Journal of Learning and Teaching in Digital Age, 2023, **8**(1), 55-70
https://dergipark.org.tr/en/pub/joltida
ISSN: 2458-8350 (online)

Research Paper

An Examination of the Relationship between College Students' Cyberbullying Awareness and Ability to Ensure their Personal Cybersecurity

Eyup Zorlu*[a]

[a](ORCID ID: 0000-0003-0964-7065), Bartın University, eyup.zorlu1982@gmail.com
*Corresponding author

ARTICLE INFO
Received: 14 March 2022
Revised: 10 October 2022
Accepted: 26 October 2022

Keywords:
Cybersecurity
Cyberbullying
College Students
Awareness

doi: 10.53850/joltida.1087377

ABSTRACT
The purpose of this study is to examine the relationship between college students' cyberbullying awareness and their ability to ensure their personal cybersecurity. A total of 401 students participated in this study. The Ability to Ensure Personal Cybersecurity Scale, the Cyberbullying Awareness Scale, and a Personal Information Form developed by the researcher were all used during data collection. A relational screening model was used in this study. Also, an unpaired t-test, one-way analysis of variance (ANOVA), and Pearson's correlation coefficients were utilized during data analysis. Study results revealed that college students are highly capable of ensuring their personal cybersecurity and possess high levels of cyberbullying awareness, that female students possess significantly higher levels of cyberbullying awareness compared to male students, and that there is a moderate, positive correlation between college students' cyberbullying awareness and their ability to ensure their personal cybersecurity. Also, college students' levels of cyberbullying awareness vary based on their reasons for using the internet and their propensity towards both online catfishing and cyberbullying others. Furthermore, college students' ability to ensure their personal cybersecurity was similarly found to differ based on their reasons for using the internet, the degree to which they had been exposed to cyberbullying, and their propensity toward online catfishing.

INTRODUCTION

In today's world, where new technological developments are a daily occurrence and the internet, mobile devices, and computers are becoming more ever more advanced, it is nearly impossible to remain unplugged and stay away from technology. People who have had to spend most of their time at home due to the COVID-19 pandemic, which emerged in December 2019 in Wuhan, China and has spread throughout the entire world, use technology for various activities such as online shopping, research, visiting social networks, and watching movies. A report (2021) by a creative agency called We Are Social revealed that 5.22 billion people (66.6%) of the world's population, which consists of nearly 7.83 billion people, are mobile phone users, 4.66 billion (59.5%) are internet users, and 4.2 billion (53.6%) are social media users and also touched on how these numbers are increasing day by day. The most striking matter discussed in the report is the fact that worldwide, the average amount on time spent online amounts to seven hours per day. In the same report, the number of internet users in Turkey was reported as 65.8 million, while 60 million were found to actively use social media. The average daily internet use in Turkey was found to be eight hours per day, higher than the worldwide average. According to a Household Use of Information Technologies study (2021) conducted by TURKSTAT (Turkish Statistical Institute), the percentage of internet users for 17 to 74-year-olds in Turkey was found to be 82.6%. Based on users' sex, this rate was found to be 87.7% for male users and 77.5% for female users. It was also found that the rate of household internet access reached 92%, while the rate of consistent internet usage hit 80.5%.

Relevant sets of digital data show that the increase in the use of technology over the years, the active, worldwide use of virtual worlds by a variety of age groups, informatics systems, technological advancements, and the convenience of many technological devices (smart phones, computers, tablets etc.) have become indisputable facts of life (Batmaz and Ayas, 2013:44; Peker, 2019:345; Şenol, 2017:1). Several factors such as the boundless opportunities offered in digital environments, the ability to infinitely surf the web, the ability to easily access information, the opportunity to become famous in a short amount of time, and the feeling of comfort and confidence while freely stating opinions online have created a new concept known as online disinhibition. Even though this restriction-free environment has some advantages, it also comes with several problems caused by users' insensitive and obtuse posts (Aktan and Çakmak, 2015:16; Suler, 2004:321; Yavanoğlu, Sağıroğlu and Çolak, 2012:15).

These problems include humiliation, ostracization, real-life threats carrying over into digital environments (Bayram and Saylı, 2013), security issues, privacy violations, cyber threats (Karaoğlan Yılmaz, Yılmaz and Sezer, 2014:177; Şenol, 2016: 11), inappropriate websites (promoting the use of drugs and/or glorifying violence), fraud, sexual harassment-related content (child pornography) (Eroğlu and Güler, 2015:119), theft, fake accounts, terrorist propaganda and other felonious material (Hekim and Başıbüyük, 2013:136), video game and internet addiction, access to inaccurate information and/or harmful content on the internet

as well as activities associated with violence, hate speech, and/or racism (Çubukçu and Bayzan, 2013:4), and malware such as Trojan horse viruses, spyware, computer worms, and many other types of viruses (Öğün and Kaya, 2013:151).

The fact that these problems have been encountered all over the world has turned them into a universal matter of concern (Baştürk and Sayımer, 2017: 2; Pekşen, Süslü, and Oktay, 2018: 1880). People expressing their emotions, thoughts, and views in digital environments may cause those who disagree to display adverse reactions such as anger, aggression, instances of hate speech, and racist language; anger and aggression in particular have recently become significantly more noticeable in virtual and digital worlds (Kozan and Bulut Özek, 2019:108). The virtual conveyance of such feelings by ill-intentioned people to the innocent or vulnerable via messages, videos, or emails has led to the emergence of a relatively new concept in the literature: cyberbullying.

The term cyberbullying was coined by a Canadian educator, Bill Belsey, in the early 2000s, and it has since become the subject of many studies (Yaman, Karakülah, and Dilmaç, 2013). Cyberbullying is also known as digital bullying, online bullying, electronic bullying (Kowalksi and Limber, 2007), mobile phone bullying, and internet bullying (Tamer and Vatanartıran, 2014:4) in the relevant literature. Cyberbullying can be exposed and detected by checking bullies' computer systems, mobile phones and/or other technological devices (Patchin and Hinduja, 2006:148; Peker and Ekinci, 2016:2127; Price and Dalgleish, 2010:51; Smith and Ananiadou, 2003:189), emails, personal websites, blogs, discussion forums, social networks, text and video messages, and/or instant messages (Belsey, 2021; Gökçe Turan, 2021:114; Peker and Ekinci, 2016:2128; Smith et al., 2008:376). There are many definitions of cyberbullying in the relevant literature as researchers have failed to agree on a single definition.

Lacey (2007) states that cyberbullying is an exhibition of violence and aggression in social contexts over various communication mediums, while Willard (2007) defines it as a body of misbehaviors that manifest themselves through sending or posting inflammatory content to others using technologies such as computers, smartphones, and the internet. Smith et al. (2008) identifies it as a set of aggressive actions performed multiple times by a single person or a group of people using communication technologies against those who have difficulty defending themselves. Cyberbullying is also defined as "a set of intentional, consistent, and hostile behaviors exhibited by a single person or a group of people to hurt others using information and communication technologies" (Belsey, 2021; Price and Dalgleish, 2010:51). Taking these definitions into account, it is evident that cyberbullying is, by its very nature, performed using communication technologies, contains intentional and hostile behaviors, aims to hurt and harm others, and targets vulnerable people.

Analysis of the characteristics of cyberbullying reveals that regardless of their physical strength, an individual can turn into a cyberbully as long as they have enough knowledge about digital environments (Patchin and Hinduja, 2006) and can easily victimize the gullible and/or those who lack situational awareness. In addition, a victim of cyberbullying can be bullied online regardless of time and place and can also receive distressing text messages and emails at any time (Kowalski and Limber, 2007:23; Patchin and Hinduja, 2006:150; Slonje and Smith, 2008:148). Moreover, cyberbullying can affect larger numbers of people when compared to traditional bullying, where the number of bystanders is smaller. For instance, when a violent act occurs in a school setting, there might be five or ten people in a classroom or hallway, while a video posted and spread on the internet can be viewed by millions of people (Campbell, 2005:3; Peker and Ekinci, 2016:2127; Slonje and Smith, 2008:148)

Furthermore, while bullies' identities are usually known in traditional bullying, it is easier for cyberbullies to remain anonymous on the internet and social media (Baştürk and Sayımer, 2017: 2; Belsey, 2021; Campbell, 2005:3; Dikmen and Çağlar, 2017:101; Morales, 2011:407; Slonje and Smith, 2008:148; Tamer and Vatanartıran, 2014:4). It should also be kept in mind that the faintest ink is more powerful than the strongest memory. Put another way, even though the victim is subjected to hurtful deeds in traditional bullying, the incident can be forgotten over time. However, insults, distressing content, and/or messages posted by a cyberbully can be viewed dozens of times by the victim in cyberbullying; thus, it may have a larger impact on the victim when compared to traditional bullying (Campbell, 2005:3). When the aforementioned characteristics of cyberbullying are considered as a whole, it is clear that cyberbullying is both detrimental and damaging.

In digital environments, cyberbullying can manifest itself in a variety of different ways: invasion of privacy, insult, assault (Doğan, Çaka, and Şahin, 2016:507; Yavanoğlu, Sağıroğlu, and Çolak, 2012:18), harassment, humiliation, profanity, defamation, sending hurtful or abusive photos and/or messages (Peker and Ekinci, 2016:2128), hate speech (Hanewald, 2008:2), making rude, discouraging, or embarrassing comments (Ybarra and Mitchell, 2004:1308), or even anonymously sending spam emails and/or email viruses (Arıcak et al., 2008:253). While these vulnerabilities and adverse elements of digital environments lower people's trust in virtual mediums, it becomes evident that necessary precautions must be taken to prevent cyberbullying.

The number of cyber threats increases at the same rate as the rapid advancement of technology that has little to no restrictions on usage. Vulnerabilities become more prominent in these platforms as there is a lack of proper personal information security, determination of legal boundaries, and web filtering (Avcı and Oruç, 2020:288). Individuals are not well-informed about the risks they may encounter, especially because they use the internet improperly and possess low awareness of threats that target their personal information (Aslankara and Usta, 2018:121; Çam and Aslay, 2019:2; Öğütçü, Testik, and Oumout, 2016:83-84). A study conducted by Öğütçü (2010) showed that people's levels of awareness regarding information security weren't very high. Results from the same study also revealed that individuals haven't developed any behaviors that enabled them to take precautions against cyber threats. In their study, Tekerek and Tekerek (2013) found that participants had very low awareness of matters such as creating strong passwords, malware protections, document protection, safe online communication, security of personal computers, online chat rooms, and general internet safety.

In a study conducted by Erdoğmuş (2017), cybersecurity awareness was found to have the most positive effect on information security awareness among individuals. In addition, another study by Avcı and Oruç (2020) revealed that 92% of students who participated in the study had never received any cybersecurity or information security training.

People usually think that they are completely safe while surfing the internet due to the presence of antivirus software and other protective measures. However, spyware and computer viruses increase the risk of various threats on the internet. Therefore, the need to raise awareness of security and privacy matters takes on renewed urgency. Although it is not at all true to say that users are solely accountable for their own security in digital environments, they have to take precautions in order to protect themselves (Furnell, 2008).

It is important to raise awareness of information security in order to minimize risk factors in digital environments and to ensure that users feel secure (Abawajy, 2012:238; Öğütçü, 2010:1-2; Sasse, Brostoff and Weirich, 2001:122; Yılmaz, Ulus, and Gönen, 2015:143). Much suffering and aggrievement can be prevented by becoming aware of problems with and taking necessary security precautions on digital mediums (Abawajy, 2012:237; Arıcak, Kınay, and Tanrıkulu, 2012; Aslan and Önay Doğan, 2017:105; Doğan, Çaka, and Şahin, 2016:518; Eminağaoğlu and Gökşen, 2009:7; Karaoğlan Yılmaz, Yılmaz, and Sezer, 2014:177; Keser and Güldüren, 2015:1169; Odacı and Çelik, 2018:1176; Önaçan and Atan, 2016:13; Sertçelik, 2015:39; Yenilmez and Seferoğlu, 2013:423) and thusly, individuals can become more conscious of the effects of cyberbullying.

Awareness can be defined as sensitivities developed by an individual that are employed when they come across any potentially unfavorable situations (Bayezid, 2000:100; Bridge and Duman, 2019: 159; Krahé, Möller, Berger, and Felber, 2011; Rohrmann, Netter, Hennig, and Hodapp, 2003, Akt. Tanrıkulu, Kınay, and Arıcak, 2013:40) or as their tendency to avoid or ignore threatening stimuli (Roger and Schapals, 1996). Individuals may face dangerous situations in everyday life as well as in digital environments and may develop sensitivities towards them. Thus, cyberbullying awareness can be defined as "a set of behaviors that keep individuals away from actions which may lead to them being exposed to cyberbullying while using technological devices such as smart phones, enable users to become more aware of cyberbullying threats, help them take precautions against said threats, and ensure that they pay more attention to possible threats" (Tanrıkulu, 2011, Akt., Tanrıkulu, Kınay, and Arıcak, 2013). It is crucial for both individuals and institutions to be well-informed about cybersecurity so that they are conscious of risks they may encounter in digital environments and aware of risks and problems that may occur in said environments. Therefore, it is also important to be familiar with cybersecurity terminology and concepts. In addition, raising cyberbullying awareness will both reduce the risk of people being cyberbullied and prevent others from becoming victims of cyberbullying (Doğan, Çaka, and Şahin, 2016:518).

It is essential to rigorously train new users about online risks, particularly when they first start using digital environments. One study noted that behaviors that constitute risks on virtual media gradually intensify during adolescence between the ages of 15 to 18 and subsequently lessen during the university years when individuals step into young adulthood and levels of awareness increase (Aslankara and Usta, 2020:136). Even though the intensity of cyberbullying depends on age and starts to decrease during the university years, its effects continue to impact individuals who were exposed to it in the past. In Arıcak's study (2009) of college students, it was found that 19.7% of the participants had cyberbullied others at least once in their lives and more than half of the participants (54.4%) had cyberbullied at least once in their lifetime.

Similarly, another study done by Dilmaç (2009) revealed that 22.5% of college students had cyberbullied others while 55.3% stated that they had been cyberbullied at least once in their lifetime. Obviously, the results and data from both Arıcak's and Dilmaç's study paint similar pictures and illustrate the gravity of the situation. College students' ability to ensure their own cybersecurity and their levels of cyberbullying awareness have become an issue of concern during the COVID-19 pandemic even more so than before as they spend more time online consuming entertainment, researching, and using social media. This study examines the relationship between college students' ability to ensure their personal cybersecurity and their cyberbullying awareness.

Purpose and Goals

The main purpose of this study is to examine the relationship between college students' cyberbullying awareness and their ability to ensure their personal cybersecurity. The secondary objective of the study is to answer the questions below:

1. To what extent are college students able to ensure their personal cybersecurity and to what degree are they aware of cyberbullying?
2. Does college students' levels of cyberbullying awareness and their ability to ensure their personal cybersecurity differ significantly based on sex, college grade level, college departments, the amount of time they spend on the internet, their reasons for using the internet, whether or not they employ catfishing, and whether or not they had been cyberbullied and/or have ever cyberbullied others?
3. Is there any statistically significant relationship between college students' ability to ensure their personal cybersecurity and their cyberbullying awareness?

METHOD

Model

A relational screening model, one of the designs used in quantitative research, was used in this study. As the relationship between college students' cyberbullying awareness and their ability to ensure their personal cybersecurity was examined within the purview of this study, a relational screening model was deemed an appropriate way to analyze this relationship. Relational screening models are research models that aim to describe the relevant features of a situation by determining the relationship between specific variables (Karasar, 2003:77).

Population and Sample

The population of this study consisted of a total of 401 undergraduates (301 (75.1%) female and 100 (24.9%) male students), who were selected using a relevant sampling method, studying in a variety of different departments at Bartın University in Turkey during the 2020-2021 academic year.

Table 1. Demographic Profile of the Participants

Demographic Variables of College Students		N	%
Sex	Female	301	75.1
	Male	100	24.9
College Grade Level	Freshman	112	27.9
	Sophomore	70	17.5
	Junior	106	26.4
	Senior	113	28.2
Department	Elementary-Level Mathematics Teacher Education	60	15
	Theology	64	16
	Psychological Counselling and Guidance	225	56.1
	Elementary-Level Classroom Education	21	5.2
	Social Studies Teacher Education	31	7.7
Daily internet use	1-3 hours	106	26.4
	4-5 hours	187	46.6
	6+ hours	108	26.9
Reasons for Using Internet	Study - Research	119	29.7
	Movies – Music - Entertainment	54	13.5
	Social Media	203	50.6
	Keeping up with news and the world	25	6.2
Catfishing	Yes	74	18.5
	No	327	81.5
Being cyberbullied	Yes	140	34.9
	No	261	65.1
Cyberbullying others	Yes	20	5
	No	381	95
Total		401	100

Data Collection Tools

Personal Information Form: In this study, a personal information form was used to collect undergraduate students' demographic data including sex, grade level, and department. The personal information form also contains relevant questions that helped the researcher get more familiar with the participants, such as the amount of time they spend on the internet, their reasons for using the internet, the degree to which they had been exposed to cyberbullying, and their propensity toward online catfishing.

Cyberbullying Awareness Scale

The Cyberbullying Awareness Scale was created by Tanrıkulu, Kınay, and Arıcak (2013). After conducting factor analysis, a scale consisting of one factor that accounts for 46.65% of the total variance was devised. The internal consistency coefficient for the scale was found to be between 0.83 and 0.90, while the split-half reliability coefficient was calculated to be between 0.75 and 0.84. The item-total correlation score of the scale fell between 0.42 and 0.63 for the integrated group; the mean scores of 27% of the upper and lower groups were found to be statistically significant.

The scale consists of 13 items, and scores on the scale vary based on participants' answers: *No* = 1 point, *Sometimes* = 2 points, and *Yes* = 3 points. The lowest score that a participant can get from the scale is 13, while the highest score is 39. The higher the score that a participant gets, the more likely it is that they have higher levels of cyberbullying awareness.

Ability to Ensure Personal Cybersecurity Scale

The Ability to Ensure Personal Cybersecurity Scale was developed by Erol, Şahin, Yılmaz, and Haseski (2015) and consists of 25 items and five sub-dimensions that seek to determine individuals' ability to ensure their own cybersecurity. The sub-scales are Personal Privacy Protection (ten items), Avoiding Unreliable Sources (four items), Prevention and Precaution (five items), Payment Information Security (two items), and Remaining Anonymous (four items). Also, the M6, M8, M13, M14, M18, M19, M20, M21, M25, and M26 items were set as reversed items. Each score that a participant receives by responding each item represents a trait: *Never* = 1, *Rarely* = 2, *Sometimes* = 3, *Often* = 4, *Always* = 5. After conducting a factor analysis, a scale that consisted of five factors was created, and it accounted for 48.026% of the total variance. In order to calculate the internal consistency of the scale, the Cronbach's alpha coefficient (α) was used. It was found to be 0.735 for the entire scale, which has five sub-dimensions, while it was calculated to be 0.763 for the Personal Privacy Protection sub-dimension, 0.771 for the Avoiding Unreliable Sources sub-dimension, 0.704 for the Prevention and Precaution sub-dimension, 0.829 for the Payment Information Security sub-dimension, and 0.557 for the Remaining Anonymous sub-dimension.

Data Collection and Analysis

The scales and the personal information form were posted on Google Forms by the researcher. Prior to the process of answering questions, participants were given a brief rundown and asked to fill out the assessment tools on a volunteer basis. Data gathered from participants' answers was entered into a computer, and SPSS 22.0 (Statistical Package for the Social Sciences) was used to analyze the data set. A relational screening method was used during data analysis. Before conducting data analysis, the data set was tested for normality, and both kurtosis and skewness were found to fall between -2 and +2. Also, the Kolmogorov-Smirnov value was calculated to be $p>0.05$, which indicated that the data is normally distributed.

The independent *t*-test was used to identify statistical differences between two groups, while one-way ANOVA was used while comparing more than two groups. After conducting the one-way ANOVA test on normally distributed data, the Tukey Test, a type of post hoc test, was used to find out which specific groups' means were different. Lastly, correlation analysis was used to determine the relationship between the variables related to sensitivity: the ability to ensure personal cybersecurity and cyberbullying awareness.

FINDINGS

Data obtained from the personal information forms given to students to answer the study question and findings from quantitative data analysis of the scales used in this study are presented in this section.

To what degree are college students who participated in this study aware of cyberbullying (Cyberbullying Awareness Levels – CAL)?

Table 2. Descriptive Data regarding the Cyberbullying Awareness Scale

Sub-dimensions	N	$\overline{X}$	Highest Possible Score	Standard Deviation
CAL	401	33.20	65	3.92

Table 2 contains the means and standard deviations of participants' scores from the CAL scale. The scale, which has a single dimension, consists of 13 items. The highest score a participant can get from the scale is 65.00 while the lowest score is 13.00. The mean and the standard deviation were calculated to be $\overline{X}$= 33.20 and SD=3.92 respectively. Also, the mean was found to be higher

the median (32.50), which indicates that college students who participated in this study possess high levels of cyberbullying awareness.

To what extent are college students who participated in this study able to ensure their personal cybersecurity (Ability to Ensure Personal Cybersecurity – AEPC)?

Table 3. Descriptive Data regarding the Ability to Ensure Personal Cybersecurity Scale and its Sub-dimensions

Sub-dimensions	N	$\overline{X}$	Highest Possible Score	Standard Deviation
Personal Privacy Protection	401	36.34	50	5.51
Avoiding Unreliable Sources	401	16.33	20	3.70
Prevention and Precaution	401	16.00	25	4.06
Payment Information Security	401	8.08	10	2.31
Remaining Anonymous	401	13.46	20	2.66
AEPC TOTAL **Total**	401	90.24	125	10.73

Table 3 contains college students' scores from the Ability to Ensure Personal Cybersecurity Scale as well as means and standard deviations regarding the sub-dimensions of the scale. The Personal Privacy Protection sub-dimension has 10 items, and the highest score a participant can get is 50.00. The mean and the standard deviation of this sub-dimension were found to be $\overline{X}$= 36.34 and SD= 5.51 respectively. The mean of the Personal Privacy Protection sub-dimension is higher than the median (25.00). The second sub-dimension, Avoiding Unreliable Sources, consists of four items, and the highest score a participant can get from this sub-dimension is 20.00. The mean and the standard deviation of this sub-dimension were found to be $\overline{X}$= 16.33 and SD= 3.70 respectively. The mean of the Avoiding Unreliable Sources sub-dimension is higher than the median (10.00). The third sub-dimension, Prevention and Precaution, consists of five items, and the highest score a participant can get from this sub-dimension is 25.00. The mean and the standard deviation of this sub-dimension were found to be $\overline{X}$= 16.00 and SD= 4.06 respectively. The mean of the Prevention and Precaution sub-dimension is higher than the median (12.50).

The fourth sub-dimension, Payment Information Security, contains two items, and the highest score a participant can get from this sub-dimension is 10.00. The mean and the standard deviation of this sub-dimension were found to be $\overline{X}$= 8.08 and SD= 2.31 respectively. The mean of the Payment Information Security sub-dimension is higher than the median (5.00). The last sub-dimension, Remaining Anonymous, consists of four items, and the highest score a participant can get from this sub-dimension is 20.00. The mean and the standard deviation of this sub-dimension were found to be $\overline{X}$= 13.46 and SD= 2.66 respectively. The mean of the Remaining Anonymous sub-dimension is higher than the median (10.00). The highest score a participant can get from the entire scale is 125.00 and the mean and standard deviation of the scale as a whole were found to be $\overline{X}$= 90.24 and SD= 10.73 respectively. The mean of the scale is higher than the median (62.50) which shows that college students are highly capable of ensuring their personal cybersecurity.

Does college students' ability to ensure their personal cybersecurity and their levels of cyberbullying awareness differ significantly based on sex, college grade level, academic department, the amount of time they spend on the internet, propensity toward catfishing, and whether or not they had been cyberbullied and/or cyberbullied others?

The *t*-test was used to analyze whether or not there is a statistically significant difference between both college students' ability to ensure their personal cybersecurity and their levels of cyberbullying awareness and variables such as sex, catfishing, being cyberbullied, and cyberbullying. Results gathered from this analysis are shown in the relevant tables.

Table 4: *t*-Test Results of the Relationship between both Participants' Cyberbullying Awareness Levels (CAL) and their Ability to Ensure Personal Cybersecurity (AEPC) and Sex

Variables	**Sex**	**N**	$\overline{X}$	**SD**	**df**	**t**	**p**	**Cohen's d**
AEPC Total	Male	100	90.36	12.25	399	.121	**.90**	-
	Female	301	90.20	10.20				
CAL Total	Male	100	32.09	5.20	399	-3.529	**.00**	**.40**
	Female	301	33.84	3.95				

Table 4 shows the results from the independent samples *t*-test, which indicate that there isn't any statistically significant difference between the means of the AEPC and sex ($t(399) = .121$, $p>.05$). The mean value for male students ($\overline{X}_{male}$=90.36) was found to be higher than that of the female students ($\overline{X}_{female}$=90.20) in terms of their ability to ensure personal cybersecurity. Results from the independent sample *t*-test also show that there is a statistically significant difference between means of the CAL and sex ($t(399) = -3.529$, $p<.05$). The mean value for female students ($\overline{X}_{female}$=33.84) was higher than that of the male students ($\overline{X}_{male}$=32.09) in terms

of their levels of cyberbullying awareness; that is to say, the significant difference found in the *t*-test favors female students. In addition, the Cohen's d coefficient, which is designed to reveal the effect size of the difference between two groups, indicates that the effect size (0.40) is medium.

Table 5: *t*-Test Results of the Relationship between both Participants' Cyberbullying Awareness Levels (CAL) and their Ability to Ensure Personal Cybersecurity (AEPC) and Catfishing

Variables	Catfishing	N	□	SD	df	t	p	Cohen's d
AEPC Total	Yes	74	85,36	10,21	399	-4,433	**.000**	.57
	No	327	91,35	10,55				
CAL Total	Yes	74	32,45	5,22	399	-2,073	**.039**	**.27**
	No	327	33,61	4,11				

As shown in Table 5, the difference between the means of the AEPC and the catfishing variable was found to be statistically significant ($t(399) = -4.433$, $p<.05$) after conducting the independent samples *t*-test, which shows whether or not college students' ability to ensure their personal cybersecurity is affected by catfishing. Mean values show that students who said *no* ($\overline{X}_{no}=91.35$) when asked whether or not they catfish online were found to have a higher mean than those who said *yes* ($\overline{X}_{yes}=85.36$); the significant difference found in the *t*-test favors the students who said *no*. Also, the Cohen's d coefficient, which is designed to reveal the effect size of the difference between two groups, indicates that the effect size (0.57) is medium. Moreover, the difference between the means of the CAL scale and the catfishing variable was found to be statistically significant ($t(399) = -3.529$, $p<.05$) after conducting the independent samples *t*-test, which shows whether or not college students' levels of cyberbullying awareness is affected by catfishing. Mean values show that students who said *no* ($\overline{X}_{no}=33.61$) when asked whether or not they catfish online were found to have a higher mean than those who said *yes* ($\overline{X}_{yes}=32.45$); the significant difference found in the *t*-test favors the students who said *no*. The Cohen's d coefficient, which is designed to reveal the effect size of the difference between two groups, indicates that the effect size (0.27) is small.

Table 6: *t*-Test Results of the Relationship between both Participants' Cyberbullying Awareness Levels (CAL) and their Ability to Ensure Personal Cybersecurity (AEPC) and Being Cyberbullied

Variables	Being Cyberbullied	N	$\overline{X}$	SD	df	t	p	Cohen's d
AEPC Total	Yes	140	88,04	10,60	399	-3,043	**.003**	.32
	No	261	91,42	10,63				
CAL Total	Yes	140	33,63	4,56	399	-,779	**.436**	**-**
	No	261	33,27	4,24				

Table 6 shows that the difference between the means of the AEPC and the being cyberbullied variable was found to be statistically significant ($t(399) = -3.043$, $p<.05$) after conducting the independent samples *t*-test, which shows whether or not college students' ability to ensure their personal cybersecurity is affected by being cyberbullied. Mean values show that students who said *no* ($\overline{X}_{no}=91.42$) to whether or not they had been cyberbullied were found to have higher mean than those who said *yes* ($\overline{X}_{yes}=88.04$); the significant difference found in the *t*-test favors the students who said *no*. Also, the Cohen's d coefficient, which is designed to reveal the effect size of the difference between two groups, indicates that the effect size (0.32) is medium. Also, the difference between the means of the CAL and being cyberbullied variable was found to be statistically significant ($t(399) = -0.779$, $p>.05$) after conducting the independent samples *t*-test, which shows whether or not college students' levels of cyberbullying awareness are affected by being cyberbullied. Mean values show that students who said *yes* ($\overline{X}_{yes}=33.63$) when asked whether or not they had been cyberbullied were found to have a higher mean than those who said *no* ($\overline{X}_{no}=33.27$).

Table 7: *t*-Test Results of the Relationship between both Participants' Cyberbullying Awareness Levels (CAL) and their Ability to Ensure Personal Cybersecurity (AEPC) and Cyberbullying Others

Variables	Cyberbullying Others	N	$\overline{X}$	SD	df	t	p	Cohen's d
AEPC Total	Yes	20	87,85	10,81	399	-1,025	**.306**	-
	No	381	90,37	10,72				
CAL Total	Yes	20	31,05	4,90	399	-2,494	**.013**	**.57**
	No	381	33,52	4,30				

Table 7 shows that the difference between the means of the AEPC and cyberbullying others variable was found to be statistically significant ($t(399) = -1.025$, $p>.05$) after conducting the independent samples *t*-test, which shows whether or not college students' ability to ensure their personal cybersecurity is affected by cyberbullying others. Mean values show that students who said *no* ($\overline{X}_{no}=90.37$) when asked whether or not they had cyberbullied others were found to have a higher mean than those who said *yes* ($\overline{X}_{yes}=87.85$). Also, the difference between the means of the CAL and cyberbullying others variable was found to be statistically significant ($t(399) = -2.494$, $p<.05$) after conducting the independent samples *t*-test, which shows whether or not college students' levels of cyberbullying awareness are affected by cyberbullying others. Mean values show that students who said *no* ($\overline{X}_{no}=33.52$) to whether or not they cyberbully others were found to have higher mean than those who said *yes* ($\overline{X}_{yes}=31.05$); the significant

difference found in the *t*-test favors the students who said *no*. The Cohen's d coefficient, which is designed to reveal the effect size of the difference between two groups, indicates that the effect size (0.57) is medium.

Descriptive statistics and one-way ANOVA were used while analyzing the effects of college students' grade level, department, daily internet use, and reasons for using the internet on both their ability to ensure personal cybersecurity and their cyberbullying awareness. Also, within the purview of the data obtained from the one-way ANOVA, the Tukey Test, a type of post hoc test, was used to find out which specific groups' means were different with regard to statistically significant sets of data. Findings can be found in relevant tables.

Table 8. Descriptive Statistics regarding Participants' College Grade Level

Variables	**College Grade Level**	**N**	$\overline{X}$	**SD**
AEPC	Freshman	112	90,28	11,47
	Sophomore	70	88,82	8,39
	Junior	106	90,12	10,70
	Senior	113	91,20	11,30
	Total	401	90,24	10,73
CAL	Freshman	112	34,00	4,03
	Sophomore	70	33,52	3,73
	Junior	106	32,68	4,93
	Senior	113	33,40	4,41
	Total	401	33,40	4,35

Table 9. Results from One-Way ANOVA that Shows the Difference Between Participant's College Grade Level and the AEPC and CAL Scales

Variables		Sum of Squares	df	Mean Square	F	p	(Tukey)
AEPC	Between Groups	246,034	3	82,011	0,710	.55	-
	Withins Groups	45632,524	397	115,447			
	Total	46078,559	400				
CAL	Between Groups	95,110	3	31,703	1,677	.17	-
	Withins Groups	7505,44	397	18,905			
	Total	7600,554	400				

Table 9 contains data from one-way ANOVA that shows the difference between participants' college grade level and both the AEPC and CAL scales. There wasn't any statistically significant difference found between participants' college grade level and their ability to ensure their personal cybersecurity (F (3.397) = 0.710; p>.05). Also, no statistically significant difference was found between participants' levels of cyberbullying awareness and their college grade level (F (3.397) = 0.710; p>.05).

Table 10. Descriptive Statistics regarding College Students' Reasons for Using Internet

Variables	**Reasons for Using Internet**	**N**	$\overline{X}$	**SD**
AEPC	I- Study, research	119	92,59	11,41
	II-Film, music, fun	54	90,83	11,13
	III-Social media	194	88,11	9,73
	IV- Keeping up with news and the world	34	93,26	10,94
	Total	401	90,24	10,73
CAL	I- Study, research	119	34,10	4,26
	II-Film, music, fun	54	32,59	4,29
	III-Social media	194	33,48	4,17
	IV- Keeping up with news and the world	34	31,79	5,31
	Total	401	33,40	4,35

Table 11. One-Way ANOVA and Tukey Test Results that Show Differences between College Students' Reasons for Using Internet and Total Scores of AEPC and CAL Scales

Variables		Sum of Squares	df	Mean Square	F	p	(Tukey)
AEPC	Between Groups	1868,29	3	622,766	5,592	**.001**	I>III; IV>III Eta-squared (η2): 0,04
	Withins Groups	44210,26	397	111,361			
	Total	46078,55	400				
CAL	Between Groups	182,71	3	60,905	3,260	**.022**	I>IV Eta-squared (η2): 0,02
	Withins Groups	7417,83	397	18,685			
	Total	7600,55	400				

Table 11 reveals results from one-way ANOVA, which is used to determine whether or not there is a statistically significant difference between college students' reasons for using the internet and the total scores of AEPC and CAL scales. Based on the results, there was a statistically significant difference between college students' reasons for using the internet and their ability to ensure their personal cybersecurity (F (3.397) = 5.592; p<.05). The Tukey test, a type of post hoc test, was used to find out which specific groups' means were different after variances were found to be equal. Based on the Tukey test results, there was a statistically significant difference between the means of participants whose reasons for using the internet is study/research ($\overline{X}$= 92.59) and those who use the internet for social media ($\overline{X}$= 88.11); additionally, college students who said they use the internet for keeping up with news and the world ($\overline{X}$= 93.26) and those who use the internet for social media ($\overline{X}$= 88.11) have significantly different means. Put another way, participants whose reason for using the internet is study/research are more capable of ensuring their personal cybersecurity when compared to those who use the internet for social media. Similarly, participants whose reason for using the internet is keeping up with news and the world are more capable of ensuring their personal cybersecurity when compared to those who use the internet for social media.

The eta-squared (η2) value, which measures effect size, was calculated to be 0.04, which reveals that participants' reasons for using the internet accounts for 4% of their ability to ensure their personal cybersecurity. In addition, there was a statistically significant difference found between participants' levels of cyberbullying awareness and their reasons for using the internet (F (3.397) = 3.260; p<.05). The Tukey test, a type of post hoc test, was used to find out which specific groups' means were different after variances were found to be equal. Based on the Tukey test results, there was a statistically significant difference found between means of participants whose reasons for using the internet are study/research ($\overline{X}$= 34.10) and those who use the internet for keeping up with news and the world ($\overline{X}$= 31.79). The significant difference found in the test favors college students who use the internet for study/research. In other words, students whose reasons for using the internet are study/research possess higher levels of cyberbullying awareness than those who use the internet for keeping up with news and the world. The eta-squared value that measures the effect size was calculated to be 0.02, which reveals that participants' reasons for using the internet accounts for 2% of their levels of cyberbullying awareness.

Table 12. Descriptive Statistics regarding College Students' Departments

Variables	**Department**	**N**	$\overline{X}$	**SD**
AEPC	Elementary-Level Mathematics Teacher Education	60	89,08	10,81
	Theology	64	91,40	12,02
	Psychological Counselling and Guidance	225	90	10,26
	Elementary-Level Classroom Education	21	90,19	9,64
	Social Studies Teacher Education	31	91,87	12,01
	Total	401	90,24	10,73
CAL	Elementary-Level Mathematics Teacher Education	60	33,80	4,15
	Theology	64	33,43	4,48
	Psychological Counselling and Guidance	225	33,16	4,37
	Elementary-Level Classroom Education	21	31,61	4,04

	Social Studies Teacher Education	31	35,48	4,03
	Total	401	33,40	4,35

Table 13. One-Way ANOVA and Tukey Test Results that Show Differences between College Students' Departments and Total Scores of AEPC and CAL Scales

Variables		Sum of Squares	df	Mean Square	F	p	(Tukey)
AEPC	Between Groups	261,83	4	65,45	0,566	.68	-
	Withins Groups	45816,72	396	115,69			
	Total	46078,55	400				
CAL	Between Groups	222, 92	4	55,73	2,991	**.019**	V>III; V>IV Eta-squared (η2): 0,02
	Withins Groups	7377,62	396	18,63			
	Total	7600,55	400				

Table 13 reveals results from one-way ANOVA, which is used to determine whether or not there is a statistically significant difference between college students' departments and the total scores of AEPC and CAL scales. There wasn't any statistically significant difference found between college students' departments and their ability to ensure their personal cybersecurity (F (4.396) = 0.566; p>.05), while there was a statistically significant difference between their cyberbullying awareness and their college departments (F (4.396) = 2.991; p<.05). The Tukey test, a type of post hoc test, was used to find out which specific groups' means were different after variances were found to be equal. Based on the Tukey test results, a statistically significant difference was found between students in the social studies teacher education department ($\overline{X}$= 34.10) and those in the psychological counseling and guidance department ($\overline{X}$= 31.79). Also, there was a statistically significant difference found between students who study social studies teacher education ($\overline{X}$= 34.10) and those who study elementary-level classroom education ($\overline{X}$= 31.79). The significant difference found in the test favors college students who study social studies teacher education. That is to say, students whose department is social studies teacher education possess significantly higher levels of cyberbullying awareness when compared to those who study psychological counseling and guidance and elementary-level classroom education. The eta-squared value (η2) that measures the effect size was calculated to be 0.02, which reveals that participants' reasons for using the internet accounts for 2% of their levels of cyberbullying awareness.

Table 14. Descriptive Statistics regarding College Students' Daily Internet Use

Variables	**Daily Internet Use**	**N**	$\overline{X}$	**SD**
AEPC	1-3 hours	106	90,73	10,39
	4-5 hours	187	90,09	10,63
	6+ hours	108	90,02	11,29
	Total	401	90,24	10,73
CAL	1-3 hours	106	33,09	4,58
	4-5 hours	187	33,18	4,38
	6+ hours	108	34,09	4,05
	Total	401	33,40	4,35

Table 15. One-Way ANOVA and Tukey Test Results that Show Differences between College Students' Daily Internet Use and Total Scores of AEPC and CAL Scales

Variables		Sum of Squares	df	Mean Square	F	p	(Tukey)
AEPC	Between Groups	34,771	2	17,385	0,150	.86	-
	Withins Groups	46043,788	398	115,68			
	Total	46078,55	400				
CAL	Between Groups	70, 605	2	35,302	1,866	.15	-
	Withins Groups	7529,949	398	18,919			
	Total	7600,55	400				

Table 15 reveals results from one-way ANOVA, which was used to determine whether or not there is a statistically significant difference between college students' daily internet use and total scores of AEPC and CAL scales. There wasn't any statistically significant difference found between college students' daily internet use and their ability to ensure their personal cybersecurity (F (2.398) = 0.150; p>.05). Similarly, there wasn't any statistically significant difference between college students' levels of cyberbullying awareness and their daily internet use (F (2.398) = 1.866; p>.05).

Is there a statistically significant relationship between college students' levels of cyberbullying awareness and their ability to ensure their personal cybersecurity?

Pearson's correlation coefficient was used to measure the statistical relationship between college students' levels of cyberbullying awareness and their ability to ensure their personal cybersecurity. Findings obtained from this analysis are shown in Table 16.

Table 16. Pearson's Correlation Coefficient Analysis of the Relationship between College Students' Levels of Cyberbullying Awareness and their Ability to Ensure their Personal Cybersecurity

Variables		AEPC	CAL
AEPC	r	1	,311**
	p		,000
	N		401
CAL	r		1
	p		
	N		
**p<.001			

As shown in Table 16, there is a positive, moderate, and statistically significant relationship (r=0.31, p<.01) between college students' scores from the AEPC and CAL scales. That is to say, as college students' levels of cyberbullying awareness increase, their level of ability to ensure their personal cybersecurity also increases.

DISCUSSION, CONCLUSION and RECOMMENDATIONS

Discussion and Conclusion

This study examines the relationship between college students' levels of cyberbullying awareness and their ability to ensure their personal cybersecurity.

Analysis of the question "*To what degree are college students aware of cyberbullying?"* shows that college students who participated in this study possess high levels of cyberbullying awareness. Results of this study are similar to findings obtained from a variety of studies conducted by Gezgin and Çuhadar (2012), Uysal, Duman, Şahin, and Yazıcı (2014), Aktan and Çakmak (2015), Dikmen and Çağlar (2017), Odacı and Çelik (2018), Kozan and Özek (2019), Bridge and Doğan (2019), Hendekçi and Kadiroğlu (2020), and Gelmez (2020). Similarly, in their study, Uysal, Duman, Şahin, and Yazıcı (2014) found that participants were well aware of the types of cyberbullying they might encounter in digital environments and tend to take necessary measures to ensure their personal cybersecurity against potential cyberattacks.

Also, Odacı and Çelik (2018) noted that participants possess cyberbullying awareness as they were well-informed regarding etiquette in technology; however, Hendekçi and Kadiroğlu (2020) stressed that the main reason why participants develop cyberbullying awareness is because they themselves have been cyberbullied in digital environments. People who spend a significant amount of time online may be cyberbullied more frequently due to the fact that they are unable to know the intentions of the people whom they interact and communicate with. As a result, people learn how to be more cautious in digital environments over the years to protect themselves from such interactions and create an online environment for themselves where they communicate with those whom they know and visit trustworthy websites they are familiar with.

Analysis of the question "*To what extent are college students able to ensure their personal cybersecurity?"* showed that college students are highly capable of ensuring their personal cybersecurity. Results obtained from this study dovetail neatly with results from previous studies conducted by Avcı and Oruç (2020) and Karacı, Akyüz, and Bilgici (2017). Given that college students possess higher levels of awareness and common sense when using the internet (Aslankara and Usta, 2020), it is safe to say that they are well-equipped to ensure their personal cybersecurity. Akgün and Topal (2015) stated that surprisingly, there wasn't any statistically significant difference between participants who attended information security training and those who didn't.

Analysis of the question *"Does college students' ability to ensure their personal cybersecurity and their levels of cyberbullying awareness differ significantly based on sex?"* revealed that college students' levels of cyberbullying awareness significantly differ based on their sex, but there wasn't any statistically significant difference found between college students' sex and their ability to ensure their personal security; the difference regarding levels of cyberbullying awareness favors female students. A close scrutiny of a variety of previous studies in the relevant literature that target students from different ages (middle school, high school, college students) shows that there is a statistically significant relationship between participants' levels of cyberbullying awareness and sex; female participants were found to possess higher levels of cyberbullying awareness compared to male participants in many studies (Aktan and Çakmak 2015; Ata and Adnan, 2016; Bridge and Duman, 2019; Dikmen and Çağlar, 2017; Gelmez 2020; Gezgin, and Çuhadar, 2012; Hendekçi and Kadiroğlu, 2020:21; Horzum and Ayas, 2013; Odacı and Çelik, 2018; Peker, 2019; Pınar, Cesur, Koca, Sayın, and Sancak, 2017).

These results dovetail with the findings of this study. İkiz (2009) and Horzum and Ayas (2013) attributed the results that found that women possess higher levels of cyberbullying awareness to the fact that women are by nature more empathetic. Also, İkiz (2009) pointed out that parenting styles and gender role expectations in Turkish culture play a role in creating this situation. Peker (2019) noted that women are more cautious and aware of dangers in digital environments compared to men as they are more sensitive to potential threats in real-life environments as well. Pınar, Cesur, Koca, Sayın, and Sancak (2017) pointed out that Turkish women have higher emotional intelligence due to their roles and the values imposed upon them by Turkish society and are more aware of how to protect themselves from cyberbullying. Aktan and Çakmak (2015), on the other hand, found out that women possess higher levels of cyberbullying awareness compared to men simply because they don't feel secure in digital environments.

They also noted that women are able to actively use virtual mediums by creating environments that allow them to feel more secure. Taking all these findings into account, it is safe to say that women are more cautious as they are worried that they may be cyberbullied in digital environments as a result of real-life bullying they had had to face in society; they tend to avoid putting themselves into situations where they may be cyberbullied, and consequently they develop cyberbullying awareness. However, contrary to the results of this study, some studies suggest that there is no statistically significant relationship between cyberbullying awareness and sex (Ayas and Horzum, 2011; Uysal, Duman, Şahin, and Yazıcı, 2014; Kozan and Özek, 2019). Uysal, Duman, Şahin, and Yazıcı (2014) ascribed this finding to the fact that college students tend to attach importance to such matters and their point of view is pretty much the same regardless of their sex.

No statistically significant difference was found between sex and the ability to ensure personal cybersecurity. As such, the results of this study dovetail with the findings of several studies in the relevant literature (Gökmen and Akgün, 2015; Karacı, Akyüz, and Bilgici, 2017; Subramaniam, 2017; Yiğit and Seferoğlu, 2019). Therefore, it can be stated that both female and male students have similar capacities when it comes to ensuring their personal cybersecurity. However, contrary to the findings of this study, several studies conducted by Tekerek and Tekerek (2013), Akgün and Topal (2015), and Karakaya and Yetgin (2020) showed that female students are highly capable of ensuring their personal cybersecurity, more so than their male counterparts.

Analysis of the question "*Do college students' levels of cyberbullying awareness and their ability to ensure their personal cybersecurity differ significantly based on their propensity to catfish?"* revealed that there was a statistically significant difference found between catfishing and college students' ability to ensure their personal cybersecurity; the difference favors students who said *no* when asked whether or not they catfish online. Individuals typically set up a fake online identity because they are worried about being harmed in some way or about unwittingly becoming a part of illegal or illicit activities. During adolescence in particular, people may catfish because they haven't yet reached the age of criminal responsibility and also have lower levels of information security awareness. However, it can be assumed that college students have higher levels of both cognition and awareness (Aslankara and Usta, 2020), and they should be better equipped to ensure their personal cybersecurity as well.

There was also a statistically significant difference between cyberbullying awareness and catfishing; the difference regarding levels of cyberbullying awareness favors students who said *no* when asked whether or not they have ever engaged in online catfishing. It appears that students who possess higher levels of cyberbullying awareness and sensitivity visit secure websites without the need to catfish or construct a fake identity. However, contrary to the findings of this study, a study conducted by Dikmen and Çağlar (2017), showed that there was no statistically significant relationship between cyberbullying awareness and catfishing or frequency of catfishing.

Analysis of the question "*Do college students' levels of cyberbullying awareness and their ability to ensure their personal cybersecurity differ significantly based on whether or not they had been cyberbullied?"* revealed that there was a statistically significant difference between a student's experience being cyberbullied and their ability to ensure their personal cybersecurity; the difference favors students who said *no* when asked whether or not they have ever been cyberbullied. As stated by Aslankara and Usta (2020), given that the frequency of many risky behaviors in digital environments decreases particularly during the college period (entry into adulthood) where people have higher levels of awareness in general, it is safe to state that college students are more conscious of ensuring their personal cybersecurity, and consequently, they aren't cyberbullied by others. On the other hand, there was no statistically significant relationship found between cyberbullying awareness and incidences of being cyberbullied. Similarly, both Odacı and Çelik (2018) and Dikmen and Çağlar (2017) found that there wasn't any significant relationship between cyberbullying awareness and incidences of being cyberbullied.

Moreover, a study conducted by Gezgin and Çuhadar (2012) revealed that cyberbullying awareness isn't affected by whether or not people are expose to cyberbullying. This could be explained by the fact that the number of people in the sample group who had been cyberbullied is considerably lower than the number of people who haven't been cyberbullied. Also, people who have been exposed to cyberbullying firsthand may possess low levels of cyberbullying awareness and lack an empathetic perspective. Our study showed that the mean values of both cyberbullying awareness and participants' answers when asked whether or not they had been cyberbullied were very close, which indicates that people may be indifferent to and/or dismissive of cyberbullying in general regardless of whether or not they had been cyberbullied.

Analysis of the question "*Do college students' levels of cyberbullying awareness and their ability to ensure their personal cybersecurity differ significantly based on cyberbullying others?"* revealed that there was a statistically significant relationship between college students' cyberbullying awareness and whether or not they had cyberbullied others; the difference favors students who said *no* when asked whether or not they had cyberbullied others. This result reveals that people who are conscious of negative aspects of digital environments and consequently develop awareness tend not to exhibit behaviors such as cyberbullying others. A

study conducted by Dikmen and Çağlar (2017), on the other hand, showed that there wasn't any statistically significant relationship between cyberbullying awareness and cyberbullying others.

Our study revealed that there wasn't any statistically significant difference between cyberbullying others and the ability to ensure personal cybersecurity; this may be the result of the difference between the number of participants who answered *yes* or *no*. Also, college students' belief that they are not going to be cyberbullied could also stem from the idea that they take all necessary precautions in digital environments and/or the fact that they play down the importance of cyberbullying in general.

Analysis of the question "*Do college students' levels of cyberbullying awareness and their ability to ensure their personal cybersecurity differ significantly based on college grade level?"* revealed that there wasn't any statistically significant difference between college students' grade level and either their ability to ensure their personal cybersecurity or their cyberbullying awareness. This result dovetails with findings obtained from a study conducted by Gezgin and Çuhadar (2012). Taking this result into consideration, it can be asserted that college students from different grade levels are similar in terms of their levels of cyberbullying awareness and their ability to ensure their personal cybersecurity.

Analysis of the question "*Does college students' ability to ensure their personal cybersecurity differ significantly based on their reasons for using the internet?"* revealed that there was a statistically significant difference between college students' reasons for using the internet and their ability to ensure their personal cybersecurity. Simply put, college students who use the internet for study/research were found to be more capable of ensuring their personal security compared to those who use it for social media. Similarly, college students who use the internet to keep up with news and the world are more capable of ensuring their personal cybersecurity compared to those who use it for social media. Bearing this in mind, it can be asserted that college students who possess higher levels of awareness in digital environments and who use the internet for educational and academic purposes as well as keeping up with news and the world are quite capable of ensuring their personal cybersecurity.

Analysis of the question "*Do college students' levels of cyberbullying awareness differ significantly based on their reasons for using the internet?"* revealed that there was a statistically significant difference between college students' cyberbullying awareness and their reasons for using the internet. Thus, college students who use the internet for study/research have significantly higher levels of cyberbullying awareness compared to those who use it to keep up with news and the world. Similarly, in their study with pre-service teachers, Odacı and Çelik (2018) found that levels of cyberbullying awareness differ based on users' reasons for using the internet. They noted that people who use the internet for educational purposes appear to have higher levels of cyberbullying awareness compared to those who use it for entertainment; this can be considered a sign that people who use the internet for educational purposes are more cognizant of how they are using it.

Another study conducted by Bridge and Duman (2019) similarly revealed that teenage users' reasons for using the internet were studying, doing homework, playing online games, watching movies, connecting to social networks, online shopping, listening to music, checking personal emails, and various other activities; they found that scores from the cyberbullying awareness scale differ significantly based on users' reasons for using the internet. Thusly, teenagers who use the internet for doing their homework or studying were found to have higher levels of cyberbullying awareness than those who use it for playing online games. These results dovetail with the results of our study. It should also be noted that college students use the internet to advance in their academic lives as they have reached a certain level of maturity and are equipped with a relevant set of skills that allow them to more effectively use these mediums.

Analysis of the question "*Does college students' ability to ensure their personal cybersecurity differ significantly based on their departments?"* revealed that there wasn't any statistically significant difference between college students' departments and their ability to ensure their personal cybersecurity. However, a study conducted by Yiğit and Seferoğlu (2019) revealed that there were statistically significant differences between sub-scales created for their study and college students' ability to ensure their personal security; students whose departments were closely related to computer sciences such as computer education and instructional technology (CEIT) and computer programming were found to be better at ensuring their personal cybersecurity compared to students from other departments.

Analysis of the question "*Do college students' levels of cyberbullying awareness differ significantly based on their departments?"* revealed that there was a statistically significant difference between college students' levels of cyberbullying awareness and their departments. Based on these results, students from the social studies teacher education department have significantly higher levels of cyberbullying awareness than students from the psychological counselling and guidance department *and* students from the elementary-level classroom education department.

Analysis of the question "*Do college students' levels of cyberbullying awareness and their ability to ensure their personal cybersecurity differ significantly based on their daily internet use?"* showed that there wasn't any statistically significant difference between college students' daily internet use and their ability to ensure their personal cybersecurity. In their study, Yiğit and Seferoğlu (2019) found that students whose weekly internet use was 20 hours or more had a better understanding of personal cybersecurity than those whose weekly internet use was between 6 and 10 hours. However, all things considered, they stated that the evaluation of users' weekly internet use was not a very effective way to gain insight into students' ability to ensure their personal cybersecurity. Thusly, these results are somewhat similar to the results of our study.

Furthermore, a study conducted by Gökmen and Akgün (2015) similarly revealed that there wasn't any statistically significant difference between students' levels of knowledge regarding information security and their daily internet use. Contrarily, Akgün and Topal (2015) found that daily internet use had a significant effect on information security awareness. The analysis of the study question also revealed that there wasn't any statistically significant relationship between students' daily internet use and their levels of cyberbullying awareness. This result dovetails with results of studies conducted by both Dikmen and Çağlar (2017) and Gezgin and Çuhadar (2012). Keeping this in mind, it should be noted that the amount of time college students spend on the internet on a daily basis is fairly uniform.

Analysis of the question "*Is there any statistically significant relationship between college students' levels of cyberbullying awareness and their ability to ensure their personal cybersecurity?"* showed that there is a positive, moderate correlation between college students' cyberbullying awareness and their ability to ensure their personal cybersecurity. Thus, college students' levels of cyberbullying awareness increase as they become more capable of ensuring their personal cybersecurity. It appears that college students will have higher levels of cyberbullying awareness as they become more knowledgeable about ensuring their personal cybersecurity.

Recommendations

As a consequence, individuals who have developed an awareness of digital environments and who use the internet consciously are more aware of and sensitive to cyberbullying attacks and threats. Therefore, raising awareness of such matters and creating university classes where subjects such as information systems and internet security are taught could be beneficial in terms of reaching more people. As a final recommendation, universities could place more emphasis on promoting and enrolling students in classes that delve into these topics in detail.

Ethics Committee Approval Information: Ethics committee approval for this study was received from the Ethics Committee of Bartın University (Date: 07/05/2021; Approval Number: 2021-SBB-0221).

REFERENCES

Abawajy, J. (2012). User preference of cyber security awareness delivery methods, *Behaviour & Information Technology, 33*(3), 237-248.

Akgün, Ö. E. & Topal, M. (2015). Eğitim fakültesi son sınıf öğrencilerinin bilişim güvenliği farkındalıkları: Sakarya Üniversitesi Eğitim Fakültesi örneği. *Sakarya University Journal of Education, 5*(2), 98-121.

Aktan, E. & Çakmak, V. (2015). Halkla ilişkiler öğrencilerinin sosyal medyadaki siber zorbalık duyarlılıklarını ölçmeye ilişkin bir araştırma, *Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi, 3*(2), 159-176.

Arıcak, O.T., Sıyahhan, S., Uzunhasanoğlu, A., Sarıbeyoğlu, S., Çıplak, S., Yılmaz, N. & Memmedov, C. (2008). Cyberbullying among Turkish adolescents, Cyberpsychology & *Behavior, 11*(3), 253-261.

Arıcak, O. T. (2009). Psychiatric symptomatology as a predictor of cyberbullying among university students. *Egitim Arastirmalari-Eurasian Journal of Educational Research*, *34,* 167-184.

Arıcak, O.T., Kınay, H. & Tanrıkulu, T. (2012). Siber zorbalık ölçeği'nin ilk psikometrik bulguları, *Hasan Ali Yücel Eğitim Fakültesi Dergisi, 17*, 101-114.

Arslankara, V.B. & Usta, E. (2018). Sanal dünya risk algısı ölçeği (SDRAÖ)'nin geliştirilmesi, *Bartın Üniversitesi Eğitim Fakültesi Dergisi, 7*(1), 111-131.

Arslankara, V.B. & Usta, E. (2020). Lise öğrencilerinde sanal risk algısı: Problemli internet kullanımı ve eleştirel düşünme bağlamında bir araştırma, *Ahmet Keleşoğlu Eğitim Fakültesi Dergisi, 2*(1), 134-153.

Aslan, A. & Önay Doğan, B. (2017). Çevrimiçi şiddet: Bir siber zorbalık alanı olarak 'Potinss' örneği. *Marmara İletişim Dergisi, 27,* 95-119.

Ata, R. & Adnan, M. (2016). Cyberbullying sensitivity and awareness among entry-level university students. *Journal of Human Sciences*, *13*(3), 4258-4267.

Avcı, Ü. & Oruç, O. (2020). Investigation of the students' personal cyber security behaviour and ınformation security awareness. *Inonu University Journal of the Faculty of Education*, *21*(1), 284-303.

Ayas, T. & Horzum, M. B. (2011). Exploring the teachers' cyberbullying perception in terms of various variables. *International Online Journal of Educational Sciences*, *3*(2), 619-640.

Baştürk, E. & Sayımer, İ. (2017). Siber zorbalık kavramı, türleri ve ilişkili olduğu faktörler: Mevcut araştırmalar üzerinden bir değerlendirme, *Online Academic Journal of Information Technology-Special Issue, 8*(30), 1-20.

Batmaz, M. & Ayas, T. (2013). İlköğretim ikinci kademeki öğrencilerin psikolojik belirtilere göre sanal zorbalık düzeylerinin yordanması. *Sakarya University Journal of Education*, *3*(1), 43-53.

Bayezid, G. (2000). Bastırma duyarlılık ölçeğini Türk kültürüne uyarlama çalışması, *Düşünen Adam, 13*(2), 99-106.

Bayram, N. & Saylı, M. (2013). Üniversite öğrencileri arasında siber zorbalık davranışı, *İÜHFM C. LXXI, 1*, 107-116.

Belsey, B. (2021). Cyberbullying, http://www.billbelsey.com/?cat=13 Date of access:11.04.2021.

Bridge, E.N. & Duman, N. (2019). Ergenlerde siber zorbalığa duyarlılığın demografik değişkenler açısından incelenmesi. *Cyprus Turkish Journal of Psychiatry & Psychology, 1*(3), 158-165.

Campbell, M. A. (2005). Cyber bullying: An old problem in a new guise?. *Australian Journal of Guidance and Counselling, 15*(1), 68-76.

Çam, H., Aslay, F. & Özen, Ö. (2019). Yükseköğretim kurumlarında bilgi güvenliği farkındalık düzeylerinin ölçümlenmesi, *Yönetim Bilişim Sistemleri Dergisi, 5*(2), 1-11

Çubukçu, A. & Bayzan, Ş. (2013). Türkiye'de dijital vatandaşlık algısı ve bu algıyı internetin bilinçli, güvenli ve etkin kullanımı ile artırma yöntemleri. *Middle Eastern & African Journal of Educational Research, 5*, 148-174.

Dikmen, M. & Çağlar, A. (2017). Öğretmen adaylarının siber zorbalığa yönelik duyarlılıklarının farklı değişkenler açısından incelenmesi, *Fırat Üniversitesi Sosyal Bilimler Dergisi, 27*(2), 101-111.

Dilmaç, B. (2009). Sanal zorbalığı yordayan psikolojik ihtiyaçlar: Lisans öğrencileri için bir ön çalışma, *Educational Sciences: Theory and Practice, 9*(3), 1291-1325.

Doğan, E., Çaka, C. & Şahin, Y.L. (2016). Çevrimiçi sosyal ağ oyunu oynayan bireylerin siber zorbalığa duyarlılık düzeyleri ile facebook kullanım amaçları üzerine bir çalışma, *Eğitimde Kuram ve Uygulama, 12*(3), 501-520.

Eminağaoğlu, M. & Gökşen, Y. (2009). Bilgi güvenliği nedir, ne değildir, Türkiye' de bilgi güvenliği sorunları ve çözüm önerileri, *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 11*(4), 01-15.

Erdoğmuş, A. (2017). *Üniversite öğrencilerinin bilgi güvenliği kazanımları, farklılıkları üzerindeki etkilerinin analizi: Afyon Kocatepe Üniversitesi örneği.* Yayımlanmamış Yüksek Lisans Tezi, Afyon.

Eroğlu, Y. & Güler, N. (2015). Koşullu öz-değer, riskli internet davranışları ve siber zorbalık/mağduriyet arasındaki ilişkinin incelenmesi, *Sakarya University Journal of Education, 5*(3), 118-129.

Erol, O., Şahin, Y. L., Yılmaz, E. & Haseski, H. İ. (2015). Kişisel siber güvenliği sağlama ölçeği geliştirme çalışması. *International Journal of Human Sciences*, *12*(2), 75-91.

Furnell, S. (2008). End-user security culture: A lesson that will never be learnt? *Computer Fraud ve Security*, *4*, 6-9.

Gelmez, Ö.S.Ö. (2020). Ortaokul öğrencilerinin siber zorbalığa ilişkin duyarlılıklarının incelenmesi. *Gençlik Araştırmaları Dergisi*, 8, 75-90.

Gezgin, D.M. & Çuhadar, C. (2012). Bilgisayar ve öğretim teknolojileri eğitimi bölümü öğrencilerinin siber zorbalığa ilişkin duyarlılık düzeylerinin incelenmesi, *Eğitim Bilimleri Araştırmaları Dergisi*, *2*(2), 93-104.

Gökçe Turan, S. (2021). İşyerinde siber zorbalık üzerine bir inceleme, *Journal of Organizational Behavior Review, 3*(1), 113-120.

Gökmen, Ö. F. & Akgün, Ö. E. (2015). Bilgisayar ve öğretim teknolojileri eğitimi öğretmen adaylarının bilişim güvenliği bilgilerinin çeşitli değişkenlere göre incelenmesi. *Çukurova University Faculty of Education Journal*, *44*(1), 61.

Hanewald, R. (2008). Confronting the pedagogical challenge of cyber safety, *Australian Journal of Teacher Education, 33*(3), 1-16.

Hekim, H. & Başıbüyük, O. (2013). Siber suçlar ve Türkiye'nin siber güvenlik politikaları, *Uluslararası Güvenlik ve Terörizm Dergisi, 4* (2), 135-158.

Hendekçi, A. & Kadiroğlu, T. (2020). The perception of health and cyberbullying sensitivity in adolescents. *Middle Black Sea Journal of Health Science, 6*(1), 18-23.

Horzum, M.B. & Ayas, T. (2013). Rehber öğretmenlerin sanal zorbalık farkındalık düzeyinin çeşitli değişkenlere göre incelenmesi. *Hacettepe Üniversitesi Eğitim Fakültesi Dergisi, 28*(3), 195-205.

İkiz, F. E. (2009). İlköğretim okullarında çalışan psikolojik danışmaların empati düzeylerinin incelenmesi. *İlköğretim Online*, *8*(2), 346-356.

Karacı, A., Akyüz, H.İ. & Bilgici, G. (2017). Üniversite öğrencilerinin siber güvenlik davranışlarının incelenmesi. *Kastamonu Eğitim Dergisi, 25*(6), 2079-2094.

Karakaya, A. & Yetgin, M.A. (2020). Karabük üniversitesi çalışanlarına yönelik kişisel siber güvenlik üzerine araştırma, *Kahramanmaraş Sütçü İmam Üniversitesi İktisadi ve İdari Bilimler Dergisi, 10*(2), 157-172.

Karaoğlan Yılmaz, G., Yılmaz, R. & Sezer, B. (2014). Üniversite öğrencilerinin güvenli bilgi ve iletişim teknolojisi kullanım davranışları ve bilgi güvenliği eğitimine genel bir bakış. *Bartın Üniversitesi Eğitim Fakültesi Dergisi, 3*(1), 176 – 199.

Karasar, N. (2003). *Bilimsel araştırma yöntemi* (12.Baskı), Ankara: Nobel.

Keser, H. & Güldüren, C. (2015). Bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. *Kastamonu Eğitim Dergisi, 23*(3), 1167-1184.

Kozan, M. & Bulut Özek, M. (2019). BÖTE bölümü öğretmen adaylarının dijital okuryazarlık düzeyleri ve siber zorbalığa ilişkin duyarlılıklarının incelenmesi, *Fırat Üniversitesi Sosyal Bilimler Dergisi, 29*(1), 107-120.

Kowalski, R.M. & Limber, S.P. (2007). Electronic bullying among middle school students, *Jornul of Adolescent Health, 41,* 22-30.

Lacey, B. (2007). *Social agression: A study of internet harassment*. Unpublished doctoral dissertation. Long Island University.

Morales, M. (2011). Cyberbullying, *Journal of Consumer Health on the Internet, 15*(4),406-419.

Odacı, H. & Çelik, Ç.B. (2018). Öğretmen adaylarının siber zorbalığa ilişkin duyarlılıklarının cinsiyet rolleri ve bazı değişkenlere göre incelenmesi. *Kırşehir Eğitim Fakültesi Dergisi, 19*(2), 1174-1187.

Öğün, M.N. & Kaya, A. (2013). Siber güvenliğin milli güvenlik açısından önemi ve alınabilecek tedbirler. *Güvenlik Stratejileri Dergisi, 9*(18), 145-181.

Öğütçü, G. (2010). *E-dönüşüm sürecinde kişisel bilişim güvenliği davranışı ve farkındalığının analizi,* Yayımlanmamış Yüksek Lisans Tezi, Başkent Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

Öğütçü, G., Testik, Ö.M. & Oumout, C. (2016). Analysis of personal information security behavior and awareness. *Computers & Security, 56*, 83–93.

Önaçan, M.B.K. & Atan, H. (2016). Siber güvenlikte lisans üstü eğitim: Deniz Harp Okulu örneği, *Trakya University Journal of Engineering Sciences, 17*(1), 13-21.

Patchin, J.W. & Hinduja, S. (2006). Bullies move beyond the schoolyard: a preliminary look at cyberbullying, *Youth Violence and Juvenile Justice, 4,* 148-169.

Peker, A. & Ekinci, E. (2016). Genel öz-yeterliğin siber zorbalıkla başa çıkma davranışları üzerindeki yordayıcı etkisi. *Uluslararası Türkçe Edebiyat Kültür Eğitim Dergisi, 5(4), 2126-2140.*

Peker, A. (2019). Rehberlik öğretmeni adaylarında dikkat kontrolünün siber zorbalığa ilişkin duyarlılık üzerindeki yordayıcı rolü. *Millî Eğitim, 49*(225), 343-368.

Pekşen Süslü, D. & Oktay, A. (2018). Lise öğrencilerinde siber zorbalık ve siber mağduriyetle ilişkili bazı değişkenlerin incelenmesi. *İlköğretim Online, 17*(4), 1877-1895. [Online]: http://ilkogretim-online.org.tr. Date of access:30.05.2021

Pınar, Ş.E., Cesur, B., Koca, M., Sayın, N. & Sancak, F. (2017). Emotional intelligence levels and cyberbullying sensibility among Turkish university students. *International Online Journal of Educational Sciences, 9(3), 676-685.*

Price, M & Dalgleish, J. (2010). Cyberbullying-Experiences, impacts and coping strategies as described by Australian young people. *Youth Studies Australia, 29*(2), 51-59.

Roger, D. & Schapals, T. (1996). Repression sensitization and emotion control. *Current Psychology*, *15*(1), 30-37.

Sasse, M.A., Brostoff, S. & Weirich, D. (2001). Transforming the 'weakest link' a human/computer interaction approach to usable and effective security. *BT Technology, 19(3), 122-131.*

Sertçelik, A. (2015). Siber olaylar ekseninde siber güvenliği anlamak. *Medeniyet Araştırmaları Dergisi, 2*(3), 25-42.

Slonje, R. & Smith, P.K. (2008). Cyberbullying: Another main type of bullying? *Scandinavian Journal of Psychology, 49,* 147–154.

Smith, P.K. & Ananiadou, K. (2003). The nature of school bullying and the effectiveness of school-based interventions. *Journal of Applied Psychoanalytic Studies, 5*(2), 189-209.

Smith, P.K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S. & Tippett, N. (2008). Cyberbullying: its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry, 49*(4), 376–385.

Subramaniam, S. R. (2017). Cyber security awareness among Malaysian pre-university students. *E-Proceeding of the 6th Global Summit on Education*, 1-14.

Suler, J. (2004). The online disinhibition effect. *Cyberpsychology & Behavior, 7*(3), 321-326.

Şenol, M. (2017). Türkiye'de siber saldırılara karşı caydırıcılık. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 3*(2), 1-9.

Şenol, M. (2016). Siber güçle caydırıcılık ama nasıl? *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 2*(2), 10-17.

Tamer, N. & Vatanartıran, S. (2014). Ergenlerin teknolojik zorbalık algıları. *Online Journal of Technology Addiction & Cyberbullying, 1*(2), 1-20.

Tanrıkulu, T., Kınay, H. & Arıcak, O. T. (2013). Siber zorbalığa ilişkin duyarlılık ölçeği: Geçerlik ve güvenirlik çalışması. *Trakya Üniversitesi Eğitim Fakültesi Dergisi, 3*(1), 38-47.

Tekerek, M. & Tekerek, A. (2013). A research on students' information security awareness. *Turkish Journal of Education*, *2*(3), 61-70.

Tuik, (2020). Hanehalkı bilişim teknolojileri kullanım araştırması. https://data.tuik.gov.tr. Date of access: 20.04.2021.

Uysal, İ., Duman, G., Yazıcı, E. & Şahin, M. (2014). Öğretmen adaylarının siber zorbalık duyarlılıkları ve siber zorbalık duyarlılık ölçeğinin bazı psikometrik özellikleri. *Ege Eğitim Dergisi, 15*(1), 191-210.

Wearesocial. (2021). Dünya ve Türkiye'de internet kullanımı. https://wearesocial.com/digital-2021 Date of access: 20.04.2021.

Willard, N. (2007). Cyberbullying and cyberthreats effectively managing, *Center for Safe and Responsible Use of the Internet*, 1-18.

Yaman, E., Karakülah, D. & Dilmaç, B. (2013). İlköğretim ikinci kademe öğrencilerinin değerlerini yordayan iki önemli değişken: Siber zorbalık eğilimleri ve okul kültürü arasındaki değişken, *Değerler Eğitimi Dergisi, 11*(26), 323-337.

Yavanoğlu, U., Sağıroğlu, Ş. & Çolak, İ. (2012). Sosyal ağlarda bilgi güvenliği tehditleri ve alınması gereken önlemler. *Politeknik Dergisi,* 15*(1), 15-27.*

Ybarra, M.L. & Mitchell, K.J. (2004) Online aggressor/targets, aggressors, and targets: A comparison of associated youth characteristics. *Journal of Child Psychology and Psychiatry, 45*(7), 1308–1316.

Yenilmez, Y. & Seferoğlu, S.S. (2013). Sanal zorbalık ve öğretmenlerin farkındalık durumlarına bir bakış. *Eğitim ve Bilim, 38*(169), 420-432.

Yılmaz, E.N., Ulus, H.İ. & Gönen, S. (2015). Bilgi toplumuna geçiş ve siber güvenlik. *Bilişim Teknolojileri Dergisi, 8*(3), 133-146.

Yiğit, M. F. & Seferoğlu, S. S. (2019). Öğrencilerin siber güvenlik davranışlarının beş faktör kişilik özellikleri ve çeşitli değişkenlere göre incelenmesi, *Mersin Üniversitesi Eğitim Fakültesi Dergisi, 15*(1), 186-215.