Research Article / Araştırma Makalesi

Cyber Psychology from Educational Administration Perspective: Teachers and School Administrators' Qualitative Insights

Eğitim Yönetimi Penceresinden Siber Psikoloji: Öğretmenlerin ve Okul Yöneticilerinin Nitel İçgörüleri¹

Su ERTÜRK², Gülnihal YILDIRIM³, Temel ÇALIK⁴

Keywords

1.Cyberpsychology

- 2.Cyber Awareness
- 3. Cyberbullying

4. Descriptive

phenomenology

5. Educational

Administration

Anahtar Kelimeler

- 1. Siber Psikoloji
- 2. Siber Farkındalık
- 3. Siber Zorbalık
- 4. Betimleyici
- Fenomenoloji
- 5. Eğitim Yönetimi

Received/Başvuru Tarihi 27.03.2024

Accepted / Kabul Tarihi 20.01.2025



Purpose: This study aims to cultivate awareness of the phenomena of bullying and security within the framework of cyber psychology. In line with this primary objective, the experiences and awareness levels of participating school administrators and teachers were examined.

Method: A descriptive phenomenological design, supported by a large sample, was employed to explore the semantic spectrum of cyber security and cyber bullying concepts. The study group consisted of 192 teachers and 64 school administrators, selected through purposeful sampling, specifically convenience sampling. A semi-structured online interview form served as the data collection tool. Content analysis was conducted with the goal of conceptualizing the data and identifying themes that describe the phenomenon. The findings are presented through descriptive narratives.

Findings: The findings reveal the significant emotional distress and security concerns negatively influenced by cyber psychology. Additionally, it has been found that cyberbullying and security issues lead to serious consequences for individuals, such as loss of self-confidence, social isolation, persistent anxiety, and long-term psychological trauma. The data reveal that females are the gender most frequently subjected to cyber bullying, with the most vulnerable age group being 14-18, followed by the 11-14 age range. The identified sub-themes of cyber bullying include fraud, hacking, violation of privacy, verbal abuse, blackmail, threatening and psychological violence.

Highlights: By examining the experiences of participants across a large sample, the study broadens the understanding of cyber bullying and security concepts. The detailed analysis of sub-themes provides both theoretical insights and practical recommendations for policymakers and practitioners. The study serves as an important reference to enhance awareness among teachers and school administrators who are the closest to children and youth in school and to develop measures that address the increasing challenges of internet use in education.

Öz

Amaç: Araştırmanın amacı siber psikoloji çerçevesinde zorbalık ve güvenlik olgularına yönelik farkındalık oluşturmaktır Bu temel amaç çerçevesinde, araştırmaya katılan okul yöneticileri ve öğretmenlerin deneyimleri ve farkındalık düzeyleri incelenmiştir.

Yöntem: Araştırmada siber güvenlik ve siber zorbalık kavramlarının anlam yelpazesini vurgulamak için büyük bir örneklemle desteklenen betimleyici fenomenolojik desen tercih edilmiştir. Çalışma grubu, amaçlı örnekleme yöntemlerinden uygun örnekleme ile seçilen 192 öğretmen ve 64 okul yöneticisinden oluşmaktadır. Veri toplama aracı olarak yarı yapılandırılmış çevrimiçi görüşme formu kullanılmıştır. Verilerin ayıklanması ve düzenlenmesinden sonra gerçekleştirilen içerik analizi, kavramsallaştırma ve olguyu tanımlayabilecek temaları ortaya çıkarmak amacıyla titizlikle betimsel anlatımlarla sunulmuştur.

Bulgular: Araştırma bulguları, katılımcıların deneyim ve gözlemlerine dayanarak, siber psikolojinin olumsuz etkilediği önemli duygusal stres ve güvenlik kaygılarını ortaya koymaktadır. Ayrıca, siber zorbalık ve güvenlik sorunlarının, bireylerde özgüven kaybı, sosyal izolasyon, sürekli kaygı ve uzun süreli psikolojik travma gibi ciddi sonuçlara yol açtığı bulunmuştur. Veriler, siber zorbalığa en sık maruz kalan grubun kadınlar olduğunu, en savunmasız yaş grubunun ise 14-18 yaş arası olduğunu, bunu 11-14 yaş grubunun takip ettiğini göstermektedir. Belirlenen siber zorbalık alt temaları ise dolandırıcılık, hesapların hacklenmesi, mahremiyet ihlali, sözlü taciz, şantaj, tehdit ve psikolojik şiddet olarak sıralanmıştır.

Önemli Vurgular: Araştırma, geniş bir katılımcı grubunun deneyimlerini inceleyerek siber zorbalık ve güvenlik kavramlarının anlaşılırlığını genişletmektedir. Dolandırıcılık, bilgisayar korsanlığı, mahremiyetin ihlali, şantaj, tehdit ve psikolojik şiddet gibi alt temaların detaylı analizi, hem teorik içgörüler hem de politika yapıcılar ve uygulayıcılar için pratik öneriler sunmaktadır. Bu kapsamda çocukların ve gençlerin okullarda en yakınındaki öğretmen ve okul yöneticisi kesiminin farkındalığını artırmak ve eğitimde internet kullanımının artan zorluklarına karşı önlemler geliştirmek için stratejik ve önemli bir referans niteliğindedir.

² Corresponded Author, Gazi University, Gazi Education Faculty, MoNE, Ankara, TÜRKİYE; https://orcid.org/ 0000-0002-9418-7632

³ MoNE, Ankara, TÜRKİYE ; https://orcid.org/0000-0003-4803-056X



¹ This study is an extended version of the paper presented as an oral presentation at the 4th National Education Transformation Forum (13-17 November 2023).

⁴ Gazi University, Education Faculty, Ankara, TÜRKİYE; https://orcid.org/ 0000-0003-3656-6260

Citation/Alıntı: Ertürk, S.,Yıldırım, N., & Çalık, T. (2025). Cyber Psychology from Educational Administration Perspective: Teachers and School Administrators' Qualitative Insights, Kastamonu Education Journal, 33(1), 108-123. doi: 10.24106/kefdergi.1628420

INTRODUCTION

Changing lifestyles and constant digital presence are affecting the minds of millions of young people as the average time spent on the internet is rapidly increasing. Young people spend a lot of time chatting online with their friends through social networks, playing online games with their peers, and shopping for products online (Ahuja & Alavi, 2017). In this respect, although digital technologies and the internet provide great convenience in our lives, they turn into a significant problem when used unconsciously. It is known that not having sufficient awareness and the use of technology and internet reaching the addiction level hinders the development of young generations in particular and leads to the development of individuals harmful to society (Akcan, Öztürk & Şarlak, 2020). In addition, activities related to daily life are carried out in the cyberspace, away from all physicality and boundaries, and have penetrated into each individual's home and even into their room. Individuals have to integrate their representations and identities in this cyberspace with their representations and identities in the real, actual space. It is stated that the failure to carry out this integration process in a functional manner most of the time causes grievances (Öztürk, Ateş & Erdoğan, 2020). On the other hand, processes related to the wrong and negative use of digital technologies, also called cyber bullying, which are also emphasized by the United States, European countries, China, Korea and Taiwan, attract attention (Baek & Bullock, 2013). In this regard, it can be said that one of the sources of these grievances is cyber bullying.

In the research conducted by Rigby (2003) on cyber bullying, it is stated that students who are victimized in this sense face many mental, physical and psychological problems such as 'low psychological well-being', 'poor social adaptation', 'psychological stress and anxiety', 'physical disorders'. Telephones, computers, etc., which are also used as a part of learning in the context of the digital and technological processes mentioned above. It is also stated that the use of internet along with technological devices will cause some difficulties for educators. In this context, the concept of cyber psychology, which is also discussed as internet psychology or web psychology (Ahuja & Alavi, 2017; Singh, 2019), focuses on the psychological aspects associated with the increasing presence and use of technology.

Cyber psychology refers to the study of mind and behavior in the context of interactions with technology. It also considers how people interact with each other in these environments and considers the impact of emerging trends such as technological convergence and the digital divide on individuals (Kirwan, 2010a). The importance of the field of cyber psychology in educational circles is increasing day by day, due to the prevalence of digital technologies in daily life and the inevitable use of them in educational processes. In this direction, undergraduate and graduate programs have begun to be opened in this field in Ireland, England and Russia (Voiskounsky, 2021). It can be said that academic research on the basis of cyber psychology and security has increased in recent years. In these studies, Extending the school grounds? Bullying experiences in cyberspace (Juvonen and Gross, 2008); the impact of parental online security practices, bonding, and online impulsiveness (Floros et al. 2013); student safety from cyberbullies, in chat rooms, and in instant messaging (Wolfsberg & Jeffrey, 2006); return of the hacker as hero: fictions and realities of teenage technological experts (Dudek and Johnson, 2011); effects of cyber bullying on students' academic, social and emotional states (Akbiyik & Kestel 2016), gratitude as a protective factor for cyberbullying victims: Conditional effects on school and life satisfaction (Oriol, Varela & Miranda, 2021); cyberbullying and victimization status of secondary school students: change in 10 years (Ayas & Horzum, 2023) as can be understood from the titles, there are studies covering student safety, the academic, psychological and emotional effects of cyberbullying, and the safety of those who are exposed to cyberbullying at school and their families.

Cyber Psychology

A new branch has emerged that focuses on the psychological aspects associated with the increasing presence and use of technology. This field, defined as cyberpsychology, refers to the examination of mind and behavior in the context of interactions with technology (Singh, 2019). Cyber psychology is an interdisciplinary field of study that focuses on psychological phenomena that occur as a result of human interaction with digital technology, especially the internet (Saltik, 2021). Cyber psychology emphasizes the study of people's interactions with the internet, mobile computing, cell phones, game consoles, virtual reality, artificial intelligence, and other technologies that have proven ability to change human behavior (Kirwan, 2010b). As developing digital technologies and internet use become a very important part of our daily lives, the study areas of cyber psychology have spread over a wide area. In this context, the aim of cyber psychology is to maintain and formalize a scientific understanding of the impact, dynamic processes and outcomes that digital technologies enable in individuals, groups and wider society (The British Psychological Society, 2019).

Cyber Bullying

Although technological developments make people's lives easier, they also bring negative effects on the lives of individuals or groups. Some digital platforms can serve as an environment where individuals engage in malicious behavior, including harassing others. In this regard, individuals may find themselves in the process of cyberbullying, which means the repeated and intentional use of various types of technology such as mobile phones, pagers, e-mail, instant messaging and Web sites by individuals or groups to harm others (Beran & Li, 2005). According to Ybarra and Mitchel (2004), one of the first researchers on cyber bullying, cyber bullying is a deliberate and open attack against another person online. Examples of this action include making rude or abusive comments towards someone, or deliberately shaming another user in retaliation for perceived wrongdoing. It is stated that clarifying the conceptual and operational definitions of cyberbullying can strengthen the ability of various stakeholders to identify,

prevent and respond to relevant activities (Patchin and Hinduja, 2015). In this context, the conceptual definition of cyberbullying; It can be defined as the conscious use of communication technologies by an individual or a group by sending or publishing offensive text, images, in order to intentionally and repeatedly harass or threaten another individual or group (Mason, 2008).

Cyber Security

Cyber security is defined by the International Telecommunication Union (ITU) as "guidelines, policies, tools, risk management approaches, practices, ensuring the integrity and usability of information and data in the cyber environment belonging to individuals, private and public institutions within the scope of confidentiality protocols, and the sustainability of infrastructures." It is expressed as the use of "technologies and trainings" (ITU, 2018). Within the framework of cyber security studies, the Cyber Security Board was established in Turkey. Through this board, the National Cyber Security Strategy and Action Plan 2013-2014 came into force in 2012. In addition, the target determined within the scope of the National Cyber Security Strategy and Action Plan 2020-2023 is expressed as reducing the effects of cyber threats, developing national capabilities, creating a safer national cyber environment and ensuring that our country ranks at the top at the international level in the field of cyber security (Transportation and Infrastructure Ministry, 2020).

This research aims to raise awareness about the psychological and physical effects of uncontrolled and uneducated digital use within the context of educational management and seeks to fill a significant gap in the field of cyber psychology. By examining the perspectives and experiences of school administrators and teachers, who are key figures in reaching children and young people, the study provides valuable data and strategic recommendations. The significance of this research lies in offering guidance and innovative insights by linking these issues to national and international educational strategies, thereby making a unique contribution to the academic literature. With the prediction that education administrators and teachers need more research and awareness about the problems encountered in the cyber world, this research aims to examine cyber psychology within the framework of educational management and raise awareness about cyber security. In this context, the lack of groundwork on cyber psychology will be addressed, and results and recommendations based on research findings will be presented to researchers. It is expected that this study will guide decision-makers at both national and international levels regarding the importance of cyber psychology and cyber threats.

Within the framework of the main purpose of the research, answers were sought for the following sub-objectives:

- 1. According to school administrators and teachers, what is their experience of being subjected to a cyber attack/bullying by themselves or a relative/ an acquaintance?
- 2. What are the effects of cyberbullying and cybersecurity problems on victims, according to school administrators and teachers?
- 3. How do school administrators and teachers interpret the age group and gender most exposed to cyberbullying?
- 4. What are the themes and subthemes that emerge according to the cyberbullying experiences of school administrators and teachers?

METHOD

Pattern of the Research

The research employed a phenomenological design, a qualitative research method that seeks to understand the essence of experiences related to a specific phenomenon. Phenomenology aims to answer the question, "What is truth?" by focusing on individual experiences and emphasizing description over generalization (Groenewald, 2004). In this research, the Descriptive Phenomenology approach was chosen to understand the effects of participants' experiences with cyberbullying, cyber psychology, and cybersecurity in an unbiased way and to reveal the essence of these experiences. Husserl (1931), the founder of Descriptive Phenomenology, emphasized understanding how a phenomenon is experienced by participants and identifying commonalities in these experiences. Husserl highlighted the importance of describing individuals' subjective experiences objectively, requiring researchers to set aside personal biases (*epoche*). Our study aims to detail the psychological and social impacts of cyberbullying as described by participants and to emphasize the significance of these experiences for societal awareness. This methodological framework enables a clear depiction of the phenomenon and faithfully reflects participants' experiences (Creswell, 2013; Husserl, 1931).

To ensure the validity of phenomenology, well-defined inclusion criteria were crucial. Participants were selected from Ankara's central districts, areas characterized by continuous migration and demographic shifts that influence social dynamics and increase the risk of bullying, including cyberbullying (Yıldırım & Şimşek, 2021; TÜİK, 2022). These economically developed districts provide significant access to digital technologies, facilitating both positive and negative online interactions, which is critical for understanding cyber phenomena (Livingstone & Smith, 2014; Tokunaga, 2010). According to data from the Household Information Technologies Usage Survey (2023) by the Turkish Statistical Institute (TÜİK), the rates of internet and computer access are high in these economically developed regions. Similarly, the Ministry of National Education's (MoNE) " Technology and Education from the Perspective of Teachers on the 100th Anniversary of the Republic: Regional Workshop Report" (2024) states that schools are

110

better equipped in terms of access to digital resources, which significantly influences the online experiences of students and teachers. This economic infrastructure is a critical factor in understanding cyber interactions within the context of the research.

Inclusion criteria ensured that participants, specifically school administrators and teachers, had direct and meaningful experiences with cyberbullying and cyber security. The pandemic's shift to remote education further emphasized the importance of digital literacy among students and educators in these areas. Additionally, migration to Ankara increased after the February 2023 earthquake, as the city is outside the disaster zone, adding to integration challenges that can lead to conflict and bullying (UNESCO, 2021; Yıldırım & Şimşek, 2021). Exclusion criteria were established to maintain the study's focus, excluding individuals not employed in formal elementary, middle, or high schools in Ankara's central districts during the 2022-2023 academic year. Other exclusions included staff from private institutions, preschool teachers, and those who did not fully respond to research questions or lacked relevant experiences. This structured approach ensured that the study captured a comprehensive range of perspectives related to cyber psychology, cyber security, and cyberbullying.

Study Group

In this study, a purposive sampling method, specifically convenience sampling, was employed to select participants with potentially rich and relevant information such as teachers and school administrators, who possess direct knowledge and experience of the phenomenon, allowing for an in-depth investigation of cyberbullying, an issue affecting educational environments (Yıldırım & Şimşek, 2021). This method not only facilitated the collection of rich and meaningful data from participants but also offered practical advantages in terms of time and resource constraints (Creswell & Poth, 2018). Additionally, such sampling methods are highly beneficial in exploratory research, where the goal is to gather in-depth insights from a specific group (Patton, 2002). Initially, the target sample size was set between 100-150 participants. However, as data emerged, it became clear that the contributions to the field were substantial, which encouraged us to expand the sample size. Literature on phenomenological research, including works by Polkinghorne (1989) and Smith and Shinebourne (2012), highlights the importance of larger samples for certain topics. Consequently, the sample size was increased as a result of the numerous interesting and indepth responses, leading to the continuation of the data collection process. In phenomenological research, sample size can vary depending on the research objectives and subject matter. While Polkinghorne (1989) suggests up to 325 participants, Dukes (1984) recommends smaller groups of 3-10 individuals. However, in fields like education and healthcare, larger samples are often preferred to enhance data diversity and facilitate comprehensive analysis (Smith & Shinebourne, 2012; Finlay, 2014). Given the multifaceted nature of cyberbullying as a societal issue, a larger, more diverse sample allowed for a more thorough understanding of the phenomenon, with teachers and school administrators offering various perspectives that enriched the analysis.

District	Duty		School Type			Age				Gender	
	Teacher	School Administrator	Primary	Secondary	High School	24- 34	35- 45	46- 56	57&Upper	Female	Male
Altındağ	9	5	6	7	1	6	4	3	1	9	5
Çankaya	37	9	27	12	7	9	26	11	-	37	9
Etimesgut	12	7	7	7	5	6	11	1	1	17	2
Gölbaşi	10	6	6	4	6	1	7	7	1	10	6
Keçiören	24	9	9	7	17	7	17	8	1	20	13
Mamak	13	8	4	10	7	6	11	4	-	14	7
Pursaklar	48	10	11	24	23	15	28	13	2	38	20
Sincan	11	4	4	8	3	4	10	1	-	10	5
Yenimahalle	28	6	7	18	9	12	16	6	-	25	9
Total	192	64	81	97	78	66	130	54	6	180	76

Table 1. Demographic Properties of Participants

Participants were reached through a structured online approach, where a semi-structured questionnaire was distributed to school administrators and teachers via district education directorates. Data collection was carried out with participants voluntarily completing the forms using their personal devices, ensuring ethical standards and privacy were upheld. According to Creswell (2013) and Bryman (2016), online data collection methods provide flexibility and anonymity, which can lead to more honest and reliable responses. Reips (2002) also emphasizes that the absence of physical and social pressure in online surveys enhances the

accuracy of responses. This method contributed to the reliability and validity of the data, particularly in the context of cyberbullying and online safety issues. After a month of data collection, we observed that new responses began to overlap with prior explanations, signaling data saturation. This indicated that no new significant insights were being gained from additional participants. As a result, we decided to close the survey and halt data collection. Ultimately, the final sample consisted of 192 teachers and 64 school administrators from formal primary, secondary, and high schools in central districts of Ankara, all affiliated with the Ministry of Education. The demographic data of the participants who filled out the data collection tool on a voluntary basis and whose data were evaluated are shown in Table 1. The large sample size proved beneficial in gaining a comprehensive understanding of the complex nature of cyberbullying and contributed valuable insights to the field. This research lays a solid foundation for future educational policies and interventions aimed at addressing cyberbullying (Creswell & Poth, 2018; Van Manen, 2016; Moustakas, 1994).

Data Collection Tool

The online semi-structured interview form, used as a data collection tool, was meticulously developed through a comprehensive process based on both quantitative and qualitative research related to cyberbullying. Surveys and guides developed by Hinduja & Patchin (2009), Brighi et al. (2012), and Smith et al. (2008) were reviewed to ensure the robustness of the form's content. The purpose of this form is to capture participants' personal or observed experiences and to raise awareness in this field. Each question was carefully crafted to explore these experiences in detail and was administered in a secure and user-friendly online environment. The development process of the semi-structured form adhered to the principles of qualitative data collection and phenomenological research (Creswell, 2013; Patton, 2002; Merriam, 2009).

The form included only essential demographic questions, such as role, age, gender, and school type, to understand participants' profiles. Additional questions aimed to assess participants' awareness and experiences related to cybersecurity without causing discomfort. Feedback was gathered from a cybersecurity specialist and an educational measurement expert to improve the tool's validity, clarity, and ethical integrity. Expert support is considered an essential strategy for ensuring content validity in qualitative research (Guba & Lincoln, 1994; Merriam, 2009), and in this context, feedback from two field experts was sought to verify whether the interview questions adequately covered the area of interest.

The cybersecurity specialist suggested adding the response option "I would not disclose even if it occurred" to the question "Have you or a relative been subjected to a cyber attack/bullying?" to protect participants' privacy and make them feel more comfortable when answering sensitive questions. Additionally, the measurement expert recommended rephrasing the question "Have you experienced cyberbullying?" to a softer and more inclusive form: "Would you like to share any experiences related to cyberbullying or cybersecurity involving yourself or a relative?" This adjustment aimed to collect data in a non-intrusive manner. These expert-informed modifications ensured that the instrument was theoretically sound, ethically appropriate, and effective for collecting meaningful data. The introductory section of the form clearly stated that participation was entirely voluntary, responses would be coded for analysis, no personal information would be collected, and the data would be used solely for academic purposes (Büyüköztürk et al., 2010).

Data Collection Process

The finalized online semi-structured interview form was distributed using a carefully coordinated process designed to ensure both broad and secure access. The survey link was initially shared with district education directors, who then disseminated it to school administrators and teachers across the selected districts. This hierarchical distribution approach leveraged the existing administrative structure to facilitate efficient communication and enhance participation rates. Utilizing an online platform minimized logistical challenges and allowed participants to complete the survey at their convenience, thereby reducing response biases and increasing the overall reliability of the data (Patton, 2002; Creswell, 2013). The digital format also upheld ethical research standards by ensuring participant anonymity and data security, as no personally identifiable information was collected. Given the sensitive topic of cyberbullying, this method created a safe and private environment, enabling participants to share their experiences more openly and comfortably (Merriam, 2009).

Data Analysis of Data

Phenomenological research aims to uncover the lived experiences and meanings of participants, revealing the psychological essence of a phenomenon (Groenewald, 2004). In this study, content analysis was employed to conceptualize data and identify themes that describe the phenomenon. Codes were generated by examining the data, and superordinate categories (themes) were formed by grouping similar codes. Descriptive interpretations were made based on the themes identified. The coding process involved categorizing responses from different groups, such as researcher questions (Q1, Q2), school administrators (A1, A2), and teachers (T1, T2). On the other hand, in order to enhance generalizability, a large sample size was used, with 256 participants from diverse age groups and educational contexts with different experiences and insights. Following ethical guidelines and maintaining participant confidentiality, data were analyzed using phenomenological principles. Inter-rater reliability was calculated, yielding coefficients of 85%, 85.7%, and 84.8%, ensuring the robustness and validity of the identified themes (Creswell & Poth, 2018). This

approach, which considered demographic diversity, provided a comprehensive understanding of cyberbullying and laid a solid foundation for developing educational policies and interventions (Finlay, 2014; Van Manen, 2016; Moustakas, 1994).

Validity and Reliability

Several strategies based on Lincoln and Guba's (1985) framework were carefully implemented to ensure the rigor and trustworthiness of the research. To establish credibility, peer debriefing, expert consultation, and triangulation were utilized. Input from two field experts during the development of research questions ensured scientific validity, while peer debriefing with fellow researchers validated the impartiality and accuracy of codes, themes, and interpretations. Triangulation cross-verified findings with existing literature and alternative data sources.

The evidence chain played a critical role in enhancing the reliability and validity of the study. Each stage, from data collection to analysis, was conducted transparently and systematically. Contextual justifications for the emerging themes were comprehensively articulated (Miles & Huberman, 2014, Tracy,2010). An evidence chain table, created using direct quotes from participants, enriched the contextual depth and validity of the findings (Creswell, 2013). The appendix, specifically Table 2, clearly illustrated the relationship between the findings and the source data, enabling readers to understand the analytical process better. This structured evidence chain justified how themes were linked to specific findings, reinforcing the transparency and reliability of the analysis (Patton, 2002). On the other hand, transferability was addressed through thick description, offering detailed context and participant experiences, which allows others to assess the applicability of the findings. Dependability was reinforced through an inquiry audit by an experienced academic, ensuring consistency in methods and findings. An audit trail documented all analytical decisions from initial coding to theme development, providing a clear, replicable account of the analysis process. Confirmability was further ensured through reflexivity, where researchers critically examined their biases and their potential impact on the study. Collectively, these measures significantly contributed to the study's validity and reliability.

FINDINGS

The findings of the research regarding the demographic data of the participants and the descriptive analyzes regarding the questions sought to be answered with sub-purposes are summarized under two separate titles below.

Demographic Findings

The study group of the research was determined by appropriate sampling method among school administrators and teachers working in schools affiliated with the Ministry of Education in the central districts of Ankara. The participants who filled out the data collection tool on a voluntary basis and whose data were evaluated are 192 teachers and 64 school administrators from 9 central districts of Ankara (See Table 1). In the study, which included a total of 256 participants, the majority of participants were from secondary schools (n=97), while a similar number of participants were from primary schools (n=81) and high schools (n=78). It is seen that the number of female participants (n=180) is higher than that of men (n=76), and the districts with the highest participation are Pursaklar (n=58) and Çankaya (n=46).

Descriptive Findings

In the findings section of the research, descriptive statistics related to the answers given by the participants in the study group to the research sub-aims are presented. Additionally, selected expressions that emerged through content analysis are included to provide deeper insight. Direct quotes from participants, which support the formation of themes and serve as an evidence chain, are presented in Table 2, which is included in the appendix of the study.

Findings for Research Question 1

According to the first aim of the research, participants share various examples of their own or their acquaintances' experiences with cyber attacks and bullying. T3 states, "A parent's child was defrauded through an online gaming platform," illustrating incidents of fraud in gaming environments. T5 describes, "My Dad's salary account was hacked and they stole the money" highlighting the financial and security impact of such attacks. A8 mentions, "One of our students told us they were defrauded by a fake bank message," recounting a direct experience of fraud. T27 shares, "When I was student in university, My own account was hacked, and offensive content was sent to my friends" emphasizing the personal and social consequences of account hacking. A28 says, "A student's social media profile was stolen, and they were threatened," pointing out the impact of social media threats. T48 explains, "My daughter's social media account was hacked, and her private photos were posted," providing a concrete example of how cyberattacks affect families. A45 notes, "A student's photos were leaked online, and it deeply affected them," highlighting the psychological impact of cyberbullying. T66 states, "It has become common for students' accounts to be hacked and for them to receive threatening messages," indicating the prevalence of account hacking. T33 adds, " My close friend private video was hacked from phone. She lived many bad things socially" and A22 describes, "A student's social media account was hacked, and private information was shared," detailing a case of compromised account and life security.

The findings related to the first aim of the research reveal that participants shared detailed accounts of their own or their acquaintances' experiences with cyberattacks and bullying. These examples underscore the widespread and serious social, psychological, and financial impacts of cyberbullying.

Findings for Research Question 2

According to the second aim of the research, participants detail the various effects of cyberbullying and cybersecurity issues on victims through different examples. A82 shares, "One of my students reported being blackmailed for money," highlighting how cyber threats create fear and helplessness among students. T83 states, "Students are threatened and forced to do things against their will," emphasizing the manipulative nature of such bullying. A84 mentions, "My daughter was blackmailed with the threat of having her photos released," illustrating how personal and familial boundaries are violated by cyber threats. T85 explains, "Students are frightened by threats that their social media accounts will be hacked," pointing out the constant worry caused by security concerns. A86 says, "A student had to seek psychological support after being blackmailed with private information," underscoring the emotional trauma inflicted by such incidents. T87 describes, "Blackmail cases create a significant fear among students," highlighting the widespread anxiety caused by cyberbullying.

A88 notes, "One student was continuously threatened with the misuse of their private information," pointing out the persistent stress that victims face. T89 adds, "Classmates use blackmail to put each other in difficult situations," indicating how cyberbullying affects peer relationships. A90 states, "Social media blackmail severely undermines students' confidence," emphasizing the loss of trust and self-assurance. T91 explains, "One of our students was forced to comply with demands due to threats," demonstrating how threats restrict personal freedom. A102 shares, "A student said they received threatening messages and were too scared to attend classes," pointing out the impact on academic life. T103 mentions, "Threatening messages create a sense of insecurity in students' social circles," showing how bullying erodes trust among peers. A104 says, "We have students who receive malicious threats over social media," illustrating the prevalence of such incidents. T105 describes, "A student told us they didn't want to come to school because they were being threatened by classmates," showing how threats affect school attendance. A106 states, "As school administrators, we take immediate action when students report being threatened," highlighting the need for preventive measures. T107 explains, "Sending threatening messages to each other is quite common among students," demonstrating the normalcy of such behaviors. A108 notes, "One of our students reported receiving severe threats while playing an online game," indicating that threats occur in various digital settings. T109 shares, "Online threats damage students' social relationships and sense of security," illustrating the broader impact on social well-being.

A122 describes, "There are students who constantly apply psychological pressure on others, deeply affecting the victims," emphasizing the long-lasting emotional wounds caused by psychological violence. T123 mentions, "A student fell into depression because they were constantly belittled by their peers," highlighting the severe impact on mental health. A124 states, "Psychological violence destroys students' self-esteem and isolates them," pointing out the sense of loneliness and loss of confidence. T125 explains, "One student doesn't want to participate in class because they are constantly made fun of," illustrating how psychological bullying affects academic engagement. A126 notes, "Insults and belittlement cause lasting trauma for students," emphasizing the enduring effects of such behavior. T127 says, "A group of friends continuously excludes one student, making them feel worthless," drawing attention to the social isolation aspect of bullying. A128 describes, "Psychological pressure has become a significant source of stress for young people," pointing out the impact on emotional well-being. T129 explains, "Students feel insecure because of the psychological violence they face on digital platforms," highlighting how bullying erodes a sense of safety.

The findings related to the second aim of the research provide detailed descriptions of the psychological and physical effects of cyberbullying on victims. Participants reported that cyberbullying can result in severe emotional trauma, as well as physical symptoms such as headaches, stomach pain, and even the need for hospital visits. While the long-term impacts may not be fully understood or easily interpreted, the evidence clearly indicates that cyberbullying leads to significant emotional and social problems. Victims often struggle with a loss of self-confidence, feelings of exclusion, and ongoing emotional distress.

Findings for Research Question 3

In the third sub-objective of the research, descriptive statistics were created regarding the question "How do school administrators and teachers interpret the age group and gender most exposed to cyberbullying?" In this context, Figure 1 and 2 created from the data obtained according to the participants' answers, are shown below.

The figure 1 reflects the perceptions of school administrators and teachers regarding which gender is most likely to be exposed to cyberbullying. A significant portion of both school administrators and teachers believe that females are more frequently targeted by cyberbullying. Specifically, 55% (105 individuals) of school administrators and 56% (36 individuals) of teachers share this view, indicating a higher perceived risk for females. In contrast, the percentage of those who think males are more likely to be victims is relatively low, with only 14% (27 individuals) of school administrators and 8% (5 individuals) of teachers holding this belief. Additionally, there is a noteworthy proportion of respondents in both groups who are uncertain or unable to determine which gender is more susceptible to cyberbullying. Among school administrators, 31% (59 individuals) and 36% (23 individuals) of teachers expressed uncertainty, suggesting that forming a definitive judgment based on the available information is challenging or that they may lack sufficient data to confidently assess the gender most at risk.

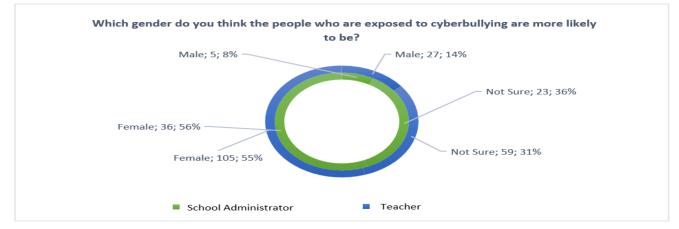
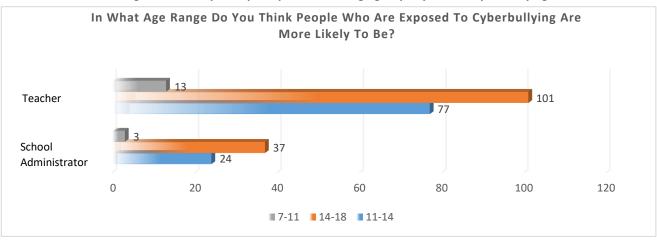
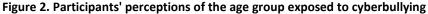


Figure 1. Participants' Perceptions Regarding the Gender Most Exposed to Cyberbullying

Figure 2 highlights the perceptions of teachers and school administrators regarding the age groups most susceptible to cyberbullying. The analysis reveals a shared view that adolescents, particularly those aged 14-18, are at the highest risk, with 101 teachers and 37 school administrators identifying this age range as the most vulnerable. The 11-14 age group is also considered at significant risk, noted by 77 teachers and 24 school administrators, indicating heightened concern for early adolescents. Conversely, the 7-11 age group is perceived as having minimal exposure to cyberbullying, with only 13 teachers and 3 school administrators indicating concern for this age range. These findings suggest a consensus that the risk of cyberbullying increases with age, emphasizing the need for targeted prevention and intervention strategies for older adolescents while acknowledging the potential under-recognition of risks for younger children.





Findings for Research Question 4

The last sub-objective of the research was "What are the themes and sub-themes that emerge according to the cyberbullying experiences of school administrators and teachers?". As a result of synthesizing the codes emerging from the research on the question, it is seen that 7 theme headings were formed as verbal insult (n=31), violation of privacy (n=30), hacking (n=29) threatening (n=27), blackmail (27), fraud (n=22), psychological violence (n=21). While determining the themes during the data analysis phase, the experience codes regarding the participant comments taken into account when including the codes in the theme headings according to the participants' frequency. Some of the experiences shared by some participants were relevant to more than one theme at the same time. For example, T33's statement "My best friend's private video was hacked from her phone. She went through a lot of bad things socially" was included in the chain of evidence table in the themes of hacking and invasion of privacy. at the same time, T33's statement "my best friend went through a lot of trouble when her private video was stolen from her phone. she socially withdrew from society. After her video went viral, she received inappropriate offers and threats. He had a lot of psychological problems. She started to receive psychological support." The statement also concerned threats and psychological violence. Another example was shared by participant T166 "A student was threatened that embarrassing photos would be spread throughout the school. She was ashamed and afraid. That's why she needed psychological support. This is a huge negative social impact for children and young people in the country." This information pointed to the theme of hacking in addition to threats and psychological violence. The other example is A27's sharing. Since the statements were "I was forced to do favors

116

for someone, or they would share private screenshots. I was very scary and nervous. It took long time to heal. I couldn't tell to my family", this was included under the theme of blackmail and psychological violence. Finally T129 statements can given as an example both verbal insult and psychological violence themes such as "Hurtful comments were made about a student's family. We know that hurtful comments about his family have a psychological effect on him. We understood that he felt excluded. He preferred to be quiet and stand on the sidelines."



Figure 3. Sub-themes of Cyberbullying

In Figure 3, the size of the shapes varies based on the frequency of the seven themes. The details of these themes are further explained through the direct quotes provided in the *Appendix*. A summary of the frequency of codes that form these themes is presented below:

1. Verbal Insult: There are quotes that include the concepts of swearing, verbal abuse, and provocation, which we have included under the theme of Verbal Insult. The Verbal Insult theme, mentioned n=31 times (A14, A2,A16, A18, A20, A26,T124,T125,T127,T128,T129,T133,T134,T136,T137,T138,T139,T116,T117,T13,T130,T14,T140,T141,T148,T149,T150) illustrates how online platforms are used to deliver abusive language, threats, and provocations. The relatively high frequency of this theme indicates that verbal abuse remains a persistent problem in digital spaces, affecting students' emotional stability and social relationships. This reinforces the findings about the psychological toll of cyberbullying, as victims often face ongoing harassment that undermines their confidence and sense of security.

2. Violation of Privacy: The theme of Violation of Privacy encompasses concepts such as taking photos or videos of a person's private parts without their consent and sexual harassment. Violation of Privacy, referenced n=30 times(A58, A1, A10, A17, A19, A21, T1, T33, T80, T78, T83, T93, T94, T105, T106, T102, T10, T100, T101, T132, T107, T108, T111, T112, T114, T120, T121, T122, T123, T166), emphasizes the serious consequences of having personal information or images shared without consent. The frequent mention of this theme reflects the psychological trauma and long-term impact experienced by victims, particularly when intimate or sensitive content is involved. This theme aligns closely with findings that indicate a heightened risk for females, reinforcing the need for gender-sensitive approaches to prevention and intervention.

3.Hacking: We have included the concepts of Social Media Account Stealing, Unauthorized Acquisition of Personal Information, and Fake Account under the theme of hacking. The theme of Hacking, with n=29 mentions (A33, A34, A48, A56, A50, A55, T181, T182, T183, T188, T19, T190, T185, T2, T34, T27, T22, T24, T32, T33, T43, T45, T3, T55, T66, T7, T67, T64, T88), underscores the widespread issue of unauthorized access to personal and social media accounts. The high frequency suggests that hacking is not only a threat to personal privacy but also a tool used for subsequent forms of harassment and manipulation, such as sending inappropriate content or impersonating victims to damage their reputations. This theme highlights the need for stronger digital literacy and cybersecurity measures within educational settings.

4. Threatening: Within the research, we have categorized *Threatening* under the themes of exclusion and comments indicating the intent to cause harm. When examining the participants' data, it is evident that their experiences align with the content of this

theme. For instance, the examples shared reflect how threats and harmful comments are used to instill fear, isolate individuals, or suggest malicious intentions, emphasizing the psychological impact of such behavior. The theme of Threatening was cited n=27 times(A32, A3, A30, A35, A36, T173, T175, T176, T177, T179, T164, T165, T166, T167, T171, T187, T189, T184, T186, T191, T192, T51, T21, T31, T33, T42, T46), reflecting the use of digital platforms to intimidate and isolate individuals through exclusion and threats of harm. The frequency of this theme demonstrates how pervasive and damaging such threats can be, affecting victims' willingness to participate in social and academic activities. The impact on victims' psychological well-being is profound, as constant fear and anxiety disrupt their daily lives and academic performance.

5.Blackmail: Within the theme of Blackmail, which involves coercing individuals to comply with demands using personal or sensitive data, numerous participants shared impactful and concerning experiences. For instance, some reported that private data, such as personal or family information, had been exploited to issue threats or demands, while others detailed incidents where compromising photographs were used to exert pressure. Blackmail, with n=27 (A23, A24, A27, A28, A29, A31, T15, T143, T144, T145, T146, T152, T151, T155, T156, T157, T174, T178, T168, T169, T160, T161, T163, T170, T18, T180, T17) occurrences, highlights the coercive tactics used to force victims into compliance by exploiting their personal data or images. The prevalence of blackmail cases suggests that students are particularly vulnerable to this form of manipulation, which can lead to severe psychological consequences, including anxiety, fear, and helplessness. This theme underscores the need for educational policies that address both prevention and support for victims.

6.Fraud: Within the theme of *Fraud*, we considered the concepts of Asking for Money and Transferring Money to an Account Without Authorization. Fraud was one of the most frequently mentioned themes, with a frequency of n=22 (A13, A11, A15, A22, T103, T104, T126, T135, T109, T110, T113, T11, T118, T119, T147, T142, T153, T158, T154, T159, T162, T172) indicating that financial scams and unauthorized money transfers are critical issues that impact both the digital safety of students and the emotional well-being of those affected. Participants described experiences involving fraudulent messages and impersonation schemes that lead to significant distress and financial loss.

7. Psychological Violence: In the research, the theme of Psychological Violence encompasses the codes of Humiliation, Ridicule, and Exclusion, supported by participants' views. Psychological Violence, with n=21 mentions (A17, A27, T101, T142, T143, T144, T145, T146, T147, T148, T166, T190, T191, T192, T32, T127, T33, T34, T49, T99, T129), points to experiences of humiliation, ridicule, and social exclusion. Although it had a slightly lower frequency among other themes, psychological violence can cause long-lasting emotional scars. Therefore this theme should continue to be a critical area of concern. Victims often experience a decline in self-esteem, feelings of worthlessness, and social isolation, highlighting the need for a comprehensive approach that includes mental health support and awareness programs.

DISCUSSION

This study utilized a phenomenological approach, a qualitative research method focused on exploring individual experiences to reveal the essence of a phenomenon (Groenewald, 2004). Through content analysis of school administrators' and teachers' responses gathered via a structured information form, the research aimed to address cyber psychology awareness and the challenges faced in cyberspace. Among the 255 participants—comprising 192 teachers and 64 school administrators—78% were unaware of Turkey's National Cyber Security Strategy, while 21% had only superficial knowledge of it. The literature indicates a lack of prior research on awareness of this national strategy. Muniandy, Muniandy and Samsudini (2017) argue that enhancing understanding of cyber threats requires collaborative efforts among stakeholders. While some experts question the efficacy of cybersecurity education (Schneier, 2014), others emphasize its necessity in protecting users from cyber threats (Moore, 2010). Participants underscored the need for greater awareness among educators, administrators, and families. This aligns with Franke and Brynielsson (2014), Machimbarrena et al. (2018), and Rahman, Sairi and Khalid (2020), who stress raising awareness of internet risks among children and adults. Interestingly, several educators in this study hesitated to discuss their cyberbullying experiences. Additionally, 55% of participants indicated that women were more frequently victims of cyberbullying, a finding consistent with Erbicer (2020) and Şener, Arıkan and Direkçi (2022), though it contrasts with research suggesting greater male victimization (Taştekin & Bayhan, 2018).

The study also identified the significant psychological and physical impacts of cyberbullying, consistent with prior research (Arıcak et al., 2008; Edward, Kontostathis & Fisher, 2016; Patchin & Hinduja, 2006; Şahin, 2012). Documented effects include emotional distress, school absenteeism, academic struggles, and even suicidal ideation. Akbıyık and Kestel (2016) highlighted how victims experience fear, anger, and anxiety, which strain familial and social relationships. Although the sample size and purposeful selection of educators allowed for in-depth exploration, the findings may not be fully generalizable across broader educational contexts due to cultural and socio-economic variations (Kowalski, Limber, & Agatston, 2012). Additionally, the study's cross-sectional nature offers only a snapshot in time. Slonje and Smith (2010) recommend longitudinal research to track how these issues evolve and influence student well-being. Future research could benefit from more diverse samples and employing

118

triangulation methods to mitigate interpretive subjectivity (Frechette et al.2020). Despite these limitations, this study lays a crucial foundation for understanding cyberbullying dynamics and points to areas needing further investigation.

CONCLUSION AND RECOMMENDATIONS

As indicated in the studies referenced in the discussion section, our research findings align with similar investigations in highlighting the significance of the fourth objective, which addresses the adverse effects of cyberbullying on students' psychological and social well-being at an international level. The risks posed by digital threats to students' developmental processes underscore the necessity of implementing preventive measures. Data derived from participants' experiences illustrate the multifaceted impact of cyberbullying, encompassing themes such as fraud, hacking, violation of privacy, verbal insults, blackmail, threatening behavior, and psychological violence. Moreover, the findings reveal the particular vulnerability of young people to online threats and highlight deficiencies in digital security awareness and ethical online behavior.

The research identifies adolescents aged 14-18 and female students as the most at-risk groups, with prevalent forms of cyberbullying leading to long-term psychological and social consequences. Several critical recommendations emerge from these findings. First, a collaborative, school-based approach that includes teachers, parents, peers, and government entities is essential for protecting children from cybercrime and cyberbullying. Integrating comprehensive cybersecurity and digital ethics education into school curricula is crucial. Second, partnerships should be established between governmental ministries, media organizations, and non-governmental organizations to address informational gaps among educators and families regarding cyber psychology, technological security issues, and the harmful effects of cyberbullying. Additionally, there is a need for increased scientific and academic research on cybersecurity in Turkey and for strengthening legal frameworks to provide robust institutional and legislative support. Utilizing mixed research methods to analyze psychometric data collected from families and students can yield deeper insights into the psychological impact of cyberbullying. Furthermore, regular data analysis using checklists developed by field experts should be conducted to identify cyberbullying tendencies in schools effectively. Given the growing importance of cybersecurity and cyber psychology, establishing and expanding undergraduate programs in cyber psychology is also crucial. Such initiatives will equip societies with well-trained professionals to address these challenges and emphasize the need for comprehensive, forward-thinking educational strategies.

Declaration of Conflicting Interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

Statements of publication ethics

I/We hereby declare that the study has not unethical issues and that research and publication ethics have been observed carefully.

Researchers' contribution rate

The study was conducted and reported with equal collaboration of the researchers.

Ethics Committee Approval Information

Ethics Committee approval of Gazi University Ethics Committee Commission dated 13.11.2023 and numbered E-77082166-604.01.02-797715 for the research proposal.

REFERENCES

- Akbiyik, C., & Kestel, M. (2016). Investigation of the impact of cyberbullying on students' academic, social, and emotional states. *Mersin University Journal of the Faculty of Education*, 12, 844-844. https://doi.org/10.17860/mersinefd.282384
- Ahuja, V. & Alavi, S. (2017). Cyber psychology and cyber behaviour of adolescents-the need of the contemporary era. *Procedia Computer Science*. 122. 671-676. 10.1016/j.procs.2017.11.422.
- Akcan, G., Öztürk, E., & Şarlak, D. (2020). Cyber addictions and psychological dynamics. In E. Öztürk (Ed.), *Cyber Psychology* (1st ed., pp. 33-40). Ankara: Türkiye Klinikleri.

Ayas, T., & Horzum, M. B. (2012). On Being Cyber Bully and Victim among Primary School Students. Ilkogretim Online, 11(2).

- Baek, J., & Bullock, L. M. (2014). Cyberbullying: A cross cultural perspective. *Emotional and Behavorial Difficulties*, 19(2), 226-238. doi:10.1080/136327522013.849028.
- Beran T. & Li Q. (2005). Cyber-harassment: A study of a new method for an old behavior. *Journal of Educational Computing Research*, 32(3), 265–277.
- Brighi, A., Ortega, R., Pyzalski, J., Scheithauer, H., Smith, P. K., Tsormpatzoudis, H., et al. (2012). European cyberbullying intervention project questionnaire ECIPQ [Unpublished questionnaire]. Retrieved from bullyingandcyber.net.

- British Psychological Society. (2019). Understanding and Facilitating the Psychological Impact of Digital Technologies. British Psychological Society.
- Bryman, A. (2016). Social research methods (5th ed.). Oxford University Press.
- Büyüköztürk, Ş., Çakmak, K. E., Akgün, E. Ö., Karadeniz, Ş. & Demirel, F. (2010). Bilimsel araştırma yöntemleri. Ankara: Pegem
- Creswell, J. W. (2013). Qualitative inquiry and research design: Choosing among five approaches (3rd ed.). SAGE Publications.
- Dudek, Debra & Johnson, Nicola. (2011). Return of the Hacker as Hero: Fictions and Realities of Teenage Technological Experts. *Children's Literature in Education.* 42. 184-195. 10.1007/s10583-011-9137-0.
- Creswell, J. W., & Poth, C. N. (2018). Qualitative inquiry and research design: Choosing among five approaches (4th ed.). SAGE Publications.
- Dukes, S. (1984). Phenomenological methodology in the human sciences. Journal of Religion and Health, 23(3), 197-203.
- Edwards, L., Kontostathis, A. E. & Fisher, C. (2016). Cyberbullying, race/ethnicity and mental health outcomes: A review of the literature. *Media* and Communication, 4(3), 71-78.
- Erbiçer, E. S. (2020). Investigation of Cyberbullying and Cyber Victimization in Relation to Social Cohesion and Some Demographic Variables. Pamukkale University Journal of Education, 49, 190-222. https://doi.org/10.9779/pauefd.559831
- Finlay, L. (2014). Engaging phenomenological analysis. Qualitative Research in Psychology, 11(2), 121-141.
- Floros G.D, Siomos K.E, Fisoun V, Dafouli E. and Geroukalis D.(2013). Adolescent online cyberbullying in Greece: The impact of parental online security practices, bonding, and online impulsiveness. *J Sch Health*. *83*(6):445-53. doi: 10.1111/josh.12049. PMID: 23586890.
- Franke, U. & Brynielsson, J. (2014). Cyber situational awareness A systematic review of the literature. *Computers & Security.* 46. 10.1016/j.cose.2014.06.008.
- Frechette, J., Bitzas, V., Aubry, M., Kilpatrick, K., & Lavoie-Tremblay, M. (2020). Capturing Lived Experience: Methodological Considerations for Interpretive Phenomenological Inquiry. *International Journal of Qualitative Methods*, 19. https://doi.org/10.1177/1609406920907254
- Groenewald, T. (2004). A phenomenological research design illustrated. International Journal Of Qualitative Methods, 3(1), 42-55.
- Husserl, E. (1931). *Ideas: General Introduction to Pure Phenomenology* (W. R. Boyce Gibson, Trans.). George Allen & Unwin. (Original work published 1913)
- International Telecommunication Union, (ITU). (2018). Global Cybersecurity Index 2018. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
- Juvonen, J., & Gross, E. F. (2008). Extending the School Grounds? Bullying Experiences in Cyberspace. Journal of School Health, 78(9), 496-505. doi: 10.1111/j.1746-1561.2008.00335.x. PMID: 18786042.
- Kirwan, G. (2010a). Cyberpsychology: an overview of emerging research in emerging environment. Ir J Psychol, 1(2), 69–84. https://doi.org/10.1080/03033910.2010.10446324
- Kirwan, G. (2010b). Cyberpsychology. The Irish Journal of Psychology, 31(1-2), 69-84.
- Kowalski, R.M., Limber, S.P., & Agatston, P.W. (2012). Cyberbullying: Bullying in the digital age. West Sussex: John Wiley & Sons.

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. SAGE Publications.

- Machimbarrena, J. M., Calvete, E., Fernández-González, L., Álvarez-Bardón, A., Álvarez-Fernández, L., & González-Cabrera, J. (2018). Internet risks: An overview of victimization in cyberbullying, cyber dating abuse, sexting, online grooming, and problematic internet use. *International Journal of Environmental Research and Public Health*, 15(11), 2471. https://doi.org/10.3390/ijerph15112471.
- Mason K. L. (2008). Cyberbullying: A preliminary assessment for school personnel. *Psychology in the Schools*, 45(4), 323–348.
- Merriam, S. B. (2009). Qualitative research: A guide to design and implementation (2nd ed.). Jossey-Bass.
- Miles, M., & Huberman, A. (2014). Qualitative Data Analysis (2nd ed.). London: Sage.
- Ministry of National Education (MEB). (2024). Technology and Education from the Perspective of Teachers on the 100th Anniversary of the Republic: Regional Workshop Report. MEB Publications. Retrieved from https://ttkbyayin.meb.gov.tr/yayin/199
- Ministry of Transport and Infrastructure. (2020). National Cybersecurity Strategy and Action Plan, 2020-2023. Retrieved from https://cbddo.gov.tr/siber-guvenlik-stratejisi/
- Moore, T. (2010). The Economics of Cybersecurity: Principles and Policy Options. *International Journal of Critical Infrastructure Protection*. 3. 103-117. 10.1016/j.ijcip.2010.10.002.
- Moustakas, C. (1994). Phenomenological research methods. SAGE Publications, Inc., https://doi.org/10.4135/9781412995658
- Muniandy, L., Muniandy, B. & Samsudin, Z. (2017). Cyber Security Behaviour among Higher Education Students in Malaysia. *Journal of Information Assurance & Cybersecurity*. 1-13. 10.5171/2017.800299.
- Oriol, X., Varela, J., & Miranda, R. (2021). Gratitude as a Protective Factor for Cyberbullying Victims: Conditional Effects on School and Life Satisfaction. *International Journal of Environmental Research and Public Health*, *18*(5). https://doi.org/10.3390/ijerph18052666
- Öztürk, E., Ateş, A., & Erdoğan, B. (2020). Legal aspects and psychological dynamics of cyber crimes. In E. Öztürk (Ed.), Cyber Psychology (1st ed., pp. 48-55). Ankara: Türkiye Klinikleri.
- atchin J. W. & Hinduja S. (2015). Measuring cyberbullying: Implications forresearch. Aggression and Violent Behavior, 23, 69-74.
- Patton, M. Q. (2002). Qualitative research and evaluation methods (3rd ed.). SAGE Publications.
- Polkinghorne, D. E. (1989). Phenomenological research methods. In R. S. Valle & S. Halling (Eds.), *Existential-phenomenological perspectives in psychology* (pp. 41-60). Springer.

120

- Rahman, N. A., Sairi, I. H., Zizi, N. A., & Khalid, F. (2020). The importance of cybersecurity education in school. International Journal of Information and Education Technology, 10(5), 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393
- Reips, U.-D. (2002). Standards for Internet-based experimenting. Experimental Psychology, 49(4), 243-256.
- Rigby, K. (2003). Consequences of bullying in schools. The Canadian Journal of Psychiatry, 48, 583-590.
- Saldana, J. (2016). The coding manual for qualitative researchers (3rd ed.). SAGE Publications.
- Saltik, R. (2021). *The* memory of happiness in the age of cyberpsychology: The transformation of experienced happiness on social media (Unpublished doctoral dissertation). Marmara University, Institute of Social Sciences, Istanbul.
- Schneier, Bruce. (2010). Schneier on Security: Privacy and Control. Journal of Privacy and Confidentiality. 2. 10.29012/jpc.v2i1.579.
- Seidman, I. (2019). Interviewing as qualitative research: A guide for researchers in education and the social sciences (5th ed.). Teachers College Press.
- Singh, A. (2019). The Internet of Things (IoT) and Cyber Security. Available at SSRN: https://ssrn.com/abstract=3399641 or http://dx.doi.org/10.2139/ssrn.3399641
- Slonje, R., & Smith, P. K. (2008). Cyberbullying: Another main type of bullying?. Scandinavian Journal Of Psychology, 49(2), 147-154.
- Smith, J. A., & Shinebourne, P. (2012). Interpretative phenomenological analysis. In H. Cooper (Ed.), APA handbook of research methods in psychology, Vol 2: Research designs (pp. 73-82). American Psychological Association.
- Şahin, M. (2012). The relationship between the cyberbullying/cybervictmization and loneliness among adolescents. Children and Youth Services Review, 34(4), 834-837.
- The British Psychological Society, (2019). Cyberpsychology section. https://www.bps.org.uk/member-networks/cyberpsychology-section
- UNESCO. (2021, October). Tackling cyberbullying and other forms of online violence involving children and young people. https://unesdoc.unesco.org/ark:/48223/pf0000379486
- UNICEF (2019). Safer Internet Day: UNICEF calls for concerted action to prevent bullying and harassment for the over 70 per cent of young people online worldwide. https://www.unicef.org/pacificislands/press-releases/safer-internet-day-unicef-calls-concerted-action-prevent-bullying-and-harassment
- Taştekin, E., & Bayhan, P. (2018). Examining Cyberbullying and Victimization Among Adolescents. Online Journal of Technology Addiction and Cyberbullying, 5(2), 21-45.
- Tracy, S. J. (2010). Qualitative quality: Eight "big-tent" criteria for excellent qualitative research. Qualitative Inquiry, 16(10), 837-851.
- Turkish Statistical Institute. (2023). Survey on Information and Communication Technology (ICT) Usage in Households and by Individuals. https://data.tuik.gov.tr/Bulten/Index?p=Survey-on-Information-and-Communication-Technology-(ICT)-Usage-in-Households-and-by-Individuals-2023-49407&dil=2
- Turkish Statistical Institute. (2024). Survey on Information and Communication Technology (ICT) Usage in Households and by Individuals, 2024.https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2024-5342#:~:text20g%C3%B6zlendi
- Voiskounsky, A. (2021). Teaching cyberpsychology: Today and tomorrow. IMS 2021-International Conference "Internet and Modern Society", June 24-26, 2021, St. Petersburg, Russia.
- Whitty, M. T., & Young, G. (2016). Cyberpsychology: The study of individuals, society and digital technologies. John Wiley & Sons.
- Wolfsberg, J. (2006). Student Safety from Cyberbullies, in Chat Rooms, and in Instant Messaging. *Education Digest: Essential Readings* Condensed for Quick Review. 72.
- Ybarra M. L. & Mitchell K. J. (2004). Youth engaging in online harassment: associations with caregiver–child relationships, Internet use, and personal characteristics. *Journal of Adolescence*, 27(3), 319–336.
- Van Manen, M. (2016). Researching lived experience: Human science for an action sensitive pedagogy (2nd ed.). Routledge.

Yıldırım, A., & Şimşek, H. (2021). Qualitative Research Methods in the Social Sciences (12th ed.). Seçkin Publishing.

Appendix I

Table 2. Expanded Chain of Evidence

Themes	School	Teacher	The Direct Quotes
	Administrator		
1.Fraud (n=22)	A13, A11,	T103, T104,	A13 described, "Tricking people to join something by force." A11 shared, "I have fraud from my neighbours." A15 mentioned, "A male impersonating a
	A15, A22	T126, T135,	different profile to trick female students." A22 recounted, "Students engaging with strangers on social media and being tricked." T103 provided an example,
		T109, T110,	"One of my students was pressured to pay for a game they didn't even play." T104 noted, "Our students have faced scams on social media." T126 reported,
Asking for		T113, T11,	"Email accounts were hacked." T135 pointed out, "During online classes, some students were financially scammed." T109 detailed, "Clicking on links in
money,		T118, T119,	messages led to scams." T11 explained, "Pretended to be a friend in messages to get them to click on links." T118 remarked, "People are pressured into
		T147, T142,	conforming to beauty standards." T119 described, "My friend's Instagram account was hacked, and messages were sent in their name asking for money."
Transferring		T153, T158,	T147 reported, "Social media accounts were taken over." T142 shared, "My social accounts were stolen. I faced scams on social media." T153 described,
Money to		T154, T159,	"Children of my acquaintances were pressured through online games." T154 narrated, "A phone number was cloned, and the line was used without
Account Without		T162, T172	permission." T159 revealed, "Parents reported financial scams during online lessons." T162 mentioned, "A 10-year-old boy received inappropriate messages
Authorization			through Instagram." Finally, T172 spoke of, "A friend's private account content was misused."
2.Hacking (n=29)	A33, A34,	T181, T182,	A33 shared, "Our school database was accessed without permission." A34 recounted, "Emails were hacked, and sensitive information was leaked." A48
	A48, A56,	T183, T188,	mentioned, "I was a victim of hacking, and my account was used to spread false information." A56 stated, "Several students had their social media accounts
	A50, A55	T19, T190,	compromised." A50 explained, "A friend's phone was hacked, and messages were sent pretending to be them." A55 described, "My banking app was
Account Stealing,		T185, T2,	accessed, and transactions were attempted." T181 reported, "Our systems were attacked, leading to a data breach." T182 noted, "Unauthorized login
		T34, T27,	attempts were frequent in our institution." T183 mentioned, "Hackers manipulated the school website to spread misinformation." T188 shared, "Someone
Acquisition of		T22, T24,	gained control of my friend's account and posted offensive material." T19 revealed, "My account was used by someone else to harass others." T190
Personal		Т32, Т33,	described, "Phishing emails led to multiple students losing their credentials." T185 explained, "The class notes system was hacked and rendered unusable."
Information,		T43, T45,	T2 reported, "I received a message saying my personal information was leaked." T34 stated, "People were tricked into providing passwords through fake
		T3, T55,	websites." T27 shared, "My friend's account was used to promote scams." T22 mentioned, "Unauthorized parties accessed and shared my photos." T24
Fake Account		Т66, Т7,	noted, "Hackers created fake profiles of our colleagues." T32 explained, "My student's email was hacked, and inappropriate content was sent.". T33 shared
		T67, T64,	"My close friend private video was hacked from phone. She lived many bad things socially ".T43 reported, "A social media account was taken over and
		T88	used for spam." T45 described, "Hackers posted private conversations publicly." T3 mentioned, "Our student's dad's work server was attacked, and they
			lost all data." T55 explained, "My colleague's laptop was hacked during an online class." T66 shared, "Hacking groups targeted our school's systems." T7
			stated, "Someone impersonated me online, causing misunderstandings." T67 mentioned, "Hackers sent fake emergency alerts to everyone." T64 described,
			"Private images were accessed and distributed without consent." . T88 noted, "Hackers used malicious software to gain access to our devices."
3.Violation of	A58, A1,	T1, T33,	A58 stated, "Photos of students were taken without permission and posted online." A1 described, "A close friend's private information was leaked on social
Privacy (n=30)	A10, A17,	T80, T78,	media." A10 recounted, "Sensitive videos were shared publicly, causing immense distress." A17 explained, "Gaming platforms have become places where
	A19, A21	T83, T93,	people demand private images." A19 shared, "Someone requested personal photos and later distributed them without consent." A21 noted, "Teachers'
		T94, T105,	personal information was made public, creating fear." T80 described, "Topless photos of students were circulated among strangers." T78 mentioned,
Private parts		T106, T102,	"Private conversations were made public, causing embarrassment." . T83 reported, "Someone took pictures of students in the locker room without consent."
without their		T10, T100,	T93 stated, "Hacked accounts were used to expose personal messages." T94 shared, "Girls were blackmailed with their own photos." T105 noted, "A student
consent,		T101, T132,	was threatened with a video taken secretly." T106 recounted, "Explicit images were sent to me without consent." T102 explained, "Private documents of
		T107, T108,	my neigbour were accessed and used to harass them.". T1 stated, "My private information was displayed online after my account was hacked." T10
Sexual		T111, T112,	mentioned, "Unauthorized sharing of my images led to severe anxiety." T100 reported, "A student group posted private pictures on a social platform.", T33
Harassment		T114, T120,	adds, " My close friend private video was hacked from phone. She lived many bad things socially" T101 described, "A family's private life was exposed
		T121, T122,	online, causing humiliation." T132 stated, "My student's diary entries were published on the internet without her knowledge." T107 shared, "Someone
		T123, T166	accessed our school records and shared grades publicly." T108 noted, "My address and phone number were leaked." T111 explained, "Private photos of

Kastamonu Education Journal, 2025, Vol. 33, No. 1

122			
		T124 T125	students were edited and distributed." T112 described, "A student was harassed with private details of their home life." T114 shared, "Social media was used to expose secrets between my students." T120 noted, "Our teachers' confidential files were accessed and shared widely." T121 mentioned, "Private pictures of my relative were manipulated and used for cyberbullying." T122 described, "Messages containing private information were spread without consent several times". T123 stated, "Someone hacked into my account and shared personal information without permission." T166 recounted, ""A student was threatened that embarrassing photos would be spread throughout the school. He was ashamed and afraid. That's why he needed psychological support. This is a huge negative social impact for children in the country."
4.Verbal Insult	A14, A2,	T124, T125,	A14 shared, "My students often use offensive language towards each other in the classroom, and it goes to the social media sharings and sometimes
(n=31)	A16, A18, A20, A26	T127, T128, T129, T133,	among teacher groups on social media". A2 stated, "Verbal abuse has become a daily issue among my students and We hear that students continue their activities in groups they have established among themselves." A16 mentioned, "I witnessed students provoking each other with harsh words online." A18
	A20, A26	T129, T133, T134, T136,	explained, "My son has been insulted multiple times through social media." A20 described, "Online platforms are full of verbal harassment and derogatory
Swearing,		T137, T138,	comments." A26 noted, "Even teachers are not spared online platforms from verbal attacks like students" T124 recounted, "A student was called
Verbal abuse,		T139, T116, T117, T13,	derogatory names and made fun of for their appearance." T125 shared, "Even chat groups are filled with offensive and degrading language." T127 stated, "Online insults are often used to intimidate classmates." T128 explained, "Verbal harassment escalates to bullying quickly." T129 described, "Hurtful
verbar abuse,		T130, T14,	comments in class and chat group were made about a student's family. We know these have a psychological effect on him. We understood that he felt
Provocation		T140, T141,	excluded. He preferred to be quiet and stand on the sidelines." T133 mentioned, "In chat group, I was mocked for my academic performance." T134
		T148, T149,	reported, "Offensive words were used to humiliate students during online classes." T136 shared, "Teasing and name-calling have caused emotional distress
		T150	for many." T137 noted, "I heard students using derogatory language towards teachers in chat groups." T138 stated, "A classmate made fun of another
			student's disability on social media. Human can be unmerciful." T139 explained, "Verbal insults are so common that students feel unsafe." T116 described,
			"My friends and I have been threatened and insulted repeatedly via chat." T117 reported, "A teacher was verbally abused by students online." T13
			mentioned, "I was called names that hurt my self-esteem." T130 stated, "Hateful language was used to attack a student's gender identity." T14 explained,
			"A student was ridiculed in chat group. The family came to the school, complained to the administration.
			." T140 described, "Public online shaming and verbal insults have led to fights in school." T141 noted, "Swearing is rampant in our chat groups." T148
			mentioned, "Online argument turned into a stream of insults and threats." T149 reported, "Students use profane language to express anger in online
		T45 T440	groups." T150 shared, "Verbal harassment on social media in our school is a serious issue"
5.Blackmail	A23, A24,	T15, T143,	A23 shared, "Someone threatened to release private photos if I didn't comply with their demands." A24 stated, "My friend was blackmailed with messages
(27)	A27, A28, A29, A31	T144, T145, T146, T152,	revealing secrets they wanted to keep hidden." A27 recounted, "I was forced to do favors for someone, or they would share private screenshots. I was very scary and nervous. It took long time to heal. I couldn't tell to my family". A28 explained, "A student was blackmailed into sending money through
	A29, A31	T146, T152, T151, T155,	threats." A29 mentioned, "People use blackmail to manipulate others into doing what they want." A31 described, "Photos were edited to make them look
S/he is forced		T151, T155, T156, T157,	compromising and used to blackmail me." T15 stated, "A student was coerced into sharing exam answers under threat." T143 noted, "A hacker threatened
to do		T174, T178,	to expose private conversations if we didn't pay." T144 recounted, "Girls in our class were blackmailed with fake, compromising photos." T145 explained,
whatever he		T168, T169,	"Someone used a deepfake video to blackmail my friend." T146 shared, "I had to obey demands because they had evidence of a personal matter." T152
wants with		T160, T161,	described, "A boy was blackmailed into sharing money after private details were exposed." T151 mentioned, "Photos stolen from a hacked account were
the data s/he		T163, T170,	used to threaten someone." T155 stated, "A girl was forced to send more private pictures to avoid public exposure." T156 explained, "Blackmail through
has		T18, T180,	social media is common; even teachers have been affected." T157 noted, "A student had to withdraw from sports because of blackmail threats." T174
		T17	shared, "Threats involving personal secrets have become a way to gain power over others." T178 described, "Someone threatened to reveal confidential medical records." T168 explained, "A group of boys blackmailed a classmate into doing their assignments." T169 stated, "They use personal information from hacked accounts to demand money." T160 shared, "Threats about posting private messages publicly were used to intimidate." T161 noted, "I was blackmailed with a fabricated story that could ruin my reputation." T163 mentioned, "Someone recorded a private conversation and used it to make demands." T170 described, "Financial blackmail is becoming a growing problem in our school." T18 stated, "My student was forced into doing errands for others to keep their secret safe." Finally, T180 shared, "A teacher's private life was exploited through blackmail by students." T17 explained, "Hacked information was used to manipulate my decisions."

			125
6.Threatening	A32, A3,	T173, T175,	A32 described, "I was threatened online with messages saying they would ruin my reputation." A3 stated, "Threats of physical violence were made towards
(n=27)	A30, A35,	T176, T177,	my friend if they didn't comply." A30 recounted, "Someone threatened to expose my private conversations to everyone." A35 explained, "I received
	A36	T179, T164,	messages saying I would be harmed if I didn't follow their instructions." A36 mentioned, "Students use threats to intimidate each other into doing things
		T165, T166,	they don't want to." T173 shared, "A student was excluded from all social groups and threatened with worse if they told anyone." T175 stated, "Someone
		T167, T171,	threatened to share secrets if they weren't given money." T176 noted, "Boys in my class threatened a girl if she didn't stop talking to certain friends." T177
Exclusion,		T187, T189,	explained, "There were threats of failing grades if someone didn't provide answers on a test." T179 described, "Threatening messages about being
		T184, T186,	physically harmed were sent to a student." T164 shared, "My principal was threatened with harm if they reported a student's behavior." T165 noted, "A
Comments		T191, T192,	student threatened to damage school property as revenge." T166 recounted, ""A student was threatened that embarrassing photos would be spread
indicating that		T51, T21,	throughout the school. He was ashamed and afraid. That's why he needed psychological support. This is a huge negative social impact for people in the
he/she will do		T31, T33,	country." T167 explained, "Someone said they would make life unbearable for another student if they didn't leave a group chat." T171 described, "Threats
evil,		T42, T46	about harming family members were used to control students." T187 stated, "Our teacher received anonymous threats through email." T189 shared, "I
			heard a student say they would attack another if they didn't get what they wanted." T184 mentioned, "Threats to spread rumors were made if demands
			weren't met." T186 explained, "A student was threatened with having all their secrets exposed to teachers." T191 noted, "A student was afraid to come
			to school because of threats made on social media." T192 shared, "There are a few students in our school. Threats of being expelled from groups were
			used to isolate students." T51 described, "There were threats to damage personal belongings if someone spoke up." T21 explained, "Threats about hacking
			into accounts were made to scare people." T31 shared, "A teacher was threatened with lawsuits for disciplining a student." T33 shared" my best friend
			had a lot of problems with her phone being stolen from her private video. she socially withdrew from society. She received inappropriate proposals and
			threats after her video went viral. She had a lot of psychological problems. She started to receive psychological support." T42 stated, "Someone threatened
			to share false information about me.". T46 described, "A student was threatened with expulsion if they didn't stop reporting issues."
7.Psychological	A17, A27	T101, T142,	A17 discussed issues related to digital safety among teenagers, emphasizing the risk of exclusion in social settings. A27 recounted, "I was forced to do
Violence (n=21)		T143, T144,	favors for someone, or they would share private screenshots. I was very scary and nervous. It took long time to heal. I couldn't tell to my family" T101
		T145, T146,	revealed, ""A family's private life was exposed online, causing humiliation.". T127 stated, "Insults are often used to intimidate classmates." T128 explained,
		T147, T148,	"Verbal harassment escalates to bullying quickly." T129 described, "Hurtful comments were made about a student's family. We know that hurtful
Humiliation,		T166, T190,	comments about his family have a psychological effect on him. We understood that he felt excluded. He preferred to be quiet and stand on the sidelines.".
		T191, T192,	T142 stated, "My social accounts were hacked. Humiliation and threats are more common on social media. Bullying can occur through photo manipulation
Ridicule,		T32, T127,	or publishing altered images to ridicule victims." T143 mentioned, "Social media," referencing cases where exclusion from groups has been observed. T144
		T33, T34,	described, "A social media account was hacked, and the hacker contacted friends to commit fraud, forcing victims to engage in activities they did not
Exclusion,		T49, T99,	consent to, similar to coercion." T145 reported, "The misuse of a hacked social media account often leads to humiliation." T146 said, "The hacking of a
		T129	social media account can result in severe exclusion from peer groups." T147 noted, "Social media accounts have been seized, which is a form of exclusion
Pressure			from online communities." T148 explained, "There are many seemingly innocent dangers on social media, in SMS messages, and in internet advertisements.
			People of all ages who lack adequate information and life experience can easily fall victim to this bullying, often involving humiliation or exclusion.
			Unfortunately, it is harder to provide a solution than to prevent it beforehand. People need to be informed before they are exposed." T166 recounted, ""A
			student was threatened that embarrassing photos would be spread throughout the school. He was ashamed and afraid. That's why he needed psychological
			support. This is a huge negative social impact for people in the country.". T190 remarked, "Insults and threats can lead to humiliation." T191 shared, "My
			student was blackmailed and threatened after their private images were shared on social media, causing significant humiliation.". T192 shared, "There are
			a few students in our school. Threats of being expelled from groups were used to isolate students." T32 stated, "Students can use each other's photos for
			threats, which creates fear and humiliation." T33 shared" my best friend had a lot of problems with her phone being stolen from her private video. she
			socially withdrew from society. She received inappropriate proposals and threats after her video went viral. She had a lot of psychological problems. She
			started to receive psychological support." T34 said, "A student was threatened and harassed on social platforms, resulting in a sense of exclusion." T49
			shared, "I know cases of threats, insults, humiliation, and fraud." T99 noted, "Incidents of insults, threats, and humiliation occur among students, often
			leading to social exclusion."