حملة – المركز العربي
لتطوير الإعلام الاجتماعي
7amleh - The Arab Center for
the Advancement of Social Media

Digital Security Among Palestinian Youth Citizens of Israel:

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

August 2024

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

Digital Security Among Palestinian Youth Citizens of Israel: 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
Design: Amal Shoufany

Contact Us:

info@7amleh.org | www.7amleh.org

Tel: +972 (0)774020670

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

Table of Contents

Executive Summary **4**

Chapter One **8**

General background and theoretical framework 8

Chapter Two **14**

Research Methodology 14

Chapter Three 17

Results of the analytical study 17

Summary and Discussion of General Findings **46**

Executive summary

This study sheds light on the digital security landscape among Palestinian Arab youth who hold Israeli citizenship, by examining the experiences of Palestinian internet users.

The study is conducted during a period of heightened tension and change. To ensure reliability, data was collected using two methods: focus groups (4 groups, totaling 23 participants of mixed gender) and a field survey (409 respondents of mixed gender). Additionally, a comprehensive review of relevant literature in digital security and digital rights was performed. The study, conducted in the first half of 2024, focused on participants aged 15-30 years.

The survey questionnaire consisted of 27 questions, distributed across five main axis: : Characteristics of respondants; Characteristics of internet usage among respondents; Extent of "digital security" knowledge and awareness of digital risks, types of digital attacks and assaults, and exposure to them; Questioning and investigation by Israeli security agencies and social and political entities for reasons related to digital activity; Impact of social media platform policies on Palestinian youth activity since the start of the war on the Gaza. After analyzing the survey data, the study concluded the following:

Analysis of the survey data revealed the following conclusions:

- **81%** of respondents use the internet at home.
- **48%** of respondents spend 4 to 9 hours online each day.
- The respondents use a wide variety of applications and social media networks, with the most popular being: "WhatsApp- **86%**", "Facebook- **83%**", "Instagram- **84%**" "TikTok- **60%**", "Telegram- **40%**", "Snapchat-30%" and "X (formerly Twitter)-**18%**".
- **67%** of respondents reported that they are familiar with or have heard of spyware targeting web-connected devices.
- **55%** of respondents familiar with spyware reported they obtained their information from reading or viewing content about such software in "magazines and websites".
- **55%** of respondents have never changed their password.

- **65%** of respondents configure security settings.
- **83%** of respondents rarely confirm friendship requests from people they do not know, while the rest confirm them at a varying rate.
- **55%** of respondents rarely share personal photos and details online.
- **69%** percent of respondents do not use anti-malware.
- **42%** of respondents do not perceive any benefit in using anti-malware.
- **27%** of respondents do not trust anti-malware.
- **79%** of respondents do not use anti-malware.
- **55%** of respondents disregard messages from unknown sources.
- **71%** of respondents use the geolocation feature.
- **10%** of respondents were subjected to a digital-attack.
- **74%** of respondents reported they have been subjected to verbal attacks or abuse (**47%** strangers and **37%** Arab acquaintances).
- **39%** of respondents chose to ignore all together and failed to reachout to anyone to address or resolve it.
- **53%** of respondents ignored the attack and assault.
- **42%** of respondents have been subjected to an attack involving "identity theft".
- **55%** of respondents have been subjected to an attack involving "harassment" or "phishing".
- **10%** of respondents have personally encountered or know someone who has encountered scrutiny and investigation by the Israeli authorities.
- **6%** of respondents have been subjected to social pressure to delete content they published.
- **70%** of respondents reported they automatically monitor their digital activity.
- **93%** of respondents said they have never been subjected to account suspension or deletion by social media platforms.

In addition to the field survey results, the study reached several conclusions through focus group discussions, the most prominent of which were as follows:

- **Removal of hundreds of contacts**. Since the outbreak of the war on Gaza, the focus groups participants have removed hundreds of contacts (friends, acquaintances, colleagues, and/or Jewish Israeli colleagues) from their social media accounts.

- **Insecure feelings**: These feelings have intensified since the May uprising in 2021 and have significantly deteriorated since the war on Gaza. Participants attributed this growing sense of unease to the increased policing and violent suppression by the Israeli security and judiciary authorities, targeting both activists and young people, even if they were not involved in socio-political activism.

- **Experiencing attacks**: A significant number of participants reported being subjected to attacks or "intrusiveness" from different parties, including security, political, social and religious entities. The participants reported that the attacks appeared to be coordinated.

- **Mistrust**: The perceived harmony between the attacking parties, and in some cases the complicity between the state of Israel, its institutions, including social media platforms, have fostered a deep sense of mistrust towards the entities that should be providing them with protection and solutions.

- **Diminishing awareness**: The Israeli government, through its security and judicial apparatus, has managed to enhance a state of self-censorship. This has been achieved by pursuing and detaining well-known figures due to humanitarian or religious posts on social media platforms. Consequently, some Palestinian political figures within Israel have urged the public to refrain from engaging on social media platforms and to exercise "self-restraint."

- **Despair**: Women human rights defenders felt deep despair due to the persecution, attacks, and harassment they have endured on social media platforms and in real life. They have become hopeless with any probable political or social change.

- **Digital Activity Decline**: The state of digital helplessness and fear experienced by women human rights activists has led to a decrease in their digital activity, limiting themselves to merely consuming news.

- **Inadequate preparedness among national and human rights institutions**: Since the onset of the war on Gaza strip (2023), preceded by the May uprising (2021),

national, civil and human rights organizations have been inadequately prepared to provide digital protection and security of their employees and beneficiaries.

Given these findings, it can be concluded that users experience persistent fear and anxiety, which is reflected in their behavior. This is accompanied by a sense of mistrust, leading to either complete indifference towards or disregard the surrounding risks. Additionally, there is a lack of preparedness among various organizations to provide digital literacy and security training to their employees and beneficiaries.

Chapter One

General background and theoretical framework

The Israeli government has practiced patterns of control, surveillance, and repression against Palestinians in Israel since the Nakba, though in different forms and with different tools that have changed over the years according to events and circumstances. The Israeli government and its institutions have treated Palestinian citizens as non-Jews and as a group of isolated minorities, and these divisions have contributed to enhancing control over Palestinians in Israel and restraining them. The events of Land Day and the First and Second Intifadas, along with subsequent events, popular movements, and uprisings, thwarted this fragmentation while restoring cohesion with other parts of the Palestinian people.[1] Ghanim described the situation of Palestinians in Israel resulting from the Nakba and the accumulated policies of Israeli governments as a "threshold position"; they live and work - civilly and politically - on the threshold of the Israeli system on the one hand and on the threshold of the Palestinian political and national center because they are part of the Palestinian people on the other. Israeli governments attempt to exploit this situation to justify policies of control, censorship, and repression, reinforced by laws and using classical mechanisms and tools alongside modern electronic tools and techniques.

The threshold position creates a fragile citizenship, whose fragility emerges when national identity clashes with citizenship identity. This is reflected in the policies of control and persecution practiced by the state, especially in pivotal collective events, for example the events of recent years when confronting the Prawer Plan (2013), the May uprising (2021) and the war on Gaza (2023).

Since its inception, the Israeli government has drawn lessons from its dealings with its Palestinian citizens, and has devised mechanisms for control and repression after witnessing various collective events that confronted policies of control and erasure. For example, after confronting the Prawer Plan (2013), whose organizers used the Internet and social media platforms, the Israeli Public Prosecution established the "Cyber Unit" in 2015 to assess challenges in the digital environment and combat cybercrime and digital terrorism, according to their statement. This unit has become a main tool in monitoring and prosecuting Palestinian content

1. Ghanim, Hanida, as cited in: Anbatawi, Khaled. (2023). A Gift at the Threshold: A Study of the Dignity Uprising in Palestinian Interior. **'Umran**, 46(12), pp. 105-147.

in the digital space, which includes, in addition to prosecution, erasing content and blocking websites.[2] This unit has stated that it is in constant contact with social media companies, such as Meta and YouTube. Since the beginning of this work, the unit has submitted tens of thousands of requests to remove and delete content prohibited under Israeli laws and according to the community standards of the social media sites themselves. Reports indicate that there has been an exceptional increase in the responsiveness of social media companies to these requests. For example, while Facebook (later Meta) responded to a few hundred Israeli requests to remove Palestinian content in 2015, the number of accepted requests reached about 20,000 in 2019.[3]

In 2021, after settler attempts to evict Palestinians from their homes and seize them in the Sheikh Jarrah neighborhood in Jerusalem, Palestinian demonstrations and campaigns of support and condemnation were launched in all areas - in the West Bank, Gaza Strip and inside Israel. The demonstrations in Arab towns and villages inside Israel developed into unprecedented confrontations, as right-wing extremist groups and settlers from the West Bank participated in attacking Palestinian citizens in Israel, and these confrontations were concentrated in coastal cities. This uprising - the May 2021 uprising - was characterized by its intensive use of the Internet and social media platforms. While the official Israeli response to this uprising was harsh and diverse in its methods, intending to sear the consciousness of the youth who participated in the demonstrations and campaigns. In addition to physical attacks on demonstrators, the Israeli government launched an arrest campaign that continues to this day. These arrests have targeted those who participate in demonstrations and those who write supportive or condemnatory posts on social media. This Israeli reaction created a state of panic and terror among Palestinian citizens in Israel. Today, in the midst of the war on Gaza, we see the repercussions from this state of panic and terror Despite the harshness of the scenes coming from the Gaza Strip, and despite scenes of global solidarity with the Palestinian people and the people of Gaza, the majority of Palestinian citizens in Israel remained silent in the first months of the war. Those who did not remain silent and did express their feelings, especially on social media platforms, found themselves pursued, arrested, and/or accused of terrorism, which reinforced practices of self-repression and created feelings of distrust and indifference among them.

2. AbuShanab, Anan. (2018). Hashtag Palestine 2018: An overview of digital rights abuses of Palestinians 7amleh – Arab Center for Social Media Advancement..
3. Luke Goldstein, Luke. (2021, July 12). How a secretive cyber unit censors Palestinians, The American Prospect.

Although the Internet has become a space for exercising political rights, self-expression, and declaring national identities, it has revealed many challenges, complexities, and contradictions. For example, in violating the principle of Internet neutrality, which requires governments and companies to treat all users according to the principle of equality and non-discrimination, or by imposing increased forms of censorship, the digital rights and individual freedoms of all are at stake.[4]

In our local context, the state of Israel is not content with the work of the "Cyber Unit" in developing and employing surveillance technology on Palestinians, Rather, Israel actively seeks to legislate its policy by enacting laws that expand its powers in pursuing both Palestinians and also any content in solidarity with the Palestinian cause. In 2016, the Knesset approved the "Anti-Terrorism Law," which aims to suppress the struggle of Palestinians inside Israel, and is considered a serious violation of freedom of expression, as the law allows Israeli state agencies to pursue Palestinians inside Israel who engage in activities expressing their solidarity with Palestinians in the West Bank and Gaza Strip.[5]

In the same context, the Ministerial Committee for Legislation of the Israeli government approved the "Renewed Facebook Law" project, which came as an extension of previous legislative proposals initiated in 2016 by then-Minister of Internal Security Gilad Erdan, and in 2017 by then-Minister of Justice Ayelet Shaked. This law proposal targets Palestinian content on social networks and seeks to delete content in solidarity with the Palestinian cause. According to the text of the proposed law, Facebook must grant the Israeli prosecution broad powers to delete content published on social networks and websites on charges of "incitement", and the proposed law allows Israeli security agencies to judicially pursue the owners of this content and charge them with committing a criminal offense.[6] More dangerously, this law grants authority to the Israeli Attorney General to use "secret evidence" that allows for the removal of content and deprives the owners of this content the opportunity to defend themselves. This proposed law can be considered a turning point in the nature of the relationship between Israeli authorities and social media companies, as the relationship of voluntary compliance has now become an obligation to combat content under penalty of law.[7] It is worth mentioning that most criminal cases related to freedom of expression in the digital space are based on the Anti-Terrorism Law and the Criminal Law.

4. Ibid, p. 251.
5. Adalah. (2016). Counter-Terrorism Law.
6. Harb, Hajar, 11 January 2022. A new law targeting Palestinian content on Social Media, AlQuds.
7. Nashif, Nadim. (n.d.). Israel's Facebook bill: An attack on Palestinian free speech. The New Arab.

The fear of political and security persecution on charges of incitement on social networks has become a serious concern for Palestinian youth. In a survey published by the Arab Center for the Advancement of Social Media - 7amleh in 2019, 59% of Palestinian youth in the West Bank, Gaza Strip and inside Israel expressed that one of the biggest obstacles to using the Internet and social media sites is the excessive censorship in them, and 33.6% of youth confirmed that they were questioned as a result of expressing their political opinions on social networks and other sites.[8]

Increased surveillance on posts and content, along with the actual pursuit of activists, journalists, and individuals active on social media networks, has created a state of high self-censorship among a wide sector of Palestinian society, especially inside Israel, which has led to a state of self-deterrence and distancing from exercising their right to freedom of expression and political participation.

Aftermath of October 7: A war on Palestinian existence

On May 7, 2023, a new amendment to the "Anti-Terrorism" law was proposed to the Knesset. This amendment empowers Israeli security agencies to pursue individuals deemed as supporters of terrorism based on their own assessments, effectively allowing these agencies to define what constitutes "terrorism." On November 8, 2023, the Knesset passed the ninth amendment, which criminalizes the consumption of "terrorist posts." Under this new law, anyone who regularly consumes content classified by Israeli law as "inciting terrorism" faces imprisonment.

This amendment introduces significant changes in the powers granted to Israeli security agencies, permitting them to target Palestinians for merely following, sharing, or reacting to content considered inciting by Israel, even if no overt action is taken. Consequently, Israeli security agencies are now authorized to scrutinize Palestinians based on their perceived intentions, representing a severe infringement on the rights to freedom of expression and privacy. [9]

8. 7amleh. (2019, October 20). '**Silenced net: The chilling effect among Palestinian youth in social media**'. 7amleh-The Arab Center for the Advancement of Social Media
9. 7amleh. (2024). Hashtag Palestine 2023: Palestinian Digital Rights in War. 7amleh- The Arab Center for the Advancement of Social Media.

The decision directly threatens and targets Palestinian citizens of Israel, aiming to deter them from expressing solidarity with their people in Gaza. Since the events of October 7th, the Israeli government has escalated its arbitrary measures against Palestinian citizens of Israel, including persecution, imprisonment, wrongful dismissals from employment, and expulsion from universities due to their solidarity with Palestinians in Gaza. This targeting constitutes a reckless assault on Palestinian existence and an attempt to suppress awareness of Palestinian rights, issues, and history.[10] A position paper entitled "Consumption of Terrorist Posts," issued by 7amleh - The Arab Center for the Advancement of Social Media, asserts that this law explicitly targets Palestinian citizens of Israel and Palestinian residents of Jerusalem. It predicts increased surveillance and violations of privacy, freedom of expression, and access to information. A significant concern is that the law criminalizes merely viewing news documents, meaning that reviewing news content could be interpreted as "supporting and aligning with terrorism".[11]

At the Internet and Digital Conference held in June 2024, researcher Hama Abu Kishk presented the results of an opinion poll concerning the activity of Palestinians in Israel during the war on Gaza and amid prosecutions. Among these findings:

56% of participants said they had heard about the "Counter-Terrorism Law," and 70% of those who were aware of the law stated that their online activity had decreased due to this legislation.

The research conclusions presented at the conference indicated that these laws lead to the silencing of the Arab community on social media platforms, while simultaneously ignoring incitement and provocations originating from Israeli Jewish parties, further highlighting how the law directly targets Palestinian citizens of Israel.[12]

Between October 7 and November 14, Israeli authorities sent a total of 9,500 requests to social media companies for post removal/deletion. Approximately 60% of these requests were sent to Meta, with a compliance rate of 94%.[13]

10. Watad, Muhammad. (2023) Threats in the amendments of the Counter Terrorism Law on Palestinians of 48. Aljazeera Net

11. 7amleh, (November 20, 2023). A Position Paper on the Israeli Law Prohibiting the Consumption of Terrorist Publications. 7amleh - The Arab Center for Social Media Development.

12. Abu Kishk, Hama. (June 10, 2024). The Spiral of Silence: The Digital Space in Arab Society (Lecture). Webbina:Conference on the Internet and Digital in Arab Society. Umm al-Fahm: Al-Khwarizmi Center.

13. Brewster, Thomas. (2023, Nov 14). Israel has asked Meta and TikTok to remove 8,000 posts related to Hamas War. Forbes.

The objective of this study is to investigate the concept of digital security among Palestinian youth in Israel, by providing recent data on the nature and characteristics of Internet usage by Palestinian youth. It aims to identify the challenges and threats facing Palestinian youth and relevant institutions, as well as the fundamental opportunities available to them, in relation to protecting their digital rights and empowering them in all aspects of digital security. The goal is to contribute to enhanced protection of digital rights, engaging in strategic advocacy, and addressing violations in the field of digital safety and security.

Research Questions:

The study attempts to answer the following main questions:

What is the nature of Palestinian youth's knowledge in Israel regarding digital security concepts, and to what extent are they aware of the digital risks they may face? To what extent have they been exposed to digital attacks and assaults? How are Israeli security agencies or social agencies held accountable in their investigations of digital activities? What is the impact of platform policies on platform content since the beginning of the war on Gaza? What types of threats, challenges, and risks do female activists and human rights defenders face in Israel?

Chapter Two

Research methodology

Research tools:

This research aims to unveil the state of digital security in internet use among Palestinian youth and human rights women defenders and utilizes the results as an infrastructure to launch initiatives for the enhancement of digital rights protection among Palestinian youth inside Israel. To achieve this, qualitative and quantitative research tools are utilized to draw results and scientific conclusions that help achieve the research goals.

The research is based on a theoretical framework that includes scientific literature reviews. To collect data, two research tools were employed to measure and comprehend the state of digital risks of Palestinian citizens of Israel. The first tool was a survey/field study (involving 409 participants), while the second was focus groups meetings.

The field study:

The field study questionnaire comprised 27 questions, covering 5 main areas:

1. Characteristics and personal details of the respondents, their place of residence, their gender, and their level of education.
2. Nature and patterns of internet use: connection location, number of hours spent online, and type of social media accounts.
3. Level of knowledge of "digital security" and awareness of digital risks and types of threats the respondents have been subjected to and how they dealt with them.
4. The extent to which the respondents have experienced scrutiny and investigation by Israeli security forces and socio-political bodies due to posts on social media platforms.
5. The impact of social media platform policies on the activity of Palestinian youth since the onset of the war on Gaza.

Focus groups:

Focus groups served as a second research tool to elaborate on the quantitative research findings. And for this purpose, four focus groups meetings were held throughout February and March 2024. All meetings were held on Zoom and facilitated by the researcher Afnan Kana'aneh.

Table (1): distribution of focus groups according to population, geographical area, gender, number of participants and meeting logistics.

M	Population	Area	Number of participants	Gender		Meeting logistics
				Females	Males	
1	High school students	Nazareth and its environs	5	5	-	
2	Youth and university students	Al-Naqab	6	5	1	
3	University students	Palestinian localities inside Israel except for Al-Naqab	6	4	2	
4	Women human rights defenders	Palestinian localities inside Israel except for Al-Naqab	6	6	-	
	Total	-	23	20	3	-

The focus groups involving high school students examined several key topics: the relationship between students and the internet; the types of platforms they use and their purposes for internet use; the digital risks they encounter and their sense of security on digital platforms; the availability of security measures at home; the impact of the assault on the Gaza Strip on their internet usage; the digital rights and security training they have received; and their views on the future of internet usage.

The focus groups with university students examined the following topics: their relationship with the internet and its evolution over time; their online experiences; the platforms they use and the motivations behind their usage; the nature of digital risks they face; their participation in digital security awareness training; their perspectives on solutions to the worsening digital security situation; and their outlook on the future.

For the focus groups involving women human rights defenders, the discussions focused on three main areas: first, the nature of their experiences with the digital environment, the types of digital threats they have encountered, and the entities responsible for these threats; second, their level of awareness regarding digital attacks within their institutions; and third, the impact of the persistent war on their digital activities.

All discussions were held in Arabic, utilizing both colloquial and standard forms. The structure and content of the discussions varied depending on the demographics of the group, as well as their roles, work nature, and connection to the research topic.

Chapter Three

Results of the analytical study

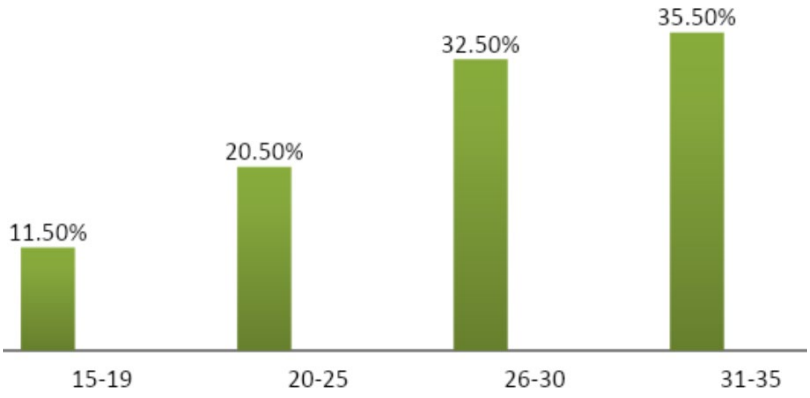
First axis: survey and focus groups findings

The first research tool was a phone opinion survey, performed by "Data New Vision" company, specializing in survey research and studies. The sample consisted of (409) respondents from Arab cities and villages in Israel.

First area: respondent demographics:

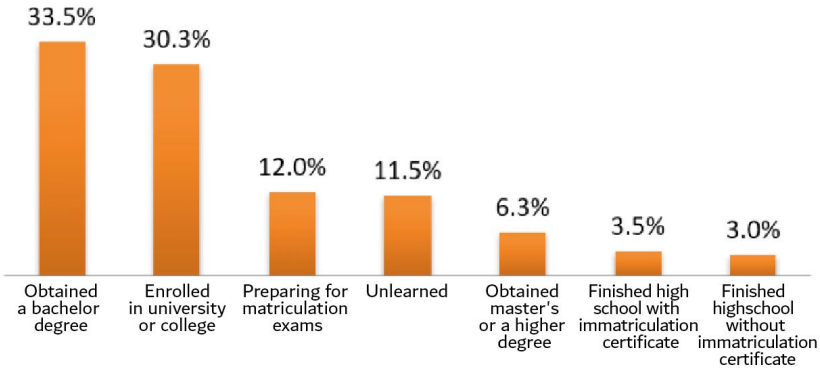
1. Distribution of respondents by age group

Figure (1) The respondents' age group



2. Respondents' level of education

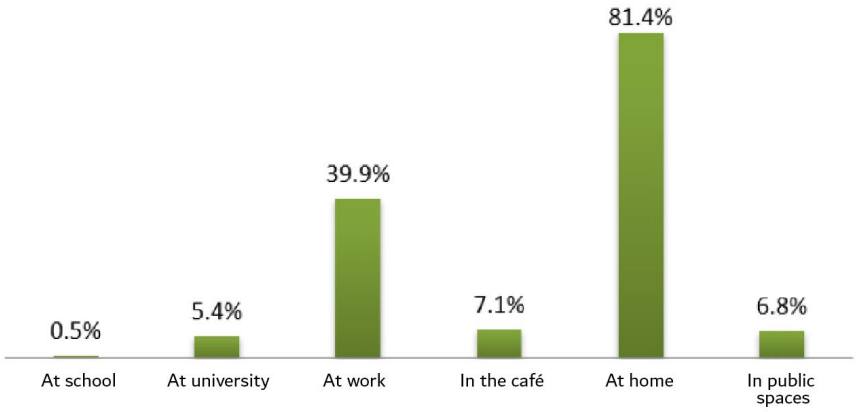
Figure (2) The respondents' level of education



Second area: patterns of internet use among youth

1. Internet Connection location

Figure (3) Distribution of respondents answers regarding main connection location



In response to this question, respondents were able to select multiple options. The results show that most of those surveyed use the Internet at home, with a percentage of 81.4%, followed by the "workplace" at 39.9%. With similar percentages, they use the Internet in cafes (7.1%), public spaces (6.8%), and universities (6.8%).

The previous results (Figure 3) indicate a decline in the percentage of Internet usage in cafes, universities, and public spaces, contrasted with an increase in usage at home. We attribute this decrease to concerns and a lack of a sense of digital security when using networks provided by cafes, universities, and those available in public spaces on the one hand, and the existence of modern communication services through Internet services offered by Israeli telecommunications companies via mobile SIM cards (3G, 4G, and 5G) on the other hand.

Despite the potential accuracy of this analysis related to the quality of Internet services, discussions with participants in the focus group organized with youth in the Negev region in the south indicated poor Internet services in those marginalized areas that are politically and administratively unrecognized. This issue was reflected in the course of the discussion held virtually via Zoom. The facilitator of the meeting faced network problems that hindered the speech of some participants, while others withdrew due to poor service and inability to speak.

2. Number of hours spent online

Figure (4) Percentage of hours the respondents spend online daily

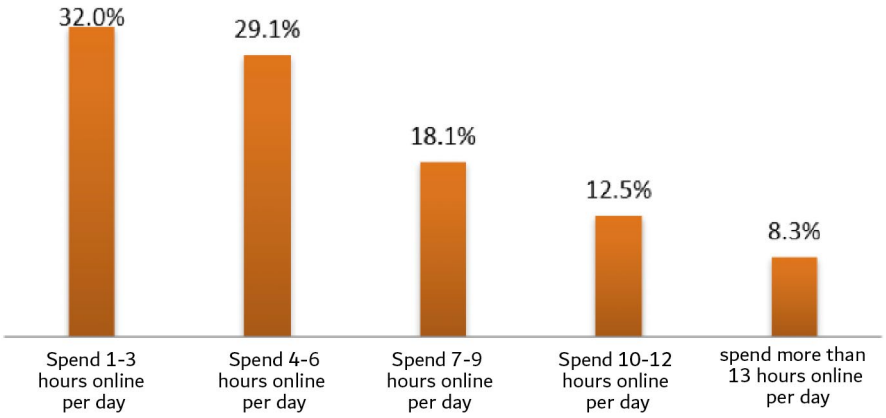
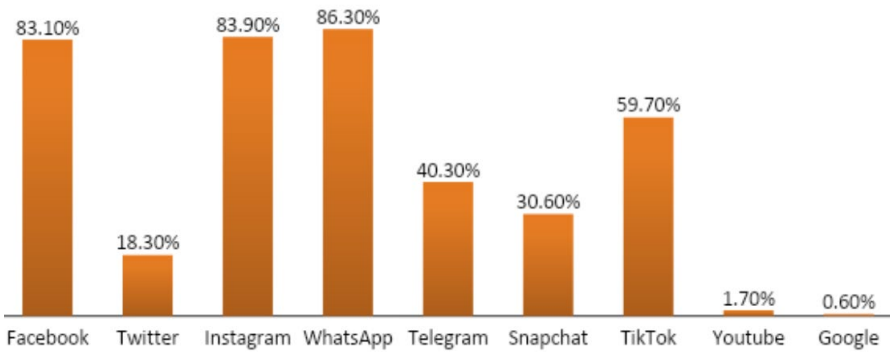


Figure (4) shows the number of hours the respondents spend online per day and the results yielded were as follows:

These findings represent a high percentage of internet use, as around half of the respondents spend 4-6 hours online per day. In discussions with the focus groups, especially youth and high school students, the participants indicated that they use the internet to consume news in the first place, and that their digital activity and involvement declined. The young respondents stated that they deactivate the feature of public posting and limit their posts visibility to friends and closed social circles.

3. Types of account on social media platforms:

Figure (5) The percentage of respondents using social media platforms and having accounts on social media platforms



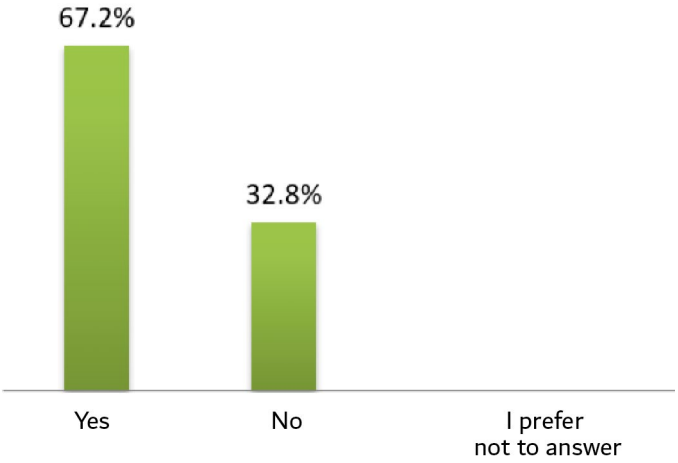
In this question, respondents could have more than one answer. Figure 5 shows the distribution of the users' activity (using or having an account) on different social media platforms. It was found that 86.3% of them use the WhatsApp application, followed by Instagram (83.9%), Facebook (83.1%), TikTok (59.7%), Telegram (40.3%), Snapchat (30.6%) and last comes X (formerly Twitter), used by 18.3% of the respondents.

The above results reflect that a group of applications and social networks such as "WhatsApp," "Instagram," "Facebook," "TikTok," and "Telegram" are at the forefront among users. The results indicate the surveyed individuals' intensive use of more than one messaging application or social network. The reasons for this may be the increasing purposes of instant messaging and following real-time news in light of heated political events. This was reflected in the focus group discussions, where some participants resorted to returning to platforms to follow daily events and news due to their inability to express themselves in public spaces within the state.

Third areas: knowledge of "digital security" and awareness of digital risks

1. The respondents 'knowledge of spyware and the risks they involve:

Figure (6) The level of knowledge among the respondents of spyware and the risks they involve



The survey posed a question to respondents regarding their awareness of spyware programs and their associated threats. The results reveal that 67.2% of respondents have heard about spyware and its threats, while 32.8% have never heard of these programs.

The proportion of individuals unaware of spyware is considered relatively high, especially in light of the increasing digital attacks, particularly those related to spyware, and specifically those developed in Israel. We view these figures with concern, even though two-thirds of respondents know about or have at least heard of these programs. However, the question remains: what are their sources of knowledge? This will be addressed in the following section.

2. Sources of knowledge of surveillance software and spyware and its associated risks

Figure (7) Sources of knowledge among respondents of surveillance software and spyware

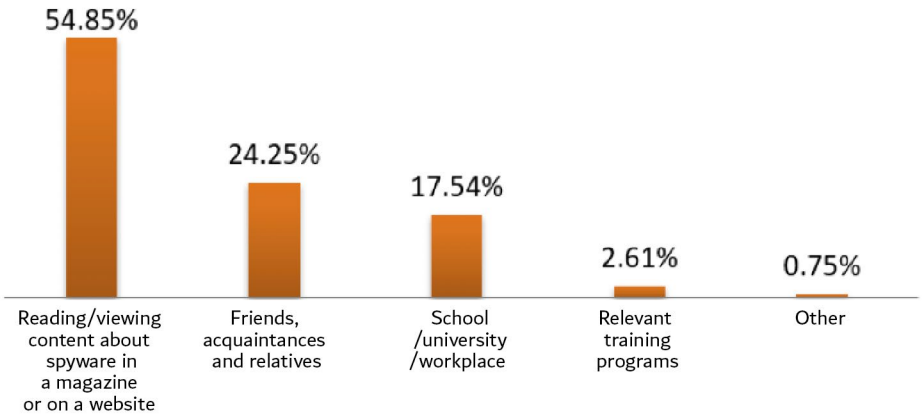
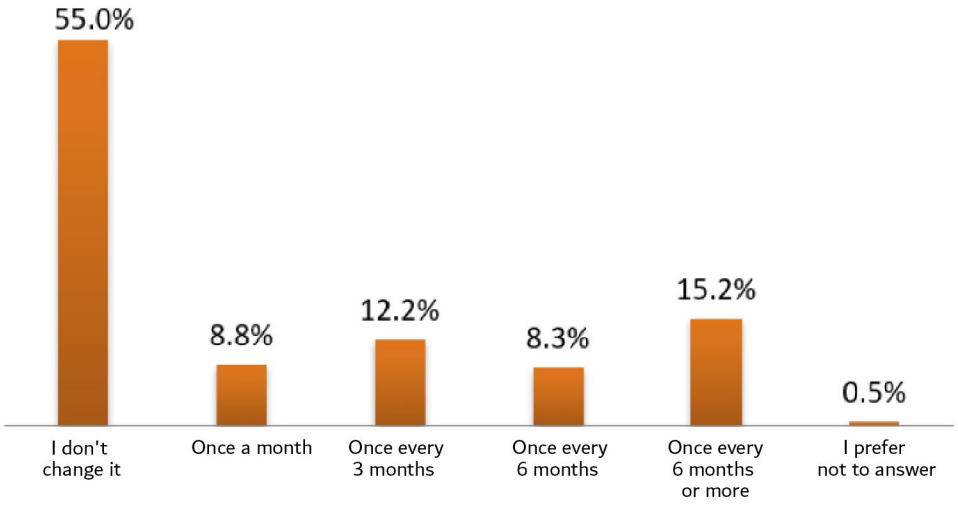


Figure 7 presents the respondents' answers concerning the sources of their knowledge about surveillance and spyware software and their threats. It shows that more than half of the respondents (54.8%) heard about or learned about this software through reading or watching about it in a 'magazine or website.' Additionally, 24.2% of respondents heard about it from 'friends, family, and relatives,' while 17.5% heard about it from 'school, university, or workplace.' Only about 2.6% heard about it through 'specialized training courses.'

The preceding results reflect an increase in the proportion of knowledge that relies on reading or watching electronic websites. Conversely, there was a decline in specialized knowledge sourced from training courses. This confirms the validity of the conclusion discussed in the previous question: Spyware and the nature of its threats require specialized and in-depth knowledge given the nature, scale, and entities behind these threats.

3. Frequency of changing the password (passwords of the different accounts)

Figure (8) Distribution of the respondents answers regarding the frequency of changing their passwords

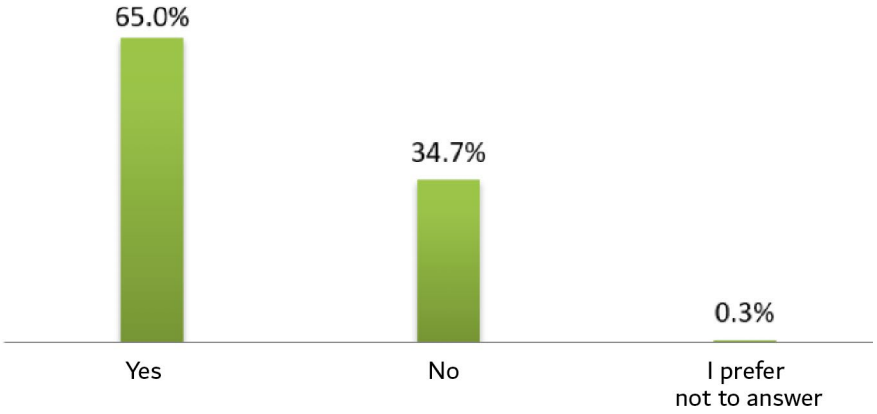


To assess the extent to which respondents engage in a set of tasks and procedures considered fundamental to digital security, they were asked a series of questions, including: 'How often do you change your passwords?' The results revealed that approximately 55% of respondents never change their passwords, while 15.2% change their passwords every 6 months or more frequently. Moreover, around 12.2% change their passwords every 3 months, 8.8% change them every 6 months, and another 8.8% change them monthly.

These findings indicate a lack of awareness regarding the importance of changing passwords, a fundamental practice for ensuring even the most basic levels of digital security. This is indicative of a lack of awareness of potential threats among more than half of the respondents. It is worth noting that understanding the significance of changing passwords does not necessarily translate into preventive practices.

4. Security settings on social media platforms

Figure (9) The percentage of respondents that activate security settings

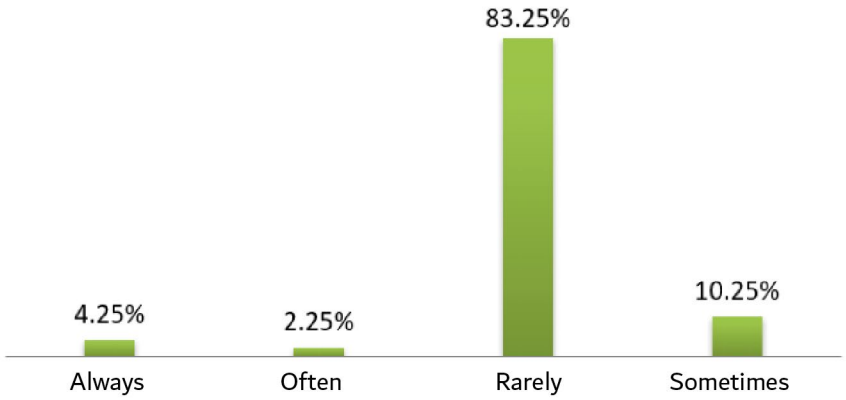


The survey revealed that approximately 65% of respondents configure their privacy settings on social media platforms, while 34.7% do not. Privacy and security settings on social media are of paramount importance for individual, group, and organizational profiles. Users should ask themselves a series of key questions when determining these settings, the answers to which provide a range of options that ensure a certain level of security if used consciously and effectively. The results indicate that nearly a third of respondents do not configure privacy settings on their social media accounts. This finding was further substantiated in focus group discussions, where a significant proportion of participants had to reset their settings, specifically disabling the public posting option, amid growing concerns about content monitoring and the targeting of activists.

reported having to reconfigure their settings, particularly by disabling public posting options, due to increasing concerns about content surveillance and the targeting of activists by extremist Jewish groups.

5. Adding unknown contacts on my social media accounts

Figure (10) The frequency of confirming friendship requests from unknown people online



Respondents were asked, "Do I add people I do not know personally to my online accounts?" Approximately 83.2% reported rarely doing so, while 10.2% indicated they do so "sometimes," 4.2% "always," and 2.2% "often." These responses carry a positive implication, as over two-thirds of young respondents do not accept friend requests from strangers. Focus group discussions revealed that participants went even further, as after the war on Gaza, they proactively removed individuals whose friend requests they had previously accepted, particularly Palestinians they did not know well or those who served or had served in the Israeli military or state security apparatus. This behavior can be seen as an indicator of the deepening trust crisis after the war. Many who had considered themselves friends or friends of friends became perceived as a threat following the onset of the Gaza conflict, as pressures, repression, and security scrutiny of political or solidarity-related posts intensified, such as through increases in practices of targeting and harassment through the reposting of content on social media for the purpose of defamation, and sometimes incitement and death threats, became more prevalent. This led participants to delete hundreds of "supposed friends" from their profiles.

6. Sharing personal photos and details online

Figure (11) The frequency of sharing personal photos and details online

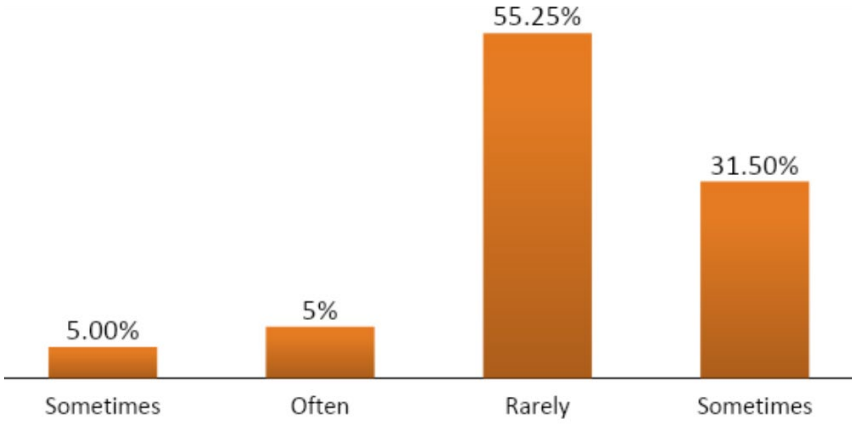
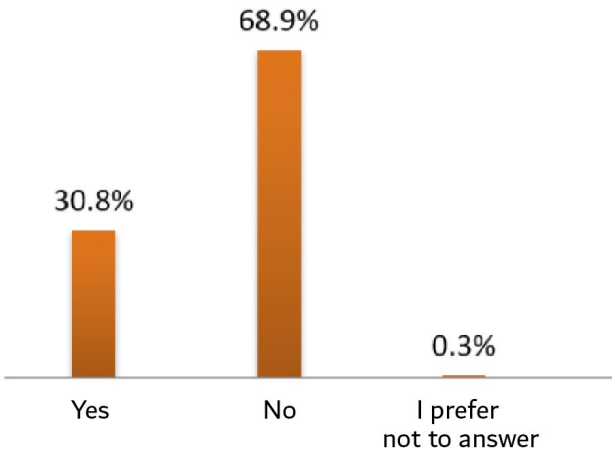


Figure 11 demonstrates that approximately half of the respondents share personal photos and information only rarely (55.2%) or occasionally (31.5%), while a small percentage share their personal matters and photos at a high frequency - often (8.2%) and always (5%). This result suggests a prevailing belief among users that the online environment is not safe and that sharing personal photos and information poses risks. However, it cannot be definitively concluded that those who reported rarely sharing personal photos and information did so due to an awareness of the risks; this could be attributed to cultural factors and habits. It is important to highlight the risks associated with sharing personal photos and information within the Palestinian context, as this data can be used for intelligence gathering and surveillance.

7. Using network security Anti-Malware software:

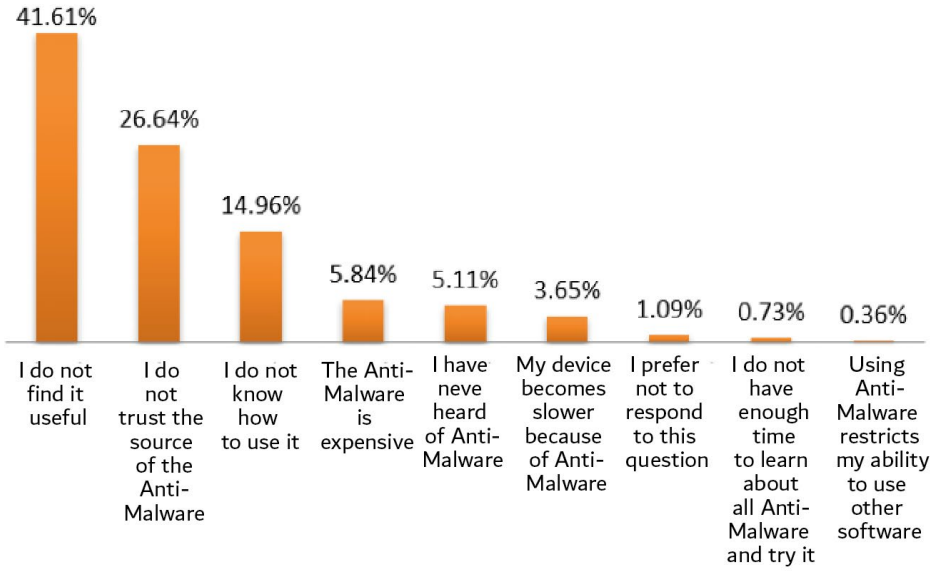
Figure (12) The percentage of respondents using Anti-Malware software



The findings reveal that 68.9% of respondents do not utilize anti-malware software on their devices, while only one-third do. This behavior, particularly among younger users, heightens their vulnerability in digital environments. The key question that arises here is: what are the reasons preventing respondents from using essential anti-malware protection? This question will be addressed in the following section.

8. Reasons for reluctance to use Anti-Malware software

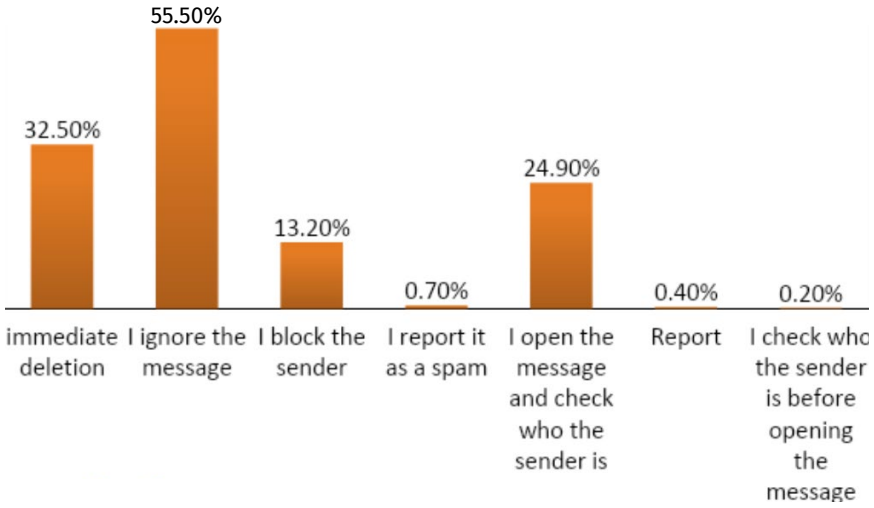
Figure (13) Distribution of the reasons behind the respondents reluctance to use



These findings shed light on the previously mentioned reluctance to use anti-malware software. Two primary reasons stand out: 41.6% of users do not find anti-malware software useful, and 26.6% do not trust it. These figures underscore a significant issue of mistrust and skepticism among Palestinian citizens of Israel. Additionally, approximately 20% of respondents indicated that they lack knowledge about anti-malware software, 14.9% stated they do not know how to use it, and 5% mentioned they have never heard of it. These results reflect a profound gap in trust, knowledge, and availability of resources for raising awareness and training on the use of anti-malware software, given the current environment of surveillance and repression.

9. Reaction to receiving messages from unknown sources

Figure (14) Distribution of the respondents' reactions upon receiving messages from an unknown source



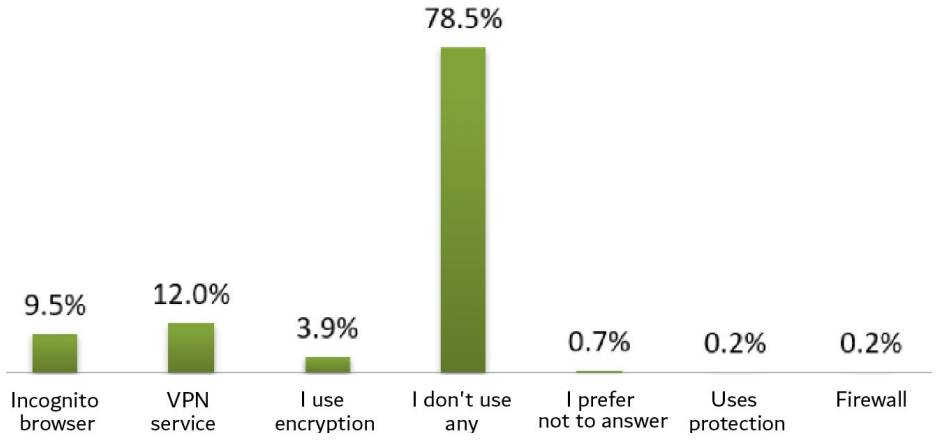
This section examines how respondents handle messages from unknown sources, where they could select more than one response. The results show that the most common reaction, chosen by 55.5% of respondents, is to ignore such messages. Other actions include deleting the message right away (32.5%) and blocking the sender (about 13.2%). Additionally, 25% of respondents said they open the message to check who the sender is.

Ignoring messages from unknown sources is generally a wise practice, but it often lacks an understanding of who the sender is or what their intentions might be (whether related to security, commercial interests, policies, or social issues). Since there is a chance that the same sender may try to contact the recipient again and that the recipient might eventually open these messages, the potential risks could be serious, particularly with the growing sophistication of phishing, surveillance, and hacking techniques.

These findings, along with insights from focus groups, highlight the urgent need for comprehensive training for users of all ages on how to handle messages from unknown sources.

10. Digital protection while using internet

Figure (15) Distribution of protection methods adopted by respondents while browsing the internet



The responses to this question are consistent with those given in earlier questions regarding digital protection. It was found that 78.5% of respondents do not use any protection tools, around 12% use a VPN;[14] 9.5% of the respondents use a blind browser,[15] and 3.9% use encryption.[16]

These figures are striking, particularly given the respondents' awareness of digital risks and threats. However, this awareness does not seem to translate into protective practices. This suggests a broader disregard for digital security risks and a sense of mistrust, especially considering focus group discussions where participants recounted their experiences with threats from personal or fake accounts, as well as from Israeli security agencies.

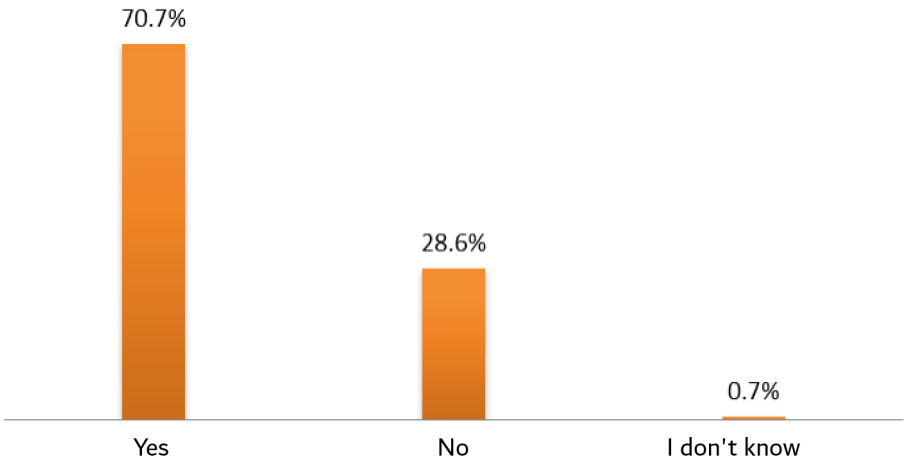
14. VPN enables internet connection without revealing the user's physical location.

15. Blind browser prevents tracking and monitoring of the websites that a user visits.

16. Encryption allows messages to be transformed into encoded information using a special algorithm.

11. Geolocation feature

Figure (16) The percentage of respondents activating geolocation feature

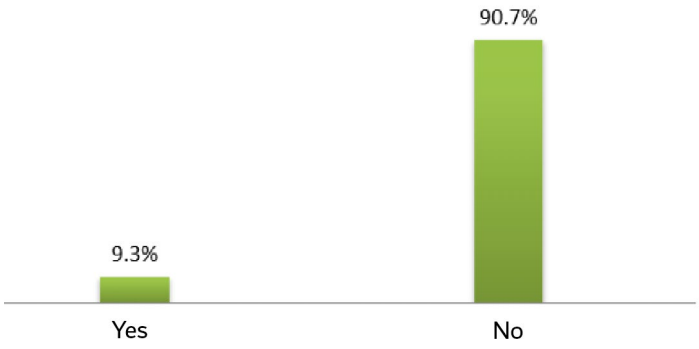


The results reveal that 70.7% of respondents use the geolocation feature, which heightens the risk of exposing their physical locations, while 28.6% of them stated that they do not use this feature. This practice introduces a range of digital risks with significant socio-political consequences, such as the potential use of location data for threats, arrests, and violations to digital privacy. This behavior indicates a lack of awareness among young people about the dangers of enabling such features offered by social media platforms. Additionally, these findings align with previous data suggesting a prevalent belief among respondents that activating protective tools is ineffective.

Fourth axis: Digital Attacks and Abuse

1. Experiencing abuse, attack or extortion by intruders or "hackers"

Figure (17) Percentage of respondents who experienced digital attack



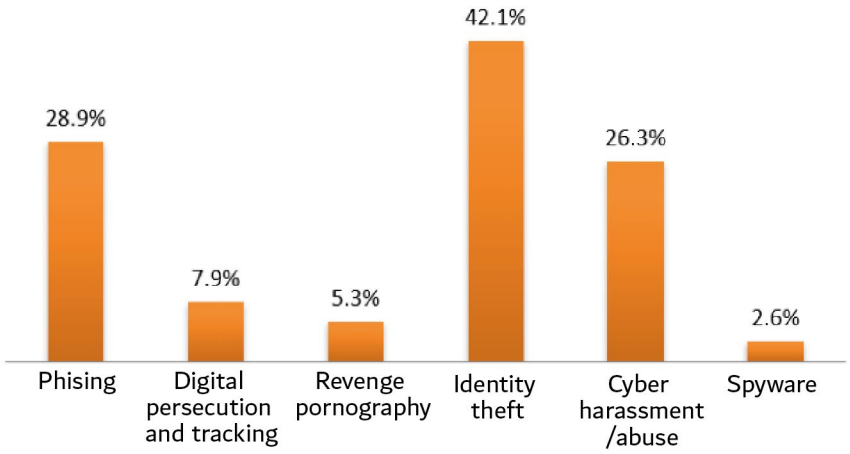
The findings reveal that a substantial majority of respondents (90%) have not faced digital attacks, abuse, threats, or extortion from intruders or hackers. Nevertheless, 9.3% of respondents reported experiencing such incidents. While this percentage might seem minor at first glance, it highlights underlying problems and behaviors among internet users involved in these situations, as further elaborated in the following sections, and reinforced by focus group discussions.

The proportion of respondents facing digital attacks highlights profound issues, including a lack of awareness and understanding of digital threats, as well as a tendency to dismiss or downplay these threats without developing the necessary skills and practices for digital protection.

Focus group discussions shed light on this statistic, revealing that many participants had encountered digital attacks from "intruders" or "hackers," often driven by national or political motives. The testimonies of youth, university students, and women human rights defenders highlighted that these attacks frequently had social, political, or religious sources. Additionally, there has been a significant rise in such attacks and digital suppression following the war on Gaza.

2. Types of digital attacks

Figure (18) Types of digital attacks experienced by respondents

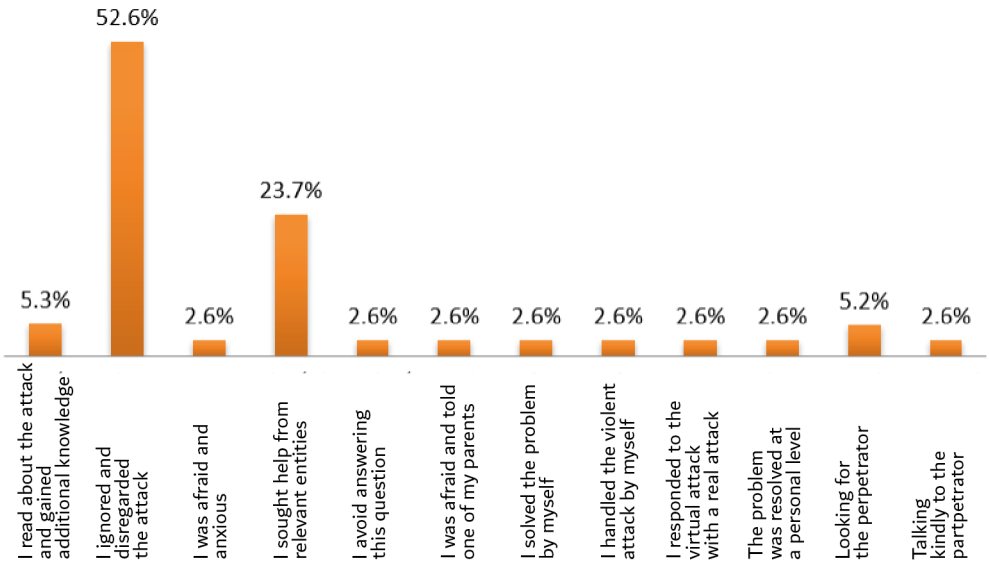


We sought to ascertain the nature and types of attacks and assaults experienced by respondents through our field survey. In this section, respondents were provided with a simple definition for each of the proposed answer options to standardize concepts among participants. The results indicated that 42.1% of attacks/assaults were of the 'impersonation' type - meaning the creation of fake social media accounts using the target's name and image, or the hacking and takeover of accounts. Attacks of the 'phishing' type accounted for 28.9% - referring to a type of cybercrime where attackers attempt to deceive individuals into providing sensitive information such as usernames, passwords, and credit card details by posing as a trusted entity. Phishing is typically carried out through email, text messages, or fake websites. Harassment and digital abuse accounted for 26.3% of attacks/assaults, referring to the hostile use of social media to bully, threaten, and harass someone by commenting on content they have posted or commented on. Attacks and assaults involving 'stalking and online harassment' - meaning pursuit that includes false accusations, defamation, and slander, or the monitoring or publication of a person's sensitive personal information online - occurred at a rate of 7.9%. Attacks and assaults involving the misuse of images (revenge porn) - meaning the publication of explicit sexual images or videos without the consent of the victim depicted in these materials, or the publication and distribution of intimate, sexual, or pornographic images or videos of individuals without their consent - occurred at a rate of 5.3%.

The results indicate a prevalence of attacks related to the categories of 'impersonation', 'phishing', and 'cyber harassment and abuse'. As for 'online stalking and harassment', the perpetrators were often extreme right-wing settler movements that sought to harm Palestinian political activists since the war on Gaza. Discussions with focus groups revealed an overlap between the entities perpetrating digital attacks, that span social, political, and security spheres. This overlap in the nature of the perpetrating entities multiplies digital threats, as Israeli police do not provide real protection and do not take complaints seriously, according to participants in in-depth discussions.

3. The respondents' response to digital attacks

Figure (19) The respondents reaction to the digital attack

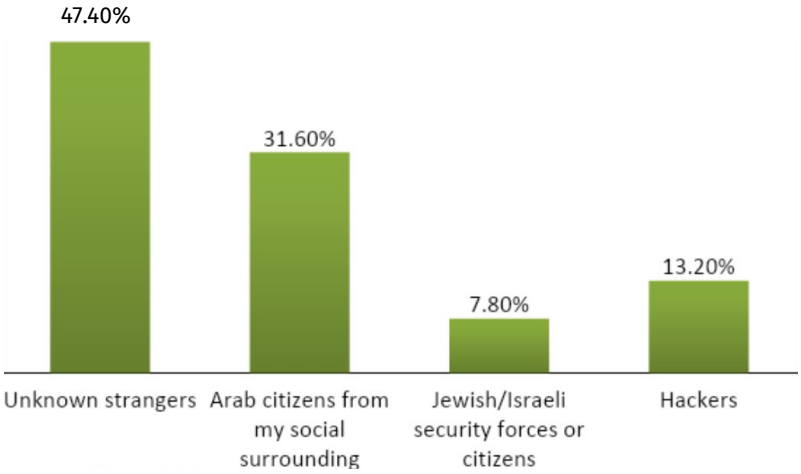


The results (see Figure 19) indicate that most respondents responded to digital attacks by disregarding and ignoring them (52.6%). Meanwhile, 23.7% sought assistance from specialized entities. A smaller segment, 5%, chose to learn more about the attack they encountered, while the same percentage opted to disclose the perpetrator's identity. These findings underscore a significant mistrust among users towards both state and non-state institutions, with only a third of respondents seeking help. This pervasive mistrust, combined with the lack of supportive entities and official institutions, contributes to the general indifference observed throughout the survey.

The focus group discussions revealed that most young respondents do not take adequate measures to address digital attacks, reflecting a broader trend of disengagement and lack of proactive response.

4. The perpetrators

Figure (20) The digital attacks perpetrators

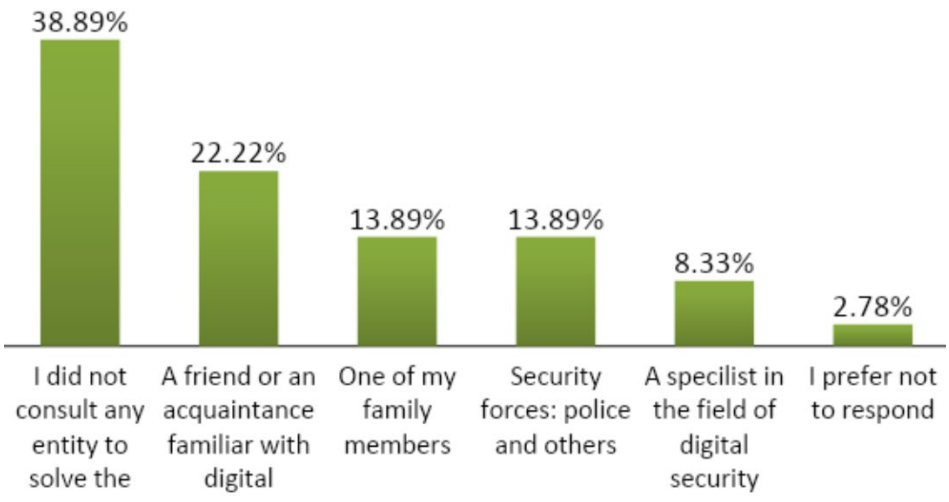


The findings (Figure 20) indicate that approximately 47.4% of the perpetrators were unknown strangers, according to respondents. Meanwhile, 31.6% reported that the attackers were individuals from their own social circles, 13.2% identified them as hackers, and 7.8% attributed the attacks to Jewish/Israeli citizens and security forces.

These results must be considered in conjunction with the previous section, particularly regarding respondents who chose to ignore the digital attacks. If the attackers are unknown strangers and the attacks are ignored, these individuals are likely to attempt further attacks due to the lack of reporting. Additionally, attacks carried out by individuals within the same social circle could exacerbate mistrust between users and their immediate environment.

5. Entities consulted by the respondents following the digital attack

Figure (21) Entities consulted by respondents following the digital attack



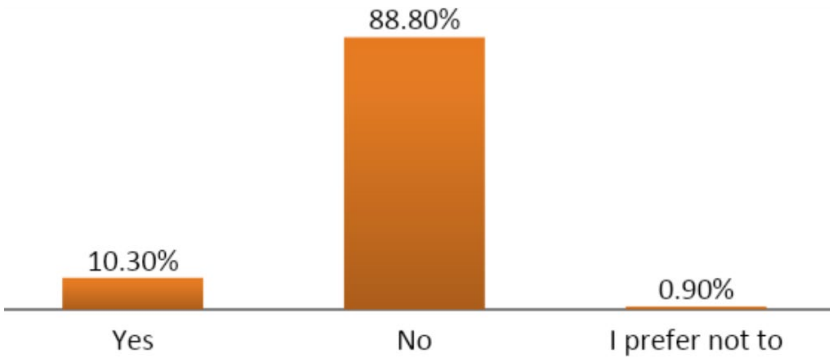
The results (Figure 21) reveal that 38.8% of respondents opted to ignore the issue and did not seek assistance. In contrast, 35% sought advice from their close circle: 22.2% consulted friends or acquaintances knowledgeable in digital security, while 13.8% turned to family members. Approximately 22% sought help from official or professional organizations, with 13.8% reaching out to police and security forces, and 8.3% consulting digital security experts.

The data indicates that Palestinian internet users and citizens of Israel frequently choose to either ignore the problem or rely on their immediate circle for support. This trend highlights a profound mistrust of official institutions that are expected to provide assistance, underscoring the need for trustworthy support systems for Palestinian youth and emphasizing the critical need for digital security awareness at the family level. These findings are further corroborated by discussions in the focus groups.

Fifth axis: scrutiny and investigations by security forces

1. Scrutiny or investigation by Israeli authorities about opinion posts

The percentage of respondents (or someone they know) convoked for investigation by Israeli security forces

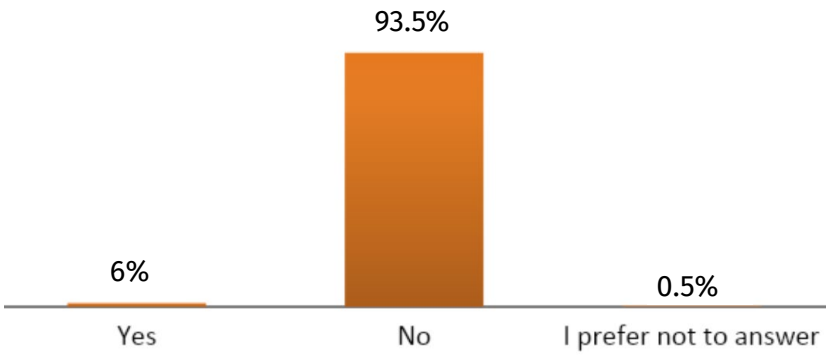


The findings reveal that about 10.3% of respondents, or individuals within their close social circles, were convoked for interrogation or investigation by Israeli authorities due to posts on social media. Conversely, 88.8% reported never having been convoked for such inquiries. However, focus group discussions painted a contrasting picture. In the candid environment of these discussions, participants felt encouraged to share

their own experiences and those of people they know, highlighting a growing trend of targeting activists. This has heightened a climate of fear and distrust around sharing political opinions online, a situation that became particularly pronounced after the Dignity Uprising in May 2021 and has further escalated since the onset of the war on Gaza on October 7, 2023.

2. Pressures exerted by close social circles to remove posts expression social or political opinions

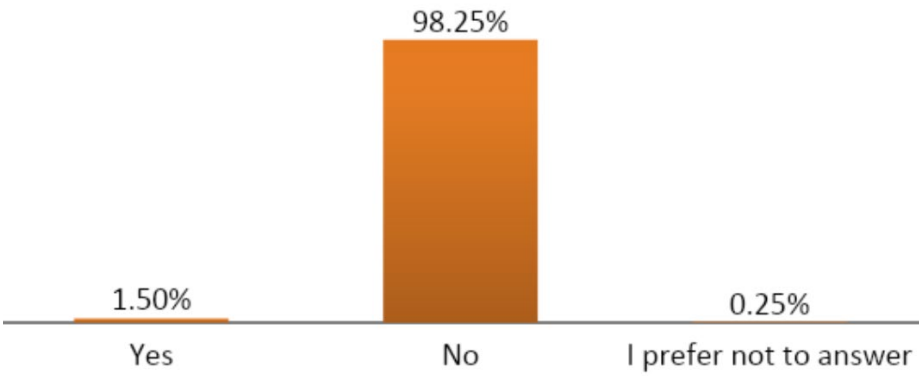
Figure (23) Experiencing pressures to remove political or social content



The results reveal that 6% of respondents have faced pressures from close social circles to remove posts or content expressing political or social views ,while93.5% reported no such pressures .Nonetheless ,focus group discussions presented a different scenario .Participants described persistent pressure from close family members—such as fathers ,brothers ,and uncles—to deter them from commenting on social and political events ,or to remove posts from social media .These discussions highlighted that the Israeli Security Agency) Shin Bet (capitalizes on the traditional, patriarchal dynamics within Palestinian society to exert influence over activists and women human rights defenders .This approach aims to stifle freedom of expression on political issues and events related to the war on Gaza .Such practices were notably prevalent among Palestinians from Al-Naqab and women human rights defenders more broadly.

3. Pressures exerted by Israeli security circles to remove political contents or posts

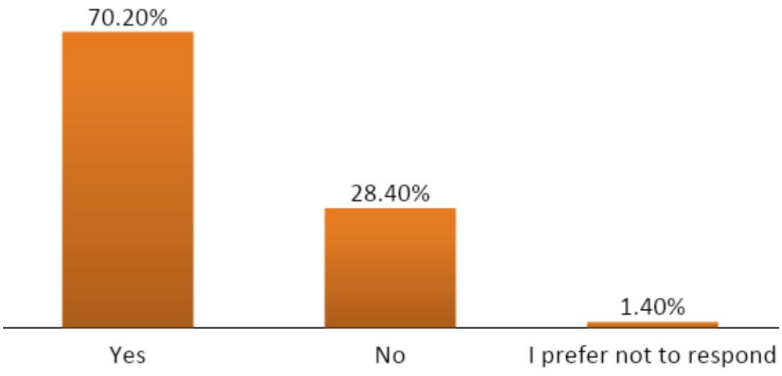
Figure (24) Experiencing pressures from Israeli security circles to remove political or social content



The results indicate that only 1.5% of respondents have reported direct pressure from Israeli security entities to remove political posts, while a substantial 98.2% have indicated they have not encountered such pressures. This disparity suggests a prevalent practice of self-censorship among respondents, driven by a desire to avoid potential scrutiny and persecution from Israeli security circles. This observation is reinforced by focus group discussions, in which a considerable number of participants—excluding high school students—recounted experiencing pressure from security circles. It is noteworthy that, since the onset of the war on Gaza, Israeli security authorities and far-right groups have intensified their intimidation tactics, inducing significant fear and anxiety among individuals. This has led to a heightened and pervasive level of self-censorship. Similar patterns of suppression were evident during the May 2021 uprising, as reported by a young participant, and have been exacerbated during the ongoing war on Gaza. The following section provides a detailed examination of these findings.

4. Self-censorship

Figure (25) Practicing auto-censorship



The results reveal that approximately 70% of respondents engage in self-censorship when posting content on social media platforms, whereas 28.4% report not practicing such restraint. These findings likely stem from the effects of digital repression policies and the social and security pressures that have cultivated a deep-seated mistrust, as detailed in previous sections. This perspective is further supported by focus group discussions, where participants described their frequent efforts to avoid commenting on or publishing content online due to the intimidation and persecution tactics employed by Israeli authorities, both officially and unofficially.

Sixth axis: the impact of social media platforms policies on the digital activity of Palestinian youth since the onset of the war on Gaza.

1. Accounts restriction by social media companies

Figure (26) Types of restrictions imposed on users' personal accounts by social media networks

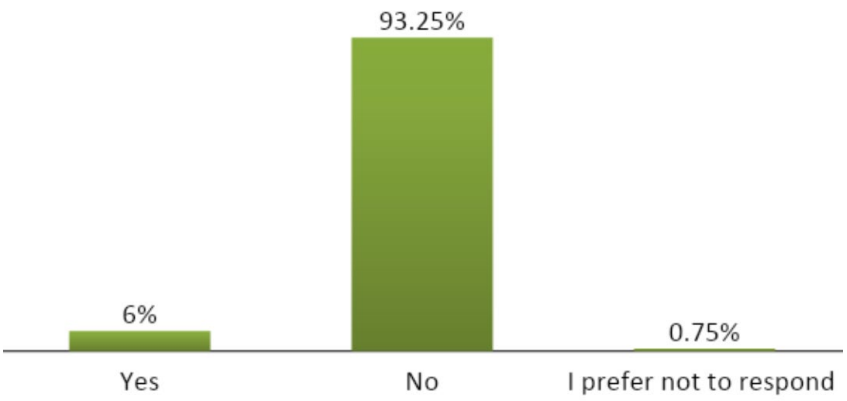
This question (Figure 26) investigated the restrictions imposed on respondents' social media accounts during the first three months of the war on Gaza. Respondents were asked to specify the types of restrictions they encountered. The data reveals that 92.7% of respondents reported no restrictions or suspensions on their accounts. Conversely, 4.2% indicated that their posts were restricted from being visible to their contacts and in news feeds, while 2.7% noted that their posts were removed for allegedly violating platform standards and policies.

These findings underscore the impact of Israeli authorities' policies on how citizens engage with the war on Gaza. They reveal that, in contrast to Palestinians in the West Bank and East Jerusalem—who face more severe restrictions on publication and visibility—the majority of respondents experienced relatively few limitations on their online activities.

The focus group discussions further illuminate these results. They indicate that Palestinian youth citizens of Israel often felt constrained to use social media solely for following news updates, refraining from commenting due to the restrictive nature of their public environments, such as universities and workplaces, which limit their freedom of expression. Additionally, some participants and activists chose to suspend their online activities or deactivate their accounts following the war on Gaza, driven by concerns that these accounts could be exploited in phishing and targeting campaigns initiated by Israelis.

2. Restrictions on social media publications, and their impact on reactions to political events

Figure (27) The impact of restrictions on reactions to political events since the onset of the Gaza war



To assess the impact of digital restrictions imposed by social media platforms on respondents, they were presented the following statement: "My accounts on social media platforms have been subjected to restrictions related to publications, which has reduced my responsiveness to various political events in the last three months (since October 7th)." Only 6% of respondents agreed with this statement, while 93.2% did not.

Focus group discussions offer valuable insights into this result, which appears paradoxical. Participants reported that their responses to the Gaza events were extremely limited, often confined to posting humanitarian content, and they faced significant scrutiny and persecution. Additionally, some participants chose to avoid political and social interactions altogether, despite their strong patriotic sentiments, which led to feelings of anger, frustration, and helplessness.

Secondly: Findings from the Focus Group of Women Human Rights Defenders (HRDs)

The focus group on women human rights defenders within the country comprised six women activists. Their professions were distributed as follows: lawyer; volunteer in a cultural and social association; media coordinator in a relief association; employee in an institution concerned with internet issues and human rights; journalist; member of the Communist Party; youth activist; volunteer in several human rights institutions. The discussion with the activists lasted for 3 hours and centered around the following points: the reality of activists' use of the internet and social media; their level of awareness of digital security; the role of the institutions they work for in providing them with digital protection; the sources of violations of digital rights and the nature of the attacks they have been subjected to; and the impact of the war on Gaza on their digital activism.

The objective of the discussion in the group was to assess the level of awareness of women human rights defenders regarding digital security in relation to their work and activism, in order to provide means of prevention and resources to ensure their safety and prevent digital risks and violations against them, and to work towards strengthening the legitimacy of their work through the enactment of laws and the development of policies, especially since they are active during times of crisis and in conflict zones.

The following are the most prominent findings of the discussion:

Women Human Right Defenders are more cautious in narrating their digital experiences

A prominent theme in the discussion was the extreme caution exercised by the participants in revealing details of their personal experiences. They strongly

emphasized the importance of not mentioning their names, the institutions they work for, or any other detail that could identify them. Furthermore, they did not fully disclose their experiences in the digital environment during the discussion, despite confirming that they had received various threats and attacks in both the digital and physical worlds where they were heavily involved. This led to a decline in their digital activism and engagement with various human rights issues, a situation that was exacerbated by the Israeli war on Gaza.

Women Human Rights Defenders Experiencing a Loss of Hope for Effecting Change

The in-depth discussions with the participants revealed a profound sense of hopelessness regarding their belief in their ability to effect political and social change. This was accompanied by feelings of general frustration, helplessness, and at times, oppression, powerlessness, and anger in the face of the political, social, cultural, and human rights circumstances they were living under. This sentiment was reflected in their reduced physical presence on the internet and social media platforms, as well as in their diminished engagement with human rights, social, and political issues on these platforms.

Diverse and Numerous Digital Attacks Against Women Human Rights Defenders

Discussions with the women activists revealed a wide range of entities perpetrating digital attacks, pressures, and threats against them. These included Arab political parties seeking to suppress activists by silencing their criticism; members, heads, or candidates of local councils in Arab cities and towns; threats and pressures from individuals belonging to large families (especially when criticism targeted family elders); digital attacks originating from the Israeli government, its institutions, and security apparatus; and finally, Israeli settler groups who monitored the activists' accounts, stalked them, and issued constant threats. While these practices intensified significantly after the war on Gaza, creating an atmosphere of repression and fear, they had also existed before the war, albeit to a lesser extent.

The discussions highlighted a common pattern in the sources of pressure exerted on female activists. These sources often resorted to the activists' immediate social circles (fathers, brothers, uncles, cousins, family elders) to demand the deletion of posts, reduce the intensity of criticism, or refrain from expressing opinions online, ultimately leading to a cessation of political and human rights activities in the field.

The participants noted widespread and frequent community interventions regarding their online content. Their motivations were often questioned, and their fathers were perceived as authoritative figures responsible for their actions, even authorized to impose restrictions and control over them. Consequently, these fathers were frequently targeted with requests to reprimand their daughters, making them intermediaries for delivering warnings and thus participating in the suppression process involving multiple parties within the activists' immediate social circles. As one participant stated, "Community warnings increased: I was warned by people who were close to me, and even by distant people who felt entitled to reach out to those close to me and tell them to make me be careful, for example... If I posted a picture of the Palestinian flag, I would be warned."

Moreover, the conversations revealed instances of attacks on women human rights defenders by powerful men holding high positions or public figures with a large following. In some cases, these public figures encouraged their supporters to attack the women human rights defenders.

Gender-Based Digital Restrictions

The women human rights defenders argue that a significant portion of the digital attacks and pressures they face are fundamentally rooted in gender-based reasons. Society grants men the authority and legitimacy to violate women's rights and subjugate them simply because they are women, regardless of the issues they address. This is often exacerbated by factors such as age (being young activists) or social status (mothers, divorced women).

Decreased Platform Usage and Account Deletion

The discussions revealed a diversity of motivations for digital attacks (including political, social, religious, etc.), which had a negative impact on all participating activists. A prevailing sense of reluctance to use digital platforms and social media networks emerged, translating into a weaker virtual presence compared to previous years. The discussions reflected a significant decline in their sense of digital security and in the guarantee of their digital rights amidst the current situation during the ongoing war on Gaza. Some activists perceived that the free space previously offered by these platforms had diminished considerably, especially after launching the war on Gaza. Everything they posted became a source of threats, persecution, arrest, and moral assassination by state agencies or extremist groups that specifically targeted Arab Palestinians and women activists.

The War on Gaza: A Turning Point for Digital Attacks

The activists unanimously agreed during the third segment of the discussion (awareness of digital security and understanding digital risks) that the war on Gaza and the escalating fears that accompanied it marked a significant turning point in their activism and self-expression.

All the activists used phrases like "*before the war it was one thing, and after the war it was another*," without implying that the situation before the war was significantly better. However, what was certain for the activists was that the risks had doubled after the war, and the sense of digital security had completely vanished in light of the scenes coming from the Strip and the fears reinforced by threats issued by state security agencies and the arrests of well-known figures for posting a single "post." The persecution and fear of participating in anti-war protests in the field had a profound impact on the digital environment and on citizens' discussions of human rights issues. Some women reported being monitored, tracked, and digitally surveilled, even for comments made by staff members within their organizations. Some organizations even removed lists of their employees' names from the internet for fear of them being pursued and monitored by security agencies or extremists due to their work in defending Palestinian rights. One activist stated:

"*Every day I wake up literally looking at the news to see if there's a report about me (defamatory material online). Not just about me specifically, but also about the employees I work with. They published a murderous report about our manager, saying: 'Why is he still alive?' Literally. They asked why this person is still alive? And the threats spread widely. Our photos as employees were spread on social networks. A lot of details about us were spread. And I think it became very scary*."

Institutions Failing to Provide Minimum Digital Security Standards"

The discussions with the group of activists revealed a significant portion of the institutions they work for do not provide even the minimum standards of digital security to ensure the safety of the activists. **This lack of institutional support exposes activists to increased risks and vulnerabilities**. On the other hand, others confirmed that the institutions they work for have implemented policies to address digital threats, particularly after the war on Gaza. These policies include a set of digital standards to ensure a minimum level of security for employees, their data, and those they serve. Additionally, some activists stated that they separate their work from their digital human rights activism and the expression of their personal opinions.

Erosion of Digital Social Capital

The testimonies of female activists reveal a concerning decline in digital social capital within online networks. This term describes the diminishing trust and solidarity between an activist and their online community – friends and followers alike. This crisis of trust has driven some activists to take drastic measures: deleting hundreds of "friends," unfollowing others, and even closing their accounts entirely.

One participant poignantly described her experience:

"Distrust has skyrocketed lately. During the war, I still used Instagram. But then I saw this... a file (a provocative report monitoring our comments). They'd been tracking girls and boys, recording the posts they made on October 7th. My fear doubled. Distrust – it means you can't even trust the people you thought were close. I noticed most of the stories used were from close friends. That was really difficult for me."

Another activist shared her experience:

"*After **Adham Bashir** (a young activist was sentenced to 10 years in prison as a result of the events of the Dignity uprising in May 2021), I posted that the state issues these extremely harsh verdicts as a deterrent. At that time, there was a Kaine account that was following me. He took a screenshot and posted it on Twitter. Now, of course, the Israeli community is very active on Twitter, and the right-wing activists started attacking me. At that time, I was really scared. The first thing I did was change my name on Instagram. He had taken a picture of me and changed it. I changed my profile. I changed everything. Maybe I even stopped posting for a week just to lessen the attack... I went into a state of fear... insults, curses, and calls for expulsion...*"

The Rise of Self-Censorship

The discussions within the group revealed a significant increase in self-censorship. Despite being human rights activists or having knowledge of their rights, the participants exhibited a heightened level of self-censorship, leading them to write a post or comment and then immediately delete it. One participant stated:

"*Sometimes I post something critical or something, it takes me a minute before I delete it and that's it. I don't want to share anything anymore.*"

This is evident even in issues that most affect women domestically, such as killings, particularly femicide crimes, where they hesitate to express their views due to the threats they face.

Group discussions revealed that experiences of digital repression and digital attacks within the social and political realm have impacted women's experiences and their stance on the human rights issues they are supposed to advocate for. Self-censorship increases as activists feel increasingly surveilled in their digital environments, perceiving these spaces as lacking safety, regardless of the perpetrators. One participant said:

"*They were even monitoring us as employees, our comments, our families, who our friends are, what our friends' orientations are. There was such a level of surveillance, frankly. So we became more cautious in our comments, in what we said. You know, awareness through instructions from the institution.*"

Another participant said:

"*They tell me that Telegram is not monitored, you can talk freely. But I don't dare. It's to that extent. We are afraid that we are being monitored, and maybe we are being monitored, or 100% monitored... I have deleted many people from my platform. I'm also afraid to comment on people I still have on Facebook. I start to write a comment, and I'm about to post it, but then I delete it.*"

An Invisible Community and Invisible Activists

The women human rights defenders focused on the invisibility of Palestinians inside Israel to the state and its various institutions. This invisibility, reflected in both their demands and lived reality, led them to question the effectiveness of their digital activism in raising awareness of oppression and injustice.

Their discussion of the legitimacy of speaking about their concerns and suffering as activists compared to the situation in Gaza was marked by high sensitivity. It was acknowledged that comparing the two situations was impossible given the genocide being perpetrated against Palestinians in Gaza.

The participants concluded that the erasure of the experiences of Palestinians inside Israel and the suppression of their visibility occurs through several interconnected factors: Self-censorship: Palestinian individuals themselves often engage in self-censorship, suppressing their own voices.; Community pressure: The Palestinian community may exert social pressure to silence activism.; Israeli state oppression: The Israeli state, through its institutions and security apparatus, actively oppresses and censors Palestinian activists; and Extremist Israeli harassment: Extremist Israelis

monitor, follow, and launch attacks on activists, contributing to the suppression of their voices.

These combined forces create a complex web of oppression that limits the visibility and impact of Palestinian activism inside Israel.

Summary and Discussion of General Findings

This study depicts a comprehensive picture of the state of digital security among Palestinian citizens of Israel by examining the experiences of Palestinian internet users. Conducted during a highly sensitive, turbulent, and transformative period, the study employed a rigorous methodology to ensure credible conclusions. Two primary data collection methods were utilized: focus groups and field surveys (opinion polls).

- The theoretical framework revealed a remarkable gap in the literature on digital experiences of Palestinian citizens of Israel. Existing research defines them as part of the Israeli society or the Palestinian people, without recognizing the unique aspects of their citizenship and national identity, which influences their internet usage and interactions on social media platforms.

- The study showed that Israel has developed its control system over internet usage and platforms by developing a harmonious legal system, instructions, and policies, resulting in severe violations of digital rights. Israel created a state of "digital fear" that pushed the youth sector to refrain from expressing opinions and interacting with national and political issues, along with exploiting traditional social systems and patriarchal structures for control, domination, and repression.

- The results revealed that internet users prefer to use the Internet at home over other places (cafes, universities, public spaces). These results may be an indicator of the state of digital insecurity and lack of trust prevalent among Palestinian internet users living inside Israel.

- Approximately half of the users spend 4-9 hours online per day, with news being the main content consumed on social media. However, they have greatly limited their political, legal, and social engagement on these platforms, reflecting a crisis of trust and self-censorship among Palestinians living inside Israel.

- Most participants use several social media platforms and messaging apps, mainly owned by Meta, which are susceptible to hacking and surveillance, the most popular being WhatsApp, followed by Instagram, Facebook, TikTok, and

Telegram. Though aware of spyware and its risks associated with it, many users do not take protective measures like frequently changing passwords or avoiding location sharing. They also demonstrated mistrust towards protection software, indicating that this mistrust derived from their socio-political context.

- The most striking result was the state of indifference and underestimation of potential risks from various sources. The sources of pressure and persecution were not limited to the state and its institutions, but also included political parties, businessmen, and family members. According to the findings, there is a prevalent attitude of ignoring and disregarding threats and dangers, particularly in terms of disregarding messages from unknown sources and not scrutinizing their senders. This reflects negative behavior at the levels of knowledge, awareness, and practice as well.

- After the start of the war on Gaza, digital repression attacks and policies doubled, and attacks and assaults on political and national grounds emerged, carried out by political, religious, and social entities, according to the statements of participants in the focus groups. The most prominent types of attacks and assaults were "identity theft," "phishing," and "harassment and abuse" (see Figure 18). These results may carry some explanation for the crisis of confidence that users suffer from, as the parties that can be relied upon and resorted to when necessary have become a source of concern and intimidation.

- Palestinian youth citizens of Israel reacted to these digital attacks mainly by ignoring them, reflecting a severe trust crisis, as they lack trustworthy authorities to consult.

- We cannot read the results in isolation from the policies of repression and persecution practiced by the State of Israel with its security and judicial apparatuses against activists in recent years, especially after the May 2021 uprising and since the beginning of the war on Gaza in 2023. The data we obtained reflects a horrific scene of self-censorship and repression, as young people preferred to use the internet silently, that is, sufficing with monitoring news and events without interacting with them. But even with this use, the Israeli government tries to exert control by enacting laws that monitor the sites that Palestinians frequent to facilitate their persecution and criminalization.

- Participants in the focus groups conveyed experiences that show the exploitation of Israeli security apparatuses (Shabak/Shin Bet) of the nature of traditional

patriarchal Palestinian society to pressure activists and human rights defenders to limit their expression of opinions about political events or about the course of the war on Gaza, and this was evident in the experiences of Palestinians from the Negev, and women human rights defenders.

- Significant gender-based differences in digital security perceptions were observed among young Bedouins in the Negev, influenced by the conservative social norms and communal living arrangements prevalent in the region. Nevertheless, these disparities have lessened over time as the adoption of digital platforms and internet connectivity has become more widespread.

- In the focus group for human rights activists, it became evident that they had been subjected to digital pressures and attacks due to their rights-based activities online. The manifestations of digital repression and assault intertwined political, security, social, and religious aspects, as well as blurred the lines between reality and the virtual world. This made the activists more cautious in recounting their digital experiences and expressing their human rights positions in digital environments, ultimately leading some to delete their social media accounts or limit their activity to passive observation and using these platforms for shopping and communicating with friends.

- The study concluded that given the extent of restrictions and risks facing Palestinians within Israel, the question of the viability of using the digital environment for human rights struggles and expressing political and social opinions has become increasingly pressing. This is due to the rising costs paid by activists and users in the face of growing hate speech and repressive measures taken by the state of Israel, its apparatus, and extreme right-wing Israeli groups against them.

- In the focus group discussions, a clear state of collision between national identity and citizenship emerged in the daily practices of the participants, especially on digital networks. This conflict and contradiction intensified after the start of the war on Gaza. This collision reinforced feelings of digital insecurity and reluctance to interact and post, or led to the deletion of Israeli Jewish friends or acquaintances from participants' social media accounts.

Suggestions and Areas for Work

First: Enhancing Digital Security Awareness-
Implement comprehensive awareness campaigns aimed at activists, youth, parents, and teachers to familiarize them with the risks posed to digital security and effective protection measures. These campaigns should include hands-on training sessions and seminars in schools, youth movements, and local communities. Participants should be instructed on the use of secure technical tools and modern protection programs, while also learning the fundamental principles of digital security to prevent themselves from falling victim to digital attacks. Emphasizing the significance of protecting personal data is a human right and ensuring safe internet use is an integral part of the right to privacy and freedom of expression.

Second: Providing Reliable Information Resources- Develop and disseminate multimedia educational materials on digital security, encompassing guidebooks, educational videos, and online training courses. These resources should be freely accessible to all and include practical guidelines for digital security best practices. Offer detailed information on how to safeguard personal data and social media accounts,emphasizing the importance of strong passwords, two-factor authentication, and advanced protection tools like antivirus software and firewalls. Provide free technical support to assist users in setting up and effectively utilizing these tools. Additionally, offer clear and concise guidelines that encourage and facilitate the widespread adoption of these tools.

Third: Confronting Digital Repression Policies-
Provide comprehensive support to activists to enhance their capacity to counter digital repression policies and attacks. Establish dedicated advisory lines and platforms offering legal and psychological support for victims of digital targeting and persecution. Additionally, provide technical support and guidance for navigating digital attacks. Develop and implement swift and effective response plans to address digital attacks, including clear mechanisms for reporting incidents and handling them. Ensure that individuals and institutions are regularly trained on these response plans and allocate budgets to support research focused on documenting and addressing digital rights violations as human rights issues. This proactive approach will ensure that individuals and institutions are well-prepared

to effectively counter any digital threat.

Fourth: Documenting Digital Violations-

Thoroughly document digital violations perpetrated against Palestinian human rights defenders and/or Palestinian content. Demand accountability from those responsible for these violations and publish regular reports summarizing the documented cases. These reports should highlight recurring patterns and existing challenges, raising awareness of digital violations as human rights abuses at both local and international levels. Conduct in-depth literacy studies and research that link these violations to their detrimental impact on fundamental rights, such as freedom of expression and the right to privacy. Moreover, train specialized groups in data analysis related to digital violations, equipping them with the necessary technical and legal expertise for effective documentation and analysis.

Fifth: Enhancing Cooperation with Local Authorities-

Forge stronger partnerships with the Higher Follow-Up Committee and the National Committee of Heads of Local Councils and political movements. Develop a comprehensive media literacy plan that addresses freedom of expression, digital rights, and enhanced digital security at the local level. Collaborate with relevant authorities to integrate this plan into local education plans, ensuring that digital rights are considered an integral part of human rights education. Emphasize the connection between digital security and individual rights protection. Allocate budgets to develop educational programs, workshops, and awareness campaigns targeting local communities to foster understanding of digital rights and freedom of expression as human rights. Establish rapid response mechanisms to address digital attacks at the local level, providing immediate support and assistance to those affected. Advocate for the inclusion of digital rights protection and digital security topics in school curricula and educational programs to promote student awareness of the importance of digital security and related rights. Finally, develop plans to improve digital infrastructure and provide necessary technical tools to enhance digital security, thereby creating a safe environment that supports freedom of expression and digital rights.

Sixth: Enhancing Cooperation with Technology Companies

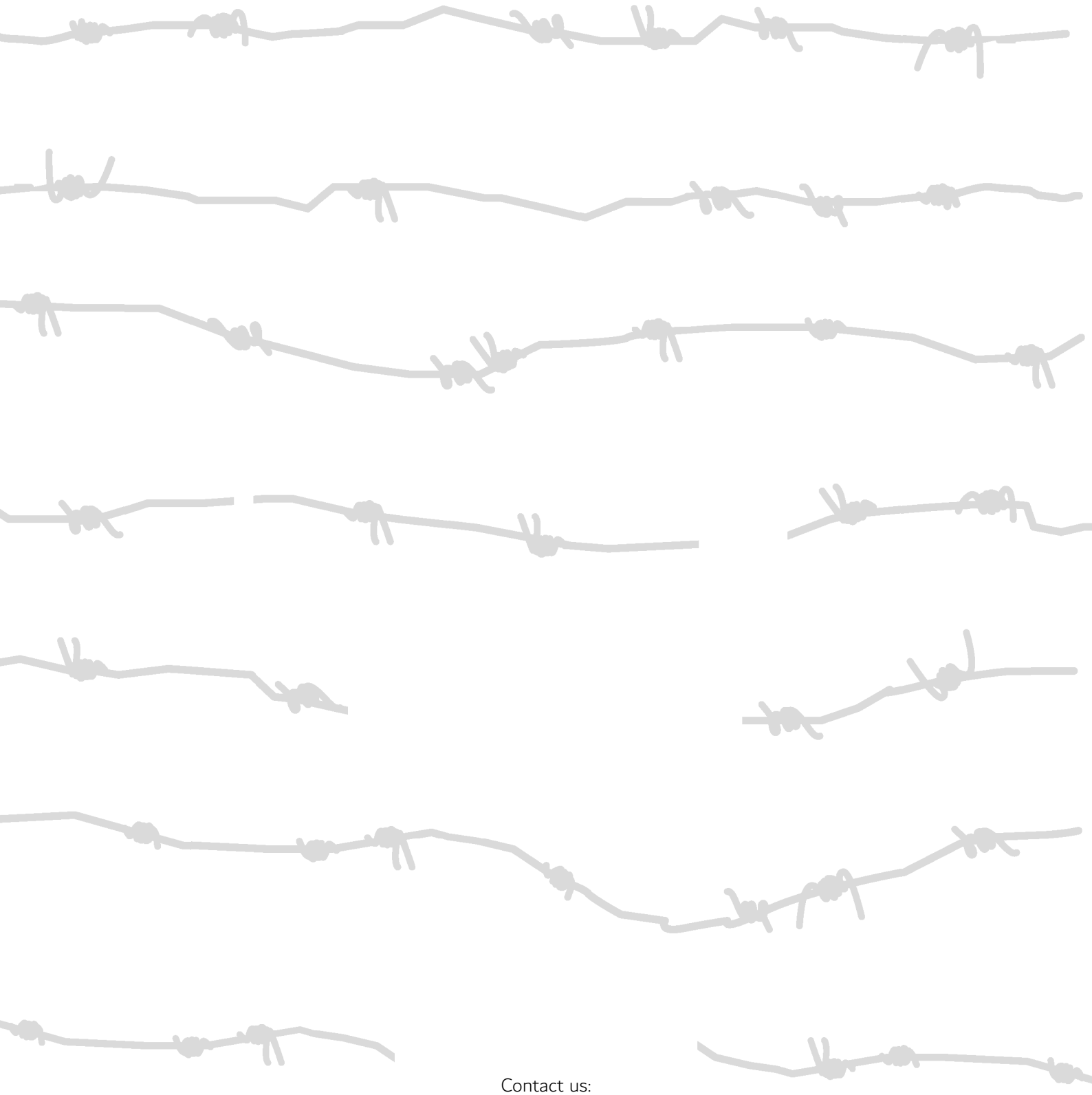
Enhance strategic partnerships with technology companies to ensure swift and effective responses to electronic threats on their platforms. Collaborate on developing content monitoring mechanisms tailored to the specific dialects and contexts within Israel. Prioritize transparency in handling requests related to Palestinian content

and uphold the digital rights of Palestinian users.

Seventh: Providing customized solutions

Conduct in-depth field studies to comprehensively understand the diverse experiences of internet users, considering gender and cultural differences. Identify specific challenges faced by various groups within the digital space and develop targeted solutions that address their unique needs and cultural contexts. Organize specialized awareness workshops to educate individuals about the challenges they may encounter and provide practical guidance on effective solutions. Collaborate with civil society organizations to offer necessary support to the groups targeted, ensuring that the provided solutions are tailored to their specific needs and contribute to their digital security.

.



Contact us:

info@7amleh.org | www.7amleh.org

Find us on social media : **7amleh**