

Araştırma Makalesi / Research Article**Antagonistic Personality And Cybersecurity Awareness: The Mediating Role of Mindfulness And Social Media Addiction**

Antagonistik Kişilik ve Siber Güvenlik Farkındalığı: Bilinçli Farkındalık ve Sosyal Medya Bağımlılığının Aracı Rolü

Kağan KIRCABURUN¹



, İbrahim DUMAN²



& Emrah EMİRTEKİN³



DOI : [10.63556/ankad.v10i3.448](https://doi.org/10.63556/ankad.v10i3.448)

Geliş/Received: 20/02/2026

Kabul/Accepted: 25/04/2026

Abstract

As social media becomes increasingly embedded in everyday life, understanding who remains vulnerable to cyber threats — and why — has become a pressing concern. This study examined whether antagonistic personality traits (narcissism, Machiavellianism, and psychopathy) undermine cybersecurity awareness (CSA) directly or through two psychological pathways: reduced mindfulness and heightened social media addiction (SMA). Using path analysis in a sample of 330 active social media users (47.6% female; Mage = 44.36), we tested these associations in the total sample and separately by gender. Results revealed a pattern of indirect, gender-specific effects. Psychopathy was the only trait with a significant direct effect on CSA, and this emerged exclusively among women. Narcissism and Machiavellianism operated indirectly — via SMA and mindfulness, respectively — yet neither produced a significant total effect on CSA, suggesting that self-enhancing and strategic cognitive tendencies partially offset their risk-related pathways. Mindfulness emerged as a protective factor, directly predicting higher CSA among men and indirectly through reduced SMA across the full sample. These findings conceptualize CSA as a psychologically complex outcome shaped by competing personality-driven processes, with meaningfully different risk profiles for men and women.

Keywords: Cybersecurity, mindfulness, social media, antagonistic personality, social media addiction.

Öz

Sosyal medyanın gündelik yaşama giderek daha fazla entegre olması, kullanıcıların siber güvenlik farkındalığına (SGF) yönelik kaygıları artırmış ve güvenli çevrimiçi davranışlarla ilişkili bireysel düzeydeki psikolojik faktörlerin belirlenmesi gerekliliğini ortaya koymuştur. Bu çalışmada, antagonistik kişilik özellikleri (narsisizm, Makyavelizm ve psikopati), bilinçli farkındalık, sosyal medya bağımlılığı (SMA) ve SGF arasındaki doğrudan ve dolaylı ilişkiler incelenmiştir. Veriler; aktif sosyal medya kullanan yetişkinlerden oluşan bir örneklemde (N = 330; %47.6 kadın; Mage = 44.36) geçerliği kanıtlanmış öz bildirim ölçekleri kullanılarak toplanmıştır. Yol analizi sonuçları, psikopatinin yalnızca kadınlarda SGF ile negatif yönde ilişkili olduğunu göstermiştir. Bilinçli farkındalık, toplam örneklemde SMA aracılığıyla SGF ile anlamlı bir dolaylı ilişki sergilerken, bilinçli farkındalık ile SGF arasındaki doğrudan pozitif ilişki yalnızca erkeklerde ortaya çıkmıştır. Makyavelizm, hem toplam örneklemde hem de erkek

¹ Sorumlu Yazar/Corresponding author: Dr. Öğr. Üyesi, Eğitim Bilimleri Bölümü, Eğitim Fakültesi, Düzce Üniversitesi, Düzce, Türkiye, kircaburunkagan@gmail.com

² Dr. Öğr. Üyesi, Eğitim Bilimleri Bölümü, Eğitim Fakültesi, Düzce Üniversitesi, Düzce, Türkiye, ibrahimduman@duzce.edu.tr

³ Dr. Öğr. Üyesi, Veri Bilimi ve Analitiği Bölümü, Bilgisayar ve Bilişim Bilimleri Fakültesi, Celal Bayar Üniversitesi, Manisa, Türkiye, emrah.emirtekin@cbu.edu.tr

Önerilen Atıf/Suggestion Citation

Kırcaburun, K., Duman, İ. & Emirtekin, E. (2026). Antagonistic Personality And Cybersecurity Awareness: The Mediating Role of Mindfulness And Social Media Addiction. *Anadolu Kültürel Araştırmalar Dergisi*, 10(3), 1506-1523.

alt örnekleminde bilinçli farkındalık aracılığıyla SGF ile dolaylı ve negatif yönde ilişkili bulunmuş; ancak bu dolaylı yol anlamlı bir toplam etkiye dönüşmemiştir. Benzer biçimde, narsisizm toplam örnekleme SMA aracılığıyla SGF ile negatif bir dolaylı ilişki göstermiş, ancak SGF üzerindeki genel etkisi anlamlı değildir. Bu bulgular, kişilik özellikleri, bilinçli farkındalık ve SMA'nın siber güvenlik farkındalığı ile ilişkilerinin karmaşık ve cinsiyete özgü yollar üzerinden şekillendiğini ortaya koymakta ve daha güvenli çevrimiçi davranışlara yönelik önemli çıkarımlar sunmaktadır.

Anahtar Kelimeler: Siber güvenlik, bilinçli farkındalık, sosyal medya, antagonistik kişilik, sosyal medya bağımlılığı

1. INTRODUCTION

Over the past decade, rapid advances in information technologies have profoundly reshaped daily life and accelerated global internet use, largely driven by the increasing accessibility of digital tools and the growing demand for online connectivity (Hong et al., 2023). Despite this widespread digital engagement, a substantial proportion of users remain insufficiently informed about online risks, commonly referred to as cyber threats or hazards (Akter et al., 2025). Many individuals lack even basic knowledge of how to protect their devices and personal data, and in extreme cases, this deficiency reflects a near absence of cybersecurity awareness, leaving users unlikely to adopt even minimal protective measures (Hong et al., 2023).

Cybersecurity awareness (CSA) can be defined as the extent to which individuals understand the importance of information security and recognize their responsibility to apply appropriate security practices to protect organizational data and network systems (Shaw et al., 2009). Prior research indicates that limited awareness of cyber risks is widespread and extends beyond technical contexts to everyday digital behaviors, such as mobile application use and information sharing on social media platforms (Arpaci et al., 2025). Importantly, malicious actors tend to target users with lower levels of CSA, as such individuals constitute the most vulnerable points of entry due to both software vulnerabilities and security gaps arising from unintentional user behavior (Akter et al., 2025; Hong et al., 2023). Collectively, these considerations suggest that CSA should be conceptualized not merely as a technical skill, but as a behavioral and psychological construct shaped by individual differences (Seki et al., 2023).

Despite growing interest in the psychological determinants of CSA, several notable gaps remain in the literature. First, empirical evidence based on adult samples from Western countries is still limited, with much of the existing research relying on student populations or non-Western contexts, thereby constraining the generalizability of current findings (Corallo et al., 2022). Second, although personality traits have been increasingly recognized as relevant antecedents of digital risk-related behaviors (Seki et al., 2023), the role of the Dark Triad — narcissism, Machiavellianism, and psychopathy — which share antagonism as a common interpersonal core (Jonason & Webster, 2010; Simpson & Schermer, 2026), remains underexplored in relation to CSA. Although these traits are traditionally referred to as the Dark Triad, the present study adopts the theoretically neutral term antagonistic personality traits to emphasize their shared interpersonal core — characterized by callousness, manipulateness, and disregard for others — rather than implying a moral judgment (Chester et al., 2025).

Moreover, little is known about the psychological mechanisms through which such traits may influence CSA. The present study addresses this gap by drawing on a self-regulation framework: antagonistic traits are theorized to impair the deliberate, effortful processing that protective cybersecurity behavior requires, both directly and through two downstream regulatory mechanisms — reduced mindfulness and heightened social media addiction (SMA) — each of which further erodes attentional control and self-regulatory capacity in digital environments (Durak, 2019; Seki et al., 2023). This impairment is expected to operate through both cognitive processes (e.g., diminished risk awareness and reduced attention to security cues) and behavioral tendencies (e.g., increased engagement in risky online practices), ultimately leading to lower levels of cybersecurity awareness.

1.1. Antagonistic personality and cybersecurity awareness

Personality plays a significant role in understanding cybersecurity-related behaviors (Shappie et al., 2020). Previous research has examined the Big Five personality traits in relation to cybersecurity behavior; however, there is no clear consensus regarding which traits are most influential (Naga et al., 2024). Existing evidence suggests that broader personality structure is meaningfully associated with

cybersecurity behaviors, with conscientiousness and openness emerging as particularly relevant traits (Shappie et al., 2020). Beyond the Big Five framework, trait emotional intelligence is positively related to CSA (Seki et al., 2023). Nevertheless, despite growing interest in dispositional predictors, the potential role of antagonistic personality characteristics has received comparatively little empirical attention in the cybersecurity literature.

The antagonistic traits (also known as the Dark Triad) framework comprises three related subclinical personality dimensions: narcissism, Machiavellianism, and psychopathy (Jonason & Webster, 2010). Narcissism involves inflated self-perceptions and includes both antagonistic tendencies toward others and agentic self-enhancement processes (Orth et al., 2024), whereas Machiavellianism reflects strategic manipulation combined with a cynical and distrustful view of others (Razmus et al., 2024). Psychopathy is commonly described as a multidimensional construct characterized by antisocial behavior, interpersonal manipulation, emotional callousness, and impulsive or erratic lifestyles (Forth et al., 2022). In the cybersecurity domain, in particular, antagonistic traits have predominantly been examined as predictors of cyber misconduct and attacks against others or organizations, rather than as individual risk factors for susceptibility to cyber victimization (Jones et al., 2021). However, a small number of research indicates that individuals with higher levels of antagonistic personality traits may also be more susceptible to online crime victimization (Stiff & Reeves, 2024). This heightened susceptibility to victimization may stem from an underlying deficit in protective cognitive frameworks, specifically in how these individuals perceive and respond to digital threats.

Individuals high in antagonistic traits may exhibit lower levels of cybersecurity awareness due to dispositional characteristics that undermine careful risk evaluation and self-regulatory control (Babakr & Fatahi, 2023). Machiavellian and psychopathic tendencies are often associated with instrumental thinking, overconfidence, and reduced concern for potential negative consequences (Sekścińska & Rudzinska-Wojciechowska, 2020), which may lead such individuals to underestimate cyber risks or ignore recommended security practices. Similarly, narcissistic individuals' inflated self-perceptions and sense of invulnerability may foster unrealistic optimism regarding their ability to avoid online threats (Brunzel, 2021), reducing motivation to engage in protective behaviors. Collectively, these traits may weaken attentional vigilance and precautionary decision-making in digital environments, thereby increasing susceptibility to cyber risks (Fenz et al., 2014). This body of evidence supports the inclusion of all three antagonistic traits—narcissism, Machiavellianism, and psychopathy—as independent predictors in the present model, as each is theoretically linked to the attentional and motivational deficits that underlie reduced cybersecurity awareness. Consequently, we expect antagonistic personality traits to inversely associate with CSA.

1.2. The mediating role of mindfulness

Mindfulness can be defined as a relatively stable individual tendency to maintain attentive awareness of present-moment experiences in daily life (Brown & Ryan, 2003). It involves both awareness and attention, which are closely intertwined processes whereby attention selects and sustains specific stimuli within the broader field of awareness (Brown & Ryan, 2003). From this perspective, mindfulness reflects a state of being mentally alert and actively engaged with ongoing internal and external events, rather than operating on automatic pilot (Tomlinson et al., 2018). In the context of cybersecurity, higher levels of mindfulness may enhance individuals' ability to notice potential digital threats, reflect on their online actions, and respond more deliberately to security-related cues. By promoting conscious attention and reducing mindless or habitual behaviors, mindfulness can play a protective role in preventing security violations and risky online practices (Seki et al., 2023).

Personality traits play a central role in shaping individuals' capacity for mindful awareness. Antagonistic personality traits can theoretically be expected to show inverse associations with mindfulness, as these traits are largely characterized by self-centeredness, emotional detachment, and instrumental interpersonal styles that conflict with mindful awareness (Jonason & Webster, 2010). One of the core functions of mindfulness involves reducing ego-driven processing and increasing sensitivity to present-moment experiences beyond the self, which may weaken tendencies toward self-enhancement and entitlement commonly observed in narcissism (Carlson, 2013). In line with this reasoning, empirical evidence suggests that narcissistic traits are consistently negatively related to mindfulness, indicating

that heightened self-focus may hinder mindful attention to others and the environment (Ganster et al., 2025). Similarly, Machiavellianism, which reflects strategic manipulation and low interpersonal trust, has been shown to exhibit a moderate negative association with mindfulness, possibly because mindful awareness is incompatible with calculative and exploitative social orientations (Yuan et al., 2020).

Moreover, mindfulness may function as a regulatory buffer for more severe antisocial tendencies. For example, among individuals high in psychopathy, higher levels of mindfulness have been linked to reduced antisocial behavior, suggesting that mindful attention may partially offset impulsivity and callousness typically associated with psychopathic traits (Bronchain et al., 2019). Extending this regulatory perspective, mindfulness has been reported to partially mediate the association between emotional intelligence and cybersecurity awareness (Seki et al., 2023), while emotional intelligence itself tends to be inversely related to antagonistic traits (Michels & Schulze, 2021). Taken together, these findings position mindfulness as a key psychological mechanism through which antagonistic personality characteristics may indirectly undermine cybersecurity awareness. Accordingly, individuals with elevated levels of antagonistic traits are expected to exhibit lower mindfulness, which may subsequently compromise their capacity to maintain adequate cybersecurity awareness. This supports the inclusion of mindfulness as the first mediator in the present model: antagonistic traits are expected to suppress mindful attention, which in turn reduces the deliberate, security-oriented processing that underlies higher CSA.

1.3. The mediating role of social media addiction

Social media addiction (SMA) refers to excessive and compulsive engagement with social media that interferes with daily functioning and negatively affects individuals' psychological well-being (Andreassen & Pallesen, 2014). Although SMA is shaped by multiple factors, personality traits have consistently been identified as key predictors of maladaptive social media use (Brand et al., 2019). In this regard, a growing body of evidence links antagonistic traits to higher levels of SMA. Specifically, narcissism and Machiavellianism have been shown to relate to SMA indirectly through cyberstalking behaviors (Kırcaburun et al., 2018), whereas psychopathy has demonstrated a direct association with SMA (Demircioğlu & Köse, 2021). Taken together, these findings suggest that the self-centered, manipulative, and impulsive characteristics inherent in antagonistic traits may foster excessive and uncontrolled social media engagement, thereby increasing vulnerability to SMA.

Beyond dispositional risk factors, SMA can be linked to self-regulatory deficits, with mindfulness acting as a protective resource that may buffer the pathway from antagonistic traits-related self-control impairments to excessive social media use. Empirical evidence indicates that mindfulness mediates the relationship between trait emotional intelligence and SMA, even after controlling for depression and rumination (Kırcaburun et al., 2019). Moreover, mindfulness has been shown to relate to SMA both directly and indirectly through enhanced attention control and reduced fear of missing out (Chang et al., 2023). By strengthening impulse regulation and reducing stress and anxiety, mindfulness may help individuals disengage from habitual and compulsive social media use, thereby lowering vulnerability to SMA (You & Liu, 2022). Taken together, these findings support the expectation that mindfulness mediates the relationship between antagonistic traits and SMA.

Despite growing interest in problematic technology use, empirical research directly linking SMA to CSA remains limited. Existing evidence from related domains suggests that higher levels of internet addiction among employees are associated with poorer information security behaviors, particularly through heightened impulsivity and reduced planning capacity (Hadlington, 2017). Complementary findings among student samples also indicate that mindfulness-based awareness is more strongly associated with improved security behaviors when internet addiction is low, whereas elevated addictive use may attenuate these benefits (Chen et al., 2021). Together, these findings imply that addictive patterns of online engagement—such as SMA—may undermine cybersecurity awareness by exacerbating impulsive responding and weakening self-regulation, highlighting the importance of addressing problematic use to enhance cybersecurity-related outcomes. This supports the inclusion of SMA as the second mediator in the present model: through its links to impulsivity and weakened self-regulation, SMA provides a behavioral pathway through which both antagonistic traits and reduced mindfulness may ultimately translate into lower cybersecurity awareness.

1.4. The role of gender

Prior research has documented notable gender differences across the key psychological constructs examined in the present study. Men consistently report higher levels of antagonistic personality traits compared to women (Craker & March, 2016; Muris et al., 2017). Gender-based differences have also been observed in mindfulness, with women scoring higher on the observing dimension, whereas men tend to report higher levels of acting with awareness (Alispahic & Hasanbegovic-Anic, 2017). In contrast, women have been found to exhibit higher levels of SMA (Kırcaburun et al., 2018, 2019). Moreover, evidence from occupational settings suggests that women may report lower cybersecurity self-efficacy and engage in riskier cybersecurity behaviors than men (Anwar et al., 2017).

Beyond these empirical observations, the inclusion of gender in the model is also theoretically grounded in established psychological frameworks. From a social role theory perspective (Koenig & Eagly, 2014), gendered socialization processes shape individuals' behavioral tendencies, self-regulatory capacities, and risk-related decision-making patterns, which may influence how personality traits are expressed and translated into technology-related behaviors. Similarly, social cognitive theory (Bandura, 2002) posits that self-efficacy beliefs and behavioral regulation are partially shaped by socially constructed experiences, suggesting that men and women may differ in how they regulate their engagement with digital environments. These theoretical perspectives imply that gender is not merely a demographic control variable but a meaningful moderator that can alter the strength and direction of relationships among personality, mindfulness, SMA, and CSA. These systematic gender differences across all key constructs in the model—personality traits, mindfulness, SMA, and CSA—justify testing the proposed pathways separately for men and women, as pooled analyses may obscure gender-specific mechanisms that are theoretically and practically meaningful.

Consequently, the present study hypothesized that antagonistic traits would be negatively associated with CSA, both directly and indirectly through mindfulness and SMA. In addition, a serial mediation pathway was proposed in which antagonistic traits influence CSA sequentially via mindfulness and SMA. To account for potential gender-related differences, the proposed model was tested in the total sample as well as separately for men and women, while statistically controlling for age.

1.5. Hypotheses

Based on the theoretical arguments outlined above, the following hypotheses were formulated:

H1: Antagonistic personality traits (narcissism, Machiavellianism, and psychopathy) will be negatively associated with CSA.

H2: Antagonistic personality traits will be negatively associated with mindfulness.

H3: Antagonistic personality traits will be positively associated with SMA.

H4: Mindfulness will be positively associated with CSA.

H5: Mindfulness will be negatively associated with SMA.

H6: SMA will be negatively associated with CSA.

H7: Mindfulness will mediate the negative association between antagonistic personality traits and CSA (antagonistic traits → mindfulness → CSA).

H8: SMA will mediate the negative association between antagonistic personality traits and CSA (antagonistic traits → SMA → CSA).

H9: The above pathways will differ in magnitude or significance between men and women.

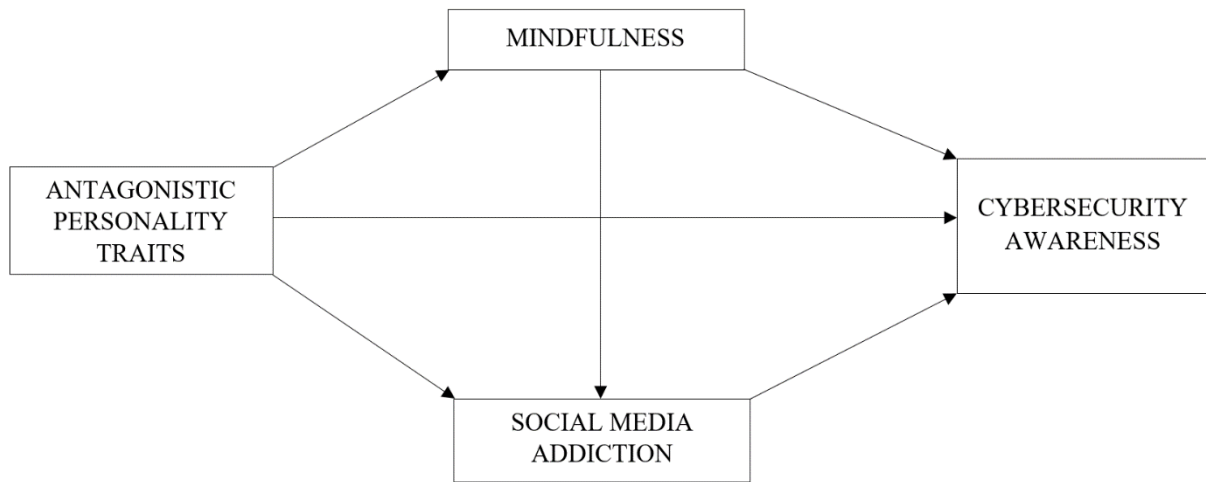


Figure 1. Theoretical model

2. METHODS

2.1. Participants and procedure

Participants were recruited through Prolific (prolific.com), a well-established and widely validated online participant recruitment platform that has been extensively used in behavioral and social science research (Peer et al., 2022). Prolific's data quality and sample representativeness have been empirically validated across multiple independent studies, with research consistently demonstrating that Prolific samples yield higher data quality, greater demographic diversity, and more replicable findings compared to both student convenience samples and alternative crowdsourcing platforms such as Amazon Mechanical Turk (Palan & Schitter, 2018; Peer et al., 2022). The final analytic sample consisted of 330 adults who indicated current use of social media platforms (47.6% female; Mage = 44.36, SDage = 13.94), with participant ages ranging from 19 to 80 years. Prior to participation, all respondents provided electronic informed consent by confirming that they had reviewed and understood the study information. Ethical approval for the study was obtained from the appropriate institutional review board, and all procedures were conducted in compliance with the ethical principles outlined in the Declaration of Helsinki.

2.2. Measures

At the outset of the survey, respondents reported basic demographic characteristics, including gender, age, country of residence, daily time spent using social media, and the social media platforms they used most frequently (see Table 1). Following the demographic section, participants completed a series of standardized self-report instruments assessing cybersecurity awareness (CSA), antagonistic personality characteristics, mindfulness, and social media addiction (SMA).

Cybersecurity Awareness Scale (CSAS): Participants' cybersecurity awareness was assessed using the CSAS (Arpaci et al., 2025). The scale comprises three subdimensions: confidentiality (8 items; e.g., "I do not share personal information such as my full name, birth date, and address on social media."), trust (6 items; e.g., "I am aware that sharing personal information on social media can pose risks such as identity theft and cyberbullying."), and privacy (5 items; e.g., "I am cautious about accepting video or voice call requests from people I do not know on social media."). All items are rated on a 5-point Likert scale ranging from 1 (never) to 5 (always). The scale demonstrated acceptable to good internal consistency, with Cronbach's alpha (α) value of .84 for the total scale. Reliability estimates for the subscales were .66 for confidentiality, .86 for trust, and .61 for privacy. Given that the CSAS had not been validated among English-speaking samples, a confirmatory factor analysis (CFA) was performed, and the results indicated acceptable to good fit indices. ($\chi^2 = 421.29$, $df = 163$, $p < .01$, RMSEA = .07, 90% CI [.06, .08], SRMR = .06, CFI = .87, GFI = .88).

Bergen Social Media Addiction Scale (BSMAS): The unidimensional BSMAS (Andreassen et al., 2016) was employed to assess social media addiction. The instrument comprises six items (e.g., “I felt an urge to use social media more and more.”), which are rated on a five-point Likert scale ranging from 1 (never) to 5 (always). The BSMAS has been extensively applied in prior research to measure a range of technology-related behavioral addictions. In the present sample, reliability analysis demonstrated satisfactory internal consistency ($\alpha = .88$).

Mindful Attention Awareness Scale (MAAS): The Mindful Attention Awareness Scale (MAAS; Brown & Ryan, 2003) was used to assess mindfulness. The scale consists of 15 items (e.g., “I find it difficult to stay focused on what’s happening in the present”), rated on a six-point Likert scale ranging from 1 (almost always) to 6 (almost never). Higher scores reflect greater levels of mindful attention and awareness. In the present sample, the scale demonstrated excellent internal consistency, with Cronbach’s α coefficient of .92.

Dark Triad Dirty Dozen Scale (DTDD): The DTDD (Jonason & Webster, 2010) was used to assess antagonistic personality characteristics. This self-report measure assesses three core personality traits: narcissism (e.g., “I tend to seek prestige or status.”), Machiavellianism (e.g., “I tend to exploit others for my own benefit.”), and psychopathy (e.g., “I tend to be unconcerned about the moral implications of my actions.”). Each trait is measured with four items, and responses are provided on a nine-point Likert-type scale ranging from 1 (strongly disagree) to 9 (strongly agree). Reliability analyses in the current sample indicated satisfactory internal consistency for narcissism ($\alpha = .87$), Machiavellianism ($\alpha = .86$), and psychopathy ($\alpha = .84$), supporting the reliability of the scale.

Table 1. Participants’ demographic characteristics

Variable		N	%
Gender			
	Men	173	52.4
	Women	157	47.6
Country			
	United Kingdom	140	42.4
	United States of America	123	37.3
	Canada	53	16.1
	South Africa	14	4.2
Daily use			
	Between 1-3 hours	160	48.5
	Between 0-1 hour	65	19.7
	Between 3-5 hours	56	17.0
	Between 5-7 hours	23	7.0
	I rarely use social media	13	3.9
	More than 7 hours	13	3.9
Platforms most used			
	YouTube	79	23.9
	Facebook	68	20.6
	Instagram	50	15.2
	Tiktok	46	13.9
	Whatsapp	36	10.9
	X (Twitter)	29	8.8
	Reddit	13	3.9
	Other	9	2.7

2.3. Data analytic strategy

Prior to conducting the primary analyses, the data were subjected to a series of preliminary screening procedures. Univariate normality was evaluated by inspecting skewness and kurtosis statistics. Descriptive statistics and bivariate correlation analyses were also performed to examine variable distributions and initial interrelationships, supporting the suitability of the data for subsequent parametric analyses. In addition, gender-related differences were tested using independent-samples t-

tests. To address the potential influence of common method variance, Harman's single-factor test was applied to determine whether a single latent factor accounted for a disproportionate share of variance across the measured constructs.

Model adequacy was evaluated using a combination of absolute and incremental fit indices, namely the comparative fit index (CFI), goodness-of-fit index (GFI), root mean square error of approximation (RMSEA), and standardized root mean square residual (SRMR). The interpretation of these indices followed established conventions in structural modeling research. Specifically, CFI and GFI values equal to or exceeding .90 were taken to reflect an acceptable level of model fit, whereas values of .95 or higher were considered indicative of a good fit. SRMR values below .08 were regarded as demonstrating satisfactory fit. With respect to RMSEA, values up to .08 were interpreted as acceptable, while values falling between .08 and .10 were viewed as indicative of a marginal yet defensible fit, particularly in the context of relatively complex models and larger sample sizes, in line with prior methodological recommendations (Byrne, 2010; Hu & Bentler, 1999; Kline, 2016).

Path analysis was employed to test the hypothesized direct and indirect relationships among antagonistic personality traits, mindfulness, social media addiction, and cybersecurity awareness (see Figure 1). Indirect pathways were evaluated using bias-corrected bootstrap procedures with 10,000 resampling iterations, with statistical significance determined via 95% confidence intervals. Furthermore, multi-group path analyses were conducted to examine whether the relationships varied as a function of gender. All analyses were performed using SPSS (Version 26) and AMOS (Version 24).

Table 2. Mean scores, standard deviations, and Pearson's correlations of the study variables (N=330)

	1	2	3	4	5	6
Cybersecurity awareness	-					
Social media addiction	-.27***	-				
Mindfulness	.27***	-.43***	-			
Narcissism	-.16**	.39***	-.22***	-		
Machiavellianism	-.24***	.35***	-.34***	.53***	-	
Psychopathy	-.24***	.18**	-.34***	.31***	.60***	-
Gender	-.06	-.05	.16**	.04	.13*	.17**
Age	.09	-.34***	.18**	-.18**	-.15**	-.00
Mean score	4.30	2.01	4.18	3.45	3.02	2.70
Standard deviation	.42	.82	.88	1.80	1.76	1.66
Skewness	-1.14	.75	-.22	.34	.59	1.11
Kurtosis	3.41	.06	-.21	-.83	-.74	.72

Note. * $p < .05$, ** $p < .01$, *** $p < .001$

2.4. Ethical approval

The conceptual framework of this study, the administration of data collection instruments, as well as the data collection, analysis, and interpretation processes were conducted in full compliance with ethical principles. ANKAD Editorial Board bears no responsibility for any potential ethical violations; all responsibility rests solely with the authors. I hereby declare that this study has not been submitted to any other academic publication venue for evaluation outside of ANKAD. All rules stipulated within the scope of the "Directive on Scientific Research and Publication Ethics of Higher Education Institutions" have been fully observed in this study. None of the actions defined under the second section of the Directive, entitled "Acts Contrary to Scientific Research and Publication Ethics", were committed. Ethical approval for this research was obtained from the Düzce University Rectorate Ethics Committee at its meeting dated 22/01/2026, meeting number 01, with decision number 2026/37.

3. RESULTS

3.1. Descriptive statistics

Table 2 summarizes the descriptive statistics along with Pearson correlation coefficients among the study variables. Cybersecurity awareness (CSA) demonstrated a positive association with mindfulness ($r = .27$, $p < .001$), while exhibiting negative associations with social media addiction (SMA) ($r = -.27$, $p <$

.001), narcissism ($r = -.16$, $p < .01$), Machiavellianism ($r = -.24$, $p < .001$), and psychopathy ($r = -.24$, $p < .001$). In addition, SMA showed an inverse relationship with mindfulness ($r = -.43$, $p < .001$) and positive relationships with narcissism ($r = .39$, $p < .001$), Machiavellianism ($r = .35$, $p < .001$), and psychopathy ($r = .18$, $p < .01$). Lastly, mindfulness was negatively associated with narcissism ($r = -.22$, $p < .001$), Machiavellianism ($r = -.34$, $p < .001$), and psychopathy ($r = -.34$, $p < .001$).

Gender differences across the study variables were assessed using independent-samples t-tests (coded as women = 1, men = 2), with detailed results not presented in tabular form. The analyses indicated that male participants scored significantly higher than female participants on Machiavellianism ($t[328] = -2.40$, $p < .05$), psychopathy ($t[328] = -3.08$, $p < .01$), and mindfulness ($t[328] = -3.01$, $p < .01$). Although female participants exhibited higher mean levels of CSA and SMA, these differences did not attain statistical significance.

3.2. Common method bias

In line with the guidelines proposed by Podsakoff et al. (2024), potential common method variance was assessed using Harman's single-factor test. Accordingly, an exploratory factor analysis was conducted on all study variables using principal component analysis with varimax rotation, constraining the extraction to a single factor. The results showed that the single factor accounted for 21.79% of the total variance, indicating that common method bias is unlikely to represent a serious concern for the validity of the findings.

3.3. Model testing

For the overall sample, the model demonstrated an acceptable fit to the data ($\chi^2 = 35.87$, $df = 15$, $p < .01$, RMSEA = .06, 90% CI [.04, .09], SRMR = .03, CFI = .97, GFI = .99). Comparable fit indices were observed in the male subsample ($\chi^2 = 29.45$, $df = 12$, $p < .01$, RMSEA = .09, 90% CI [.05, .13], SRMR = .04, CFI = .97, GFI = .97) as well as in the female subsample ($\chi^2 = 21.89$, $df = 12$, $p < .05$, RMSEA = .07, 90% CI [.02, .12], SRMR = .04, CFI = .97, GFI = .97). indicating an overall satisfactory model fit across groups.

Table 3 summarizes the standardized total, direct, and indirect effects estimated in the path analysis. Mindfulness exhibited a significant indirect positive association with CSA in the total sample ($\beta = .07$, $p < .01$; 95% CI [.02, .13]) and a strong direct association with CSA among men ($\beta = .36$, $p < .001$; 95% CI [.15, .53]). Psychopathy showed a significant negative direct effect on CSA in the female subsample ($\beta = -.32$, $p < .05$; 95% CI [-.54, -.08]). Narcissism was indirectly associated with CSA via SMA in the total sample ($\beta = -.06$, $p < .05$; 95% CI [-.13, -.02]); however, its overall (total) effect on CSA was not statistically significant. Likewise, Machiavellianism demonstrated a significant indirect association with CSA via mindfulness among men ($\beta = -.19$, $p < .01$; 95% CI [-.36, -.05]) and total sample ($\beta = -.07$, $p < .01$; 95% CI [-.15, -.02]), whereas its total effect on CSA did not reach statistical significance.

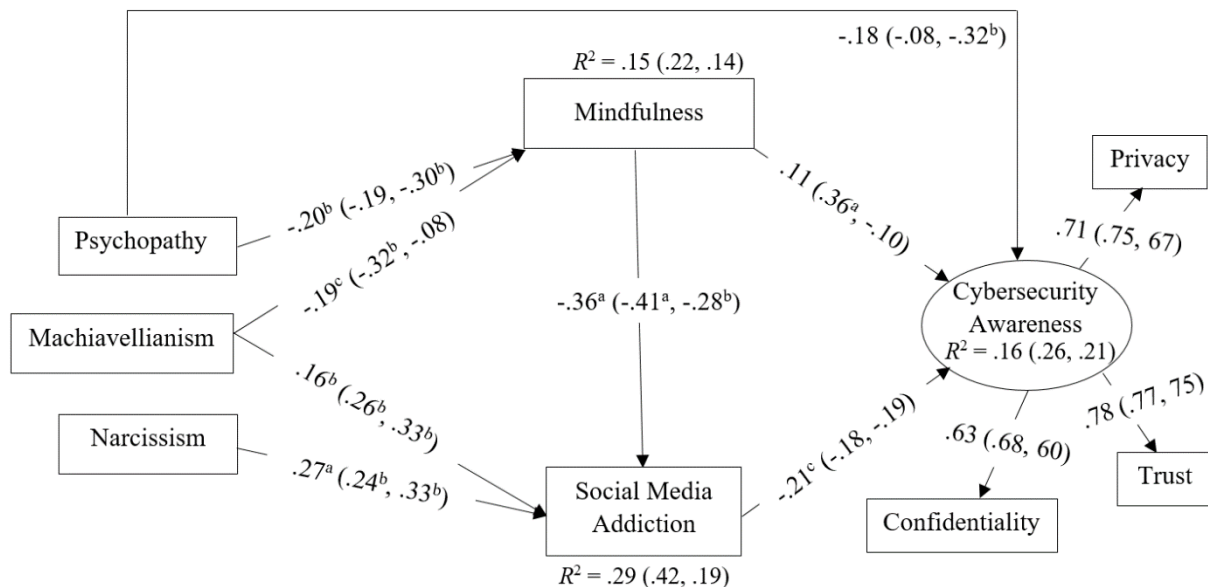
H1 (direct negative associations between antagonistic traits and CSA) received partial support: psychopathy was directly and negatively associated with CSA among women only, whereas narcissism and Machiavellianism showed no significant direct effects. H2 (antagonistic traits negatively associated with mindfulness) was supported for narcissism and Machiavellianism in the total sample and male subsample, but not for psychopathy. H3 (antagonistic traits positively associated with SMA) was supported for narcissism and Machiavellianism, but not for psychopathy. H4 (mindfulness positively associated with CSA) was supported directly among men and indirectly via SMA in the total sample. H5 (mindfulness negatively associated with SMA) was supported across samples. H6 (SMA negatively associated with CSA) was supported in the total sample only. H7 (mindfulness mediating antagonistic traits–CSA) was partially supported for Machiavellianism via mindfulness in men and the total sample. H8 (SMA mediating antagonistic traits–CSA) was partially supported for narcissism via SMA in the total sample. H9 (gender moderation) was supported, with several pathways differing meaningfully between men and women.

Table 3. Standardized estimates of total, direct, and indirect effects on cybersecurity awareness for overall sample and men and women.

	Effect (S.E.)		
	All Sample (N=330)	Men (N=173)	Women (N=157)
Narcissism → CSA (total effect)	-.09 (.09)	.01 (.13)	-.20 (.11)
→ CSA (direct effect)	-.03 (.09)	.07 (.13)	-.14 (.11)
→ SMA → CSA (indirect effect)	-.06** (.03)	-.06 (.05)	-.06 (.04)
Machiavellianism → CSA (total effect)	-.10 (.11)	-.12 (.16)	-.02 (.14)
→ CSA (direct effect)	-.03 (.10)	.07 (.13)	-.02 (.15)
→ Mindfulness → CSA (indirect effect)	-.07** (.03)	-.19** (.08)	.00 (.03)
Psychopathy → CSA (total effect)	-.19* (.09)	-.14 (.13)	-.29* (.11)
→ CSA (direct effect)	-.18 (.09)	-.08 (.13)	-.32* (.11)
→ CSA (indirect effect)	-.01 (.03)	-.06 (.06)	.03 (.04)
Mindfulness → CSA (total effect)	.19* (.08)	.43*** (.09)	-.04 (.10)
→ CSA (direct effect)	.11 (.08)	.36*** (.09)	-.10 (.11)
→ SMA → CSA (indirect effect)	.07** (.03)	.08 (.05)	.05 (.03)

Note. CSA = Cybersecurity awareness; SMA = Social media addiction. Only the significant indirect effects are shown in the table. * $p < .05$, ** $p < .01$, *** $p < .001$.

As depicted in Figure 2, the specified path model accounted for a substantial proportion of variance in CSA ($R^2 = .16$). In addition, the personality-related predictors included in the model explained notable levels of variance in mindfulness ($R^2 = .15$) and SMA ($R^2 = .29$). Notably, the model demonstrated greater explanatory power for mindfulness ($R^2 = .22$), SMA ($R^2 = .42$), and CSA ($R^2 = .26$) in the male subsample relative to the female subsample.

**Figure 2.** Final model of the significant path coefficients

Note. Latent constructs in the model are represented by circles, while observed indicators are illustrated as rectangles. Standardized path estimates are presented for the total sample outside the brackets;

estimates for men and women are reported on the left and right sides of the brackets, respectively. For presentation purposes, several paths were omitted from the figure. Specifically, non-significant associations as well as covariances among the error terms of the control, independent, and mediator variables are not displayed. $cp < .05$, $bp < .01$, $ap < .001$

4. DISCUSSION AND CONCLUSION

Rather than reflecting purely technical knowledge or skills, cybersecurity awareness (CSA) appears to be a behavioral and psychological construct that is closely intertwined with individual differences (Seki et al., 2023). The present study investigated the mechanisms underlying CSA using a path model. More specifically, the role of mindfulness and social media addiction (SMA) between antagonistic personality traits and CSA was examined among Western adults.

Partially consistent with expectations, psychopathy was directly and negatively associated with CSA only among women. Although the total effect of psychopathy on CSA was significant in the overall sample, neither direct nor indirect effects reached statistical significance when all participants were considered together. This pattern may be attributable to the absence of a theoretically relevant explanatory mechanism in the tested model that could capture the behavioral pathways through which psychopathy operates. H1 was therefore partially supported for psychopathy. The most parsimonious explanation is that psychopathic traits—impulsivity, callousness, and indifference to risk—disrupt the attentional vigilance that protective cybersecurity behavior requires, and this disruption is more pronounced in women because emotional processing deficits associated with psychopathy are expressed differently across genders (Forth et al., 2022; Pinheiro et al., 2024). The key limitation here is that the present model did not include behavioral mediators such as risk-taking propensity or security compliance, which likely capture the mechanisms through which psychopathy operates. Future studies should therefore incorporate objective behavioral measures of security practice—such as password hygiene or phishing click rates—to clarify whether the gender asymmetry reflects differential emotional processing, behavioral tendencies, or both.

Turning to H1 and H8 for narcissism; Narcissism showed an indirect negative association with CSA via SMA, yet its total effect on CSA was non-significant. The best-supported explanation for this suppression pattern is that grandiose narcissism carries competing influences: it elevates SMA through self-promotional motives (a risk-enhancing pathway), while simultaneously instilling overconfidence and perceived digital competence that attenuate the impact of compulsive social media use on security vigilance (Hepper et al., 2022; Jonason & Webster, 2010). A key limitation is that the present study did not measure these self-enhancing cognitions directly, making it impossible to confirm their buffering role. Future research should include measures of digital self-efficacy and perceived invulnerability to cyberthreats alongside narcissism, so that the compensatory mechanism can be tested rather than inferred.

Regarding H1 and H7 for Machiavellianism; Machiavellianism demonstrated a significant indirect negative association with CSA via mindfulness among men and in the total sample, yet its total effect did not reach significance. The suppression pattern here mirrors that of narcissism but operates through a different pathway: Machiavellian individuals score lower on mindfulness, which reduces security-oriented attention, but their characteristic strategic vigilance and goal-directed information processing lead them to attend to cybersecurity threats when it serves their instrumental interests—effectively neutralising the mindfulness deficit at the level of observed behaviour (Blötner & Bergold, 2022; Muris et al., 2017). The limitation is that the present model cannot disentangle these competing processes without including a measure of instrumental threat appraisal. Future research should incorporate context-specific vigilance scales to test whether Machiavellian individuals selectively attend to cyber risks that threaten their personal goals, which would directly account for the null total effect. Taken together, psychopathy appeared to be the most consistent antagonistic personality risk factor for CSA, because it lacks the cognitive compensatory resources observed in narcissism and Machiavellianism.

With respect to H4 and H7; Mindfulness was directly and positively associated with CSA among men and indirectly associated with CSA via SMA in the total sample, but showed no direct effect among women or in the total sample. The primary explanation is that mindfulness operates as a proximal cognitive resource—heightening situational awareness, strengthening impulse control, and enabling

deliberate rather than habitual online behaviour (Tomlinson et al., 2018)—and among men, these attentional benefits translate directly into security-relevant decisions without requiring the additional behavioural step of reduced social media use (Yiğit, 2025). The central limitation is that the model did not include cognitive mediators such as risk perception or security-related self-efficacy, which are the most plausible proximal mechanisms through which mindfulness acts on CSA (Ji et al., 2018). Future studies should therefore test a model in which mindfulness predicts CSA sequentially via attentional control and risk perception, and should examine whether this pathway is moderated by gender.

Addressing H6; SMA was negatively associated with CSA in the total sample, but this association did not reach significance in either gender subsample. Consistent with prior research on internet addiction and security behaviour (Chen et al., 2021; Hadlington, 2017), the most defensible interpretation is that compulsive social media engagement depletes attentional resources, promotes impulsive responding, and erodes the self-regulatory capacity needed to notice and act on cybersecurity cues (Wegmann et al., 2020)—a process that operates across the population but is not strong enough to be detected within gender-stratified subgroups of the present sample size. The principal limitation is statistical: with approximately 156 participants per subsample, the study was likely underpowered to detect the smaller within-gender effect of SMA on CSA. Future studies should recruit larger gender-balanced samples (minimum $n = 200$ per group based on power estimates for small-to-medium path coefficients) and pre-register gender-stratified SMA analyses to test whether the null subsample results reflect a genuine moderating role of gender or simply insufficient power.

Several limitations of the present study should be acknowledged. First, the use of a cross-sectional design restricts any causal interpretation of the observed associations among antagonistic personality traits, mindfulness, social media addiction, and cybersecurity awareness (CSA). Longitudinal or experimental designs would be necessary to clarify the temporal ordering of these relationships. Second, all variables were assessed using self-report measures, which may be subject to response biases such as social desirability or inaccurate self-perceptions, particularly in the context of cybersecurity-related behaviors. Third, although the model captured multiple psychological and behavioral pathways, it did not include alternative explanatory mechanisms such as risk perception, cybersecurity self-efficacy, or actual security practices, which may be especially relevant for understanding gender-specific effects. Finally, the generalizability of the findings may be limited by the characteristics of the sample, and future studies should attempt to replicate the model across different cultural contexts and occupational groups to strengthen external validity.

Despite these limitations, the present study contributes to the growing literature on cybersecurity awareness by demonstrating that CSA is shaped by a complex interplay of antagonistic personality traits, mindfulness, and social media addiction. The findings indicate that narcissism and Machiavellianism exert indirect and competing influences on CSA through behavioral and cognitive pathways, whereas psychopathy emerges as the most consistent antagonistic personality-related risk factor for lower cybersecurity awareness when traits are considered jointly. Moreover, mindfulness appears to function as a protective factor for CSA, particularly among men, while social media addiction operates as a general risk factor at the population level rather than within gender-specific groups. Taken together, these results highlight the importance of moving beyond simple bivariate associations and highlight the value of integrative models that account for both risk-enhancing and risk-mitigating processes. Such an approach may inform more targeted and psychologically informed interventions aimed at improving cybersecurity awareness in digitally intensive environments.

REFERENCES

- Akter, S., Uddin, M. R., Sajib, S., Lee, W. J. T., Michael, K., & Hossain, M. A. (2025). Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. *Annals of Operations Research*, 350(2), 673-698. <https://doi.org/10.1007/s10479-022-04844-8>
- Alispahic, S., & Hasanbegovic-Anic, E. (2017). Mindfulness: Age and gender differences on a Bosnian sample. *Psychological Thought*, 10(1), 155-166. <https://doi.org/10.5964/psyc.v10i1.224>
- Andreassen, C. S., Billieux, J., Griffiths, M. D., Kuss, D. J., Demetrovics, Z., Mazzoni, E., & Pallesen, S. (2016). The relationship between addictive use of social media and video games and symptoms

- of psychiatric disorders: A large-scale cross-sectional study. *Psychology of Addictive Behaviors*, 30(2), 252-262. <https://psycnet.apa.org/doi/10.1037/adb0000160>
- Andreassen, C. S., & Pallesen, S. (2014). Social network site addiction-an overview. *Current Pharmaceutical Design*, 20(25), 4053-4061. <https://doi.org/10.2174/13816128113199990616>
- Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69, 437-443. <https://doi.org/10.1016/j.chb.2016.12.040>
- Arpaci, I., Aslan, O., & Oner, I. E. (2025). Cybersecurity Awareness Scale (CSAS) for social media users: Development, validity and reliability study. *Information Development*, e02666669251336562. <https://doi.org/10.1177/026666669251336562>
- Babakr, Z., & Fatahi, N. (2023). Risk-taking Behaviour: The role of Dark Triad traits, impulsivity, sensation seeking and adverse childhood experience. *Acta Informatica Medica*, 31(4), 292-299. <https://doi.org/10.5455/aim.2023.31.292-299>
- Bandura, A. (2001). Social cognitive theory: An agentic perspective. *Annual Review of Psychology*, 52(1), 1-26. <https://doi.org/10.1146/annurev.psych.52.1.1>
- Blötner, C., & Bergold, S. (2022). To be fooled or not to be fooled: Approach and avoidance facets of Machiavellianism. *Psychological Assessment*, 34(2), 147-158. <https://doi.org/10.1037/pas0001069>
- Brand, M., Wegmann, E., Stark, R., Müller, A., Wölfling, K., Robbins, T. W., & Potenza, M. N. (2019). The Interaction of Person-Affect-Cognition-Execution (I-PACE) model for addictive behaviors: Update, generalization to addictive behaviors beyond internet-use disorders, and specification of the process character of addictive behaviors. *Neuroscience & Biobehavioral Reviews*, 104, 1-10. <https://doi.org/10.1016/j.neubiorev.2019.06.032>
- Bronchain, J., Monié, B., Becquie, S., Chabrol, H., & Raynal, P. (2019). To better understand the link between psychopathy and antisocial behavior: Moderation by dispositional mindfulness. *Psychopathology*, 52(3), 191-197. <https://doi.org/10.1159/000499663>
- 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), 822-848. <https://psycnet.apa.org/doi/10.1037/0022-3514.84.4.822>
- Brunzel, J. (2021). Overconfidence and narcissism among the upper echelons: A systematic literature review. *Management Review Quarterly*, 71(3), 585-623. <https://doi.org/10.1007/s11301-020-00194-6>
- Byrne, B. M. (2010). *Structural equation modeling with AMOS: Basic concepts, applications, and programming* (2nd ed.). New York: Routledge.
- Carlson, E. N. (2013). Overcoming the barriers to self-knowledge: Mindfulness as a path to seeing yourself as you really are. *Perspectives on Psychological Science*, 8(2), 173-186. <https://doi.org/10.1177/1745691612462584>
- Chang, H., Meng, X., Li, Y., Liu, J., Yuan, W., Ni, J., & Li, C. (2023). The effect of mindfulness on social media addiction among Chinese college students: A serial mediation model. *Frontiers in Psychiatry*, 14, e1087909. <https://doi.org/10.3389/fpsyt.2023.1087909>
- 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, e104131. <https://doi.org/10.1016/j.compedu.2021.104131>
- Chester, D. S., Lynam, D. R., & Miller, J. D. (2025). It is past time to abandon the term “dark” as a descriptor of antagonistic traits. *Journal of Psychopathology and Clinical Science*, 134(7), 691–692. <https://doi.org/10.1037/abn0001024>

- Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry*, 137, e103614. <https://doi.org/10.1016/j.compind.2022.103614>
- Craker, N., & March, E. (2016). The dark side of Facebook®: The Dark Tetrad, negative social potency, and trolling behaviours. *Personality and Individual Differences*, 102, 79-84. <https://doi.org/10.1016/j.paid.2016.06.043>
- Demircioğlu, Z. I., & Köse, A. G. (2021). Effects of attachment styles, dark triad, rejection sensitivity, and relationship satisfaction on social media addiction: A mediated model. *Current Psychology*, 40(1), 414-428. <https://doi.org/10.1007/s12144-018-9956-x>
- Durak, H. Y. (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>
- Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. *Information Management & Computer Security*, 22(5), 410-430. <https://doi.org/10.1108/IMCS-07-2013-0053>
- Forth, A., Sezlik, S., Lee, S., Ritchie, M., Logan, J., & Ellingwood, H. (2022). Toxic relationships: The experiences and effects of psychopathy in romantic relationships. *International Journal of Offender Therapy and Comparative Criminology*, 66(15), 1627-1658. <https://doi.org/10.1177/0306624X211049187>
- Ganster, F. M., Schwartz, K., Voracek, M., & Tran, U. S. (2025). Narcissism and mindfulness: A preregistered systematic review and three-level meta-analysis. *Personality and Individual Differences*, 246, e113299. <https://doi.org/10.1016/j.paid.2025.113299>
- Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(7), e00346. <https://doi.org/10.1016/j.heliyon.2017.e00346>
- Hepper, E. G., Ellett, L., Kerley, D., & Kingston, J. L. (2022). Are they out to get me? Individual differences in nonclinical paranoia as a function of narcissism and defensive self-protection. *Journal of Personality*, 90(5), 727-747. <https://doi.org/10.1111/jopy.12693>
- Hong, W. C. H., Chi, C., Liu, J., Zhang, Y., Lei, V. N. L., & Xu, X. (2023). The influence of social education level on cybersecurity awareness and behaviour: A comparative study of university students and working graduates. *Education and Information Technologies*, 28(1), 439-470. <https://doi.org/10.1007/s10639-022-11121-5>
- 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>
- Ji, M., Yang, C., Li, Y., Xu, Q., & He, R. (2018). The influence of trait mindfulness on incident involvement among Chinese airline pilots: The role of risk perception and flight experience. *Journal of Safety Research*, 66, 161-168. <https://doi.org/10.1016/j.jsr.2018.07.005>
- Jonason, P. K., & Webster, G. D. (2010). The dirty dozen: A concise measure of the dark triad. *Psychological Assessment*, 22(2), 420-432. <https://psycnet.apa.org/doi/10.1037/a0019265>
- Jones, D. N., Padilla, E., Curtis, S. R., & Kiekintveld, C. (2021). Network discovery and scanning strategies and the dark triad. *Computers in Human Behavior*, 122, e106799. <https://doi.org/10.1016/j.chb.2021.106799>
- Kırcaburun, K., Griffiths, M. D., & Billieux, J. (2019). Trait emotional intelligence and problematic online behaviors among adolescents: The mediating role of mindfulness, rumination, and depression. *Personality and Individual Differences*, 139, 208-213. <https://doi.org/10.1016/j.paid.2018.11.024>

- Kircaburun, K., Jonason, P. K., & Griffiths, M. D. (2018). The Dark Tetrad traits and problematic social media use: The mediating role of cyberbullying and cyberstalking. *Personality and Individual Differences*, 135, 264-269. <https://doi.org/10.1016/j.paid.2018.07.034>
- Kline, R. B. (2016). *Principles and Practice of Structural Equation Modeling* (4th ed.). Guilford Press.
- Koenig, A. M., & Eagly, A. H. (2014). Evidence for the social role theory of stereotype content: Observations of groups' roles shape stereotypes. *Journal of Personality and Social Psychology*, 107(3), 371-392. <http://dx.doi.org/10.1037/a0037215>
- Michels, M., & Schulze, R. (2021). Emotional intelligence and the dark triad: A meta-analysis. *Personality and Individual Differences*, 180, e110961. <https://doi.org/10.1016/j.paid.2021.110961>
- Muris, P., Merckelbach, H., Otgaar, H., & Meijer, E. (2017). The malevolent side of human nature: A meta-analysis and critical review of the literature on the dark triad (narcissism, Machiavellianism, and psychopathy). *Perspectives on Psychological Science*, 12(2), 183-204. <https://doi.org/10.1177/1745691616666070>
- Naga, J. F., Tinamisan, A. C., Maluya, M. O., Panal, A. D., & Tupac, T. A. (2024). Investigating the relationship between personality traits and information security awareness. *International Journal of Computing and Digital Systems*, 16(1), 1233-1246. <http://dx.doi.org/10.12785/ijcds/160191>
- Orth, U., Krauss, S., & Back, M. D. (2024). Development of narcissism across the life span: A meta-analytic review of longitudinal studies. *Psychological Bulletin*, 150(6), 643–665. <https://doi.org/10.1037/bul0000436>
- Palan, S., & Schitter, C. (2018). Prolific.ac—A subject pool for online experiments. *Journal of Behavioral and Experimental Finance*, 17, 22–27. <https://doi.org/10.1016/j.jbef.2017.12.004>
- Peer, E., Rothschild, D., Gordon, A., Evernden, Z., & Damer, E. (2022). Data quality of platforms and panels for online behavioral research. *Behavior Research Methods*, 54(4), 1643–1662. <https://doi.org/10.3758/s13428-021-01694-3>
- Pinheiro, M., Gonçalves, R. A., & Cunha, O. (2024). Emotional processing and psychopathy among women: A systematic review. *Deviant Behavior*, 45(10), 1366-1390. <https://doi.org/10.1080/01639625.2023.2295527>
- Podsakoff, P. M., Podsakoff, N. P., Williams, L. J., Huang, C., & Yang, J. (2024). Common method bias: It's bad, it's complex, it's widespread, and it's not easy to fix. *Annual Review of Organizational Psychology and Organizational Behavior*, 11(1), 17-61. <https://doi.org/10.1146/annurev-orgpsych-110721-040030>
- Razmus, W., Grabner-Kraeuter, S., & Adamczyk, G. (2024). Counterfeit brands and Machiavellianism: Consequences of counterfeit use for social perception. *Journal of Retailing and Consumer Services*, 76, e103579. <https://doi.org/10.1016/j.jretconser.2023.103579>
- 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>
- Sekścińska, K., & Rudzinska-Wojciechowska, J. (2020). Individual differences in Dark Triad traits and risky financial choices. *Personality and Individual Differences*, 152, e109598. <https://doi.org/10.1016/j.paid.2019.109598>
- Shappie, A. T., Dawson, C. A., & Debb, S. M. (2020). Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media*, 9(4), 475–480. <https://doi.org/10.1037/ppm0000247>
- Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, 52(1), 92-100. <https://doi.org/10.1016/j.compedu.2008.06.011>

- Stiff, C., & Reeves, M. (2024). Careful when you click? How the dark triad of personality can influence the likelihood of online crime victimization. *The Journal of Psychology*, 158(3), 238-256. <https://doi.org/10.1080/00223980.2023.2286451>
- Tomlinson, E. R., Yousaf, O., Vittersø, A. D., & Jones, L. (2018). Dispositional mindfulness and psychological health: A systematic review. *Mindfulness*, 9(1), 23-43. <https://doi.org/10.1007/s12671-017-0762-6>
- Wegmann, E., Müller, S. M., Turel, O., & Brand, M. (2020). Interactions of impulsivity, general executive functions, and specific inhibitory control explain symptoms of social-networks-use disorder: An experimental study. *Scientific Reports*, 10(1), e3866. <https://doi.org/10.1038/s41598-020-60819-4>
- Yiğit, M. F. (2025). Investigating the role of mindful awareness as an antecedent of university students' cyber security behaviors. *Journal of Learning and Teaching in Digital Age*, 10(2), 156-169. <https://doi.org/10.53850/joltida.1569182>
- You, C., & Liu, Y. (2022). The effect of mindfulness on online self-presentation, pressure, and addiction on social media. *Frontiers in Psychology*, 13, e1034495. <https://doi.org/10.3389/fpsyg.2022.1034495>
- Yuan, G., Liu, Z., & An, Y. (2020). Machiavellianism, mindfulness and cyberbullying among Chinese junior high school students: The mediating role of empathy. *Journal of Aggression, Maltreatment & Trauma*, 29(9), 1047-1058. <https://doi.org/10.1080/10926771.2019.1667467>

Araştırma Makalesi / Research Article

Antagonistic Personality And Cybersecurity Awareness: The Mediating Role of Mindfulness And Social Media Addiction

Antagonistik Kişilik ve Siber Güvenlik Farkındalığı: Bilinçli Farkındalık ve Sosyal Medya Bağımlılığının Aracı Rolü

Kağan KIRCABURUN¹ , İbrahim DUMAN²  & Emrah EMİRTEKİN³ 

DOI : [10.63556/ankad.v10i3.448](https://doi.org/10.63556/ankad.v10i3.448)

Geliş/Received: 20/02/2026

Kabul/Accepted: 25/04/2026

GENİŞLETİLMİŞ ÖZET

Giriş

Son on yılda bilgi ve iletişim teknolojilerindeki hızlı gelişmeler, gündelik yaşamı köklü biçimde dönüştürmüş ve internet kullanımını küresel ölçekte artırmıştır. Dijital araçlara erişimin kolaylaşması ve çevrimiçi bağlantıya yönelik artan talep, bireylerin sosyal medya, mobil uygulamalar ve çevrimiçi hizmetlerle daha yoğun etkileşim kurmasına yol açmıştır (Hong et al., 2023). Ancak bu yaygın dijital katılıma rağmen, kullanıcıların önemli bir bölümü çevrimiçi riskler ve siber tehditler konusunda yeterli bilgiye sahip değildir (Akter et al., 2025). Temel düzeyde güvenlik bilgisi eksikliği, bireylerin cihazlarını ve kişisel verilerini korumaya yönelik en basit önlemleri dahi almamasına neden olmakta ve bu durum siber güvenlik farkındalığının (SGF) ciddi biçimde zayıfladığını göstermektedir (Hong et al., 2023).

Siber güvenlik farkındalığı, bireylerin bilgi güvenliğinin önemini kavrama ve uygun güvenlik uygulamalarını hayata geçirme sorumluluğunu üstlenme düzeyi olarak tanımlanmaktadır (Shaw et al., 2009). Önceki çalışmalar, SGF'nin yalnızca teknik bilgiyle sınırlı olmadığını; mobil uygulama kullanımı ve sosyal medyada bilgi paylaşımı gibi gündelik dijital davranışlarla da yakından ilişkili olduğunu ortaya koymuştur (Arpaci et al., 2025). Özellikle düşük SGF düzeyine sahip bireyler, hem yazılımsal açıklar hem de istemeden gerçekleştirilen riskli davranışlar nedeniyle siber saldırganlar için en kırılgan hedefleri oluşturmaktadır (Akter et al., 2025; Hong et al., 2023). Bu bağlamda SGF, teknik bir beceriden ziyade bireysel farklılıklar tarafından şekillenen davranışsal ve psikolojik bir yapı olarak ele alınmalıdır (Seki et al., 2023).

Literatürde SGF'nin psikolojik belirleyicilerine yönelik ilgi giderek artsa da önemli boşluklar devam etmektedir. Özellikle Batı ülkelerinde yetişkin örneklerle yürütülen çalışmalar sınırlıdır ve mevcut bulgular çoğunlukla öğrenci ya da Batı dışı örneklemle dayanmaktadır (Corallo et al., 2022). Ayrıca kişilik özelliklerinin dijital risk davranışlarıyla ilişkisi bilinse de, antagonistik kişilik özelliklerinin (narsisizm, Makyavelizm ve psikopati) SGF ile ilişkisi ve bu ilişkinin altında yatan psikolojik mekanizmalar yeterince incelenmemiştir. Bu çalışma, öz-düzenleme ve davranışsal çerçevelerden hareketle, bilinçli farkındalık (mindfulness) ve sosyal medya bağımlılığını (SMA) antagonistik kişilik özellikleri ile SGF arasındaki ilişkide aracı değişkenler olarak ele almaktadır (Durak, 2019; Seki et al., 2023).

Yöntem

Araştırmanın örneklemi, davranış bilimleri alanında yaygın olarak kullanılan Prolific platformu aracılığıyla toplanmıştır. Çalışmaya sosyal medya kullandığını belirten 330 yetişkin katılmıştır (%47.6

kadın; Mage = 44.36, SD = 13.94; yaş aralığı = 19–80). Katılımcılardan çevrimiçi bilgilendirilmiş onam alınmış ve çalışma etik kurul onayı ile Helsinki Bildirgesi ilkelerine uygun olarak yürütülmüştür.

Veri toplama sürecinde siber güvenlik farkındalığı, antagonistik kişilik özellikleri, bilinçli farkındalık ve sosyal medya bağımlılığını ölçen standart özbebildirim ölçekleri kullanılmıştır. SGF, Arpacı et al. (2025) tarafından geliştirilen Siber Güvenlik Farkındalığı Ölçeği ile değerlendirilmiştir. Sosyal medya bağımlılığı Bergen Sosyal Medya Bağımlılığı Ölçeği (Andreassen et al., 2016) ile, bilinçli farkındalık Mindful Attention Awareness Scale (Brown & Ryan, 2003) ile ve antagonistik kişilik özellikleri Dark Triad Dirty Dozen ölçeği (Jonason & Webster, 2010) ile ölçülmüştür. Tüm ölçekler kabul edilebilir ya da yüksek iç tutarlılık değerleri göstermiştir.

Veri analizi sürecinde tanımlayıcı istatistikler, korelasyon analizleri ve yapısal yol analizi uygulanmıştır. Dolaylı etkiler, 10.000 bootstrap örnekleme ile test edilmiştir. Ayrıca model, cinsiyete göre çoklu grup analiziyle incelenmiş ve yaş değişkeni kontrol edilmiştir. Analizler SPSS 26 ve AMOS 24 programları kullanılarak gerçekleştirilmiştir.

Bulgular ve Sonuç

Korelasyon analizleri, SGF'nin bilinçli farkındalık ile pozitif; sosyal medya bağımlılığı, narsisizm, Makyavelizm ve psikopati ile negatif ilişkili olduğunu göstermiştir. Bilinçli farkındalık antagonistik kişilik özellikleriyle negatif, sosyal medya bağımlılığı ise pozitif yönde ilişkili bulunmuştur. Erkekler Makyavelizm, psikopati ve bilinçli farkındalıkta daha yüksek puanlar alırken, kadınların SGF ve SMA puanları daha yüksek olmasına rağmen bu farklar istatistiksel olarak anlamlı değildir.

Yol analizi sonuçları, modelin genel örneklem ve cinsiyet alt gruplarında kabul edilebilir uyum değerlerine sahip olduğunu göstermiştir. Psikopati, yalnızca kadınlarda SGF'yi doğrudan ve negatif yönde yordamıştır. Narsisizm SGF'yi SMA üzerinden, Makyavelizm ise bilinçli farkındalık üzerinden dolaylı olarak etkilemiştir; ancak bu dolaylı etkiler toplam etkiye yansımamıştır. Bilinçli farkındalık erkeklerde SGF ile güçlü bir doğrudan ilişki göstermiştir. Model, SGF'deki varyansın %16'sını açıklamıştır.

Bu çalışma, siber güvenlik farkındalığının teknik bilgidan öte, bireysel psikolojik özelliklerle yakından ilişkili bir yapı olduğunu göstermektedir (Seki et al., 2023). Bulgular, antagonistik kişilik özellikleri içinde psikopatinin SGF açısından en tutarlı risk faktörü olduğunu ortaya koymuştur. Psikopatinin özellikle kadınlarda SGF'yi doğrudan azaltması, cinsiyete özgü psikolojik ve davranışsal süreçlerin önemine işaret etmektedir (Pinheiro et al., 2024).

Narsisizm ve Makyavelizmin SGF üzerindeki dolaylı etkileri, bu kişilik özelliklerinin hem risk artırıcı hem de dengeleyici yönleri olabileceğini düşündürmektedir. Narsistik bireylerin aşırı özgüveni ve Makyavelist bireylerin stratejik dikkati, düşük bilinçli farkındalık ya da yüksek SMA'nın olumsuz etkilerini kısmen telafi ediyor olabilir (Hepper et al., 2022; Blötnner & Bergold, 2022). Bu durum, yalnızca toplam etkilere odaklanmanın yanıltıcı olabileceğini göstermektedir.

Bilinçli farkındalık, özellikle erkeklerde SGF için güçlü bir koruyucu faktör olarak öne çıkmıştır. SMA ise genel örneklemde SGF'yi olumsuz etkilemiş, ancak cinsiyete göre ayrıldığında bu etki zayıflamıştır. Bu bulgular, SMA'nın cinsiyetten bağımsız genel bir risk faktörü olabileceğini düşündürmektedir (Hadlington, 2017; Chen et al., 2021).

Sonuç olarak, bu çalışma SGF'nin antagonistik kişilik özellikleri, bilinçli farkındalık ve sosyal medya bağımlılığı arasındaki karmaşık etkileşimler yoluyla şekillendiğini göstermektedir. Bulgular, siber güvenlik müdahalelerinde yalnızca teknik eğitime değil, psikolojik süreçleri hedefleyen bütüncül yaklaşımlara da ihtiyaç olduğunu vurgulamaktadır.