Mustafa Kemal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi
Mustafa Kemal University Journal of Graduate School of Social Sciences
Yıl/Year: 2016 ♦ Cilt/Volume: 13 ♦ Sayı/Issue: 33, s. 178-193

ÖĞRETMEN ADAYLARININ BİLİŞİM SUÇLARINA YÖNELİK DENEYİMLERİ VE BİLİŞİM GÜVENLİĞİ DERS İÇERİĞİNE YÖNELİK GÖRÜŞLERİ

Ömer Faruk GÖKMEN
Sakarya Üniversitesi, Eğitim Fakültesi, BÖTE Bölümü, ofgokmen@sakarya.edu.tr
Özcan Erkan AKGÜN
İstanbul Medeniyet Üniversitesi, Eğitim Bilimleri Fakültesi, BÖTE Bölümü,
ozcan.akgün@medeniyet.edu.tr

Özet

Bu araştırmanın amacı, eğitim fakültesinde okuyan öğretmen adaylarının bilişim suçlarıyla ilgili deneyimlerinin ve bilişim güvenliği dersi içeriğinde yer alması gereken konulara yönelik görüşlerinin tespit edilmesidir. Çalışma nitel araştırma yöntemlerinden olgu bilim deseni ile yürütülmüştür. Araştırmanın çalışma grubunu, farklı öğretmenlik programlarında okuyan öğretmen adayları oluşturmuştur. Çalışma kapsamında yarı-yapılandırılmış görüşmeler gerçekleştirilmiştir. Görüşmeler ile toplanan veriler üzerinde içerik analizi yapılmıştır. Araştırma sonuçlarına göre; bazı öğretmen adaylarının bilişim suçu işledikleri, bilişim suçuna maruz kaldıkları, bilişim suçu konusunda bilgilerinin olmadığı ve bir bilişim suçuyla karşılaştıklarında ne yapabileceklerini bilmedikleri tespit edilmiştir. Ayrıca öğretmen adaylarının birçoğunun bilişim güvenliğinin tanımı ve kapsamı konusunda yetersiz bilgiye sahip oldukları görülmüştür. Son olarak öğretmen adaylarının; bilişim teknolojilerinin güvenli kullanımı, kişisel bilgilerin güvenliğini sağlama, bilişim güvenliğini tehdit eden unsurlara karşı önlemler alma, güvenlik yazılımları, güvenli çevrimiçi alışveriş ve internet bankacılığı, web sitelerinin güvenliği, sosyal ağların güvenli kullanımı, güvenli şifre oluşturma, virüslerden korunma, güncellemeler, e-posta hesaplarının güvenliği, işletim sisteminin güvenliği gibi konularda eğitime ihtiyaç duydukları belirlenmiştir. Buradan yola çıkarak ileride hazırlanacak bilişim güvenliği eğitimlerinin içeriğinin belirlenmesinde bu araştırmanın sonuçlarının dikkate alınmasının faydalı olacağı düşünülmektedir.

Anahtar Kelimeler: *Bilişim Güvenliği, Bilişim Suçu, Öğretmen Adayları, İhtiyaç analizi.*

TEACHER CANDIDATES' EXPERIENCES OF CYBER CRIME AND THEIR VIEWS FOR THE INFORMATION SECURITY COURSE CONTENT

Abstract

The purpose of this study is to determine student teachers' experience of cybercrime and their opinions about what should be the content of information technology security course. The study was conducted with phenomenology model of qualitative research methods. The study group of the study was consisted of student teachers from different teaching programs. In scope of this study semi-structured interviews were carried out. For data analysis, content analysis was conducted on data collected through interviews. According to the results it was identified that some of the student teachers' are exposed to cybercrimes, some of them have no information about cybercrime and some of them have no knowledge about what they can do when faced with a cybercrime. Besides it was found that many student teachers' have no sufficient knowledge regarding to the definition and scope of information technology security. Finally, student teachers have expressed that they need to learn some important security topics. The topics are identified as; safe use of information technology, ensuring the security of personal information, taking security precautions against the information technology threats, learning and using security software installation, secure online shopping and internet banking, security of the website, safe use of social networks, generating secure password, protection from viruses, security updates, security of the e-mail account, security of operating systems. From these findings, it is considered that it will be useful to take into account the results of this research in determining the content of the information security training in the future studies.

Key Words: *Information Security, Cyber Crime, Teacher candidates, Needs analysis.*

Giriş

Bilişim teknolojilerinde yaşanan hızlı gelişmeler yeni bir çağın başlamasında etkili olmuştur. Bilgi çağı olarak adlandırılan bu çağın en önemli araçları olan bilişim teknolojileri; birçok bireyin bir konuya dair bilgi ve kaynaklara ulaştığı, yeni insanlarla tanıştığı, alışveriş yaptığı ve her hangi bir olay hakkında anında haberdar olduğu araçlar olmuşlardır (Çalık ve Pınar, 2009). Bu teknolojiler sayesinde insanlar hızlı ve artan bir şekilde bilgi üretme, üretilen bilgiyi paylaşma, üretilen bilgiyi depolama ve bilgiye kolay ulaşma imkânına kavuşmuştur. Bunun neticesinde bilişim teknolojileri sayesinde bilgilere kolay, ucuz ve hızlı bir şekilde erişimin sağlanması toplum hayatında teknoloji tabanlı bir değişimi meydana getirmiştir. Bu değişim günlük yöntemlerimizi değiştirerek bilişim kültürünü yaratmıştır. Bu anlamda bilişim kültürü ile klasik yaşam biçimlerimizde değişmeler yaşandığı, yeni uğraşlar meydana geldiği ve yeni sorunlar meydana geldiği de açık bir şekilde görülmektedir (Gözgü ve Mutioğlu, 2012).

Son zamanlarda bilişim teknolojilerinin evlerde ve işletmelerde kullanımının artmasıyla beraber (Türkiye İstatistik Kurumu [TUİK], 2013) bireyler ve kurumlar pek çok etik ve güvenlik sorunu yaşamaktadırlar. Cerrah (2002) bilişim teknolojilerinin; bireyleri ve toplumu olumsuz etkileme, toplumun başarı ve bütünlüğünü bozma ve ahlak ilkelerinin dikkate alınmaması gibi ihlalleri doğurma potansiyelinin yüksek olduğuna dikkat çekmektedir. Çalık ve Pınar (2009) bilişim teknolojilerinin günlük yaşama gittikçe fazla indirgenmesinin aile içi ve genel olarak iletişimi azalttığını belirtmekte ve bunun yanında bilginin her kesime açık hale gelmesinin etik sorunlara da yol açtığını vurgulamaktadırlar. Batıgün ve Kılıç (2011) internetin kuşkusuz insanların pek çok ihtiyacını karşıladığını fakat bir yandan da sık kullanımı nedeniyle internet bağımlılığın gelişmesine neden olduğunu belirtmektedir. Bu konuda Ayas ve Horzum (2013) ailelerin ihmalkâr tutumunun öğrencilerin internet bağımlısı olmalarında önemli rolünün olduğunu ortaya çıkarmışlardır.

Dünya genelinde araştırmalar gerçekleştiren Symantec'in (2014) yayınladığı bilişim güvenliği tehdidi raporunda, her geçen gün tehdit türünün ve sayısının arttığı görülmektedir. Bu saldırıların daha çok zararlı yazılımlar, sahte web sitelerine yönlendirme, internet hizmetlerinin kesintisine sebep olan saldırılar ve sunuculara yönelik saldırılar şeklinde gerçekleştiği tespit edilmiştir. Ayrıca söz konusu raporda günümüzde kullanımı artan Android işletim sistemine sahip mobil telefonlara yönelik saldırıların da her geçen gün arttığına yönelik sonuçlara ulaşılmıştır. Benzer şekilde Marinos (2013) bilişim güvenliğini tehdit eden saldırıların en fazla; internetten kasıtlı veya kasıtsız indirilen programlar, zararlı yazılımlar, kod enjekte etme, hizmet kesintisi saldırıları, sahte web sitelerine yönlendirme, spam, veri ihlali, kimlik hırsızlığı, fiziksel zarar, bilgi sızdırma şeklinde gerçekleştiğini ve bu saldırıların kritik altyapılar, mobil bilişim, sosyal ağlar, bulut bilişim gibi alanlara yönelik olduğunu tespit etmiştir.

Artan bilişim güvenliği tehditlerinin neticesinde ülkemizde bilişim suçlarında da artış yaşanmıştır. Kaçakçılık ve Organize Suçlarla Mücadele (KOM) Daire Başkanlığı tarafından hazırlanan ve 2011 yılında yayınlanan rapora göre bilişim suçları ile ilgili fazla sayıda olay gerçekleştiği ve bu olayların en fazla; banka ve kredi kartı dolandırıcılığı, bilişim sistemleri (sisteme girme, engelleme, bozma, verileri yok etme), internet bankacılığı, internet aracılığıyla nitelikli dolandırıcılık, müstehcenlik, kumar ve gizlilik ihlali şeklinde işlendiği tespit edilmiştir. Bilişim güvenliği tehditlerinin artmasından ve bilişim suçlarında yaşanan artıştan yola çıkarak özellikle bireylere bilişim teknolojilerinin güvenli kullanımı konusunda bilgilendirmelerin yapılmasının önemli olduğu anlaşılmaktadır. Kaşıkçı, Çağıltay, Karakuş, Kurşun ve Ogan (2014) Türkiye ve 23 Avrupa ülkesinin dâhil olduğu "Avrupa Çevrimiçi Çocukları Projesi" bulgularını dikkate aldıkları araştırmalarında çocukların aşırı internet kullanımı, cinsel içerikli fotoğraf görme, siber zorbalığa maruz kalma, cinsel içerikli mesaj alma, internet üzerinden yeni kişilerle tanışma gibi çevrimiçi risklerle karşılaştıkları sonucuna ulaşmışlardır. Tekerek ve Tekerek (2013) öğrencilerin güvenli şifre kullanımı, çevrimiçi güvenli iletişim, kötücül yazılım denetlemesi yapma, belge koruma, kişisel bilgisayar güvenliği, güvenlik duvarı ve filtreleme yazılımları kullanımı gibi konularda bilgilerinin düşük olduğunu tespit etmişlerdir. Benzer şekilde alanyazında bireylerin bilişim güvenliğini tehdit eden unsurlar konusunda bilgilerinin düşük düzeyde olduğuna yönelik araştırma sonuçları bulunmaktadır (Akgün ve Topal, 2015; Dijle, 2006; Dijle ve Doğan 2011; Gökmen, 2014; Gökmen ve Akgün, 2015; Kaçıkçı ve diğer. 2014; Karaoğlan-Yılmaz, Yılmaz ve Sezer, 2014; Pusey ve Sadera, 2011; Shehri, 2012; Tekerek ve Mart, 2010; Tekerek ve Tekerek, 2013).

Alanyazındaki araştırma sonuçları göz önüne alındığında özellikle geleceğimizin teminatı çocuklarımızın bilinçli ve güvenli bilişim teknolojileri ve internet kullanımını sağlamak önemli bir durum olarak karşımıza çıkmaktadır. Bu konuda okullarda görev yapacak öğretmen adaylarının, öncelikle kendilerinin bilişim güvenliğini sağlama konusunda bilgili ve bilinçli olmaları ve öğrencilerini bu konularda bilgilendirme yeterliliğine sahip olmaları gerekmektedir. Nitekim Uluslararası Eğitimde Teknoloji Topluluğu (International Society for Technology in Education-ISTE) yayınladığı Ulusal Eğitim Teknolojisi Standartlarında (The National Educational Technology Standards-NETs) öğretmenlerin dijital bilginin ve teknolojinin güvenli, yasal ve etik kullanımını destekleme ve öğretme becerilerine sahip olmaları gerektiği ifade edilmektedir (ISTE, 2008).

Yurtdışında öğrencileri bilişim güvenliği konusunda bilgilendirebilme ve bu konuları öğretebilme yeterliliklerine yönelik gerçekleştirilen araştırmada, öğretmen adaylarının bilişim güvenliği konusunda sınırlı bilgilere sahip oldukları ve kendilerini pek çok bilişim güvenliği konusunu öğretme açısından yetersiz buldukları sonucuna ulaşılmıştır (Pusey ve Sadera, 2011). Benzer şekilde Tekerek ve Mart (2010) öğretmenlerin ve ebeveynlerin internette güvenliği sağlama konusunda yeterli bilinç düzeyine sahip olmadıklarını ve bu durumun endişe verici olduğunu

belirtmektedirler. Amerika Birleşik Devletleri'nde (ABD) National Cyber Security Alliance (NCSA) tarafından gerçekleştirilen araştırmada ise okullarda görev yapan öğretmenlerin öğrencilere öğrettikleri bilişim güvenliği konularının düşük seviyede olduğu tespit edilmiştir (NCSA, 2011). Pruitt-Mentle ve Pusey (2010) öğretmenlerin %25'inin şifre değiştirme, %14'ünün anti virüs yazılımı kullanma, %12'sinin bilişim korsanlığı, %16'sının güvenlik duvarı, %33'ünün sosyal ağların tehlikeleri, %39'unun yabancılarla bilgi paylaşma, %33'ünün özel hayata saygı gösterme gibi temel internet becerilerini öğrettikleri sonucuna ulaşmıştır.

Buradan hareketle öğretmen adaylarının bilişim güvenliği bilgilerini artıracak ve gerekli önlemleri almalarını sağlayacak bilişim güvenliği eğitimlerine ihtiyaç duydukları anlaşılmaktadır. Bu açıdan verilebilecek bilişim güvenliği eğitimlerinden önce bu eğitimlerin içeriğinde neler olmasının ve ihtiyaçların neler olduğunun tespit edilmesi gerekli görülmektedir. Ayrıca bu çalışmada tespit edilen ihtiyaçların ileride bilişim güvenliği eğitimlerinin içeriğinde hangi konuların olması gerektiğine ışık tutacağı düşünülmektedir. Araştırma kapsamında şu sorulara cevap aranmıştır:

1. Bilişim suçu ile ilgili hiç deneyiminiz oldu mu?
2. Bilişim suçuna maruz kalsanız ne yapmanız gerektiğini, nereye başvurmanız gerektiğini biliyor musunuz?
3. Bilişim güvenliği denince aklınıza neler gelmektedir?
4. Bilişim güvenliğini sağlamak için ihtiyaç duyduğunuz ve öğrenmek istediğiniz konular nelerdir?

Yöntem

Araştırma Modeli

Bu araştırma, nitel araştırma desenlerinden olgubilim (fenomenoloji) deseni ile gerçekleştirilmiştir. Yıldırım ve Şimşek (2013) olgu bilim desenlerini, farkında olduğumuz fakat derinlemesine ve ayrıntılı bir anlayışa sahip olmadığımız olgulara odaklanan desenler olarak tanımlamaktadırlar. Bu olgular yaşadığımız dünyada olaylar, deneyimler, algılar, yönelimler ve durumlar gibi çeşitli şekillerde karşımıza çıkabilmektedir (Yıldırım ve Şimşek, 2013). Dolayısıyla buradan yola çıkarak bu araştırmada öğretmen adaylarının bilişim güvenliğini sağlamaya yönelik ihtiyaçlarının neler olduğu ve bilişim güvenliğine yönelik bir eğitimin içeriğinde hangi konuların yer alması gerektiği olgusu araştırılmıştır. Araştırmanın gerçekleştirilmesinde yarı-yapılandırılmış görüşme türü kullanılmıştır. Büyüköztürk, Kılıç-Çakmak, Akgün, Karadeniz ve Demirel (2012) yarı-yapılandırılmış görüşmeleri, hem sabit seçenekli cevaplamayı hem de ilgili alanda derinlemesine bilgi edinmeyi birleştiren görüşme türü olarak tanımlamaktadır. Yarı-yapılandırılmış görüşme sırasında Büyüköztürk ve diğer. (2012)'nin belirtikleri görüşme süreci ilkeleri göz önüne alınarak kişisel yönlendirmelerden kaçınılmasına, yansız olunmasına ve her soru için maksimum cevabın alınmasına özen gösterilmiştir.

Katılımcılar

Araştırmanın katılımcılarını, Sakarya Üniversitesi Eğitim Fakültesinin yedi farklı programında okuyan son sınıf öğretmen adayları oluşturmaktadır. Araştırmanın katılımcıları oluşturulurken çeşitliliği artırmak amacıyla adayların farklı bölümlerinden olması dikkate alınmıştır. Öğretmen adaylarının bölümlerine ve cinsiyetlerine göre dağılımları Tablo 1'de verilmiştir.

Tablo 1. *Katılımcıların Demografik Bilgiler*

			n
Cinsiyet	Kadın		8
	Erkek		6
Bölüm	Bilgisayar ve Öğretim Teknolojileri Eğitimi		3
	Sınıf Öğretmenliği		3
	İlköğretim Matematik Öğretmenliği		2
	Fen Bilgisi Öğretmenliği		2
	Türkçe Öğretmenliği		2
	Sosyal Bilgiler Öğretmenliği		1
	İngilizce Öğretmenliği		1
		Toplam	14

Veri Toplama Aracı ve Verilerin Toplanması

Araştırmada veri toplama aracı olarak araştırmacılar tarafından geliştirilen ve açık uçlu sorulardan oluşan görüşme formu kullanılmıştır. Görüşme formunda beş soru yer almıştır. Görüşme formu bilişim suçları, bilişim güvenliği, siber zorbalık, internetin güvenli kullanımı, teknolojinin etkili ve güvenli kullanımı vb. gibi konularında tez ve araştırmalar yürüten 5 öğretim üyesine sunulmuştur. Uzmanlar, bilişim suçları ve bilişim güvenliği eğitimi içeriğine yönelik hazırlanan soruların yeterli ve uygun olduğunu belirterek, yapılacak görüşmelerle daha derinlemesine bilgi edinileceği konusunda görüş belirtmişlerdir. Görüşmelere başlanmadan önce bir öğretmen adayı ile görüşme gerçekleştirilerek soruların anlaşılırlığı test edilmiştir. Ayrıca görüşmeler gerçekleştirilmeden önce farklı programların son sınıflarında okuyan katılımcılarla birebir görüşülerek görüşme için uygun vakitlerde karar kılınmıştır. Görüşmeler, belirlenen gün ve saatte yapılmıştır. Bu sırada öğretmen adaylarının izni dâhilinde görüşmeler ses kayıt cihazı ile kaydedilmiştir. Ses Kayıt cihazı ile kaydedilen görüşmeler verilerin analizi için yazıya dökülmüştür

Verilerin Analizi

Araştırma kapsamında toplanan verilerde 2 araştırmacı tarafından içerik analizi yapılmıştır. Yıldırım ve Şimşek (2013) içerik analizinin, birbirine benzeyen verilerin belli kavramlar ve temalar altında bir araya getirilerek anlamlı şekilde düzenlenip yorumlanması şeklinde yapıldığını belirtmektedirler. İçerik analiz sürecinin dört aşamadan oluşmaktadır. Bunlar: (1) Verilerin kodlanması, (2) Temaların bulunması, (3) Verilerin kodlara ve temalara göre düzenlenmesi ve tanımlanması, (4) Bulguların yorumlanması (Yıldırım ve Şimşek, 2013). Dolayısıyla araştırmanın ilk aşamasında değerlendirmeciler, araştırmanın gizliliği kapsamında

öğretmen adaylarına ÖA1,ÖA2, ... ÖA14. şeklinde kodlar vermiş ve elde edilen verileri inceleyerek bir sözcük veya bir cümle şeklinde anlamlı kodlar oluşturmuşlardır. İkinci aşamada, kodları genel düzeyde açıklayan ve bu kodları belli kategoriler altında toplayan temalar belirlenmiştir. Bu aşamada değerlendirmecilerin çıkardığı kategoriler temalar için uyuşum yüzdesi hesaplanmıştır. Cohen'in kappa katsayısı hesaplanarak bu değer 0.81 olarak bulunmuştur. Bu uyuşum yüzdesi iyi derecede bir uyuşum yüzdesi olarak kabul edilmektedir (Landis ve Koch, 1977). Üçüncü aşamada oluşturulan kodlar ve temalar düzenlenerek anlamlı bir biçimde sunulmuştur. Son aşamada, ayrıntılı bir biçimde tanımlanan ve sunulan bulgular yorumlanmış ve gerekli yerlerde araştırma bulguları doğrudan alıntılarla desteklenmiştir (Yıldırım ve Şimşek, 2013).

Bulgular

Bu bölümde öğretmen adaylarının bilişim suçuna maruz kalma durumlarına, bilişim suçuna maruz kalındığında neler yapabileceklerine, bilişim güvenliği denince hangi anlamları çıkardıklarına ve bir bilişim güvenliği eğitiminin hangi konuları kapsaması gerektiğine yönelik görüşlerine yer verilmiştir.

Öğretmen Adaylarının Bilişim Suçuna Maruz Kalma Durumları

Öğretmen adaylarının bilişim suçuna maruz kalma durumları Tablo 2'de verilmiştir.

Tablo 2. *Öğretmen Adaylarının Bilişim Suçuna Maruz Kalma Durumları*

Kategoriler	**Katılımcılar**	**n**
Bilişim Suçunu Maruz Kalmadım	ÖA1,ÖA2,ÖA5, ÖA11,ÖA14	5
Fikrim Yok.	ÖA4,ÖA9, ÖA7, ÖA12	4
Bilişim Suçuna Maruz Kaldım	ÖA3,ÖA8,ÖA10	3
Bilişim Suçu İşledim	ÖA6,ÖA13	2
	Toplam	14

Tablo 2 incelendiğinde öğretmen adaylarının bilişim suçunu işleme, bilişim suçuna maruz kalma, bilişim suçuna maruz kalmama durumlarına yer verilmiştir. Öğretmen adaylarının 5'i bilişim suçuna maruz kalmadıklarını, 4'ü bilişim suçu ile ilgili bir fikirlerinin olmadığını, 3'ü bilişim suçuna maruz kaldıklarını ve 2'si bilişim suçu işlediklerini belirtmişlerdir. Bu konuya yönelik bazı öğretmen adaylarının görüşleri şu şekildedir:

ÖA6 : "*Bir okuldaki öğrencilerin kişisel verilerini ele geçirmiştim. Sonra ben de başka kişilerin tuzağına kurban gittim*."

ÖA8: "*Bir defasından Facebook hesabımı çaldılar. Hesabıma ondan sonra giremedim."*

ÖA10 : "*Ben bir ara internetten alışveriş yaparken farkında olmadan sitenin sahtesine kredi kartı bilgilerimi girdim. Daha sonra alışveriş yaptığım firma öyle bir isteğin olmadığını söyleyince hemen bankamı arayıp kredi kartını iptal ettirdim*."

ÖA11: "*Bilişim suçuna hiç maruz kalmadım. Bu konuda bir deneyimim olmadı*."

Tablo 2'den anlaşılacağı üzere öğretmen adaylarının yarısından fazlasının (9) bilişim suçuna maruz kalmadıkları ya da konuyla ilgili bilgilerinin olmadığı görülmektedir. Geriye kalan 5 öğretmen adayının bilişim suçları ile ilgili kötü deneyimlerinin olması endişe verici bir bulgu olarak düşünülmektedir. Bu bulgular, öğretmen adaylarının bilişim suçları konusunda bilgilendirmeye ve bilişim güvenliği eğitimlerine ihtiyaç duyduklarını göstermektedir. Ayrıca bu bulgular öğretmen adaylarına verilecek bilişim güvenliği eğitimlerinde bilişim suçları ile ilgili konulara değinilmesinin faydalı olacağı düşünülmektedir.

Öğretmen Adaylarının Bilişim Suçuyla Karşılaştıklarında Neler Yapabileceklerine Yönelik Görüşleri

Öğretmen adaylarının bilişim suçuyla karşılaştıklarında neler yapabileceklerine yönelik görüşleri Tablo 3'de verilmiştir.

Tablo 3. *Öğretmen Adaylarının Bilişim Suçuyla Karşılaştıklarında Neler Yapabileceklerine Yönelik Görüşleri*

Kategoriler	**Katılımcılar**	**n**
Ne Yapacağımı Bilmiyorum	ÖA2,ÖA3,ÖA4,ÖA5,ÖA6,ÖA8	6
Emniyet Müdürlüğü Siber Suçlar Birimine Başvururum	ÖA9,ÖA10,ÖA11,ÖA13,ÖA14	5
Hukuk Alanında Biriyle Görüşürüm.	ÖA1,ÖA7	2
Cumhuriyet Savcılığına Başvururum.	ÖA12	1
	Toplam	**14**

Tablo 3'te öğretmen adaylarının bilişim suçuyla karşılaştıklarında neler yapabileceklerine yönelik görüşlerine yer verilmiştir. Adayların yarısına yakını bir bilişim suçuyla karşılaştıklarında ne yapabileceklerini bilmediklerini belirtmişlerdir. Örneğin bu konuda ÖA2: "Hayır bilmiyorum. Çünkü daha önce başıma gelmedi." diyerek ne yapağını bilmediğini belirtmiştir. Ayrıca adayların 5'i Emniyet Müdürlüğü Siber suçlar birimine başvurabileceklerini, 2'si hukuk alanında ilgili biriyle görüşebileceğini, 1'i cumhuriyet savcılığına başvurabileceğini ifade etmişlerdir. Bu konuya yönelik öğretmen adayların bazı ifadeleri aşağıdaki gibidir:

ÖA1: "*Bilişim suçu ile ilgili bir suça maruz kalma durumumda ilk önce bu konuyu rahat bir şekilde konuşabileceğim hukuk alanında bir arkadaşımla görüşürüm*."

ÖA10: "*Türk ceza kanununda bununla ilgili maddeler olduğunu ve gerekirse emniyette siber suçlar birimine başvurabileceğimi biliyorum*."

ÖA11: "*Emniyet güçlerinin bilişim suçları ile mücadele bürosuna başvurabileceğimi biliyorum*."

ÖA3: "*Bilişim suçunun içine girer mi bilemiyorum ama sosyal medyada kullandığımız hesapların şifreleri de çalınabiliyor. Bu durumda açıkçası nereye başvurmamız gerektiği konusunda ise bir bilgim yok*."

Tablo 3'te görüldüğü üzere öğretmen adaylarının yarısına yakınının bilişim suçuna maruz kaldıklarında neler yapabilecekleri ve nereye başvuracakları konusunda bilgilerinin olmadığı anlaşılmaktadır. Dolayısıyla öğretmen adaylarına bilişim suçu ile karşılaştıklarında neler yapabilecekleri ve nereye başvurabilecekleri konusunda bilgilendirmelerin yapılmasının faydalı olacağı düşünülmektedir. Ayrıca öğretmen adaylarına verilecek bilişim güvenliği eğitimlerinde bilişim suçlarına maruz kaldıklarında neler yapmaları gerektiği konusunda adım adım izlenecek aşamaların belirtilmesi yararlı olacaktır.

Öğretmen Adaylarının Bilişim Güvenliği Denildiğinde Akıllarına Gelen Kavramlar

Öğretmen adaylarının bilişim güvenliğinin ne olduğuna yönelik sorulan soruya verdikleri cevaplara yönelik görüşleri Tablo 4'te verilmiştir.

Tablo 4. *Öğretmen Adayların Bilişim Güvenliği Denildiğinde Akıllarına Gelen Kavramlar*

Kategoriler	**Katılımcılar**	**f**
Bilişim Teknolojilerinin Güvenliği (Bilgisayar, Tablet, Akıllı Telefon, İnternet, Sosyal Ağlar, E-posta vb.)	ÖA1,ÖA2,ÖA3,ÖA6,ÖA7,ÖA8,ÖA10,Ö 11,Ö14	9
Virüslerden Korunma ve Anti-virüs Kullanımı	ÖA1,ÖA2,ÖA5,ÖA8,ÖA10,ÖA11, Ö14	7
Güvenli Bilgiye Erişme ve Kullanma	ÖA5,A9,ÖA11,ÖA12,ÖA13, ÖA14	7
Kişisel Bilgilerin Güvenliğinin Korunması	ÖA3,Ö4,Ö6,ÖA8,ÖA11,Ö12,ÖA14	7
Elektronik Ortamda Bilginin Korunması	ÖA2,ÖA5,ÖA9,ÖA11,ÖA12, ÖA14	6
Güvenli Şifre Kullanımı	Ö1,Ö4,ÖA5,ÖA6,ÖA8	5
Güvenli İnternet Bankacılığı Kullanımı	ÖA8,ÖA10,Ö13	3
Güvenli Online Alış-Veriş Yapma	ÖA5,ÖA7	2
İnternet Ortamında Uygunsuz Davranış ve İçeriklerden Korunma	ÖA5	1
Sanal Dolandırıcılıktan Korunma	ÖA8	1
	Toplam	**48**

Öğretmen adaylarının bilişim güvenliğinin ne olduğuna yönelik görüşleri ve bu görüşlerin söylenme sıklıkları Tablo 4'te belirtilmiştir. Tablodan anlaşılacağı üzere öğretmen adayları bilişim güvenliğini en çok bilişim teknolojilerinin güvenli kullanımı olarak görmektedirler. Örneğin bu konuda ÖA7: "*Bilişim güvenliği denince bilgisayarların, tabletlerin ve şu an yaygın bir şekilde kullandığımız akıllı telefonların güvenli kullanımı aklıma geliyor*." şeklinde görüşünü belirtmiştir. İkinci sırada ise virüslerden korunma ve anti-virüs kullanımı gelmektedir. Daha sonra öğretmen adaylarının 7'si bilişim güvenliğini "Güvenli Bilgiye Erişme ve Kullanma", 7'si "Kişisel Bilgilerin Güvenliğinin Korunması", 6'si "Elektronik Ortamda Bilginin Korunması", 5'i "Güvenli Şifre Kullanımı" olarak tanımlamaktadır. Bu konulara yönelik bazı öğretmen adaylarının görüşleri şu şekildedir:

ÖA8: "*İnternet bankacılığını kullanırken dikkatli olmak, sanal dolandırıcılıktan korunma, virüs programları kullanma, rakamların harflerin özel karakterlerin karışından oluşan güvenli şifreler oluşturma. Bunların hepsi bilişim güvenliğine giriyor diye düşünüyorum*."

ÖA14: "*Bilişim güvenliği bilişim teknolojilerinde yani bilgisayar, akılı telefon, internet, sosyal ağlar vb. teknolojilerinde bulunan bilgilerin korunması, değiştirilmemesi, bu teknolojileri kullanırken kişisel bilgilerimizin korunmasıdır. Ayrıca bilişim güvenliği doğru bilgiye güvenli şekilde erişmek demektir*."

Tablo 4'ten anlaşılacağı üzere bilişim güvenliği denince öğretmen adaylarının aklına pek çok konu gelmektedir. Genel itibari ile bilişim güvenliğinin bilişim teknolojilerinin güvenli kullanımı olduğu göz önüne alındığında, öğretmen adaylarının yarısına yakının bu şekilde görüş bildirmeleri olumlu bir bulgu olarak görülmektedir.

Öğretmen Adaylarının İhtiyaç Duydukları Bilişim Güvenliği Konuları

Öğretmen adaylarının öğrenmek istedikleri ve ihtiyaç duydukları bilişim güvenliği konularına yönelik görüşleri Tablo 5'te verilmiştir.

Tablo 5. *Öğretmen Adaylarının İhtiyaç Duydukları Bilişim Güvenliği Konuları*

Kategoriler	Katılımcılar	f
Bilgisayar, Tablet, Akıllı Telefon vb. Güvenliği	ÖA1,ÖA2,ÖA3,ÖA5,ÖA6, ÖA8,ÖA9, ÖA11,ÖA12,ÖA13,ÖA14	11
Kişisel Bilgilerin Güvenliği	ÖA1,ÖA2, ÖA4,ÖA6, ÖA8, ÖA9, ÖA10,ÖA11,ÖA12, ÖA13	10
Bilişim Güvenliğini İhlal Eden Yöntemlere Karşı Önlemler	ÖA1,ÖA3,ÖA4, ÖA6, ÖA7,ÖA8, ÖA9, ÖA12, ÖA13	9
Bilişim Güvenliğini Sağlayacak Yazılımlar	ÖA2,ÖA3,ÖA4,ÖA5, ÖA6,ÖA8,ÖA10, ÖA11, ÖA12	9
Bilişim Güvenliğinin Önemi	ÖA1,ÖA2,ÖA3, ÖA4,ÖA6,ÖA9,ÖA10, ÖA12	8
Güvenli İnternet Kullanımı	ÖA2,ÖA3, ÖA4,ÖA5,ÖA6,ÖA9, ÖA12,ÖA13	8
Güvenli Online Alış-Veriş	ÖA1,ÖA4,ÖA6,ÖA7, ÖA8 ÖA10, ÖA14	7
İnternet Bankacılığı güvenliği	ÖA1,ÖA2,ÖA6,ÖA7, ÖA8, ÖA10, ÖA14	7
Web Sayfaların Güvenliği	ÖA1,ÖA5, ÖA6,ÖA7,ÖA8, ÖA11, ÖA13	7
Sosyal Ağların Güvenli Kullanımı	ÖA1,ÖA2, ÖA4,ÖA5,ÖA8,ÖA9,ÖA14	7
Bilişim Suçları ve Korunma	ÖA2, ÖA7,ÖA9, ÖA11, ÖA14	5
Güvenli Şifre Kullanımı	ÖA2,ÖA6, ÖA7,ÖA11, ÖA14	5
Virüslerden Korunma ve Anti-virüs Kullanımı	ÖA2, ÖA4,AÖ5,ÖA9,ÖA11	5
Yazılımların Güncelleştirilmesi	ÖA2,ÖA5,ÖA8,ÖA11	4
E-Posta Hesaplarının Güvenli Kullanımı	ÖA6, ÖA7,ÖA11, ÖA14	4
İnternetteki Zararlı İçeriklerden Korunma	ÖA5, ÖA9	2
Yetkisiz Erişimden Korunma	ÖA1,ÖA11	2

İşletim Sistemi Güvenliği	ÖA5,ÖA6		2
İnternet Tarayıcısı Güvenliği	ÖA6, ÖA12		2
Sanal Dolandırıcılık	ÖA2,ÖA7		2
Bilişim Etiği	ÖA11		1
Kablosuz Ağ Güvenliği	ÖA11		1
		Toplam	**108**

Tablo 5'te öğretmen adaylarının bilişim güvenliğini sağlamaya yönelik verilecek veya hazırlanacak bir eğitimde hangi konuların yer alması gerektiğine yönelik görüşleri yer almaktadır. Adayların tamamına yakını bilişim teknolojilerinin (Bilgisayar, Tablet, Akıllı Telefon vb.) güvenli kullanımına yönelik konuların yer almasını istemektedirler. Ayrıca öğretmen adaylarının yarısından fazlası bilişim güvenliğini sağlamaya yönelik hazırlanacak bir eğitimde bilişim güvenliğinin önemine değinilmesi, kişisel bilgilerin güvenliğini sağlamaya yönelik bilgilerin yer alması, güvenli internet bankacılığı, bilişim güvenliğini ihlal eden unsur veya yöntemlere karşı alınabilecek önlemlerin olması, bilişim güvenliğini sağlayacak yazılımlara ve bu yazılımların kullanımlarına yer verilmesi gerektiğini belirtmişlerdir. Öğretmen adaylarının yine yaklaşık yarısı güvenli çevrimiçi alışveriş, güvenli internet bankacılığı, güvenli web sayfaları ve sosyal ağlarda güvenlik konularının hazırlanacak bilişim güvenliği eğitimlerinde yer almasının gerekli olduğunu ifade etmişlerdir. Bunların yanında az sayıda öğretmen adayı bilişim güvenliğine yönelik hazırlanacak bir eğitimin içeriğinde; bilgisayarlardaki yazılımların güncelleştirilmesi, e-posta hesapların güvenli kullanımı, işletim sisteminin güvenliği, internet tarayıcılarının güvenli kullanımı, bilişim etiği, sanal dolandırıcılık ve kablosuz ağ güvenliği gibi konuların yer alması gerektiğini belirtmişlerdir. Öğretmen adaylarının bilişim güvenliğine yönelik hazırlanacak bir eğitimde yer almasını istedikleri konulara yönelik bazı örnek ifadeleri aşağıda sunulmuştur:

ÖA1: "*Öncelikle bilişim güvenliğinin önemine değinilmesi gerekir. Güvenliği ihlal eden yöntemlere karşı bizim nasıl önlemler almamız gerektiğine yer verilmeli. Online bankacılık işlemlerimi daha güvenli bir şekilde yapmaya da ihtiyaç duyuyorum. Web sayfamı saldırılara karşı nasıl daha güçlü hale getirebilirim. Bunu öğrenmeliyim. Ayrıca son zamanlarda sosyal ağlarda çok güvenlik problemleri yaşanmaya başladı. Yani sosyal ağların güvenli kullanımı da olmalı bence*. *"*

ÖA2: "*Bilişim güvenliğinin neden önemli olduğuna? Bilgisayarların, akıllı telefonları nasıl güvenli kullanabileceğime? Kişisel bilgilerimi nasıl güvende tutabileceğime? Hangi yazılımlar bilgilerimi korumak için daha güvenlidir? Bankacılık uygulamaları, E-devlet uygulamalarını kullanırken nasıl korunabilirim? Bilişim suçuna maruz kalmamak için neler yapmalıyım? İlerde öğretmen olursam öğrencilerimi sosyal ağların tehlikelerinden kurtarmak için neler yapmalıyım? Bu gibi konulara yönelik eğitimlerin olmasını isterim*."

ÖA10: "*Bilişim güvenliği nedir ve önemi? Bilişim güvenliğini sağlamak için kullanılabilecek yazılımlar var mıdır? Varsa kullanımları nasıldır? Her kullanıcı kolayca kendi güvenliğini sağlamak için neler yapabilir? İnternetten alış veriş*

yaparken ve internet bankacılığını kullanırken dikkat edilmesi gereken noktalar nelerdir? Bunların çok önemli konular olduğunu düşünüyorum."

Bu bulgular, öğretmen adaylarının pek çok bilişim güvenliği konusunda eğitime ihtiyaç duyduklarını göstermektedir. Tablo 5 ve doğrudan alıntılar dikkate alındığında öğretmen adayların belirtikleri bilişim güvenliği konuların günümüzde önemli konular olduğu düşünülmektedir. Dolayısıyla ileriye dönük bilişim güvenliğini sağlamaya yönelik verilecek veya hazırlanacak eğitimlerde bu bulguların dikkate alınması faydalı olacaktır. Ayrıca bu konulara yönelik verilecek eğitimlerin alanda önemli bir ihtiyacı kapatacağı düşünülmektedir.

Tartışma

Öğretmen adaylarının bilişim suçu deneyimlerinin bilişim güvenliğini sağlamaya yönelik öğrenmeye ihtiyaç duydukları konuların belirlenmesine yönelik gerçekleştirilen bu araştırmada, bazı öğretmen adaylarının bilişim suçuna maruz kaldıkları, bazılarının bilişim suçunu işledikleri ve bazılarının bu konu hakkında bir fikirlerinin olmadığı görülmüştür. Benzer şekilde Dijle ve Doğan (2011) araştırmasında katılımcıların birçoğunun bilişim suçu kavramını daha önce duymadıklarını ve lisansız yazılım kullanma, internetten müzik, film oyun indirmenin bir suç olduğunu bilmediklerini tespit etmişlerdir. Bunun yanında bu araştırmada öğretmen adaylarının bilişim suçu konusunda bilgi eksikliklerinin yanında bilişim suçuna maruz kalınması durumunda ne yapacaklarını ve nereye başvuracaklarını bilmedikleri tespit edilmiştir. Öğütçü (2010) gerçekleştirdiği araştırmasında, katılımcıların başlarına gelen ya da karşılaştıkları bir bilişim suçunu hiçbir makama iletmediklerini ve bunun nedeni olarak da nereye bildireceklerini bilmediklerini belirtmeleri bu sonucu desteklemektedir. Çolak, Yalçın ve Korkmaz (2011) internet üzerinden dolandırıcılık, kullanıcıların sahte web sitelerine yönlendirilerek bilgilere erişme gibi bilişim suçlarında ciddi artış yaşandığını ve bu konuda yeterince bilgilendirme çalışmalarının yapılmamasının endişe verici olduğunu belirtmektedirler. KOM'un 2011 yılında yayınlanan raporunda; banka ve kredi kartı dolandırıcılığı, bilişim sistemlerini bozma, bilişim sistemlerindeki verileri yok etme, internet bankacılığı dolandırıcılığı, internet aracılığıyla nitelikli dolandırıcılık, müstehcenlik, kumar ve gizlilik ihlali şeklinde bilişim suçlarında artış yaşandığının görülmesi, bireyleri bu konularda bilgilendirmenin ne kadar önemli olduğunu göstermektedir. Nitekim Dijle ve Doğan (2011) bilişim suçları hukuki bir konu gibi görünse de bilişim suçlarını önleyebilmek için alınacak güvenlik tedbirlerin yanında örgün ve yaygın eğitim kurumlarının da bireyleri bilişim suçları konusunda bilgilendirmeleri gerektiğini belirtmektedirler. Bu araştırma sonuçlarına paralel olarak yapılan araştırmalarda, bireylere bilişim suçları konusunda bilinçlendirme ve bilgilendirmelerin yapılması, bu faaliyetlerin yaygınlaştırılması ve toplumsal bilgi ve farkındalığın artırılması önerilerinde bulunulmuştur (Bilek, 2012; Dijle ve Doğan, 2011; İlbaş, 2009). Dolayısıyla bu araştırma sonuçları ve yapılan araştırmalar dikkate alındığında bireylere bilişim suçunun ne olduğuna, bilişim suçlarına maruz kalındığında bu durumu ilgili mercilere iletebilme ve bilişim suçuna maruz

kalmamak için alınabilecek önlemlere yönelik bilgilendirme faaliyetlerinin yapılmasının faydalı olacağı ve bu sayede bireylerinin bilinçleneceği düşünülmektedir. Ayrıca bu bilgilendirmelerin veya eğitimlerin bilişim suçlarına karşı farkındalığın artmasına ve yaşanabilecek bilişim suçlarının azalmasında etkili olacağı düşünülmektedir.

Bu araştırmada öğretmen adaylarının yarısından fazlası bilişim güvenliğinin ne olduğu sorusuna genel olarak bilişim teknolojilerin güvenli kullanımı şeklinde cevap vermişlerdir. Bunun yanında öğretmen adaylarının bir kaçı bilişim güvenliğini; virüslerden korunma ve anti-virüs kullanımı, güvenli bilgiye erişme ve kullanma, kişisel bilgilerin güvenliği, elektronik ortamdaki bilginin korunması, güvenli şifre kullanımı olarak tanımlamışlardır. Bu sonuçlar öğretmen adaylarının bilişim güvenliğinin tanımı ve kapsamı konusunda yetersiz bilgiye sahip olduklarını göstermektedir. Nitekim alan yazında yer alan araştırmalar incelendiğinde bireylerin bilişim güvenliği konusunda bilgi düzeylerinin beklenenin altında olduğu görülmüştür (Akgün ve Topal, 2015; Gökmen ve Akgün, 2105; Karaoğlan-Yılmaz ve diğer., 2014; Kaşıkçı ve diğer., 2014; Mart, 2012; Pusey ve Sadera, 2011; Shehri, 2012; Tekerek ve Mart, 2010; Tekerek ve Tekerek, 2013). Örneğin bu konuda Pusey ve Sadera (2011) öğretmen adaylarının bilişim güvenliği konusunda kendilerini ve elektronik ortamdaki verilerini güvende tutacak yeterli bilgiye sahip olmadıkları sonucuna ulaşmışlardır. Karaoğlan-Yılmaz ve diğer. (2014)'nin üniversite öğrencilerinin; genel olarak 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 gibi güvenlik önlemlerinden yalnızca bir ya da birkaçını aldıklarına yönelik sonuçlara ulaşmaları bu araştırmanın ve alanyazındaki diğer araştırma sonuçlarını desteklemektedir. Ayrıca benzer şekilde bireylerin bilişim güvenliği farkındalıklarının tespit edildiği araştırmalarda (Mart, 2012; Öğütçü, 2010; Tekerek ve Tekerek, 2013) bireylerin farkındalıklarının düşük olduğu tespit edilmiştir. Bu açıdan bakıldığında bireylerin bilişim teknolojilerini kullanırken güvenli hareket etmelerini sağlayacak ve gerekli önlemleri almalarını sağlayacak eğitimlerin verilmesinin önemli ihtiyaç olduğu anlaşılmaktadır.

Alan yazındaki araştırmalar incelendiğinde bu araştırmalarda bilişim suçlarına (Bilek, 2012; Çolak ve diğer., 2011; Dijle ve Doğan, 2011; İlbaş, 2009; Karakoç, 2011) ve bilişim güvenliğine (Çelen, Çelik ve Seferoğlu, 2011; Demirel, Yörük ve Özkan, 2012; Gökmen ve Akgün, 2015; Karaoğlan-Yılmaz, 2014; Kaşıkçı ve diğer., 2014; Kınay, 2012; Mart, 2012; Şahinaslan, Kandemir ve Şahinaslan, 2009; Tekerek ve Tekerek, 2013) yönelik bilgilendirme faaliyetlerinin yapılmasının ve eğitimlerin verilmesinin gerekli olduğu belirtilmiştir. Öğütçü (2010) bireylerin kişisel bilişim güvenliği farkındalığının yükseltilmesi ve toplumun tüm kesimine bilişim teknolojilerinin güvenli kullanımını sağlayacak korumacı davranış geliştirmeye yönelik eğitimlerin verilmesinin bir devlet politikası olması gerektiğini vurgulamaktadır. Benzer şekilde Kınay (2012) gençlere bilişim güvenliği konusunda farkındalıklarını ve duyarlılıklarını artıracak ve bireylerin etkin olarak katıldığı

interaktif sitelerin ve yazılımların hazırlanmasını önermektedir. Başka bir araştırmada Karaoğlan-Yılmaz ve diğer. (2014) günümüzde çocukların bilişim teknolojilerini; bilgi edinme, sosyalleşme ve oyun oynama gibi amaçları gerçekleştirmek için sık kullandıklarını belirterek, okul öncesi dönemden üniversite eğitimine kadarki tüm süreçte bilişim güvenliği eğitimlerinin verilmesi gerektiğini vurgulamaktadırlar. Kaşıkçı ve diğer. (2014) bilişim güvenliğinin sağlanması konusunda ebeveynlerin büyük sorumluluklarının olduğunu fakat Türkiye'deki ebeveynlerin üçte ikisinin bilişim okur-yazarı olmadığı için, çocuklarına İnternet risklerine karşı yeterince yardımcı olmalarının beklenmediğini belirtmektedirler. Bu sorunun giderilmesi adına söz konusu araştırmada, çocukların internet risklerine karşı bilgilendirilmesi için okullardaki derslerin içeriğinin internet risklerini kapsayacak şekilde geliştirilmesinin günümüzde bir ihtiyaç olduğu üzerinde durmaktadırlar. Bu açıdan bakıldığında hiç kuşkusuz burada okullarda görev yapacak öğretmen adaylarına büyük görev ve sorumluluklar düşecektir. Buradan hareketle öğretmen adaylarına, bilişim güvenliğine yönelik farkındalıklarını ve bilgilerini artıracak, gerekli güvenlik tedbirlerini almalarını sağlayacak bilişim güvenliği eğitimlerinin verilmesinin önemli bir ihtiyacı karşılayacağı düşünülmektedir.

Bu noktada bilişim güvenliği eğitimleri verilmeden önce hedef kitlenin, içeriğinin ve eğitimin kapsamının belirlenmesi gerekmektedir. Bilişim güvenliği dersi konuları belirlenirken hedef kitleye uygun konuları içeren ve ihtiyaçlara yönelik bilişim güvenliği eğitim programının belirlenmesi doğru bir adım olacaktır. Bu konuda Şahinaslan ve diğer. (2009) temel bir bilişim güvenliği farkındalık eğitiminde; temel bilgi kavramları, bilginin korunacak nitelikleri, bilişim güvenliğine ilişkin güncel tehditler ve saldırılar, sosyal mühendislik, fiziksel güvenlik, şifre güvenliği, yasal düzenlemeler gibi konulara değinilmesi ve bu bilgilerin örneklerle zenginleştirilerek aktarılması gerektiğini belirtmektedirler. Bu araştırmada ise öğretmen adaylarının; bilişim teknolojilerinin güvenli kullanımı, kişisel bilgilerin güvenliğini sağlama, bilişim güvenliğini tehdit eden unsurlara karşı önlemler alma, güvenlik yazılımları, güvenli çevrimiçi alışveriş ve internet bankacılığı, web sitelerinin güvenliği, sosyal ağların güvenli kullanımı, güvenli şifre, virüslerden korunma, güncellemeler, e-posta hesaplarının güvenliği, işletim sisteminin güvenliği gibi konularda eğitime ihtiyaç duydukları belirlenmiştir. Dolayısıyla ileride hazırlanacak bilişim güvenliği eğitimlerinin içeriğinin belirlenmesinde bu araştırmanın sonuçlarının dikkate alınmasının faydalı olacağı düşünülmektedir.

Sonuç ve Öneriler

Sonuç olarak bu araştırmada bazı öğretmen adaylarının bilişim suçlarına maruz kaldıkları, bazılarının bilişim suçunu bilerek veya bilmeyerek işledikleri, bazılarının da bilişim suçunun ne olduğu konusunda herhangi bir fikirlerinin olmadığı ve bilişim suçlarına maruz kaldıklarında bu durumu gerekli mercilere iletme konusunda bilgi sahibi olmadıkları görülmüştür. Ayrıca öğretmen adaylarının bilişim güvenliğinin tanımı ve kapsamı konusunda yetersiz bilgiye sahip olduklarının

tespit edilmesinin yanında pek çok bilişim güvenliği konusunda eğitime ihtiyaç duydukları belirlenmiştir. Dolayısıyla araştırma sonuçlarından yola çıkarak aşağıdaki öneriler geliştirilmiştir.

- Öğretmen adayları bilişim suçunun ne olduğu ve bilişim suçuna maruz kalındığı durumlarda başvurabilecekleri merciler konusunda bilgilendirilmelidir.
- Eğitim fakültelerin öğretmenlik programlarında öğretmen adaylarının bilişim güvenliğini sağlamaya ve gerekli önlemleri almaya yönelik seçmeli ders konulabilir.
- Bu araştırmanının sonuçları hazırlanacak ders veya eğitimlerin belirlenmesine katkı sağlayabilir.
- Bilişim güvenliği konusundaki farkındalığı artırma ve gerekli bilgi ve becerileri kazandırma ihtiyacına yönelik olarak web üzerinden dersler, yazılımlar, kitaplar vb. öğrenme materyalleri hazırlanabilir.

Kaynakça

Akgün, Ö. E. ve Topal, M. (2015). Eğitim fakültesi son sınıf öğrencilerinin bilişim güvenliği farkındalıkları: sakarya üniversitesi eğitim fakültesi örneği. *Sakarya Üniversitesi Eğitim Fakültesi Dergisi, 5*(2), 98-121.

Ayas, T. ve Horzum, M.B. (2013). İlköğretim öğrencilerinin internet bağımlılığı ve aile internet tutumu. *Türk Psikolojik Danışma ve Rehberlik Dergisi, 4*(39), 46-57.

Bilek, B.T. (2012). *Bilişim suçları ve üniversite lisans öğrencilerin bilişim suçlarına yönelik görüşleri.* Yüksek lisans tezi, Gazi Üniversitesi, Bilişim Enstitüsü, Ankara.

Büyüköztürk, Ş., Kılıç Çakmak, E., Akgün, Ö. E., Karadeniz, Ş. ve Demirel, F. (2012). *Bilimsel araştırma yöntemleri* (13.Baskı), Pegem Akademi Yayınları, Ankara.

Cerrah, İ. (2002). Bilişim teknolojileri ve etik: bilişim teknolojilerinin güvenlik hizmetlerinde kullanımının "etik boyutu" ve "sosyal sonuçları". *Polis Bilimleri Dergisi, 4* (1-2). 137-156.

Çalık, D. ve Çınar, Ö.P. (2009). Geçmişten günümüze bilgi yaklaşımları bilgi toplumu ve internet. *XIV. Türkiye'de İnternet Konferansı*, 12-13 Aralık 2009, Bilgi Üniversitesi, Dolapdere, İstanbul.

Çelen, F.K., Çelik, A. ve Seferoğlu, S.S. (2011). Çocukların internet kullanımları ve onları bekleyen çevrim-içi riskler. *13. Akademik Bilişim Konferansı Bildirileri*, 2-4 Şubat 2011, İnönü Üniversitesi, Malatya.

Çolak, B., Yalçın, B. ve Korkmaz, S. (2011). Türkiye'de internet kullanımının toplumsal yansımaları. *XVI. Türkiye'de İnternet Konferansı*, 30 Kasım-2 Aralık 2011, Ege Üniversitesi Atatürk Kültür Merkezi, Konak, İzmir.

Demirel, M., Yörük, M. ve Özkan, O. (2012). 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.

Dijle, H. (2006). *Türkiye'de eğitimli insanların bilişim suçlarına yaklaşımı*. Yüksek lisans tezi. Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.

Dijle, H. ve Doğan, N. (2011). Türkiye'de bilişim suçlarına eğitimli insanların bakışı. *Bilişim Teknolojileri Dergisi, 4*(2), 43-53.

Durak-Batıgün, A. ve Kılıç, N. (2011). İnternet bağımlılığı ile kişilik özellikleri, sosyal destek, psikolojik belirtiler ve bazı sosyo-demografik değişkenler arasındaki ilişkiler. *Türk Psikoloji Dergisi, 26*(67), 1-10.

Gökmen, Ö. F. (2014). *Bilgisayar ve öğretim teknolojileri eğitimi öğretmen adaylarının bilişim güvenliği eğitimi verebilme yeterliklerinin incelenmesi*. Yüksek lisans tezi. Sakarya Üniversitesi, Eğitim Bilimleri Enstitüsü, Sakarya.

Gökmen, Ö. F. ve Akgün. Ö.E. (2015). Bilgisayar ve öğretim teknolojileri eğitimi öğretmen adaylarının bilişim güvenliği bilgilerinin çeşitli değişkenlere göre incelenmesi. *Çukurova Üniversitesi Eğitim Fakültesi Dergisi, 44* (1), 61-84.

Gözgü, F. ve Mutioğlu, H. (2012). Toplumun değişen yüzü: bilgi toplumu ve bilişim kültürü. *Batman Üniversity Journal of Life Sciences, 1*(1), 465-476.

ISTE. (2008). National educational standards for teachers. http://www.iste.org/docs/pdfs/20-14_ISTE_Standards-T_PDF.pdf adresinden 10.11.2014 tarihinde erişilmiştir.

İlbaş, Ç. (2009). *Bilişim suçlarının sosyo-kültürel seviyelere göre algı analizi*. Yüksek lisans tezi. Başkent Üniversitesi, Fen Bilimler Enstitüsü, Ankara.

Kaçakcılık ve Organize Suçlar Daire Başkanlığı.(2011). *Kaçakcılık ve organize suçlarla mücadele 2011 raporu.* Ankara: KOM Yayınları.

Karakoç, M. A. (2011). Bilişim suçlarına genel bakış, bilişim suçlarını önleme çalışmaları ve güvenli internet kullanımı. *Suç Önleme Sempozyumu*, 7-8 Ekim 2011, Merinos Atatürk Kongre ve Kültür Merkezi, Bursa.

Karaoğlan-Yılmaz, G., Yılmaz, R. ve Sezer, B. (2014). Üniversite öğrencilerinin güvenli bilgi ve iletişim teknolojisi kullanım davranışları ve bilgi güvenliği eğitimine genel bir bakış. *Bartın Üniversitesi Eğitim Fakültesi Dergisi, 3*(1), 176-199.

Kaşıkçı, D.N., Çağıltay, K., Karakuş, T., Kurşun, A. ve Ogan, C. (2014). Türkiye ve avrupa'daki çocukların internet alışkanlıkları ve güvenli internet kullanımı. *Eğitim ve Bilim, 39*(171), 230-243.

Kınay, H. (2012). *Lise öğrencilerinin siber zorbalık duyarlılığının riskli davranış, korumacı davranış, suça marüziyet ve tehlike algısı ile ilişkisi ve çeşitli değişkenler açısından incelenmesi*. Yüksek lisans tezi. Sakarya Üniversitesi, Eğitim Bilimler Enstitüsü, Sakarya.

Landis, J. R. ve Koch, G. G. (1977). The measurement of observer agreement for categorical data, Biometrics. *33*, 159-174.

Marinos, L. (2013). Enısa threat landscape 2013: overview of current and emerging cyber-threats. Heraklion: European Union Agency for Network and Information Security Publishing. ISBN 978-92-79-00077-5 doi:10.2788/14231.

National Cyber Security Alliance. (2011). The state of k-12 cyberethics, cybersafety and cybersecurity curriculum in the united states. http://news.microsoft.com/2011/05/04/2011-state-of-cyberethics-cybersafety-and-cybersecurity-curriculum-in-the-u-s-survey adresinden 10.11.2014 tarihinde erişilmiştir.

Öğütçü, G. (2010). *E-dönüşüm sürecinde kişisel bilişim güvenliği davranışı ve farkındalığın analizi*. Yüksek lisans Tezi, Başkent Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.

Pruitt-Mentle, D. & Pusey, P. (2010). State of K12 cyberethics, safety and security curriculum in u.s.: 2010 educator opinion. Educational Technology Policy, Research and Outreach.

Pusey, P. & 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), 82-88.

Shehri, Y. (2012). Information security awareness and culture. *British Journal of Arts and Social Sciences, 6*(1), 611-69. ISSN: 2046-9578.

Symantec. (2014). Internet security threat report 2014. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf adresinden 09.10.2014 tarihinde erişilmiştir.

Şahinaslan, E., Kandemir, R. ve Şahinaslan, Ö. (2009). Bilgi güvenliği farkındalık eğitim örneği. 11. *Akademik Bilişim Konferansı Bildirileri*. 11-13 Şubat 2009, Harran Üniversitesi, Şanlıurfa.

Tekerek, M. ve Mart, İ. (2010). K8 düzeyi için davranışsal bilgisayar ve internet güvenliği farkındalığı. 4.*Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildirileri*, 6-8 Mayıs 2010, Orta Doğu Teknik Üniversitesi. Ankara.

Tekerek, M. ve Tekerek, A. (2013). A research on students' information security awareness. *Turkish Journal of Education, 2*(3), 61-70.

Türkiye İstatistik Kurumu. (2013). Bilgi toplumu istatistikleri. http://www.tuik.gov.tr/UstMenu.do?metod=temelist adresinden 09.10.2014 tarihinde erişilmiştir.

Yıldırım, A. ve Şimşek, H. (2013). *Sosyal bilimlerde nitel araştırma yöntemleri.* (9. Baskı) Ankara: Seçkin Yayınevi.