Bartın Üniversitesi
Eğitim Fakültesi Dergisi
Cilt 3, Sayı 1, s. 176 - 199, Yaz 2014
BARTIN – TÜRKİYE

ISSN: 1308-7177

Bartin University
Journal of Faculty of Education
Volume 3, Issue 1, p. 176 - 199, Summer 2014
BARTIN – TURKEY

doi number: 10.14686/BUEFAD.201416213

Üniversite Öğrencilerinin Güvenli Bilgi ve İletişim Teknolojisi Kullanım Davranışları ve Bilgi Güvenliği Eğitimine Genel Bir Bakış

Dr. Gizem KARAOĞLAN YILMAZ
Ankara Üniversitesi
Eğitim Bilimleri Fakültesi
gkaraoglanyilmaz@gmail.com

Dr. Ramazan YILMAZ
Bartın Üniversitesi
Meslek Yüksekokulu
ramazanyilmaz067@gmail.com

Arş. Gör. Barış SEZER
Hacettepe Üniversitesi
Tıp Fakültesi
barissezer13@hotmail.com

Özet: Bilgi ve iletişim teknolojilerinin (BİT) bireysel ve toplumsal hayata sağladığı pek çok faydanın yanında güvenli olmayan BİT kullanımı sonucunda bireyler çeşitli problemlerle karşı karşıya kalabilmektedirler. BİT'in güvenli kullanımı konusunda eğitim sistemine ve eğitimcilere önemli görevler düşmektedir. Bu amaçla Milli Eğitim Bakanlığı (MEB) güncellenen Bilişim Teknolojileri ve Yazılım dersi müfredatında öğrenci ihtiyaçlarına bağlı olarak bilgi güvenliği eğitimlerinin verilmesi gerektiğini önermiştir. Ancak bu konuda öğrenci ihtiyaçlarını ortaya koyan çalışmaların eksikliği alanyazında hissedilmektedir. Gerçekleştirilen bu çalışmanın amacı, zorunlu eğitim süreçlerinden geçerek üniversiteye yeni başlayan öğrencilerin bilgi güvenliğine yönelik davranış durumlarını ortaya koymaktır. Çalışma üniversite birinci sınıftaki 124 öğrenci üzerinde yürütülmüştür. Araştırmanın verileri nicel ve nitel yöntemler kullanılarak elde edilmiştir. Elde edilen bulgular doğrultusunda öğrenci ihtiyaçlarına bağlı olarak Bilişim Teknolojileri ve Yazılım ders müfredatında yer alması gereken konulara ilişkin öneriler getirilmiştir.

Anahtar Sözcükler: Bilgi Güvenliği, Bilgi Güvenliği Eğitimi, Kullanıcı Davranışları

Secure Information and Communication Technology Usage Behavior of University Students and an Overview to Information Security Training

Abstract: Information and communication technologies (ICT) provide many benefits to the individual and social life whereas they can also bring about some unwanted problems as a result of their unsafe use. Educators and the education system itself have responsibilities for the students' safe use of ICT. For this purpose, in the revised version of the curriculum of Information Technology and Software (IT&S) course, the Ministry of National Education proposed that topics on safe use of ICT should be included in the curriculum based on the needs of the students. However, there is a gap in the literature with regard to the needs of the students. Therefore, the purpose of this research is to examine the behaviour of the first year undergraduate students concerning the information security. First year students as they took a compulsory Information Technology and Software course at the Ministry of National Education schools. The study was conducted on 124 first year students. Data were analyzed using the qualitative and quantitative methods. Drawing on the findings we suggested some emerged topics which could be included in the IT&S curriculum based on the students' needs.

Key Words: Information Security, Information Security Training, User Behavior

1. GİRİŞ

Bilgi ve iletişim teknolojilerinin (BİT) yaşamın her alanına sağlamış olduğu pek çok faydanın yanında kullanıcılar BİT'in doğru olmayan kullanımından kaynaklanan bir takım problemlerle karşı karşıya kalabilmektedir. Bilgi güvenliğini tehlikeye sokabilecek davranış ve uygulamaların sonucunda karşı karşıya kalınan güven ve gizlilik kaybı, çeşitli siber tehdit ve saldırılar bu problemlerden bazılarıdır. Bu problemler kullanıcılar üzerinde ciddi maddi ve manevi kayıplara yol açabilmektedir. BİT'ten doğru bir şekilde yararlanma sürecinde yöneticilere, eğitimcilere ve ebeveynlere önemli görevler düşmektedir. Bu görevlerden en önemlisi geleceğin anne-babaları olacak olan çocukların ve gençlerin BİT'in doğru ve güvenli kullanımı konusundaki farkındalık düzeylerini artırmaktır.

Hayatımızın her alanına hızla giren yeni teknolojilere yönelik olarak kullanıcı davranışları analiz edildiğinde çoğu kullanıcı davranışının bilgi güvenliği açıklarına sebebiyet verebildiği görülmüştür (Adams ve Sasse, 1999; Besnard ve Arief, 2004; Brostoff ve Sasse, 2001; Maxion ve Reeder, 2005). Güvenliğin en önemli zaafının insan davranışı olduğu bilinmektedir. Wagner ve Brooke'e (2007) göre bilgi güvenliğini oluşturan zincirin en zayıf halkası insan faktörüdür. Schneier (2000), güvenliğin sadece en zayıf halkanın güvenliği kadar olabileceğini ve insanların da bu zincirdeki en zayıf halka olduğunu belirtmiştir. Poulsen (2000) ise bilgisayar güvenliğindeki insan faktörünün gözden kaçırıldığını, kurumların güvenlik duvarları, şifreleme ve güvenli erişim cihazlarına milyonlarca dolar harcadıklarını, ancak bu teknik önlemlerin güvenlik zincirindeki en zayıf halka olan insan faktöründen kaynaklanan tehdit ve açıkları önleyemediği için harcanan paranın boşa gittiğini belirtmektedir. Gonzales ve Sawicka (2002), bilgi güvenliğinin teknoloji ve insanı içerdiğini, güvenlik sistemleri ne kadar iyi tasarlanmış ve uygulanmış olursa olsun yönetim ve kullanımının insanlara bağlı olduğunu ve bilgi sistemlerinde insan faktörünün daha iyi anlaşılması gerektiğini belirtmektedir. Bu çerçeveden bakıldığında bilgi güvenliğinin sağlanmasında teknik altyapının oluşturulması kadar insan faktörünün de dikkate alınması önemlidir.

Bilgi güvenliğini sağlamaya yönelik araştırmaların çoğunun güvenlik yazılımları ve modelleri oluşturma gibi teknik ya da cezai yaklaşımlar oluşturma gibi hukuksal ve idari boyutlu araştırmalar olduğu görülmektedir (Besnard ve Arief, 2004; Egan, 2004; Mahabi, 2010; Markotten, 2002; Vroom ve Solms, 2004). Alanyazında insan faktöründen kaynaklanan bilgi güvenliği hatalarını belirlemeye ve bunları ortadan kaldırmaya yönelik araştırmaların ise yeni yeni gerçekleştirildiği görülmektedir (Kaşıkçı, Çağıltay, Karakuş, Kurşun ve Ogan, 2014; Mart,

2012). Bilgi güvenliği zincirindeki en zayıf halkanın insan faktörü olduğu göz önüne alındığında, insan faktöründen kaynaklı bilgi güvenliği hata ve ihlallerinin belirlenmesi ve bunların giderilmesine daha çok önem verilmesi gerekmektedir (Colwill, 2009; Jones ve Colwill, 2008). Çok büyük yatırımlarla oluşturulan teknik boyuttaki güvenlik sistemlerini geliştiren, yöneten ve kullananların da insanlar olduğu göz önüne alındığında insan faktörü bilgi güvenliğinin sağlanmasındaki teknik boyutun da ötesine geçmektedir. Bu noktada kurumların ve kullanıcıların bilgi güvenliği tehditleri konusunda eğitilmesi ve farkındalıklarının yükseltilmesi gerekmektedir (Chou, Chan ve Wu, 2007; Wishart, Oades ve Morris, 2007). Söz konusu eğitimlerin verilebilmesi ve bilgi güvenliği ihtiyaçlarının belirlenebilmesi için bireylerin güvenli BİT kullanımı konusunda gösterdikleri davranış durumlarının ortaya konulması gerekir.

Talim ve Terbiye Kurulu Başkanlığı kararına (2012) göre BİT'in yaşamın her alanına hızla girmesine bağlı olarak bundan en uygun şekilde yararlanacak ve BİT'in vereceği olumsuz etkilerden bireyleri koruyacak güncel eğitim programlarına ihtiyaç duyulmuştur. Bu amaçla BİT'in olumsuz etkilerinden bireyleri korumak amacıyla da yapılandırılacak bilişim teknolojileri eğitim programlarında teknoloji kullanımı ve üretiminde etik değerler, gizlilik, bilgi ve veri güvenliği, siber suçlar, sanal zorbalık, internet bağımlılığı gibi kişisel ve toplumsal açıdan önemli konulara da yer verilmesi gerektiği belirtilmektedir. Rapora göre bilişim teknolojileri ders programlarında "yalnızca ofis otomasyonlarının öğretildiği yapıdan uzaklaşılmalı ve yukarıda belirtilen konularla birlikte yetişen bireylerin yeni teknolojileri kendi kendilerine öğrenebilme ve yeni teknolojilerin doğru kullanımı konusunda kültür geliştirmelerine olanak sağlayan bir yaklaşım benimsenmelidir. Bireyleri bilgi teknolojileri üreticileri haline getirmek ve bu bağlamdaki kültürü onların geliştirmelerini sağlamak yeni eğitim programının en temel hedeflerinden olmalıdır." Söz konusu rapora göre yeniden yapılandırılacak bilişim teknolojileri ders programlarının içeriğinin kazandırılmasında bilişim teknolojileri öğretmenlerine büyük sorumluluklar düşmektedir.

Talim ve Terbiye Kurulu Başkanlığı kararında (2012) önerilen bilişim teknolojileri çerçeve programı kapsamındaki bu konuların öğretilmesinde öğrenci ihtiyaç ve durumlarına göre bilişim teknolojileri öğretmenlerinin eğitim içeriğine yön vermesi gerektiği belirtilmektedir. Ancak önerilen çerçeve programındaki konuların güncel konular olması nedeniyle bu konuların öğretiminde öğretmenlere yol gösterebilecek araştırmalara ihtiyaç duyulmaktadır. Örneğin çerçeve programda yer alan bilgi ve veri güvenliği konusunda öğretmenlerin eğitim içeriğine karar verebilmeleri için öncelikle konuya ilişkin öğrenci

düzeyinin ve ihtiyaçlarının belirlenmesi gerekir. Aksi halde verilecek olan eğitimin amaçlara ulaşmada yetersiz kalacağı düşünülmektedir. Bu nedenle bilgi güvenliğini sağlama konusunda öğrenci ihtiyaçlarının belirlenerek, ihtiyaçlar doğrultusunda bilgi güvenliği eğitimlerinin verilmesi önem arz etmektedir.

Bilgi güvenliği araştırmalarının ulusal düzeyde yapılmasının önemli olduğu düşünülmektedir. Örneğin gelişmiş ülkelerdeki devlet politikaları çocuk ve gençlerin bilgi güvenliklerini sağlama konusunda bireysel olarak yapılacakların dışında da ciddi teknik ve yasal önlemler aldırabilmektedir. Ancak bu durum ülkeden ülkeye değişebilmektedir. Bu nedenle bilgi güvenliği araştırmalarına ulusal düzeyde bakılması önemlidir. İlgili alanyazın incelemesinde ülkemiz koşullarındaki çocuk ve gençlerin bilgi güvenliklerini sağlama konusunda çeşitli çalışmalar gerçekleştirildiği görülmektedir. Ancak söz konusu araştırmaların bir kısmında bilgi güvenliğinin çocuk ve gençler üzerinde oluşturabileceği olası etkilerden ve bilgi güvenliği eğitiminin öneminden bahsedilirken (Canbek ve Sağıroğlu, 2007; Ceylan, 2013; Çelen, Çelik ve Seferoğlu, 2011; Çubukçu ve Baysan, 2013; Demirel, Yörük ve Özkan, 2012; Ersoy ve Ersoy, 2008; Öğün ve Kaya, 2013; Şahinaslan, Kandemir ve Şahinaslan, 2009; Şahinaslan, Kantürk, Şahinaslan ve Borandağ, 2009; Vural ve Sağıroğlu, 2008), bir kısmında da güvenliğin sağlanabilmesi için gerekli teknik yöntemlerden (Canbek ve Sağıroğlu, 2006; Öğün ve Kaya, 2013; Yavanoğlu, Sağıroğlu ve Çolak, 2012; Zeydan, 2006) ve yasal-idari düzenlemelerden (Ersoy, 2007; Hekim ve Başıbüyük, 2013; Koç ve Kaynak, 2010; Tekerek, 2008) bahsedilmektedir. Söz konusu araştırmalarda da belirtildiği üzere çocuk ve gençlerin güvenli BİT kullanım davranış ve ihtiyaç durumlarını saptayarak, söz konusu ihtiyaçların giderilmesine yönelik yeni çalışmalara ihtiyaç duyulmaktadır.

1.1. Araştırmanın Amacı

Zorunlu eğitim süreçlerinden geçerek üniversiteye gelen öğrencilerin bilgi güvenliğine ilişkin davranış durumlarını ortaya koymayı amaçlayan bu çalışmadan elde edilen bulgular doğrultusunda MEB'in Bilişim Teknolojileri ve Yazılım dersi müfredatında öğrenci ihtiyaçlarına bağlı olarak hangi konulara yer verilmesi gerektiği konusunda öneriler getirilmiştir.

2. YÖNTEM

Araştırmanın bu bölümünde araştırma modeli, çalışma grubu, veri toplama aracı ile verilerin analiz ve yorumlanmasına ilişkin bilgilere yer verilmiştir.

2.1. Araştırma Modeli

Araştırmada nicel ve nitel araştırma yöntemleri kullanılmıştır. Bu çalışma iki aşamada gerçekleştirilmiştir. Araştırmanın ilk aşamasında araştırmacılar tarafından geliştirilen bir anket aracılığıyla öğrencilerin güvenli BİT kullanımına ilişkin davranışlar nicel olarak betimlenmeye çalışılmıştır. Araştırmanın ikinci aşamasında ise nicel olarak betimlenen davranışların derinlemesine analizinin yapılabilmesi için araştırmacılar tarafından geliştirilen öğrenci görüşlerini belirleme formu aracılığıyla elde edilen veriler içerik analizi kullanılarak bulgular özetlenmiştir.

2.2. Çalışma Grubu

Araştırmada MEB'in ilk ve ortaöğretim süreçlerinden geçerek üniversiteye başlayan öğrencilerin güvenli BİT kullanım davranışlarının ortaya konulması ve buna bağlı olarak MEB'in ilk ve ortaöğretim Bilişim Teknolojileri ve Yazılım ders müfredatında verilecek olan bilgi güvenliği eğitimlerine yönelik öneriler getirilmesi amaçlanmıştır. Bu nedenle araştırmanın verilerinin MEB'in ilk ve ortaöğretim müfredatlarındaki bilişim teknolojileri derslerini alan öğrencilerden elde edilmesi önemlidir. Araştırmanın verileri 2012-2013 akademik yılı güz döneminde üniversite birinci sınıfa devam eden 124 öğrenciden elde edilen verilerle sınırlıdır. Söz konusu öğrencilerle yapılan görüşme sonrasında öğrencilerin MEB'in ilk ve ortaöğretim müfredatlarındaki bilişim teknolojileri dersleri dışında bilişim teknolojisiyle ilgili herhangi bir ders ya da kurs almadıkları görülmüştür. Öğrencilerin demografik bilgilerine ilişkin veriler Tablo 1'de verilmiştir.

Tablo 1: Öğrencilerin Demografik Bilgilerine İlişkin Veriler

Değişken	Grup	N	%
Cinsiyet	Kadın	75	60.5
	Erkek	49	39.5
Yaş	16-20	87	70.2
	21-25	37	29.8
Bilgisayar, Tablet ya da Akıllı Telefona Sahip Olma Durumu	Var	99	79.8
	Yok	25	20.2
Sosyal Ağa Üyeliği	Var	116	93.5
	Yok	8	6.5

Tablo 1 incelendiğinde öğrencilerin yaklaşık %60'ının kadın, %40'ının da erkek olduğu; yaklaşık %70'inin 16-20 yaş aralığında, %30'ununda 21-25 yaş aralığında olduğu görülmektedir. Söz konusu öğrencilerin yaklaşık %80'i bilgisayara sahip iken, %20'sinin ise bilgisayara sahip

olmadığı görülmektedir. Ayrıca öğrencilerin %93.5'inin sosyal ağlara üye olduğu, %6.5'inin ise üye olmadığı görülmektedir.

2.3. Veri Toplama Aracı

Araştırmada nicel veri toplama aracı olarak bilgi güvenliği farkındalık anketi; nitel veri toplama aracı olarak ise öğrenci görüşlerini belirleme formu kullanılmıştır. Veri toplama araçları araştırmacılar tarafından geliştirilmiştir. Veri toplama araçlarındaki maddeler alanyazın incelemesine bağlı olarak araştırmacılar tarafından hazırlandıktan sonra eğitim teknolojisi alanından üç uzman maddeleri kapsam geçerliliği açısından, bir Türk dili uzmanı da dil ve anlatım açısından incelemiştir. Uzmanların görüşleri doğrultusunda maddeler üzerinde gerekli düzenlemeler yapılarak maddelere son şekli verilmiştir. Anketten elde edilen veriler frekans ve yüzde şeklinde ifade edilerek yorumlanmıştır. Nitel veri analizinde öğrenci görüşlerini belirleme formu aracılığıyla öğrencilerden elde edilen veriler bağımsız iki araştırmacı tarafından kodlanarak alt temalar ortaya konulmaya çalışılmış ve bu alt temalar frekans ve yüzde olarak ifade edilmeye çalışılarak, konuyla ilgili öğrenci görüşlerinden örnekler verilmiştir.

Alanyazın taraması ve uzmanlardan gelen öneriler doğrultusunda yapılan kapsam geçerliliği sonucunda yukarıda açıklanan nicel ve nitel veri toplama araçlarında BİT kullanımı konusunda kullanıcı davranışlarıyla ilgili mevcut durumu belirlemeye yönelik olarak; bilgisayara erişim güvenliği, zararlı programlar ve korunma yolları, sosyal mühendislik, parola güvenliği, dosya erişim ve paylaşım güvenliği, yedekleme yapma, internet ve ağ güvenliği, kablolu ve kablosuz modem güvenliği, e-posta güvenliği konularına ilişkin maddeler yer almaktadır.

3. BULGULAR

Araştırmanın bu bölümünde nicel ve nitel veri toplama araçlarından elde edilen bulgulara ilişkin bilgilere yer verilmiştir.

3.1. Nicel Verilere İlişkin Bulgular

Gerçekleştirilen nicel analizler doğrultusunda, öğrencilerin antivirüs programı kullanma durumuna ilişkin bulgular Tablo 2'de verilmiştir.

Tablo 2: Antivirüs Programı Kullanma Durumuna İlişkin Bulgular

Antivirüs Programı Kullanma Durumu	Frekans	Yüzde
Kullanıyorum	105	84.7
Kullanmıyorum	19	15.3
Toplam	**124**	**100.0**

Tablo 2 incelendiğinde, öğrencilerin %84.7'si antivirüs programı kullandığını (f=105), %15.3'ü ise antivirüs programı kullanmadığını (f=19) belirtmektedir.

Gerçekleştirilen nicel analizler doğrultusunda, üniversite öğrencilerinin antivirüs programını ne sıklıkla güncellediğine ilişkin bulgular Tablo 3'te verilmiştir.

Tablo 3: Antivirüs Programını Güncelleme Durumuna İlişkin Bulgular

Antivirüs Programını Güncelleme Durumu	Frekans	Yüzde
Otomatik Güncellerim	36	29.0
Günlük Güncellerim	5	4.0
Haftalık Güncellerim	20	16.1
Aylık Güncellerim	31	25.0
Altı Ayda Bir Güncellerim	12	9.7
Yıllık Güncellerim	2	1.6
Güncelleme Yapmıyorum	18	14.5
Toplam	**124**	**100.0**

Tablo 3 incelendiğinde antivirüs programını, öğrencilerin %29.0'u otomatik olarak güncellediğini (f=36), %4.0'ü günlük (f=5), %16.1'i haftalık (f=20), %25.0'i aylık (f=31), %9.7'si altı ayda bir (f=12), %1.6'sı yıllık (f=2) güncellediğini belirtmekte olup %14.5'i ise güncelleme yapmadıklarını (f=18) ifade etmiştir.

Gerçekleştirilen nicel analizler doğrultusunda, öğrencilerin girdikleri web sitesi veya kullandıkları programın güvenli olup olmadığına dikkat etme durumuna ilişkin bulgular Tablo 4'te verilmiştir.

Tablo 4: Girilen Web Sitesi veya Kullanılan Programın Güvenli Olup Olmadığına Dikkat Etme Durumuna İlişkin Bulgular

Web Sitesi veya Programın Güvenli Olup Olmadığına Dikkat Etme Durumu	Frekans	Yüzde
Dikkat Ederim	63	50.8
Dikkat Etmem	61	49.2
Toplam	**124**	**100.0**

Tablo 4 incelendiğinde girdikleri web sitesi veya kullandıkları programın güvenli olup olmadığına, öğrencilerin %50.8'i dikkat ettiğini (f=63), %49.2'si ise dikkat etmediğini (f=61) belirtmektedir. Bu sonuçlara göre öğrencilerin yaklaşık yarısının girdikleri web sitesinin ya da kullandıkları programın güvenli olup olmadığına yeterince dikkat etmediği görülmektedir.

Gerçekleştirilen nicel analizler doğrultusunda, öğrencilerin korsan yazılım kullanma durumuna ilişkin bulgular Tablo 5'te verilmiştir.

Tablo 5: Korsan Yazılım Kullanma Durumuna İlişkin Bulgular

Korsan Yazılım Kullanma Durumu	Frekans	Yüzde
Kullanıyorum	48	38.7
Kullanmıyorum	76	61.3
Toplam	**124**	**100.0**

Tablo 5 incelendiğinde öğrencilerin %38.7'si korsan yazılım kullandığını (f=48), %61.3'ü ise kullanmadığını (f=76) belirtmektedir. Bu sonuçlara göre öğrencilerin %38.7'si korsan yazılım kullanımından kaynaklanabilecek tehditlere açık olduğu görülmektedir.

Gerçekleştirilen nicel analizler doğrultusunda, öğrencilerin bilgisayar ortamındaki verileri ne sıklıkla yedeklediklerine ilişkin bulgular Tablo 6'da verilmiştir.

Tablo 6: Yedekleme Yapma Durumuna İlişkin Bulgular

Yedekleme Yapma Durumu	Frekans	Yüzde
Günlük	7	5.6
Haftalık	10	8.1
Aylık	40	32.3
Altı Ayda Bir	23	18.5
Yıllık	12	9.7
Yedekleme Yapmıyorum	32	25.8
Toplam	**124**	**100.0**

Tablo 6 incelendiğinde öğrencilerin %5.6'sı verilerini günlük (f=7), %8.1'i haftalık (f=10), %32.3'ü aylık (f=40), %18.5'i altı ayda bir (f=23), %9.7'si yıllık (f=12) güncellediğini belirtmekte olup %25.8'i ise yedekleme yapmadıklarını (f=32) ifade etmiştir. Öğrencilere yedekleme yaparken tercih ettikleri ortam sorulduğunda ise yedekleme yapan öğrencilerin %56.5'i usb belleği, %13.72'si aynı bilgisayarı, %13.7'si taşınabilir diskleri (hard disk), %11.3'ü cd/dvd'yi, %2.4'ü başka bilgisayarı, %1.6'sı web ortamını, %0.8'i ise diğer ortamları tercih ettiklerini belirtmiştir. Bu bulgudan hareketle öğrencilerin yarısından fazlası usb belleği yedekleme için

tercih ettikleri görülmektedir. Ancak usb belleklerin zararlı program bulaşma olasılığı en yüksek olan ortamlardan biri olması nedeniyle bu ortamlarda yapılan yedeklemelerin zarar görebileceği düşünülmektedir. Bu nedenle öğrencilerin yedekleme yapılacak ortamlar konusunda bilinçlendirilmesi önemlidir.

Gerçekleştirilen nicel analizler doğrultusunda, öğrencilerin bilgisayarlarındaki dosyaları internette paylaşıma açma durumuna ilişkin bulgular Tablo 7'de verilmiştir.

Tablo 7: Bilgisayardaki Dosyaları İnternette Paylaşıma Açma Durumuna İlişkin Bulgular

Bilgisayardaki Dosyaları İnternette Paylaşıma Açma Durumu	Frekans	Yüzde
Paylaşıma Açıyorum	26	20.9
Paylaşıma Açmıyorum	98	79.0
Toplam	**124**	**100.0**

Tablo 7 incelendiğinde öğrencilerin %20.9'u bilgisayarlarındaki dosyaları paylaşıma açtığını (f=26), %79.0'u ise paylaşıma açmadığını (f=98) belirtmektedir. Bu sonuçlar yaklaşık olarak öğrencilerin %21'inin dosya paylaşımından kaynaklanabilecek bilgi güvenliği tehditleriyle karşı karşıya kalabileceklerini göstermektedir.

Gerçekleştirilen nicel analizler doğrultusunda, öğrencilerin internetten video, müzik, film gibi dosya veya programları yasal siteler dışındaki sitelerden indirme durumuna ilişkin bulgular Tablo 8'de verilmiştir.

Tablo 8: İnternetten Video, Müzik, Film gibi Dosya veya Programları Yasal Siteler Dışındaki Sitelerden İndirme Durumuna İlişkin Bulgular

İnternetten Video, Müzik, Film gibi Dosya veya Programları Yasal Siteler Dışındaki Sitelerden İndirme Durumu	Frekans	Yüzde
İndiriyorum	103	83.1
İndirmiyorum	21	16.9
Toplam	**124**	**100.0**

Tablo 8 incelendiğinde internetten video, müzik, film gibi dosya veya programları yasal siteler dışındaki sitelerden indirme durumuyla ilgili olarak, öğrencilerin %83.1'i indirdiğini (f=103), %16.9'u ise indirmediğini (f=21) belirtmektedir.

Gerçekleştirilen nicel analizler doğrultusunda, öğrencilerin şifre gerektiren işlemlerde aynı şifreyi kullanma durumuna ilişkin bulgular Tablo 9'da verilmiştir.

Tablo 9: Şifre Gerektiren İşlemlerde Aynı Şifreyi Kullanma Durumuna İlişkin Bulgular

Şifre Gerektiren İşlemlerde Aynı Şifreyi Kullanma Durumu	Frekans	Yüzde
Aynı Şifreyi Kullanırım	67	54
Aynı Şifreyi Kullanmam	57	46.0
Toplam	**124**	**100.0**

Tablo 9 incelendiğinde öğrencilerin %54'ü şifre gerektiren işlemlerde aynı şifreyi kullandığını (f=67), %46.0'sı ise aynı şifreyi kullanmadığını (f=57) belirtmektedir. Bu sonuçlara göre öğrencilerin aynı şifre kullanımından kaynaklanabilecek bilgi güvenliği tehditleriyle karşı karşıya kalabileceklerini göstermektedir.

Gerçekleştirilen nicel analizler doğrultusunda, öğrencilerin internet kafe, okul, alışveriş merkezi gibi ortak kullanım alanlarında internetten alışveriş yapma durumuna ilişkin bulgular Tablo 10'da verilmiştir.

Tablo 10: Ortak Kullanım Alanlarında İnternetten Alışveriş Yapma Durumuna İlişkin Bulgular

Ortak Kullanım Alanlarında İnternetten Alışveriş Yapma Durumu	Frekans	Yüzde
Alışveriş Yaparım	36	29.0
Alışveriş Yapmam	88	71.0
Toplam	**124**	**100.0**

Tablo 10 incelendiğinde öğrencilerin %29'u internet kafe, okul gibi ortak kullanım alanlarında internetten alışveriş yaptığını (f=36), %71.0'i ise yapmadığını (f=88) belirtmektedir. Bu sonuçlar öğrencilerin %29'unun ortak kullanım alanlarından alışveriş yapmaktan kaynaklanabilecek bilgi güvenliği tehditleriyle karşı karşıya kalabileceklerini göstermektedir.

Gerçekleştirilen nicel analizler doğrultusunda, öğrencilerin internete erişim yerlerine ilişkin bulgular Tablo 11'de verilmiştir.

Tablo 11: Öğrencilerin İnternete Erişim Yerlerine İlişkin Bulgular

İnternete Erişim Yerleri	Frekans
Ev	96
İnternet Kafe	21
Arkadaşımdan/Komşumdan	15
Okul	46

Tablo 11 incelendiğinde üniversite öğrencilerinin büyük çoğunluğu internete evden (f=96) erişirken bunu sırasıyla internet kafe (f=21), arkadaşımdan/komşumdan (f=15) ve okuldan/işyerinden (f=46) seçenekleri takip etmektedir. Bu sonuçlar öğrencilerin ortak kullanım alanlarında internet kullanımından kaynaklanabilecek bilgi güvenliği tehditleriyle karşı karşıya kalabileceklerini göstermektedir. Örneğin okul gibi ortamlarda bilgisayarın çoğunluğunda güvenliği sağlamak adına antivirüs programları olmasına rağmen antivirüs programlarının güncellenmemesi gibi nedenlere bağlı olarak özellikle taşınabilir depolama aygıtları üzerinden zararlı programlar bulaşabilmektedir.

3.2. Nitel Verilere İlişkin Bulgular

Bilgisayara başkalarının erişimini engellemek adına öğrencilerin aldıkları önlemlerle ilgili belirtilen görüşler doğrultusunda yapılan nitel veri analizi sonucu ortaya çıkan alt temalar Tablo 12'de gösterilmektedir.

Tablo 12: Bilgisayara Başkalarının Erişimini Engellemek Adına Öğrencilerin Aldıkları Önlemlere İlişkin Nitel Analiz Sonuçları

Alt Temalar	f	%
Kullanıcı adı ve parola kullanma	87	50.3
Güvenlik duvarı kullanma	17	9.8
Antivirüs programı kullanma	10	5.8
Dosyalara şifre koyma	10	5.8
Önlem almıyorum	8	4.6
Bilgisayarın başından kalkınca oturumu şifre ile kapatma	8	4.6
Önlem almadan dosyaları paylaşıma açmama	7	4.0
Güvenlik yazılımlarını güncelleme	6	3.5
Modeme kullanıcı adı ve parola koyma	5	2.9
İnternetten gelen ve kaynağı bilinmeyen tekliflere yanıt vermeme	5	2.9
Bilgisayarın fiziksel güvenliğini sağlama	3	1.7
Başkalarına ait taşınabilir depolama aygıtlarını bilgisayara takmama	2	1.2
Bilgisayarı başkalarıyla ortak kullanmama	2	1.2
BIOS'a kullanıcı adı ve şifre koyma	1	0.6
Parmak izi ile giriş yapma	1	0.6
Kablosuz ağları ve ortak ağları kullanmama	1	0.6
Toplam	**173**	**100**

Tablo 12 incelendiğinde kullanmış oldukları bilgisayara başkalarının erişimini engellemek adına öğrencilerin aldıkları önlemlere ilişkin öğrencilerin %50.3'ü "Kullanıcı adı ve parola koyma" (f=87), %9.8'i "Güvenlik duvarı kullanma" (f=17), %5.8'i "Antivirüs programı kullanma" (f=10), %5.8'i "Dosyalara şifre koyma" (f=10) şeklinde yanıt vermektedir. Yanıtlar incelendiğinde kullanıcı adı ve parola, güvenlik duvarı kullanımının erişimleri engellemede işe

yarayabileceği ancak tek başına yeterli olmayacağı düşünülmektedir. Örneğin öğrencilerin %1.2'si "Bilgisayarı başkalarıyla ortak kullanmama" şeklinde yanıt vermektedir. Her ne kadar güvenlik duvarı aktif hale getirilse de eğer bilgisayar başkalarıyla ortak kullanılıyorsa dışarıdan erişimlere açık olunmaktadır. Öğrencilerin bu konuya dair görüş ve değerlendirmelerinden bazıları şu şekildedir:

"*Güvenlik duvarı ayarları mı zaman zaman kontrol ediyorum. Tanımadığım kişilerden gelen e-postaları açmıyorum.*"

"*Bilgisayarda erişilmesi gereken bir şey olmadığı için herhangi bir önlem almıyorum.*"

Parola güvenliğini sağlamak adına öğrencilerin aldıkları önlemlerle ilgili belirtilen görüşler doğrultusunda yapılan nitel veri analizi sonucu ortaya çıkan alt temalar Tablo 13'te gösterilmektedir.

Tablo 13: Parola Güvenliğini Sağlamak Adına Öğrencilerin Aldıkları Önlemlere İlişkin Nitel Analiz Sonuçları

Alt Temalar	f	%
Kolay tahmin edilecek şifreler yerine uzun ve karışık şifreler oluşturma	47	34.1
Şifreyi başkalarıyla paylaşmama	26	18.8
Harf, rakam ve özel karakter içeren şifreler kullanma	23	16.7
Şifreyi zaman zaman güncelleme	14	10.1
Aynı şifreyi farklı ortamlarda kullanmama	9	6.5
En az sekiz karakterden oluşan şifre kullanma	5	3.6
Şifre oluştururken deyim gibi kalıp ifadelere şifrede yer vermeme	4	2.9
Şifre oluştururken ad, soyad, doğum tarihi, doğum yeri kişisel bilgilere şifrede yer vermeme	2	1.4
Şifreyi ajanda gibi bir yerlere kaydetmeme	2	1.4
Akılda kalıcı parolalar kullanma	2	1.4
Başka bilgisayarlardan mümkün olduğunca kullanıcı adı ve şifre gerektiren işlemleri yapmama	2	1.4
Şifre oluşturmada klavyede ya da sistematik olarak art arda gelen harf ya da rakamlara yer vermeme	2	1.4
Toplam	**138**	**100**

Tablo 13 incelendiğinde parola güvenliğini sağlamak adına öğrencilerin aldıkları önlemlere ilişkin öğrencilerin %34.1'i "Kolay tahmin edilecek şifreler yerine uzun ve karışık şifreler oluşturma" (f=47), %18.8'i "Şifreyi başkalarıyla paylaşmama" (f=26), %16.7'si "Harf, rakam ve özel karakter içeren şifreler kullanma" (f=23), %10.1'i "Şifreyi zaman zaman güncelleme" (f=14) şeklinde görüş bildirmektedir. Örneğin çok az öğrencinin parola oluşturmada "Şifre oluşturmada klavyede ya da sistematik olarak art arda gelen harf ya da rakamlara yer vermeme" (f=2, %1.4) şeklinde davranış gösterdiği görülmektedir. Bunun da konuyla ilgili bilgi ve farkındalık eksikliğinden kaynaklanabileceği düşünülmektedir. Öğrencilerin bu konuya dair görüş ve değerlendirmelerinden bazıları şu şekildedir:

"Parolamı sayılardan ve rakamlardan oluşturuyorum. Parolamı hatırla gibi seçeneklerden uzak duruyorum."

"İnternet ve bilgisayarı benden başkası kullanmadığı için özel bir önlem almıyorum."

İnternet ortamında dosya paylaşımı yaparken bilgi güvenliğini sağlamak adına öğrencilerin aldıkları önlemlerle ilgili belirtilen görüşler doğrultusunda yapılan nitel veri analizi sonucu ortaya çıkan alt temalar Tablo 14'te gösterilmektedir.

Tablo 14: İnternet Ortamında Dosya Paylaşımı Yaparken Bilgi Güvenliğini Sağlamak Adına Öğrencilerin Aldıkları Önlemlere İlişkin Nitel Analiz Sonuçları

Alt Temalar	f	%
Dosyanın/dosyaların paylaştığım kişiler dışında başkaları tarafından görünüp görünmediğine dikkat etme	30	27.0
İnternet ortamında dosya paylaşımı yapmama	20	18.0
Paylaşacağım/paylaşılan dosyanın virüslü olup olmadığına dikkat etme	19	17.1
Dosya paylaşımında aldığım herhangi bir güvenlik önlemi yoktur	16	14.4
Paylaşım yapılan sitenin/ortamın güvenli olup olmadığına dikkat etme	14	12.6
Paylaşılan dosyaların kişisel bilgileri içerip içermemesine dikkat etme	4	3.6
Dosya paylaşımı yaparken paylaşılan dosyanın şifrelenmesine dikkat etme	4	3.6
Paylaşılacak dosyaları ayrı bir klasör altında toplayarak paylaşma	2	1.8
Kaynağı bilinmeyen dosyaları açmama	1	0.9
Paylaşılan dosyaların yedeklenmesine dikkat etme	1	0.9
Toplam	**111**	**100**

Tablo 14 incelendiğinde internet ortamında dosya paylaşımı yaparken bilgi güvenliğini sağlamak adına alınan önlemlere ilişkin öğrencilerin %27.0'ı "Dosyanın/dosyaların paylaştığım kişiler dışında başkaları tarafından görünüp görünmediğine dikkat etme" (f=30), %18.0'ı "İnternet ortamında dosya paylaşımı yapmama" (f=20), %17.1'i "Paylaşacağım/paylaşılan dosyanın virüslü olup olmadığına dikkat etme" (f=19), %14.4'ü "Dosya paylaşımında aldığım herhangi bir güvenlik önlemi yoktur" (f=16) şeklinde görüş bildirmektedir. Örneğin öğrencilerin bazıları dosya paylaşımında "Paylaşılacak dosyaları ayrı bir klasör altında toplayarak paylaşma" (f=2, %1.8) şeklinde yanıt vermektedir. Bu durum dosya paylaşımını kolaylaştırması açısından kullanışlı olsa da güvenliği sağlamaya doğrudan bir katkısının olmadığı düşünülmektedir. Bu durumda yine kullanıcı bilgi ve farkındalık durumuna dikkat çekmektedir. Öğrencilerin bu konuya dair görüş ve değerlendirmelerinden bazıları şu şekildedir:

"Paylaşımlarımın kendi arkadaşlarım dışındaki kişilerin görmesini engelliyorum."

"Fazla dosya paylaşımı yapmıyorum, güvenlik için ne yapılması gerekiyor tam olarak bilmiyorum."

Zararlı programlardan korunmak adına öğrencilerin aldıkları önlemlerle ilgili belirtilen görüşler doğrultusunda yapılan nitel veri analizi sonucu ortaya çıkan alt temalar Tablo 15'te gösterilmektedir.

Tablo 15: Zararlı Programlardan Korunmak Adına Öğrencilerin Aldıkları Önlemlere İlişkin Nitel Analiz Sonuçları

Alt Temalar	f	%
Antivirüs programı kullanma	76	38.2
Antivirüs programını güncelleme	32	16.1
Güvenlik duvarını aktif kılma	23	11.6
Bilinmeyen web sitelerine girmeme	14	7.0
Kaynağı bilinmeyen dosyaları açmama	9	4.5
E-posta içeriklerinin güvenli olup olmadığına dikkat etme	8	4.0
Reklam içerikli web sitelerine tıklamama	8	4.0
Güvenli şifre kullanımına dikkat etme	6	3.0
Başkalarına ait taşınabilir aygıtları bilgisayara takmama	6	3.0
Korsan yazılım/program vb. kullanmama	6	3.0
Herhangi bir önlem almıyorum	6	3.0
Dosyaları bilgisayarda açmadan önce güvenlik taraması yapma	3	1.5
Yedekleme yapma	1	0.5
Güvenli dosya paylaşımlarına dikkat etme	1	0.5
Toplam	**199**	**100**

Tablo 15 incelendiğinde zararlı programlardan korunmak adına öğrencilerin aldıkları önlemlere ilişkin öğrencilerin %38.2'si "Antivirüs programı kullanma" (f=76), %16.1'i "Antivirüs programını güncelleme" (f=32), %11.6'sı "Güvenlik duvarını aktif kılma" (f=23), %7'si "Bilinmeyen web sitelerine girmeme" (f=14) şeklinde ifade etmektedir. Örneğin çok az öğrenci zararlı programlardan korunmak adına "Korsan yazılım/program vb. kullanmama" (f=6, %3) şeklinde yanıt vermiştir. Zararlı programlardan korunmak adına antivirüs kullanımı gibi çeşitli önlemler alınsa da eğer bilgisayar ya da mobil aygıtta kullanılan yazılım korsan ise yine bilgi güvenliği açıkları olabilecektir. Bu nedenle bu konularda öğrenci bilgi ve farkındalığının artırılması önemlidir. Öğrencilerin bu konuya dair görüş ve değerlendirmelerinden bazıları şu şekildedir:

"Antivirüs programı kullanıyorum ve güvenmediğim dosya ve sitelere girmemeye özen gösteriyorum."

"İstesek de istemesek de bunlar bir şekilde bize ulaşan şeyler ve yeri geldiğinde antivirüs programı bile bunları yakalayamıyor o yüzden çok fazla önlem almıyorum. Gerekli gördüğümde antivirüs programıyla müdahale ediyorum o kadar."

E-posta güvenliğini sağlamak adına öğrencilerin aldıkları önlemlerle ilgili belirtilen görüşler doğrultusunda yapılan nitel veri analizi sonucu ortaya çıkan alt temalar Tablo 16'da gösterilmektedir.

Tablo 16: E-Posta Güvenliğini Sağlamak Adına Öğrencilerin Aldıkları Önlemlere İlişkin Nitel Analiz Sonuçları

Alt Temalar	f	%
Kaynağı bilinmeyen e-postaları açmadan silme	52	39.1
Güvenli şifre kullanma	28	21.1
Tanımadıkları kişilerden gelen e-postalara yanıt vermeme	10	7.5
İstenmeyen e-postaları açmama	9	6.8
Şifre kullanımı dışında bir şeye dikkat etmeme	7	5.3
E-posta şifresini zaman zaman güncelleme	6	4.5
E-posta adresini tanımadıkları kişilerle paylaşmama	6	4.5
Antivirüs programı kullanma	5	3,8
E-posta ile kişisel bilgileri paylaşmama	3	2.3
E-postaları gruplandırmaya/filtreleme dikkat etme	2	1.5
Karşı tarafın iletişim bilgilerinin e-postada olup olmadığına dikkat etme	2	1.5
Önemli işlerde e-postayı kullanmama	1	0.8
Halka açık yerlerde kablosuz ağ üzerinden e-posta hesabına giriş yapmama	1	0.8
Şüpheli gördükleri e-postalarda teyit amaçlı karşı tarafı telefonla arama	1	0.8
Toplam	**133**	**100**

Tablo 16 incelendiğinde e-posta güvenliğini sağlamak adına öğrencilerin aldıkları önlemlere ilişkin öğrencilerin %39.1'i "Kaynağı bilinmeyen e-postaları açmadan silme" (f=52), %21.1'i "Güvenli şifre kullanma" (f=28), %7.5'i "Tanımadığım kişilerden gelen e-postalara yanıt vermeme" (f=10), %6.8'i "İstenmeyen e-postaları açmama" (f=9) şeklinde ifade etmektedir. Örneğin çok az öğrenci "E-posta ile kişisel bilgileri paylaşmam" (f=3, %2.3) şeklinde yanıt vermiştir. Her ne kadar güvenli şifre kullanımı, antivirüs programı kullanımı gibi önlemlere dikkat edilse de eğer e-postada kişisel bilgiler paylaşılıyorsa söz konusu kişiler sosyal mühendislik saldırılarına maruz kalabilirler. Bu konularda da öğrenci bilgi ve farkındalığının artırılması yararlı olacaktır. Öğrencilerin bu konuya dair görüş ve değerlendirmelerinden bazıları şu şekildedir:

"Tanımadığım ve şüphelendiğim kişilerden gelen e-postaları derhal spam olarak işaretliyorum ve engelliyorum."

"Şifre kullanımı dışında bu konuda şimdiye kadar hiçbir şeye dikkat etmedim."

Kablolu ve kablosuz ağ güvenliğini sağlamak adına öğrencilerin aldıkları önlemlerle ilgili belirtilen görüşler doğrultusunda yapılan nitel veri analizi sonucu ortaya çıkan alt temalar Tablo 17'de gösterilmektedir.

Tablo 17: Kablolu ve Kablosuz Ağ Güvenliğini Sağlamak Adına Öğrencilerin Aldıkları Önlemlere İlişkin Nitel Analiz Sonuçları

Alt Temalar	f	%
Modem şifresini tanımadık kişiler ile paylaşmama	42	50.6
Kullandıktan sonra modemi kapatma	8	9.6
Herhangi bir önlem almam	8	9.6
Modemin alınışında gelen arayüz şifresini değiştirme	7	8.4
Tahmin edilmesi zor şifreler oluşturma	7	8.4
Modem şifresini zaman zaman güncelleme	5	6.0
Modemi ve kablosuz ağı başkalarıyla ortak kullanıma açmama	4	4.8
Modemde kullanılmayan portları kapatma	2	2.4
Toplam	**83**	**100**

Tablo 17 incelendiğinde kablolu ve kablosuz ağ güvenliğini sağlamak adına öğrencilerin aldıkları önlemlere ilişkin öğrencilerin %50.6'sı "Modem şifresini tanımadıklarımla paylaşmama" (f=42), %9.6'sı "Kullandıktan sonra modemi kapatma" (f=8), %9.6'sı "Herhangi bir önlem almam" (f=8), %8.4'ü "Modemin alınışında gelen arayüz şifresini değiştirme" ve "Tahmin edilmesi zor şifreler oluşturma" (f=7) şeklinde ifade etmektedir. Örneğin çok az öğrenci "Modemde kullanmadığım portları kapatma" (f=2, %2.4) şeklinde yanıt vermiştir. Bu durumun doğrudan konu hakkında bilgi sahibi olma ile ilişkisi olduğu düşünülmektedir. Her ne kadar modem şifresini zaman zaman güncelleme gibi önlemlere dikkat edilse de modemdeki kullanılmayan portlar kapatılmadığı sürece kullanıcılar bu açıklıklardan dolayı bilgi güvenliği tehditleriyle karşı karşıya kalabilirler. Bu konularda da öğrenci bilgi ve farkındalığının artırılması yararlı olacaktır. Öğrencilerin bu konuya dair görüş ve değerlendirmelerinden bazıları şu şekildedir:

"Kablosuz ağ güvenlik şifremi kimseyle paylaşmıyorum. Evime gelen eşim dostum cep ten internete girmek isterse şifremi vermek zorunda kalırsam da kimseyle paylaşmaması konusunda uyarıyorum. Çok yayıldığını düşünürsem de değiştirebiliyorum."

"Modemimi kullanmadığım zaman kapalı tutmaya ve modem şifremi kimseyle paylaşmamaya dikkat ediyorum."

Nicel ve nitel veri analizi sonuçları genel olarak değerlendirildiğinde öğrencilerin bilgi güvenliğini sağlama konusunda temel düzeyde güvenlik önlemi aldığı anlaşılmaktadır. Örneğin çoğu öğrenci zararlı programlardan korunmak için antivirüs programı kullanımının yeterli olduğunu düşünmekte ve ek önlemler almamakta ya da bu ek önlemleri bilmemektedir. Analiz sonuçlarına dayalı olarak yine öğrencilerin güvenlik konusunda bir takım yanlış bilgilere de sahip olduğu görülmektedir. Örneğin öğrencilerin bir kısmı tanımadıkları kişilerden gelen e-postaları istenmeyen e-posta olarak düşünmekte ve bu e-postaları okumadan silmektedirler.

4. TARTIŞMA VE SONUÇ

Yükseköğretim programlarında öğrenim gören öğrencilerin güvenli BİT kullanım davranışlarını belirlemeyi amaçlayan bu çalışmadan elde edilen sonuçlara genel olarak bakıldığında öğrencilerin belirli bir güvenli BİT kullanım davranışları gösterdiği ancak bunların gelişen ve hızla değişen teknolojik koşulların oluşturduğu yeni durumlara yanıt vermede yetersiz olduğu görülmektedir. Yapılan analiz sonuçları öğrencilerin bilgisayara erişim güvenliği, zararlı programlar ve korunma yolları, sosyal mühendislik, parola güvenliği, dosya erişim ve paylaşım güvenliği, internet ve ağ güvenliği, e-posta güvenliği, yedekleme yapma konularında temel düzeyde ve en popüler olarak bilinen güvenlik önlemlerinden yalnızca bir ya da birkaçını aldığını, diğer güvenlik önlemlerini ise almadıklarını göstermektedir. Öğrencilerin diğer güvenlik önlemlerini almamalarının temelinde yatan neden öğrencilerin ek güvenlik tedbirlerini bilmemeleri ve/veya tek bir güvenlik önlemi almanın bilgi güvenliğini sağlamada yeterli olacağını düşünmeleri olabilir. Örneğin, öğrencilerin büyük çoğunluğu zararlı programlardan korunmak için antivirüs programı kullanarak önlem aldıklarını düşünmekte ve antivirüs programı kullanımı dışındaki güvenlik önlemlerini çok az öğrencinin aldığı görülmektedir. Ayrıca öğrencilerin bilgi güvenliğini sağlamak adına yaptıkları doğru bilinen bazı hatalı davranışlar bilgi güvenliğini riske sokabilmektedir. Bu nedenle söz konusu konularla ilgili öğrenci bilgi ve farkındalığının artırılarak bunun davranışa dönüştürülmesi bilişim teknolojileri öğretmenlerine düşen önemli bir sorumluluktur.

Araştırma bulguları, bilgisayara başkalarının erişimini engellemek adına öğrencilerin yaklaşık olarak yarısının kullanıcı adı ve parola kullanımı ile önlem aldıklarını; ancak çok az öğrencinin bilgisayarını başkalarıyla ortak kullanmamaya dikkat ettiğini göstermektedir. Dolayısıyla ortak kullanım yapılması durumunda erişim güvenliğini sağlamada parola ile önlem almanın etkisi de azalacaktır. Bunun dışında antivirüs programı, güvenlik duvarı kullanımı, bilgisayarın başından kalkınca oturumu şifre ile kapatma, bilgisayarın fiziksel güvenliğini sağlama gibi önlemlere ise çok fazla dikkat etmediklerini göstermektedir. Bu nedenle bilgisayarın fiziksel güvenliği ve erişim güvenliğini sağlamak adına kullanıcı adı ve parola kullanımı dışındaki önlemler konusunda öğrencilerin bilgi ve farkındalıklarının artırılması faydalı olacaktır.

Araştırma bulgularına göre öğrencilerin çoğunluğu zararlı programlardan korunmak adına antivirüs programları kullandıklarını belirtmiştir. Ancak bulgular öğrencilerin antivirüs programlarını düzenli olarak güncellemediklerini ve bu konuya çok fazla önem vermediklerini

göstermektedir. Gelişen teknolojiye bağlı olarak zararlı programlara her gün bir yenisinin eklenmesi ise güncelleme işleminin ne kadar önemli olduğuna işaret etmektedir. Dolayısıyla antivirüs programı kullanımı ve güncellenmesi konularında öğrenci bilgi ve farkındalığının artırılması gerekmektedir. Benzer şekilde bir diğer araştırma bulgusu öğrenciler arasında korsan yazılım kullanımının yaygın olduğunu göstermektedir. Bu nedenle söz konusu öğrenciler korsan yazılım kullanımından kaynaklanabilecek tehditlerle karşı karşıya kalabilirler. Bunu önlemek adına öğrencilerin zararlı programların neler olduğu, hangi yollarla bulaşabileceği ve bunlardan korunmak adına neler yapılabileceği, yasal yazılım/program kullanımının önemi ve bu konudaki yasal ve etik boyut hakkında öğrencileri bilgilendirmek önemlidir.

Araştırma bulguları öğrencilerin çoğunluğunun yedekleme yapmadığını ya da üç aydan daha uzun süreli olarak yedekleme yaptıklarını, yedekleme yapanların büyük bir kısmının ise yedeklemelerini usb belleklere ya da aynı bilgisayara yaptıklarını göstermektedir. Bu bulgular öğrencilerin yedekleme yapmaya çok fazla önem vermediğini ve yedekleme yapma konusunda doğru bilgi ve davranışları göstermediklerini ortaya koymaktadır. Örneğin usb belleklerin zararlı program bulaşma olasılığı en yüksek olan depolama ortamlarından biri olduğu dikkate alındığında bu ortamlarda yedekleme yapmanın riskler oluşturduğu göze çarpmaktadır. Bu nedenle öğrencilere verilecek olan bilgi güvenliği eğitimleri kapsamında yedekleme yapmanın önemi, ne sıklıkla ve hangi ortamlarda yedekleme yapmanın doğru olacağının açıklanması uygun olacaktır.

Araştırmadan elde edilen bir diğer sonuca göre öğrencilerin önemli bir kısmı internet ve ağ ortamında dosya paylaşımı yaptıklarını belirtmektedirler. Dosyaları paylaşıma açmadıklarını belirten öğrenciler ise bunun temel nedenini dosya paylaşımının nasıl yapılacağını bilmedikleri ve dosya paylaşımını güvenli bulmadıkları şeklinde belirtmektedir. Dosya paylaşımı yapan öğrencilerin büyük çoğunluğu ise paylaşımla ilgili herhangi bir güvenlik önlemi almadıklarını belirtmektedir. Bu nedenle öğrencilere dosya paylaşımının nasıl yapılacağı, paylaşım esnasında hangi güvenlik önlemlerinin alınması gerektiği ve nitel analiz bulgularında belirtilen bu konudaki yanlış davranışlar konusunda kullanıcıların bilinçlendirilmesi faydalı olacaktır. Ayrıca araştırmanın bir diğer sonucuna göre öğrencilerin yarısına yakını internetten video, müzik, film gibi dosya veya programları yasal siteler dışındaki sitelerden indirdiklerini belirtmiştir. Bu bulgudan hareketle öğrencilerin yasal site/program kullanımıyla ilgili etik davranışlar konusunda bilgilendirilmesinin ve yasal olmayan kaynaklardan edinilecek

dosya ve program kullanımının verebileceği zarar konusunda farkındalıklarının artırılması yararlı olacaktır.

Araştırma bulguları öğrencilerin yaklaşık yarısının kullanıcı adı ve şifre gerektiren ortamların çoğunda benzer şifreyi kullandıklarını göstermektedir. Ayrıca öğrencilerin çok az bir kısmının parola güvenliğini sağlama konusunda; şifreyi başkalarıyla paylaşmama; harf, rakam ve özel karakter içeren şifreler kullanma; şifreyi zaman zaman güncelleme; en az sekiz karakterden oluşan şifre kullanma; şifre oluştururken deyim gibi kalıp ifadelere şifrede yer vermeme; şifre oluştururken ad, soyad, doğum tarihi, doğum yeri kişisel bilgilere şifrede yer vermeme; şifreyi ajanda gibi başkalarının görebileceği bir yerlere kaydetmeme gibi tedbirleri aldıklarını göstermektedir. Bu nedenle öğrencilere verilecek parola güvenliği ile ilgili eğitimlerde güvenli parola oluşturmada nelere dikkat edilmesi gerektiğinin açıklanması yararlı olacaktır.

Araştırma bulguları öğrencilerin çoğunun ortak kullanım alanlarından internete girdiklerini ve bu alanlarda internetten alışveriş yaptıklarını göstermektedir. Kablolu ve kablosuz ağ güvenliğinin sağlanması konusunda ise öğrencilerin yarısına yakını modem şifresini tanımadık kişiler ile paylaşmama şeklinde önlem almaktadır. Fakat modem şifresini güncelleme, şifreyi başkalarıyla paylaşmama, kullanılmayan portları kapatma gibi önlemleri ise çok az öğrencinin aldığı görülmektedir. Bu nedenle ortak kullanım alanlarında internet kullanımından, kablolu ve kablosuz ağ kullanımından kaynaklanabilecek bilgi güvenliği ihlal ve tehditlerine karşın öğrencilerin internet ve ağ güvenliği konusunda bilinçlendirilmesinin ve farkındalığının artırılmasının yararlı olacağı düşünülmektedir.

E-posta kullanımı ile ilgili bulgular incelendiğinde bazı öğrencilerin bilgi güvenliğini sağlamak adına istenmeyen e-posta alanına gelen postaları okumadan sildikleri görülmektedir. Ancak istenmeyen e-posta dışındaki postalarında istenmeyen e-posta alanına düşebileceği dikkate alındığında kullanıcılar bu konuda bilgi kayıpları yaşayabilirler. Ayrıca bulgular öğrencilerin sosyal mühendislik amaçlı gönderilen e-postaları ayırt etmede zorlandıklarını ve bu postaları dikkate alabildiklerini göstermektedir. Bu nedenle öğrencilere e-posta güvenliğinin sağlanması, sosyal mühendislikle mücadele adına neler yapılabileceği konusunda eğitimler verilmesi faydalı olacaktır.

Yukarıda belirtilen konular dışında öncelikle öğrencilere bilgi güvenliği ve önemi, bilgi güvenliği ile kullanıcı sorumluluğu hakkında bilgi verilerek bilgi güvenliğinin ne olduğu, ne tür

davranışların güvenli nelerin güvensiz olduğu, bilgi güvenliği ihlallerin kullanıcıları ne gibi tehlikelerle karşı karşıya bırakabileceğinin, bilgi güvenliğinin sağlanması konusunda kullanıcılara ne gibi sorumluluklar düştüğü konularında farkındalıklarının artırılması gerekmektedir. Çünkü bu konuda yeterli farkındalığa sahip olmayan kullanıcıların güvenli BİT kullanım davranışlarını da göstermeyeceği düşünülmektedir.

Türk eğitim sisteminin genel amaçlarından biri de bireylerin beden, zihin, ahlâk, ruh ve duygu bakımından dengeli ve sağlıklı şekilde gelişimlerini tamamlamalarına yardımcı olmaktır. BİT'teki gelişim ve değişmelerin yansımaları sonucunda bireysel ve toplumsal hayatta önemli ve köklü değişiklikler yaşanır olmuştur. Türk eğitim sistemi de bireylerin beden, zihin, ahlâk, ruh ve duygu bakımından dengeli ve sağlıklı şekilde gelişimlerini sağlamada bu değişimlere ayak uydurmalıdır. Örneğin internet teknolojilerinin ucuzlaması ve hızlanmasına bağlı olarak hemen hemen her birey bu teknolojiyi kullanır duruma gelmiştir. Bu teknolojinin aşırı ve doğru olmayan kullanımına bağlı olarak da bireylerin çeşitli bilgi güvenliği tehdit ve saldırılar ile karşı karşıya kalmakta, bu durumun ortaya çıkması ise bireylere maddi ve manevi zararlar verebilmektedir.

Milli Eğitim Bakanlığı öğrencilerin bilgi güvenliği konusundaki farkındalıklarını artırmak amacıyla hazırlanan Bilişim Teknolojileri ve Yazılım dersi çerçeve programında öğrenci ihtiyaçlarına göre bilgi güvenliği konularında da eğitim verilmesi gerektiğini belirtmektedir (Talim ve Terbiye Kurulu Başkanlığı Kararı, 2012). Bu noktada bilgi güvenliği konusunda öğrencilerin ihtiyaçları, yaşadıkları problemlerin belirlenmesi önemlidir. Söz konusu dersler kapsamında bilgi güvenliği konularının öğretiminde bu araştırmadan elde edilen bulgular dikkate alınarak gerçekleştirilecek bilgi güvenliği eğitimlerinin öğrenci ihtiyaçlarına uygun olacağı düşünülmektedir.

Günümüzde Z kuşağının temsilcileri olarak adlandırılan çocukların sokakta oyun oynamak yerine tablet bilgisayarlarıyla sosyalleştikleri dikkate alındığında ihtiyaca uygun bilgi güvenliği eğitimlerinin erken yaşta verilmesinin ne denli önemli olduğu sonucuna varılmaktadır. Okul öncesi dönemden üniversiteye kadar eğitimin her sürecinde verilmesi gereken bilgi güvenliği eğitimleri ile öğrencilerin farkındalık düzeyleri artırılabilir.

KAYNAKLAR

Adams, A. & Sasse, M. A. (1999). Users are not the enemy. *Communications of The ACM, 42*(12), 40-46.

Besnard, D. & Arief, B. (2004). Computer security impaired by legitimate users. *Computers and Security*, *23*, 253-264.

Brostoff, S. & Sasse, M. A. (2001). Safe and sound: A safety-critical approach to security. *Proceedings New Security Paradigms Workshop, 41-47. New York: The Association for Computing Machinery Press*. Web: http://citeseer.ist.psu.edu/brostoff01safe.html adresinden 3 Mayıs 2012'de alınmıştır.

Canbek, G. ve Sağıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. *Gazi Üniversitesi Politeknik Dergisi, 9*(3).

Canbek, G. ve Sağıroğlu, Ş. (2007). Çocukların ve gençlerin bilgisayar ve internet güvenliği. *Gazi Üniversitesi Politeknik Dergisi, 10*(1).

Ceylan, Y. (2013). Türkiye'de çocukların güvenliğine yönelik "güvenli internet" uygulamasının yazılı basında yankıları. *Akademik Bakış Dergisi, 37*.

Çelen, F. K., Çelik, A. ve Seferoğlu, S. S. (2011). Çocukların internet kullanımları ve onları bekleyen çevrim-içi riskler. *XIII. Akademik Bilişim Konferansı (AB11). İnönü Üniversitesi, Malatya, 2-4.*

Chou C., Chan, P. S. & Wu, H. C. (2007). Using a two-tier test to assess students' understanding and alternative conceptions of cyber copyright laws. *British Journal of Educational Technology, 38*(6), 1072-1084.

Chou, C., Condron, L. & Belland, J. C. (2005). A review of the research on internet addiction. *Educational Psychology Review, 17*(4), 363-388.

Colwill, C. (2009). Human factors in information security: The insider threate who can you trust these days? *Information Security Technical Report*, *14*, 186-196.

Demirel, M., Yörük, M. ve Özkan, O. (2013). Çocuklar için güvenli internet: Güvenli internet hizmeti ve ebeveyn görüşleri üzerine bir araştırma. *Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 4*(7), 54-68.

Egan, M. (2004). *The executive guide to information security: Threats, challenges and solutions*. Harlow: Addison-Wesley.

Ersoy, E. (2007). Gizlilik, bireysel haklar, kişisel verilerin korunması. *Akademik Bilişim Konferansı 2007.*

Ersoy, A. F. ve Ersoy, A. (2008). İnternet ve çocuk hakları eğitimi. *Web:* http://ietc2008.home.anadolu.edu.tr/ adresinden 12 Kasım 2013 tarihinde alınmıştır.

Fatih Projesi Çalıştay Raporu. (2012). Web: http://fatih.inetd.org.tr/Calistay/Fatih-calistay-rapor.pdf adresinden 5 Eylül 2013'de alınmıştır.

Gonzales, J. J. & Sawicka, A. (2002). A framework for human factors in information security. *Presented at the 2002 WSEAS Int. Conf. On Information Security. Rio de Janerio*. Web: http://ikt.hia.no/josejg/ adresinden 2 Eylül 2013'de alınmıştır.

Hekim, H. ve Başıbüyük, O. (2013). Siber suçlar ve türkiye'nin siber güvenlik politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi, 4*(2).

Jones, A. & Colwill, C. (2008). Dealing with the malicious insider. *In Australian Information Security Management Conference (p. 52)*.

Kaşıkçı, D. N., Çağıltay, K., Karakuş, T., Kurşun, E. ve Ogan, C. (2014). Türkiye ve avrupa'daki çocukların internet alışkanlıkları ve güvenli internet kullanımı. *Eğitim ve Bilim, 39*(171).

Koç, S. ve Kaynak, S. (2010). Bilişim suçları bağlamında yeni medya olarak internet ve kişisel güvenlik. *Akademik Bilişim Konferansı 2010.*

Mahabi, V. (2010). *Information security awareness: system administrators and end-users perspectives at florida state university.* Electronic Theses, Treatises and Dissertations.

Markotten, D. G. (2002). User-centered security engineering. Web: http://tserv.iig.uni-freiburg.de/telematik/atus/publications/Ge2002.pdf adresinden 12 Ağustos 2013'de alınmıştır.

Maxion, R. A. & Reeder, R. W. (2005). Improving user-interface dependability through mitigation of human error. *International Journal of Human Computer Studies*, *63*(1-2), 25-50.

Mart, İ. (2012). *Bilişim kültüründe bilgi güvenliği farkındalığı*. Yüksek Lisans Tezi, Kahramanmaraş Sütçü İmam Üniversitesi Fen Bilimleri Enstitüsü.

Öğün, M. N. ve Kaya, A. (2013). Siber güvenliğin milli güvenlik açısından önemi ve alınabilecek tedbirler. *Güvenlik Stratejileri Dergisi, 18*, 145-181.

Poulsen, K. (2000). Mitnick to lawmakers: People, phones and weakest links. Web: http://www.politechbot.com/p-00969.html adresinden 13 Mart 2013'de alınmıştır.

Şahinaslan, E., Kandemir, R. ve Şahinaslan, Ö. (2009). Bilgi güvenliği farkındalık eğitim örneği. *XI. Akademik Bilişim Konferansı Bildirileri, Şanlıurfa.*

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

Talim ve Terbiye Kurulu Başkanlığı Kararı (2012). Web: http://ttkb.meb.gov.tr/ adresinden 26 Şubat 2014' tarihinde alınmıştır.

Tekerek, M. (2008). Bilgi güvenliği yönetimi. *KSÜ Fen ve Mühendislik Dergisi, 11*(1), 132.

Vroom, C. & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers and Security*, *23*(3), 191-198.

Vural, Y. ve Sağıroğlu, Ş. (2008). Ülke bilgi güvenliği. *3. Uluslararası Katılımlı Bilgi güvenliği ve Kriptoloji konferansı, 25-27 Aralık 2008, Ankara.*

Wagner, A. E. & 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.

Wishart, J. M., Oades, C. E. & Morris, M. (2007). Using online role play to teach internet safety awareness. *Computers & Education, 48*(3), 460-473.

Yavanoğlu, U., Sağıroğlu, Ş. ve Çolak, İ. (2012). Sosyal ağlarda bilgi güvenliği tehditleri ve alınması gereken önlemler. *Gazi Üniversitesi Politeknik Dergisi, 15*(1).

Zeydan, Ö. (2006). Kişisel bilgisayarlar ve internet güvenliği. *XI. "Türkiye'de İnternet" Konferansı, 21 - 23 Aralık 2006, TOBB Ekonomi ve Teknoloji Üniversitesi, Ankara*.

SUMMARY

It is seen that most of the studies towards ensuring information security are on such methods as security walls, strong authentication methods and safety models; and technical studies towards developing software. It is also seen that some of the studies carried out are on penal policies and sanctions, directives and developing models on information security. In the literature, very few studies are found on determining the errors caused by human factor and on removing these errors. When the fact that the weakest link in information security chain is human, it is understood that more attention should be paid on determining information security mistakes and violations caused by human and on resolving these mistakes and violations. The fact that it is human beings who develop, manage and use security systems, for which big investments are made, the human factor goes beyond the technical dimension in ensuring information security.

Preventing human-based mistakes and violations in protecting institutions and users against information security threats is of great importance. At this point, it is necessary to train and improve the awareness of both institutions and individuals on information security threats. When all these are taken into account, this current study will work on identifying information security mistakes and violations of students studying at higher education programmes and forming the objective and scope of the information security trainings to be provided in line with the needs and deficiencies to be presented. The study was conducted on 124 first year students. When Table 1 is examined, it is seen that almost 60% of the sample group were female students while 40% were male students. It is also seen that 70% of the students are between 16-20 years of age while 30% are 21-25 years of age. 80% of the students in the sample group have computers while 20% did not. Moving from this data, it is seen that the sample group on which information security study has been carried out are young adults who have computer and similar devices. Data were analyzed using the qualitative and quantitative methods.

When the results of the current study, which aims to determine the information security mistakes and violations of students studying at higher education programmes, are examined it is seen that students have a certain level of awareness on information security, however, this level of awareness is inadequate to respond to the new situations that occur as a result of rapidly growing and changing technology. The results of the analyses carried out shows that students take basic safety measures on such issues as computer access safety, password security, uploading and updating software, file access and sharing security, backup, detrimental programmes, social engineering, internet and network safety, security walls, protection, web safety, e-mail safety, modem safety and that they only take one or a few most well-known measures and that they do not take other safety measures. Among the main reasons behind the fact that students do not take other safety measures are students do not know these measures and the misconception that taking one measure would be enough. While

this is the case concerning the adult learners at higher education, the case for learners at lower levels of education is believed to be a lot more worrying.

The results of the study showed that almost 15% of the students did not use an antivirus software; while almost 14% of them never updated their anti-virus software; almost 50% of the them did not always pay attention to whether the web site or program is secure when they entered a web site or used a program. Besides, it is seen that almost 15% of the students opened the e-mails intended for social engineering. It is also found in the study that almost 40% of the students used piracy software. The results of the study also reveal that almost 20% of the students shared filed and almost 80% did not. Among the reasons of not sharing files is facing with information security threats, which is remarkable. According to another result of the study, almost 54% of the students said that they used the same password in different mediums. Based on this result, password of a student who shares their password belonging to a system or whose password belonging to a system has been hacked will be under the risk. Almost 29% of the students in the study said that they did shopping online. This result is a finding which shows why information security factors should be paid attention to. Possible mistakes during shopping might lead to both financial losses and intangible damages. According to another finding of the study, almost 66% of the students use internet in public areas. This result emphasizes the significance of information security measures to be followed while accessing internet in public areas.

The results from the study reveal that most of the students at higher education institutions take information security measures at basic level but that these measures are only at basic level and they do not take more than one measure. Considering the fact that the sample group on which this study had been carried out was university students, it is predicted that the results would be more negative. Taking the fact that today's Z generation is socializing via IPad instead of tipcat, the importance of providing information security trainings at early ages becomes clear. Through information security trainings which should be provided at every phase of education from preschool education until university education could increase students' level of awareness.