From Normalization to Awareness: The Impact of Empowerment-Oriented Problem Exposure in Reshaping Adolescent Girls' Digital Risk Perception*

Laura Tarantino*, Dajana Cassioli and Antinisca Di Marco

Università degli Studi dell'Aquila, Via Vetoio s.n.c., I-67100, L'Aquila, Italy
**Corrisponding author*

Abstract

Adolescents build their digital identities within an increasingly hyper-connected social media ecosystem, which exposes them to systemic, gender-specific online risks such as cyberbullying and digital harassment. While theoretical awareness of web dangers is moderately widespread among high school girls, literature highlights a significant gap between this passive knowledge and the adoption of active defense practices. Furthermore, a strong gender segregation persists in STEM fields and cybersecurity, fueled by pervasive societal stereotypes and a lack of women role models. To address these socio-technical challenges, this experience paper presents a multi-disciplinary framework implemented during the "Pinkamp" summer school hosted by the University of L'Aquila. The primary research objective is twofold: mapping teenagers' digital risk perception and technological agency and evaluating the impact of an integrated intervention encompassing technical, legal, and socio-psychological dimensions. Adopting a quasi-experimental pre-test/post-test methodology with a sample of high school girls enrolled in the PinKamP summer school, the study evaluates how targeted training combined with exposure to STEM role models can transform girls from passive users into active digital citizens. In particular, baseline cyber-risk awareness was evaluated on N = 52 participants, while the longitudinal impact of the intervention was measured on a correctly matched pre/post sample of N = 35 girls. Serving as a pilot study, this work provides transferable insights to inform larger-scale school interventions and gender-sensitive educational policies that foster digital agency and reduce the gender divide.

Keywords

Digital agency, privacy protection behavior, cyber-security education

1. Introduction

Adolescent girls' digital identities today develop in a context of hyper-connectivity and pervasive use of social media, which, while offering opportunities for participation, also exposes girls to systemic gender-related risks. The literature highlights how girls are privileged targets of specific forms of abuse, including body shaming, sexualized harassment, and surveillance of intimate relationships via technological devices [3,9,10].

STPIS2026: Proceedings of the 12th International Conference on Socio-Technical Perspectives in IS, September 16-17th L'Aquila, Italy
* Corresponding author.
laura.tarantino@univaq.it (L. Tarantino); dajana.cassioli@univaq.it (D. Cassioli); antinisca.dimarco@univaq.it (A. Di Marco)
0000-0002-9926-0296 (L. Tarantino); 0000-0001-7574-5099 (D. Cassioli); 0000-0001-7214-9945 (A. Di Marco)
© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR-WS.org/Vol-4334/paper20.pdf

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073
published 2026-11-19

Although younger generations display a moderate theoretical awareness of the dangers of the Internet, recent studies reveal a profound gap between knowledge of risks and the adoption of active defense practices [4]. Many high school girls, even when aware of concepts such as phishing or doxing, fail to implement fundamental protection measures such as two-factor authentication or strict privacy management, often due to a perceived illusion of security or a lack of practical computer literacy [1]. This is coherent with general results on the "privacy paradox" phenomenon, i.e., the mismatch between users' online privacy attitudes and their actual behavior [2,19]: when faced with the dilemma of whether choosing online privacy over personalization, usability and interactivity, users often prefer to utilize the affordances and the richness of services of the cyberspace at the expense of privacy and anonymity protection [34].

Furthermore, research highlights how standard school education often lacks digital etiquette (a set of rules of good manners, respect, and behavior to be adopted in online communication) and the legal implications of online behavior, leading to an underestimation of the criminal consequences for both victims and perpetrators [6,18]. In this scenario, the need for multidisciplinary training interventions emerges, providing technical, legal, and psychological tools, with the multifaceted objective of enhancing girls' technological agency to allow them to shift from passive reception of tools to effective active digital defense, deconstructing gender biases and promoting active and informed digital citizenship under a socio-technical lens [36,38,39].

In this experience paper we address these socio-technical challenges by reporting on the design, the operationalization and the result of a study conducted withing the framework of the Pinkamp program [30], a two-week summer school of the University of L'Aquila aimed at introducing young women to STEM disciplines and careers. Unlike traditional educational programs, which primarily focus on learning outcomes, Pinkamp adopts a holistic educational model [16,30] pursuing three complementary objectives: (i) fostering vocational interests, (ii) providing a broad understanding of STEM disciplines and their societal impact, and (iii) promoting self-confidence, collaboration, and women empowerment.

Specifically, the present study involved a cohort of adolescent girls aged 16 to 18. This target age range was deliberately selected as it represents a critical developmental stage characterized by high exposure to online relational and digital security risks, alongside pivotal decision-making processes regarding high school choices and future university orientations. By evaluating a multidisciplinary intervention centered on interactive scenario-based workshops, role-model exposure, and pre/post empirical evaluations, we address two core research questions:

RQ1 (On Risk Perception, Literacy and Agency): *To what extent does a multidisciplinary socio-technical intervention transform adolescent girls' passive risk awareness into actionable digital agency, particularly across system-level vs. interpersonal cyber-threats?*

RQ2 (On Gender in Cybersecurity): *How does exposure to women role models and gender-sensitive cybersecurity training influence career aspirations of high school girls in STEM fields?*

To answer these research questions and assess the effectiveness of the initiative, we conducted a two-fold evaluation: a baseline cross-sectional analysis to map initial cyber-risk awareness among participants (N = 52), followed by a longitudinal quasi-experimental assessment (N = 35 correctly paired responses) to quantify the impact of the intervention on participants' agency and skills.

We also observe that, beyond evaluating knowledge gain and vocational shifts, this study acts as an empirical opportunity for the structural validation of the measurement scale itself and the proposed scenarios within an adolescent female cohort, in view of future larger-scale interventions across regional schools.

The remainder of this paper is organized as follows: Section 2 presents the research design, participant demographics, data collection protocols, and measurement instruments. Section 3 discusses the operational structure of the interactive workshop scenarios. Section 4 reports the empirical findings and experience data analysis, detailing baseline evaluations and real-time decision-making dynamics. Section 5 evaluates the post-intervention impacts on risk awareness and privacy behavior, as well as on vocational outcomes, by a descriptive analysis of observed trends. To bridge empirical observations with actionable guidelines for future research and practice, the critical insights emerging in Section 4 and Section 5 from the experience data analysis are synthesized throughout the text through dedicated 'Lessons Learned'. Section 6 addresses the research questions, and, finally, Section 7 discusses key lessons learned and research limitations and outlines future work.

2. Methodology

The research aims to map awareness of cyber risks and perceptions of cybersecurity careers in a sample of high school girls (third and fourth grades of high school), simultaneously evaluating the effectiveness of a multidisciplinary training intervention in improving risk perception and promoting career orientation towards STEM fields. More specifically, we have the following objectives:

- **Mapping cyber-risk knowledge**: To evaluate participants' baseline awareness of digital threats across consolidated taxonomies, specifically investigating risks related to content, contact, conduct (e.g., cyberbullying and legal consequences), and consumption (e.g., unauthorized profiling and data exploitation) [37]. Crucially, this socio-psychological framework is mapped directly onto concrete cybersecurity mechanisms — such as Two-Factor Authentication (2FA) and phishing prevention — thereby bridging social conduct with technical infrastructure in line with our socio-technical approach.
- **Assessment of Technological Agency**: To measure participants' capacity to transition from theoretical understanding to active defense, examining their perceived self-efficacy in implementing concrete technical safeguards and coping strategies.
- **Analysis of socio-psychological barriers**: To identify the underlying factors hindering the adoption of security practices, investigating whether the failure to use defenses stems from technical skill gaps or social pressures, such as fear of peer exclusion (e.g., FOMO) or trade-offs between privacy and digital identity presentation.
- **Evaluation of intervention impact on awareness and agency**: To quantify how the Pinkamp intervention alters participants' perceptions, assessing the shift from passive consumption toward empowered, proactive, and risk-aware digital citizenship and to provide a scientific basis for future interventions.

- **Assessment of vocational and educational impact**: To assess the influence of the training intervention on participants' vocational inclinations, analyzing changes in interest toward STEM and cybersecurity careers while identifying key motivating factors (e.g., social utility, career potential) and possible gender-related barriers.

2.1. Quasi-Experimental Research Design and Procedure.

A quasi-experimental research design with a pre-test/post-test approach was adopted. This choice was motivated by the impossibility of randomizing the subjects, as the sample was drawn voluntarily from those enrolled in the Pinkamp training project. The protocol involved three phases:

1. **Phase 1 (Pre-test)**. The baseline data collection comprised two instruments: a *primary structured questionnaire* assessing initial condition (such as risk awareness and prior experiences) and a second brief questionnaire focusing on participants' vocational inclinations. The study objectives and the questionnaires were presented during the online Pinkamp presentation event (prior to the start of Pinkamp activities), to be completed online. Pre-test data collection was concluded by mid-week of Week 1 of the camp; this timeframe was essential for an initial analysis of the results, which helped us to dynamically adapt some aspects of the training intervention planned for the second week based on the specific vulnerabilities identified in the pre-test data (according to a data-driven approach, as we will discuss in Section 4.1) and thus ensure maximum pedagogical relevance with respect to the gaps and attitudes identified by the sample. To adapt some dynamic aspects of the training interventions
2. **Phase 2 (Training Intervention)**. The intervention was structured around two key moments during the second week of Pinkamp:
    - an interactive multidisciplinary workshop covering the technological, legal, and psychological dimensions of cyber risks, scheduled for the afternoon of the first day of Week 2.
    - an event aimed at deconstructing the historical invisibility of women in tech through meetings with role models in Pinkamp core areas (Physics, Computer Science, Information Engineering, Industrial Engineering, and Mathematics), who provided testimonials from women STEM professionals, scheduled for the afternoon of the second day of Week 2.
3. **Phase 3 (Post-test)**. A second questionnaire on cyber-risks was administered on the third day of Week 2, to assess changes in risk perception and any reduction in barriers to adopting security measures. A second questionnaire on vocational inclinations was administered after the presentation of our Study Programs, in the afternoon of the fourth day of Week 2.

Data were collected in pseudonymized form via Microsoft Forms, stored on encrypted University servers, and restricted to research leads through two-factor authentication. To align longitudinal pre- and post-test responses while ensuring full GDPR compliance, participants generated a unique pseudonymization code based on non-identifiable personal variables. Upon reconciling the longitudinal datasets, these linking keys were permanently deleted, resulting in a fully anonymized final dataset for research publication. Additionally, demographic variables

were collected at an aggregate level to prevent re-identification through cross-referencing with administrative records.

2.2. Participants and recruitment.

Participants to this study were recruited on a voluntary basis from those enrolled in the Pinkamp project. Application to PinKamP is open to girls attending the third and fourth years of any Italian upper secondary school through a national public call. Since the number of applications generally exceeds the available places, participants are selected using two equally weighted criteria: academic performance and a motivation letter.

As a result, the study involved a cohort of high school girls enrolled in the PinKamP summer school (held in June) who had just completed their third or fourth year of secondary education. The participants ranged in age from 16 to 18 years. The presence of 18-year-old participants is aligned with the Italian educational timeline and the June timing of the intervention: fourth-year students born in the first half of the calendar year (or having entered school early) had already turned 18 by the end of the academic year, prior to attending the summer camp. No fifth-year students were included in the cohort.

Because the target group comprised minors and young adults, recruitment took place through the project's official channels after outlining the educational and research objectives. The information on data processing and the informed consent form was provided before the start of the Pinkamp activities (for minors, the consent form was signed by their parents or legal guardians). The document specified the anonymous nature of the data collection, the exclusively scientific purpose of the research, and the right to withdraw at any time without any consequences for the Pinkamp training program.

Table 1
Participant Selection and Data Matching Flow

Stage	N	Description	Attrition/drop out
Total enrolled	65	Girls participating in Pinkamp	—
Informed consent	58	Participants provided consent/agreement	-7 declined/incomplete consent
Baseline assessment	52	Completed the pre-workshop questionnaire	-6 missed pre-test
Post-workshop assessment	45	Completed the post-workshop questionnaire	-7 missed post-test
Matched datasets	35	Successfully paired pre/post-workshop responses	-10 unmatched pairs

A total of 65 girls enrolled in the PinKamP summer school. Of these, 58 participants provided valid informed consent (or parental consent where required). Baseline questionnaires were completed by 52 participants, while 45 completed the post-workshop evaluation. To ensure data integrity for longitudinal analysis, individual responses were paired using unique anonymous identifiers, resulting in a final analytical sample of N = 35 fully matched pre- and post-intervention questionnaires (see Table 1).

It is important to clarify the distinction between institutional recruitment criteria and our analytical focus. While program enrollment relied on binary administrative criteria to target high school girls for a dedicated STEM initiative, our empirical framework evaluates the impact of gendered socialization on digital risk experience and technological agency. Online threats such as body shaming, relational coercion, and sexualized harassment are deeply embedded in socio-cultural dynamics rather than biological determinants. Consequently, our analysis examines how adolescent girls navigate these socially constructed vulnerabilities, assessing how targeted socio-technical interventions can foster active defense practices and deconstruct internalized gender constraints.

2.3. Survey Instrument and Operationalization

To systematically evaluate the multidimensional impact of the intervention, the designed survey instrument serves as the primary quantitative measurement tool. Administered in a pre- and post-test design, the questionnaire was informed by consolidated literature on adolescent online risk, socio-technical cybersecurity awareness, and behavioral protection frameworks [1,4,6,9,18,21,25,26,33,37].

Generally speaking, the questionnaire revolved around the two macro-areas: **perception and awareness of online risks** to map how adolescents perceive the spread and danger of critical digital phenomena and **defense practices, legal protections, and digital habits** to analyze cyber protection measures by capturing baseline daily habits in the pre-test and the projection toward future behavioral intention in the post-test as a result of the newly acquired competencies. More specifically, the questionnaire is structured into three main sections.

The section on **Cyber-Risk Knowledge and Perception** assesses participants' cognitive and evaluative disposition toward digital threats across three primary risk categories; *Interpersonal Abuse & Cyberbullying***,** evaluating risks arising from peer dynamics (Denigration & Flaming, Social Exclusion, Body Shaming, Doxing, and Sexualized Harassment); *Privacy & Data Exploitation,* covering platform-level and data-driven vulnerabilities (Unauthorized Profiling, Covert Tracking, and manipulation via Dark Patterns), and *Technological Abuse & Coercion*, focusing on relational and technical control mechanisms (Forced Password Sharing, Spyware & Location Monitoring, and Account Impersonation).

For each specific risk item, the instrument captures three distinct perceptual vectors on 5-point Likert scales: *Confidence in Recognition (Knowledge / Self-Efficacy)* measures the subjective competence in identifying and distinguishing the specific threat (1 = Very Uncertain to 5 = Very Confident); *Perceived Prevalence* measures the perceived frequency of these occurrences in daily digital experience (1 = Not at all prevalent to 5 = Extremely prevalent); *Perceived Severity (Danger)* measures the evaluated gravity/harm of the threat (1 = Not at all dangerous to 5 = Extremely dangerous).

The section on **Coping Strategies and Emotional Impact** explores the behavioral and psychological responses to cyber-attacks by analyzing the likelihood (1-5) of adopting specific coping mechanisms (e.g., self-management/blocking, peer support, seeking parental/educator support, reporting to law enforcement/Polizia Postale, or passive avoidance), and by measuring perceived psychological harm (isolation, anxiety, self-doubt, helplessness, self-blame) as well as the perceived motivations and consequences for perpetrators.

The section on **Defense Practices, Netiquette, Barriers** shifts from threat perception to operational defense mechanisms, tracking behavioral change from reported habits (*Pre-test*) to

future implementation intent (*Post-test*) as to technical defense actions, Netiquette, and socio-psychological barriers (e.g., technical complexity, fear of social exclusion/FOMO, aesthetic concerns, optimism bias).

3. Workshop Design & Interactive Mechanics

The multidisciplinary event held in the afternoon of the first day of Week 2 was structured as an interactive workshop named "*NOT A TARGET: Security and Agency in the Digital World*", including two activities:

- The *anti-fraud path* "InsospettABILI - let's develop skills against online fraud," an interactive and itinerant program designed by the Italian State Police to teach citizens how to defend themselves from digital scams. The project is implemented through multimedia totems: after accessing the digital platform directly from the smartphone, through quizzes and exploration of real-life situation users face phishing simulations, deceptive messages, and fake banking communications. At the end of the test, a "vulnerability report" provides users a personalized analysis showing how exposed their personal data is to online risks.
- A *multidisciplinary scenario-based session* centered on three realistic scenarios mapped directly to the three risk categories of the survey (Interpersonal Abuse, Privacy & Data Exploitation, Technological Abuse). Designed around a "Fork in the Road" dilemma structure, each narrative challenges participants with non-trivial decision crossroads reflecting varying degrees of cyber-agency. Interactive discussions on scenarios and possible endings are facilitated by a multidisciplinary panel of women professionals spanning cybersecurity, sociology, privacy behavioral science, interactive system design, data science, and legal studies, to address the technical, social, and protective dimensions of risks and digital safety in an integrated manner.

In the remaining of this section, we provide insights on the multidisciplinary session, focusing on design principles, scenario structures and plots, and panel preparatory activities.

3.1. Scenario design principles

The design of the scenarios was informed by consolidated literature on engagement, risk perception, reasoning in cybersecurity contexts, and different socio-technical facets of cyber-security awareness.

Identification and Realism. The protagonists and situations reflect the daily lives of high school students (e.g., the use of social media, group chats, managing peer privacy) to ensure authentic context and contextual engagement, thus facilitating the transfer of skills from the classroom to everyday life [14,15,20].

The "Fork in the Road" (Dilemma) structure. To operationalize this approach, the workshop design introduces a series of decision crossroads. This structure is grounded in socio-technical principles [38], acknowledging that conventional, linear problem-solving mechanisms are insufficient for navigating the overlapping social and systemic complexities of modern digital threats. Specifically, each scenario presents a critical situation that ends with a non-trivial choice: there should not be a simple "right or wrong" answer, but rather multiple options that reflect nuanced awareness, risk perception, or social pressures [7,11] fostering complex

decision-making and ethical reasoning in cybersecurity contexts [27]. More specifically, three options are proposed, reflecting distinct degrees of cyber-agency and operationalizing the full spectrum of coping strategies mapped in the baseline survey: from passive submission or silent avoidance (*no action/silent coping*) to informal peer-level management (*individual/informal coping*), up to proactive technical defense and official reporting (*technical, family, and legal coping*).

Participants are requested to answer two questions: "*What ending do you think your story will have?*", to try to discover their perception of peers' actual behavior (the **descriptive norm**), and "*What if we could change things? What ending should this story have to truly protect?*", to evaluate their perception of effective protection, thereby measuring the tension between perceived social reality and technological/legal empowerment (the **injunctive norm**).

Multidisciplinarity. Each scenario allows for a discussion in which different skills intersect and integrate, following a socio-technical approach to cybersecurity awareness [33] along lines encompassing people, law, society, and technology:

- The **technical dimension** (*How did it happen?*): Analysis of IT vulnerability, device security, and data protection [22].
- The **social and relational dimension** (*Why does it happen and what does it entail?*): Understanding the underlying gender dynamics, deconstructing stereotypes, and analyzing the behavior of bystanders (those who observe, approve, or ignore online) [23,26].
- The **protection and counteraction dimension** (*How do you defend yourself legally and operationally?*): Defining legal boundaries, operational defense, digital evidence collection, and reporting procedures [5].

Ultimately, by combining contextual realism and structured decision-making into a socio-technical framework, this approach ensures that learning extends beyond passive awareness, empowering participants to critically navigate complex digital dilemmas with both technical competence and social responsibility.

3.2. The three scenario "dilemmas"

Building upon these methodological design principles, three narrative scenarios were designed to directly align with the three macro-risk categories investigated in the measurement questionnaire (*Interpersonal Abuse and Cyberbullying*, *Privacy and Data Exploitation*, and *Technological Abuse and Coercion*). Each scenario leads participants to a critical dilemma offering three alternative narrative endings (E1, E2, E3). Tables 2–4 outline the narrative plots, target risk factors, and decision-making branches corresponding to each scenario, illustrating how the technical, social, and protective dimensions are practically integrated into the participant journey. The endings of Scenario 3 are more extensively detailed since – at discussed later in the paper – the findings related to this scenario require a more in-depth analysis.

Table 2

Operational structure of Scenario 1 (*Interpersonal Abuse and Cyberbullying*): Narrative plot, target risk factors, and decision-making branches across coping strategies.

Scenario 1: Interpersonal Abuse and Cyberbullying	
Focus	Denigration/Flaming, Exclusion, Body Shaming, Doxing.
Characters	Camilla, Vera (the victim)
Plot idea	Camilla receives offensive edits or harsh comments (*Body Shaming/Flaming*) in a group chat regarding Vera, one of her classmates. The group was created specifically to exclude the victim (*Exclusion*)
The Cyber-Agency Dilemma	
S1-E1 *Silent Action*	Camilla leaves the group and deletes the chat.
S1-E2 *Advice in a "small" group*	Camilla takes a screenshot, sends it privately to her best friend, and warns Vera.
S1-E3 *Institutional support*	Camilla intervenes publicly, risking *doxing* or retaliation then leaves, saves the screenshots, and discusses it with an adult to formally report the matter.

Table 3

Operational structure of Scenario 2 (*Privacy and Data Management*): Narrative plot, target risk factors, and decision-making branches across technical defense and cyber-agency levels.

Scenario 2: Privacy and Data Management	
Focus	Unauthorized Profiling, Covert Tracking, Dark Patterns
Characters	Camilla, group of friends
Plot idea	Camilla experiences the strong temptation to download a viral app of the moment that requires intrusive and covert access to personal data, disguised by deceptive graphical interfaces.
The Cyber-Agency Dilemma	
S2-E1 *No Action*	Camilla quickly clicks "Accept all."
S2-E2 *Digital defense (technical compromise)*	Camilla denies access to her location and contacts in her phone settings, leaving only the camera.
S2-E3 *Informal support (awareness raising)*	Camilla doesn't install the app. She takes a screenshot of the abusive permissions screen and sends it to her friends' group, warning them of the risks

Table 4
Operational structure of Scenario 3 (*Coercion and Control / Technological Abuse*): Narrative plot, target risk factors, and decision-making branches across individual, relational, and institutional coping responses.

Scenario 3: Coercion and control	
Focus	Forced Access, Impersonation, Awareness of the Crime of Unauthorized Access
Characters	Camilla, Samuele (her boyfriend)
Plot idea	Camilla finds herself dealing with her boyfriend's insistent request for the passwords to her social media profiles as "proof of love," later discovering the consequences of a total loss of control over her digital identity: someone has accessed her account and sent extremely harmful messages to various people without her knowledge (*Impersonation/Unauthorized Access*)..
The Cyber-Agency Dilemma	
S3-E1 *No Action/Submission*	Camilla secretly changes her password but keeps quiet about it to Samuele to avoid angering him or ending the relationship. She tries to apologize privately to her friends, saying it was "an app error" or a prank in poor taste by an unknown hacker.
S3-E2 *Individual technical management*	Camilla confronts Samuele via text message, takes back her account, activates Two-Factor Authentication (2FA), and disconnects all associated devices. However, she decides not to discuss this with any adults or teachers because she feels stupid for having given him the password in the first place.
S3-E3 *Family, institutional and legal support*	Camilla understands the gravity of the situation. She saves screenshots of the abusive messages and access logs. She immediately discusses the matter with her parents and the school (since classmates are involved) and decides to end the relationship, also supported by the opinion of an expert or the authorities.

3.3. The multidisciplinary mapping

To ensure a cohesive and impactful workshop experience, a structured preparation phase was conducted during the two weeks leading up to the event, with the objective of aligning the diverse multidisciplinary perspectives of the invited women panelists around the narrative dilemmas. Each panelist was provided with a comprehensive briefing document detailing the scenario design principles, the full narrative plots for the three scenarios, and structured multidisciplinary mapping matrices connecting each narrative ending of each scenario to the underlying *coping strategy*, the relevant socio-psychological *barriers* (whether active or

successfully overcome by the protagonist), and specific multidisciplinary *discussion hints* structured along the social, technical, and protection/legal dimensions to guide expert interventions during the workshop. As an illustrative example, Table 5 presents the mapping matrix for Scenario 3.

Table 5
Multidisciplinary mapping matrix for Scenario 3 (**Coercion and Control / Technological Abuse**): Overview of coping strategies, active/overcome barriers, and structured discussion hints across social, technical, and protection dimensions for each narrative ending.

Ending	Coping strategies	Barriers (Active/Overcome)	Discussion hints
S3-E1	No Action	**Active**: Fear of relational breakdown, shame, and guilt (feeling guilty for giving out the password).	**Social dimension**: Analyzing the signs of a toxic or controlling relationship. The myth of "total transparency" as proof of love. Victim guilt. **Technical dimension:** Why sharing credentials nullifies any security measure (e.g., it also makes 2FA useless).
S3-E2	Individual technical management	**Active**: Underestimation of long-term risk, fear of adult judgment.	**Technical dimension:** How to "reclaim" an account, control connected devices, and the importance of 2FA. **Protection dimension:** This option solves the technical problem but not the relational one. Samuele could use other methods (e.g., demanding to see the screen live or installing spyware).
S3-E3	Family, institutional and legal support	**Overcome**: Pressure for transparency Fear of isolation.	**Protection dimension:** Explain that accessing someone else's profile, even if you know the password, constitutes the crime of "Unauthorized Access to a Computer System". Explain how to protect yourself legally if your ex-partner begins threatening or engaging in cyberstalking.

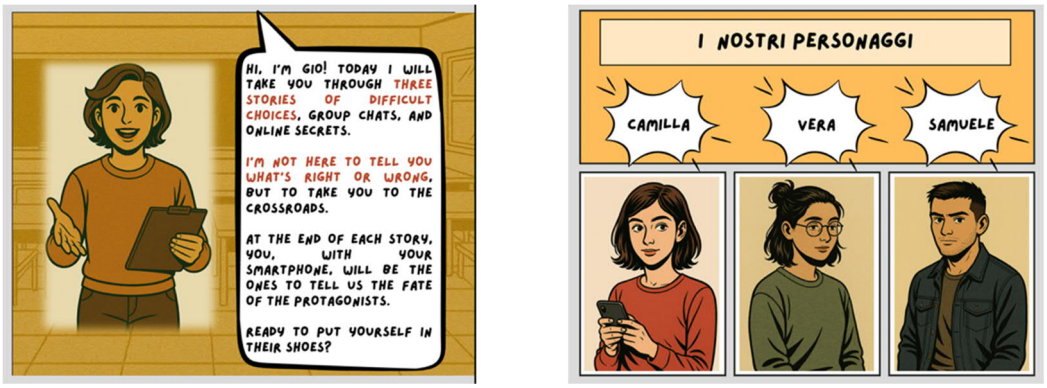
The alignment process among panelists was facilitated through collective email exchanges and a series of targeted bilateral coordination calls with individual experts. This preparation framework provided each panelist with clear discussion anchors.

3.4. Workshop Delivery Dynamics

To maximize engagement and foster empathy among adolescent participants, during the multidisciplinary session the scenarios were delivered through a **graphic novel format**, to reduce cognitive load and enhance immersion [12,14,31]. The graphic panels were crafted through a hybrid design workflow. Individual character illustrations and scene assets were generated using Microsoft Copilot based on detailed descriptive prompts, while single frames and comic layouts were manually assembled and structured using Canva. To avoid moralizing bias and promote psychological safety, the educational narrative is mediated by "Gio," a gender-

neutral guide character acting as an empathetic facilitator who frames the socio-technical dilemmas and invites participants to critically navigate decision-making crossroads independently.

Figures 1 and 2 show samples from the graphic novel scenes: the narrative introduction by the gender-neutral guide character ("Gio"), the recurring protagonists designed to reflect relatable high school peer dynamics, the graphic depiction of a critical threat event (unauthorized account access / impersonation), and the visual representation of a decision crossroad (A: Passive/Silent Action, B: Informal Peer Support, C: Institutional/Adult Support).



(a) (b)

Figure 1: Overview of the graphic novel elements: (a) the guide character Gio, and (b) the recurring story characters (Camilla, Vera, and Samuele).



(a) (b)

Figure 2: Narrative structure and decision dilemmas: (a) A scene from Scenario 2, depicting a crucial narrative event, and (b) the three-option decision dilemma from Scenario 1, illustrating different intervention strategies (A, B, and C) after the cyberbullying incident.

Following the presentation of scenario dilemmas during the multidisciplinary session, data collection was conducted in real time using Microsoft Forms. At the conclusion of each scenario, participants were prompted to evaluate the two consecutive questions regarding the *Most Likely Outcome* and the *Most Secure Outcome*. Each participant was permitted a single submission per scenario under a strict 5-minute time limit to ensure that responses were captured before the panel discussion began and preventing external influence from experts or peers. Immediately

following each voting phase, a guided discussion took place, with the real-time aggregated results serving as a foundation to address the observed gaps between expected reality and optimal security practices.

4. Experience data analysis

This section analyzes the empirical findings gathered throughout the educational initiative, across the levels of *Baseline Evaluation (Pre-test)*, to assess the initial maturity profile of the participants, and *Interactions & Decision-Making Dynamics*, to examine how participants navigated the interactive scenario-based dilemmas, based on the real-time ending voting outcomes collected via MS Forms.

4.1. Baseline evaluation (pre-test)

As previously discussed, midway through the first week of campus, we conducted a preliminary analysis of the results of the baseline questionnaire to gain a general idea of participants' level of awareness regarding cyber-risks, their behaviors regarding privacy protection, and their digital agency, and, thanks to this, to be able to better direct the panel discussion.

As illustrated in Table 6 participants were almost evenly distributed between third-year (46%) and fourth-year students (54%). Geographically, the majority originated from Northern and Central Italy (64%), compared to Southern and Insular regions (36%). Regarding educational background, a large majority attended technical or scientific high schools (83%), compared to those enrolled in humanities and social science tracks (17%).

Table 6
Demographic Breakdown of the participants (N=52)

Category	Subcategory	Percentage
School year	3rd year	46%
	4th year	54%
Geographic region	Northern & Central Italy	64%
	Southern & Insular Italy	36%
School type	Scientific/technical	83%
	Humanities/social science	17%

To establish a pre-intervention baseline of participants' cognitive and evaluative awareness regarding digital risks, Table 7 summarizes the quantitative results from the survey's initial section, detailing the cohort's baseline maturity profile. As operationalized in the measurement framework, each threat item is analyzed across three distinct macro-risk categories and along three core perceptual vectors. To facilitate interpretation, the sample mean scores derived from the 5-point Likert scales (1.00 - 5.00) were categorized into five standardized qualitative levels using an equal interval width of 0.80: L1 (1.00–1.80), L2 (1.81–2.60), L3 (2.61–3.40), L4 (3.41–4.20), and L5 (4.21–5.00). Across the five intervals the qualitative descriptors are assigned as follows:

- **Confidence in Recognition**: *Uncertain* (L1), *Deficient* (L2), *Basic* (L3), *Proficient* (L4), and *Advanced* (L5).
- **Perceived Prevalence**: *Absent* (L1), *Rare* (L2), *Occasional* (L3), *Widespread* (L4), and *Pervasive* (L5).
- **Perceived Severity**: *Negligible* (L1), *Minor* (L2), *Moderate* (L3), *Severe* (L4), and *Critical* (L5).

Table 7
Self-perceived confidence in risk recognition, reported online prevalence, and perceived severity across categories (N=35)

Threat Category & Specific Risks	Confidence in Recognition	Perceived Prevalence	Perceived Severity
Interpersonal Abuse & Cyberbullying			
Flaming & Public Insults	Proficient (4.00)	Occasional (3.29)	Severe (4.17)
Social Exclusion	Proficient (3.85)	Occasional (3.19)	Moderate (3.35)
Body Shaming	Advanced (4.31)	Occasional (3.38)	Critical (4.50)
Doxing	Basic (3.25)	Rare (2.38)	Critical (4.60)
Sexualized Harassment	Proficient (3.87)	Occasional (2.79)	Critical (4.58)
Privacy & Data Exploitation			
Unauthorized Profiling	**Deficient** (2.54)	Occasional (2.63)	Severe (3.96)
Covert Tracking	**Deficient** (2.54)	Occasional (2.62)	Critical (4.21)
Dark Patterns	Basic (2.94)	Occasional (3.08)	Severe (3.62)
Technological Abuse & Coercion			
Forced Password Sharing	Proficient (3.96)	Occasional (2.71)	Severe (4.15)
Spyware & Location Monitoring	Basic (3.19)	Occasional (2.67)	Severe (4.13)
Account Impersonation	Basic (3.23)	Rare (2.29)	Critical (4.35)

The baseline quantitative analysis of Table 7 reveals a distinct divergence in how adolescent girls perceive and evaluate different categories of digital threats prior to the training intervention across the three perceptual vectors:

- **Interpersonal Abuse & Cyberbullying**: Participants displayed the highest confidence in recognizing relational threats (*Proficient* to *Advanced*), evaluating them as highly severe (*Severe* to *Critical*, peaking at M = 4.60 for Doxing) despite reporting *Occasional* to *Rare* direct prevalence.
- **Privacy & Data Exploitation**: Identified as a **core vulnerability area**. While recognized as highly severe (*Severe* to *Critical*), recognition confidence was exceptionally low (*Deficient* for tracking and profiling, *Basic* for dark patterns), exposing a gap between threat awareness and operational identification skills.
- **Technological Abuse & Coercion**: Occupies a mid-tier position, characterized by *Proficient* recognition of password coercion but *Basic* levels for spyware and impersonation. Though perceived as less frequent (*Rare* to *Occasional*), its potential consequences are universally judged as *Severe* to *Critical*.

Summarizing, the baseline data highlight a **structural imbalance**: adolescent girls feel well-equipped to identify visible, interpersonal cyber risks, yet exhibit marked vulnerabilities in identifying opaque, system-driven threats like tracking and profiling. Nevertheless, because all categories are rated as "severe" or "critical" in potential impact, the findings emphasize an urgent need for targeted educational interventions aimed at bridging the gap between high threat-severity awareness and actionable technical recognition.

It must also be observed that the analysis of the qualitative responses collected to the open-text question *"Which of the above risks frightens you the most or do you find most difficult to manage?"* provides crucial context to the quantitative findings, revealing a stark paradox in participants' risk perception. While baseline knowledge regarding privacy and data exploitation appeared comparatively limited, the open-text responses demonstrate that issues pertaining to data privacy, loss of control over personal information, and unauthorized monitoring represent the primary source of anxiety and perceived helplessness among participants. A qualitative thematic analysis of open-ended responses regarding baseline risk concerns reveals a distinct hierarchy of perceived digital threats. **Privacy, Data Exploitation, and Covert Surveillance** emerged as the primary area of concern (around 44% of responses), driven by pervasive anxieties over hidden tracking, unauthorized profiling, and systemic algorithmic monitoring (e.g., *"the fact that the system controls what I search for or write"*). **Interpersonal Abuse, Body Shaming, and Sexualized Harassment** constituted the second largest cluster (around 38% of responses), characterized by socio-emotional threats such as non-consensual image sharing and the recognized difficulty of controlling peer behaviors on social media platforms. Finally, **Technological Abuse, Impersonation, and Spyware** accounted for the remaining share (around 18% of responses), with participants highlighting invasive digital control, identity theft, and covert location tracking.

This data-driven baseline revealed critical vulnerabilities regarding data privacy and exploitation, which directly informed the dynamic adaptation of the Week 2 activities (as anticipated in Section 2.1): it prompted an expanded focus on anti-fraud and tracking mechanisms during the interactive session with the Polizia Postale, while simultaneously guiding the multidisciplinary panel discussion toward the legal, technical, and socio-behavioral dimensions of data protection. This data-driven intervention design mirrors the collaborative problem-solving approach advocated by [38], who emphasized the necessity of integrating academic socio-technical research with practical law enforcement and professional institutional expertise to address escalating electronic threats.

4.2. Decision-making dynamics in the multidisciplinary session

The results of the multidisciplinary scenario-based session, illustrating how participants navigated digital dilemmas and measuring the alignment between perceived real-world peer behaviors and ideal security practices, are summarized in Table 8. The table presents the percentage distribution of participants' responses across the three scenarios as to the *Most Likely Outcome* (capturing their perception of actual peer behavior and realistic outcomes) and *Most Secure Outcome* (identifying the resolution that provides optimal protection and effective counteraction) for each narrative dilemma. The resulting *Gap* (calculated as percentage point difference) highlights the discrepancy between what participants expected to happen in peer dynamics versus what they recognized as normative and protective behavior.

Across all three scenarios, these results highlight a structural divergence between what participants recognize as ideal protection (E3) and what they expect peers to do in practice (E1 and E2). Rather than a simple lack of cybersecurity knowledge, this discrepancy highlights complex socio-emotional friction in enacting safe behaviors. The following subsections analyze these findings, examining the cognitive-behavioral intention gap, the role of social pressure, and the perceived barriers to reporting online threats.

Table 8
Percentage distribution of student perceptions comparing expected vs. safe behaviors across scenarios. N is the number of collected responses. Bold values highlight primary concentrations.

Scenario	N	Ending	Most Likely Outcome (%)	Most Secure Outcome (%)	Gap
Scenario 1 Abuse and Cyberbullying	53	**S1-E1**	17	0	-17
		S1-E2	**74**	0	-74
		S1-E3	9	**100**	+91
Scenario 2 Privacy and Data Management	51	**S2-E1**	**72,5**	0	-72,5
		S2-E2	21,6	21.6	0
		S2-E3	5.9	**78,4**	+72,5
Scenario 3 Coercion and Control	46	**S3-E1**	39	2	-37
		S3-E2	**48**	22	-26
		S3-E3	13	**76**	+53

4.2.1. Cognitive-Behavioral Intention Gap

A cross-cutting finding of fundamental scientific importance concerns the clear divide between theoretical safety knowledge and behavioral projections of reality, in line with literature on privacy paradox [2,34]. Across all three scenarios, a profound cognitive-behavioral gap was observed between theoretical understanding of digital safety and expectations of real-world peer behavior. While participants demonstrated near-unanimous consensus regarding the safest resolution — overwhelmingly endorsing formal/institutional intervention (Option 3: 100%, 78%, and 76%) — their predictions for the most probable outcome strongly favored non-protective trajectories, thus pointing to the existence of socio-emotional barriers (e.g., fear of isolation, shame, distrust of adult mediation) that inhibit the implementation of known protective behaviors. This misalignment between formal awareness and everyday execution aligns with broader socio-technical literature tracking behavioral detachment from security mandates. As discussed in [40], a profound disconnect frequently emerges when safety protocols are treated as external overlays rather than being organically integrated into the user's active, real-world context and operational routines.

The comparative analysis of the "Most Likely Outcome" in Table 8 reveals three clearly distinct response patterns depending on the nature of the threat:

- In **Scenario 1** (Interpersonal abuse and cyberbullying), when faced with *cyberbullying or doxing attacks from their classmates*, students primarily anticipated a **compromise**-oriented or intermediate response as the dominant social norm (Option 2: 74.0%). They

avoid total submission (Option 1 = 17%) but hesitate to seek formal support (Option 3 = 9%), preferring to attempt informal mediation or non-escalating technical action.

- In **Scenario 2** (Privacy and data management), when the *threat comes from a stranger online or from a grooming dynamic*, the most probable outcome shifted drastically toward high-risk compliance (Option 1: 73.0%), highlighting acute perceived **vulnerability to external manipulation**. Curiosity, the aggressor's psychological manipulation, and an underestimation of the danger lead most to believe that, in reality, the victim will give in to the interaction or remain isolated in the digital trap before seeking help.
- In **Scenario 3** (Coercion and control) response expectations fragmented between compliance (Option 1: 39.0%) and self-managed negotiation (Option 2: 48.0%). This close distribution reflects profound **relational ambivalence**, where boundaries between affection, emotional loyalty, privacy, protection of their digital rights and control remain blurred. The criticality of the Scenario 3 dilemma will be further addressed also by the next two subsections.

4.2.2. The Nuances of the Perception of "Security"

An aspect of great theoretical relevance concerns the variability with which participants conceptualize Option 1 and Option 2 as "safe" responses in different scenario contexts. While institutional/formal intervention (Option 3) was overwhelmingly recognized as the safest pathway across all scenarios (100%, 78%, and 76%), a consistent minority (22%) in both Scenarios 2 and 3 identified self-managed technical resolution (Option 2) as the most secure outcome.

This suggests an '**illusion of technical self-sufficiency',** where participants rely on autonomously managed digital barriers (e.g., blocking, two-factor authentication) to mitigate threats while actively avoiding adult disclosure due to fears of the social and reputational consequences associated with adult involvement (e.g., secondary sanctions like smartphone requisition and loss of autonomy). Option 2 may hence represent a compromise between technical security and the protection of one's privacy from adults [21,35]. Rather than displaying a simple lack of intent, this reliance on localized technical barriers illustrates how users actively recalculate safety parameters when official protocols present social friction, deprioritizing formal rules in favor of immediate coping mechanisms [40]. Ultimately, attempting to deploy a purely technical countermeasure to resolve an intimately relational vulnerability highlights a classic socio-technical misalignment, bypassing the structural, human-centric systems necessary for long-term safety [39].

Notably, in Scenario 3, a residual proportion (2.0%) designated complete compliance and silence (Option 1) as the safest choice. Though minimal, the fact that in Scenario 3 some consider submission/silence (Option 1) to be the "safer" choice (compared to 0% in Scenarios 1 and 2) deserves pedagogical attention.

Lesson learned. This highlights how intimate relational coercion can warp risk perception, leading victims to define 'safety' as the immediate avoidance of conflict with an abusive partner rather than the assertion of digital sovereignty: by giving in to demands or remaining silent, the victim seeks to calm their partner's anger, perceiving submission as the only way to avoid de-escalation or escalation of emotional violence [13,25,28].

4.2.3. Decrease in response rates

A progressive decrease in response rates was observed across the sequence of scenarios (N1 = 53, N2 = 51, N3 = 46). The most notable decrease occurred in Scenario 3, which addressed intimate partner coercion and technological abuse (13.2% reduction compared to Scenario 1). On the one hand, this may depend on "survey fatigue", since in interactive school contexts the physiological decline in attention in the final stages of the activity may lead to a drop-out rate [24]. On the other hand, the specific plot of Scenario 3 (affecting intimate spheres of young romantic relationships) suggests interpreting this decline through two additional lenses.

First, it highlights the *heightened topic sensitivity* and *emotional burden/discomfort* associated with peer-on-peer relational control, which may induce hesitation or non-response in adolescent populations compared to threat vectors where the perpetrator is outside the victim's immediate emotional or romantic sphere (such as platform-level risks or classroom-level cyberbullying): reluctance to answer or abandonment of the question may reflect an emotional defense mechanism or the fear of exposing oneself on a topic directly or indirectly experienced within one's personal experiences [17].

Second, the systemic *relational ambiguity* surrounding password sharing as a perceived 'proof of love' increases the *cognitive complexity of the dilemma*, leading to potential decision paralysis among participants: the social pressure associated with the "myth of transparency" within couples makes the decision less immediate. Participants may have found themselves having to balance emotional loyalty to their partner with the protection of their own digital autonomy [13,25]. This increased cognitive load, along with the ambivalence of the situation may have led to a higher abstention rate among those unsure of which position to take.

Lesson learned. These findings suggest that digital coercion within romantic and interpersonal relationships introduces emotional defense mechanisms and cognitive complexity that directly distort user engagement and data collection metrics. Consequently, educational and technical interventions cannot address relational cyber-threats merely as gaps in security awareness; they must be structurally designed to accommodate socio-emotional friction, offering safe pathways that reduce decision paralysis and protect digital autonomy without imposing social costs

5. Evaluating the impact of the Pinkamp intervention

In this section we outline a descriptive analysis of the effectiveness of the intervention in reshaping girls' cyber risk awareness and increasing their cyber agency and qualitatively explore the intervention's impact on participants' vocational inclinations.

5.1. Evaluation with respect to cyber-risk awareness and privacy protection

Forty-five girls completed the post-test administered midway through the second week of campus, but 10 responses were excluded from the comparative analysis due to a mismatch in the anonymous ID codes (final paired sample: N = 35).

5.1.1. Quantitative insights on the maturity profile

To provide a comprehensive evaluation of the intervention, the results are presented in two complementary steps: Table 9 illustrates the post-intervention maturity profile by combining

qualitative competency levels with average scores (N = 35), while Table 10 details the quantitative change (Delta) between baseline and post-test measurements across all target dimensions (N = 35).

Overall, the post-test maturity profile in Table 9 demonstrates a remarkably high baseline of risk awareness across almost all evaluated dimensions. With the sole exception of Doxing (*Basic*, 3.34), participants achieved *Proficient* or *Advanced* levels of *Confidence in Recognition* for every threat, with average scores consistently exceeding 3.50 and peaking at 4.49. Furthermore, *Perceived Severity* remained predominantly at a *Critical* level (exceeding 4.30 in most items), reflecting a mature and acute assessment of online dangers following the intervention.

Table 9
Post-intervention of self-perceived confidence in risk recognition, reported online prevalence, and perceived severity across categories (N = 35)

Threat Category & Specific Risks	Confidence in Recognition	Perceived Prevalence	Perceived Severity
Interpersonal Abuse & Cyberbullying			
Flaming & Public Insults	Advanced (4.49)	Widespread (3.83)	Critical (4.37)
Social Exclusion	Proficient (4.06)	Widespread (3.54)	Moderate (3.31)
Body Shaming	Advanced (4.40)	Widespread (3.77)	Critical (4.49)
Doxing	Basic (3.34)	Occasional (3.14)	Critical (4.63)
Sexualized Harassment	Advanced (4.29)	Occasional (3.31)	Critical (4.66)
Privacy & Data Exploitation			
Unauthorized Profiling	Proficient (3.57)	Occasional (3.29)	Severe (4.06)
Covert Tracking	Proficient (3.89)	Occasional (3.40)	Critical (4.31)
Dark Patterns	Proficient (4.06)	Widespread (3.91)	Severe (4.00)
Technological Abuse & Coercion			
Forced Password Sharing	Advanced (4.43)	Occasional (3.34)	Critical (4.54)
Spyware & Location Monitoring	Proficient (3.80)	Occasional (3.11)	Critical (4.34)
Account Impersonation	Proficient (3.83)	Occasional (3.23)	Critical (4.60)

The analysis of the pre- to post-intervention data (N = 35) in Table 9 reveals notable shifts across qualitative competency tiers, reflecting both enhanced risk literacy and heightened contextual awareness. The most pronounced knowledge gains occurred within the **Privacy & Data Exploitation** category where, across all three specific threats, participants achieved significant multi-tier qualitative jumps in *Confidence in Recognition*:

- *Unauthorized Profiling* and *Covert Tracking* both experienced a **two-level qualitative increase**, transitioning from *Deficient* to *Proficient* (Delta = +1.14 and Delta = +1.52, respectively).
- *Dark Patterns* shifted by **one level**, progressing from *Basic* to *Proficient* (Delta = +1.12).

This highlights the high efficacy of the intervention in shedding light on previously opaque, background-level digital threats.

A crucial pattern emerges regarding how risk knowledge influences threat perception: *increased recognition confidence directly correlates with higher reported online prevalence.* As participants learn to identify subtle or hidden threats, they become also more adept at recognizing their occurrence in everyday digital environments among peers. Notably, this phenomenon holds true even when the growth in confidence does not trigger a full qualitative tier jump. For instance, across the *Interpersonal Abuse* and *Technological Abuse* categories, positive delta values in confidence (e.g., *Flaming* Delta = +0.46; *Body Shaming* Delta = +0.14; *Spyware* Delta = +0.63) consistently aligned with upward shifts in perceived prevalence (e.g., *Flaming* moving from *Occasional* to *Widespread*, Delta = +0.57). This signals that **enhanced literacy does not merely increase theoretical knowledge, but it also sharpens participants' observational acuity toward ongoing digital risks.**

Table 10

Comparison of pre- and post-test mean scores and delta values across threat categories, evaluating changes in self-perceived confidence in risk recognition, reported online prevalence, and perceived severity following the intervention

Threat Category & Specific Risks	Confidence in Recognition		Perceived Prevalence		Perceived Severity	
	Pre/Post	*Delta*	*Pre/Post*	*Delta*	*Pre/Post*	*Delta*
Interpersonal Abuse & Cyberbullying						
Flaming & Public Insults	4.03/4.49	**+0.46**	3.26/3.83	**+0.57**	4.17/4.37	**+0.20**
Social Exclusion	3.77/4.06	**+0.29**	3.23/3.54	**+0.31**	3.31/3.31	**+0.00**
Body Shaming	4.26/4.40	**+0.14**	3.31/3.77	**+0.46**	4.51/4.49	**-0.02**
Doxing	3.11/3.34	**+0.23**	2.37/3.14	**+0.77**	4.54/4.63	**+0.09**
Sexualized Harassment	3.80/4.29	**+0.49**	2.77/3.31	**+0.54**	4.63/4.66	**+0.03**
Privacy & Data Exploitation						
Unauthorized Profiling	2.43/3.57	**+1.14**	2.71/3.29	**+0.58**	3.77/4.06	**+0.29**
Covert Tracking	2.37/3.89	**+1.52**	2.57/3.40	**+0.83**	4.17/4.31	**+0.14**
Dark Patterns	2.94/4.06	**+1.12**	3.17/3.91	**+0.74**	3.57/4.00	**+0.43**
Technological Abuse & Coercion						
Forced Password Sharing	3.91/4.43	**+0.52**	2.86/3.34	**+0.48**	4.31/4.54	**+0.23**
Spyware & Location Monitoring	3.17/3.80	**+0.63**	2.71/3.11	**+0.40**	4.06/4.34	**+0.28**
Account Impersonation	3.20/3.83	**+0.63**	2.26/3.23	**+0.97**	4.31/4.60	**+0.29**

Conversely, the data highlights a specific area requiring instructional design refinements: *Doxing* remained locked at the *Basic* confidence level post-intervention (3.11/3.34, Delta = +0.23), making it the only threat item that failed to register a qualitative level progression. While Doxing was addressed within Scenario 1, this stagnation indicates that its conceptual nuances and protective counteractions were likely overshadowed by the dominant socio-emotional dynamics of cyberbullying and public insults.

Lesson learned. Consequently, Scenario 1 must be further refined and optimized in future iterations to ensure that Doxing is more explicitly unpacked, enabling participants to achieve a comparable leap in recognition confidence.

5.1.2. Qualitative Insights on Perceived Threats and Data Exploitation Risks

Following the training intervention, an analysis of the qualitative responses collected in the post-test open-text question regarding the most feared or difficult-to-manage risks demonstrates both a shift in perspective and a refined, more technically precise understanding of digital threats. While participants continued to acknowledge the emotional burden of interpersonal abuse, their vocabulary shifted significantly toward structured technical terminology (e.g., explicit references to *"Dark Patterns"*, *"Spyware"*, and *"Accesso forzato"*), reflecting the conceptual and technical mastery acquired during the course.

A qualitative categorization of the N=35 free-text responses regarding the most complex threats to manage highlights that *Interpersonal Abuse & Cyberbullying* emerged as the primary concern (45.7%, n=16), driven largely by recurring mentions of body shaming, sexualized harassment, flaming, and doxing. *Privacy & Data Exploitation* represented the second most reported category (31.4%, n=11), characterized by anxieties surrounding covert tracking, unauthorized data sales, and dark patterns. Finally, *Technological Abuse & Coercion* accounted for 22.9% (n=8) of responses, with participants emphasizing account impersonation, unauthorized device access, and spyware/location monitoring.

As to the concern about privacy and data exploitation singled out in the baseline analysis (see Section 4.1), we observe that the persistent representation of platform-level risks (data selling, tracking, dark patterns) in around 31% of responses confirms that the intervention successfully anchored structural privacy concerns alongside the more immediately visible interpersonal risks. Anyhow, the decrease in concern regarding data privacy and exploitation (dropping from **44%** at baseline to **31%** post-test) represents one of the most compelling indicators of the intervention's efficacy: rather than signaling a drop in vigilance, this shift reflects a transition from paralyzing, ambiguous anxiety toward informed digital control and operational agency.

At baseline, participants' fears surrounding data tracking and profiling were largely driven by a perceived lack of transparency and an inability to counteract "invisible" system-level threats. The interactive anti-fraud module conducted in collaboration with the *Polizia Postale* along with Scenario 2 played a pivotal role in demystifying these risks. By providing concrete technical knowledge, demonstrating practical defense mechanisms, and clarifying legal protections, the interactive anti-fraud path and the multidisciplinary session transformed an abstract threat into a manageable set of actionable practices.

Lesson learned. Consequently, the 13-percentage-point reduction demonstrates that when adolescent girls are equipped with practical tools and clear legal frameworks, their baseline sense of helplessness diminishes. Data exploitation shifts from being viewed as an overwhelming, uncontrollable threat to a risk scenario that can be proactively mitigated through informed settings, critical awareness, and technical self-defense.

5.1.3. Shift in Perceived Self-Defense Capability and Barriers to Protection

The paired analysis revealed a substantial increase in perceived self-defense capabilities. Prior to the intervention, participants were evenly split regarding their perceived empowerment,

with 51.4% (n=18) claiming to possess adequate technological and legal tools to defend against cyber-attacks, while 48.6% (n=17) reported a complete lack of such instruments. Following the multidisciplinary intervention, **the proportion of empowered participants rose dramatically to 85.7%** (n=30), leaving only 14.3% (n=5) with lingering uncertainty.

A granular analysis of the barriers cited by the participants who rarely or never adopt recommended protective measures (where multiple selections were permitted) further clarifies the nature of this transformation. In the pre-test, non-adoption was heavily driven by operational friction and baseline informational gaps as highlighted by the 33 selections. Specifically, **54.5%** of total selections cited knowing the protective tools but lacking the procedural knowledge to configure them, while **33.3%** reflected unawareness of the tools or risks altogether.

In the post-test, total reported barriers dropped from 33 to 22 selections, marked by a sharp decline in pure lack of awareness (which dropped to just 9.1%). Conversely, operational complexity remained the primary residual constraint (63.6%), alongside a slight relative increase in optimistic bias (*"nothing serious will happen to me"*, 22.7%).

Lesson learned. These findings indicate that while the workshop effectively dismantled cognitive and awareness barriers (drastically elevating participants' overall self-defense agency) **procedural complexity and platform usability remain the critical bottlenecks** preventing the immediate translation of knowledge into active routine configuration, **underscoring the critical need for system designs that facilitate direct user control over privacy settings.**

5.2. Evaluation with respect to vocational aspects

To evaluate the vocational impact of the intervention, a separate, standalone companion questionnaire was administered, likewise employing a pre/post design, as a reflection on the impact of women presence in technology sectors and the personal motivations that attract or deter girls from the STEM fields in general and cybersecurity careers more specifically. Both the response rate and the specific survey outcomes highlight critical, unresolved issues regarding gender and cybersecurity.

The baseline pre-test yielded 48 responses, whereas the post-test saw a reduction to 34 responses, with a 29.2% attrition rate. Note that, because this companion questionnaire was administered as an independent instrument, its completion and matching dynamics slightly differed from the primary cyber-risk survey, yielding a distinct analytical subsample (N =34) specifically evaluating vocational perceptions.

While the response drop-out in the post-test was partially due to **administration timing** (the post-test was administered near the conclusion of the intensive two-week camp, close to project presentation preparation) and thus driven by end-of-camp survey fatigue, qualitative feedback highlighted that several participants experienced **psychological reactance to the stereotype-centric framing** when confronted with traditional vocational items measuring gender-based obstacles, family discouragement, or perceived intellectual superiority of man and boys in technical domains. Participants explicitly reported that they felt "unrepresented" by these items, underlining that some of the proposed questions assumed a vulnerability that did not align with their experiences and feelings.

This qualitative reaction highlights a critical demographic characteristic of the sample: the cohort consisted of highly motivated, self-selected adolescent girls possessing robust baseline

STEM self-efficacy. Unlike general-population samples where external socio-cultural barriers and perceived gender incompatibility are prominent predictors of STEM avoidance, these girls explicitly reject the idea that their academic choices are constrained by traditional gender norms and stereotypes.

Interestingly enough, while this explicit rejection of these items reflects a sense of personal agency, it can also create a "gender-blindness mask" that conceals how systemic domain framing influences their career choices, as revealed by their position regarding potential careers in cybersecurity: across both pre- and post-evaluations the empirical data revealed a striking divergence between general STEM motivation and specific career interest in cybersecurity, with participants' interest in pursuing a specialized career in cybersecurity disproportionately low compared to STEM disciplines as a whole (see Figure 3, which contrasts cybersecurity interest against general STEM career interest).

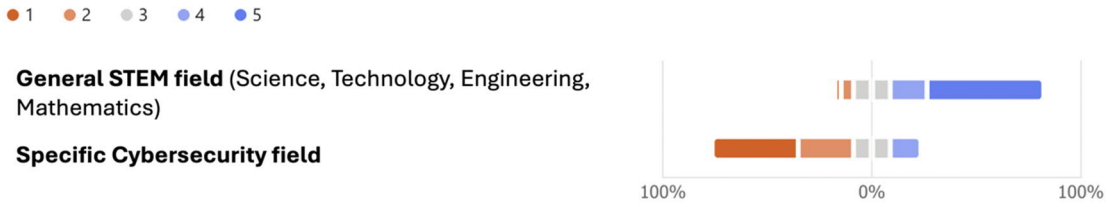


Figure 3: The Diverging Stacked Bar Chart regarding girls' projections concerning possible future careers.

It must be observed that this lack of interest does not stem from a lack of appreciation for women contributions to the domain. On the contrary, participants demonstrated overwhelming agreement with statements regarding the technical and societal value of women cybersecurity professionals: a strong majority agreed or strongly agreed that having more women cybersecurity experts is essential to effectively counter online harassment and abuse, and participants overwhelmingly recognized that women may bring a distinct, crucial sensitivity to managing digital privacy protection. This creates what might be named "**cybersecurity attraction paradox**": though young women recognize that cybersecurity is a vital domain where women expertise can yield significant prosocial and ethical benefits, nonetheless they systematically do not imagine *themselves* into these career paths. When asked to motivate their lack of interest, participants overwhelmingly attributed their choice to purely personal preferences, insisting that gender played no role in their orientation.

Anyhow, if we look at consolidated vocational literature, we recognize the specific socio-cultural framing of cybersecurity compared to other STEM disciplines: while research in vocational psychology indicates that young women frequently prioritize careers with high prosocial utility and disciplines where technical skills visibly translate into human, social, or environmental benefit (e.g., biomedical engineering, environmental data science) [8,29] cybersecurity is still overwhelmingly framed through defensive, military, or adversary-driven narratives (e.g., "hacking," "perimeter defense," "threat intelligence"), masking its profound human-centric and societal-protection dimensions [3]. Even among tech-savvy girls, cybersecurity seems to retain the idea of isolated, highly adversarial, or purely operational work

environments, rather than as a multidisciplinary, prosocial discipline protecting human rights and societal infrastructure.

However, it must be remarked that we revealed a slight increase in interest in cybersecurity during the post-evaluation phase. Beyond participants who were already interested before the camp (*"The world of cybersecurity has fascinated me since I was little..."*), some participants attributed their growing interest specifically to the perspective gained through the campus activities (*"After addressing this topic, I was interested..."*; *"I'm not particularly attracted... however, thanks to the activities during the camp, I better understand the topic..."*). Furthermore, some participants emphasized the broader social impact of the field (*"Helping make the web a safer place against potential conflict-related attacks."*).

Lesson learned. These findings offer crucial guidance for designing interventions targeting high-performing high-school girls, **evolving beyond explicit debiasing toward domain reframing**: intervention strategies for cohorts with high baseline self-efficacy should not focus on dismantling explicit gender self-doubt (these girls do not need to be convinced that they are capable of governing technology). Instead, interventions and educational pathways must reframe cybersecurity away from traditional adversarial, militaristic or purely technical narratives toward its multidisciplinary, human-centric, legal, and ethical dimensions—depicting a socio-technical culture and professional identity that fosters personal identification while aligning with their prosocial motivations and values.

6. Addressing the Research Questions

The empirical findings, along with the key lessons learned from this pilot implementation, provide nuanced insights into the two research questions that guided this investigation, offering both theoretical answers and practical guidance for future educational interventions.

As to **RQ1** (on Risk Perception, Literacy, and Agency)**,** *the multidisciplinary socio-technical intervention proved highly effective in transforming adolescent girls' passive risk awareness into actionable digital agency.* In particular, we observed a systemic Maturity Profile growth and the Exposure-Knowledge Dynamic: the quantitative assessment of participants' maturity profiles revealed a significant overall upward trajectory across knowledge, awareness, and agency levels following the intervention. Notably, the findings demonstrate a direct correlation between increased technical and operational knowledge and an expanded perception of threat prevalence. Furthermore, the analysis shows a distinct impact across system-level versus interpersonal cyber-threats and provides interesting insights.

Addressing Opaque vs. Visible Threats: Prior to the intervention, participants exhibited an acute socio-technical gap, characterized by high severity perception for visible interpersonal threats alongside deficient recognition confidence for opaque, system-level data exploitation (e.g., unauthorized profiling and covert tracking). Hands-on exposure to these hidden mechanisms dramatically shifted participants' disposition from paralyzing privacy anxiety, which constituted the primary source of baseline helplessness, to proactive operational self-defense. This transformation mirrors the socio-technical dynamics identified by [40], proving that when safety frameworks resolve real-world user friction rather than acting as a rigid external policy, the behavioral disconnect dissolves.

Navigating the Cognitive-Behavioral Intention Gap: The real-time evaluation of scenario-based dilemmas revealed a structural discrepancy between what adolescent girls recognize as

normative/safe protection strategies (e.g., formal institutional support) and their expectations of actual peer behavior. In practical dynamics, expected behavior shifts toward informal compromise or high-risk compliance, driven by fear of social exclusion, shame, and peer pressure.

Overcoming Relational Coercion and Protective Barriers: In intimate partner contexts, relational dynamics (such as the "myth of total transparency" via password sharing) interfere with threat recognition. Moreover, fear of adult secondary sanctions (such as phone confiscation) often fosters an "illusion of technical self-sufficiency," leading girls to rely solely on individual technical controls while avoiding formal reporting mechanisms. Overall, while the intervention successfully dismantled cognitive and informational barriers, procedural complexity remains the main residual bottleneck to routine protection adoption. This operational hesitation underlines that multi-layered modern threats cause severe psychological and cognitive friction, demanding non-linear, adaptive user interfaces, as discussed in [38].

As to **RQ2** (on Gender in Cybersecurity)**,** *the intervention shed light on the complex relationship between gender-sensitive training, STEM self-efficacy, and cybersecurity career orientations among high-performing high school girls*. Findings show that high-efficacy high school girls explicitly reject traditional stereotype-centric framing, showing strong baseline technical confidence and acknowledging the societal value of women cybersecurity experts; yet their personal career interest in the field remains disproportionately low compared to general STEM fields. This tells us that engaging empowered cohorts of young women demands a fundamental "domain reframing": shifting cybersecurity away from adversarial, defensive, or purely technical narratives toward a multidisciplinary, human-centric, legal, and prosocial discipline that directly aligns with their career motivations and resolves the attraction paradox.

7. Conclusions and future work

This experience paper presented the design, implementation, and empirical evaluation of a multidisciplinary educational intervention conducted with a socio-technical lens within the framework of the Pinkamp summer school at the University of L'Aquila. Aimed at bridging the gap between passive cyber-risk awareness and actionable digital agency among adolescent girls, the framework integrated technical, legal, and socio-psychological perspectives through scenario-based workshops, interactive anti-fraud paths, and exposure to STEM role models.

Ultimately, our findings demonstrate that a socio-technical approach to cybersecurity is not merely beneficial, but imperative for the future of cybersecurity education and practice. This perspective serves a dual purpose: on the one hand, it moves beyond the overly operational view of privacy controls — whose cognitive and procedural complexity proved to be a major barrier hindering users' agency — and, on the other hand, it fosters a systemic "degendering" of the field by dismantling its historically masculine, adversarial coding, thereby making cybersecurity genuinely accessible and attractive to young women. Crucially, these two dimensions are deeply intertwined: empowering women to enter cybersecurity infuses the discipline with new fresh perspectives that, in turn, may reshape future technological design, effectively closing the loop between inclusive pedagogy/participation and human-centered innovation. Ultimately, this dual focus on technical simplification and domain reframing fulfills the foundational democratic intent of socio-technical design, humanizing technology to empower historically marginalized user groups [39].

7.1. Limitations

The findings and contributions of this pilot study should be interpreted in light of some operational and methodological limitations.

Exploratory Nature of Quantitative Evaluation. Given the exploratory nature of this pilot intervention, the quantitative evaluation focused on a descriptive analysis of mean score variations between the pre- and post-workshops. While these preliminary trends effectively capture the shift in participants' awareness, formal non-parametric testing (e.g., Wilcoxon signed-rank test) is planned for future analysis, possibly on larger-scale iterations, to validate statistical significance.

Limited and Self-Selected Sample. The study involved a cohort of 58 consenting high school girls (aged 16–18) enrolled in a STEM-oriented summer school, yielding N = 52 baseline responses and a final matched sample of N = 35 for the short-term pre/post intervention assessment. While ideal for validating the research protocol and measurement instruments, this self-selected sample size is not representative of the general adolescent population.

Panel Facilitation and Interdisciplinary Alignment. Due to scheduling constraints, preparatory briefing sessions with multidisciplinary experts were conducted asynchronously. This constrained full real-time cross-disciplinary coordination during the live panel, occasionally resulting in contrasting viewpoints during discussions.

Contextual and Institutional Influences. The workshop was conducted in close sequence with an anti-fraud campaign organized by the Italian State Police (Polizia Postale). The physical presence of uniformed officers, alongside mandatory legal disclaimers regarding criminal reporting in informed consent forms, though ethically and legally required, may have induced hesitation or discouraged participants from sharing sensitive personal experiences. Specifically, this institutional framing might have subtly shifted participants' perception from an open, collaborative learning space toward a formal regulatory context, potentially triggering social desirability bias or self-censorship regarding non-standard online behaviors.

Workshop Design and Fatigue Effects. Participant engagement naturally declined toward the end of the session, leading to a drop in response rates for the final scenario addressing intimate partner coercion. Beyond physiological survey fatigue, this response drop-out reflects the heightened cognitive load and psychological friction that emerge when users face non-linear socio-technical dilemmas where emotional loyalty and systemic risk overlap [38]. Furthermore, presenting fixed response options across scenarios may have introduced response habituation.

7.2. Future Work

Building upon the lessons learned and addressing current study limitations, future research will progress along several interconnected lines.

First, expanding the refined research protocol and validated measurement scales to a *larger, gender-diverse, and heterogeneous student sample* across regional high schools will be essential to evaluate the broader transferability of the framework. Beyond scaling, direct interventions will benefit from a *refinement of the workshop mechanics*. In particular, re-ordering the activities by introducing sensitive relational dynamics (such as digital control in intimate relationships) at the beginning can maximize participant engagement before cognitive fatigue sets in. Furthermore, randomizing response choices will help mitigate habituation bias, while

redesigning Doxing scenarios will more effectively highlight specific technical and legal counteractions.

To support these methodological refinements, the delivery process itself requires an *enhanced facilitation framework*. Implementing joint training sessions and shared protocols for multidisciplinary panelists prior to live interventions will ensure seamless narrative alignment across technical, legal, and socio-psychological perspectives.

Ultimately, these insights point toward the development of a domain-reframing educational curriculum. By translating key learnings into modular toolkits for schools, future initiatives can systematically reframe cybersecurity not merely as a technical skill set, but as an essential socio-technical pillar of human rights protection, digital citizenship, and prosocial ethics.

Ethical considerations

The study was conducted in accordance with the Declaration of Helsinki and approved by the Ethics Committee of the University of L'Aquila (id: 14-2026) for studies involving humans. Formal agreement and informed consent (signed either by themselves if legal adults, or by a parent/legal guardian in the case of minor) was obtained from all subjects involved in the study.

Declaration on Generative AI

During the preparation of this work, the authors used MS Copilot to generate the illustrations of the graphic novels (starting from textual descriptions). Further, the authors used Google Translator to translate to English the internal project submitted to the Ethics Committee of the University of L'Aquila and for general style feedback throughout the paper and used Gemini in order to format the list of reference according to the template. After using these tools/services, the author reviewed and edited the content as needed and takes full responsibility for the publication's content.

Acknowledgements

PinKamP 2026 is co-financed by the University of L'Aquila, by the donation of Elena Grifoni Winters, by the Scientific Degree Plan in Computer Science and Physics, by the Engineering Orientation and Tutoring Plan and by the European Union - NextGenerationEU - National Recovery and Resilience Plan (PNRR) on the "SAFI3" project (Synergies to orient and promote Higher Education eligible for funding pursuant to MUR Decree no. 1792 of 20/11/2024 (CUP: D13C24001960001), for which the GSSI is the lead school of the network of Higher Education Schools) and is carried out in collaboration with the Gran Sasso National Laboratories of the National Institute for Nuclear Physics, Living Lab, and Papert digital Class@Univaq..

References

[1] M. H. M. Altarawneh, A. Althunibat, M. H. Almajali, N. Alzriqat, S. Alazzam, Cybersecurity awareness among school students: Exploring influencing factors, legal implications, and knowledge gaps, International Journal of Innovative Research and Scientific Studies 8 (2025) 1516–1529. doi:10.53894/ijirss.v8i1.3533.

[2] S. Barth, M. D. T. de Jong, The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review, Telematics and Informatics 34 (2017) 1038–1058. doi:10.1016/j.tele.2017.04.013.
[3] R. Bencivenga, F. Bosco, S. Pozzolo, Gender and Technology: new capabilities or old masked prejudices?, AboutGender - International Journal of Gender Studies 5 (2016) I–XIV.
[4] N. Bhatnagar, M. Pry, Student attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media: An initial study, Information Systems Education Journal (ISEDJ) 18 (2020) 48–58.
[5] E. Casey, Digital evidence and computer crime: Forensic science, computers, and the internet, Academic Press, 2011.
[6] C. U. Chavan, S. J. Gaddam, A study of cybercrime awareness among adolescents, Journal of Emerging Technologies and Innovative Research (JETIR) 11 (2024) b633–b639.
[7] R. E. Clark, R. E. Mayer, E-Learning and the Science of Instruction: Proven Guidelines for Consumers and Designers of Multimedia Learning, John Wiley & Sons, 2016. doi:10.1002/9781119239086.
[8] A. B. Diekman, E. R. Brown, A. M. Johnston, E. K. Clark, Seeking Congruity Between Goals and Roles: A New Look at Why Women Opt Out of Science, Technology, Engineering, and Mathematics Careers, Psychological Science 21 (2010) 1051–1057.
[9] M. Duggan, Online Harassment 2017, Pew Research Center, 2017. URL: https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/.
[10] eSafety Commissioner, Technology-facilitated abuse: family, domestic and sexual violence literature scan, Australian Government, Canberra, 2023. URL: https://www.esafety.gov.au/sites/default/files/2023-10/Technology-facilitated-abuse-family-domestic-sexual-violence-literature-scan.pdf.
[11] E. P. Errington, Mission possible: using near-world scenarios to prepare graduates for the professions, International Journal of Teaching and Learning in Higher Education 23 (2011) 84–91.
[12] M. Farinella, The potential of comics in science communication, JCOM 17 (2018) Y01. doi:10.22323/2.17010401.
[13] D. Freed, J. Palmer, D. Minchala, K. Levy, T. Ristenpart, N. Dell, "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology, in: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, CHI '18, ACM Press, New York, NY, USA, 2018, pp. 1–13. doi:10.1145/3173574.3174241.
[14] M. C. Green, T. C. Brock, The role of transportation in the persuasiveness of public narratives, Journal of Personality and Social Psychology 79 (2000) 701–721. doi:10.1037/0022-3514.79.5.701.
[15] J. Herrington, R. Oliver, An instructional design framework for authentic learning environments, ETR&D 48 (2000) 23–48. doi:10.1007/BF02319856.
[16] ITEA, Technological literacy for all. A rationale and structure for the study of technology, 2nd ed., International Technology Education Association, Reston, 2006.
[17] A. E. Jaffe, D. DiLillo, L. Hoffman, M. Haikalis, R. E. Dykstra, Does it hurt to ask? A meta-analysis of participant reactions to trauma research, Clin. Psychol. Rev. 40 (2015) 40–56. doi:10.1016/j.cpr.2015.05.004.

[18] C. Kalapriya, K. B. Chammampati, Awareness of cyber security and digital etiquette among adolescent girls across academic streams, International Journal of Home Science 11 (2025) 110–111.
[19] S. Kokolakis, Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon, Computers & Security 64 (2015). doi:10.1016/j.cose.2015.07.002.
[20] J. Lave, E. Wenger, Situated learning: Legitimate peripheral participation, Cambridge University Press, 1991. doi:10.1017/CBO9780511815355.
[21] A. Marwick, d. Boyd, Networked privacy: How teenagers negotiate context in social media, New Media & Society 16 (2014) 1051–1067. doi:10.1177/1461444814543995.
[22] W. Newhouse, S. Keith, B. Scribner, G. Witte, National initiative for cybersecurity education (NICE) cybersecurity workforce framework, NIST special publication 800 (2017) 181.
[23] S. Pabian, Bystanders' perceptions on online hate speech: Investigating the effects of perpetrators' justifications and the bystander's role on bystanders' attitude and prosocial intervention intentions, Cyberpsychology: Journal of Psychosocial Research on Cyberspace 19 (2025). doi:10.5817/CP2025-4-6.
[24] S. R. Porter, M. E. Whitcomb, W. H. Weitzer, Multiple surveys of students and survey fatigue, New Directions for Institutional Research 2004 (2004) 63–73. doi:10.1002/ir.101.
[25] L. A. Reed, R. M. Tolman, L. M. Ward, Snooping and Sexting: Digital Media as a Context for Dating Aggression and Abuse Among College Students, Violence Against Women 22 (2016) 1556–1576.
[26] J. Ringrose, R. Gill, S. Livingstone, L. Harvey, A qualitative study of children, young people and 'sexting': a report prepared for the NSPCC, NSPCC, 2012.
[27] M. Ryan, M. McEwan, V. Sansare, P. Formosa, D. Richards, M. Hitchens, Design of a serious game for cybersecurity ethics training, in: Proceedings of the 2022 Digital Games Research Association (DiGRA) International Conference: Bringing Worlds Together, Kraków, Poland, 2022. URL: http://www.digra.org/wp-content/uploads/digital-library/DiGRA_2022_paper_156.pdf.
[28] E. Stark, Coercive Control: How Men Entrap Women in Personal Life, 2nd ed., Oxford University Press, New York, 2024. doi:10.1093/oso/9780197639986.001.0001.
[29] R. Su, J. Rounds, All STEM fields are not created equal: People and things interests explain gender disparities across STEM fields, Front. Psychol. 6 (2015) 189. doi:10.3389/fpsyg.2015.00189.
[30] L. Tarantino, A. Di Marco, Gender equality: the need for explicit address and actions in ICT and STS agendas, in: Proc. of 7th International Workshop on Socio-Technical Perspective in IS development (STPIS'21), 2021.
[31] M. Tatalovic, Science comics as tools for science education and communication: a brief, exploratory study, JCOM 8 (2009) A02. doi:10.22323/2.08040202.
[32] A. Van Langen, R. Bosker, H. Dekkers, Exploring cross-national differences in gender gaps in education, Educational Research and Evaluation 12 (2006) 155–177. doi:10.1080/13803610600587016.
[33] R. Von Solms, J. van Niekerk, From information security to cyber security, Computers & Security 38 (2013) 97–102.

[34] M. Weinberger, D. Bouhnik, M. Zhitomirsky-Geffet, Factors Affecting Students' Privacy Paradox and Privacy Protection Behavior, Open Information Science 1 (2017) 3–20. doi:10.1515/opis-2017-0002.
[35] P. Wisniewski, A. K. Ghosh, H. Xu, M. B. Rosson, J. M. Carroll, Parental Control vs. Teen Self-Regulation: Is there a middle ground for mobile online safety?, in: Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing, CSCW '17, ACM Press, New York, NY, USA, 2017, pp. 51–69. doi:10.1145/2998181.2998352.
[36] C. Clegg, Sociotechnical principles for system design, Applied Ergonomics 31 (2000) 463–477.
[37] S. Livingstone, M. Stoilova, The 4Cs: Classifying online risk to children, CO:RE Short Report Series on Key Topics, Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI), Hamburg, 2021. doi:10.21241/ssoar.71817.
[38] E. Mumford, Dangerous Decisions: Problem Solving in Tomorrow's World, Kluwer Academic/Plenum Publishers, New York, NY, 1999. doi:10.1007/978-1-4615-4797-6.
[39] E. Mumford, The story of socio-technical design: reflections on its theory, success and practice, Information Systems Journal 16 (2006) 317–342. doi:10.1111/j.1365-2575.2006.00221.x.
[40] M. Sadok, S. Alter, P. Bednar, "It is not my job": exploring the disconnect between corporate security policies and actual security practices in SMEs, Information and Computer Security 28 (2020) 467–483. doi:10.1108/ICS-01-2019-0010.