Elementary Education Online, 2016; 15(2): 682-695,
İlköğretim Online, 15(2), 682-695, 2016. [Online]:http://ilkogretim-online.org.tr
doi: http://dx.doi.org/10.17051/io.2016.27218

Ortaöğretim Öğrencilerine Yönelik Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması

Development of Information Security Awareness Scale (ISAS) for Secondary Education Students

Can Güldüren, *Ankara üniversitesi, Eğitim Bilimleri Enstitüsü, cangulduren@yahoo.com*
Levent Çetinkaya, *Ankara üniversitesi, Eğitim Bilimleri Enstitüsü, cetinkayalevent@gmail.com*
Hafize Keser, *Ankara üniversitesi, Eğitim Bilimleri Fakültesi, keser@ankara.edu.tr*

ÖZ. Bu çalışmanın amacı, ortaöğretim kurumlarında öğrenim gören öğrencilerin bilgi güvenliği farkındalık düzeylerini belirlemeye yönelik bir ölçek geliştirmektir. Araştırma, ortaöğretim kurumlarında öğrenim gören 607 öğrenciyle gerçekleştirilmiştir. Çalışmanın ilk aşamasında, 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. Çalışmanın ikinci aşamasında, 200 kişilik katılımcı grubu ile gerçekleştirilen doğrulayıcı faktör analizi (DFA) sonucunda 3 faktörlü yapı doğrulanmıştır. Ölçeğin tamamı için Cronbach's Alpha güvenirlik katsayısı .955; her alt boyut için sırasıyla St:.954, Ma:.890 ile Kvk:.808'dir. Bu çalışma sonucunda ortaöğretim kurumlarındaki öğrencilerin bilgi güvenliği farkındalık düzeylerini belirlemek için kullanılabilecek geçerli ve güvenilir bir ölçek geliştirilmiştir. Ayrıca geliştirilen ölçek üzerinde yapılan analizler sonucunda öğrencilerin bilgi güvenliği farkındalıkları ile cinsiyetleri arasında anlamlı bir farklılığın olduğu belirlenmiştir.
Anahtar Kelimeler. Bilgi, Güvenlik, Farkındalık, Bilinçlendirme, Bilgi Güvenliği, Ölçek Geliştirme

ABSTRACT. The purpose of this study is to develop an "information security awareness scale" for secondary education students to determine their level of information security awareness. The study was conducted with 607 secondary education students in various secondary education institutions. In the first phase of the study, exploratory factor analysis (EFA) was conducted with 407 participating students. As a result of the EFA, it was determined that the scale consists of 36 items and 3 subscales ('attacks and threats: At', 'privacy: Pr' and 'the protection of personal data: Ppd'). In the second phase of the study, confirmatory factor analysis (CFA) was conducted with 200 participating students. Three-factor structure was confirmed. Cronbach's Alpha reliability coefficient is .955 for the entire scale; and At:.954, Pr:.890 and Ppd:.808, respectively, for each subscale. Consequently, a valid and reliable scale that can be used to determine the level of information security awareness of secondary education students has been developed. In addition, as a result of the analyzes carried out with the scale, a significant difference has been determined between information security awareness and gender of the students.
Keywords. Information, Security, Awareness, Awareness Raising, Information Security, Scale Development

SUMMARY

Purpose and Significance: The information security and the provision of the security measures are very important in terms of people and institutions. Although there are technological solutions provided for the provision of information security, still, they are the people who use them. When the studies conducted on the information security are considered, the studies that examine the human factor and the information security, and that try to determine the level of the awareness of the young people leading lives intertwined with technology, seem very limited. Considering the lack of research on this subject, this study was carried out to develop a scale which determines the level of information security awareness and the pre-psychometric properties of the students in secondary schools.

Methodology: The study was applied to 607 secondary school students between the ages of 14-18 attending at 6 different schools during the Spring semester of 2014-2015 academic year in Turkey. At the end of the data collection process which took 4 months, the validity and the reliability study of the scale was assessed. The whole scale was tested to check whether a significant difference exists between the sub factor scores and the gender of the students.

Geliş tarihi: 24/12/2015, Kabul tarihi: 31/03/2016, Yayımlanma tarihi: 01/05/2016

Results: KMO and Barlett sphericity test was performed to determine the suitability of data for exploratory factor analysis (EFA). KMO coefficient is computed to be 0.94, Bartlett sphericity test was found meaningful at the 0.01 level of significance and another premise of the factor analysis was met. In the first phase of the study, EFA was conducted with groups of 407 people. As a result of EFA, it was determined that the scale consists of 36 items and 3 subscales ('At:attacks and threats', 'Pr:privacy' and 'Ppd:the protection of personal data'). As a result of EFA, the total explained variance for the scale which consists of three sub-factors is 47.34% and scale load factor remained above 0.55 value for thirty-six items in the scale. In the second phase of the study, confirmatory factor analysis was conducted among a randomly selected group of 200 students and three-factor structure was confirmed. Cronbach's Alpha reliability coefficient is .955 for the entire scale; and At:.954, Pr:.890, Ppd:.808 respectively, for each subscale. All these facts indicate that the scale has satisfactory level of reliability.

Discussion and Conclusions: As a result of this study, a scale which consists of 36 items and 3 dimensions has been developed and its validity and reliability has been computed. Furthermore, the results of the analyses have shown a significant difference between the gender and information security awareness of the students. Male students' information security awareness was found to be higher than that of the female students in the whole scale and all subscales. The scale developed in this study is expected to fill the gap in information security awareness of the high school students at the ages of 14-18. Since the levels of information security awareness of the students could be determined, guidance services to create awareness within the framework of information technologies could be realised. Furthermore several hypotheses can be tested with information security awareness of the students by variables such as internet usage cases and demographic characteristics.

GİRİŞ

Bilgi ve iletişim teknolojilerindeki hızlı gelişmeler bireyler arasında iletişime yeni boyutlar katarak, etkileşimi farklı boyutlara taşımıştır. Bu noktada teknolojiyi benimseyenler, bulundukları ortamda kendilerini rahat hissederken, benimsemeyenler ortamdan rahatsızlık duyup uzaklaşma eğilimine girmişlerdir (Berman, 2004). Nitekim yeni teknolojilerin hayatımıza girmesiyle birlikte, bu teknolojileri benimseyenler ve benimsemeyenler arasında etkileşim kavramının anlamı da farklı şekillerde algılanmaya başlamıştır. Bu durumda hayatımıza giren yeni teknolojilerin kabul edilebilirliği, algılanışı ve etkileri de toplumun yapısı ve zamana bağlı olarak değişim göstermiştir.

Günümüz gençliğinin hemen hemen bütün aktivitelerinde, dijital teknolojiler yer almakta ve bu teknolojileri usta bir şekilde kullanabilmektedirler. Bu teknolojiler bireyin dış dünya ile bağlantı kurmasını ve bu yolla bilgiyi paylaşmasını mümkün kılmanın yanı sıra bireyi izole edici bir faktör olarak da görülebilmektedir (Mackay, 1997). Nitekim gelinen son noktada gerçek ile sanal yaşantılar birbiriyle iç içe geçmiş durumdadır. Bu noktada da, özellikle ulaşılan bilgi ve bu bilginin güvenliği, yaşantının dengeli bir biçimde devamı için önemli bir unsur olarak karşımıza çıkmaktadır. Özellikle bilginin paylaşımı aşamasında, kişisel bilgilerimiz başta olmak üzere bize ait tüm kritik bilgiler, teknolojik cihazlarımızda veya bu cihazlarda barındırdığımız uygulamalar aracılığı ile sanal dünyanın bize ayrılan bir yerinde saklanmaktadır. Bu noktada da bilgi güvenliği ve bu konudaki güvenlik önlemlerinin sağlanması 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. Her ne kadar bilgi güvenliğinin sağlanmasına yönelik standartlar (ISO/IEC 2700X) ve yazılımlar (Antivirüs yazılımları, Güvenlik duvarları, vb.) geliştirilerek, teknoloji temeli çözümler sağlanmaya çalışılsa da bu teknolojileri kullananlar yine insanlardır. Yalnızca teknoloji temelli önlemlerle bilgi güvenliğinin sağlanması ve olası problemlere çözüm bulma düşüncesi, bilgi güvenliğinin sağlanmasında belki de en önemli unsur olan insan faktörünün göz ardı edilmesine

neden olmaktadır (Chen, Shaw ve Yang, 2006; Kjorvik, 2010; Öztemiz ve Yılmaz, 2013; Rezgui ve Marks, 2008). Oysaki bilgi güvenliğine yönelik zaman içerisinde gelişen teknolojiler sayesinde, olası güvenlik zafiyetleri gittikçe azalmakta ve bu durumda da insan hatalarından faydalanılmaya çalışılmaktadır. Bu nedenle de kişisel ve kurumsal bilgilerin güvenliğinin en zayıf halkasını insan unsuru oluşturmaktadır (Kritzinger ve Smith, 2008; Mahabi, 2010; Penmetsa, 2010; Veiga, 2008). Bu durum bilgi güvenliği sorunun, insan faktörünü göz ardı ederek ve yalnızca teknoloji temelli yöntemlerle çözümlenemeyeceğini göstermektedir.

Bilginin yönetimi ve bu bilginin güvenliğinin sağlanması oldukça karmaşık bir süreçtir ve bu sürecin süreklilik gerektiren iyi planlamayla yönetilmesi gerekmektedir. Kurumsal ve kişisel bilgilerin güvenliğini sadece teknik güvenlik önlemleriyle (güvenlik duvarı, sanal özel ağ, saldırı tespit/önleme sistemi, anti virüs, içerik kontrolü yazılımı, veri şifreleme, kimlik doğrulama, yetkilendirme vb.) sağlamak mümkün değildir (Rezgui ve Marks, 2008). Dolayısıyla bilgi güvenliğinin sağlanmasında teknoloji temelli tedbirlerinin 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; Şahinaslan, Kandemir ve Şahinaslan, 2009; Vardal, 2009; Vural, 2007). Bu noktada da bilgi güvenliği risklerinden korunmanın en iyi yolu insanların bilinçlenmesi ve ihtiyaç duyulan güvenlik teknolojisini doğru yer ve zamanda kullanmakla mümkündür (Albrechtsen, 2007; Al-Shehri, 2012; Puhakainen, 2006; Siponen, 2001; Şahinaslan, Kantürk, Şahinaslan, ve Borandağ, 2009).

Çocuklar, özellikle de gençler hepsi birbiri ile iletişim kapasitesine sahip, hızla ilerleyen ve karmaşıklaşan teknolojiler ile kuşatılmış bulunmaktadır. Bu teknolojilerden farklı tür ve boyutta kişisel bilgisayarlardan internete bağlı televizyonları, oyun konsollarını, artık neredeyse sınırsız iletişim gücüne sahip cihazlara dönüşmüş akıllı cep telefonlarını sayabiliriz. Bu teknolojilerin belki de en önemli ortak özelliği çevrimiçi bağlantı kurabilmeleridir. Ancak, iletişim açısından büyük kolaylık olarak algılanabilecek bu gelişmeler, aynı zamanda gençleri çeşitli tehlikelere de açık hale getirmektedir. Bazen teknoloji hedeflenen kurbana ulaşmak için oldukça elverişli bir araç da olabilmektedir. Söz konusu bu tehditler, bilgisayar korsanlığı, kötü amaçlı yazılımlar (örn., virüs, trojen), casus yazılımlar, uygunsuz içerikler, siber zorbalık gibi çok çeşitli olabilmektedir. Bazen bir tehditle ya da sosyal ağlarda dikkatsizce yapılan kişisel bilgi paylaşımları gençleri tehlikeli ve sıkıntılı durumlara sokabilmektedir. İnternette çoğu insan gerçek dünyadakinden farklı davranmaktadır. İnsanlar internet ortamında gerçek yaşamdakinden farklı davranabilmekte, rahatlıkla bilgi, resim ve video paylaşabilmektedirler. Ancak bu paylaşımlar bazen arkadaşlarla sınırlı kalmayabilmektedir. Sıklıkla bu bilgiler suistimale maruz kalıp, sonrasında tehdit oluşturabilmektedir (Eckertova, 2013). Bu tehditlerin bazıları, özellikle gençlere özgü olmamakla birlikte, gençlerin yeni bir teknolojiyi benimsemekteki tutkuları, karşılaşabilecekleri tehditler konusundaki saflıkları ile birleşince onları bu tehditlere karşı daha açık kılmaktadır (Atkinson, Furnell ve Phippen, 2009).

Teknoloji geliştikçe bilgi güvenliğine yönelik tehdit ve saldırı yöntemleri de çeşitlenmektedir. Bu noktada insanları doğru olmayan bilgiler ile kandırmaya dayanan sosyal mühendislik, çevrimiçi ortamlarda saldırganların çok sık kullandığı bir taktik haline gelmiştir (Mitnick, 2002). Eposta ile gelen bir kartpostalı alan bir genç farkında olmadan bir truva atı programını da kullandığı cihaza yükleyip, akıllıca düzenlenmiş bir sosyal mühendisliğin kurbanı olabilir (Marks, 2007). Kimlik hırsızlığının ilk dönemlerinde kurbanın bir evrakta ya da kredi kartında yazılı bilgilerine izinsizce erişilirken, günümüzde birçok farklı yöntem kullanılmakta özellikle de sosyal ağlar bunun için büyük kaynak haline gelmiştir (Kim, 2013). Sahip olunan bilgilere yönelik tehditler ve de bunları ele geçirmeye yönelik yöntemlerin çeşitliliği bilgi güvenliğini her geçen gün daha önemli kılmaktadır. Ancak, bilgi güvenliğini sağlamak için öncelikle eğitim programları vasıtasıyla farkındalık oluşturulmalı (Pltier, 2005) ve gençlere, güvenliğin kendileri için ne kadar önemli olduğu anlatılmalıdır (Brady, 2010).

Bintziou ve ark. (1999), bilgi güvenliğine yönelik eğitim için en uygun dönemin ortaöğretim olduğunu ifade etmektedir. Bu yaşlarda insan bilgisayarla ilk defa ciddi anlamda karşılaşır. Korunmaya ihtiyaç duyar, örneğin bilgisayardaki çalışmasını silinmeye, üzerinde değişiklik

yapılmaya karşı koruma altına almak ister, dahası bu özel bilgilere diğer insanların erişimini engellemek ister. Bu dönemlerde mevcut tehditlerin bilincine varır ve fikir edinir. Fakat gençleri bu tehditlere karşı korumak için çoğu durumda yine teknoloji temelli çözümler aranmakta ve gençlerin çevrimiçi yapabildiklerine sınırlamalar getirilmektedir. Ancak teknoloji, kısmi çözümler sağlamaktadır ve sorunu bütününde çözmede yetersiz kalmaktadırlar. Aynı zamanda çevrimiçi ortamlarda özgürlük talep eden gençlerin beklentilerini karşılamayabilmektedir. Bilgi güvenliği konusunda gençlerin eğitim süreçlerine bizzat dâhil olmaları gerektiği konusunda büyük bir görüş birliği bulunmaktadır (Atkinson, Furnell ve Phippen, 2009). Böylece gençlerin bilgi güvenliği konusundaki farkındalıkları artacak ve kendi güvenliklerini sağlamada sorumluluk alma yönünde çaba göstereceklerdir.

Bilgi güvenliğine yönelik 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, teknolojiyle iç içe yaşam sürdüren gençlerin bilgi güvenliği farkındalık düzeyinin ne olduğunu belirleyecek bir çalışmaya ulaşılamamıştır. Diğer taraftan yapılan çalışma sonuçlarında, özellikle gençlerin bilgi güvenliği konusunda öz değerlendirme yapabilmesinin ve başta çevrimiçi ortamlar olmak üzere olası tehlikelerden kendilerini koruyabilmesinin önemli olduğu, bu konuda bilinçlendirme çalışmalarının yapılmasının gerekliliği net bir şekilde ortaya çıkmaktadır. Bu duruma bağlı olarak gençlerin bilgi güvenliğine yönelik farkındalıklarının belirlenmesi, eksiklerin ortaya çıkartılması ve var olan durumlarının analiz edilmesine katkı sağlayabilecek bir ölçme aracının geliştirilmesine gereksinim duyulmuştur. Bu gereksinimden hareketle çalışma, orta öğretim kurumlarında öğrenim gören öğrencilerin, bilgi güvenliği farkındalık düzeyini belirleyecek olan bir ölçeğin geliştirilmesi ve ön-psikometrik (preliminary) özelliklerinin belirlenmesi amacıyla gerçekleştirilmiştir.

YÖNTEM

Araştırma Deseni

Araştırma bir ölçek geliştirme çalışmasıdır. Ortaöğretim öğrencilerine yönelik "Bilgi Güvenliği Farkındalık Ölçeği" geliştirme çalışmasının hangi aşamalarda gerçekleştiği ve çalışma grubunun özellikleri aşağıda sunulmuştur.

Çalışma Grubu

Araştırmanın çalışma grubunu, 2014-2015 öğretim yılı 1. döneminde ortaöğretim kurumu türlerini kapsayacak nitelikte belirlenen 6 farklı okulda (1 Fen Lisesi, 3 Anadolu Lisesi ile 2 Meslek ve Teknik Lise) öğrenim görmekte olan 607 ortaöğretim öğrencisi oluşturmaktadır. Çalışmanın yapılacağı okul türü, okul türü oranları ve öğrenci sayıları belirlenirken Millî Eğitim Bakanlığı 2013-2014 Eğitim-Öğretim dönemi örgün eğitim istatistikleri (MEB, 2014) dikkate alınmıştır. Belirlenen çalışma grubunu oluşturan öğrencilerin; % 18.9'u Fen Lisesinde, %50.4'ü Anadolu Lisesinde ve % 30.6 ise Mesleki Lisesinde öğrenim görmektedir. Çalışma grubundaki öğrencilerin yaş ve cinsiyete göre dağılımları Tablo 1'de sunulmuştur.

Tablo 1. *Çalışma Grubundaki Öğrencilerin yaş ve Cinsiyet Dağılımları*

		f	%
Cinsiyet	Kız	352	58.00
	Erkek	255	42.00
	Toplam	607	100
Yaş	14	101	16.6
	15	153	25.2
	16	167	27.5
	17	124	20.4
	18	62	10.2
	Toplam	607	100

Tablo 1'de görüldüğü gibi, çalışma grubunun %58.0'i kız ve %42.0'si erkek öğrencilerden oluşmaktadır. Öğrencilerin %16.6'sı 14 yaşında, %25.2'si 15 yaşında, %27.5'i 16 yaşında, %20.4'ü 17 yaşında ve %10.2'sinin 18 yaşında olduğu görülmektedir.

Veri Toplama Aracı

Çalışmayla ilgili uygulamanın ilk aşamasında alanyazın incelenerek bilgi güvenliği farkındalığı kavramına ilişkin göstergelerin neler olabileceği araştırılmıştır. Bilgi güvenliği farkındalığına ilişkin tespit edilmiş kategoriler, göstergeler ve madde sayıları Tablo 2'de sunulmuştur. Bilgi güvenliği farkındalığına ilişkin her bir gösterge göz önünde bulundurularak toplamda 90 maddelik bir havuz oluşturulmuştur.

Kapsam geçerliği çalışmalarında, Lawshe (1975) kapsam geçerliği tekniğinden yararlanılmıştır. Oluşturulan 90 maddelik deneme formu, Bilgisayar ve Öğretim Teknolojileri Eğitimi (BÖTE): 13, Bilgisayar Mühendisliği: 4, Bilgisayar Enformatik/Bilgi Teknolojileri: 4, Elektronik Mühendisliği: 1 ve Bilişim Hukuku: 1 olmak üzere toplam 23 uzman tarafından değerlendirilmiştir. Her bir madde, bilgi güvenliği farkındalığını ölçebilme, ilgili alt boyutla ilişkili olma, ifadenin anlaşılırlığı başlıkları altında değerlendirilmiştir. Bu maksatla uzmanların herhangi bir maddeye ilişkin görüşleri toplanarak Kapsam Geçerlilik Oranları (KGO) elde edilmiştir. KGO'larının istatistiksel olarak anlamlılığı α=0.05 anlamlılık düzeyinde Veneziano ve Hooper (1997) tarafından tabloya dönüştüren kapsam geçerlik ölçütüyle (KGO20 = 0.42) karşılaştırılmış ve bu değerin altında kalan 23 madde çalışma kapsamından çıkartılmış (Keser ve Güldüren, 2015) ve bazı maddeler üzerinde düzeltmeler yapılmıştır. Çalışma sonucu oluşturulan 67 maddelik formun kapsam geçerlik indeksi 0.89 olarak hesaplanmıştır. 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	***f***	**Madde Sayısı**
Genel Güvenlik	Bilgi güvenliği, Bilgi güvenliği sorumluğu, 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 sürücüleri	8
Mahremiyet	Dosyaları n 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, Internet protokolü ses teknolojisi, İşletim sistemleri	5
Toplam		90

Verilerin Toplanması ve Analizi

Toplamda 4 ay süren veri toplama süreci sonunda 631 ortaöğretim öğrencisi, oluşturulan formun basılı halini doldurmuştur. Yapılan inceleme sonucunda öğrencilerin doldurduğu 631 formdan 607' sinin istatistiksel analize uygun olduğu tespit edilmiştir. Elde edilen veriler ile ölçeğin geçerlik ve güvenirlik çalışması yapılmıştır. Çakmak ve diğerleri (2014), ölçek geliştirme

çalışmalarında ideal olan durumun, Açımlayıcı Faktör Analizi (AFA) ve Doğrulayıcı Faktör Analizlerinin (DFA) farklı örneklem gruplarından elde edilen veriler üzerinde yapılması gerektiği şeklinde ifade etmektedir.

Örneklem büyüklüğü, madde ya da faktör sayısı gibi bağıl 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 örneklemlerle çalışmanın daha uygun olacağını vurgulamaktadır. Çokluk, Şekercioğlu ve Büyüköztürk (2010), faktör analizinde en az 300 örneklem sayısının uygun olduğu genel kuralını ortaya koymaktadır. Bu çalışmada gerek zaman gerekse de maddi olanaklar göz önünde bulundurularak, araştırmaya katılan grup rasgele olarak iki alt gruba bölünmüştür (n1=407; n2=200). İlk grup üzerinde AFA, diğer grup üzerinde ise DFA yapılmıştır.

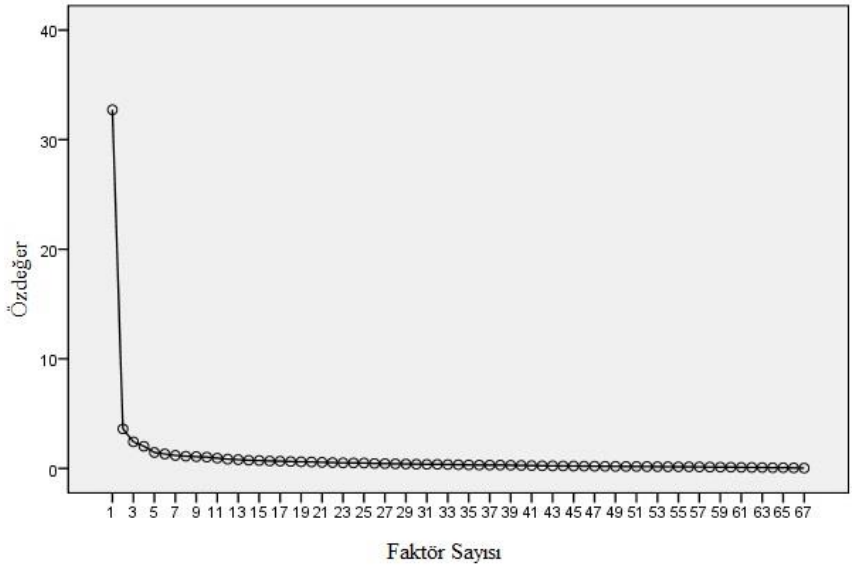
BULGULAR

Bu bölümde ortaöğretim öğrencilerine yönelik ölçek geliştirme sürecine yönelik öğrencilerin sorulara verdiği cevapların incelenip değerlendirilmesiyle elde edilen bulgular; açımlayıcı faktör analizi, madde analizleri, doğrulayıcı faktör analizi, öğrencilerin bilgi güvenliği farkındalığı ile cinsiyetlerine yönelik bulgular alt başlıklarında sunulmuştur.

Açımlayıcı Faktör Analizi

Verilerin AFA'ne uygunluğunu saptamak üzere Kaiser-Meyer-Olkin (KMO) Testi katsayısı hesaplanmış ve Barlett Küresellik testi yapılmıştır. Örneklem büyüklüğü için değer, .50'den düşük ise teste devam edilmez, .90 üzerinde ise "mükemmel" olduğu şeklinde yorumlanır (Çokluk ve ark., 2010; Tavşancıl, 2005). KMO katsayısı değeri .94 olarak belirlenmiştir ve bu nedenle veri yapısının faktör analizi yapabilmek için mükemmel derecede yeterli olduğu değerlendirmesi yapılabilir. Çalışma içerisinde yapılan analiz sonucunda Barlett Küresellik testi .01 düzeyinde manidar bulunmuştur [$\chi 2$= 13983.562; df=1326; p=0,000]. Bu bulgu, verilerin çok değişkenli normal dağılımdan geldiğini ve dolayısıyla faktör analizinin bir diğer sayıltısının karşılandığı anlamına gelmektedir.

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 edilir (Büyüköztürk, 2002; Çokluk ve ark., 2010). Ölçek, özdeğerleri 1'den büyük 12 faktör yapısına sahiptir. Bu faktörlerin sırasıyla özdeğeri ve açıklanan toplam varyansa katkı düzeyleri: 1.faktör: 23.90; % 35.67, 2.faktör: 4.20; % 6.26, 3.faktör: 2.97; % 4.43, 4.faktör: 2.12; % 3.17, 5.faktör: 1.77; % 2.64, 6.faktör: 1.62; % 2.42, 7 faktör: 1.57; % 2.35, 8.faktör: 1.45; % 2.16, 9.faktör: 1.23; % 1.84, 10.faktör: 1.20: %1.80, 11.faktör: 1.12: %1.67 ve 12.faktör: 1.05: %1.56 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. Şekil 1'de faktör özdeğerlerine ait çizgi grafiği sunulmaktadır.



Şekil 1. *Faktör Özdeğerlerine İlişkin Çizgi Grafiği*

AFA sonucunda ölçeğin öz değerinin 2'den büyük 4 faktör altında toplandığı görülmüştür. Bu 4 faktörün ölçeğe ilişkin açıkladığı varyans ise %49.53'dur. 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 Yaptırmalarının Nedeni*

AB*	Madde	F1	OFV*	AB	Madde	F2	OFV	AB	Madde	F3	OFV
Saldırı ve Tehditler	M32	0.79	0.65	Mahremiyet	M57	0.67	0.56	Kişisel Verilerin Korunması	M06	0.68	0.57
	M30	0.79	0.66		M54	0.65	0.52		M02	0.67	0.47
	M31	0.77	0.63		M44	0.64	0.51		M17	0.64	0.54
	M26	0.74	0.60		M45	0.63	0.49		M01	0.61	0.41
	M34	0.73	0.57		M43	0.62	0.47		M07	0.61	0.46
	M29	0.72	0.59		M52	0.61	0.53		M16	0.57	0.42
	M24	0.72	0.61		M46	0.59	0.51				
	M28	0.71	0.64		M55	0.59	0.41				
	M25	0.71	0.58		M39	0.57	0.40				
	M35	0.71	0.55		M51	0.57	0.38				
	M36	0.70	0.51		M61	0.56	0.46				
	M33	0.69	0.50								
	M27	0.68	0.57								
	M23	0.67	0.52								
	M65	0.62	0.56								
	M59	0.61	0.57								
	M60	0.60	0.58								
	M22	0.58	0.42								
	M38	0.56	0.53								
		Özdeğer:	18.30			**Özdeğer**:	4.05			**Özdeğer**:	2,29
Açıklanan Varyans:			35.20			**Açıklanan Varyans**:	7.78			**Açıklanan Varyans**:	4.40
										Açıklanan Toplam Varyans:	47.30

* AB:Alt Boyut;
OFV: Ortak Faktör Varyansı

Tablo 3 incelendiğinde ölçekte yer alan 19 maddeden oluşan birinci faktöre ait faktör yük değerlerinin .56 ile .79 arasında, maddelere ilişkin ortak faktör varyanslarının ise .53 ile .65 arasında değiştiği; 11 maddeden oluşan ikinci faktöre ait faktör yük değerlerinin .56 ile .67 arasında, maddelere ilişkin ortak faktör varyanslarının ise .46 ile .56 arasında değiştiği; 6 maddeden oluşan üçüncü faktöre ait faktör yük değerlerinin .57 ile .68 arasında, maddelere ilişkin ortak faktör varyanslarının ise .42 ile .57 arasında değiştiği görülmektedir. Toplam varyansa en yüksek katkıyı .79 faktör yük değeri ve .65 ortak faktör varyansı ile 32. maddenin, en düşük katkıyı ise .56 faktör yük değeri ve .46 ortak faktör varyansı ile 61. maddenin yapmakta olduğu ifade edilebilir. Birinci faktörün açıklayabildiği toplam varyans %35.20 düzeyinde olup, alanyazın da dikkate alınarak "saldırı ve tehditler" olarak isimlendirilmiştir. İkinci faktörün açıklayabildiği varyans %7.78 düzeyinde olup, alanyazın da dikkate alınarak "mahremiyet" olarak isimlendirilmiştir. Üçüncü faktörün açıklayabildiği varyans %4.40 düzeyinde olup, alanyazın da dikkate alınarak "kişisel verilerin korunması" olarak isimlendirilmiştir.

Üç faktörlü yapının açıklayabildiği toplam varyans %47.,34 düzeyindedir. Alanyazında çok faktörlü ölçek yapılarında, sosyal bilimlerde açıklanan varyansın %40 ile %60 arasında olması yeterli olarak kabul edilir (Tavşancıl, 2005). Bu ölçüte dayanarak elde edilen üç faktörlü ölçek yapısı ortaöğretim öğrencilerine yönelik bilgi güvenliği farkındalığını ölçmek için yeterli bulunmuştur. Ölçekte yer alan otuz altı 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; Kline, 2000). Bu ölçüte dayanarak ölçeğin üç faktör altında otuz altı maddenin tamamını içermesine karar verilmiştir.

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 güvenirliğini 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 verilmiştir.

Faktör analizi ile belirlenen ve üç boyutu oluşturan 36 maddenin madde analizleri yapılmıştır. Buna göre; saldırı ve tehditler faktöründe madde-toplam test korelasyonları incelendiğinde değerler r=.55 ile r=.74 arasında değişmektedir. Mahremiyet faktöründe madde-toplam test korelasyonları incelendiğinde değerler r=.34 ile r=.63 arasında değişim göstermektedir. Kişisel verilerin korunması faktöründe madde-toplam test korelasyonları incelendiğinde değerler r=.35 ile r=.51 arasında değişim göstermektedir. Madde- toplam korelasyonlarının .30 ve daha yüksek olması ölçek maddelerinin geçerliğine bir kanıt olarak kullanılmaktadır (Nunnally ve Bernstein, 1994). Madde-toplam test korelasyonları incelendiğinde, her bir madde için r=.30'un üzerindedir. 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 6.96-20.27 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 ortaöğretim öğrencilerine 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 28. ve en düşük olarak 51. maddeyi göstermektedir.

Tablo 4. *Madde Analiz Sonuçları*

F1	Madde	DM-TK *	Ü/A %27 **	F2	Madde	DM-TK *	Ü/A %27 **	F2	Madde	DM-TK *	Ü/A %27 **
Saldırı ve Tehditler	M32	0.65	13.93*	Mahremiyet	M57	0.63	16.10*	Kişisel Verilerin Korunması	M06	0.51	12.05*
	M30	0.69	15.15*		M54	0.54	13.10*		M02	0.37	7.65*
	M31	0.68	14.28*		M44	0.54	11.23*		M17	0.51	10.00*
	M26	0.67	15.94*		M45	0.57	12.86*		M01	0.35	7.03*
	M34	0.64	13.68*		M43	0.55	13.21*		M07	0.45	9.42*
	M29	0.68	16.16*		M52	0.59	14.27*		M16	0.41	8.48*
	M24	0.72	19.23*		M46	0.61	13.71*				
	M28	0.74	20.27*		M55	0.51	11.53*				
	M25	0.69	16.83*		M39	0.52	11.89*				
	M35	0.65	13.65*		M51	0.34	6.96*				
	M36	0.60	11.22*		M61	0.59	14.91*				
	M33	0.55	10.16*								
	M27	0.70	18.94*								
	M23	0.65	15.38*								
	M65	0.66	15.17*								
	M59	0.71	19.42*								
	M60	0.72	18.25*								
	M22	0.59	14.09*								
	M38	0.68	18.11*								

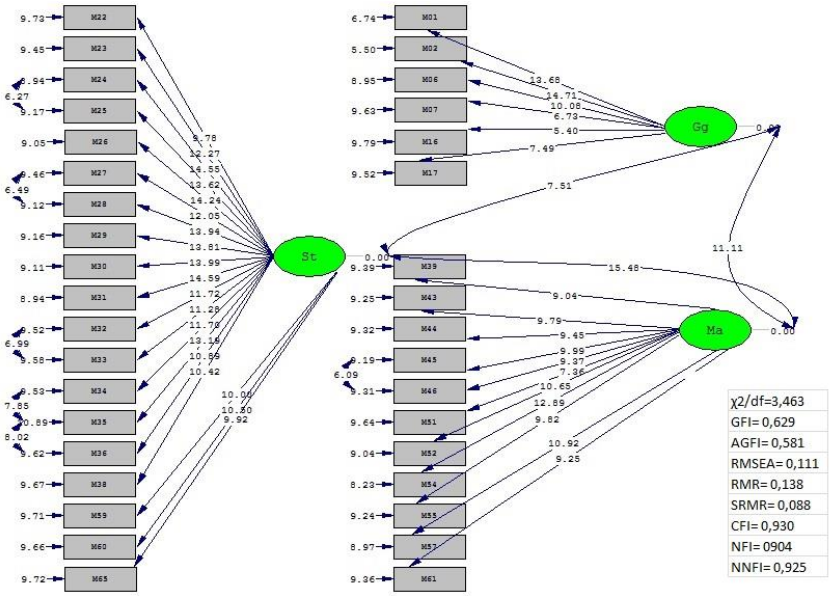
* DM-TK: Düzeltilmiş Madde-Toplam Korelasyonu

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

Ölçeğin güvenirliğini 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 .955, birinci alt faktöre ilişkin Cronbach Alfa iç tutarlılık katsayısı .954, ikinci alt faktöre ilişkin Cronbach Alfa iç tutarlılık katsayısı .890 ve üçüncü alt faktöre ilişkin Cronbach Alfa iç tutarlılık katsayısı .808 olarak hesaplanmıştır. Tüm bu bulgular ölçeğin tatmin edici düzeyde güvenirliğe 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 ($\chi 2$) 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.



Şekil 2. *Doğrulayıcı Faktör Analizi*

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: [χ2/df=3,463 (p=,000); GFI= 0.629; AGFI= 0.581; RMSEA= 0.111; RMR= 0.138; SRMR= 0.088; CFI= 0.930; NFI= 0.904; NNFI= 0.925]. Analizler sonucunda ortaya çıkan modifikasyon önerileri incelendiğinde; S36 ve S35; S35 ve S34; S33 ve S32; S28 ve S27; S25 ve S24; S46 ve S45 maddeleri arasında altı 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. Modifikasyonun ardından modele ilişkin uyum iyiliği indeksleri şu şekilde oluşmuştur: [χ2/df=2.491 (p=.000); GFI= 0.710; AGFI= 0.669; RMSEA= 0.0864; RMR= 0.137; SRMR= 0.0871; CFI= 0.958; NFI= 0.932; NNFI= 0.955]. Şekil 2'de üç faktörlü yapıya ilişkin yapısal eşitlik modeli ve Tablo 5'te ölçek maddelerine ilişkin t ve R^2 (çoklu korelasyon katsayısı) değerleri sunulmaktadır.

Tablo halinde sunulan yapısal eşitlik modelinde uyum indeksleri kriterleri ve kabulü için kesme noktaları göz önüne alınarak modelin uyum iyiliği indeksleri incelendiğinde Ki-Kare/serbeslik derecesi iyilik uyumu değerinin 2.491 olduğu görülmektedir (küçük örneklemler için 2.5'in altındaki modellerde mükemmel uyum, Çokluk ve arkadaşları, 2010; Kline, 2005). Hesaplanan RMSEA değerinin .086 olduğu görülmektedir (iyi uyum, Brown, 2006; Jöreskog ve Sörbom, 1993). Modelin GFI değeri .71 ve AGFI değeri .67 için zayıf uyuma sahip olduğu söylenebilir (GFI, AGFI > .90 mükemmel uyum; GFI> .85 ve AGFI>.80 kabul edilebilir uyum, Jöreskog ve Sörbom, 1993). Alanyazın irdelendiğinde bu indekslerin aldıkları değerlerin örneklem büyüklüğünden etkilenebildikleri görülmektedir (Şimşek, 2007). Örneklem büyüklüğü etkilerinden arındırılmış uyum iyiliği indekslerinden olan CFI, NFI ve NNFI üzerinde durulmuştur. CFI ve NNFI değerlerinin .95'den büyük olduğu, NFI değerinin ise .90'dan büyük olduğu görülmektedir (CFI, NFI, NNFI > .95 mükemmel uyum; NFI >=.90= iyi uyum; Sümer, 2000; Thompson, 2004). Modele ilişkin t değerleri incelendiğinde tüm gözlenen değişkenlerin gizil değişken tarafından .01'lik anlamlılık düzeyinde yordanabildiği görülmektedir.

Önemli bir ölçüt de her bir gözlenen değişken için açıklanan varyansı ifade ederek, gözlenen değişkenin gizil değişkendeki değişimin ne kadarını açıklayabildiğini ortaya koyan R^2 değeridir (Şimşek, 2007: 86). Modele ilişkin λx, t ve R^2 değerleri incelendiğinde bilgi güvenliği farkındalığının ölçümüne en yüksek katkıyı sırasıyla 28, 59, 24, 27 ve 60 maddelerin, en düşük katkıyı ise sırasıyla 51, 1, 2, 16 ve 7. maddelerin sağladığı görülmektedir. Bu bulgu, açımlayıcı faktör analizinde elde edilen bulguları doğrulamaktadır.

Tablo 5. *Madde İlişkin t ve R^2 Değerleri*

F1	Madde	t	R2	F2	Madde	t	R2	F3	Madde	t	R2
Saldırı ve Tehditler	M28	20.27	0.66	Mahremiyet	M57	16.10	0.49	Kişisel Verilerin Korunması	M06	12.05	0.44
	M59	19.42	0.41		M61	14.91	0.38		M17	10.00	0.27
	M24	19.23	0.70		M52	14.27	0.47		M07	9.42	0.23
	M27	18.94	0.54		M46	13.71	0.39		M16	8.48	0.15
	M60	18.25	0.44		M43	13.21	0.41		M02	7.65	0.76
	M38	18.11	0.44		M54	13.09	0.62		M01	7.03	0.69
	M25	16.83	0.64		M45	12.86	0.43				
	M29	16.16	0.66		M39	11.89	0.36				
	M26	15.94	0.68		M55	11.53	0.42				
	M23	15.38	0.56		M44	11.23	0.39				
	M65	15.17	0.41		M51	6.96	0.26				
	M30	15.15	0.67								
	M31	14.28	0.70								
	M22	14.09	0.40								
	M32	13.93	0.52								
	M34	13.68	0.52								
	M35	13.65	0.62								
	M36	11.22	0.47								
	M33	10.16	0.49								

Öğrencilerin Bilgi Güvenliği Farkındalığı ile Cinsiyetlerine Yönelik Bulgular

Ölçek geliştirme çalışması sonucunda elde edilen üç faktörlü yapının her biri ve ölçeğin tamamından elde edilen toplam puanlar ile öğrencilerin cinsiyetleri arasında anlamlı bir farkın olup olmadığı t-testi ile sınanmıştır.

Tablo 6. "Cinsiyet" ile "Bilgi Güvenliği Farkındalığı" Arasındaki Farklılık

Ölçek	Cinsiyet	N	$\overline{X}$	Ss	Sd	t	p
Saldırı ve Tehditler (St)	Kız	352	36.60	14.64	605	10.248	**.000***
	Erkek	255	50.74	19.34			
Mahremiyet (Ma)	Kız	352	34.88	9.69	605	4.396	**.000***
	Erkek	255	38.33	9.34			
Kişisel Verilerin Korunması (Kvk)	Kız	352	20.77	4.55	605	2.608	**.009***
	Erkek	255	21.75	4.58			
Ölçek tamamı	Kız	352	92.24	24.62	605	8.447	**.000***
	Erkek	255	110.81	29.40			

* p<.05 düzeyinde anlamlıdır.

Çalışma sonucunda, öğrencilerin bilgi güvenliği farkındalıklarını belirlemek için geliştirilen ölçeğin tamamından aldıkları ortalama puanların, cinsiyete göre anlamlı bir farklılık gösterdiği belirlenmiştir [$t_{(605)}$= 8.447, p<.05]. Elde edilen bu bulguya göre, erkek öğrencilerin ($\overline{X}$ = 110.81) bilgi güvenliği farkındalıklarının, kız öğrencilere ($\overline{X}$ = 92.24) göre daha yüksek olduğu görülmektedir. Diğer taraftan çalışma sonucunda ölçeği oluşturan; saldırı ve tehditler [t(605)= 10.248, p<.05], mahremiyet [$t_{(605)}$= 4.396, p<.05] ve kişisel verilerin korunması [$t_{(605)}$= 2.608, p<.05] faktörlerinde de cinsiyete göre anlamlı bir farklılığın olduğu belirlenmiştir. Ölçeğin alt faktörlerinden

elde edilen ortalama puanlar incelendiğinde, ölçeğin tamamında olduğu gibi alt faktörlerin de de erkek öğrencilerin kız öğrencilerden daha yüksek olduğu görülmektedir. Özellikle erkek öğrencilerin bilgi güvenliği farkındalığına yönelik ortalama puanlar arasındaki farkın en fazla saldırı ve tehditler faktöründe, en az ise kişisel verilerin korunması alt faktöründe olduğu belirlenmiştir.

TARTIŞMA ve SONUÇ

Alanyazın taramasında çalışılan konuların bilgi güvenliği ve bilgi güvenliği yönetim sistemlerine yönelik olduğu ve bu kapsamda bilgi güvenliğinin "en zayıf halkası" olan insan unsurunu bu konuda bilinçlendirme üzerinde durulduğu görülmüştür. İncelenen çalışmalarda, bilgi güvenliği farkındalık seviyesini artıracak öneriler ve alınması gereken çeşitli tedbirler sunulmaktadır. Ayrıca ulaşılan kaynaklar kapsamında, kullanıcıların mevcut farkındalık düzeylerini belirleyebilecek iki çalışmadan birinin yurt-dışı kaynaklı olduğu, yurt içinde öğretim elemanlarının bilgi güvenliği farkındalık düzeylerinin değerlendirilmesine yönelik olarak yapıldığı tespit edilmiştir. Bu araştırma kapsamında alanyazından elde edilen bilgi güvenliği farkındalık göstergeleri esas alınarak ortaöğretim öğrencilerinin bilgi güvenliği farkındalık düzeylerini belirleyecek yeni bir ölçek geliştirilmiştir.

Yapı geçerliliği çalışmalarında ölçekte yer alan 36 madde 3 faktör altında toplanmış ve açıklayabildiği toplam varyans %47.34 olarak hesaplanmıştır. Bu oran çok faktörlü ölçek yapısı için yeterli (%40-%60) kabul edilmektedir. İlk faktör 'saldırı ve tehditler' olarak isimlendirilmiş ve açıklayabildiği toplam varyans %35.20'dir. İkinci faktör 'mahremiyet' olarak isimlendirilmiş ve açıklayabildiği toplam varyans %7.78'dir. Üçüncü faktör 'kişisel verilerin korunması' olarak isimlendirilmiş ve açıklayabildiği toplam varyans %4,40'dır. Madde analizlerinde, madde toplam puanları arasında güçlü bir korelasyonel ilişki belirlenmiştir. Ölçeğin tamamına ait Cronbach Alfa iç tutarlılık katsayısı .955, alt faktörlere ilişkin değerler St:.954, Mr:.890 ve Kvk:.808 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 ve NNFI değerleri göz önüne alındığında yapının mükemmel uyuma sahip olduğunu ortaya koymaktadır. RMSEA, NFI 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 göstermektedir. Bu durumun örneklemin AFA ve DFA'nın aynı anda kullanılmasından kaynaklandığı ve noktada da araştırmanın sınırlılığı olarak kabul edilebilir olduğu söylenebilir. Dolayısıyla doğrulayıcı faktör analizinde kabul edilebilirlik sınırı altında değer gösteren indekslerin araştırma grubunun sınırlılığından etkilenmiş olabilecekleri düşünülmektedir.

Çalışmada sonucunda, Keser ve Güldüren (2015) tarafından gerçekleştirilen bilgi güvenliği farkındalığı ölçek geliştirme çalışmasından farklı olarak ölçekte 2 faktör yapısı yerine 3 faktör yapısı oluşmuştur. Araştırmacıların öğretim elemanları üzerinde geliştirdikleri ölçekte, "Saldırı ve Tehditler" ve "Kişisel Verilerin Korunması" faktörleri oluşurken, Lise öğrencileri üzerinde gerçekleştirilen çalışmada bu faktörlere ek olarak "Mahremiyet" faktörü oluşmuştur.

Geliştirilen ölçek üzerinde yapılan analizler sonucunda, öğrencilerin bilgi güvenliği farkındalıklarına ilişkin ortalama puanlarının, cinsiyete göre anlamlı bir farklılık gösterdiği belirlenmiştir. Elde edilen veriler ölçeğin tamamı ve alt faktörlerinde bilgi güvenliği farkındalığı ölçeğinden elde edilen puan ortalamalarının erkeklerin kızlardan daha fazla olduğu belirlenmiştir. Bu doğrultuda çalışmada, ölçek alt faktörlerinden alınan ortalama puanlar incelendiğinde ortalamalar arasında farklılığın en çok saldırı ve tehditler alt faktöründe olduğu ve kişisel verilerin korunması alt faktöründe ise bu ortalama puanlar arasındaki farklılığın en az olduğu sonucuna ulaşılmıştır.

Teknolojinin hayatımızı şekillendiren en önemli unsurlardan biri olduğu bilinmektedir. Özellikle bu teknolojilerin içinde doğan ve aktif olarak kullanan bir neslin, teknolojilerin avantajları ve dezavantajları konusunda bilinçlendirilmesi oldukça önemlidir. Nitekim ki bunun içinde özellikle internet teknolojilerinin gelişmesiyle, her bilgiye kolaylıkla ulaşan günümüz gençlerinin bilgi güvenliği farkındalıklarının belirlenmesi gerekmektedir. Bu noktada geliştirilen ölçek özellikle başta

internet ve internet temelli uygulamaları sıklıkla kullanan gençlerin bilgi güvenliği farkındalıklarını belirlemek için geçerliği ve güvenirliği saptanmış bir araç olma özelliği taşıdığı ortaya çıkmaktadır.

Bu çalışmada lise öğrencilerinin bilgi güvenliği farkındalıkları ele alınmıştır. Çalışma sonucunda elde edilen ölçeğin 14-18 yaş aralığında öğrenim gören lise öğrencilerinin, bilgi güvenliği farkındalık düzeylerini belirlemede kullanılabileceği düşünülmektedir. Bu çerçevede, gerek liseye yeni başlayan gerekse üst sınıflarda öğrenim gören öğrencilerin bilgi güvenliği farkındalık düzeylerini belirleyip gereksinimi olan öğrencilere bilişim teknolojileri rehberlik hizmetleri çerçevesinde programlar uygulanarak, farkındalık oluşturmaya yönelik rehberlik etkinlikleri gerçekleştirilebilir. Lise öğrencilerinin bilgi güvenliği farkındalıklarıyla birlikte demografik özellikleri, internet bağımlılığı, problemli internet kullanım düzeyleri, siber zorba ve mağdur olma durumları gibi değişkenlerle çeşitli hipotez modeller 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.

Atkinson, S., Furnell, S. ve Phippen, A. (2009). Securing the next generation: enhancing e-safety awareness among young people. *Computer Fraud & Security, 7*, 13-19.

Berman, M. (2004). *Katı Olan Her Şey Buharlaşıyor* (Çev. Ümit Altuğ, Bülent Peker). İstanbul: İletişim Yayınları.

Bintziou, A., Alexandris, N. ve Chrissikopoulos, V. (1999). *Introducing IT- security Awareness in schools: the Greek Case.* IFIP WG 11.8st World Conference on Information Security Education WISE1. Citeseer.

Brady, C. (2010). *Security Awareness for Children.* Technical Report RHUL–MA–2010–05 (Department of Mathematics Royal Holloway, University of London Egham, Surrey TW20 0EX, England.) [Online]: https://www.ma.rhul.ac.uk/static/techrep/2010/RHUL-MA-2010-05.pdf adresinden 25.10.2015 tarihinde erişilmiştir.

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

Büyüköztürk, Ş. (2011). *Sosyal bilimler için veri analizi el kitabı.* Ankara: Pegem Akademi Yayıncılık.

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 Bulunuşluk 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.

Eckertova, L., Docekal, D., ve Pozar, J. (2013). *Child Safety on the Internet: Mentor responsible parents.*1st Ed. Brno: Computer Press, 54-78.

Gülmüş, M. (2010). *Kurumsal bilgi güvenliği yönetim sistemleri ve güvenliği*. Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi, Elektrik Mühendisliği Anabilim Dalı, İstanbul.

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.

Kim, B. E. (2013). Information security awareness status of business college: Undergraduate students. *Information Security Journal: A Global Perspective, 22*(4), 171-179.

Kjorvik, 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.

Kritzinger, 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.

Lawshe, C. H. (1975). Aquantitative approach to content validity. *Personnel Psychology, 28,* 563–575.

Mackay H. (Ed) (1997). *Consumption and everyday life. Culture, Media & Identity.* London: Sage Publications in association with the Open University.

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.

Marks A. (2007). *Exploring universities' information systems security awareness in a changing higher education environment: a comparative case study research.* PhD thesis, University of Salford.

MEB (2014). *Millî Eğitim İstatistikleri, Örgün Eğitim 2013-2014.* T.C. Millî Eğitim Bakanlığı Strateji Geliştirme Başkanlığı, Ankara. [Online]: http://sgb.meb.gov.tr/www/milli-egitim-istatistikleri-orgun-egitim-2013-2014/icerik/95 adresinden 11.04.2014 tarihinde erişilmiştir.

Mitnick, K. (2002). *The Art of Deception.* Hoboken, NJ: John Wiley & Sons.

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, Gjovik University, College Department of Computer Science and Media Technology, Hogskolen. [Online]: http://brage.bibsys.no/ adresinden 17.09.2015 tarihinde erişilmiştir.

Pltier, T. R. (2005). Implementing an Information Security Awareness Program, CISSP,CISM Information system security. *security management practices. 14*(2), 37-49.

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.

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

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.

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

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

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.

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

Vural, Y. (2007). *Kurumsal bilgi güvenliği ve sızma (penetrasyon) testleri.* Yüksek lisans tezi, Gazi Üniversitesi, Bilgisayar Mühendisliği Anabilim Dalı, Ankara.

Zwick, W. R. ve Velicer, W. F. (1986). Comprasion of five rules for determining the number ofcomponents to retain. *Psychological Bulletin, 99*(3), 432-442.