

Article

Digital Safety and Risk Perception in Higher Education: Insights from Spanish University Students with Intellectual Disabilities

Joanne Mampaso-Desbrow ¹, Margarita Alonso-Criado ¹, María Dolores López-Salmerón ²
and Ángel Vicario-Merino ^{3,*}

¹ Faculty of Education, Camilo Jose Cela University, 28692 Villanueva de la Cañada, Spain; jmampaso@ucjc.edu (J.M.-D.); malonso@ucjc.edu (M.A.-C.)

² Faculty of Psychology and Health Sciences, Universidad a Distancia de Madrid, 28400 Collado Villalba, Spain; mariadolores.lopez.s@udima.es

³ Faculty of Health Sciences, Universidad Internacional de La Rioja, Avenida de la Paz, 137, 26006 Logroño, Spain

* Correspondence: angel.vicario@unir.net

Abstract

As digital technologies become increasingly integrated into daily life, individuals with intellectual disabilities face both opportunities and risks in virtual environments. Despite widespread internet access and frequent use of digital devices among the general population, many individuals with disabilities continue to experience significant barriers to digital participation. These include difficulties in using technological tools, limited access to devices at home, and challenges in navigating online environments safely and independently. This study investigates the cybersecurity knowledge, risk perception, and privacy practices of 28 university students with mild intellectual disabilities in Spain. Utilizing a validated, accessible self-assessment questionnaire, the research analyzes participants' understanding of digital threats, self-protective behaviors, and gender-based differences in knowledge and decision-making. Results reveal a generally high awareness of online risks and appropriate use of privacy settings, though inconsistencies in password security and high social media usage persist. Female participants demonstrated slightly higher levels of theoretical knowledge. The findings underscore the urgent need for inclusive, accessible cybersecurity education tailored to cognitive diversity. Promoting digital autonomy and safety through targeted interventions can reduce the digital divide and foster full social participation. This research contributes to the broader discourse on digital inclusion and protection for individuals with disabilities in an increasingly connected world.

Keywords: university; intellectual disability; cybersecurity; social networks; profile privacy



Academic Editor: Malcolm MacLachlan

Received: 10 June 2025

Revised: 10 October 2025

Accepted: 1 November 2025

Published: 20 November 2025

Citation: Mampaso-Desbrow, J.; Alonso-Criado, M.; López-Salmerón, M.D.; Vicario-Merino, Á. Digital Safety and Risk Perception in Higher Education: Insights from Spanish University Students with Intellectual Disabilities. *Disabilities* **2025**, *5*, 108. <https://doi.org/10.3390/disabilities5040108>

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Intellectual disability is a developmental disorder that affects both intellectual (cognitively in reasoning, abstract thinking, and learning from experiences) and adaptive levels (difficulty in meeting established sociocultural standards, such as independence or responsibility). Individuals with intellectual disabilities require support in activities of daily living across different domains (conceptual, social, and practical) as described by the American Psychiatric Association in the Diagnostic and Statistical Manual of Mental Disorders, Fifth Edition, Text Revision (DSM-5-TR) [1]. In Spain, the prevalence of young adults with intellectual disabilities between 20 and 29 years old is 1.19%, gradually decreasing as age range increases [2].

In recent years, Spanish higher education institutions have increasingly implemented inclusive academic programs and vocational pathways for young adults with intellectual disabilities. This expansion, supported by national and European initiatives, has led to a growing presence of these students in university settings. As a result, new educational and professional scenarios are emerging, requiring adapted guidance models and tools to support their development. Within this context, the present study focuses on university students with intellectual disabilities, recognizing the importance of equipping them with digital competencies and cybersecurity awareness to foster autonomy, inclusion, and safe participation in online environments.

There are significant advocates for inclusion, such as national entities that actively work for complete inclusion, respect, and equality supported by international frameworks like the United Nations Convention on the Rights of Persons with Disabilities (UNCRPD), particularly Article 24 on inclusive education, and reinforced by national policies such as Spain's Organic Law 3/2007 of 22 March, for the effective equality between women and men, and Law 15/2022 of 12 July, on equal treatment and non-discrimination, which promote accessibility, participation, and non-discrimination. They focus their efforts on advocating for rights, development, and autonomy, as well as supporting families and creating opportunities in various aspects of daily life [3]. Nevertheless, despite these initiatives, significant challenges to achieving comprehensive inclusion persist, manifesting both within educational contexts—where structural and attitudinal barriers hinder full participation [4]—and within the labor market, contributing to exclusion from employment opportunities [5].

Recent national statistics confirm the widespread use of Information and Communication Technologies (ICT) in Spain. According to the National Institute of Statistics [6], 95.4% of the population has internet access, and 82.6% of the population has a computer at home. Additionally, nine out of ten individuals aged 16 to 74 regularly use ICT tools. The State Observatory on Disability [7] further reports that 88.8% of the population uses computers, 95.5% of the population uses mobile phones, 86.7% of the population engages in instant messaging (e.g., WhatsApp), and 70% of the population participates in social networks such as Facebook or Twitter.

However, these general figures obscure the persistent digital divide affecting people with disabilities. According to Fundación Adecco [8], 45% of individuals with disabilities report difficulties in using technological devices, citing accessibility barriers (32%), economic limitations (15.9%), and fear of online fraud (20.6%). Moreover, 13% lack internet access at home, and among those who do, 38% admit to struggling with online navigation. In the context of higher education, Fernández-Batanero et al. [9] emphasize that while ICTs can enhance inclusion, students with disabilities continue to face technological, pedagogical, and institutional barriers that hinder their full participation in digital learning environments [10].

Young people with intellectual disabilities are also connected to the internet and/or social networks and utilize technological tools [11]. It is asserted that it is crucial to consider that the rights of individuals must also be safeguarded in cyberspace [12]. Therefore, it is necessary to develop a series of digital adaptations, such as appropriate use of social networks and training to learn to protect their private data and avoid the vulnerability of their rights to third parties [13].

The theory of positive risk-taking emphasizes the importance of enabling individuals to make informed decisions that involve manageable risks, fostering autonomy, confidence, and personal growth. In the context of cybersecurity, this approach shifts the focus from merely protecting individuals with intellectual disabilities to equipping them with the skills and knowledge needed to navigate digital environments safely and independently [14,15].

Rather than framing online engagement as inherently dangerous, positive risk-taking encourages the development of critical thinking, self-protective behaviors, and responsible digital citizenship. This perspective is particularly relevant when addressing inconsistencies in password management or high social media usage, as it supports the idea that individuals can learn to assess risks and make secure choices without being excluded from digital participation.

Recent research highlights that adults with intellectual disabilities, when supported appropriately, can develop resilience and independence in managing online risks [16]. Moreover, Seale, Nind, and Simmons [14] propose that positive risk-taking, when embedded in inclusive educational practices, can challenge risk-averse cultures and promote meaningful participation in digital life. This perspective aligns with the growing recognition that accessible cybersecurity education, grounded in human rights, must not only focus on technical skills but also on safeguarding dignity and democratic participation [17].

Aligned with the principles of inclusive education and the right to digital participation, this study contributes to the development of pedagogical responses that support the digital competence of university students with intellectual disabilities.

In this context, the study aims to analyze the extent to which individuals with intellectual disabilities possess the necessary knowledge to protect themselves from potential digital threats. This study begins with the premise that there is limited understanding of the level of knowledge that tertiary students with intellectual disabilities have regarding digital risks, such as information security, privacy, and personal data protection. Recognizing and valuing their existing digital practices is essential to identifying areas where further support or training may be beneficial. The specific objectives of the study will be:

- Explore the cybersecurity knowledge perceived by the participants;
- Identify, by gender, the knowledge about dangers expressed by the participants;
- Analyze the self-perception of the participants regarding potential risks associated with the use of social networks;
- Examine the knowledge of and practices carried out by the participants regarding the privacy of their profiles on social networks.

Cybersecurity for People with Intellectual Disabilities

Currently, legislation and best practices consider cybersecurity and protection for the general public, with a focus on protecting children. However, despite support in healthcare, financial assistance, and education, individuals with intellectual disabilities are rarely considered when it comes to cybersecurity [18].

The use of the internet and social networks is a gradual phenomenon worldwide, mainly in North America and Europe. In Western Europe, 54% (Eastern Europe, 44%) of the population uses social networks [19]. Social networks entail both opportunities and risks, and it is essential for professionals and policymakers to increase opportunities for benefiting from and reducing the harms of the internet [20]. These aspects affect all young people today, including those with intellectual disabilities. More research is needed to ensure that young people with intellectual disabilities have equitable access to information and skills related to cybersecurity, especially in contexts such as tertiary education, where digital autonomy is increasingly important [21].

Furthermore, the internet seems to provide an opportunity for both adults and young people with intellectual disabilities [22–27], but there are differences between these groups, especially regarding barriers to internet access, also referred to as the “digital divide” [15]. This is an important issue concerning adults, but it is not as prominent concerning young people with intellectual disabilities. This “digital divide” is a recurring and significant issue,

highlighting the disparity in internet access between people with and without disabilities to varying degrees worldwide [28].

People with intellectual disabilities experience both benefits and risks when using social networks [23]. However, it is worth noting that these young people rarely articulate concerns about risk, vulnerability, and support themselves. Nevertheless, parents, professionals, and researchers express concern about the need to assess possible vulnerability, need for guardianship, and guidance [20]. In this line, Seale [29] suggests the theory of positive risk-taking as a framework for providing support [27]. This positive risk-taking allows people with intellectual disabilities to have greater control over how they live their lives, which can lead to independence and well-being but also entails risks [29–32]. Several studies emphasize the potential risks associated with this theory [24,33,34].

To develop and enact changes in all aspects of life, it is necessary to understand risk [32]. In the virtual context, it is important to highlight the relevance of the theory of positive risk assumption, often associated with thinking and speaking about technologies as tools capable of changing the lives of people with intellectual disabilities [29].

Within current educational processes and designs, cybersecurity training is an essential component of the Information and Communication Technology subject. Safe use of media is part of the curriculum for all students. Educators are promoting cyber well-being through social-emotional learning (hereafter SEL), incorporating digital and media literacy skills [35,36].

Students with intellectual disabilities can safely interact in virtual environments, whether for social activities, learning, or employment, when equipped with appropriate functional skills and provided with accessible methods and tools. Student awareness of potential online dangers, coupled with the development of digital literacy skills, may motivate them to approach online risks positively [37]. While most research reports risks, few emphasize the need for further studies on the training of individuals with intellectual disabilities in social media use [38].

According to Jimenez and O'Neill [39], despite the benefits of incorporating such technologies to support education, there is still a need for vigilance to counteract the inherent risks associated with their use, as protecting students and their information is fundamental to the effective deployment of any technology in education.

When it comes to using digital media, individuals differ in their intellectual capabilities and perceptions [40]. Some perceived online risks for people with intellectual disabilities include being bullied, deceived, or harassed online; disclosing personal information to others; and being vulnerable to online fraud [23]. Therefore, the use of social networks by people with disabilities largely depends on the support of those around them [26,38,41].

In addressing cybersecurity for individuals with intellectual disabilities, it is essential to situate the discussion within a broader human rights framework that accounts for the accelerating expansion of AI-driven surveillance and the rights to education. The normalization of technologies such as facial recognition, predictive policing algorithms, and smart sensors has redefined digital environments as spaces of continuous monitoring, often without transparency or consent.

As Chan and Lo [16] demonstrate, these systems pose a profound threat to the right to privacy, particularly for vulnerable populations, by enabling the covert collection and analysis of personal data and reinforcing privatized mechanisms of social control. Therefore, cybersecurity education must not only promote technical competence and autonomy but also critically engage with the ethical implications of dataveillance. This includes advocating for privacy-by-design, algorithmic transparency, and human oversight to ensure that digital inclusion does not come at the expense of dignity, freedom, and democratic values.

Additionally, privacy, information, and cybersecurity (hereafter PICS) are interrelated features that have become a concern for most individuals. The majority of PICS responsibility falls on the end user, in this case, the students, who are expected to adopt PICS tools, guidelines, and functions to stay safe. However, the literature reflects that many users do not apply these PICS tools. The utilization of PICS tools is a fundamental concern, especially for youth with intellectual disabilities. Cognitive skills determine how young individuals perceive the utility of PICS tools, and as such, usage guidelines should consider the diverse cognitive abilities within various groups and their shared perceptions of their usage [42].

2. Materials and Methods

2.1. Sample

This is a descriptive cross-sectional study conducted at a private university over two consecutive academic years of a program for young adults with intellectual disabilities within a university setting in the Autonomous Community of Madrid.

The Socio-Labor Competencies Program at UCJC supports young people with intellectual disabilities in preparing for both university life and future employment. Adopting a holistic approach, it combines individualized and group tutoring, complementary training, participation in mainstream university classrooms, and well-being activities. Students also engage in mentoring and develop a professional portfolio and learning dossier as tools for self-reflection and transition planning.

Experiential learning is central to the program, with on-campus and external placements implemented within a supported employment framework. These placements, guided by mentors and job coaches, enable students to apply acquired competencies in authentic professional contexts, thereby fostering meaningful inclusion in higher education and the labor market.

The minimum criterion to be eligible for admission to the program was the presentation of a medical report certifying an intellectual disability of at least 33%. The selection process included a personal interview with the candidate and their legal guardians, conducted by program staff composed of two psychologists. In this interview, special attention was given to the expressed desire of the individual with a disability to participate in the program, recognizing their autonomy and personal motivation as essential components of the admission decision. In addition to reviewing the medical documentation, the process involved functional skills assessments and an evaluation of the individual's current life circumstances. These elements were considered essential to determine the suitability of the program for each candidate, ensuring that their participation aligned with both their developmental needs and personal goals. Data collection occurred with a one-year difference between academic years.

The participants in this study were 28 university students with intellectual disabilities, comprising 57.1% ($n = 16$) males and 42.9% ($n = 12$) females, aged between 18 and 33 years, with a mean age of 23 years. They belonged to two cohorts of students from consecutive academic years, both of which shared equivalent conditions in terms of access to educational and technological resources, instruction provided by the same teaching staff, and a homogeneous initial diagnosis regarding competence level and academic profile. Data collection was conducted six months apart, corresponding to the midpoint of each academic year. Participants had a diagnosis of mild intellectual disability associated with other degrees of developmental disorders. The inclusion criteria for this study were as follows: (a) possession of an official disability certificate equal to or greater than 33%, (b) documented diagnosis of intellectual disability, and (c) successful completion of the program's admission process.

According to the report on administratively recognized persons with disabilities [43], there are 224,708 individuals aged 18–35 in Spain with a diagnosed disability of 33% or more. Considering a heterogeneity of 99% (understanding heterogeneity as the diversity of the population and considering that access to education involves a pre-selection process), a margin of error of 5%, and a confidence level of 94%, a sample size of $n = 14$ (per year) is considered significant. There are no new available data on administratively recognized persons with disabilities.

Participation was voluntary and followed an open call issued within the program. All participants received accessible information regarding the study's objectives, the anonymous and confidential nature of the data, and their right to withdraw at any time. Informed consent was obtained through easy-to-read documents featuring pictograms, validated by specialized support staff.

The selection of university students as the study population was based on criteria of accessibility and educational relevance. This group is at a critical stage in the development of digital competencies. Although the questionnaires analyzed focused on the use of social technologies—such as social media, messaging platforms, and video games—many of the skills assessed, including privacy management, information security, and awareness of digital violence, are highly pertinent within the context of higher education.

Data were collected over two consecutive academic years, involving independent cohorts of students with homogeneous characteristics in terms of age, academic level, and admission criteria. Due to the limited access of this population to higher education, the sample size was necessarily small. Consequently, the study adopts a descriptive and exploratory approach, aimed at generating initial evidence to support future research with larger samples.

2.2. Instrument

The instrument chosen for assessing self-perception regarding aspects related to knowledge of identifying associated risks was a cybersecurity self-assessment questionnaire. This is an ad hoc questionnaire aimed at obtaining maximum information through specific, clear, and accessible questions adapted to the needs of individuals with mild intellectual disabilities. For its validation, the content validation method was used through the expert judgment method, followed by reliability analysis through Cronbach's alpha calculation.

A questionnaire comprising 21 questions was used, including dichotomous (yes/no) questions, questions assessed using a 5-point Likert scale (1 "I didn't know", 2 "I am unable", 3 "Yes, but with help", 4 "Yes, always", and 5 "Yes, and I could explain it"), and open-ended questions. The items were adapted and validated from self-assessments developed by the Spanish National Cybersecurity Institute (hereafter, INCIBE). For content validity, experts in the field were consulted, all with professional backgrounds in online privacy, personal data protection, and image rights in virtual environments. Specialists were required to have over five years of professional experience and prior involvement in designing educational interventions for young people with intellectual disabilities [44].

For validation, a score was assigned to each pre-selected item using a scale of 0–5 based on three validation criteria: clarity, relevance, and pertinence. Recommendations regarding validation by expert judgment were followed [45–47]. Thus, 9 professionals were included in the sample by intentionality. The correspondence between the center of interest and questionnaire items can be seen in Table 1.

Table 1. Correspondence between the center of interest and questionnaire items INCIBE [44].

Area of Interest	Items of the Questionnaire
Knowledge about cybersecurity and educational platforms [35]	1, 2, 6, 7, 8, 11
Knowledge about dangers [35]	3, 5, 14, 15
Relationship with the internet [35]	4
Privacy of personal profiles on social networks [40]	9, 10, 13,
Risk perception [40]	12, 16, 17, 19
Updates on cybersecurity [35]	15, 18, 20, 21

Source: original work.

Although people with intellectual disabilities were not included as part of the expert panel, pilot testing of the questionnaire was conducted with students from the same educational program to ensure comprehension and appropriateness, allowing further adjustments before final administration.

For construct validity, analysis of selected items, correlation analysis, suitability tests, and reliability tests were conducted. To measure the instrument's reliability, Cronbach's alpha coefficient of internal consistency was used (Table 2), analyzing the test in a unidimensional manner, i.e., integrating all items. Including all items yielded a Cronbach's alpha for the overall questionnaire of 0.76, indicating good internal consistency [48].

Table 2. Index of Reliability of the Questions on Knowledge.

Reliability Statistics of Each Element	
Items	Cronbach α
1. How would you define a social network? Explain it in your own words.	0.770
2. What do the initials ICT stand for?	0.758
3. How would you define the concept of "Tech addiction"?	0.765
5. What actions do you think could be called "cyberbullying"?	0.713
7. Which password do you think is more secure?	0.750
8. Justify the previous answer.	0.745
12. What are the risks of excessive use of social networks?	0.712
15. Threatening and blackmailing the victim with the publication of intimate or sexual photos or videos is called.	0.757
16. How can cyberbullying be prevented?	0.732
17. Of the following techniques, which do you think correspond to...	0.727
19. If someone finds that after opening a program, their entire computer is encrypted and they are asked for a password to access their computer by paying a sum to someone, they are a victim of: (a) Spyware, (b) Backdoors, (c) Ransomware, or (d) Trojan.	0.765
20. What are the methods of propagation of malware?	0.742
21. What are the consequences of software piracy?	0.729

Thus, regarding items concerning profile privacy and risk perception, it is worth mentioning that the items developed by Alonso-Ruido et al. [49] were taken as a reference and as indispensable elements that complement the study's objective and thus analyze knowledge about aspects such as security, privacy, and protection of information and personal data.

2.3. Procedure

Data collection was conducted prior to initiating a training proposal to design training in line with informative and formative guidelines coherent with the educational demands of the participants. Complete freedom was granted to respond using the anonymous and confidential nature of the participants, informed consent, and assent in cases where it

was required due to modified legal capacity, following parameters approved by the ethics committee of Camilo José Cela University. The collection of such information was carried out by specialized personnel with prior knowledge of the participants, spanning at least more than six months.

For the online version, the Microsoft Forms program was used. Additionally, response types were complemented with pictograms. Considering the population to whom the questionnaire would be applied, accessibility adaptations were made, including adaptation of instructions for easy reading and inclusion of visual support in the expected response type, complemented with pictograms to understand possible responses. Additionally, font size was increased in the printed version to improve accessibility of the information contained in the evaluation instruments.

Data analysis was performed using the statistical software Jamovi v2.6.23.0 based on the “R” engine and Microsoft Excel v16.102.2 for data organization, initial analysis, and graphical representation. Descriptive analyses were conducted, supplemented with correlation analyses. The Shapiro–Wilk test was used to identify normality, Pearson’s correlation coefficient (R) was utilized for normally distributed elements, and Spearman’s correlation for those not meeting normality assumptions.

To analyze the obtained data, the most relevant aspects are included below, organized based on the results obtained. They are structured according to risk perception. Furthermore, to analyze the data, the nature of the items was considered, grouping them into three possible categories: knowledge about the topic, actions taken, and decision-making in response to risk perception.

3. Results

3.1. Decision-Making Regarding Risk Perception

Participants generally reported risk-averse behavior when deciding whether to accept friend requests on social networks. Most justified their rejection of unknown contacts by emphasizing caution and the potential for harmful intentions.

Regarding data visibility (item 11), 82.1% of participants ($n = 23$) restricted profile information to friends, 14.3% ($n = 4$) kept data open to the public, and 3.6% ($n = 1$) were unsure of their privacy settings. No statistically significant gender differences were observed: $\chi^2(2, N = 28) = 0.52, p = 0.77$, Cramer’s $V = 0.14$ (small effect). Percentages are reported in Table 3.

Table 3. Percentage breakdown of information configuration on social media.

Items	Male	Female
I have restricted who can see my information and who cannot.	81.3% ($n = 13$)	83.3% ($n = 10$)
I have all my data open to anyone who can see it.	18.8% ($n = 3$)	8.3% ($n = 1$)
I don’t know how exposed my data is on social media.	0.0%	8.3% ($n = 1$)

With respect to password practices, 60% ($n = 17$) reported using strong and secure passwords, 17.8% ($n = 5$) reported weak passwords, and 21.4% ($n = 6$) reported mixed levels of security. Gender differences were not significant: $\chi^2(2, N = 28) = 0.03, p = 0.98$, Cramer’s $V = 0.03$.

Regarding inviting unknown individuals, both male (94%) and female (100%) participants reported refraining from accepting such requests, with no significant difference: Fisher’s Exact Test $p = 0.46$.

Clearer differences were observed across academic year levels in the use of communication applications (Table 4), indicating that social media preferences evolve with educational stage. These findings align with the first two points of the nine-point framework, which stress awareness of online risks and adaptive security behaviors.

Table 4. One-way ANOVA with gender as the grouping factor.

One-Way ANOVA (Welch)				
Items	<i>F</i>	<i>gl1</i>	<i>gl2</i>	<i>p</i>
Item 1	1.621	1	25.6	0.214
Item 8	0.911	1	24.6	0.349
Item 12	2.391	1	26.0	0.134
Item 15	3.633	1	23.5	0.069
Item 16	3.105	1	26.0	0.090
Item 20	1.431	1	21.7	0.245

3.2. Results Regarding Actions Taken in Response to Risky Situations

When asked about witnessing cyberbullying, 58% of male participants and 83% of female participants reported having observed such cases. Although descriptive differences appear large, the difference was not statistically significant: $\chi^2(1, N = 28) = 2.21, p = 0.14$, Cramer's $V = 0.28$ (medium effect size). Thus, gender may play a role, but the evidence is not conclusive.

Responses to item 18 ("What is the main modus operandi of phishing?") indicated that 58.3% of female participants correctly identified phishing behaviors compared to 37.5% of males. Again, the difference was not statistically significant: $\chi^2(1, N = 28) = 1.10, p = 0.29$, Cramer's $V = 0.20$ (small-to-medium effect).

These results suggest a tendency toward stronger recognition of risky digital behaviors among females, but this pattern should be interpreted cautiously. The practical implication is the need for targeted training interventions, especially among male participants, even if statistical evidence remains limited.

3.3. Results Associated with Cybersecurity Knowledge

The average scores in the cybersecurity knowledge test are shown in Table 5. Across several items (e.g., items 1, 8, 12, 15, and 20), female participants obtained descriptively higher scores than males. For example, in item 15 (knowledge of threats involving black-mail with intimate images), females scored 6.67 on average compared to 3.13 for males (Cohen's $d = 1.02$, large effect).

Table 5. Mean scores by item and gender.

	1	2	3	5	7	8	12	15	16	17	19	20	21
Mean	6.61	7.50	8.96	6.96	7.75	5.50	7.44	4.64	7.70	5.35	2.14	5.73	5.82
Boys	5.81	8.75	8.94	6.64	7.44	4.81	6.70	3.13	6.91	5.16	1.88	5.07	5.69
Girls	7.67	5.83	9.00	7.38	8.17	6.42	8.42	6.67	8.75	5.61	2.50	6.60	6.00
Differences	−1.85	2.92	−0.06	−0.74	−0.73	−1.6	−1.72	−3.54	−1.84	−0.45	−0.63	−1.53	−0.31

It is necessary to consider and highlight the responses to question 15, which aims to determine the level of knowledge regarding situations that individuals may encounter in the digital environment, such as threats and/or blackmail associated with the publication of intimate photos or videos. The results show that, once again, female participants demonstrate a higher level of knowledge with an average difference of 3.5 points.

This clear difference is further evidenced in questions 1, 8, 12, 16, and 20, where the average scores on knowledge range between 1 and 2 points higher. These questions pertain to what constitutes a social network (question 1), the rationale behind selecting a particular type of password (question 8), the risks associated with excessive use of social networks (question 12), actions to take to prevent cyberbullying (question 16), and knowledge about methods of malware propagation (question 20).

Upon analyzing the variance of a factor (ANOVA) by comparing means to determine if there are statistically significant differences based on gender, p -values greater than 0.05 are observed. Therefore, the differences in means are not significant, indicating discrepancies between boys and girls (Table 5).

Correlation analyses showed significant associations between knowledge of digital threats (item 15) and awareness of risks from excessive social media use (item 12), $p < 0.05$, as well as between cyberbullying prevention (item 16) and malware propagation (item 20), $p < 0.05$ (Table 6). These findings highlight how different aspects of cybersecurity knowledge are interconnected.

Table 6. Correlations between questionnaire items.

Items	p -Values
Item 15 & Item 12	$p < 0.05$
Item 16 & Item 12	$p < 0.001$
Item 20 & Item 12	$p < 0.05$
Item 20 & Item 16	$p < 0.05$

In sum, while no gender differences reached statistical significance, effect size estimates suggest potentially meaningful trends, particularly regarding threat recognition and digital self-protection. The practical significance lies in tailoring educational interventions that reinforce weaker areas (e.g., phishing recognition) and promote knowledge integration across domains. These results directly support the nine-point framework by demonstrating both strengths and gaps in participant awareness.

4. Discussion

This study investigates the extent to which young university students with disabilities possess knowledge to protect themselves from potential digital threats. Thus, the results are positive, indicating a good level of knowledge among participants, aiming to contribute to understanding the status of specific actions' development regarding cybersecurity in young people with intellectual disabilities in Spain.

The first specific objective was to explore the cybersecurity knowledge expressed by participants with intellectual disabilities. The results show that, in general, the participants adopt protective behaviors against digital risks, such as keeping their profiles private and rejecting friend requests from strangers. The results indicate that they had good cybersecurity knowledge across both academic years. In contrast, various studies with neurotypical university populations found low levels of cybersecurity knowledge, coupled with risky activities endangering their computers. Examples include failure to install antivirus software, use of public Wi-Fi networks, or ignorance of the risks associated with downloading software [50].

However, practices such as inconsistent password use or a lack of clarity regarding data visibility should not be interpreted as individual deficits but rather as manifestations of structural opacity in the design of digital platforms. This perspective aligns with the findings of Binsedeeq et al. [51], who point out that there is a gap between theoretical

knowledge and the practical application of cybersecurity among people with disabilities, attributable to the lack of accessible technological safeguards.

Although it is often assumed that young people—regardless of whether they are neurotypical or have intellectual disabilities or other challenges—are more familiar with computing and cybersecurity due to growing up in digital environments, this assumption does not always translate into solid practical skills. For example, it has been observed that many digital natives (born after 1990) lack basic skills in using programs such as Excel or Word [52]. This gap between expected and actual knowledge highlights the urgent need to strengthen cybersecurity behaviors among youth. This is not only an educational issue but also essential preparation for future employment, as insufficient training can lead to vulnerabilities that compromise both their devices and personal data [53].

Regarding the objective of identifying, by gender, the knowledge of dangers expressed by participants, the results show that female university students with intellectual disabilities exhibit better knowledge compared to their male counterparts. Thus, females better identify phishing behaviors compared to males. For example, women more accurately identified phishing behaviors and demonstrated greater awareness of threats such as blackmail involving intimate images. Although the differences were not statistically significant, the effect sizes suggest relevant trends that should be considered in the design of educational interventions. Nevertheless, these findings cannot be generalized beyond the scope of this study, as they are based on a specific sample and context.

These findings are consistent with previous studies that highlight the greater exposure of women with intellectual disabilities to risky situations in digital environments, such as cyberbullying and technological abuse. Ruiz and Cortés [54] point out that women with intellectual disabilities are more vulnerable to experiencing harassment and digital violence, which leads to feelings of insecurity, discomfort, and, in many cases, a voluntary restriction in the use of technology. This limitation [55] not only affects their emotional well-being but also restricts their full participation in digital life, constituting a form of social exclusion. In this regard, it is essential that cybersecurity educational interventions be gender-sensitive, recognizing differentiated experiences and promoting safe and accessible digital environments for all individuals.

Although gender is a relevant factor, the increase in digital abuse toward people with intellectual disabilities highlights the urgent need to provide appropriate training. After receiving such training, it has been shown that individuals with intellectual disabilities are capable of recognizing and reporting digital risk situations [56].

Regarding the specific objective of analyzing participants' self-perception of social media risks, it seems that the lack of understanding of these risks complicates and increases the digital divide [57]. Based on the results obtained, it is observed that young people who tend to excessively use social media consider the "excess" itself as a high risk. These same results were found in a sample of 128 Spanish adolescents without pathologies, where online security behaviors and risk perception were measured, indicating that girls exhibited fewer secure behaviors compared to males, such as sending photographs. It is imperative to sensitize adolescents about the appropriate use of the internet [58].

Regarding the last objective of the research associated with identifying participants' knowledge and practices regarding profile privacy, the results of the study indicate that students with intellectual disabilities tend to keep their profiles restricted, especially female students, which reinforces certain aspects of personal cybersecurity. According to El-Asam et al. [59], students with special educational needs are considered to have higher online risks compared to their peers without difficulties. However, as mentioned by Domínguez-Vergara et al. [60], greater support for online security and parental support

regarding technology and the internet is needed, which would lead to increased burden on primary caregivers of people with intellectual disabilities.

The widespread use of AI-powered surveillance technologies by government agencies and commercial enterprises poses a significant and unprecedented threat to the fundamental human right to privacy. These technologies enable the covert collection, integration, and analysis of revealing personal information, rendering traditional notions of privacy obsolete. The lack of transparency, fairness, and accountability in AI systems often marginalizes vulnerable populations and establishes privatized systems of social control. Without intervention, such technologies risk creating a dystopian future where individuality, freedom of choice, and opposition are illusions under oppressive AI surveillance. In response, this research advocates for corrective frameworks that prioritize human rights, including privacy-by-design, algorithmic transparency, and human oversight [16].

Another study on basic security aspects, such as authentication to access everyday systems and services, does not consider the needs of individuals with any disability. Increasing adaptations to these needs, according to the disability presented, achieves a more inclusive digital society [61]. It is worth highlighting the conclusions of Johansson et al. [62], where discrepancies within the vulnerable population group (pathologies and impairments) were differentiated. They considered that the digital divide is greater in people with a disability; specifically, individuals with intellectual disabilities perceive greater exclusion from the digital society compared to the rest of the vulnerable population.

It is important to recognize that for individuals with intellectual disabilities, the digital world evolves rapidly, requiring ongoing adaptation to technological change. However, this evolution does not decrease the digital divide; on the contrary, it increases it in cases where a recognized disability exists (cognitive, visual, motor, or auditory). Thus, not only technological inclusion but also digital inclusion with security should be considered [61].

Based on all the aforementioned, it is necessary to generate cybersecurity that is adaptable and inclusive, responding to the diverse needs of individuals—whether related to disability, mental health, or socioeconomic status. Young people with intellectual disabilities must be considered not only as users of digital technologies but also as individuals with the right to access secure and accessible digital environments [63,64].

To achieve this, Renaud and Coles-Kemp [64] propose nine key aspects for ensuring accessibility in cybersecurity design:

- (1) Summary of basic concepts;
- (2) Design for social accessibility;
- (3) Provide authentication alternatives;
- (4) Design accessibility throughout the process;
- (5) Develop guidelines for cybersecurity user interface accessibility;
- (6) Development of heuristic guidelines to support interface review by experts;
- (7) Evaluate technologies at the intersections of a variety of insecurities, especially in disadvantaged individuals;
- (8) Establish dissemination spaces;
- (9) Provide counseling and support.

This study presents several limitations that should be considered when interpreting the findings. First, the sample was selected through convenience sampling, which may introduce biases and limit the generalizability of the results to broader populations of individuals with intellectual disabilities. Additionally, the sample size is small and not representative, further restricting the applicability of the findings.

The data were collected at specific points across different academic years, limiting the ability to identify evolving trends. Moreover, the creation of subgroups within the sample

was limited, which restricts the depth of comparative analysis between different profiles or conditions.

Although the instrument used was accessible and validated for this study, it is not standardized or specifically adapted to the target population. This underscores the need to develop new tools that are cognitively appropriate and tailored to the needs of individuals with intellectual disabilities. As a future improvement, it is recommended to include items that assess data surveillance literacy, given the increasing relevance of digital privacy and online risk awareness.

Furthermore, the study did not employ non-parametric statistical tests, which could have provided more robust insights given the characteristics of the sample and the nature of the data. This methodological choice carries its own limitations, particularly in terms of statistical assumptions and the interpretation of results.

The specific digital divide addressed in this study must be analyzed over time, considering the rapid evolution of digital technologies and the changing nature of online risks.

Finally, future studies should strengthen the practical relevance of cybersecurity education by incorporating concrete examples applicable to university settings—such as privacy review routines, guided phishing simulations, and the use of accessible password managers. It is also recommended to explore the concept of data surveillance literacy as a complementary line of inquiry. Moreover, future research could benefit from measuring students' perceptions of AI surveillance and their awareness of digital rights alongside cybersecurity knowledge. Evaluating rights-based training modules—such as privacy-by-design principles adapted with pictorial supports—may offer valuable insights into the effectiveness of inclusive digital education strategies.

5. Conclusions

To address the study objectives, the following conclusions can be drawn:

Regarding the assessment of participants' knowledge of cybersecurity, the scores obtained indicate a medium–high level of knowledge, with consistency across both academic years. Although no statistically significant gender differences were observed, effect size estimates suggest that female participants tend to score higher on several key items, particularly those related to threats such as blackmail involving intimate images. Responses related to the practical application of knowledge meet safety and protection criteria, indicating an adequate transfer of theoretical knowledge to digital behavior.

In terms of identifying participants' awareness of risks by gender, it is concluded that women demonstrated a greater ability to recognize digital risk behaviors such as phishing and cyberbullying, although these differences were not statistically significant. The practical implication is the need for specific training interventions, particularly aimed at male participants.

When analyzing participants' self-perception of social media risks, the results show that excessive use of these platforms is perceived as a high risk, indicating a certain level of awareness. Additionally, significant correlations were observed between knowledge of digital threats and other aspects of online safety, reinforcing the idea that different components of cybersecurity knowledge are interrelated.

Regarding the identification of knowledge and practices related to profile privacy among participants, the results indicate very similar responses between genders, although girls tend to keep their profiles more restricted, which can be interpreted as a digital self-protection strategy. Only two participants reported having open profiles, while one was unaware of their privacy settings.

Training and information on the advantages of ICT in various areas are essential to promote greater educational inclusion and independence, which positively impacts the daily lives of people with intellectual disabilities [65]. The implementation of digital training in the educational field contributes to the prevention of and reduction in the existing digital divide in terms of disability, increasing digital inclusion and making it a reality for the most vulnerable populations [66].

In this regard, a promising approach to addressing this issue is to provide more training and information that supports communicative development and autonomy in the virtual space for people with intellectual disabilities. Technologies such as CapacitaBOT make it possible to create real social situations that facilitate active learning of good digital interaction practices, increasing autonomy, knowledge, and participation in digital environments [67].

Although there are numerous studies on young people and social media [68,69], few focus specifically on young people with intellectual disabilities, likely due to the difficulty of accessing this population. Therefore, it is necessary to identify both the problems they perceive and those that go unnoticed in order to design effective prevention measures and study the coping strategies they use. Expanding the analytical framework can guide the development of future technologies, systems, and services that are not only digitally inclusive in their functionality but also safe [61].

Future Policies and Practical Implications

The results of this study, together with the broader context of digital vulnerability among students with intellectual disabilities, point to the need for universities to adopt inclusive policies that promote safe and rights-respecting digital environments. First, it is recommended to implement privacy-by-design defaults in institutional platforms, including data minimization, opt-in tracking, and accessible privacy dashboards. Universities should also require algorithmic transparency from technology providers, presented in plain and easy-to-read formats that explain what data are collected, how models are used, and how information is retained and shared.

In addition, institutions should establish human oversight mechanisms and appeal pathways for AI-enabled tools that students may encounter, such as online proctoring systems, plagiarism detection software, or early-alert platforms. To ensure informed consent, it is advisable to co-design explanatory materials using pictograms and layered formats. Finally, procurement processes should include checklists that assess accessibility and privacy impact, periodic audits of data practices, and student education on data rights, delivered with the same accessibility standards applied in this study's instruments.

Author Contributions: Introduction, M.D.L.-S. and J.M.-D.; Methodology and formal analysis, Á.V.-M.; Data curation, J.M.-D. and Á.V.-M.; Writing—original draft preparation, J.M.-D. and M.A.-C.; Writing—review and editing, J.M.-D., M.A.-C. and M.D.L.-S.; Supervision, J.M.-D. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki and approved by the Ethics Committee of the Camilo Jose Cela University (CEI-UCJC) 05_23_CDI on 21 December 2022) for studies involving humans.

Informed Consent Statement: Informed consent was obtained from all participants involved in the study.

Data Availability Statement: Data is available upon request.

Conflicts of Interest: The authors declare no conflicts of interest.

Disability Language/Terminology Positionality Statement: In this study, we use disability terminology that reflects the preferences expressed by our participant group and the conventions within health research and education in our regional and disciplinary context. Our research team has longstanding engagement with neurodiversity communities through collaborative projects, participatory research, and educational work. Across these activities, we have observed that participants and community partners frequently articulate a preference for person-first terminology, particularly when discussing systemic barriers, identity, and rights-based frameworks. At the same time: we recognize that preferences regarding identity-first versus person-first language vary across individuals and communities. We approached these differences with respect and sensitivity, ensuring that participants' autonomy, dignity, and perspectives guided our interactions and informed the way we describe disability in this manuscript. Our terminology choice reflects this contextual and methodological alignment rather than an attempt to generalize linguistic preferences beyond the scope of our study.

Abbreviations

The following abbreviations are used in this manuscript:

ICT	Information and Communication Technologies
OED	State Observatory of Disability
WHO	World Health Organization

References

1. American Psychiatric Association. *Diagnostic and Statistical Manual of Mental Disorders: DSM-5*, 5th ed.; American Psychiatric Publishing: Arlington, VA, USA, 2013. [CrossRef]
2. Bardají, J.P. Epidemiología de la Discapacidad Intelectual: Base Estatal de Datos de Personas con Valoración del Grado de Discapacidad 2017. Available online: <https://pascalpsi.es/Docs/BDEPD2017.pdf> (accessed on 5 May 2025).
3. Plena Inclusión. Así Nos Organizamos. Available online: <https://www.plenainclusion.org/conocenos/asi-nos-organizamos/> (accessed on 27 May 2025).
4. Cobeñas, P. Exclusión educativa de personas con discapacidad: Un problema pedagógico. *Rev. Iberoam. Calid. Efic. Cambio Educ.* **2020**, *18*, 65–81. [CrossRef]
5. Moreno, I.; Belmonte, M.L. Orientación laboral para estudiantes con discapacidad intelectual de la Universidad de Murcia. *Dialogos Pedagog.* **2022**, *20*, 51–70. [CrossRef] [PubMed]
6. Instituto Nacional de Estadística (INE). *Survey on Equipment and Use of Information and Communication Technologies in Households*; INE: Madrid, Spain, 2023. Available online: <https://www.ine.es> (accessed on 11 September 2025).
7. Observatorio Estatal de la Discapacidad (SOD). *Report on the Use of Digital Technologies by People with Disabilities*; OED: Albacete, Spain, 2023. Available online: <https://www.observatoriodeladiscapacidad.info> (accessed on 11 September 2025).
8. Fundación Adecco. *Technology and Disability: Report on the Digital Divide*; Fundación Adecco: Madrid, Spain, 2020. Available online: <https://fundacionadecco.org/informe-tecnologia-y-discapacidad/> (accessed on 11 September 2025).
9. Fernández-Batanero, J.M.; Román-Graván, P.; Montenegro-Rueda, M.; Fernández-Cerero, J. The impact of ICT on students with disabilities in higher education: A systematic review (2010–2020). *EDMETIC* **2021**, *10*, 81–105. [CrossRef]
10. State Observatory of Disability. *Personas con Discapacidad Administrativamente Reconocida en España*. Available online: <https://www.observatoriodeladiscapacidad.info/personas-con-discapacidad-administrativamente-reconocida-en-espana/> (accessed on 16 May 2025).
11. State Observatory of Disability. *Informe Sobre Evaluación Final del Plan de Acción 2014–2020 de la Estrategia Española Sobre la Discapacidad*. 2022. Available online: <https://www.observatoriodeladiscapacidad.info/wp-content/uploads/Microinforme-Evaluacion-final-del-Plan-de-Accion-2014-2020.pdf> (accessed on 18 May 2025).
12. Garcés, A.E.N.; Ruiz, J.N. La violencia digital en México (Ley Olimpia). *Rev. Crim. Nueva Epoca.* **2020**, *87*, 709–724.
13. Agencia Estatal Boletín Oficial del Estado. *Ley Orgánica 8/2021, de 4 de Junio, de Protección Integral a la Infancia y la Adolescencia Frente a la Violencia*. Boletín Oficial del Estado, n° 134, 5 de Junio de 2021. Available online: <https://www.boe.es/eli/es/lo/2021/06/04/8> (accessed on 16 May 2025).
14. Seale, J.; Nind, M.; Simmons, B. Transforming positive risk-taking practices: The possibilities of creativity and resilience in learning disability contexts. *Scand. J. Disabil. Res.* **2013**, *15*, 233–248. [CrossRef]
15. Caton, S.; Landman, R. Internet safety, online radicalisation and young people with learning disabilities. *Br. J. Learn. Disabil.* **2021**, *50*, 88–97. [CrossRef]

16. Chan, H.W.H.; Lo, N.P.K. A study on human rights impact with the advancement of artificial intelligence. *J. Posthumanism* **2025**, *5*, 1114–1153. [CrossRef]
17. Baldassarre, M.T.; Fernández Nieto, B.; Ragone, A. Human rights education as a component of the European Union cybersecurity curricula. *CEUR Workshop Proc.* **2023**, *3408*, 1–10. Available online: <https://ceur-ws.org/Vol-3408/short-s3-10.pdf> (accessed on 11 September 2025).
18. Chang, Y.W.; Sitbon, L.; Simpson, L. Towards a secured and safe online social media design framework for people with intellectual disability. In Proceedings of the ASSETS'21: Proceedings of the 23rd International ACM SIGACCESS Conference on Computers and Accessibility, Virtual, 18–22 October 2021; pp. 1–4. [CrossRef]
19. Statista. Social Media Statistics & Facts. Available online: <https://www.statista.com/topics/1164/social-networks/> (accessed on 16 May 2025).
20. Borgström, Å.; Daneback, K.; Molin, M. Young people with intellectual disabilities and social media: A literature review and thematic analysis. *Scand. J. Disabil. Res.* **2019**, *21*, 129–140. [CrossRef]
21. EU Kids Online. *Findings Methods Recommendations*; London School of Economics and Political Science: London, UK, 2025. Available online: <https://lsedesignunit.com/EUKidsOnline/html5/index.html?page=1&noflash> (accessed on 25 May 2025).
22. Caton, S.; Chapman, M. The use of social media and people with intellectual disability: A systematic review and thematic analysis. *J. Intellect. Dev. Disabil.* **2016**, *41*, 125–139. [CrossRef]
23. Chadwick, D.; Wesson, C.; Fullwood, C. Internet access by people with intellectual disabilities: Inequalities and opportunities. *Future Internet* **2013**, *5*, 376–397. [CrossRef]
24. Holmes, K.M.; O'Loughlin, N. The experiences of people with learning disabilities on social networking sites. *Br. J. Learn. Disabil.* **2014**, *42*, 1–5. [CrossRef]
25. Löfgren-Mårtenson, L. Love in cyberspace: Swedish young people with intellectual disabilities and the Internet. *Scand. J. Disabil. Res.* **2008**, *10*, 125–138. [CrossRef]
26. Molin, M.; Sorbring, E.; Löfgren-Mårtenson, L. Teachers' and parents' views on the Internet and social media usage by pupils with intellectual disabilities. *J. Intellect. Disabil.* **2015**, *19*, 22–33. [CrossRef]
27. Sorbring, E.; Molin, M.; Löfgren-Mårtenson, L. "I'm a mother, but I'm also a facilitator in her every-day life": Parents' voices about barriers and support for Internet participation among young people with intellectual disabilities. *Cyberpsychology* **2017**, *11*, 3. [CrossRef]
28. Scholz, F.; Yalcin, B.; Priestley, M. Internet access for disabled people: Understanding socio-relational factors in Europe. *Cyberpsychology* **2017**, *11*, 4. [CrossRef]
29. Seale, J. The role of supporters in facilitating the use of technologies by adolescents and adults with learning disabilities: A place for positive risk-taking? *Eur. J. Spec. Needs Educ.* **2014**, *29*, 220–236. [CrossRef]
30. Alaszewski, A.; Alaszewski, H. Towards the creative management of risk: Perceptions, practices and policies. *Br. J. Learn. Disabil.* **2002**, *30*, 56–62. [CrossRef]
31. Manthorpe, J.; Walsh, M.; Alaszewski, A.; Harrison, L. Issues of risk practice and welfare in learning disability services. *Disabil. Soc.* **1997**, *12*, 69–82. [CrossRef]
32. Morgan, S. Positive Risk-Taking: An Idea Whose Time Has Come. Available online: <http://static1.1.sqspcdn.com/static/f/586382/9538512/1290507680737/OpenMind-PositiveRiskTaking.pdf> (accessed on 21 May 2025).
33. Buijs, P.C.M.; Boot, E.; Shugar, A.; Fung, W.L.A.; Bassett, A.S. Internet safety issues for adolescents and adults with intellectual disabilities. *J. Appl. Res. Intellect. Disabil.* **2017**, *30*, 416–418. [CrossRef] [PubMed]
34. Lough, E.; Flynn, E.; Riby, D.M. Mapping real-world to online vulnerability in young people with developmental disorders: Illustrations from autism and Williams syndrome. *Rev. J. Autism Dev. Disord.* **2015**, *2*, 1–7. [CrossRef]
35. Erstad, O. *Digital Learning Lives: Trajectories, Literacies, and Schooling*, 3rd ed.; Peter Lang: New York, NY, USA, 2013; pp. 154–196.
36. Lorenz, B. Improving cybersecurity education in schools: An assessment of the "Digitally Safer School" proposal. In *Learning and Collaboration Technologies*; Smith, B.K., Borge, M., Eds.; Springer Nature: Cham, Switzerland, 2025; pp. 315–327.
37. Holzman, P.; Thompson, W. Digital literacy for students with intellectual disabilities. In *Advances in Educational Technologies and Instructional Design*; Jimenez, R., O'Neill, V.E., Eds.; IGI Global: Hershey, PA, USA, 2023; pp. 233–249.
38. Patrick, P.A.; Obermeyer, I.; Xenakis, J.; Crocitto, D.; O'Hara, D.M. Technology and social media use by adult patients with intellectual and/or developmental disabilities. *Disabil. Health J.* **2020**, *13*, 100840. [CrossRef]
39. Jimenez, R.; O'Neill, V.E. *Handbook of Research on Current Trends in Cybersecurity and Educational Technology*; IGI Global: Hershey, PA, USA, 2023. Available online: www.igi-global.com/book/handbook-research-current-trends-cybersecurity/299371 (accessed on 21 May 2025).
40. Jacob, U.S.; Pillay, J. A systematic literature review of social media usage among people with intellectual disability. *J. Cult. Values Educ.* **2023**, *6*, 42–61. [CrossRef]
41. Chadwick, D.D.; Fullwood, C. An online life like any other: Identity, self-determination, and social networking among adults with intellectual disabilities. *Cyberpsychology Behav. Soc. Netw.* **2018**, *21*, 56–64. [CrossRef]

42. Kävrestad, J.; Hagberg, A.; Roos, R.; Rambusch, J.; Nohlberg, M. Usable privacy and security from the perspective of cognitive abilities. In *Privacy and Identity Management. Between Data Protection and Security*; Friedewald, M., Krenn, S., Schiering, I., Schiffner, S., Eds.; Springer International Publishing: Cham, Switzerland, 2022; pp. 105–121.
43. Ministry of Social Rights and 2030 Agenda. Subdirector General for Planning, Organization and Evaluation. In *National Database of Persons with Officially Recognized Disability Degree: Report as of 31/12/2019*; Ministry of Social Rights and 2030 Agenda: Madrid, Spain, 2021.
44. Spanish National Cybersecurity Institute. Tests de Autoevaluación. Available online: <https://www.incibe.es/ciudadania/formacion/autoevaluacion> (accessed on 1 January 2025).
45. Almenara, J.; Gutiérrez Castillo, J.J.; Palacios-Rodríguez, A.; Guillen-Gamez, F. Digital competence of university students with disabilities and factors that determine it: A descriptive, inferential and multivariate study. *Educ. Inf. Technol.* **2022**, *28*, 9417–9436. [CrossRef]
46. Galicia Alarcón, L.A.; Balderrama Trápaga, J.A.; Edel Navarro, R. Validez de contenido por juicio de expertos: Propuesta de una herramienta virtual. *Apert* **2017**, *9*, 42–53. [CrossRef]
47. Garrote, P.R.; Rojas, M.C. La validación por juicio de expertos: Dos investigaciones cualitativas en lingüística aplicada. *Rev. Nebrija Lingüíst. Apl. Enseñanza Leng.* **2015**, *18*, 124–139. [CrossRef]
48. Cho, E.; Kim, S. Cronbach's coefficient alpha: Well-known but poorly understood. *Organ. Res. Methods* **2015**, *18*, 207–230. [CrossRef]
49. Alonso-Ruido, P.; Rodríguez-Castro, Y.; Lameiras-Fernández, M.; Carrera-Fernández, M.V. Hábitos de uso en las redes sociales de los y las adolescentes: Análisis de género. *Rev. Estud. Investig. Psicol. Educ.* **2015**, *13*, 54–57. [CrossRef]
50. Alharbi, H. Practical steps towards developing successful inclusive education supports in the Middle East. *Int. J. Whole Sch.* **2022**, *18*, 95–126.
51. Binsedeeq, A.; Furnell, S.; Helkala, K.; Woods, N.; Chadwick, D.; Fullwood, C.; Carpent, X.; Gervassis, N. *Assessing the Cybersecurity Needs and Experiences of Disabled Users*; University of Nottingham: Nottingham, UK, 2024. Available online: https://www.open-access.bcu.ac.uk/16012/1/Binsedeeq_et_al._2024.pdf (accessed on 16 September 2025).
52. Peiro, M.; Moraleda, A.; Galán-Casado, D. Nuestros Alumnos son Nativos Digitales, pero no Saben Utilizar Excel o Word—Magisnet. Available online: <https://www.magisnet.com/2024/02/alvaro-moraleda-nuestros-alumnos-son-nativos-digitales-pero-no-saben-utilizar-excel-o-word/> (accessed on 28 May 2025).
53. Caldentey, J.M.; Urquijo, B.S.; Almazor, M.G. Competency-based cybersecurity training and awareness: A systematic literature review. *Pixel-Bit Rev. Medios Educ.* **2022**, *63*, 197–225. [CrossRef]
54. Ruiz, C.B.; Cortés Borrero, R. Los ciberdelitos y la ciberseguridad: Una cuestión de género. *Inform. Derecho Rev. Iberoam. Derecho Inform.* **2023**, *9*, 73–84. [CrossRef]
55. Woodlock, D.; Harris, B. “You have to be really careful”: Technology and the abuse of women with intellectual and cognitive disabilities. *Disabil. Soc.* **2024**, *39*, 953–973. [CrossRef]
56. Venkatasubramanian, K.; Skorinko, J.L.M.; Kobeissi, M.; Lewis, B.; Nocera, N. Exploring a reporting tool to empower individuals with intellectual and developmental disabilities to self-report abuse. In Proceedings of the CHI Conference on Human Factors in Computing Systems, Yokohama, Japan, 8–13 May 2021.
57. Anderson, S.; Araten-Bergman, T.; Steel, G. Adults with intellectual disabilities as users of social media: A scoping review. *Br. J. Learn. Disabil.* **2023**, *51*, 544–564. [CrossRef]
58. Marcos Martínez, V.; González Amado, B.; Gancedo, Y. Conductas en la red y diferencias de género en población adolescente. In Proceedings of the Actas del XII Congreso (Inter)Nacional de Psicología Jurídica y Forense, Madrid, Spain, 13–15 February 2020.
59. El-Asam, A.; Colley-Chahal, L.J.; Katz, A. Social isolation and online relationship-risk encounters among adolescents with special educational needs. *Youth* **2023**, *3*, 671–688. [CrossRef]
60. Domínguez-Vergara, J.; Santa-Cruz-Espinoza, H.; Chávez-Ventura, G. Zarit caregiver burden interview: Psychometric properties in family caregivers of people with intellectual disabilities. *Eur. J. Investig. Health Psychol. Educ.* **2023**, *13*, 391–402. [CrossRef]
61. Furnell, S.; Helkala, K.; Woods, N. Accessible authentication: Assessing the applicability for users with disabilities. *Comput. Secur.* **2022**, *113*, 102561. [CrossRef]
62. Johansson, S.; Gulliksen, J.; Gustavsson, C. Disability digital divide: The use of the Internet, smartphones, computers and tablets among people with disabilities in Sweden. *Univers. Access Inf. Soc.* **2021**, *20*, 105–120. [CrossRef]
63. Murphy, E.; Shiels, O.; Fiori, S.; McCausland, D.; Bergström, H.; Koster, R.; Noorlandt, H.; Korfage, I.; Wallén, E.F. Bridging the digital divide for individuals with intellectual disabilities: Implications for well-being and inclusion. *Br. J. Learn. Disabil.* **2024**, *53*, 17–31. [CrossRef]
64. Renaud, K.; Coles-Kemp, L. Accessible and inclusive cyber security: A nuanced and complex challenge. *SN Comput. Sci.* **2022**, *3*, 346. [CrossRef]
65. Krasniqi, V.; Zdravkova, K.; Dalipi, F. Impact of assistive technologies to inclusive education and independent life of Down syndrome persons: A systematic literature review and research agenda. *Sustainability* **2022**, *14*, 4630. [CrossRef]

66. Afzal, A.; Khan, S.; Daud, S.; Ahmad, Z.; Butt, A. Addressing the digital divide: Access and use of technology in education. *J. Soc. Sci. Rev.* **2023**, *3*, 883–895. [[CrossRef](#)]
67. Mateos-Sanchez, M.; Melo, A.C.; Blanco, L.S.; García, A.M.F. Chatbot as educational and inclusive tool for people with intellectual disabilities. *Sustainability* **2022**, *14*, 1520. [[CrossRef](#)]
68. Oliva Marañón, C. Redes sociales y jóvenes: Una intimidad cuestionada en Internet. *Aposta Rev. Cienc. Soc.* **2012**, *3*, 1–16.
69. Ebrahim, A.; Lorenzo, T.; Kathard, H. Traversing disability: Building social capital through skill development for employment. *Disabilities* **2022**, *2*, 439–450. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.