YÖNETİM BİLİŞİM SİSTEMLERİ DERGİSİ
http://dergipark.gov.tr/ybs

Yayın Geliş Tarihi: 23.10.2019
Yayına Kabul Tarihi: 23.12.2019
Online Yayın Tarihi:31.12.2019

Cilt:5, Sayı:2, Yıl:2019, Sayfa:1-11
e-ISSN: 2630-550X

YÜKSEKÖĞRETİM KURUMLARINDA BİLGİ GÜVENLİĞİ FARKINDALIK DÜZEYLERİNİN ÖLÇÜMLENMESİ[1]

Doç. Dr. Handan ÇAM

Gümüşhane Üniversitesi, Yönetim Bilişim Sistemleri Bölümü

Dr. Öğr. Üyesi Fulya ASLAY

Erzincan Binali Yıldırım Üniversitesi, Bilgisayar Mühendisliği Bölümü

Prof. Dr. Üstün ÖZEN

Atatürk Üniversitesi, Yönetim Bilişim Sistemleri Bölümü

Özet

Teknolojinin hızla geliştiği ve Internet kullanımının da giderek yaygınlaştığı günümüzde, bilgi sistemlerinden ve kişilerden kaynaklı güvenlik açıkları kişileri, kurumları ve devletleri etkilemektedir. Bilgiye yetkisiz veya izinsiz bir biçimde erişilmesini ve kullanılmasını, değiştirilmesini, tamamen ortadan kaldırılmasını, başka kişiler tarafından ele geçirilmesini önlemek bilgi güvenliği kapsamı içerisindedir. Özellikle kurumların, teknik güvenlik önlemlerinin yanında insan faktörünü de öncelikli olarak göz önüne alarak dijital veri güvenliğini sağlamaları gerekmektedir. Yapılan çalışmalar kurumlarda çalışan kişilerin güvenliğin en zayıf halkasını oluşturduğunu göstermektedir. Bilginin üretildiği ve yeni nesillere aktarıldığı yükseköğretim kurumlarında yapılan çalışmalarda özellikle bilgi güvenliği farkındalığı açısından kişisel ve kurumsal bilgi güvenliğinin önemi vurgulanmaktadır. Bu çalışmada; Gümüşhane Üniversitesi'ndeki öğrenci, çalışan ve akademisyenlerin İnternet kullanım düzeyleri ve kişisel bilişim güvenliği tutumları incelenmektedir. Verilerin analizi için açımlayıcı faktör analizi, tanımlayıcı istatistiksel analizler ve iki yönlü varyans analizi kullanılmıştır. Araştırma sonuçları, yükseköğretim kurumlarında bilgi güvenliği farkındalık düzeylerinin artırılmasına ilişkin çalışmaların yapılması gerektiğini desteklemektedir.

Anahtar Kelimeler: Bilgi Güvenliği, Kişisel Bilgilerin Korunması, Bilgi Güvenliği Farkındalığı

MEASUREMENT OF INFORMATION SECURITY AWARENESS LEVELS IN HIGHER EDUCATION INSTITUTIONS[2]

Abstract

Security gaps caused by information systems and individuals affect people, institutions, governments in today's world in which technology is developing rapidly and Internet use is becoming more widespread. The scope of information security includes accessing, using, changing, and completely removing information without authority and permission as well as preventing to take over the information by others. Especially institutions have to ensure digital data security by considering primarily human factor along with technical security precautions. The studies have indicated that people working in institutions are the weakest link of security. The studies conducted at higher education institutions where information is produced and transferred to new generations have emphasized the importance of personal and corporate information security particularly in terms of information security

[1] 6.Uluslararası Yönetim Bilişim Sistemleri Konferansı
[2] 6th International Management Information Systems Conference

awareness. This study was constituted in order to investigate Internet use levels and personal information security attitudes of students, employees, and academicians at Gümüşhane University. In the data analysis, descriptive statistical analyses, exploratory factor analysis, and two-way analysis of variance has been used. The results of the study support the need for studies on increasing the levels of information security awareness at higher education institutions.

Keywords: Information Security, Protection of Personal Information, Information Security Awareness

GİRİŞ

Son yıllarda oldukça gelişen bilgi ve iletişim teknolojileri ile birlikte İnternet kullanımı da oldukça yaygınlaşmıştır. We Are Social ve HootSuite (2019)'nın yayınladığı 2019 yılı Küresel Dijital Raporuna göre dünya genelinde bulunan 4,38 milyar İnternet kullanıcısının 59,38 milyonu Türkiye'de bulunmaktadır. Raporda Türkiye'de var olan kullanıcıların yüzde 84'ünün İnterneti her gün, yüzde 12'sinin ise haftada en az bir kez kullandığı belirtilmektedir. Sosyal medya hesapları Türkiye'de 52 milyon kullanıcının sosyal medyayı aktif bir şekilde kullandığını ve bu kullanıcıların 44 milyonunun mobil cihazları kullanan sosyal medya kullanıcısı olduğunu belirtmektedir. İnternet kullanımının yaygınlaşması ile kişiler bilgiye daha kolay bir şekilde erişmeye başlamışlardır. Ancak birtakım güvenlik ve gizlilik ihlalleri sebebiyle, kişiler bir yandan kolayca bilgiye erişirken bir yandan da mevcut bilgilerinin kaybolmasına, değiştirilmesine ya da değiştirilmesine maruz kalmaktadırlar. Özellikle İnternet üzerinden dosya paylaşımı ve alışveriş yapan kişilerin risk oluşturduğu tutumları, bilgi güvenliği noktasında kendilerini ve eğer çalışıyorlarsa, işletmedeki tüm çalışanları da etkileyebilmektedir. Bu çalışmada bilginin de üretildiği merkezler olarak kabul edilen bir yükseköğretim kurumundaki çalışanların ve öğrencilerin İnternet kullanım düzeyleri ve kişisel bilişim güvenliği tutumları incelenmektedir. Bu kapsamda birinci kısmında bilgi güvenliğine ve bilgi güvenliği ile ilgili yapılan çalışmaların literatür özetine yer verilmiştir. İkinci kısımda çalışma için uygulanan anketin verilerin analizi için yapılan açımlayıcı faktör analizi, tanımlayıcı istatistiksel analizler ve iki yönlü varyans analizi bulguları paylaşılmaktadır. Çalışma tartışma ve sonuç bölümüyle sona ermektedir.

BİLGİ GÜVENLİĞİ

Bilgiye yetkisiz veya izinsiz bir biçimde erişilmesini ve kullanılmasını, değiştirilmesini, ortadan kaldırılmasını, üçüncü kişiler tarafından elde edilmesini önlemek genel olarak bilgi güvenliğinin kapsamı içerisindedir. Bilgi güvenliği gizlilik, bütünlük ve erişilebilirlik olmak üzere üç ana etmenden meydana gelmektedir (Puhakainen, 2006). Gizlilik; Kurumsal çapta sağlanması için kurumun hazırladığı politika ve sözleşmelerde bilginin gizlilik seviyesi ile birlikte karşılıklı yapılması gereken işlemlerin tanımlanması gerekmektedir (Ganbat 2013). Bilginin bütünlüğünde; Bilgi ve bilgi işlemlerinde veri içeriğinin bozulmadığı garanti altına alınmalıdır (Özcan, 2009). Erişilebilirlik; Kullanıcıların yetki düzeyleri doğrultusunda ihtiyaç duydukları bilgi ve ilişkili varlıklara erişme haklarının sağlanması olarak tanımlanmıştır. Burada kurumlar kullanıcı yetkilendirmelerini güvenli ve doğru bir şekilde sağlamalıdırlar (Ganbat 2013). Bu üç temel bilgi güvenliği öğesinden herhangi birinin ya da hepsinin zarar görmesi ciddi güvenlik açıklarının oluşmasına sebep olmaktadır. Bilgi güvenliğini tehdit eden bu unsurlarda teknik özelliklerden önce fiziki olarak bilginin güvenliğinin sağlanması olarak algılansa da günümüzde dijital platformların yetenekleri ve kapasiteleri değerlendirildiğinde, bilgi güvenliğini genel olarak dijital veri güvenliği olarak değerlendirmek mümkündür (Yılmaz vd. 2016). Dijital veri güvenliğini tehdit eden etkenler ise genel olarak fiziksel, yazılımsal ve kullanıcı kaynaklı tehditler olarak değerlendirilebilir (Moody et al.,2018; Gülmüş, 2010; keser ve Güldüren, 2015).

Yapılan araştırmalar, bilgi güvenliğinde problemlerin daha çok teknik olarak incelenerek, insan faktörünün çoğu zaman göz ardı edildiğini göstermektedir (Chen, Shaw ve Yang, 2006; Rezgui ve Marks, 2008; Kjorvik, 2010). Öncelikle güvenlik duvarı, antivirüs yazılımları, sanal öz ağ kullanımları ile saldırıları tespit ve önleme sistemleri ile kurumsal ve kişisel bilgilerin güvenliğini fiziksel anlamda sağlamak mümkündür ancak sadece teknik güvenlik önlemleri bilgi güvenliği için yeterli olmamaktadır (Rezgui ve Marks, 2008). Bununla birlikte kurum yöneticileri ve çalışanlarının bilgi güvenliğinin bilincinde olmaları gerekmektedir. Çünkü güvenliğin en zayıf halkasının kurum çalışanlarının olduğu bilinmektedir (Mathisen, 2004; Kritzinger ve Smith, 2008; Veiga, 2008; Penmetsa, 2010; Mahabi, 2010). Bu nedenle çalışanların bilgi güvenliği konusundaki mevcut durumlarının tespit edilmesi ve eksik yönleriyle ilgili eğitimlerin verilmesi oldukça önemlidir. Ayrıca bilgi güvenliğini sağlamak için

korunacak bilgi öğelerinin seçilmesi ve bu öğelerin sınıflandırılarak uygun güvenlik önlemlerinin buna göre tespit edilmesi gibi işlemler de oldukça önemlidir ve çoğunlukla göz ardı edilmektedir (Henkoğlu 2017).

LİTERATÜR TARAMASI

Literatür taraması yapıldığında özellikle son yıllarda bilgi güvenliği ile ilgili oldukça fazla çalışma yapıldığı görülmektedir. Bu çalışmanın da kapsamında olan yükseköğretim kurumlarında yapılan çalışmalarda ise özellikle bilgi güvenliği farkındalığı açısından kişisel ve kurumsal bilgi güvenliğinin çok iyi durumda olmadığı dikkat çekmektedir (Connolly ve Currall, 2001; Cox, Rezgui ve Marks, 2008; Vardar, 2009). Oysaki kurumlarda bilgi güvenliği ve bilişim sistemleri güvenliği için çalışanlara eğitim verilmesi gerekli olup, bu eğitimlerin diğer kurumlarda olduğu gibi yükseköğretim kurumlarında da verilmesi çok önemlidir. ABD'de Winsconsin Üniversitesi tarafından yapılan bir çalışmada 435 yükseköğretim kurumuna bir anket uygulanmıştır. Anket sonuçlarına göre enstitülerin yalnızca üçte birinde personel ve öğrenci için bilgi güvenliği farkındalığına yönelik eğitimlerin verildiği vurgulanmaktadır (Caruso, 2003). Keser ve Güldüren (2015), yükseköğretim kurumlarında görev yapan öğretim elemanlarının bilgi güvenliği farkındalığını belirlemek üzere bir ölçeğin geliştirildiği çalışmada bulunmuşlardır. Topal ve Akgün (2015), eğitim fakültesinde eğitim gören öğrencilerin bilgi güvenliği seviyelerini tespit etmek için bir çalışma yapmışlardır ve bu çalışmanın sonucunda bilgi güvenliği seviyesinin yeterli olmadığını tespit etmişlerdir. Ayrıca bilgi güvenliği konusunda eğitim alan katılımcılar ile eğitim almayanlar arasında önemli bir farklılık olduğunu tespit etmişlerdir. Bilgi güvenliğinde uzman olan kişilerle yapılan bir çalışmaya göre ise, yükseköğretim kurumlarının özellikle bilişim sistemleri güvenliği açısından birçok açıklarının ve zayıf yönlerinin bulunduğu ve bu nedenle yükseköğretim kurumlarının dünyadaki en güvensiz kurumlardan biri olduğu vurgulanmaktadır (Rezgui ve Marks, 2008; Foster, 2004; Mahabi, 2010). Yılmaz vd. (2016), öğretmenler üzerinde dijital veri güvenliği farkındalığını değerlendirmek için yaptığı çalışmada, öğretmenlerin dijital veri güvenliğinin çok iyi bir seviyede olduğunu, farkındalıklarının ise elektronik cihaz çeşitliliği, kullanım sıklığı ve cinsiyet gibi faktörlere göre değiştiğini tespit etmiştir. Erdoğmuş (2017), üniversite öğrencilerine yaptığı bir çalışmada öğrencilerin bilgi güvenliği farkındalıklarının; sosyal medya kullanımı, sosyal medya tuzakları, İnternet güvenliği, ağ güvenliği ve şifre oluşturma olmak üzere 5 alt boyutta olduğunu belirlemiştir.

ARAŞTIRMANIN AMACI

Örneklem Süreci, Analiz Yöntemi

Çalışmada kullanılan veri seti anket yöntemi kullanılarak yüz yüze görüşme tekniği ile derlenmiştir. Gümüşhane Üniversitesinde yer alan öğrenci, çalışan ve akademisyenlere uygulanmıştır. Anakütle dikkate alındığında örneklem hacmi 0,05 anlamlılık düzeyinde z=1,96, d=0,05 ve p ile q=0,5 alındığında uygun örneklem kütlesi ise 384 olarak bulunmaktadır. Araştırmaya 387 katılımcı kolayda örnekleme yöntemi ile dahil edilmiştir. Veri seti toplandığında 37 veri elenerek toplamda 350 veri çalışmaya dahil edilmiştir. Anket formunda yer alan ilk bölüm demografik özellikleri kapsayan 7 değişkenden oluşmaktadır. İkinci bölüm İnternet kullanım düzeyini ölçümleyen 5 değişkenden oluşmaktadır. Üçüncü bölüm ise kişisel bilişim güvenliği tutumlarını ölçümleyen 5'li likert ölçeği formunda 32 değişkenden oluşmaktadır. Verilerin analizinde tanımlayıcı istatistiksel analizlerle birlikte, açımlayıcı faktör analizi ve iki yönlü varyans analizi kullanılmıştır.

Analiz Yönteminin Uygulanması ve Bulgular

Demografik Özelliklere İlişkin Bulgular

Çalışmada ankete katılan kişilerin demografik özellikleri incelenmiş olup, Tablo 1'de sunulmaktadır. Buna göre katılımcıların cinsiyetinin dengeli dağıldığı görülmekle birlikte, çoğunluğu öğrenci olmakla birlikte yaklaşık %75'inin bekar olduğu görülmektedir. Gelir seviyeleri ise çoğunlukla 2000 TL ve altındadır.

Tablo 1. Anket Katılımcılarının Demografik Özellikleri

Cinsiyet	**Frekans(f)**	**Yüzde(%)**
Erkek	193	55,1
Kadın	157	44,9
Eğitim	**Frekans(f)**	**Oran**
İlkokul	1	0,002
Ortaokul	5	0,014
Lise	190	0,542
Yüksek Öğretim	154	0,440
Gelir Seviyeniz	**Frekans(f)**	**Oran**
2000 ve altı	196	**0,560**
2001 ve 3500 arası	35	**0,100**
3501 ve 5000 arası	90	**0,257**
5001 ve üzeri	29	**0,082**
Yaş	**Frekans(f)**	**Oran**
20 yaş ve altı	35	0,100
20-34 yaş arası	270	0,771
35-50 yaş arası	45	0,128
Medeni Durum	**Frekans(f)**	**Oran**
Evli	88	0,251
Bekar	262	0,748

Katılımcıların Internet Kullanım Düzeyleri

Tablo 2. Katılımcıların Internet Kullanım Düzeyleri

Internetten Alışveriş Yapma Sıklığı	**Frekans(f)**	**Oran**
Günde bir defa veya fazla	6	0,017
Haftada bir defa veya fazla	52	0,148
Ayda bir defa veya fazla	252	0,720
Yılda bir Defa veya fazla	40	0,114
Son bir ayda Internetten kaç kere ürün veya hizmet aldınız		
Hiç almadım	104	0,297
1-2	202	0,577
3-4	24	0,068
5-6	11	0,031
7 ve üstü	9	0,025
Internet alışverişine ayırdığınız aylık bütçe ne kadar		
1000 ve altı	281	0,802
1001-2000	30	0,085
2001-3000	28	0,080

3000 ve üzeri	11	0,031
Internette genellikle hangi sektörden alışveriş yaparsınız		
Elektronik	91	0,260
Giyim	198	0,565
Yemek-gıda	14	0,040
Kitap-CD	34	0,097
Diğer	13	0,037
Genelde tercih ettiğiniz Internet sitesi		
N11	39	0,111
Hepsiburada	51	0,145
Gittigidiyor	28	0,080
Sanal Pazar	22	0,062
Morhipo	25	0,071
Trendyol	97	0,277
Diğer	88	0,251

Tablo 3. Kullanıcıların Internet Kullanım Tutumlarına İlişkin Ortalama ve Standart Sapma

Değişkenler	Ortalama	Standart Sapma
Elektronik posta(e mail)'yı bir iletişim aracı olarak kullanırım.	4,30	1,177
Internette varolan e-posta gruplarına üye olurum.	2,22	1,464
Sosyal ağ sitelerini (Facebook, Twitter ve benzeri) kullanırım.	4,14	1,375
Sosyal ağlardan gelen uygulama davetlerini kabul ederim.	2,24	1,449
Internet bankacılığı kullanırım.	4,06	1,501
Internet üzerinden alışveriş yaparım.	4,42	1,043

Tablo 4. Kullanıcıların Risk Oluşturan Tutumlarına İlişkin Ortalama ve Standart Sapma Değerleri

Değişkenler	Ortalama	Standart Sapma
S7-E-vatandaşlık hizmetleri sağlayan web sayfalarını (Hastane Randevu sistemi, e-devlet vb.) kullanırım.	4,07	1,321
S8-Internetten yazılım/program, müzik, film ve çeşitli dosyaları indiririm/ kaydederim.	4,39	1,190
S9-Web sayfalarını kullanırken gerektiği zamanlarda iletişim bilgilerimi (Adres, GSM No, E-posta) paylaşırım.	3,96	1,407
S10-Internet sitelerini kullanırken gerektiği zamanlarda özlük bilgilerimi paylaşırım. (Doğum Tarihi, Ad-Soyad, vb…)	4,02	1,297
S11-Sohbet (chat) yaparken dosya transferi yaparım.	2,11	1,902
S12-Bilgisayarımdaki dosyaları paylaşıma açarım.	1,64	1,098
S13-Parolalarımı başkalarıyla paylaşırım.	1,53	1,065
S14-Bilmediğim kaynaklardan gelen e postaları açarım, e-postlardan gelen ekleri indiririm	1,77	1,218

Tablo 5. Kullanıcıların Tehditlerden Korunma Amaçlı Tutumlarına İlişkin Ortalama ve Standart Sapma Değerleri

Değişkenler	Ortalama	Standart Sapma
S15-Bilgisayarımda lisanslı yazılım/program kullanmaya özen gösteririm.	3,77	1,181
S16-Virüs/zararlı yazılım temizleme, casus yazılım önleme vb. programlarını kullanırım.	3,79	1,286
S17- Reklam engelleyici, güvenlik duvarı vb. programları kullanırım.	3,47	1,337
S18-E-posta filtreleme yazılımları kullanırım.	3,00	1,444
S19-İçerik filtreleme programları kullanırım.	2,89	1,456
S20-Herkesin kullanımına açık bir bilgisayarı kullandıktan sonra web arama geçmişlerini ve geçici Internet dosyalarını silerim.	4,05	1,357
S21-Dosyalarımı şifrelerim.	2,99	1,712
S22-Internette var olan hesaplarımda kolay bulunamayacak şekilde uzun ve karmaşık şifreler kullanırım.	3,44	1,420
S23-Elektronik/ Mobil imza kullanırım.	2,33	1,524
S24-Bilgisayarım şifre ile açılır.	3,32	1,747
S25-Parolalarımı sık sık değiştiririm.	2,54	1,578
S26-Kullandığım programların güncellemelerini düzenli olarak yaparım.	3,76	1,257

Tablo 6. Kullanıcıların Bilişim Suçuna Maruziyetlerine İlişkin Ortalama ve Standart Sapma Değerleri

Değişkenler	Ortalama	Standart Sapma
S27-Bilgisayar virüsleri nedeniyle sorun yaşadım.	2,25	1,538
S28-Online alışverişten dolayı maddi zarara uğradım.	1,90	1,382
S29-Kredi kartım kopyalandı.	1,33	0,875
S30-Kişisel/Özel bilgilerimi Internette paylaştığım için güç duruma düştüm.	1,43	0,995
S31- Kişisel/Özel bilgilerim iznim olmadan üçüncü şahıslarla paylaşıldı/ Internette yayınlandı.	1,33	0,885
S32-Bilgisayarımdaki dosyalarım çalındı/silindi.	1,37	0,999

Faktör Analizi Bulguları

Katılımcılardan derlenen verilere öncelikle güvenilirlik analizi uygulanmıştır. Daha sonra değişkenleri gruplayarak fark analizleri uygulayabilmek için faktör analizi uygulanmıştır. Değişkenlerin tamamında kullanılan güvenilirlik testinin sonucuna göre Croncbach's Alpha değeri 0,898 şeklinde elde edilmiştir. Elde edilen değer 0,70 den yüksek olduğundan dolayı ölçeğin güvenli olduğu değerlendirilerek, değişkenlere açımlayıcı faktör analizi yapılmıştır. Yine ölçeğin faktör analizine uygunluğunun belirlenmesi için ise verilerin birbirleri arasında ilişki olup olmadığını belirten Bartlett sınaması ve faktör analizi için alınan örneklem büyüklüğünün uygunluğunu değerlendiren Kaiser Mayer Olkin (KMO) ölçütlerinden faydalanılmıştır. Sonuç olarak Bartlett Değeri: 2374,676; P: 0,000 ve KMO: 0,774 şeklinde hesaplanarak istatistiklerin, faktör analizi için uygun olduğu tespit edilmiştir.

Faktör analizi sonucuna göre bilişim güvenliğine ait değişkenlerden 0,40 ve üzeri faktör yükleri olan değişkenler faktör için dikkate alınarak bu doğrultuda 5 faktör bulunmuştur. Bu faktörlerin ise toplam varyansın %60,058'ini açıkladığı görülmüştür.

Tablo 7'de elde edilen 5 faktörün açılımları ve bu faktörlere ait faktör yükleri, varyans yüzdeleri ile özdeğerleri ve her faktöre ait Croncbach's Alpha değerleri gösterilmektedir.

Tablo 7. Faktör Analizi Sonuçları

Değişkenler	**Faktör Yükleri**	**Varyans Yüzdesi**	**Özdeğeri**	**Croncbach's Alpha**
F1- Internet'te İşlem Yapılması Kaynaklı Riskler		17,241	5,954	0,821
S7- E-vatandaşlık hizmetleri sağlayan web sayfalarını (Hastane Randevu sistemi, e-devlet vb.) kullanırım.	0,704			
S8- Internetten yazılım/program, müzik, film ve çeşitli dosyaları indiririm/ kaydederim	0,669			
S11-Internette sohbet (chat) ederken dosya transferi yaparım.	0,725			
S12-Bilgisayarımda var olan dosyaları erişime/paylaşıma açarım.	0,665			
F2- Kişisel Bilgi Paylaşımı Kaynaklı Riskler		12,153	3,715	0,785
S9-Internet sitelerini kullanırken gereken zamanlarda iletişim bilgilerimi (Fiziksel adres, GSM No, e-posta) paylaşırım.	0,754			
S10- Internet sitelerini kullanırken gereken zamanlarda özlük bilgilerimi paylaşırım. (Doğum Tarihi, Ad-Soyad vb…)	0,809			
S13-Parolalarımı başkalarıyla paylaşırım	0,587			
S14-Tanımadığım kişilerden gelen e postaları açarım, gelen ekleri indiririm.	0,769			
F3- Tehditlerden Korunma Yönelik Tutumlar		11,681	2,391	0,879
S15-Bilgisayarımda orijinal (lisanslı) yazılım/program kullanmaya dikkat ederim.	0,434			
S16-Virüs temizleme, casus yazılım önleme vb. yazılımları kullanırım.	0,610			
S17- Reklam engelleyici, güvenlik duvarı vb. programları kullanırım.	0,798			
S18-E-posta filtreleme yazılımları kullanırım.	0,768			
S19-İçerik filtreleme programları kullanırım.	0,750			
S20-Herkesin kullanımına açık bir bilgisayarı kullandıktan sonra geçici İnternet dosyalarını ve web gezinti geçmişlerini silerim.	0,669			
S21-Dosyalarımı şifrelerim.	0,739			
S22-Internette var olan hesaplarımda kolay elde edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım.	0,712			
S23-Elektronik/ Mobil imza kullanırım.	0,626			
S24-Bilgisayarım şifre ile açılır.	0,625			
S25-Parolalarımı sık sık değiştiririm.	0,730			
S26-Kullandığım programların güncellemelerini düzenli olarak yaparım.	0,754			
F4- Kişisel Hatalardan Dolayı Ortaya Çıkan Zarar		10,451	1,716	0,722

S27-Bilgisayar virüsleri nedeniyle güçlükler yaşadım.	0,521			
S28-Online alışveriş yapmamdan ötürü maddi zarara uğradım.	0,585			
S30-Kişisel/Özel bilgilerimi Internette paylaşmamdan güç duruma düştüm.	0,816			
F5- Dışsal Tehditlerden Ortaya Çıkan Zarar		9,054		
S29-Kredi kartım kopyalandı.	0,737		1,120	0,701
S31- Kişisel/Özel bilgilerim iznim dışında üçüncü şahıslarla paylaşıldı/ İnternette yayımlandı.	0,882			
S32-Bilgisayarımdaki dosyalarım çalındı/silindi.	0,825			

Bağımsız Örneklem İki Yönlü Varyans Analizi Bulguları

Bağımlı değişken olarak "Internet üzerinden alışveriş yaparım" değişkeni kullanılmıştır. Bağımsız değişkenler ise faktör analizi sonucu elde edilen "F1- Internette İşlem Yapılması Kaynaklı Riskler" kapsayan 4 değişkenden oluşmaktadır. Varyans analizi sonucunda tabloda yer alan değerler elde edilmiştir. Internet üzerinden alışveriş yapan katılımcıların S7, S11 ve S12'de yer alan tutumlara katılmadıklarını ortaya koyarak anlamlı bir farklılık olmadığı analiz sonuçlarından görülmektedir. Fakat analiz sonucunda Internet üzerinden alışveriş yapan katılımcıların Internet üzerinden müzik, film, program ve dosya indirerek kaydetme tutumlarına bağlı olarak farklılık gösterdiği Tablo 8'de yer alan P (0,001≤ 0,05) değerinden tespit edilmiştir.

Tablo 8. Varyans Analizi Sonuçları

	Kareler Toplamı	Df	Ortalama Kare	F	Sig.
MODEL	153,277	75	2,044	4,005	0,000
S7	3,030	1	0,757	1,484	0,211
S8	10,033	4	2,508	4,915	0,001
S11	2,890	4	0,578	1,133	0,347
S12	3,761	5	0,940	1,842	0,125

Bağımlı değişken olarak "Internet üzerinden alışveriş yaparım" değişkeni kullanılmıştır. Bağımsız değişkenler ise faktör analizi sonucu elde edilen "F2-Kişisel Bilgi Paylaşımı Kaynaklı Riskler" kapsayan 4 değişkenden oluşmaktadır. Varyans analizi sonucunda tabloda yer alan değerler elde edilmiştir. Internet üzerinden alışveriş yapan kişilerin kişisel bilgi paylaşımı kaynaklı riskler konusunda çoğunun bilinçli olmadıkları ve bu bağlamda zarar görebilecekleri tespit edilmiştir. Çünkü varyans analizi sonucunda Internetten alışveriş yapan katılımcılar S9, S10, S13 değişkenlerine bağlı olarak anlamlı farklılıklar göstermekte olduğu Tablo 9'da yer alan P (0,015, 0,020, 0,016 ≤ 0,05) değerleri ile teyit edilmiştir.

Tablo 9. Varyans Analizi Sonuçları

	Kareler Toplamı	Df	Ortalama Kare	F	Sig.
MODEL	151,960	72	2,111	4,150	0,000
S9	6,544	4	1,636	3,216	0,015
S10	6,186	4	1,547	3,041	0,020
S13	6,451	4	1,613	3,171	0,016
S14	4,706	4	1,177	2,313	0,061

Bağımlı değişken olarak "Internet Bankacılığı Kullanırım" değişkeni kullanılmıştır. Bağımsız değişkenler ise faktör analizi sonucu elde edilen "F4- Kişisel Hatalardan Dolayı Ortaya Çıkan Zarar" kapsayan 3 değişkenden oluşmaktadır. Varyans analizi sonucunda tabloda yer alan değerler elde edilmiştir. S27, S28 ve S30'da yer alan ifadelere Internet bankacılığı kullanan katılımcıların anlamlı bir şekilde farklı cevaplar vermedikleri bu değişkenlerdeki tutumlarının ortalamalarının birbirinden farklı olmadığı hipotezi kabul edilmiştir. Analiz sonucunda elde edilen tanımsal istatistik tablosunda S27'ye 129 kişinin katılmadığı, S28'e 150 kişinin katılmadığı, S30'a ise 179 kişinin katılmadığı tespit edilmiştir. Analiz sonucunda Internet bankacılığı kullanan katılımcıların kişisel hatalardan dolayı zarar görmedikleri söylenebilir. Araştırma yapılan örneklemde yer alan kütlenin çoğunun bilgisayar virüsleri, online alışveriş ve kişisel bilgilerini güvensiz ortamlarda paylaşma konularında zarar görmedikleri ve bilinçli oldukları söylenebilmektedir.

Tablo 10. Varyans Analizi Sonuçları

	Kareler Toplamı	df	Ortalama Kare	F	Sig.
MODEL	106,953	53	2,018	0,863	0,728
S27	13,152	4	3,288	1,406	0,235
S28	1,650	4	0,413	0,176	0,950
S30	17,693	4	4,423	1,891	0,115

TARTIŞMA VE SONUÇ

Çalışmada Gümüşhane Üniversitesi'ne mensup öğrenci, çalışan ve akademisyenlere uygulanan anketteki analiz sonuçlarına göre; kullanıcıların Internet kullanım tutumlarına ilişkin çoğunlukla iletişim aracı olarak e-posta hesaplarını kullandıkları ayrıca Facebook, Twitter ve benzeri sosyal ağ sitelerini kullandıkları görülmektedir. Bununla birlikte yine büyük bir çoğunlukla Internet bankacılığı kullandıkları ve Internet üzerinden alışveriş yaptıkları da görülmektedir.

Internet üzerinden alışveriş yapan katılımcıların, Internet'ten işlem yapılması kaynaklı riskler içerisinde müzik, film, program ve dosya indirerek kaydetme tutumlarına bağlı olarak anlamlı bir farklılık olduğu değerlendirilmektedir. Yine Internet üzerinden alışveriş yapan katılımcıların kişisel bilgi paylaşımı kaynaklı risklerden sanal ortamda gereken durumlarda fiziksel adres, GSM No, e-posta gibi iletişim bilgilerini bununla birlikte ad soyad, doğum tarihi gibi özlük bilgilerini ve ayrıca sahip oldukları parolalarını paylaşmaları tutumlarına bağlı olarak anlamlı bir farklılık olduğu sonucuna ulaşılmaktadır. Internet bankacılığı kullanan katılımcıların ise kişisel hatalardan dolayı ortaya çıkan zaralar kapsamında çok fazla etkilenmedikleri ve bu konuda daha bilinçli oldukları tespit edilmektedir.

Çalışma kapsamında kullanıcıların özellikle Internetten alışveriş yaparken paylaştığı kişisel bilgilerden dolayı risk altında oldukları tespit edildiğinden, özellikle bu bağlamda farkındalık oluşturulmasının faydalı olacağı düşünülmektedir. Ayrıca sosyal medya paylaşımlarında kişilerin kültürel, siyasi, dini vb. görüşlerine ayrıca kişinin çalıştığı kurum bilgilerine, adresine, çalışma alanlarına üçüncü şahıslar tarafından ulaşılabileceğinden ötürü özellikle kritik kurumlardaki ve kritik görevlerdeki çalışanların, günlük yaşantısı ile çalışma bilgilerini sosyal medya üzerinden paylaşmamaları konusunda bilgilendirilmeleri gerekmektedir.

Yapılan benzer çalışmalarla karşılaştırıldığında (Caruso, 2003; Kritzinger ve Smith, 2008; Veiga, 2008; Mahabi, 2010; Mathisen, 2004; Penmetsa, 2010; Akgün ve Topal, 2015) genel olarak bilgi güvenliği kapsamında en zayıf halkanın insan faktörü olduğu göz önüne alınarak, fiziksel ve pahalı teknik güvenlik önlemlerinin öncesinde kişilerde farkındalık oluşturulması, bilgi güvenliği ile ilgili verilecek eğitimler ile kişilere güvenlik bilinci kazandırılmasının işletmelere katkı sağlayacağı düşünülmektedir.

KAYNAKÇA

Caruso, J. B. (2003). Information technology security: Governance, strategy, and practice in higher education. ECAR, 1-7.

Chen, C. C., Shaw, R., and 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.

Cox, A., Connolly, S., and Currall, J. (2001). Raising Information Security Awareness In The Academic Setting, VINE, Vol.31 Iss:2, pp.11-16, Glasgow, United Kingdom. doi: 10.1108/03055720010803961.

Erdoğmuş, A. (2017). Üniversite Öğrencilerinin Bilgi Güvenliği Kazanimlarinin, Farkindaliklari Üzerindeki Etkilerinin Analizi: Afyon Kocatepe Üniversitesi Örneği. Yayınlanmamış Yüksek Lisans Tezi, Afyon Kocatepe Üniversitesi, Fenbilimleri Enstitiüsü, Afyon.

Foster, A. L. (2004). Insecure and Unaware. Chronicle of Higher Education, 50(35), 33-35.

Ganbat, O. (2013). Bilgi Güvenliği Yönetim Sistemi ISO/IEC 27001 ve Bilgi Güvenliği Risk Yönetimi ISO/LEC 27005 Standartlarının Uygulanması. Yayınlanmamış Yüksek Lisans Tezi, Ege Üniversitesi, Fen Bilimleri Enstitüsü, İzmir.

Gülmüş, M. (2010). Kurumsal Bilgi Güvenliği Yönetim Sistemleri ve Güvenliği. Yayınlanmamış Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi, Elektrik Mühendisliği Anabilim Dalı, İstanbul.

Henkoğlu, T. (2017). Kişisel Verilerimiz Ne Kadar Güvende: Bilgi Güvenliği Kapsamında Bir Değerlendirme. Arşiv Dünyası Dergisi, 17: 46-56.

Keser, H., ve Güldüren, C. (2015). Bilgi Güvenliği Farkındalık Ölçeği Geliştirme Çalışması. Kastamonu Üniversitesi, Eğitim Dergisi, 23: 1167-1184.

Kjorvik, H. (2010). Implementing and improving awareness in information security. Master's thesis, University of Agder, Faculty of Engineering and Science, Grimstad. http://brage.bibsys.no/

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

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).

Mathisen, J. (2004). Measuring information security awareness - A survey showing the Norwegian way to do it.(Master's thesis, Gjovik University, College Institutionen for Dataoch Systemvetenskap, Hogskolen).

Moody, G.D., Siponene, M., and Pahnila, S. (2018). Toward A Unifield Model Of Information Security Policy Compliance, MIS Quarterly, 42: 285-A22.

Özcan, B. (2009). Kurumsal Bilgi Güvenliği ve Cobit. Yayınlanmamış Yüksek Lisans Tezi, Haliç Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

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.

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.

Rezgui, Y., and Marks, A. (2008). Information security awareness in higher education: An exploratory study. Computer and Security, 27, 241-253.

Topal, M. ve Akgün, Ö. E. (2015). Eğitim fakültesinde okuyan öğretmen adaylarının eğitim amaçlı internet kullanımı öz-yeterlik algılarının incelenmesi: Sakarya Üniversitesi Örneği. Kastamonu Eğitim Dergisi, 23(1), 343-364.

Vardal, N. (2009). Yükseköğretimde bilgi güvenliği: Bilgi güvenlik yönetim sistemi için bir model önerisi ve uygulaması. Yayınlanmamış 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.

We are Social and Hootsuite (2019), https://wearesocial.com/global-digital-report-2019 Son Erişim Tarihi: 28.06.2019

Yılmaz, E., Şahin, Y. L., ve Akbulut, Y. (2016). Öğretmenlerin Dijital Veri Güvenliği Farkındalığı. Sakarya Üniversitesi Eğitim Bilimleri Dergisi, 6: 26-45.