digital age**. [Unesco Publishing](#).

16. Ibid. P. 7.

17. Ibid. P. 8.

## **The dark side of social networks: Digital repression, disinformation, and harassment of Individuals**

If the advent of the Internet has brought about an unprecedented revolution in informatics, the emergence of social media networks has marked a milestone in the history of the Internet. Online social media has opened unprecedented communication possibilities, especially among age groups that have not previously had the opportunity for political or civic participation within traditional systems, namely youth. Researchers claim that social media networks created alternative public spaces that have reshaped the patterns of youth participation in everyday civic and political spaces. However, the study of youth participation is still emerging, especially in light of the many challenges related to the diversity of societies on social networks and their different experiences according to geographical, cultural, and social distribution.<sup>18</sup> While nascent experiences among democratic societies appear promising, others emerging in undemocratic or repressive political and social systems face difficulties and dilemmas.

While digital spaces provide opportunities for youth participation, individuals' activity and content are censored, along with other practices of digital repression. In other words, social networks create an opportunity for social and political mobility and, in parallel, provide tools that will enhance the ability of the controlling elite to conduct highly efficient collective censorship.<sup>19</sup> The term digital repression is a recent term with increasing use, although there is disagreement among researchers about its exact meaning. Digital repression generally refers to practices directed against individuals to undermine their political and social activity through social networks. For example, it includes traditional repressive practices against digital activists, arrest, persecution, personal harassment, and even physical violence. It also includes novel repressive practices related to the digital environment, such as digital censorship or the development and employment of IT strategies designed to limit and reduce digital opposition activity.<sup>20</sup>

The importance and sensitivity of this debate lie in the position of social media networks among young people, as they have become a pillar in their daily lives. For example, according to a statistical study conducted by the Palestinian Central Bureau

18. Lee, Ashley. (2018). Invisible Networked Publics and Hidden Contention: Youth Activism and Social Media Tactics under Repression. [New Media & Society](#), 20(11). P. 4096.

19. Ibid. P. 4097.

20. Earl, Jennifer, Thomas v. Maher, & Pan, Jennifer. (2022). The Digital Repression of Social Movements, Protest, and Activism: A Synthetic Review. [Science Advances](#), 8 (10). Pp. 1–15.

of Statistics in 2022, 95% of the Palestinian youth between the ages of 18-29 use the Internet, and 89% of the youth own a smartphone. Users' activity on social media networks generally revolves around interactive services, user-generated content, groups, etc. However, one cannot isolate this activity from the dark and hidden side of social media networks, which can be described as a set of negative phenomena and behaviors associated with the uses of information technology, such as the increased risk of exposure to disinformation, rumors, false propaganda, cyberbullying, hate speech, and harassment. These uses and behaviors clearly violate the well-being and rights of individuals, organizations, and communities.<sup>21</sup>

### **Palestinian youth on social networks: The struggle for digital presence**

The Internet has introduced cultural, political, and economic transformations of a unique nature, especially in the Palestinian context, given the long history of occupation and struggle waged by the Palestinian people since the Nakba in 1948, specifically regarding the struggle for the right to have a narrative. The beginning of the Palestinian political, civil, and social movement on the Internet coincided with the outbreak of the Second Intifada (September 28, 2000).<sup>22</sup> At the time, Palestinians took advantage of the possibilities offered by the Internet to make their voices heard to the world and communicate with each other, especially under the siege imposed by Israel. Ever since Palestinians became a player in the virtual world, Israel has exerted pressure, restrictions, and violations of Palestinians' digital rights.<sup>23</sup> Since then, the digital space has become an arena for political and intellectual conflict. Recent years have witnessed unprecedented efforts by Israeli government to promote Israeli Hasbara,<sup>24</sup> as they engage in direct propaganda campaigns through official endeavors with owners and managers of social media networks, such as X (formerly Twitter) and others. The Israeli authorities regularly submit formal requests

21. Norri-Sederholm, Teija, Riikonen, Reetta, Moilanen, Panu & Aki-Mauri, Huhtinen. (2020). Young People and the Dark Side of Social Media: Possible Threats to National Security. In Thaddeus, Eze, Lee, Speakman & Cyril, Onwubiko (Eds.). [Proceedings of the 19th European Conference on Cyber Warfare](#) (pp. 278-283). ACPI.

22. YEEN, J.K.H. (2009). The Electronic Intifa'da: The Palestinian Online Resistance in the 2nd Intifada. [Journal of Information Warfare](#), 8(1). P. 1.

23. Khoury-Machool, Makram. (2007). Palestinian Youth and Political Activism: The Emerging Internet Culture and New Modes of Resistance. [Policy Futures in Education](#), 5(1). Pp. 17–36.

24. Aouragh, Miriyam. (2016). Hasbara 2.0: Israel's Public Diplomacy in the Digital Age. [Middle East Critique](#), 25(3). Pp. 271–72.

The term "Hasbara" refers to organized and systematic propaganda campaigns to which the official Israeli establishment allocates resources necessary to prepare and train supporters and promoters of Israeli propaganda.

to delete, block, or restrict access to Palestinian content. Moreover, the Israeli army's accounts are characterized by their social media activism, where leaders sometimes post military statements and announcements about military campaigns, which can be described as digital militarization.<sup>25</sup>

The struggle for the right to exist in digital spaces is accompanied by the escalation of the discourse of digital rights. The demand for digital rights for Palestinians has become part of advocacy campaigns and struggles on social media networks. Naturally, these campaigns have become part of a global movement demanding the recognition and protection of digital rights. The specificity and sensitivity of the Palestinian context is a rare case suitable for studying the relations of power and political freedoms and the manifestations of these relations in the digital space.<sup>26</sup>

One of the most prominent challenges to Palestinians' digital rights is the loss of Palestinian control over the infrastructure of telecommunications networks, as all communication systems are still under the control of Israel. The Palestinian Authority enjoys little sovereignty over the digital space, despite the affirmation in the second Oslo Accords in 1995 of the right of Palestinians to have an independent communications technology sector and to have autonomy over infrastructure. In other words, the Oslo Accords ensure the Palestinians' right to establish and operate separate and independent communication systems with infrastructures including telecommunication networks, television, and radio networks. However, Israel continuously practices a flagrant violation of the terms of this agreement and controls the infrastructure of the telecommunications system in Palestine. The Palestinians' inability to control communications infrastructure and the lack of an independent and separate communications network has created a significant obstacle to achieving digital security for Palestinians.<sup>27</sup>

Moreover, Palestinian activists and content are subject to the censorship from Israeli authorities, which exposes them to interrogation, prosecution, arrest, and punishment. The Israeli authorities invest in the development of automated tracking and censorship technologies by developing social network algorithms systems

---

25. Cristiano, Fabio. (2019). [Internet Access as Human Right: A Dystopian Critique from the Occupied Palestinian Territory](#). In Iouin-Genest G., Doran M.C., and Paquerot, S. (Eds.). **Human Rights as Battlefields** (pp. 249-269). Ottawa, ON, Canada: Human Rights Interventions.

26 Ibid .P.257 .

27. Cristiano, Fabio. (2020). [Palestine: Whose Cyber Security without Cyber Sovereignty?](#) In Romaniuk S. N. and Manjikian M. (Eds.). **Routledge Companion to Global Cyber-Security Strategy**, Basingstoke: Palgrave Macmillan (pp. 418-426).

to examine Palestinian content.<sup>28</sup> These algorithms focus on vetting status posts, comments, and photos to identify content that violates Israeli policies or that falls within what Israeli authorities consider incitement to violence.<sup>29</sup>

---

28. Fatafta, Marwa & Nashif, Nadim. (2017, October 23). Surveillance of Palestinians and the Fight for Digital Rights. [Al-Shabaka Policy Brief](#).

29. Cristiano, Fabio. (2019). Ibid, pp. 249-268.

## Part Three

### Methodology

#### Research tools:

This study seeks to detect and investigate the digital security of Palestinian youth via the Internet, aiming to employ the results to enhance the protection of the digital rights of Palestinian youth in the West Bank and East Jerusalem. It was not possible to conduct research in the Gaza Strip due to conditions of war. The research used quantitative and qualitative research mechanisms to achieve comprehensive results according to the research objectives.

The research was based on a theoretical framework that ensured a scientific literature review and used two research tools to collect and measure data to understand the reality of digital risks in the West Bank and Jerusalem. The tools used in this research are a questionnaire/field survey and meetings with focus groups from two geographical areas: the West Bank and Jerusalem.

#### Field Survey:

The field survey was conducted in February 2024 via telephone by Mina Analytics, an institution specializing in research and survey studies. The sample included (449) participants from different areas in the West Bank and East Jerusalem. Due to the war conditions, it was impossible to include the Gaza Strip in the survey sample. A research questionnaire was used for the purposes of the field survey containing thirty-one questions distributed over five axes:

1. Characteristics of the respondents and their personal data, place of residence, gender, and educational attainment.
2. The nature and characteristics of Internet use, in terms of the location of the Internet connection, the number of hours of use, and the nature of accounts on the platforms.
3. The extent of awareness and knowledge of digital security and digital risks, and the nature of the threats to which participants were exposed, and how they acted in response to them.
4. The extent to which participants are interrogated and questioned by security or social bodies because of what they publish on the social media platforms.
5. The impact of social media platforms' policies on Palestinian youth digital activity since the start of the war on the Gaza Strip.



### Focus groups:

The study used focus groups as a second tool to enhance and deepen understanding of the results of the quantitative study. Therefore, five meetings with focus groups were held throughout February and March 2024. Three groups were organized via Zoom, and two in person meetings were organized for high school students. The first meeting was held at the Tamer Institute for Community Education in Ramallah. The second meeting was held in a café in Jerusalem.

**Table :1 Focus Group Details**

	Group characteristics	Region	Number of participants	Gender		Nature of the meeting
				females	males	
1	University students and activists	Northern West Bank (Jenin, Nablus, Tulkarm)	6	5 females	1 Male	Zoom
2	University students and activists	Central and South West Bank and Jerusalem	7	6 females	1 Male	Zoom
3	High school students	The West Bank (Ramallah Allah)	11	8 females	3 Males	in person meetings / Ramallah
4	High school students	Jerusalem	5	3 females	2 Males	in person meetings / Jerusalem
5	Activists and employees of institutions interested in digital rights	The West Bank and Jerusalem	6	1 Female	5 Males	Zoom
	<b>Total</b>		<b>35</b>	<b>23</b>	<b>12</b>	

The questions that established the discussions in the focus groups were selected based on the main findings reflected in the field survey. Topics of discussion within the high school students' focus group included: students' relationship with the Internet, the nature of the platforms they use and are active on; their goals for using the Internet; the nature of the digital threats they are exposed to; the extent to which they feel safe while active on digital platforms; the availability of security measures at their home; the nature of Internet use since the war on the Gaza Strip; the training they received on digital rights and digital security; their vision of the future of network use.

The topics of discussion within the university students' focus group included the nature of the relationship with the Internet and its stages of development; the experiences the students underwent in their relationship with the Internet; the platforms they use and their motivations to use them; the nature of the threats they have been exposed to; trainings they received to raise their knowledge in digital security; their vision of solutions related to the decline in the state of digital security; their vision of the future of using the Internet in light of the growing digital risks and threats.

The topics of discussion within the institutions and activists focus group consisted of three main axes: the nature of the experience associated with the participants' use of the digital environment (being exposed to a digital threat) and the extent to which this experience has affected them; the extent to which officials and activists are familiar with the nature of attacks and violations based on the social aspect (as well as the political and national aspects) and the danger of digital attacks, especially on younger generations ; Approach to solution and action, the scope and areas of work and activity that can be worked on.

The discussions were conducted in Arabic language, whether it was spoken or classical language. The structure and components of the questions differed according to the sector represented by the group, as well as the group members' position regarding the research subject and the nature of their work within the subject. The researcher has personally moderated four of the five discussions and was unable to moderate the in person meeting in Jerusalem due to security restrictions and restrictions on access to Jerusalem.

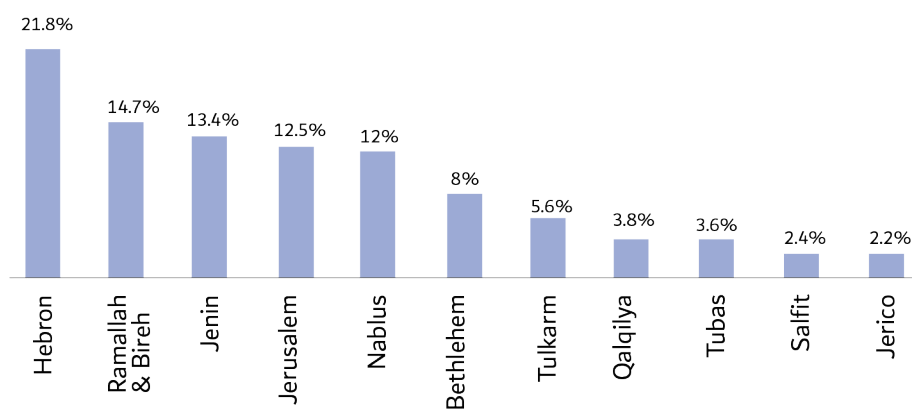
## Part Four

### Results of the analytical study :The survey and focus groups

#### 1. Characteristics of participants

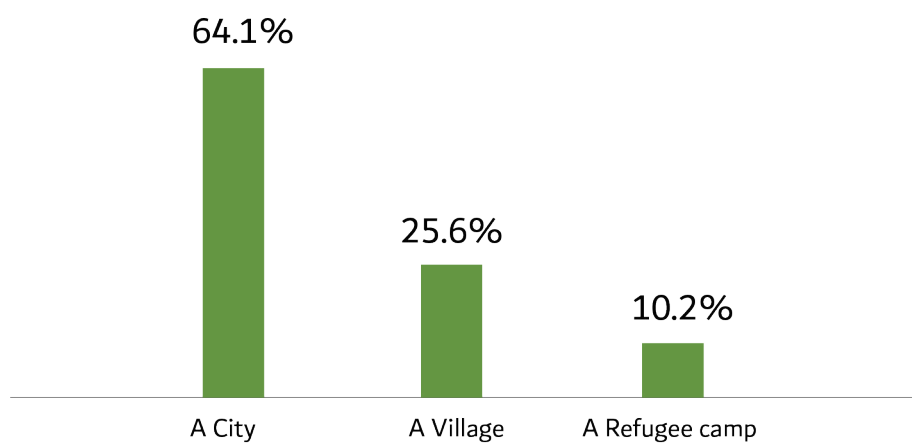
##### 1.1 Place of residence

Figure :(1) Percentage of participants by place of residence



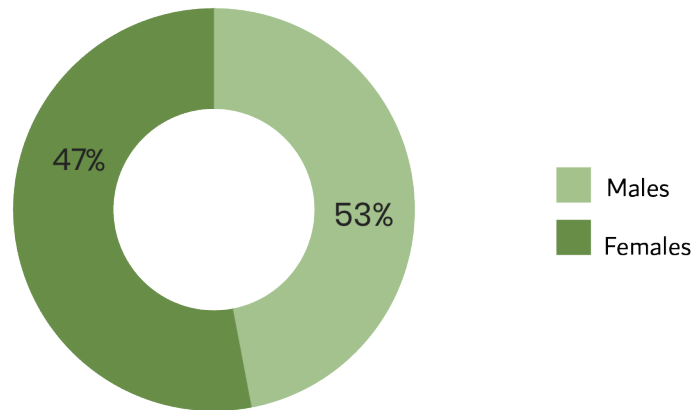
##### 1.2 The nature of the place of residence

Figure (2): Nature of participants' place of residence



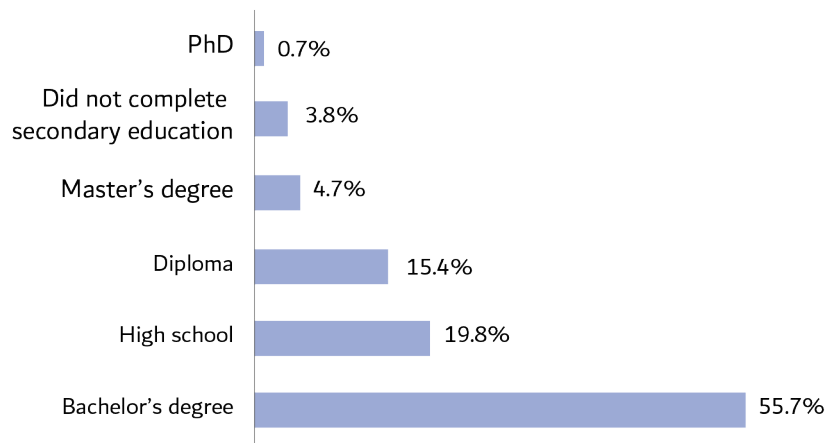
### **1.3 Gender**

**Figure (3): Percentage of males and females in the research sample**



### **1.4 Educational attainment**

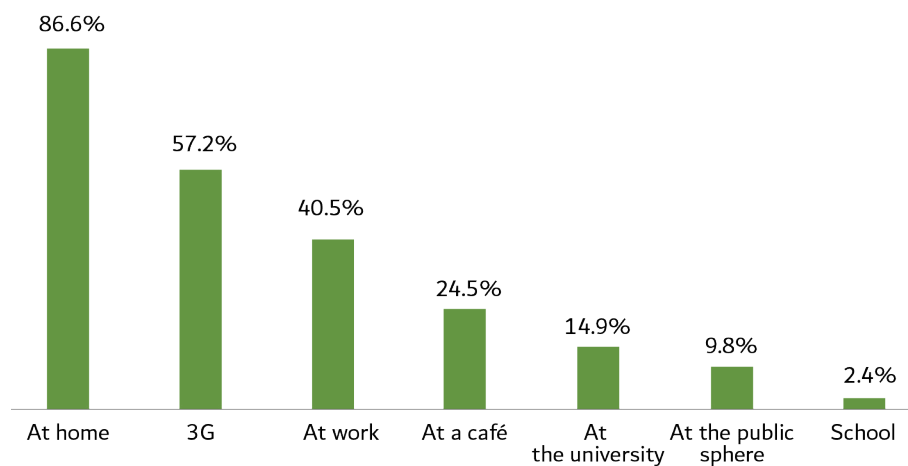
**Figure :(4) Percentage of participants according to educational attainment**



## 2. The nature and characteristics of the use of the Internet

### 2.1 Location of connection to the Internet

Figure (5): Percentage of participants according to location of connection to the Internet



The results show that a large majority of respondents use the Internet at home (86.6%), followed by the use of 3G service by 57% (the service allows network connectivity everywhere), followed by 40.5% who use the Internet at work, and 24.5% at a café, 15% at the university, and finally approximately 10% who use the Internet in the public sphere, according to the public services available in Palestinian cities. In this question, more than one answer was allowed.

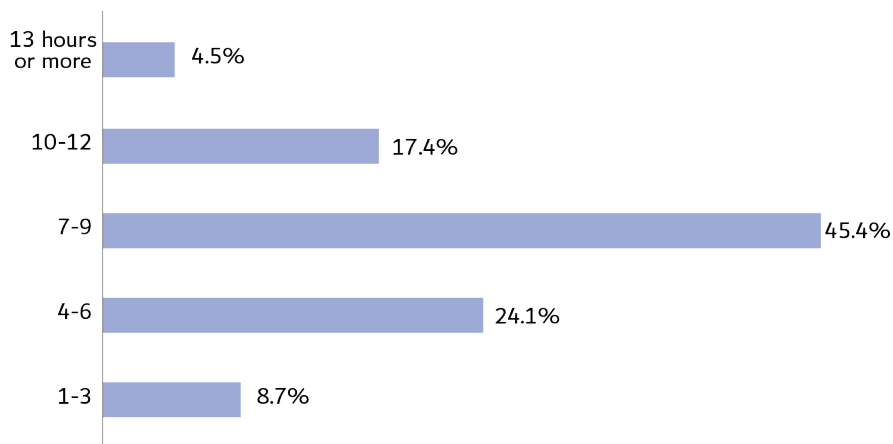
The results are in line with the results of the Labour Force Survey 2022, which stated that 92% of households in Palestine (or at least one member of the household) have access to internet service at home (93% in the West Bank), and 79% of individuals in Palestine own a mobile phone (86% in the West Bank.) Ministry of Telecommunication and Digital Economy data for the year 2022 indicates an increase in the number of cellular subscriptions in Palestine by the end of 2022, that reached 4.4 million subscribers, compared to 2.6 million at the end of 2010, which constitutes an increase of 69%.<sup>30</sup> These figures indicate that there has been a serious development in communication services in various areas of Palestine, especially in cities. All of this raises our questions about the extent of Israel's control and surveillance over

30. The Palestinian Central Bureau of Statistics, *ibid.*

Palestinian digital activity, especially since all this development is happening under Israel’s control of the telecommunications infrastructure and in practice The West Bank is part of the Israeli digital sphere..

## **2.2 Internet use number of hours of**

**Figure (6): Percentage of participants by hours of Internet use**



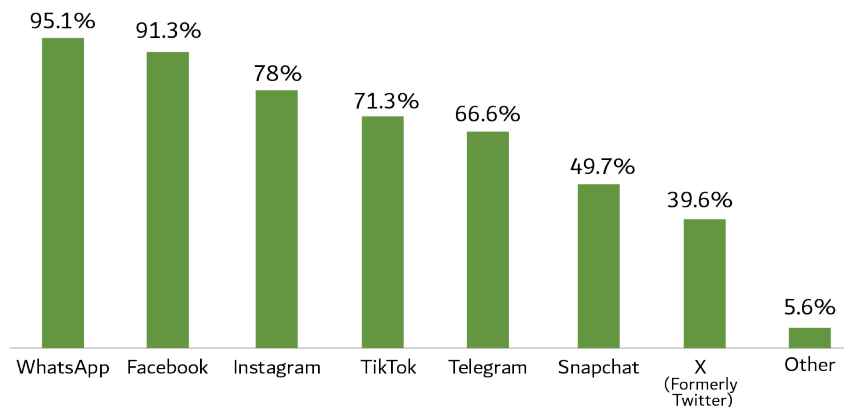
According to the survey results, about 67% of the participants spend at least seven hours a day using the Internet. Participants in the focus groups, especially young people and high school students, described this pattern as addictive. Although they consider it an unsafe place, the participants in the focus groups described a state of inability to stay away from the Internet as it provides them with advantages, including the ability to communicate with friends, exposure to news, self-expression, and study. The participants in the focus groups spend increasing hours online and are more immersed<sup>31</sup> when it comes to the nature of the relationship with the Internet and its use, and are "deeply immersed" within the Internet, which is understandable since all the junctures of young people’s lives are based on connection to the Internet, or in the words of some participants in the focus groups, "Internet connectivity is absolutely irreplaceable."

---

31. Immersion is a word used to describe the user’s relationship with the Internet, as he/she navigates the Internet as if he/she is immersed in water. It is an indication that the issue is more than just about entering the Internet or the traditional use of it.

## 2.3 Types of accounts on social media sites

Figure (7): Percentage of participants' use of social media accounts



The most prominent results are that most respondents use (and have accounts) WhatsApp (95%) and Facebook (91%), followed by Instagram (78%), TikTok (71%), Telegram (66.6%), Snapchat (59%), X/Twitter (39.6%). The respondents were allowed to choose more than one answer to this question.

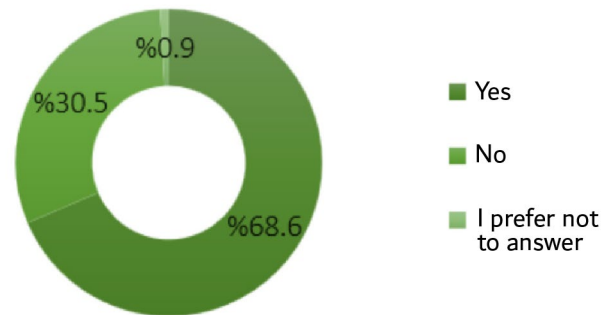
The respondents use more than one social platform to communicate and follow the news, especially considering the current political events. Notably, the most popular platforms among users are the ones that most suppress the Palestinian narrative, especially those owned by Meta..

The responses of participants in the focus groups explained the reasons for the popularity of Instagram among young people and their preference for it over other platforms. They stated that Facebook is considered a "formal" platform that does not align with the "vitality and flexibility of youth," in their words, in addition to the increasing implementation of censorship and digital repression policies on Facebook.

### 3. Awareness about digital security and digital risks

#### 3.1 Respondents' awareness of spyware and its threats

Figure (8): Percentage of participants aware/unaware of spyware and its threats.



The results show that about two-thirds of respondents are aware (without specifying the nature of their awareness) of spyware and the threats it inflicts. Their awareness may be due to the widespread talk about such software in the Palestinian context, as Israel has targeted groups of activists and human rights defenders with the Pegasus spyware in order to hack their smartphone<sup>32</sup> In contrast, about 30% of respondents did not hear or have no information about spyware and its threats, despite their constant activity on the Internet.

These results are worrisome. Let's consider that the answers to knowledge about spyware do not necessarily mean that the respondent has full awareness or ability to provide protection and avoid the harm and dangers of spyware. We will find that we are facing a reality that raises serious questions about the effects and magnitude of the risks to which Palestinians are exposed on the Internet.

Discussions within the focus groups show that some Palestinian university students and high school students in Jerusalem received training on digital security, from a Palestinian, Arab, or international body, such as 7amleh, ARIJ Network in Jordan, or UNICEF. Participants from the focus group of high school students in Jerusalem schools stated that a group of lawyers and Jerusalemite NGOs provided special training to students on awareness of digital risks, focusing mainly on what Israeli law considers incitement to terrorism. Considering the increase in sources of threat

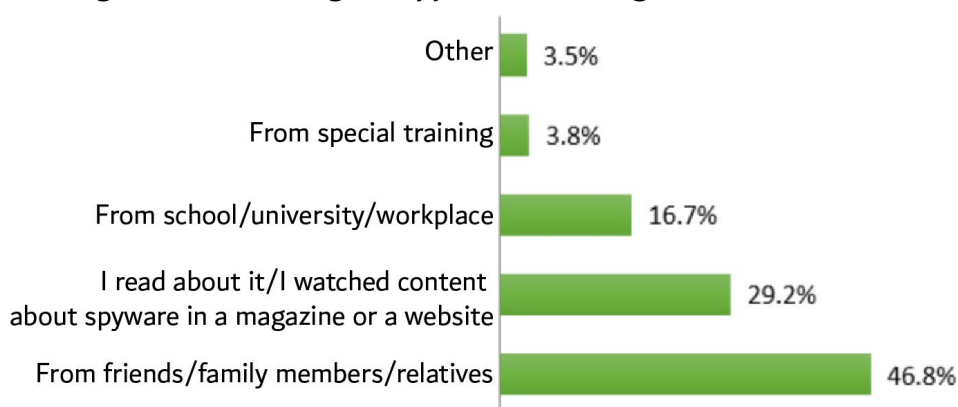
32. Spyware developed and sold by NSO GROUP.



since the beginning of the war on the Gaza Strip and the diversity of manifestations and threats of espionage and censorship, we cannot guarantee that the training has reached all schools and all groups.

### **3.2 Sources of knowledge about surveillance and spyware and their threats**

**Figure (9): Percentage of spyware knowledge sources and threats**



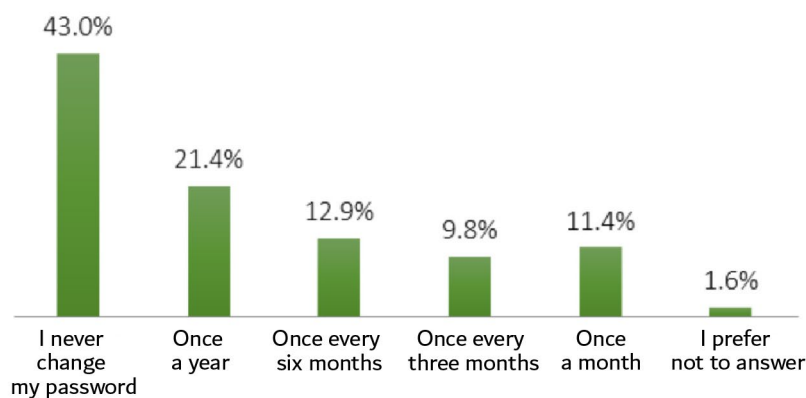
The results show that 46% of the information source regarding digital security is from the first social circle, i.e., family, relatives, and friends, and it is the highest among the sources of information. Next are sources from school/university/workplace and designated training courses (16.7% and 3.8%, respectively.) These results are important and lead us to wonder about the nature of the information that stems from the first social circle, which can be described as not specialized and may be inaccurate and exaggerated. Moreover, this type of information source may be fueled by fear and anxiety due to lack of professionalism and not being scientifically based, especially considering the decline in knowledge and information from traditional institutions that are supposed to produce knowledge, such as schools, universities, and workplaces.

These results have reinforced discussions with focus groups (high school students, university students, activists, and institutions) and raised this imbalance associated with a noticeable lack of awareness on issues of espionage and digital attacks or violations, especially among societal groups considered the most vulnerable and most targeted – high school groups. According to the participants in the focus groups, students – female students in particular – have been subjected to digital

attacks at an early age (10-12 years, and sometimes less), and the elderly (50 years and above) have been extorted and threatened. We must seriously consider the low percentage of knowledge and information from specialized sources – training courses – the most important source of sound knowledge of spyware and its threats, and how to address and avoid them.

### **3.3 Frequency of password change**

**Figure (10): Frequency of password change**



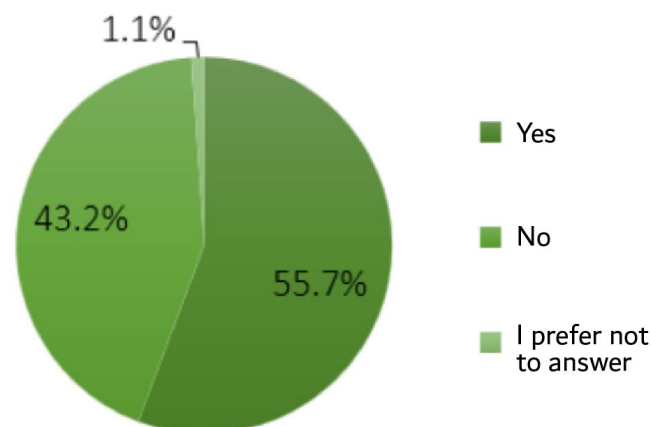
To find out how well participants take actions considered basic digital security measures, they were asked a series of questions related to these basics, including how often they change the password for their different accounts. The results show that about 43% of respondents do not change passwords at all, while 21.4% change passwords at most once a year, about 13% change passwords an average of once every half year, about 10% change passwords once every three months, and 11.4% change passwords monthly.

Changing passwords is one of the most basic foundations of digital security. The results show that about half of the participants do not change passwords, which may be due to the lack of awareness and knowledge of the importance of passwords and changing them. Participants may have basic knowledge of the importance of changing passwords but do not bother changing them and do not care about them. One may deduce from the second reason that there is a need to motivate users to change their behavior, and that the responsibility to do so lies with the relevant authorities.

It must be noted that the discussion in the focus groups revealed that most of the participants were exposed to attacks such as account theft or attempted account theft, extortion, and digital threats, which exposed them to anxiety, stress, and a sense of insecurity and danger. It was shown in the focus groups of university and high school students that there is a direct relationship between exposure to digital attacks and the extent of knowledge and ways to protect against them. According to students' statements in the target groups, targeting or attacking them digitally prompted them to develop their knowledge of digital security and apply security measures accordingly. A female participant said, "My knowledge and awareness are a result of pain and suffering [...] The assault on me has completely changed my life, my outlook on life, of the Internet, and of everyone around me."

### **3.4 Security settings on social networks**

**Figure (11): Percentage of participants who configure security settings**

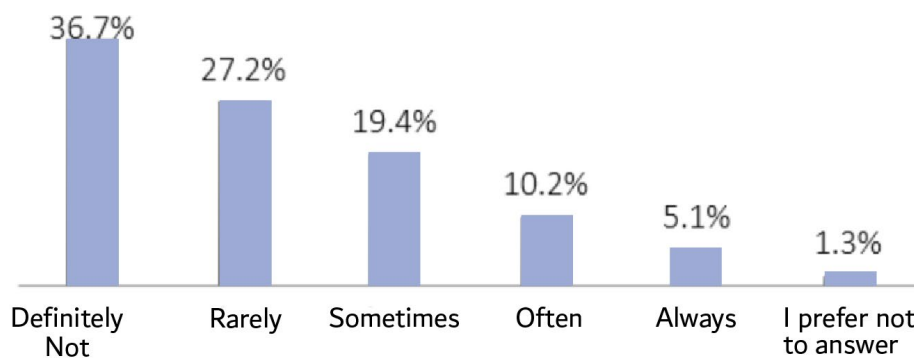


Concerning pages of individuals, groups or organizations, security, and privacy (safety) settings in social networks are very important. The settings include a set of critical questions that the user must ask themselves while determining these settings, including, for example, the nature of sharing posts with the public or with a specific group of people who can comment, reply, or interact with the user's messages or posts, and the possibility of finding the user or the organization in which he/she works, the user's desire to automatically share their location when posting, the extent to which they want to block or mute hostile accounts, and the desire to block certain words or keyword tags. These settings provide users with a list of options that guarantee their "safety" if used and well perceived.

The results in Figure 11 reflect that about half of the respondents do not use security settings at all, which makes them vulnerable to attacks, violations, hacks, and tracking, thus, allowing privacy violations. The focus groups confirmed these results, and some participants stressed that they created their accounts without having any previous knowledge of the security settings that the platforms provide to users. Some participants in the focus groups said that some mothers open accounts for their children without considering the nature of using the accounts or without realizing the risks inherent in these platforms. This behavior amounts to naïve understanding of the nature of the platforms or digital environment in which adolescents and children are immersed. In addition, a deep sense of Internet insecurity prevailed among focus group members.

### **3.5 Adding unknown people to my Internet accounts**

**Figure (12) Frequency of friendship requests authorization from unknown people on the Internet**

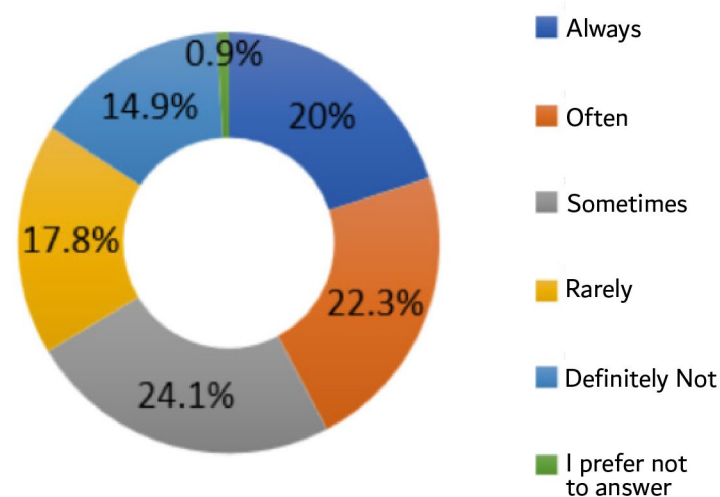


The results show that about two-thirds of respondents accept friend requests or add people they do not know on social media platforms. The authorization frequency ranges from rarely (27.2%) to often and always (15%). Due to the policies of Israel, it is commonly known that this behavior will make them vulnerable and increase their risk, in addition to the increase in cases of commercial fraud, theft, extortion, manipulation of feelings, and misinformation. In addition, this behavior indicates a lack of knowledge of the Internet environment and the nature of the threats to which users can be exposed.

The focus groups of high school students pointed to a range of serious problems caused by adding unknown people to their friends lists. Students stated that the most targeted group was adolescent females, and sometimes in pre-adolescence age. The participants said that the behavior of the unknown persons begins with a friendly approach and ends with suffering, extortion, threats and harassment.

### **3.6 Sharing photos and personal matters over the Internet**

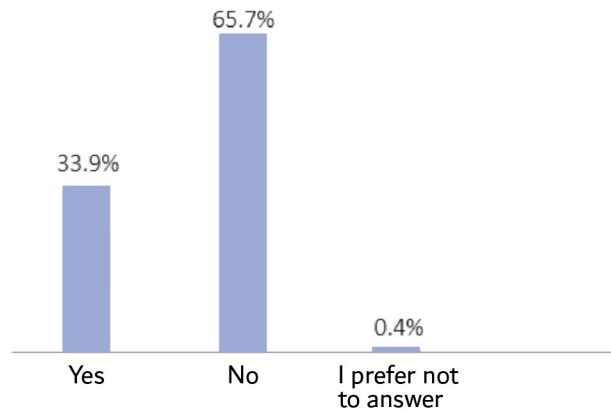
**Figure (13): Frequency of sharing photos and personal matters over the Internet**



The results show that about 66% of respondents' behavior regarding sharing photos and personal matters across the Internet proportionately varied between often, always, and sometimes. One may conclude from the results that there is a widespread belief among users that the Internet is secure and that there is no risk to sharing personal matters. We cannot assert that those who responded by rarely sharing photos and personal matters did so because of their knowledge of the risks, as it may be due to cultural reasons and customs. In the Palestinian context, it is important to point out the risks emanating when sharing photos and personal matters because they are used as a source of information and a reason for censoring activists and political actors, which may lead to their prosecution and arrest, in addition to other known social risks, such as blackmail and threats.

### **3.7 Use of online protection software**

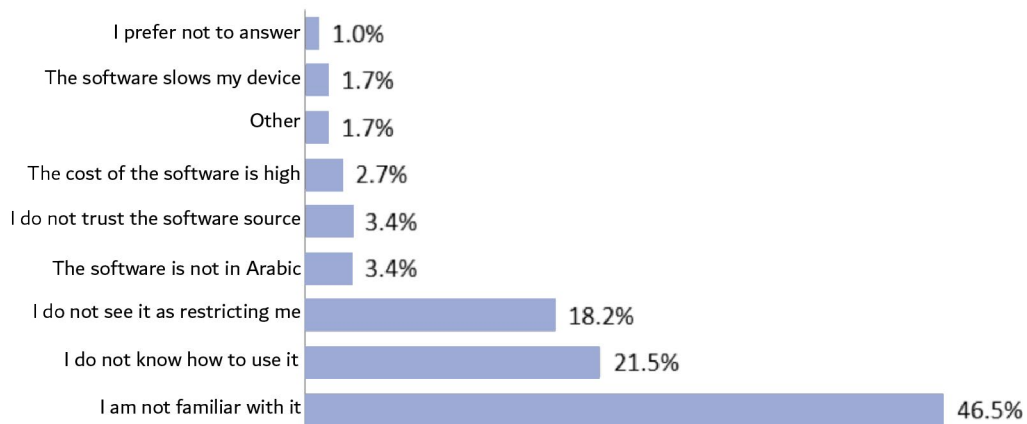
**Figure (14): Percentage of participants using protection software**



The results show that about 66% of respondents do not use security software for their devices, while about a third of respondents use it. This behavior of users enhances the chances of being targeted in digital environments, especially young people. The most important question we need to ask here is: What reasons prevent respondents from using basic protection programs? We will answer this question in the next item.

### **3.8 Reasons not to use security software on electronic devices**

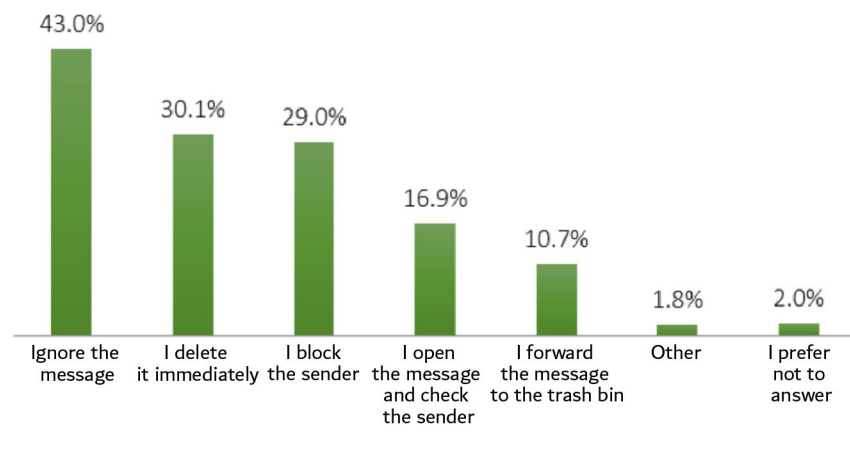
**Figure (15) Distribution of reasons why protection software is not used by respondents**



The results of this item explain the lack of use of protection programs. We can classify the answers into two groups: a group that is not familiar with protection programs– 46.5% of the respondents answered that they do not use them; and a group that is familiar with protection programs but does not use them – 53.5%. Interestingly, about half of those who chose not to use the software from the second group did not use them due to lack of experience (about 25%), and the other half due to technical reasons. These findings reflect a deep knowledge crisis and an opportunity to raise awareness about security programs and conduct training in their use. When asked about this question, the focus group of institutions and activists confirmed this insight. The focus group members pointed to the importance and necessity of intensifying work on digital protection and prevention training.

### **3.9 Behavior when receiving messages from an unknown source**

**Figure (16): Distribution of respondents' behavior when they receive messages from an unknown source**

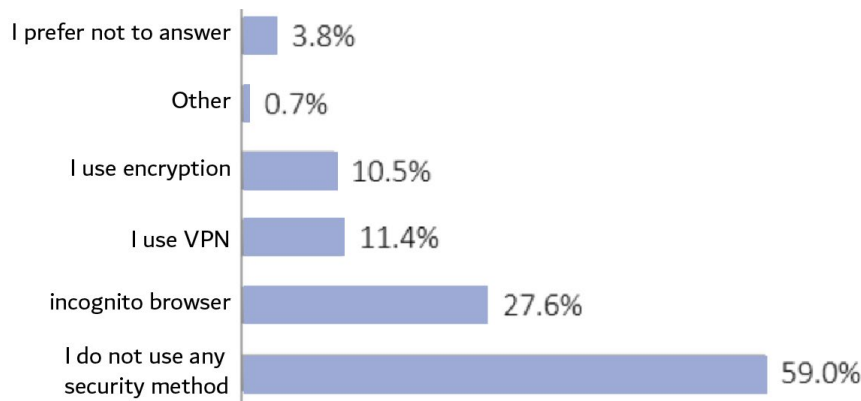


This item checks the behaviors of respondents when they receive messages from an unknown source (they could have chosen more than one answer). The results show that the most common behavior among the respondents, approximately half of them (43%), is to ignore the message and the sender. Some respondents' behaviors may be considered prevention and protection behaviors, for example, deleting directly and preventing the sender from communicating (30% each).

Ignoring anonymous messages may be a good thing. However, it is an act that was not taken consciously and without taking into consideration the sender or the nature of the targeting (security/commercial/political/social.) If we consider the possibility that the act of sending a message from the same entity may be repeated and the possibility that the user will open this message, the consequences can be dire, especially in light of the development of fraud, censorship, and hacking methods.

### **3.10 Digital protection while using the Internet**

**Figure (17): Distribution of the protection methods taken by respondents while browsing the Internet.**



The answers to this question are consistent with respondents' answers to previous questions related to digital protection and prevention. The results show that more than half of the respondents do not use any means of digital protection (59%.) The rest of the respondents stated that they use various means of protection, most notably incognito browser<sup>33</sup> (27.6%), while 11.4% and 10.5% of the respondents stated that they use VPN<sup>34</sup> and encryption<sup>35</sup> (respectively.) The protections presented in the answers to this question are basic, easy to use, and can provide digital protection and safe use of the Internet. These findings complement the picture presented in the previous answers, namely that the public does not know what protection programs can provide them with safe use of the Internet, and there seems to be an urgent need to make this knowledge accessible to all users.

33. The incognito browser offers the possibility of not tracking the sites that the user browses.

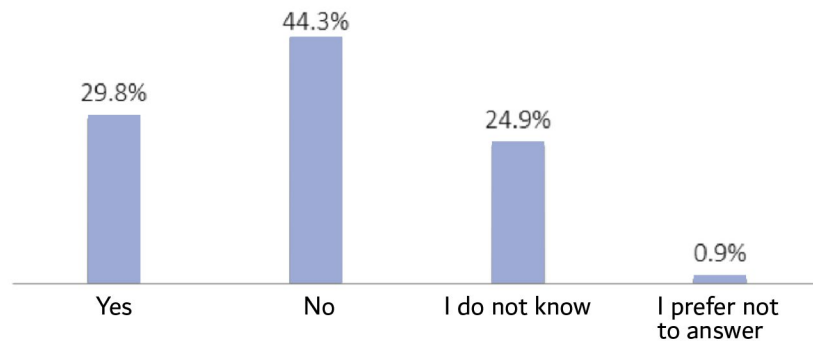
34. VPN provides the ability to connect to the Internet without revealing the location of the connection.

35. Encryption allows converting the text of messages into information encrypted by special algorithms.



### 3.11 Geolocation feature

Figure (18): Geolocation operator percentage among respondents

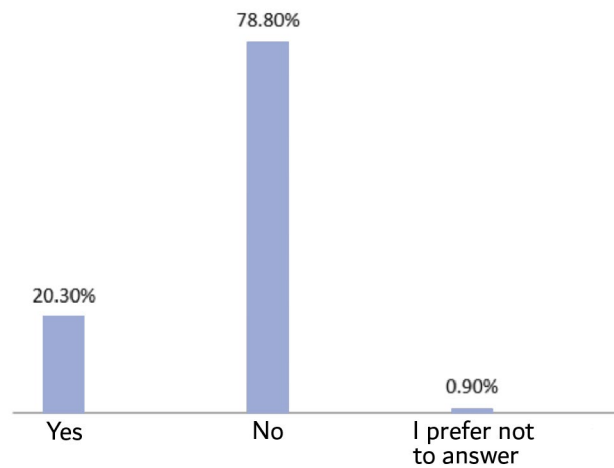


The results show that a third of respondents (29%) use geolocation, which means that they reveal where they are. While 44% of the respondents stated that they do not use this feature, it seems that this feature is more common than other means of protection. Discussion with the various focus groups showed anecdotes and stories of thefts that occurred due to the geographical location of users. The harm to Palestinian youth may be serious at the political level, considering the escalation of policies of repression, threats, and arrests. For example, authorities can determine their whereabouts, gatherings, movements, and political activity by using this feature. It should be noted that if a user posts, photos, and the geolocation detection feature is effective, the security authorities can use them as evidence of threats and arrests and increase the likelihood of violating their digital privacy.

## 4. Digital Attacks and Assaults

### 4.2 Being exposed to abuse ,attack ,or blackmail by intruders or hackers

Figure (19): Percentage of cyber-attacks and assaults

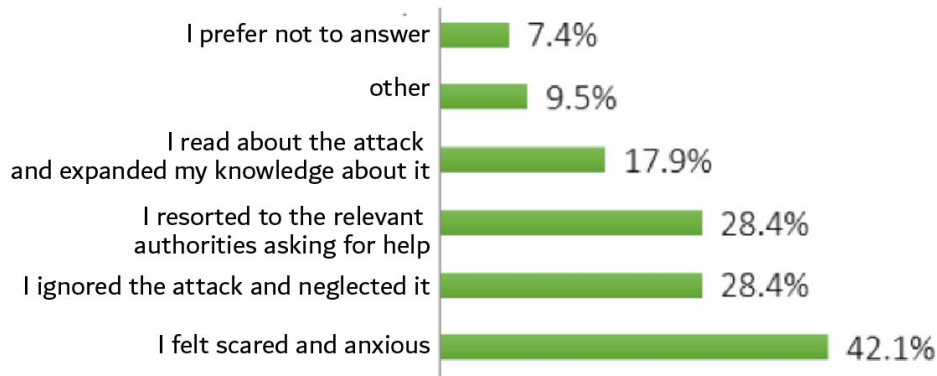


The results show that the vast majority of respondents (79%) have not been subjected to abuse, attacks, threats, assaults, or digital blackmail from intruders or hackers, while 20% of respondents said that they have been subjected to digital attacks.

The percentage of respondents subjected to digital assaults cannot be underestimated. Although it may seem small, it is considered relatively high, and it indicates the problems and behaviors of Internet users on both sides of the attack (see the following two items.) The percentage of those who were attacked from the research sample indicates deep problems in the absence of awareness and knowledge at times, ignoring threats and dealing with them as if they did not exist at other times, or dealing lightly with digital attacks so that the awareness of digital risks is not reflected in the acquisition of skills and practices that ensure fortification in digital environments.

## **4.2 Respondents 'handling of digital attack or assault**

**Figure (20): Behavior of respondents after a digital attack**

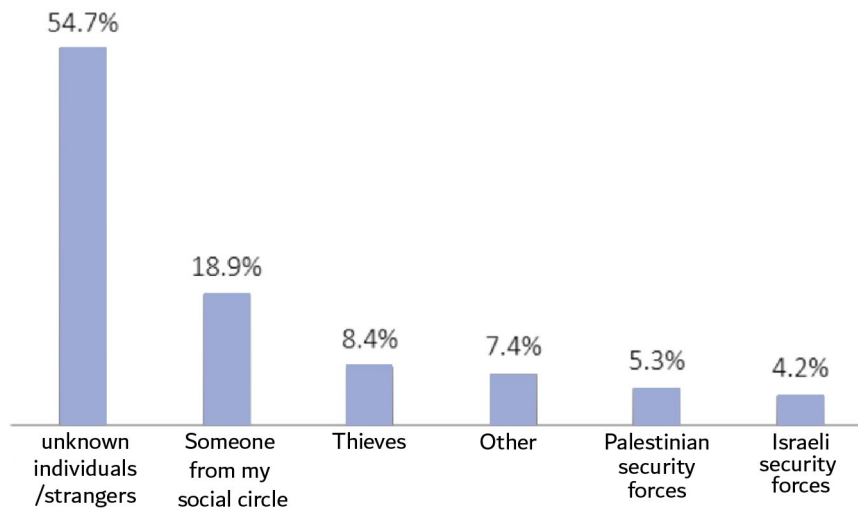


The results show that the reaction of the majority of respondents who were attacked was fear and anxiety as a result of the attack (42%.) 28.4% of the respondents answered that they ignored the attack or resorted to the relevant authorities for help (in equal proportions), and 18% said that they chose to expand their knowledge about the attack.

The results reflect problems and contradictions in dealing with digital attacks. While attacks make users feel afraid and anxious, many of those exposed to them ignore and neglect the attacks instead of dealing with them. When this issue was discussed in all focus groups, it became clear that the majority of the respondents do not take the necessary measures when seeking to address the assault or digital attack. This was evident in the groups of high school and university students.

### **4.3 Behind the attack or assault**

**Figure (21): Actors behind digital attacks and assaults**



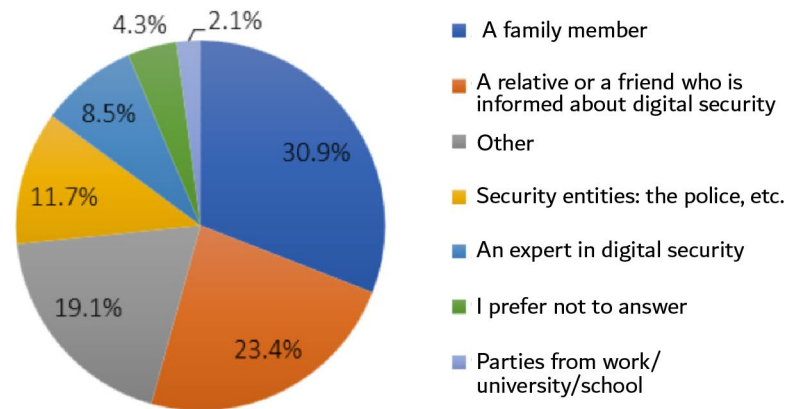
The results show that about 55% of the attackers (according to the respondents) were unknown individuals/strangers, while about 20% said that those who attacked them were members of their social circle; about 9% said that thieves attacked them, and the attacks issued by Palestinian or Israeli security forces were 5.3% and 4.2% respectively.

When reading these results, we must consider the previous item's results, especially the respondents who ignore the attack and the digital assault on them. If the attackers are unknown individuals and we choose to ignore the attack, the attackers are bound to repeat their act, because they have not been reported. The aggressors usually turn to the possibilities provided by the Internet and multiple communication networks in the West Bank, as some of them resort to using an Israeli telecommunications provider to open fake accounts to attack users. This makes it difficult to trace the details of the attackers and assailants in the West Bank.

One of the most prominent conclusions of the focus group discussions in this regard is that there has been an increase in attacks by members of the social circle of the victim (relatives/friends.) We are facing a new scourge and social mechanism of abuse and bullying among family members and friends.

#### **4.4 Entities respondents resorted to after a digital attack or assault**

**Figure (22): Entities respondents resorted to after a digital attack or assault**



The results show that half of the respondents prefer to resort to someone from their close circle, about 30% resort to a family member, and about 23% resort to a relative or friend who is informed in digital security. The other half resort to parties other than those mentioned in the question (19%), and 12% resort to security and police authorities, and 8.5% resort to an expert in the field of digital security.

When reading these results, we must pay attention to two essential things: first, respondents resort to relatives and acquaintances, and this may be related to the results of the previous item, i.e., 19% of attacks are carried out by members of the close circle, and thus they prefer to solve problems internally; second, that the path of resorting to security and police authorities, which is the apparent path for filing complaints against aggressors, is not the primary option in dealing with digital attacks. In addition, these results may be an indicator of trustworthiness among young people and an indicator of institutions' need to raise awareness about digital security at the household level.

Discussions in the focus groups supported the results of the survey. Opinions within the Jerusalem focus group were divided over the specialist authorities that users should resort to because the entity that should provide protection and digital security for young people is an Israeli security apparatus that practices policies of occupation and repression against them, which is a source of threat to them, and not a source of protection and safety.

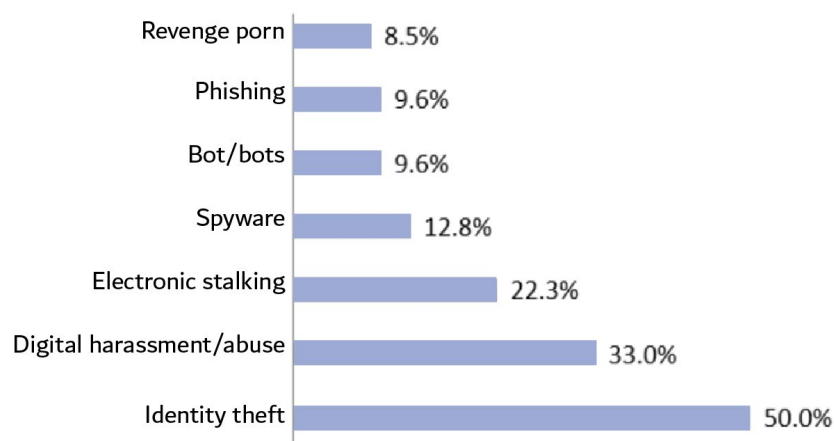
Discussions in high school and university groups have shown that resorting to parents was the last resort and that resorting to parents takes place only after exhausting all attempts to deal with the abuse personally. This troubling finding may require in-depth research to explain why young people are not telling their parents about being exposed to digital attacks.

The depth of the problem regarding the options available to citizens seeking protection dominated the discussion in the focus group dedicated to institutions working in digital rights. These problems prevail, especially in the West Bank, due to young people’s distrust in the security services, the weak capacity of these technical agencies, and their inability to deal with attacks that use Israeli Internet services (Israeli chips.) Moreover, the work of Palestinian security forces is indolent due to high bureaucracy, and not serious in dealing with citizens’ complaints. In addition, the Palestinian security forces base their police practices on The Cybercrime Law, which raises questions for human rights and civil society institutions.

Focus group discussions reflect a real crisis of trust prevailing between users and their surroundings on several levels, including personal, professional, and official. If we wish to overcome the risks of digital attacks, we must rebuild that trust, rehabilitate official authorities, and provide training for all users in digital security.

#### **4.5 Types of digital attacks and assaults**

**Figure (23): Types of assaults and attacks to which respondents were exposed**



Through the field survey, we tried to identify the type and nature of attacks and assaults to which the respondents were subjected. In this item, the respondents were given a simple definition of the proposed answers to unify the participants' concepts regarding the definitions. The results show that half of the attacks/assaults were of the type of identity theft – i.e., creating fake social media accounts that use the name and image of the targeted person or stealing and controlling accounts. One-third of the attacks/assaults (33%) were of the type of digital harassment and abuse – i.e., a hostile use of social networks with the aim of bullying, threatening, and annoying someone, by commenting on contents posted by the victim or commenting on his comments.

Another popular attack/assault is Cyber surveillance and stalking (22.3%) – i.e., a stalking involving false accusations, defamation and slander, or surveillance or dissemination of someone's sensitive personal information online.

Spyware attacks/assaults – i.e., software installed on the device without the consent of the owner of the device that hacks and controls all accounts, e.g., Pegasus – were 12.8% common. The discussion in the focus groups shows that young people have been attacked by this type of attack more than other groups.

Attacks of the type of bots – i.e., computer programs performing repetitive tasks from fake accounts programmed to send abusive messages – were found to be about 10%.

Phishing attacks – meaning worms or viruses – a type of social engineering attack used to steal data. For example, login credentials and credit card numbers were 9.6%.

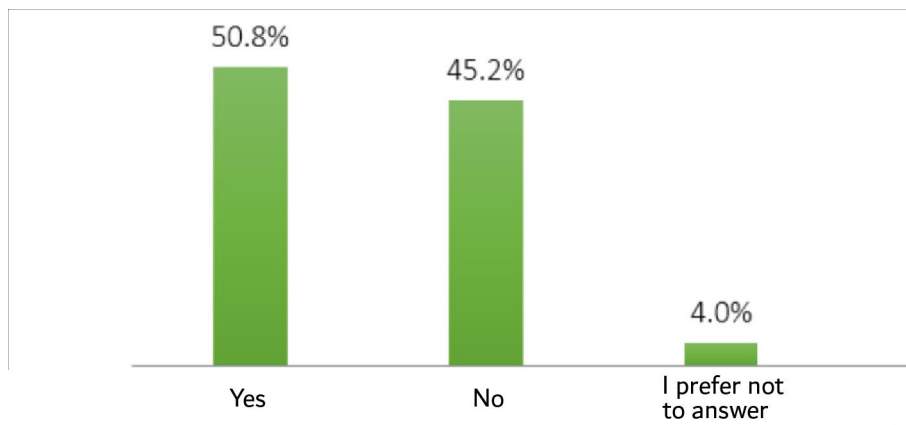
Finally, revenge porn attacks/assaults – i.e., the dissemination of sexually explicit images or videos without the consent of the victim that appears in these materials, or the publication and distribution of intimate, sexual, or pornographic images and videos of individuals without their consent – were 8.5%.

The findings indicate the emergence of attacks related to the categories of identity theft, harassment, and abuse across platforms, which was emphasized by focus groups, especially among high school and university students. In addition, the groups focused their discussion on attacks linked to Israeli security agencies, security threats of arrest, and the practice of policies to combat Palestinian digital content in various digital platforms.

## 5 .Interrogation and investigation by security agencies

### 5.1 Interrogation and investigation by security agencies for" expression of opinion "posts

Figure (24): Percentage of respondents (or someone they know) summoned for interrogation by Israeli security agencies



The results show that about half of the respondents (51%) or members of their social circle were summoned for investigation or interrogation by the Israeli authorities because of posts on social media platforms. Compared to previous years, this percentage is high,<sup>36</sup> and reflects the escalation of the Israeli authorities' policies of repression and persecution against Palestinian activists. We can consider these results an indicator of the level of insecurity and fear that users experience before any click or post across social media platforms. This is a flagrant violation of the right to freedom of expression, including digital expression and interaction with political publications, particularly related to the practices of the Israeli authorities in the West Bank and Jerusalem. One of the methods of repression used by the Israeli authorities (Israeli officers) is sending text messages to Palestinian phones containing an order not to enter Jerusalem and revoking their permits to visit the city because they published "inciting content and support of Hamas through social networks," according to what was mentioned in the text message.

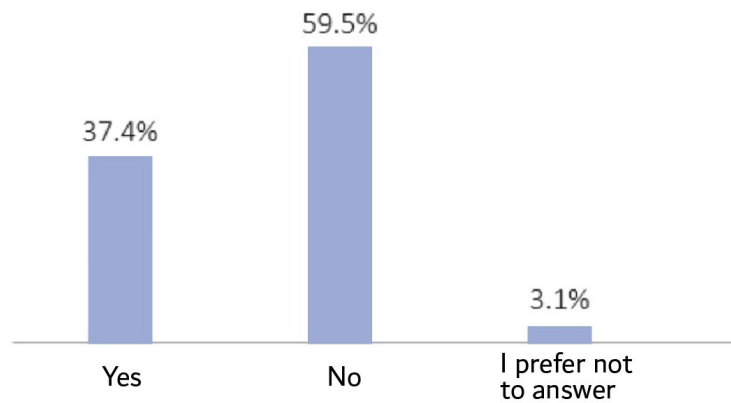
36. Al-Rajoub, Awad. (2023, November). This is how the occupation violates the privacy of Palestinians... By tracking their accounts and publishing about them. [Al Jazeera Network](#).



One of the reasons that has contributed to the intensification of policies of repression and persecution towards digital activists is the success of Palestinians in their digital campaigns in 2021 during the Sheikh Jarrah uprising. Digital campaigns and activities raised attention and placed the issue of Force eviction of the PAlestinian residents of the neighborhood at the top of local and international public opinion.

## **5.2 Interrogation or investigation by the Palestinian security services for" expression of opinion "publications**

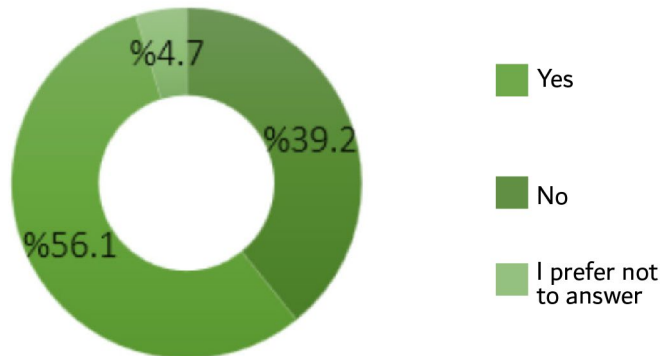
**Figure (25): Percentage of respondents (or someone they know) summoned for interrogation by Palestinian security authorities**



The results show that 37% of the respondents or one of their acquaintances were questioned by Palestinian security authorities for their digital activity. We notice that this percentage is close to the percentage of those persecuted by the Israeli security services. On the one hand, this fact indicates the escalation of the policies of repression pursued by the Palestinian security authorities. On the second hand, it indicates a state of fear and insecurity that Palestinian activists have been living in since the beginning of the war on Gaza. Participants emphasized this situation in focus groups, particularly the group containing activists and workers in digital rights institutions.

### **5.3 Pressure from social circles to remove posts expressing political or social views**

**Figure (26): Pressure to delete political or social posts**



The results show that about 39% of respondents were pressured by members of their close circle to delete political and social posts.

The results in the table appear shocking in terms of the high percentage of those who were subjected to pressure to delete posts of a political or social nature. They indicate danger associated with policies of repression, prevention, and the promotion of a culture of fear emanating from relatives in the family or close social circles.<sup>37</sup>

The discussion in the focus groups sought to find the reasons that promote accountability, review, and pressures emanating from the social circle (politically and socially.) We found two main reasons that push to pressure and practice social control to limit the capabilities of expression and political participation through the Internet: First, the pressure practiced by the Palestinian security agencies pushes to strengthen self-censorship, represented by relatives and friends, especially the elders. The second reason is increased likelihood of political and security risks emanating from the Israeli authorities, specifically after October 7th, 2023.

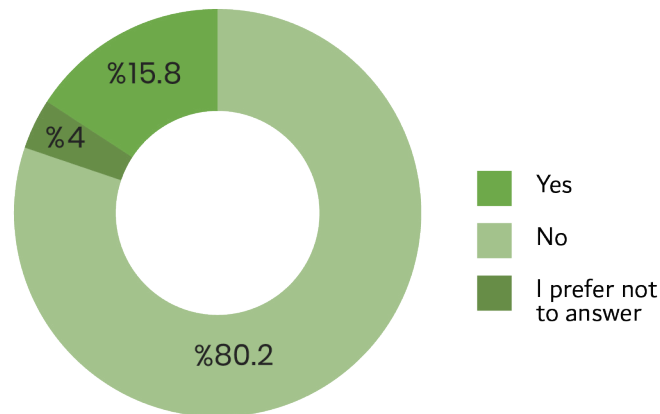
37. For more information ,see:

[Zamleh Center](#). (2017). Digital Safety and Palestinian Youth in the West Bank, Gaza Strip, and 48' territories, field survey.

Bireqdar, Muhannad. (2020). [Digital Security for Jerusalemite Youth](#). The specter of persecution and the absence of reference. Haifa – Ramallah Allah: Zamleh – The Arab Center for the Advancement of Social Media.

## **5.4 Pressure from Palestinian security services to delete political or social posts**

**Figure (27): Exposure to Palestinian official pressure to delete political or social publications**

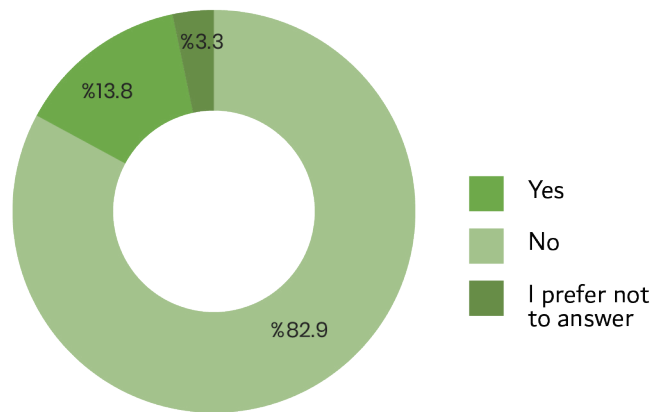


According to the results, the official Palestinian security services exerted pressure on the respondents to delete their posts by 15.8%. In comparison, about 80% of them responded that they had not been pressured to delete their posts.

This finding, when analyzed in relation to previous results, reflects an escalation in the policies of pressure on citizens, to restrain the expression of political and social positions. In this context, we can see from the discussions in the focus groups that the Palestinian security services do not exert direct pressure on young people and activists, as they sometimes resort to social circles close to the activist (father, brother, uncle, husband, friend... etc.) in order to influence and exert pressure to delete publications and stop expressing an opinion on internal Palestinian political issues. According to some group participants, "these practices are more effective than summoning for interrogation by the security services or asking directly to delete posts or stop writing on specific topics."

## **5.5 Pressure from Israeli security services to delete political posts or content**

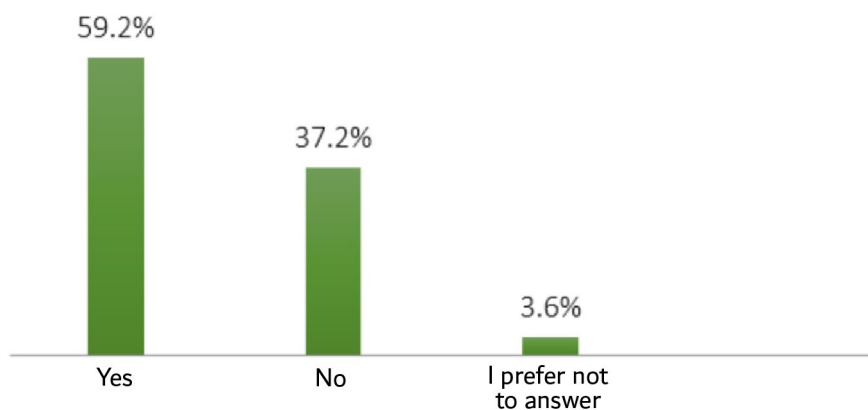
**Figure (28): Exposure to Israeli security pressure to delete political or social publications**



Findings show that 13.8% of the respondents have been pressured by Israeli security to delete posts of a political nature. Remarkably, this percentage is close to the percentage of respondents who were subjected to similar pressure from the Palestinian security services. In addition, it is important to highlight the difference in respondents' responses in item 5.1, which deals with being questioned and interrogated by Israeli security agencies personally or knowing an individual who has been questioned (51%). We must ask, "to what extent does this difference foster fear and self-censorship in users?"

## **5.6 Self-censorship**

**Figure (29): Extent to which self-censorship is practiced**

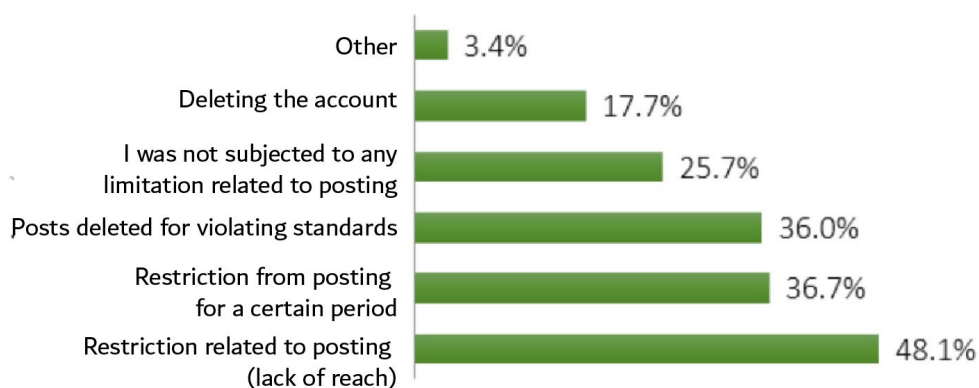


The results show that about 60% of respondents practice self-censorship when posting on social media platforms. This is the result of policies of digital repression and security and social pressure (Israeli and Palestinian) whose mark and impact have been shown in the previous items. These results confirm the validity of the conclusions of the data analysis of this research and indicate an increase in fear and anxiety among Palestinian users, especially the youth.

## 6 .The impact of social media policies on Palestinian youth activism since the start of the war on the Gaza Strip

### 6.1 Restrictions imposed on accounts by social networks

Figure (30): Types of restrictions imposed on users' accounts by social media networks

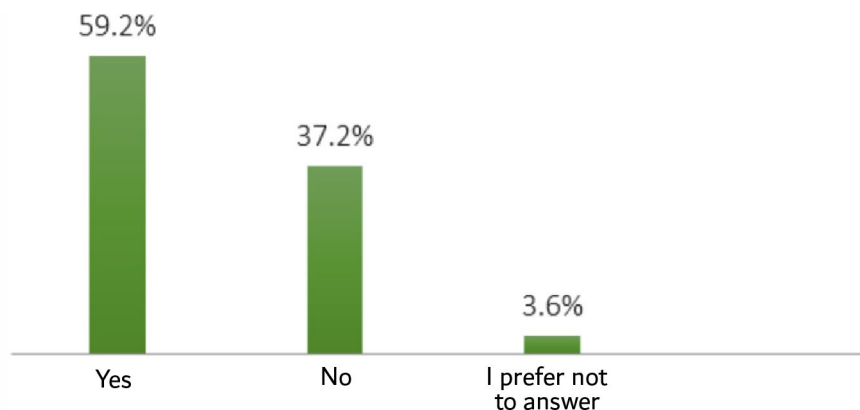


This question was devoted to the restrictions on user accounts in the first three months of the Gaza war. Respondents had to choose the type of restrictions imposed on their accounts. The results show that 48% said that their posts were subject to restrictions in access to the news feed and their friends; 36% responded that they were subjected to a publication restriction; a similar percentage said that their posts were deleted for allegedly violating the platform's standards and policies; only 25% said that they were not subjected to any restriction or deletion, and finally 17.7% responded that their accounts had been deleted.

The above list of violations shows that the most common restrictions were related to publishing. Social media companies' policies of repression of Palestinian users, as well as repressive Israeli and Palestinian security policies against activists in Jerusalem and the West Bank, resulted in a reluctance to share, write, and publish. New forms of Israeli persecution emerged in this period, as reflected in the discussion with focus groups, such as: examination of new devices at checkpoints and access to messaging applications. During the same period, arrests, prosecutions, and attacks against citizens were recorded by Israeli soldiers at various checkpoints, which reinforced feelings of fear and the choice to refrain from publishing, as the results will be presented in the next item.<sup>38</sup>

## **6.2 Cross-platform publishing restrictions and their impact on interaction with political events**

**Figure (31): Impact of publishing restrictions on interaction with political events since the start of the war on Gaza**



In order to know the impact of the digital restrictions imposed by the platforms on the respondents, the following statement was read to them: "During the past three months (after October 7th, 2023), my social media accounts have been subjected to restrictions related to publishing, which has reduced my interaction with various political events" 45% of the respondents agreed with this statement, while 50.6% answered no.

38. 7amleh Center. (2023, November). Palestinian digital rights under war: Suppression of voices, disinformation, and Incitement. [A brief](#).

The result reflects the impact of the discriminatory policies of digital platforms that are biased towards Israel and against Palestinian content. It does not reflect concerns related to Israeli authorities' persecution affecting respondents' interaction with political events in Gaza and the West Bank after October 7th last year.

The five focus groups reflected this result, with about 90% of the participants in the groups confirming that their activity on the platforms they use in all matters related to political affairs has decreased and is limited to follow-up without publishing or participating. This change of behavior was evident through discussions within the focus groups, particularly within the fifth group, which was dedicated to activists and institutions concerned with digital rights. Participants confirmed that they see a sharp escalation in digital platforms' restriction policies in general, which is proven by the field survey results.

## **Discussion, general conclusions, and recommendations:**

This study sheds light on the digital security landscape in the West Bank and Jerusalem by tracing the experiences of Palestinian internet users. This study comes at an extremely sensitive, turbulent, and shifting phase. To draw credible conclusions, the study used two methods to collect data: focus groups and a field survey (an opinion poll.)

The results presented by the study show that the issue of digital security – in the Palestinian context – has become complex and cumulative considering the different parties that violate Palestinian digital rights, and the diversity of sources of digital threats. The study found that Israel, digital platforms, Palestinian authority, as well as individuals and private commercial companies, all violate digital rights, and some have become a source of threat and extortion.

The results of the study carry strong indications of a deep gap in knowledge and awareness of digital security issues and practices among users, which made them vulnerable to various digital attacks and threats. The results show that there is a lack of basic knowledge and information structure to ensure a minimum level of digital security for Palestinian youth, for example, poor knowledge of spyware and not using the basics of digital security (changing the password periodically, setting security configurations, adding unknown people, sharing photos and personal matters, not using and running security programs for devices connected to the Internet.)

At the same time, Palestinian users realize that the Internet is not secure at all as it contains a set of risks that increase when users interact with political topics (national topics related to Israel), and these risks do not disappear if users interact with topics related to internal Palestinian political affairs as well.

The results show that exposure to threats and digital attacks prompted users to learn and become familiar with methods to protect and prevent these threats. On the other hand, it was found that a good number of users does not have any knowledge of protection programs. However, the common thing to these groups is the feeling of fear, anxiety, tension, and insecurity. It turned out that this feeling was one of the motives for self-censorship in users, in addition to social pressure practices to silence users and delete their posts. The fragmented and hybrid political reality in Palestinian occupied territory reflects the absence of freedoms, and the prevalence of gagging policies through legal texts or security practices, a situation that has become permanent and perpetuated the absence of digital rights and the loss of



security in digital environments. About 60% of respondents stated that they practice self-censorship, and more than half stated that they have been pressured by social circles to delete political and social posts.

The results indicate there is a social problem that harms Internet users and exacerbates a crisis of confidence. On the one hand, we found that one of the parties perpetrating assaults (extortion, harassment, identity theft, surveillance, and electronic prosecution) are members of social circles surrounding the users. On the other hand, the victims lack sufficient trust in the official relevant authorities to resort to them to deal with the aggressors and punish them if necessary. We found that the users' last option is to go to the police in its capacity as the law enforcement authority and that they usually prefer to resort to their family and relatives.

The results reveal that a high percentage (about 50%) of users were personally questioned by Israeli security agencies or heard about cases of investigation and questioning by Israeli security agencies. Over a third of respondents said they had personally been exposed or heard of individuals being interrogated and questioned by Palestinian security agencies.

Finally, the results show that with the start of the Israeli war on the Gaza Strip after October 7th, 2023, there is a new Palestinian digital reality in terms of the practices of digital platforms against Palestinian digital content, censorship policies, reducing access, and deleting posts, which led to a decline in the effective political participation of young people in social networks.

### **Suggestions and domains for action:**

Inspired by the results of the field study and discussions within the focus groups, the study concluded with a set of suggestions for action, which can be summarized as follows:

#### **First: Palestinian Civil Society**

- \* The digital space is an indispensable space for Palestinians of all segments, specifically the youth, and it is a space that is increasingly discussed with every confrontation with the Israeli authorities. As a result of this fact, and in light of the cases of repression and the accretion of digital attacks, prosecution

policies, and the bias of platforms and their hostility to the Palestinian human rights discourse, there is a place for collective institutional action to combat the policies of repression, at the local and global levels, through active participation in human rights groups and the activation of alternative sites, in order to introduce a new digital approach to struggle.

- \* There is a need for complementary efforts in providing professional support, whether technical, psychological, or legal call centers, to provide direct and immediate support to Palestinian citizens around the clock and throughout Palestinian communities in the different areas while taking into account the specificity of each area.
- \* As a result of the lack of institutions working in the field of digital security (or digital culture in general), as well as specialists and experts in this field, there is a need for complementarity in the activities and programs of the relevant operating institutions, and intensification in the activities of the National Coalition for Media Education, to focus on establishing and developing the concepts of digital security and digital rights. Limitations of institutions and capabilities reinforce the idea of an inclusive coalition, task sharing, and joint planning. Considering the inability of any Palestinian entity to bear all the requirements of the awareness and educational effort of all segments of society, the attacks and violations of Palestinian rights that have begun to penetrate artificial intelligence applications are deepening. This imposes integration in work and tasks and requires fostering an open line and continuous cooperation with Palestinian official authorities as well.

### **Second: The Youth**

There is a need to go beyond awareness activities on digital security issues, as it is not the only option. It is important to think about establishing institutions concerned with cybercrime and digital rights, which imposes the need to form independent civil youth groups that work to build competencies to work in everything related to digital Activism.

### **Third: The Palestinian Authority**

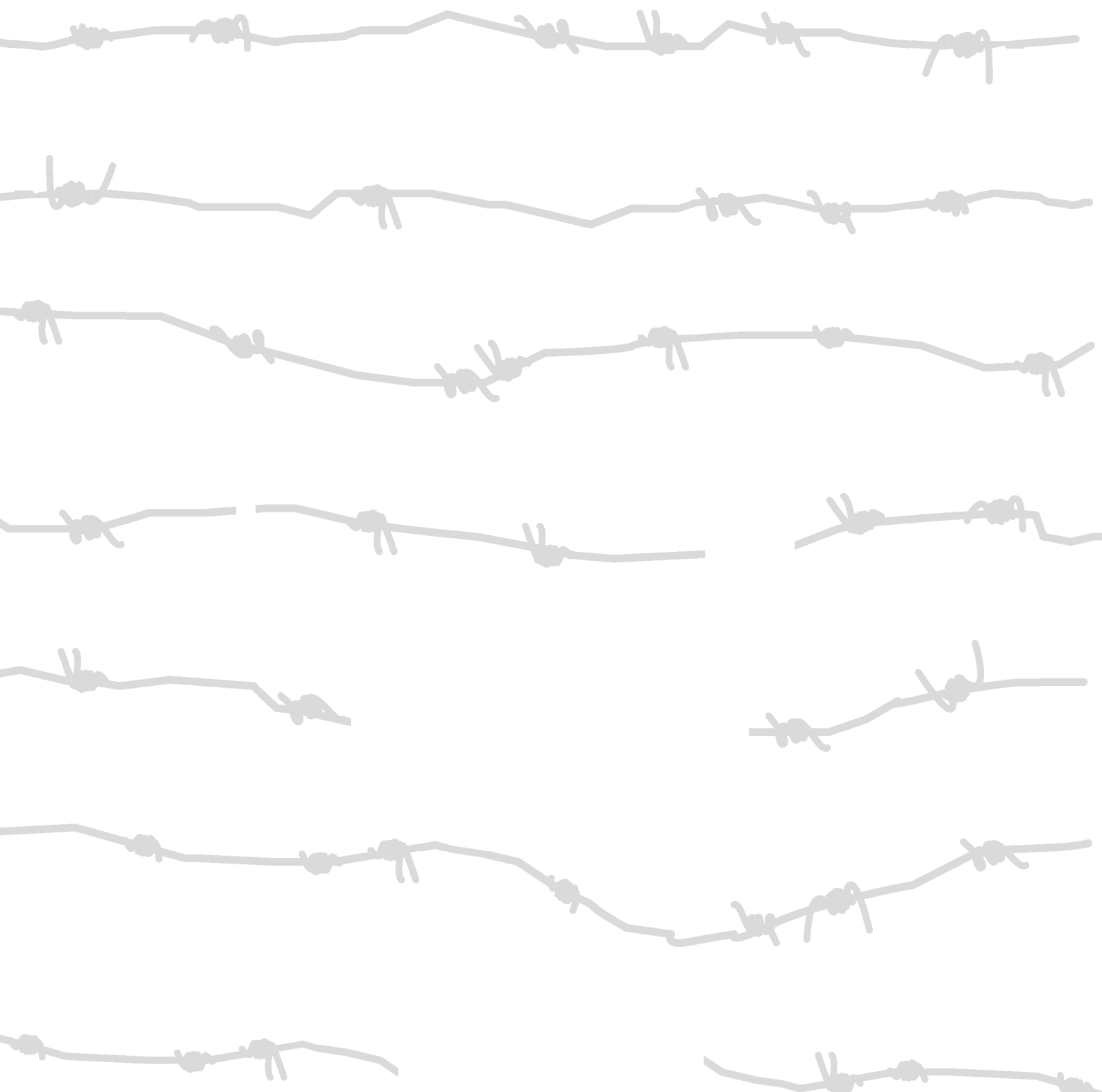
- \* There is a need for a Palestinian curriculum, and for those in charge of it to respond to the current digital reality and its transformations, as education for digital safety is an issue that is supposed to be the most necessary update in light of the

development and speed of innovation of methods of attack and assault, which is supposed to be matched by development and speed in innovating methods of protection and providing safety. This requires programmed awareness and education, and the introduction of flexible curricula that can adjust to a field that is witnessing unprecedented acceleration and progress.

- \* Considering the escalation and expansion of digital attacks, the Palestinian security services (the police) are supposed to develop their way of working and technical tools, to build a bridge of trust with Palestinian youth. Considering the increasing presence of Palestinians through the Internet, digital attacks are increasing quantitatively and qualitatively, and with them, the risks and threats increase.

#### **Fourth: Donors and the international community**

In light of the complexities of the digital security scene in Palestinian society and the overlap of many factors that cause digital violations and attacks, donors and the international community are supposed to deal with this specificity, whether in terms of becoming more aware of the complex nature of the environment that enhances a state of lack of digital security, or in terms of domains of action and work to promote and consecrate digital rights, which is an issue that imposes special local activities and approaches that deal with this particularity and start from it to fund, support, and create campaigns and action plans designed for a rapidly growing digital environment, or by mobilizing international support to strengthen digital security policies.



Contact us:

[info@7amleh.org](mailto:info@7amleh.org) | [www.7amleh.org](http://www.7amleh.org)

[Find us on social media : 7amleh](#)

