International Journal of Human Sciences
ISSN:1303-5134

Volume: 12 Issue: 2 Year: 2015

Personal Cyber Security Provision Scale development study

Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması

Osman Erol[1]
Yusuf Levent Şahin[2]
Eray Yılmaz[3]
Halil İbrahim Haseski[4]

Abstract

The aim of this study is to develop a scale to determine internet users behavior related to cyber security. In this context created an item pool in accordance with expert opinion. This item pool was administered to 810 people for exploratory factor analysis. In exploratory factor analysis; principal component analysis method which is commonly used and Varimax vertical rotation method to determine the factor structure was used. Scale was administered to 292 people and structural equation modeling approach was applied to confirmation study.As a result of factor analysis,"Personal Cyber Security Provision Scale" which consists of 5 factors and 25 items and has a good compatibility was occurred.

Keywords: Personal Cyber Security Provision Scale, adaptation, validity, reliability, cyber security

(Extended English abstract is at the end of this document)

Özet

Bu araştırmanın amacı internet kullanıcılarının siber güvenlik ile ilgili davranışlarını belirlemeye yönelik bir ölçek geliştirmektir. Bu bağlamda öncelikle uzman görüşü doğrultusunda 26 maddelik bir madde havuzu oluşturulmuştur. Bu madde havuzu yapı geçerliliğinin test edilmesi için Facebook sosyal paylaşımda bir uygulamayı kullanan 810 kişiye uygulanarak açımlayıcı faktör analizi yapılmıştır. Açımlayıcı faktör analizinde en sık kullanılan yöntem olan temel bileşenler analizi yöntemi kullanılmış, ölçekteki faktör yapısını belirlemek için ise Varimax - dikey döndürme yöntemi kullanılmıştır. Ölçeğin doğrulama çalışması için ise aynı sosyal ağ uygulamasını kullanan ve daha önce ölçeğin uygulandığı kişilerin elendiği292 kişinin verisi kullanılarak yapısal eşitlik modeli yaklaşımı uygulanmıştır. Açımlayıcı faktör analizi sonucunda 5 faktörlü ve 25 maddeden oluşan; doğrulayıcı faktör analizi sonucunda ise elde edilen uyum indekslerine göre iyi bir uyuma sahip "Kişisel Siber Güvenliği Sağlama Ölçeği" ortaya çıkmıştır.

Anahtar Kelimeler: Kişisel Siber Güvenliği Sağlama Ölçeği, uyarlama, geçerlilik, güvenirlik, siber güvenlik

[1] Öğr. Gör. Dr., Mehmet Akif Ersoy Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğrt. Tekn. Eğt. Bölümü, oerol@mehmetakif.edu.tr
[2] Yrd. Doç. Dr., Anadolu Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğrt. Tekn. Eğt. Bölümü, ylsahin@anadolu.edu.tr
[3] Dr., Balıkesir T.C. Ziraat Bankası Fen Lisesi, eray_yilmaz@yahoo.com
[4] Arş. Gör., Anadolu Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğrt. Tekn. Eğt. Bölümü, himhaseski@anadolu.edu.tr

Erol, O., Şahin, Y. L., Yılmaz, E. & Haseski, H. İ. (2015). Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması. *International Journal of Human Sciences*, *12*(2), 75-91. doi: 10.14687/ijhs.v12i2.3185

Giriş

İnternet kullanıcı sayısı dünya genelinde hızla artmaya devam etmektedir. Türkiye İstatistik Kurumu'nun 2012 yılında yayınladığı rapora göre Türkiye' de de 2011 yılında internete erişim hane oranı %42'lerde iken 2012 yılında bu oran %48 seviyesine yükselmiştir (TUİK, 2012). Neredeyse her iki kişiden birinin kullanıcısı olduğu internet, oldukça popüler bir teknolojidir.Ancak internet, sağladığı birçok olanağın yanı sıra çeşitli güvenlik sorunlarını da beraberinde getirmiştir (Goodman,2008; Öğün ve Kaya, 2013).Bu durum, kullanıcılar açısından birçok risk doğurmuştur (Çubukçu ve Bayzan, 2013).

İnternetin kullanımı ile doğan riskler kullanıcıyı ruhsal ve fiziksel olarak doğrudan etkileyebildiği gibi, kullanıcılara sosyal ve maddi açıdan da zarar verebilmektedir (De Moor, Dock, Gallez, Lenaerts, Scholler ve Vleugels, 2008; Kim, Jeong, Kim ve So, 2011; Valcke, Bonte, De Wever ve Rots, 2010; Çubukçu ve Bayzan, 2013). Virüsler, istenmeyen mesajlar (spam), korsanlık faaliyetleri (hacking), oltalama (phishing) ve reklam dolandırıcılığı gibi tehditler doğrudan teknoloji odaklı iken; siber zorbalık, istismar, terör ve gizlilik ihlalleri gibi tehditler de teknoloji odaklı olmayan risklerdir (Kim ve diğerleri, 2011). De Moor ve arkadaşlarına (2008) göre ise nefret söylemi, şiddet, ırkçılık, yanlış bilgilendirme, olumsuz propaganda ve porno gibi tehditler "içerik" başlığı altında; siber zorbalık, cinsel istismar ve gizlilik ihlalleri gibi tehditler "temas" başlığı altında; oltalama ve zararlı (casus) yazılımlar ile kimlik hırsızlığı ile dolandırıcılık gibi tehditler ise "ticari riskler" başlığı altında toplanmaktadır (Valcke ve diğerleri, 2010; Çubukçu ve Bayzan, 2013).

Zararlı yazılımlar internet aracılığıyla karşılaşılan tehditlerin başında gelmektedir. Bu yazılımlar genellikle, girdikleri sisteme doğrudan zarar verdiği gibi kullanıcılara ait bilgileri ele geçirerek dolaylı olarak da zarar vermektedirler. Servislere ve programlara zarar veren virüsler, kendini kopyalayan solucanlar, oyun gibi zararsız öğelerin içinde bilgisayarlara sızan casus yazılımlar (truva atları, keylogger spyware) zararlı yazılımlara örnek gösterilebilir (Graham ve Howard, 2010). İnternet üzerinden karşılaşılabilecek tehditlerden biri olan gizlilik ihlalleri de sık karşılaşılan siber tehditlerden birisidir (Valcke ve diğerleri, 2010).Kimlik numarası, iletişim bilgileri, adres ve kredi kartı numarası gibi şahsi bilgilerin bilerek ya da bilmeyerek üçüncü şahıslarla paylaşılması birçok risk oluşturmaktadır.Son zamanlarda ise sosyal mühendislik yöntemleri ile kimlik hırsızlığı ve dolandırıcılık gibi tehditlerde de artış görülmüştür(Garfinkel, 2012). Kimlik hırsızlığında en sık kullanılan yöntemlerden biri oltalama (phishing) adı verilen saldırı yöntemidir .Bu yöntemde genellikle sahte web sayfaları kullanılmaktadır. Bir banka yada alış veriş sitesinden e posta geldiğini düşünen kullanıcı; kredi kartı yada bankacılık bilgilerini sahte web sayfasına girerek yada e postayı yanıtlayarak bu tuzağa düşmektedir (Çubukçu ve Bayzan, 2013). Hatta kurumlara ait bilgi ve logolar kullanılarak sahte e postanın gerçekliği artırılmaktadır.Bilgisayarlara sızmak için kullanılan keylogger

Erol, O., Şahin, Y. L., Yılmaz, E. & Haseski, H. İ. (2015). Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması. *International Journal of Human Sciences*, *12*(2), 75-91. doi: 10.14687/ijhs.v12i2.3185

ve truva atı gibi zararlı yazılımlar da kimlik hırsızlığı için kullanılabilmektedir. İnternet kullanıcıları ayrıca,internet üzerinden siber zorbalığa ve cinsel istismara uğrama tehdidi altındadır. Siber zorbalık, bilgi ve iletişim teknolojilerini kullanarak bir birey ya da gruba karşı yapılan teknik ya da ilişkisel tarzda zarar verme, kaba davranma ve kötü söz söylemeyi kapsayan davranışlar bütünü olarak tanımlanmaktadır (Smith, Mahdavi, Carvalho, Fisher, Russel ve Tippet, 2008). Siber zorbalık kavram olarak genel zorbalıktan farklıdır. Bir davranışın siber zorbalık tanımına uyması, dijital bir teknolojinin kullanılmış olmasını gerektirir. Genellikle sahte profil kullanılarak yapılan cinsel istismar ise bazen sadece sanal ortamda kalmakta, bazen de gerçek hayata taşınmaktadır. Doğrudan yada dolaylı şekilde ortaya çıkan siber tehditlerin dünya ekonomisine verdiği zarar yaklaşık 1 trilyon dolar civarındadır (Kane, 2010).

Tüm bu riskler bazen maddi zararlara bazen de hayati tehlikelere yol açabilmektedir. Ancak birtakım temel önlemler ile sanal dünyanın gerçek tehlikelerinden korunmak mümkündür. Bu tedbirler bireysel olabildiği gibi devlet eliyle ve yasalar yoluyla da olabilmektedir.Bu konuda yapılmış çalışmalar ışığında ulaşılan güvenlik önlemleri aşağıdaki gibi maddelenebilir (Karakoç, 2011; Yavanoğlu, Sağıroğlu ve Çolak, 2012; Yılmaz, Yılmaz ve Sezer, 2014):

- Web sayfalarında kendiliğinden açılan sayfaların(pop-up) kapatılması,
- Bilgisayarda antivirüs yazılımı bulundurulması,
- Bilgisayarda bulunan yazılımlarının, özellikle güvenlik yazılımlarının güncel olması,
- Web sayfalarının güvenlik sertifikalarını kontrol edilmesi,
- Kullanılan şifrelerin kolay tahmin edilebilir olmaması ve farklı simge, karakter, rakam içermesi,
- Şifre hatırlatma için kullanılan gizli soruların ve cevaplarının basit seçilmemesi,
- Kullanılan şifrelerin birbiriyle aynı olmaması ve bağımsız olması,
- Bilgisayarda yer alan dosyaların yedeklenmesi,
- Güvenli olmayan e-postaların açılmadan silinmesi,
- E-postalara gelebilecek kimlik bilgilerinin doğrulama (şifre, kart bilgisi vb.) mesajlarına itibar edilmemesi,
- E postalarda farklı bağlantılardan gelen web sayfa linklerinin açılmaması,
- E postalarda farklı bağlantılardan gelen web sayfa linklerine giriş işlemi yapılmaması,
- Şifreli işlemlerde işlem bitince oturumun kapatılması;
- Kablosuz ağ modemlerinin şifresiz kullanılmaması,
- Kablosuz ağ modemlerinin şifrelerinin belli aralıklarla değiştirilmesi
- Sosyal paylaşım ağlarında şahsi bilgilerin paylaşılmaması,

Erol, O., Şahin, Y. L., Yılmaz, E. & Haseski, H. İ. (2015). Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması. *International Journal of Human Sciences*, *12*(2), 75-91. doi: 10.14687/ijhs.v12i2.3185

- Sosyal paylaşım ağlarında gerekmedikçe özel olduğu düşünülen fotoğrafların paylaşımının yapılmaması,
- Sosyal paylaşım ağlarında gerekmedikçe yer bildirimi yapılmaması,
- Sosyal paylaşım ağlarında gelen arkadaşlık isteklerinde dikkat edilmesi,
- Sosyal paylaşım ağlarında gelen reklamlar üzeriden alış veriş yapılmaması,
- Bankacılık ve çevrimiçi alışveriş işlemlerinin gerekmedikçe şahsi bilgisayarlar dışında kullanılmaması,
- Çevrimiçi alışveriş işlemlerinde sanal kart ve limit kullanılması,
- Sosyal paylaşım ağları üzerinden yada e posta ile yapılan para, kontör vb. isteklere itibar edilmemesi,
- Sosyal paylaşım ağlarında yada sohbet sitelerinde yabancı kişiler ile görüntülü ve sesli iletişime geçilmemesi,
- Sosyal paylaşım ağlarında yada sohbet sitelerinde tanışılan yabancı kişiler ile gerçek hayatta yüz yüze iletişime geçilmemesi,
- İnternet üzerinden tehdit, şantaj yada cinsel istismara maruz kalma durumunda yasal yollara başvurulması şeklinde tedbirler alınabilir.

Birçok internet kullanıcısının yukarıda maddelenen güvenlik önlemlerinin farkında olmadığı görülmektedir. Öğütçü (2010) yaptığı çalışmasında, katılımcıların bilişim güvenliği farkındalık oranlarının çok yüksek olmadığı ve bireysel olarak korumacı davranışların henüz tam olarak gelişmediği bulgusuna ulaşmıştır. Furnell, Jusoh ve Katsabas' ın yaptıkları çalışmaya (2005) göre ise internet kullanıcılarının virüs benzeri zararlı yazılımlar ile ilgili tehlikelerle ilgili farkındalıkları yüksek iken, sosyal mühendisliğe dayalı oltalama (phishing) saldırılarına dair farkındalıkları düşüktür. Diğer bir çalışmada katılımcılarının yarısından fazlasının kredi kartı bilgilerinin ele geçirileceği endişesiyle çevrimiçi alışveriş yapmaktan kaçındıkları görülmektedir (Yenisey, Ozok ve Savendy, 2008). Yılmaz ve arkadaşları (2014) ise üniversite öğrencileri ile yaptıkları çalışmada öğrencilerin genel olarak BİT kullanımında güvenli davrandığı ancak antivirüs kullanma dışındaki önlemleri almakta yetersiz kaldığı sonucuna ulaşmıştır. Kaşıkçı, Çağıltay, Karakuş ve Ogan (2014) Avrupa ve Türkiye' yi kapsayan çalışmalarına göre çalışmaya katılan çocukların birçok çevrimiçi risklere maruz kaldığı ve ebeveynlerin çocuklarını internette karşılaşabilecekleri risklerden uzak tutmayı sağlayacak yeterli bilgiye sahip olmadıkları görülmektedir. Tüm bu sonuçlar her yaştan internet kullanıcısının bilişim güvenliği konusundaki bilinçsizliğin göstergesi olarak değerlendirilebilir.

Erol, O., Şahin, Y. L., Yılmaz, E. & Haseski, H. İ. (2015). Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması. *International Journal of Human Sciences*, *12*(2), 75-91. doi: 10.14687/ijhs.v12i2.3185

Yapılan çalışmalar incelendiğinde her yaştan, meslekten ve topluluktan bilgisayar ve internet kullanıcısının aslında siber güvenlik riskleri ile ilgili farkındalıklarının genel olarak yetersiz olduğu görülmektedir (Çubukçu ve Bayzan, 2013; Demirel, Yörük ve Özkan, 2012; Kaşıkçı ve diğerleri, 2014; Öğütçü, 2010; Yavanoğlu ve diğerleri, 2012, Yılmaz ve diğerleri, 2014). Çalışmalarda genellikle veri toplama aracı olarak anket kullanıldığı, görüşme yapıldığı yada örnek olayların analiz edildiği görülmektedir. Bu çalışmada; yapılmış çalışmalara katkı sağlamak amacıyla internet kullanıcılarının siber güvenlik ile ilgili davranışlarını belirlemeye yönelik bir ölçek geliştirmek amaçlanmaktadır.

Yöntem

Araştırma Grubu

Araştırmaya 810 kişi katılmıştır. Katılımcılar ile iletişim Facebook sosyal ağında bulunan bir uygulama üzerinden sağlanmıştır. Sözü edilen uygulama her yaştan bireyin kullandığı Türkçe bir uygulamadır. Böylelikle demografik özellikler açısından daha geniş bir örnekleme ulaşılması amaçlanmıştır. Katılımcıların yaş dağılımı ele alındığında en genç katılımcının 11 yaşında en yaşlı katılımcının ise 58 yaşında olduğu görülmüştür. Katılımcıların büyük çoğunluğu (%65) 18 ile 30 yaş arasında bireylerden oluşmaktadır.Ancak katılımcıların 72' si(%9)kadın, 738' i (%91) erkektir. Katılımcıların erkek ağırlıklı olması ve sadece Facebook sosyal ağında yer alan uygulamayı kullanan katılımcıların olması araştırma açısından bir sınırlılık olarak ele alınabilir. Faktör analizi için; Tabchnick ve Fidel (1996)' e ve Field (2000)' e göre 300 katılımcı yeterli iken Kass ve Tinsley' e (1979) göre ise 300 katılımcıya kadar her bir madde için en az 10 kişi yeterli gelmektedir (Akbulut, 2010). Bu durumda katılımcı sayısının faktör analizi için uygun olduğu söylenebilir.

Ölçeğin doğrulama çalışması için ise aynı sosyal ağ uygulaması üzerinden 510 kişiye ölçeğin son hali uygulanmıştır. Fakat doğrulama çalışması için daha önce ölçeğin uygulandığı kişiler, kullanıcı numaraları üzerinden elenerek analiz dışı bırakılmıştır. Böylelikle ölçeğin doğrulama çalışması için geriye kalan 292 kişiye ait veri analiz edilmiştir.

Ölçme Aracının Geliştirilmesi

Ölçeğin geliştirilmesi aşamasında öncelikle madde havuzu oluşturulmaya çalışılmıştır. Bu doğrultuda araştırmacılar tarafından literatür taraması (Karakoç, 2011; Kaşıkçı ve diğerleri, 2014; Mert, Bülbül ve Sağıroğlu, 2012; Öğün ve Kaya, 2013; Öğütçü, 2010; Yavanoğlu ve diğerleri, 2012) yapılarak 55 maddelik bir madde havuzu oluşturulmuştur. Kapsam geçerliliğinin sağlanması amacıyla "Bilgisayar ve Öğretim Teknolojileri Eğitimi" bölümünden iki öğretim üyesi ve aynı alanda doktora yapan üç doktora öğrencisi taslak maddeleri inceleyerek değerlendirmişlerdir. Uzman görüşü doğrultusunda 29 madde atılarak ölçek 26 maddeye düşürülmüştür. Ölçek 5' li likert tipi olarak hazırlanmıştır ve her bir madde, "1-Hiçbir zaman", "2-Nadiren", "3-Arasıra", "4-Sıksık" ve

Erol, O., Şahin, Y. L., Yılmaz, E. & Haseski, H. İ. (2015). Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması. *International Journal of Human Sciences*, *12*(2), 75-91. doi: 10.14687/ijhs.v12i2.3185

"5-Her zaman" arası değerler almaktadır. Ayrıca ölçekte yer alan M6, M8, M13,M14, M18,M19,M20,M21,M25,M26 maddeleri ters madde olarak belirlenmiştir.

Verilerin Analizi

Ölçeğin yapı geçerliliğinin test edilmesi için açımlayıcı faktör analizi yapılmıştır. Faktör analizi sonucunda oluşan ölçeğin tamamında ve faktör analizi sonucu belirlenen her alt boyutta ölçek maddelerinin güvenilirlik analizi yapılmıştır. Faktör analizinde temel bileşenler analizi yöntemi kullanılmıştır. Temel bileşenler analizi faktör analizinde hata terimini ihmal eden, değişken azaltma ve anlamlı kavramsal yapılara ulaşmayı amaçlayan en sık kullanılan yöntemdir (Büyüköztürk, 2012).Örneklemin faktör analizine uygunluğunu belirlemek için Kaiser- Meyer-Olkin (KMO) katsayısı belirlenmiş, veri matrisinin faktör analizine uygunluğu için Barlett Küresellik testi uygulanmıştır. KMO değerinin 0.60 dan büyük olması ve Barlett Sphericity değerinin anlamlı çıkması ($p<0.05$) örneklemin ve veri setinin faktör analizi için uygun olduğunu gösterir (Büyüköztürk, 2012; Tabachnick ve Fidell, 2001).Faktör sayısını belirlemede öz değer olarak alt sınır 1.00 alınmıştır. Ölçekteki faktör yapısını en anlamlı görebilmek için eksen döndürme yöntemi yapılmış ve bunun için sosyal bilimlerde en sık kullanılan Varimax - dikey döndürme yöntemi kullanılmıştır (Çokluk, Şekercioğlu, Büyüköztürk, 2010).

Ölçeğin doğrulama çalışması için ise LISREL paket programı kullanılarak yapısal eşitlik modeli yaklaşımı kullanılmıştır. Ölçek modelinin test edilmesi için χ^2, RMSEA,RMSEA, SRMR, NFI, NNFI, CFI, GFI ve AGFI uyum indeksleri referans alınmıştır.

Bulgular

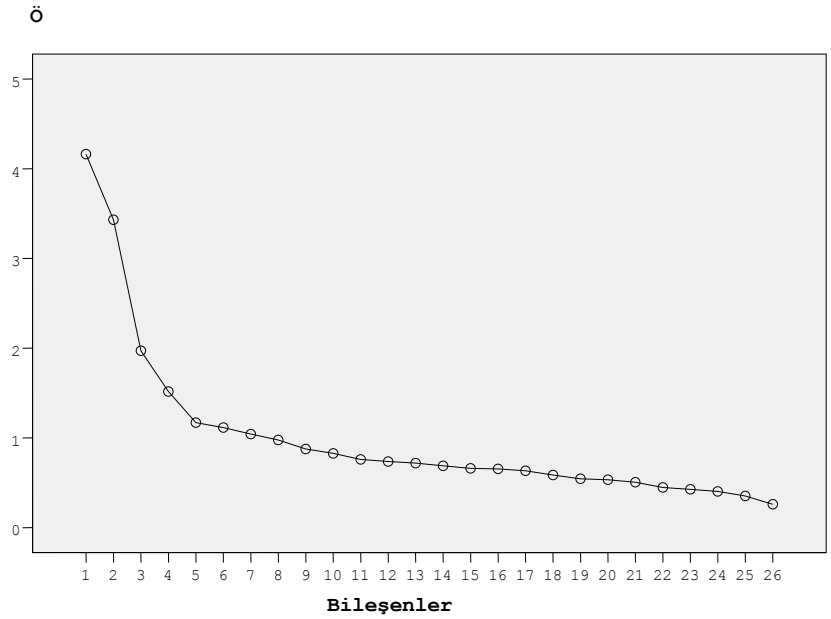
Yapı Geçerliliğine İlişkin Bulgular

Ölçeğin yapı geçerliliğinin test edilmesi için açımlayıcı faktör analizi yapılmış ve temel bileşenler analizi yöntemi kullanılmıştır. Veri matrisinin ve örneklemin faktör analizine uygunluğu incelendiğinde KMO uyum ölçüsü değeri 0.799 ve Barlett Küresellik testinin ise anlamlı olduğu bulunmuştur ($p<0.01$). Buna göre KMO değerinin 0.60' dan büyük olması ve Barlett Küresellik testinin anlamlı çıkması veri matrisinin ve örneklemin faktör analizi için uygun olduğunu göstermektedir (Büyüköztürk, 2012).

Faktör analizi yapılırken maddelerin faktörler altındaki yük değerlerinin en az 0.45 olması madde seçimi için iyi bir ölçüdür fakat bu değer 0.30'a kadar indirilebilir. Yine ayrıca ölçekte maddelerin faktörler altında toplanırken birden fazla faktör altında toplanması maddenin binişik olduğunu gösterir. Yüksek iki yük arasındaki farkın en az 0.10 olması binişiklik açısından önemlidir

Erol, O., Şahin, Y. L., Yılmaz, E. & Haseski, H. İ. (2015). Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması. *International Journal of Human Sciences*, *12*(2), 75-91. doi: 10.14687/ijhs.v12i2.3185

(Büyüköztürk, 2012). Madde yükleri açısından analiz sonucunda 1. madde iki faktör altında da yüksek madde yükü oluşturmuş ve binişiklik göstermiştir. Bu yüzden ölçekten çıkarılmış ve analiz tekrar yapılmıştır.



Şekil1. Özdeğer - bileşen grafiği

Başlangıç özdeğer - bileşen grafiği (Şekil1) incelendiğinde eksen döndürmesi (Rotasyon) yapılmamış faktör analizinde ilk belirlemede özdeğeri 1.00 dan yüksek 7 faktör ortaya çıkmıştır. Bu 7 faktörlü ilk yapıda açıklanan varyans %55.413 olarak hesaplanmıştır. Fakat başlangıç özdeğer bileşen grafiği incelendiğinde eğrinin 5. bileşende keskin düşüşünü ivmeli bir düşüşe çevirdiği görülmektedir. Bundan dolayı ilk etapta ortaya çıkan 7 faktörlü yapı yerine 5 faktörlü yapı ile sınırlandırılarak eksen döndürme ile faktör analizi yeniden yapılmıştır. Maddelerin faktör altındaki madde yükleri tekrar incelenmiş ve madde yükü 0.30 dan düşük ve binişiklik gösteren hiçbir madde kalmamıştır. Buna göre son yapılan faktör analizine göre maddelerin faktörlere dağılımı aşağıdaki gibidir.

Erol, O., Şahin, Y. L., Yılmaz, E. & Haseski, H. İ. (2015). Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması. *International Journal of Human Sciences*, *12*(2), 75-91. doi: 10.14687/ijhs.v12i2.3185

Tablo1. Faktörlere ilişkin tanımlayıcı istatistikler ve maddeler

Faktörler ve Maddeler	Açıklanan Varyans (%)	Yük Değeri	Döndürme Sonrası Yük Değerleri
Faktör1: Kişisel Gizliliği Koruma			
M21. Sosyal ağlarda yer alan reklamlar üzerinden alışveriş yaparım	15.721	.687	.684
M18. Tanımadığım kişilerden gelen e-posta eklerini açarım		.669	.664
M26. Banka, online alışveriş sitesi gibi sitelerden gelen e postalara (kart numarası, şifre vb. istekler) itibar ederim ve yanıtlarım		.637	.639
M14. İnternet ortamında gerektiğinde kişisel bilgilerimi (TC No,Doğum tarihi,Gsm No vb.)paylaşırım		.635	.625
M19. Sosyal paylaşım sitelerinde kişisel bilgilerime yer veririm		.574	.570
M13.Tanımadığım kişiler ile web kamerası kullanarak sesli ve görüntülü iletişim kurarım		.527	.537
M25. Unutmamak için akılda kalan kolay bir şifre belirlerim		.546	.536
M20. İnternet üzerinden yer bildirimi yaparım		.492	.513
M8. E- posta ile gelen kimlik doğrulama mesajlarını (kullanıcı adı, şifre vb. istekler)cevaplarım		.413	.460
M6.İnternet şifrelerimin tümünün aynı olmasına dikkat ederim		.438	.434
Faktör2: Güvenilmeyenden Kaçınma			
M12 Güvenmediğim sitelere üye olmam	13.721	.644	.844
M10 İnternet üzerinden yapılan para ve kontör isteklerini dikkate almam.		.617	.798
M11 Tanımadığım kişilerden gelen sosyal ağ arkadaşlık isteğini kabul etmem.		.610	.774
M23 Güvenmediğim sitelerden dosya indirmem		.533	.566
Faktör3: Önlem Alma			
M3 Kullandığım yazılımları güncellerim.	7.861	.582	.716
M4 Bilgisayarımda antivirus yazılımı bulundururum		.412	.669
M2 Web sayfalarında güvenlik bağlantılarını (https://) ve sertifikalarını kontrol ederim		.523	.581
M5 Şifrelerimi belirlerken basit dizilimler kullanmaktan kaçınırım		.539	.551
M7 Web tarayıcımın güvenlik ayarlarını düzenlerim		.532	.527
Faktör4: Ödeme Bilgilerini Koruma			
M17 Online alışveriş işlemlerini şahsi bilgisayarımdan yaparım	6.043	.732	.882
M16 İnternet bankacığı işlemlerini şahsi bilgisayarımdan yaparım.		.738	.870
Faktör5: İz Bırakmama			
M24 İnternette kullandığım (eposta, sosyal ağ vb.)şifreleri değiştiririm	4.440	.483	.633
M15 Web geçmişimi temizlerim		.494	.510
M22 Sosyal ağ - e-posta gibi hesaplarda işim bittiğinde oturumu kapatırım		.487	.496
M9 Şahsi bilgisayarım dışında kullanılan bilgisayarlarda bilgilerimin kalmamasına dikkat ederim		.539	.461
Toplam: Kişisel Siber Güvenliği Sağlama Ölçeği	48.026		

Faktör analizi sonucunda 5 faktörlü bir ölçek ortaya çıkmıştır.Bu yapı toplam varyansın %48.026' sını açıklamaktadır. Birinci faktör toplam varyansın %15.721' ini, ikinci faktör %13.721' ini, üçüncü faktör %7.861' ini, dördüncü faktör %6.043' ünü ve beşinci faktör ise %4.440' ını

Erol, O., Şahin, Y. L., Yılmaz, E. & Haseski, H. İ. (2015). Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması. *International Journal of Human Sciences*, *12*(2), 75-91. doi: 10.14687/ijhs.v12i2.3185

açıklamaktadır. Dunteman (1989)' a göre sosyal bilimlerde açıklanan varyansın yüzde 40-60 arasında olması makul bir orandır(Akbulut, 2010).

Tablo2. Ölçek maddelerinin faktörlere dağılımına ait son durum

Faktör	Madde Sayısı	Faktör Adı	İçerdiği Maddeler
1	10	Kişisel Gizliliği Koruma	M5-M7-M12-M13- M17-M18-M19-M20-M24 - M25
2	4	Güvenilmeyenden Kaçınma	M9-M10-M11-M22
3	5	Önlem Alma	M1-M2-M3-M4-M6
4	2	Ödeme Bilgilerini Koruma	M15-M16
5	4	İz Bırakmama	M8-M14- M21-M23

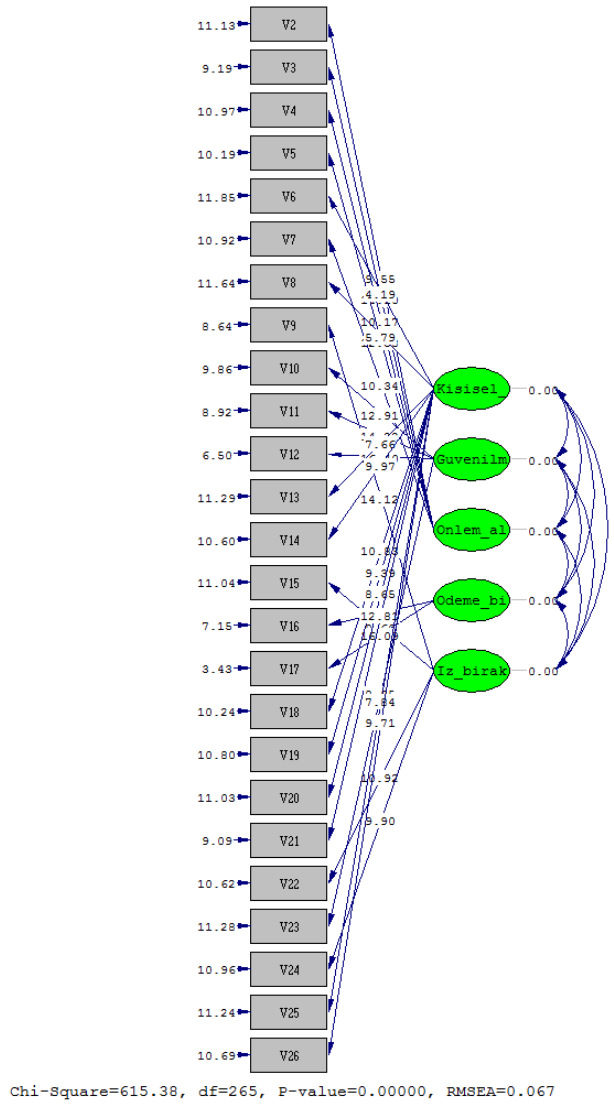
Her bir faktördeki maddeler ele alındığında1. faktöre "Kişisel Gizliliği Koruma", 2. faktöre " Güvenilmeyenden Kaçınma", 3. faktöre "Önlem Alma", 4. faktöre "Ödeme Bilgilerini Koruma" ve 5. faktöre ise "İz Bırakmama" ismi verilmiştir.

Güvenilirliğe İlişkin Bulgular

Ölçeğin iç tutarlılık katsayısının hesaplanması için Cronbach Alpha katsayısı (α)kullanılmıştır. Buna göre ölçeğin tamamı için güvenilirlik kat sayısı 0.735; 1. alt boyut "Kişisel Gizliliği Koruma" için 0.763; 2. alt boyut " Güvenilmeyenden Kaçınma" için 0.771; 3. alt boyut " Önlem Alma" için 0.704; 4. alt boyut " Ödeme Bilgilerini Koruma" için 0. 829; 5. alt boyut " İz Bırakmama" için ise 0.557 olarak bulunmuştur.

Erol, O., Şahin, Y. L., Yılmaz, E. & Haseski, H. İ. (2015). Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması. *International Journal of Human Sciences*, *12*(2), 75-91. doi: 10.14687/ijhs.v12i2.3185

Doğrulayıcı Faktör Analizine İlişkin Bulgular



Şekil2. Ölçek modeli için gizli değişkenlerin gözlenen değişkenleri açıklama oranlarının anlamlılık düzeyleri

Şekil 2' de görüldüğü üzere, gizil değişkenlerin gözlenen değişkeni açıklama durumlarına ilişkin t değerleri oklar üzerinde gösterilmiştir. Parametre tahminleri eğer t değerleri 1.96' yı aşarsa .05 düzeyinde ve 256' yı aşarsa .01 düzeyinde anlamlıdır (Çokluk ve diğerleri, 2010). Bu durumda Şekil2 incelendiğinde tüm değerlerin .01 düzeyinde anlamlı olduğu görülmektedir. Ayrıca tahminler bölümünden gözlenen değişkenlerin hata varyansları da incelenmiş ve yüksek hata varyansına sahip hiçbir değişken gözlenmemiştir.

Erol, O., Şahin, Y. L., Yılmaz, E. & Haseski, H. İ. (2015). Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması. *International Journal of Human Sciences*, *12*(2), 75-91. doi: 10.14687/ijhs.v12i2.3185

Tablo3.Ölçek modeline ilişkin uyum indeksleri tablosu

Uyum İndeksi	Değer	Kriter Değer	Durum	Kaynak
χ^2	p=0.000	0.05 ≤p≤ 1.00		
χ^2 /sd	2.322	0 ≤ χ^2 /sd ≤ 2.5	Mükemmel uyum	Kline, 2005
RMSEA	.067	0 ≤ RMSEA ≤ 0.07	İyi uyum	Steiger, 2007
SRMR	.076	0 ≤ SRMR ≤ 0.08	İyi uyum	Brown, 2006; Hu ve Bentler, 1999
NFI	.89	0.90 ≤ NFI ≤ 1.00		
NNFI	.93	0.90 ≤ NNFI ≤ 1.00	İyi uyum	Kelloway, 1998; Sümer, 2000
CFI	.94	0.90 ≤ NNFI ≤ 1.00	İyi uyum	Hu ve Bentler, 1999; Sümer, 2000;
GFI	.86	0.90 ≤ GFI≤ 1.00		
AGFI	.82	0.90 ≤ AGFI≤ 1.00		

χ^2 : 615.38 ; sd: 265

Tablo3uyum indeksleri incelendiğinde ilk olarak beklenen kovaryans matrisi ile gözlenen kovaryans matrisi arasındaki farkın anlamlı olduğu görülmektedir ($\chi^2_{(265)}$:615.38; p<.01). Fakat bu durum arzu edilen bir durum değildir. Çünkü değerinin anlamlı çıkmaması gerekmektedir. Fakat örneklem büyüklüğünden kaynaklı olarak birçok doğrulayıcı faktör analizi çalışmasında bu değerin anlamlı çıkması normaldir. Bu yüzden bu durum tolere edilebilmektedir (Çokluk ve diğerleri, 2010).Bir diğer uyum indeksi değeri ise χ^2 ve χ^2/sd değerleridir. χ^2 değeri tek başına değerlendirilen bir değer değildir. χ^2/sd değeri ile birlikte ele alındığında χ^2 değerinin sd ye oranı 2.322 bulunmuştur. Bu değer Kline (2005)' a göre mükemmel uyuma karşılık gelmektedir.Yol şemasında yer alan RMSA (yaklaşık hataların ortalama karekökü) uyum indeksi değeri incelendiğinde 0.067 değerinin iyi uyuma işaret ettiği görülmektedir (Steiger, 2007).Standardize edilmiş RMR uyum indeksi değeri ise 0.076 olarak hesaplanmıştır. Bu değer de iyi uyuma karşılık gelmektedir (Brown, 2006; Hu ve Bentler, 1999). Normlaştırılmış uyum indeksi (NFI) ve Normlaştırılmamış uyum indeksi değerleri (NNFI) incelendiğinde NFI 0.89; NNFI ise 0.93 olarak hesaplanmıştır. NNFI uyum indeksinde 0.90' ın üzerinde iyi uyuma rastlanmış (Kelloway, 1998; Sümer, 2000) fakat NFI da ise iyi uyuma yakın bir uyuma rastlanmıştır. Karşılaştırmalı uyum indeksi (CFI) incelendiğinde 0.94 olduğu görülmektedir. Bu değer CFI değerinin iyi uyuma sahip olduğunu göstermektedir (Hu ve Bentler, 1999; Sümer, 2000). Son olarak iyilik uyum indeksi (GFI)ve düzenlenmiş iyilik uyum indeksi (AGFI) incelendiğinde GFI' nın 0.86, AGFI' nın ise 0.82 olduğu görülmektedir. Hem GFI uyum indeksinin hem de AGFI uyum indeksinin 0.90' a yakın bir değer olması ise iyi uyuma yakın bir uyum olduğunu göstermektedir (Schumacker ve Lomax, 1996; Kelloway, 1998; Sümer, 2000). Sonuç olarak elde edilen bu uyum indeksleri; geliştirilen Kişisel Siber Güvenliği Sağlama Ölçeğinin genel olarak iyi bir uyuma sahip olduğunu ortaya koymuştur.

Erol, O., Şahin, Y. L., Yılmaz, E. & Haseski, H. İ. (2015). Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması. *International Journal of Human Sciences*, *12*(2), 75-91. doi: 10.14687/ijhs.v12i2.3185

Sonuçlar ve Tartışma

İnternet bir çok faydasının yanında, kullanıcılar açısından bir çok riskler oluşturmaktadır. Bu riskler bazen maddi bazen de doğrudan fiziksel ve ruhsal sorunlara yola açabilmektedir.Yapılan araştırmalar incelendiğinde internet kullanıcılarının genel olarak zararlı yazılımlar ile ilgili güvenlik önlemlerinin farkında olduğu ancak internet üzerinden oluşabilecek tehlikeler hakkında farkındalıklarının yetersiz olduğu görülmektedir. Bu bağlamda bu çalışmada internet kullanıcılarının siber güvenliği sağlamaya ilişkin görüşlerinin belirleyen bir ölçek geliştirilmiştir. Ölçek oluşturulmadan önce alan yazın taramasına göre 55 maddeden oluşan madde havuzu oluşturulmuştur. Uzman görüşü doğrultusunda 29 madde atılarak 26 maddelik ölçek formu oluşturulmuştur. Bu form 810 kişiye uygulanmış ve faktör analizi yapılarak yapı geçerliliği test edilmiştir. Analiz sonucunda 25 maddeli 5 faktörlü bir ölçek elde edilmiştir. Ölçek toplam varyansın%48.026' sını açıklamaktadır. Birinci faktör olan "Kişisel Gizliliği Koruma" faktörü toplam varyansın %15.721' ini, ikinci faktör olan " Güvenilmeyenden Kaçınma " faktörü toplam varyansın %13.721' ini, üçüncü faktör olan " Önlem Alma " faktörü toplam varyansın %7.861' ini, dördüncü faktör olan " Ödeme Bilgilerini Koruma" faktörü toplam varyansın %6.043' ünü ve beşinci faktör olan "İz Bırakmama" faktörü toplam varyansın %4.440' ını açıklamaktadır. Oluşan ölçeğin güvenilirlik kat sayısı 0.735 olarak hesaplanmıştır, faktörlerin güvenilirlik kat sayıları ise 0.557 ile 0.829 arasında değişmektedir. Yapılan doğrulama çalışmasında genel olarak elde edilen uyum indeksleri ölçeğin iyi bir uyuma sahip olduğunu ortaya koymuştur.

Alanyazında birçok çalışmada katılımcıların bilgi güvenliği, güvenli internet yada internet davranışları hakkındaki görüşleri belirlenirken anketler kullanılmıştır. Bu anketler yoluyla elde edilen veriler yüzde ve frekans hesaplanarak mevcut durum belirlenmeye çalışılmıştır (Demirel ve diğerleri, 2012; Kaşıkçı ve diğerleri, 2014; Yılmaz ve diğerleri, 2014). Geliştirilen ölçek ile alan yazında yer alan bu çalışmalara ek olarak; ölçek ile elde edilecek veriler cinsiyet, bilgisayar kullanma sıklığı ve benzeri farklı bağımsız değişkenler ile karşılaştırılarak test edilebilir yada farklı ölçekler ile ilişkisinin incelendiği çalışmalar yapılabilir. Ancak çalışmanın Facebook uygulamasını kullanan katılımcıların yer aldığı bir örneklem üzerinden geliştirilmesi bir sınırlılık olarak ele alınmalıdır. Bu yüzden geliştirilen ölçek farklı örneklem gruplarında (orta okul, lise, üniversite öğrencileri, öğretmenler vb.) uygulanarak test edilmelidir.

Erol, O., Şahin, Y. L., Yılmaz, E. & Haseski, H. İ. (2015). Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması. *International Journal of Human Sciences*, *12*(2), 75-91. doi: 10.14687/ijhs.v12i2.3185

Kaynaklar

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

Brown, T. A. (2006). *Confirmatory Factor Analysis for Applied Research*. New York: GuilfordPress.

Büyüköztürk, Ş. (2012). *Sosyal Bilimler için Veri Analizi El Kitabı*. Pegem Akademi Yayıncılık.

Çokluk, Ö., Şekercioğlu, G. & Büyüköztürk, Ş. (2010). *Sosyal Bilimler İçin Çok Değişkenli İstatistik SPSS ve Lisrel Uygulamaları*. Ankara : Pegem Akademi.

Çubukçu, A. & Bayram Ş. (2013). Türkiye'de Dijital Vatandaşlık Algısı ve Bu Algıyı İnternetin Bilinçli, Güvenli ve Etkin Kullanımı ile Artırma Yöntemleri. *Middle Eastern & African Journal of Educational Research*, 5, 148-174.

De Moor, S., Dock, M., Gallez, S., Lenaerts, S., Scholler, C., & Vleugels, C., (2008). *Teens and ICT: Risksand Opportunitie*s. 11.10.2013 tarihindehttp://www.belspo.be/ belspo/fedra/TA/synTA08_nl.pdf.

Demirel, M., Yörük, M. & Özkan, O. (2012). Çocuklar İçin Güvenli İnternet: Güvenli İnternet Hizmeti ve Ebeveyn Görüşleri Üzerine Bir Araştırma. *Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,*4(7), 54-68.

Dunteman, G. H. (1989). *Principal component analysis. Quantitative applications in the social sciences series* (vol. 69). Thousand Oaks, CA: Sage Publications.

Field, A. (2000). *Discovering statistics using SPSS for windows*. London: Sage Publications.

Furnell, S. M., Jusoh, A. & Katsabas, D. (2005). The challenges of understanding and using security : A survey of end-users. *Computers & Security*,25(5),27 - 35.

Garfinkel, S. L. (2012). The cybersecurity risk. *Magazine Communications of the ACM*, 55(6),29-32.

Goodman, S. E. (2008). Critical Information Infrastructure Protection. *Centre of Excellence Defence Against Terrorism* (Ed.), Responses to Cyber Terrorism NATO Science for Piece and Security. Ankara: IOS Press.

Graham, J. & Howard R. (2010). *Cyber Security Essentials*. Boca Raton: Auerbach Publications.

Hu, L.T. & Bentler, P.M. (1999). Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria Versus New Alternatives. *Structural Equation Modeling*, 6 (1), 1-55.

Kane,R. K. (2010).*Internet Governance in an Age of Cyber Insecurity*. Council Special Report No. 56, 11.10.2013 tarihinde <http://i.cfr.org/ content/publications /attachments/ Cybersecurity_ CSR56.pdf>

Karakoç. M. (2011). Bilişim Suçlarına Genel Bakış. Bilişim Suçlarını Önleme Çalışmaları Ve Güvenli İnternet Kullanımı. *Suç ve Önleme Sempozyumu.*

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

Kaşıkçı, D.N., Çağıltay, K., Karakuş, T., Kurşun, E. & Ogan, C. (2014).Türkiye ve Avrupa'daki Çocukların İnternet Alışkanlıkları ve Güvenli İnternet Kullanımı. *Eğitim ve Bilim*, 39 (171), 230-243.

Kelloway, K. E.(1998). *Using Lisel for Structural Equation Modeling: A Researcher' s Guide*. London: Sage.

Kim, W., Jeong, O.-R., Kim, C. & So, J. (2011, 5). The dark side of the Internet: Attacks, costs and responses. *Information Systems*, 675-705.

Kline, R. B. (2005). *Principles and practice of structural equation modeling* (2nd ed.). New York: Guilford Press.

Mert, M., Bülbül. H.İ. & Sağıroğlu. Ş. (2012).Milli Eğitim Bakanlığına Bağlı Okullarda Güvenli İnternet Kullanımı. *TUBAV Bilim Dergisi*, 5(4), 1-12.

Öğün. M.N. & Kaya. A. (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler. *Journal of Security Strategies*, 18. 145-181.

Öğütçü. G. (2010). *E-Dönüşüm Sürecinde Kişisel Bilişim Güvenliği Davranışı Ve Farkındalığının Analizi*. Yüksek Lisans Tezi. Başkent Üniversitesi.

Schumacher, R. E., & Lomax, R. G. (1996). *A Beginner's Guide to Structural Equation Modeling*. New Jersey: Lawrence Erlbaum Associates Publishers.

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying, its forms and impact in secondary school pupils. *The Journal of Child Psychology and Psychiatry*, 49, 376–385.

Sümer, N.(2000). Yapısal Eşitlik Modelleri. *Türk Psikoloji Yazıları*, 3(6), 49-74.

Tabachnick, B. G. & Fidell, L. S. (1996). *Using multivariate statistics (3rd edition*). New York: Harper & Row.

Tabachnick, G.B. & Fidell, L.S. (2001). *Using multivariate statistics (fourth edition*). USA: Allyon and Bacon Press.

TUİK (2012). http://www.tuik.gov.tr/PreTablo.do?alt_id=1028 Erişim Tarihi: 11.1.2013

Valcke, M., Bonte , S., De Wever , B. & Rots , I. (2010). Internet parenting styles and the impact on Internet use of primary school children. *Computers & Education*, *55(2*), 454-464.

Yavanoğlu. U., Sağıroğlu. Ş. & Çolak.İ. (2012). Sosyal Ağlarda Bilgi Güvenliği Tehditleri ve Alınması Gereken Önlemler. *Politeknik Dergisi*. 15 (1). 15-27.

Yenisey, M. M.,Ozok A.A., & Salvendy G. (2008). Perceived security determinants in e-commerce among Turkish university students. *Proceedings Of World Academy Of Science, Engineering and Technology*, 24(4), 259 - 274.

Yılmaz, K. F.G., Yılmaz, R. & Sezer, B. (2014). Üniversite Öğrencilerinin Güvenli Bilgi ve İletişim Teknolojisi Kullanım Davranışları ve Bilgi Güvenliği Eğitimine Genel Bir Bakış. *Bartın Üniversitesi Eğitim Fakültesi Dergisi*, 3(1),176 - 199.

Erol, O., Şahin, Y. L., Yılmaz, E. & Haseski, H. İ. (2015). Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması. *International Journal of Human Sciences*, *12*(2), 75-91. doi: 10.14687/ijhs.v12i2.3185

EK- Kişisel Siber Güvenliği Sağlama Ölçeği

Kişisel Siber Güvenliği Sağlama Ölçeği	1- Hiçbir zaman	2- Nadiren	3- Arasıra	4- Sıksık	5- Her zaman
1. Web sayfalarında güvenlik bağlantılarını (https://) ve sertifikalarını kontrol ederim					
2. Kullandığım yazılımları güncellerim.					
3. Bilgisayarımda antivirus yazılımı bulundururum					
4. Şifrelerimi belirlerken basit dizilimler kullanmaktan kaçınırım					
5. İnternet şifrelerimin tümünün aynı olmasına dikkat ederim					
6. Web tarayıcımın güvenlik ayarlarını düzenlerim					
7. E- posta ile gelen kimlik doğrulama mesajlarını (kullanıcı adı, şifre vb. istekler) cevaplarım					
8. Şahsi bilgisayarım dışında kullanılan bilgisayarlarda bilgilerimin kalmamasına dikkat ederim					
9. İnternet üzerinden yapılan para ve kontör isteklerini dikkate almam.					
10. Tanımadığım kişilerden gelen sosyal ağ arkadaşlık isteğini kabul etmem.					
11. Güvenmediğim sitelere üye olmam					
12. Tanımadığım kişiler ile web kamerası kullanarak sesli ve görüntülü iletişim kurarım					
13. İnternet ortamında gerektiğinde kişisel bilgilerimi (TC No,Doğum tarihi,Gsm No vb.)paylaşırım					
14. Web geçmişimi temizlerim					
15. İnternet bankacığı işlemlerini şahsi bilgisayarımdan yaparım.					
16. Online alışveriş işlemlerini şahsi bilgisayarımdan yaparım					
17. Tanımadığım kişilerden gelen e-posta eklerini açarım					
18. Sosyal paylaşım sitelerinde kişisel bilgilerime yer veririm					
19. İnternet üzerinden yer bildirimi yaparım					
20. Sosyal ağlarda yer alan reklamlar üzerinden alışveriş yaparım					
21. Sosyal ağ - e-posta gibi hesaplarda işim bittiğinde oturumu kapatırım					
22. Güvenmediğim sitelerden dosya indirmem					
23. İnternette kullandığım (eposta, sosyal ağ vb.)şifreleri değiştiririm					
24. Unutmamak için akılda kalan kolay bir şifre belirlerim					
25. Banka, online alışveriş sitesi gibi sitelerden gelen e postalara (kart numarası, şifre vb. istekler) itibar ederim ve yanıtlarım					

Erol, O., Şahin, Y. L., Yılmaz, E. & Haseski, H. İ. (2015). Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması. *International Journal of Human Sciences*, *12*(2), 75-91. doi: 10.14687/ijhs.v12i2.3185

Extended English Abstract

Introduction

Due to the number of Internet users increases and as the Internet users' profiles become more diverse, this has led to various security problems. These problems also led to financial damage and psychological or physical damage. Viruses, spams, hacking activities, phishing, advertising scams, cyber bullying, exploitation, terror and privacy breaches are commonly threads on the internet (Kim et al., 2011). All of these threats can sometimes cause damage to property and can even be life-threatening at times. However, it is possible to avoid some of the real dangers of the virtual world with the basic measures. These measures can be individual or through legislation.

Literature indicated that internet and computer users of all ages, professions and social backgrounds have low awareness about cyber security risks (Çubukçu and Bayzan, 2013; Demirel, Yörük and Özkan, 2012; Öğütçü, 2010; Yavanoğlu, Sağıroğlu and Çolak, 2012). Questionnaires and case studies were mainly used in these studies. However, scale development studies related to cyber security or information and communication technology security were not found in literature. For this reason, this study is thought to contribute to the literature. In this context, the main purpose of this study is to develop a scale about determining the internet users' behaviors related to cyber security.

Method

In this study initially was applied an exploratory factor analysis, then applied a confirmatory factor analysis to determine the internet users' behavior related to cyber security. Before the factor analysis, 26-point item pool was created through the expert opinion. Item pool was applied to 810 people via an application in Facebook, for factor analysis. In exploratory factor analysis; principal component analysis method which is commonly used and Varimax vertical rotation method to determine the factor structure was used. Then scale was administered to 292 people and structural equation modeling approach was applied to confirmation study. For testing of the scale model χ^2, RMSEA, RMSEA, SRMR, NFI, NNFI, CFI, GFI and AGFI fit indexes were referenced.

Findings

Exploratory factor analysis was applied to test the structure validity. In this respect, KMO measure value was found .079 and Barlett sphericity was found significant ($p<.01$). Therefore data matrix and sample appropriateness were appropriate for factor analysis. When the item load examined, first item has a high item load under two factors. Thus first item was taken from the scale and analysis was repeated. As a result of analysis initially seven-factor structure was occurred. However, while eigenvalues graph examined, five factor structure was found to be more accurate. Factor analysis was repeated with limited five structure and doing axis rotation. As a result of the analysis, a structure with five factors and explained the 48.026% total variance was occurred. According to the analysis; "Privacy Protection" name was given the first factor, "Avoiding unsafe" name was given the second factor, "Take Precautions" name was given the third factor, "Protection Payment Information" name was given the forth factor and "Left No trace" name was given the fifth factor. Then final version of scale was applied for the confirmation study. Confirmatory factor analysis indicated that scale; has a perfect fit according to χ^2/sd value, has a good fit according to RMSA value, has a good fit according to SRMR value, has a near good fit according to NFI value, has a good fit according to NNFI value, has a good fit according to CFI value, has a near good fit according to GFI and AGFI values. As a result of confirmatory factor analysis all fit indexes

Erol, O., Şahin, Y. L., Yılmaz, E. & Haseski, H. İ. (2015). Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması. *International Journal of Human Sciences*, *12*(2), 75-91. doi: 10.14687/ijhs.v12i2.3185

indicate that Personal Cyber Security Provision Scale has a good compatibility. In addition the reliability coefficient for the whole scale was calculated as .735.For other sub-scales reliability coefficient; first sub scale is calculated .763; second sub scale is calculated.771; third sub scale is calculated .704; forth sub scale is calculated .829; fifth sub scale is calculated .557. In general, it can be said that the scale is a reliable scale.

Result

In the literature, it is indicated that internet and computers user of all ages, professions and social backgrounds have low awareness about cyber security risks and there is no scale related to determine the internet users' views and trends about providing cyber security. In this context a scale was developed which aims to determine internet users' views about providing cyber security. As a result of factor analysis structure, validity was tested and five factor Personal Cyber Security Provision Scale, which has a good compatibility, has emerged.