

Bilgi Güvenliđi Farkındalıđı Üzerine Üniversite Öğrencilerine Yönelik Araştırma

Nurdan DEĞİRMENCİ *

Dilek GÖNÇER DEMİRAL **

Öz

Bu çalışma Recep Tayyip Erdoğan Üniversitesinde öğrenim gören öğrencilerin bilişim güvenliđi farkındalıklarını incelemek amacıyla gerçekleştirilmiştir. Çalışma 2021-2022 eğitim öğretim yılında Rize ilinde yer alan Recep Tayyip Erdoğan Üniversitesi Fındıklı Uygulamalı Bilimler Yüksekokulu ve Sosyal Bilimler Meslek Yüksekokulu öğrencilerini kapsamaktadır. Araştırmanın çalışma grubunu 345 öğrenci oluşturmaktadır. Araştırmada elde edilen veriler SPSS 23 paket programı kullanılarak analiz edilmiştir. Analiz sonuçları incelendiğinde, cinsiyete, öğrencilerin ait oldukları sınıflara ve bölümlere göre bilişim güvenliđi farkındalıđının farklılık gösterdiđi ortaya koyulmuştur.

Anahtar Kelimeler: Bilgi Güvenliđi, Bilgi Güvenliđi Farkındalıđı, Bilgi Teknolojisi

Research on Information Security Awareness Among University Students

Abstract

This study was conducted to examine the awareness of information security among students studying at Recep Tayyip Erdogan University. The study included students from Recep Tayyip Erdogan University, Fındıklı School of Applied Sciences and Vocational School of Social Sciences in Rize province during the 2021-2022 academic year. The research group was comprised of 345 students. The data obtained in this study were analyzed using the SPSS 23 software package. The analysis results revealed that the awareness of information security varied according to gender, the classes students belonged to, and the programmes they were enrolled in.

Keywords: Information Security, Information Security Awareness, Information Technology

Geliş/Received: 21.08.2023

Kabul/Accepted: 31.10. 2023

Etik Kurul Beyanı: Bu çalışma için Recep Tayyip Erdoğan Üniversitesi Sosyal ve Beşeri Bilimler Etik Kurulu'ndan (2022/141 sayılı toplantı kararınca 07-06-2022 tarihinde) etik kurul onayı alınmıştır.

* Doç. Dr., Recep Tayyip Erdoğan Üniversitesi, Fındıklı Uygulamalı Bilimler Yüksekokulu, Uluslararası Ticaret Ve Lojistik Bölümü, nurdan.degirmenci@erdogan.edu.tr, ORCID: 0000-0002-8759-8871

** Dr. Öğretim Üyesi, Recep Tayyip Erdoğan Üniversitesi, Sosyal Bilimler Meslek Yüksekokulu, Dış Ticaret Bölümü, dilek.goncerdemiral@erdogan.edu.tr, ORCID: 0000-0001-7400-1899

(Makale Türü: Araştırma Makalesi)

Giriş

Son yıllarda bilişim teknolojilerindeki hızlı gelişmeler modern toplumun vazgeçilmez bir parçası olmuştur. Teknolojik araçların sürekli gelişiminin yanı sıra, kullanımındaki düşük maliyetler, teknolojiyi herkes tarafından tercih edilir hale getirmiştir. Hem işletmeler açısından hem de son kullanıcılar için, birçok iş sürecinde dijital araçlardan yoğun bir şekilde faydalanmak, aynı zamanda bu araçların kullanımını da zorunlu kılmıştır. Özellikle, 1990'lı yılların sonunda “internet çağı”nın başlaması, büyük dönüşümlere de sebep olmuştur. İnternet kullanımının günden güne artması bilgiye kolayca erişimi sağladığı gibi, tüm işlemlerin de en hızlı ve ekonomik yoldan tamamlanmasını gerçekleştirmektedir.

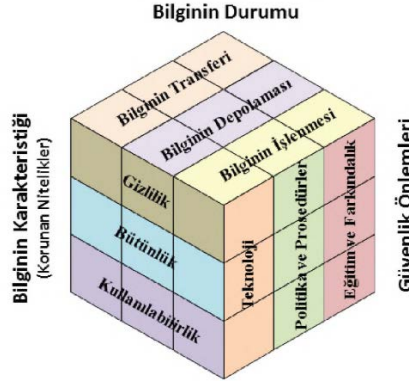
Uluslararası Telekomünikasyon Birliği tarafından yayınlanan rapora göre; 2022 yılında yaklaşık 5.3 milyar insanın ve dünya nüfusunun yaklaşık %66'sının internet kullandığı tahmin edilmektedir. 2019 yılından bu yana %24'lük bir artışla birlikte, tahminen 1,1 milyar insanın çevrimiçi olduğu belirtilmektedir. TÜİK verilerine göre, 16-74 yaş grubundaki bireylerde, 2021 yılında internet kullanım oranı %82,6 iken 2022 yılında %85,0 olmuştur (TÜİK, 2022). Tüm bu veriler ışığında internet kullanımının daha hızla artacağı öngörülebilir.

İnternet kullanımının vazgeçilmez olmasıyla birlikte bilgi güvenliği kavramı da ön plandadır. Birçoğumuz internet kullanırken, bazı web sitelerine üye olma zorunluluğu ile karşılaşmaktadır. İşlemleri tamamlayabilmek adına, kişisel bilgilerin paylaşılmasına zaman zaman izin verilmektedir. Yasal sınırlar içerisinde toplanan ve verilerimizi değerli bir varlık olarak gören işletmeler, kendi pazarlama stratejileri için bu verileri kullanmaktadırlar. Kullanıcıların bilgisi dışında toplanan veriler ise bilgi güvenliği açısından çok büyük riskler doğurabilmektedir.

Bilgi, sahibi ve hedef kullanıcıları için onu değerli kılan bazı özelliklere sahiptir. Buna göre, McCumber (1991:329) bilginin gizliliğini, bütünlüğünü ve kullanılabilirliğini bilginin karakteristik özellikleri olarak nitelendirmiştir. Gizlilik, bilginin yetkisiz kişilerin eline geçmemesi veya geçmesinin engellenmesidir. Kişisel bilgilerin ve bireysel hakların korunması gizliliğin en kapsamlı konularıdır. Bütünlük; bilginin yetkisiz kişiler tarafından değiştirilmemiş olmasıdır. Henkoğlu ve Yılmaz (2013: 455)'a göre, bilgi bütünlüğünün korunması, bilginin değeri açısından da oldukça önemlidir. Kullanılabilirlik ise bilginin yetkili kişilerce ulaşılabilir ve kullanılabilir durumda olmasıdır. Bilgi güvenliği bileşenleri de bu üç temel özellik üzerinden değerlendirilebilir. McCumber (2005), bilgi güvenliğini, bilgi ve bilgi sistemlerine yetkisiz erişim, bilginin kullanımı, ifşa edilmesi, bozulması, değiştirilmesi veya bilginin gizlilik, bütünlük ve kullanılabilirliğine zarar vermek için yapılan kötü niyetli girişimlere karşı

sağlanacak koruma olarak tanımlamıştır. Kısaca, bilginin kullanım hakkı kimde ise, o kişi dışında kullanımı durumunda bilgi güvenliğinden söz edilemez.

Şekil 1’de belirtilen McCumber’in geliştirmiş olduğu bilgi güvenliği modeli, uygulanabilirliği olan en güncel ve en temel yaklaşımdır. Bilgi güvenliğinden söz edebilmek için, gizlilik, bütünlük ve kullanılabilirlik birbirini tamamlamalı ve ayrılmaz bir bütün olmalıdır. Aksi durumda güvenlik açıklarının oluşması kaçınılmazdır.



Şekil 1. Bilgi Güvenliği Modeli
(McCumber, 1991: 334)

Kötü niyetli bilgisayar kullanıcıları, insanların bilgi sistemlerine karşı olan davranışları hakkında bilinçli uzman kişilerdir. Kullanıcıların hangi alanlarda hata yapabileceğini ve zayıf olduklarını çok iyi bilirler. Bu zafiyetten de faydalanmak isterler. Aloul (2010:2) 'a göre, saldırganlar genellikle, siyasi bir mesaj yaymak, finansal bir kazanç elde etmek, kişilerin bilgilerini çalıp farklı alanlarda kullanmak ve tüm bunların sonucunda kişileri zarara uğratmak veya kişisel tatmin elde etmek için motive olurlar. Bu nedenlerden dolayı, son kullanıcıların tehditlerden, saldırılardan ve risklerden haberdar ve bilinçli olması, yapılan tüm teknolojik yatırımlardan çok daha önemlidir ki araştırmalar da kullanıcı davranışlarıyla bilgi güvenliği arasında bir ilişki olduğunu söylemektedir (Crossler vd.,2013: 94; Öğütücü vd.,2016: 83; Şen, 2020: 51; Kruger vd.,2010: 317).

Dünya çapında bilgi güvenliği problemlerinin temel nedenleri arasında; internet kullanımının ve dolayısıyla elektronik verilerin artması, mobil cihaz kullanım oranlarının yükselmesi, organize siber suç gruplarındaki artış, saldırganların artması ve çeşitlenmesi ve onları takip etmenin zorluğu kullanıcıların bu konudaki yetersizlikleridir. Özellikle işletmeler, bilgi güvenliği sağlamada yüksek maliyetli ve teknoloji tabanlı güvenlik mekanizmaları kullanırlar. Fakat araştırmalar göstermektedir ki bilgi güvenliğindeki en zayıf halka halen daha kullanıcılardır (Parsons vd., 2017: 40; Arce, 2003: 72; Abawajy, 2014: 240; Zhang vd., 2009: 330).

Çalışmanın amacı, kullanıcılar grubundaki üniversite öğrencilerinin bilgi güvenliği düzeylerini ortaya çıkarmaktır. Bu amaçla çalışmada öncelikle literatüre yer verilmiş, sonrasında Recep Tayyip Erdoğan Üniversitesi(RTEÜ) öğrencilerinin bilgi güvenliğine yönelik anket çalışması yapılmıştır.

Literatür

Bilgi güvenliği; bilgilerin korunmasına yönelik teknik, davranışsal, yönetsel ve organizasyonel yaklaşımları içeren geniş kapsamlı araştırmaları içermektedir. Bu anlamda literatürde bilgi farkındalığına yönelik birçok araştırma yapılmıştır. Özellikle bilgi güvenliğinin eğitim kurumlarındaki öneminin artmasıyla birlikte öğrenciler üzerindeki çalışmalar dikkat çekmektedir.

Albayrak ve Bağcı (2022) öğrencilerin kişisel özelliklerinin bilgi güvenliği farkındalığı üzerine etkisini araştırmışlardır. Araştırma sonucunda, sınıf ve cinsiyetin bilgi güvenliği farkındalığına doğrudan etkisi olmadığı sonucuna erişmişlerdir. Kritzingler, Veiga ve Staden (2022) bilgi güvenliği farkındalık düzeyini ölçmüşlerdir. Kurumlardaki farkındalığı artırmaya yönelik çeşitli önerilerde bulunmuşlardır. Zwilling vd.(2022) araştırmalarında internet kullanıcılarının yeterli siber tehdit farkındalığına sahip olduğunu ortaya koymuşlardır. Taha ve Dahabiyeh (2021), üniversite öğrencilerinin bazı bilgi güvenliği konularında bilinçli oldukları sonucuna erişmişlerdir. Emmungil ve Uzun (2021) sağlık alanındaki öğrencilerin bilişim güvenliği farkındalıklarının diğer bölümlere göre daha düşük olduğunu tespit etmişlerdir. Moletsane ve Tsibolane (2020) öğrencilerin mobil güvenlik davranışının, güvenlik tehditleri hakkındaki bilgilerden etkilendiği sonucuna ulaşmışlardır. Garba vd.(2020) araştırmalarında öğrencilerin temel siber güvenlik bilgisinde eksik oldukları sonucuna ulaşmışlardır. Avcı ve Oruç (2020), üniversite öğrencilerinin bilgi güvenliği ile ilgili eğitim almadıkları sonucuna erişmişlerdir. Kara ve Topaloğlu (2019), birçok öğrencinin bilgi güvenliği hakkında düşük seviyede bilgileri olduğunu tespit etmişlerdir. McCormac vd.(2017), bireysel farklılıklar ile bilgi güvenliği farkındalığı arasındaki ilişkiyi incelemişlerdir ve yaş ve cinsiyetin bilgi güvenliğinde anlamlı bir farklılığın olmadığını vurgulamışlardır. Öğütçü vd.(2016), kullanıcıların bilgi güvenliğini tehdit edebilecek davranışlarını ve kullanmış oldukları önleyici faaliyetler ile maruz kaldıkları tehditleri incelemişlerdir. Akgün ve Topal (2015), üniversite öğrencilerinin yeterli düzeyde bilişim farkındalıklarının olmadığını tespit etmişlerdir. Farooq vd.(2015), üniversite öğrencilerinin bilgi güvenlik düzeylerini ve bireysel faktörlerin bilgi güvenliğine olan etkisini araştırmışlardır. Erkeklerin bilgi güvenliği konusunda kız öğrencilere göre daha yetkin oldukları ortaya çıkmıştır. Tekerek ve Tekerek (2013), ilköğretim ve lise öğrencilerinin bilişim etiği konusunda yeterli düzeyde olmalarına rağmen, bilgi ve bilgisayar güvenliği farkındalığı

konularında yetersiz oldukları sonuçlarına erişmişlerdir. Bulgurcu vd.(2010), organizasyon içerisindeki çalışanların bilgi güvenliği farkındalığını değerlendirmişlerdir. Bilgi güvenliği farkındalığının organizasyon uyumu ile doğrudan önemli bir etkisi olduğunu bulmuşlardır.

Literatürde öğrenciler üzerinde bilgi güvenliği farkındalığı ile ilgili yapılan araştırmalarda, bilgi güvenliği hakkında yetersiz bilgiye sahip oldukları, farkındalık düzeylerinin düşük olduğu ve bu konuda eğitim almadıkları görülmektedir.

Yöntem

Bu çalışma 2021-2022 eğitim öğretim yılında, RTEÜ Fındıklı Uygulamalı Bilimler Yüksekokulu ve Sosyal Bilimler Meslek Yüksekokulunda öğrenim gören öğrencilerin bilişim güvenliği farkındalıklarını incelenmek üzere yapılmıştır.

Araştırmanın çalışma grubunu 345 öğrenci oluşturmaktadır. Araştırmanın sınırlılıkları, araştırma yapılan çalışma grubu ile sınırlı olmasıdır. Araştırma çevrimiçi ortamda ulaşılabilen katılımcılar ile sınırlandırılmıştır. Anketteki sorular araştırmanın bir diğer sınırlılığını oluşturmuştur.

Anket, RTEÜ Sosyal ve Beşeri Bilimler Etik Kurulu tarafından 2022/141 sayılı toplantı kararınca 07-06-2022 tarihinde etik kurul onayı alındıktan sonra uygulanmıştır.

Araştırmada Akgün & Topal (2015)'in geliştirdikleri anket kullanılmış olup, veriler basit tesadüfi örnekleme yöntemi ile elde edilmiştir. Ankette yapılandırılmış soru türleri kullanılmıştır. 4 soru demografik özelliklerle ilgili olmak üzere, 1 soru kapalı uçlu (Evet/Hayır), 44 soru 5'li Likert (1-Kesinlikle katılıyorum, 2-Katılıyorum, 3-Kararsızım, 4-Katılmıyorum, 5-Kesinlikle Katılmıyorum) ölçeğine dayalı ve 4 soru da açık uçludur.

Çalışmanın güvenilirliğini belirlemek için Cronbach Alpha iç tutarlılık katsayısı hesaplanmış ve 0.889 olarak bulunmuştur¹. Maddelerden herhangi biri atıldığında Alfa değeri yükselmektedir. Bu bulgu anketin güvenilirliğinin iyi düzeyde olduğunu göstermektedir.

Tablo 1. Güvenilirlik Katsayısı

<i>Cronbach's Alpha</i>	<i>N</i>
0,889	44

Çalışmada öncelikle araştırmaya katılan 345 öğrencinin demografik özelliklerine ilişkin frekans dağılımı yapılmıştır. Yöntem olarak bağımsız gruplar t-testi ve ANOVA kullanılmıştır.

¹Akgün ve Topal (2015)'in çalışmasında likert tipi 48 maddenin güvenilirliği için Cronbach Alfa iç tutarlık katsayısı 0.87 bulunmuştur.

Bağımsız 2 grubun birbirlerinden farklı olup olmadıklarını araştırmak için grup varyanslarının homojen olup olmadıklarına bağlı olarak t testi veya Mann-Whitney-U testi kullanılabilir. Normallik varsayımının geçerli sağlanıyor olması koşulu altında bu yöntemlerden hangisinin uygun olduğunu belirlemek için öncelikle varyansların homojenlikleri Levene testi ile incelenmektedir.

H_0 : Her iki grubun ilgili değişken için ortalama değerleri eşittir.

H_1 : Her iki grubun ilgili değişken için ortalama değerleri eşit değildir.

Bağımsız grupların sayısı ikiden fazla olduğunda bu grupların birbirlerinden farklı olup olmadıklarını araştırmak için ANOVA veya Kruskal Wallis analizi kullanılmaktadır. Normallik varsayımının geçerli olduğu durumda grup varyansları homojen değilse uygun olan yöntem Kruskal Wallistir. Bu nedenle öncelikle varyansların homojen olup olmadıkları Levene testi ile kontrol edilmektedir.

H_0 : Grup ortalamaları arasında ilgili değişken açısından farklılık yoktur.

H_1 : En azından bir grubun ilgili değişken açısından ortalama değeri diğerlerinden farklıdır.

ANOVA sonucunda istatistiksel bir fark bulunduğunda, bunun hangi gruplardan kaynaklandığı Post-Hoc testleri ile belirlenir. Bu çalışmada farklılığın hangi gruplardan kaynaklandığını bulmak için LSD testi kullanılmıştır.

Çalışmada çok fazla tablo gösterilemeyeceğinden sadece istatistiki olarak anlamlı bulunan ($P \leq 0,05$) sonuçlara yer verilmiştir.

Bulgular

Demografik dağılımlar Tablo 2’de gösterilmiştir. Araştırmaya %59,1 kız, %40,9 erkek öğrenci katılmış olup, %84,9’u 1. ve 2. Sınıf öğrencileridir.

Tablo 2. Demografik Özellikler

	Değişkenler	Sayı	Yüzde
Cinsiyet	<i>Kız</i>	204	59,1
	<i>Erkek</i>	141	40,9
Sınıf	<i>1</i>	130	37,7
	<i>2</i>	163	47,2
	<i>3</i>	37	10,7
	<i>4</i>	15	4,3
Bölüm	<i>Büro Yönetimi ve Yönetici Asistanlığı(BYY)</i>	46	13,3
	<i>Dış Ticaret(DT)</i>	40	11,6
	<i>Muhasebe ve Vergi Uygulamaları(MVU)</i>	25	7,2
	<i>Lojistik(L)</i>	65	18,8
	<i>İşletme Yönetimi(İY)</i>	25	7,2
	<i>Halkla İlişkiler ve Tanıtım(HİT)</i>	33	9,6

	<i>Sivil Hava Ulaştırma İşletmeciliği (SHUİ)</i>	11	3,2
	<i>Uluslararası Ticaret ve Lojistik (UTL)</i>	48	13,9
	<i>Finans ve Bankacılık (FB)</i>	52	15,1
Kendime ait bir bilgisayarım var	<i>Evet</i>	215	62,3
	<i>Hayır</i>	130	37,7

Tablo 3'e göre öğrencilerin %34,2' si bilişim güvenliği konusunda yeterli bilgiye sahip olduğunu düşünürken, %2'si bu görüşe kesinlikle katılmamakla birlikte, %40,9'u kararsızdır.

Tablo 3. Bilişim Güvenliği Konusunda Yeterli Bilgiye Sahiplik Düzeyi

	Frekans	Oran
<i>Kesinlikle Katılıyorum</i>	118	34,2
<i>Katılıyorum</i>	37	10,7
<i>Kararsızım</i>	141	40,9
<i>Katılmıyorum</i>	42	12,2
<i>Kesinlikle Katılmıyorum</i>	7	2,0

Çalışmanın bundan sonraki değerlendirilmesinde, anlaşılabilirliği artırmak açısından bazı alanlarda "kesinlikle katılıyorum" ve "katılıyorum" seçenekleri tek bir ifade "katılıyorum" olarak; katılmıyorum ve kesinlikle katılmıyorum ifadeleri ise " katılmıyorum" olarak tanımlanmış olup, oranlar da birleştirilerek ifade edilmiştir.

Tablo 4'de parola kullanımı ifadelerinin dağılımları görülmektedir. Öğrencilerin %79,7'si güvenli bir parolanın nasıl belirleneceği konusunda bilgi sahibidir. Parola güvenliğinin zayıf, orta ve yüksek olmasının güvenliği etkilediği fikrine, öğrencilerin %81,5'i katılarak güçlü bir parolanın belirlenmesinde bilgi düzeylerinin yüksek olduğu ortaya çıkmaktadır. %58,9'u parola yazarken yakın arkadaşlarından sakındıkları ve büyük bir kısmının başka kişilerle kullanıcı adı, şifre paylaşımında bulunmadıkları izlenmektedir. Bu oranlar, bilgi güvenliği açısından parola kullanımındaki farkındalığa işaret etmektedir. Buna rağmen, parolanın değiştirilmesinde (%24,1) ve parolayı yönetebilmek için bir yazılımın kullanılmasında (%24,3) kararsızların oranı dikkat çekmektedir. Öğrencilerin %40,9'ı (kararsızla) şifrelerini güvendiği kişilerle paylaşabileceğini ifade etmişler.

Tablo 4. Parola Kullanımı İfadelerinin Dağılımları

	Kesinlikle Katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle Katılmıyorum
Bilgisayarımın parolasını belirli zaman aralıklarında değiştiririm	36,5	11,3	24,1	17,1	11
Nasıl güvenli bir parola belirleyeceğim hakkında bilgi sahibiyim	39,4	40,3	14,5	4,1	1,7

Parolanın zayıf, orta, yüksek olmasının etkilerini biliyorum	40,3	41,2	13,6	3,8	1,2
Parolamı saklamak için bir yazılım kullanırım	22,3	7,5	24,3	31,9	13,9
Farklı sitelere üye olurken aynı kullanıcı adı ve parolayı kullanırım	29,9	11,9	19,4	27,8	11
Farklı e-posta adreslerim için aynı parolayı kullanırım	24,3	10,7	12,5	37,7	14,8
Parolamı yazarken arkadaşlarımın parolamı görmesi sorun değildir	19,1	4,9	17,1	32,2	26,7
Güvendiğim insanlara kullanıcı adı ve şifre veririm	17,7	6,4	16,8	29,6	29,6

Tablo 5 Virüs ve zararlı yazılımlarla ilgili ifadelerin dağılımını göstermektedir. Öğrencilerin %62,3'ü antivirüs yazılımların güncelliğini takip etmektedir. Bilgisayara indirilen dosyaları (%55,1) ve USB cihazlarını (%55,7) antivirüs taramasından geçirmeleri, virüsler konusunda bilgili olduklarının bir işareti olsa da, kararsızların ve katılmayanların oranı yaklaşık %45 olduğu için bu alanda yeterince farkındalıklarının olmadığını düşündürmektedir. Ayrıca, %34,2'sinin internet tehditleri hakkında kararsız oldukları dikkati çekmektedir. E-postaya eklenmiş dosyayı antivirüs taramasından geçirmeden açanlar %20,8'dir. Bu ifade için kararsızlar %25,5 olup, bu konuda yeterince farkındalığın olmadığı görülmektedir.

Tablo 5. Virüs ve Zararlı Yazılımlarla İlgili İfadelerin Dağılımları

	Kesinlikle Katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle Katılmıyorum
Anti-virüs yazılımının güncelliğini denetlerim	40,3	22	16,8	13	7,8
İndirdiğim dosyaları virüs taramasından geçiririm	38,3	16,8	25,2	14,5	5,2
USB, harici disk kullanırken anti-virüs taramasından geçiririm	37,4	18,3	27	12,5	4,9
Gönderenini tanımadığım bir dosyayı anti-virüs taramasından geçirmeden açarım	15,9	4,9	25,5	32,8	20,9
İnternet kaynaklı tehditlerle ilgili yeterli bilgiye sahibim	37,7	18	34,2	6,4	3,8

Tablo 6, sosyal ağlarla ilgili ifadelerin dağılımını göstermektedir. Tabloya göre, sosyal medyadaki gizlilik ayarları hakkında öğrencilerin %70,8'inin bilgiye sahip olduğunu görebilmekteyiz. Sosyal ağlarda kişisel bilgilerin %71,6 oranında paylaşılmadığı, %61,2'sinin tanımadığı kişileri listelerine eklemediği görülebilmektedir. %50,2'si kişisel fotoğraf ve videoları paylaşmazken, geri kalan %48,8'i ise paylaştığını (kararsızlarla) ifade etmiştir. Sosyal ağlarda tanıştıkları kişilerle öğrencilerin %50,7'sinin görüşmediği, geri kalan %48,3'ünün ise

kararsız veya görüşebileceği ifadelerle yansımaktadır. Kişisel bilgilerin paylaşılmasında ve tanımadıklarıyla görüşmede öğrencilerin yeterli düzeyde bilinçli olmadıkları söylenebilir.

Tablo 6. Sosyal Ağlarla İlgili İfadelerin Dağılımı

	Kesinlikle Katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle Katılmıyorum
Sosyal medyadaki hesaplarımın gizlilik ayarlarımı yönetebilecek bilgiye sahibim	40,9	29,9	21,4	4,6	3,2
Sosyal ağlarda kişisel bilgilerimi paylaşırım	9	4,6	14,8	33,9	37,7
Sosyal ağlarda tanımadıklarımı listeme eklerim	16,2	7	15,7	29,9	31,3
Anında ileti yazılımları kullanırken yazışmaları arşivlerim	33,6	19,7	20,6	18,6	7,5
Kişisel fotoğraf ve videolarımı erişebilir ortamlarda paylaşırım	20,9	4,9	24,1	26,7	23,5
İnternette, sosyal ağlarda, anında ileti yazılımlarıyla tanıştıklarıyla yüz yüze görüşürüm	18	7,5	23,8	26,1	24,6

Bilgisayar koruma ve güvenliğiyle ilgili ifadelerin dağılımı Tablo 7’de gösterilmektedir. Öğrencilerin %61,4’ü bilgisayarlarındaki önemli belgelerin şifrelendikleri ifadesine katılmışlardır. %66,1’i işletim sistemi güncellemelerini zamanında yaptığı ve %61,2’sinin ofis yazılım güncellemelerini denetledikleri ifadelerine katılmışlardır. Bilgisayarı belli zaman aralıklarında güvenlik taramasından geçiren öğrenciler %61,1’dir. Lisanslı yazılım öğrencilerin %35,4’ü satın almaktadır. Güvenliği sağlayacak yazılımları bulma konusunda öğrencilerin %40,6’sı kararsız kalmıştır.

Tablo 7. Bilgisayar Koruma ve Güvenliği İle İlgili İfadelerin Dağılımı

	Kesinlikle Katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle Katılmıyorum
Bilgisayarımnda önemli belgeler şifrelidir	40	21,4	15,7	16,5	6,4
Bilgisayarımı kullanmak isteyenlerin sadece konuk oturumunu kullanmasına izin veririm	34,8	13,3	23,8	19,7	8,4
İşletim sistemi güncellemelerini kontrol ederim	43,8	22,3	18,8	10,4	4,6
Ofis yazılımlarımın güncellemelerini denetlerim	40,9	20,3	19,1	15,1	4,6
Bilgisayarımı belli zaman aralıklarında güvenlik taramasından geçiririm	39,7	21,4	24,6	7,8	6,4
Bilgisayarımnda crack yazılımlar bulunmaktadır	11,6	9,9	24,6	35,7	18,3

Bilgisayarımı kullanmak isteyenler için ayrı bir oturum vardır	25,2	15,1	20,3	29,9	9,6
Bilgisayarındaki yazılımları lisans bedellerini ödeyerek kullanırım	25,8	9,6	32,8	19,4	12,5
Bilgisayarın güvenliğini sağlayacak yazılımları kullanmada yeterli bilgiye sahibim	27	14,8	40,6	13	4,6

Tablo 8, öğrencilerin %69,8'i, sahte içerikleri spam olarak işaretlediğini, %22'si göndereni bilmeseler de postaları cevapladığını göstermektedir. Öğrencilerin %51,6'sı, e-posta adresinin kötü niyetli kişilerin eline geçerse nasıl geri alınacağı konusunda yeterli bilgiye sahip değildir.

Tablo 8. E-Posta Kullanımıyla İlgili İfadelerin Dağılımı

	Kesinlikle Katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle Katılmıyorum
E-postama gelen sahte içerikli postaları “Spam” olarak işaretlerim	38,8	31	17,4	8,4	4,3
Göndereni tanımadığım postaları yanıtlarım	15,9	6,1	25,2	28,7	24,1
E-postam kötü niyetli kişilerin eline geçerse, nasıl geri alabileceğimi biliyorum	31,3	17,1	30,7	13,9	7

Tablo 9'a göre, öğrencilerin %84'u farklı bir bilgisayardan internete girdiklerinde bilgilerinin kaydedip kaydedilmediğini kontrol etmektedir. %81,4'u internetten ödeme güvenliğinde nelere dikkat etmesi gerektiğini bilmektedir. Öğrencilerin %83,1'i, internet ağında şifre kullanmaktadır. Cep telefonu ile ağlara bağlanma konusunda öğrencilerin %20,3'ünün kararsızlık yaşadığı ve kaynağını bilmedikleri ağlara %53'ünün katılabileceği görülmektedir. İnternet tarayıcısının güvenlik ayarları hakkında öğrencilerin %35,9'unun ve sanal klavye kullanımında %28,7'sinin kararsızlık yaşadığı söylenebilir.

Tablo 9. İnternet Kullanımıyla İlgili İfadelerin Dağılımı

	Kesinlikle Katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle Katılmıyorum
Başka bilgisayardan internete girerken, tarayıcının bilgilerimi kaydedip kaydetmediğini kontrol ederim	33,3	50,7	10,4	4,1	1,4
İnternette alışveriş yaparken, ödeme güvenliği hakkında nelere dikkat etmem gerektiğini bilirim	42,3	39,1	13,6	3,2	1,7
İnternette gezindiğim web sitelerinin güvenilirliğiyle ilgili bilgi edinmeye çalışırım	47,5	18,3	26,1	6,7	1,4
Kablosuz internet ağımda şifre kullanırım	41,4	41,7	11,9	3,5	1,4
Kaynağını bilmediğim ağlara bağlanırım	20,3	7,2	20,3	31,3	20,9
Farklı bilgisayarlar üzerinden alışveriş yaparım	16,5	7,8	19,4	35,4	20,9
Kaynağını bilmediğim ağlara bağlanırım	21,7	6,4	24,9	27,8	19,1
İnternet tarayıcısının güvenlik ayarları hakkında bilgi sahibiyim	38,3	13,9	35,9	8,1	3,8
Kredi kartımla ilgili bilgileri girerken sanal klavye kullanırım	31,6	13,9	28,7	20	5,8

Tablo 10'a göre, öğrencilerin %29,6'sı bilişim suçuyla karşılaştıklarında kime başvuru yapacağı hakkında kararsızdırlar. Bilişim güvenliği konusunda bilgi alınabilecek adresleri %52,2'si bilirken, geri kalanı kararsız kalmış veya bilmiyordur. Telif haklarının kullanımında %40'ının kararsızlık yaşadığı ve sadece %38'nin bu konuda yeterli bilgiye sahip oldukları görülmektedir.

Tablo 10. Yasal, Etik ve Bilişim Güvenliğiyle İlgili İfadelerin Dağılımı

	Kesinlikle Katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle Katılmıyorum
Bilişim suçuna maruz kalırsam kime başvuracağımı biliyorum	37,4	19,7	29,6	9,6	3,8
Bilişim güvenliğiyle ilgili siteleri takip ederim	21,4	10,1	37,7	25,5	5,2
Bilişim güvenliği konusunda bilgi alabileceğim adresleri bilirim	36,5	15,7	31,9	12,2	3,8
Yazılım kullanmada telif hakları konusunda bilgiliyim	26,4	11,6	40	14,8	7,2

Bilişim güvenliğinin cinsiyet üzerindeki farklılıklarını tespit edebilmek için T testi analizi kullanılmıştır. Analiz sonucunda Tablo 11’ de görülen her bir ifadede anlamlı fark olduğu ortaya çıkmıştır.

Tablo 11 ve Tablo 12, cinsiyet açısından bilişim güvenliğine yönelik T Testi sonuçlarını göstermektedir. Parola ve internet kullanımı, virüs ve zararlı yazılımlara yönelik ifadelerden “Kullandığım anti-virüs yazılımının güncelliğini denetlerim’e” göre erkeklerin kızlara göre daha rahat davrandığı hipotezi 0.05 anlamlılık düzeyinde (%95 güvenle) reddedilemez.

Tablo 11. Cinsiyet Açısından Bilişim Güvenliğine Yönelik T Testi Sonuçları I

Parola Kullanımı	Grup	N	X	SS	T testi			Levene
					t	sd	p	p
Güvendiğim insanlara kullanıcı adı ve şifremi veririm	K	204	3,324	1,4531	-2,302	343	0,02	0,216
	E	141	3,681	1,3644				
İnternet Kullanımı	Grup	N	X	SS	T testi			Levene
					t	sd	p	P
Bana ait olmayan bir bilgisayardan internete girerken tarayıcının kişisel bilgilerimi kaydedip kaydetmediğini kontrol ederim	K	204	1,824	0,8234	-1,904	343	0,05	0,213
	E	141	2	0,8783				
Virüs ve Zararlı Yazılımlar	Grup	N	X	SS	T testi			Levene
					t	sd	p	p
İnternet kaynaklı tehditlerle ilgili yeterli bilgiye sahibim	Kız	204	2,309	1,1132	2,048	343	0,04	0,149
	Erkek	141	2,057	1,1388				
Anti-virüs yazılımının güncelliğini denetlerim.	Kız	204	2,118	1,2811	-2,447	343	0,01	5
	Erkek	141	2,468	1,3446				
Bilgisayar Koruma ve Güvenliği	Grup	N	X	SS	T Testi			Levene
					t	sd	p	p
Bilgisayarım güvenliğini sağlayacak yazılımları bulma ve kullanmada yeterli bilgiye sahibim.	Kız	204	2,725	1,1417	3,734	343	0,00	0,498
	Erkek	141	2,262	1,1190				
Sosyal Ağlar	Grup	N	X	SS	T testi			Levene
					t	sd	p	p
Sosyal ağ sitelerinde	Kız	204	3,672	1,4159	2,246	343	0,02	0,935

tanımadığım insanları arkadaş listeme eklerim	Erkek	141	3,326	1,3861			5	
Sosyal ağlarda tanıştığım bir insanla görüşürüm	Kız	204	3,711	1,2864	6,664	343	0,00	0,290
	Erkek	141	2,752	1,3531			0	
Fotoğraf/ videolarımı erişilebilir ortamlarda paylaşırım	Kız	204	3,475	1,3841	3,280	343	0,00	0,980
	Erkek	141	2,972	1,4290			1	

Sosyal ağlar, e-posta yönetimi, internet kullanımında bilgi güvenliği, bilişim güvenliği; internet kaynaklı tehditler ve e-postaya eklenmiş dosyayı anti-virüs taramasından geçirmeden açılması ifadelerine göre kızların, erkeklere göre daha rahat davrandıkları söylenebilir (Tablo 11 ve 12).

Tablo 12. T Testi Sonuçları II

Virüs ve Zararlı Yazılımlar	Grup	N	X	SS	T testi			Levene İstatistiği
					t	sd	p	p
Göndereni tanımadığım bir e-postaya eklenmiş dosyayı anti-virüs taramasından geçirmeden açarım	Kız	204	3,490	1,2653	1,944	343	0,053	0,251
	Erkek	141	3,213	1,3565				
E-Posta Yönetimi	Grup	N	X	SS	T testi			Levene İstatistiği
					t	sd	p	p
Göndereni tanımasam da ilgimi çeken postaları yanıtlarım	Kız	204	3,588	3,588	3,376	343	0,001	0,932
	Erkek	141	3,099	1,3379				
E-posta adresim kötü niyetli kişilerin eline geçerse, nasıl geri alabileceğim konusunda bilgi sahibiyim	Kız	204	2,588	1,2700	1,913	343	0,057	0,346
	Erkek	141	2,326	1,2218				
İnternet Kullanımında Bilgi Güvenliği	Grup	N	X	SS	T testi			Levene İstatistiği
					t	sd	p	p
Kaynağını bilmediğim kablosuz ağlara bağlanırım	Kız	204	3,525	1,2920	4,447	343	0,000	0,12
	Erkek	141	2,858	1,4715				

Bilişim Güvenliği	Grup	N	X	SS	T testi			
					t	sd	p	Levene İstatistiği
Şifrelenmemiş ve kaynağını bilmediğim kablosuz ağlara bağlanırım	Kız	204	3,299	1,3623	2,196	343	0,029	0,464
	Erkek	141	2,965	1,4313				
Bir bilişim suçuna maruz kalırsam kime başvuracağımı biliyorum	Kız	204	2,328	1,1468	1,981	343	0,048	0,377
	Erkek	141	2,078	1,1654				
Bilişim güvenliğiyle ilgili siteleri takip ederim	Kız	204	2,931	1,1640	1,942	343	0,053	0,084
	Erkek	141	2,681	1,1971				

Öğrencilerin kendine ait bilgisayarının olup olmaması açısından bilişim güvenliğine yönelik fark olup olmadığını tespit ederken T testi kullanılmıştır. Analiz sonucunda Tablo 13’de görülen her bir ifadeye anlamlı fark olduğu tespit edilmiştir. “Bilgisayarında kendi oturumumdaki önemli belgeler şifrelidir” ifadesi için kendisine ait bilgisayarı olan öğrencilerin olmayanlara göre daha rahat davrandıkları söylenebilir. “İnternet kaynaklı tehditlerle ilgili yeterli bilgiye sahibim” ve “Bilgisayarın güvenliğini sağlayacak yazılımları bulma ve kullanmada yeterli bilgiye sahibim” ifadelerinde kendisine ait bilgisayarı olmayan öğrencilerin olanlara göre daha rahat davrandıkları söylenebilir. “E-posta adresim kötü niyetli kişilerin eline geçerse, nasıl geri alabileceğim konusunda bilgi sahibiyim” ifadesi için kendisine ait bilgisayarı olmayan öğrenciler olanlara göre daha rahat davranmaktadır. “Bilişim güvenliği konusunda bilgi alabileceğim adresleri bilirim” ifadesinde, kendisine ait bilgisayarı olmayan öğrencilerin olanlara göre daha rahat davranmaktadır.

Tablo 13. T Testi Sonuçları

	Grup	N	X	SS	T testi			Levene İstatistiği
					t	sd	p	p
Bilgisayarında önemli belgeler şifreli haldedir	Evet	215	2,386	1,2915	1,972	343	,049	0,575
	Hayır	130	2,100	1,3286				
İnternet kaynaklı tehditlerle ilgili bilgiye sahibim	Evet	215	2,098	1,1417	-2,302	343	,022	0,870
	Hayır	130	2,385	1,0882				
E-postam kötü niyetli kişilerin eline geçerse, nasıl geri alabileceğim konusunda bilgi sahibiyim	Evet	215	2,372	1,2309	-2,085	343	,038	0,769
	Hayır	130	2,662	1,2793				
Bilişim güvenliği	Evet	215	2,186	1,1612	-2,508	343	,013	0,280

konusunda bilgi alabileceğim adresleri bilirim	Hayır	130	2,515	1,2151					
Bilgisayarın güvenliğini sağlayacak yazılımları kullanmada bilgiliyim	Evet	215	2,381	1,1206	-3,219	343	,001	0,327	
	Hayır	130	2,792	1,1660					

Tablo 14’de yapılan Levene Testine göre varyansların homojen dağıldığı görülmektedir (P=0,209). ANOVA sonucuna göre gruplar arasında anlamlı bir fark olduğu ortaya koyulmuştur (P=<0,05). Farklılığın olduğu sınıfı belirleyebilmek için PostHoc LSD testi yapılmıştır. LSD testi sonuçları aşağıdaki tabloda görülmektedir.

Tablo 14. Öğrencilerin Sınıf Düzeyleri Açısından Bilişim Güvenliği Üzerindeki Etkisinin ANOVA Sonuçları

Bana ait olmayan bilgisayardan internete girerken, tarayıcının bilgilerimi kaydedip kaydetmediğini kontrol ederim									
Levene İstatistiği (P)		0,299							
Sınıf	N	Ort.	SS	Var.K	KT	SD	KO	F	P
1.	130	2,031	0,9145	Grup Arası	6,350	3	2,117	2,984	,031
2.	163	1,798	0,8474	Grup İçi	241,893	341	0,709		
3.	37	1,730	0,5602	Toplam	248,243	344			
4.	15	2,200	0,6761						
Toplam	345	1,896	0,8495						

Tablo 15’de, hangi gruplar arasında anlamlı farklılık olduğunu belirlemek için gerçekleştirilen LSD test sonuçlarına göre “Bana ait olmayan bilgisayardan internete girerken, tarayıcının kişisel bilgilerimi kaydedip kaydetmediğini kontrol ederim” ifadesi 1. ve 2. Sınıf grupları arasında farklılık göstermektedir. 1. Sınıf öğrencileri kendilerine ait olmayan bilgisayardan internete girerken tarayıcının bilgileri kaydedip kaydetmediğini, 2. Sınıflara göre daha fazla kontrol ettikleri şeklinde yorumlanabilir.

Tablo 15. LSD Testi Sonuçları

Sınıf	Sınıf	Ortalama Fark	Standart hata	P
1,0	2,0	,2332*	,0990	,019
	3,0	,3010	,1569	,056
	4,0	-,1692	,2297	,462
2,0	1,0	-,2332*	,0990	,019
	3,0	,0678	,1534	,659
	4,0	-,4025	,2273	,077
3,0	1,0	-,3010	,1569	,056
	2,0	-,0678	,1534	,659
	4,0	-,4703	,2578	,069
4,0	1,0	,1692	,2297	,462
	2,0	,4025	,2273	,077
	3,0	,4703	,2578	,069

*, 0.05 düzeyinde anlamlılığı ifade etmektedir.

Tablo 16’da öğrencilerin sınıf düzeyleri açısından “Kullandığım anti-virüs yazılımının güncelliğini denetlerim” ifadesi üzerinde farklılık olup olmadığı Varyans analiziyle incelenmiştir. Yapılan Levene Testinde varyansların homojen dağıldığı görülmektedir (p=0,096). ANOVA sonucuna göre gruplar arasında anlamlı bir fark olduğu ortaya koyulmuştur (p=<0,05).

Tablo 16. Öğrencilerin Sınıf Düzeyleri Açısından Bilişim Güvenliği Konusu Üzerindeki Etkisinin ANOVA Sonuçları

Kullandığım anti-virüs yazılımının güncelliğini denetlerim									
Levene İstatistiği (P)						0,096			
Sınıf	N	Ort.	SS	Var.K	KT	SD	KO	F	P
1.	130	2,246	1,2823	Grup Arası	18,886	3	6,295	3,716	0,012
2.	163	2,252	1,3349						
3.	37	1,946	1,1042						
4.	15	3,267	1,5337	Grup İçi	596,522	344			
Toplam	345	2,261	1,3168						

Tablo 17’de hangi gruplar arasında anlamlı farklılık olduğunu belirlemek için gerçekleştirilen LSD test sonuçlarına göre ise “Kullandığım anti-virüs yazılımının güncelliğini denetlerim” ifadesi 4. sınıfla 1. 2. ve 3. sınıfları arasında anlamlı farklılık göstermektedir. Burada 4. sınıf öğrencilerinin anti-virüs yazılımının güncelliğini, 1, 2. ve 3. sınıflara göre daha iyi denetledikleri ifade edilebilir.

Tablo 17. LSD Testi Sonuçları

Sınıf	Sınıf	Ortalama Fark	Standart hata	P
1,0	2,0	-,0054	,1530	,972
	3,0	,3002	,2425	,217
	4,0	-1,0205*	,3549	,004
2,0	1,0	,0054	,1530	,972
	3,0	,3056	,2370	,198
	4,0	-1,0151*	,3512	,004
3,0	1,0	-,3002	,2425	,217
	2,0	-,3056	,2370	,198
	4,0	-1,3207*	,3984	,001
4,0	1,0	1,0205*	,3549	,004
	2,0	1,0151*	,3512	,004
	3,0	1,3207*	,3984	,001

*, 0.05 düzeyinde anlamlılığı ifade etmektedir.

Tablo 18’de öğrencilerin okudukları bölüm açısından “Bilişim güvenliği konusunda bilgi alabileceğim adresleri bilirim” ifadesi üzerinde farklılık olup olmadığı Varyans analiziyle incelenmiştir. Yapılan Levene Testinde varyansların homojen dağıldığı görülmektedir (p=0,096). ANOVA sonucuna göre gruplar arasında anlamlı bir fark olduğu ortaya koyulmuştur (p=<0,05).

Tablo 18. Öğrencilerin Okudukları Bölüm Açısından Bilişim Güvenliği Konusu Üzerindeki Etkisinin ANOVA Sonuçları

Bilişim güvenliği konusunda bilgi alabileceğim adresleri bilirim									
Levene İstatistiği (P) 0,600									
Grup	N	Ortalama	SS	Var.K	KT	SD	KO	F	P
BY	46	2,022	1,1053	Grup Arası	24,086	8	3,011	2,181	0,028
DT	40	2,775	1,1206		Grup İçi	463,728	336		
MVU	25	2,880	1,3013	Toplam	487,814	344			
L	65	2,246	1,1730						
İY	25	2,240	1,3626						
Hİ	33	2,394	1,2485						
SHUİ	11	2,182	1,2505						
UTL	48	2,229	1,1530						
FB	52	2,096	1,0712						
Toplam	345	2,310	1,1908						

Tablo 19’da gerçekleştirilen LSD sonuçlarına göre “Bilişim güvenliği konusunda bilgi alabileceğim adresleri bilirim” ifadesi;

- “Büro Yönetimi-Dış Ticaret, Muhasebe ve Vergi”
- “Dış Ticaret- Büro Yönetimi, Lojistik, UTL, Finans ve Bankacılık”
- “Muhasebe ve Vergi-Büro Yönetimi, Lojistik, UTL, Finans ve Bankacılık”

- d “Lojistik- Dış Ticaret, Muhasebe ve Vergi”
e “UTL-Dış Ticaret, Muhasebe ve Vergi”
f “Finans ve Bankacılık- Dış Ticaret, Muhasebe ve Vergi”

grupları arasında anlamlı farklılıkları göstermektedir.

Dış ticaret, Muhasebe ve Vergi Uygulamaları bölümleri öğrencilerinin Bilişim güvenliği konusunda bilgi alabilecekleri adresleri Büro Yönetimi, Lojistik, Uluslararası Ticaret ve Lojistik, Finans ve Bankacılık öğrencilerinden daha iyi bildikleri söylenebilir.

Tablo 19. LSD Testi Sonuçları

Bölüm	Bölüm	Ortalama Fark	Std. Hata	P	Bölüm	Bölüm	Ortalama Fark	Std. Hata	P	
Büro Yönetimi	DT	-,7533*	,2540	,003	Lojistik	BY	,2244	,2264	,322	
	MVU	-,8583*	,2919	,004		DT	-,5288*	,2361	,026	
	L	-,2244	,2264	,322		MVU	-,6338*	,2765	,022	
	İY	-,2183	,2919	,455		İY	,0062	,2765	,982	
	Hİ	-,3722	,2680	,166		Hİ	-,1478	,2511	,557	
	SHUİ	-,1601	,3943	,685		SHUİ	,0643	,3830	,867	
	UTL	-,2074	,2424	,393		UTL	,0170	,2236	,939	
	FB	-,0744	,2378	,755		FB	,1500	,2186	,493	
	BYY	,7533*	,2540	,003		BY	,2074	,2424	,393	
	MVU	-,1050	,2995	,726		DT	-,5458*	,2515	,031	
Dış Ticaret	L	,5288*	,2361	,026	MVU	-,6508*	,2898	,025		
	İY	,5350	,2995	,075	UTL	L	-,0170	,2236	,939	
	Hİ	,3811	,2763	,169		İY	-,0108	,2898	,970	
	SHUİ	,5932	,4000	,139		Hİ	-,1648	,2657	,536	
	UTL	,5458*	,2515	,031		SHUİ	,0473	,3927	,904	
	FB	,6788*	,2471	,006		FB	,1330	,2351	,572	
	BY	,8583*	,2919	,004		BY	,0744	,2378	,755	
	DT	,1050	,2995	,726		DT	-,6788*	,2471	,006	
	L	,6338*	,2765	,022		MVU	-,7838*	,2859	,006	
	Muhasebe ve Vergi	İY	,6400	,3323		,055	Finans ve Bankacılık	L	-,1500	,2186
Hİ		,4861	,3115	,120		İY		-,1438	,2859	,615
SHUİ		,6982	,4251	,101	Hİ	-,2978		,2615	,256	
UTL		,6508*	,2898	,025	SHUİ	-,0857		,3899	,826	
FB		,7838*	,2859	,006	UTL	-,1330		,2351	,572	

*, 0.05 düzeyinde anlamlılığı ifade etmektedir.

Sonuç

Bu çalışmanın amacı RTEÜ Fındıklı Uygulamalı Bilimler Yüksekokulu ve Sosyal Bilimler Meslek Yüksekokulunda öğrenim gören öğrencilerin bilişim güvenliği farkındalıklarını incelemektir. Öğrencilere yöneltilen sorular parola, virüs ve zararlı yazılımlar, sosyal ağlar, internet kullanımı, bilgisayar koruma ve güvenliği, yasal, etik ve bilişim güvenliğiyle ilgilidir. Öğrencilerin en bilinçli oldukları ve farkındalığı daha yüksek olan alanlar; sosyal ağ ve internet kullanımındır.

Öğrencilerin güvenli bir parolanın nasıl belirleneceği konusunda (%79,7) yüksek düzeyde bilgiye ve farkındalığa sahip oldukları görülebilmektedir. Parolanın güvenli kişilerle

paylaşılmasında öğrencilerin %24,1'i bir sakınca görmezken, %16,8 'i ise kararsız kalmaktadır. Parolanın belirlenmesinde yakın arkadaşların görmesi %24'lük kesim için bir problem yaratmazken, %16,8'lik bu konuda kararsız kalmıştır. Bu sonuçlardan, parolanın nasıl belirleneceği konusunda öğrenciler bir farkındalığa sahip olmasına rağmen, parolanın gizliliği konusunda yeterince bilgi düzeyinde olmadıkları görülebilmektedir. Erdoğan(2017:37) çalışmasında öğrencilerin %48'sinin parola paylaşma konusunda bir sakınca görmediği sonucu bu çalışmanın sonucuyla benzerlik göstermektedir. Paralel olarak, Akgün&Topal(2015:104), Tekerek&Tekerek(2013:62) ve Aslan(2019:10) çalışmalarındaki parola kullanımına yönelik güvenlik açığı olduğunu ifade etmeleri çalışmanın bulgularını desteklemektedir.

Sosyal ağların gizlilik ayarlarıyla ilgili öğrencilerin %70,8'inin bilgi sahibi olduğu ve %71,6'sının kişisel bilgileri paylaşmamasıyla farkındalık göstermesine rağmen, %48'sinin tanımadığı kişiler ile fotoğraf/videoları paylaşabileceği görülmektedir. Kişisel bilgilerin paylaşılmaması gerektiği çoğu öğrenci tarafından bilinmesine rağmen, fotoğraf/video yüklemeye bir sakınca görmemeleri bir çelişki doğurmaktadır. Sosyal ağların kullanım amacı ve düzeyi geçmiş yıllara göre artarak ve çeşitlenerek devam etmektedir. Özellikle bu alanda öğrencilere bir bilinçlendirme programı düzenlenebilir.

Öğrenciler, internet kullanımında, ödemede ve kablosuz ağlara şifre kullanarak bağlanmada yeterince bilgili olmalarına rağmen, kaynağı belirsiz olan ağlara %53'ünün katılması ile yeterli düzeyde farkındalık olmadığını göstermektedir.

Yazılım, telif hakları konusunda öğrencilerin büyük çoğunluğunun kararsız kaldıkları veya bilmedikleri ortaya çıkmıştır. İşletim sistemi güncellemelerini öğrencilerin %66,1'inin yaptıkları halde, %40,1'inin bilgisayar güvenliğini sağlayacak yazılımlar konusunda kararsız oldukları görülmektedir. Öğrencilerin yaklaşık %30'u bilişim suçuyla karşılaştıklarında kime başvuru yapacakları hakkında kararsızdırlar. Ögütçü vd.(2016: 88), çalışmasında da kullanıcıların %40,4'ünün bilişim suçlarını nereye bildirecekleri konusundaki kararsızlık sonucumuzu desteklemektedir.

Çalışmada öğrencilerin cinsiyeti ve kendine ait kullanabileceği bilgisayarının olup olmaması açısından T testi kullanılmıştır. Analiz sonucunda bilişim güvenliğiyle ilgili yöneltilen ifadeler açısından kızların erkek öğrencilere göre daha bilinçli davrandıkları görülmektedir. Bu sonuç Farooq vd.(2015:356)'nin çalışmasının bulgularıyla benzerlik göstermektedir. Döner(2022:45) ise çalışmasında, cinsiyetin bilgi güvenliği farkındalığı üzerinde etkisi olduğunu belirlemiş fakat bu çalışmanın bulgularının aksine erkeklerin bilgi güvenliği farkındalıklarının daha fazla olduğunu ifade etmiştir. Albayrak&Bağcı(2022:7) çalışmaları incelendiğinde ise cinsiyetin bilişim güvenliği farkındalığı üzerinde etkisinin

bulunmadığı görülmüştür. Kendisine ait bilgisayarı olmayan öğrencilerin ise olanlara göre bilişim güvenliği farkındalığı konusunda daha rahat davrandıkları görülmüştür.

Yapılan Varyans analizleri sonucunda, 1. Sınıf öğrencilerinin kendilerine ait olmayan bir bilgisayardan internete girerken, tarayıcının kişisel bilgilerini kaydedip kaydetmediğini 2. Sınıflara göre daha fazla kontrol ettiği bulgusuna ulaşılmıştır. 4. sınıf öğrencilerinin kullandıkları anti-virüs yazılımının güncelliğini 1., 2. ve 3. sınıf öğrencilerine göre daha iyi denetledikleri görülmüştür. Dış Ticaret, Muhasebe bölümleri öğrencilerinin ise bilişim güvenliği konusunda bilgi alabilecekleri adresleri Büro Yönetimi, Lojistik, Uluslararası Ticaret ve Lojistik, Finans ve Bankacılık öğrencilerinden daha iyi bildikleri tespit edilmiştir. Literatüre bakıldığında Albayrak&Bağcı (2022: 6) çalışmasının aksine sınıfların bilişim güvenliği farkındalığı üzerindeki etkisi olduğu görülmektedir. Yine Albayrak&Bağcı (2022:7)'nin çalışmasında, bu çalışmada olduğu gibi, farklı bölümlerde okuyan öğrencilerin bilişim güvenliği farkındalığı üzerinde etkisi olduğu ileri sürülmüştür.

Bilgi güvenliği, bilginin üç temel unsuru olan gizlilik, bütünlük ve erişilebilirlik unsurlarının var olması halinde sağlanabilecektir. Bu üç unsurun tamamı gerçekleştirildiği takdirde bilgi güvenliğinden bahsedilebilir. Bilgi güvenliğinin sağlanmasında; insan, süreç ve teknoloji üçlüsünün birbirleriyle uyumu gereklidir. Bilgi güvenliğinin en önemli aşamasını oluşturan “insan” ile ilgili gerçekleşen bu çalışmada, öğrencilerin bilişim güvenliğiyle ilgili bazı alanlarda yeterli düzeyde bilgi sahibi olduğu fakat farkındalıklarının aynı düzeyde olmadığı görülmektedir ki Akgün&Topal(2015), Gökmen&Akgün(2014); Tekerek&Tekerek(2013) çalışmaları da bunu desteklemektedir. Çalışmada aynı alanda farklı soru tiplerinin sorulması öğrencilerin bildiklerini uygulayıp uygulamadıklarını da sorgulamaktadır. Çapraz soruların sonucu olarak, öğrenciler bilgi güvenliği konusunda önemli noktaları bildiklerini ama uygulamadıkları paradoksunu da doğurmaktadır.

Kurumların riskleri azaltmak ve bilgi güvenliğini sağlayabilmek için genellikle teknoloji tabanlı ve maliyetli çözüm önerileri getirmelerine rağmen, çözümleri kullanacak olan “insan” olduğu için, bu uygulamalar tek başına yeterli değildir. Tüm bu yatırımlardan önce kullanıcıların bilişim güvenliği konusunda bilinçlendirilmesi gerekmektedir. Kurumların bilgi güvenliğinde başarı elde edebilmeleri teknik altyapı yatırımlarına olduğu kadar, sosyo-örgütsel kaynaklar yatırımıyla da sağlanabilir. Üniversiteler, öğrencilerin iş hayatına başlamadan önce eğitim aldıkları son kurumlar olarak değerlendirildiğinde, karşılaşılabilecek tehditler ve riskler konusunda bilinçlendirilmeleri ve bu alanda yetkinliğe ulaşabilecek seviyeye gelmeleri beklenir. Bu bağlamda, üniversitelerde bilgi güvenliği konusunda eğitimler ve bilinçlendirme programları düzenlenerek öğrencilerin sorumluluklarının ve farkındalık düzeylerinin artırılması büyük önem

taşımaktadır. Bilişim teknolojilerinin kullanım alanlarının genişlemesi ve kullanım düzeyinin hızla artması, öğrencilere ilkökul seviyesinden itibaren bilişim güvenliği bilincinin verilmesi gerektiğini da hatırlatmaktadır. Bu da ancak, eğitim kurumlarında bilgi güvenliğinin sürekli eğitim haline gelmesiyle gerçekleşebilecektir.

Yazar Katkıları: Bu çalışmada yer alan giriş, literatür, yöntem ve sonuç bölümlerinde her iki yazar da eşit oranda katkı sağlamıştır.

Çıkar Beyanı: Yazarlar arasında çıkar çatışması olmamıştır.

Kaynakça

- Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour and Information Technology*, 33(3), 237–248. <https://doi.org/10.1080/0144929X.2012.708787>
- Akgün, Ö. E. ve Topal, M. (2015). Eğitim fakültesi son sınıf öğrencilerinin bilişim güvenliği farkındalıkları: Sakarya üniversitesi eğitim fakültesi. *Sakarya University Journal of Education*, 5(2), 98–121. <https://doi.org/10.19126/suje.73391>
- Albayrak, E. ve Bağcı, H. (2022). Modelling the effects of personal factors on information security awareness. *Journal of Information Science*. <https://doi.org/10.1177/01655515221127609>
- Aloul, F. A. (2010). Information security awareness in UAE: a survey paper. 2010 International Conference for Internet Technology and Secured Transactions, ICITST.
- Arce, I. (2003). The weakest link revisited. *IEEE Security and Privacy*, 1(2), 72–76. <https://doi.org/10.1109/MSECP.2003.1193216>
- Aslan, S. (2019). Bilişim teknolojileri alanındaki meslek lisesi öğrencilerinin siber güvenliğe yönelik bilgi düzeylerinin belirlenmesi (Yüksek Lisans Tezi). Necmettin Erbakan Üniversitesi, Konya.
- Avcı, Ü. ve Oruç, O. (2020). Üniversite öğrencilerinin kişisel siber güvenlik davranışları ve bilgi güvenliği farkındalıklarının incelenmesi. *İnönü Üniversitesi Eğitim Fakültesi Dergisi*, 21(1), 284–303. <https://doi.org/10.17679/inuefd.526390>
- Bulgurcu, B., Çavuşoğlu, H. ve Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS*, 34(3), 523–548. <https://doi.org/10.2307/25750690>
- Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M. ve Baskerville, R. (2013). Future directions for behavioral information security research. *Computers and Security*, 32, 90–101. <https://doi.org/10.1016/j.cose.2012.09.010>
- Emmungil, E. A. ve Uzun, Y. (2021). Bilgi ve iletişim teknolojisi dersi alan sağlık meslek yüksekokul öğrencilerinin bilişim güvenliği farkındalığı. *Ufuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 10(19), 69–83.
- Erdoğan, A. (2017). Üniversite öğrencilerinin bilgi güvenliği kazanımlarının, farkındalıkları üzerindeki analizi: Afyon Kocatepe Üniversitesi örneği (Yüksek Lisans Tezi). Afyon Kocatepe Üniversitesi, Afyon
- Farooq, A., Isoaho, J., Virtanen, S. ve Isoaho, J. (2015). Information security awareness in educational institution: an analysis of students' individual factors. 13th IEEE Int.

- Symp. Parallel and Distributed Processing with Applications (ISPA '15), (352–359). Helsinki, Finlandiya. <https://doi.org/10.1109/Trustcom.2015.394>
- Garba, A., Maheyzah Binti Sirat, Siti Hajar ve Ibrahim Bukar Dauda. (2020). Cyber security awareness among university students: a case study. *Science Proceedings Series*, 2(1), 82–86. <https://doi.org/10.31580/sps.v2i1.1320>
- Gökmen, Ö. F. ve Akgün, Ö. E. (2014). Bilgisayar ve öğretim teknolojileri eğitimi öğretmen adaylarının bilişim güvenliği bilgilerinin çeşitli değişkenlere göre incelenmesi. *Çukurova Üniversitesi Eğitim Fakültesi Dergisi*, 44(1), 61–84. <https://doi.org/10.14812/cufej.2015.004>
- Henkoğlu, T., ve Yılmaz, B. (2013). Avrupa Birliği (AB) bilgi güvenliği. *Türk Kütüphaneciliği*, 27(3), 451–471.
- Kara, O., ve Topaloğlu, M. (2019). Bilgisayar teknolojileri ve bilişim sistemleri öğrencilerinin bilişim güvenliği alanında yeterliliklerinin incelenmesi. *Ege Eğitim Teknolojileri Dergisi*, 3(1), 20–27.
- Kritzinger, E., Veiga, A. Da, ve Staden, W. Van. (2022). Measuring organizational information security awareness in South Africa. *Information Security Journal: A Global Perspective*, 00(00), 1–14. <https://doi.org/10.1080/19393555.2022.2077265>
- Kruger, H., Drevin, L., ve Steyn, T. (2010). A vocabulary test to assess information security awareness. *IMCS*, 18(5), 316–327. <https://doi.org/10.1108/09685221011095236>
- McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. ve 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>
- McCumber, J. (1991). Information systems security: a comprehensive model. 14th National Computer Security Conference sunulan bildiri. Baltimore, MD.
- McCumber, J. (2005). *Assessing and managing security risk in IT systems: a structured methodology*. CRC Press LLC: Florida.
- Moletsane, T. ve Tsibolane, P. (2020). Mobile information security awareness among students in higher education: an exploratory study. 2020 Conference on Information Communications Technology and Society'de sunulan bildiri. <https://doi.org/10.1109/ICTAS47918.2020.233978>
- Öğütçü, G., Testik, Ö. M. ve Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers and Security*, 56, 83–93. <https://doi.org/10.1016/j.cose.2015.10.002>
- Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., ve Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers and Security*, 66, 40–51. <https://doi.org/10.1016/j.cose.2017.01.004>
- Şen, R. (2020). Üniversite öğrencilerinin bilgi güvenliği davranışlarını etkileyen faktörler(Yüksek Lisans Tezi). Kıbrıs Üniversitesi, Lefkoşa.
- Taha, N. ve Dahabiyeh, L. (2021). College students information security awareness: a comparison between smartphones and computers. *Education and Information Technologies*, 26(2), 1721–1736. <https://doi.org/10.1007/s10639-020-10330-0>
- Tekerek, M. ve Tekerek, A. (2013). A research on students' information security awareness. *TURJE Turkish Journal of Education*, 2(3), 61–70. <https://doi.org/10.19128/turje.181065>

- TÜİK. (2022). Hanehalkı bilişim teknolojileri (bt) kullanım araştırması, 2022, 2022–2023.
- Zhang, J., Reithel, B. J. ve Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management and Computer Security*, 17(4), 330–340. <https://doi.org/10.1108/09685220910993980>
- Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł. ve Cetin, F. (2022). Cyber security awareness , knowledge and behavior: a comparative study cyber. *Journal of Computer Information Systems*, 62(1), 82–97. <https://doi.org/10.1080/08874417.2020.1712269>