Journal of Education and New Approaches 2026, 9(1), 83-103

Journal of Education and New Approaches

Öğretmenlerin Bilgi Güvenliği Farkındalığının Bireysel ve Mesleki Değişkenler Bağlamında Analizi

Sinan Bilici s.bilici84@gmail.com
Milli Eğitim Bakanlığı

Öz:
Bilişim teknolojilerindeki hızlı değişimler insanoğlunun teknoloji ile yapabildiklerinin sınırlarını çok genişletmiş ve bilgiye erişimi kolaylaştırmıştır. Her yaştan insanın yoğun bir şekilde internet ve bilgi teknolojilerini kullanma durumu ise bazı güvenlik sorunlarını beraberinde getirmiştir. Bu açıdan siber güvenlik bilgi toplumu için önemli bir endişe kaynağı haline gelmiş ve bilgi güvenliği farkındalığını ön plana çıkarmıştır. Bu çalışmada öğretmenlerin bilgi güvenliği farkındalığının cinsiyet, okul türü, hizmet süresi, idari görev alma durumu, bilgisayar kullanma becerisi ve günlük internet kullanma süresi gibi bireysel ve mesleki değişkenlere göre incelenmesi amaçlanmıştır. Çalışma nicel araştırma yöntemi ve tarama modelinde yürütülmüştür. Veriler ulaşılabilir örneklem yöntemiyle lise ve ilköğretim okullarında görev yapan 248 öğretmen ve idareciden toplanmıştır. Veri toplama aracı olarak kişisel bilgi formu ve bilgi güvenliği farkındalık ölçeği kullanılmıştır. Normal dağılım varsayımını karşılayan veri seti üzerinde öncelikle betimsel istatistikler hesaplanmış, ardından gruplar arası farklılıkların incelenmesi amacıyla bağımsız örneklem t-testi ve tek yönlü varyans analizi (ANOVA) uygulanmıştır. Çalışmadan elde edilen başlıca sonuçlara göre, öğretmenlerin bilgi güvenliği farkındalıkları orta düzeyde çıkmıştır. Bilgi güvenliği farkındalıkları cinsiyet ve okul türüne göre farklılık göstermemiş ancak hizmet süresi arttıkça azalmıştır. Ayrıca idari görevi olan öğretmenlerde bilgi güvenliği farkındalığı daha düşük çıkmıştır. Bilgisayar kullanma becerisi arttıkça farkındalık düzeylerinin de arttığı tespit edilmiştir. Çalışma, K-12 öğretmen ve idarecilerini Koruma Motivasyonu Teorisi çerçevesinde ele alarak literatürdeki önemli bir teorik boşluğu doldurmakta ve bilgisayar yetkinliği ile hizmet süresinin farkındalık üzerindeki en güçlü belirleyiciler olduğunu ortaya koymaktadır. Ayrıca, siber güvenlik zincirinde genellikle ihmal edilen ve yüksek veri erişim yetkisine sahip olan okul idarecilerini örnekleme dahil etmesi, çalışmanın özgünlüğünü ve kapsayıcılığını arttırmaktadır. Elde edilen sonuçlar doğrultusunda, idari görev alan ve hizmet süresi fazla olanlar başta olmak üzere öğretmenlere bilgi güvenliği farkındalıklarını arttırmaya yönelik hizmet içi eğitimler verilmesi önerilmektedir.

Anahtar Kelimeler: Teknoloji, bilgi güvenliği, siber tehditler, farkındalık.

Bilici, S. (2026). Öğretmenlerin Bilgi Güvenliği Farkındalığının Bireysel ve Mesleki Değişkenler Bağlamında Analizi. *International Journal of Education and New Approaches*, *9*(1), 83-103. https://doi.org/10.52974/jena.1866617

Submission Date:	*19.01.2026*
Acceptance Date:	*24.06.2026*
Publication Date:	*30.06.2026*

Abstract:
Rapid changes in information technologies have greatly expanded the boundaries of what humans can do with technology and facilitated access to information. The intensive use of the internet and information technologies by people of all ages has brought about some security problems. In this respect, cyber security has become an important source of concern for the information society and has brought information security awareness to the forefront. This study aims to examine teachers' information security awareness in relation to individual and professional variables such as gender, school type, years of service, administrative duty status, computer proficiency, and daily internet usage time. The study was conducted using the quantitative research method and the survey model. Data were collected from 248 high school and primary school teachers using the convenience sampling method. Personal information form and information security awareness scale were used as data collection tools. Descriptive analyses, independent sample t-test and one-way analysis of variance (ANOVA) were performed on normally distributed data set. According to the main findings of the study, teachers' information security awareness was found to be at a moderate level. Information security awareness did not differ according to gender and school type, but decreased as the length of service increased. In addition, information security awareness was lower in teachers with administrative duties. It has been determined that as computer usage skills increase, awareness levels also increase. By addressing K-12 teachers and administrators within the framework of Protection Motivation Theory, this study fills a significant theoretical gap in the literature and reveals that computer proficiency and length of service are the strongest predictors of awareness. Additionally, including school administrators—who possess the highest level of data access authority but are rarely studied in the literature—enhances the inclusiveness of the research. In line with the results obtained, it is recommended that in-service training be provided to teachers, especially those with administrative duties and long service periods, to increase their information security awareness.

Keywords: Technology, information security, cyber threats, awareness.

GİRİŞ

Yaşadığımız dönemi bilgi toplumu, bilgi çağı veya dijital çağ olarak adlandırmak mümkündür. Dijital çağ, sanal ortamlar, dijital hizmetler, akıllı uygulamalar, makine öğrenimi, bilgi tabanlı sistemler gibi farklı teknolojik çözümlerin bir koleksiyonu olarak tanımlanabilmektedir (Romansky & Noninska, 2020). Bilgi çağında internet ve hızla gelişen teknolojilerin bilgiye erişimi gün geçtikçe daha da kolay hale getirdiği açıktır. Özellikle son on yılda, mobil cihazlar ve dijital uygulamalar küresel ölçekte günlük yaşamı dönüştürmüş ve birçok alanda çeşitli yaşam tarzlarını kolaylaştırmıştır (Zwilling vd., 2022). Hayatın olağan akışı içerisinde bankacılık, e-ticaret, eğitim, eğlence gibi pek çok alanda bilgi ve iletişim teknolojileri sıklıkla kullanılmaktadır. Okuma yazma bilmeyen insanlar bile sesli komutlar yardımıyla interneti kullanabilmektedir (Talan & Aktürk, 2021). Ayrıca internet devrimi ile birlikte insan hayatının gerçek dünya ve sanal dünya olarak ikiye ayrılması (Raiyn, 2014), bireyler arası iletişim ve bilgi paylaşım süreçlerinin de artık daha çok sanal ortamlara kaymasının yolunu açmıştır. Dijital ortamların çocuklardan yetişkinlere ve yaşlı bireylere kadar her yaştan insan tarafından yoğun biçimde kullanımı yerli ve yabancı raporlara da açıkça yansımaktadır. "*Digital 2025*" Türkiye raporuna göre, 2025 başı itibarıyla Türkiye'de 77,3 milyon kişi internet kullanıcısıdır; bu rakam toplam nüfusun yaklaşık %88,3'üne denk gelmektedir. 16 yaş üstü internet kullanıcılarının %96,9'u internete cep telefonuyla bağlanmakta ve buna akıllı telefon sahipliği de eşlik etmektedir (%95,2 oranında). Günlük internet kullanım süresi ortalama 7 saat 13 dakika gibi yüksek seviyelere ulaşırken, sosyal medya kullanıcı sayısı da yaklaşık 58,5 milyon seviyesine çıkmıştır. TÜİK (2025) "Hane halkı Bilişim Teknolojileri Kullanım Araştırması" sonuçları da bu verilerle paralellik göstermektedir.

Gerçek ile sanal yaşantıların bu denli iç içe geçtiği günümüzde, ulaşılan bilgi ve bu bilginin güvenliği her iki yaşantının da dengeli bir biçimde devamı için önemli görülmektedir

(Çetinkaya vd., 2017; Keser & Yayla, 2021). Hem dünyada hem de ülkemizde insanları aktif ve yoğun bir şekilde sistemin içinde tutan internet ve diğer bilgi teknolojileri hayatı kolaylaştırmanın yanı sıra çeşitli risk ve tehditleri de beraberinde getirmiştir. Diğer bir ifadeyle, bilgi güvenliği hepimiz için önemli bir endişe kaynağı haline gelmiş (Haseski, 2020) ve siber saldırılar bilgi güvenliği için potansiyel bir tehdit oluşturmuştur (Zwilling vd., 2022). Bireyler bazen fark edemedikleri güvenlik açıklarının varlığını ancak olumsuz durumlarla yüzleştiklerinde öğrenmektedir (Aydın vd., 2023). Tüm bu durumlar siber ortamda bilgi güvenliği konusunu önemli bir yere oturtmaktadır. Siber hijyen olarak da adlandırılan siber güvenli davranış (Witsenboer vd., 2022), sanal dünyaya adım atan herkesi ilgilendiren bir konu olmuştur.

Siber Tehditler ve Sosyal Mühendislik

Bilgi güvenliği, kişi veya kurumlara ait bilgi kaynaklarına izinsiz bir şekilde erişilmesini, kullanılmasını, ifşa edilmesini, değiştirilmesini ya da tahrip edilmesini önleme amacıyla gerçekleştirilen çabalar olarak tanımlanmaktadır (Çetinkaya vd., 2017; Keser & Güldüren, 2015). Bilginin gizliliği ise, uluslararası öneme sahip temel bir insan hakkıdır ve her birey kişisel verilerinin korunması hakkına sahiptir (Romansky & Noninska, 2020). Siber ortamda bilgi güvenliğini tehdit eden unsurlar sahte antivirüs yazılımları, casus yazılımlar (spyware), mesaj sağanakları (spam), servisi engelleyen saldırılar (denial of service/dos), bilişim korsanlığı (hacking), zincir e-postalar, tuş kaydediciler (keylogger), truva atları (trojan horse), internet aldatmacası (hoax) ve sosyal mühendislik olarak sınıflandırılabilmektedir (Yılmaz & Avcı, 2022). Bilgi güvenliği zincir halkalarının birleşiminden oluşan bir yapı olarak düşünüldüğünde, güvenlik sistemindeki en zayıf halka insandır (Hadlington vd., 2020). Bu zayıf halkanın istismarı ile veri elde etmek sosyal mühendislik kavramını ortaya çıkarmıştır (Gündüz & Daş, 2016). Sosyal mühendislik saldırılarına karşı önlem almak daha zordur çünkü bu saldırılar kişilerin zaaflarından istifade etmeyi, insanı zayıf anında manipüle etmeyi (Hekim, 2015), güven duygusu oluştururken korku ve aciliyet duygusunu kullanmayı içermektedir (Conteh & Schmick, 2021). Teknoloji sürekli geliştiği ve yeni alanlar oluşturduğu için sosyal mühendisler de yeni yöntemler geliştirmiş, başarı oranlarını arttırmışlardır (Ecek & Çakmak, 2022; Yalçın & Avşar, 2018). Kullanıcılara yönelik sosyal mühendislik saldırıların başında oltalama (phishing) saldırıları gelmektedir. İnternet dolandırıcılığı yöntemleri arasında en tehlikelisi olarak göze çarpan "phishing" yöntemi, Türkçeye sazan avlama veya yemleme olarak çevrilmiştir.

Bilgi Güvenliği Farkındalığı

Siber güvenlik tehditleri yalnızca şirketleri değil, aynı zamanda akıllı cihazları kullanan tüm bireyleri etkileyebilmektedir. Sanal ortamda çeşitli amaçlarla bulunan herkes için siber güvenliği sağlayabilme yetkinliği artık olmazsa olmaz bir özellik haline gelmiştir (Haseski, 2020). Araştırmalar, insan hatalarının güvenlik olaylarının %95'inde rol oynadığını göstermiştir (Witsenboer vd., 2022). Dolayısıyla insanların siber saldırıları önlemek için eğitilmedikleri sürece yazılım veya donanım çözümleri kullanılarak saldırıların önlenemeyeceği açıktır (Salahdine & Kaaboch, 2019). Herhangi bir kuruluştaki çalışanların bilgi güvenliği farkındalığını artırmak, hassas verilerin kaybı ve sisteme doğrudan saldırılar dâhil olmak üzere kuruluşu çeşitli tehditlerden korumak için kritik öneme sahiptir (Hadlington vd., 2020). Bu açıdan, bilgi güvenliğini sağlama konusunda en hızlı ve etkili yöntemlerden birinin mümkün olduğunca yüksek farkındalık oluşturma ve bilinçlendirme olduğu belirtilmektedir (Kubacka vd., 2021). Zira bilgi güvenliklerini tehdit eden durumların farkında olan bireyler kendilerini

daha fazla koruyabilmektedir (Avcı & Oruç, 2020; Gökçearslan vd., 2021). Bu açıdan bilgi güvenliği farkındalığı, insan odaklı bilgi güvenliği noktasında merkezi bir aktör olarak kabul görülmekte ve ilk adımı oluşturmaktadır (Ecek & Yılmaz, 2023). Farkındalığın davranıştan önce geldiği ve farkındalığın ölçülmesi ile siber hijyen sorununun kökenine inmenin daha kolay olacağı savunulmaktadır (Vishwanath vd., 2020).

Öğretmenlerin bilgi güvenliği farkındalıklarının incelendiği çalışmalarda farkındalık düzeylerinin genel olarak orta düzeyde seyrettiği görülmektedir (Ecek & Yılmaz, 2023; Erdoğan & Coşar, 2026; Özdemir & Uluyol, 2021). Cinsiyetin bilgi güvenliğine etkisi konusunda literatürde bir fikir birliği olmamakla birlikte, erkeklerin lehine olan bulgular ağırlıktadır (Keser & Yayla, 2021; Özdemir & Uluyol, 2021; Yılmaz vd., 2016). Mesleki kıdem ve yaş arttıkça farkındalık seviyelerinde belirgin bir düşüş gözlemlenmektedir (Canoğulları, 2021; Keser & Yayla, 2021; Nezgitli & Gökçeaslan, 2022). Uzmanlık alanı da bilgi güvenliği davranışlarını şekillendiren güçlü değişkenlerden birisi olarak ön plana çıkmaktadır. Teknik branşlarda görev yapan öğretmen ve personelin daha yüksek farkındalık düzeyine sahip olduğu belirtilmektedir (Erdoğan & Coşar, 2026; Hakkari, 2022; Özdemir & Uluyol, 2021). Teknoloji kullanım alışkanlıkları açısından bakıldığında günlük internet ve bilgisayar kullanım süresi arttıkça farkındalık düzeylerinin de arttığı vurgulanmaktadır (Aksoğan, 2023; Öztrak vd., 2025; Talan & Aktürk, 2021; Yılmaz vd., 2016).

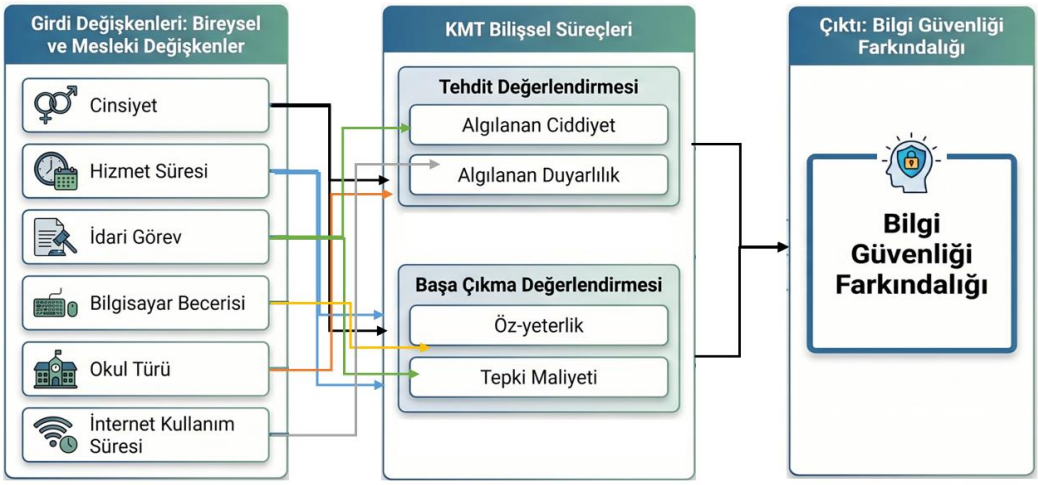
Koruma Motivasyonu Teorisi

Koruma Motivasyonu Teorisi (KMT), ilk olarak Rogers (1975) tarafından yılında bireylerin tehditler karşısında nasıl korunma davranışı geliştirdiklerini açıklamak için ortaya atılmıştır. Teori, bireyin bir tehdit karşısında "tehdit" ve "başa çıkma" olmak üzere iki farklı bilişsel değerlendirme sürecinden geçtiğini savunmaktadır. Tehdit değerlendirmesinde, tehdidin ne kadar ciddi olduğu (Algılanan Ciddiyet) ve kişinin bu tehdide karşı ne kadar savunmasız olduğu (Algılanan Duyarlılık) değerlendirilmektedir (Pratama vd., 2025). Başa çıkma değerlendirmesinde ise önerilen korunma yönteminin etkililiği (Tepki Etkinliği), kişinin bu yöntemi uygulama becerisine olan inancı (Öz-yeterlilik) ve korunma davranışının getirdiği maddi/manevi yükler (Tepki Maliyeti) analiz edilmektedir (Verkijika, 2018). Tehdit ve başa çıkma değerlendirmelerinin toplamı ise bireyde bir korunma motivasyonu (davranışsal niyet) meydana getirmekte ve koruyucu davranışların benimsenmesini sağlamaktadır (Han vd., 2025).

KMT, bireylerin bilgi güvenliğine ilişkin davranışlarını açıklamada ve siber tehditler karşısında neden koruyucu önlemler alıp almadıklarını yorumlamada da başvurulan kuramsal çerçevelerden biridir (Dodge vd., 2023; Ghazali vd., 2023; Mou vd., 2022). Teorinin temel bileşenleri, bilgi güvenliği kavramının doğasıyla yüksek düzeyde örtüşmekte ve bireylerin tehdit algıları ile başa çıkma değerlendirmelerini sistematik biçimde açıklamaktadır (Han vd., 2025). Alan yazında KMT temelinde kullanıcıların bilgi güvenliğine yönelik niyet ve davranışlarını inceleyen çalışmalara bakıldığında farklı örneklem grupları göze çarpmaktadır. Pratama vd. (2025) devlet işletmelerinde çalışanların oltalama (phishing) e-postalarına karşı güvenlik davranışı niyetini incelemiştir. Tsai vd. (2016) internet kullanıcılarının siber tehditleri fark etmeleri ile bunları önleyecek güvenlik adımlarını atma niyetleri arasındaki boşluğu anlamak için KMT çerçevesini kullanmıştır. Bunların yanı sıra banka çalışanları (Alrawhani vd., 2025), sosyal ağ kullanıcıları (Mousavi vd., 2020) ve akıllı telefon kullanıcılarının (Verkijika, 2018) da bilgi güvenliği davranışlarını etkileyen KMT faktörleri incelenmiştir. Eğitim paydaşları ile yapılan çalışmalara bakıldığında ise kısıtlı bir literatür göze çarpmaktadır. Han vd. (2025) üniversite öğrencilerinde bilgi güvenliği davranışlarını etkileyen faktörleri,

Başarmak ve Ateş (2026) ise yine üniversite öğrencilerinde yapay zekâ destekli oyun tabanlı öğrenmeyi benimseme niyetlerini etkileyen faktörleri KMT kapsamında incelemişlerdir. Öğretmenler ile yapılan sadece bir çalışmada ise (Ateş & Gündüzalp, 2025) fen bilgisi öğretmenlerinin artırılmış gerçeklik temelli oyunlaştırmayı benimseme niyetlerini belirleyen unsurları KMT çerçevesini içeren bir modelle incelemişlerdir. Mevcut çalışmada KMT bileşenleri aracılığıyla öğretmenlerin bilgi güvenliği farkındalığını etkileyebileceği öngörülen bireysel ve mesleki değişkenler analize dahil edilerek araştırma hipotezleri test edilmiştir.

Çalışmada öğretmenlerin siber tehditlere karşı kendilerini ne kadar savunmasız hissettikleri (algılanan duyarlılık) ve bu tehditlerle baş etme becerilerine olan inançları (öz-yeterlik) açısından cinsiyete dayalı bilişsel farklılıklar yaşayabilecekleri varsayılmıştır. Farklı okul türlerinin ve yönetilen verinin niteliğinin, öğretmenlerin siber risklere dair algılanan duyarlılık düzeylerini değiştirebileceği öngörülmüştür. Hizmet süresi bağlamında kuşaksal farkların, teknolojiyi kullanma konusundaki öz-yeterlik algısını ve güvenlik önlemlerini uygulamanın getirdiği yükü ifade eden tepki maliyeti algısını şekillendirdiği düşünülmektedir. Kritik verilere doğrudan erişimi olan idarecilerin siber tehdit sonuçlarını daha ciddi (algılanan ciddiyet) görmeleri beklenirken, güvenlik adımlarını zaman kaybı ve iş yükü olarak (tepki maliyeti) algılayabilecekleri varsayılmıştır. Teknik yetkinliklerin KMT'nin öz-yeterlik bileşeniyle doğrudan ilişkili olmasından hareketle bilgisayar kullanma becerisi yüksek bireylerin tehditleri tanımlama ve önlem alma kapasitelerine daha fazla güveneceği (öz-yeterlik) öngörülmüştür. İnternette geçirilen sürenin artması, bireyin siber risklerle daha sık karşılaşmasına neden olacağı için algılanan duyarlılık düzeyini etkileyebileceği gerekçesiyle analize dahil edilmiştir. Çalışma hipotezlerine ilişkin bu kuramsal eşleştirmeler, ilgili değişkenlerin bireylerin tehdit değerlendirmesi ve başa çıkma süreçleri üzerindeki olası etkilerini bütüncül bir çerçevede incelemeyi amaçlamaktadır. Çalışma kapsamında incelenen değişkenlerin KMT bileşenleri ile ilişkisi Şekil 1'de modellenmiştir.



Şekil 1. Değişkenlerin KMT bileşenleri ile ilişkisi

Bilgi güvenliğinin çağımızın öncelikli problemlerinden biri olması bu konuyu hem alan yazında ilgi odağı haline getirmiş hem de bu çalışmanın araştırma konusu yapmıştır. Alanyazındaki araştırmalar, farklı hedef kitlelerin bilgi güvenliği farkındalık düzeylerinin genellikle orta ile yüksek arasında değiştiğini göstermekle birlikte, teknik beceri gerektiren konularda zafiyetler yaşandığı da dikkat çekmektedir (Aksoğan, 2023; Canoğulları, 2021; Ecek & Yılmaz, 2023;

Erdoğan & Coşar, 2026). Yapılan araştırmalar, üniversite öğrencilerinden kamu çalışanlarına kadar geniş bir kitlenin temel siber güvenlik bilgilerine sahip olduklarını iddia etseler de dijital verilerini koruma yöntemleri ve bilişim suçlarına ilişkin yasal sorumluluklar konusunda ciddi bilgi eksiklikleri yaşadıklarını ortaya koymaktadır (Akgün & Topal, 2015; Gabra vd., 2020; Kubacka vd., 2021; Zwilling vd., 2022). Benzer durum dijital rol model olması beklenen öğretmenler için de geçerlidir. Bazı çalışmalarda öğretmenlerin farkındalık seviyeleri öz-bildirime dayalı olarak yüksek olarak tanımlansa da, nitel veriler ve uygulamalı simülasyonlar teknik konularda ve karmaşık saldırılar karşısında ciddi zafiyetler yaşandığını ortaya koymaktadır (Ateş & Küçük, 2023; Genç & Yücel, 2025). Bu durum bilgi güvenliği farkındalığı konusunda öğretmen örneklemi üzerinde daha fazla güncel araştırma yapılması ihtiyacını ortaya koymaktadır.

Öte yandan okullarda bilgi güvenliği farkındalığı sadece bireysel bir korunma meselesi değil; hassas öğrenci ve personel verilerinin yönetilmesi nedeniyle stratejik bir kamusal gereklilik olarak görülmektedir (Erdoğan & Coşar, 2026). Dolayısıyla öğretmen ve idareciler e-Okul ve MEBBİS gibi dijital sistemler üzerinden kritik verileri yönettikleri için okullarda bilgi güvenliği zincirinin önemli halkalarından birini oluşturmaktadır (Ateş & Küçük, 2023; Keser & Yayla, 2021). Teknolojiyle içi içe olan Z ve Alfa kuşağı öğrencilerinin bilgi güvenliğini sağlama konusunda da öğretmenlere büyük sorumluluklar düştüğü bilinen bir gerçektir. Bu noktada öğretmen ve idarecilerin bilgi güvenliği farkındalığı düzeylerinin bireysel ve mesleki değişkenlerine göre değerlendirilmesi ve bu doğrultuda da gerekli tedbirlerin alınması önem arz etmektedir. Alan yazın incelendiğinde eğitim alanında bilgi güvenliği farkındalığı ile ilgili yapılan araştırmaların çoğunlukla akademik personel (Ecek & Yılmaz, 2023; Keser & Güldüren, 2015; Öztrak, vd., 2025) ve üniversite öğrencileri üzerinde (Gültekin & Özel, 2023; Değirmenci & Demiral, 2023; Karapınar & Daş, 2022; Mai & Tick, 2021; Gabra vd., 2020) yoğunlaştığı görülmektedir. Öğretmenlerin bilgi güvenliği farkındalıkları üzerinde yapılan çalışmaların ise nispeten daha sınırlı kaldığı görülmüştür. Bu çalışmaların bazıları ölçek geliştirme çalışması olup (Çetinkaya vd., 2017; Yılmaz, 2015), bazılarında ise nitel araştırma yöntemine başvurulmuştur (Ateş & Küçük (2023; Aydın vd., 2023). Üniversite ve özel sektör idarecileri hariç tutulduğunda MEB okul idarecilerinin dahil edildiği sadece bir çalışma tespit edilmiştir (Karabatak & Karabatak, 2019). Bununla birlikte KMT'nin bilgi güvenliği kavramının doğasıyla yüksek düzeyde örtüşmesine rağmen öğretmen örnekleminde çok az çalışılmış olması da alan yazındaki çalışma boşluğunu kapatması açısından mevcut çalışmayı değerli kılmaktadır. Bu doğrultuda öğretmen ve idarecilerin bilgi güvenliği farkındalıklarının bazı bireysel ve mesleki değişkenlere göre incelenmesi amacıyla aşağıdaki alt problemlere cevap aranmıştır:

- Öğretmenlerin bilgi güvenliği farkındalık düzeyleri nasıldır?
- Öğretmenlerin bilgi güvenliği farkındalık düzeyleri;
  - Cinsiyete
  - Okul türüne
  - Hizmet süresine
  - İdari görev alma durumuna
  - Bilgisayar kullanma becerisine ve
  - Günlük ortalama internet kullanma süresine göre farklılaşmakta mıdır?

Bu araştırma soruları doğrultusunda aşağıdaki hipotezler test edilmiştir:

- H_1: Öğretmenlerin bilgi güvenliği farkındalık düzeyleri yüksek seviyededir.

- H_2: Öğretmenlerin bilgi güvenliği farkındalık düzeyleri cinsiyete göre anlamlı bir farklılık göstermektedir.
- H_3: Öğretmenlerin bilgi güvenliği farkındalık düzeyleri görev yaptıkları okul türüne göre anlamlı bir farklılık göstermektedir.
- H_4: Öğretmenlerin bilgi güvenliği farkındalık düzeyleri mesleki hizmet sürelerine göre anlamlı bir farklılık göstermektedir.
- H_5: Öğretmenlerin bilgi güvenliği farkındalık düzeyleri idari görev alma durumuna göre anlamlı bir farklılık göstermektedir.
- H_6: Öğretmenlerin bilgi güvenliği farkındalık düzeyleri bilgisayar kullanma becerilerine göre anlamlı bir farklılık göstermektedir.
- H_7: Öğretmenlerin bilgi güvenliği farkındalık düzeyleri günlük ortalama internet kullanma sürelerine göre anlamlı bir farklılık göstermektedir.

YÖNTEM

Araştırma Modeli

Nicel araştırma yönteminin kullanıldığı bu çalışmada tarama modeline başvurulmuştur. Tarama modeli mevcut durumu betimlemeyi, ortaya koymayı amaçlamakta ve bu amaca yönelik olarak çoğunlukla geniş bir kitleden araştırmacı tarafından bilgi toplanılmasını gerektirmektedir (Büyüköztürk vd., 2020).

Örneklem Grup

Çalışmada veriler ulaşılabilir örnekleme yöntemi ile Van il merkezindeki lise ve ilköğretim okullarında görev yapan toplam 248 öğretmenden 2023-2024 eğitim öğretim yılında elde edilmiştir. Çalışma grubuna hızlı ve pratik bir şekilde erişim sağlanabilmesi amacıyla ulaşılabilir örneklem tercih edilmiştir. Örneklem gruba ilişkin demografik bileşenler Tablo 1'de sunulmuştur.

Tablo 1. Örneklem Grubun Demografik Özellikleri

Demografik özellik	f	%
Cinsiyet		
Kadın	92	37.1
Erkek	156	62.9
Okul türü		
Lise	174	70.2
İlköğretim	74	29.8
Hizmet süresi		
0-5 yıl	78	31.5
6-10 yıl	78	31.5
11-15 yıl	48	19.4
16-20 yıl	22	8.9
21 yıl ve üstü	22	8.9
İdari görev alma durumu		
İdari görevi var	32	12.9
İdari görevi yok	216	87.1
Bilgisayar kullanma becerisi		
Düşük	30	12.1
Orta	172	69.4

İleri	46	18.5
Günlük internet kullanım süresi		
0-2 saat	72	29
2-4 saat	114	46
4-6 saat	52	21
6 saat ve üzeri	10	4

Tablo 1'deki verilere göre örneklem grubu erkek ağırlıklı ve çoğunluğu lisede görev yapmaktadır. Yüzde 70'e yakını orta düzeyde bilgisayar kullanabildiğini belirtmiştir. Günlük internet kullanım süresi en çok 2-4 saat aralığına denk gelmektedir.

Veri Toplama Araçları

Çalışmada veri toplama aracı olarak kişisel bilgi formu ve bilgi güvenliği farkındalık ölçeği kullanılmıştır.

Kişisel bilgi formu

Öğretmenlerin cinsiyet, okul türü, hizmet süresi, idari görev alma durumu, bilgisayar kullanma becerisi ve günlük internet kullanma süresine ilişkin kişisel demografik bilgileri bu form ile elde edilmiştir.

Bilgi Güvenliği Farkındalık Ölçeği

Çalışmada kullanılan bilgi güvenliği farkındalık ölçeği Çetinkaya vd., (2017) tarafından geliştirilmiştir. Ölçek "mobil cihazlar, mahremiyet ve iletişim", "saldırı ve tehditler" ve "genel güvenlik" olmak üzere 3 boyutlu ve toplam 48 maddeden oluşmaktadır. Ölçek maddeleri, 5'li Likert tipi olup "1 – Kesinlikle katılmıyorum", "2- Katılmıyorum", "3- Kararsızım", "4- Katılıyorum", ve "5- Kesinlikle katılıyorum" şeklinde puanlanmaktadır. Ölçekten en az 48 puan, en fazla ise 240 puan alınabilmektedir. Yapı geçerliliği testinde faktörlerin açıkladığı toplam varyans %61,74'dir. Ölçek alt faktörleri, faktörlere dâhil olan sorular ile en düşük ve en yüksek farkındalık düzeyi puanları Tablo 2'de verilmiştir. Ölçeğin tamamına ait Cronbach Alfa iç tutarlılık katsayısı .980, alt faktörlere ilişkin değerler sırasıyla .967, .969 ve .926 olarak hesaplanmıştır. Mevcut çalışmada ise ölçeğin tamamına ilişkin güvenirlik katsayısı .971 olarak hesaplanmıştır. Alt faktörlere ilişkin iç tutarlılık değerleri ise sırasıyla .922, .938 ve .938 olarak hesaplanmıştır.

Tablo 2. Ölçek Faktörlerine Ait En Düşük ve En Yüksek Farkındalık Düzeyi Puan Aralıkları

Faktör Adı	**Faktör soruları**	**En düşük puan**	**En yüksek puan**	**Farkındalık Düzeyi**			
				Düşük	**Orta**	**Normal**	**Yüksek**
Mobil cihazlar, mahremiyet ve iletişim	1-18	18	90	18-36	37-54	55-72	73-90
Saldırı ve tehditler	19-35	17	85	17-34	35-51	52-68	69-85
Genel güvenlik	36-48	13	65	13-26	27-39	40-52	53-65
Ölçek geneli	1-48	48	240	48-96	97-144	145-192	193-240

Verilerin Toplanması ve Analizi

Ölçek formları çevrim içi ortama aktarılarak resmi izinler alındıktan sonra Whatsapp kanalı ile Van merkez ilçelerdeki (Tuşba, İpekyolu, Edremit) okul öğretmen gruplarına ulaştırılmıştır. Çevrim içi anketler "Google Formlar" aracılığıyla oluşturulduğu için sadece çalışmaya dahil olan 248 katılımcının yanıt bilgisine ulaşılabilmektedir. Katılımın gönüllük esasına dayandığı çalışmada örneklem gruptan elde edilen veriler bilgisayar ortamında SPSS paket programı kullanılarak analiz edilmiştir. Analizlere başlamadan önce verilerin normal dağılım gösterip göstermediğinin anlaşılması için normallik testi yapılmıştır. Ölçek puanları ve alt faktörlerin çarpıklık ve basıklık değerlerinin kabul edilebilir seviye olan -1.5 ile +1.5 arasında çıkması sonucu (Tabachnick ve Fidell, 2013) parametrik testler uygulanmıştır. Ortak yöntem varyansı riskini değerlendirmek için Harman'ın tek faktörlü testi uygulanmıştır. Analiz sonucunda birden fazla faktör yapısının ortaya çıktığı ve ilk faktörün toplam varyansın %43'ünü açıkladığı belirlenmiştir. Araştırmanın alt problemlerine yanıt bulmak amacıyla ortalama, standart sapma değerleri ile birlikte cinsiyet, okul türü ve idari görev alma değişkenleri için bağımsız örneklem t-testi uygulanmıştır. Hizmet süresi, bilgisayar kullanma becerisi ve günlük internet kullanma değişkenleri içinse tek yönlü varyans analizi (ANOVA) testinden yararlanılmıştır.

Etik Kurul İzin Bilgisi

Bu araştırma, Van Tuşba İlçe Milli Eğitim Müdürlüğü Etik Kurulunun 10/06/2024 ve E-89601435-20-104153505 sayılı kararı ile alınan izinle yürütülmüştür.

BULGULAR

Öğretmenlerin Bilgi Güvenliği Farkındalık Düzeyleri

Bilgi güvenliği farkındalık ölçeği genelinde ve alt faktörlerinde ortaya çıkan betimsel bulgular Tablo 3'te sunulmuştur.

Tablo 3. Bilgi Güvenliği Farkındalık Düzeyleri

Faktör	N	$\bar{X}$	Ss	Durum
Mobil cihazlar, mahremiyet ve iletişim	248	54.85	11.27	Normal
Saldırı ve tehditler	248	46.42	12.59	Orta
Genel güvenlik	248	41.25	9.95	Normal
Ölçek geneli	248	142.53	30.87	Orta

Tablo 3'teki verilere göre, öğretmenlerin bilgi güvenliği farkındalıkları genel olarak orta düzeyde çıkmıştır. Alt faktörlere bakıldığında ise, "mobil cihazlar, mahremiyet ve iletişim" faktörü ile "genel güvenlik" faktör ortalamaları normal düzeyde çıkarken "saldırı ve tehditler" faktörü ise orta düzeyde çıkmıştır. Bu bulgular doğrultusunda H_1 hipotezi reddedilmiştir.

Bilgi Güvenliği Farkındalık Düzeylerinin Cinsiyet Değişkenine Göre İncelenmesi

Katılımcıların cinsiyet değişkenine göre bilgi güvenliği farkındalık düzeylerini tespit etmek amacıyla gerçekleştirilen bağımsız örneklem t-testi öncesinde Levene testi uygulanmış ve varyansların homojen dağıldığı belirlenmiştir (p>. 05). Elde edilen t-testi sonuçları Tablo 4'te sunulmuştur.

Tablo 4. Cinsiyete Göre Bilgi Güvenliği Farkındalık Düzeyleri

Faktör	Grup	N	$\bar{X}$	SS	sd	t	p
Mobil cihazlar, mahremiyet ve iletişim	Kadın	92	53.78	11.18	246	-1.151	.251
	Erkek	156	55.48	11.31			
Saldırı ve tehditler	Kadın	92	45.50	13.28	246	-.890	.374
	Erkek	156	46.97	12.17			
Genel güvenlik	Kadın	92	41.93	10.46	246	.866	.387
	Erkek	156	40.84	8.98			
Ölçek geneli	Kadın	92	141.21	32.31	246	-.514	.608
	Erkek	156	143.30	30.07			

Tablo 4'e göre katılımcıların bilgi güvenliği farkındalık düzeylerinin cinsiyete göre anlamlı fark göstermemiştir (p>.05). Mobil cihazlar, mahremiyet ve iletişim ($t(246) = -1.151$, $p > .05$), saldırı ve tehditler ($t(246) = -.890$, $p > .05$), genel güvenlik ($t(246) = .866$, $p > .05$) alt boyutları ile ölçek genelinde ($t(246) = -.514$, $p > .05$) cinsiyete bağlı olarak istatistiksel açıdan anlamlı bir fark bulunmamıştır. Bu bulgular doğrultusunda H_2 hipotezi reddedilmiştir.

Bilgi Güvenliği Farkındalık Düzeylerini Okul Türü Değişkenine Göre İncelenmesi

Katılımcıların okul türü değişkenine göre bilgi güvenliği farkındalık düzeylerini tespit etmek amacıyla gerçekleştirilen bağımsız örneklem t-testi öncesinde Levene testi uygulanmış ve varyansların homojen dağılmadığı belirlendiğinden ($p < .05$) Welch t-testi sonuçları dikkate alınmıştır. Elde edilen Welch t-testi sonuçları Tablo 5'de sunulmuştur.

Tablo 5. Okul Türüne Göre Bilgi Güvenliği Farkındalık Düzeyleri

Faktör	Grup	N	$\bar{X}$	SS	sd	t	p
Mobil cihazlar, mahremiyet ve iletişim	Lise	174	54.24	11.90	246	-1.437	.152
	İlköğretim	74	56.29	9.54			
Saldırı ve tehditler	Lise	174	45.60	13.65	246	-1.816	.071
	İlköğretim	74	48.35	9.46			
Genel güvenlik	Lise	174	40.51	10.36	246	-2.158	.052
	İlköğretim	74	42.97	7.08			
Ölçek geneli	Lise	174	140.36	33.27	246	-1.939	.054
	İlköğretim	74	147.62	23.76			

Tablo 5'e göre katılımcıların bilgi güvenliği farkındalık düzeyleri okul türü değişkenine göre anlamlı fark göstermemiştir (p>.05). Mobil cihazlar, mahremiyet ve iletişim (t=-1.437; p=.152), saldırı ve tehditler (t=-1.816; p=.071) ve genel güvenlik (t=-2.158; p=.052) alt boyutu ile ölçek geneli puanlarında (t=-1.939; p=.054) lise ve ilköğretim düzeyinde görev yapan öğretmenler arasında anlamlı bir fark tespit edilmemiştir. Bu bulgular doğrultusunda H_3 hipotezi reddedilmiştir.

Bilgi Güvenliği Farkindalik Düzeylerinin Hizmet Süresi Değişkenine Göre İncelenmesi

Katılımcıların hizmet süresi değişkenine göre bilgi güvenliği farkındalık düzeylerini tespit etmek amacıyla gerçekleştirilen tek yönlü ANOVA öncesinde Levene testi uygulanmış ve varyansların homojen dağıldığı belirlenmiştir (p>. 05). Elde edilen ANOVA testi sonuçları Tablo 6'da sunulmuştur.

Tablo 6. Hizmet Süresine Göre Bilgi Güvenliği Farkındalık Düzeyleri

	Varyansın kaynağı	Kareler toplamı	Sd	Kareler ortalaması	F	*p*	η²	Anlamlı fark
Mobil cihazlar, mahremiyet ve iletişim	Gruplar arası	1676.373	4	419.093	3.426	.010*		0-5 yıl>16-20 yıl 6-10 yıl>16-20 yıl
	Gruplar içi	29722.402	243	122.314			.053	
	Toplam	31398.774	247					
Saldırı ve tehditler	Gruplar arası	1686.528	4	421.632	2.733	.030*		0-5 yıl>16-20 yıl
	Gruplar içi	37486.166	243	154.264			.043	
	Toplam	39172.694	247					
Genel güvenlik	Gruplar arası	2702.136	4	675.534	8.270	.000**		0-5 yıl>16-20 yıl 6-10 yıl>16-20 yıl
	Gruplar içi	19848.364	243	81.681			.120	11-15 yıl >16-20 yıl
	Toplam	22550.500	247					
Ölçek geneli	Gruplar arası	16736.086	4	4184.022	4.648	.001*		0-5 yıl>16-20 yıl 6-10 yıl>16-20 yıl
	Gruplar içi	218761.656	243	900.254			.071	
	Toplam	235497.742	247					

**p<.05 **p<.001*

Tablo 6'ya göre katılımcıların bilgi güvenliği farkındalık düzeyleri; mobil cihazlar, mahremiyet ve iletişim ($F(4,243)=3.426$, $p<.05$, $\eta^2=.053$, %95 GA [.01, .10]), saldırı ve tehditler ($F(4,243)=2.733$, $p<.05$, $\eta^2=.043$, %95 GA [.00, .09]) ve genel güvenlik ($F(4,243)=8.270$, $p<.001$, $\eta^2=.120$, %95 GA [.06, .18]) alt faktörleri ile ölçek genelinde ($F(4,243)=4.648$, $p<.05$, $\eta^2=.071$, %95 GA [.02, .12]) hizmet süresine göre istatistiksel olarak anlamlı farklılık göstermektedir. Etki büyüklükleri incelendiğinde, elde edilen η^2 değerlerinin küçük ile orta düzey arasında değiştiği, özellikle genel güvenlik boyutunda hizmet süresinin daha belirgin bir etkiye sahip olduğu görülmektedir. Farklılığın hangi gruplar arasında olduğunu görmek için Tukey HSD Post Hoc analizi yapılmıştır. Alt faktörler ve ölçek genelinde hizmet süresi 0-5 yıl olan ($\bar{X}=44.48$, $SS=9.63$) öğretmenlerin hizmet süresi 16-20 yıl olan ($\bar{X}=32.27$, $SS=8.96$) öğretmenlere göre daha yüksek bilgi farkındalığına sahip olduğu göze çarpmaktadır. Bu bulgular doğrultusunda H_4 hipotezi kabul edilmiştir.

Bilgi Güvenliği Farkındalık Düzeylerinin İdari Görev Alma Durumuna Göre İncelenmesi

Katılımcıların idari görev alma değişkenine göre bilgi güvenliği farkındalık düzeylerini tespit etmek amacıyla gerçekleştirilen bağımsız örneklem t-testi öncesinde Levene testi uygulanmış ve varyansların homojen dağıldığı belirlenmiştir (p>. 05). Elde edilen t-testi sonuçları Tablo 7'de sunulmuştur.

Tablo 7. İdari Görev Alma Durumu Değişkenine Göre Bilgi Güvenliği Farkındalık Düzeyleri

Faktör	Grup	N	$\bar{X}$	*SS*	*sd*	*t*	*p*	*Cohen'd*
Mobil cihazlar, mahremiyet ve iletişim	İdari görevi var	32	50.81	14.06	246	-2.190	.029*	-0.415
	İdari görevi yok	216	55.45	10.71				
Saldırı ve tehditler	İdari görevi var	32	41.93	15.29	246	-2.177	.030*	-0.413
	İdari görevi yok	216	47.09	12.04				
Genel güvenlik	İdari görevi var	32	35.62	9.69	246	-3.657	.000**	-0.693
	İdari görevi yok	216	42.08	9.27				
Ölçek geneli	İdari görevi var	32	128.37	35.55	246	-2.818	.005*	-0.582

İdari görevi yok	216	144.62	26.64

*p<.05**p<.001

Tablo 7'ye göre katılımcıların bilgi güvenliği farkındalık düzeyleri idari görev alma durumlarına göre tüm alt faktörler ve ölçek genelinde istatistiksel olarak anlamlı şekilde farklılaşmaktadır. Mobil cihazlar, mahremiyet ve iletişim boyutunda (t(246)=-2.190, p<.05, d=-0.41, %95 GA [-0.77, -0.05]), saldırı ve tehditler boyutunda (t(246)=-2.177, p<.05, d=-0.41, %95 GA [-0.77, -0.05]), genel güvenlik boyutunda (t(246)=-3.657, p<.001, d=-0.69, %95 GA [-1.06, -0.32]) ve ölçek genelinde (t(246)=-2.818, p<.05, d=-0.58, %95 GA [-0.94, -0.21]) anlamlı farklılıklar bulunmuştur. Etki büyüklükleri incelendiğinde, mobil cihazlar ile saldırı ve tehditler boyutlarında etki büyüklüğünün orta düzeye yakın, genel güvenlik boyutunda orta-yüksek düzeyde, ölçek genelinde ise orta düzeyde olduğu görülmektedir. Bu bulgular doğrultusunda, H_5 hipotezi kabul edilmiştir.

Bilgi Güvenliği Farkındalık Düzeylerinin Bilgisayar Kullanma Becerisi Değişkenine Göre İncelenmesi

Katılımcıların bilgisayar kullanma becerisi değişkenine göre bilgi güvenliği farkındalık düzeylerini tespit etmek amacıyla gerçekleştirilen tek yönlü ANOVA öncesinde Levene testi uygulanmış ve varyansların homojen dağıldığı belirlenmiştir (p>. 05). Elde edilen ANOVA testi sonuçları Tablo 8'de sunulmuştur.

Tablo 8. Bilgisayar Kullanma Becerisine Göre Bilgi Güvenliği Farkındalık Düzeyleri

	Varyansın kaynağı	**Kareler toplamı**	**Sd**	**Kareler ortalaması**	**F**	***p***	**η²**	**Anlamlı fark**
Mobil cihazlar, mahremiyet ve iletişim	Gruplar arası	4182.103	2	2091.052	18.823	.000**		Düşük<ileri Orta<ileri
	Gruplar içi	27216.671	245	111.088			.133	
	Toplam	31398.774	247					
Saldırı ve tehditler	Gruplar arası	5488.373	2	2744.186	19.960	.000**		Düşük<ileri Orta<ileri
	Gruplar içi	33684.321	245	137.487			.140	
	Toplam	39172.694	247					
Genel güvenlik	Gruplar arası	2480.569	2	1240.285	15.141	.000**		Düşük<ileri Orta<ileri
	Gruplar içi	20069.931	245	81.918			.110	
	Toplam	22550.500	247					
Ölçek geneli	Gruplar arası	35446.500	2	17723.250	21.705	.000**		Düşük<ileri Orta<ileri
	Gruplar içi	200051.242	245	816.536			.151	
	Toplam	235497.742	247					

**p<.001

Tablo 8'e göre katılımcıların bilgi güvenliği farkındalık düzeyleri bilgisayar kullanma becerisine göre; mobil cihazlar, mahremiyet ve iletişim (F(2,245)=18.823, p<.001, η^2=.133, %95 GA [.08, .19]), saldırı ve tehditler (F(2,245)=19.960, p<.001, η^2=.140, %95 GA [.09, .20]), genel güvenlik (F(2,245)=15.141, p<.001, η^2=.110, %95 GA [.06, .17]) alt faktörleri ile ölçek genelinde (F(2,245)=21.705, p<.001, η^2=.151, %95 GA [.10, .21]) istatistiksel olarak anlamlı farklılık göstermektedir. Etki büyüklükleri incelendiğinde, tüm boyutlarda η^2 değerlerinin .110 ile .151 arasında değiştiği ve bu etkilerin orta ile büyük düzey arasında olduğu görülmektedir. Farklılığın hangi gruplar arasında olduğunu görmek için Tukey HSD Post Hoc analizi yapılmıştır. Alt faktörlerin tümünde bilgisayar kullanma becerisi ileri olanların düşük ve orta

seviyede olanlara göre farkındalık düzeyinin de daha yüksek olduğu görülmektedir. Aynı şekilde ölçek genelinde de bilgisayar kullanma becerisi ileri olanların ($\bar{X}$=167.39, SS=22.13), düşük ($\bar{X}$=132.93, SS=22.71) ve orta seviyede ($\bar{X}$=137.55, SS=30.87) olanlara göre farkındalık düzeyinin de daha yüksek olduğu göze çarpmaktadır. Bu bulgular doğrultusunda H_6 hipotezi kabul edilmiştir.

Bilgi Güvenliği Farkındalık Düzeylerinin Günlük İnternet Kullanım Süresi Değişkenine Göre İncelenmesi

Katılımcıların günlük internet kullanım süresi değişkenine göre bilgi güvenliği farkındalık düzeylerini tespit etmek amacıyla gerçekleştirilen tek yönlü ANOVA öncesinde Levene testi uygulanmış ve varyansların homojen dağıldığı belirlenmiştir (p>. 05). Elde edilen ANOVA testi sonuçları Tablo 9'da sunulmuştur.

Tablo 9. Günlük İnternet Kullanım Süresine Göre Bilgi Güvenliği Farkındalık Düzeyleri

	Varyansın kaynağı	**Kareler toplamı**	**Sd**	**Kareler ortalaması**	**F**	***p***	**η²**	**Anlamlı fark**
Mobil cihazlar, mahremiyet ve iletişim	Gruplar arası	173.513	3	57.838	.452	.716		-
	Gruplar içi	31225.261	244	127.972				
	Toplam	31398.774	247					
Saldırı ve tehditler	Gruplar arası	325.587	3	108.529	.682	.564		-
	Gruplar içi	38847.107	244	159.209				
	Toplam	39172.694	247					
Genel güvenlik	Gruplar arası	809.105	3	269.702	3.027	.030*	.036	0-2 saat<4-6 saat
	Gruplar içi	21741.395	244	89.104				
	Toplam	22550.500	247					
Ölçek geneli	Gruplar arası	3353.107	3	1117.702	1.175	.320		-
	Gruplar içi	232144.635	244	951.412				
	Toplam	235497.742	247					

**p<.05*

Tablo 9'a göre katılımcıların bilgi güvenliği farkındalık düzeyleri günlük internet kullanım süresine göre; mobil cihazlar, mahremiyet ve iletişim (F(3,244)=.452, p>.05), saldırı ve tehditler (F(3,244)=.682, p>.05) ve ölçek geneli (F(3,244)=1.175, p>.05) açısından istatistiksel olarak anlamlı bir farklılık göstermemektedir. Buna karşın genel güvenlik boyutunda anlamlı bir farklılık bulunmuştur (F(3,244)=3.027, p<.05, η^2=.036, %95 GA [.00, .08]). Etki büyüklüğü incelendiğinde, genel güvenlik boyutunda elde edilen η^2=.036 değerinin küçük düzeyde olduğu görülmektedir. Farklılığın hangi gruplar arasında olduğunu görmek için Tukey HSD Post Hoc analizi yapılmıştır. Buna göre genel güvenlik alt faktöründe, günlük 4-6 saat internet kullanım süresine ($\bar{X}$=44.50, SS=9.78) sahip olan öğretmenlerin farkındalık ortalamaları 0-2 saat olanlara göre ($\bar{X}$=39.38, SS=10.26) daha yüksek çıkmıştır. Bu bulgular doğrultusunda H7 hipotezi kısmen reddedilmiştir.

TARTIŞMA ve SONUÇ

Bu çalışmada öğretmenlerin bilgi güvenliği farkındalık düzeyleri çeşitli bireysel ve mesleki değişkenlere göre incelenmiştir. Elde edilen sonuçlara göre öğretmenlerin bilgi güvenliği farkındalıkları genel olarak orta düzeyde çıkmıştır. Bu sonuç alan yazında yapılan bazı araştırmaları destekler niteliktedir (Ecek & Yılmaz, 2023; Hakkari, 2022; Özdemir & Uluyol, 2021). Üniversite öğrencisi örneklemi ile çalışılan bazı araştırmalarda ise bilgi güvenliği farkındalığının daha yüksek çıktığı ifade edilmiştir (Avcı & Oruç, 2020; Göldağ, 2021). Bu

farklılık gençlerin siber güvenlik davranışlarında yaşlılara göre daha dikkatli olma eğilimi göstermeleri ve çevrimiçi olarak daha aktif olmaları nedeniyle siber saldırılara karşı daha duyarlı olmaları ile açıklanabilir (Witsenboer vd., 2022). Mevcut çalışmada genel bilgi güvenliği farkındalıklarının orta düzeyde çıkması, KMT'deki algılanan tehdit boyutunun da sınırlı düzeyde geliştiğine işaret etmektedir. Dolayısıyla öğretmenlerin dijital risklerin varlığının farkında olmakla birlikte, bu tehditlerin ciddiyeti ve kendilerine yönelik olasılığı konusunda yeterince güçlü bir algıya sahip olmadıkları söylenebilir. Bu durum koruyucu davranışlarının da orta düzeyde kalmasına yol açabilmektedir. Çünkü potansiyel tehditler hakkındaki farkındalık düzeyinin ve algılanan tehdit seviyelerinin koruyucu davranışları da doğrudan şekillendirdiği vurgulanmaktadır (Han vd., 2025; Mousavi vd., 2020).

Mevcut çalışma sonuçlarına göre bilgi güvenliği farkındalık ölçeğinin "saldırı ve tehditler" faktörünün ortalaması diğer faktörlerden daha düşük çıkmıştır. Öğretmenlerin "saldırı ve tehditler" alt faktöründe farkındalıklarının daha düşük çıkması teknik bilgi içeren siber tehdit türleri açısından daha az bilgiye sahip olmalarıyla açıklanabilir. Nitekim ölçeğin saldırı ve tehditler faktörü altında yer alan "Aldatmaca (hoax) nedir biliyorum", "Hizmet aksatma (Denial of Service – DoS) saldırısı nedir biliyorum", "Web sayfalarında kullanılan aktif içeriğin (active content) ne işe yaradığını biliyorum" gibi bazı maddelerde bu tür terimler göze çarpmaktadır. Benzer şekilde "Sosyal mühendislik (social engineering) saldırısı nedir biliyorum" ve "Kimlik avı (phishing) saldırısı nedir biliyorum" gibi maddeler de yine saldırı ve tehditler faktörü altında yer alan ve öğretmenlerin daha az bilgi sahibi olduğu maddeler olarak ön plana çıkmıştır. "Saldırı ve tehditler" faktör puanlarının diğer boyutlara göre daha düşük çıkması KMT bağlamında algılanan ciddiyet ve algılanan duyarlılık bileşenleriyle doğrudan ilişkilendirilebilir. Öğretmenlerin Hoax, DoS, phishing veya sosyal mühendislik gibi teknik tehditler konusunda bilgi eksikliği, tehdit algısının zayıf olduğunu düşündürmektedir. Tehdit doğru algılanmadığında, bireylerin korunma motivasyonu da düşük olmakta ve bu durum savunma mekanizmalarının hiç tetiklenmemesine yol açmaktadır (Pratama vd., 2025). Bu noktada öğretmenlerin güncel siber saldırı türlerine ilişkin farkındalıklarının arttırılması için araştırma ya da eğitime ihtiyaç duydukları ifade edilebilir. Benzer durum başka araştırma sonuçlarında da göze çarpmaktadır. Aksoğan ve Atıcı'nın çalışmasında da (2023) katılımcıların giriş işlemlerinde cep telefonlarına gönderilen şifrelerin kullanılmasının güvenliği arttırdığı konusunda farkındalıkları yüksek bulunurken, güvenlik duvarı yazılımları gibi konular hakkında yeterli bilgiye sahip olmadıkları belirtilmiştir. Siber tehlike farkındalığını ele alan başka bir çalışmada ise (Zwilling vd., 2022), yeterli düzeyde siber tehdit farkındalığına sahip olan internet kullanıcılarının sadece nispeten daha basit olan güçlü parola koruması kullanma ve anti virüs yazılımı yükleme gibi minimal koruyucu önlemler uyguladıkları görülmüştür. Gabra vd.'nin çalışmasında (2020) ise üniversite öğrencilerin çoğunluğunun kimlik avı saldırıları bilgisinden yoksun olduğu ortaya çıkmıştır. Diğer bir çalışmada (Hadlington, 2018) katılımcılarda görülen aynı parolayı birden fazla web sitesi için kullanma, parolaları meslektaşları ile paylaşma ve e-postalardaki bağlantılara tıklama gibi riskli davranışların farkındalık eksikliğinden kaynaklandığı ifade edilmiştir.

Öğretmenlerin bilgi güvenliği farkındalık düzeylerinin cinsiyet değişkenlerine göre farklılaşmadığı ortaya çıkmıştır. KMT bağlamında değerlendirildiğinde erkek ve kadın öğretmenlerin hem tehdit algıları hem de baş etme değerlendirmeleri açısından benzer bilişsel süreçlere sahip oldukları söylenebilir. Bu sonuçla paralel şekilde Özdemir ve Uluyol'un (2021) çalışmasında da erkek ve kadın katılımcıların benzer seviyede bilgi güvenliği farkındalığına sahip oldukları görülmüştür. Bazı çalışmalarda ise farkındalık düzeyi erkekler lehine yüksek çıkmıştır (Aksoğan & Atıcı, 2023; Canoğulları, 2021; Keser & Yayla, 2021). Bu farklılığın,

araştırmalarda kullanılan örneklem özellikleri, ölçme araçlarının kapsamı, katılımcıların teknoloji kullanım alışkanlıkları ve bilgi güvenliği eğitimine erişim düzeyleri gibi değişkenlerden kaynaklanabileceği düşünülmektedir.

Çalışmadan elde edilen başka bir sonuca göre, öğretmenlerin bilgi güvenliği farkındalık düzeyleri hizmet süresi arttıkça düşüş göstermiştir. Akademisyenlerle çalışan Aksoğan ve Atıcı'nın çalışmasında da (2023) mesleki deneyimi 1-5 yıl arasında olan katılımcıların daha yüksek farkındalığa sahip oldukları, en düşük farkındalığın ise 21 yıl ve daha fazla mesleki deneyime sahip olanlarda görüldüğü belirtilmiştir. Bu ters orantı bazı araştırmalarda katılımcıların farkındalık seviyeleri ile yaşları arasında da ön plana çıkmıştır (Canoğulları, 2021; Gündüzalp, 2021; Keser & Yayla, 2021; Özdemir & Uluyol, 2021). Yaş ile hizmet süresinin çoğunlukla birlikte arttığı düşünüldüğünde, bu araştırma sonuçlarının da mevcut çalışmadan elde edilen sonucu desteklediği söylenebilir. Öte yandan bilgi güvenliği farkındalık düzeylerinin idari görev alan öğretmenlerde de daha düşük çıktığı tespit edilmiştir. Yönetici konumundaki öğretmenlerin çoğunlukla hizmet süresi ve yaşça daha büyük olmalarının bunda etkisi olduğu söylenebilir. Bunun yanında bilgi güvenliği farkındalığına ilişkin Nezgitli ve Gökçearslan'ın (2022) belirtmiş olduğu kurumsal bilgi güvenliği politikasının planlanması ve uygulanmasında yetersizlik yaşanmasının da bu sonuca katkı sağladığı düşünülmektedir. Hizmet süresi arttıkça farkındalığın azalması bulgusu, KMT modelinde özellikle öz-yeterlik ve tepki yeterliği bileşenleri ile açıklanabilir. Mesleki deneyimi yüksek öğretmenlerin teknolojik gelişmeleri daha sınırlı takip etmeleri ve güncel dijital tehditlere daha az maruz kalmaları, kendilerini bu tehditlerle başa çıkma konusunda da daha az yeterli hissetmelerine yol açabilir. Bu da koruyucu davranış motivasyonunu düşürmektedir. İdarecilerin farkındalığının düşük çıkması ise tepki maliyeti ile ilişkilendirilebilir. Yoğun iş yükü altında güvenlik prosedürlerini uygulamak idareciler için zaman alıcı ve zor bir maliyet olarak algılanabilmektedir (Wang vd., 2021).

Çalışmada elde edilen diğer bir sonuca göre, katılımcıların bilgisayar kullanma becerisi düzeyleri arttıkça bilgi güvenliği farkındalık düzeyleri de artmıştır. Bu doğrultuda bilgisayar kullanma becerisi yüksek ve bilişim teknolojilerinin doğasına daha hâkim olan öğretmenlerin siber tehditlerin daha çok farkında oldukları ifade edilebilir. Bilgisayar kullanma becerisi arttıkça farkındalığın artması KMT'nin öz-yeterlik bileşenini güçlü biçimde desteklemektedir. Araştırmalar bireylerin öz yeterlilikleri arttıkça, bilgi tehditlerinden kaçınma davranışında bulunma motivasyonlarının da arttığını göstermiştir (Han vd., 2025; Ng vd., 2021). Bazı çalışmalarda siber tehditlere karşı güvenli davranış göstermede öz-yeterlik bileşeni KMT'nin en önemli bileşeni olarak görümektedir (Ezati Rad vd., 2021; Pratama vd. (2025). Bilişim teknolojilerine hâkim olan öğretmenler, hem tehditleri daha iyi tanımlayabilmekte hem de bu tehditlere karşı hangi önlemlerin işe yarayacağını bilmektedir. Bu durum onların koruyucu davranış geliştirme olasılığını artırmaktadır. Çalışmalarda bilgi güvenliği farkındalığı açısından bilişim teknolojileri öğretmenleri lehine çıkan sonuçlar da bunu desteklemektedir (Canoğulları, 2021; Keser & Yayla, 2021). Zwilling vd.'nin (2022) çalışmasında da bilgisayar bilimi bilgisi ile siber güvenlik farkındalığı açısından yüksek düzeyde pozitif ilişki elde edilmiştir.

Elde edilen bulgular KMT çerçevesinde bütüncül bir yaklaşımla değerlendirildiğinde, öğretmenlerin özellikle oltalama ve siber saldırı konusunda teknik bilgi eksikliğine bağlı olarak tehdit algılarının zayıf olduğu ve bu durumun bilişsel koruma mekanizmalarını tetikleyemediği görülmektedir. Bu siber zafiyet durumunun salt demografik özelliklerden ziyade teknik yetkinlik ve mesleki dinamiklerle şekillendiği düşünülmektedir. Nitekim bilgisayar becerisi yüksek olan öğretmenlerin siber tehditlerle başa çıkma noktasında öz-yeterlik algıları güçlü ve

farkındalıkları yüksek çıkarken; hizmet süresi artan kıdemli öğretmenlerin teknolojik dönüşüme direnç göstermeleri veya güvenlik adımlarını birer iş yükü (tepki maliyeti) olarak görmeleri nedeniyle farkındalık düzeyleri doğrusal bir düşüş sergilemiştir. Çalışmanın en kritik ve yönetimsel risk doğuran sentez sonucu ise, dijital sistemler üzerinden hassas verilere doğrudan erişim yetkisi bulunan okul idarecilerinin, yoğun iş temposunun getirdiği zaman baskısı ve kuşaksal faktörlerin etkisiyle tüm boyutlarda en düşük farkındalık düzeyine sahip olması ve dolayısıyla kurumsal bilgi güvenliği zincirinin en zayıf halkasını oluşturmasıdır.

Sınırlılıklar ve Öneriler

Bu çalışmada ulaşılabilir örnekleme yöntemi kullanılmış olması, elde edilen bulguların evreni temsil gücünü sınırlayabilmektedir. Bu yöntem, pratiklik ve erişilebilirlik açısından avantaj sağlasa da örneklemin rastgele seçilmemesi nedeniyle sonuçların genellenebilirliğini azaltmaktadır. Ayrıca verilerin yalnızca tek bir ilden toplanmış olması da elde edilen bulguların Türkiye genelindeki öğretmenlere genellenmesini güçleştirmektedir. Ulusal düzeyde daha temsili bir tablo elde edebilmek için, gelecekteki araştırmalarda farklı coğrafi, kültürel ve sosyo-ekonomik özelliklere sahip birden fazla il dahil edilebilir ve tabakalı rastgele örnekleme yöntemleri kullanılabilir. Bununla birlikte çalışmadan elde edilen sonuçlar doğrultusunda aşağıdaki önerilerde bulunulabilir:

- Bigi güvenliği farkındalığı düşük çıkan başta idareciler olmak üzere hizmet yılı ve yaşı yüksek öğretmenlere yönelik hizmet içi farkındalık eğitimleri sunulabilir.
- Hizmet içi seminer veya eğitimlerde öğretmenlerin daha az bilgiye sahip olduğu görülen sosyal mühendislik ve güncel siber tehdit türlerine ağırlık verilebilir.
- Güvenlik riskleri ile alakalı olarak okullarda bilgilendirici basılı posterler, duyurular, broşürler ile birlikte sosyal medya gruplarında dijital paylaşımlar ile farkındalık düzeyleri arttırılabilir.
- Bilgi güvenliği farkındalığının erken yaşlarda kazanılması için ders olarak öğretim programlarına yerleştirilerek öğretmenlerin göreve başlamadan bu farkındalığı kazanmaları sağlanabilir.
- Okullarda bilişim teknolojileri öğretmenleri kendi okullarındaki diğer paydaşlarını güncel siber tehditler hakkında bilgilendirerek olası risklerden haberdar edebilir.

Gelecekteki çalışmaların nicel yöntemle birlikte görüşme ve gözlem gibi nitel teknikler ile yürütülerek öğretmenlerden bilgi güvenliği farkındalıklarına ilişkin daha detaylı veriler elde edilebilir.

KAYNAKÇA

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

Aksoğan, M. & Atıcı, B., (2023). Akademisyenlerin dijital veri güvenliği farkındalıkları üzerine bir araştırma: Malatya örneği. *Gümüşhane Üniversitesi Sosyal Bilimler Dergisi*, *14*(2), 429-439.

Alrawhani, E. M., Romli, A., & Al-Sharafi, M. A. (2025). Evaluating the role of protection motivation theory in information security policy compliance: Insights from the banking sector using PLS-SEM approach. *Journal of Open Innovation: Technology, Market, and Complexity*, *11*(1), 100463. https://doi.org/10.1016/j.joitmc.2024.100463

Ateş, H., & Gündüzalp, C. (2025). The convergence of GETAMEL and protection motivation theory: A study on augmented reality-based gamification adoption among science teachers. *Education and Information Technologies, 30*(12), 17361-17403. https://doi.org/10.1007/s10639-025-13480-1

Ateş, S., & Küçük, S. (2023). Öğretmenlerin bilgi güvenliği farkındalık ve dijital okuryazarlık durumlarının incelenmesi. *Necmettin Erbakan Üniversitesi Ereğli Eğitim Fakültesi Dergisi, 5*(2), 491-534. https://doi.org/10.51119/ereegf.2023.66

Avcı, Ü., & Oruç, O. (2020). Üniversite öğrencilerinin kişisel siber güvenlik davranışları ve bilgi güvenliği farkındalıklarının incelenmesi. *Inonu University Journal of the Faculty of* Education *(INUJFE), 21*(1), 284-303. https://doi.org/10.17679/inuefd.526390

Aydın, M., Hali, Ö., Kırımlı, H., & Çakıroğlu, Ü. (2023). Lise öğrencilerinin bilgi güvenliği farkındalıkları ne düzeyde? Öğretmenler bu farkındalıkların neresinde?. *Bilgi Yönetimi*, *6*(1), 179-195. https://doi.org/10.33721/by.1237672

Başarmak, U., & Ateş, H. (2026). Integrating UTAUT-2 and protection motivation theory to explain pre-service teachers' adoption of AI-supported game-based learning. *Education and Information Technologies*, 1-43. https://doi.org/10.1007/s10639-026-13975-5

Büyüköztürk, Ş., Kılıç Çakmak, E., Akgün, Ö. E., Karadeniz, Ş., & Demirel, F. (2020). *Bilimsel araştırma yöntemleri* (28. baskı). Pegem Akademi.

Canoğulları, E. (2021). Öğretmenlerin bilgi güvenliği konusundaki farkındalıklarının incelenmesi. *Kalem Eğitim ve İnsan Bilimleri Dergisi*, *11*(2), 651-679. https://doi.org/10.23863/kalem.2021.219

Conteh, N. Y., & Schmick, P. J. (2021). *Cybersecurity risks, vulnerabilities, and countermeasures to prevent social engineering attacks. In Ethical hacking techniques and countermeasures for cybercrime prevention* (pp. 19-31). IGI Global.

Çetinkaya, L., Güldüren, C., & Keser, H. (2017). Öğretmenler için bilgi güvenliği farkindalik ölçeği (BGFÖ) geliştirme çalişmasi. *Milli Eğitim Dergisi*, *46*(216), 33-52.

Değirmenci, N., & Demiral, D. G. (2023). Bilgi güvenliği farkındalığı üzerine üniversite öğrencilerine yönelik araştırma. *Karadeniz Sosyal Bilimler Dergisi, 15*(29), 613-635.

Digital, 2025. https://datareportal.com/reports/digital-2025-turkey

Dodge, C. E., Fisk, N., Burruss, G. W., Moule Jr, R. K., & Jaynes, C. M. (2023). What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory. *Criminology ve Public Policy, 22*(4), 849-868. https://doi.org/10.1111/1745-9133.12641

Ecek, N., & Çakmak, A. F. (2022). Çalışanların bilgi güvenliği önlemlerine dair tutumları: Ampirik bir değerlendirme. *International Journal of Applied Economic and Finance Studies*, *7*(2), 26-44.

Ecek, N., & Yılmaz, S. (2023). Öğretim elemanlarının bilgi güvenliği farkındalığı üzerine bir araştırma. *Turkish Management Review*, *2*(1), 18-39. https://doi.org/10.5281/zenodo.8148647

Erdoğan, M., & Coşar, M. (2026). Öğretmenlerin branş bazında siber güvenlik farkındalık düzeylerinin belirlenmesi. *Kamu Yönetimi ve Teknoloji Dergisi, 8*(1), 36-58. https://doi.org/10.58307/kaytek.1694363

Ezati Rad, R., Mohseni, S., Kamalzadeh Takhti, H., Hassani Azad, M., Shahabi, N., Aghamolaei, T., & Norozian, F. (2021). Application of the protection motivation theory for predicting COVID-19 preventive behaviors in Hormozgan, Iran: a cross-sectional study. *BMC Public Health, 21*(1), 466. https://doi.org/10.1186/s12889-021-10500-w

Gabra, A., Sirat, M. B., Hajar, S., & Dauda, I. B. (2020). Cyber security awareness among university students: A case study. *Science Proceedings Series, 2*(1), 82-86.

Genç, N., & Yücel, M. (2025). Öğretmenlerin oltalama saldırılarına karşı farkındalık düzeyleri. *İstanbul Eğitim Dergisi,* (2), 84-105. https://doi.org/10.71270/istanbulegitim.istj.1660280

Ghazali, N. N., Hassan, S., & Ahmad, R. (2023). Fortifying against cyber fraud: instrument development with the protection motivation theory. *International Journal of Advanced Computer Science and Applications, 14*(10).

Gökçearslan, Ş., Günbatar, M. S., & Sarıtepeci, M. (2021). Ortaöğretim öğrencilerinin bilgi güvenliği farkındalıklarının incelenmesi. *Van Yüzüncü Yıl Üniversitesi Eğitim Fakültesi Dergisi*, *18*(1), 354-373. https://doi:10.33711/yyuefd.867015

Göldağ, B. (2021). Üniversite öğrencilerinin dijital okuryazarlık düzeyleri ile dijital veri güvenliği farkındalık düzeyleri arasındaki ilişkinin incelenmesi. *e-Uluslararası Eğitim Araştırmaları Dergisi, 12*(3), 82-100.44(1), 61-84. https://doi.org/10.19160/e-ijer.950635

Gültekin, V., & Özel, N. (2023). Üniversite öğrencilerinin bilgi güvenliği farkındalığı: Ankara Üniversitesi örneği. *Bilgi Yönetimi, 6*(2), 310-331. https://10.33721/by.1366855

Gündüz, M. Z., & Daş, R. (25-26 Ekim, 2016). *Sosyal mühendislik: Yaygın ataklar ve güvenlik önlemleri*. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 1-8, Ankara, Türkiye.

Gündüzalp, C. (2021). Üniversite çalışanlarının dijital veri ve kişisel siber güvenlik farkındalıkları (Bilgi İşlem Daire Başkanlıkları örneği). *Journal of Computer and Education Research*, *9*(18), 598-625. https://10.18009/jcer.907022

Hadlington, L. (2018). Employees attitude towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom. *International Journal of Cyber Criminology, 12*(1), 269-281. https://10.5281/zenodo.1467909

Hadlington, L., Binder, J., & Stanulewicz, N. (2020). Fear of missing out predicts employee information security awareness above personality traits, age, and gender. *Cyberpsychology, Behavior, and Social Networking, 23*(7), 459-464. https://doi.org/10.1089/cyber.2019.0703

Hakkari, F. (2022). Ön lisans öğrencilerinin bilgi güvenliği kazanimi ve farkindalik düzeylerinin belirlenmesi: Kırıkhan Meslek Yüksekokulu örneği. *Bilgi ve İletişim Teknolojileri Dergisi*, *4*(1), 66-86. https://doi.org/10.53694/bited.1121085

Han, M., Zhao, H., Ma, X., & Shi, R. (2025). Influencing factors of information security behavior among college students based on protection motivation theory: evidence from China. *Frontiers in Public Health*, *13*, 1677024. https://doi.org/10.3389/fpubh.2025.1677024

Haseski, H. I. (2020). Cyber security skills of pre-service teachers as a factor in computer-assisted education. *International Journal of Research in Education and Science, 6*(3), 484-500.

Hekim, H. (2015). *Oltalama (Phishing) Saldirilari. http://www.academia. edu/35136881/Oltalama_Phishing_Saldirilari*

Karabatak, S., & Karabatak, M. (2019, June). *Information security awareness of school administrators*. In 2019 7th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6). IEEE.

Karapınar, D. Ç., & Daş, A. (2022). Açik ve uzaktan eğitim öğrencilerinin bilgi güvenliği farkindaliği: Atatürk Üniversitesi örneği. *EKEV Akademi Dergisi, 93*, 103-118.

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

Keser, H., & Yayla, H. G. (2021). Fatih projesi uygulanan okullardaki öğretmenlerin bilgi güvenliği farkındalık düzeylerinin incelenmesi. *Milli Eğitim Dergisi*, *50*(229), 9-40.

Kubacka, A., Biały, D., & Gołąb, R. (2021). Perception of information security in the process of distance learning during the COVID-19 pandemic on the example of university teachers' experiences. *International Journal of Research in E-learning IJREL, 7*(2), 1-18. https://doi.org/10.31261/IJREL.2021.7.2.05

Mai, P. T., & Tick, A. (2021). Cyber security awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam. *Acta Polytechnica Hungarica, 18*(8), 67-89.

Mou, J., Cohen, J. F., Bhattacherjee, A., & Kim, J. (2022). A test of protection motivation theory in the information security literature: A meta-analytic structural equation modeling approach. *Journal of the Association for Information Systems, 23*(1), 196-236. https://10.17705/1jais.00723

Mousavi, R., Chen, R., Kim, D. J., & Chen, K. (2020). Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory. *Decision Support Systems*, 135, 113323. https://doi.org/10.1016/j.dss.2020.113323

Nezgitli, S., & Gökçearslan, Ş., (2022). Kamu kurumu ve özel sektöre yönelik bilgi güvenliği farkındalığı üzerine bir inceleme. *Instructional Technology and Lifelong Learning*, *3*(1), 19-44. https://doi.org/10.52911/itall.1115701

Ng, K. C., Zhang, X., Thong, J. Y., & Tam, K. Y. (2021). Protecting against threats to information security: An attitudinal ambivalence perspective. *Journal of management information systems, 38*(3), 732-764. https://doi.org/10.1080/07421222.2021.1962601

Özdemir, A., & Uluyol, Ç. (2021). Kamu kurum ve kuruluşlarında bilgi güvenliği farkındalığı. *Türkiye Sosyal Araştırmalar Dergisi*, *25*(3), 649-666.

Öztrak, S., Şahin, H., & Efe, Ö. F. (2025). Üniversite öğretim elemanlarının kişisel siber güvenlik farkındalığı. *Journal of Statistics and Applied Sciences*, *12*, 9-23. https://doi.org/10.52693/jsas.1720217

Pratama, O., Aladin, R. A., Lim, B., & Sundjaja, A. M. (2025). Determinants of security behavior intention in state-owned enterprises: Applying protection motivation theory to phishing emails. *International Journal of Safety ve Security Engineering, 15(*3). https://doi.org/10.18280/ijsse.150304

Raiyn, J. (2014). A survey of cyber attack detection strategies. *International Journal of Security and Its Applications, 8*(1), 247-256. http://dx.doi.org/10.14257/ijsia.2014.8.1.23

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology, 91*(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

Romansky, R. P., & Noninska, I. S. (2020). Challenges of the digital age for privacy and personal data protection. *Mathematical Biosciences and Engineering, 17*(5), 5288-5303. https://doi.org/10.3934/mbe.2020286

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future internet, 11*(4), 89. https://doi.org/10.3390/fi11040089

Tabachnick, B. G., & Fidell, L. S. (2013). *Using Multivariate Statistics.* Always learning.

Talan, T., & Aktürk, C. (2021). Orta öğretim öğrencilerinin dijital okuryazarlık ve bilgi güvenliği farkındalığı seviyelerinin incelenmesi. *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi*, *18*(1), 158-180. https://doi.org/10.33437/ksusbd.668255

TÜİK, (2025). *Hane halkı bilişim teknolojileri kullanım araştırması Erişim adresi https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2025-53925*

Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, 59, 138-150.

Wang, H. W., Kuo, S. Y., & Chen, L. B. (2021). Exploring the relationship between internal information security, response cost, and security intention in container shipping. *Applied Sciences, 11*(6), 2609. https://doi.org/10.3390/app11062609

Witsenboer, J. W. A., Sijtsma, K., & Scheele, F. (2022). Measuring cyber secure behavior of elementary and high school students in the Netherlands. *Computers & Education, 186*, 104536. https://doi.org/10.1016/j.compedu.2022.104536

Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers & Security*, 77, 860-870. https://doi.org/10.1016/j.cose.2018.03.008

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, 128, 113160. https://doi.org/10.1016/j.dss.2019.113160

Yalçın, N., & Avşar, A. (2018, 31 Ocak-2 Şubat). *Sosyal mühendislik atakları ve alınması gereken önlemler*. 20. Akademik Bilişim Konferansı, Karabük, Türkiye.

Yılmaz, E., Şahin, Y. L., & Akbulut, Y. (2016). Öğretmenlerin dijital veri güvenliği farkındalığı. *Sakarya University Journal of Education, 6*(2), 26-45. http://dx.doi.org/10.19126/suje.29650

Yılmaz, S. Y., & Avcı, E. (2022). Oltalama saldırılarının yeni hedefi otel web siteleri. *Journal of Gastronomy, Hospitality and Travel, 5*(2), 588-606. https://doi.org/10.33083/joghat.2022.153

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 62*(1), 82-97. https://doi.org/10.1080/08874417.2020.1712269

EXTENDED ABSTRACT

Analysis of Teachers' Information Security Awareness in the Context of Individual and Professional Variables

Introduction

In the information age, it is clear that the internet and rapidly developing technologies make access to information easier day by day. Especially in the last decade, mobile devices and digital applications have transformed daily life on a global scale and facilitated various lifestyles in many areas (Zwilling et al., 2022). However, the internet and other information technologies that keep people actively and intensively in the system both in the world and in our country have not only made life easier, but also brought various risks and threats. Cybersecurity threats can affect not only companies, but also all individuals who use smart devices. Studies have shown that human errors play a role in 95% of security incidents (Witsenboer et al., 2022). In this respect, it is stated that one of the fastest and most effective methods for ensuring information security is to create and raise awareness as much as possible (Kubacka et al., 2021). Teachers use information and communication technologies extensively both during and outside the education-training process (Çetinkaya et al., 2017; Yılmaz et al., 2016). It is important for teachers, who are an important part of the information society and who will guide the new generations, to be aware of the elements that will threaten information security and to take the necessary precautions in order to protect the new generations they raise together with teachers. For this purpose, first of all, determining the awareness levels of teachers and making the necessary plans in this direction come to the fore (Canoğulları, 2021). When the literature is examined, it is seen that the research on information security in the field of education is mostly conducted on academic staff, teacher candidates and university students. It is seen that the number of studies on the information security awareness of teachers and administrators is limited and there is a gap in the literature on this subject. In this direction, the aim of this study is to determine the information security awareness levels of teachers and to examine them according to some variables.

Method

In this study, where the quantitative research method was used, the screening model was used. In the study, data were obtained from a total of 248 teachers working in high schools, primary schools and middle schools (primary education) in the city center of Van using the accessible sampling method. Personal information form and information security awareness scale (Çetinkaya et al., 2017) were used as data collection tools in the study. Data obtained from the sample group were analyzed using the SPSS package program in a computer environment. First, normality analysis was performed to understand whether the data showed a normal distribution. Parametric tests were applied as a result of the skewness and kurtosis values of the scale scores and sub-factors being between -1.5 and +1.5, which is acceptable (Tabachnick & Fidell, 2013).

Findings

Teachers' general information security awareness was at a moderate level. When the sub-factors were examined, the "mobile devices, privacy and communication" factor and "general security" factor averages were at a normal level, while the "attacks and threats" factor was at a moderate level. No significant difference was found according to gender and school type. Teachers with

more years of service and administrative duties had lower information security awareness. As their computer skills increased, their information security awareness levels also increased.

Conclusion, Discussion

The fact that teachers' information security awareness was at a moderate level supports some studies in the literature (Ecek & Yılmaz, 2023; Hakkari, 2022; Özdemir & Uluyol, 2021). In addition, the fact that teachers' awareness was lower in the "attacks and threats" sub-factor can be explained by the fact that they have less knowledge about current cyber threat types that include technical information. Similarly, in the study by Aksoğan and Atıcı (2023), it was seen that the participants did not have sufficient knowledge about issues such as firewall software, and in the study by Gabra et al. (2020), the majority of the participants lacked knowledge about phishing attacks.

The information security awareness levels of teachers did not show a significant difference according to the gender variable. In parallel with this result, it was seen that male and female participants had similar levels of information security awareness in the study by Özdemir and Uluyol (2021). In some studies, the level of awareness was found to be higher in favor of men (Aksoğan & Atıcı, 2023; Canoğulları, 2021; Keser & Yayla, 2021). However, teachers' information security awareness levels decreased as their length of service increased and according to their administrative duties. This result can be associated with the fact that teachers in managerial positions are mostly older and have a longer length of service.

In line with the results obtained, in-service awareness training can be provided to increase the information security awareness levels of teachers, especially administrators. These trainings can be arranged by taking into account differences such as years of service and age. In addition, the trainings can focus on social engineering and current cyber threat types, which teachers are less knowledgeable about.

JENA
Journal of Education and New Approaches

Makale Bilgileri:	Öğretmenlerin Bilgi Güvenliği Farkındalığının Bireysel ve Mesleki Değişkenler Bağlamında Analizi
Makale Türü:	*Araştırma Makalesi*
Geliş Tarihi:	*19.01.2026*
Kabul Tarihi:	*24.06.2026*
Yayım Tarihi:	*30.06.2026*
Sorumlu yazar	*Sinan Bilici*
Değerlendirme:	*Çift Taraflı Kör Hakemlik*
Etik Beyan:	** * Bu çalışmanın hazırlanma sürecinde bilimsel ve etik ilkelere uyulduğu ve yararlanılan tüm çalışmaların kaynakçada belirtildiği beyan olunur.*
Benzerlik Taraması:	*Yapıldı / Turnitin /intihal.net vb.*
Etik Kurul Kararı:	*Bu araştırma Van Tuşba İlçe Milli Eğitim Müdürlüğü'nün 10/06/2024 ve E-89601435-20-104153505 sayılı kararı ile alınan izinle yürütülmüştür.*
Katılımcı Rızası:	*Katılımcı onam formu*
Mali Destek:	*Çalışma için herhangi bir kurum ve projeden mali destek alınmamıştır.*
Çıkar Çatışması:	*Çalışmada kişiler ve kurumlar arası çıkar çatışması bulunmamaktadır.*
Yazar Katkısı	*Bütün yazarlar eşit katkıda bulunmuşlardır.*
Telif Hakları & Lisans:	*Dergi, dergide yayınlanan çalışmalarının telif hakkına sahiptir ve çalışmaları Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License altında yayımlanmaktadır.*