Makale Gönderim Tarihi: 03-04-2015 *Makale Kabul Tarihi:16-07-2015*
Sakarya University Journal of Education, 5/2 (Ağustos/August 2015) ss. 98-121.

Eğitim Fakültesi Son Sınıf Öğrencilerinin Bilişim Güvenliği Farkındalıkları: Sakarya Üniversitesi Eğitim Fakültesi Örneği*

Özcan Erkan AKGÜN** **Murat TOPAL *****

Öz

Bu çalışma eğitim fakültelerinde öğrenim gören öğrencilerin bilişim güvenliği farkındalıklarını incelemek amacıyla gerçekleştirilmiştir. Araştırma tarama modelinde yürütülmüştür. Katılımcı grubu Sakarya Üniversitesi Eğitim Fakültesi son sınıfında okuyan farklı bölümlerden toplam 217 öğrenci oluşturmaktadır. Veri toplama aracı olarak araştırmacılar tarafından geliştirilen "Bilişim Güvenliği Anketi" kullanılmıştır. Veriler betimleyici ve anlam çıkarıcı istatistikler kullanılarak analiz edilmiştir. Araştırma sonuçlarına göre bilişim güvenliği konuları ile ilgili farkındalıklarının yeterli olmadığını belirten azımsanmayacak sayıda öğrenci olduğu görülmüştür. Cinsiyete, ortalama bilgisayar-internet kullanım yılına göre bazı konularda anlamlı farklılıklar olduğu gözlenmekle birlikte, bilişim güvenliği eğitimi aldığını belirten adaylar ile almayan adaylar arasında beklendiği gibi ciddi bir anlamlı farklılık gözlenmemiştir. Öğretmen adayları için kapsamı iyi belirlenmiş bir bilişim güvenliği eğitimi verilmesi önerilmektedir.

Anahtar Kelimeler: Bilişim Teknolojileri, Bilişim Güvenliği, Bilgi Güvenliği, Öğretmen Adayı

Information Security Awareness of the Senior Teacher Students: Sakarya University Sample

Abstract

This study was conducted in survey model to determine awareness of information security of the 217 prospective teachers from different departments that attending Faculty of Education at Sakarya University. "Information Security Questionnaire" that developed by authors was used for data collection. The findings of the survey revealed, that there were important number of students at low levels of awareness. There were significant differences in some cases about awareness level of information security between gender, average computer-internet usage experience by year. Contrary to expectations there were no significant difference between prospective teachers that had education about information security and prospective teachers that have no education about information

* Bu çalışma 19 Eylül 2014 tarihinde 8. Uluslararası Bilgisayar ve Öğretim Teknolojileri Sempozyumunda sunulan ve tam metin olarak bildiriler kitapçığında yer almayan aynı adlı bildirinin genişletilmiş ve geliştirilmiş halidir.

** Yrd. Doç. Dr, Sakarya Üniversitesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, oakgun@sakarya.edu.tr
*** Arş. Gör., Sakarya Üniversitesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, mtopal@sakarya.edu.tr

security. It is suggested to give inclusive and effective information security education to prospective teachers attending Educational Faculties.

Keywords: Information Technologies, Information Security, Information Security Awareness, Prospective Teachers

1. GİRİŞ

Hayatımıza sayısız kolaylık sağlayan bilişim teknolojileri geleneksel birçok uygulama ve hizmetin sunulmasında yer alırken aynı zamanda sağladığı üstünlükler sayesinde de gittikçe vazgeçilmez olmaktadır. Bilişim teknolojilerinden yararlanılan alanların gün geçtikçe artması birçok uygulama ve hizmeti elektronik ortama taşımaktadır. E-devlet, e-ticaret, e-belediye, e-öğrenme ve e-sağlık gibi uygulama ve hizmetler günlük yaşamımızın bir parçası haline gelmiştir (Dedeoğlu, 2006). Diğer yandan bilişim teknolojilerinin hayatımızda yaygın kullanımının artması bu teknolojilerin kolaylıklarının yanında bazı olumsuz yanlarını da beraberinde getirmektedir. Bilişim güvenliği konusu da bunlardan biridir. Bilişim teknolojilerini kullanarak işlemlerin gerçekleştirilmesi, depolama yapılması, iletişim kurulması, dijital ortamlarda bulunan bilginin güvenliğini dolayısı ile bilişim güvenliğini önemli bir hale getirmektedir (Yavuz ve Ulaş, 2013; Çalık ve Çınar, 2009).

Herkes tarafından erişilen bir bilginin güvenli bir biçimde gönderen ve alıcı arasında bütünlüğü bozulmadan, belli bir gizlilik içinde güvenli bir biçimde iletilmesi bilgi güvenliği olarak ifade edilebilir (ISO, 2005; Akt. Vural ve Sağıroğlu, 2008). Bilgi güvenliğinin üç temel unsuru; gizlilik, bütünlük ve kullanılabilirlik olarak ifade edilmektedir (Baykara, Daş ve Karadoğan, 2013). Gizlilik, bilginin yetkisiz erişiminin engellenmesini; bütünlük, bilginin yetkisiz kişilerce tahrip edilmesinin engellenmesini; kullanılabilirlik ise bilginin ihtiyaç olunduğunda erişilebilir olmasıdır (Baykara, Daş ve Karadoğan, 2013; Tekerek, 2008). Bilginin dijital ortamlarda depolandığı, iletildiği ve ulaşıldığı çağımızda bilgi güvenliği kavramı ve bilişim güvenliği kavramı artık içe içe hale geçmiştir.

Bilişim teknolojileri ve özellikle internet yasadışı yollarla diğer bireyler veya kurumlardan faydalanmak isteyen kötü niyetli kişilere şimdiye kadar benzeri görülmemiş olanaklar sağlamaktadır (Mann ve Sutton, 1998). Bilginin rahatlıkla açık hedef haline gelebildiği dijital ortamlarda (Pro-G, 2003) bilişim korsanları bu bilgilerin depolandığı ve kullanıldığı sistemlere zarar verebilmekte, sistemi kullanılmaz hale getirebilmekte ve bilgiler çalınabilmektedir. Bilişim suçu veya siber suç (Siber, 2013) olarak adlandırılabilen bu zararlı faaliyetler Gordon ve Ford'a göre (2006) genel olarak kötü niyetli kişiler tarafından bizzat yönlendirilen veya bu kişiler tarafından bilişim suçu işlemek amacıyla oluşturulmuş programlar kullanılarak kişisel bilgilerin edinilmesine yönelik sistemlerin açıkları ve zayıf yönlerinden yararlanılması ile gerçekleştirilir. Bu zararlı faaliyetlerin bir sonucu olarak kurumsal bilgilerin çalınması ve yasadışı yollarda kullanılması (Thomson ve Solms, 1998), kurum ve organizasyonlar için ekonomik anlamda kayıplar oluşturması (Gordon ve Loeb, 2002) gibi durumlar ortaya çıkarmakla birlikte kişisel kullanıcılar için de bilgilerin gizliliğinin ihlali ve ekonomik maddi kayıplar meydana getirebilmektedir (Cavusoglu, Cavusoglu ve Raghunathan, 2004). Bilişim güvenliğine yeteri kadar önem verilmediği takdirde, özellikle banka/kart bilgilerinin çalınması, telif hakkı ihlalleri, müstehcenlik, çocuk istismarı, kişisel verilerin çalınması ve internetteki yasa dışı yayınlar ülkemizde en sık rastlanan bilişim suçları arasındadır (İlbaş ve Köksal, 2011). Bu tip sorun ve kayıplarla karşı-

laşmamak için bilgi güvenliği dolayısı ile bilişim güvenliği konusunda önlemler almak, gerekirse kurumsal düzeyde potansiyel risklere karşı politikalar geliştirmek gereklidir (Whitman ve Mattord, 2012).

Türk Ceza Kanunu'nun (TCK) (2014) "Bilişim Alanında Suçlar" bölümünde (Onuncu bölüm) bilişim suçları genel olarak; bir bilişim sistemine hukuka aykırı yollarla girme, bir bilişim sistemini engelleme, bozma, sistemdeki verileri yok etme veya değiştirme, banka veya kredi kartlarının kötüye kullanılması olarak sınıflandırılmıştır. Avrupa Birliği Siber Suç Sözleşmesi'ne (**t.y.**) göre bilişim suçları veya siber suçlar; yasadışı erişim, yasadışı müdahale, verilere müdahale, sistemlere müdahale ve bu fiilleri gerçekleştirmeye yönelik araç ve yazılım geliştirme; bilişim teknolojileri kullanarak sahtecilik ve dolandırıcılık yapma, çocuk pornografisi, telif haklarının ihlal edilmesi, bilişim suçlarına yardım etmek veya azmettirmek olarak belirtilmektedir. Kurumsal ve bireysel olarak bilgilerin çalınması ve kötüye kullanılmasını içeren bu faaliyetler (Sağıroğlu ve Vural, 2008) çeşitli saldırı yöntemleri kullanarak gerçekleştirilmektedir (Canberk ve Sağıroğlu, 2006). Bu faaliyetler arasında şifre ve gizli soru tahmini, omuz sörfü ve çöpe dalma, virüsler, truva atları (trojens), solucanlar, tuş kaydedici yazılımlar (keylogger), ekran kaydedici yazılımlar (screenlogger), casus yazılımlar (spyware), reklam yazılımları (adware), istenmeyen postalar (spam), DoS (Denial of service) saldırıları, robot (bots) ve köle (zombie) yazılımlar, mantık bombaları, SQL enjeksiyon, arka kapılar (back doors), izleme (sniffing) ve gizleme (spoofing) (Gökmen, 2014) sayılabilir.

Computer Crime & Security (CSI, 2011: 17) kurumu tarafından gerçekleştirilen 2010/2011 yılı raporuna göre, 2005 ile 2010 yılları arasında gerçekleşen siber saldırı teknikleri ve bu tekniklerin kullanımının yıllara göre dağılımını aşağıdaki gibidir (Tablo 1).

Tablo 1. Computer Crime & Security Survey 2010/2011**,** 2005-2010 yılları arası gerçekleşen siber saldırı türlerinin dağılımı

Saldırı Türleri	2005	2006	2007	2008	2009	2010
Kötü Amaçlı Yazılım (Malware)	%74	%65	%52	%50	%64	%67
Kurum içi Yazılım Robotları (Bots)	2007'de eklendi		%21	%20	%23	%29
Oltalama (phishing) ile bilgilerin çalınması girişimi	2007'de eklendi		%26	%31	%34	%39
Parola dinleme (Password Sniffing)	2007'de eklendi		%10	%9	%17	%12
Finansal Sahtekarlık (Financial fraud)	%7	%9	%12	%12	%20	%9
Dos Atakları (Denial of service)	%32	%25	%25	%21	%29	%17
Verilerin çalınması ve saldırı tehlikesi ile şantaj ve zorbalık	2009'da eklendi				%3	%1
Web site saldırıları	%5	%6	%10	%6	%14	%7
Kamusal sayfalara yetkisiz erişim	2009'da eklendi				%6	%7
Kablosuz ağlara yetkisiz erişim	%16	%14	%17	%14	%8	%7
DNS Sunuculara yetkisiz erişim	2007'de eklendi		%6	%8	%7	%2
İstemci web tarayıcılarına yetkisiz erişim	2009'da eklendi				%11	%10
Kullanıcıların sosyal ağ profillerine yetkisiz erişim	2009'da eklendi				%7	%5
Anlık mesajlaşma suiistimalleri	2007'de eklendi		%25	%21	%8	%5
Kurum içi güvenlik ve yetki suiistimalleri	%48	%42	%59	%44	%30	%25
Yetkisiz erişim veya sistem içi imtiyazların artışı	2009'da eklendi				%15	%13

Sistemlere dışarda sızma	2009'da eklendi				%14	%11
Dizüstü veya mobil cihazların çalınması/yitirilmesi	%48	%47	%50	%42	%42	%34
Mobil cihazların çalınması/yitirilmesi sonucu kişisel bilgilerin çalınması/yetkisiz erişim	2008'de eklendi			%8	%6	%5
Mobil cihazların çalınması/yitirilmesi sonucu fikri mülkiyete taciz	2008'de eklendi			%4	%6	%5
Diğer nedenlerden dolayı kişisel bilgilerin çalınması/yetkisiz erişim	2008'de eklendi			%8	%10	%11
Diğer nedenlerden dolayı fikri mülkiyete taciz	2008'de eklendi			%5	%8	%5

Tablo 1'de görüldüğü gibi gerçekleşme oranı görece yüksek olan: Kötü amaçlı yazılım (Malware), DoS atakları (Denial of service), oltalama (phishing), kurum içi suiistimaller, dizüstü veya mobil cihaz kaynaklı siber suçlar gibi siber saldırılar kullanıcıların önlem alarak kendilerini koruyabilecekleri nitelikte saldırılardır. Symantec tarafından gerçekleştirilen internet güvenliği tehditleri raporunda da belirtildiği gibi güncel güvenlik yazılımlarının kullanılması dışında alınabilecek en önemli önlemlerden biri de bilişim güvenliği ve siber saldırılar konusunda kullanıcıların bilgilendirilmesidir (Symantec, 2014; Şahinaslan, Kandemir ve Şahinaslan, 2009). Çoğunlukla insan faktörüne bağlı olan (Wagner ve Brooke, 2007) bilgi ve bilişim güvenliği risklerini en düşük seviyeye çekebilmek kullanıcıların bilgi ve bilişim güvenliği ilkelerine uygun davranması ile sağlanabilir (Şahinaslan, Kaantürk, Şahinaslan ve Borandağ, 2009).

Eğitim kurumları bilişim güvenliği farkındalığının oluşturulmasında oldukça önemli görülmektedir. Eğitim fakültelerinde yürütülen öğretmen yetiştirme programları incelendiğinde bazı Bilgisayar ve Öğretim Teknolojileri Eğitimi programlarında bilişim güvenliği konusu ile ilgili dersler olduğu, diğer öğretmenlik programlarında ise bu tür dersler olmadığı dikkat çekmektedir. Ülkemizde Fırsatları Artırma ve Teknolojiyi İyileştirme Hareketi (FATİH) projesi ile beraber eğitim kurumlarında bilişim teknolojilerinin kullanımın yoğunluğunun arttığı tüm öğretmen ve öğrencilere tabletlerin dağıtıldığı bu dönemde eğitim kurumlarında görev yapacak öğretmenlerin ve öğretmen adaylarının bilişim güvenliği ile ilgili farkındalık düzeyleri önemli bir konu haline gelmektedir.

Bu bağlamda araştırmanın amacı eğitim fakültesi son sınıf öğrencilerinin bilişim güvenliği farkındalıklarını incelemektir. Bu amaç bağlamında aşağıdaki sorulara yanıt aranmıştır.

Eğitim fakültesi son sınıf öğrencilerinin;

1) Bilişim güvenliği ile ilgili:
a) Parola
b) İnternetten alış-veriş
c) Bilgisayar kullanıcı hesapları güvenliği
d) Anti-virüs ve zararlı yazımları engelleme
e) Güncelleme
f) Sosyal ağ
g) Eposta ve anlık mesajlaşma yazılımları
h) Kablosuz ağlar
i) Yasal ve etik konular
j) Bilgilerini güncelleme, ilkelerine uyma farkındalık düzeyleri nedir?
2) Öğrencilerin bilişim güvenliği düzeyleriyle ilgili yanıtlarının seçeneklere dağılımı:
a) Cinsiyet
b) Bilgisayar ve internet kullanım yılı
c) Bilişim güvenliği ile alakalı bir eğitim alıp almama durumu, değişkenlerine göre anlamlı farklılık göstermekte midir?
3) Bilişim güvenliği ile ilgili olarak katılımcılar:

a) Bir alış-veriş sitesinden alış-veriş yaparken sitenin hangi özelliklerine dikkat etmektedirler?
b) Parola belirlerken parolanın hangi özellikleri olmasına dikkat etmektedirler?
c) Bir yazılıma ihtiyaç duyduklarında nasıl temin etmektedirler?
d) Bilişim güvenliği konusunda bilgi aldıkları kaynaklar nelerdir?

2. YÖNTEM

Bu çalışma belirlenmiş bir kitleden veri toplayarak kitlenin özelliklerini ortaya koymaya yöneliktir. Bu nedenle araştırmanın modeli kesitsel tarama modelidir. Kesitsel araştırmalarda değişkenler betimlenmek üzere bir tek seferde ölçülür (Büyüköztürk, Kılıç Çakmak, Akgün, Karadeniz ve Demirel, 2012). Araştırma kapsamında geliştirilen ankette farkındalık düzeyleri incelenmiş ayrıca anket sonunda yer verilen açık uçlu sorularla katılımcıların bilişim güvenliğinde dikkat ettikleri konular belirlenmeye çalışılmıştır.

2.1 Katılımcılar

Bu araştırmanın evrenini Sakarya Üniversitesi Eğitim Fakültesi Bilgisayar ve Öğretim Teknolojileri Eğitimi (BÖTE), İlköğretim Matematik Eğitimi (İME), Türkçe Eğitimi (TRE) ve Zihin Engelliler Eğitimi (ZEÖ) 1. öğretim programlarında okuyan toplam 259 son sınıf lisans öğrencisi oluşturmaktadır. Araştırma evreninde konu alanı uzmanlığı olması beklenen BÖTE bölümü öğrencilerinin yanı sıra bir sayısal, bir sözel ve bir eşit ağırlık programının yer almasına dikkat edilmiştir. Araştırma kapsamında bu evren biriminin tamamına anket ulaştırılmıştır. Anketi gönüllü olarak doldurarak çalışmaya 212 kişi katılmıştır. Analizler 212 kişinin verileri üzerinden yapılmıştır. Örneklemin bölümlere göre dağılımı şu şekildedir: BÖTE 64, İME 39, TRE 74, ZEÖ 35.

2.2 Veri Toplama Aracı

Bu çalışmada veri toplama aracı olarak araştırmacılar tarafından geliştirilen "Bilişim Güvenliği Anketi" kullanılmıştır. Anket geliştirilirken alan yazındaki araştırmalardan ve kullanıcı sayısı en yüksek (donanımhaber, shiftdelete.net, chip.com.tr gibi) forumlarda paylaşılan bilişim güvenliği ile ilgili sorunlardan yola çıkarak bir madde havuzu oluşturulmuştur. Özellikle Kritzinger ve Smith'in (2008) temel bilgi güvenliği ilkelerinden yola çıkılarak sorular kategorilere ayrılmıştır. Güvenlik duvarları ve saldırı önleme/sezme sistemleri ilkesi için "Anti-virüs ve zararlı yazılımları engelleme" ve "Güncelleme" başlıkları altında; şifreleme yöntemleri, parola güvenliği ve bireysel parola güvenliği ilkeleri için "Parola" başlığı altında; erişim/yetki kontrolü ilkesi için "Bilgisayar kullanıcı hesapları güvenliği" başlığı altında; yasal yönler ve etik ilkesi için "Yasal ve etik konular" başlığı altında; bilgi güvenliği ve gizliliği kültürü ilkesi için "Bilgilerini güncelleme (bilişim güvenliği ile ilgili)" başlığı altında alan yazın ve forumlarda özellikle son kullanıcıların yaşadığı sorunlar dikkate alınarak anket soruları hazırlanmıştır. Sosyal ağ, eposta ve anlık mesajlaşma yazılımları, kablosuz ağlar başlığı altındaki sorular ise daha çok forumlarda yer alan son kullanıcı sorunları dikkate alınarak hazırlanıp araştırmacılar tarafından eklenmiştir. Anketin kapsam geçerliliği için oluşturulan bu maddelerle ilgili bilişim güvenliği konusunda çalışmış beş alan uzmanından ve ayrıca bir Türkçe uzmanından uzman görüşü alınmıştır. Yeniden düzenlenen bu form 48'i 5'li likert tipi 18'i demografik ve kullanım alışkanlıklarını belirlemeye yönelik toplam 66 sorudan oluşmuştur. Likert tipi hazırlanan soruların yanıt seçenekleri öğrencilerin "Benim için kesinlikle doğru", "Benim için doğru", "Benim için doğru olup olmadığından emin değilim", "Benim için doğru değil" ve "Benim için kesinlikle doğru değil" şeklinde kendilerini

yakın hissettikleri düzeyde yanıt verebilmeleri için düzenlenmiştir. Anketteki Likert tipi sorular 10 bilişim güvenliği konu başlığı altında toplanmıştır. Bu başlıklar ve soru sayılarının dağılımı şu şekildedir:

- Parola (8 soru)
- İnternetten alış-veriş (3 soru)
- Bilgisayar kullanıcı hesapları güvenliği (5 soru)
- Anti-virüs ve zararlı yazılımları engelleme (6 soru)
- Güncelleme (3 soru)
- Sosyal ağ (5 soru)
- Eposta ve anlık mesajlaşma yazılımları (7 soru)
- Kablosuz ağlar (3 soru)
- Yasal ve etik konular (3 soru)
- Bilgilerini güncelleme (bilişim güvenliği ile ilgili) (5 soru)

Geliştirilen bu anketten toplam puan elde edilmemektedir. Her bir soru o soruda ölçülmek istenen özellikle ilgili gerçek durumu ortaya koymaya yöneliktir. Anketin kapsam geçerliği için uzman görüşü temel alınmıştır. Uzmanlar farkındalık düzeyini ölçmeyi hedefleyen tüm soruları ve dolayısıyla anketi kapsam geçerliği açısından yeterli bulmuşlardır. Likert tipi 48 maddenin güvenirliği için Cronbach Alfa iç tutarlık katsayısı hesaplanarak değer .87 bulunmuştur. Maddelerden herhangi biri atıldığında Alfa değeri yükselmemektedir. Bu bulgular anketin güvenilir kabul edilebileceğini göstermektedir (Büyüköztürk, 2012).

2.3 Verilerin Analizi

Veriler aşağıda belirtilen üç kategori altında analiz edilmiştir.

1. Ankette yer alan maddelerin toplandığı 10 konu başlığına yönelik soruların yanıtları ayrı ayrı başlıklar altında verilerek yüzde ve frekans ile betimlenmiştir. Bu bulgular verilirken okumayı ve yorumlamayı kolaylaştırmak amacıyla "Benim için kesinlikle doğru" ile "Benim için doğru" yanıtları birleştirilerek "Benim için doğru" şeklinde; "Benim için doğru değil" ile "Benim için kesinlikle doğru değil" yanıtları da birleştirilerek "Benim için doğru değil" başlığı altında sunulmuştur.
2. Aşağıdaki değişkenlere göre katılımcıların yanıtlarının farklılaşıp farklılaşmadığı iki değişkenli ki-kare ile incelenmiştir.
   a) Cinsiyet,
   b) Bilgisayar ve Internet kullanım yılı,
   c) Bilişim güvenliği ile alakalı bir eğitim alıp almama durumu.
3. Açık uçlu sorulara yönelik verilen yanıtlardan elde edilen temalar ve bunların frekanslarına ait bulgular içerik analizi yapılarak sunulmuştur.

3. BULGULAR

Bulgular ankette yer alan maddelerin kategorilendirildiği yukarda belirtilen 10 başlık altında sunulmuştur.

3.1.1 Parola Sorularına Verilen Yanıtlara Ait Bulgular

Katılımcıların parola güvenliği ile ilgili verdikleri yanıtlar Tablo 2'de sunulmuştur.

Tablo 2. Parola Sorularına Verilen Yanıtlara Ait Frekans ve Yüzdelikler

Soru		f	%
S1- Farklı e-posta adreslerim için aynı parolayı (şifreyi) kullanırım.	Benim için doğru	129	59,5
	Kararsızım	13	6,0
	Benim için doğru değil	75	34,5

S2 - Farklı sitelere üye olurken aynı kullanıcı adı ve parolayı kullanırım.	Benim için doğru	129	60,0
	Kararsızım	15	7,0
	Benim için doğru değil	71	33,0
S7 - İnternette parolamı yazarken yakın arkadaşlarımın parolamı görmesi benim için sorun değildir.	Benim için doğru	109	50,7
	Kararsızım	32	14,9
	Benim için doğru değil	74	34,4
S8 - Güvendiğim insanlara kullanıcı adı ve şifremi veririm.	Benim için doğru	125	54,3
	Kararsızım	25	11,7
	Benim için doğru değil	64	30
S13 - Parolamı yönetmek (saklamak) için bir bilgisayar yazılımı kullanırım.	Benim için doğru	37	17,5
	Kararsızım	25	11,8
	Benim için doğru değil	150	70,7
S28 - Parolamı belirli zaman aralıklarında değiştiririm.	Benim için doğru	93	43,3
	Kararsızım	36	16,7
	Benim için doğru değil	86	40,0
S43 - Nasıl güvenli bir parola belirleyeceğim hakkında bilgi sahibiyim.	Benim için doğru	149	71,6
	Kararsızım	27	13,0
	Benim için doğru değil	32	15,4
S44 - Parola güvenliğinin zayıf, orta, yüksek olmasının parolamın güvenliğini nasıl etkilediğini biliyorum.	Benim için doğru	152	73,8
	Kararsızım	27	13,1
	Benim için doğru değil	27	13,1

Tablo 2'deki değerler incelendiğinde, öğrencilerin yaklaşık %60'ının farklı site üyelikleri ve eposta adresleri için aynı kullanıcı adı ve şifreyi kullandıkları ve %54,3 oranında arkadaşlarına ve güvendikleri insanlara parolalarını gösterdikleri ve söyledikleri görülmektedir. Bu durum öğrencilerin çoğunluğunun parola kullanımı konusunda güvenlik açığı olduğunu bu konuda farkındalıklarının düşük olduğunu göstermektedir. Diğer yandan katılımcıların %71,6'sının nasıl güvenli bir parola belirleyecekleri hakkında bilgi sahibi olduklarını düşündükleri görülmektedir. Ayrıca, katılımcıların %70,7 oranında parolalarını saklamak ve yönetmek için bilgisayar yazılımı kullanmadıklarını ve parolalarını belirli zaman aralıkları ile değiştirmenin öneminin farkında olanlar (%43,3) ile olmayanlar (%40) arasında ciddi bir fark olmadığı görülmektedir. Ancak parola belirlemek ve gizlemek ile ilgili diğer sorular olan 1, 2, 7, 8, 13'ün yanıtları incelendiğinde, oranların çeliştiği, öğrencilerin parola konusu ile ilgili farkındalıklarının az olduğu söylenebilir.

3.1.2 İnternetten Alış-Veriş Sorularına Verilen Yanıtlara Ait Bulgular

Katılımcıların internetten alış-veriş yaparken dikkat ettikleri özelliklere yönelik sorulara verdikleri cevaplar Tablo 3'te sunulmuştur.

Tablo 3. İnternetten Alış-Veriş Sorularına Verilen Yanıtlara Ait Frekans ve Yüzdeler

Soru		f	%
S4 - Kişisel bilgisayarımın dışındaki bilgisayarlar üzerinden internet aracılığı ile alış veriş yaparım.	Benim için doğru	62	28,6
	Kararsızım	28	13,0
	Benim için doğru değil	126	54,8
S5 - İnternette alış-veriş yaparken internetten ödeme güvenliği hakkında nelere dikkat etmem gerektiğini bilirim.	Benim için doğru	146	68,9
	Kararsızım	31	14,6
	Benim için doğru değil	35	16,5

S6 - Kredi kartım ile ilgili önemli bilgileri girerken eğer varsa sanal klavye kullanırım.	Benim için doğru	90	42,6
	Kararsızım	43	20,4
	Benim için doğru değil	78	37,0

Tablo 3'teki internetten alış-veriş yapma ile ilgili katılımcıların verdikleri yanıtlar incelendiğinde bilişim güvenliği ilkelerine uygun olarak %68,9 oranında internetten alış-veriş yaparken ödeme güvenliği hakkında yeterli bilgi sahibi olduklarını belirttikleri ve %54,8 oranında kişisel bilgisayarları dışında internetten alış-veriş yapmadıkları görülmektedir. Diğer yandan, internetten alış-veriş yaparken sanal klavye kullanımının öneminin, farkında olanlar (%42,6) ve olmayanların (%37) oranları birbirine yakındır. Bu nedenlerden dolayı öğrencilerin internetten alış-veriş konusunda nelere dikkat edecekleri konusunda genel olarak farkındalık sahibi oldukları, ancak sanal klavye kullanımı konusunda bilgi sahibi olmadığını belirten %37'lik bir grubun olduğu kararsızlarla birlikte oranının %57,4 olduğu söylenebilir. Ortaya çıkan bu sonuç farkındalık sahibi olanlar bulunmakla birlikte bir eğitim gereksinimi de olduğuna işaret etmektedir.

3.1.3 Bilgisayar Kullanıcı Hesapları Güvenliği Sorularına Verilen Yanıtlara Ait Bulgular

Katılımcıların bilgisayar kullanıcı hesapları güvenliği ile ilgili sorulara verdikleri cevaplar Tablo 4'te sunulmuştur.

Tablo 4. Bilgisayar Kullanıcı Hesapları Güvenliği Sorularına Verilen Yanıtlara Ait Frekans ve Yüzdelikler

Soru		f	%
S3 - Bana ait olmayan bir bilgisayardan internete girerken, tarayıcının kişisel bilgilerimi kaydedip kaydetmediğini kontrol ederim.	Benim için doğru	173	79,8
	Kararsızım	20	9,2
	Benim için doğru değil	24	11,1
S9 - Bilgisayarımda bir açılış parolası kullanırım.	Benim için doğru	131	60,6
	Kararsızım	22	10,2
	Benim için doğru değil	63	29,2
S10 - Bilgisayarımı kullanmak isteyen kişiler için açtığım, ayrı, sınırlı bir oturum vardır.	Benim için doğru	58	27,0
	Kararsızım	16	7,4
	Benim için doğru değil	141	65,6
S11 - Bilgisayarımda kendi oturumumdaki önemli belgeler şifreli haldedir.	Benim için doğru	72	34,0
	Kararsızım	25	11,8
	Benim için doğru değil	115	54,2
S12 - Bilgisayarımı kullanmak isteyen olursa sadece konuk oturumunu kullanmasına izin veririm.	Benim için doğru	154	72,0
	Kararsızım	19	8,9
	Benim için doğru değil	41	19,1

Katılımcıların bilgisayar kullanıcı güvenliği ile ilgili verdikleri yanıtlar incelendiğinde (bkz. Tablo 4) %65,6 oranında öğrencilerin kendi bilgisayarlarını kullanmak isteyenler için misafir veya konuk oturumu kullanmadığı ve %54,2 oranında öğrencilerin bilgisayarında önemli belgelerin şifreli olmadığı görülmektedir. Diğer yandan yanıtların %79,8'i öğrencilerin başka bir bilgisayardan internete girerken tarayıcının kişisel bilgilerini kaydedip kaydetmediğini kontrol ettiği ve %60,6 oranında bilgisayarlarında açılış parolası kullandıklarını ifade etmektedirler. Öğrenciler bir taraftan konuk oturumlarının olmadığını belirtirken (%65,6) diğer taraftan bilgisayarlarını başkasına verirken konuk oturumunda verdiklerini belirtmek-

tedirler (%72). Bu durum öğrencilerin bu konuda çelişen yanıtların olduğunu göstermektedir.

3.1.4 Anti-Virüs ve Zararlı Yazılımları Engelleme Sorularına Verilen Yanıtlara Ait Bulgular

Katılımcıların anti-virüs ve zararlı yazılımları engelleme konularıyla ilgili sorulara verdikleri yanıtlar Tablo 5'te sunulmuştur.

Tablo 5. Anti-Virüs ve Zararlı Yazılımları Engelleme Sorularına Verilen Yanıtlara Ait Frekans ve Yüzdelikler

Soru		f	%
S21 - İnternetten bilgisayarıma indirdiğim dosyaları açmadan önce virüs taramasından geçiririm.	Benim için doğru	113	52,8
	Kararsızım	43	20,1
	Benim için doğru değil	58	27,1
S22 - USB Bellek, harici disk veya cd-dvd medyası bilgisayarıma bağlandığında öncelikle anti-virüs taramasından geçiririm.	Benim için doğru	125	68,2
	Kararsızım	36	16,7
	Benim için doğru değil	54	25,1
S29 - Bilgisayarımı belli zaman aralıklarında güvenlik taramasından geçiririm.	Benim için doğru	130	61,0
	Kararsızım	39	18,3
	Benim için doğru değil	34	20,7
S35 - İnternet kaynaklı tehditler ile ilgili yeterli bilgiye sahibim.	Benim için doğru	105	49,1
	Kararsızım	65	30,4
	Benim için doğru değil	44	10,5
S42 - İnternet tarayıcım vasıtasıyla internette gezindiğim web sitelerinin güvenirliği ile ilgili bilgi edinmeye çalışırım.	Benim için doğru	92	45,5
	Kararsızım	58	28,0
	Benim için doğru değil	57	27,5
S48 - Bilgisayarın güvenliğini sağlayacak yazılımları bulma ve kullanmada yeterli bilgiye sahibim.	Benim için doğru	101	49,5
	Kararsızım	53	26,0
	Benim için doğru değil	50	24,5

Tablo 5'te öğrencilerin verdikleri yanıtlar incelendiğinde bilişim güvenliği ilkelerine uygun olarak, öğrencilerin yarıdan fazlasının virüs taraması yapma konusunda farkındalık sahibi oldukları görülmektedir. Diğer yandan internet kaynaklı tehditler (%49,1) ve bilişim güvenliği sağlayacak yazılımları bulma ve kullanma konusunda yeterli olduğunu düşünenler (%49,5) ile internet kaynaklı tehditler konusunda yetersiz ve kendinden emin olmayanların toplam oranı (%40,9) ve bilişim güvenliği sağlayacak yazılımları bulma ve kullanma konusunda yetersiz ve kendinden emin olmayanların toplam oranı (%50,5) birbirine yakındır. Bu nedenle dikkate alınır düzeyde farkındalığın düşük olduğu ve bu konularda bilgi eksikliği olabileceği söylenebilir.

3.1.5 Güncelleme Sorularına Verilen Yanıtlara Ait Bulgular

Katılımcıların işletim sistemi, güvenlik yazılımı ve ofis yazılımlarının güncellemesi ile ilgili sorulara verdikleri yanıtlar Tablo 6'da sunulmuştur.

Tablo 6. Güncelleme Sorularına Verilen Yanıtlara Ait Frekans ve Yüzdelikler

Soru		f	%
S14 - Kullandığım anti-virüs yazılımının güncelliğini denetlerim.	Benim için doğru	136	63,8
	Kararsızım	23	10,8
	Benim için doğru değil	54	25,4

S15 - İşletim sistemi güncellemelerini kontrol eder ve zamanında yüklerim.	Benim için doğru	112	52,4
	Kararsızım	36	16,8
	Benim için doğru değil	54	30,8
S16 - Kullandığım ofis yazılımlarının güncellemelerini denetlerim.	Benim için doğru	112	53,5
	Kararsızım	39	18,7
	Benim için doğru değil	58	27,8

Güncelleme konusu ile ilgili bulgulara bakıldığında (bkz. Tablo 6) genel olarak öğrencilerin yarıdan fazlasının güncelleme ile ilgili konularda farkındalık sahibi oldukları ve güncelleme ile ilgili hususlara dikkat ettikleri görülmektedir. Bununla birlikte kararsız olanların ve olumsuz yanıt verenlerin %25-%31 dolaylarındaki oranı bu konuda önemli düzeyde farkındalık eksikliği yaşayan katılımcılar olduğunu göstermektedir.

3.1.6 Sosyal Ağ Sorularına Verilen Yanıtlara Ait Bulgular

Katılımcıların sosyal ağ konularıyla ilgili sorularına verdikleri yanıtlar Tablo 7'de sunulmuştur.

Tablo 7. Sosyal Ağ Sorularına Verilen Yanıtlara Ait Frekans ve Yüzdelikler

Soru		f	%
S18 - Sosyal ağ sitelerinde tanımadığım insanları arkadaş listeme eklerim.	Benim için doğru	36	17,0
	Kararsızım	17	8,0
	Benim için doğru değil	159	75,0
S19 - Sosyal ağlarda kişisel bilgilerimi paylaşırım.	Benim için doğru	39	18,8
	Kararsızım	35	16,8
	Benim için doğru değil	134	64,4
S26 - Sosyal ağlarda tanıştığım insanlarla yüz yüze buluşurum.	Benim için doğru	46	21,5
	Kararsızım	26	12,1
	Benim için doğru değil	142	66,4
S27- Kişisel fotoğraf ve videolarımı herkesin erişebileceği ortamlarda paylaşırım.	Benim için doğru	51	23,8
	Kararsızım	28	13,1
	Benim için doğru değil	135	63,1
S40 - Sosyal medya platformlarında bulunan kullanıcı hesaplarımın gizlilik ayarlarını yönetebilecek bilgiye sahibim.	Benim için doğru	139	67,8
	Kararsızım	34	16,6
	Benim için doğru değil	32	15,6

Tablo 7'deki öğrencilerin verdikleri yanıtlar incelendiğinde öğrencilerin %60'ından fazlasının sosyal ağlardaki gizlilik ve kişisel bilgilerin korunması ile alakalı konuları önemsedikleri ve bu konularla ilgili düzenlemeleri kişisel sosyal ağ hesaplarında yapabildikleri görülmektedir. Bu sorulara verilen yanıtlar öğrencilerin sosyal ağlarda gizlilik ve güvenlik konusunda diğer konulara göre daha duyarlı olduklarını göstermektedir. Bununla birlikte diğer başlıklara oranla daha az olsa da %16 - %24 dolaylarında farkındalık eksikliği bulunan dikkate alınır düzeyde öğrenci bulunmaktadır.

3.1.7 Eposta ve Anlık Mesajlaşma Yazılımları Güvenliği Sorularına Verilen Yanıtlara Ait Bulgular

Katılımcıların e-posta kullanımı ve anlık mesajlaşma yazılımı kullanımı güvenliği ile ilgili sorulara verdikleri yanıtlar Tablo 8'de sunulmuştur.

Tablo 8. Eposta ve Anlık Mesajlaşma Yazılımları Güvenliği Sorularına Verilen Yanıtlara Ait Frekans ve Yüzdelikler

Soru		f	%
S17 - Anında ileti yazılımı kullanarak benimle dosya paylaşıldığında gelen dosya ile ilgili bilgim yoksa gönderen kişiye sormadan dosyayı açmam.	Benim için doğru	104	49,3
	Kararsızım	54	25,6
	Benim için doğru değil	33	25,1
S20 - Gönderenini tanımadığım bir epostaya eklenmiş dosyayı anti-virüs taramasından geçirmeden açarım.	Benim için doğru	59	24,7
	Kararsızım	38	17,7
	Benim için doğru değil	118	54,6
S30 - Göndereni tanımasam da tepkimi çeken postaları yanıtlarım.	Benim için doğru	53	35,0
	Kararsızım	35	16,5
	Benim için doğru değil	174	58,5
S31 - Anında ileti yazılımları kullanırken yazışmaları arşivlerim.	Benim için doğru	52	24,9
	Kararsızım	42	19,9
	Benim için doğru değil	107	50,2
S34 - Eposta adresime gelen sahte içerikli postaları ''Spam'' olarak işaretlerim.	Benim için doğru	114	49,3
	Kararsızım	44	21,1
	Benim için doğru değil	41	19,6
S37 - Eposta adresim kötü niyetli kişilerin eline geçerse, nasıl geri alabileceğim konusunda bilgi sahibiyim.	Benim için doğru	83	39,5
	Kararsızım	58	27,6
	Benim için doğru değil	69	32,9
S38 - Göndereni tanımadığım halde ilgimi çeken epostaları yanıtlarım.	Benim için doğru	53	25,4
	Kararsızım	27	12,9
	Benim için doğru değil	129	61,7

Tablo 8'de yer alan değerler incelendiğinde öğrencilerin çoğunun bilişim güvenliği ilkelerine uygun olarak gönderenini tanımadıkları eposta ve dosyaları anti-virüs taramasından geçirmeden açmadıklarını (%49,3), göndereni tanımadıkları mesajları yanıtlamadıklarını belirttikleri (%58,5) görülmektedir. Diğer yandan öğrencilerin eposta adresleri kötü niyetli kişilerin eline geçerse, nasıl geri alabilecekleri konusunda önemli oranda kararsız (%27,6) ve yeterli bilgi sahibi olmadıkları (%32,9) görülmektedir. Bu başlık altında alınan yanıtlar birlikte dikkate alındığında güvenlik konularına dikkat edenlerin yanıtları ile kararsız olan ve olumsuz yanıtların toplam oranı birbirine yakın çıkmaktadır. Bu bulgu önemli sayıda öğrencinin e-posta ve anlık ileti güvenliğine dikkat ettiği bununla birlikte tehditlerin farkında olmayan önemli düzeyde katılımcı olduğu şeklinde yorumlanabilir.

3.1.8 Kablosuz Ağ Güvenliği Sorularına Verilen Yanıtlara Ait Bulgular

Katılımcıların kablosuz ağ güvenliği ile ilgili sorulara verdikleri yanıtlar Tablo 9'da sunulmuştur.

Tablo 9. Kablosuz Ağ Güvenliği Sorularına Verilen Yanıtlara Ait Frekans ve Yüzdelikler

Soru		f	%
S23 - Cep telefonum ya da bilgisayarım ile kaynağını/sahibini bilmediğim kablosuz ağlara bağlanırım.	Benim için doğru	70	39,4
	Kararsızım	31	14,5
	Benim için doğru değil	113	48,1
S32- Şifrelenmemiş ve kimin sağladığını bilmediğim kablosuz ağlara bağlanırım.	Benim için doğru	70	32,7
	Kararsızım	30	14,0
	Benim için doğru değil	114	53,3

S33 - Kablosuz internet ağımda şifre kullanmam.	Benim için doğru	30	13,1
	Kararsızım	24	11,3
	Benim için doğru değil	159	74,6

Öğrencilerin verdikleri yanıtlar incelendiğinde öğrenci yanıtlarının yarıdan fazlasının, sahibini bilmedikleri ve şifresiz kablosuz ağlara bağlanmadıkları (%48,1) kablosuz ağlarını şifre ile kullandıkları (%75) ve güvenilir olduğundan emin olmadıkları ağlara bağlanmadıkları (%53,3) görülmektedir. Bununla birlikte %39,4 oranında katılımcının kaynağını bilmediği ağlara bağlandığını %32,7 oranında katılımcının da şifrelenmemiş ağlara bağlandığını belirtmesi önemli bir güvenlik açığı olarak dikkat çekmektedir.

3.1.9 Bilişim Güvenliği ile İlgili Yasal ve Etik Konular Sorularına Verilen Yanıtlara Ait Bulgular

Katılımcıların bilişim güvenliğine yönelik yasal ve etik konularla alakalı sorulara verdikleri yanıtlar Tablo 10'da sunulmuştur.

Tablo 10. Bilişim Güvenliği ile İlgili Yasal ve Etik Konular Sorularına Verilen Yanıtlara Ait Frekans ve Yüzdelikler

Soru		f	%
S24 - Bilgisayarımdaki yazılımları lisans bedellerini ödeyerek satın aldıktan sonra kullanırım.	Benim için doğru	49	23,5
	Kararsızım	54	25,8
	Benim için doğru değil	106	50,7
S25- Bilgisayarımda yasa dışı yolla edinilmiş (kırılmış) yazılımlar bulunmaktadır.	Benim için doğru	78	37,0
	Kararsızım	34	16,1
	Benim için doğru değil	99	46,9
S39 - Yazılım kullanmada telif hakları konusunda yeterli bilgi sahibiyim.	Benim için doğru	82	40,6
	Kararsızım	61	30,2
	Benim için doğru değil	59	29,2

Öğrencilerin yasal ve etik konularla ilgili verdikleri yanıtlar incelendiğinde (bkz. Tablo 10) yazılım telif hakkı konusunda bilgi sahibi olduğunu belirtenlerin oranı (%40,6), bilgi sahibi olmadığını (%29,2) veya emin olmadığını (%30,2) belirten kişilerin toplam oranından azdır. Bu bulgu öğrencilerin bu konuda yeteri kadar farkındalık sahibi olmadığının bir işareti olabilir. Yasal yolla edinilmemiş yazılımların kullanım oranı (%37) lisanslı yazılım kullanım oranından (%23,5) yüksek görünmektedir. Bilişim teknolojilerinin kanuni ve etik kullanımı konusunda önemli düzeyde bilgilendirme ihtiyacı olduğu ve bu konuda farkındalığın az olduğu görülmektedir.

3.1.10 Bilişim Güvenliği ile İlgili Bilgilerini Güncelleme Sorularına Verilen Yanıtlara Ait Bulgular

Öğrencilerin bilişim güvenliğiyle ilgili bilgilerini yenilemeye yönelik sorulara verdikleri yanıtlar Tablo 11'de sunulmuştur.

Tablo 11. Bilişim Güvenliği ile İlgili Bilgilerini Güncelleme Sorularına Verilen Yanıtlara Ait Frekans ve Yüzdelikler

Soru		f	%
S36 - Kullandığım internet tarayıcısının güvenlik ayarları hakkında yeterli bilgi sahibiyim.	Benim için doğru	130	61,9
	Kararsızım	50	23,8
	Benim için doğru değil	30	14,3
S41 - İnternet tarayıcım vasıtasıyla internette gezindiğim web sitelerinin güvenirliği ile ilgili bilgi edinmeye çalışırım.	Benim için doğru	133	64,0
	Kararsızım	47	22,5
	Benim için doğru değil	28	13,5

S45 - Bilişim güvenliği konusunda bilgi alabileceğim adresleri bilirim.	Benim için doğru	99	47,9
	Kararsızım	64	30,9
	Benim için doğru değil	44	21,2
S46 - Bir bilişim suçuna maruz kalırsam kime başvuracağımı biliyorum.	Benim için doğru	94	45,4
	Kararsızım	57	27,5
	Benim için doğru değil	54	27,1
S47 - Bir bilişim güvenliği sitesini düzenli olarak takip ederim.	Benim için doğru	51	24,6
	Kararsızım	61	29,5
	Benim için doğru değil	95	45,9

Öğrencilerin Tablo 11'de verdikleri yanıtlar incelendiğinde öğrenci yanıtlarının %61,9'unun kullandıkları web tarayıcısının güvenlik ayarlarını ve web tarayıcıları aracılığı ile girdikleri sitelerin güvenilirliğini test etmede bilgi sahibi olduklarını belirttikleri görülmektedir. Diğer yandan öğrencilerin bilişim suçuna maruz kaldıklarında veya bilişim güvenliği ile ilgili bir konuda nereye danışacaklarını bilme oranları (%45,4) ile bilmeme (%27,1) ile emin olmama (%27,5) oranlarının toplamı (%55,6) arasında bilgi eksikliği lehine bir oran dikkat çekmektedir. Benzer durum düzenli bir şekilde bir bilişim güvenliği web sitesini takip etme açısından da görülmektedir. Bu nedenle öğrencilerin bu konuda yeteri kadar farkındalık sahibi olmadıkları ve öğrencilerin bilgilerini güncelleme ve bir siber suçla karşı karşıya kaldıklarında kime başvuracaklarını bilme açısından eksikliklerinin olduğu söylenebilir.

3.2.1 Cinsiyetine Göre Verilen Yanıtların Dağılımının Farklılık Gösterdiği Sorulara İlişkin Bulgular

Katılımcıların verdikleri yanıtlar cinsiyet değişkenine göre çaprazlandığında dağılımın anlamlı farklılık gösterdiği sorular Tablo 12'de verilmiştir.

Tablo 12. Cinsiyete Göre Kay-Kare Testi Sonuçları

Soru		Kız %	Erkek %	χ^2	sd	p
S23 – Cep telefonu ya da bilgisayar ile kaynağını/sahibini bilmediğim kablosuz ağlara bağlanırım.	Benim için doğru	28,2	**48,8**	13,58	4	,008
	Kararsızım	12,9	17,4			
	Benim için doğru değil	**58,9**	33,8			
S26 – İnternette, sosyal ağlarda, anında ileti yazılımlarıyla tanıştığım bir insan ile yüz yüze görüşürüm.	Benim için doğru	13,0	33,7	22,31	4	,000
	Kararsızım	8,8	16,2			
	Benim için doğru değil	**78,2**	**50,1**			
S27 – Kişisel fotoğraf ve videolarımı herkesin erişebileceği ortamlarda paylaşırım.	Benim için doğru	16	35,2	24,92	4	,000
	Kararsızım	9,6	18,8			
	Benim için doğru değil	**74,4**	**46,0**			
S30 – Göndereni tanımasam da tepkimi çeken epostaları yanıtlarım.	Benim için doğru	19,5	32,9	13,72	4	,006
	Kararsızım	12,1	23,5			
	Benim için doğru değil	**68,4**	**43,6**			
S32– Şifrelenmemiş ve kimin sağladığını bilmediğim kablosuz ağlara bağlanırım.	Benim için doğru	28,8	**38,8**	14,71	4	,002
	Kararsızım	8,8	22,3			
	Benim için doğru değil	**62,4**	38,9			
S37 – E-posta adresim kötü niyetli kişilerin eline geçerse, nasıl geri alabileceğim konusunda bilgi sahibiyim.	Benim için doğru	29,2	**54,7**	15,62	4	,003
	Kararsızım	34,6	17,4			
	Benim için doğru değil	**36,2**	27,9			

S46 – Bir bilişim suçuna maruz kalırsam kime başvuracağımı biliyorum.	Benim için doğru	**37**	**57,7**	11,65	4	,020
	Kararsızım	30,3	23,5			
	Benim için doğru değil	32,7	18,8			
S48 – Bilgisayarımın güvenliğini sağlayacak yazılımları bulma ve kullanmada yeterli bilgiye sahibim.	Benim için doğru	**40,1**	**63,2**	12,90	4	,009
	Kararsızım	28,3	22,6			
	Benim için doğru değil	31,6	14,2			

Tablo 12'deki bulgulara bakıldığında cep telefonu ile kaynağı bilinmeyen kablosuz ağlara erkeklerin (%48,8) kızlara göre (%28,2) daha yüksek oranda bağlandıkları görülmektedir. Erkek öğrencilerin %50,1'i sosyal ağlarda tanıştıkları insanlarla yüz-yüze görüşmekten kaçınırken, kız öğrencilerde ise %78,2 oranında bu durumdan kaçmaktadırlar. Erkek katılımcıların %35,2'si kişisel fotoğraf ve videolarını herkesin erişebileceği sanal ortamlarda paylaşırken bu duruma kızların %74,4'ü olumsuz yanıt vermektedir. Erkeklerin %32,9'u göndereni tanımasa da tepkisini çeken mesajları yanıtlarken kızlarda bu oran %19,5'dir. Kızlar (%62,4) erkeklere göre (%38,8) şifrelenmemiş kablosuz ağlara daha az bağlanmaktadırlar. Erkek katılımcılar e-posta adresleri ele geçirilirse (%54,7) yada bir bilişim suçuna maruz kalırlarsa (%57,7) kızlara göre (%29,2 ve %37) ne yapacakları konusunda daha bilgili olduklarını belirtmektedirler. Benzer biçimde bilgisayar ve yazılım güvenliği konusunda da erkekler (%63,2) kızlara göre (%40,1) daha bilgili olduklarını belirtmektedirler. Tüm bu bulgular dikkate alındığında yukarıda belirtilen bazı bilişim güvenliği konularında kızların erkeklere göre farkındalık sahibi oldukları söylenebilir.

3.2.2 Bilgisayar ve İnternet Kullanım Yılına Göre Yanıtların Dağılımının Anlamlı Farklılık Gösterdiği Kay-Kare Testi Sonuçları

Ankette katılımcılara bilgisayar ve interneti kaç yıl kullandığı sorulmuştur. Daha sonra öğrencilerin ortalama bilgisayar ve internet kullanım yılları hesaplanmıştır. Öğrencilerin ortalama bilgisayar kullanım süreleri 8,8 yıl, ortalama internet kullanım süreleri ise 7,8 yıl olarak hesaplanmış olup öğrencilerin ortalama bilgisayar kullanımı ve internet kullanımı, sürelerinin ortalamanın altında veya üstünde olma durumlarına göre, anket maddeleri ile her madde bazında anlamlı bir farklılık oluşturup oluşturmayacağı incelenmiştir. Anlamlı farklılık gösteren maddeler aşağıdaki tabloda verilmiştir.

Tablo 13. Ortalama Bilgisayar Kullanımı Göre Kay-Kare Testi Sonuçları

Soru		Ortalamanın Üstü (%)	Ortalamanın Altı (%)	χ^2	sd	p
S3 – Bana ait olmayan bir bilgisayardan internete girerken, tarayıcının kişisel bilgilerimi kaydedip kaydetmediğini kontrol ederim.	Benim için doğru	**71,0**	**61,1**	27,92	4	,000
	Kararsızım	4,0	8,4			
	Benim için doğru değil	35,0	30,5			
S21 – İnternetten bilgisayarıma indirdiğim dosyaları açmadan önce virüs taramasından geçiririm.	Benim için doğru	**48,9**	**58,0**	13,79	5	,017
	Kararsızım	23,5	14,7			
	Benim için doğru değil	27,6	27,3			

Bilgisayar kullanım yılı ortalamanın üzerinde olan öğrencilerin, ortalamanın altında olan öğrencilere kıyasla internet tarayıcılarının kişisel bilgi güvenliği konusunda daha farkındalık sahibi oldukları görülmektedir. İnternetten indirilen dosyaların açılmadan önce incelenmesi konusunda ise ortalamanın altındaki grup daha çok farkındalık sahibidir. Bu bulgular bilgisayar kullanma süresinin bazı konularda farkındalığa yol açarken bazı konularda farkındalığı artırmayabileceği şeklinde yorumlanabilir. Bu nedenle bilişim güvenliği konusu katılımcıların kullanım süresi yüksek diye göz ardı edilmemelidir.

Tablo 14. Ortalama İnternet Kullanımı Göre Kay-Kare Testi Sonuçları

Soru		Ortalamanın Üstü (%)	Ortalamanın Altı (%)	χ^2	sd	p
S1 – İnternetten alış-veriş yaparken internetten ödeme güvenliği hakkında nelere dikkat etmem gerektiğini bilirim.	Benim için doğru	**51,0**	**66,1**	9,52	4	,049
	Kararsızım	7,2	4,9			
	Benim için doğru değil	41,6	28,9			
S3 – İnternetten alış-veriş yaparken internetten ödeme güvenliği hakkında nelere dikkat etmem gerektiğini bilirim.	Benim için doğru	**80,7**	**60,0**	10,00	4	,040
	Kararsızım	7,5	20,0			
	Benim için doğru değil	11,8	20,0			
S25 – Bilgisayarımda (kırılmış) yasa dışı yolla edinilmiş yazılımlar bulunmaktadır.	Benim için doğru	**47,4**	28,9	10,10	4	,039
	Kararsızım	17,2	15,2			
	Benim için doğru değil	35,4	**55,9**			
S35 – İnternet kaynaklı tehditler ile ilgili yeterli bilgiye sahibim.	Benim için doğru	**59,7**	**40,9**	12,54	4	,014
	Kararsızım	26,5	33,3			
	Benim için doğru değil	13,8	25,8			
S44 – Parola güvenliğinin zayıf, orta, yüksek olmasının parolamın güvenliğini nasıl etkilediğini biliyorum.	Benim için doğru	**83,0**	**66,3**	9,91	4	,042
	Kararsızım	7,4	17,8			
	Benim için doğru değil	9,6	15,9			

Tablo 14'te sunulan bulgulara göre ortalamanın üzerinde internet kullanan bireylerle ortalamanın altında internet kullanan bireylerin çoğunluğu genellikle güvenlik konularıyla ilgili farkındalık sahibidir. Ancak 25. madde de gruplara göre yanıtların farklılaştığı önemli bir farklılık görülmemektedir. Bu farklılığa göre ortalamanın üstünde internet kullanan bireyler daha çok yasa dışı (kaçak) yazılım kullandıklarını belirtmişlerdir. Bu durum daha çok internet kullananların öncelikli olarak etik ve ahlaki kurallarla ilgili bilgilendirilmesi ve farkındalık oluşturulması gerektiğini göstermektedir. Bunun dışında genel olarak ortalamanın üstünde-

ki grubun bilişim güvenliği farkındalıkları ortalama altı gruba göre daha yüksektir. Bu iki bulgu birlikte dikkate alındığında ortalamanın üstündeki grup için farkındalığın artmasıyla birlikte etik dışı kullanımında artması dikkat çekici önemli bir ikilemi ortaya koymaktadır. Güvenliğe yönelik farkındalık artarken etik farkındalık daha düşük çıkmaktadır.

3.2.3 Bilişim Güvenliği Eğitimi Alıp Almama Durumuna Göre Kay-Kare Testi Sonuçları

Bilişim güvenliği eğitimi aldığını belirtenler "Evet", bilişim güvenliği ile ilgili eğitim almadığını belirtenler ise "Hayır" olarak tabloda gösterilmiştir.

Tablo 15. Bilişim Güvenliği Eğitimi Alıp Almama Durumuna Göre Kay-Kare Testi Sonuçları

Soru		Evet(%)	Hayır(%)	χ^2	sd	p
S2 – Farklı sitelere üye olurken aynı kullanıcı adı ve parolayı kullanırım.	Benim için doğru	51,3	66,8	10,68	4	,030
	Kararsızım	0	6,9			
	Benim için doğru değil	**48,7**	**26,3**			
S28 – Parolamı belirli zaman aralıklarında değiştiririm.	Benim için doğru	**42,5**	**37,6**	10,67	4	,030
	Kararsızım	12,5	20,8			
	Benim için doğru değil	45,0	41,6			

Tablo 15'te verilen bulgulara göre anlamlı farklılık çıkan madde sayısının azlığı verilen bilişim güvenliği eğitimlerinin yeteri kadar etkili olmadığı göstermektedir. Bu nedenle daha etkili bir biçimde bu dersin nasıl verilmesi gerektiği, içerik vb. konularla ilgili yeni çalışmalar yapılabileceği akla gelmektedir. Eğitim alıp almama durumuna göre dağılımın anlamlı olarak farklı çıktığı sorularda eğitim alan grubun farkındalığı olmayanlara göre görece daha yüksektir. Ancak her iki grupta da farkındalık sahibi olmayan önemli düzeyde katılımcı bulunmaktadır.

3.3.1 "Bir Alış-Veriş Sitesinden Alış-Veriş Yaparken Sitenin Hangi Özelliklerine Dikkat Edersiniz?" Sorusuna Verilen Yanıtların Dağılımı

Katılımcıların e-alışverişle ilgili dikkat ettikleri özellikler Tablo 16'da sunulmuştur.

Tablo 16. "Bir Alış-Veriş Sitesinden Alış-Veriş Yaparken Sitenin Hangi Özelliklerine Dikkat Edersiniz?" Sorusuna Verilen Yanıtların Dağılımı

Yanıtlar	%	f
Alış-veriş yapacağım sitenin güvenilir olmasına	44,02	81
Alış-veriş yapacağım sitenin kullanılma ve tercih edilme oranı ve tanınmışlığı	17,93	33
Güvenlik sertifikasının olmasına	8,69	16
İnternetten alış-veriş yapmam	7,60	14
Ödeme seçeneklerinin çeşitliliği	4,34	8
Site tasarımının güzel olması	4,34	8
Ürün teslimat süresi ve kalitesi	2,71	5
Ürün kalitesi	2,17	4
Fiyatlar	1,63	3
3 boyutlu güvenlik (3d Secure) kullanması	1,08	2
Dekont ve makbuz vermesi	1,08	2
İçeriğinin zengin olması	1,08	2
Ürünler hakkında yeterli bilgi vermesi	1,08	2

Ödeme ekranında ekran klavyesi olması	0,54	1
Site hakkındaki olumlu yorumlar	0,54	1
Kullanıcı sayısı	0,54	1
Kurumsallığı	0,54	1

Tablo 16'da yer alan değerlere göre öğrencilerin internetten alış-veriş yaparken en çok sitenin güvenilir olmasına ve tercih edilme oranına dikkat ettikleri görülmektedir. Bilişim güvenliği ilkelerine göre de bireylerin internetten alışveriş yaparken dikkatli olmaları beklenmektedir. Bununla birlikte katılımcılar alışveriş sitesinin güvenilir olmaya yönelik özelliklerine beklenen düzeyde atıfta bulunmamışlardır. Bu durum bir kavram olarak "güvenlik" kavramı ile ilgili farkındalık olmasına rağmen, bu kavramı dikkate alıp uygulamada eksikler olabileceğini göstermektedir. Öğrencilerin alış-veriş siteleriyle ilgili bazı özelliklere dikkat ettikleri bununla birlikte 3 boyutlu güvenlik (3d secure), ekran klavyesi gibi internet alış-verişi için önemli olan teknik konular hakkında yeterli bilgi sahibi olmadıkları görülmektedir.

3.3.2 "Parola belirlerken parolanın hangi özellikleri taşımasına dikkat edersiniz?" Sorusuna Verilen Yanıtların Dağılımı

Katılımcıların parola belirlerken dikkat ettikleri özellikler Tablo 17'de sunulmuştur.

Tablo 17. "Parola belirlerken parolanın hangi özellikleri taşımasına dikkat edersiniz?" Sorusuna Verilen Yanıtların Dağılımı

Yanıtlar	%	f
Farklı kombinasyonlar; sayı, noktalama, harf	44,26	81
Hatırlayabileceğim şeyler	17,48	32
Tahmin edilmesi zor	15,30	28
Güvenli olması	5,46	10
Uzun olması	4,91	9
Güçlü olması	3,27	6
Benim için özel olan şeyler	2,18	4
Büyük küçük harf olması	1,63	3
Noktalama olması	1,63	3
Asal sayı olması	1,09	2
Gizli olması	1,09	2
Doğum tarihi	1,09	2
Sitedeki parola yönergelerine uygun	0,54	1

Bulgulara göre öğrencilerin bilişim güvenliği ilkelerine uygun olan güçlü parola belirleme kriterlerine uygun şekilde farklı kombinasyonları parola belirlerken önemli oranda kullandıkları ve genellikle tahmin edilmesi zor şifreleri tercih etme oranlarının yarıya yakın olduğu görülmektedir. Bilişim güvenliği ilkelerine uygun olmayan doğum tarihi gibi tahmin edilmesi kolay şifreleri tercih etmedikleri görülmektedir. Bununla birlikte öğrencilerin önemli bir kısmı beklenen yanıtı tam olarak belirtmemiştir.

3.3.3 "Bir yazılıma ihtiyaç duyduğunuzda bunu nasıl temin edersiniz?" Sorusuna Verilen Yanıtların Dağılımı

Katılımcıların ihtiyaç duydukları yazılımları nasıl temin ettiklerine ilişkin yanıtların derlendiği sonuçlar Tablo 18'de sunulmuştur.

Tablo 18. "Bir yazılıma ihtiyaç duyduğunuzda bunu nasıl temin edersiniz?" Sorusuna Verilen Yanıtların Dağılımı

Yanıtlar	%	f
İnternetten indirerek kullanırım	64,70	88
Arkadaşımdan isterim	20,58	28
Bilgisayar mağazasından satın alırım	9,55	13
Korsan alırım	2,20	3
Bu konuda bilgisi olan birinden yardım alırım	1,47	2
Abimden, erkek kardeşimden alırım	1,47	2

Öğrencilerin genellikle yazılımları internet kullanarak indirip kullandıkları veya arkadaşlarından isteyerek kullandıkları görülmektedir. Diğer yandan bir mağazaya gidip satın alarak yazılım kullanan öğrencilerin de sayısının oldukça az olduğu görülmektedir. İnternetten indirilen ve arkadaştan alınan yazılımlar akla doğrudan bunların ne kadarının kaçak yazılım olduğu sorusunu akla getirmektedir. Diğer bulgularla birlikte dikkate alındığında kaçak yazılım kullanımının bilişim güvenliği ve bilişim etiği ile ilgili en önemli sorunlardan biri olduğu söylenebilir.

3.3.4 "Bilişim güvenliği konusunda bilgi aldığınız bir web sitesi, kurum, kuruluş vb. varsa lütfen adını yazınız." Sorusuna Verilen Yanıtların Dağılımı

Katılımcıların bilişim güvenliği konusunda bilgilenme amaçlı kullandıklarını belirttikleri kaynaklar Tablo 19'da sunulmuştur.

Tablo 19. "Bilişim güvenliği konusunda bilgi aldığınız bir web sitesi, kurum, kuruluş vb. varsa lütfen adını yazınız." Sorusuna Verilen Yanıtların Dağılımı

Yanıtlar	%	f
Sakarya Üniversitesi	17,39	4
Shiftdelete.net	17,39	4
Donanımhaber.com	13,04	3
Forumlar	8,69	2
Anadolu Üniversitesi	4,34	1
Çizgi Tagem	4,34	1
Vitamin	4,34	1
Chip.net	4,34	1
BTK- Bilgi Teknolojileri ve İletişim Kurumu	4,34	1
Turkhackteam.com	4,34	1
Gezginler.com	4,34	1
Türk Bilişim Derneği	4,34	1
Egm-Emniyet Genel Müdürlüğü	4,34	1
Wardom.org	4,34	1
Arkadaş	4,34	1

Tablo 19'da sunulan bulgulara bakıldığında bilişim güvenliği ile ilgili öğrencilerin genellikle kullanıcı sayısı yüksek olan forum ve web sitelerinden (shiftdelete.net, donanımhaber.com, Çizgi Tagem vb..) bilgi aldıkları ayrıca üniversitelerden bilgi aldıkları görülmektedir. Bununla birlikte öğrencilerin çok azının bilgi almaya yönelik çabasının olduğu (f=2) dikkat çekmektedir. Ayrıca öğrencilerin bilişim güvenliği için bilgi aldıklarını söyledikleri bazı sitelerin bilişim güvenliği ile doğrudan ilgili olmaması dikkat çekmektedir. Bu nedenle öğrencilere hem bilişim güvenliği farkındalığı kazandırmaya hem de bilgilerini geliştirip

güncel kalmalarını sağlayacak geçerli ve güvenilir öğrenme kaynaklarını öğretmek bir ihtiyaç olarak ortaya çıkmıştır. 112 katılımcıdan sadece 24'ünün kendini geliştirmeye yönelik olarak bir adres gösterebilmesi dikkat çekicidir. Bu adreslerden bazıları da amaca uygun değildir. Bu bulgu katılımcıların bilişim güvenliği konusunda kendilerini geliştirme açısından web sitelerinden ve diğer kaynaklardan beklenen düzeyde yararlanmadıklarını, bu konuda farkındalıklarının düşük olduğunu göstermektedir.

4. SONUÇ ve ÖNERİLER

Genel olarak sonuçlara bakıldığında öğrencilerin çoğunun bilişim güvenliği konusunda farkındalıklarının olduğu görülmektedir. Alan yazında bu konuda yapılan bazı çalışmalarda bireylerin bilişim güvenliği/bilgi güvenliği bilgi düzeyleri iyi iken (İlkan, İşçioğlu, Egelioğlu ve Doğanalp, 2010) ağırlıklı olarak bilişim güvenliği/bilgi güvenliği farkındalıklarının düşük olduğu gözlenmektedir (Dijle, 2006; Dijle ve Doğan, 2011; Pusey ve Sadera, 2011). Bununla birlikte ele alınan birçok boyut açısından azımsanmayacak sayıda öğrencinin kararsız ya da olumsuz yanıt verdiği durumlar da bulunmaktadır. Örneğin öğrencilerin büyük çoğunluğu parola güvenliği konusunda bilgi sahibi olduklarını belirtirken, aynı zamanda farklı sitelerde aynı parolayı ve kullanıcı adını kullandıklarını, başka insanlarla parola ve şifrelerini paylaştıklarını da belirtmektedirler. Bu bulgu Bilek (2012), Tekerek ve Tekerek (2013), İlkan, İşçioğlu, Egelioğlu ve Doğanalp (2010) bulguları ile benzerlik göstermektedir. Bununla birlikte internetten alış-verişle ilgili bilgilerinin olduğunu söyleyen %65'lik gruba karşılık %37'lik grup sanal klavye kullanmamaktadır. Öğrencilerin %72'si arkadaşlarına bilgisayarlarını kullandırırken konuk oturum açtıklarını belirtirken %66'lık bölümü bilgisayarlarında konuk oturumun olmadığını belirtmektedir. Antivirüs, sosyal ağ güvenliği, e-posta ve anlık ileti yazılımları, kablosuz ağ kullanımı, yasal ve etik konular ve kendini geliştirme konularıyla ilgili öğrencilerin çoğu belirtilen ifadelere katıldıklarını söylemekle birlikte genellikle %30 dolaylarında katılımcı kararsız ya da olumsuz yanıt vermiştir. Bu bulgular Kruger ve Kearney'in (2006), Agamba ve Keengwe'in (2012) çalışmalarında olduğu gibi bireylerin bilişim güvenliğine yönelik tutumları, davranışları ve bilgileri arasında farklılıklar olduğunu göstermektedir.

Bilişim teknolojileri güvenliği maddelerinin cinsiyete göre farklılaşıp farklılaşmadığı incelendiğinde erkek öğrencilerin kız öğrencilere göre kaynağını ve güvenirliğini bilmedikleri kablosuz ağlara bağlanma konusunda daha çok risk aldıkları görülmüştür. Kınay (2012) ve Topçu'nun (2008) bulgularında da erkeklerin kızlara göre güvenlikle ilgili konularda daha fazla risk aldığı görülmektedir. Ancak Mart'ın (2012) bulgularında cinsiyet açısından bilgi güvenliği farkındalıklarının değişmediği ifade edilmiştir. İlbaş (2009) ise çalışmasında kızların erkeklere oranla bilişim suçlarını suç olarak görme oranlarının genel olarak daha fazla olduğunu ifade etmektedir. Ancak bu çalışmanın sonuçları bilişim güvenliği konusunda kızların görece temkinli olduğunu göstermektedir.

İnternet kullanımı süresine göre bilişim güvenliği maddelerine verilen yanıtlar incelendiğinde ortalamanın üstünde internete bağlanan katılımcıların daha çok korsan yazılım kullandıklarını belirtmiş olmaları dikkat çekici bir sonuçtur. Bilişim teknolojilerinden daha çok yararlanmak daha etik kullanım konusunda bir ilerlemeye neden olmamaktadır. Hatta verilecek eğitimlerde daha çok deneyim sahibi kullanıcılara etik ve kanuni kullanımla ilgili öncelik verilmesi gerektiği söylenebilir. Bu bulgu Mart'ın (2012) bulgularından farklılaşmaktadır.

Mart (2012) bilgi güvenliği farkındalığı ile bilgisayar, internet kullanımı arasında bir fark olmadığı belirtilmiştir. Bu çalışmada ise bilgisayar deneyimi arttıkça farkındalığın ve ne yazık ki etik dışı kullanımın arttığı görülmüştür. Diğer yandan alan yazındaki bazı çalışmalarda korsan yazılım kullanım oranının orta-yüksek düzeyde olduğunu göstermektedir (Bilek, 2012; Dijle ve Doğan, 2011).

Öğrencilerin sorulara verdikleri yanıtlar bilişim güvenliği ve etikle ilgili bir ders alıp almamaları açısından bir farklılık göstermemektedir. Bu bulgu Tekerek'nin (2012) bulguları ile benzerlik göstermektedir. Bu nedenle bilişim güvenliği ve etikle ilgili bir ders ihtiyacı açığa çıkmasıyla birlikte bu dersin etkili olabilmesi için içeriğin nasıl olması gerektiği ile ilgili yapılacak çalışmalara ihtiyaç duyulduğu söylenebilir. Mevcut alınan derslerin önemli bir farkındalık ortaya çıkarmadığı görülmektedir. Bu nedenle farkındalık oluşturmanın ötesinde davranışa dönüşecek etkililikte derslere ihtiyaç duyulduğu söylenebilir.

İnternet güvenliğiyle ilgili olarak öğrenciler internetten alış-veriş yaparken dikkat edecekleri birçok özellik belirtmişlerdir. Bununla birlikte güvenli kullanım açısından yeterli düzeyde belirtilmemiş önemli araçların olduğu dikkat çekmektedir. Bu sonuç öğrencilerin internetten alış-verişte güvenlikle ilgili farkındalıkları olduğu diğer taraftan gerekli bilgi ve beceriler açısından zayıf olduklarını akla getirmektedir. Bu sonucu destekleyen bir araştırma sonucu da bireylerin internetten alış-veriş konusunda çekingen davrandığını göstermektedir (Bilek, 2012).

Sonuç olarak öğrencilerin bir kısmı farkındalık sahibi iken önemli bir kısmı bu açıdan dezavantajlıdır. Katılımcıların bilişim güvenliği konusunda kendilerini hangi kaynaklardan geliştirmeye çalıştıkları sorusuna tatminkâr bir yanıt alınamamıştır. Bu nedenle bilişim güvenliği ile ilgili verilebilecek derslerin yanı sıra bireylerin bilgilerini güncelleyecekleri, kendilerini geliştirecekleri olanaklar sunmaya yönelik araştırmalar yapılması ve önerilerin geliştirilmesi güvenli bilişim teknolojisi kullanımına katkı sağlayacaktır.

Alan yazında yapılan çalışma sonuçlarına göre de bilişim güvenliği farkındalığı kazandırmaya yönelik eğitimlerin verilmesi gerektiği ifade edilmektedir (Bilek, 2012; İlbaş, 2009; Dijle ve Doğan, 2011; Gökmen, 2014). İleride yapılacak araştırmalarda bilişim güvenliği ve bilişim etiği konularında öğretmenlik programında okuyan öğrencilerin farkındalıklarını artırmak ve yeterli düzeyde bilgilendirmek için neler yapılabileceğini belirlemeye yönelik araştırmalar yapılabilir. Bu araştırmalarda öğrencilerin ihtiyaçları ve beklentileri belirlenerek bu konularla ilgili kitaplar, elektronik kitaplar, web siteleri vb. öğretim materyalleri geliştirerek bunların etkililiği incelenebilir. Bu konulara yönelik kurslar, dersler tasarımlanarak bunların etkililiğine yönelik deneysel çalışmalar ve araştırma-geliştirme projeleri yapılabilir. Ancak yalnızca bireylere sadece bilgi kazandırmak yerine tutum ve davranış kazandırmaya yönelik etkinliklerin yapılması bu araştırma sonuçlarında ortaya çıkan önemli bulgulardan biri olarak görülmektedir. Bu çalışmaların gerçekleşmesi için, bu sınırlı çalışmada elde edilen bulguların ihtiyaç analizlerine ve geliştirilecek eğitimlere yönelik ipuçları sunması umulmaktadır.

Kaynakça

Agamba, J. ve Keengwe, J. (2012). Pre-Service Teachers' Perceptions of Information Assurance and Cyber Security. *International Journal of Information and Communication Technology Education*, *8*(2), 94-101.

Avrupa Birliği Siber Suç Sözleşmesi. (**t.y.**). http://www.coe.int/t/dghl/cooperation/economiccrime/ Source/Cybercrime/TCY/ETS%20185%20turkish.pdf

Baykara, M., Daş, R. ve Karadoğan, İ. (2013). *Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi.* 1st International Symposium on Digital Forensics and Security, Elazığ. http://perweb.firat.edu.tr/personel/yayinlar/fua_721/721_80043.pdf adresinden 27.01.2015 tarihinde erişilmiştir.

Bilek, B.T. (2012). *Bilişim Suçları ve Üniversite Lisans Öğrencilerin Bilişim Suçlarına Yönelik Görüşleri.* Yüksek lisans tezi, Gazi Üniversitesi, Bilişim Enstitüsü, Ankara.

Büyüköztürk, Ş. (2012). *Sosyal Bilimler İçin Veri Analizi El Kitabı* (17. Baskı). Ankara: PegemA Yayıncılık.

Büyüköztürk, Ş., Kılıç Çakmak, E., Akgün, Ö. E., Karadeniz, Ş. ve Demirel, F. (2012). *Bilimsel Araştırma Yöntemleri* (11. Baskı). Ankara: PegemA Yayıncılık.

CSI. (2011). *Computer Crime & Security.* http://gatton.uky.edu/FACULTY/PAYNE/ACC324/ CSISurvey2010.pdf

Canbek, G. (2005). *Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme.* Yayınlanmamış Yüksek lisans tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.

Canbek, G. ve Sağıroğlu, Ş. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. *Politeknik Dergisi*, *9*(3), 165-174.

Cavusoglu, H., Cavusoglu, H. ve Raghunathan, S. (2004). Economics of IT Security Management: Four Improvements to Current Security Practices. *Communications of the Association for Information Systems*, *14*, 65-75.

Çalık, D. ve Çınar, Ö. P. (2009). Geçmişten Günümüze Bilgi Yaklaşımları Bilgi Toplumu ve Internet. *14. Türkiye'de Internet Konferansı Bildirileri,* 12-13 Aralık, İstanbul.

Dedeoğlu, G. (2006). *Bilişim Toplumu ve Etik Sorunlar.* Bursa: Alfa Aktüel Yayınları.

Dijle, H. (2006). *Türkiye'de Eğitimli İnsanların Bilişim Suçlarına Yaklaşımı.* Yayınlanmamış yüksek lisans tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.

Dijle, H. ve Doğan, N. (2011). Türkiye'de Bilişim Suçlarına Eğitimli İnsanların Bakışı. *Bilişim Teknolojileri Dergisi*, *4*(2), 43-53.

Gordon, S. ve Ford, R. On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*, 13-20.

Gordon, L. A. ve Loeb, M. P. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, *5*(4), 438-457.

Gökmen, Ö. F. (2014). *Bilgisayar ve Öğretim Teknolojileri Eğitimi Öğretmen Adaylarının Bilişim Güvenliği Eğitimi Verebilme Yeterliklerinin İncelenmesi.* Yayınlanmamış yüksek lisans tezi, Sakarya Üniversitesi, Eğitim Bilimleri Enstitüsü, Sakarya.

İlbaş, Ç. (2009). *Bilişim Suçlarının Sosyo-Kültürel Seviyelere Göre Algı Analizi.* Yayınlanmamış Yüksek lisans tezi, Başkent Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.

İlbaş, Ç. ve Köksal, M. A. (2011). Türkiye Bilişim Suçları Raporu: 1990-2011 Temmuz. *2. Uluslararası Bilişim Hukuku Kurultayı Bildiriler Kitabı.* İzmir.

İlkan, M., İşçioğlu, E., Egelioğlu, F. ve Doğanalp, A. (2010). *Information Security Awareness of Academic Staff Members: An Example of Eastern Mediterranean University School of Computing and Technology.* 4. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildirileri, Orta Doğu Teknik Üniversitesi, Ankara.

Kınay, H. (2012). *Lise Öğrencilerinin Siber Zorbalık Duyarlılığının Riskli Davranış, Korumacı Davranış, Suça Maruziyet ve Tehlike Algısı İle İlişkisi ve Çeşitli Değişkenler Açısından İncelenmesi.* Yüksek lisans tezi. Sakarya Üniversitesi, Eğitim Bilimler Enstitüsü, Sakarya.

Kritzinger, E. ve Smith, E. (2008). Information Security Management: An Information Security Retrieval and Awareness Model for Industry. *Computers & Security, 27*(5-6), 224-231.

Kruger, H. A. ve Kearney, W. D. (2006). A Prototype for Assessing Information Security Awareness. *Computers & Security, 25*, 289-296.

Mann, D. ve Sutton, M. (1998). NETCRIME, More Change in the Organization of Thieving. *British Journal of Criminology, 38*(2), 201-229.

Mart, İ. (2012). *Bilişim Kültüründe Bilgi Güvenliği Farkındalığı*. Yüksek lisans tezi. Kahramanmaraş Sütçü İmam Üniversitesi, Fen Bilimleri Enstitüsü, Kahramanmaraş.

Pro-G. (2003). *Bilişim Güvenliği. Sürüm 1.1.* Proje Bilişim Güvenliği ve Araştırma San. ve Tic. Ltd. Şti. http://www.pro-g.com.tr/whitepapers/bilisim-guvenligi-v1.pdf 02.05. 2014 tarihine erişilmiştir.

Pusey, P. ve Sadera, W. A. (2011). Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference. *Journal of Digital Learning in Teacher Education, 28*(2), 82-85.

Sağıroğlu, Ş. ve Vural, Y. (2008). Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme. *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 23*(2), 507-522.

Siber. (2013). *Siber Suçlarla Mücadele Daire Başkanlığı.* http://www.siber.pol.tr

Symantec. (2014). *Internet Security Threat Report.* http://www.symantec.com/content/en/us/ enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

Şahinaslan, E., Kandemir, R. ve Şahinaslan, Ö. (2009). *Bilgi Güvenliği Farkındalık Eğitimi Örneği.* XI. Akademik Bilişim Konferansı Bildirileri, Şanlıurfa.

Şahinaslan, E., Kaantürk, A., Şahinaslan, Ö. ve Borandağ, E. (2009). *Kurumlarda bilgi güvenliği farkındalığı, önemi ve oluşturma yöntemleri.* XI. Akademik Bilişim Konferansı Bildirileri, Şanlıurfa.

TCK. (2014).*Türk Ceza Kanunu*. http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.doc

Thompson, M. E. ve Solms V. R. (1998). Information security awareness: educating your users effectively. *Information Management & Computer Security, 6*(4), 167-173.

Topcu, Ç. (2008). *The Relationship Of Cyberbullying to Empathy, Gender, Traditional Bullying, Internet Use and Adult Monitoring.* Yayınlanmamış Yüksek lisans Tezi. Orta Doğu Teknik Üniversitesi Sosyal Bilimler Enstitüsü. Ankara.

Tekerek, M. (2008). Bilgi Güvenliği Yönetimi. *KSÜ Fen ve Mühendislik Dergisi, 11*(1), 132-137.

Tekerek, M.(2012). *İlköğretim ve Lise Öğrencilerinin Bilgi ve Bilgisayar Güvenliği Farkındalığı: Kahramanmaraş Örneği.* Uluslararası Bilgi Güvenliği ve Kriptoloji Konferans, Ankara.

Tekerek, M. ve Tekerek, A. (2013). A Research on Students' Information Security Awareness. *Turkish Journal of Education, 2*(3), 61-70.

Wagner, A. E. ve Brooke, C. (2007). Wasting time: The mission impossible with respect to technology-oriented security approaches electronic. *Journal of Business Research Methods, 5*(2), 117-124.

Whitman, M. E. ve Mattord, H. J. (2012). *Principles of Information Security (Fourth Edition)*. Boston, USA: Course Technology.

Yavuz, H. ve Ulaş, M. (2013). Adli Bilişime konu olan Bilişim Suçları ve Bilgi Güvenliği Farkındalık Tespiti. *1. International Symposium on Digital Forensics and Security Proceding Book.* Fırat Üniversitesi, Elazığ.

Vural, Y. ve Sağıroğlu, Ş. (2008). Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme. *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 23*(2), 507-522.

Extended Summary

Information and communication technologies penetrate almost every aspect of life with computers, mobile phones and tablet computers. These technologies provide us with many advantages for a efficient and effective learning. At the same time they have many risks with vulnerabilities and improper unsafe use. Therefore safely and proper use of information and communication technologies (ICT) are vital.

Cybercriminals, hackers and other bad-intended people can try to harm people with using ICT as well. That makes information security an important issue for ICT users. A long with the FATIH project same ICT technologies were provided to teachers and students in most of anatolian high school in Turkey. Therefore it is important to let them gain necessary knowledge and skills in information security. Especially teachers may have an important role for guiding their students to use ICT safely and properly. The purpose of this study is to investigate information security awareness of prospective teachers enrolled in Sakarya University Faculty of Education.

In this context following questions investigated:

1- How is the level of awareness of faculty of education senior students at password security, online shopping, anti-virus and anti-malware software, security updates, social network security, email and instant message security, wireless networks, legal and ethical issues, improving and updating their knowledge.

2- Is awareness level of information security significantly change according to; gender, computer and internet experience by year and whether taking an education or course about information security or not.

3- What are the views of participants about considering security of shopping online, deciding a password, obtaining or buying software and how do they update their ICT security information?

This study is conducted in cross-sectional survey model with 212 senior students from Elementary Mathematics Education (39), Computer and Instructional Technologies Education (64), Turkish Language Education (74), Mentally Handicapped Education departments (35). Data was collected through "Information Security Questionnaire" developed by authors. Questionnaire includes 48 number of 5-likert-type and 18 number of usage, demographics questions. Data was analyzed by using Chi-Squire, frequencies, descriptive statics via SPSS.

According to the results, there is not little number of students having low level awareness about ICT security. This result shows important needs of education about ICT security for participants. On the other hand there are some contradictory results. Although most of the participants report that they know how to create a strong password, they admit they tell their passwords to friends and use same passwords. This result show that the participants are at high level of awareness about some issues but not well enough in others.

65% of the participants report that they know how to shop online, but 37% of them admit they don't use secure virtual keyboard. Therefore it takes notice that there are important differences in their reports and usage patterns.

In addition to these results female participant are more cautious than males in some security issues. There is not a significant effect of whether taking a course or a education about information security on participants' responses. This means existing courses are not enough for improving significantly change ICT security awareness and usage patterns. It is suggested to design and implement proper and efficient courses about ICT security for prospective teachers. New studies and research projects are needed to improve ICT security awareness, knowledge and skills of prospective teachers.