

ÖĞRETMENLER İÇİN BİLGİ GÜVENLİĞİ FARKINDALIK ÖLÇEĞİ (BGFÖ) GELİŞTİRME ÇALIŞMASI

Levent ÇETİNKAYA*
Can GÜLDÜREN**
Hafize KESER***

Öz: Bilgi güvenliği ve bu konuda alınan güvenlik önlemlerinin sağlanması kişisel ve kurumsal açıdan oldukça önemlidir. Her ne kadar bilgi güvenliğinin sağlanmasına yönelik, kurumlar tarafından teknoloji temelli çözümler hayata geçirilse de bu teknolojileri kullananlar yine de insanlardır. Bu çalışmanın, amacı öğretmenlerin bilgi güvenliği farkındalık düzeylerini belirlemeye yönelik bir ölçek geliştirmektir. Çalışmanın ilk aşamasında, 316 kişilik katılımcı grubu ile açıklayıcı faktör analizi (AFA) yapılmış ve ölçeğin üç alt boyut altında ("Mobil cihazlar, Mahremiyet ve İletişim: MMI," "Saldırı ve Tehditler: ST" ve "Genel Güvenlik: GG") 48 maddeden oluştuğu belirlenmiştir. Çalışmanın ikinci aşamasında, 200 kişilik katılımcı grubu ile gerçekleştirilen doğrulayıcı faktör analizi (DFA) sonucunda üç faktörlü yapı doğrulanmıştır. Ölçeğin tamamı için Cronbach Alfa güvenilirlik katsayısı .980; her alt boyut için sırasıyla: MMI:.967, ST:.969 ile GG:.926'dır. Bu çalışma sonucunda öğretmenlerin bilgi güvenliği farkındalık düzeylerini belirlemek için kullanılacak geçerli ve güvenilir bir ölçek geliştirilmiştir.

Anahtar Kelimeler. Bilgi, Güvenlik, Farkındalık, Bilgi Güvenliği, Öğretmen, Ölçek Geliştirme

* Dr., Ankara Üniversitesi Eğitim Bilimleri Enstitüsü.

** Yrd. Doç. Dr., Ufuk Üniversitesi Bilgisayar Teknolojileri Bölümü.

*** Prof. Dr., Ankara Üniversitesi Eğitim Bilimleri Fakültesi.

DEVELOPMENT OF INFORMATION SECURITY AWARENESS SCALE (ISAS) FOR TEACHERS

Levent ÇETİNKAYA*
Can GÜLDÜREN**
Hafize KESER***

Abstract

Information security and provision of the security measures are very important in terms of people and institutions. Although there are technological solutions adopted by the institutions to enable information security, they are the people themselves who use them. Bearing this in mind, the aim of this study is to develop an "information security awareness scale" for teachers which is intended to determine their level of information security awareness. In the first phase of the study, exploratory factor analysis (EFA) was conducted with 316 teachers and it was determined that the scale consists of 48 items under 3 sub dimensions ("Mobile devices, Privacy and Communication: MPC", "Attacks and Threats: AT" and "General Security: GS"). In the second phase of the study, confirmatory factor analysis (CFA), which was conducted with 200 teachers, revealed three-factor structure. Cronbach's Alpha reliability coefficient is .980 for the entire scale; and MPC:.967, AT:.969 and GS:.926, respectively for each sub dimension. Consequently, a valid and reliable scale that can be used to determine the level of information security awareness of teachers has been developed.

Keywords. Information, Security, Awareness, Information Security, Teacher, Scale Development

Giriş

Günümüzde insanlar, hemen hemen bütün aktivitelerinde kullandıkları dijital teknolojiler aracılığıyla dış dünya ile bağlantı kurmanın yanı sıra, bilginin farklı formlarda yayılımını gerçekleştirmektedirler. Öyle ki bireyler arası iletişim ve bilgi paylaşım süreçleri artık gerçek ortamlardan daha çok sanal ortamlarda gerçekleşmektedir. Gerçek ile sanal yaşantıların iç içe geçtiği günümüzde, özellikle ulaşılan bilgi ve bu bilginin güvenliği, her iki yaşantının da dengeli bir biçimde devamı için önemlidir.

* Dr., Educational Technologist, Ankara University, Institutes of Educational Sciences.

**Assistant Prof. Dr., Ufuk University, Department of Computer Technologies.

*** Prof. Dr., Ankara University, Faculty of Educational Sciences.

Özellikle bilginin paylaşımı aşamasında, kişisel bilgilerimiz başta olmak üzere bize ait tüm kritik bilgiler, teknolojik cihazlar veya bu cihazlarda barındırılan uygulamalar aracılığı ile sanal dünyanın kullanıcılara ayrılan bir yerinde saklanmaktadır (Güldüren, Çetinkaya ve Keser, 2016). Bu noktada da bilgi güvenliğinin sağlanması ve gerekli önlemlerinin alınması kişisel ve kurumsal açıdan oldukça önemlidir.

Bilgi güvenliği, bir varlık türü olarak bilginin izinsiz veya yetkisiz bir biçimde erişimini, kullanımını, değiştirilmesini, ifşa edilmesini, ortadan kaldırılmasını, el değiştirmesini ve hasar verilmesini önlemek olarak tanımlanabilir; gizlilik, bütünlük ve erişilebilirlik olarak isimlendirilen üç temel unsurdan meydana gelir (Puhakainen, 2006). Bu unsurlardan herhangi birinin eksik olması ya da zarar görmesi durumunda bilgi güvenliği açıkları söz konusu olur ve bu durumda güvenlik zafiyetlerine yol açar. Bu açıkların giderilmesi ve zafiyetlerin önlenmesine yönelik geliştirilen teknoloji temelli standart ve yazılımlarla çözüm bulma düşüncesi, bilgi güvenliğinin sağlanmasında belki de en önemli unsur olan insan faktörünün göz ardı edilmesine neden olmaktadır (Chen, Shaw ve Yang, 2006; Kjørvik, 2010; Öztemiz ve Yılmaz, 2013; Rezgui ve Marks, 2008). Her ne kadar teknoloji temelli uygulamalar aracılığıyla güvenlik zafiyetleri büyük ölçüde giderilebiliyor olsa da bu teknolojileri kullananların insanlar olduğu unutulmaması gereken bir gerçektir. Nitekim bu gerçek kişisel ve kurumsal bilgilerin güvenliğinin, en zayıf halkası olan insan faktörünün göz ardı edilerek teknoloji temelli yöntemlerle çözümlenemeyeceğini göstermektedir (Güldüren, Çetinkaya ve Keser, 2016; Kritzingler ve Smith, 2008; Mahabi, 2010; Penmetsa, 2010; Veiga, 2008).

Bilginin yönetimi ve dolayısıyla yönetilebilen bilginin güvenliğinin sağlanması oldukça karmaşık bir süreçtir ve bu sürecin iyi bir planlamayla yönetilmesi gerekmektedir. Sadece teknik önlemlerin alınarak, başta insan hataları olmak üzere diğer faktörlerin dikkate alınmaması sürecin sağlıklı işleminin önündeki en önemli engeldir. Dolayısıyla bilgi güvenliğinin sağlanmasında teknoloji temelli önlemlerin alınmasının yanı sıra, insan faktörünün göz ardı edilmemesi ve bu noktada da bilgi güvenliği konusunda farkındalığın kazandırılması risklerin en aza indirgenmesinde oldukça önemlidir. İnsan faktörüne bağlı bilgi güvenliği risklerini tamamen ortadan kaldırmak mümkün olmasa da, iyi planlanmış bir farkındalık etkinliği ile güvenlik risklerinin kabul edilebilir bir seviyeye çekilmesiyle sağlanabilir (Acılar, 2009; Gülmüş, 2010; Keser ve Güldüren, 2015; Kruger ve Kearney, 2006; Vardal, 2009; Vural, 2007). Bu noktada da bilgi güvenliği risklerinden korunmanın en iyi yolu insanların bilinçlenmesi ve ihtiyaç duyulan güvenlik teknolojilerini doğru yer ve zamanda kullanmakla mümkündür (Albrechtsen, 2007; Al-Shehri, 2012; Puhakainen, 2006; Siponen, 2001; Şahinaslan, Kantürk, Şahinaslan ve Borandağ, 2009).

Hepsi birbiri ile iletişim kapasitesine sahip, hızla ilerleyen ve karmaşıklaşan teknolojiler ile kuşatılmış olan günümüz insanının iletişiminde yeni bir boyuta geçtiği açıkça görülebilmektedir. Artık neredeyse sınırsız iletişim gücüne sahip cihazlarla çevrimiçi bağlantı kurabilir hale gelmesi, iletişim açısından büyük kolaylık olarak algılan-

bilir, ancak bu durum aynı zamanda bireyleri çeşitli tehlikelere de açık hale getirebilmektedir. Bu tehlikelerin başında ise özel bilgilerin paylaşımıyla birlikte, sanal ve gerçek yaşam arasındaki sınırların çizilememesi gelmektedir. Bu paylaşımların bazen sınırları aşması bireyin suistimale maruz kalmasına ve sonrasında yaşamında tehdit oluşturmasına sebep olabilmektedir (Eckertova, 2013). Teknolojinin gelişmesine paralel olarak bilgi güvenliğine yönelik tehdit ve saldırı yöntemlerinin çeşitlenmesi, bilgi güvenliği farkındalığının belirlenmesi ve bu çerçevede geliştirilmesini her geçen gün daha önemli kılmaktadır. Bu doğrultuda yapılan çalışmalar incelendiğinde daha çok bilginin korunmasında teknoloji temelli unsurların dikkate alındığı, bilgi güvenliği yönetim sistemleri, bilgi güvenliği sorunları, risk değerlendirmesi ve bilgi güvenliği farkındalık eğitimleri üzerine yapılan araştırmalara yer verildiği görülmektedir. Yapılan bu araştırmalar daha çok genel durum tespitine yönelik iken bilgi güvenliğinde insan unsurunun dikkate alındığı ve dijital teknolojilerin içinde genç nesille sürekli temas içinde olan öğretmenlerin bilgi güvenliği farkındalık düzeyinin ne olduğunu belirleyecek nitelikte bir çalışmaya ulaşılamamıştır. Bilgi güvenliği farkındalığına yönelik gerçekleştirilen en kapsamlı çalışmalardan birisi Güldüren (2015) tarafından gerçekleştirilen, “Yükseköğretim kurumlarındaki öğretim elemanlarının bilgi güvenliği farkındalık düzeylerinin değerlendirilmesi” başlıklı doktora tezidir. Araştırmacı çalışmayı oluşturmuş olduğu madde havuzundan hareketle, Türkiye’de çeşitli yükseköğretim kurumunda görev yapan 363 öğretim elemanı ile gerçekleştirmiştir. Açımlayıcı faktör analizi sonucunda, ölçeğin 34 madde ve 2 alt boyuttan (“saldırı ve tehditler” ile “kişisel verilerin korunması”) oluştuğu belirlenmiştir. Katılımcılar arasından rastgele seçilen 200 kişilik grup üzerinde yapılan doğrulayıcı faktör analizi sonucunda 2 faktörlü yapı doğrulanmıştır. Diğer bir çalışma ise Güldüren, Çetinkaya ve Keser (2016) tarafından ortaöğretim öğrencileri bilgi güvenliği farkındalık düzeylerini belirlemeye yönelik ölçek geliştirme çalışmasıdır. Araştırmacılar, ortaöğretim kurumlarında öğrenim gören 607 öğrenciyle gerçekleştirdikleri çalışmada, 407 kişilik katılımcı grubu ile açımlayıcı faktör analizi (AFA) yapılmıştır. AFA sonucunda, ölçeğin 36 madde ve 3 alt boyuttan (“saldırı ve tehditler: St”, “mahremiyet: Ma” ile “kişisel verilerin korunması: Kvk”) oluştuğu belirlenmiştir.

Günümüzde, özellikle eğitim öğretim süreçlerine doğrudan ya da dolaylı şekilde giren ve bir şekilde süreçleri etkileyen teknolojiler ile bunlara bağlı uygulamalar öğretmenlerin bilgi güvenliği farkındalığının önemini arttırmaktadır. Nitekim bu teknolojiler dünyanın sayılı eğitimde teknoloji entegrasyonu reformlarından biri olan FATİH projesiyle okullarda hızla yerini almıştır. Türkiye ve Güney Kore gibi ülkelerde devlet politikası şeklinde ilerleyen bu süreç, okuldaki tüm paydaşları ilgilendirmekle birlikte sürecin sağlıklı işleyebilmesi için bilgi güvenliği farkındalığı açısından da önem kazanmıştır. Bu noktada teknolojiyi günlük yaşamıyla birlikte okulunda da kullanmak durumunda olan öğretmenlerin bilgi güvenliği farkındalığının belirlenmesi ve bu doğrultuda da gerekli tedbirlerin alınması gerekmektedir. Diğer taraftan özellikle genç bireylerle ortak bir yaşam alanı olan öğretmenlerin, bilgi güvenliği konusunda

öz değerlendirme yapabilmesinin ve olası tehlikelerden öğrencileriyle birlikte kendilerini de koruyabilmesi önemlidir. Bu noktada, özellikle de bilginin yayılımından ve genç nesillerin yetiştirilmesinden sorumlu öğretmenlerde, bilgi güvenliği farkındalığı ve kültürünün oluşturulması bir zorunluluk haline gelmektedir. Ancak, bunun için öncelikle farkındalık düzeylerinin doğru bir biçimde belirlenmesi ve gerekli önlemlerin alınması gerekmektedir. Nitekim bilgi güvenliğinin sağlanması için sadece teknik önlemlerin alınmasının yeterli olamayacağı gerçeği, bu teknolojileri kullanan ya da kullanacak olan öğretmenlerin bilgi güvenliği farkındalığının belirlenmesini gerekli kılmaktadır. Bu gereksinimden hareketle çalışma, öğretmenlerin, bilgi güvenliği farkındalık düzeyini belirleyecek olan bir ölçeğin geliştirilmesi amacıyla gerçekleştirilmiştir.

Yöntem

Araştırma Deseni

Araştırmanın modeli (deseni), araştırma sorularına cevap vermeyi ya da araştırmanın hipotezlerini test etmeyi güvence altına alan, verilerin araştırmanın amacına uygun ve ekonomik olarak toplanmasını ve çözümlenmesini sağlayan koşulların düzenlenmesidir (Balci, 2009). Öğretmen bilgi güvenliği farkındalık ölçeğinin geliştirilmesi ve ön-psikometrik (preliminary) özelliklerinin belirlenmesi amacıyla yönelik olarak Yurdağül (2005) tarafından tanımlanan kapsam geçerlilik oranı, faktör analizi ve güvenilirlik (iç ve test-tekrar test) katsayıları ile madde analizine dayanan kuramsal ölçek geliştirme modeli kullanılmıştır. Öğretmenlere yönelik “Bilgi Güvenliği Farkındalık Ölçeği” geliştirme çalışmasının hangi aşamalarda gerçekleştiği ve çalışma grubunun özellikleri aşağıda sunulmuştur.

Çalışma Grubu

Araştırmanın çalışma grubunu, 2015-2016 öğretim yılı 2. döneminde ortaöğretim kurumu türlerini kapsayacak nitelikte belirlenen AFA uygulamasında 316, DFA uygulamasında 200 olmak üzere toplam 516 öğretmen oluşturmaktadır. Çalışmanın yapılacağı okul türü, okul türü oranları ve öğrenci sayıları belirlenirken Millî Eğitim Bakanlığı 2014-2015 eğitim-öğretim dönemi örgün eğitim istatistikleri (MEB, 2015) dikkate alınmıştır. Belirlenen çalışma grubunun % 51.9’u kadın ve % 48.1’i erkek öğretmenlerden oluşmuştur. Öğretmenlerin %18.4’ü 0-5 yıl, %20.5’i 6-10 yıl, %21.3’ü 11-15 yıl, %20.3’ü 16-20 yıl ve %19.4’ü ise 20 yıl üstü kıdeme sahiptirler. Çalışma grubundaki öğretmenlerin AFA ve DFA uygulamalarındaki cinsiyete göre kıdem dağılımları Tablo 1’de detaylandırılmıştır.

Tablo 1. Çalışma Grubundaki Öğretmenlerin Cinsiyet ve Kıdem Dağılımları

	Cinsiyet	Kıdem(Yıl)										Toplam	
		0-5		6-10		11-15		16-20		20+		f	%
		f	%	f	%	f	%	f	%	f	%		
AFA	Kadın	31	9.8	33	10.4	36	11.4	33	10.4	31	9.8	164	51.9
	Erkek	28	8.9	32	10.1	31	9.8	31	9.8	30	9.5	152	48.1
	Toplam	59	18.7	65	20.6	67	21.2	64	20.3	61	19.3	316	100
DFA	Kadın	19	9.5	22	11.0	22	11.0	21	10.5	20	10.0	104	52.0
	Erkek	17	8.5	19	9.5	21	10.5	20	10.0	19	9.5	96	48.0
	Toplam	36	18.0	41	20.5	43	21.5	41	20.5	39	19.5	200	100
Toplam		95	18.4	106	20.5	110	21.3	105	20.3	100	19.4	516	100

Tablo 1’de görüldüğü üzere, AFA çalışma grubunu %51.9’u kadın ve %48.1’i ise erkek öğretmenlerden oluşmaktadır. Öğretmenlerin %18.7’si 0-5 yıl, %20.6’sı 6-10 yıl, %21.2’si 11-15 yıl, %20.3’ü 16-20 yıl ve %19.3’ü ise 20 yıl üstü kıdeme sahiptirler. DFA çalışma grubunun ise %52.0’ı kadın ve %48.0’i ise erkek öğretmenlerden oluşmaktadır. Öğretmenlerin %18.0’ı 0-5 yıl, %20.5’i 6-10 yıl, %21.5’i 11-15 yıl, %20.5’i 16-20 yıl ve %19.5’i ise 20 yıl üstü kıdeme sahiptirler. AFA ve DFA çalışma gruplarını cinsiyete göre kıdem dağılımları birlikte incelendiğinde ise, her iki çalışma grubunu dağılımlarının birbiriyle ve MEB (2015) verileriyle paralellik gösterdiği görülmektedir.

Veri Toplama Aracı

Ölçek geliştirme ilk önce maddelerin hazırlanmasıyla başlayan, daha sonra geçerlik ve güvenilirlik çalışması ile devam eden kapsamlı bir çalışmadır. Bir ölçek için pek çok geçerlik ölçütünden söz edilebilirse de Karasar’a (2005, s.151) göre en çok yararlanılanlar: içerik/muhteva/kapsam geçerliği (content validity), uygulama (deneysel) geçerliği (predictive validity) ve yapı geçerliğidir (construct validity).

Çalışmanın ilk aşamasında alanyazın incelenerek bilgi güvenliği farkındalığı kavramına ilişkin göstergelerin neler olabileceği tespit edilmiştir. Bu doğrultuda Tablo 2’de detaylandırılan ve Güldüren’in (2015) bilgi güvenliği farkındalığına ilişkin tespit etmiş olduğu kategoriler, göstergeler ve madde sayılarından faydalanılmasına karar verilmiştir. Bu doğrultuda araştırmacının 90 maddeden oluşan madde havuzundan, kapsam geçerlik indeksi 0.89 olarak hesaplanan ve 67 maddeyi içeren form çalışma grubuna uygulanmıştır. Uygulanan ölçek formunda, bireylerin ölçekteki maddelere katılma düzeylerini belirlemek üzere “hiç katılmıyorum (1)”, “katılmıyorum (2)”, “kararsızım (3)”, “katılıyorum (4)” ve “kesinlikle katılıyorum (5)” şeklinde Likert tipi beşli derecelendirme ölçeği kullanılmıştır.

Tablo 2. Bilgi Güvenliği Farkındalığı Kategori, Gösterge ve Madde Sayıları

Kategoriler	<i>f</i>	Madde Sayısı
Genel Güvenlik	Bilgi güvenliği, Bilgi güvenliği sorumluluğu, Anti-virüs yazılımları, Güvenlik duvarı, Şifre seçimi ve korunması, Virüs ve casus yazılımlar, Bazı yaygın söylenceler, İyi güvenlik alışkanlıkları, Çocukların güvenli şekilde çevrimiçi tutulması, Verilerin güvence altına alınması	34
Saldırı ve Tehditler	Çevrimiçi ticaret tuzakları, Sosyal mühendislik ve sazan avlama / yemleme saldırıları, Siber zorbalık, Aldatmacalar ve şehir efsaneleri, Kimlik hırsızlığı, Casus yazılımlar, Virüsler, solucanlar ve truva atları, Hizmet aksattırma saldırıları, Bozuk yazılım dosyaları, Kök kullanıcı takımı (rootkit) ve botnet'ler, Sahte anti-virüs yazılımları	21
E-posta ve İletişim	Anlık mesajlaşma ve sohbet odaları, Ücretsiz e-posta servislerinin faydaları ve riskleri, Mesaj sağanağı, Sosyal ağ siteleri, Dijital imza, E-posta istemcileri, E-posta ekleri	8
Mobil Cihazlar	Elektronik cihazlar için siber güvenlik, Cep telefonları ve kişisel dijital yardımcılar, Şahsi internet-etkin cihazlar ile seyahat, Taşınabilir cihazlarda veri güvenliği ve fiziksel güvenlik, Kablosuz ağ güvenliği, USB sürücüler	8
Mahremiyet	Dosyaların etkili bir şekilde silinmesi, Mahremiyetin korunması, Şifrelerin ilave önlemler ile desteklenmesi, Şifrelemenin anlaşılması	8
Güvenli Gezinme	Telif hakkı ihlalleri, Web sitesi sertifikaları, Web tarayıcıları, Aktif içerik ve çerezler, Web tarayıcılara ait güvenlik ayarları, Çevrimiçi güvenli alışveriş, Bluetooth teknolojisi, Uluslararası etki alan adları	6
Yazılım ve Uygulamalar	Son kullanıcı lisans sözleşmeleri, Dosya paylaşım teknolojileri ve riskler, Yazılım yamaları, İnternet protokolü ses teknolojisi, İşletim sistemleri	5
Toplam		90

Verilerin Toplanması ve Analizi

Ölçek geliştirme çalışmalarında ideal olan durumun Açıklayıcı Faktör Analizi (AFA) ve Doğrulayıcı Faktör Analizlerinin (DFA) farklı örneklem gruplarından elde edilen veriler üzerinde yapılması gerekmektedir (Çakmak ve diğerleri 2014). Örneklem büyüklüğü, madde ya da faktör sayısı gibi bağlı ölçütlere dayalı olarak tahmin edilmektedir. Genel olarak örneklem büyüklüğünün ölçekteki madde sayısının 5-10 katı kadar olması istenmektedir (Kass ve Tinsley, 1979; Kline, 1994; Tavşancıl, 2005).

Kline (1994) mutlak ölçüt olarak 200 kişilik örneklemin yeterli olacağını, ancak büyük örneklemle çalışmanın daha uygun olacağını vurgulamaktadır. Çokluk, Şekercioğlu ve Büyüköztürk (2010), faktör analizinde en az 300 örneklem sayısının uygun olduğu genel kuralını ortaya koymaktadır. Bu çerçevede gerçekleştirilen çalışmanın AFA uygulaması için 369 öğretmen, oluşturulan formun basılı halini doldurmuş ve yapılan inceleme sonucunda öğretmenlerin doldurduğu formlardan 53'ü geçersiz sayılmış ve 316'sının istatistiksel analize uygun olduğu tespit edilmiştir. Toplanan verilerin analiz edilmesi sonrasında yeniden düzenlenen ölçek formu DFA uygulaması için 200 öğretmen tarafından doldurulmuş ve formların hepsi geçerli sayılmıştır Böylelikle çalışmanın AFA uygulaması aşamasında 316, DFA uygulaması aşamasında ise 200 olmak üzere toplam 516 öğretmenin katılımıyla ölçeğin geçerlik ve güvenilirlik çalışması yapılmıştır.

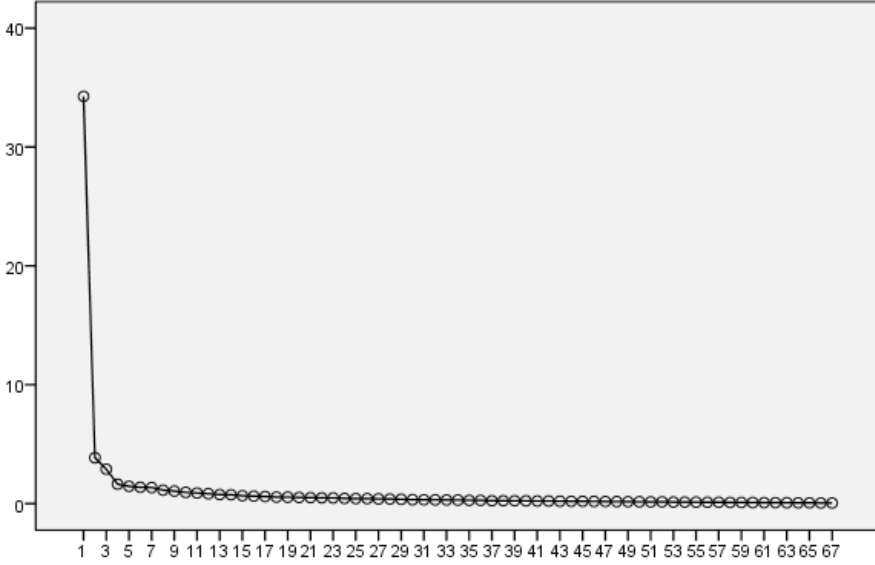
Bulgular

Bu bölümde öğretmenlerin bilgi güvenliği farkındalıklarının belirlenmesine yönelik ölçek geliştirme sürecinde elde edilen bulgular; açımlayıcı faktör analizi, madde analizleri ve doğrulayıcı faktör analizi ile ilgili bulgular alt başlıklarında sunulmuştur. Çalışmada verilerin AFA'ya uygunluğunu saptamak üzere Kaiser-Meyer-Olkin (KMO) Testi katsayısı hesaplanmış ve Barlett Küresellik testi yapılmıştır. Örneklem büyüklüğü için değer, 0.50'den düşük ise teste devam edilmez, .90 üzerinde ise "mükemmel" olduğu şeklinde yorumlanır (Tavşancıl, 2005; Çokluk ve ark., 2010). KMO katsayısı değeri .967 olarak belirlenmiştir ve veri yapısının faktör analizi yapabilmek için mükemmel derecede yeterli olduğu değerlendirilmiştir. Çalışma içerisinde yapılan analiz sonucunda Barlett Küresellik testi .01 düzeyinde manidar bulunmuştur [$\chi^2=22393.316$; $df=2211$; $p=0.000$]. Bu bulgu, verilerin çok değişkenli normal dağılımdan geldiğini ve dolayısıyla faktör analizinin bir diğer sayılısının karşılandığı anlamına gelmektedir.

Açımlayıcı Faktör Analizi

Maddeler için, önceden belirlenmiş bir yapı bulunmadığı için faktör yapısını ortaya koymak için öncelikle döndürülmemiş temel bileşenler analizi gerçekleştirilmiştir (Tabachnick ve Fidell, 1996). Faktör sayısının belirlenmesinde Kaiser-Guttman ilkesi uyarınca özdeğerleri 1'den büyük faktörlerin incelenmesi yoluna gidilmiş; faktör özdeğerlerine ilişkin çizgi grafiği ve açıkladıkları varyans oranları incelenmiştir (Zwick ve Velicer, 1986). Çünkü faktör analizinde, sadece öz değerleri bir ve birin üzerinde olan faktörler kararlı olarak kabul edilmektedir (Büyüköztürk, 2002; Çokluk ve ark., 2010). Ölçek, özdeğerleri 1'den büyük 9 faktör yapısına sahiptir. Bu faktörlerin sırasıyla özdeğeri ve açıklanan toplam varyansa katkı düzeyleri: 1.faktör:34,26; %51,13, 2.faktör: 3,86; %5,75, 3.faktör: 2,90; %4,32, 4.faktör: 1,63; %2,44, 5.faktör: 1,45; %2,17, 6.faktör: 1,37; %2,04, 7 faktör: 1,35; %2,00, 8.faktör: 1,13; %1,70 ve 9.faktör: 1,05; %1,57 şeklindedir. Alanyazın incelendiğinde faktör yapılarına karar verebilmek için ortaya

konulan çözümün kuramsal olarak temellenebilmesi olduğu görülmektedir (Zwick ve Velicer, 1986). Tek faktörlü desenlerde açıklanan varyansın %30 ve daha fazla olması yeterli görülebilir (Tabachnick ve Fidell, 1996). Çok faktörlü desenlerde ise açıklanan varyansın daha yüksek olması beklenir. Açıklanan varyansı arttırmak için iki tür yol izlenir. Bunlardan ilki, önemli faktör sayısını arttırmak, ikincisi ise açıklanan madde seçiminde daha yüksek faktör yük değerini aramaktır (Büyüköztürk, 2002). Bu kapsamda AFA analizine başlarken öz değer 2 ve faktör yük değeri 0.55 olarak kabul edilmiştir (Çokluk, Şekercioğlu ve Büyüköztürk, 2010). Şekil 1’de faktör özdeğerlerine ait çizgi grafiği sunulmaktadır.



Şekil 1. Faktör Özdeğerlerine İlişkin Çizgi Grafiği

AFA sonucunda ölçeğin öz değerinin 2'den büyük üç faktör altında toplandığı görülmüştür. Bu üç faktörün ölçeğe ilişkin açıkladığı varyans ise %61,70'dır. AFA sonucu oluşan maddeler binişiklik ve faktör yük değerlerinin kabul düzeyini karşılayıp karşılamaması açısından değerlendirilmiştir. Çok faktörlü desenlerde, binişik ve yük değeri düşük olan maddeler bir arada olabilir. Kesin bir kural olmamakla birlikte, madde çıkarma işlemine binişik maddelerden başlanması tercih edilebilir (Çokluk ve ark., 2010). Binişik ve yük değeri düşük olan maddeler ölçekten çıkartılarak AFA 16 kez tekrarlanmıştır. Nihai AFA sonucu oluşan, maddelere ilişkin faktör yükleri ve ortak faktör varyansı Tablo 3'de sunulmuştur.

Tablo 3. Faktör Yük Değerleri ve Ortak Faktör Varyansı

Alt Boyut	Madde	F1		Ortak Faktör Varyansı	Alt Boyut	Madde	F2		Ortak Faktör Varyansı	Alt Boyut	Madde	F2		Ortak Faktör Varyansı
		F1	Ortak Faktör Varyansı				F2	Ortak Faktör Varyansı				F2	Ortak Faktör Varyansı	
Mobil Cihazlar, Mahremiyet ve İletişim	M44	0,81	0,75			M33	0,81	0,73			M02	0,69	0,58	
	M41	0,81	0,70			M32	0,81	0,72			M18	0,65	0,72	
	M45	0,77	0,77			M30	0,79	0,71			M17	0,65	0,72	
	M46	0,74	0,74			M31	0,77	0,74			M06	0,64	0,64	
	M39	0,73	0,56			M36	0,76	0,75			M07	0,63	0,41	
	M43	0,71	0,66			M35	0,75	0,75			M01	0,62	0,47	
	M51	0,71	0,58			M26	0,72	0,72			M16	0,61	0,58	
	M42	0,70	0,71			M28	0,70	0,76			M21	0,59	0,64	
	M61	0,68	0,68			M34	0,70	0,66			M04	0,59	0,44	
	M54	0,67	0,71			M25	0,67	0,71			M14	0,59	0,38	
	M38	0,66	0,59			M58	0,66	0,70			M19	0,58	0,59	
	M47	0,64	0,71			M22	0,65	0,58			M05	0,56	0,44	
	M50	0,64	0,68			M29	0,63	0,68			M13	0,55	0,58	
	M49	0,64	0,68			M48	0,61	0,68						
	M52	0,64	0,63			M59	0,60	0,67						
	M62	0,61	0,53			M24	0,60	0,66						
	M40	0,60	0,57			M23	0,59	0,60						
	M53	0,59	0,56											
Özdeğer: 26,03				Özdeğer: 3,37				Özdeğer: 2,71						
Açıklanan Varyans: 50,05				Açıklanan Varyans: 6,49				Açıklanan Varyans: 5,20						
Açıklanan Toplam Varyans: 61,74														

* 0.55'den düşük yük değerleri tabloda gösterilmemiştir.

Tablo incelendiğinde ölçekte yer alan 18 maddeden oluşan birinci faktöre ait faktör yük değerlerinin .59 ile .81 arasında, maddelere ilişkin ortak faktör varyanslarının ise .56 ile .77 arasında değiştiği; 17 maddeden oluşan ikinci faktör ait faktör yük değerlerinin .59 ile .81 arasında, maddelere ilişkin ortak faktör varyanslarının ise .58 ile .76 arasında değiştiği ve 13 maddeden oluşan üçüncü faktöre ait faktör yük değerlerinin .55 ile .69 arasında, maddelere ilişkin ortak faktör varyanslarının ise .38 ile .72 arasında değiştiği görülmektedir. Toplam varyansa en yüksek katkıyı .81 faktör yük değeri ve .75 ortak faktör varyansı ile 44. maddenin, en düşük katkıyı ise .59 faktör yük değeri

ve .38 ortak faktör varyansı ile 14. maddenin yapmakta olduğu ifade edilebilir. Birinci faktörün açıklayabildiği toplam varyans %50,05 düzeyinde olup, alanyazın da dikkate alınarak “mobil cihazlar, mahremiyet ve iletişim” olarak isimlendirilmiştir (Örnek maddeler: USB sürücülerini kullanırken dikkat edilmesi gereken hususları biliyorum. İstemeyen elektronik posta nedir biliyorum. İnternette gezinirken mahremiyetimi korumak için alınması gereken tedbirleri biliyorum). İkinci faktörün açıklayabildiği varyans %6,49 düzeyinde olup, alanyazın da dikkate alınarak “saldırı ve tehditler” olarak isimlendirilmiştir (Örnek maddeler: Sosyal mühendislik saldırısı nedir biliyorum. Hizmet aksatırma saldırısı nedir biliyorum. Kimlik avı saldırısı nedir biliyorum.). Üçüncü faktörün açıklayabildiği varyans %5,20 düzeyinde olup, alanyazın da dikkate alınarak “genel güvenlik” olarak isimlendirilmiştir (Örnek maddeler: Bilgi güvenliği ile ilgili sorumluluklarımın ne olduğunu biliyorum. Kullandığım bilgi sistemlerinde tanımlanmış olan kuralları nasıl uygulayacağımı biliyorum. Bilgi güvenliğinin ne anlama geldiğini biliyorum.).

Üç faktörlü yapının açıklayabildiği toplam varyans %61,74 düzeyindedir. Alanyazında çok faktörlü ölçek yapılarında, sosyal bilimlerde açıklanan varyansın %40 ile %60 arasında olması yeterli olarak kabul edilmektedir (Tavşancıl, 2005). Bu ölçüte dayanarak elde edilen üç faktörlü ölçek yapısı öğretmenlere yönelik bilgi güvenliği farkındalığını ölçmek için yeterli bulunmuştur. Ölçekte yer alan 48 maddenin tamamı için faktör yük değerleri .55’in üzerinde kalmıştır. Alanyazında .45 ve üzerinde faktör yük değeri gösteren maddeler ölçekte kesinlikle tutulması gereken maddeler olarak nitelenmektedir (Büyüköztürk, 2011: 124; Kline, 2000: 167-168). Bu ölçüte dayanarak ölçeğin üç faktör altında 48 maddenin tamamını içermesine karar verilmiştir. Ölçeğin alt faktörleri (mobil cihazlar, mahremiyet ve iletişim, saldırı ve tehditler, genel güvenlik) faktörlere dahil olan sorular, ölçekten alınan en düşük ve en yüksek puanlara ilişkin puanlar ile farkındalık düzeyleri Çizelge 1’de sunulmuştur.

Çizelge 1. Ölçek Alt Faktörleri, Faktörlere Dâhil Olan Sorular ile En Düşük ve En Yüksek Farkındalık Düzeyi Puanları.

Faktör/Alt Faktör Adı	Faktör Soruları	En Düşük Puan	En Yüksek Puan	Farkındalık Düzeyi			
				Düşük	Orta	Normal	Yüksek
Bilgi Güvenliği ve Farkındalık Ölçeği	1-48	48	240	48-96	97-144	145-192	193-240
Mobil Cihazlar, Mahremiyet ve İletişim	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

Madde Analizleri

Ölçekte yer alan her bir maddenin, ölçmek istediği özelliği ölçüp ölçmediği ve ölçtükleri özellik açısından kişileri ayırt etmede ne kadar yeterli olduklarının belirlenmesi amacıyla ilk olarak madde-toplam korelasyonları hesaplanmıştır. İkinci olarak ise toplam puana göre üst %27 ve alt %27'lik grupların madde puanları arasındaki farkın anlamlılığı için t-testi kullanılmıştır. Ayrıca, ölçeğin güvenilirliğini belirlemek için Cronbach Alfa iç tutarlılık katsayısına bakılmıştır. Ölçekte yer alan her bir madde için madde-toplam korelasyonları ve toplam puana göre belirlenen üst ve alt %27'lik grupların madde puanları arasındaki farkın anlamlılığını irdeleyen bağımsız t-testi sonuçları Tablo 4'te sunulmaktadır.

Tablo 4. Madde Analiz Sonuçları

F1	Madde	DM-TK	Ü/A	F2	Madde	DM-TK	Ü/A	F3	Madde	DM-TK	Ü/A	%27
		*	**			*	**			*	**	
Mobil Cihazlar, Mahremiyet ve İletişim	M38	0,71	17,45*	Saldırı ve Tehditler	M22	0,65	11,89*	Genel Güvenlik	M01	0,49	9,18*	
	M39	0,57	11,62*		M23	0,74	17,42*		M02	0,57	11,38*	
	M40	0,71	17,42*		M24	0,78	19,26*		M04	0,40	6,93*	
	M41	0,68	16,50*		M25	0,79	19,08*		M05	0,55	10,88*	
	M42	0,80	23,96*		M26	0,78	19,19*		M06	0,71	15,85	
	M43	0,74	18,72*		M28	0,82	19,13*		M07	0,38	8,14*	
	M44	0,75	18,60*		M29	0,80	21,52*		M13	0,71	18,55*	
	M45	0,81	24,71*		M30	0,69	12,79*		M14	0,32	5,54*	
	M46	0,81	23,20*		M31	0,76	16,12*		M16	0,65	15,77*	
	M47	0,82	26,76*		M32	0,68	12,37*		M17	0,76	20,93*	
	M49	0,80	22,91*		M33	0,69	12,95*		M18	0,77	20,33*	
	M50	0,80	22,77*		M34	0,71	15,05*		M19	0,68	16,00*	
	M51	0,66	15,12		M35	0,77	17,84*		M21	0,72	16,41*	
	M52	0,76	18,17*		M36	0,76	17,53*					
M53	0,72	16,12*	M48	0,78	19,24*							
M54	0,81	21,88*	M58	0,79	17,45*							
M61	0,79	20,94*	M59	0,78	17,28*							
M62	0,68	16,47*										

* DM-TK: Düzeltilmiş Madde-Toplam Korelasyonu

** Üst-Alt %27 Farkın Anlamlılık Testi (Bağımsız t-testi)

Faktör analizi ile belirlenen 3 boyutu oluşturan 48 maddenin madde analizleri yapılmıştır. Buna göre; mobil cihazlar, mahremiyet ve iletişim faktöründe madde-toplam korelasyonları incelendiğinde $r=.57$ ile $r=.82$ arasında değişmektedir. Saldırı ve tehditler faktöründe madde-toplam test korelasyonları incelendiğinde değerlerin $r=.65$ ile $r=.82$ arasında değiştiği görülmektedir. Kişisel verilerin korunması faktöründe madde-toplam test korelasyonları incelendiğinde ise değerler $r=.32$ ile $r=.77$ arasında değişim göstermektedir. Madde-toplam korelasyonlarının .30 ve daha yüksek olması ölçek maddelerinin geçerliğine bir kanıt olarak kullanılmaktadır (Nunnally ve Bernstein, 1994). Analizler sonucunda, madde-toplam test korelasyonları incelendiğinde, her bir madde için .30'un üzerinde olduğu belirlenmiştir. Bu durum, ölçek maddelerinin ölçülmek istenen özelliği ölçme amacına hizmet ettiğine işaret etmektedir. Ayrıca, ölçeğin t-testi sonuçlarına göre %27 alt ve üst gruplarının madde puanları arasındaki farklara ilişkin t testi değerlerinin 5.54-26.76 arasında değiştiği ve hepsinin de anlamlı olduğu ($p<.001$) görülmektedir. Üst %27'lik grubun tüm maddelere ilişkin madde

puan ortalamaları alt %27'lik grubun madde puan ortalamalarından anlamlı biçimde yüksektir. Buna göre ölçekte yer alan maddeler aynı davranışı; yani öğretmenlere yönelik bilgi güvenliği farkındalığını ölçmekte ve farklı farkındalık seviyelerindeki katılımcıları anlamlı biçimde ayırt edebilmektedir. Hem madde-toplam korelasyonları hem de üst ve alt %27'lik grupların madde ortalama puanlarına ilişkin t-testi sonuçları ayırt ediciliği en yüksek olarak 47. ve en düşük olarak 14. maddeyi göstermektedir.

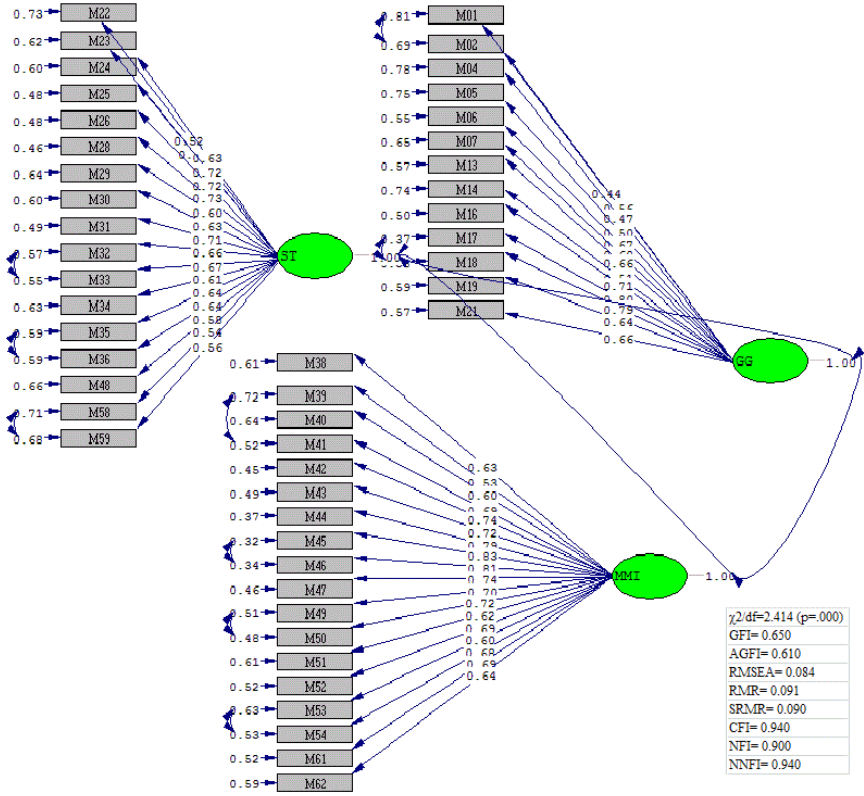
Ölçeğin güvenilirliğini ortaya koymak amacıyla Cronbach Alfa iç tutarlılık katsayısı hesaplanmıştır. Genel olarak, güvenilirlik katsayılarının .70 veya daha yüksek olması, yeterli olarak değerlendirilmektedir (Nunnally, 1978). Ölçeğin tümüne ait Cronbach Alfa iç tutarlılık katsayısı .980, birinci alt faktöre ilişkin Cronbach Alfa iç tutarlılık katsayısı .967, ikinci alt faktöre ilişkin Cronbach Alfa iç tutarlılık katsayısı .969 ve üçüncü alt faktöre ilişkin Cronbach alfa iç tutarlılık katsayısı .926 olarak hesaplanmıştır. Tüm bu bulgular ölçeğin tatmin edici düzeyde güvenilirliğe sahip olduğunu göstermektedir. Bunun yanında madde-toplam korelasyonlarının yüksekliği de ölçeğin iç tutarlılığının gücüne işaret etmektedir.

Doğrulayıcı Faktör Analizi

AFA sonrasında ortaya çıkan modelin, yapı geçerliğini değerlendirmek için DFA yapılmıştır (Kline, 2000). Bu çalışmada model uyum indeksleri olarak Ki-Kare (χ^2) İyilik Uyumu, İyilik Uyum İndeksi (GFI), Düzenlenmiş İyilik Uyum İndeksi (AGFI), Yaklaşık Hataların Ortalama Karekökü (RMSEA), Artık Ortalamaların Karekökü (RMR), Standardize Edilmiş Artık Ortalamaların Karekökü (SRMR), Karşılaştırmalı Uyum İndeksi (CFI), Normlaştırılmış Uyum İndeksi (NFI) ve Normlaştırılmamış Uyum İndeksi (NNFI) göz önünde bulundurulmuştur.

Üç faktörden oluşan yapıya ilişkin olarak gerçekleştirilen doğrulayıcı faktör analizlerinde model üzerinde hiçbir sınama yapılmadan ve önerilen modifikasyonlar gerçekleştirilmeden önce ulaşılan uyum iyiliği indeksleri şöyledir: [$\chi^2/df=3.489[3758,16/1077]$ ($p=.000$); GFI= 0.560; AGFI= 0.520; RMSEA= 0.112; RMR= 0.100; SRMR= 0.100; CFI= 0.900; NFI= 0.870; NNFI= 0.900]. Analizler sonucunda ortaya çıkan modifikasyon önerileri incelendiğinde; M36 ve M35; M02 ve M01; M46 ve M45; M18 ve M17; M59 ve M58; M54 ve M53; M50 ve M49; M41 ve M39; M33 ve M32 maddeleri arasında dokuz modifikasyon önerisinin ortaya çıktığı görülmüştür. Kuramsal olarak incelendiğinde; bu maddelerin benzer durumları ölçtükleri, dolayısıyla iki madde arasında gizil bir ilişkinin kabul edilebilir olacağı görülmüş ve modifikasyon önerisi dikkate alınmıştır.

Şekil 2. Doğrulayıcı Faktör Analizi



Modifikasyonun ardından modele ilişkin uyum iyiliği indeksleri şu şekilde oluşmuştur: [$\chi^2/df=2.414[2578,38/1068]$ ($p=.000$); GFI= 0.650; AGFI= 0.610; RMSEA= 0.084; RMR= 0.091; SRMR= 0.090; CFI= 0.940; NFI= 0.900; NNFI= 0.940]. Şekil 2’de üç faktörlü yapıya ilişkin yapısal eşitlik modeli ve Tablo 4’te ölçek maddelerine ilişkin t ve R2 (çoklu korelasyon katsayısı) değerleri sunulmaktadır.

Tablo 5’de sunulan yapısal eşitlik modelinde uyum indeksleri kriterleri ve kabulü için kesme noktaları göz önüne alınarak modelin uyum iyiliği indeksleri incelendiğinde Ki-Kare/serbestlik derecesi iyilik uyumu değerinin 2.414 olduğu görülmektedir (küçük örneklem için 2.5’in altındaki modellerde mükemmel uyum, Çokluk ve arkadaşları, 2010; Kline, 2000). Hesaplanan RMSEA değerinin .084 olduğu görülmektedir (iyi uyum, Brown, 2006; Jöreskog ve Sörbom, 1993’ten aktaran Çokluk ve arkadaşları, 2010). Modelin GFI değeri .650 ve AGFI değeri .610 için zayıf uyuma sahip olduğu söylenebilir (GFI, AGFI > .90 mükemmel uyum; GFI> .85 ve AGFI>.80 kabul edilebilir

uyum; Jöreskog ve Sörbom, 1993'ten aktaran; Çokluk ve arkadaşları, 2010). Alanyazın irdelendiğinde bu indekslerin aldıkları değerlerin örneklem büyüklüğüne çok duyarlı olduğu ve büyük örneklerde daha uygun değerler verdiği görülmektedir (Çokluk ve arkadaşları, 2010). Örneklem büyüklüğü etkilerinden arındırılmış uyum iyiliği indekslerinden olan CF, NFI ve NNFI üzerinde durulmuştur. CFI, NFI ve NNFI değerlerinin .90'dan büyük olduğu görülmektedir (CFI, NFI, NNFI > .95 mükemmel uyum; Sümer, 2000; Thompson, 2004). RMR ve SRMR değerinin .09'den küçük olması iyi uyuma sahip olduğunu göstermektedir (Brown, 2006; Byrne, 1994). Modele ilişkin t değerleri incelendiğinde tüm gözlenen değişkenlerin gizil değişken tarafından .01'lik anlamlılık düzeyinde yordanabildiği görülmektedir.

Tablo 5. Madde Analiz Sonuçları

F1	Madde	t	R ²	F2	Madde	t	R ²	F3	Madde	t	R ²
Mobil Cihazlar, Mahremiyet ve İletişim	M45	8,59	0,68	Saldırı ve Tehditler	M28	8,96	0,54	Genel Güvenlik	M17	7,88	0,63
	M46	8,73	0,66		M25	9,02	0,52		M18	7,94	0,62
	M44	8,90	0,63		M26	9,03	0,52		M16	8,79	0,50
	M42	9,22	0,55		M31	9,06	0,51		M06	9,01	0,45
	M47	9,23	0,54		M33	9,25	0,45		M13	9,08	0,43
	M43	9,31	0,51		M32	9,29	0,43		M21	9,10	0,43
	M50	9,28	0,49		M35	9,36	0,41		M19	9,16	0,41
	M41	9,39	0,48		M36	9,36	0,41		M07	9,34	0,35
	M52	9,40	0,48		M24	9,38	0,40		M02	9,46	0,31
	M61	9,40	0,48		M30	9,39	0,40		M14	9,57	0,26
	M54	9,42	0,47		M23	9,43	0,38		M05	9,60	0,25
	M62	9,54	0,41		M34	9,46	0,37		M04	9,65	0,22
	M38	9,57	0,39		M29	9,47	0,36		M01	9,70	0,19
	M51	9,58	0,39		M48	9,53	0,34				
	M53	9,61	0,37		M59	9,57	0,32				
	M40	9,63	0,36		M58	9,61	0,29				
M49	9,35	0,34	M22	9,64	0,27						
M39	9,72	0,28									

Önemli bir ölçüt de her bir gözlenen değişken için açıklanan varyansı ifade ederek, gözlenen değişkenin gizil değişkendeki değişimin ne kadarını açıklayabildiğini ortaya koyan R2 değeridir (Şimşek, 2007). Modele ilişkin t ve R2 değerleri incelendiğinde bilgi güvenliği farkındalığının ölçümüne en yüksek katkısı sırasıyla 45, 46, 44, 42 ve 47. maddelerin, en düşük katkısı ise sırasıyla 1, 4, 5, 14, ve 22. maddelerin sağladığı

görülmektedir. Bu bulgu, açımlayıcı faktör analizinde elde edilen bulguları doğrulamaktadır.

Tartışma ve sonuç

Alanyazın incelemesinde bilgi güvenliği konusunda yapılan çalışmaların genelde bilgi güvenliği ile bilgi güvenliği yönetim sistemlerine yönelik olduğu ve bu bağlamda “en zayıf halka” olan insan unsurunu bilgi güvenliği konusunda bilinçlendirme üzerinde durulduğu tespit edilmiştir. Bu çalışmalarda, bilgi güvenliği farkındalığına yönelik çeşitli tavsiyeler ve alınması gereken tedbirler sunulmaktadır. Ayrıca ulaşılan kaynaklar kapsamında, kullanıcıların mevcut farkındalık düzeylerini belirleyebilecek yurtdışı kaynaklı bir çalışma (Kruger ve Kearney, 2006) ile yurt içinde Güldüren (2015) tarafından yüksek öğretim kurumlarındaki öğretim elemanlarına yönelik ölçek geliştirme çalışması ile Güldüren, Çetinkaya ve Keser (2016) tarafından ortaöğretim öğrencilerine yönelik olarak geliştirilen bir ölçek çalışmasına ulaşılmıştır. Bu araştırma kapsamında alanyazından elde edilen bilgi güvenliği farkındalık göstergeleri esas alınarak öğretmenlere yönelik bilgi güvenliği farkındalık düzeylerini belirleyecek yeni bir ölçek geliştirilmiştir.

Yapı geçerliliği çalışmalarında ölçekte yer alan 48 madde üç faktör altında toplanmış ve açıklayabildiği toplam varyans %61,74’dir. Bu oran çok faktörlü ölçek yapısı için yeterli kabul edilmektedir. İlk faktör ‘mobil cihazlar, mahremiyet ve iletişim’ olarak isimlendirilmiş ve açıklayabildiği toplam varyans %50,05’dir. İkinci faktör ‘saldıırı ve tehditler’ olarak isimlendirilmiş ve açıklayabildiği toplam varyans %6,49’dur. Üçüncü faktör ‘genel güvenlik’ olarak isimlendirilmiş ve açıklayabildiği toplam varyans %5,20’dir. Madde analizlerinde, madde toplam puanları arasında güçlü bir korelasyonel ilişki belirlenmiştir. Ölçeğin tamamına ait Cronbach Alfa iç tutarlılık katsayısı .980, alt faktörlere ilişkin değerler .967, .969 ve .926 olarak hesaplanmıştır. Madde toplam korelasyonları ve iç tutarlılık katsayıları dikkate alındığında geliştirilen ölçeğin güvenilir olduğu değerlendirilmektedir.

Doğrulayıcı faktör analizinin ortaya koyduğu uyum iyiliği indeksleri ve standart değerler açımlayıcı faktör analiziyle ortaya konan çok faktörlü yapının uygunluğuna işaret etmektedir. Özellikle X²/df, CFI, NFI ve NNFI değerleri göz önüne alındığında yapının mükemmel uyuma sahip olduğunu ortaya koymaktadır. RMSEA, RMR ve SRMR değerleri göz önüne alındığında iyi uyuma sahip olduğunu ortaya koymaktadır. GFI, AGFI değerleri göz önüne alındığında, yakın olmakla birlikte kabul edilebilirlik sınırlarının dışında değer göstermektedirler. GFI ve AGFI indeksleri 0 ile 1 arasında değişir ve örneklem büyüklüğüne çok duyarlı olduğu için büyük n’lerde daha uygun değerler verir (Sümer, 2000; Schumacker ve Lomax, 1996; Tabachnick ve Fidell, 2001). Araştırmadaki diğer bir sınırlılık öğretmenlerin bu tür çalışmalara katılmada gönülsüz olmalarıdır. Bu duruma ölçek geliştirme esnasında araştırma grubunu oluşturan öğretmenlerin iş yoğunluğu ve araştırma konusuna yeterli zaman ayıramamalarının

sebeplendirildiği düşünülmektedir. Geliştirilen ölçeğe ilişkin faktör yük değerleri, iç tutarlılık katsayıları gibi istatistiksel parametrelerdeki birtakım değişimlerde bu isteksizliğin de etkili olabileceği düşünülmektedir. Ayrıca çalışma grubunun büyüklüğü açılımlı faktör analiziyle elde edilen değerleri de etkileyebilecek bir sınırlılık olarak ele alınabilir. Gelecekte daha geniş katılımcı grupları üzerinde ölçeğin faktör yapısının yeniden sorgulanmasının yararlı olacağı düşünülmektedir.

Bu çalışma sonucu ölçeğin psikometrik özellikleri, geçerli ve güvenilir bir yapıda olduğunu göstermektedir. Bu çerçevede geliştirilen ölçeğin öğretmenlerin bilgi güvenliği farkındalık düzeylerini belirlemeye yönelik çalışmalarda kullanılabilir olduğu söylenebilir. Böylelikle farkındalık düzeyleri belirlenen öğretmenlerin, eksiklerine yönelik gerekli tedbirler alınabilir ya da farkındalık oluşturmaya yönelik rehberlik etkinlikleri gerçekleştirilebilir. Gelecek çalışmalarda farklı örneklem grubu üzerinde geliştirilen ölçeğin geçerlik ve güvenilirlik değerleri test edilebilir. Ayrıca geliştirilen bu ölçek ile birlikte öğretmenlerin bilgi güvenliği farkındalıkları; internet bağımlılığı, problemli internet kullanım düzeyleri, siber zorba ve mağdur olma durumları gibi değişkenlerle çeşitli hipotez modelleri sınanabilir.

Kaynakça

- Acılar, A. (2009). İşletmelerde Bilgi Güvenliği ve Örgüt Kültürü. *Organizasyon ve Yönetim Bilimleri Dergisi*, 1(1), 25-33.
- Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computer & Security*, 26(4), 276-289.
- Al-Shehri, Y. (2012). Information security awareness and culture. *British Journal of Arts and Social Sciences*, 6(1), 61-69.
- Brown, T. A. (2006). *Confirmatory factor analysis for applied research (1st Ed.)*. NY: Guilford Publications, Inc.
- Balcı, A. (2009). Sosyal bilimlerde araştırma yöntem, teknik ve ilkeler. (7.b.). Ankara: Pegem Akademi.
- Büyüköztürk, Ş. (2011). *Sosyal bilimler için veri analizi el kitabı*. Ankara: Pegem Akademi Yayıncılık.
- Byrne, B. M. (1994). *Structural equation modeling with EQS and EQS/Windows: Basic concepts, applications, and programming (1st Ed.)*. NJ: Lawrence Erlbaum Associates, Inc.
- Chen, C. C., Shaw, R. ve Yang, S. C. (2006). Mitigating Information Security Risks By Increasing User Security Awareness: A Case Study Of An Information Security Awareness System. *Information Technology, Learning and Performance Journal*, 24(1), 1-14.
- Çakmak, E. K., Çebi, A. ve Kan, A. (2014). E-öğrenme Ortamlarına Yönelik "Sosyal Bulunusluk Ölçeği" Geliştirme Çalışması. *Kuram ve Uygulamada Eğitim Bilimleri*, 14(2), 755-768.
- Çokluk, Ö., Şekercioğlu, G. ve Büyüköztürk, Ş. (2010). *Sosyal bilimler için çok değişkenli istatistik SPSS ve LISREL uygulamaları*. Ankara: Pegem Akademi.

◆ Levent Çetinkaya / Can Güldüren / Hafize Keser

- Eckertova, L., Docekal, D., ve Pozar, J. (2013). *Child Safety on the Internet: Mentor responsible parents*. 1st Ed. Brno: Computer Press, 54-78.
- Güldüren, C. (2015). *Yükseköğretim kurumlarındaki öğretim elemanlarının bilgi güvenliği farkındalık düzeylerinin değerlendirilmesi*. Doktora Tezi, Ankara Üniversitesi, Eğitim Bilimleri Ana Bilim Dalı, Ankara.
- Güldüren, C., Çetinkaya, L. ve 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*. Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi, Elektrik Mühendisliği Anabilim Dalı, İstanbul.
- Karasar, N. (2005). *Bilimsel araştırma yöntemi kavramlar ilkeler teknikler*. Ankara: Nobel Yayınları.
- Kass, R. A. ve Tinsley, H. E. A. (1979). Factor analysis. *Journal of Leisure Research*, 11, 120-138.
- Keser, H. ve Güldüren, C. (2015). Bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. *K.Ü. Kastamonu Eğitim Dergisi*, 23(3), 1167-1184.
- Kjørvik, H. (2010). *Implementing and improving awareness in information security*. Master's thesis, University of Agder, Faculty of Engineering and Science, Grimstad. [Online]: <http://brage.bibsys.no/> adresinden 15.09.2015 tarihinde erişilmiştir.
- 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.
- Kritzing, E. ve Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computer and Security*, 27, 224-231.
- Kruger, H. ve Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computer and Security*, 25, 289-296.
- Mahabi, V. (2010). *Information security awareness: System administrators and end-user perspectives at Florida State University*. Doctoral dissertation, The Florida State University, College of Communication and Information, Florida. [Online]: <http://diginole.lib.fsu.edu/etd/2798/> adresinden 15.09.2015 tarihinde erişilmiştir.
- MEB (2015). *Millî Eğitim İstatistikleri, Örgün Eğitim 2013-2014*. T.C. Millî Eğitim Bakanlığı Strateji Geliştirme Başkanlığı, Ankara. [Online]: http://sgb.meb.gov.tr/istatistik/meb_istatistikleri_orgun_egitim_2014_2015.pdf adresinden 13.09.2015 tarihinde erişilmiştir.
- Nunnally, J. C. (1978). *Psychometric testing*. New York: McGraw-Hill.
- Nunnally, J. C. ve Bernstein, I. (1994). *Psychometric theory*. New York: McGraw-Hill.
- Öztemiz ve Yılmaz (2013). Bilgi Merkezlerinde Bilgi Güvenliği Farkındalığı: Ankara'daki Üniversite Kütüphaneleri Örneği. *Bilgi Dünyası*, 14(1), 87-100.
- Penmetsa, M. K. (2010). *A methodology for measuring information security maturity in Norwegian and Indian MSME's with special focus on people factor*. Master's thesis, Gjøvik University,

- College Department of Computer Science and Media Technology, Hogskolen. [Online]: <http://brage.bibsys.no/> adresinden 17.09.2015 tarihinde erişilmiştir.
- Puhakainen, P. (2006). *A Design theory for information security awareness*. Master's thesis, Acta University of Oulu, Faculty of Science Department of Information Processing Science, Oulu. [Online]: <http://herkules.oulu.fi> adresinden 15.09.2015 tarihinde erişilmiştir.
- Rezgui, Y., and Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computer and Security*, 27, 241-253.
- Schumacker, R. E. Ve Lomax, R. G. (1996). *A beginner's guide to structural equational modeling (1st Ed.)*. NY: Taylor & Francis Group.
- Siponen, M. T. (2001, June). Five Dimensions Of Information Security Awareness. *Computer and Society*, 31(2) 24-29.
- Sümer, N. (2000). Yapısal Eşitlik Modelleri. *Türk Psikoloji Yazıları*, 3(6) 49-74.
- Şahinaslan, E., Kantürk, A., Şahinaslan, Ö. ve Borandağ, E. (2009). *Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri*. Akademik Bilişim '09 - XI.Akademik Bilişim Konferansı Bildirileri, (s. 597-602). Şanlıurfa.
- Şimşek, Ö. F. (2007). *Yapısal Eşitlik Modellemesine Giriş Temel İlkeler ve LISREL Uygulamaları*. Ankara: Ekinox.
- Tabachnick, B. G. ve Fidell, L.v S. (1996). *Using multivariate statistics (3th Ed.)*. New York: Harper Collins College Publishers.
- Tabachnick, B. G. ve Fidell, L.v S. (2001). *Using multivariate statistics (4th Ed.)*. MA: Allyn & Bacon, Inc.
- Tavşancıl, E. (2005). *Tutumların ölçülmesi ve SPSS ile veri analizi*. Ankara: Nobel.
- Thompson, B. (2004). *Exploratory and confirmatory factor analysis: Understanding concepts and applications (1st Ed.)*. Washington: American Psychological Association.
- Vardal, N. (2009). *Yükseköğretimde bilgi güvenliği: Bilgi güvenlik yönetim sistemi için bir model önerisi ve uygulaması*. Doktora Tezi, Gazi Üniversitesi, Eğitim Bilimleri Ana Bilim Dalı, Ankara.
- Veiga, A. d. (2008). *Cultivating and assessing information security culture*. Doctoral dissertation, University of Pretoria, Faculty of Engineering, Built Environment and Information Technology, Pretoria. [Online]: <http://upetd.up.ac.za/thesis/available/etd-04242009-165716/> adresinden 16.09.2015 tarihinde erişilmiştir.
- Vural, Y. (2007). *Kurumsal bilgi güvenliği ve sızma (penetrasyon) testleri*. Yüksek lisans tezi, Gazi Üniversitesi, Bilgisayar Mühendisliği Anabilim Dalı, Ankara.
- Yurdagül, H. (2005). Ölçek geliştirme çalışmalarında kapsam geçerliği için kapsam geçerlik indekslerinin kullanılması. *XVI. Ulusal Eğitim Bilimleri Kongresi içerisinde (s.1-6)*. Pamukkale Üniversitesi Eğitim Fakültesi. Denizli.
- Zwick, W. R. ve Velicer, W. F. (1986). Comprasion of five rules for determining the number of components to retain. *Psychological Bulletin*, 99(3), 432-442.