AJIT-e: Online Academic Journal of Information Technology
2015 Fall/Güz – Cilt/Vol: 6 - Sayı/Num: 21
DOI: 10.5824/1309-1581.2015.4.002.x
http://www.ajit-e.org/?menu=pages&p=details_of_article&id=172

Dijital Veri Güvenliği Farkındalığı Ölçeğinin Geliştirilmesi[1]

Eray YILMAZ, Dr., *T.C. Ziraat Bank Science High School, Balıkesir, Turkey, eray_yilmaz@yahoo.com*

Yusuf Levent ŞAHİN, *Asst. Prof. Dr., Anatolian University, Faculty of Education, Department of Computer and Instructional Technologies Education, Eskişehir, Turkey, ylsahin@anadolu.edu.tr*

Yavuz AKBULUT, *Assoc. Prof. Dr., Anatolian University, Faculty of Education, Department of Computer and Instructional Technologies Education, Eskişehir, Turkey, yavuzakbulut@anadolu.edu.tr*

ÖZET *Bilgi ve iletişim teknolojilerindeki hızlı gelişmeler sonucunda geçmişte daha çok basılı materyallerle çalışan öğretmenler, günümüzde bilgiyi dijital ortamlarda üretmekte ve saklamaktadır. Öğretim etkinliklerinde güncel teknolojileri kullanması beklenen öğretmenlerin sahip oldukları dijital verilerin güvenliği son derece önemlidir. Veri güvenliğinin öneminden yola çıkan bu araştırmanın amacı, öğretmenlerin dijital veri güvenliği farkındalıklarının belirlenmesine yönelik bir ölçek geliştirmektir. Alanyazın taraması ve kritik paydaşlarla yapılan odak grup görüşmeleri sonucunda 93 maddeden oluşan bir madde havuzu oluşturulmuştur. 12 alan uzmanının görüşü alındıktan sonra taslak ölçek formunun ön deneme uygulaması 79 öğretmen ile gerçekleştirilmiştir. Ölçeğin yapı geçerliği için 529 öğretmenden toplanan veriler ile açımlayıcı faktör analizi (AFA) yapılmış, 32 maddeden oluşan tek faktörlü bir yapı ortaya konmuştur. Kabul edilebilir iç tutarlılık (α:0.945) ve açıklanan varyans (% 36.1) değerlerine sahip olan beşli Likert tipindeki ölçek, 335 farklı katılımcıya daha uygulanmış ve doğrulayıcı faktör analizi (DFA) gerçekleştirilmiştir. Modifikasyon indeksleri yardımı ile ideal değerlere ulaşan tek faktörlü yapı, dijital veri güvenliği farkındalık ölçeğinin (DVGFÖ) geçerli ve güvenilir olduğunu, ileride yapılacak araştırmalarda kullanılabileceğini göstermiştir.*

Anahtar Kelimeler: *öğretmen yetiştirme, dijital veri güvenliği, veri güvenliği farkındalığı, ölçek geliştirme, açımlayıcı faktör analizi, doğrulayıcı faktör analizi*

[1]Bu çalışma Eray Yılmaz'ın "Öğretmenlerin Dijital Veri Güvenliği Farkındalığı" başlıklı doktora tezinden üretilmiştir.

AJIT-e: Online Academic Journal of Information Technology
2015 Fall/Güz – Cilt/Vol: 6 - Sayı/Num: 21
DOI: 10.5824/1309-1581.2015.4.002.x

Development of the Digital Data Security Awareness Scale

ABSTRACT *Contemporary teachers, who used to work with printed materials in the past, produce and store the information in digital environments thanks to rapid advances in information and communication technologies. The safety of the digital information processed by today's teachers carries utmost importance as they are supposed to employ current information technologies in their instructional endeavors. In this regard, the purpose of the current study has been derived from the importance of sustaining digital data security of teachers. Thus, the aim was to develop a scale to identify the digital data awareness of teachers. A comprehensive literature review followed by focus group interviews with critical partners led to an item pool of 93 statements. After the revisions of 12 field experts, the draft form was piloted with 79 teachers. An exploratory factor analysis was performed with 529 teachers to investigate the construct validity of the scale, which revealed a single-factor structure sheltering 32 items. The five-point Likert structure revealed acceptable internal consistency (α: 0.945) and variance values (36.1 %). A confirmatory factor analysis with a new sample of 335 teachers was conducted to confirm the factor structure. Through modification indices, the single factor structure reached ideal values. As the reliability and validity features of the scale were acceptable, it can be used in further research successfully.*

Keywords: *teacher education, digital data security, data security awareness, scale development, exploratory factor analysis, confirmatory factor analysis*

1. Giriş

Yeni teknolojilerin ortaya çıkması ve topluma yayılması, yaşam alışkanlıklarının değişmesine, sosyal kavramların da yeniden biçimlenmesine neden olmuştur. Bilgi toplumu olma yolundaki hızlı değişim sürecinde etkin rol oynayan bilgi ve iletişim teknolojileri; iletişim, bankacılık, elektronik imza, uzaktan eğitim, kamu hizmetleri ve e-devlet uygulamaları gibi pek çok alanda günlük deneyimlerimizi bütünüyle değiştirmeye başlamıştır. Toplumların üretim, iletişim, ulaşım, eğitim, ticaret tarzları da bu değişimden etkilenmiştir (Karakaş, 2002). Ülkemizde de bilgisayar ve mobil iletişim cihazlarının her geçen gün artarak kullanılmasının bir sonucu olarak her alanda üretilen bilgi miktarı da hızla artmaktadır.

Bilgi toplumuna dönüşüm sürecinde ekonomik ve sosyal yaşamdaki pek çok kolaylığın yanı sıra bilgi güvenliğine karşı çeşitli risk ve tehditler de ortaya çıkmaktadır. Bu teknolojileri kullanan kişilerin büyük çoğunluğu bilgi güvenliğine karşı oluşabilecek risk ve tehditlerin farkında değildir (Özenç, 2007). Oluşan bu risk ve tehditler, kişilerin çoğunlukla maddi kayba uğramalarına ya da bilgilerinin değiştirilmesi, silinmesi ya da bilgilerine izinsiz olarak erişilmesi gibi istenmeyen durumlara neden olabilmektedir.

Bilgi güvenliğinin temel unsurları; gizlilik, bütünlük ve erişilebilirliktir (Fussell, 2005; McCumber, 2005; Schlienger & Teufel, 2001). Gizlilik (Confidentiality) yetkisiz kişilerce bilgiye erişilememesi; bütünlük (Integrity) bilginin doğruluğunun ve tamlığının sağlanması, içeriğinin değiştirilmemiş, silinmemiş ya da yok edilmemiş olması; erişilebilirlik (Availability) ise yetkisi olanlar tarafından bilginin istenildiği anda kullanılabilir olmasıdır. Bu üç temel unsur, bilgi güvenliğinin birbirinden bağımsız düşünülemeyeceği bileşenleridir.

Bilgi güvenliği kavramı 1990'lı yıllara kadar olan süreçte yazılı ve basılı ortamlardaki bilgilerin daha çok fiziksel anlamda güvenliğinin sağlanması olarak ifade edilmiştir. Cep telefonu, bilgisayar ve İnternet'in günlük yaşamda etkin bir biçimde kullanılması sonrasındaki büyük dönüşüm ve bilgi transferindeki artış, bilgi güvenliğinin tanımının da değişmesine neden olmuştur. Günümüzde bilgi güvenliği kavramına bilişim teknolojileri açısından bakıldığında dijital veri güvenliği kavramı ön plana çıkmaktadır. Elektrik kesintisi ile oluşan veri kayıpları, dosyalara dışarıdan erişimin engellenmesine yönelik bilgisayarların korunması ve şifrelenmesi, gizlilik ve telif hakları gibi gerekçelerle elektronik ortamdaki dijital verilerin güvenliği önem kazanmıştır. Bu noktadan hareketle bilgi güvenliği konusunda yapılan çalışmalar dijital veri güvenliği kapsamında değerlendirilmiştir. Canbek ve Sağıroğlu (2006:168) dijital veri güvenliğini, "elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması sırasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür" biçiminde tanımlamıştır.

Bilgisayarların ve İnternet'in yoğun olarak kullanılması sonucunda yaşanan kolaylıkların yanı sıra pek çok dijital veri güvenliği sorunu da ortaya çıkmıştır. Bu sorunlardan bazıları; bilgisayar virüsleri, teknik problemler, bilgisayar hileleri, bilgi hırsızlığı, erişim yetkisini kötüye kullanma, doğal afetler nedeniyle güç kaynaklarının, kamera sistemlerinin ve telefon santrallerinin arızalanması, donanım kaynaklı sorunlar ile yazılım tehditleri olarak sıralanabilir.

Dijital veri güvenliğini tehdit eden belki de en önemli unsur insan kaynaklı tehditlerdir. Tekerek'e göre (2008) bu tehditler kullanıcının bilinçsizce ve bilgisizce, yeterli eğitime sahip olmadan teknoloji kullanması sonucu veya sisteme zarar verme amaçlı yapılan davranışlar sonucu ortaya çıkar. Canbek ve Sağıroğlu (2007:9) bilinçli olarak sisteme zarar verme noktasında ortaya çıkan ve son yıllarda sıklıkla kullanılan toplum mühendisliği kavramını, bir bilgisayar korsanının ilgilendiği bilgisayar sistemini kullanan veya yöneten meşru kullanıcılar üzerinde psikolojik ve sosyal hileler kullanarak, sisteme erişmek için gerekli bilgileri elde etme teknikleri olarak tanımlamaktadır. Dijital dünyada yaşanan olumsuzluklar ile birlikte anılan "hacker" sözcüğü ise dilimize bilgisayar korsanı olarak çevrilmiştir. Türk Dil Kurumu'na göre bilgisayar korsanı, bilgisayar ve haberleşme teknolojileri konusundaki bilgisini gizli verilere ulaşmak, ağlar üzerinde yasal olmayan zarar verici işler yapmak için kullanan kimsedir (Türk Dil Kurumu, 2015).

Bazı basit önlemler ile sanal dünyanın gerçek tehlikelerinden korunmak olanaklıdır. Bu önlemler bireysel olabileceği gibi devlet eliyle ve yasalar yoluyla da alınabilmektedir. Bilgi güvenliği konusunda yaşanabilecek sorunların hukuki boyutu incelenecek olursa, Yeni Türk Ceza Kanunu'nun 525. maddesinin (b/1) bendi; elektronik verilerin silinmesi, bozulması,

DOI: 10.5824/1309-1581.2015.4.002.x

değiştirilmesi, sistemlerin yanlış biçimde işlemesine neden olunması ya da sistemlerin işlemesine tamamen engel olunması konularına yaptırımlar getirmektedir (Dülger, 2004). 525. maddesinin (d) bendinde ise kişisel bilgilerin korunması hakkında gerekli bilgiler verilmiş, bilgisayarda bulunan özel bilgilerin kopyalanması, silinmesi veya bozulması durumunda bu işlemi yapan kişilere cezai işlem uygulanacağı belirtilmiştir (Balaman, 2013).

Bilişim teknolojilerindeki gelişmeler elbette yaşamımızı kolaylaştırmaktadır. Öte yandan bu teknolojilerin uygunsuz ve kötü amaçlı kullanılması sonucu oluşabilecek risklerin tahmin edilememesi ve tehditlerden habersiz olunması nedenleriyle dijital veri güvenliği riskleri de artmaktadır. Riskleri gidermenin ya da en aza indirmenin yolu bireyler üzerinde farkındalık oluşturmaktan geçmektedir. Bu bağlamda günlük yaşamda sıkça kullanılan farkındalık kavramını incelemek yerinde olacaktır. Acar (2004:56) farkındalığı, "bireyin tüm duyu organlarıyla, başka birey veya çevresiyle temasa geçerken neyi, nasıl yaşadığının ayırdında olması" olarak tanımlamıştır.

Alanyazın incelendiğinde bireylerin çeşitli alanlardaki farkındalıklarının belirlenmesine yönelik ölçme araçlarına gereksinim duyulduğu ve bu gereksinimi gidermeye yönelik çalışmalar gerçekleştirildiği söylenebilir (Güven & Aydoğdu, 2012; Kuzucu, 2008; Özyeşil, Arslan, Kesici & Deniz, 2011; Sargın, 2010). Bilgi ve iletişim teknolojilerindeki gelişmeler ve bu teknolojilerin yoğun kullanımı dikkate alındığında, bireylerin dijital veri güvenliği konusundaki farkındalıkları da bir başka çalışma alanını oluşturmuştur.

Dijital veri güvenliği konusunda yapılan, hedef kitlesi öğrenci ve öğretmen olan yurt dışındaki çalışmaların 2000'li yılların başından bu yana sürdüğü görülmektedir. Bu araştırmalar arasında en dikkat çekici olanı 2000-2009 yılları arasındaki 10 yıllık süreçte Tayvan'daki ilkokul ve ortaokul öğretmenlerine yönelik olarak geliştirilen İnternet Güvenliğinde Öğretmen Farkındalığı (Teacher Awareness of Internet Safety-TAIS) projesidir. Projede; eğitim seminerleri, atölye çalışmaları, konferanslar gibi çok çeşitli etkinlikler yer almıştır. Ayrıca 7/24 hizmet veren e-Öğretmen web sitesi sayesinde; çevrimiçi öğretmen-öğrenme toplulukları kurulmasına yardımcı olunmuş, öğretim programına uygun güvenli içerikler ve öğretmenlerin sınıflarında kullanabileceği üniteler sunulmuştur (Chou & Peng, 2011).

Yurt içindeki çalışmalarda ise çoğunlukla katılımcı görüşüne dayalı olarak anket veya ölçek ile veri toplandığı görülmektedir. Bilgi güvenliği farkındalığı temalı çalışmalardan birinde Mart (2012) geliştirdiği anketi, farklı meslek gruplarından 157'si öğretmen 501 katılımcıya uygulamış, öğretmenlerin farkındalık düzeylerinin diğer meslek gruplarından farklı olmadığı sonucuna ulaşmıştır. Benzer bir çalışmada MEB Bilgi İşlem Dairesi Başkanlığı (2012) tarafından 7484 katılımcıya yine anket uygulanmış ve MEB personelinin bilgi güvenliği farkındalık düzeyleri ölçülmüştür. Alanyazın incelendiğinde, pek çok ölçme aracı bulunmasına rağmen doğrudan öğretmenlerin dijital veri güvenliği farkındalıklarına yönelik bir ölçme aracının bulunmadığı ve bu konuda bir ihtiyaç olduğu görülmektedir.

Öğretmenlerin özlük işlemleri elektronik ortamda MEBBİS (Milli Eğitim Bakanlığı Bilişim Sistemleri) üzerinden yürütülmekte ve eğitim sisteminin tamamına ait verileri de e-Okul sisteminde yer almaktadır. Aynı zamanda öğretmenler; özlük işlemlerini yürütme, sınav

sorusu hazırlama, ders içeriklerini elektronik ortama aktarma gibi etkinliklerinde bilgisayarı ve İnternet'i yoğun olarak kullanmaktadır. Üzerinde durulması gereken bir başka nokta ise MEB tarafından eğitimde teknoloji entegrasyonu üzerine hayata geçirilmiş büyük ölçekli projelerdir. İki büyük projeden ilki olan MEGP (Milli Eğitimi Geliştirme Projesi) kapsamında açılan kurslar ile yürütülen hizmet içi eğitim etkinlikleri arasında öğretmenlerin dijital veri güvenliğine yönelik farkındalıkları ile ilgili bir eğitim başlığı bulunmamaktadır. Bir diğer proje ise halen yürütülmekte olan Fırsatları Arttırma ve Teknolojiyi İyileştirme Hareketi'dir (FATİH). Eğitim ve öğretimde fırsat eşitliğini sağlamak ve okullardaki teknolojiyi iyileştirmek amacıyla bilişim teknolojileri araçlarının öğrenme-öğretme sürecinde daha çok duyu organına hitap edilecek biçimde ve etkin kullanımını sağlamayı amaçlayan bu proje (FATİH Projesi, 2012), dijital veri üzerine kurgulanmıştır ve proje için dijital veri güvenliği son derece önemlidir.

MEB tarafından son yıllarda uygulamaya konulan büyük ölçekli projelerdeki öğretmen eğitimleri ve yürütülen hizmetiçi eğitim etkinlikleri incelendiğinde dijital veri güvenliği konusuna yer verilmediği görülmektedir. Öğretmenlerin bu konudaki farkındalıklarının ortaya konmasına yönelik bir ölçme aracının geliştirilmesi bu çalışmayı önemli kılmaktadır. Bu bağlamda bu araştırmanın amacı, öğretmenlerin dijital veri güvenliği konusundaki farkındalıklarının belirlenmesine yönelik geçerli ve güvenilir bir ölçek geliştirmektir.

2. Yöntem

Çalışma Grubu

Madde havuzunun oluşturulması aşamasında altışar kişilik gruplarla üç odak grup oturumu gerçekleştirilerek kritik paydaşların görüşüne başvurulmuştur. 18 katılımcıdan oluşan bu çalışma grubunun çeşitliliğini ideal bir düzeye çıkarabilmek için; cinsiyet, mesleki deneyim, öğrenim kademesi ve görev türü değişkenleri dikkate alınmıştır. Çalışmaya gönüllü olarak katılmayı kabul eden bu katılımcılardan 12'si Balıkesir ilinin farklı ilçelerinde görev yapan öğretmenlerden, diğerleri ise Anadolu Üniversitesi'nde görev yapan öğretim elemanlarından oluşmuştur. Ölçek geliştirme sürecinde ön deneme uygulaması için 79, açımlayıcı faktör analizi (AFA) için 529 ve doğrulayıcı faktör analizi (DFA) için 327 olmak üzere toplam 935 öğretmene ulaşılmıştır.

Dijital Veri Güvenliği Farkındalık Ölçeğinin (DVFÖ) Geliştirilmesi

Önceden geliştirilmiş bir ölçek ile bireyin tepkilerine göre ilgili psikolojik özelliğin ne derece var olduğu ortaya konmaya çalışılırken; ölçek geliştirmede ise amaç, o psikolojik özelliğin ne olduğunu belirleyecek maddelerin yapılandırılmasıdır (Erkuş, 2014). Bu nedenle öğretmenlerin dijital veri güvenliği konusundaki farkındalıklarını ölçmeye yönelik olarak hazırlanan ölçeğin hazırlık aşamasında ilk olarak madde havuzu oluşturulmuştur.

Madde Havuzunun Oluşturulması

Odak grup oturumları sonrasında 74 madde ortaya konmuştur. Bununla birlikte ilgili alanyazında yer alan İnternet'te, sosyal ağlarda ve e-devlet uygulamalarında güvenlik, bilgi güvenliği ve bilişim suçları konulu çalışmalardan yararlanılarak 16 madde daha yazılmıştır

DOI: 10.5824/1309-1581.2015.4.002.x

(Karakoç, 2011; Ketizmen & Ülküderner, 2007; Mart, 2012; Tekerek & Tekerek, 2013; Yavanoğlu, Sağıroğlu & Çolak, 2012). Tüm maddeler dikkatle incelendikten sonra ölçekte yer alması gerektiği düşünülen 3 madde de araştırmacılar tarafından eklenmiştir. Böylece ölçeğin hedef kitlesinden seçilen kritik paydaşların görüşleri ve alanyazında dijital veri güvenliği kapsamında yapılmış çalışmalar dikkate alınarak 93 maddeye ulaşılmıştır.

Kapsam ve Görünüş Geçerliği İçin Uzman Görüşlerinin Alınması

Maddelerin, ölçülmek istenen davranışı (özelliği) ölçmede nicelik ve nitelik olarak yeterli olup olmadığının göstergesi kapsam geçerliğidir (Büyüköztürk, 2009). Madde havuzunda yer alan maddelerin dijital veri güvenliği farkındalığını ölçmedeki yeterliliğini ve kapsama uygunluğunu belirlemek amacıyla 12 alan uzmanından madde görüş formu kullanılarak uzman görüşü alınmış ve maddeleri "uygun değil", "kısmen uygun" ve "tamamen uygun" biçiminde değerlendirmeleri istenmiştir. Uzman görüşleri doğrultusunda 32 madde, havuzdan çıkartılmış, 24 madde yeniden düzenlenmiş ve 1 öneri maddesi de eklenerek 62 madde elde edilmiştir.

Yazılan tüm maddeler, alanında doktora derecesine sahip, lisede görevli bir edebiyat öğretmeni ile lisans mezunu, ortaokulda görevli bir Türkçe öğretmeni tarafından Türkçe dil uygunluğunun değerlendirilmesi amacıyla incelenmiştir. Uzmanlar tarafından maddeler üzerinde imla, noktalama, dil, anlam ve anlatıma ilişkin gerekli düzenlemeler yapılmıştır.

Taslak ölçek için amaca ilişkin açıklamaları ve katılımcılardan beklenenleri yansıtan bir yönerge hazırlanmıştır. Farkındalık ifadeleri beşli Likert dereceleme ile ölçeklendirilmiştir. Likert tipindeki derecelemeler; "Kesinlikle Katılıyorum (5)", "Katılıyorum (4)", "Kararsızım (3)", "Katılmıyorum (2)", "Kesinlikle Katılmıyorum (1)" biçimindedir. Ölçekten elde edilen toplam puan arttıkça dijital veri güvenliği farkındalığı da artmaktadır. Ölçekteki tüm maddeler olumlu ifadeler içermektedir.

Ön denemeye hazır hale getirilen taslak ölçek, ölçek geliştirme konusunda deneyimli doktora derecesine sahip iki öğretim üyesi tarafından değerlendirilmiştir. Tüm bu süreçte uzman görüşleri doğrultusunda maddeler; farkındalık ifadesi olup olmadığı, maddelerin ifade ediliş biçimi, çalışmanın amacına uygunluğu ve kapsam geçerliği bakımından değerlendirilmiştir.

Ön Deneme Uygulamasının Gerçekleştirilmesi

Ölçek geliştirme sürecindeki deneme uygulamasında örneklem, yalnızca ölçülen özelliğin kapsamını temsil etmeli, heterojen olmalı ve kesinlikle gönüllü katılımcılardan oluşmalıdır (Erkuş, 2014). Buna göre ön denemeye hazır hale getirilen taslak ölçek ile ilkokul, ortaokul ve lise düzeyinde birer okulda gönüllü öğretmenlerle uygulama yapılmıştır. Karasar (1995), bir ölçeğin geliştirilmesi aşamasında yapılacak ön deneme için katılımcı sayısının 50'den az olmaması gerektiğini belirtmektedir. Buna göre, Balıkesir İli Karesi İlçesindeki 23 Nisan İlkokulu'nda görevli 23 sınıf öğretmeni, Karahallılar Ortaokulu'nda görevli 22 branş öğretmeni ve T.C. Ziraat Bankası Balıkesir Fen Lisesi'nde görevli 34 branş öğretmeni olmak üzere toplam 79 katılımcı ile ölçeğin ön deneme uygulaması gerçekleştirilmiştir. Ölçeğin ortalama yanıtlama süresi 10 dakika olarak belirlenmiştir. Uygulama sonunda boş bırakılan

ve anlaşılamayan altı madde çıkartılmıştır. Yapı geçerliğini test etmek için örnekleme uygulanacak taslak ölçeğin son halinde 56 madde yer almıştır.

Verilerin Toplanması

Nitel verilerin toplanması sürecinde öncelikle uygulama için Balıkesir İl Milli Eğitim Müdürlüğü Araştırma Değerlendirme Komisyonu'ndan gerekli izinler alınmıştır. Öğretmenlerden oluşan iki odak grup oturumu için katılımcılar, araştırmacının görevli olduğu okula davet edilmiş ve kendilerini rahat hissedecekleri bir ortamda görüşmeler yapılmıştır. Üniversitede görevli katılımcılar ile yapılan odak grup oturumu ise görevli oldukları üniversitede uygun bir ortamda gerçekleştirilmiştir. Görüşmeler öncesinde katılımcılara sunulan görüşme onay formu ile izinleri alınmıştır. Görüşmelerden ilki 54 dakika, ikincisi 84 dakika ve son görüşme 48 dakika sürmüştür. Görüşmeler ses kayıt cihazı ile kayıt altına alınmış ve sonrasında elektronik ortama aktarılmıştır.

56 maddelik taslak ölçeğin AFA uygulaması için farklı türden 18 okul maksimum çeşitlilik örnekleme yöntemine göre belirlenmiştir. Çeşitliliği maksimum düzeye çıkarabilmek için; okulun bulunduğu yerleşim yeri, öğrenim kademesi, okul türü ve resmi/özel okul olma durumları dikkate alınmıştır. Araştırmacı tarafından okulların eğitim yöneticilerine bırakılan veri toplama araçları 10 günlük süreden sonra geri toplanmıştır. Örneklemde yer alan 844 öğretmenden dönen veri toplama aracı sayısı 541'dir (% 64). Bunlardan 12 tanesi (% 2) uygun biçimde doldurulmadığından değerlendirmeye alınmamıştır. Analiz 529 veri toplama aracı ile gerçekleştirilmiştir.

AFA sonrasında 32 maddelik ölçeğin DFA uygulaması için farklı türden 13 okul yine maksimum çeşitlilik örnekleme yöntemine göre belirlenmiştir. Araştırmacı tarafından okulların eğitim yöneticilerine bırakılan veri toplama araçları bir haftalık süreden sonra geri toplanmıştır. Örneklemde yer alan 519 öğretmenden dönen veri toplama aracı sayısı 335'tir (% 65). Bunlardan 8 tanesi (% 2) uygun biçimde doldurulmadığından değerlendirmeye alınmamıştır. Analiz 327 veri toplama aracı ile gerçekleştirilmiştir.

Verilerin Analizi

Odak grup görüşmelerinden elde edilen nitel veriler üzerinde içerik analizi gerçekleştirilmiştir. Yıldırım ve Şimşek'e göre (2013) bu analizde temel amaç, verileri açıklayabilecek kavramlara ve ilişkilere ulaşmak için, birbirine benzer olan verileri bir araya getirerek yorumlamaktır. Buna göre, katılımcıların görüşlerini ifade ederken kullandıkları cümleler analiz birimi olarak seçilmiştir. Cümleler analiz edildikten sonra katılımcı görüşleri bir araya getirilerek üç alan uzmanı ile birlikte temalar belirlenmiştir.

Ölçeğin yapı geçerliğini incelemek için SPSS 18.0 yazılımı kullanılarak AFA yapılmıştır. Tavşancıl'a göre (2006) faktör analizi, her bir madde ile yanıtlayıcıların verdiği tepkiler arasındaki düzeni ortaya koymada ve psikolojik boyutların içeriğini tanımlamada kullanılan çok değişkenli analiz tekniklerinden biridir.

AFA sonucunda ortaya konan faktör yapısını doğrulamak için LISREL 8.7 programı kullanılarak DFA yapılmıştır. Çokluk, Şekercioğlu ve Büyüköztürk'e göre (2012) bu analiz

DOI: 10.5824/1309-1581.2015.4.002.x

sayesinde daha önceden tanımlanmış ve sınırlandırılmış bir yapının, bir model olarak doğrulanıp doğrulanmadığı test edilmektedir.

3. Bulgular

Odak Grup Görüşmeleri

Gerçekleştirilen odak grup görüşmeleri sonrasında18 katılımcı, kendilerine yöneltilen sorulara ilişkin 10 farklı tema altında 477 adet görüş bildirmiştir. Benzer olmalarına ve dijital veri güvenliği ile ilgili olma durumlarına göre düzenlenen ve geliştirilen ölçeğe alt yapı oluşturan bu maddelerin temalara göre dağılımı Tablo 1'de verilmiştir.

Tablo 1. Maddelerin Temalara Göre Dağılımı

Tema Adı	Madde Sayısı
Bilişim cihazlarında veri güvenliği	18
Parola güvenliği	12
Verilerin saklanması, yedeklenmesi ve taşınması	6
Bilgisayar ağlarında ve modemlerde veri güvenliği	7
e-devlet uygulamalarında veri güvenliği	4
Sosyal paylaşım ağlarında veri güvenliği	5
e-posta kullanımında veri güvenliği	5
İnternet bankacılığı ve çevrimiçi alışverişte veri güvenliği	9
Veri güvenliğinde hukuki boyut	3
Lisanslı yazılımlar ve telif hakları	5
Toplam	74

Tablo 1'e göre, öğretmenlerin dijital veri güvenliği farkındalıklarını belirlemeye yönelik geliştirilen ölçeğe alt yapı oluşturan 74 maddenin 10 farklı tema altında toplandığı görülmektedir.

Ölçeğin Geçerlik ve Güvenirlik Analizleri

Açımlayıcı Faktör Analizi

Faktör analizi öncesinde 56 maddelik taslak ölçek üzerinde madde istatistikleri hesaplanmıştır. Buna göre 1. ve 8. maddelerin madde toplam korelasyonlarının .40'tan küçük olduğu görülmüştür. Aynı zamanda çıkarıldıklarında Cronbach Alfa (α) değeri de yükselmektedir. Beklenen sınırlarda yer almayan bu iki madde analizden çıkartılmıştır.

AFA 529 katılımcıya ait veri toplama aracı ile gerçekleştirilmiştir. Örneklem büyüklüğü konusunda Comrey ve Lee (1992), 100 katılımcının yetersiz, 200'ün ortalama, 300'ün iyi, 500'ün çok iyi ve 1000 katılımcının ise mükemmel olduğunu belirtmektedir (akt. Akbulut, 2010). Toplanan verilerin faktör analizine uygunluğu Kaiser-Meyer-Olkin (KMO) ve Barlett Küresellik testi ile sınanmıştır.

Örneklem büyüklüğünün uygunluğu KMO ve Barlett istatistiği ile onaylanmıştır (KMO=.951, X^2 =15113.267, p<.001). KMO değerinin eşik değerolan .600'den büyük olması ve Barlett-Küresellik testi için bulunan X^2 değerinin anlamlı olması nedeniyle örneklemin faktör analizine uygun olduğu söylenebilir (Cohen, Manion & Morrison, 2007).

Faktör yapısını ortaya koyabilmek için SPSS 18.0ile AFA yapılmıştır ve Maksimum Olabilirlik yöntemi kullanılmıştır. Bu yöntem Stevens'a göre (1996) ölçek geliştirme çalışmalarında faktörler altında gerçekten işe yarayan ortak varyansı dikkate alır ve düşük varyansa karşı daha sağlam bir yapı sunar.

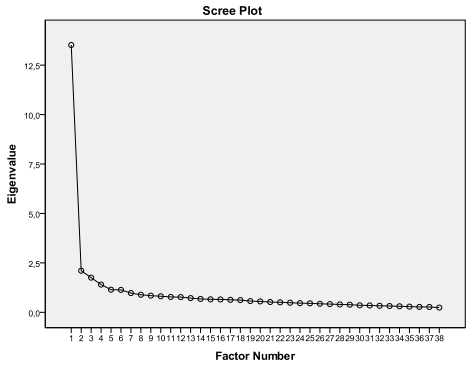
54 maddeden oluşan veri seti üzerinde döndürme (rotation) yapılmamış, maksimum olabilirlik analizinde özdeğeri 1'den büyük olan dokuz boyut ile toplam varyansın % 50.167'sinin açıklandığı görülmüştür. Ancak özdeğeri 1'den büyük dokuz faktör görünse de, ideal faktör yapısının belirlenebilmesi için döndürme yapılmıştır. Döndürme işlemlerinde "varimax" yöntemi tercih edilmiştir. Tavşancıl (2006), varimax yönteminde basit yapıya ve anlamlı faktörlere ulaşmada faktör yükleri matrisinin sütunlarına öncelik verildiğini ve daha az değişkenle faktör varyanslarının en yüksek olması sağlanacak şekilde döndürme yapıldığını belirtmektedir. Farklı denemelerden sonra madde istatistikleri incelenmiş ve beklenen sınırlarda yer alamayan 17 madde çıkartılarak yeniden AFA yapılmıştır.

Analiz başlangıcında 39 madde olmasına karşın 1. maddenin madde toplam korelasyonu .40'tan küçük ve ortak faktör varyansı da .30'dan küçüktür. Atıldığında Cronbach Alfa (α) değeri yükselmektedir. Bu madde çıkartılarak 38 madde ile AFA yapılmıştır. Analiz sonucunda elde edilen değerler Tablo 2'de, yamaç birikinti grafiği ise Şekil 1'de verilmiştir.

Tablo 2. Toplam Açıklanan Varyans

Bileşen	Başlangıç Özdeğerleri			Yük Değerleri		
	Toplam	Varyans (%)	Birikimli (%)	Toplam	Varyans (%)	Birikimli (%)
1	13.517	35.571	35.571	12.988	34.179	34.179
2	2.105	5.539	41.110	1.578	4.153	38.332
3	1.753	4.613	45.723	1.219	3.208	41.540
4	1.403	3.691	49.414	.925	2.434	43.974
5	1.145	3.014	52.428	.664	1.747	45.721
6	1.134	2.985	55.414	.642	1.691	47.411
7	.972	2.558	57.971			
8	.888	2.338	60.309			
9	.843	2.218	62.527			
10	.813	2.140	64.667			
…	…	…	…			

DOI: 10.5824/1309-1581.2015.4.002.x



Şekil 1. Yamaç-Birikinti Grafiği

Tablo 2'deözdeğeri 1'den büyük altı faktör görünse de birinci faktöre ait özdeğer, ikinci faktöre ait özdeğerin yaklaşık sekiz katıdır. Aynı zamanda Şekil 1 incelendiğinde, birinci faktöre ait özdeğerden sonra hızlı bir düşüş görülmektedir ve ikinci faktörden itibaren toplam varyansa katkı azalmaktadır. Çokluk, Şekercioğlu ve Büyüköztürk (2012) bu tür durumlarda faktör sayısının "1" olarak belirlenmesine karar verilebileceğini belirtmiştir.

Büyüköztürk'e göre (2009) faktör yük değerlerinin.45 ya da daha yüksek olması seçim için iyi bir ölçüdür. Pek çok araştırmada bu değer .50 olarak kabul edilmiştir (Demir & Akengin, 2010; Ursavaş, Şahin & McIlroy, 2014). Bu araştırmada da madde faktör yük değerlerinin alt kesme noktası .50 olarak belirlenmiştir. Tek faktöre göre yapılan analizde faktör yük değerleri .50'nin altında olan altı madde ölçekten çıkartılmıştır.

AFA sonucunda 32 maddeden oluşan tek faktörlü DVGFÖ'nün toplam açıklanan varyans oranı % 36.053 olarak bulunmuştur. Büyüköztürk (2009) tek faktörlü desenlerde açıklanan varyansın % 30 ve üzerinde olmasının yeterli görülebileceğini ifade etmiştir. Buna göre ortaya konulan tek faktörün, açıklanan varyansa katkısının yeterli olduğu söylenebilir. Ölçeğin tek faktörlü yapısına ilişkin yük değerleri Tablo 3'te verilmiştir.

Tablo 3. Maddelerin Faktör Yük Değerleri

Madde	Faktör Yükü	Madde	Faktör Yükü	Madde	Faktör Yükü
M37	.689	M25	.625	M10	.566
M49	.688	M56	.621	M18	.565
M41	.677	M53	.600	M16	.560
M52	.664	M51	.597	M28	.557
M43	.663	M19	.592	M40	.554
M50	.662	M35	.591	M29	.536
M24	.642	M54	.588	M39	.531
M26	.640	M32	.587	M6	.512
M42	.637	M22	.583	M9	.510
M31	.633	M27	.571	M30	.506
M45	.627	M11	.568		

Tablo 3'egöre, maddelerin faktör yükleri .506 - .689 arasında değişmektedir ve Cronbach Alfa (α) iç tutarlılık katsayısı .945'tir. Bu değer Kalaycı'nın (2009) önerdiği yüksek güvenilirlik sınırı olan .80'in üzerindedir. Buna göre ölçüm sonuçlarının yüksek derecede güvenilir olduğu söylenebilir. Benzer konularda gerçekleştirilen çalışmalarda Cronbach Alfa (α) katsayıları; Dönmez ve diğerlerinin (2014) geliştirdiği Öğretmen Adaylarının Algılanan İnternet Riskleri Ölçeği'nde .856, Tekerek ve Tekerek (2013) tarafından geliştirilen Bilgi Güvenliği Farkındalığı Ölçeği'nde .720 ve Mart'ın (2012) geliştirdiği Bilgi Güvenliği Farkındalığı Belirleme Anketi'nde .638 olarak hesaplanmıştır.

Tablo 4. Madde-Toplam Korelasyonu

Madde	Korelasyon Katsayısı	Madde	Korelasyon Katsayısı	Madde	Korelasyon Katsayısı
M6	.512	M27	.552	M42	.623
M9	.488	M28	.533	M43	.639
M10	.553	M29	.515	M45	.603
M11	.558	M30	.483	M49	.668
M16	.560	M31	.620	M50	.643
M18	.557	M32	.563	M51	.568
M19	.583	M35	.561	M52	.644
M22	.564	M37	.671	M53	.575
M24	.624	M39	.511	M54	.582
M25	.605	M40	.535	M56	.604
M26	.628	M41	.664		

Tablo 4'teki madde analizi sonuçları incelendiğinde madde toplam korelasyonu değerlerinin .483 ile .671 arasında değiştiği gözlenmektedir. Büyüköztürk'e göre (2009) bu değerin .40'tan büyük olması çok iyi derecede bir madde olduğunun göstergesidir. Buradan hareketle ölçek maddelerinin ayırt edici, güvenirliği yüksek ve benzer davranışı ölçmeye yönelik olduğu söylenebilir.

Doğrulayıcı Faktör Analizi

Açımlayıcı faktör analizinde, değişkenler arasındaki ilişkilerden yola çıkılarak faktör bulma ve kuram üretmeye yönelik bir işlem; doğrulayıcı faktör analizinde ise değişkenler arasındaki ilişkiye dair daha önce belirlenen bir yapının test edilmesi söz konusudur (Stevens, 1996; Tabachnick & Fidell, 2001).

DOI: 10.5824/1309-1581.2015.4.002.x

AFA sonucunda elde edilen modelin uygunluğu LISREL 8.7 yazılımı kullanılarak DFA (Confirmatory Factor Analysis) ile incelenmiştir. Alanyazın bu analiz sonucunda uygun modelin belirleyicisi olarak χ^2, RMSEA, CFI ve GFI ölçütlerini işaret etmektedir (Brown, 2006; Tabachnick & Fidell, 2001). Buna göre elde edilen modelin uygunluğu; Ortalama Hataların Karekökü (Root Mean Square Error of Approximation; RMSEA), Karşılaştırmalı Uygunluk İndeksi (Comparative Fit Index; CFI) ve Uygunluk İndeksi (Goodness of Fit Index; GFI) ölçütleri ile sınanmıştır. Analiz sonuçları Tablo 5'te verilmiştir.

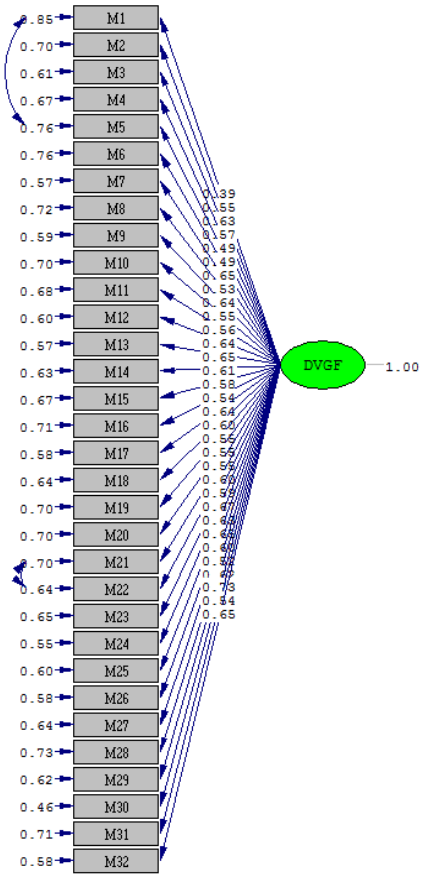
Tablo5. Doğrulayıcı Faktör Analizinin Değerlendirilmesi

Uyum İndeksi	Değer	Değerlendirme
χ^2	1801.58	-
sd	462	-
p	.000	-
χ^2/sd	3.90	Orta düzeyde uyum
RMSEA	.09	Zayıf uyum
SRMR	.07	İyi uyum
NFI	.93	İyi uyum
NNFI	.95	İyi uyum
CFI	.95	İyi uyum
GFI	.74	İyi uyuma yakın
AGFI	.71	İyi uyuma yakın

Tablo 5'teki uyum indekslerine göre beklenen ve gözlenen kovaryans matrisleri arasındaki fark anlamlıdır (χ^2 (462):1801.58; p<.01). p değerinin kritik değer bağlamında >.05 olması beklenmektedir, ancak birçok doğrulayıcı faktör analizi çalışmasında bu değer örneklem büyüklüğüne bağlı olarak anlamlı çıkmaktadır (Çokluk, Şekercioğlu & Büyüköztürk, 2012). χ^2/sd değeri 3.90 olarak hesaplanmıştır. Bu değer Sümer'e göre (2000) orta düzeyde uyum anlamına gelmektedir.

Modelin uygunluğuna ilişkin RMSEA değerinin sıfıra yaklaşması uygun modelin habercisi olarak kabul edilmektedir (Steiger, 2007). Araştırmada bu değer .09 olarak bulunmuştur ve kabul edilebilir uyumun biraz altındadır (Kelloway, 1999; Tabachnick & Fidell, 2001). SRMR değerinin .07 olması ise iyi uyum anlamına gelmektedir (Brown, 2006; Hu & Bentler,1999). NFI değeri .93, benzer şekilde NNFI değeri de .95'tir ve bu değerlerin iyi uyuma işaret ettiği görülmektedir (Kelloway, 1989; Schumacher & Lomax, 1996; Sümer, 2000; Tabachnick & Fidell, 2001; Thompson, 2004). Bir diğer ölçüt olan CFI değeri .95 olarak hesaplanmıştır ve farklı kaynaklara göre iyi uyumun göstergesidir (Hu & Bentler, 1999; Sümer, 2000; Tabachnick & Fidell, 2001). GFI değeri .74 ve AGFI değeri de .71 hesaplanmıştır. AGFI ve GFI değerlerinin .90'a yaklaşması nedeniyle bu iki değerin iyi uyuma yakın olduğu söylenebilir.

İncelenen göstergeler tek boyuttan oluşan ölçme modelinin iyi uyuma sahip olduğunu ortaya koymuştur. Bu modelin elde edilmesinde hata kovaryansları eklenerek M1-M5 ve M21-M22 maddeleri ilişkilendirilmiştir. Modele ilişkin diyagram (path diagram) Şekil 2'de verilmiştir.



χ^2=1801.58, df=462, RMSEA=0.094

Şekil 2. Yapısal Eşitlik Modeline İlişkin Diyagram

Şekil 2'de her bir maddenin hata varyansı ve korelasyon katsayıları verilmiştir. Maddelere ilişkin korelasyon katsayılarının .39 ile .73 arasında değiştiği görülmektedir. Bununla birlikte ölçekte yer alan tüm maddelerin t değerleri p<.01 düzeyinde anlamlıdır (t>2.56).

4. Sonuç

Dijital veri güvenliğine yönelik olası zararların ve yaşanabilecek sorunların hukuki boyutlarının bilinmesi, öğretmenlerin dijital veri güvenliği farkındalıklarının ortaya konması ve gereksinimlere uygun olarak gerçekleştirilecek eğitimler yoluyla kolaylaştırılabilir. Erkuş'un da (2014) belirttiği gibi psikolojik bir değişkenin ölçülmesi bir gereksinimden kaynaklanmaktadır. Bu araştırmada öğretmenlerin dijital veri güvenliğine yönelik farkındalıklarının belirlenmesi amacıyla bir ölçek geliştirilmiştir. Böylece öğretmenlerin eğitim öğretim etkinliklerinde bilişim teknolojilerini kullanırken dikkat etmeleri gereken noktalardan biri olan dijital veri güvenliğine yönelik farkındalıklarını ortaya çıkaracak önemli bir veri toplama aracı alanyazına kazandırılmıştır.

DOI: 10.5824/1309-1581.2015.4.002.x

Geliştirilen ölçeğin madde havuzu oluşturulması aşamasında, kritik paydaşlardan olan öğretmenler ile bilişim teknolojileri alanında görev yapan öğretim üyelerinin ve araştırma görevlilerinin görüşleri alınmıştır. Böylece ölçeğin güncel alanyazını, uygulamaları ve paydaş algılarını daha iyi yansıtması sağlanmıştır.

Yapı geçerliliğini test etmek üzere gerek açımlayıcı gerekse doğrulayıcı faktör analizlerine başvurulmuş, her bir analiz için farklı ve maksimum çeşitlilik gösteren kalabalık örneklemlerden veri toplanmıştır. Böylece ölçeğin güncelliğinin yanı sıra Türkiye genelindeki farklı öğretmen örneklemleri ile rahatlıkla ve güvenilir bir biçimde uygulanabilir olması hedeflenmiştir.

Özetle; alanyazın taraması, paydaş görüşleri, örneklem çeşitliliği ve farklı örneklemlerle gerçekleştirilen faktör analizleri sonucunda güncel, geçerli ve güvenilir bir dijital veri güvenliği farkındalığı ölçeği ortaya konmuştur. Öte yandan süreç içerisinde bireylerin bilişim teknolojilerini kullanım alışkanlıklarının, tutum ve davranışlarının değişebileceği düşünüldüğünde geliştirilen tüm ölçekler gibi bu ölçeğin de uzun vadede güncel gereksinimlere yanıt veremeyebileceği göz önünde bulundurulmalıdır.

Bu araştırmanın örneklemi öğretmenlerden oluşturulmuş ve ortaya konulan ölçek bu meslek grubuna yönelik olarak geliştirilmiştir. Diğer meslek gruplarına yönelik örneklemler oluşturulabileceği gibi öğrenciler için de ilgili ölçeğin yeniden yapı geçerliği ve güvenirlik çalışmalarının yapılması önerilmektedir.

EK - Dijital Veri Güvenliği Farkındalığı Ölçeği (DVGFÖ)

No	Dijital Veri Güvenliği Farkındalığı	Katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Katılmıyorum
1	Zararlı yazılımlar (virüs, solucan, truva atı vb.) konusunda bilgi sahibiyim.	□	□	□	□	□
2	Parola oluştururken harf, sayı ve özel karakter kullanmanın önemini bilirim.	□	□	□	□	□
3	Farklı işlemler için farklı parola kullanmanın önemini bilirim.	□	□	□	□	□
4	İzinsiz kullanılmaması için dosyalara parola konulabileceğinin farkındayım.	□	□	□	□	□
5	Güvenlik duvarı yazılımları konusunda bilgi sahibiyim.	□	□	□	□	□
6	Flash bellekleri, veri saklamak yerine sadece veri taşımak için kullanmanın farkını bilirim.	□	□	□	□	□
7	İşletim sisteminin (Windows, Android vb.) güncel olmasına dikkat ederim.	□	□	□	□	□
8	E-posta ile gelen kimlik bilgilerini doğrulama mesajlarına (parola, kredi kartı vb.) itibar edilmemesi gerektiğini bilirim.	□	□	□	□	□
9	Taşınabilir depolama birimlerini (Flash bellek, taşınabilir sabit disk)	□	□	□	□	□

	kullanmadan önce virüs taraması yapılması gerektiğini bilirim.					
10	Güvenli olmadığını düşündüğüm e-postaları açmadan silmeye dikkat ederim.	□	□	□	□	□
11	Programların, üreticinin kendi sitesinden indirilmesinin önemini bilirim.	□	□	□	□	□
12	Antivirüs yazılımı kullanmanın önemini bilirim.	□	□	□	□	□
13	Parola hatırlatmak için kullanılan güvenlik sorularına başkalarının tahmin edemeyeceği cevaplar verilmesi gerektiğini bilirim.	□	□	□	□	□
14	Parola oluştururken karakter sayısının fazla olmasının önemini bilirim.	□	□	□	□	□
15	Parolaların herhangi bir ortamda saklanmasının güvenlik riski oluşturacağının farkındayım.	□	□	□	□	□
16	Verilerin, çeşitli uygulamalar (dropbox, google drive vb.) kullanılarak İnternet ortamında saklanabileceğini bilirim.	□	□	□	□	□
17	Üzerinde çalışma yapılan dosyaların birden fazla ortamda yedeklenmesi gerektiğini bilirim.	□	□	□	□	□
18	Başkalarının tahmin edemeyeceği parolalar oluşturmaya dikkat ederim.	□	□	□	□	□
19	İnternet adres çubuğunda yanlış yönlendirme olup olmadığına dikkat ederim.	□	□	□	□	□
20	Taşınabilir depolama birimlerini (Flash bellek, taşınabilir sabit disk) "Donanımı Güvenle Kaldır" seçeneğini kullanarak çıkartmaya dikkat ederim.	□	□	□	□	□
21	Karmaşık yapıdaki parolaların kırılabileceğini bilirim.	□	□	□	□	□
22	Parolaların belirli aralıklarla değiştirilmesi gerektiğinin farkındayım.	□	□	□	□	□
23	Almak istemediğim çöp e-postaları "spam/gereksiz/önemsiz" olarak işaretlemeye dikkat ederim.	□	□	□	□	□
24	İzinsiz kullanılmaması için cihazlara (akıllı telefon, tablet, bilgisayar vb.) parola konulabileceğinin farkındayım.	□	□	□	□	□
25	Kendime ait olmayan cihazlarda, parola gerektiren işlemler yapmamaya dikkat ederim.	□	□	□	□	□
26	İşletim sisteminin (Windows, Android vb.) güvenlikle ilgili uyarılarını dikkate alırım.	□	□	□	□	□
27	Elektrik kesintisine karşı dizüstü bilgisayarları bataryası ile kullanmanın önemini bilirim.	□	□	□	□	□
28	Cep telefonuna gelen tek kullanımlık parola ile yapılan giriş işlemlerinin, güvenliği arttırdığını bilirim.	□	□	□	□	□
29	Sanal klavye kullanmanın önemini bilirim.	□	□	□	□	□

DOI: 10.5824/1309-1581.2015.4.002.x

30	İnternet sitelerinde kullanıcı oturumunu kapatırken "güvenli çıkış" bağlantısını kullanmanın önemini bilirim.	□	□	□	□	□
31	İnternet sitelerinde kullanılan güvenlik sertifikaları hakkında bilgi sahibiyim.	□	□	□	□	□
32	Lisanslı olmayan yazılımların güvenlik açıkları oluşturabileceğinin farkındayım.	□	□	□	□	□

5. Kaynakça

Acar, N. V. (2004). Ne kadar farkındayım: Gestalt terapi (2. Baskı). Ankara: Babil Yayınevi.

Akbulut, Y. (2010). Sosyal bilimlerde SPSS uygulamaları: Sık kullanılan istatistiksel analizler ve açıklamalı SPSS çözümleri. İstanbul: İdeal Kültür ve Yayıncılık.

Balaman, Y. (2013). Ortaöğretim bilgi ve iletişim teknolojisi ders kitabı. Ankara: Fırat Yayıncılık.

Brown, T. A. (2006). Confirmatory factor analysis for applied research. New York: Guilford Press.

Büyüköztürk, Ş. (2009). Sosyal bilimler için veri analizi el kitabı (9. Baskı). Ankara: Pegem Akademi.

Canbek, G., & Sağıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. Politeknik Dergisi, 9(3), 165-174.

Canbek, G., & Sağıroğlu, Ş. (2007). Bilgisayar sistemlerine yapılan saldırılar ve türleri: Bir inceleme. Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 23(1-2), 1-12.

Chou, C., & Peng, H. (2011). Promoting awareness of Internet safety in Taiwan in-service teacher education: A ten-year experience. Internet and Higher Education, 14, 44-53.

Cohen, L., Manion, L., & Morrison, K. (2007). Research methods in education (6th ed). London: Routledge.

Comrey, A. L., & Lee, H. B. (1992). A first course in factor analysis (2nd Ed). Hillsdale, NJ: Erlbaum.

Çokluk, Ö., Şekercioğlu, G., & Büyüköztürk, Ş. (2012). Sosyal bilimler için çok değişkenli istatistik: SPSS ve LISREL uygulamaları (2. Baskı). Ankara: Pegem Akademi.

Demir, S. B., & Akengin, H. (2010). Sosyal bilgiler dersine yönelik bir tutum ölçeğinin geliştirilmesi: Geçerlik ve güvenirlik çalışması. e-Uluslararası Eğitim Araştırmaları Dergisi, 1(1), 26-40.

Dönmez, O., Odabaşı, H. F., Kabakçı Yurdakul, I., Kuzu, A., & Girgin, Ü. (2014). Öğretmen adayları için hazırlanan algılanan İnternet riskleri ölçeğinin güvenirlik ve geçerlik çalışmaları. 8. Uluslararası Bilgisayar ve Öğretim Teknolojileri Sempozyumu, 18-20 Eylül 2014, Trakya Üniversitesi, Edirne.

Dülger, V. M. (2004). Bilişim suçları. Ankara: Seçkin Yayıncılık.

Erkuş, A. (2014). Psikolojide ölçme ve ölçek geliştirme I: Temel kavramlar ve işlemler(2.Baskı). Ankara: Pegem Akademi.

FATİH Projesi. (2012). Proje hakkında. http://fatihprojesi.meb.gov.tr/tr/icerikincele.php?id=6 adresinden 17.12.2013 tarihinde edinilmiştir.

Fussell, R. S. (2005). Protecting information security Availability via self-adapting intelligent agents. Military Communications Conference, IEEE, 297.

Güven, E., & Aydoğdu, M. (2012). Çevre sorunlarına yönelik farkındalık ölçeğinin geliştirilmesi ve öğretmen adaylarının farkındalık düzeylerinin belirlenmesi. Öğretmen Eğitimi ve Eğitimcileri Dergisi, 1(2), 185-202.

Hu, L. T., & Bentler, P. M. (1999). Cut off criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. Structural Equation Modeling, 6(1), 1-55.

Karakaş, Z. (2002). Teknoloji yönetimi. Yayımlanmamış Yüksek Lisans Tezi, Sakarya Üniversitesi Sosyal Bilimler Enstitüsü, Sakarya.

Karakoç, M. (2011). Bilişim suçlarına genel bakış, bilişim suçlarını önleme çalışmaları ve güvenli İnternet kullanımı. Suç ve Önleme Sempozyumu, Bursa.

Karasar, N. (1995). Bilimsel araştırma yöntemi: Kavramlar, ilkeler ve teknikler. Ankara: 3A Araştırma Eğitim Danışmanlık Ltd. Şti.

Kelloway, K. E. (1998). Using Lisrel for structural equation modeling: A researcher's guide. London: Sage.

Ketizmen, M., & Ülküderner, Ç. (2007). E-devlet uygulamalarında kişisel verilerin korun(ma)ması. XII. Türkiye'de İnternet Konferansı, 8-10 Kasım 2007, Ankara.

Kuzucu, Y. (2008). Duygusal farkındalık düzeyi ölçeğinin uyarlanması: Geçerlik ve güvenirlik çalışmaları. Türk Psikolojik Danışma ve Rehberlik Dergisi, 3(29), 51-64.

Mart, İ. (2012). Bilişim kültüründe bilgi güvenliği farkındalığı. Yayımlanmamış Yüksek Lisans Tezi, Kahramanmaraş Sütçü İmam Üniversitesi, Fen Bilimleri Enstitüsü, Kahramanmaraş.

McCumber, J. (2005). Assessing and managing security risk in IT systems. Washington: CRC Press.

MEB Bilgi İşlem Dairesi Başkanlığı. (2012). Bilgi ve sistem güvenliği yönergesi. http://bigb.meb.gov.tr/meb_iys_dosyalar/2012_06/18113300_yonerge.pdf adresinden 17 Mart 2014 tarihinde edinilmiştir.

Özenç, K. (2007). Bilgi ve iletişim teknolojilerinde kişisel ve kurumsal bilgi güvenliğinin sağlanması. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, 13-14 Aralık 2007, Ankara.

Özyeşil, Z., Arslan, C., Kesici, Ş., & Deniz, M. E. (2011). Bilinçli farkındalık ölçeğini Türkçeye uyarlama çalışması. Eğitim ve Bilim, 36(160), 224-235.

Sargın, N. (2010). Öğretmen adaylarının çatışma ve şiddete ilişkin farkındalık düzeylerinin çeşitli değişkenlere göre incelenmesi. Kuram ve Uygulamada Eğitim Yönetimi, 16(4), 601-616.

DOI: 10.5824/1309-1581.2015.4.002.x

Schlienger, T., & Teufel, S. (2001). Analyzing information security culture: Increased trust by an appropriate information security culture. University of Fribourg, Fribourg.

Schumacher, R. E., & Lomax, R. G. (1996). A beginner's guide to structural equation modeling. New Jersey: Lawrence Erlbaum Associates Publishers.

Stevens, J. (1996). Applied multivariate statistics for the social sciences (3rd Ed.). Mahwah, New Jersey: Lawrence Erlbaum.

Sümer, N. (2000). Yapısal eşitlik modelleri. Türk Psikoloji Yazıları, 3(6), 49-74.

Tabachnick, G. B., & Fidell, L. S. (2001). Using multivariate statistics (4th Ed.). USA: Allyon and Bacon Press.

Tavşancıl, E. (2006). Tutumların ölçülmesi ve SPSS ile veri analizi. Ankara: Nobel Yayın Dağıtım.

Tekerek, M. (2008). Bilgi güvenliği yönetimi. KSÜ Fen ve Mühendislik Dergisi, 11(1), 132.

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

Thompson, B. (2004). Exploratory and confirmatory factor analysis: Understanding concepts and applications. Washington, DC: American Psychological Association.

Türk Dil Kurumu [TDK]. (2015). Güncel Türkçe sözlük.http://www.tdk.gov.tr/ adresinden 30.01.2015 tarihinde edinilmiştir.

Ursavaş, Ö. F., Şahin, S., & McIlroy, D. (2014). Öğretmenler için teknoloji kabul ölçeği: Ö-TKÖ. Eğitimde Kuram ve Uygulama, 10(4), 885-917.

Yavanoğlu, U., Sağıroğlu. Ş., & Çolak. İ. (2012). Sosyal ağlarda bilgi güvenliği tehditleri ve alınması gereken önlemler. Politeknik Dergisi, 15(1), 15-27.

Yıldırım, A., & Şimşek, H. (2013). Sosyal bilimlerde nitel araştırma yöntemleri (9. Baskı). Ankara: Seçkin Yayıncılık.