Hacettepe Üniversitesi Eğitim Fakültesi Dergisi

Hacettepe University Journal of Education

e-ISSN: 2536-4758

Enhancing Digital Security Awareness Among University Students with Disabilities: A Training-Based Intervention

Hatice OĞUZ ÖZGÜR*

Article Information

Received: 16.09.2025

Accepted: 02.03.2026

Online First: 30.07.2026

Published: 31.07.2026

ABSTRACT

This study, designed as a quasi-experimental single-group pretest-posttest model, examines changes in knowledge levels associated with an educational intervention designed to enhance the knowledge levels of university students with physical and sensory disabilities regarding the safe use of digital information and communication tools. Within the scope of the research, 15 students with disabilities were included in workshops on topics such as online dangers, digital literacy, digital addiction, cybercrime and methods of combating them. In the quantitative data collection process of this application, the data were obtained by pre-test, post-test and retention test forms. According to the data obtained, the average of the pre-test applied to determine the level of knowledge of the participants about the safe use of digital information and communication technologies is 3.14; the average of the posttest is 4.40; the average of the permanence test is 4.02. To examine whether digital security knowledge changed significantly over time, a Friedman test was conducted comparing pretest, posttest, and retention test scores for the entire sample (N=15). The results indicated a statistically significant effect of time on participants' knowledge levels ($\chi^2(2)=24.60$, $p<0.001$). Post hoc Wilcoxon signed-rank tests with Bonferroni correction showed that posttest and retention test scores were significantly higher than pretest scores ($p<0.01$), while the difference between posttest and retention test scores was not statistically significant ($p>0.05$), indicating that the knowledge gains were largely retained over time. The findings reveal that the training was associated with a statistically significant increase in knowledge levels of knowledge of the participants about digital security and that this improvement was sustained to a certain extent level. As a result, the study draws attention to the risks faced by people with disabilities in digital environments and emphasizes the importance of educational support for them to cope with these risks.

Keywords: Digital technologies, Digital security, Digital inclusion, Students with disabilities

doi: 10.16986/hunefd.1785156 Article Type: Research Article

Citation Information: Oğuz Özgür, H. (2026). Enhancing Digital Security Awareness Among University Students with Disabilities: A Training-Based Intervention. *Hacettepe University Journal of Education, 41*(3), 656-668. https://doi.org/10.16986/hunefd.1785156

1. INTRODUCTION

The widespread use of digital information and communication technologies (DICT) -including internet-based platforms, social media applications, mobile communication tools, and online information systems- in diverse areas of daily life-ranging from communication and education to socialization and work activities-has brought the issue of digital security to the forefront. The literature on digital risks indicates that users' unconscious or problematic use of digital technologies leads to various threats in online environments, including persistent surveillance, unauthorized sharing of personal information, targeting, othering, dissemination of reputation-damaging content, fraud, and digital harassment (Arslankara & Usta, 2020; Oğuz Özgür & Özkul, 2022; Karakuş, 2024; Doğan & Gündüz, 2025). Such digital risks often stem from malicious uses and largely occur beyond the victim's control. Consequently, acquiring knowledge about the safe use of digital information and communication technologies, as well as the potential risks encountered in digital spaces, has become an imperative at both the individual and societal levels in today's increasingly digitalized societies.

Digital technologies, particularly internet-based communication platforms such as social networking sites, instant messaging applications, and online community spaces, provide not only risks but also significant opportunities in terms of social participation and identity construction. Individuals can reconstruct their identities, enrich their social capital, and sustain their social relations through digital networks without being confined to physical space (Castells, 1996; 2009). This transformation increasingly amplifies the role of digitally mediated communication environments in individuals' social lives. According to Sherry Turkle (2011), digital environments intensify the state of "being alone together," while simultaneously providing opportunities for individuals to connect with others who share similar experiences. As a result, digital spaces serve

*Lecturer PhD., Isparta University of Applied Sciences, Uluborlu Selahattin Karasoy Vocationan School, Theraphy and Rehabilitation, Isparta, Türkiye, haticeoguz@isparta.edu.tr, 0000-0001-5901-3488.

as important platforms for socialization, particularly for individuals whose access to traditional forms of social interaction is limited by physical or social barriers.

For individuals with disabilities, such digital opportunities -primarily accessed through online communication platforms and assistive digital technologies- contribute to enhancing social participation and preventing exclusion (Söderström & Hemmingsson, 2017; Yeon & Choi, 2019; Nagornaya & Nagornyi, 2023). However, alongside the opportunities afforded by the digital sphere, the lack of digital literacy and insufficient security measures also generate significant risks (Talan & Aktürk, 2021; Özsarı & Deli, 2023). Therefore, acquiring knowledge about the safe use of digital information and communication technologies is essential for benefiting securely from the opportunities provided by digital communication tools.

Research indicates that individuals with disabilities are more frequently exposed to negative attitudes in offline environments, such as harassment, othering, and exclusion (Emerson & Roulstone, 2014; Oğuz Özgür, 2023). These experiences are associated with factors such as health-related stigmatization (Blake et al., 2012), being categorized as vulnerable (Quarmby, 2015), and persistent social stigma (Sentenac et al., 2011). With the widespread adoption of digital communication tools, such discriminatory attitudes have increasingly been transferred into online environments and reproduced in new forms. As a result, individuals with disabilities face risks of exclusion, discrimination, and abuse not only in physical but also in digital spaces (Gültekin & Ünal, 2021). Moreover, the anonymity afforded by online environments enables perpetrators to conceal their identities, thereby intensifying the prevalence of digital violence (Wells & Mitchell, 2014).

Beyond these structural risks, the intensity and nature of digital technology further shape individuals' exposure to online threats. Individuals with disabilities rely heavily on digital technologies to meet everyday needs ranging from education and health services to communication and entertainment (Chadwick et al., 2013; Caton et al., 2024). Studies show that they spend considerable time in online environments, particularly on social media platforms that prioritize interaction and visibility (Arslan & Bulut Özek, 2020; Sir & Yıldız, 2023). However, frequent engagement in such environments, when not accompanied by adequate digital security awareness, may increase vulnerability to risks such as digital harassment, exclusion, and exploitation (Şentürk & Keskin, 2018; Gültekin & Ünal, 2021). This vulnerability is further amplified among individuals with intellectual disabilities, for whom limited digital awareness and protective skills constitute a critical risk factor (Tan & Şenkal, 2024).

When individuals with disabilities are subjected to digital violence, they often share their experiences only with close acquaintances and refrain from reporting incidents to official authorities (Kowalski & Toth, 2018). This tendency toward informal disclosure and non-reporting reflects both a lack of knowledge regarding digital security and the inadequacy of effective coping mechanisms. Moreover, exposure to such risky situations is associated with adverse outcomes, including anxiety, depression, diminished self-esteem, and social isolation. In severe cases, these impacts may escalate to suicidal ideation (Didden et al., 2009; Kowalski et al., 2016; Martínez Cao et al, 2021).

In this context, rather than the mere ability to be online, it is the way digital tools are used that becomes decisive in determining the level of digital risk. Skills such as privacy awareness, access to reliable sources, and digital behavior consciousness are of critical importance for ensuring a safe digital experience (Kowalski et al., 2016; Martínez Cao et al., 2021). The literature demonstrates that structured digital literacy and digital security programs enhance such awareness among individuals with disabilities, thereby providing a protective effect against digital violence (Jenaro et al., 2018; Martínez Cao et al., 2021; Marnewick et al., 2022).

However, while international studies have increasingly addressed issues of digital exclusion and cyber victimization among individuals with disabilities (Jenaro et al., 2018; Chadwick et al., 2022; Black & de Pablos Ortega, 2025), there remains a notable scarcity of intervention-based empirical research focused on enhancing digital security awareness through structured educational programs tailored specifically to this population. The extant literature underscores a critical gap concerning the long-term effectiveness and sustainability of such interventions across diverse disability types and contexts. Based on this gap, the present study seeks to examine the effects of a structured digital security training program designed for university students with physical and sensory disabilities. By employing a pretest–posttest–retention design, the study not only examines immediate knowledge gains but also evaluates the durability of digital security awareness over time, an aspect that has received limited attention in prior research.

The main objective of the study is to determine whether such a program significantly improves participants' knowledge and awareness regarding the safe use of digital information and communication technologies, and whether these gains are retained over time. To this end, the study seeks to answer the following research questions: (1) Does digital security training lead to a statistically significant increase in participants' knowledge levels regarding digital safety? (2) To what extent are the knowledge gains sustained over time? (3) Do the effects of the training vary according to participants' type of disability or prior experience with digital security problems?

2. METHODOLOGY

This study, which aims to increase the knowledge levels of individuals with disabilities regarding digital security through adapted training, was conducted as quasi-experimental research using a single-group pretest–posttest design. Quasi-experimental designs are structured research models in which full experimental control cannot be established, yet changes associated with an intervention can be systematically examined (Büyüköztürk et al., 2016; Sönmez & Alacapınar, 2016). In this study, only one experimental group was included, and measurements were carried out before the intervention, immediately after the intervention, and at a follow-up stage.

In determining the research design, it was considered that the participant group consisted of individuals with disabilities, and that implementing an intervention on a control group would not be ethically appropriate. Therefore, instead of a controlled experimental design with random assignments, a single-group structure composed of volunteers who agreed to participate in the intervention was chosen. This decision was deemed more appropriate in terms of both ethical considerations and practical feasibility.

2.1. Participants

In calculating the sample size, the G*Power software was used, selecting the F test for repeated measures ANOVA (within-subjects design). According to the power analysis, assuming a significance level of 0.05, a statistical power of 0.80, and a large effect size (f=0.4), a minimum of 14 participants was deemed sufficient (Cohen, 1988). Taking potential attrition into account, 15 participants were included in the study. While this sample size is sufficient to statistically detect large effects, its limited scope may restrict the detection of small- and medium-sized effects; therefore, this limitation was acknowledged as part of the study's constraints. Although the sample size estimation was conducted based on a parametric repeated measures ANOVA model, the final analyses were performed using non-parametric methods due to the small sample size and the conservative analytical approach adopted in this study. While power analysis procedures for non-parametric repeated-measures tests are less straightforward and less commonly implemented in standard software, the ANOVA-based estimation was used as an approximate reference framework to determine the minimum required sample size for detecting large within-group effects. Given that non-parametric tests such as the Friedman test are generally slightly less powerful than their parametric counterparts under normality assumptions, the obtained sample size should be interpreted as providing a conservative estimate of statistical power. Therefore, the power analysis results are considered indicative of the study's capacity to detect large effects rather than definitive evidence of optimal power under non-parametric conditions.

The participant group consisted of 15 university students in Türkiye with physical and sensory disabilities, selected through purposive sampling using the criterion sampling technique. This approach was chosen to ensure that participants met a set of predetermined inclusion criteria aligned with the research objectives. The primary selection criteria were: (1) being a registered university student in Türkiye, (2) having a physical disability, (3) having regular access to digital communication tools (e.g., smartphone, tablet, computer), (4) having prior experience with digital environments (regardless of security awareness level), and (5) voluntary consent to participate in the entire training process.

Although the literature on digital risks and digital safety awareness broadly addresses individuals with disabilities across different age groups and social contexts, the present study specifically focused on university students with physical and sensory disabilities for several methodological and practical reasons. First, university students represent a subgroup with intensive and routine exposure to digital environments due to academic requirements such as online learning platforms, digital communication with instructors and peers, and frequent use of social media and institutional digital systems (Park, 2022a). This high level of engagement increases both their exposure to digital risks and the relevance of digital safety awareness as an intervention target. Second, university students with disabilities often navigate digital environments with a higher degree of autonomy compared to younger individuals, while still facing accessibility barriers and digital vulnerabilities associated with disability. This positioning makes them a particularly appropriate group for examining the effects of a structured digital safety awareness training. Finally, focusing on university students allowed for the implementation of an intensive, adapted training program and repeated measurements under ethically and logistically feasible conditions. From an ethical standpoint, university students represent an adult population capable of providing informed consent independently, thereby minimizing concerns related to guardianship or parental authorization. Logistically, the university context ensured consistent access to digital tools, institutional support services, and sustained participant availability, which were necessary for implementing an intensive multi-day training and follow-up assessment. Therefore, while the findings are not intended to be generalized to all individuals with disabilities, the selected sample provides a theoretically justified and methodologically appropriate context for examining the effectiveness of the intervention.

The training required close monitoring, individual accommodation, and accessibility support, which imposed practical constraints on the sample size. Therefore, 15 participants were recruited who fully met the established criteria and agreed to participate throughout the pretest, training, posttest, and retention test phases. Detailed demographic information about the participants is provided in Table 1.

Table 1.
Demographic Characteristics of the Participants

Participant	Gender	Age	Level of Education	Type of Disability
P1	Male	20	Undergraduate	Mobility impairment
P2	Female	18	Associate degree	Visual impairment
P3	Female	25	Undergraduate	Cerebral palsy
P4	Male	20	Undergraduate	Developmental limb impairment
P5	Female	22	Undergraduate	Cerebral palsy
P6	Male	29	Associate degree	Developmental limb impairment
P7	Male	20	Undergraduate	Mobility impairment
P8	Female	35	Undergraduate	Limb loss
P9	Male	18	Undergraduate	Developmental motor disorder
P10	Male	32	Associate degree	Visual impairment
P11	Male	21	Associate degree	Hearing impairment
P12	Female	18	Associate degree	Developmental limb impairment
P13	Female	20	Associate degree	Cerebral palsy
P14	Female	19	Associate degree	Cerebral palsy
P15	Female	18	Associate degree	Visual impairment

Accordingly, eight participants were female and seven were male, with a mean age of 21.33±5.15 years. Most of the participants were enrolled in associate degree programs (n=8), and the most common disability types were cerebral palsy (n=4) and developmental limb impairment (n=3). This diversity allowed the study to capture differentiated impacts of the intervention across various disability subgroups.

2.2. Data Collection Process

Data were collected using a demographic information form and the Digital Security Awareness Assessment Form (DSAAF) developed specifically for this intervention-based study. The demographic information form served to learn the basic information of the participants such as age, gender, education, as well as the practices of using digital communication tools. DSAAF was designed to assess participants' self-reported levels of knowledge and awareness about digital security before and after the training program; It does not function as a standard psychometric scale. The item pool was generated based on a review of international digital competence frameworks, particularly DigComp (Carretero et al., 2017; Vuorikari et al., 2022), and empirical studies on digital literacy, online safety, and disability-focused digital inclusion (Söderström & Hemmingsson, 2017; Jenaro et al., 2018; Martínez Cao et al., 2021; Marnewick et al., 2022).

The instrument consists of Likert-type items designed to capture participants' perceived level of knowledge and awareness within each thematic domain. Sample items include statements such as "I know how to adjust privacy settings on social media platforms" and "I can recognize suspicious or fraudulent digital content."

Content validity was ensured through expert review. The initial item pool was evaluated by scholars with expertise in digital literacy, disability studies, and educational sociology. Based on their feedback, items were revised for clarity, relevance, and accessibility. Content Validity Ratio (CVR) values ranged from 0.71 to 1.00, exceeding the minimum acceptable thresholds according to Lawshe's (1975) criteria. The overall Content Validity Index (CVI) was calculated as 0.92, indicating a high level of content validity.

To examine construct validity and conduct item analyses, the preliminary version of the DSAAF was pilot tested with a sample of 76 university students with physical and sensory disabilities who did not participate in the main study. An exploratory factor analysis (EFA) was performed to explore the underlying structure of the test. The analysis revealed a unidimensional structure, accounting for 52.6% of the total variance. Given that the instrument aimed to measure general digital security knowledge for within-group intervention assessment rather than multidimensional diagnostic profiling, a single-factor structure was considered theoretically coherent and methodologically sufficient. Confirmatory factor analysis was not conducted, as the primary purpose of the instrument was not full-scale validation but the assessment of within-group changes in knowledge over time in a small-sample quasi-experimental design.

Item-total correlations ranged from 0.42 to 0.68, indicating satisfactory item discrimination. Item difficulty indices (interpreted as mean item endorsement levels in Likert-type format) ranged between 0.40 and 0.85, reflecting an adequate distribution of item variability. Internal consistency was high (Cronbach's $\alpha = 0.89$), supporting the reliability of the scale for within-group change assessment.

The training program was implemented over six consecutive days. On the first day, participants were informed about the study procedures and the pretest was administered.

The educational intervention consisted of interactive lessons, hands-on workshops, and digital gamification-based activities. The program covers the role of digital communication tools in daily life; responsible and safe use of digital technologies; problem solving in digital environments; information and data literacy; risks associated with online gaming and shopping; cybercrime and digital threats; digital addiction; virtual reality and the metaverse; and strategies for dealing with and reporting digital violence. The selection of these topics was shaped by the existing literature on digital risks and the evidence showing that individuals with disabilities primarily encounter digital threats in their everyday digital practices.

During the implementation phase, particular attention was paid to individual differences among participants, including disability type, prior digital experience, and learning needs. Instructional materials and activities were adapted to enhance accessibility and comprehension, for example by using clear and simplified language, visually supported content, step-by-step demonstrations, flexible pacing, and repeated practice opportunities. These adaptations were intended to ensure that the training program was inclusive, accessible, and responsive to the heterogeneous needs of individuals with physical disabilities, thereby strengthening the program's educational effectiveness and practical relevance. All 15 participants completed the training program in its entirety.

Following the completion of the six-day intervention, the posttest was administered using the same form. To evaluate the sustainability of the observed knowledge gains, a retention test was conducted approximately three months after the posttest. All participants voluntarily completed the retention test.

2.3. Data Analysis

Prior to statistical analysis, the distributional characteristics of the total scores obtained from the Digital Security Awareness Assessment Form were examined. Given the small sample size (N=15) and the structure of repeated measurements, parametric test assumptions were not considered sufficient to support inferential analysis. Although skewness and kurtosis values fell within acceptable ranges and the Shapiro–Wilk test did not indicate significant deviations from normality ($p>0.05$), sample size limitations posed a constraint on the use of parametric procedures.

Therefore, in line with methodological recommendations for small samples and repeated measures designs, non-parametric statistical methods were employed. Specifically, the Friedman test was used to examine whether there were statistically significant differences among participants' pretest, posttest, and retention test scores. This test is appropriate for analyzing related samples when parametric assumptions cannot be confidently met. When the Friedman test indicated a significant overall difference, post hoc pairwise comparisons were conducted using Wilcoxon signed-rank tests with Bonferroni correction to identify the specific measurement points between which differences occurred. This analytical approach enabled a robust examination of within-group changes in digital security knowledge over time while minimizing threats to statistical validity arising from limited sample size.

Each item of the form used to measure the digital security knowledge levels of the participants was evaluated on a 5-point Likert scale, and the answer choices ranged from 1 (strongly disagree) to 5 (strongly agree). Total scores ranged from 50 to 250, with higher scores indicating higher levels of digital security knowledge. For interpretive clarity and comparability across measurement points, raw total scores were transformed into mean item scores by dividing the total score by the number of items (50), resulting in values ranging from 1 to 5. This transformation preserved the original response metric while facilitating direct comparison across pretest, posttest, and retention measurements. All statistical analyses were performed using SPSS-27 software.

3. FINDINGS

Regarding the use of digital communication tools, 14 participants reported that the device they most frequently used in daily life was a smartphone, while only one participant indicated that they used a computer more often. In addition, 6 participants reported frequent use of tablets and smartwatches. These devices were primarily used for communication and interaction purposes (n=13), followed by information seeking and research, and, in third place, for entertainment (e.g., gaming, social media). Furthermore, 3 participants stated that they used these tools for work or production purposes, while five reported using them for educational purposes.

In terms of daily usage, 5 participants indicated that they engaged with digital communication tools for approximately nine hours or more, 8 participants reported usage ranging between five and eight hours, while 2 participants reported a daily usage of approximately two to four hours.

8 participants reported prior experiences with digital security problems, 1 participant indicated no such experience, 2 participants noted witnessing problems encountered by others, and 4 stated that they were unaware of such issues. The reported digital security incidents encompassed, among others, the hacking of social media and online gaming accounts, unauthorized disclosure of personal information, duplication of payment credentials, and the installation of malware or viruses on computers and smartphones.

The mean score of the pretest administered to assess participants' knowledge levels regarding the safe use of digital information and communication technologies was 3.14 (SD=0.37) out of 5 (based on mean item scores on a 5-point scale); the mean score of the posttest was 4.40 (SD=0.32); and the mean score of the retention test was 4.02 (SD=0.37). The score changes for each participant are presented in Figure 1.

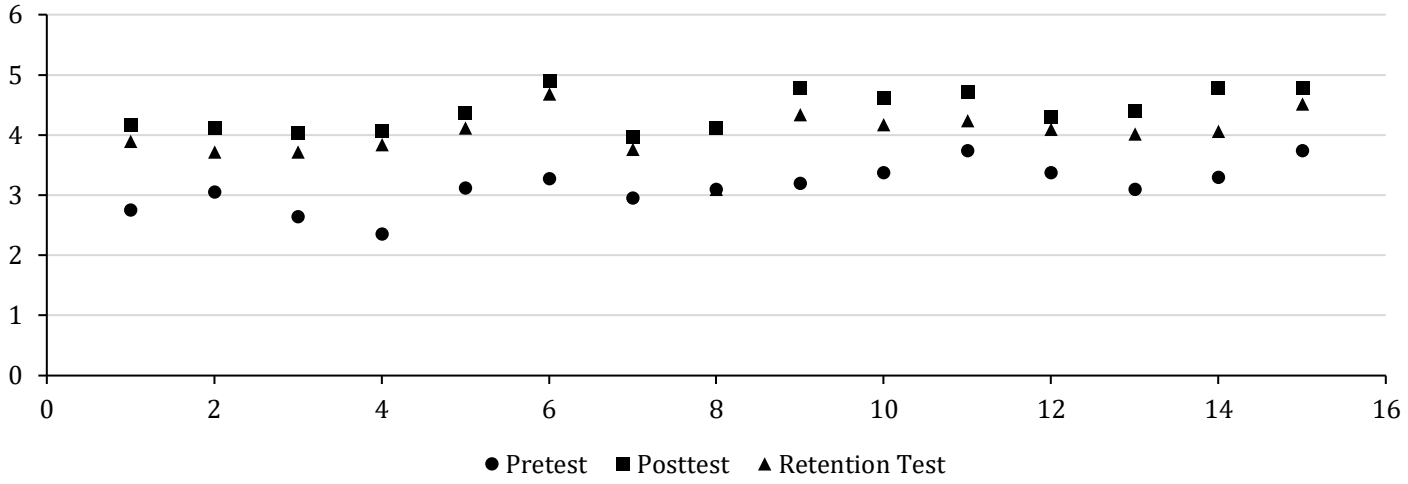

Figure 1. Mean Pretest, Posttest, and Retention Test Scores of Participants

To examine whether there was a statistically significant change in digital security knowledge over time, a Friedman test was conducted comparing pretest, posttest, and retention test scores for the entire sample (N=15). The results indicated a statistically significant difference across measurement points ($\chi^2(2)=24.60$, $p<0.001$). Post hoc pairwise comparisons were subsequently performed using Wilcoxon signed-rank tests with Bonferroni correction. These analyses revealed that posttest scores were significantly higher than pretest scores ($p<0.01$), and retention test scores were also significantly higher than pretest scores ($p<0.01$). Although mean scores slightly decreased from posttest to retention test, this difference was not statistically significant ($p>0.05$), suggesting that the observed score improvements were largely maintained at the follow-up measurement.

Descriptively, when comparing individual pretest and retention test scores, 14 participants demonstrated an increase in their scores, while one participant showed nearly identical scores across the two measurements. This observation is reported descriptively, and no inferential analysis was conducted to examine potential associations with individual or socio-demographic characteristics.

Given the very small and uneven group sizes across disability categories, inferential statistical comparisons between disability groups were not conducted. Instead, test scores by disability type are presented descriptively to illustrate observed patterns of knowledge change following the intervention (Table 2). While increases in mean scores were observed across most disability categories from pretest to posttest, followed by relatively stable retention scores, these patterns should be interpreted cautiously and not as evidence of systematic differences between disability types. For example, participants with mobility impairments showed an increase in mean scores from pretest (M=2.86) to posttest (M=4.07), with a slight decline at retention (M=3.83). Participants with visual impairments demonstrated a rise from a pretest mean of 3.39 to a posttest mean of 4.50, with a retention mean of 4.14. Similar improvement patterns were observed among participants with cerebral palsy and developmental limb impairments.

Table 2.
Descriptive Statistics of Pretest, Posttest, and Retention Test Scores by Type of Disability

Type of Disability	Test Type	Mean	Std. Deviation
Mobility impairment (n=2)	Pretest	2.860	.265
	Posttest	4.070	.239
	Retention Test	3.830	.223
Visual impairment (n=3)	Pretest	3.393	.216
	Posttest	4.507	.195
	Retention Test	4.140	.182
Cerebral palsy (n=4)	Pretest	3.040	.187
	Posttest	4.395	.169
	Retention Test	3.980	.158
Developmental limb impairment (n=3)	Pretest	3.007	.216
	Posttest	4.420	.195
	Retention Test	4.207	.182
Limb loss (n=1)	Pretest	3.100	-
	Posttest	4.120	-
	Retention Test	3.100	-
Developmental motor disorder (n=1)	Pretest	3.200	-
	Posttest	4.780	-
	Retention Test	4.340	-
Hearing impairment (n=1)	Pretest	3.740	-
	Posttest	4.720	-
	Retention Test	4.240	-

Descriptive comparisons were also conducted based on participants' self-reported prior experiences with digital security problems (Table 3). Participants who reported having previously experienced digital security issues exhibited notable increases in mean scores from pretest to posttest, with relatively high retention scores. Participants who reported no prior experience or awareness of digital security problems also demonstrated improvements, though their mean gains appeared more modest. Participants who reported witnessing digital security problems encountered by others showed a similar pattern of improvement. Due to the small and uneven group sizes, no inferential statistical testing was performed for these comparisons, and the findings are presented solely as descriptive tendencies.

Table 3.
Descriptive Distribution of Pretest, Posttest, and Retention Test Scores by Participants' Prior Experience with Digital Security Issues

Experience with Digital Security Problems	Test Type	Mean	Std. Deviation
Yes, I have experienced (n=8)	Pretest	2.955	.114
	Posttest	4.333	.118
	Retention Test	4.018	.139
No, I have not experienced (n=1)	Pretest	3.740	-
	Posttest	4.780	-
	Retention Test	4.520	-
I have witnessed others experiencing (n=2)	Pretest	3.200	.227
	Posttest	4.590	.237
	Retention Test	4.040	.278
I am not aware (n=4)	Pretest	3.335	.161
	Posttest	4.375	.167
	Retention Test	3.890	.197

Overall, the results of the Friedman test and subsequent post hoc analyses indicate that digital security awareness scores increased significantly following the training in participants' knowledge levels. Both immediate learning gains and longer-term retention were observed. While descriptive analyses suggest that knowledge gains may vary across disability types and prior digital security experiences, these observations remain exploratory and require further investigation with larger and more balanced samples.

4. RESULTS, DISCUSSION AND RECOMMENDATIONS

The findings of this research demonstrate that digital security awareness training produced a statistically significant increase in the knowledge levels of university students with physical disabilities, and that this improvement was largely sustained over time. The substantial rise observed between the pretest and posttest, together with the considerable retention of these gains at the follow-up assessment, suggests the potential value of structured, participant-centered digital security training (Figure 1).

Beyond demonstrating score differences over time, this study contributes conceptually by positioning digital security awareness as a dimension of digital inclusion rather than merely a technical competence. Much of the existing literature treats digital literacy and cybersecurity training as skill-based interventions (Turkle, 2011; Jain, 2017; Avcı & Arslan, 2019; Veerabathiran, 2025). The present findings support a broader framing in which digital security knowledge functions as a form of protective digital capital that mediates participation, autonomy, and vulnerability in digitally mediated environments. In this respect, the study extends discussions on digital inclusion by empirically linking accessibility-oriented instructional design with protective knowledge formation among university students with disabilities.

Furthermore, by documenting retention over a three-month period, the study adds to intervention literature that often focuses solely on short-term outcomes. The findings suggest that digital safety awareness may be shaped not only by access to technology but also by structured pedagogical engagement, reinforcing the argument that digital participation requires both infrastructural and epistemic resources. The results have consistently shown that digital literacy programs that are accessible, contextualized, and interactive yield positive learning outcomes, particularly for individuals with disabilities (Jenaro et al., 2018; Martínez Cao et al., 2021; Marnewick et al., 2022). However, this study differs in three respects: (1) its focus on university students with physical and sensory disabilities within a higher education setting; (2) the integration of accessibility-sensitive pedagogy into a concentrated, short-term intervention; and (3) the inclusion of a delayed measurement point to assess retention. These features extend prior research by highlighting the relevance of institutional context and instructional adaptation in shaping digital security awareness.

The statistically significant differences among pretest, posttest, and retention test scores align with earlier intervention studies involving individuals with disabilities, which have demonstrated the positive impact of digital security–oriented training programs (Sivrikaya & Aygül, 2026). In this regard, the present study contributes to the literature by showing that even a relatively short, six-day training program can yield meaningful and enduring learning outcomes. This finding is particularly noteworthy given the heterogeneity of participants' prior exposure to digital security risks. Although inferential subgroup analyses were not feasible due to small and uneven sample sizes, descriptive patterns suggest that experiential familiarity with digital risks may facilitate learning, offering useful insights for the design of future interventions.

Retention test results further indicate that the knowledge acquired through the training was largely maintained over a three-month period. Although a slight decrease in average scores was observed between the posttest and the retention test, this can be considered normal, suggesting that the intervention supports more than just short-term learning. Similar patterns have been documented in studies emphasizing the importance of relevance, experiential learning, and reinforcement in sustaining digital safety awareness (Nguyen et al., 2023; Berens et al., 2024). At the same time, the observed decline underscores the potential risk of information attrition and highlights the need for periodic reinforcement and ongoing support mechanisms.

An important finding of the study concerns the discrepancy between participants' high levels of digital device usage and their limited awareness of digital security risks. Although most participants reported easy access to digital technologies and frequent use for communication and information-seeking purposes, concerns related to data protection, privacy, and platform vulnerabilities were rarely articulated. This finding corroborates Biricik's (2022) assertion that frequent digital engagement does not necessarily translate into digital competence. Similarly, Park's (2022b) research emphasizes digital competence and security awareness as psychosocial protective factors for individuals with disabilities, particularly during periods of intensified digital reliance. Taken together, these findings suggest that digital accessibility alone is insufficient without the parallel development of critical digital awareness and security knowledge.

The results of the present study are largely consistent with both national and international literature demonstrating the effectiveness of targeted digital education programs for individuals with disabilities (Inan et al., 2016; Atasoy & Ormanlı, 2019; Chadwick et al., 2022; Talan & Aktürk, 2021). For example, interventions aimed at promoting digital citizenship and healthy online relationships have reported comparable improvements in knowledge, particularly when instruction is guided, interactive, and gamified (Karadağ et al., 2022). In contrast, findings from the DA4You project indicate that existing digital accessibility trainings are often fragmented and insufficient (Black & de Pablos Ortega, 2025). The intensive and holistic design of the six-day training program implemented in this study directly addresses this gap, responding to a critical concern identified in the literature.

Descriptive analyses also suggest potential differences in knowledge acquisition and retention across disability categories (Table 2). These patterns indicate that disability-related factors -such as attention span, interaction with digital interfaces, and cognitive load- may influence engagement with training content (Demir & Şen, 2009). While participants with visual

impairments and cerebral palsy appeared to retain knowledge more effectively, those with mobility impairments showed a relatively greater decline between posttest and retention assessments. Although the limited representation of certain disability groups restricts generalizability, the findings nevertheless point to the importance of individualized and accessible instructional design.

Similarly, participants who reported prior experiences with digital security problems tended to demonstrate more pronounced improvements following the training (Table 3). Although no statistically significant relationship was established between prior experience and learning outcomes, this exploratory pattern aligns with experiential learning theories, which emphasize the role of real-life encounters in shaping learners' engagement with educational content (Mutlu, 2014; Peri Mutlu & Mutlu, 2017). Importantly, participants who had no prior exposure also benefited from the intervention, highlighting the preemptive value of digital safety training. These findings highlight that digital safety training can function as both a remedial and preventive educational tool, while further research with larger examples is needed to clarify the role of prior digital experience (Yiğit & Seferoğlu, 2020; Arar et al., 2022).

Throughout this discussion, the findings have been interpreted using cautious and non-causal language. Given the quasi-experimental design and limited sample size, the results should be understood as evidence of within-group change rather than as generalizable causal effects. Accordingly, observed differences across disability types and prior experience levels are presented as indicative patterns rather than definitive conclusions, in line with methodological recommendations for small-sample intervention research (Zimmermann et al., 2019).

Overall, the study demonstrates that digital security awareness training has substantial potential to enhance protective knowledge among university students with disabilities. However, the sustainability and magnitude of these effects appear to vary depending on disability type, prior experience, and engagement with digital technologies. These findings underscore the need for educational programs that are not only technically robust but also pedagogically adaptive, socially inclusive, and institutionally supported. Future research should extend this work through larger samples, longitudinal designs, and mixed-method approaches that capture the nuanced experiences of learners in diverse digital ecologies.

Based on these findings, several practical recommendations can be offered. First, higher education institutions should integrate digital safety awareness training into broader disability support and accessibility frameworks, moving beyond simply providing access to develop comprehensive digital competencies. Second, educational programs should utilize participatory-centered and adaptive instructional designs that consider diverse disability types, learning preferences, and levels of digital experience. Third, to mitigate information loss, digital safety training should be reinforced through periodic follow-up sessions, supplementary materials, and ongoing support. Finally, policymakers and education practitioners should develop interventions that recognize digital safety as a fundamental dimension of digital inclusion and equity, particularly for students with disabilities who may face increased risks in digital environments.

4.1 Limitations

This study has several limitations that should be acknowledged:

First, although the Digital Security Awareness Assessment Form (DSAAF) demonstrated acceptable internal consistency and content validity within the present sample, the instrument has not yet undergone extensive validation across larger and more diverse populations. The unidimensional structure identified through exploratory factor analysis requires further confirmation through larger-scale studies and confirmatory factor analyses to establish structural stability and broader applicability.

Second, the quasi-experimental single-group design limits causal interpretation. Without a control group, alternative explanations such as testing effects, increased familiarity with the instrument, short-term motivational influences, or external exposure to digital security information cannot be ruled out. Therefore, the observed score differences should be interpreted as within-group changes rather than definitive intervention effects.

Third, the small sample size (n=15) restricts statistical power and limits generalizability. The study may not have been sufficiently powered to detect smaller effects or to examine potential moderating variables. As a result, the findings should be considered preliminary and interpreted with caution.

Fourth, subgroup analyses by disability type and prior digital security experience were based on very small and uneven group sizes. These conditions precluded inferential comparisons and limited the ability to examine whether specific disability-related or experiential factors systematically influenced outcomes. Consequently, subgroup patterns are exploratory and require investigation in larger, stratified samples.

Finally, the study relied on self-reported knowledge measures. Although changes in reported awareness were observed, self-report data do not necessarily reflect behavioral change in real-world digital contexts. Future research

incorporating behavioral assessments or longitudinal follow-up designs would provide a more comprehensive evaluation of digital security competence.

Research and Publication Ethics Statement

Ethical approval for the study was obtained from the Scientific Research and Publication Ethics Committee of Isparta University of Applied Sciences (29/01/2024, 179-01). Participants were duly informed about the study's aims, procedures, and related considerations, and verbal informed consent was obtained from all volunteer participants by the researcher.

Contribution Rates of Authors to the Article

The study was prepared by a single author.

Support Statement

This study was supported by TÜBİTAK (The Scientific and Technological Research Council of Türkiye) under the 4008-Support Program for Inclusive Society Practices for Individuals with Special Needs (Project Number: 124B571).

Acknowledgement

The author extends gratitude to the experts, trainers, mentor students, and participants who contributed to the success of the project.

Statement of Interest

There is no conflict of interest.

5. REFERENCES

Arar, K., Saiti, A., & Guajardo, M. (2022). Redesigning and recomputing the future of education: The role of technology, the learning process, personality traits, and diversity in learning systems. *Power and Education, 15*(2), 243-258. https://doi.org/10.1177/17577438221117346

Arslan, S., & Bulut Özek, M. (2020). Internet usage habits and parental opinions of students with mild mental disabilities. *Manisa Celal Bayar University Journal of The Faculty of Education, 8*(1), 59-72

Arslankara, V. B., & Usta, E. (2020). Virtual risk perception in high school students: A research in the context of problematic internet usage and critical thinking. *Ahmet Keleşoğlu Eğitim Fakültesi Dergisi, 2*(1), 134-153

Atasoy, İ., & Ormanlı, O. (2019). Technology and cyber security the future of digital society. *İstanbul Aydın Üniversitesi Dergisi, 11*(4), 399-409

Avcı, Ü., & Arslan, E. (2019). The effect of in-service training with digital data security awareness and information literacy. *Ankara University Journal of Faculty of Educational Sciences, 52*(3), 891-914. https://doi.org/10.30964/auebfd.493124

Berens, B. M., Mossano, M., & Volkamer, M. (2024). Taking 5 minutes protects you for 5 months: Evaluating an anti-phishing awareness video. *Computers & Security, 137*, 103620. https://doi.org/10.1016/j.cose.2023.103620

Biricik, Z. (2022). Digital addictions and digital minimalism as a road to escape from digital addictions. *Turkish Online Journal of Design Art and Communication, 12*(3), 897-912. https://doi.org/10.7456/11203100/022

Black, S., & de Pablos Ortega, C. (2025). Digital accessibility tools and training and the DA4You course: Views and experiences of users with disabilities. *Universal Access in the Information Society, 24*, 1643-1657. https://doi.org/10.1007/s10209-024-01168-1

Blake, J. J., Lund, E. M., Zhou, Q., Kwok, O. M., & Benz, M. R. (2012). National prevalence rates of bully victimization among students with disabilities in the United States. *School Psychology Quarterly, 27*(4), 210-222. https://doi.org/10.1037/spq0000008

Büyüköztürk, Ş., Çakmak, E. K., Akgün, Ö. E., Karadeniz, Ş., & Demirel, F. (2016). *Bilimsel araştırma yöntemleri*. Pegem Akademi

Carretero, S., Vuorikari, R., & Punie, Y. (2017). *DigComp 2.1: The digital competence framework for citizens with eight proficiency levels and examples of use*. Publications Office of the European Union

Castells, M. (1996). *The rise of the network society*. Blackwell Press

Castells, M. (2009). *Communication power*. Oxford University Press

Caton, S., Hatton, C., Gillooly, A., Oloidi, E., Clarke, L., Bradshaw, J., Flynn, S., Taggart, L., Mulhall, P., Jahoda, A., Maguire, R., Marriott, A., Todd, S., Abbott, D., Beyer, S., Gore, N., Heslop, P., Scior, K., & Hastings, R. P. (2024). Online social connections and Internet use among people with intellectual disabilities in the United Kingdom during the COVID-19 pandemic. *New Media & Society, 26*(5), 2804-2828. https://doi.org/10.1177/14614448221093762

Chadwick, D., Ågren, K. A., Caton, S., Chiner, E., Danker, J., Gómez-Puerta, M., Heitplatz, V., Johansson, S., Normand, C. L., Murphy, E., Plichta, P., Strnadova, I., & Wallén, E. F. (2022). Digital inclusion and participation of people with intellectual disabilities during COVID-19: A rapid review and international bricolage. *Journal of Policy and Practice in Intellectual Disabilities, 19*(3), 242-256. https://doi.org/10.1111/jppi.12410

Chadwick, D., Wesson, C., & Fullwood, C. (2013). Internet access by people with intellectual disabilities: Inequalities and opportunities. *Future Internet, 5*(3), 376-397. https://doi.org/10.3390/fi5030376

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences*. Routledge

Demir, T., & Şen, Ü. (2009). A study on learning sytles of visually impaired students in accordance with certain variables. *Uluslararası Sosyal Araştırmalar Dergisi, 2*(8), 154-161

Didden, R., Scholte, R. H. J., Korzilius, H., de Moor, J. M. H., Vermeulen, A., O'Reilly, M., Lang, R., & Lancioni, G. E. (2009). Cyberbullying among students with intellectual and developmental disability in special education settings. *Developmental Neurorehabilitation, 12*(3), 146–151. https://doi.org/10.1080/17518420902971356

Doğan, E. Ş., & Gündüz, U. (2025). Exploring emerging digital-age fears linked to the internet and social media. *IBAD Sosyal Bilimler Dergisi,* 18, 88-116. https://doi.org/10.21733/ibad.1627789

Emerson, E., & Roulstone, A. (2014). Developing an evidence base for violent and disablist hate crime in Britain: Findings from the life opportunities survey. *Journal of Interpersonal Violence, 29*(17), 3086-3104. https://doi.org/10.1177/0886260514534524

Gültekin, U., & Ünal, Ö. Ü. F. (2021). Otizm spektrum bozukluğu ve siber zorbalık ile ilgili araştırmalara yönelik derleme çalışması. In M. Ak (Ed.), *Otizm araştırmalarında güncel eğilimler* (pp. 163-177). Nobel Akademik Yayıncılık

Inan, F. A., Namin, A. S., Pogrund, R. L., & Jones, K. S. (2016). Internet use and cybersecurity concerns of individuals with visual impairments. *Journal of Educational Technology & Society, 19*(1), 28-40

Jain, S. (2017). ICT access, disability human rights, and social inclusion in India. In J. Lazar & M. Ashley Stein (Ed.), *Disability, human rights, and information technology* (pp. 263-278) University of Pennsylvania Press. https://doi.org/10.9783/9780812294095-018

Jenaro, C., Flores, N., Vega, V., Cruz, M., Pérez, M. C., & Torres, V. A. (2018). Cyberbullying among adults with intellectual disabilities: Some preliminary data. *Research in Developmental Disabilities,* 72, 265-274. https://doi.org/10.1016/j.ridd.2017.12.006

Karadağ, B., Erbaşı, Z., Karagöz, K. T., & Özmen, S. (2022). Digital academy for mentally disabled. *Orclever Proceedings of Research and Development, 1*(1), 58–74. https://doi.org/10.56038/oprd.v1i1.152

Karakuş, M. (2024). Digital violence and social media: A bibliometric study. *TRT Akademi, 9*(20), 204-227. https://doi.org/10.37679/trta.1401797

Kowalski, R. M., & Toth, A. (2018). Cyberbullying among youth with and without disabilities. *Journal of Child & Adolescent Trauma,* 11, 7-15. https://doi.org/10.1007/s40653-017-0139-y

Kowalski, R. M., Morgan, C. A., Drake-Lavelle, K., & Allison, B. (2016). Cyberbullying among college students with disabilities. *Computers in Human Behavior, 57*, 416-427. https://doi.org/10.1016/j.chb.2015.12.044

Lawshe, C. H. (1975). A quantitative approach to content validity. *Personnel Psychology, 28*(4), 563–575. https://doi.org/10.1111/j.1744-6570.1975.tb01393.x

Marnewick, C., Meda, L., Condy, J., & Phillips, H. (2022). Using an intervention programme to empower intellectually disabled learners to use WhatsApp in a special needs unit in Cape Town, South Africa. *Cogent Education, 9*(1), 2142447. https://doi.org/10.1080/2331186X.2022.2142447

Martínez Cao, C., Gómez, L. E., Alcedo, M. Á., & Monsalve, A. (2021). Systematic review of bullying and cyberbullying in young people with intellectual disability. *Education and Training in Autism and Developmental Disabilities, 56*(1), 3-17. https://www.jstor.org/stable/27077943

Mutlu, M. E. (2014). Öğrenme deneyimlerinin yorumlanması. *Eğitim ve Öğretim Araştırmaları Dergisi, 3*(4), 21-45

Nagornaya, L. A., & Nagornyi, N. N. (2023). Current digital socialization of physically disabled people. In S. G. Maximova (Ed.), *Complex social systems in dynamic environments*. (pp. 901-907), Springer. https://doi.org/10.1007/978-3-031-23856-7_77

Nguyen, C., Jensen, M., & Day, E. (2023). Learning not to take the bait: A longitudinal examination of digital training methods and overlearning on phishing susceptibility. *European Journal of Information Systems, 32*(2), 238-262. https://doi.org/10.1080/0960085X.2021.1931494

Oğuz Özgür, H. (2023). Engelli bireylerin güncel tehdit alanı: çevrimiçi dünya. In M. Ö. Kalaç & V. Tecim (Ed.), *Engelsiz bilişim 2023: Engelsiz dijital dönüşüm* (pp. 27-47). Kriter Yayınevi

Oğuz Özgür, H., & Özkul, M. (2022). Generations' new violence experience in risk society: Digital violence. *Turkish Studies, 17*(3), 551-568. https://doi.org/10.7827/TurkishStudies.62045

Özsarı, A., & Deli, Ş. C. (2023). The relationship between digital literacy and digital addiction: A research of hockey athletes. *The Online Journal of Recreation and Sports, 12*(4), 491-501. https://doi.org/10.22282/tojras.1283899

Park, E. Y. (2022a). Digital competence and internet use/behavior of persons with disabilities in PC and smart device use. *Universal Access in the Information Society, 21*, 477–489. https://doi.org/10.1007/s10209-020-00782-z

Park, E. Y. (2022b). Effect of COVID-19 on Internet usage of people with disabilities: A secondary data analysis. *International Journal of Environmental Research and Public Health, 19*(13), 7813. https://doi.org/10.3390/ijerph19137813

Peri Mutlu, A., & Mutlu, M. E. (2017). Öğrenme deneyimi tasarımı. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi, 3*(1), 39-76

Quarmby, K. (2015). Disability hate crime motivation survey. Retreived May 28, 2025 from https://katharinequarmby.wordpress.com/

Sentenac, M., Gavin, A., Arnaud, C., Molcho, M., Godeau, E., & Nic Gabhainn, S. (2011). Victims of bullying among students with a disability or chronic illness and their peers: A cross-national study between Ireland and France. *Journal of Adolescent Health, 48*(5), 461-466. https://doi.org/10.1016/j.jadohealth.2010.07.031

Sir, Ö., & Yıldız, M. (2023). Dijital dönüşümün engellilerin istihdamı üzerindeki etkisi. In K. Y. Genç, Y. Mamur Işıkçı, & E. Gökçen Kaygısız (Ed.), *Engelliliğe dair güncel konular* (pp. 200-214). Ekin Yayınevi

Sivrikaya, T., & Aygül, N. (2026). The effectiveness of video modeling in teaching digital safety skills to individuals with intellectual disabilities. *Journal of Special Education Technology, 41*(3), 391-406. https://doi.org/10.1177/01626434251414866

Söderström, S., & Hemmingsson, H. (2017). Digitalised communication and social interaction: New opportunities for young disabled people's participation. In A. H. Eide, S. Josephsson, & K. Vik (Ed.), *Participation in Health and Welfare Services* (pp. 170-183). Routledge

Sönmez, V., & Alacapınar, F. G. (2016). *Örneklendirilmiş bilimsel araştırma yöntemleri*. Anı Yayıncılık

Şentürk, Ş., & Keskin, A. (2018). İşitme engelli öğrencilerde internet bağımlılığı: Samsun ili örneği. *Gazi Eğitim Bilimleri Dergisi, 4*(2), 51-60

Talan, T., & Aktürk, C. (2021). Investigation of digital literacy and information security awareness levels of secondary school students. *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi, 18*(1), 158-180. https://doi.org/10.33437/ksusbd.668255

Tan, H., & Şenkal, Y. (2024). Examining the psychological and behavioral effects of cyberbullying and defense mechanisms developed against cyberbullying through digital natives. *Uluslararası Sosyal Bilimler Akademi Dergisi,* 16, 410-441. https://doi.org/10.47994/usbad.1510397

Turkle, S. (2011). *Alone together: Why we expect more from technology and less from each other.* Basic Books

Veerabathiran, R., & Thomas, S. M. (2025). Technological inovations and their impact on disability in Asian and African continents. In R. Veerabathiran, & S. M. Thomas (Ed.), *Disability Across Continents* (pp. 69-90). Springer

Vuorikari, R., Kluzer, S., & Punie, Y. (2022). *DigComp 2.2: The digital competence framework for citizens with new examples of knowledge, skills and attitudes*. Publications Office of the European Union

Wells, M., & Mitchell, K. J. (2014). Patterns of internet use and risk of online victimization for youth with and without disabilities. *The Journal of Special Education, 48*(3), 204-213. https://doi.org/10.1177/0022466913479141

Yeon, E. M., & Choi, H. S. (2019). Relationship between digital informatization capability, digital informatization accessability and life satisfaction of disabled people: Multigroup analysis of perceived social support network. *Journal of the Korea Academia-Industrial cooperation Society, 20*(12), 636-644. https://doi.org/10.5762/KAIS.2019.20.12.636

Yiğit, M. F., & Seferoğlu, S. S. (2020). Bireylerin siber güvenlik davranışlarını etkileyen faktörler üzerine bir inceleme. In H. F. Odabaşı, B. Akkoyunlu, & A. İşman (Ed.), *Eğitim teknolojileri okumaları 2020* (pp. 55-75). Pegem Akademi

Zimmermann, G., Bolter, L.-M., Sluka, R., Höller, Y., Bathke, A. C., Thomschewski, A., Leis, S., Lattanzi, S., Brigo, F., & Trinka, E. (2019). Sample sizes and statistical methods in interventional studies on individuals with spinal cord injury: A systematic review. *Journal of Evidence-Based Medicine, 12*(3), 200–208. https://doi.org/10.1111/jebm.12356