JOLTIDA Journal of Learning and Teaching in Digital Age, 2025, **10**(2), 156-169
https://dergipark.org.tr/en/pub/joltida
ISSN: 2458-8350 (online)

Research Paper

Investigating the Role of Mindful Awareness as an Antecedent of Undergraduate Students' Cyber Security Behaviors

Mehmet Fatih Yiğit[a*]

[a](ORCID ID: 0000-0002-3476-7619), Hakkari University, Faculty of Education, The Department of Educational Sciences, Hakkari, Türkiye, mehmetfatihyigit57@gmail.com
[*]Corresponding author

ARTICLE INFO

Received: 17 October 2024
Revised: 27 February 2025
Accepted: 27 February 2025

Keywords:
Mindful awareness, Mindfulness, Cyber security, Cyber security behaviors, Undergraduate students

doi: 10.53850/joltida.1558922

ABSTRACT

Technology, while enhancing efficiency and effectiveness, also poses significant cyber threats and risks. Overcoming these challenges necessitates individuals to have high levels of cybersecurity awareness and to exhibit proper cybersecurity behaviors. Correspondingly, in recent years, the exploration of individual factors influencing cybersecurity behaviors has become a popular topic in the relevant literature. Building upon this, the present study examines the predictive effect of mindful awareness on the cybersecurity behaviors of undergraduate students, a group deeply intertwined with technology and hence potentially exposed to cyber risks. Conducted using a relational survey methodology, the study involved 179 undergraduate students enrolled in a state university during the academic year 2022-2023. Data for the study were collected through an online form utilizing the "Personal Cyber Security Provision Scale" and the "Mindful Attention Awareness Scale." Results showed no significant differences in cybersecurity behaviors between male and female students. Department differences in cybersecurity behavior were only observed between Elementary Mathematics Teacher Education and Turkish Language Teacher Education, with students in the former exhibiting better behaviors. No differences in cybersecurity behaviors were found across grade levels. Also, a moderate positive correlation was found between mindful awareness and cybersecurity behaviors, with mindful awareness explaining 9.4% of the variance in cybersecurity behaviors. Finally, the investigation of moderating effects revealed that gender, department, and grade level did not significantly influence this effect. Practical and theoretical recommendations are provided based on these findings.

INTRODUCTION

The field of Information and Communication Technologies (ICT) exhibits a continuously evolving and iterative nature, characterized by the ongoing development and accumulation of innovations. A comparative analysis between the initial instances of emerging technologies and their current state of development underscores this phenomenon more prominently. In a similar vein, examining how people handle daily tasks from the past to the present reveal a progressive integration of technology into society, with traces and impacts of technology evident in nearly every aspect of life. As of 2023, empirical data further corroborates this reality, indicating approximately 5.3 billion internet users worldwide (STATISTA, 2024a), 6.5 billion mobile internet users (STATISTA, 2024b), and 5 billion social media users (STATISTA, 2024c).

In today's modern society, the widespread presence of technology in various domains such as communication, education, transportation, healthcare, industry, manufacturing, and security can be attributed to the benefits and conveniences it brings to human life. However, just as any tool can be used for both good and malicious purposes depending on the underlying intent and motive, a similar dual-edged sword analogy can be applied to technology (Misra *et al.*, 2022). In other words, it is the actions and decisions individuals exhibit while utilizing technology that determine whether it is used for positive or negative ends. In this context, technology can be utilized to create cyber-threats such as viruses, worms, trojans, spyware, phishing, and cyberbullying (Achuthan *et al*., 2023; Martins, De Wolf, & De Marez, 2019; Naqvi *et al.*, 2023). Those engaged in such malicious activities often exploit the anonymity and untraceability afforded by technology, particularly the internet, as a shield (Moore, 2014). Generally, the underlying driver behind cyber-attacks targeting individuals and organizations is to achieve financial gain. Consequently, cybersecurity emerges as an imperative concept that requires constant attention to protect individuals and businesses from both material and psychological harm inflicted by cyber threats (Alsharida *et al*., 2023).

In the literature, cybersecurity is defined as the technology-based practices and individual-specific skills and competencies necessary for preventing inappropriate actions such as unauthorized access, usage, disclosure, tampering, alteration, or destruction of information systems (National Initiative for Cybersecurity Careers and Studies [NICCS], 2018; Paliszkiewicz, 2019). Given the pervasive integration of technology into nearly every facet of life, cybersecurity is of paramount importance for both individuals and organizations due to the inherent risk of exposure to technological threats. While technologies such as firewalls, antivirus software, encryption, and multi-factor authentication are essential and necessary for ensuring cybersecurity,

relying solely on these technological measures is not entirely dependable or sufficient. Implementing these measures does not guarantee comprehensive cybersecurity or absolute protection against potential risks and threats (Abajawy, 2014).

As indicated in the definition above, ensuring cybersecurity requires not only technological capabilities but also individuals' awareness, knowledge, and skills related to cybersecurity, along with adopting, demonstrating, and sustaining appropriate behavioral patterns in this regard (Yan *et al*., 2018). Indeed, it is frequently emphasized in the literature that humans constitute the weakest link in cybersecurity, and a significant majority of cybersecurity incidents occur due to human errors (Abajawy, 2014; Merhi & Ahluwalia, 2019). Human beings are inherently more prone to making mistakes compared to technological hardware and software, which holds true in the realm of cybersecurity as well. This situation has led cyber attackers to increasingly target individuals over time, taking advantage of their vulnerabilities in cybersecurity through social engineering techniques, as the advancement of cybersecurity technologies has made it more difficult to exploit security vulnerabilities and execute attacks (Keser & Güldüren, 2015; Lallie *et al*., 2021).

As described, human negligence accounts for a significant percentage of cybersecurity incidents. In this regard, individuals often tend to prioritize convenience over security, engaging in actions such as choosing simple passwords, falling for phishing traps, and neglecting system updates, which can make them more vulnerable to cyber-attacks. Therefore, accounting for the human factor in cybersecurity and thoroughly examining this issue is critical. Indeed, the significance of this topic has been recognized in the literature, leading researchers in this field to conduct studies focusing on human behaviors in the context of cybersecurity (Gratian *et al*., 2018).

Examining the relevant literature reveals numerous variables related to human characteristics and behaviors that are studied for their potential impact on cybersecurity. These include stress (Al-Balushi *et al*., 2023), personality traits (Frauenstein & Flowerday, 2020; Yiğit & Seferoğlu, 2019), threat appraisal (Gerdenitsch, Wurhofer, & Tscheligi, 2023; Wu, 2020), coping appraisal (Jansen & Van Schaik, 2017; Sulaiman *et al*., 2022), subjective norm (Alanazi, Freeman, & Tootell, 2022), descriptive norm (Chen *et al*., 2018), attitude (Sommestad, Karlzén, & Hallberg, 2015), psychological ownership (Thompson, McGill, & Wang, 2017), anticipated regret (Verkijika, 2019), IT usage (Kovačević, Putnik, & Tošković, 2020), online game addiction (Yıldız-Durak, 2019), digital literacy (Sarıtepeci *et al*., 2024), and cyberbullying awareness (Zorlu, 2023).

Besides the aforementioned variables, another variable believed to have an impact on cybersecurity is mindful awareness, yet little is known about this subject. Consequently, this study aims to investigate the predictive effect of mindful awareness on cybersecurity behaviors, with the conceptual details and rationale for its consideration as a variable in the cybersecurity context elucidated in the subsequent section. Additionally, the moderating effects of gender, department, and grade level on this effect were also examined within the context of this study. Under this research scope, undergraduate students were chosen as the participant group. This choice stems from several reasons: undergraduate students are highly engaged with technology and online platforms, thus representing a demographic vulnerable to cyber-attacks; the digitalization of future job fields they will enter post-graduation require a strong understanding of cybersecurity; and university environments are conducive to implementing practical recommendations derived from such studies into education and intervention programs.

Mindful Awareness and Cyber Security Behaviors

Mindful awareness is generally defined as being attentive and aware of the present moment without judgment, as expressed by Bishop (2002) and Brown & Ryan (2003), or in simpler terms, by Hanh (1976) as “keeping one’s consciousness alive to the present reality”. Mindful awareness is a skill that keeps an individual alert, awake, and less passive and distracted in the present moment (Özyeşil *et al*., 2011). Additionally, it is noted as a trait that enhances an individual's self-control and self-regulation abilities regarding ongoing events (Chatzisarantis & Hagger, 2007; Leary, Adams, & Tate, 2006). Moreover, mindful awareness encourages individuals to pause and reflect on events without haste, thus allowing them to avoid overlooking critical messages and act more cautiously (Langer, 2016). Thus, considering both its definition and the positive traits associated with individuals possessing this skill, it seems plausible to suggest that mindful awareness could have a determinant and contributory effect on cybersecurity behaviors. As a matter of fact, prerequisites for successfully ensuring cybersecurity include attributes of mindful awareness such as attentiveness, alertness, self-control, self-regulation, and thoughtful reflection.

Understanding the impact of mindful awareness on cybersecurity behavior and the mechanisms that drive this relationship requires drawing from established psychological frameworks. One such theory is the Self-Regulation Theory (Zimmerman, 2002). According to this theory, individuals with strong self-regulation skills are better equipped to control their impulses, resist immediate temptations, and make decisions that align with their long-term goals. In this context, mindfulness plays a crucial role by enhancing individuals' awareness of their thoughts and emotions. This heightened awareness enables them to make more deliberate and cautious decisions in cybersecurity-related situations, such as resisting the urge to hastily click on suspicious links or avoiding the use of weak passwords. Thus, mindfulness fosters a more vigilant and self-disciplined approach to online security. Another pivotal theory shedding light on the influence of mindful awareness on individuals' cybersecurity behaviors is the Protection Motivation Theory (Rogers, 1975). This theory contends that an individual’s drive to safeguard themselves against a perceived threat is largely determined by their evaluation of the severity of the threat, their perceived vulnerability to it, and their confidence in their capacity to manage and effectively counter the threat. Within this framework, mindful awareness assumes a

crucial function by mitigating stress and anxiety, thereby enabling individuals to appraise cybersecurity threats with greater composure and precision. As a result, this enhanced clarity and emotional stability enable individuals to implement more proactive and well-informed protective measures while formulating more effective and timely responses to potential cyber threats.

Lastly, to deepen our understanding of the connection between these two variables, we can turn to the Dual Process Theory, proposed by Kahneman (2011). This theory posits that human thinking and decision-making processes are governed by two separate cognitive systems: System 1 and System 2. While System 1 operates swiftly, unconsciously, and automatically, System 2 is characterized by slower, more deliberate, and analytical thought. Within the domain of cybersecurity, mindful awareness plays a pivotal role in bolstering and nurturing the capabilities of System 2, facilitating more thoughtful and reasoned decision-making in response to potential cyber threats. This enables individuals to take more calculated actions instead of acting on impulse, thereby improving their capacity to address cyber risks in a more effective manner.

The literature reveals studies examining the impact of mindful awareness on variables such as psychological well-being (Deniz, Erus, & Büyükcebeci, 2017), depression, and perceived stress (Arslan, 2018), problematic drinking (Bramm, Cohn, & Hagman, 2013), online impulse buying (Vihari *et al*., 2022), internet gaming disorder (Li *et al*., 2017), internet addiction (Arslan, 2017), problematic internet use (Gámez-Guadix & Calvete, 2016), and smartphone addiction (Lan *et al*., 2018). However, there is only one study examining the impact of mindful awareness on cybersecurity (Seki, Çimen, & Dilmaç, 2023), and a limited number of studies have explored its effects on variables closely related to cybersecurity behaviors, such as problematic information security behavior (Chen *et al*., 2021) and phishing attacks (Jensen *et al*., 2017). This scarcity of research underscores the motivation behind conducting this study, which focuses on exploring the impact of mindful awareness on the cybersecurity behaviors of undergraduate students.

Significance of the Study

The conveniences and advantages brought into our lives by technology do not imply its sole goodness; rather, it can potentially transform into a weapon threatening human life when wielded by malicious actors through cyber-attacks. In mitigating these risks posed by technology-driven threats, technology itself can indeed be utilized as a shield. However, effective cybersecurity becomes achievable when coupled with human awareness, knowledge, and skills (Yiğit & Seferoğlu, 2020). Therefore, academic endeavors explaining the factors influencing desired behaviors in the context of cybersecurity among individuals become pivotal (Gratian *et al*., 2018). Thus, this study delves into the role of mindful awareness in the cybersecurity behaviors of undergraduate students, a significant cohort within the realm of cybersecurity.

The significance of the current study, both in theoretical understanding and practical applications, is threefold. Firstly, while numerous variables influencing cybersecurity behaviors have been examined, the literature on the potential impact of mindful awareness is notably limited. This underscores the need for further research to clarify our understanding in this context. For this reason, this study holds theoretical importance as it extends the cybersecurity literature by incorporating mindful awareness. Additionally, the study explored the moderating effects of gender, department, and grade level on the effect of mindful awareness on cybersecurity behaviors, a consideration that has not been addressed in previous research. By incorporating these moderating factors, the study aimed to offer a more nuanced understanding of how these elements interact with the core variables, thereby providing deeper insights into the dynamics of the underlying effect.

Secondly, identifying factors influencing individuals' behaviors in the cyber domain provides crucial input for intervention programs aimed at enhancing these behaviors. Understanding the role of mindful awareness in cybersecurity behaviors will offer valuable insights for cybersecurity education and intervention activities, enriching them with mindfulness strategies and thereby enhancing their effectiveness. This aspect underscores the practical importance of the current study.

Lastly, it is believed that the current study has the potential to offer broader implications for building societal cybersecurity resilience. The participants of this study, undergraduate students, represent the future workforce and digital citizens. Thus, promoting mindful awareness practices among this group can facilitate the display of desired cybersecurity behaviors, ultimately contributing to the widespread adoption of appropriate cybersecurity practices in society in the long term and fostering a cybersecurity-conscious community. In summary, as discussed above, this study holds both theoretical and practical importance as it contributes to the existing literature and aids in efforts to improve cybersecurity behaviors.

Purpose of the Study

The aim of this study is to uncover the role of mindful awareness in cybersecurity behaviors. To achieve this goal, the following research questions were addressed:

1. What are the levels of mindful awareness and cybersecurity behaviors among undergraduate students?
2. How do undergraduate students' levels of cybersecurity behaviors differ based on gender, department, and grade level?
3. What is the predictive effect of mindful awareness on undergraduate students' cybersecurity behaviors?

4. How do gender, department, and grade level moderate the predictive effect of mindful awareness on undergraduate students' cybersecurity behaviors?

METHOD

Since the study examines the predictive effect of mindful awareness on undergraduate students' cybersecurity behaviors, a relational survey methodology is employed for the research. Relational survey method aims to determine the presence and/or degree of co-variation between two or more variables (Karasar, 2013). Additionally, the study examined whether cybersecurity behaviors vary according to various variables. For this purpose, a descriptive survey model was also employed in the study (Fraenkel, Wallen, & Hyun, 2012).

Study Group

The study group consists of 179 undergraduate students enrolled in a state university in Türkiye during the 2022-2023 academic year, selected through convenient sampling method. Bryman and Cramer (2002) suggest that the ideal sample size should be between 5 to 10 times the number of items, while Alpar (2013) recommends it to be 20 times the number of variables. Therefore, it can be stated that the number of participants in the current study is appropriate in terms of sample size. Participation in the study is based on voluntary basis. Further demographic characteristics of the study group are presented in Table 1.

Table 1. The demographic characteristics of the study group

Variable	Category	Frequency (f)	Percentage (%)
Gender	Female	118	65.92
	Male	61	34.08
Department	Art Education	11	6.15
	Elementary Mathematics Teacher Education	67	37.43
	English Language Education	25	13.97
	German Language Education	14	7.82
	Primary Teacher Education	15	8.38
	Psychological Counseling and Guidance	26	14.53
	Turkish Language Teacher Education	21	11.73
Grade Level	1	70	39.11
	2	81	45.25
	3	28	15.64
	TOTAL	179	100.00

Table 1 presents the demographic characteristics of the study group in terms of gender distribution, department, and grade level. Approximately two-thirds of the 179 participants are female (65.92%), while the remaining are male (34.08%). In addition, the study includes participation from 7 different departments, with the highest participation observed in the "Elementary Mathematics Teacher Education" department (37.43%), and the lowest participation observed in the "German Language Education" (7.82%) and "Art Education" (6.15%) departments. Regarding grade level, higher participation rates are observed in the first and second years, with percentages of 39.11% and 45.25%, respectively, while the participation rate in the third year is lower at 15.64%.

Data Collection Tools

In this study, data were collected using two instruments: the "Personal Cyber Security Provision Scale" and the "Mindful Attention Awareness Scale".

Personal Cyber Security Provision Scale

To determine the cybersecurity behaviors of undergraduate students, the "Personal Cyber Security Provision Scale" developed by Erol *et al*. (2015) was utilized. This scale, which consists of 25 items rated on a 5-point Likert scale, encompasses five factors named "Personal Privacy Protection", "Avoiding from Unsafe", "Taking Precautions", "Protecting Payment Information", and "Leaving No Trace". The five-factor structure accounts for 48.026% of the total variance. Confirmatory Factor Analysis was conducted to examine the construct validity of the scale, yielding a Comparative Fit Index (CFI) value of 0.92, Goodness of Fit Index (GFI) value of 0.86, and Root Mean Square Error of Approximation (RMSEA) value of 0.067, indicating that these fit indices fall within acceptable ranges (Hu & Bentler, 1990). Regarding the reliability of the scale, the Cronbach's Alpha reliability coefficient was found to be 0.735 for the entire scale, which is within acceptable reliability values (Nunnaly, 1994).

Mindful Attention Awareness Scale

To determine undergraduate students' levels of mindful awareness, the "Mindful Attention Awareness Scale" developed by Brown and Ryan (2003) and adapted into Turkish by Özyeşil *et al*. (2011) was utilized. This scale, based on a 6-point Likert scale, comprises 15 items and demonstrates a unidimensional structure, which explains 58.109% of the total variance. Confirmatory Factor Analysis yielded a Goodness of Fit Index (GFI) value of 0.93, Adjusted Goodness of Fit Index (AGFI) value of 0.91, and Root Mean Square Error of Approximation (RMSEA) value of 0.60, indicating a good fit between the data and the structure (Hu & Bentler, 1990). The Cronbach's Alpha reliability coefficient of the scale was calculated as 0.80, providing evidence for the scale's reliability (Nunnally, 1994).

Data Collection Process

Before commencing the data collection process, the necessary ethical approval for the study was obtained from the Hakkari University Ethics Committee (Date: 22.12.2022, Approval No: 2022/118). Subsequently, the scales used in data collection were prepared electronically via Google Forms and shared with students through an online link.

Data Analysis

In the initial stage of data analysis, the data collected online were transformed into a numerical format and prepared for analysis in a Microsoft Excel spreadsheet. Subsequently, to examine how undergraduate students' levels of cybersecurity behaviors differ across gender, department, and grade level, the normal distribution of these two dependent variables was first assessed in relation to the subgroups of the independent variables. Given that the skewness (min: -1.375; max: 0.701) and kurtosis (min: -0.989; max: 1.318) values fell within the acceptable range of ±1.5, parametric tests were deemed appropriate for analysis (Tabachnick & Fidell, 2013). Therefore, independent samples t-tests and ANOVA were employed to identify any significant differences.

In addition, simple linear regression analysis was employed to examine the predictive effect of mindful awareness on undergraduate students' cybersecurity behaviors, aligning with the research question of the study. Before conducting the analysis, assumptions such as outliers, normality, linearity, homogeneity of variances, and autocorrelation were tested. To conduct simple linear regression analysis, it is crucial to ensure that the dataset does not contain outliers, or if there are any, they should be identified and removed. To identify outliers, the standardized residuals (z-scores of residuals) were examined to see if they fell within the range of ±3.29 (Tabachnick & Fidell, 2007). The analysis revealed that none of the values exceeded this threshold, with the observed range of standardized residuals falling between -2.55 and 2.30. Additionally, the calculated skewness and kurtosis values for this study fell within the range of ±1.5 (see Table 2), indicating that the data for both the dependent and independent variables are normally distributed (Tabachnick & Fidell, 2013). Linearity and homogeneity of variances assumptions were assessed by examining the scatterplot in Figure 1, which confirmed that both assumptions were met. Lastly, for simple linear regression analysis, it is important to ensure that there is no autocorrelation between the variables. For this purpose, the Durbin-Watson (D-W) statistic should ideally fall between 1.5 and 2.5, and it was found that this assumption was also met in this study (D-W=1.89).

Finally, the moderating role of gender, department, and grade level in the impact of mindful awareness on cybersecurity behaviors was examined in the study. Moderation analyses were conducted using multiple regression techniques, with interaction terms included in the models to assess whether these variables significantly influenced the strength or direction of the relationship. To address potential issues of multicollinearity, the data were standardized by converting the variables into z-scores.

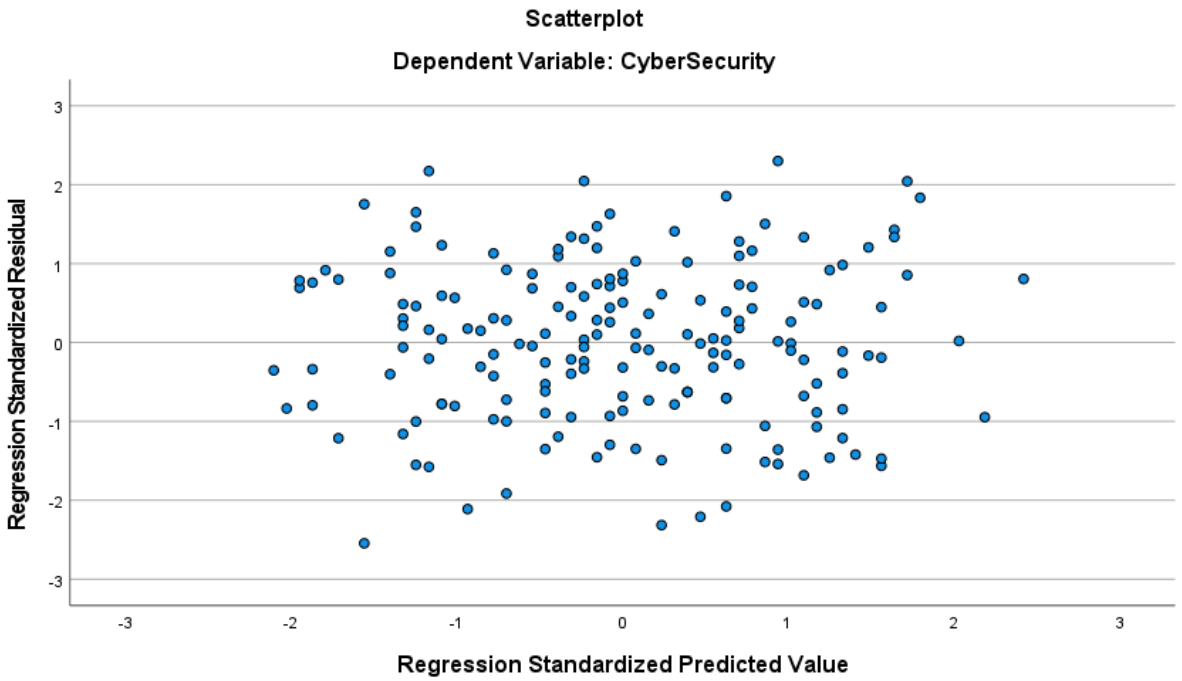

Figure 1. Scatterplot of Standardized Residuals and Standardized Predicted Values of a Simple Linear Regression Model

FINDINGS

In this section, the results for each research question are presented in distinct subsections, allowing for a clear and organized presentation of the findings.

RQ-1: Levels of Mindful Awareness and Cybersecurity Behaviors Among Undergraduate Students

Descriptive statistics for the variables addressed in the study are presented in Table 2. According to the table, scores for mindful awareness range from 2.13 to 6.00, with a mean score of 3.93, indicating that undergraduate students exhibit a moderate level of mindful awareness. On the other hand, concerning cybersecurity behaviors, the minimum score is 2.16, while the maximum score obtained is 4.64. The average score of 3.50 indicates that students exhibit moderate to high levels of cybersecurity behaviors.

Table 2. Descriptive statistics for the variables

Variable	Min	Max	Mean	*sd*	Skewness	Kurtosis
Mindful Awareness	2.13	6.00	3.93	0.85	-0.016	-0.699
Cyber Security Behavior	2.16	4.64	3.50	0.46	-0.014	-0.123

RQ-2: Levels of Cybersecurity Behaviors Among Undergraduate Students Based on Gender, Department, And Grade Level

The study also explores how cybersecurity behaviors among undergraduate students differ based on gender, department, and grade level. Given that the data for the subgroups followed a normal distribution, an independent samples t-test was employed for variables with two categories, while ANOVA was utilized for variables with more than two categories. The results of these analyses are summarized in Table 3.

Table 3. Results of t-tests and ANOVA for the comparison of subgroups

Category	Group	N	Mean	*sd*	*t*	*F*	*p*	Difference
Gender	Female [a]	118	3.48	0.46	-0.650	-	0.517	b>a
	Male [b]	61	3.53	0.45				
Department	AE [a]	11	3.35	0.35	-	3.214	0.005	b>g
	EMTE [b]	67	3.64	0.47				
	ELE [c]	25	3.57	0.51				
	GLE [d]	14	3.33	0.49				
	PTE [e]	15	3.39	0.37				
	PCG [f]	26	3.49	0.38				

	TLTE [g]	21	3.23	0.41				
Grade Level	1 [a]	70	3.57	0.48				
	2 [b]	81	3.43	0.43	-	1.807	0.167	-
	3 [c]	28	3.52	0.46				

AE: Art Education; EMTE: Elementary Mathematics Teacher Education; ELE: English Language Education; GLE: German Language Education; PTE: Primary Teacher Education; PCG: Psychological Counseling and Guidance; TLTE: Turkish Language Teacher Education

This table presents the results of t-tests and ANOVA for the comparison of cybersecurity behaviors across gender, department, and grade level. For gender, no significant difference was found between female (M=3.48, sd=0.46) and male students (M=3.53, sd=0.45; t=-0.650, p=0.517), indicating that female and male students exhibited similar cybersecurity behaviors. In terms of department, a significant difference was observed (F=3.214, p=0.005), with students from the Elementary Mathematics Teacher Education (EMTE) department (M=3.64, sd=0.47) showing higher cybersecurity behaviors compared to students from the Turkish Language Teacher Education (TLTE) department (M=3.23, sd=0.41). No other significant differences were found among the remaining departments. For grade level, no significant differences were observed in cybersecurity behaviors across the three levels (F=1.807, p=0.167), indicating that students in different grade levels displayed comparable levels of cybersecurity behaviors.

RQ-3: Predictive Effect of Mindful Awareness on Undergraduate Students' Cybersecurity Behaviors

The impact of undergraduate students' mindful awareness levels on cybersecurity behaviors was examined using simple linear regression analysis. It was found that the assumptions that needed to be tested before the analysis were met. The results of the analysis are presented in Table 4.

Table 4. Simple Linear Regression Result

Variable	*B*	*Std. Error*	*β*	*t*	*p*
(Constant)	2.834	0.154		18.361	0.000
Mindful Awareness	0.169	0.038	0.314	4.405	0.000
r=0.314 R^2=0.094 $F_{(1, 177)}$=19.403 p=0.000					

The results of the simple linear regression analysis indicate that the model is significant (p=0.000). Accordingly, with an r value between 0.30 and 0.70, there is a moderate and positive significant correlation between mindful awareness and cybersecurity behaviors (Büyüköztürk, 2007). Furthermore, mindful awareness is found to be a significant predictor of undergraduate students' cybersecurity behaviors, explaining 9.4% of the total variance. Therefore, for each increase in standard deviation of mindful awareness, there will be an approximate increase of 0.17 units in the standard deviation of cybersecurity behaviors.

RQ-4: The Moderating Role of Gender, Department and Grade Level in The Predictive Effect of Mindful Awareness on Undergraduate Students' Cybersecurity Behaviors

Multiple regression analysis was conducted to assess the moderating effects of gender, department, and grade level on the effect of mindful awareness on students' cybersecurity behaviors. In moderation analysis, the primary focus is on the interaction terms in the regression models, as these reflect how moderator variables interact with the independent variable to influence the dependent variable. The results related to these moderating effects are provided in Table 5 below.

Table 5. Multiple Linear Regression Result

Variable	*B*	*Std. Error*	*β*	*t*	*p*
(Constant)	3.243	0.659		4.925	0.000
Mindful Awareness (MA)	0.122	0.161	0.228	0.761	0.448
Gender (G)	-0.027	0.071	-0.027	-0.377	0.707
Department (D)	-0.047	0.018	-0.190	-2.542	0.012
Grade Level (GL)	-0.022	0.048	-0.033	-0.452	0.651
Moderator (MAxG)	0.070	0.070	0.223	1.004	0.317
Moderator (MAxD)	-0.009	0.018	-0.077	-0.484	0.629
Moderator (MAxGL)	-0.021	0.052	-0.084	-0.399	0.690
r=0.380 R^2=0.110 $F_{(7, 171)}$=4.134 p=0.000					

The results of the multiple regression analysis show that the moderator effects of gender, department, and grade level on the effect of mindful awareness on cybersecurity behaviors are not significant. Specifically, the interaction terms for gender (MAxG), department (MAxD), and grade level (MAxGL) all yielded non-significant results ($p > 0.05$), indicating that these factors do not significantly moderate the effect of mindful awareness on cybersecurity behaviors.

DISCUSSION AND CONCLUSION

In today's world, where every aspect of human life is enveloped by cyber technologies, individuals may encounter various security risks stemming from these technologies. In the face of daily pervasive threats and dangers, cybersecurity has become a phenomenon demanding significant attention and sustainable implementation by humans, notably acknowledged as the weakest link in scholarly discourse. Consequently, the issue of the factors contributing to individuals exhibiting appropriate cybersecurity behaviors has become highly popular in the literature, leading to numerous studies within the field of cyberpsychology examining the potential roles of various variables in this regard. In this study, however, the relatively underexplored yet considered intriguing variable of mindful awareness has been examined, focusing on its impact on the cybersecurity behaviors of undergraduate students. In the subsequent subsections, the findings related to each research question are thoroughly examined and interpreted. This section aims to provide an in-depth discussion by comparing the results with existing literature, highlighting consistencies or discrepancies, and offering possible explanations for the observed outcomes.

Levels of Mindful Awareness and Cybersecurity Behaviors Among Undergraduate Students

The descriptive statistics reveal that undergraduate students display moderate to high levels of cybersecurity behaviors, indicating a reasonable awareness of and adherence to cybersecurity practices. When the findings of previous studies are considered, similar results have been reported, showing that students generally exhibit an adequate level of cybersecurity behaviors (Avcı & Oruç, 2020; Yan *et al*., 2018; Yiğit & Seferoğlu, 2019). However, contrasting evidence also exists in the literature. Some studies have found that undergraduate students' cybersecurity behaviors fall short of the desired levels (Akgün & Topal, 2015; Aksoğan et al., 2024; Karaoğlan-Yılmaz, Yılmaz, & Sezer, 2014). These inconsistencies could be attributed to differences in sample characteristics, or the extent of cybersecurity education provided in various institutions.

The findings regarding mindful awareness reveal that undergraduate students, on average, exhibit a moderate level of mindful awareness. The moderate mean score suggests that although mindful awareness is present within the student population, it is neither widespread nor consistently high. These results align with previous studies in the literature, which have similarly found that undergraduate students tend to demonstrate lower levels of mindful awareness (Alper, Akpınar, & Akpınar, 2021; Çalışkan *et al*., 2024). However, it is worth noting that other research has reported more favorable findings, indicating that some students exhibit a higher level of mindfulness (Akman & Demir, 2021; Bekirler & Bilaloğlu, 2022). This divergence in findings suggests that mindful awareness among undergraduates may be influenced by various factors, such as differences in educational environments, personal experiences, or exposure to mindfulness practices.

Levels of Cybersecurity Behaviors Among Undergraduate Students Based on Gender, Department, And Grade Level

This study also examined the differences in cybersecurity behaviors of undergraduate students based on gender, department, and grade level. The findings indicate that there were no significant differences between female and male students in terms of their cybersecurity behaviors. This suggests that both genders exhibit similar levels of awareness and practices when it comes to cybersecurity. These results are consistent with previous studies that have found no significant gender differences in cybersecurity behaviors (Subramaniam, 2017; Yan et al., 2018; Yiğit & Seferoğlu, 2019). However, other research has reported gender differences, with some studies indicating that males exhibit more cybersecurity awareness (Aksoğan et al., 2024; Gültekin & Özel, 2023), while others have found female students to be more proficient (Tekerek & Tekerek, 2013). The absence of a significant gender difference in this study may be attributed to the equal opportunities now available to both male and female students in terms of technology access and cybersecurity education. Moreover, considering the current student profiles, interest in and use of technology have become less gender-specific and are increasingly widespread among young generations. Consequently, gender no longer appears to be a critical variable in cybersecurity behavior.

Regarding the department variable, a significant difference was found between students from the Elementary Mathematics Teacher Education (EMTE) department and the Turkish Language Teacher Education (TLTE) department, with students from the former demonstrating higher levels of cybersecurity behavior. Previous studies have suggested that students in technology-related fields tend to exhibit more advanced cybersecurity behaviors compared to students from other disciplines (Tokmak, 2023; Yiğit & Seferoğlu, 2019). However, there are also studies that found no significant differences between departments (Aksoğan et al., 2024). The result in this study, where EMTE students outperformed TLTE students, may be due to the more analytical thinking skills of mathematics students, which could make them more cautious in their use of technological tools and online environments. On the other hand, students from the Turkish Language department may have had less exposure to technology-focused education, which could limit their awareness of cybersecurity issues.

Finally, no significant differences were found in terms of grade level, suggesting that students, regardless of their academic year, exhibit similar attitudes and behaviors toward cybersecurity. This finding is supported by other studies (Karacı, Akyüz, & Bilgici, 2017; Yan et al., 2018). One possible explanation for this result is that technology is an integral part of students' academic lives at all levels, with its widespread use across all grade levels. Additionally, the fact that students are required to take a course on "Information Technologies," which covers cybersecurity topics, during the early stages of their university education may have contributed to this result.

Predictive Effect of Mindful Awareness on Undergraduate Students' Cybersecurity Behaviors

The study has demonstrated a significant positive impact of mindful awareness on cybersecurity, a finding that aligns with the results of other limited studies in this field (Chen *et al*., 2021; Seki, Çimen, & Dilmaç, 2023). While the former study revealed a negative relationship between mindful awareness and problematic internet security behavior, the latter identified a moderate positive correlation between these variables. Thus, it can be inferred that enhancing mindful awareness may lead to an improvement in cybersecurity behaviors.

It can be argued that certain factors underlie the emergence of a significant predictive effect of mindful awareness on undergraduate students' cybersecurity behaviors. Firstly, as frequently emphasized in the literature, one of the core components of mindful awareness is enhanced attention (Goilean, Gracia, & Tomás, 2023; Semple *et al*., 2010; Verhaeghen, 2021), which can justify why mindful awareness is effective in shaping cybersecurity behaviors. Mindful individuals, through their enhanced attention, are consciously present in the moment and are alert, sensitive, and attentive to their thoughts, emotions, and surrounding events (Brown & Ryan, 2003). When these attributes of mindful awareness are applied to the context of cybersecurity, they translate into increased focus on digital activities, a more cautious approach while engaging in these activities, and heightened vigilance against potential cyber threats such as suspicious emails, messages, and websites. In these respects, mindful awareness plays a significant role in reducing individuals' vulnerability to cyber-attacks and ensuring cybersecurity.

Secondly, scholarly literature highlights the link between mindful awareness and decision-making skills (Gautam & Mathur, 2018; Liu, Liu, & Ni, 2018; Shapiro, Jazaieri, & Goldin, 2012), which could explain its significant impact on cybersecurity behaviors of undergraduate students. Individuals with high level of mindfulness tend to adopt a more cautious and confident approach to decision-making in the context of cybersecurity, enabling them to be more adept at evaluating the benefits and potential risks associated with their online actions and to be aware of their digital footprints. Therefore, by enhancing individuals' decision-making abilities, thus encouraging greater caution before downloading a file, clicking on a link, or sharing information, mindful awareness proves to be a significant contributory factor in ensuring cybersecurity.

Thirdly, the connection between mindful awareness and reduced impulsive behaviors (Murphy & MacKillop, 2012; Stratton, 2006) could be one of the underlying reasons for its positive impact on cybersecurity behaviors. Impulsive behavior refers to actions carried out spontaneously, without sufficient thought or consideration of potential consequences (Reynolds *et al*., 2006). The literature associates mindful awareness with a lower tendency towards impulsive behaviors (Franco *et al*., 2016; Peters *et al*., 2011). Therefore, when considered in the context of cybersecurity, individuals with mindful awareness are more likely to refrain from impulsive actions such as clicking on suspicious links or hastily responding to phishing attempts. Instead, they are more likely to pause, reflect on the situation, and make thoughtful decisions, thereby protecting themselves from cyber risks. Consequently, mindful awareness emerges as a helpful factor in promoting appropriate cybersecurity behaviors among undergraduate students.

As discussed earlier, the positive impact of mindful awareness on undergraduate students' cybersecurity behaviors is influenced by factors such as enhanced attention, thoughtful decision-making skills, and reduced impulsivity. Addressing these factors within an educational context will also provide valuable insight into how mindful awareness can be leveraged to improve students' cybersecurity behaviors. The positive impact of mindful awareness on the cybersecurity behaviors of undergraduate students can be further understood by examining the factors of enhanced attention, thoughtful decision-making skills, and reduced impulsivity within an educational context. Specifically, the enhanced attention that comes with mindful awareness plays a crucial role in the digital age, where learners are increasingly engaging with digital learning tools and online resources. In this context, students may be exposed to cyber threats like phishing scams or compromised educational resources when accessing academic materials online. By fostering enhanced attention, mindful awareness allows students to be more vigilant and cautious, thereby reducing their susceptibility to these digital risks.

Similarly, thoughtful decision-making skills, which are developed through mindful awareness, are beneficial when students are deciding whether to download educational resources onto their devices or share them with peers. Mindful students are better equipped to assess the cybersecurity risks of these actions, considering factors like the security of the websites or potential threats associated with downloading certain files. This improved decision-making extends to recognizing the safety of academic resources, making students more capable of distinguishing between secure and potentially dangerous online educational content. Furthermore, mindful awareness plays a significant role in minimizing impulsive behaviors, a key factor in students' exposure to cybersecurity risks. In today’s educational landscape, much of students’ academic work takes place online, where they may encounter risky situations, such as downloading unreliable sources or falling victim to phishing attacks. Through mindful awareness, students are more likely to pause and reflect before acting, avoiding hasty decisions that could expose them to cybersecurity threats. This reflective approach allows students to act more cautiously, decreasing the likelihood of engaging with potentially harmful digital learning content.

The Moderating Role of Gender, Department and Grade Level in the Predictive Effect of Mindful Awareness on Undergraduate Students' Cybersecurity Behaviors

Lastly, the study also revealed that the demographic variables of gender, department, and grade level do not significantly moderate the effect of mindful awareness on cybersecurity behaviors. While mindful awareness was positively associated with cybersecurity behaviors, the lack of significant moderation by gender, department, or grade level indicates that these variables do not substantially influence the impact of mindful awareness on students' cybersecurity practices. When reviewing the literature, no previous studies were found that specifically addressed moderator effects in relation to mindful awareness and cybersecurity behaviors, making this a relatively novel finding.

One possible explanation for the absence of moderation is that mindful awareness may be a universal construct, influencing students' cybersecurity behaviors in a similar manner, irrespective of their gender, academic discipline, or year of study. Additionally, as discussed earlier, students' cybersecurity behaviors did not significantly differ by gender or grade level, and only a minimal difference was observed between two departments. Therefore, given that these demographic variables did not notably influence cybersecurity behaviors, it is not surprising that they did not moderate the relationship between mindful awareness and cybersecurity behaviors. This suggests that the impact of mindful awareness on students' cybersecurity practices may be consistent across various demographic and academic backgrounds.

Practical Recommendations

The results of the study indicate that mindful awareness serves as a critical and contributory factor in enhancing cybersecurity behaviors among undergraduate students. Therefore, based on these results, universities could integrate mindfulness-related courses into curricula and organize intervention programs and workshops aimed at improving students' mindful awareness skills. These courses could incorporate the core principles of mindful awareness, such as attention control, reducing impulsivity, and emotion regulation. Furthermore, the workshops could include practical experiences and skill-building exercises aimed at improving students' cybersecurity behaviors. Role-playing scenarios would be an effective way to simulate risky online situations, allowing students to practice how to respond to various cybersecurity threats in a controlled, supportive environment. This approach not only provides students with theoretical knowledge but also with the practical tools they need to navigate digital risks more effectively.

Additionally, faculty and staff can be trained to serve as role models in establishing a campus-wide mindfulness culture. In this context, professional development programs can be organized to teach educators how to integrate mindfulness techniques into their pedagogical approaches. These programs could also focus on equipping faculty and staff with the tools to teach mindfulness skills to their students, particularly how these skills can be applied in cybersecurity scenarios.

Furthermore, mindfulness strategies can be incorporated into cybersecurity training programs to enrich the content. Traditional cybersecurity training often focuses on technical skills and knowledge, but integrating mindfulness could enhance its effectiveness. Indeed, such training that emphasizes and reinforces the key aspects of mindful awareness, such as acting cautiously, avoiding haste, pausing to reflect, and taking careful steps, could be highly effective in encouraging undergraduate students to engage in vigilant online behavior and exhibit appropriate cybersecurity behaviors.

Limitations and Future Directions

While this research provides valuable insights into the impact of mindful awareness on undergraduate students' cybersecurity behaviors, it is essential to acknowledge certain limitations to ensure a robust interpretation of the study results and to guide future research endeavors. The primary limitation of the study pertains to the sample. The participants in the study are limited to undergraduate students from a single university, potentially constraining the generalizability of the findings. Students from other universities, particularly those with different demographic, cultural, or academic backgrounds, may exhibit distinct behaviors or attitudes towards cybersecurity and mindfulness. Therefore, it is recommended that future studies replicate this research with a more diverse sample, including students from different universities. This would help in determining whether the observed relationships hold true in more varied contexts.

Additionally, although a positive significant relationship between the two variables has been identified in the study, the effect size is relatively small. This suggests that mindful awareness alone may not fully account for students' cybersecurity behaviors. Hence, it is deemed crucial to conduct studies incorporating various other factors that may serve as an antecedent to cybersecurity behaviors alongside mindful awareness. In this context, through structural equation modeling (SEM), future studies should consider expanding the scope of factors influencing cybersecurity behaviors by incorporating other variables, such as personal characteristics, digital literacy, or risk perception etc.

In addition, future research could adopt longitudinal or mixed methods approaches to deepen the understanding of the relationship between mindful awareness and cybersecurity behaviors. Longitudinal studies would allow researchers to examine how mindful awareness influences cybersecurity behaviors over time, while mixed-methods approaches could provide both

quantitative data and qualitative insights into students' experiences with mindfulness practices and how they apply them in real-world online contexts.

Finally, another limitation relates to the potential for social desirability bias, especially given the use of self-report measures (Nederhof, 1985). Students may have been inclined to provide responses that reflect socially acceptable behaviors. This could lead to an overestimation of the actual impact of mindful awareness on cybersecurity behaviors. Future research could mitigate this limitation by incorporating objective measures of cybersecurity behaviors, such as tracking real-time online actions or using behavioral data, to complement self-report surveys.

Ethical Approval and Participant Consent: The necessary ethical approval for the study was obtained from the Hakkari University Ethics Committee (Date: 22.12.2022, Approval No: 2022/118).

REFERENCES

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology, 33*(3), 237-248. https://doi.org/10.1080/0144929X.2012.708787

Achuthan, K., Nair, V. K., Kowalski, R., Ramanathan, S., & Raman, R. (2023). Cyberbullying research - Alignment to sustainable development and impact of COVID-19: Bibliometrics and science mapping analysis. *Computers in Human Behavior, 140*, 107566. https://doi.org/10.1016/j.chb.2022.107566

Akgün, Ö. E., & Topal, M. (2015). Eğitim fakültesi son sınıf öğrencilerinin bilişim güvenliği farkındalıkları: Sakarya Üniversitesi Eğitim Fakültesi örneği [Information security awareness of the senior teacher students: Sakarya University sample]. *Sakarya University Journal of Education, 5*(2), 98-121. https://doi.org/10.19126/suje.73391

Akman, T. P., & Demir, M. (2021). Üniversite öğrencilerinin bilinçli farkındalıkları ile bilişsel esneklikleri arasındaki ilişki [The relationship between mindfulness and cognitive flexibility of university students]. *Yaşam Becerileri Psikoloji Dergisi*, *5*(9), 11-20. https://doi.org/10.31461/ybpd.879554

Aksoğan, M., Bayer, H., Gülada, M. O., & Çelik, E. (2024). İletişim fakültesi öğrencilerinin siber güvenlik farkındalığı: İnönü üniversitesi örneği [Cyber security awareness of the students of the faculty of communication: İnönü University sample]. *Kesit Akademi Dergisi*, *13*, 271-288. https://dergipark.org.tr/en/pub/kesitakademi/issue/59829/864303

Alper, R., Akpınar, S., & Akpınar, Ö. (2021). Spor bilimleri fakültesi öğrencilerinin bilinçli farkındalık düzeylerinin belirlenmesi [Determining the levels of mindfulness of the students of the faculty of sports sciences]. *Düzce Üniversitesi Spor Bilimleri Dergisi*, *1*(1), 1-8. https://dergipark.org.tr/tr/pub/dujoss/issue/67645/1041330

Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior*, *136*, 107376. https://doi.org/10.1016/j.chb.2022.107376

Alpar, R. (2013). *Uygulamalı çok değişkenli istatistiksel yöntemler (4th ed.) [Applied multivariate statistical methods (4th ed.)]*. Detay Yayıncılık.

Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*, 102258. https://doi.org/10.1016/j.techsoc.2023.102258

Al-Balushi, A., Tarhini, A., Acikgoz, F., & Ali, S. (2023). Examining the factors that influence user information security behavior toward COVID-19 scams. *International Journal of Human-Computer Interaction*, 1-18. https://doi.org/10.1080/10447318.2023.2291608

Arslan, G. (2017). Psychological maltreatment, forgiveness, mindfulness, and internet addiction among young adults: A study of mediation effect. *Computers in Human Behavior, 72*, 57-66. https://doi.org/10.1016/j.chb.2017.02.037

Arslan, I. (2018). Bilinçli farkındalık, depresyon düzeyleri ve algılanan stres arasındaki ilişki [The relationship between mindfulness, levels of depression, and perceived stress]. *Birey ve Toplum Sosyal Bilimler Dergisi, 8*(2), 73-86. https://doi.org/10.20493/birtop.477445

Avcı, Ü., & Oruç, O. (2020). Üniversite öğrencilerinin kişisel siber güvenlik davranışları ve bilgi güvenliği farkındalıklarının incelenmesi [Investigation of the students' personal cyber security behaviour and information security awareness]. *İnönü Üniversitesi Eğitim Fakültesi Dergisi*, *21*(1), 284-303. https://doi.org/10.17679/inuefd.526390

Bekirler, A., & Bilaloğlu, R. G. (2022). Relationships between preschool teachers' cognitive flexibility, mindfulness, and self-efficacy. *Ege Eğitim Dergisi*, *23*(3), 301-318. https://doi.org/10.12984/egeefd.1084301

Bishop, S. R. (2002). What do we really know about mindfulness-based stress reduction?. *Psychosomatic Medicine, 64*(1), 71-83. https://doi.org/10.1097/00006842-200201000-00010

Bramm, S. M., Cohn, A. M., & Hagman, B. T. (2013). Can preoccupation with alcohol override the protective properties of mindful awareness on problematic drinking?. *Addictive Disorders & Their Treatment, 12*(1), 19-27. https://doi.org/10.1097/ADT.0b013e31824c886b

Bryman, A., & Cramer, D. (2002). *Quantitative data analysis with SPSS release 10 for Windows: A guide for social scientists*. Routledge. https://doi.org/10.4324/9780203471548

Brown, K. W., & Ryan, R. M. (2003). The benefits of being present: Mindfulness and its role in psychological well-being. *Journal of Personality and Social Psychology, 84*(4), 822. https://doi.org/10.1037/0022-3514.84.4.822

Büyüköztürk, Ş. (2007). *Sosyal bilimler için veri analizi el kitabı [Data analysis handbook for social sciences]*. Ankara: Pegem A Yayıncılık.

Chatzisarantis, N. L., & Hagger, M. S. (2007). Mindfulness and the intention-behavior relationship within the theory of planned behavior. *Personality and Social Psychology Bulletin, 33*(5), 663-676. https://doi.org/10.1177/0146167206297401

Chen, X., Wu, D., Chen, L., & Teng, J. K. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information & Management*, *55*(8), 1049-1060. https://doi.org/10.1016/j.im.2018.05.011

Çalışkan, F. C., Akmehmet-Şekerler, S., Kızıltepe, Z., Aydın Sünbül, Z., & Börkan, B. (2024). The mediating role of depression and anxiety on the relationship between mindfulness and college adjustment. British Journal of Guidance & Counselling, 52(4), 613-627. https://doi.org/10.1080/03069885.2023.2220896

Chen, Y. T., Shih, W. L., Lee, C. H., Wu, P. L., & Tsai, C. Y. (2021). Relationships among undergraduates' problematic information security behavior, compulsive internet use, and mindful awareness in Taiwan. *Computers & Education, 164*, 104131. https://doi.org/10.1016/j.compedu.2021.104131

Deniz, M. E., Erus, S. M., & Büyükcebeci, A. (2017). Bilinçli farkındalık ile psikolojik iyi oluş ilişkisinde duygusal zekanın aracılık rolü [Relationship between mindfulness and psychological well-being: The mediating role of emotional intelligence]. *Turkish Psychological Counseling and Guidance Journal, 7(*47), 17-31. https://dergipark.org.tr/en/pub/tpdrd/issue/42743/515880

Fraenkel, J., Wallen, N. ve Hyun, H. (2012). *How to design and evaluate research in education. 8th edition*. Columbus, OH: McGraw-Hill.

Franco, C., Amutio, A., López-González, L., Oriol, X., & Martínez-Taboada, C. (2016). Effect of a mindfulness training program on the impulsivity and aggression levels of adolescents with behavioral problems in the classroom. *Frontiers in Psychology, 7*, 1385. https://doi.org/10.3389/fpsyg.2016.01385

Frauenstein, E. D., & Flowerday, S. (2020). Susceptibility to phishing on social network sites: A personality information processing model. *Computers & Security*, *94*, 101862. https://doi.org/10.1016/j.cose.2020.101862

Gámez-Guadix, M., & Calvete, E. (2016). Assessing the relationship between mindful awareness and problematic Internet use among adolescents. *Mindfulness, 7*, 1281-1288. https://doi.org/10.1007/s12671-016-0566-0

Gautam, A., & Mathur, R. (2018). Influence of mindfulness on decision making and psychological flexibility among aircrew. *Journal of Psychosocial Research, 13*(1), 199-207. https://doi.org/10.32381/JPR.2018.13.01.19

Gerdenitsch, C., Wurhofer, D., & Tscheligi, M. (2023). Working conditions and cybersecurity: Time pressure, autonomy and threat appraisal shaping employees' security behavior. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *17*(4). https://doi.org/10.5817/CP2023-4-7

Goilean, C., Gracia, F. J., & Tomás, I. (2023). Clarifying the relationship between trait mindfulness and objective performance. *Current Psychology*, *42*(14), 12241-12256. https://doi.org/10.1007/s12144-021-02414-y

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security, 73*, 345-358. https://doi.org/10.1016/j.cose.2017.11.015

Gültekin, V., & Özel, N. (2023). Üniversite öğrencilerinin bilgi güvenliği farkındalığı: Ankara Üniversitesi örneği [Information security awareness of university students: Example of Ankara University]. *Bilgi Yönetimi*, *6*(2), 310-331. https://doi.org/10.33721/by.1366855

Hanh, T. N. (1976). *Miracle of mindfulness*. Boston: Beacon.

Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal, 6*(1), 1-55. https://doi.org/10.1080/10705519909540118

Jansen, J., & Van Schaik, P. (2017). Comparing three models to explain precautionary online behavioural intentions. *Information & Computer Security, 25*(2), 165-180. https://doi.org/10.1108/ICS-03-2017-0018

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems, 34*(2), 597-626. https://doi.org/10.1080/07421222.2017.1334499

Kahneman, D. (2011). *Fast and slow thinking*. Farrar, Straus and Giroux, New York, USA.

Karacı, A., Akyüz, H. İ. ve Bilgici, G. (2017). Üniversite öğrencilerinin siber güvenlik davranışlarının incelenmesi [Investigation of cyber security behaviors of university students]. *Kastamonu Eğitim Dergisi*, *25*(6), 2079-2094. https://doi.org/10.24106/kefdergi.351517

Karaoğlan-Yılmaz, F. G., Yılmaz, R., & Sezer, B. (2014). Üniversite öğrencilerinin güvenli bilgi ve iletişim teknolojisi kullanım davranışları ve bilgi güvenliği eğitimine genel bir bakış [Secure information and communication technology usage behavior of university students and an overview to information security training]. *Bartın University Journal of Faculty of Education*, *3*(1), 176-199. https://dergipark.org.tr/en/pub/buefad/issue/3814/51178

Karasar, N. (2011). *Bilimsel araştırma yöntemleri (25. Basım)*. Nobel Yayınevi.

Keser, H., & Güldüren, C. (2015). Bilgi güvenliği farkindalik ölçeği (BGFÖ) geliştirme [Development of information security awareness scale]. *Kastamonu Eğitim Dergisi*, *23*(3), 1167-1184. https://dergipark.org.tr/en/pub/kefdergi/issue/22598/241397

Kovačević, A., Putnik, N., & Tošković, O. (2020). Factors related to cyber security behavior. *IEEE Access*, *8*, 125140-125148. https://doi.org/10.1109/ACCESS.2020.3007867

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security, 105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Lan, Y., Ding, J. E., Li, W., Li, J., Zhang, Y., Liu, M., & Fu, H. (2018). A pilot study of a group mindfulness-based cognitive-behavioral intervention for smartphone addiction among university students. *Journal of Behavioral Addictions, 7*(4), 1171-1176. https://doi.org/10.1556/2006.7.2018.103

Langer, E. J. (2016). *The power of mindful learning*. Hachette UK.

Leary, M. R., Adams, C. E., & Tate, E. B. (2006). Hypo-egoic self-regulation: Exercising self-control by diminishing the influence of the self. *Journal of Personality, 74*(6), 1803-1832. https://doi.org/10.1111/j.1467-6494.2006.00429.x

Li, W., Garland, E. L., McGovern, P., O'brien, J. E., Tronnier, C., & Howard, M. O. (2017). Mindfulness-oriented recovery enhancement for internet gaming disorder in US adults: A stage I randomized controlled trial. *Psychology of Addictive Behaviors, 31*(4), 393. https://doi.org/10.1037/adb0000269

Liu, S., Liu, Y., & Ni, Y. (2018). A review of mindfulness improves decision making and future prospects. *Psychology, 9*(2), 229-248. https://doi.org/10.4236/psych.2018.92015

Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior, 92*, 139-150. https://doi.org/10.1016/j.chb.2018.11.002

Merhi, M. I., & Ahluwalia, P. (2019). Examining the impact of deterrence factors and norms on resistance to information systems security. *Computers in Human Behavior, 92*, 37-46. https://doi.org/10.1016/j.chb.2018.10.031

Misra, G., Singh, P., Ramakrishna, M., & Ramanathan, P. (2022). Technology as a double-edged sword: Understanding life experiences and coping with COVID-19 in India. *Frontiers in Psychology, 12*, 800827. https://doi.org/10.3389/fpsyg.2021.800827

Moore, R. (2014). *Cybercrime: Investigating high-technology computer crime*. Routledge. https://doi.org/10.4324/9781315721767

Murphy, C., & MacKillop, J. (2012). Living in the here and now: Interrelationships between impulsivity, mindfulness, and alcohol misuse. *Psychopharmacology, 219*, 527-536. https://doi.org/10.1007/s00213-011-2573-0

Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S., & Porras, J. (2023). Mitigation strategies against the phishing attacks: A systematic literature review. *Computers & Security*, 103387. https://doi.org/10.1016/j.cose.2023.103387

Nederhof, A. J. (1985). Methods of coping with social desirability bias: A review. *European Journal of Social Psychology*, *15*(3), 263-280. https://doi.org/10.1002/ejsp.2420150303

NICCS (2018). *Explore terms: A glossary of common cybersecurity words and phrases*. Retrieved April 24, 2024 from https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary

Nunnally, J. C. (1994). *Psychometric theory 3E*. Tata McGraw-Hill Education.

Özyeşil, Z., Arslan, C., Kesici, Ş., & Deniz, M. E. (2011). Bilinçli farkındalık ölçeği'ni Türkçeye uyarlama çalışması [Adaptation of the mindful attention awareness scale into Turkish]. *Eğitim ve Bilim, 36*(160), 224-235. https://eb.ted.org.tr/index.php/EB/article/view/697

Paliszkiewicz, J. (2019). Information security policy compliance: Leadership and trust. *Journal of Computer Information Systems, 59*(3), 211-217. https://doi.org/10.1080/08874417.2019.1571459

Peters, J. R., Erisman, S. M., Upton, B. T., Baer, R. A., & Roemer, L. (2011). A preliminary investigation of the relationships between dispositional mindfulness and impulsivity. *Mindfulness, 2*, 228-235. https://doi.org/10.1007/s12671-011-0065-2

Reynolds, B., Ortengren, A., Richards, J. B., & De Wit, H. (2006). Dimensions of impulsive behavior: Personality and behavioral measures. *Personality and Individual Differences, 40*(2), 305-315. https://doi.org/10.1016/j.paid.2005.03.024

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

Sarıtepeci, M., Yıldız-Durak, H., Özüdoğru, G., & Atman-Uslu, N. (2024). The role of digital literacy and digital data security awareness in online privacy concerns: A multi-group analysis with gender. *Online Information Review*, (ahead-of-print). https://doi.org/10.1108/OIR-03-2023-0122

Seki, T., Çimen, F., & Dilmaç, B. (2023). The effect of emotional intelligence on cyber security: The mediator role of mindfulness. *Bartın University Journal of Faculty of Education, 12*(1), 190-199. https://doi.org/10.14686/buefad.1040614

Semple, R. J., Lee, J., Rosa, D., & Miller, L. F. (2010). A randomized trial of mindfulness-based cognitive therapy for children: Promoting mindful attention to enhance social-emotional resiliency in children. *Journal of Child and Family Studies, 19*, 218-229. https://doi.org/10.1007/s10826-009-9301-y

Shapiro, S. L., Jazaieri, H., & Goldin, P. R. (2012). Mindfulness-based stress reduction effects on moral reasoning and decision making. *The Journal of Positive Psychology, 7*(6), 504-515. https://doi.org/10.1080/17439760.2012.723732

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information & Computer Security*, *23*(2), 200-217. http://doi.org/10.1108/ICS-04-2014-0025

STATISTA (2024a). *Internet usage worldwide - statistics & facts*. Retrieved April 11, 2024 from https://www.statista.com/topics/1145/internet-usage-worldwide.

STATISTA (2024b). Mobile i*nternet usage worldwide - statistics & facts*. Retrieved April 11, 2024 from https://www.statista.com/topics/779/mobile-internet.

STATISTA (2024c). *Social media - statistics & facts*. Retrieved April 11, 2024 from https://www.statista.com/topics/1164/social-networks.

Stratton, K. J. (2006). Mindfulness-based approaches to impulsive behaviors. *The New School Psychology Bulletin, 4*(2), 49-71. https://nspb.net/index.php/nspb/article/view/145/81

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

Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity behavior among government employees: The role of protection motivation theory and responsibility in mitigating cyberattacks. *Information*, *13*(9), 413-430. https://doi.org/10.3390/info13090413

Tabachnick, B. G., & Fidell, L. S. (2007). Multivariate analysis of variance and covariance. *Using Multivariate Statistics, 3*, 402-407.

Tabachnick, B. G., & Fidell, L. S. (2013). *Using multivariate statistics. 6th ed*. Boston, MA: Pearson Education.

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

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security*, *70*, 376-391. https://doi.org/10.1016/j.cose.2017.07.003

Tokmak, M. (2023). Öğrencilerin siber güvenlik farkındalık düzeylerinin makine öğrenmesi yöntemleri ile belirlenmesi [Determination of cyber security awareness levels of students with machine learning methods]. *Yüzüncü Yıl Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, *28*(2), 451-466. https://doi.org/10.53433/yyufbed.1181694

Verhaeghen, P. (2021). Mindfulness as attention training: Meta-analyses on the links between attention performance and mindfulness interventions, long-term meditation practice, and trait mindfulness. *Mindfulness, 12*, 564-581. https://doi.org/10.1007/s12671-020-01532-1

Verkijika, S. F. (2019). "If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender. *Computers in Human Behavior*, *101*, 286-296. https://doi.org/10.1016/j.chb.2019.07.034

Vihari, N. S., Sinha, N. K., Tyagi, A., & Mittal, S. (2022). Effect of mindfulness on online impulse buying: Moderated mediation model of problematic internet use and emotional intelligence. *Frontiers in Psychology, 13*, 1012331. https://doi.org/10.3389/fpsyg.2022.1012331

Wu, D. (2020). Empirical study of knowledge withholding in cyberspace: Integrating protection motivation theory and theory of reasoned behavior. *Computers in Human Behavior*, *105*, 106229. https://doi.org/10.1016/j.chb.2019.106229

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?. *Computers in Human Behavior, 84*, 375-382. https://doi.org/10.1016/j.chb.2018.02.019

Yıldız-Durak, H. (2019). Human factors and cybersecurity in online game addiction: An analysis of the relationship between high school students' online game addiction and the state of providing personal cybersecurity and representing cyber human values in online games. *Social Science Quarterly*, *100*(6), 1984-1998. https://doi.org/10.1111/ssqu.12693

Yiğit, M. F., & Seferoğlu, S. S. (2019). Öğrencilerin siber güvenlik davranışlarının beş faktör kişilik özellikleri ve çeşitli diğer değişkenlere göre incelenmesi [Investigating students' cyber security behaviors in relation to big five personality traits and other various variables]. *Mersin Üniversitesi Eğitim Fakültesi Dergisi*, *15*(1), 186-215. https://doi.org/10.17860/mersinefd.437610

Yiğit, M. F., & Seferoğlu, S. S. (2020). Bireylerin siber güvenlik davranışlarını etkileyen faktörler üzerine bir inceleme [An examination of factors influencing individuals' cybersecurity behaviors]. H. F. Odabaşı, B. Akkoyunlu & A. İşman (Ed). *Eğitim teknolojileri okumaları 2020* (4. Bölüm, ss. 55-75). Pegem Akademi, Ankara.

Zimmerman, B. J. (2002). Becoming a self-regulated learner: An overview. *Theory into Practice*, *41*(2), 64-70. https://doi.org/10.1207/s15430421tip4102_2

Zorlu, E. (2023). An examination of the relationship between college students' cyberbullying awareness and ability to ensure their personal cybersecurity. *Journal of Learning and Teaching in Digital Age*, *8*(1), 55-70. https://doi.org/10.53850/joltida.1087377