

## SAĞLIK YÖNETİMİ BÖLÜMÜ ÖĞRENCİLERİNİN MOBİL GÜVENLİK FARKINDALIĞI VE DİJİTAL VERİ GÜVENLİĞİ FARKINDALIKLARININ BELİRLENMESİ

\*\*\*

### DETERMINATION OF STUDENTS IN DEPARTMENT OF HEALTH MANAGEMENT ON MOBILE SECURITY AND DIGITAL DATA SECURITY AWARENESS

Yrd. Doç. Dr. Zülfiye BIKMAZ

Kırklareli Üniversitesi, Sağlık Yüksekokulu, Sağlık Yönetimi Bölümü  
zbkamaz@gmail.com

#### Öz

Bu çalışmada, Sağlık Yönetimi bölümünde okuyan ve Temel Bilgi Teknolojileri dersine devam eden öğrencilerin mobil güvenlik ve dijital veri güvenliği farkındalığı ve aralarındaki ilişkinin belirlenmesi amaçlanmıştır. Veriler 2016-2017 bahar döneminde toplanılmıştır. Soru formu; sosyo-demografik özelliklere ilişkin sorular, öğrencilerin akıllı telefon güvenlik farkındalıklarını belirlemek amacıyla "Mobil Uygulamalarda Güvenlik Farkındalığı" anketi, dijital veri güvenliği farkındalık düzeylerini belirlemek için "Dijital Veri Güvenliği Farkındalığı Ölçeği" kullanılmıştır. Veriler Google Form aracılığıyla toplanılmıştır. Verilerin analizinde frekans, yüzde, ikili ve çoklu karşılaştırma analizleri kullanılmıştır. Öğrencilerin dijital veri güvenliği farkındalıklarının; akıllı telefonlarda kötü amaçlı yazılımlar ve güvenlik yazılımlarından haberdar olmak, uygulama indirirken güvenlik mesajlarına dikkate etmek ve kişisel verilere ulaşmak istemesine dikkat etme durumuna göre değiştiği sonucuna ulaşılmıştır.

**Anahtar Kelimeler:** Mobil Güvenlik, Dijital Veri Güvenliği, Sağlık Yönetimi, Öğrenci

#### Abstract

In this study, it is aimed to determine the relationship between mobile security and digital data security awareness among students who read in Department of Health Management and who attend Basic Information Technologies course. The data were collected during spring 2016-2017. Question form; "Security awareness in mobile applications" survey to determine smartphone security awareness of students and "Digital Data Security Awareness Scale" to determine digital data security awareness levels were used in the questions related to socio-demographic characteristics. The data is collected via Google Form. In the analysis of the data, frequency, percentage, binary and multiple comparison analyzes were used. Students' awareness of digital data security; the result is that smartphones have become aware of malware and security software, changed the way the application is considering security considerations, and paying attention to not wanting to access personal data.

**Keywords:** Mobile Security, Digital Data Security, Health Management, Student

## 1. GİRİŞ

Günümüz şartlarında akıllı telefon kullanımı oldukça yaygınlaşmıştır ve bu durumun sonucu olarak da birçok işlemi mobil telefonlar aracılığıyla gerçekleştirmekteyiz. We Are Social ve Hootsuite tarafından yayınlanan “Digital in 2017 Global Overview” raporuna göre dünyanın yarısından fazlası artık en az 1 akıllı telefon kullanıyor, dünya genelinde web trafiğinin yarısından fazlası cep telefonları aracılığıyla sürdürülmekte ve dünyadaki mobil bağlantılarının yarısından çoğunun genişbant bağlantı ile sağlandığı bildirilmektedir (<https://wearesocial.com/special-reports/digital-in-2017-global-overview>, 2017). Türkiye Hane halkı Bilişim teknolojileri Kullanım Araştırması (2017)’na göre, internet kullanan bireylerini oranının %66,8 olduğu ve %72,4’ünün mobil geniş bant bağlantı ile internet erişimi sağladığı belirtilmektedir (TUIK, 2017).

Teknolojideki gelişmeler sayesinde artık akıllı telefonlar hayatımızın gerçeği halinde gelmiştir. Günümüzde birçok kurum işlemlerin daha kolay ve hızlı sürdürülebilmesi için akıllı telefonlara yönelik mobil uygulamalar sunmaktadır. İşletim sistemleri sayesinde akıllı telefonlar salt telefon fonksiyonundan çıkarak mini cep bilgisayarlarına dönüşmüş durumdadır (Özkoçak, 2016; Kuyucu, 2017). Bu fonksiyonların kullanılabilmesinde önemli bir paya sahip olan ise işletim sistemleridir. 2016 yılının dördüncü çeyreğinden itibaren, satılan akıllı telefonların yüzde 80’den fazlası Android işletim sistemine sahiptir. Apple’ın işletim sistemi olan IOS ise piyasanın yaklaşık yüzde 15’ini oluşturmaktadır (<https://www.statista.com/topics/840/smartphones/>, 2017).

Akıllı telefonlar, gündelik hayatın bir parçası olduktan sonra bir takım problemleri de beraberinde getirmiştir (Kuyucu, 2017). Alışverişten eğlenceye, bankacılık işlemlerinden sağlık hizmetlerinin sunumuna kadar birçok alanda mobil uygulamalar mevcuttur. Online süreçler içerisinde gerçekleştirilen ve finansal cezbediciliği olan bu işlemlerin mobil telefonlarla gerçekleştirilmesi kötü niyetli kullanıcılar için kişiyi hedef konumuna getirmektedir. Özellikle Android işletim sistemi kullanıcı sayısının artması ve Android tabanlı sistemlerin açık kaynak kodlu sistemler olması kötücül niyetli kullanıcıların bu alanlarda yoğunlaşmasını arttırmaktadır (Utku ve Doğru, 2016).

Tabi ki burada kötü amaçlı kullanıcıların varlığı da dijital veri güvenliği ve mobil güvenlik için önemli sorun teşkil etmektedir. Hassan, Lass ve Makinde’ye (2012) göre Nijerya’daki siber suçların sebepleri arasında; kentleşme, işsizlik, açgözlü bir şekilde aşırı derecede servet arayışı, siber suç yasalarının zayıf bir şekilde uygulanması ve yeterli donanıma sahip olmayan hukuk kurumları yer aldığını belirtmektedirler. Bununla birlikte bilişim suçlarına ilişkin yapılan araştırmalar bilişim suçu faillerinin genellikle; genç, eğitilmiş, teknik yeteneğe sahip ve agresif oldukları yönündedir (Karagülmez, 2005; Yılmaz, 2015). Her ne kadar günümüzde dijital verilere ulaşmak kolay olursa olsun bu fiilleri gerçekleştirmek için günlük kullanıcı bilgisinden fazlasına ihtiyaç vardır (Yılmaz, 2015). Özellikle hedef yapı banka veya kamu kurumları gibi yüksek düzey güvenlikle korunan kurumlar ise bu işlemi gerçekleştirebilmek için failin teknolojik bilgi düzeyinin en üst seviyede olması gerekmektedir. Günümüzde bu tarz saldırıların giderek arttığı ve genellikle içeriden değil de yetkisiz erişimlerle meydana gelemeye başladığı belirtilmektedir (Dülger, 2013; Yılmaz, 2015).

Sağlık alanında da yaşanan gelişmelerden birisi de dijital hastanelerdir. Hastalara ait bilgilere zaman ve mekan kısıtlaması olmaksızın ulaşım sağlamak ve en çok memnuniyetsizlik sebeplerinden biri olan hasta bekleme sürelerini kısaltması gibi birçok avantaj sağlayacağı düşünülen dijital hastaneler yavaş yavaş günlük hayatımızın içerisine girmektedir (Sağlık Bakanlığı, 2014). Mobil sağlık uygulamalarından bir tanesi de e-nabız uygulamasıdır. Bu tarz uygulamalar kullanıcılar için birçok avantaj sağlamakla birlikte sıkıntılar da getirebilmektedir. Mobil uygulamalar zaman zaman kullanıcılar açısından sorunlar oluştururken, son zamanlarda kurumlar için de önemli bir sorun olan fidye yazılımlar sağlık yöneticilerinin de önemli sorunları arasında yer almaktadır. Kurumsal bilgi güvenliğine etki eden unsurlar içerisinde en zayıf halka olarak

betimlenen insanın en tehlikeli açığı olarak kabul gören durum; güvenlik bilinci zayıflığıdır (Vural ve Sağıroğlu, 2011).

Tutum-davranış ilişkisini etkileyen bir faktör de farkındalıktır. Yapılan araştırmalar, yüksek farkındalığın tutum-davranış ilişkisini güçlendirdiğini göstermektedir (Kağıtçıbaşı ve Camalcılar, 2016). Bireysel farkındalığımız ne kadar yüksek ise o davranışın gösterilme ihtimali de o derece artmaktadır. Bu bağlamda sağlık sektörü için önemli bir yere sahip olacağı düşünülen sağlık yönetici adaylarının mobil güvenlik ve dijital veri güvenliği farkındalıkları artırılması gelecekte bu alanda çalışmalarını yürütürken; bu alanda duyarlı olacakları ve önemli bir maliyet kalemi olan güvenlik yazılımları için daha bilinçli bir bakış açısı geliştirecekleri düşünülmektedir.

## 2. YÖNTEM VE METOT

**Araştırmanın Amacı ve Tipi:** Bu çalışma, akıllı telefon kullanıcılarının mobil güvenlik ve dijital veri güvenliği farkındalığı ve aralarındaki ilişkinin belirlenmesi amacıyla tanımlayıcı tipte planlanmıştır.

**Araştırmanın Evren ve Örneklemi:** Araştırmanın evrenini, 2016-2017 eğitim öğretim yılı bahar döneminde bir üniversitenin Sağlık Yüksekokulu'nda öğrenim gören, Sağlık Yönetimi bölümü öğrencileri arasında Temel Bilgi Teknolojileri dersi alan 1. Sınıf öğrencileri (N:85) oluşturmuştur. Evrenin tamamına ulaşılması hedeflenilmiştir. Çalışmaya gönüllü katılım gösteren ve sorulara tam yanıt veren 68 (%74,1) kişi örneklemi oluşturmuştur.

**Veri Toplama Araçları:** Veri toplama aracı; sosyo-demografik özellikler ilişkin sorulardan oluşan "Bilgi Formu", öğrencilerin akıllı telefon güvenlik farkındalıklarını belirlemek amacıyla Mylonas, Kastania ve Gritzalis (2013) tarafından geliştirilen ve Talan, Aktürk, Korkmaz ve Gülseçen (2015) tarafından Türkçe kullanımı sağlanan anket ve öğrencilerin dijital veri güvenliği farkındalık düzeylerini belirlemek için Yılmaz (2015)'in Doktora Tez çalışmasında geliştirmiş olduğu "Dijital Veri Güvenliği Farkındalığı Ölçeği" (DVGFO)'nden oluşmuştur. DVGFO 32 madden oluşan tek boyutlu bir ölçektir. 5'li Likert ölçüm tekniğine sahip ölçek 5=kesinlikle katılıyorum ve 1=kesinlikle katılmıyorum şeklinde puanlanmaktadır. Ölçekten alınan yüksek düzey puan ortalaması yüksek düzey dijital veri güvenliği farkındalığı anlamı taşımaktadır (Yılmaz, 2015; Yılmaz, Şahin ve Akbulut, 2016). Yılmaz (2015)'in çalışmasında iç tutarlılık katsayısı  $\alpha=0,945$  bulunmuştur. Bu örneklem için Dijital Veri Güvenliği Farkındalığı Ölçeği'nin (DVGFO) Cronbach's Alpha değeri 0,965'tir.

### Verilerin Toplanması:

Veri toplanması sürecinde, Google Form aracılığıyla oluşturulan formun 2016-2017 Eğitim-Öğretim yılı bahar dönem sonunda öğrenciler tarafından doldurulabilmesi için katılımcılara elektronik ortamda iletilmiştir. Elde edilen veri seti içerisinde istatistiksel analiz için uygun olan 68 veri analizlerde kullanılmıştır.

**Verilerin Analizi:** Verilerin analizinde SPSS paket program kullanılmıştır. Analizde yüzde, frekans gibi betimleyici istatistikler, ikili ve çoklu karşılaştırmalarda ise normal dağılım gösterip göstermemesine göre t testi, ANOVA, Mann Whitney U testi ve Kruskal Wallis testi uygulanmıştır. Yapılan analizlerde anlamlılık düzeyi 0,05 olarak alınmıştır.

## 3. BULGULAR

Öğrencilerin %76,5'i (n:52) kadın, %79,4'ü 19-21 yaş grubunda, YGS not ortalaması  $317,71 \pm 20,30$  (min:239, max:352)'dur. %76,5'inin anne eğitim düzeyi ve %55,9'unun baba eğitim düzeyi ilköğretim seviyesindedir. %52,9'u aile ekonomik seviyesini gelir-gider denk olarak belirtmiştir. %92,6'sı internet erişimini mobil aygıtından gerçekleştirmektedir. Öğrencilerin mobil aygıt kullanım süresi ortalama  $5,32 \pm 3,01$  (min:1, max:13) yıldır. %98,5'inin akıllı telefonu vardır.

Öğrencilerin %60,6'sının ailesinde kendisinden başka 1 akıllı telefon kullanıcısı varken, %39,4'ünün birden fazla akıllı telefon kullanıcısı mevcut. Kullanıcıların %47,1'i (n:32) anne, %54,4 'ü (n:37) baba, %63,2'si (n:43) kardeş, %2,9'u (n:2) abla, %1,5'i hepsi ve %1,5'i hiç kullanan yok şeklinde belirtmiştir.

**Tablo 1:** Öğrencilerin Bilgi Teknolojileri Deneyimi ve Gizlilik Tutumu Dağılımı

<i>Değişken</i>	<i>Kategori</i>	<i>Frekans</i> (f)	<i>Yüzde</i> (%)
<i>Bilgi güvenliği kursuna katılım durumu</i>	Evet	1	1,5
	Hayır	67	98,5
<i>Bilişim teknolojileri kullanım deneyimi</i>	Kötü	-	-
	Orta	36	52,9
	İyi	27	39,7
	Mükemmel	5	7,4
<i>Kişisel verilerin gizliliği ve korunması konusunda endişe etme durumu</i>	Evet	46	67,9
	Hayır	22	32,4
<i>Akıllı telefonunuzda kişisel bilgilerinizi saklama durumu</i>	Evet	47	69,1
	Hayır	21	30,9
<i>Akıllı telefonunuzda iş bilgilerinizi saklama durumu</i>	Evet	33	48,5
	Hayır	35	51,5
<i>Akıllı telefonu unutma / kaybetme durumu</i>	Evet	21	30,9
	Hayır	47	69,1
<i>Kötü amaçlı yazılımların varlığından haberdar olma durumu</i>	Evet	40	58,8
	Hayır	28	41,2
<b>Toplam</b>		<b>68</b>	<b>100</b>

Tablo 1. incelendiğinde öğrencilerin akıllı telefonlarında kullandıkları işletim sisteminin %73,5'inin Android işletim sistemidir. %98,5'i daha önce bilgi güvenliği kursuna katılmadıkları, bilgi teknolojileri kullanım deneyimlerini %52,9'u orta olarak değerlendirmiştir. Kişisel verilerin gizliliği ve güvenliği konusunda %67,9'unun (n:46) endişe duyduğu, %69,1'inin (n: 47) akıllı telefonunda kişisel bilgilerinizi sakladığı ve %30,9'unun (n:21) daha önce akıllı telefonunu unutma/kaybetme deneyimi yaşadığı belirlenmiştir. %41,2'sinin (n:28) akıllı telefonlardaki kötü amaçlı yazılımlardan haberdar olmadığı bulunmuştur.

**Tablo 2:** Öğrencilerin Güvenlik Tutumu Dağılımı

<i>Değişken</i>	<i>Kategori</i>	<i>Frekans</i> (f)	<i>Yüzde</i> (%)
<i>Hangi cihazlarda güvenlik için bir yazılım kullanıldığı</i>	Akıllı telefon	29	42,6
	Laptop	24	35,3
	Diğer	-	-
	Hiçbiri	15	22,1
<i>Akıllı telefon güvenlik yazılımlarının varlığından haberdar olma durumu</i>	Evet	42	61,8
	Hayır	26	38,2
<i>Akıllı telefon güvenlik yazılımlarının gerekli olduğunu düşünme durumu</i>	Evet	59	86,8
	Hayır	9	13,2
<i>Mobil uygulama marketlerinden ücretsiz akıllı telefon güvenlik yazılımı araştırma durumu</i>	Evet	6	8,8
	Hayır	62	91,2
<i>Toplam</i>		68	100

Tablo 2. incelendiğinde öğrencilerin %42,6’sının akıllı cihazlarında güvenlik için bir yazılım kullandıkları, %61,8’inin akıllı telefonlar için güvenlik yazılımlarından haberdar olduğu, %86,8’i güvenlik yazılımlarının gerekli olduğunu düşündüğü belirlenmiştir. %91,2’si mobil uygulama marketlerinden ücretsiz telefon güvenlik yazılımı araştırmamaktadırlar.

Öğrencilerin akıllı telefonuna uygulama yükleme kriterleri arasında; %45,6’sı (n:31) güvenilir olmasını, %11,8’i (n:8) indirme oranının yüksek olması, %13,2’si (n:9) ücretsiz olması ve %16,2’si (n:11) etkinliğinin yüksek olması ve diğer özellikler yer almaktadır. Akıllı telefonlarında kullandıkları koruma sistemleri arasında %35,4’ü (n:23) dosya şifreleme ve %52,3’ü (n:34) cihaz parolası kilidi öne çıkmaktadır. %54,4’ü mobil uygulama marketlerindeki uygulamaları akıllı telefonlarına kurmanın güvenli olduğunu düşünüyor. %61,8’i (n:42) mobil uygulama marketlerindeki uygulamaları indirmeden önce güvenlik testin geçtiğini düşünmemektedir. Akıllı telefonlarına yeni bir uygulama yüklerken güvenlik mesajlarına/lisans sözleşmelerine bazen dikkat edenler %66,2 (n:45)’dir. %82,4’ü orijinal uygulama versiyonunu tercih etmektedir. Korsan tercih edenlerin gerekçeleri sorulduğunda korsan uygulamaların daha basit olması ve daha ucuz olması gibi gerekçeler belirtmektedir. Bir öğrenci bu durum için “biz öğrenciyiz hocam yemek yemeye zor para bulurken bir de uygulama mı satın alalım?” şeklinde belirtmiştir.

Öğrencilerin %72,1’i (n:49) uygulama yüklerken kişisel verilere erişip erişmediğini dikkat etmektedir. %69,1’i (n:47) kişisel verilerine erişmek istediğinde uygulamayı indirmekten vazgeçtiği belirtilmektedir.

DVGFÖ puan ortalaması  $4,10 \pm 0,79$  (min:1,84, max:5,00) ‘dur. Ölçekten en düşük ortalama  $3,34 \pm 1,23$  “internet sitelerinde kullanılan güvenlik sertifikaları hakkında bilgi sahibiyim” maddesi olduğu belirlenmiştir. En yüksek puan ortalaması ise  $4,59 \pm 1,10$  ile “izinsiz kullanılmaması için cihazlara (akıllı telefon, tablet, bilgisayar vb.) parola konulabileceğinin farkındayım” maddesinde bulunmuştur.

DVGFÖ’i puan ortalaması açısından akıllı telefonlardaki kötü amaçlı yazılımlardan haberdar olan ve olmayan kişiler arasında anlamlı fark olduğu belirlenmiştir ( $U=367,000$ ,  $Z=-0,849$ ,  $p<0,05$ ).

Akıllı telefon güvenlik yazılımlarından haberdar olan ve olmayan gruplar arasında DVGFÖ’i puan ortalamaları arasında anlamlı fark olduğu belirlenmiştir ( $U=387,500$ ,  $Z=-2,001$ ,  $p<0,05$ )

Yapılan Kruskal-Wallis H non-parametrik çoklu karşılaştırma testi sonucuna göre akıllı telefonuna yeni bir uygulama yüklerken güvenlik mesajlarına/lisans sözleşmelerine “bazen” dikkat eden ve “hiçbir zaman” dikkat etmeyen grup ( $p=0,010$ ) ve “her zaman” dikkat eden ve “hiçbir zaman” dikkat etmeyen grup arasında ( $p=0,004$ ) DVGFÖ puan ortalamaları arasında anlamlı farkın olduğu belirlenmiştir ( $KWX^2=11,397$ ,  $p=0,003$ ).

Uygulama yüklerken kişisel verilere ulaşıp ulaşmadığını dikkate edenler ve etmeyenler arasında DVGFÖ puan ortalamaları açısından anlamlı fark olduğu bulunmuştur ( $U=18,000$ ,  $Z=-3,805$ ,  $p=0,000$ ).

Öğrencilerin yaş, cinsiyet, aile ekonomik durumu, anne ve baba eğitim düzeyi, bilgi teknolojileri kullanım deneyimi, kişisel verilerin gizliliği ve korunması konusunda endişe, akıllı telefonda kişisel ve iş ile ilgili verileri saklama durumu, hangi cihazlarda güvenlik yazılımı kullanma durumu gibi özelliklerin DVGFÖ puan ortalamaları açısından istatistiksel anlamlı fark yaratmadığı belirlenmiştir ( $p>0,05$ ).

#### 4. TARTIŞMA VE SONUÇ

Akıllı telefon kullanıcılarının mobil güvenlik ve dijital veri güvenliği farkındalığı ve aralarındaki ilişkinin belirlenmesi amacıyla yapılan bu çalışmaya katılanların %67,9’unun kişisel verilerin gizliliği ve korunması konusunda endişe duyarken %69,1’i kişisel verilerini akıllı telefonunda sakladığı bulunmuştur. Talan ve ark. (2015) çalışmasında kullanıcıların %63,8’i verilerin gizliliği ve korunması konusunda endişe duyarken %72,2’si akıllı telefonda bu kişisel verileri sakladığı belirtilmektedir. Büyükgöze ve ark. (2017) çalışmasında %63,7 oranında bir bilgi gizliliğine ilişkin endişe duyulurken %71,6 oranında bilgilerin mobil telefonlarda saklandığı bulunmuştur. Gkioulos ve ark. (2017) mobil güvenlikle ilgili bilgi düzeyine bakılmaksızın çalışma gruplarının %29,1’inin yapılan uyarılara rağmen kişisel parolalarını mobil cihazlarında sakladıklarını belirtmektedirler. Mylonas ve ark. (2013) çalışmalarında kullanıcıların hem iş hem kişisel amaçlı olarak aynı cihazı kullandıklarını ve bu nedenle depolanmış bilgilere yetkisiz erişimin etkisinin daha fazla olduğunu belirtmektedir. Ayrıca, önemli sayıda kullanıcının akıllı telefon için güvenlik yazılımına gereksinim duymadığını bulmuşlardır. Çalışmalardan da anlaşıldığı üzere bilgi gizliliği konusunda endişe duyulmasına rağmen bireylerin kişisel bilgilerini akıllı telefonlarında saklama eğiliminde oldukları görülmektedir.

Çalışmada, öğrencilerin %72,1’i uygulama yükleme aşamasında uygulamanın kişisel verilere erişip erişmediğini dikkat ettiği belirlenmiştir. %69,1’i kişisel verilerine erişmek istediğinde bulunan uygulamayı indirmekten vazgeçtiği bulunmuştur. Büyükgöze ve ark (2017) çalışmasında ise %67,6’sı bir uygulama yüklerken kişisel verilere erişip erişmediğine dikkat ettiği ve %70,6’sı uygulama, kişisel verilere erişmek istediğinde, o uygulamanın kullanımına karşı karar verdiği bulunmuştur. Çalışmada uygulama yüklerken kişisel verilere ulaşıp ulaşmadığına dikkat eden ve etmeyenler arasında dijital veri güvenliğine farkındalık düzeylerinin de anlamlı fark yarattığı belirlenmiştir. Ögütçü’nün (2010) çalışmasında, katılımcıların %83,8’inin kişisel bilgilerinin

başkaları tarafından kötü niyetli kullanılabileceğinin farkında olduğu, bununla birlikte %45,4'ünün hacker olmak istediği bulgusu paylaşılmaktadır.

Zaaba ve ark. (2011) çalışmasında kimlik avı uyarısı ile karşılaşan kullanıcıların %75'inin uyarıyı anladığı, ama %13,3'lük bir grubun mesajın ne anlama geldiğini anlamak için daha fazla bilgiye ihtiyaç duyduğu belirlenmiştir. Bu katılımcıların kimlik avı uyarılarında anlayamadıkları 3 ana konu ise; teknik terminoloji (%62), tanımlanan olayın doğası (%55) ve mevcut seçeneklerdir (%25). Kötü niyetli kullanımların farkında olmanın tek başına yeterli olmadığı, son kullanıcı için kullanıcı dostu ve anlaşılır yönergelerin bireylerin kendilerini korumak için doğru kararlar almasına yardımcı olacağı düşünülmektedir.

Çalışmada, en yüksek puan ortalaması ise  $4,59 \pm 1,10$  ile "izinsiz kullanılmaması için cihazlara (akıllı telefon, tablet, bilgisayar vb.) parola konulabileceğinin farkındayım" maddesinde bulunmuştur. Ögütçü'nün (2010) çalışmasında bilgisayar açılışında şifre kullananların oranı %47,1 olarak belirtilmektedir.

Çalışmada öğrencilerin %17,6'sının korsan uygulama yüklediği belirlenmiştir. Gkioulos ve ark. (2017)'in çalışmasında potansiyel güvenlik tehditlerine bakılmaksızın %12,3'lük bir oranda kişilerin resmi olmayan dijital kaynakları kullandığını bildirmiştir. Ögütçü'nün (2010) çalışmasında, bilgisayarlarında lisanslı yazılım kullanmaya hiçbir zaman dikkate etmeyenlerin oranı %9,4 olarak bulunmuştur.

Yılmaz (2015) çalışmasında öğretmenlerin dijital veri güvenliği farkındalıklarını ortalama 4,16'dır. Bu çalışmada Sağlık Yönetimi bölümü öğrencilerinin dijital veri güvenliği farkındalıkları ortalama 4,10 olarak bulunmuştur. Yılmaz'ın (2015) öğretmenler üzerindeki yapmış olduğu çalışmayla benzer sonuç bulunmuştur. Sağlık yönetici adaylarında görevleri gereği hizmet verecekleri birçok insanın dijital verilerini korumakla yükümlü olacakları düşünüldüğünde bu farkındalık düzeyinin daha da artırılması gerektiği düşünülmektedir.

Çalışmada cinsiyetin DVGFO puan ortalamaları açısından istatistiksel fark oluşturmadığı belirlenmiştir. Yılmaz ve ark. (2016) çalışmalarında erkeklerin kadınlara göre dijital veri güvenliği farkındalığının daha yüksek olduğu belirtilmektedir. Güldüren ve ark. (2016) çalışmalarında erkeklerin bilgi güvenliği farkındalıklarının kızlara göre anlamlı düzeyde farklı olduğunu bildirmektedir. Tekerek ve Tekerek (2013) çalışmalarında kadınların erkeklere göre bilgi güvenliği farkındalıklarının anlamlı düzeyde daha yüksek olduğu belirtilmektedir. Literatürde kadın ve erkeklerin dijital veri güvenliğine ilişkin farkındalıklarına yönelik farklı sonuçlar elde edildiği görülmektedir.

Toplumumuzun sorunlara, genel olarak reaktif yapıya sahip davranış kalıplarıyla tepkisel yanıt veriyor olması sebebi ile mobil güvenlik ve dijital veri güvenliği konusunda genelde yapılması gereken tavrın önlem almaya yönelik girişimler olduğu konusunda ayrıca bilinçlendirilmesi gerekmektedir. Zorunlu sigortalar hariç, sigorta sahibi olmamak, Sosyal Güvenlik Kurumu primlerini ödememek gibi davranışlar bu tutumun bir örneğidir. Aynı durum güvenlik yazılımları için de geçerli olmaktadır. Güvenlik yazılımlarının maliyetli olması, sürekli güncellenme gereksiniminin olması, kurulduğu sistemlerin işlem hızlarında düşme yaşanması, gerekliliğine inanmama gibi birçok sebepten dolayı bireyler bu yazılımları kullanmama eğiliminde olabilmektedir.

Mobil güvenlik ve dijital veri güvenliği açısından kilit noktaya sahip olan ise insan faktörüdür. Bu anlamda bireyin dijital platformlarda kendini koruyabilecek düzeye getirilmesi gerekmektedir. Bu açıdan çeşitli eğitim kademelerinde eğitilecek popülasyonun gereksinimlerine göre dizayn edilmiş çeşitli seviyedeki mobil güvenlik ve dijital veri güvenliğine yönelik eğitimlerin düzenlenmesi bireylerin bilinçlendirilmesi açısından önem arz etmektedir.

## KAYNAKÇA

- Global Overview (2017). Digital in 2017 Global Overview. <https://wearesocial.com/special-reports/digital-in-2017-global-overview>. ET: 30.12.2017.
- Büyükgöze S., Bıkmaz Z., Dereli E., Korkmaz A.(2017). Bilgisayar Programcılığı Öğrencilerinin Mobil Güvenlik Farkındalıkları, 2. Uluslararası Çağdaş Eğitim Araştırmaları Kongresi CEAD, 28 Eylül-1 Ekim 2017, Muğla, Türkiye.
- Gkioulos, V., Wangen, G., Katsikas, S.K., Kavallieratos, G.& Kotzanikolaou, P. (2017). Security awareness of the digital natives. *Information*, 8(42): 3-13.doi:10.3390/info8020042
- Güldüren, C., Çetinkaya, L.ve Keser, H. (2016) Ortaöğretim öğrencilerine yönelik Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) geliştirme çalışması. *Elementery Education Online*, 15(2): 682-695.
- Hassan, A.B., Lass, F.D. & Makinde, J. (2012). Cybercrime in Nigeria: Causes, effects, and the way out. *ARNP Journal of Science and Technology*, 2(7):626-631.
- Kağıtçıbaşı, Ç. ve Cemalçılar, Z. (2016). *Dünden Bugüne İnsan ve İnsanlar Sosyal Psikolojiye Giriş*. 18. Basım. Evrim Yayınevi ve Bilgisayar San. Tic. Ltd. Şti. İstanbul.
- Kuyucu, M. (2017). Gençlerde akıllı telefon kullanımı ve akıllı telefon bağımlılığı sorunsalı: “akıllı telefon(kolik)” üniversite gerçeği. *Global Media Journal TR Edition*, 7(14):328-359.
- Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, 34, 47-66.
- Öğütçü, G. (2010). E-dönüşüm sürecinde kişisel bilişim güvenliği davranışı ve farkındalığının analizi. Yayınlanmamış Yüksek Lisans Tezi. Başkent Üniversitesi Fen Bilimleri Enstitüsü, Ankara.
- Özkocak, Y. (2016). Türkiye’de akıllı telefon kullanıcılarının oyalanma amaçlı tercih ettikleri mobil uygulamalar. *Global Media Journal TR Edition*, 6(13): 106-130.
- Statista (2017). Smartphones Industry: Statistics & Facts. <https://www.statista.com/topics/840/smartphones/>. ET: 30.12.2017.
- T.C. Sağlık Bakanlığı (2014). Neden Dijital Hastane. <http://dijitalhastane.saglik.gov.tr/TR,5009/neden-dijital-hastane.html> ET:30.12.2017.
- Talan, T., Aktürk, C., Korkmaz, A., & Gülseçen, S. (2015). Üniversite öğrencilerinin akıllı telefon kullanımında güvenlik farkındalığı. *İstanbul Açık ve Uzaktan Eğitim Dergisi (AUZED)*, 1(2).
- Tekerek, M. ve Tekerek, A. (2013). A research on students’ information security awareess. *Turkish Journal of Education*, 2(3):61-70.
- Türkiye İstatistik Kurumu (2017) Hane Halkı Bilişim Teknolojileri Kullanım Araştırması. <http://www.tuik.gov.tr/PreHaberBultenleri.do?id=24862>. ET: 30.12.2017.
- Utku, A. ve Doğru, İ.A. (2016). Mobil kötücül yazılımlar ve güvenlik çözümleri üzerine bir inceleme. *Gazi Üniversitesi Journal of Scinece*, 4(2): 49-64.
- Vural, Y. ve Sağiroğlu, Ş. (2011). Kurumsal bilgi güvenliğinde güvenlik testleri ve önemi. *Gazi Üniv. Müh. Mim. Fak. Dergisi*, 26(1): 89-103.
- Yılmaz, E. (2015). *Öğretmenlerin dijital veri güvenliği farkındalığı*. Yayınlanmamış Doktora Tezi, Anadolu Üniversitesi, Eğitim Bilimleri Enstitüsü, Eskişehir.
- Yılmaz, E., Şahin, Y.L ve Akbulut, Y. (2016). Öğretmenliğin dijital veri güvenliği farkındalığı. *Sakarya University Journal of Education*. 6/2, ss. 26-45 DOI: <http://dx.doi.org/10.19126/suje.29650>



Yılmaz, F. (2015) *Türkiye’de bilişim suçlarının sosyolojik bir analizi: tehditler ve çözüm stratejileri*. Yayınlanmamış Yüksek Lisans Tezi. Anadolu Üniversitesi Sosyal Bilimler Enstitüsü. Eskişehir.

Zaaba, Z.F., Furnell, S.M & Dowland, P.S. (2011). End-user perception and usability of information security. Proceedings of the Fifth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2011), pp:97-107.