

## ÖĞRETİM ELEMANLARININ BİLGİ GÜVENLİĞİ FARKINDALIĞI ÜZERİNE BİR ARAŞTIRMA

Nurgül ECEK<sup>1</sup>, Sinan YILMAZ<sup>2</sup>

### ÖZ

Günümüzde bilgi güvenliğinin sağlanması ve sürdürülmesi daha güç ve karmaşık bir hale dönüşmüştür. Bu süreçte bilgi güvenliği farkındalığı en önemli faktör olarak ifade edilebilir. Bu çalışmada bireylere farkındalığın kazandırılmasında kritik role sahip olduğu düşünülen öğretim elemanlarının bilgi güvenliği farkındalıklarının incelenmesi amaçlanmıştır. Çalışmada Parsons vd. (2017) tarafından geliştirilen ölçek uyarlanarak 5'li likert skalası ile Türkiye'deki öğretim elemanlarına çevrimiçi uygulanmıştır. 1548 kişiden toplanan veri IBM SPSS paket programı ile analiz edilmiştir. Analiz sonucunda öğretim elemanlarının farkındalığının orta düzeyde olduğu görülmüştür. Ayrıca yürütülen Ki-Kare testleri sonucunda cinsiyet-yaş, cinsiyet-üniversite türü, cinsiyet-akademik alan, cinsiyet-akademik unvan, cinsiyet-işte bilgisayar kullanma saati, yaş-işte bilgisayar kullanma saati, üniversite türü-işte bilgisayar kullanma saati ve meslekte toplam çalışma süresi-işte bilgisayar kullanma saati ilişkileri arasında anlamlı bulgular elde edilmiştir.

**Anahtar Kelimeler:** Bilgi Güvenliği, Farkındalık, Öğretim Elemanları.

<sup>1</sup> Dr., Zonguldak, Türkiye, [nurgulecek67@gmail.com](mailto:nurgulecek67@gmail.com), <https://orcid.org/0000-0002-3763-4571>

<sup>2</sup> Dr. Öğr. Üyesi, Bülent Ecevit Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Zonguldak, Türkiye, [svilmaz@beun.edu.tr](mailto:svilmaz@beun.edu.tr), <https://orcid.org/0000-0002-8576-9913>

## AN INVESTIGATION OF INFORMATION SECURITY AWARENESS OF TERTIARY EDUCATORS

Nurgül ECEK<sup>1</sup>, Sinan YILMAZ<sup>2</sup>

### ABSTRACT

Currently, providing and maintaining of information security has become more difficult and complex. Information security awareness can be expressed as the most important factor in this process. In this study, it is aimed to examine the awareness of tertiary educators, who are thought to have a critical role in raising awareness to individuals. In the study, the scale developed by Parsons et al. (2017) was adapted and applied online to tertiary educators in Turkey with a 5-point Likert scale. Data collected from 1548 people were analyzed with IBM SPSS package program. As a result of the analysis, it was seen that the awareness level of the tertiary educators was at moderate level. In addition, as a result of the Chi-Square tests carried out, significant findings were obtained between the relationships gender and age, gender and university type, gender and academic field, gender and hours of computer use at work, age and hours of computer use at work, the total working time in the profession and the hours of computer use at work.

Keywords: Information Security, Awareness, Tertiary Educators.

<sup>1</sup> PhD., Zonguldak, Türkiye, [nurgulecek67@gmail.com](mailto:nurgulecek67@gmail.com), <https://orcid.org/0000-0002-3763-4571>

<sup>2</sup> Assistant Professor, Bülent Ecevit University, Faculty of Economics and Administrative Sciences, Zonguldak, Türkiye, [yilmaz@beun.edu.tr](mailto:yilmaz@beun.edu.tr), <https://orcid.org/0000-0002-8576-9913>

## 1. GİRİŞ

Bilgi güvenliğinin sağlanması çağımızın öncelikli problemlerinden biridir. Hemen hemen her alanda bilgi sistemlerine bağımlı olunması (Laudon & Laudon, 2011, s. 12; Vroom & Solms, 2004, s. 192), bilgi teknolojilerinin sürekli ve hızlı gelişimi (Chase, 2021, s. 1; Çıfci, 2013, s. 191; Romansky & Noninska, 2020, s. 5292), bilgi güvenliğine yönelik saldırıların gittikçe daha karmaşık araç ve yöntemlerle gerçekleştirilmesi (Harkins, 2013), kapsam ve etki hızının giderek artması (Hawker, 2000) konuyu ilgi odağı haline getirmiştir. Dolayısıyla işletmelerin gerekli güvenlik önlemlerini alması, güvenliği sağlaması ve sürdürmesi zorlaşmaktadır.

Bilgi sistemlerinin oluşturulması, geliştirilmesi ve desteklenmesinden kullanımına kadar (Bourgeois vd., 2019) bilgi güvenliğinin çeşitli süreçlerinde yer alan insanlar psikolojik faktörleri, duyarsızlıkları, hataları ve kasıtlı ya da kasıtsız davranışları ile güvenlik açıklarına yol açabilmektedir (Bulgurcu vd., 2010; Gelişken, 2009; Parsons vd., 2014). Bilgi güvenliği alanında küresel olarak faaliyet gösteren şirketler grubu InfoWatch Analytical Center (2018), küresel veri sızıntıları üzerine yayımladığı raporda veri sızıntılarının %64'ünün çalışanlardan kaynaklandığını ifade etmektedir. Benzer şekilde Dhillon ve Backhouse (2000) çalışanların güvenlik ihlallerinin önemli bir bölümüne neden olduğunu belirtirken Rao ve Nayak (2014) güvenlik olaylarının %80'inin kurum içindeki kişilerden kaynaklandığını ifade etmektedir. Diğer yandan işletmelerin bilgi güvenliğini sağlaması ve sürdürebilmesi de bilgi güvenliğine en büyük tehditlerden biri (Safa vd., 2016; Whitman & Mattord, 2021, s. 50) olarak kabul edilen çalışanlara bağlıdır (Bulgurcu vd., 2010; Hart vd., 2020, s. 18; İleri, 2018; Ögütçü vd., 2016; Siponen & Anthony, 2010). Diğer bir ifade ile güvenlik olaylarının önlenmesi ya da belirlenmesinde çalışanların rolü önemlidir (Ng vd., 2009, s. 815) ve bilgi güvenliğinin yönetilmesinde insan unsuruna odaklanması gerekmektedir (Karaoğlu Yılmaz vd., 2014, s. 178).

Bilgi güvenliği sorunu insan odaklı olarak ele alındığında bilgi güvenliği farkındalığı ilk adımı oluşturmaktadır. Safa vd. (2016, s. 15) farkındalığın güvenlik ihlali risklerini azaltmada en önemli faktör olduğunu belirtmiştir. Farkındalığın kazandırılması veya geliştirilmesi sayesinde çalışanların konuyla ilgili dikkatsizliklerinin ve hatalarının azalacağı, güvenlik teknik ve prosedürlerin etkinliğinin artacağı öngörülmektedir (Hwang vd., 2021, s. 1).

Çalışanların konu ile ilgili farkındalıklarının sürece dâhil edilmesinin niyet ve davranışların öngörülmesinde ve bilgi güvenliği yönetim sürecinde faydalı olacağı düşünülmektedir. Özellikle bilgi teknolojilerinin yoğun kullanıldığı üniversiteler gençlere/bireylere bilgi güvenliği farkındalığının kazandırılmasında ve mevcut farkındalıklarının geliştirilmesinde önemli bir yere sahiptir (Akgün & Topal, 2015, s. 101). Yükseköğretim kurumlarının bilişim sistemleri güvenliği açısından en güvensiz yerlerden biri olarak kabul edilmesi (Keser & Güldüren, 2015, s. 1169) bir bilgi üretim merkezi olan ve önemli miktarda gizli bilgi içeren (Katz, 2005, s. 44) bu kurumlarda konuyla ilgili gerçekleştirilecek bir çalışmanın değerli sonuçları olabileceğini düşündürmektedir. Bu bağlamda bu çalışmada öğretim elemanlarının bilgi güvenliği farkındalıklarının incelenmesi amaçlanmıştır. Öğretim elemanlarının farkındalıklarının değerlendirilmesi ile farkındalığın düşük olduğu konuların belirlenmesinin konuyla ilgili olarak güvenlik politikalarının yeniden düzenlenmesi ve güvenlik sorunlarının ortadan kaldırılması açısından faydalı olabileceği düşünülmektedir. Ayrıca bu çalışma, öğretim elemanlarının bilgi güvenliği farkındalıklarına ilişkin detaylı bulgular sunarak alanyazında konuyla ilgili yapılan çalışmaların teorik bulguları ile karşılaştırmalar yapılmasına katkı sağlayacaktır.

Bu çalışmada sırasıyla bilgi güvenliği farkındalığı ve bu kavrama ilişkin alt boyutları kapsayan bir literatür taraması özeti sunulmuş; ardından yürütülen ampirik araştırma bulgularına dayalı güvenilirlik analizlerine yer verilmiştir. Bunun ardından ampirik araştırma bulguları betimleyici istatistiksel analizler ve bu analizlere dayalı bulgularla birlikte raporlanmıştır.

## 2. BİLGİ GÜVENLİĞİ FARKINDALIĞI

Bilgi güvenliği farkındalığı bilgi güvenliğinde merkezi bir aktör olarak kabul görmektedir (Grassegger & Nedbal, 2021; McCormac, vd., 2017). Farkındalık, kurum ve kuruluşların bilgi varlıklarını korumasının yanı sıra sürdürülebilirliğini sağlamada oldukça önemlidir (Eminağaoğlu & Gökşen, 2009, s. 3).

Bulgurcu vd. (2010, s. 532) bilgi güvenliği farkındalığını bir çalışanın bilgi güvenliği ile ilgili genel bilgisi ve kuruluşunun güvenlik politikalarını bilmesi şeklinde tanımlarken benzer şekilde Ahlan vd. (2015) farkındalığı kullanıcıların çalıştığı kurum ve kuruluşun kurallarına göre sorumluluklarının önemini anladığı ve buna göre hareket ettiği bir bilinç durumu olarak tanımlamıştır. Lionel (2020) ise farkındalığı eğitim yolu ile öğretilen ve güvenlik politikaları ile desteklenen güvenlik uygulamaları ve politikaları ile ilgili bilgi olarak ifade etmiştir.

Yine Pattinson vd. (2017, s. 183) farkındalığı çalışanların kuruluşlarında kabul edilebilir bir güvenlik düzeyi sağlamanın önemini ve sonuçlarını ne ölçüde anladığının bir ölçüsü olarak tanımlamıştır. Krutz ve Vines (2001, s. 26-27) ise bir kuruluşun çalışanlarının güvenlik ve güvenlik kontrolleri ile ilgili genel ve kolektif farkındalığına vurgu yaparken çalışanların önemsiz görünen eylemlerinin bile bir kuruluşun güvenliğini nasıl büyük ölçüde etkileyebileceğini açık bir şekilde anlamaları gerektiğine dikkat çekmiştir.

Farkındalık güvenlik risklerinin azaltılması (Wiley vd., 2020, s. 2) ve güvenlik açıklarının kapatılması açısından oldukça önemlidir (Veseli, 2011, s. 7). Bulgurcu vd. (2010) farkındalığın çalışanların bilgi güvenliği davranışını etkilediğini; Safa vd. (2015) ise farkındalığın kullanıcıların güvenlik davranışı üzerinde pozitif bir etkiye sahip olduğunu belirlemiştir. Bulgurcu vd. (2010) gerçekleştirdikleri çalışma sonucunda çalışanların güvenlik politikalarına uyma niyetinin tutum, normatif inançlar ve özyeterlilik algısından önemli bir şekilde etkilendiğini, farkındalığın da tutum ve sonuç inançlarını olumlu olarak etkilediğini ortaya koymuştur.

Grassegger ve Nedbal (2021) çalışmalarında bilgi güvenliği farkındalığının çalışanların sosyal mühendislik saldırıları ile baş etme niyetine dolaylı etkisinin yanı sıra tutum, algılanan davranışsal kontrol ve öznel norm üzerindeki etkisine de dikkat çekmiştir. Ecek ve Çakmak (2022) çalışanların bilgi güvenliği önlemlerine dair tutumlarını inceledikleri çalışmada farkındalığın bazı alt boyutlarının algılanan fayda, algılanan kullanım kolaylığı ve tutum üzerinde kısmen anlamlı bir etkisi olduğunu ortaya koymuştur. Fianty (2023) yürüttüğü araştırma sonucunda güvenlik eğitimi, bilgi güvenliği farkındalığı, çalışanlar arasındaki güçlü ilişkiler ve çalışanların sorumluluk düzeyi olmak üzere dört ana faktörün çalışanların bilgi sistemlerini kullanma davranışlarını etkilediğini ifade etmiştir.

Okenyi ve Owens (2007)'e göre farkındalık davranış değişikliği sağlayarak çalışanlardan kaynaklanan açıkları azaltmakla birlikte çalışanları bu açıklardan ortaya çıkan tehditlere karşı korumaktadır. Ayrıca farkındalık dinamik bir süreç olduğu için risk profillerinin sürekli olarak takibini, ölçümünü ve yönetilmesini gerektirmektedir (Kruger & Kearney, 2006, s. 290). Dolayısıyla farkındalığın hem kurum ve kuruluşlar hem de çalışanlar tarafından titizlikle ele alınması gereken önemli bir konu olduğu açıktır.

### 3. İNSAN YÖNELİMLİ BİLGİ GÜVENLİĞİ FARKINDALIĞI ANKETİ

Parsons vd. (2014) bilgi güvenliği farkındalığını ölçmek için Bilgi-Tutum-Davranış (BTD) modeline dayanan insan yönelimli bilgi güvenliği farkındalığı anketini geliştirmiştir. Bu ölçek bir çalışanın bilgi güvenliği politika ve prosedürleri ile ilgili bilgisi arttıkça, güvenlik politika ve prosedürlerine yönelik tutumlarının gelişeceğini ve çalışanın daha fazla riskten kaçınarak güvenlik davranışlarının iyileşeceğini varsaymaktadır. Ölçekte yer alan boyutlar birkaç bilgi güvenliği politikasının incelenmesi ve kıdemli yöneticiler ile yapılan görüşmeler neticesinde belirlenmiştir. Parola yönetimi, e-posta kullanımı, internet kullanımı, sosyal medya kullanımı, mobil cihazlar, bilgi işleme ve olay raporlama olmak üzere yedi odak noktası ortaya konulmuştur (Parsons vd., 2014, s. 167). Her odak alanı alt bölümlere ayrılmakta olup ölçekte toplamda 63 ifade yer almaktadır. Bu ölçek ile çalışanların bilgi güvenliği farkındalığının genel/kapsamlı bir şekilde belirlenmesi amaçlanmıştır.

Ölçek, farkındalığa ilişkin çok sayıda faktörün farklı açılardan incelendiği çeşitli araştırma projelerinde farklı popülasyonlar üzerinde test edilmiş, geçerlilik ve güvenilirliği sağlanmıştır (Dharmawansa & Madhuwanthi, 2020; Hadlington & Chivers, 2020; McCormac vd., 2016; McCormac vd., 2017; Pattinson vd., 2017; Pattinson vd., 2019; Wiley vd., 2020). McCormac vd. (2017) ölçeği kullandığı çalışmalarında, yaş, cinsiyet, kişilik ve risk alma eğilimi gibi bireysel farklılık değişkenleri ile farkındalık arasındaki ilişkiyi incelemiş ve yaş ile cinsiyetin farkındalık varyansını açıklamadığını belirlemiştir. Pattinson vd. (2017) banka çalışanlarının daha fazla farkındalığa sahip olduğunu doğrulamak ve farkındalığa katkıda bulunan faktörleri belirlemek için gerçekleştirdikleri çalışma sonucunda banka çalışanlarının ortalama farkındalık seviyelerini çeşitli sektörlerde çalışanlardan %20 daha yüksek bulmuştur. Mahardika vd. (2020) Endonezya Cumhuriyeti Yargı Komisyonu Analiz ve Bilgi Hizmetleri Merkezindeki çalışanların farkındalık seviyesini ölçtüğü çalışmada farkındalık seviyesini orta düzeyde bulmuştur.

Hadlington vd. (2020) çalışanlarda farkındalık ve kaybetme korkusu arasındaki ilişkiyi araştırdıkları çalışmada daha yüksek kaybetme korkusu seviyeleri bildiren katılımcıların daha düşük genel bilgi güvenliği farkındalığına, daha zayıf bilgiye, daha olumsuz bir tutuma sahip olduğu ve daha riskli davranışlarda bulunduğu görülmüştür. Zulfia vd. (2019) çalışanların dosya indirme, süpheli dosyalara erişme ve bilinen kullanıcılardan gelen e-posta linkine tıklama alt boyutlarında en düşük puanları aldığını belirtmiştir. Murphy (2022) güvenlik farkındalığı ile eğitim düzeyleri arasındaki ilişkiyi araştırmak ve hemşirelerin tutum ve davranışlarını motive edici faktörleri tahmin etmek için yaptığı tez çalışmasında bilgi ve tutum arasında güçlü

bir ilişki olduğunu ortaya koymuştur. Yine Pattinson vd. (2019) tarafından gerçekleştirilen çalışmada bireyin farkındalığa ilişkin aldığı eğitimin öğrenme tercihleri ile ne ölçüde örtüştüğü farkındalık ile pozitif yönde ilişkili bulunmuş ancak eğitim sıklığı farkındalık seviyelerini doğrudan tahmin edememiştir.

Wiley vd. (2020)'in çalışmaları sonucunda örgüt kültürü ve güvenlik kültürünün farkındalık ile ilişkili olduğu, güvenlik kültürünün örgütsel kültür ve farkındalık arasındaki ilişkiye aracılık ettiği görülmüştür. Sturman vd. (2023) kimlik avı saldırılarına ilişkin çalışmada katılımcıların saldırı aracını tanımada kimlik avcılığı hakkındaki bilgisi ve zaman baskısının rolünü incelerken bu ölçeğin e-posta kullanımı alt boyutundan yararlanmışlardır.

Hadlington vd. (2019) bilgi güvenliği farkındalığında, işyerinde algılanan kontrol ve iş kimliğinin rolünü araştırdığı çalışmalarında iş kontrol odağının bilgi güvenliği farkındalığı ölçüsündeki toplam puanlar için önemli bir yordayıcı olduğunu ortaya koymuştur. Hadlington ve Parsons (2017)'in siber aylaklık, internet bağımlılığı ve farkındalık arasındaki ilişkiyi araştırdığı çalışmada daha yüksek internet bağımlılığı ve siber aylaklık eğilimleri bildiren katılımcıların daha düşük farkındalığa sahip olduğu görülmüştür.

Reeves vd. (2017) mevcut ölçeğin mobil cihazlar bölümünü kullanarak gerçekleştirdiği çalışmada, algılanan risk, örgütsel bağlılık ve farkındalık arasındaki ilişkiyi incelemiş, örgütsel bağlılık ve algılanan risk değişkeninin farkındalığın önemli tahmin edicileri olduğu sonucuna varmıştır. Witsenber vd. (2022)'in Hollandalı ilkökul ve lise öğrencilerinin siber güvenlik davranışının gelişim düzeyini araştırdıkları çalışmada, aynı ölçeğin sadece davranış ölçen sorularına yer vermiş ve okul müfredatının konuya neredeyse hiç dikkat çekmediğini ve birçok öğrencinin farkındalığa ilişkin pervasız davranışlar sergilediğini ifade etmiştir. Genel olarak öğrencilerin gizlilik ayarlarını kontrol etmedikleri, lise öğrencisi erkeklerin kimlik avı tanıma puanlarının daha yüksek olduğu, kız öğrencilerin de yaşadıkları tuhaf online deneyimleri ebeveynleri ile paylaşma puanlarının daha yüksek olduğu görülmüştür. Fujs vd. (2021) üniversite öğrencileri üzerinde gerçekleştirdiği çalışmada bilgi güvenliği performansına göre kilit grupları belirlemek için söz konusu ölçeği kullanmış ve eğitimin uyarlanmasına olanak tanıyan kullanıcı segmentasyonuna dayalı bir eğitim yaklaşımı önermiştir. Arisya vd. (2020) yürütülen çalışma sonucunda mobil bankacılık uygulaması kullanıcılarının farkındalık seviyesinin iyi olduğunu belirlerken sosyal medya kullanımına ilişkin bilgi, tutum ve davranış boyutlarında farkındalık seviyelerinin ise orta düzey ve tatmin edici olmayan sonuçları olduğunu ortaya koymuştur.

## 4. YÖNTEM

### 4.1. Araştırmanın Amacı ve Önemi

Bu araştırmanın temel amacı farklı düzeylerdeki öğretim üyelerinin bilgi güvenliği farkındalık düzeylerine ilişkin bir ampirik analiz yürütmek ve söz konusu araştırma bulgularını yazına dayalı kişisel analizlerle birlikte sunmaktır. Yürütülen yazın taraması sonucunda bilgi güvenliği farkındalık düzeyinin alt boyutlarının parola yönetimi, e-posta kullanımı, internet kullanımı, sosyal medya kullanımı, mobil cihazlar, bilgi işleme ve olay raporlama olduğu gözlenmiştir. Bu yedi alt boyut yazında ön plana çıkan araştırma eğilimleri ekseninde incelenmiş; elde edilen sonuçlar betimleyici istatistiksel teknikleri kullanılarak sınıflandırılmıştır. Çalışma kapsamında Türkiye'de farklı akademik kurumlarda görev yapmakta olan akademik çalışanlardan toplanan veriler, betimleyici istatistik analiz teknikleri kullanılarak yazında ön plana çıkan araştırma bulguları ile kıyaslamalı olarak incelenmiştir. Alanyazın incelendiğinde bilgi güvenliği yönetim sürecinde öğretim elemanlarının etkin bir rol üstlendiği görülürken bilgi güvenliği farkındalığı alt boyutları açısından yükseköğretim kurumlarında yürütülen detaylı bir çalışmaya rastlanılmamıştır. Bu çalışmanın güvenlik önlemlerinin belirlenmesi ve önceliklendirilmesine ilişkin ipuçları sunacağı, sürece yol göstereceği düşünüldüğünden alanyazına katkı sağlayacak önemli bir çalışma olduğu düşünülmektedir.

### 4.2. Araştırmanın Evreni ve Örneklemi

Çalışmanın araştırma evreni Türkiye'deki yükseköğretim kurumlarında görev yapan öğretim elemanlarıdır. Yükseköğretim Bilgi Yönetim Sisteminden 15/10/2022 tarihinde ulaşılan veriye göre Türkiye'de görev yapan öğretim elemanlarının sayısı 184566'dır. Çalışmada örnekleme yapılmamış olup araştırma evreninin tamamına ulaşılmaya çalışılmıştır. Yökakademik (Yükseköğretim Akademik Arama) sitesinde yer alan e-posta adreslerine anket formunun iletilmesinin ardından 2727 geri dönüş yapılmış ancak uç değerlere sahip olduğu belirlenen 1179 anket değerlendirmeye alınmamıştır. Araştırma kapsamında araştırma evrenini temsil eden 1548 öğretim elemanından oluşan bir örneklem hacmine ulaşılmıştır (Sekaran, 2003, s. 294).

### 4.3. Veri Toplama Araçları ve Süreci

Çalışmada Parsons vd. (2017) tarafından geliştirilen ölçek uyarlanarak 5’li likert skalası ile kullanılmıştır. Anket online olarak hazırlanmış ve 15/10/2022-15/12/2022 tarihleri arasında öğretim elemanlarına elektronik posta aracılığı ile gönderilmiştir. Anket formunun ilk bölümünde demografik özellikleri inceleyen 8 ifade, ikinci bölümünde parola yönetimi, e-posta kullanımı, internet kullanımı, sosyal medya kullanımı, mobil cihazlar, bilgi işleme ve olay raporlama örtük değişkenlerine ilişkin farkındalık düzeyini ölçümleyen bilgi, tutum ve davranış açısından 9’ar ifade olmak üzere toplam 63 ifade yer almaktadır. Ölçekte yer alan alt boyutlara ilişkin örnek ifadeler bulgular bölümünde sırasıyla belirtilmiştir.

### 4.4. Verilerin Analizi

Verilerin analizinde IBM SPSS paket programı kullanılarak betimleyici istatistiksel analizler ve Ki-kare testleri yürütülmüştür. Betimleyici istatistikler, verilerin düzenlenmesi, sunulması ve analiz edilmesi için kullanılmakta olup varsayımların test edilmesi için değişkenlere ait ortalama, standart sapma, puan aralığı, çarpıklık ve basıklığı içermektedir (Fisher ve Marshall, 2009: 95; Pallant, 2020: 90). Ki-kare testi ise parametrik olmayan testler içerisinde yaygın kullanılan bir dağılım olup farklı kategorilere ayrılmış olan iki olay arasındaki ilişkinin testidir. İlişki katsayıları ile ilişkinin olup olmadığı, ilişki varsa ilişkinin yönü ve büyüklüğü belirlenmektedir (Karagöz, 2019: 560).

## 5. BULGULAR

### 5.1. Demografik İstatistikler

Çalışmada katılımcıların demografik özelliklerine ilişkin bilgiler Tablo 1’de sunulmaktadır.

		N	%
Cinsiyet	Erkek	778	50,3
	Kadın	770	49,7
	<b>Toplam</b>	<b>1548</b>	<b>100,0</b>
Yaş	21-30	292	18,9
	31-40	557	36,0
	41-50	432	27,9
	51-60	222	14,3
	60<	45	2,9
	<b>Toplam</b>	<b>1548</b>	<b>100,0</b>
Öğrenim Durumu	Yüksek Lisans	352	22,7
	Doktora	1196	77,3
	<b>Toplam</b>	<b>1548</b>	<b>100,0</b>
Üniversite Türü	Devlet	1389	89,7
	Vakıf	158	10,2
	<b>Toplam</b>	<b>1548</b>	<b>100,0</b>
Mensubu olunan akademik alan	Fen Bilimleri	401	25,9
	Sağlık Bilimleri	410	26,5
	Sosyal Bilimler	627	40,5
	Diğer	109	7,1
	<b>Toplam</b>	<b>1548</b>	<b>100,0</b>

Tablo 1. devamı		N	%
Akademik Unvan	Araştırma Görevlisi	373	24,1
	Öğretim Görevlisi	332	21,4
	Dr. Öğretim Üyesi	369	23,8
	Doçent	251	16,2
	Profesör	223	14,4
	<b>Toplam</b>	1548	100,0
Meslekteki toplam çalışma süresi (yıl)	<1	15	1,0
	2-5	426	27,5
	6-10	327	21,1
	10<	780	50,4
	<b>Toplam</b>	1548	100,0
İşte bilgisayar kullanma saati (günlük ortalama)	1-4	480	31,0
	5-8	965	62,3
	9<	103	6,7
	<b>Toplam</b>	1548	100,0

Tablo 1 incelendiğinde; katılımcıların cinsiyet açısından dengeli dağıldığı, katılımcıların en çok 31-40 yaş aralığında (%36), en az 60 üzeri yaş grubunda (%3) yer aldığı ve katılımcıların %77'sinin doktora mezunu olduğu görülmektedir. Katılımcıların %90'ının devlet üniversitesinde görev yaptığı ve katılımın en çok sosyal bilimler alanından (%41) olduğu dikkat çekmektedir. Katılımcıların en çok araştırma görevlisi (%24) unvanında ve en az profesör (%14) unvanında görev yaptığı görülmektedir. Katılımcıların yarısının (%50) 10 yıl üzeri çalışma süresi grubunda yer aldığı ve %62'sinin iş yerinde ortalama 5-8 saat aralığında bilgisayar kullandığı görülmektedir.

## 5.2. Güvenilirlik Analizi

Araştırmada kullanılan ölçeğin güvenilirliği Cronbach alpha katsayısı ile test edilmiş olup yapılarla ilişkin güvenilirlik analizi sonuçları Tablo 2'de sunulmuştur.

Tablo 2. Güvenilirlik Analizi	
Yapılar	Cronbach Alfa
Parola Yönetimi	0,73
E-posta Kullanımı	0,81
İnternet Kullanımı	0,68
Sosyal Medya Kullanımı	0,71
Mobil Cihazlar	0,86
Bilgi İşleme	0,83
Olay Raporlama	0,88

Tablo 2'de görüldüğü gibi, güvenilirlik analizi sonucunda internet kullanımı değişkeni hariç araştırmada yer alan değişkenlerin alfa güvenilirlik katsayıları 0,71-0,88 arasında bulunmuştur. George ve Mallery (2003)'nin skalasına göre ölçeğin güvenilirliği iyi olarak kabul edilmiştir. İnternet kullanımı değişkeni için yeterli güvenilirlik sağlanamadığından analizden çıkarılmıştır.

## 5.3. Değişkenlere Ait Ortalama ve Standart Sapma Değerleri

Araştırmada yer alan örtük değişkenlere ait ortalama ve standart sapma değerleri Tablo 4'te sunulmuştur.

Bu araştırmada farkındalık düzeyi altı alt boyuta ait ortalamaların ortalaması alınarak ölçülmüştür. Salem vd. (2021)'nin üniversite öğrencileri üzerinde yürüttükleri çalışmada kullanılan Bilgi Güvenliği Farkındalığı (BGF) skalası Tablo 3'te gösterilmiştir.

Tablo 3. BGF Skalası	
BGF Seviyesi Skalası	Ortalama
Yüksek	> 4,5
Orta	4,0 – 4,5
Düşük	< 4

Tablo 3'te görüldüğü gibi, bu skalaya göre farkındalık seviyesi  $M > 4,5$  için yüksek,  $M: 4 - 4,5$  arasında ise orta ve  $M < 4$  için düşük olarak belirlenmiştir.

**Tablo 4. Betimleyici İstatistiksel Analiz**

Değişkenler	Ortalama	Std. Sapma
Parola Yönetimi	4,19	1,03
E-posta Kullanımı	4,26	0,82
Sosyal Medya Kullanımı	4,14	0,95
Mobil Cihazlar	4,43	0,77
Bilgi İşleme	4,41	0,83
Olay Raporlama	4,07	0,88

Tablo 4'te yer alan ifadelerle göre, örtük değişkenler için farkındalık seviyesinin ( $M=4,07-4,43$ ) orta düzeyde olduğu görülmüştür.

**Tablo 6. Parola Yönetimine İlişkin Yapılan Bazı BGF Araştırmaları**

Değişken	BGF Araştırmalarına Ait Ortalamalar							
	Salem, vd. (2021)	Wang (2022)	Erdoğan (2017)	Avcı ve Oruç (2020)	Dharmawansa ve Madhuwanthi (2020)	Kritzinger vd. (2022)	Ceylan (2019)	Alese vd. (2007)
Parola Yönetimi Ortalama	Üniversite Öğrencisi n=200	Üniversite Öğrencisi n=111	Üniversite Öğrencisi n=550	Üniversite Öğrencisi n=88	Srilanka Banka Çalışanı n=357	Çeşitli Sektör Çalışanı n=356	Bilişim Sektörü Çalışanı n=200	Nijerya İnternet Kullanıcısı n=430
	4,19	4,06	3,73	3,87	4,04	3,85	4,52	3,64

Tablo 6 incelendiğinde; bu çalışmada parola yönetimine ilişkin farkındalık seviyesi Salem vd. (2021)'nin BGF skalasına göre orta düzeyde ( $M=4,19$ ) bulunmuştur. Benzer şekilde aynı skalaya göre Salem vd. (2021), Witsenboer vd. (2022) ile Avcı ve Oruç (2020) tarafından üniversite öğrencileri üzerinde gerçekleştirilen çalışmalarda farkındalık seviyesi orta düzeyde bulunmuştur. Buna karşın yine aynı skalaya göre Kritzinger vd. (2022) çeşitli sektörlerde çalışanlar üzerinde gerçekleştirdiği çalışmada farkındalık seviyesini yüksek düzeyde gözlemlerken Ceylan (2019) bilişim sektörü çalışanlarında, Dharmawansa ve Madhuwanthi (2020) banka çalışanlarında, Wang (2022), Erdoğan (2017) ve Alese vd. (2007) ise üniversite öğrencilerinde farkındalık seviyesini düşük düzeyde gözlemlemiştir.

**Tablo 7. E-posta Kullanımına İlişkin Farkındalığa Ait Ortalama ve Standart Sapma**

E-posta Kullanımı	İfadeler	Aritmetik Ortalama	Std. Sapma
Bilgi 4	Tanıdık kişilerden gelen e-postalardaki bağlantılara tıklanılabilir.*	3,00	1,122
Tutum 4	Tanıdığım kişilerden gelen e-postalardaki bağlantıları tıklamak her zaman güvenlidir.*	3,91	1,011
Davranış 4	Tanıdığım birinden gelen e-postalardaki bağlantılara her zaman tıklamam.	3,82	1,081
Bilgi 5	Bilinmeyen bir gönderenden gelen e-postadaki bağlantıya tıklanmamalıdır.	4,69	,691
Tutum 5	Bilinmeyen bir gönderenden gelen e-postadaki bağlantıya tıklarsam kötü bir şey olmaz.*	4,63	,611
Davranış 5	Bilinmeyen bir gönderenden gelen bir e-posta ilginç görünüyorsa içindeki bağlantıya tıklarım.*	4,55	,717
Bilgi 6	Bilinmeyen gönderenlerden gelen e-posta ekleri açılabilir.*	4,57	,704
Tutum 6	Bilinmeyen bir gönderenden gelen bir e-posta ekini açmak risklidir.	4,66	,596
Davranış 6	Gönderen bilinmiyorsa e-posta eklerini açmam.	4,51	,823

Not: (\*) Ters kodlama yapılan ifadeler



**Tablo 8. E-posta Kullanımına İlişkin Bazı BGF Araştırmaları**

E-Posta Kullanımı Ortalama	BGF Araştırmalarına Ait Ortalamalar						
	Salem, vd. (2021)	Witsenboer vd. (2022)		Wang (2022)	Dharmawansa ve Madhuwanthi (2020)	Kritzinger vd.(2022)	Ceylan (2019)
	Üniversite Öğrencisi n=200	Hollanda'da Ortaokul Öğrencisi n=146		Yüksekokul Öğrencisi n=96	Üniversite Öğrencileri n=111	Srilanka Banka Çalışanı n=357	Çeşitli Sektör Çalışanı n=356
4,26	4,66	3,69	3,97	3,82	3,99	3,99	4,04

Tablo 8 incelendiğinde; bu çalışmada e-posta kullanımına ilişkin farkındalık seviyesi Salem vd. (2021)'nin BGF skalasına göre (M= 4,26) orta düzeyde bulunmuştur. Salem vd. (2021) üniversite öğrencileri üzerinde gerçekleştirdikleri çalışmada e-posta kullanımına ilişkin farkındalık seviyesini yüksek düzeyde gözlemlerken Dharmawansa ve Madhuwanthi (2020) banka çalışanlarında, Kritzinger vd. (2022) çeşitli sektör çalışanlarında, Wang (2022), Witsenboer vd. (2022) öğrencilerde farkındalık seviyelerini aynı skalaya göre düşük düzeyde gözlemlemiştir. Ceylan (2019) ise söz konusu skalaya göre bilişim sektörü çalışanları üzerinde gerçekleştirdiği çalışmada bu çalışmanın bulguları ile uyumlu olarak farkındalık seviyesini orta düzeyde gözlemlemiştir.

**Tablo 9. Sosyal Medya Kullanımına İlişkin Farkındalığa Ait Ortalama ve Standart Sapma**

Sosyal Medya Kullanımı	İfadeler	Aritmetik Ortalama	Std. Sapma
Bilgi 7	Sosyal medya hesaplarımdaki gizlilik ayarlarımı düzenli olarak incelemeliyim.	4,15	,869
Tutum 7	Sosyal medya gizlilik ayarlarımı düzenli olarak gözden geçirmek iyi bir fikirdir.	4,36	,725
Davranış 7	Sosyal medya gizlilik ayarlarımı düzenli olarak gözden geçirmiyorum.*	3,38	1,258
Bilgi 8	Sosyal medyada paylaştığım bir şey için kovulmam.*	3,81	1,183
Tutum 8	Sosyal medyada normalde açıkça söylemediğim bir şeyi yayınlamamın önemi yoktur.*	3,81	1,389
Davranış 8	Olumsuz sonuçlarını düşünmeden sosyal medyada hiçbir şey yayınlamam.	4,48	,767
Bilgi 9	İşle ilgili istediğim şeyi sosyal medyada paylaşabilirim.*	4,19	,971
Tutum 9	İşle ilgili bazı bilgileri sosyal medyada yayınlamak risklidir.	4,49	,711
Davranış 9	İşimle ilgili istediğim her şeyi sosyal medyaya gönderiyorum.*	4,56	,718

Not: (\*) Ters kodlama yapılan ifadeler

**Tablo 10. Sosyal Medya Kullanımına İlişkin Bazı BGF Araştırmaları**

Değişken	BGF Araştırmalarına Ait Ortalamalar								
	Yaman vd. (2021)	Witsenboer vd. (2022)			Erdoğan (2017)	Avcı ve Oruç (2020)	Dharmawansa ve Madhuwanthi (2020)	Kritzinger vd. (2022)	Ceylan (2019)
Sosyal Medya Kullanımı Ortalama	Hollanda'da								
	Üniversite Öğrencisi n=200	Ortaokul Öğrencisi n=146	Yüksekokul Öğrencisi n=96	Üniversite Öğrencisi n=550	Üniversite Öğrencisi n=88	Srilanka Banka Çalışanı n=357	Çeşitli Sektör Çalışanı n=356	Bilişim sektörü çalışanı n=200	
	4,14	4,38	3,45	3,31	3,96	4,27	3,87	4,26	3,83

Tablo 10 incelendiğinde; bu çalışmada sosyal medya kullanımına ilişkin farkındalık seviyesi Salem vd. (2021)'nin BGF skalasına göre (M= 4,14) orta düzeyde bulunmuştur. Salem vd. (2021) ile Avcı ve Oruç (2020) öğrenciler üzerinde, Kritzinger vd. (2022) ise çalışanlar üzerinde gerçekleştirdikleri çalışmalarda farkındalığı aynı skalaya göre orta düzeyde gözlemlemiştir. Dharmawansa ve Madhuwanthi (2020) banka çalışanlarında, Ceylan (2019) bilişim sektörü çalışanlarında, Witsenboer vd. (2022) ile Erdoğan (2017) ise öğrencilerde yürüttüğü çalışma sonucunda farkındalık seviyesini aynı skalaya göre düşük düzeyde gözlemlemiştir.

**Tablo 11. Mobil Cihazlara İlişkin Farkındalığa Ait Ortalama ve Standart Sapma**

Mobil Cihazlar	İfadeler	Aritmetik Ortalama	Std. Sapma
Bilgi 13	Halka açık bir yerde (kafe vb.) çalışırken mobil cihazımı (laptop, notebook, cep telefonu vb.) yanımdan ayırmamalıyım.	4,59	,739
Tutum 13	Halka açık bir yerde çalışırken mobil cihazımı kısa süreliğine gözetimsiz bırakmak güvenlidir.*	4,74	,509
Davranış 13	Halka açık bir yerde çalışırken mobil cihazımı gözetimsiz bırakırım.*	4,81	,440
Bilgi 14	Önemli iş dosyaları herkese açık bir Wi-Fi ağı aracılığıyla gönderilebilir.*	4,26	,941
Tutum 14	Önemli iş dosyalarını herkese açık bir Wi-Fi ağı aracılığıyla göndermek risklidir.	4,34	,890
Davranış 14	Önemli iş dosyalarını herkese açık bir Wi-Fi ağı kullanarak gönderiyorum.*	4,15	1,034
Bilgi 15	Önemli bir belge üzerinde çalışırken yabancıların mobil cihaz (dizüstü bilgisayar vb.) ekranımı görmediklerinden emin olmam gerekir.	4,36	,777
Tutum 15	Yabancılar ekranımı görebiliyorsa mobil cihazımdan önemli iş dosyalarına erişmek risklidir.	4,34	,784
Davranış 15	Önemli bir belge üzerinde çalışırsam yabancıların mobil cihaz ekranımı görmediğini kontrol ederim.	4,28	,831

Not: (\*) Ters kodlama yapılan ifadeler

Tablo 12. Mobil Cihazlara İlişkin Bazı BGF Araştırmaları								
Değişken	BGF Araştırmalarına Ait Ortalamalar							
Mobil Cihazlar Ortalama	Salem vd. (2021)	Witsenboer vd. (2022) Hollanda'da		Wang (2022)	Dharmawansa ve Madhuwanthi (2020)	Kritzinger vd. (2022)	Ceylan (2019)	
	Üniversite Öğrencisi n=200	Ortaokul Öğrencisi n=146	Yüksekokul Öğrencisi n=96	Üniversite Öğrencisi n=111	Srilanka Banka Çalışmanı n=357	Çeşitli Sektör Çalışmanı n=356	Bilişim Sektörü Çalışmanı n=200	
	4,43	4,52	3,31	4,16	3,82	3,92	4,52	4,04

Tablo 12 incelendiğinde; bu çalışmada mobil cihazlara ilişkin farkındalık seviyesi Salem vd. (2021)'nin BGF skalasına göre orta düzeyde (M=4,43) bulunmuştur. Bu çalışmanın bulgusu ile uyumlu olarak Ceylan (2019) bilişim sektörü çalışanları üzerinde gerçekleştirdiği çalışmada farkındalık seviyesini aynı skalaya göre orta düzeyde gözlemlemiştir. Diğer taraftan Salem vd. (2021) öğrenciler üzerinde, Kritzinger vd. (2022) çalışanlar üzerinde gerçekleştirdikleri çalışmada farkındalık seviyesini aynı skalaya göre yüksek düzeyde gözlemlerken Dharmawansa ve Madhuwanthi (2020) banka çalışanlarında, Witsenboer vd. (2022) ile Wang (2022) ise öğrencilerde farkındalık seviyesini aynı skalaya göre düşük düzeyde gözlemlemiştir.

Tablo 13. Bilgi İşlemeye İlişkin Farkındalığa Ait Ortalama ve Standart Sapma			
Bilgi İşleme	İfadeler	Aritmetik Ortalama	Std. Sapma
Bilgi 16	Önemli çıktılar hassas olmayanlarla aynı şekilde imha edilebilir.*	4,01	1,130
Tutum 16	Önemli çıktıları çöp kutusuna koyarak imha etmek güvenlidir.*	4,20	1,044
Davranış 16	Önemli çıktıların imha edilmesi gerektiğinde bunların parçalanmasını, tahrip olmasını sağlarım.	4,35	,854
Bilgi 17	Halka açık bir yerde bir USB bellek bulursam iş bilgisayarına takmamalıyım.	4,75	,510
Tutum 17	Halka açık bir yerde bulduğum bir USB belleği iş bilgisayarına takarsam kötü bir şey olmaz.*	4,72	,537
Davranış 17	Halka açık bir yerde bulunan bir USB belleği iş bilgisayarına takmam.	4,74	,536
Bilgi 18	Önemli bilgiler içeren çıktıları bir gece masamda bırakabilirim.*	4,22	1,016
Tutum 18	Önemli bilgiler içeren çıktıları bir gece masa üzerinde bırakmak risklidir.	4,34	,897
Davranış 18	Orada olmadığımda önemli bilgileri içeren çıktıları masamda bırakırım.*	4,32	,957

Not: (\*) Ters kodlama yapılan ifadeler

Tablo 14. Bilgi İşlemeye İlişkin Bazı BGF Araştırmaları			
Değişken	BGF Araştırmalarına Ait Ortalamalar		
Bilgi İşleme Ortalama	Dharmawansa ve Madhuwanthi (2020)	Kritzinger vd. (2022)	
	Srilanka'da Özel bir Banka Çalışmanları n=357	Çeşitli Sektör Çalışmanları n=356	
	4,41	3,91	4,4

Tablo 14 incelendiğinde; bu çalışmada bilgi işlemeye ilişkin farkındalık seviyesi Salem vd. (2021)'in BGF skalasına göre orta düzeyde (M=4,41) bulunmuştur. Benzer şekilde aynı BGF skalasına göre Kritzinger vd. (2022) çeşitli sektörlerde çalışanlar üzerinde gerçekleştirdikleri çalışmada farkındalık seviyesini orta düzeyde gözlemlerken Dharmawansa ve Madhuwanthi (2020) ise banka çalışanları üzerinde gerçekleştirdikleri çalışmada farkındalığı aynı skalaya göre düşük düzeyde gözlemlemiştir.

**Tablo 15. Olay Raporlamaya İlişkin Farkındalığa Ait Ortalama ve Standart Sapma**

Olay Raporlama	İfadeler	Aritmetik Ortalama	Std. Sapma
Bilgi 19	İş yerinde şüpheli davranan birini görürsem rapor etmeliyim.	4,06	,888
Tutum 19	İş yerinde şüpheli davranan birini görürsem kötü bir şey olmayabilir.*	3,99	,894
Davranış 19	İş yerinde şüpheli davranan birini görürsem bu konuda bir şeyler yaparım.	4,00	,847
Bilgi 20	Çalışma arkadaşımın zayıf güvenlik davranışlarını görmezden gelmemeliyim.	3,98	1,029
Tutum 20	Çalışma arkadaşımın zayıf güvenlik davranışını görmezden gelirim kötü bir şey olmaz.*	4,19	,776
Davranış 20	Çalışma arkadaşımın güvenlik kurallarını göz ardı ettiğini fark etseydim herhangi bir işlem yapmazdım.*	4,02	,874
Bilgi 21	Güvenlik olaylarını bildirmek isteğe bağlıdır.	3,93	1,071
Tutum 21	Önemli olmadıklarını düşünsem bile güvenlik olaylarını göz ardı etmek risklidir.	4,28	,786
Davranış 21	Bir güvenlik olayı fark etseydim rapor ederdim.	4,22	,800

Not: (\*) Ters kodlama yapılan ifadeler

**Tablo 16. Olay Raporlamaya İlişkin BGF Araştırmaları**

Değişken	BGF Araştırmalarına Ait Ortalamalar	
Olay Raporlama Ortalama	Dharmawansa ve Madhuwanthi (2020)	Kritzinger, Veiga ve Staden (2022)
	Srilanka'da Özel bir Banka Çalışanları n=357	Çeşitli Sektör Çalışanları n=356
4,07	3,92	4,51

Tablo 16 incelendiğinde; bu çalışmada olay raporlamaya ilişkin farkındalık seviyesi Salem vd. (2021)'nin BGF skalasına göre orta düzeyde (M= 4,07) bulunmuştur. Dharmawansa ve Madhuwanthi (2020) banka çalışanları üzerinde gerçekleştirdikleri çalışmada farkındalık seviyesini aynı skalaya göre düşük düzeyde gözlemlerken Kritzinger vd. (2022) çeşitli sektör çalışanları üzerinde gerçekleştirdikleri çalışmada farkındalık seviyesini yüksek düzeyde gözlemlemiştir.

#### 5.4. Ki-Kare Testi Analizi

Cinsiyet-yaş, cinsiyet-üniversite türü, cinsiyet-akademik alan, cinsiyet-akademik unvan, cinsiyet-işte bilgisayar kullanma saati, yaş-işte bilgisayar kullanma saati, üniversite türü-işte bilgisayar kullanma saati, akademik unvan-işte bilgisayar kullanma saati ve meslekte toplam çalışma süresi-işte bilgisayar kullanma saati ilişkileri için Ki-Kare testi yapılarak ilgili değişkenler arasında anlamlı bir ilişki olup olmadığı incelenmiştir.

**Tablo 17. Cinsiyet ve Yaş Çapraz Tablosu**

Cinsiyet	Yaş					Toplam
	21-30	31-40	41-50	51-60	60<	
<b>Erkek</b>	98	269	244	139	28	778
<b>Kadın</b>	194	288	188	83	17	770
<b>Toplam</b>	292	557	432	222	45	1548

Tablo 17 incelendiğinde hem erkek hem kadın bireylere ilişkin frekans değerlerinin 31-40 yaş grubu aralığında yoğunlaştığı; en düşük frekans değerlerinin ise 60<yaş grubunda olduğu görülmüştür.

<b>Tablo 18. Cinsiyet ve Yaş Ki- Kare Testi</b>			
	Değer	Serbestlik Derecesi	Anlamlılık (Çift taraflı)
Pearson Ki-Kare	56,244 <sup>a</sup>	4	0,000
Geçerli Veri Sayısı	1548		

<b>Tablo 19. Cinsiyet ve Yaş Etki Boyutu</b>			
Nominal by Nominal	Phi	0,191	0,000
	Cramer's V	0,191	0,000
Geçerli Veri Sayısı		1548	

Tablo 18'de sunulan Ki-Kare bağımsızlık testi, cinsiyet ve yaş değişkenleri arasında anlamlı bir fark olduğunu göstermiştir,  $X^2(4, n=1548) = 56.24, p=.00$ , Cramer's  $V=0,19$ . Bu durum Cohen (1988)'in skalasına göre yaş ve cinsiyet değişkenleri arasındaki etkileşimin zayıf olduğu anlamına gelmektedir.

<b>Tablo 20. Cinsiyet ve Üniversite Türü Çapraz Tablosu</b>				
Cinsiyet	Üniversitenizin Türü		Toplam	
	Devlet	Vakıf		
Erkek	712	66		778
Kadın	678	92		770
Toplam	1390	158		1548

Tablo 20'de hem erkek hem kadın bireylere ilişkin frekans değerlerinin devlet üniversitesinde yoğunlaştığı görülmüştür.

<b>Tablo 21. Cinsiyet ve Üniversite Türü Ki-Kare Testi</b>			
	Değer	Serbestlik Derecesi	Asimptotik Anlamlılık (2 taraflı)
Sürekli Düzeltme <sup>b</sup>	4,698	1	,030
Geçerli Veri Sayısı	1548		

<b>Tablo 22. Cinsiyet ve Üniversite Türü Etki Boyutu</b>			
Nominal by Nominal	Phi	Değer	Yaklaşık Anlamlılık
	Cramer's V	,057	,024
Geçerli Veri Sayısı		,057	,024
		1548	

Tablo 21'de sunulan Ki-kare bağımsızlık testi, cinsiyet ve üniversite türü değişkenleri arasında anlamlı bir ilişki bulunduğunu göstermiştir,  $X^2(1, n=1548) = 4.70, p =.03, phi=.06$ . Bu durum Cohen (1988)'in skalasına göre cinsiyet ve üniversite türü değişkenleri arasındaki etkileşimin zayıf olduğu anlamına gelmektedir.

<b>Tablo 23. Cinsiyet ve Akademik Alan Çapraz Tablosu</b>					
Cinsiyet	Akademik Alan				Toplam
	Fen Bilimleri	Sağlık Bilimleri	Sosyal Bilimler	Diğer	
Erkek	254	133	349	41	777
Kadın	147	277	278	68	770
Toplam	401	410	627	109	1547

Tablo 23'te erkek bireylere ilişkin frekans değerlerinin sosyal bilimler alanında yoğunlaştığı; kadın bireylere ilişkin frekans değerlerinin ise sosyal bilimler ve sağlık bilimleri alanında yoğunlaştığı görülmüştür.

<b>Tablo 24. Cinsiyet ve Akademik Alan Ki-Kare Testi</b>			
	Değer	Serbestlik Derecesi	Asimptotik Anlamlılık (Çift taraflı)
Pearson Ki-Kare	93,825 <sup>a</sup>	3	,000
Geçerli Veri Sayısı	1547		

**Tablo 25. Cinsiyet ve Akademik Alan Etki Boyutu**

		Değer	Yaklaşık Anlamlılık
Nominal by Nominal	Phi	,246	,000
	Cramer's V	,246	,000
Geçerli Veri Sayısı		1547	

Tablo 24'te sunulan Ki-Kare bağımsızlık testi cinsiyet ve akademik alan değişkenleri arasında anlamlı bir ilişki olduğunu göstermiştir,  $X^2(3, n = 1548) = 93.83, p = .00$ ,  $cramer's v = .25$ . Bu durum Cohen (1988)'in skalasına göre cinsiyet ve akademik alan değişkenleri arasındaki etkileşimin zayıf olduğu anlamına gelmektedir.

**Tablo 26. Cinsiyet ve Akademik Unvan Çapraz Tablosu**

Cinsiyet	Akademik Unvan					Toplam
	Araştırma Görevlisi	Öğretim Görevlisi	Dr. Öğretim Üyesi	Doçent	Profesör	
Erkek	135	172	186	140	145	778
Kadın	238	160	183	111	78	770
Toplam	373	332	369	251	223	1548

Tablo 26'da kadın bireylere ilişkin frekans değerlerinin araştırma görevlisi unvanında yoğunlaştığı; erkek bireylere ilişkin en düşük frekans değerlerinin ise aynı unvanında olduğu görülmüştür. Ayrıca hem erkek hem kadın bireylere ilişkin frekans değerlerinin Dr. öğretim üyesi kadrosundaki yoğunluğu benzerlik göstermiştir.

**Tablo 27. Cinsiyet ve Akademik Unvan Ki-Kare Analizi**

	Değer	Serbestlik Derecesi	Asimptotik Anlamlılık (Çift taraflı)
Pearson Ki-Kare	52,341 <sup>a</sup>	4	,000
Geçerli Veri Sayısı	1548		

**Tablo 28. Cinsiyet ve Akademik Unvan Etki Boyutu**

		Değer	Yaklaşık Anlamlılık
Nominal by Nominal	Phi	,184	,000
	Cramer's V	,184	,000
Geçerli Veri Sayısı		1548	

Tablo 27'de sunulan Ki-Kare bağımsızlık testi, cinsiyet ve akademik unvan değişkenleri arasında anlamlı bir farklılık olduğunu göstermiştir,  $X^2(4, n = 1548) = 52.34, p = .000$ ,  $Cramer's V = .18$ . Bu durum Cohen (1988)'in skalasına göre cinsiyet ve akademik unvan değişkenleri arasındaki etkileşimin zayıf olduğu anlamına gelmektedir.

**Tablo 29. Cinsiyet ve İşte Bilgisayar Kullanma Saati Çapraz Tablosu**

Cinsiyet	İşte Bilgisayar Kullanma Saati (Günlük ortalama)			Toplam
	1-4	5-8	9<	
Erkek	276	456	46	778
Kadın	204	509	57	770
Toplam	480	965	103	1548

Tablo 29'da hem erkek hem kadın bireylere ilişkin frekans değerlerinin 5-8 saat aralığında yoğunlaştığı; en düşük frekans değerlerinin ise 9<saat aralığında olduğu görülmüştür.

**Tablo 30. Cinsiyet ve İşte Bilgisayar Kullanma Saati Ki-Kare Testi**

	Değer	Serbestlik Derecesi	Asimptotik Anlamlılık (çift taraflı)
Pearson Ki-Kare	14,845 <sup>a</sup>	2	,001
Geçerli Veri Sayısı	1548		

**Tablo 31. Cinsiyet ve İşte Bilgisayar Kullanma Saati Etki Boyutu**

		Değer	Yaklaşık Anlamlılık
Nominal by Nominal	Phi	,098	,001
	Cramer's V	,098	,001
Geçerli Veri Sayısı		1548	

Tablo 30'da sunulan Ki-Kare bağımsızlık testi, cinsiyet ve işte bilgisayar kullanma saati değişkenleri arasında anlamlı bir ilişki olduğunu göstermiştir,  $X^2(2, n=1548) = 14.85, p = .001$ , Cramer's  $V = .10$ . Bu durum Cohen (1988)'in skalasına göre cinsiyet ve işte bilgisayar kullanma saati değişkenleri arasındaki etkileşimin zayıf olduğu anlamına gelmektedir.

**Tablo 32. Yaş ve İşte Bilgisayar Kullanma Saati Çapraz Tablosu**

Yaş	İşte bilgisayar kullanma saati (günlük ortalama)			Toplam
	1-4	5-8	9<	
21-30	66	200	26	292
31-40	162	358	37	557
41-50	148	253	31	432
51-60	86	129	7	222
60<	18	25	2	45
Toplam	480	965	103	1548

Tablo 32'de tüm yaş gruplarındaki bireylere ilişkin frekans değerlerinin 5-8 saat aralığında yoğunlaştığı; en düşük frekans değerlerinin ise 9< saat aralığında olduğu görülmüştür.

**Tablo 33. Yaş ve İşte Bilgisayar Kullanma Saati Ki-Kare Testi**

	Değer	Serbestlik Derecesi	Asimptotik Anlamlılık (Çift taraflı)
Pearson Ki-Kare	25,126 <sup>a</sup>	8	,001
Geçerli Veri Sayısı	1548		

**Tablo 34. Yaş ve İşte Bilgisayar Kullanma Saati Etki Boyutu**

		Değer	Yaklaşık Anlamlılık
Nominal by Nominal	Phi	,127	,001
	Cramer's V	,090	,001
Geçerli Veri Sayısı		1548	

Tablo 33'de sunulan Ki-Kare bağımsızlık testi, yaş grubu ve işte bilgisayar kullanma saati değişkenleri arasında anlamlı bir ilişki olduğunu göstermiştir,  $X^2(8, n=1548) = 25.13, p = .001$ , Cramer's  $V = .09$ . Bu durum Cohen (1988)'in skalasına göre yaş ve işte bilgisayar kullanma saati değişkenleri arasındaki etkileşimin zayıf olduğu anlamına gelmektedir.

**Tablo 35. Üniversite Türü ve İşte Bilgisayar Kullanma Saati Çapraz Tablosu**

Üniversite Türü	İşte Bilgisayar Kullanma Saati (Günlük ortalama)			Toplam
	1-4	5-8	9<	
Devlet	445	855	90	1390
Vakıf	35	110	13	158
Toplam	480	965	103	1548

Tablo 35'de hem devlet hem vakıf üniversitesindeki bireylere ilişkin frekans değerlerinin 5-8 saat aralığında yoğunlaştığı; en düşük frekans değerlerinin ise 9< saat aralığında olduğu görülmüştür.

**Tablo 36. Üniversite Türü ve İşte Bilgisayar Kullanma Saati Ki-Kare Testi**

	Değer	Serbestlik Derecesi	Asimptotik Anlamlılık (Çift taraflı)
Pearson Ki-Kare	6,602 <sup>a</sup>	2	,037
Geçerli Veri Sayısı	1548		

**Tablo 37. Üniversite Türü ve İşte Bilgisayar Kullanma Saati Etki Boyutu**

		Değer	Yaklaşık Anlamlılık
Nominal by Nominal	Phi	,065	,037
	Cramer's V	,065	,037
Geçerli Veri Sayısı		1548	

Tablo 36'da sunulan Ki-Kare bağımsızlık testi, üniversite türü ile işte bilgisayar kullanma saati değişkenleri arasında anlamlı bir ilişki olduğunu göstermiştir,  $X^2(2, n=1548) = 6.60, p = .04$ , Cramer's  $V = .07$ . Bu durum Cohen (1988)'in skalasına göre üniversite türü ve işte bilgisayar kullanma saati değişkenleri arasındaki etkileşimin zayıf olduğu anlamına gelmektedir.

**Tablo 38. Meslekteki Toplam Çalışma Süresi ve İşte Bilgisayar Kullanma Saati Çapraz Tablosu**

Meslekteki toplam çalışma süresi (Yıl)	İşte Bilgisayar Kullanma Saati (Günlük ortalama)			Toplam
	1-4	5-8	9<	
<1	5	9	1	15
2-5	101	286	39	426
6-10	96	216	15	327
10<	278	454	48	780
<b>Toplam</b>	<b>480</b>	<b>965</b>	<b>103</b>	<b>1548</b>

Tablo 38'de tüm çalışma yıllarındaki bireylere ilişkin frekans değerlerinin 5-8 saat aralığında yoğunlaştığı; en düşük frekans değerlerinin ise 9< saat aralığında olduğu görülmüştür.

**Tablo 39. Meslekteki Toplam Çalışma Süresi ve İşte Bilgisayar Kullanma Saati Ki-Kare Testi**

	Değer	Serbestlik Derecesi	Asimptotik Anlamlılık (Çift taraflı)
Pearson Ki-Kare	23,878 <sup>a</sup>	6	,001
Geçerli Veri Sayısı	1548		

**Tablo 40. Meslekteki Toplam Çalışma Süresi ve İşte Bilgisayar Kullanma Saati Etki Boyutu**

		Değer	Yaklaşık Anlamlılık
Nominal by Nominal	Phi	,124	,001
	Cramer's V	,088	,001
Geçerli Veri Sayısı		1548	

Tablo 39'da sunulan Ki-Kare bağımsızlık testi, meslekteki toplam çalışma süresi ve işte bilgisayar kullanma saati değişkenleri arasında anlamlı bir ilişki olduğunu göstermiştir,  $X^2(6, n=1548) = 23.88, p = .001$ , Cramer's  $V = .09$ . Bu durum Cohen (1988)'in skalasına göre meslekteki toplam çalışma süresi ve işte bilgisayar kullanma saati değişkenleri arasındaki etkileşimin zayıf olduğu anlamına gelmektedir.

Ayrıca yürütülen analizler sonucunda akademik unvan ve işte bilgisayar kullanma saati değişkenleri arasında anlamlı bir ilişki bulunamadığından bulgular raporlamaya dahil edilmemiştir.

## 6. SONUÇ

Bilgi ve iletişim teknolojilerinin hızlı ve sürekli gelişimi ile birlikte bilgi güvenliğinin sağlanması ve sürdürülmesi giderek daha güç ve karmaşık bir hale dönüşmüştür. Bu çalışmada bilgi güvenliğinin sağlanmasında en önemli faktör olduğu düşünülen bilgi güvenliği farkındalığının kazandırılmasında etkin rol oynayan öğretim elemanlarının farkındalıkları incelenmiştir.

Bu çalışmada elde edilen verilerin analizi sonucunda öğretim elemanlarının bilgi güvenliği farkındalık seviyesinin Salem vd. (2021)'nin skalasına göre beş puan üzerinden değerlendirildiğinde orta düzeyde olduğu görülmüştür. Ancak güçlü parola kullanma, bilinmeyen gönderenlerden gelen e-postaların açılması, mobil cihazların fiziksel güvenliği, USB bellek kullanımı alt boyutlarının ortalamaları yüksek düzeyde gözlemlenirken aynı parolayı kullanma, parolayı paylaşma, tanıdık kişilerden gelen e-postalardaki bağlantıları açma, sosyal medya gizlilik ayarları, sosyal medyadaki paylaşımların sonuçlarını düşünme ve şüpheli davranışları raporlama alt boyutlarının ortalamaları düşük düzeyde gözlemlenmiştir. Bu çalışmanın bulguları Salem vd. (2021)'nin ve Avcı ve Oruç (2020)'un üniversite öğrencileri üzerinde yürüttükleri çalışmalar ile Kritzinger vd. (2022)'nin çeşitli sektörlerde çalışanlar üzerinde yürüttükleri çalışmanın bulguları ile örtüşmektedir. Ayrıca yürütülen Ki-Kare testleri sonucunda cinsiyet-yaş, cinsiyet-üniversite türü, cinsiyet-



akademik alan, cinsiyet-akademik unvan, cinsiyet-işte bilgisayar kullanma saati, yaş-işte bilgisayar kullanma saati, üniversite türü-işte bilgisayar kullanma saati ve meslekte toplam çalışma süresi-işte bilgisayar kullanma saati değişkenleri arasında anlamlı, ancak zayıf bir ilişki olduğu görülmüştür. Hem erkek hem kadın katılımcıların frekans değerlerinin 31-40 yaş aralığında, devlet üniversitesinde, sosyal bilimler alanında yoğunlaştığı; Dr. öğretim üyesi kadrosundaki yoğunluklarının da benzerlik gösterdiği dikkat çekmiştir. Yine hem devlet hem vakıf üniversitelerinde, tüm yaş gruplarında, tüm çalışma yıllarında yer alan katılımcıların ve hem erkek hem kadın katılımcıların bilgisayar kullanma sürelerinin ortalama 5-8 saat aralığında yoğunlaştığı görülmüştür. Bu yoğunlaşma, akademisyenlerin görev rolleri ve yükleri göz önünde bulundurulduğunda bilgisayar kullanımlarının mesai saatleri ve işyeri ile sınırlı kalmadığı şeklinde yorumlanabilir.

Araştırma elektronik anket uygulaması ile ulaşılan Türkiye'deki yükseköğretim kurumlarında görevli öğretim elemanları ile sınırlıdır. Bazı katılımcıların geri bildirimleri doğrultusunda gönderilen elektronik anketin spam kutusuna düştüğünün öğrenilmesi, iş yoğunluğu ve bilimsel etkinlikler nedeniyle elektronik anketin e-posta sıralamasında gerilere düşmesi kısıtlardan bazılarıdır.

Mevcut araştırma evren ve örneklemini oluşturan yükseköğretim çalışanlarının bilgi güvenliği farkındalığı seviyesinin tespitinin ardından kurum ve kuruluşların bilgi güvenliği politikaları doğrultusunda farkındalık düzeyinin ve davranış biçimlerinin istenilen biçimde geliştirilmesine yönelik olarak gerekli eğitimler planlanarak ve uygulanarak istenilen sonuçlara ulaşılabilir. Benzer şekilde farklı sektör ve faaliyet alanında örgütler ve çalışanlar üzerinde benzer araştırmalar yapılarak kişilerin bilgi güvenliği farkındalıkları aracılığıyla kurumların bilgi güvenliği politikaları geliştirilebilecektir. Benzer araştırmalar farklı meslek grupları ve bilgisayar kullanıcıları profilleri üzerinde gerçekleştirilerek toplumun genel anlamda bilgi ve internet güvenliğine ilişkin farkındalık düzeyi ve davranış biçimlerini ortaya koyarak bilgi toplumunun en önemli altyapılarından biri olan internetin daha güvenli bir ortam olmasına katkı sağlayabilecektir.

**KAYNAKÇA**

- Ahlan, A. R., Lubis, M., & Lubis, A. R. (2015). Information security awareness at the knowledge-based institution: its antecedents and measures. *Procedia Computer Science*, 72(2015), 361-373. <https://doi.org/10.1016/j.procs.2015.12.151>
- Arisya, K. F., Ruldeviyani, Y., Prakoso, R., & Fadhilah, A. L. (2020, November 3-4). *Measurement of information security awareness level: A case study of mobile banking (m-banking) users*. [Conference presentation]. In 2020 Fifth International Conference On Informatics And Computing (Icic), Gorontalo, Indonesia.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 34(3), 523-548. <https://doi.org/10.2307/25750690>
- Chase, J. L. (2021). *Examining the effect of organizational Culture on End-User Attitude Towards Information Security Awareness* [Doctoral dissertation]. Colorado Technical University.
- Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Hillsdale, NJ: Erlbaum
- Çelik Çöp, Ç. (2017). *Kalite Yönetim Direktörlerinin Bilgi Güvenliği Farkındalığı: İstanbul İli Örneği*. [Doktora Tezi]. Okan Üniversitesi Sağlık Bilimleri Fakültesi.
- Çıfci, H. (2013). *Her Yönüyle Siber Savaş*. TÜBİTAK Popüler Bilim Kitapları.
- Dharmawansa, A. D., & Madhuwanthi, R. A. M. (2020, October 15-16). *Evaluating the Information Security Awareness (ISA) of employees in the banking sector: A case study* [Conference presentation]. General Sir John Kotelawala Defence University Ratmalana, Sri Lanka.
- Ecek, N., & Çakmak, A. F. (2022). Çalışanların Bilgi Güvenliği Önlemlerine Dair Tutumları: Ampirik Bir Değerlendirme. *International Journal of Applied Economic and Finance Studies*, 7 (2), 26-44.
- Eminağaoğlu, M., & Gökşen, Y. (2009). Bilgi Güvenliği Nedir, Ne Değildir, Türkiye'de Bilgi Güvenliği Sorunları ve Çözüm Önerileri. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 11(4), 1-15.
- Fianty, M. I. (2023). The impact of employees' information security awareness on information security behaviour. *International Journal of Information System and Technology*, 6(5), 629-636.
- Fisher, M. J. & Marshall, A. P. (2009). Understanding descriptive statistics. *Australian critical care*, 22(2), 93-97.
- George D, & Mallery P. (2003). *SPSS for Windows step by step: A simple guide and reference. 11.0 update* (4th ed.). Allyn & Bacon.
- Grassegger, T., & Nedbal, D. (2021). The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering. *Procedia Computer Science*, 181(2021), 59-66. DOI:10.1016/j.procs.2021.01.103
- Fujs, D., Vrhovec, S., & Vavpotič, D. (2021, November). *Know Your Enemy: User Segmentation Based on Human Aspects of Information Security* [Conference presentation]. Access, 9(2021), 157306-157315. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9623526>
- Hadlington, L., & Parsons, K. (2017). Can cyberloafing and Internet addiction affect organizational information security?. *Cyberpsychology, Behavior, and Social Networking*, 20(9), 567-571. DOI: 10.1089/cyber.2017.0239
- Hadlington, L., Popovac, M., Janicke, H., Yevseyeva, I., & Jones, K. (2019). Exploring the role of work identity and work locus of control in information security awareness. *Computers & Security*, 81, 41-48. <https://doi.org/10.1016/j.cose.2018.10.006>
- Hadlington, L., & Chivers, S. (2020). Segmentation analysis of susceptibility to cybercrime: Exploring individual differences in information security awareness and personality factors. *Policing: A Journal of Policy and Practice*, 14(2), 479-492. <https://doi.org/10.1093/police/pay027>

- Hadlington, L., Binder, J., & Stanulewicz, N. (2020). Fear of missing out predicts employee information security awareness above personality traits, age, and gender. *Cyberpsychology, Behavior, and Social Networking*, 23(7), 459-464. DOI: [10.1089/cyber.2019.0703](https://doi.org/10.1089/cyber.2019.0703)
- Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. *Computers & Security*, 95, 101827. DOI:[10.1016/j.cose.2020.101827](https://doi.org/10.1016/j.cose.2020.101827)
- Herbert, F., Farke, F. M., Kowalewski, M., & Dürmuth, M. (2021, October 11-12). *Vision: Developing a Broad Usable Security & Privacy Questionnaire* [Conference presentation]. In Proceedings of the 2021 European Symposium on Usable Security. Karlsruhe, Germany.
- Kapanoğlu, G. (2016). *Öğretmenlerin Bilgi Güvenliği Farkındalığının İncelenmesi*. [Yüksek lisans tezi]. Gazi Üniversitesi Eğitim Bilimleri Enstitüsü.
- Karagöz, Y. (2019). *SPSS AMOS META Uygulamalı Nitel-Nitel-Karma Bilimsel Araştırma Yöntemleri ve Yayın Etiği*. Nobel Yayıncılık.
- Kritzinger, E., Da Veiga, A., & van Staden, W. (2022). Measuring organizational information security awareness in South Africa. *Information Security Journal: A Global Perspective*, 32(2), 120-133. <https://doi.org/10.1080/19393555.2022.2077265>
- Krutz, R. L., Vines, R. D., & Stroz, E. M. (2001). *The CISSP Prep Guide: Mastering the ten domains of computer security*. John Wiley & Sons, Inc.
- Lionel, B. (2020). *Examining the Relationship between Cybersecurity-Employee Vulnerabilities and Reduction of Security Breaches in Information Technology Organization* [Doctoral dissertation]. Colorado Technical University.
- Mahardika, M. S., Hidayanto, A. N., Paramartha, P. A., Ompusunggu, L. D., Mahdalina, R., & Affan, F. (2020). Measurement of employee awareness levels for information security at the center of analysis and information services judicial commission Republic of Indonesia. *Adv. Sci. Technol. Eng. Syst*, 5(3), 501-509. DOI:[10.25046/aj050362](https://doi.org/10.25046/aj050362)
- McCormac, A., Calic, D., Parsons, K., Zwaans, T., Butavicius, M., & Pattinson, M. (2016). *Test-retest reliability and internal consistency of the Human Aspects of Information Security Questionnaire (HAIS-Q)* [Conference Presentation]. Australasian Conference on Information Systems, Wollongong.
- McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, 69, 151-156. <https://doi.org/10.1016/j.chb.2016.11.065>
- Murphy, S. (2022). *A Quantitative Study Using the Protection Motivation Theory to Examine Information Protection Awareness in a Healthcare Organization* [Doctoral dissertation] Northcentral University.
- Okenyi, P. O., & Owens, T. J. (2007). On the anatomy of human hacking. *Information Systems Security*, 16(6), 302-314. <https://doi.org/10.1080/10658980701747237>
- Ögütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, 56, 83-93. <https://doi.org/10.1016/j.cose.2015.10.002>
- Pallant, J. (2020). *Survival Manual A Step by Step Guide to Data Analysis Using IBM SPSS* (7th Edition). Routledge Taylor&Francis Group.
- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & security*, 42, 165-176. DOI:[10.1016/j.cose.2013.12.003](https://doi.org/10.1016/j.cose.2013.12.003)
- Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2017). Managing information security awareness at an Australian bank: A comparative study. *Information & Computer Security*, 25(2), 181-189. DOI: [10.1108/ICS-03-2017-0017](https://doi.org/10.1108/ICS-03-2017-0017)
- 
- Pattinson, M., Butavicius, M., Lillie, M., Ciccarello, B., Parsons, K., Calic, D., & McCormac, A. (2019). Matching training to individual learning styles improves information security awareness. *Information & Computer Security*, 28(1), 1-14. DOI:[10.1108/ICS-01-2019-0022](https://doi.org/10.1108/ICS-01-2019-0022)

- Rao, U. H., & Nayak, U. (2014). *The Infosec Handbook: An Introduction to Information Security*. Friendsoft Apress. Nisan 20, 2022 tarihinde <https://library.oapen.org/bitstream/handle/20.500.12657/28165/1001829.pdf?sequence=1> adresinden alındı.
- Reeves, A., Parsons, K., & Calic, D. (2017, November). *Securing mobile devices: evaluating the relationship between risk perception, organisational commitment and information security awareness* [Conference presentation]. Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017), Adelaide, South Australia.
- Romansky, R. P., & Noninska, I. S. (2020). Challenges of the Digital Age for Privacy and Personal Data Protection. *Mathematical Biosciences and Engineering*, 17(5), 5288-5303. doi: [10.3934/mbe.2020286](https://doi.org/10.3934/mbe.2020286)
- Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, 53(2015), 65-78. <http://dx.doi.org/10.1016/j.cose.2015.05.012>
- Safa, N. S., Von Solms, R., & Futcher, L. (2016). Human aspects of information security in organisations. *Computer Fraud & Security*, 2016(2), 15-18. DOI:[10.1016/S1361-3723\(16\)30017-3](https://doi.org/10.1016/S1361-3723(16)30017-3)
- Salem, Y., Moreb, M., & Rabayah, K. S. (2021, July 14-15). *Evaluation of Information Security Awareness among Palestinian Learners* [Conference presentation]. In 2021 International Conference on Information Technology (ICIT), Amman, Jordan.
- Sekaran. U. (2003). *Research methods for business: A skill building approach* (Fourth Edition). John Wiley & Sons Inc.
- Sturman, D., Valenzuela, C., Plate, O., Tanvir, T., Auton, J. C., Bayl-Smith, P., & Wiggins, M. W. (2023). The role of cue utilization in the detection of phishing emails. *Applied Ergonomics*, 106(2023), 1-13. <https://doi.org/10.1016/j.apergo.2022.103887>
- Teker, E. (2019). *Öğretmenlerin ve Lise Öğrencilerinin Bilgi Güvenliği Farkındalık Düzeylerinin Değerlendirilmesi* [Yüksek lisans tezi]. Ankara Üniversitesi Eğitim Bilimleri Enstitüsü.
- Veseli, I. (2011). *Measuring the effectiveness of information security awareness program* [Master's dissertation]. Gjovik University College.
- Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & security*, 23(3), 191-198. <https://doi.org/10.1016/j.cose.2004.01.012>
- Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security*, 88(2020), 1-8. <https://doi.org/10.1016/j.cose.2019.101640>
- Witsenboer, J. W. A., Sijtsma, K., & Scheele, F. (2022). Measuring cyber secure behavior of elementary and high school students in the Netherlands. *Computers & Education*, 186(2022), 1-11. <https://doi.org/10.1016/j.compedu.2022.104536>
- Zulfia, A., Adawiyah, R., Hidayanto, A. N., & Budi, N. F. A. (2019, April 11-13). *Measurement of employee information security awareness using the human aspects of information security questionnaire (HAIS-Q): Case study at PT. PQS* [Conference presentation]. In 2019 5th International Conference on Computing Engineering and Design (ICCED), Singapore.

## **ÇALIŞMANIN ETİK İZİNİ**

“Yapılan bu çalışmada “Yükseköğretim Kurumları Bilimsel Araştırma ve Yayın Etiği Yönergesi” kapsamında uyulması belirtilen tüm kurallara uyulmuştur. Yönergenin ikinci bölümü olan “Bilimsel Araştırma ve Yayın Etiğine Aykırı Eylemler” başlığı altında belirtilen eylemlerden hiçbiri gerçekleştirilmemiştir.”

### **Etik kurul izin bilgileri**

Etik değerlendirmeyi yapan kurul adı: Zonguldak Bülent Ecevit Üniversitesi İnsan Araştırmaları Etik Kurulu  
Etik değerlendirme kararının tarihi: 29.09.2022

Etik değerlendirme belgesi sayı numarası: 29.09.2022/219198

## **ARAŞTIRMACILARIN KATKI ORANI**

Bu çalışmada yazarların katkıları eşit düzeydedir.

## **ÇATIŞMA BEYANI**

“Araştırmada herhangi bir kişi ya da kurum ile finansal ya da kişisel yönden bağlantı bulunmamaktadır. Araştırmada herhangi bir çıkar çatışması bulunmamaktadır.”

## EXTENDED SUMMARY

Currently, providing and maintaining information security has become increasingly difficult and complex. Information security awareness plays a vital role in this process. Psychological factors, insensitivity, mistakes, and intentional or unintentional behaviors of individuals can lead to security vulnerabilities (Bulgurcu et al., 2010; Gelişken, 2009; Parsons et al., 2014). Research shows that 80% of security incidents are caused by people within an organization (Rao and Nayak, 2014), highlighting the importance of employees in preventing or detecting such incidents (Ng et al., 2009).

Universities, as extensive users of information technologies, have a significant role in raising information security awareness among young individuals and improving their current knowledge (Akgün & Topal, 2015). Conducting a study on this subject within educational institutions, which serve as information production centers and handle a substantial amount of confidential data (Katz, 2005), can yield valuable insights. Therefore, the main objective of this research is to empirically analyze the information security awareness levels of tertiary educators at different levels and present the research findings, along with exploratory analyses based on existing literature. Assessing the awareness of tertiary educators and identifying areas with low awareness can be beneficial for reorganizing security policies and addressing potential security issues. Additionally, this study aims to contribute to the existing literature by presenting detailed findings on the awareness of tertiary educators, allowing for meaningful comparisons with theoretical studies on the subject.

The research population for this study consists of tertiary educators in higher education institutions in Turkey. The study encompassed the entire research population without employing sampling techniques. A sample size of 1548 tertiary educators, representative of the research population, was included in the study. The researchers adapted and administered the scale developed by Parsons et al. (2017) to tertiary educators using a 5-point Likert scale. The scale comprises seven sub-dimensions: password management, email use, internet use, social media use, mobile devices, information handling, and event reporting.

The collected data underwent descriptive statistical analyses and Chi-square tests using the IBM SPSS package program. The results indicated that the awareness level of tertiary educators was moderate overall. However, certain sub-dimensions, such as using strong passwords, handling emails from unknown senders, ensuring the physical security of mobile devices, and utilizing USB memory, exhibited high levels of awareness. Conversely, sub-dimensions like using the same password, sharing passwords, clicking on links in emails from known senders, configuring social media privacy settings, considering the consequences of sharing information, and reporting suspicious behaviors demonstrated lower levels of awareness.

Furthermore, the Chi-Square tests revealed significant findings regarding the relationships between gender and age, gender and university type, gender and academic field, gender and hours of computer use at work, age and hours of computer use at work, total working time in the profession, and hours of computer use at work. Both male and female participants were predominantly concentrated in the 31-40 age range, enrolled in state universities, and affiliated with social sciences. Additionally, it was observed that both male and female participants, across all age groups and working years, from both state and foundation universities, had an average computer usage time of 5-8 hours. This concentration suggests that computer usage extends beyond working hours and the workplace, taking into account the academic responsibilities and workload of educators.

Conducting similar research across various sectors and occupational groups will aid in developing information security policies that account for individuals' awareness levels. Additionally, conducting studies on different professional groups and computer user profiles to determine societal awareness levels and behavioral patterns concerning information and internet security will contribute to establishing a safer online environment—an essential infrastructure for the information society.