Cumhuriyet International Journal of Education, 11(4): 696-708, 2022
DOI: https://dx.doi.org/10.30703/cije.1131545

Cumhuriyet International Journal of Education

| cije.cumhuriyet.edu.tr | Founded: 2011 Available online, ISSN: 2147-1606 Publisher: Sivas Cumhuriyet Üniversitesi

Development of Information Security Awareness Scale for Secondary School Learners

Levent Çetinkaya[1,a,*], Bülent Öktelik[2,b]

[1]*Faculty of Education, Canakkale Onsekiz Mart University, Çanakkale, Türkiye*

[2]*School of Graduate Studies, Canakkale Onsekiz Mart University, Çanakkale, Türkiye*

**Corresponding author*

Research Article

Acknowledgment

#This study is a part of master's thesis

History

Received: 16/06/2022

Accepted: 13/10/2022

iThenticate

This paper was checked for plagiarism using iThenticate during the preview process and before publication.

ABSTRACT

Although technology-based solutions are implemented against the increasing and diversifying risks towards information security, the human factor should also be taken in consideration. It is necessary to determine the levels of awareness at an early age and take the necessary measures in order to minimize these man-made risks, which are critical in ensuring information security. Considering this fact, it was aimed to develop a measurement tool that would determine the level of information security awareness of the students studying at primary school. At first, Exploratory Factor Analysis (EFA) was performed with a group of 410 participants, which yielded that the scale consisted of 30 items with three sub-dimensions ("online security awareness: osa", "online curiosity: oc" and "cyber threat awareness: cta). Then the measurement tool was applied to a group of 265 participants and a 3-factor structure was confirmed by Confirmatory Factor Analysis (CFA). Cronbach's alpha reliability coefficient for the entire scale is .90; and for each sub-dimension; osa: .94, oc: .90, and cta: .86. As a result of this study, a valid and reliable scale was developed to determine the information security awareness levels of students studying at secondary school. In addition, a statistically significant difference was found between the average information security awareness scores of students studying at secondary school.

Keywords: Information security, awareness, information security awareness, scale development, secondary school level

Ortaokul Düzeyi Öğrencilerine Yönelik Bilgi Güvenliği Farkındalık Ölçeği Geliştirme Çalışması

Bilgi

#Bu çalışma yüksek lisans tezinin bir parçasıdır.

**Sorumlu yazar*

Süreç

Geliş: 16/06/2022

Kabul: 13/10/2022

Bu çalışma ön inceleme sürecinde ve yayımlanmadan önce iThenticate yazılımı ile taranmıştır.

ÖZ

Bilgi güvenliğine yönelik çeşitlenerek artan risklere karşı her ne kadar teknoloji temelli çözümler hayata geçiriliyor olsa da insan faktörünün göz ardı edilmemesi gerekmektedir. Bilgi güvenliğinin sağlanmasında kritik öneme sahip olan insan faktörlü risklerin en aza indirgenmesi için ise erken yaşta farkındalık düzeylerinin belirlenmesi ve bu çerçevede tedbirlerin alınması gerekmektedir. Bu durum göz önünde bulundurularak gerçekleştirilen çalışmada ilköğretim düzeyi ortaokul kademesinde öğrenim gören öğrencilerin bilgi güvenliği farkındalık düzeylerinin belirlenmesine yönelik ölçme aracının geliştirilmesi amaçlanmıştır. Çalışmanın ilk aşamasında 410 katılımcı grubuyla Açımlayıcı Faktör Analizi (AFA) yapılmış ve ölçeğin üç alt boyut altında ("çevrimiçi güvenlik farkındalığı: çgf", "çevrimiçi merak: çm" ve "siber tehdit farkındalığı: stf) 30 maddeden oluştuğu belirlenmiştir. AFA ardından elde edilen ölçme aracı 265 kişilik katılımcı grubuna uygulanmış ve gerçekleştirilen Doğrulayıcı Faktör Analizi (DFA) sonucu 3 faktörlü yapı doğrulanmıştır. Ölçeğin tamamı için Cronbach alfa güvenirlik katsayısı .90; her alt boyut için Cronbach Alfa katsayısı ise çgf: .94, çm: .90, ve stf: .86 olarak hesaplanmıştır. Bu çalışma sonucunda ortaokul kademesinde eğitim almakta olan öğrencilerin bilgi güvenliği farkındalık düzeylerini belirlemeye yönelik geçerli ve güvenilir bir ölçme aracı geliştirilmiştir. Ayrıca geliştirilen ölçek üzerinde ortaokul kademesinde öğrenim gören öğrencilerin bilgi güvenlik farkındalığı ortalama puanlarının, cinsiyetlerine göre istatiksel olarak anlamlı bir farklılık gösterdiği tespit edilmiştir.

Anahtar Kelimeler: Bilgi güvenliği, farkındalık, bilgi güvenliği farkındalığı, ölçek geliştirme, ortaokul kademesi

[a] lcetinkaya@comu.edu.tr https://orcid.org/0000-0002-0167-4846 [b] oktelikbulent@gmail.com https://orcid.org/0000-0002-3462-3973

How to Cite: Cetinkaya, L. & Oktelik, B. (2022). Ortaokul düzeyi öğrencilerine yönelik bilgi güvenliği farkındalık ölçeği geliştirme çalışması. *Cumhuriyet International Journal of Education, 11*(4):696-708

Giriş

Teknolojinin hızla dönüşüm gerçekleştirdiği ve geliştiği günümüz dünyasında bilgi dijitalleşerek depolanır, işlenir ve transfer edilebilir bir hâl almıştır. Bireyler hayatın normal akışı içinde, birçok alan ve konuda bu teknolojileri yoğun bir şekilde kullanmalarının sonucu olarak bilgi güvenliğinin sağlamasına yönelik hızla çeşitlenen sorunlarla karşı karşıya kalmaya başlamışlardır (Taha & Dahabiyeh, 2021). Genel olarak bireye, şirkete ya da kuruma ait olan bilgilerin başkalarının eline geçmesinin engellenmesi olarak tanımlanan bilgi güvenliği (Canbek & Sağıroğlu, 2006) bilgi teknolojilerinin bir alt kümesi olarak kabul edilmektedir (Haufe, Brandis, Colomo-Palacios, Stantchey & Dzombeta, 2016). Bilginin korunması, veri güvenliği, ağ güvenliği, bilgiyi kullanan, saklayan ve ileten sistemler gibi önemli unsurları bir arada barındıran bilgi güvenliği kavramı (Koohang, Anderson, Nord & Paliszkiewicz, 2020) günümüzde dijitalleşme sürecinin başarısını etkileyebilecek kadar kritik bir unsur olarak karşımıza çıkmaktadır.

Bilgi güvenliği genel olarak gizlilik, bütünlük ile birlikte ulaşılabilirliği sağlamak amacıyla bilgi ve bilgi sistemlerinin; yetkisiz erişim, kullanım, ifşa, kesinti, değişiklik ve yok olmasından korunması olarak tanımlanmaktadır (Paliszkiewicz, 2019). Gizlilik, bütünlük ve ulaşılabilirlik olmak üzere üç temel kavramdan meydana gelen bilgi güvenliği, bu unsurlardan birinin zarar görmesi veya ortadan kaybolması durumunda riske girer (Keser & Güldüren, 2015; Puhakainen, 2006). Bu riskler ise ciddi ve telafisi güç sonuçlara neden olabilir. Bu temel kavramlardan gizlilik, bilgiye yetkisiz kişiler tarafından erişilmemesi gerektiği fikrini ifade eder (Koohang vd., 2020; Topa & Karyda, 2019) ve oldukça kritik verilere ait bilgileri (finansal kayıtlar, teknik bilgiler, müşteri bilgileri, kişisel bilgiler, vb.) içeren kavramların bir bütünüdür. Diğer bir kritik unsur ise bütünlüktür ve bilginin bozulmamış ya da değiştirilmemiş olması gerekliliği ile ilgilidir (Leszczyna, 2018). Ulaşılabilirlik ise bilgiye talep üzerine her zaman ulaşılabilir olması gerektiğini ifade etmektedir (Whitman & Mattord, 2018).

Bilgi güvenliği tehditlerinden korunmak için bilgi güvenliği farkındalık eğitimlerini ve güvenlik stratejilerini kullanabilmek önemlidir (Puhakainen, 2006; Siponen, 2001). Bilgi güvenliği faktörü üzerinde önemli bir etkiye sahip bilgi güvenliği farkındalığının eksikliği durumunda güvenlik tehditlerinin risklerini ve güvenlik sorunlarını arttırdığı belirtilmektedir (bkz., Alkalbani, Deng & Kam, 2015; Chandarman & Van Niekerk, 2017; Hanus & Wu, 2016). Yapılan araştırmalar veri ihlallerinde kazara, doğrudan, kasıtlı veya kötü niyetli insan faktörü hatalarının önemli etkisinin olduğunu göstermektedir (Pricewaterhouse Coopers, 2015). Her ne kadar bilgi güvenliğinin sağlanmasında sadece insan faktörlü olası zararları tamamen bitirmek çok mümkün olmasa da iyi bir eğitim stratejisiyle hazırlanmış bir farkındalık eğitimi ile güvenlik risklerinin en aza indirgenmesi söz konusu olabilir (Acılar, 2009; Gülmüş, 2010; Keser & Güldüren, 2015).

Günümüz gelişme çağında olan çocuklar birbirleriyle iletişim kapasitesine sahip ve hızla ilerleyen çevrimiçi teknolojilerle çevrelenmiş durumdadırlar (Mustafaoğlu, Zirek, Yasacı & Özdinçler, 2018). Giderek artan çeşitli çevrimiçi teknolojilere bağlı kalmaya yönelik kalıcı psikolojik ihtiyaç, bireyleri çevrimiçi risklere daha fazla maruz bırakmaktadır (Mochiko, 2016). Diğer taraftan çevrimiçi teknolojilerin iletişim ve sosyalleşme anlamında büyük faydalar sunmasının yanında çocukları çeşitli risklerle karşı karşıya bırakabilmektedir (Çelen, Çelik & Seferoğlu, 2011). Bu riskler her yaş grubundan bireyleri tehdit etse de çocukların yeni teknolojileri benimsemekteki istekleri ve karşılaşabilecekleri riskler konusundaki bilgi eksiklikleri gibi faktörler sebebiyle çocukları daha kolay birer hedef haline getirmektedir (Atkinson, Furnell & Phippen, 2009; Güldüren, Çetinkaya & Keser, 2016; Pattinson, Butavicius, Parsons, McCormac & Calic, 2015). Diğer taraftan eğitim kurumlarındaki hızlı dijitalleşme süreci ile birlikte teknolojiyi kullanan yenilikçi öğrenme yöntemleri hayata geçirilmeye ve beraberinde eğitim materyalleri çevrimiçi ortamlara aktarılmaya başlanmıştır. Bu durum kişisel kullanımın yanı sıra eğitsel amaçlı da çevrimiçi ortamların kullanım sıklığını artırarak çocukların bilgi güvenliği tehditleriyle daha çok karşılaşma olasılıklarını arttıracaktır. Nitekim bilgi güvenliğini sağlamada, teknoloji temelli önlemler ya da yazılımsal önlemler (virüs yazılımları, güvenlik duvarları, vb.) bir dereceye kadar işe yarayabilir. Bu bağlamda bilgi güvenliği farkındalığı sağlamak için öncelikle eğitim programları oluşturulması ve çocuklara bilgi güvenliği kavramının, karşılaşabilecekleri risklerin uğratacağı hasarı en aza indirebileceği eğitim programları aracılığıyla aktarılması gerekmektedir (Brady, 2010; Güldüren, Çetinkaya & Keser, 2016; Whitman & Mattord, 2018).

Günümüz çocuklarının dijital teknolojilerin yoğun olarak kullanılmaya başlandığı bir dönemde doğdukları ve bu teknolojilerle iç içe yaşadıkları göz önünde bulundurularak bilgi güvenliğine yönelik farkındalıklarının erken dönemde geliştirilmesi önemlidir. Bu çerçevede bilgi güvenliği farkındalığının kazandırılmasına yönelik eğitim faaliyetlerinin ilköğretim düzeyinde başlatılması karşılaşabilecekleri olası risklerin en aza indirgenmesine olumlu katkı sağlayacaktır. Bilgi güvenliği farkındalıklarının kazandırılması bakımından eğitim faaliyetlerine doğrudan çocukların dahil olması gerekmektedir (Atkinson, Furnell & Phippen, 2009). Böylece bilgi güvenliği farkındalığı kazanan çocuklar kendi güvenliklerini sağlama konusunda çaba sarf edecekler ve olası risklerin en aza indirgenmesini sağlayabileceklerdir. Halihazırda hızla eğitim ortamlarına teknolojinin entegre olmaya başladığı günümüzde özellikle eğitim kurumlarında bilgi güvenliği farkındalığının oluşturulması artık bir zorunluluk haline gelmiştir. Diğer taraftan ise bilgi güvenliği farkındalığının arttırılmasına yönelik hazırlanan eğitim programlarında bireylerin bilgi düzeyleri ve beklentileri göz önünde bulundurulması gerekmektedir (Şahinaslan, Kandemir & Şahinaslan, 2009). Bu noktada farkındalığın belirlenmesi ve bu çerçevede bilgi güvenliği yeterliliklerin kazandırılması noktasında önlemlerin alınması önemlidir. Özellikle bilgi güvenliğinin sağlanmasında "zayıf halka" olarak

tanımlanan insan faktörünün göz ardı edilmemesi (Güldüren, 2015; Kritzinger & Smith, 2008; Veiga, 2008) ve bu noktada erken dönemde durum tespiti ile birlikte önleyici tedbirlerin alınması gerekmektedir.

Bilgi güvenliği bağlamında yapılan araştırmalar incelendiğinde bilginin korunumuna yönelik teknoloji temelli unsurların daha çok dikkate alındığı ve insan faktörünün ise göz ardı edilebildiği görülmektedir (Öztemiz & Yılmaz, 2013). Oysaki dijitalleşme sürecinde bilginin depolanmasından yönetimine kadar tüm süreçlerde insan vardır ve insana yönelik faktörler dikkatle ele alınmalıdır (Ki-aries & Faily, 2017). Özellikle internet temelli teknolojiler ile beraberindeki uygulamaların yaygınlaşmasının da etkisiyle son dönemlerde bilgi güvenliğinde insan faktörünü ön plana alan ve özellikle çocukların bilgi güvenliğine yönelik öz değerlendirme yapabilmelerinin önemine vurgu yapan çalışmalar hız kazanmaya başlamıştır. Yine bu çalışmalarda başta çevrimiçi ortamlar olmak üzere olası tehlikelerden korunabilmenin önemi ile birlikte bu konuda bilinçlendirme çalışmaları yapılması gerekliliği net bir şekilde vurgulanmaktadır (örn. Allers, Drevin, Snyman, Kruger & Drevin, 2021; Güldüren, Çetinkaya & Keser, 2016; Karaahmetoğlu, 2021; Theofanos, Choong & Murphy, 2021). Bu tespitlerden yola çıkarak teknoloji ile erken dönemde iç içe bir yaşam sürmeye başlayan çocukların bilgi güvenliği farkındalık düzeylerinin belirlenmesi, durumlarının analiz edilmesine ve ortaya çıkan eksikliklerin değerlendirilmesine yardımcı olabilecek bir ölçme aracının geliştirilmesine ihtiyaç duyulmuştur. Bu doğrultuda gerçekleştirilen çalışmada ilköğretim düzeyi ortaokul kademesinde (10-14 yaş) öğrenimlerine devam eden öğrencilerin bilgi güvenliği farkındalık düzeyini belirlemeye yönelik ölçme aracının geliştirilmesi ile birlikte ön-psikometrik (preliminary) özelliklerinin belirlenmesi amaçlanmıştır.

Yöntem

Araştırma Deseni

İlköğretim düzeyi ortaokul kademesinde eğitim gören öğrencilerin bilgi güvenliği farkındalık düzeyini belirlemeye yönelik bir ölçme aracının geliştirilmesi ile birlikte ön-psikometrik özelliklerinin belirlenmesi amaçlanan çalışma iki boyuttan oluşmaktadır. İlk aşamada bilgi güvenlik farkındalığını ölçmeye yönelik bir ölçek geliştirme süreci işe koşulmuştur. İkinci aşamada ise geliştirilen ölçeğin öğrencilerin psikometrik özellikleri göz önünde bulundurularak bilgi güvenliği farkındalıkları belirlenmiştir. Çalışmanın gurubu özellikleri ile birlikte araştırma sürecinin hangi aşamalardan gerçekleştiğine yönelik detaylı bilgi aşağıda sunulmuştur.

Çalışma Grubu

Araştırma 2021-2022 öğretim yılında ilköğretim düzeyi ortaokul kademesinde öğrenimlerine devam eden toplam 675 öğrenci ile gerçekleştirilmiştir. Ölçme aracı geliştirilmesi sürecinin Açımlayıcı Faktör Analizi (AFA) aşamasında 410 öğrencinin verisi değerlendirilmiş ve analizler sonucunda ölçme aracı yeniden düzenlenmiştir. Elde edilen yeni form ise çalışmanın Doğrulayıcı Faktör Analizi (DFA) için tekrar uygulanmış ve bu aşamada toplam 265 öğrenciden elde edilen verilerin analizi gerçekleştirilmiştir. Çalışma grubunda bulunan öğrencilerin cinsiyet ve sınıf düzeyleri dağılımları Çizelge 1'de sunulmuştur.

Araştırmanın AFA ve DFA süreçlerinde verileri analiz edilen 675 öğrencinin cinsiyetlerine göre dağılımı incelendiğinde 355'i (%52.60) kız, 320'si (%47.40) ise erkek öğrencilerden oluşmaktadır. Öğrencilerin 176'sı (%26.07) 5. sınıf, 158'i (%23.4) 6. sınıf, 168'i (%24.88) 7. sınıf ve 173'ü (%25.62) 8. sınıfta öğrenimlerine devam ettiği görülmüştür.

Veri Toplama Aracı

Araştırma sürecinin ilk aşamasında bilgi güvenliği farkındalığı kavramına ilişkin alanyazın incelenmiş ve bu kavrama ilişkin göstergeler göz önünde bulundurulmuştur. Elde edilen bulgular doğrultusunda bilgi güvenliği farkındalığına yönelik tüm gösterge ve kategorilerin göz önünde bulundurulduğu 124 maddelik bir madde havuzu oluşturulmuştur. Bu aşamada daha önce bilgi güvenliği farkındalığına yönelik kapsamlı çalışmalarının olduğu görülen Puhakainen (2006) ile Güldüren ve Keser 'in (2015) çalışmalarından da sıklıkla faydalanılmıştır. Farkındalık kavramı cümle yapısı ile oluşturulan maddelerin derecelendirilmesinde likert tipi beşli derecelendirme ("kesinlikle katılıyorum (5), katılıyorum (4), kısmen katılıyorum (3), katılmıyorum (2) ve kesinlikle katılmıyorum (1)") ölçek yapısı işe koşulmuştur. Bu doğrultuda oluşturulan bilgi güvenliği kavramı ile ilişkili tespit edilen kategoriler, kavramlar ve madde sayılarına ilişkin veriler Çizelge 2'de sunulmuştur.

Çalışmada kapsam geçerliliği için Lawshe (1975) tarafından geliştirilen teknikten faydalanılmış ve oluşturulan 124 maddelik ilk deneme formu aracılığı ile; Bilgisayar ve öğretim teknolojileri eğitimi alanından 4 ve ölçme değerlendirme alanından 1 olmak üzere alanlarında uzman 5 akademisyenin yanı sıra çalışmanın yapıldığı okullarda görevli olan 4 bilişim teknolojileri öğretmeni olmak üzere 9 uzman görüşü alınmıştır. Uzmanlar her bir maddeyi, bilgi güvenliğine yönelik farkındalığı ölçebilme, ilgili kategoriyle ilişkili olma, ifadenin uygunluğu ve anlaşılırlığı başlıkları altından değerlendirmişlerdir. Gerçekleştirilen ilk uygulama sonucunda elde edilen veriler doğrultusunda ortaya çıkan Kapsam Geçerlilik Oranı (KGO) değeri, Veneziano ve Hooper (1997) tarafından tabloya dönüştürülen kapsam geçerlik ölçütü (KGO9=.75) ile karşılaştırma yapılmıştır. İstatistiksel olarak α=.05 anlamlılık düzeyinde gerçekleştirilen analizler sonucunda belirtilen değerin altında değer alan 20 madde çalışma kapsamından çıkartılmış ve üzerinde düzeltmeler yapılan maddelerle birlikte çalışma sonucunda oluşan 104 maddelik formun kapsam geçerlik indeksi .90 olarak hesaplanmıştır.

Çizelge 1. Öğrencilerin cinsiyet ve sınıf düzeyi dağılımları

		AFA Aşaması		DFA Aşaması		Toplam	
		f	%	f	%	f	%
Cinsiyet	Kız	210	52.60	145	52.60	355	52.60
	Erkek	200	47.40	120	47.40	320	47.40
	Toplam	410	100	265	100	675	100
Sınıf Düzeyi	5. Sınıf	110	26.82	66	24.90	176	26.07
	6. Sınıf	86	20.97	72	27.16	158	23.40
	7. Sınıf	108	26.34	60	22.64	168	24.88
	8. Sınıf	106	25.85	67	25.28	173	25.62
	Toplam	410	100	265	100	675	100

Çizelge 2. Kategori, nitelik ve madde sayıları

Kategoriler	Nitelikler	Madde Sayısı
Bilgi Güvenliği	Bilgi, güvenlik, Bilgi güvenliği farkındalığı, Şifre güvenliği, Verilerin güvende tutulması	24
Siber Tehditler ve Siber Güvenlik	Virüs ve casus yazılımlar, Hizmet aksattırma saldırıları, Oltalama, Korsan yazılımlar, Sosyal mühendislik, Kimlik hırsızlığı	33
Çevrimiçi Teknolojiler	Cep telefonları, kullanım süresi, kişisel bilgiler, taşınabilir cihazlar, Kablosuz ağ güvenliği, Yazılımlar, taşınabilir cihazlar, anlık mesajlaşma, e-posta, web sitesi sertifikaları, işletim sistemleri	34
Mahremiyet	Telif hakkı ihlalleri, Tarayıcılara ait güvenlik işlemleri, Çevrimiçi güvenli alışveriş, kişisel bilgilerin korunması	18
Siber Zorbalık ve Siber Mağdur	Siber zorbalık, Bilişim suçları, Dolandırıcılık, Sosyal medya, Sosyal medya güvenliği	15
Toplam		**124**

Verilerin Toplanması ve Analizi

Veri toplama süreci toplam 6 ay süren çalışmanın AFA aşamasında 410, DFA aşamasında 265 olmak üzere oluşturulan formun basılı halini dolduran toplam 675 öğrenci verisinin istatistiksel analiz için uygun olduğu tespit edilmiştir. Çalışmanın örneklem büyüklüğünün belirlenmesinde madde ve faktör sayısı gibi bağıl ölçütler göz önünde bulundurulmuştur. Bu noktada genel olarak örneklem büyüklüğüne yönelik, ölçme aracını oluşturan toplam madde sayısının 5-10 katı olması (Kass & Tinsley, 1979; Kline, 1994) ve en az 300 örneklem sayısının faktör analizi için uygun olabileceği genel kuralı ortaya konulmaktadır (Çokluk, Şekercioğlu, & Büyüköztürk, 2010). Kline (1994) ise büyük örneklemler üzerinde çalışmanın daha uygun olacağını vurgulamakla birlikte mutlak ölçüt olarak 200 kişilik örneklemin yeterli olabileceğini belirtmiştir. Diğer taraftan genel olarak ölçek geliştirme süreçlerinde ideal olanın; AFA ve DFA'nın farklı örneklem gruplarından elde edilen verilerin üzerinde yapılması olduğu ifade edilmektedir (Çakmak, Kılıç, Çebi & Kan, 2014). Bu doğrultuda gerçekleştirilen çalışmanın örneklemini oluşturan ilk uygulama grubu üzerinde AFA (n1=410), ikinci uygulama grubu üzerinde ise DFA (n2=265) yapılmıştır.

Bulgular

Bu bölümde ilköğretim düzeyi ortaokul kademesi öğrencilerinden elde edilen veriler doğrultusunda; AFA, madde analizi, DFA'nın yanı sıra öğrencilerin bilgi güvenliği farkındalık düzeyleri ile psikometrik (cinsiyetlerine yönelik) özelliklerine yönelik bulgular başlıklar halinde sunulmuştur.

Açımlayıcı Faktör Analizine Yönelik Bulgular

Araştırmada elde edilen verilerin AFA için uygunluğunun saptanması amacıyla; Kaiser-Meyer-Olkin (KMO) ile birlikte Barlett Küresellik testi ölçümlerinden faydalanılmıştır. Çokluk ve diğerleri (2010) örneklem büyüklüğüne göre ortaya çıkan değerin .50'den düşük olması durumunda teste devam edilmemesi gerektiğini ancak .90'ın üzerinde bir değer alması durumunda ise "mükemmel" olarak nitelendirmiştir. Gerçekleştirilen araştırmada KMO katsayı değeri .903 olarak belirlenmiştir.

Elde edilen bu sonuç doğrultusunda faktör analizinin yapabilmesi için veri yapısının mükemmel düzeyde yeterli olduğu yönünde değerlendirme yapılabilir. Ayrıca yapılan analizler Barlett Küresellik testinin .01 düzeyinde anlamlı olduğunu göstermiştir [$\chi 2$= 34349.808; df=5356; p=.000]. Elde edilen bu bulgular çalışmanın örnekleminin yeterli seviyede olduğu, verilerin çok değişkenli normal

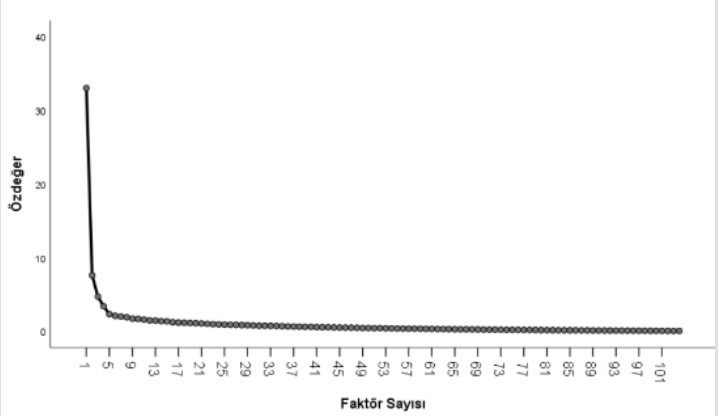
dağılımdan geldiği ve dolayısıyla da faktör analizi için bir diğer varsayımın karşılandığı anlamına gelmektedir.

Ölçme aracının faktör yapısının belirlenmesi amacıyla öncelikle döndürülmemiş temel bileşenler analizi yapılmıştır (Tabachnick & Gidell, 1996). Faktör sayısının belirlenmesi sürecinde Kaiser-Guttman ilkesi gereği özdeğerleri 1 ve üzeri faktörlerin incelenmesi yoluna gidilerek, faktör özdeğerlerine ait çizgi grafiği ile birlikte açıkladıkları varyans oranlarına bakılmıştır (Zwick & Velicer, 1986). Ölçme aracı özdeğerleri 1 ve üzeri 22 faktör yapısına sahip olduğu ve faktörlerin özdeğeri ile açıklanan toplam varyansa katkı düzeyleri resim 1'de görüldüğü üzere sırasıyla; 1.faktör: 33.03 (%31.76), 2.faktör: 7.59 (%7.29), 3.faktör 4.69 (%4.51), 4.faktör: 3.37 (%3.25), 5.faktör: 2.31 (%2.22), 6.faktör: 2.08 (%2.00), 7.faktör: 1.98 (%1.90), 8.faktör: 1.89; (%1.81), 9.faktör: 1.70 (%1.63), 10.faktör: 1.67 (%1.61), 11.faktör 1.57 (%1.50), 12.faktör: 1.46 (%1.41), 13.faktör: 1.44 (%1.38), 14.faktör: 1.35 (%1.30), 15.faktör: 1.33 (%1.28), 16.faktör: 1.21 (%1.16), 17.faktör: 1.16 (%1.12), 18.faktör: 1.14 (%1.09), 19.faktör: 1.11 (%1.07), 20.faktör: 1.08 (%1.04), 21.faktör: 1.04 (%1.00), 22.faktör: 1.00 (%.96) şeklindedir.

Ölçek faktör yapılarının karar sürecinde ortaya konulan çözümlemenin kuramsal olarak temellendirilmesi gerekmektedir (Zwick & Velicer, 1986). Genel olarak tek faktörlü ölçek yapılarında açıklanan varyans oranının %30 ve üzeri olması yeterli görülürken çok faktörlü yapılarda bu oranının daha fazla olması beklenmektedir (Tabachnick & Fidell 1996). Açıklanan toplam varyansı yükseltmek için ise faktör sayısını arttırmak ya da faktör yük değeri yüksek olan maddelerin seçilmesi olmak üzere iki yol izlenebilir (Büyüköztürk, 2002). Madde faktör yük değerinin düşük olarak ortaya çıkması o maddenin faktörle yeterli seviyede bir bağlantısının olmadığını göstermektedir. Faktör yük değerlerinin faktör sayısının belirlenmesinde belirleyici rol oynaması için bütüncül ve yüksek bir yapıya sahip olması beklenmektedir (Büyüköztürk, 2002). Faktörde bulunan maddelerin .60 ve üzeri yük değerleri yüksek seviye, .30 ile .59 arası yük değerleri ise orta seviye büyüklük olarak tanımlanmaktadır (Büyüköztürk, 2002; Watkins, 2021). Bu doğrultudan yola çıkarak ölçek maddelerinin faktörlerle olan ilişkisinin yüksek düzeyde olması, bu maddelerin bir kavramı daha iyi ölçtüğü anlamına geldiği göz önünde bulundurularak çalışmanın özdeğeri 2 ve faktör yük değeri .65 olarak belirlenerek analize devam edilmiştir. AFA' ya göre ölçek özdeğeri 2'den büyük olan 6 faktörde toplandığı ve bu faktörlerin açıkladığı varyans değeri ise %51.06 olarak ortaya çıkmıştır. Çokluk ve diğerleri (2010) maddenin yük değerinin .40'tan büyük olması ve madde çıkarılması işlemine binişik maddelerden başlanılması gerektiğini savunmaktadır. Bu çalışmada faktör yük değeri düşük olan maddelerle birlikte binişik maddeler de ölçekten çıkartılmıştır. Bu aşamada açımlayıcı faktör analizi 28 kez tekrarlanmış ve ortaya çıkan maddelerin faktör yük değerleriyle birlikte ortak faktör varyans değerleri Çizelge 3'te sunulmuştur.

Çizelge 3'te yer alan veriler incelendiğinde 15 maddenin yer aldığı birinci faktöre ilişkin yük değerlerinin .65 ile .77 arasında değişim gösterdiği ve maddelere ait ortak faktör varyans değerlerinin .54 ile .80 arasında değişim gösterdiği görülmüştür. Birinci faktör açıklayabildiği toplam varyans %33.04 değerinde olup alanyazın da göz önünde bulundurularak "çevrimiçi güvenlik farkındalığı" olarak isimlendirilmiştir. İkinci faktör 9 maddeden oluşmakta olup maddelere ait faktör yük değerleri .65 ile .84, maddelere ait ortak faktör varyans değerleri ise .55 ile .86 arasında değişim göstermiştir. İkinci faktörün açıklayabildiği toplam varyans %15.63 değerinde olup alanyazın da göz önünde bulundurularak "çevrimiçi merak" olarak isimlendirilmiştir. Üçüncü faktör ise 6 maddeden oluşmakta olup maddelerin faktör yük değerleri .71 ile .75 aralığında, maddelere ait ortak faktör varyans değerleri ise .69 ile .86 aralığında değişim göstermektedir. Üçüncü faktörün ise açıklayabildiği toplam varyans %7.63 değerinde olup alanyazın da göz önünde bulundurularak "siber tehdit farkındalığı" olarak isimlendirilmiştir. 30 maddeden oluşan ölçeğin toplam varyansına en düşük desteği .68 faktör yük değeri ve .54 ortak faktör varyansı ile 54. maddenin, en yüksek desteği ise .73 faktör yük değeri ve .86 ortak faktör varyansı ile 93. maddenin verdiği gözlemlenmiştir.

Nihai olarak ortaya çıkan 3 faktörlü yapının toplam varyansın %56.30'unu açıkladığı belirlenmiştir. Tavşancıl'a (2005) göre sosyal bilimlerde ölçekte bulunan maddelerin açıklanan varyans oranının %40 ile %60 arasında bir oranda olmasını beklenmektedir. Bu ölçüt doğrultusunda elde edilen 3 faktörlü yapının, ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeyini belirlemek için yeterli olduğu söylenebilir. Diğer taraftan ölçeği oluşturan 30 maddenin tamamının faktör yük değeri .65'in üzerinde kaldığı görülmektedir. Alanyazında .60 ve üstü yük değeri, yüksek büyüklük olarak tanımlanmakta ve ölçme aracında kesinlikle yer alması beklenen maddeler olarak nitelendirilmektedir (Büyüköztürk, 2006; Kline, 2000; Watkins, 2021). Bu ölçütler doğrultusunda ölçeğin, 3 faktörlü yapı altında toplanan 30 maddenin tamamının yer alması uygun görülmüştür.



Resim 1. Ölçeğin faktör özdeğerlerine ilişkin çizgi grafiği

Çizelge 3. Ölçeğin faktör analizi sonuçları

AB	Madde	F1	OFV	AB	Madde	F2	OFV	AB	Madde	F3	OFV
Çevrimiçi Güvenlik Farkındalığı	S51	.65	.61	Çevrimiçi Merak	S44	.65	.86	Siber Tehdit Farkındalığı	S89	.75	.85
	S53	.73	.69		S46	.65	.85		S90	.72	.83
	S54	.68	.54		S78	.67	.55		S92	.71	.76
	S55	.72	.65		S85	.76	.78		S93	.73	.86
	S56	.77	.63		S86	.84	.77		S97	.71	.69
	S57	.75	.57		S91	.74	.72		S99	.74	.83
	S58	.71	.72		S101	.73	.65				
	S59	.75	.64		S103	.77	.85				
	S60	.71	.63		S104	.70	.84				
	S64	.74	.66								
	S65	.69	.71								
	S67	.68	.75								
	S69	.67	.61								
	S70	.66	.80								
	S73	.67	.64								
Özdeğer: 9.91				Özdeğer: 9.91				Özdeğer: 9.91			
Açıklanan Varyans: 33.04				Açıklanan Varyans: 33.04				Açıklanan Varyans: 33.04			
								Açıklanan Toplam Varyans:56.30			

AB: Alt Boyut, OFV: Ortak Faktör Varyansı

Çizelge 4. Madde analizi sonuçları

F1	Madde	DM-TK	Ü/A %27	F2	Madde	DM-TK	Ü/A%27	F3	Madde	DM-TK	Ü/A %27
Çevrimiçi Güvenlik Farkındalığı	S51	.651	10.51	Çevrimiçi Merak	S44	.567	3.334	Siber Tehdit Farkındalığı	S89	.669	9.819
	S53	.658	9.717		S46	.580	2.549		S90	.641	10.03
	S54	.677	12.86		S78	.597	3892		S92	.665	9.332
	S55	.683	12.09		S85	.670	7.078		S93	.681	10.05
	S56	.736	13.42		S86	.775	9.994		S97	.713	12.35
	S57	.676	11.47		S91	.646	7.912		S99	.660	8.737
	S58	.728	17.15		S101	.638	7.893				
	S59	.728	12.27		S103	.691	9.570				
	S60	.705	14.81		S104	.599	10.02				
	S64	.713	13.43								
	S65	.660	12.47								
	S67	.668	11.94								
	S69	.684	14.04								
	S70	.689	14.00								
	S73	.672	13.29								

DM-TK: Düzeltilmiş Madde-Toplam Korelasyonu, Ü/A %27: Üst ve Alt %27 Farkın Anlamlılık Testi (Bağımsız t-testi)

Madde Analizleri

Geliştirilen ölçekte bulunan maddelerin, ölçülmek istenen özelliği ölçüp ölçmediği ve ayırt ediciliğini belirlemek amacıyla öncelikle madde-toplam korelasyonları ardından ise üst ve alt %27'lik gruplara ait madde puanları arasında anlamlı bir farkın olup olmadığı t-testi ile analiz edilmiştir. Ölçeğin iç tutarlılığının belirlenmesi amacıyla ise Cronbach Alfa iç tutarlılık katsayısına bakılmıştır. Bu doğrultuda ölçekte yer alan her bir maddenin madde-toplam korelasyonları ile toplam puanlara göre belirlenen üst ve alt %27'lik gruplara ait madde puanları arasındaki farkın anlamlılığının irdelendiği bağımsız t-testi analiz sonuçları Çizelge 4'te sunulmuştur.

Faktör analizi sonucunda belirlenen ve üç faktör altında toplanan 30 maddenin madde analizleri yapılmıştır. Analiz sonucunda madde-toplam test korelasyonları değerlerinin; çevrimiçi güvenlik farkındalığı faktöründe r=.65 ile r=.74 arasında, çevrimiçi merak faktörünün r=.57 ile r=.77 arası, siber tehdit farkındalığı faktöründe ise r=.64 ile r=.71 arası değişim gösterdiği belirlenmiştir. Madde-toplam korelasyonlarının .30 ve üstü değer alması ölçek maddelerinin geçerliğine yönelik bir kanıt olarak görülmektedir (Nunnally & Bernestein, 1994). Ölçekte yer alan 30 maddenin madde-toplam test korelasyonlarına bakıldığında her bir madde için r=.30'un üzerinde değer aldığı tespit edilmiştir. Elde edilen bu bulgu, ölçekte bulunan maddelerin ölçülmek istenen niteliği ölçme amacına yardımcı olduğunun göstergesidir. Ölçeğin t-testi sonuçları incelendiğinde ise %27 üst ve alt grupların madde puanları arasındaki farklara ilişkin t değerlerinin 2.54 ile 17.15 arasında değişim gösterdiği ve tüm maddelerin anlamlı olduğu görülmektedir (p<.001). Ayrıca üst %27 grubun bütün maddelere ait madde puan ortalamaları alt %27 gruba göre anlamlı bir şekilde yüksektir. Buna göre ölçekte bulunan her bir maddenin aynı davranışı ölçtüğü ve ölçeğin tümümde olduğu gibi alt faktörlerin de ayırt ediciliğinin yüksek olduğu söylenebilir. Madde-toplam korelasyonları ile üst ve alt %27'lik gruplara ait madde ortalama puanları t-testi sonuçlarına göre ayırt ediciliği en yüksek maddenin 58. ve en düşük maddenin ise 46. madde olduğu tespit edilmiştir.

Ölçme aracının güvenirliğinin ortaya koyulması amacıyla Cronbach Alfa iç tutarlılık katsayı değerine bakılmıştır. Genel olarak güvenilirlik katsayısının .70 ve üzeri değer alması yeterli olarak değerlendirilmektedir (Nunnally, 1978). Ölçeği oluşturan 30 maddenin Cronbach Alfa iç tutarlılık katsayısı .90 olarak belirlenmiştir. Ölçeğin alt faktörlerinin belirlenmesi amacıyla gerçekleştirilen Cronbach Alfa iç tutarlılık analiz değerleri ise; çevrimiçi güvenirlik farkındalığı faktörü için .94, çevrimiçi merak faktörü için .90 ve siber tehdit farkındalığı faktörü için .86 olarak ortaya çıkmıştır. Buna göre faktörlerin Cronbach Alfa iç tutarlılık katsayısı .70'ten yüksek olduğu tespitinde yola çıkarak ölçeğin güvenilir ve tutarlı bir ölçek olduğu sonucuna ulaşılmıştır (Nunnally, 1978; Tavşancıl, 2005).

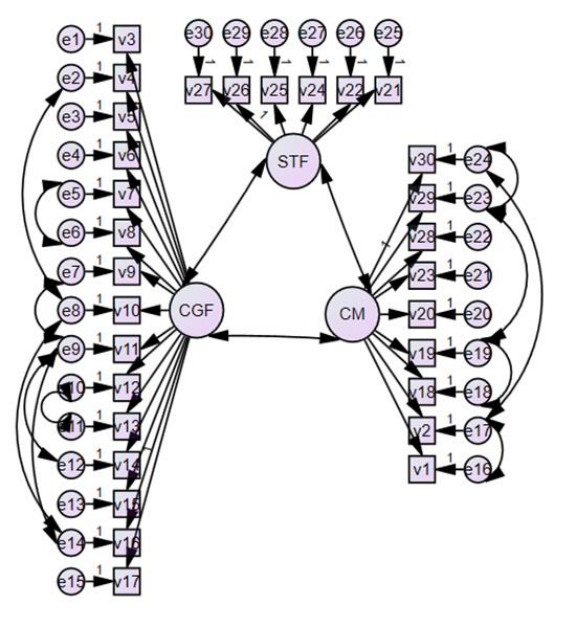
Doğrulayıcı Faktör Analizine Yönelik Bulgular

Çalışmanın AFA aşaması sonrası ortaya çıkan modele ilişkin yapı geçerliğinin değerlendirilmesi amacıyla DFA yapılmış (Kline, 2000) ve 30 maddeden oluşan üç faktörlü yapıya ilişkin DFA aşaması 265 öğrenci ile gerçekleştirilmiştir. Çalışmada model uyum indekslerinden; Ki-Kare İyilik Uyumu (χ2/df), İyilik Uyum İndeksi (GFI), Düzenlenmiş İyilik Uyum İndeksi (AGFI), Yaklaşık Hataların Ortalama Karekökü (RMSEA), Standardize Edilmiş Artık Ortalamaların Karekökü (SRMR), Karşılaştırmalı Uyum İndeksi (CFI), Normlaştırılmış Uyum İndeksi (NFI) ve Normlaştırılmamış Uyum İndeksi (NNFI) göz önünde bulundurulmuştur.

Ölçeği oluşturan 3 faktörlü yapıya ilişkin DFA sonrası model üzerinde önerilen modifikasyonlar yapılmadan önce ortaya çıkan uyum iyiliği indeksleri şöyledir: [χ2/df= 2.152 (p=.000); GFI= .83; AGFI= .80; RMSEA= .066; SRMR= .000; CFI= .89; NFI= .82; NNFI= .89]. Analiz sonucu ortaya çıkan modifikasyon önerileri dikkate alındığında M6 ve M5; M17 ve M16; M19 ve M18; M23 ve M19; M24 ve M17; M24 ve M23; M8 ve M2; M9 ve M7; M11 ve M10; M12 ve M9; M14 ve M8; M14 ve M9 maddeleri arasında 12 modifikasyon önerisinin ortaya çıktığı görülmektedir. Alanyazın incelendiğinde; maddeler arasında gizil bir bağlantının olabileceği ve maddelerin benzer durumları, ölçtükleri göz önünde bulundurularak modifikasyona yönelik öneri dikkate alınmıştır. Modifikasyon ardından ortaya çıkan uyum indeksleri Çizelge 5'te sunulmuştur (Schermelleh-Engel, Moosbrugger & Müller, 2003; Jöreskog & Sörbom, 1993).

Çizelge 5. Standart uyum iyiliği ölçütleri ile araştırma sonuçlarının karşılaştırılması

Uyum Ölçüleri	İyi Uyum	Kabul Edilebilir Uyum	Uyum değerleri
χ2/df	0 ≤ χ2/df ≤ 2df	2df ≤ χ2 /df≤ 3df	1.52
RMSEA	0 ≤ RMSEA ≤ 0.05	0.05 <RMSEA ≤ 0.10	.044
SRMR	0 ≤ SRMR ≤ 0.05	0.05<SRMR≤0.10	.00
NFI	0.95<NFI≤1.00	0.90 ≤ NFI <0.95	.88
NNFI	0.95 ≤ NNFI ≤ 1.00	0.90 ≤ NNFI ≤ 0.95	.95
CFI	0.95 ≤ CFI ≤ 1.00	0.90 ≤ CFI ≤ 0.95	.95
GFI	0.95 ≤ GFI ≤ 1.00	0.90 ≤ GFI <0.95	.88
AGFI	090 ≤ AGFI ≤ 1.00	0.85 ≤ AGFI <0.90	.85



Resim 2. Ölçeğin birinci düzey doğrulayıcı faktör analizi bağlantı diyagramı

Çizelge 6. Maddelere ilişkin çoklu korelasyon katsayısı (t ve R2) değerleri

F1	Madde	t	R^2	F2	Madde	t	R^2	F3	Madde	t	R^2
Çevrimiçi Güvenlik Farkındalığı	S3	8.53	.33	Çevrimiçi Merak	S1	12.25	.64	Siber Tehdit Farkındalığı	S21	8.55	.39
	S4	7.68	.26		S2	11.58	.60		S22	7.34	.27
	S5	9.89	.45		S18	10.65	.48		S24	9.66	.53
	S6	10.09	.47		S19	10.31	.45		S25	9.11	.45
	S7	10.83	.55		S20	13.40	.77		S26	11.28	.51
	S8	10.27	.49		S23	11.96	.60		S27	9.74	.44
	S9	10.79	.55		S28	12.06	.62				
	S10	8.49	.32		S29	15.93	.78				
	S11	10.17	.48		S30	12.66	.50				
	S12	9.66	.43								
	S13	10.40	.51								
	S14	9.98	.46								
	S15	9.37	.40								
	S16	10.88	.45								
	S17	9.88	.46								

Çizelge 7. Cinsiyet ile bilgi güvenliği farkındalığı arasındaki farklılık

	Cinsiyet	N	$\bar{X}$	Ss	df	t	p*
Çevrimiçi Güvenlik Farkındalığı	Kız	355	61.35	10.10	568.93	7.84	**.000**
	Erkek	320	53.84	14.22			
Çevrimiçi Merak	Kız	355	31.50	10.58	672.57	1.89	**.098**
	Erkek	320	30.02	9.78			
Siber Tehdit Farkındalığı	Kız	355	25.07	4.86	609.38	5.35	**.000**
	Erkek	320	22.78	6.10			
Ölçeğin tamamı	Kız	355	117.94	16.75	619	7.82	**.002**
	Erkek	320	106.65	20.33			

*p<.05 düzeyinde anlamlıdır.

Çizelge 5'te görülen DFA sonuçlarına göre, ki-kare $\chi 2$ = 586; (df=386, p<.01); ($\chi 2$/df) = 1.52 olarak bulunmuştur. Küçük örneklemler için 2.5 ve altı değer alan modelleri mükemmel uyumlu olarak nitelendirmektedir (Çokluk vd., 2010; Kline, 2005). Diğer taraftan yapılan analizler sonucunda RMSEA=.044; SRMR=.00; GFI=.88; AGFI=.85; NFI=.88; CFI=.95 ve NNFI=.95 olarak bulunmuştur. Araştırmada elde edilen uyum indeks değerleri göz önüne alındığında $\chi 2$ /df, RMSEA, SRMR, NNFI ve CFI iyi uyumu, AGFI uyum indeksi kabul edilebilir uyumu ancak GFI, NFI, uyum indeksleri ise yakın olmakla birlikte zayıf uyum gösterdiği görülmektedir. Şimşek (2007), uyum indekslerinin aldıkları değerlerin örneklem büyüklüğünden etkilenebildiklerini belirtmiştir. Bütüncül bir değerlendirme yapıldığında uyum indeks değerlerinin iyi uyumu gösterdiği görülmektedir. Buna göre ortaya konan modelin doğrulandığı görülmektedir. Ölçeğin faktöriyel modeli resim 2'de gösterilmiştir. Ölçek maddelerine ait elde edilen çoklu korelasyon katsayı (t ve R2) değerleri Çizelge 6'da sunulmuştur. Üç faktörlü yapıya ait t değerleri göz önünde bulundurulduğunda gözlenen değişkenlerin, gizil değişken tarafından .01 anlamlılık düzeyinde olduğu öngörülmektedir.

Alanyazın incelendiğinde önemli olan bir şart ise gözlenen değişkenin adına açıklanan varyansı ifade eden ve gözlenen değişkenin gizil değişkendeki farkı ne seviyede açıklayabildiği R2 değeri ile ortaya koyulmaktadır (Şimşek, 2007). Yapıya ait değerler sonucunda bilgi güvenliği farkındalığı düzeyine en yüksek katkıyı sırasıyla 29, 20, 1, 28 ve 23. maddelerin, en düşük katkıyı ise sırasıyla 22, 10, 4, 3, ve 21. maddelerin verildiği gözlemlenmektedir. Ortaya çıkan bu bulgu, açımlayıcı faktör analizinde ortaya çıkan bulguları desteklemektedir.

Öğrencilerin Cinsiyetleri ile Bilgi Güvenliği Farkındalık Düzeylerine İlişkin Bulgular

Ölçek geliştirme çalışması sonucunda ortaya çıkan üç faktörlü yapıdan elde edilen puanlar ile cinsiyet faktörü arasında istatiksel olarak anlamlı bir farkın olup olmadığı t-testi kullanılarak hesaplanmıştır.

Çizelge 7'de görüldüğü üzere ortaokul kademesinde öğrenim gören öğrencilerin bilgi güvenliği farkındalığı ölçeğinden aldıkları ortalama puanların, cinsiyet faktörüne göre istatiksel olarak anlamlı bir farklılık gösterdiği belirlenmiştir ($t_{(619)}$ =7.82, p<.05). Elde edilen bu bulguya göre, kız öğrencilerin ($\bar{X}$ =117.94) farkındalığa ilişkin ortalama puanlarının, erkek öğrencilere ($\bar{X}$ = 106.65) göre daha yüksek olduğu belirlenmiştir. Bunun yanı sıra ölçeği oluşturan; çevrimiçi güvenlik farkındalığı [t (568.93) =7.84, p<.05] ve siber tehditlerin farkındalığı [$t_{(609.38)}$ = 5.35, p<.05] faktörlerin ortalama puanları incelendiğinde cinsiyete göre kız öğrenciler lehine istatiksel olarak anlamlı bir farklılık olduğu ancak çevrimiçi merak [$t_{(672.57)}$ = 1.89, p<.05] faktöründe anlamlı bir fark olmadığı belirlenmiştir. Ayrıca faktörlerin ortalama puanlarına bakıldığında ölçeğin tamamında olduğu gibi alt faktörlerinde de kız öğrencilerin bilgi güvenliği farkındalık düzeylerinin erkek öğrencilere oranla daha yüksek olduğu tespit edilmiştir.

Tartışma, Sonuç ve Öneriler

Bilgi güvenliği ve farkındalığına yönelik yapılan araştırmalar incelendiğinde bilgi güvenliği sistemlerinde en zayıf halkanın insan unsurunun olduğu ve bu kapsamda mevcut durumun belirlenmesinin yanı sıra bilgi güvenliği konusunda bilinçlendirme çalışmalarının yapılması gerekliliği ön plana çıkmaktadır. Yine bu çalışmalarda bireylerin öğrenim gördükleri okullarda ve toplum genelinde bilgi güvenlik farkındalıklarını geliştirmeye yönelik bilinçlendirme çalışmalarının yapılması gerekliliğini göstermektedir (örn., Güldüren 2015; Güldüren, Çetinkaya & Keser, 2016; Yılmaz, Şahin & Akbulut, 2016). Konuyla ilgili Talan ve Aktürk'ün (2021) yaptıkları çalışmada ortaöğretim öğrencilerinin çevrimiçi teknolojileri kullanımı konusunda yeterli bilgiye sahip olduklarını ancak bilgi güvenliği konusunda eksik olduklarını gözlemlemiştir. Akgün ve Topal (2015) tarafından yapılan çalışmada ise bilgisayar deneyimi arttıkça bilgi güvenliğine yönelik farkındalığın arttığı fakat buna paralel olarak etik dışı kullanıma yönelik davranışların da arttığını tespit edilmiştir. Alanyazında ortaokul kademesinde öğrenim gören öğrenciler üzerinde bilgi güvenliği farkındalıklarını belirlemeye yönelik çalışmalar yer alsa da bu çalışmalarda farklı yaş grupları için hazırlanmış olan ölçeklerin kullanıldığı görülmektedir (örn. Serter, 2021; Talan & Aktürk, 2021). Yine yapılan alanyazın taraması sonucunda ilköğretim düzeyi ortaokul kademesinde öğrenim gören öğrencilerin (10-14 yaş) bilgi güvenlik farkındalık düzeylerini belirlemeye yönelik ihtiyacı karşılayabilecek bir ölçek geliştirme çalışmasına rastlanmamıştır. Bu tespitlerde hareketle gerçekleştirilen bu araştırmada alanyazın incelenerek ortaya konulan bilgi güvenliği kavramları göz önünde bulundurularak ortaokul kademesinde öğrenimlerine devam eden öğrencilerin bilgi güvenliği farkındalık düzeylerinin belirlenmesi amacıyla bir ölçme aracı geliştirilmiştir.

Yapı geçerliliği hesaplamalarının ardından toplam 30 madde ve 3 faktör altında toplanan ölçeğin açıklayabildiği toplam varyans %56.30'dir. Ortaya çıkan oran Büyüköztürk'e (2002) göre çok faktörlü ölçek yapısı bakımından yeterli düzeyde olduğu kabul edilmektedir. Üç faktörlü yapıdan oluşan ölçeğin birinci faktörü "çevrimiçi güvenlik farkındalığı" olarak isimlendirilmiş ve bu faktörün toplam varyansın %33.04'ünü açıkladığı belirlenmiştir. Ölçeğin ikinci faktörü "çevrimiçi merak" olarak isimlendirilmiş ve bu faktöründe toplam varyansın %15.63'ünü açıkladığı görülmüştür. Son olarak üçüncü faktör ise "siber tehdit farkındalığı" olarak isimlendirilmiş ve toplam varyansın %7.63'ünü açıklayabildiği ortaya çıkmıştır. Madde analizlerinin ardından madde toplam puanları arasında güçlü bir korelasyonel bağlantı olduğu görülmektedir. Oluşturulan ölçeğin tümüne ait Cronbach Alfa iç tutarlılık katsayısı .90, alt faktörlerin iç tutarlılık katsayıları ise sırasıyla; .94, .90 ve .86 olarak ortaya çıkmıştır. Sonuçlar incelendiğinde Cronbach Alfa iç tutarlılık değerlerinin .70'ten yüksek olduğu ve madde toplam puanları arasında güçlü bir bağlantı olduğu belirlenmiştir. Elde edilen bu bulgular doğrultusunda,

geliştirilen ölçeğin güvenilir ve tutarlı bir ölçme aracı olduğu söylenebilir.

DFA sonucunda ortaya çıkan uyum iyiliği indeksleri AFA sonucu ortaya çıkan üç faktörlü yapının doğrulandığını göstermektedir. Özelikle χ2 /df, RMSEA, SRMR, NNFI ve CFI indeks uyum iyiliği değerleri ele alındığında ortaya çıkan yapının mükemmel uyuma sahip olduğunu göstermektedir. AGFI uyum indeksi değeri kabul edilebilir uyuma sahip olduğunu, GFI, NFI, kabul edilebilir değerlere yakın olduğu görülmekle birlikte kabul edilebilirlik sınırlarının altında değer göstermektedir. Kabul edilebilirlik değeri altında kalan indekslerin ise araştırma grubunun sınırlılığından etkilenmiş olabileceği düşünülmektedir.

Yapılan analizler sonucunda, ortaokul kademesinde öğrenim gören öğrencilerin bilgi güvenlik farkındalığı ortalama puanlarının cinsiyetlerine göre istatiksel olarak anlamlı bir farklılık gösterdiği belirlenmiştir. Ölçeğe ait alt faktörlerden elde edilen ortalama puanlar incelendiğinde de yine ölçeğin tamamında olduğu gibi kız öğrencilerin bilgi güvenliği farkındalıklarına yönelik ortalama puanların erkek öğrencilere göre daha yüksek olduğu tespit edilmiştir. Çalışmada çıkan sonuçları destekler nitelikte Serter (2021) tarafından yapılan çalışmada da ortaokul kademesinde öğrenim gören kız öğrencilerinin erkek öğrencilere göre kişisel verilerin korunması, mahremiyet, saldırı ve tehditler boyutlarında farkındalığın daha yüksek olduğu belirlenmiştir. Beder ve Ergün'ün (2015) yaptıkları çalışma sonucunda da kız öğrencilerin farkındalık düzeylerinin erkek öğrencilere oranla daha yüksek olduğu tespit edilmiştir. Yine Derin ve Gençoğlu'nun (2020) 400 ortaokul öğrencisi üzerinde gerçekleştirmiş oldukları anket çalışması sonucunda kız öğrencilerin erkeklere göre internet ortamında karşılaşabilecekleri tehlikeli durumlardan daha çok haberdar oldukları belirlenmiştir. Bunun dışında alanyazında farklı yaş grupları üzerinde bilgi güvenliği farkındalığına yönelik yapılan çalışmalarda farklı sonuçların gözlendiği de görülmektedir. Örneğin; Güldüren, Çetinkaya ve Keser'in (2016) ortaöğretim kademesinde öğrenim gören öğrenciler üzerinde yaptıkları çalışmada erkek öğrencilerin kız öğrencilere göre bilgi güvenlik farkındalık düzeylerinin daha yüksek olduğu belirlenmiştir. Yine Yılmaz, Şahin ve Akbulut (2016) tarafından öğretmenler üzerinde gerçekleştirilen çalışmada erkek öğretmenlerin dijital veri güvenliği farkındalıklarının kadın öğretmenlere göre daha yüksek olduğu görülmüştür. Bu noktada bilgi güvenliğine yönelik farkındalığın yaş gruplarına göre farklılık gösterdiği ve mevcut durumun belirlenmesinde bu durumun göz önünde bulundurularak ölçme aracının kullanılması gerektiği söylenebilir.

İlköğretim düzeyi ortaokul kademesinde (10-14 yaş) öğrenim gören öğrencilerin bilgi güvenliği farkındalık düzeyinin ele alındığından bu çalışma ve sonucunda elde edilen ölçeğin bu konudaki boşluğu dolduracağı düşünülmektedir. Elde edilen veriler geliştirilen ölçeğin ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeylerinin belirlenmesinde tutarlı, geçerli ve güvenilir ölçümler yaptığı göstermektedir. Bu çerçevede, ortaokul kademesinde öğrenimlerine devam eden öğrencilerin bilgi güvenliğine yönelik farkındalık düzeyleri belirlenerek gereksinim duyulması halinde rehberlik hizmetleri kapsamında eğitimler düzenlenebilir, materyaller geliştirilebilir ve farkındalık oluşturmaya yönelik rehberlik hizmetleri sunulabilir. Öğrencilerin bilgi güvenliği farkındalıklarının arttırılmasına yönelik ilköğretim düzeyinde bilişim teknolojileri ve yazılım dersi müfredatta daha fazla yer almalı, bilgi güvenliği konusunda sosyal kulüpler kurulmalı ve bilgi güvenliği farkındalığı konusunda panolara içerikler dahil edilmelidir. Ayrıca geliştirilen ölçek ile ortaokul kademesinde öğrenim gören öğrencilerin bilgi güvenliği farkındalık düzeyleri ile birlikte internet temelli teknoloji ve uygulamaları kullanım davranışlarına yönelik çeşitli hipotezler sınanabilir.

Summary

Introduction

In today's world where technology transforms and develops rapidly, information has been stored, processed and transferred digitally. As a result of the intensive usage of these technologies in many fields and subjects in the normal flow of life, individuals have begun to face rapidly diversifying problems in providing information security (Taha & Dahabiyeh, 2021). Information security, which is generally described as preventing the information belonging to the individual, company or corporation from being surpassed into the palms of others (Canbek & Sağıroğlu, 2006), is accepted as a subset of information technologies (Haufe et al., 2016). The concept of information security, which encompasses important elements such as information protection, data security, network security, and systems that use, store and transmit information (Koohang et al., 2020), is a critical element that can affect the success of today's digitization process.

Research shows that accidental, direct, intentional or malicious human factor errors have a significant impact on data breaches (Pricewaterhouse Coopers, 2015). Particularly with the effect of the widespread use of internet-based technologies and accompanying applications, studies that prioritize the human factor in information security have recently started to gain momentum. Again, in these studies, while emphasizing the importance of children's ability to self-assess information security and to protect them from possible dangers, notably in online environments, the need for awareness-raising activities has become evident. Based on these findings, it has become necessary to determine the information security awareness levels of children who have started to live a life intertwined with technology, analyze their situation and develop a measurement tool that can help assess the resulting deficiencies. This study both aims to develop a measurement tool that will determine the level of information security awareness of secondary level (10-14 years) students and identify their pre-psychometric (preliminary) characteristics.

Method

Along with the development of a measurement tool to determine the information security awareness level of secondary school students, the study, which aims to determine the pre-psychometric characteristics, consists of two dimensions. First, a scale development process was used to measure information security awareness. Second, the information security awareness of the students was determined by considering the psychometric properties of the developed scale.

The study was carried out with a total of 675 students who continued their education at secondary school level in the 2021-2022 academic year. During the Exploratory Factor Analysis (EFA) phase of the measurement tool development process, the data of 410 students were evaluated and revised accordingly. The new form obtained was applied again for the Confirmatory Factor Analysis (CFA) of the study, and at this stage, the data obtained from a total of 265 students were analyzed.

Results

As a result of the analysis of the data obtained, the KMO coefficient value was determined as .903 and it was seen that the data structure was perfectly sufficient for factor analysis. In addition, as a result of the analyzes, the Bartlett Sphericity test was found to be significant at the .01 level. These findings meant that the sample was at an adequate level, the data came from a multivariate normal distribution and therefore another assumption of factor analysis was met. In this direction, as a result of the EFA process, which was the first stage of the research conducted with the data obtained from 410 students; the factor loading value of the scale is .65 with 3 factors consisting of 30 items ("online security awareness: osa", "online curiosity: oc" and "cyber threat awareness: cta") structure was emerged. The new form was created with the items of this 3-factor structure, which was found to explain 56.30% of the total variance, was reapplied and the 3-factor structure was confirmed after the CFA stage with 265 students whose data were considered valid. As a result of the analysis, the Cronbach's alpha reliability coefficient for the whole scale was determined as.90. Cronbach's alpha coefficient for each sub-dimension of the scale is as follows; osa: .94, oc: .90, and cta: .86. In line with these results, a valid and reliable scale was developed to determine the information security awareness levels of students studying at secondary school level.

Whether there was a statistically significant difference between the total scores obtained from each of the three-factor structure of the scale development study and the gender factor of the students was calculated using t-test. As a result of the analyses, it was determined that the average scores of the students studying at the secondary school level from the information security awareness scale showed a statistically significant difference according to the gender factor.

Discussion

When the studies on information security awareness were examined, it came to the forefront that the weakest link in information security systems was the human element and that awareness-raising studies on information security should be carried out in addition to determining the current situation. Based on these findings, it was seen that there was a need to develop a measurement tool that can help analyze the situation and evaluate the deficiencies that arise by determining the information security awareness levels of children who start to live a life intertwined with technology in the early period of their lives. As a result of the research conducted within this framework, a scale consisting of 30 items and 3 factors was developed. In examining whether there was a statistically significant difference between the three-factor structure emerging from the scale development study and the gender factor of the students, it was determined that the average scores of students' information security awareness had a statistically significant difference according to their gender. When the average scores obtained from the sub-factors of the prepared scale were examined, it was determined that the average scores of female students were higher than male students in the sub-factors as well as in the whole scale.

Pedagogical Implications

Since the level of information security awareness of students studying at the secondary school level (10-14 years old) is addressed, it is believed that this study and the scale developed could fill the gap in the field. The data obtained showed that the developed scale provides consistent, valid and reliable measurements in determining the information security awareness levels of secondary school students. In this context, training can be organized, materials can be developed, and guidance services can be provided to raise awareness within the scope of information technologies guidance services for students who need to determine the level of information security awareness of students studying at the secondary school level. In order to increase students' information security awareness, information technologies and software courses should be included more in the curriculum at the primary education level, social clubs on information security should be established, and content on information security awareness could be included in the boards. In addition, with the scale developed, various hypotheses can be tested regarding the information security awareness levels of students studying at the secondary school level and their usage behaviors of internet-based technologies and applications.

Araştırmanın Etik Taahhüt Metni

Yapılan bu çalışmada bilimsel, etik ve alıntı kurallarına uyulduğu; toplanan veriler üzerinde herhangi bir tahrifatın yapılmadığı, karşılaşılacak tüm etik ihlallerde “Cumhuriyet Uluslararası Eğitim Dergisi ve Editörünün” hiçbir sorumluluğunun olmadığı, tüm sorumluluğun Sorumlu

Yazara ait olduğu ve bu çalışmanın herhangi başka bir akademik yayın ortamına değerlendirme için gönderilmemiş olduğu sorumlu yazar tarafından taahhüt edilmiştir.

Kaynaklar

Acılar, A. (2009). İşletmelerde Bilgi Güvenliği ve Örgüt Kültürü. *Organizasyon ve Yönetim Bilimleri Dergisi, 1*(1), 25-33.

Akgün, Ö. E., & Topal, M. (2015). Eğitim Fakültesi Son Sınıf Öğrencilerinin Bilişim Güvenliği Farkındalıkları: Sakarya Üniversitesi Eğitim Fakültesi Örneği. *Sakarya University Journal of Education, 5*(2), 98-121.

AlKalbani, A., Deng, H., & Kam, B. (2015). Organisational security culture and information security compliance for e-Government development: The moderating effect of social pressure. In *Pacific Asia Conference on Information System.* Singapore.

Allers, J., Drevin, G. R., Snyman, D. P., Kruger, H. A., & Drevin, L. (2021). Children's Awareness of Digital Wellness: A Serious Games Approach. In *IFIP World Conference on Information Security Education*. 95-110.

Atkinson, S., Furnell, S., & Phippen, A. (2009). Securing The Next Generation: Enhancing E-Safety Awareness Among Young People. *Computer Fraud & Security, 7*, 13-19.

Beder, A., & Ergün, E. (2015). Ortaokul öğrencilerinin güvenli internet kullanım durumlarının belirlenmesi. *Eğitim Bilimleri ve Uygulama*, *14*(27), 23-41.

Brady, C. (2010). Security awareness for children. Royal Holloway.

Büyüköztürk, Ş. (2002). Faktör Analizi: Temel Kavramlar ve Ölçek Geliştirmede Kullanımı. *Kuram ve Uygulamada Eğitim Yönetimi, 32*, 470-483.

Büyüköztürk, Ş. (2006). *Sosyal Bilimler İçin Veri Analizi El Kitabı. İstatistik, Araştırma Deseni SPSS Uygulamaları ve Yorum (6. baskı).* Ankara: PegemA yayıncılık.

Canbek, G., & Sağıroğlu, Ş. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. *Politeknik Dergisi, 9*(3), 165-174.

Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educationalinstitution. *African Journal of Information and Communication, 20*, 133–155.

Çakmak, E.Kılıç, Çebi, A., & Kan, A. (2014). E-öğrenme Ortamlarına Yönelik "Sosyal Bulunuşluk Ölçeği" Geliştirme Çalışması. *Kuram ve Uygulamada Eğitim Bilimleri, 14(*2),755-768.

Çelen, F. K., Çelik, A., & Seferoğlu, S S. (2011). *Çocukların İnternet kullanımları ve onları bekleyen çevrim-içi riskler.* XIII. Akademik Bilişim Konferansı (AB11)*,* İnönü Üniversitesi, Malatya.

Çokluk, Ö., Şekercioğlu, G., & Büyüköztürk, Ş. (2010). *Sosyal bilimler için çok değişkenli istatistik SPSS ve LISREL uygulamaları.* Ankara: Pegem Akademi.

Derin, M. A., & Gençoğlu M. T. (2020). Ortaokul Öğrencilerinin Bilgi Güvenliği Farkındalığı. *Savunma Bilimleri Dergisi*, *38*, 159-181.

Güldüren, C. (2015). *Yükseköğretim kurumlarındaki öğretim elemanlarının bilgi güvenliği farkındalık düzeylerinin değerlendirilmesi* (Kayıt No. 396156) [Doktora Tezi, Ankara Üniversitesi]. YÖK Tez Merkezi.

Güldüren, C., Çetinkaya, L., & Keser, H. (2016). Ortaöğretim öğrencilerine yönelik bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. *İlköğretim Online 15*(2),682-695.

Gülmüş, M. (2010). *Kurumsal bilgi güvenliği yönetim sistemleri ve güvenliği* (Kayıt No. 295662) [Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi]. YÖK Tez Merkezi.

Hanus, B., & Wu, Y. A. (2016). Impact of users'security awareness on desktop security behavior: Aprotection motivation theory perspective. *Information Systems Management, 33*(1), 2–16.

Haufe, K., Brandis, K., Colomo-Palacios, R., Stantchev, V., & Dzombeta, S. (2016). A process framework for information security management. *International Journal of Information Systems and Project Management, 4*(4), 27–47

Jöreskog, K. G., & Sörbom, D. (1993). *LISREL 8: Structural equation modeling with the SIMPLIS command language.* Scientific Software International; Lawrence Erlbaum Associates, Inc.

Karaahmetoğlu, G. (2021). Ortaokul Öğrencilerinin Bilgisayar Kullanımı ve İnternet Bağımlılığı Düzeylerinin İncelenmesi. *Erciyes Üniversitesi Sağlık Bilimleri Fakültesi Dergisi*, *7*(2), 1-9.

Kass, R. A., & Tinsley, H. E. A. (1979). Factor analysis. *Journal of Leisure Research, 11*, 120-138.

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

Ki-Aries, D., & Faily, S. (2017). Persona-centred information security awareness. *Computers & security*, *70*, 663-674.

Kline, P. (1994). *An easy guide to factor analysis.* New York: Routledge.

Kline, P. (2000). *The Handbook of Psychological Testing* (2nd Edition). London and Newyork: Routledge.

Kline, P. (2005). *Principles and Practice of Structural Equation Modeling* (2nd ed.). New York: Guilford.

Koohang, A., Anderson, J., Nord, J. H., & Paliszkiewicz, J. (2020). Building an awareness-centered information security policy compliance model. *Industrial Management & Data Systems, 120*(1), 231- 247.

Kritzinger, E., & Smith, E. (2008). Information security management:An information security retrieval and awareness model for industry. *Computer & Security*, 27, 224-231.

Lawshe, C. H. (1975). A quantitative approach to content validity. *Personnel psychology, 28*(4), 563-575.

Leszczyna, R. (2018). A review of standards with cybersecurity requirements for smart grid. *Computers & security*, *77*, 262-276.

Mochiko, T. (2016). *Cybercrime "will rise" with internet of things*. Business Live.

Mustafaoğlu, R., Zirek, E., Yasacı, Z., & Özdinçler, A. R. (2018). Dijital teknoloji kullanımının çocukların gelişimi ve sağlığı üzerine olumsuz etkileri. *Addicta: The Turkish Journal on Addictions, 5*(2), 1-21.

Nunnally, J. C. (1978). *Psychometric testing.* New York: McGraw-Hill.

Nunnally, J. C., & Bernstein, I. (1994). *Psychometric theory.* New York: McGraw-Hill.

Öztemiz, S., & Yılmaz, B. (2013). Bilgi Merkezlerinde Bilgi Güvenliği Farkındalığı: Ankara'daki Üniversite Kütüphaneleri Örneği. *Bilgi Dünyası, 14*(1), 87-100.

Paliszkiewicz, J. (2019). Information Security Policy Compliance: Ladership and Trust. *Journal of Computer Information Systems, 59*(3):1-7.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2015). Factors that influence information security behavior: An Australian web-based study. *Human Aspects of Information Security, Privacy, and Trust*, 231-241.

PricewaterhouseCoopers PwC (2016). *Turnaround and transformation in cybersecurity – Key findings from The*

Global State of Information Security Survey 2016. https://www.pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf adresinden 20.01.2022 tarihinde erişildi.

Puhakainen, P. (2006). *A Design theory for information security awareness* (Kayıt No. 9514281144), [Doctoral Dissertation, Acta University of Oulu]. Jultika.

Schermelleh-Engel, K., & Moosbrugger, H. (2003). Evaluating the fit of structural equation models: Tests of significance and descriptive goodness-of-fit measures. *Methods of Psychological Research Online, 8*(2),23-74.

Siponen, M. T. (2001). Five Dimensions Of Information Security Awareness. *Computer and Society, 31*(2), 24-29.

Şahinaslan, E.,Kandemir, R., & Şahinaslan, Ö. (2009). Bilgi Güvenliği Farkındalık Eğitim Örneği. *Akademik Bilişim Konferansı.* Şanlıurfa, 189-194.Serter, B. (2021). *Ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeyinin belirlenmesi* (Kayıt No.679722) [Yüksek Lisans Tezi, Gazi Üniversitesi]. YÖK Tez Merkezi.

Şimşek, Ö. F. (2007). *Yapısal eşitlik modellemesine giriş: Temel ilkeler ve LISREL uygulamaları.* Ankara: Ekinoks Yayınları

Tabachnick, B. G., & Fidell, L.v S. (1996). *Using multivariate statistics* (3. Ed.). New York: Harper Collins College Publishers.

Taha, N., & Dahabiyeh, L. (2021). College students information security awareness: a comparison between smartphones and computers. *Education and Information Technologies, 26*, 1721–1736.

Talan, T. & Aktürk, C. (2021). Orta Öğretim Öğrencilerinin Dijital Okuryazarlık ve Bilgi Güvenliği Farkındalığı Seviyelerinin İncelenmesi. *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi*, *18*(1), 158-180.

Tavşancıl, E. (2005). *Tutumların ölçülmesi ve SPSS ile veri analizi.* Ankara: Nobel.

Theofanos, M., Choong, Y. Y., & Murphy, O. (2021). Passwords Keep Me Safe–Understanding What Children Think about Passwords. *In 30th USENIX Security Symposium (USENIX Security 21)*. 19-35

Topa, I., & Karyda, M. (2019). From theory to practice: Guidelines for enhancing information security management. *Information and Computer Security, 27*(3), 326-342.

Veiga, A. D. (2008). *Cultivating and assessing information security culture* (Doctorate of Philosophy). University of Pretoria, Pretoria.

Veneziano L., & Hooper J. (1997). A method for quantifying content validity of health-related questionnaires. *American Journal of Health Behavior, 21*(1),67-70.

Zwick, W. R., & Velicer, W. F. (1986). Comparison of five rules for determining the number of components toretain. *Psychological Bulletin, 99*(3), 432-442.

Watkins, M. W. (2021). *A step-by-step guide to exploratory factor analysis with SPSS*. New York: Routledge.

Whitman, M., & Mattord, H. (2018*). Principles of Information Security. Boston*: Cengage Learning.

Yılmaz, E., Şahin, Y. L., & Akbulut Y. (2016). Öğretmenlerin Dijital Veri Güvenliği Farkındalığı. *Sakarya University Journal of Education, 6*(2), 26-45.