Elementary Education Online, 2015; 14(4): 1208-1221
İlköğretim Online, 2015; 14(4): 1208-1221. [Online]: http://ilkogretim-online.org.tr
doi: http://dx.doi.org/10.17051/io.2015.04635

Analysis of Computer Education and Instructional Technology Teacher Candidates' Efficacy Perceptions to Teach Information Security[1]

Ömer Faruk Gökmen[2], Özcan Erkan Akgün[3]

ABSTRACT. With the increasing information technologies usage, attacks and threats towards information technologies have been increasing in the same way. Because of this, it is necessary to examine Computer Education and Instructional Technology (CEIT) teacher candidates' efficacy perceptions to teach information security. The study carried out with survey method and participants were consisted of 375 CEIT teacher candidates. Data were collected with "Information Security Efficacy Perceptions Survey" (Pusey & Sadera, 2011). And the survey was adapted to Turkish by authors. According to the results, the majority of participants haven't taken any course or lecture about information security. Furthermore, CEIT teacher candidates' efficacy perceptions to teach information security is not well enough in many information security topics. Based on the results, it is thought that it will be useful to put a compulsory course to CEIT program.
Keywords: Information Security, efficacy perception, CEIT, teacher candidates

SUMMARY

Purpose and significance: Information technologies hold many benefits in education through problem solving, interaction, communication etc. In addition to these benefits, information technologies are known to cause some problems. The treats and cyber-attacks to information technology have been increasing; while usages of these technologies have been dramatically increasing. From this point, it is a crucial responsibility for teachers to protect our children from information security problems. Therefore, CEIT teacher candidates' information security capabilities should be investigated. This study examined these CEIT teacher candidates' efficacy perceptions about teaching information security topics.

Method: The study was carried out with survey method. Participants of this study were consisted of 375 CEIT teacher candidates from 4 Universities. Purposive sampling has been chosen in accordance to research purposes. From this point Sakarya, Amasya, Erzincan and Siirt Universities have been selected. The survey was applied to 3th and 4th grade students of these universities. Information Security Efficacy Perceptions Survey which was developed by Pusey & Sadera (2011), have been used. The survey was adapted to Turkish by authors. The data gathered during the study, was analyzed by using the SPSS 22.0 program. Descriptive statistics were used while analyzing data.

Results: In total 375 CEIT teacher candidates participated in the study, 79,1 % were between 21-23 years old, 53.9% were boys, 46,1% were girls, 66% were 4th grade students, 34% were 3th grade students. In this study 30,4 % of participants have taken information security course or lecture and 69,6 % of participants haven't taken any kind of information security education. According to the findings, CEIT teacher candidates' efficacy perceptions to teach information security is not well enough in many information security topics.

Discussion and Conclusions: According to the results, it was found that CEIT teacher candidates' efficacy in many topics about information security seems insufficient. Most of CEIT teacher candidates have no knowledge what DoS attacks, plagiarism, spoofing, zombie, sniffing, phishing, bot and botnet, social engineering, back door, keylogger, cybercrime law in the Turkish legal system meaning. Except this, CEIT teacher candidates have point out that they could teach firewall, file sharing security, malware, software updates, security settings, copyright, safer internet service, privacy. Based on the results it was considered that it would be useful to put an information security course to the CEIT program.

[1] This study has been composed by the first author in consultation with the second author by benefiting a part of master dissertation named "Analysis of Computer Education and Instructional Technology Teacher Candidates' Efficacy to Teach Information Security", and a part of this study was presented at 2nd International Instructional Technologies and Teacher Education Symposium.
[2] Research Assistant, Sakarya University, Faculty of Education, omerfarukgokmenn@gmail.com
[3] Assist. Prof. Dr., Istanbul Medeniyet University, Faculty of Educational Sciences, ozcanakgun@gmail.com

Gönderildiği tarih: 14-04-2015 Kabul edildiği tarih: 22-09-2015

Elementary Education Online, 2015; 14(4): 1208-1221
İlköğretim Online, 2015; 14(4): 1208-1221. [Online]: http://ilkogretim-online.org.tr
doi: http://dx.doi.org/10.17051/io.2015.04635

Bilgisayar ve Öğretim Teknolojileri Eğitimi Öğretmen Adaylarının Bilişim Güvenliği Eğitimi Verebilmeye Yönelik Yeterlilik Algılarının İncelenmesi[1]

Ömer Faruk GÖKMEN[2], Özcan Erkan AKGÜN[3]

ÖZ. Bilişim teknolojileri günümüz eğitim-öğretim faaliyetlerinde sıklıkla kullanılmaktadır. Bilişim teknolojilerin kullanımı pek çok güvenlik problemine de neden olmaktadır. Buradan yola çıkıldığında bilişim teknolojilerinin, öğrenciler tarafından bilinçli ve güvenli kullanımını sağlama önemli bir konu haline gelmiştir. Bu araştırmanın amacı, Bilgisayar ve Öğretim Teknolojileri Eğitimi (BÖTE) bölümü öğretmen adaylarının bilişim güvenliği eğitimi verebilmeye yönelik yeterlilik algılarının tespit edilmesidir. Çalışma kesitsel tarama modeli ile yürütülmüştür. Araştırmanın çalışma grubunu BÖTE bölümünden 375 öğretmen adayı oluşturmuştur. Araştırma verileri, Pusey ve Sadera (2011) tarafından geliştirilen ve yazarlar tarafından Türkçe 'ye uyarlanan "Bilişim Güvenliği Eğitimi Verebilme Yeterliliği Algısı Anketi" ile elde edilmiştir. Araştırma sonuçlarına göre; adayların büyük çoğunluğunun, bilişim güvenliğini sağlamaya yönelik bir kurs veya ders almadıkları tespit edilmiştir. Bunun yanında adayların birçoğunun, bilişim güvenliği konularını öğretebilme açısından yeterli olmadıkları belirlenmiştir. Ayrıca özellikle bazı teknik konular hakkında birçok öğretmen adayının bilgi sahibi olmadığı görülmüştür. Bu sonuçlardan yola çıkarak, BÖTE öğretmen yetiştirme programında bu çalışmada ele alınan güvenlik konularını kapsayan zorunlu bir derse yer verilmesinin yararlı olacağı düşünülmektedir.
Anahtar Sözcükler: Bilişim Güvenliği, Yeterlilik Algısı, BÖTE, Öğretmen Adayı

GİRİŞ

Bilişim teknolojilerinde her geçen gün takip edilemeyecek bir hızda gelişmeler yaşanmaktadır. Bu gelişmeler sonucunda farklı işlevleri ve amaçları barındıran teknolojiler günlük hayatta yer edinmektedir. Bu teknolojiler kullanıcıların, yer ve zaman sınırlaması olmaksızın kolay ve hızlı bir şekilde bilgiye ulaşabilmelerini sağlamaktadır. Bilişim teknolojilerinin kullanım alanına bakıldığında; bu teknolojilerin eğitimden sağlık hizmetlerine, ticaretten mühendislik uygulamalarına ve daha birçok alanda kullanıldığı görülmektedir (Çelik, 2007). Bilişim teknolojilerinin kullanımı alanındaki genişlik ve sunduğu fırsatlar, bu teknolojilerin her alanda önemli rol oynamasına ve vazgeçilmez araçlar olmasına imkân tanımaktadır.

Bilişim teknolojilerinin kullanımında yaşanan artış beraberinde internet hizmetinin kullanımını da getirmiştir. Bu artışın Türkiye İstatistik Kurumu'nun (TUİK, 2013) istatistiklerine yansıdığı görülmektedir. TUİK 2013 istatistiklerinde bilgisayar kullanımı kurum ve kuruluşlarda % 92 iken bu oranın evlerde % 49,9 olduğu, internet erişiminin ise kurum ve kuruluşlarda % 90,8 iken evlerde %48,9 olduğu belirlenmiştir. TUİK'in her sene gerçekleştirdiği bu araştırma, her geçen yıl bilgisayar ve internet kullanımının arttığını doğrulamaktadır. İnternet ve bilişim teknolojileri sahip olduğu özellikler sayesinde hiç kuşkusuz pek çok fayda sağlamaktadır. Bu teknolojilerin; iletişimi kolaylaştırma, sorunlara çözümler üretme, kültürler arası etkileşimi artırma, zamanı etkili kullanmayı sağlama, bilgi edinme, bireylerin haberleşmelerini sağlama, zaman ve mekân sınırını ortadan kaldırma vb. daha birçok konuda faydasının olduğu belirtilmektedir (Demir, 2006).

Diğer taraftan bilişim teknolojileri ve internetin yaygın kullanımı, bireyler ve kurumlar için güvenlik problemlerine yol açmakta ve bu teknolojiler vasıtasıyla suçlar işlenmektedir. Bilişim suçları bireylere, bireylerin mülkiyet haklarına, kurumlara, kurumların teknik sistemlerine karşı işlenebilmektedir (Pati, t.y). Bilek (2012) bilişim suçunun, bilişim teknolojilerini kullanarak hali hazırda bulunan sistemlerdeki verilerde silme, değiştirme veya ekleme yapılarak gerçekleştiğini belirtmektedir. Alan yazında bilişim suçunun; siber suç (cybercrime), dijital suç (digital crime), bilgisayarla ilgili suç (computer related crime), internet suçu (internet crime), bilgisayar suçu (computer crime) ve ileri teknoloji suçu (hi-tech crime) gibi farklı kavramlarla ifade edildiği

[1] Bu çalışma ikinci yazar danışmanlığında birinci yazar tarafından hazırlanan "Bilgisayar ve Öğretim Teknolojileri Eğitimi Öğretmen Adaylarının Bilişim Güvenliği Eğitimi Verebilme Yeterliliği" adlı tez çalışmasından bir bölümünden faydalanılarak oluşturulmuştur ve bu çalışmanın bir kısmı 2. Uluslararası Öğretim Teknolojileri ve Öğretmen Eğitimi Sempozyumunda sunulmuştur.

[2] Arş. Gör., Sakarya Üniversitesi, Eğitim Fakültesi, omerfarukgokmenn@gmail.com
[3] Yrd. Doç. Dr, İstanbul Medeniyet Üniversitesi, Eğitim Bilimleri Fakültesi, ozcanakgun@gmail.com

Gönderildiği tarih: 14-04-2015 Kabul edildiği tarih: 22-09-2015

Elementary Education Online, 2015; 14(4): 1208-1221
İlköğretim Online, 2015; 14(4): 1208-1221. [Online]: http://ilkogretim-online.org.tr
doi: http://dx.doi.org/10.17051/io.2015.04635

görülmektedir (Pallı, 2008). Genel anlamda bu ifadeler değerlendirildiğinde yapılan tanımların benzer olduğu görülmekte, bilgisayar ve internet kullanılarak bu teknolojiler vasıtasıyla gerçekleştirilen suçların bilişim suçu olarak tanımlandığı anlaşılmaktadır (Maheshwari, Hyman ve Agrawal (2011).

Bilişim suçları farklı şekillerde işlenmekte ve bu suçların işlenmesinde farklı yöntemlere başvurulmaktadır. Özellikle son yıllarda enerji, su, gıda ve sağlık hizmetleri gibi kritik altyapılara, mobil teknolojilere, bulut bilişim teknolojilerine ve sosyal ağlara yapılan saldırılar artmaktadır (Marinos, 2013). Richardson (2008) araştırmasında Amerika Birleşik Devletleri'nde (ABD) bilişim sistemlerine en fazla gerçekleştirilen saldırı yöntemlerini tespit etmiştir. Söz konusu araştırmada bilişim sistemlerine saldırıların en fazla; bilişim sisteminin hizmet vermesini engelleyen DoS (Denial of service) saldırıları, dizüstü veya mobil cihazların çalınması veya kaybolması, zararlı yazılım bulaşması, bireyleri sahte adrese yönlendiren oltalama saldırıları, programların içine gömülmüş kötü amaçlı dosyalar, dolandırıcılık ve web sitesi tahrifatı şeklinde gerçekleştiği görülmüştür. Marinos (2013) yaptığı araştırmada benzer şekilde saldırıların en fazla; zararlı yazılımlar, internetten indirilen programlar, sistemlere zararlı kodlar ekleme, DoS saldırıları, oltalama, sahte içerikli e-postalar, kimlik hırsızlığı, veri ihlali, bilgi sızdırma, fiziksel zarar, şeklinde olduğunu belirlemiştir. Kaçakçılık ve Organize Suçlarla Mücadele (KOM), 2011) 2011 raporunda en fazla işlenen bilişim suçlarının; banka, kredi kartı ve internet bankacılığı dolandırıcılığı, bilişim sistemlerine zarar verme, telif hakları, müstehcenlik ve çocuk istismarı olduğu tespit edilmiştir. Genel olarak bakıldığında bilişim sistemlerine gerçekleştirilen saldırıları özetlemek mümkündür. Bunlar; arka kapılar, zararlı yazılımlar, casus yazılımlar, sistem aracı gibi görünen rootkitler, uzaktan yönetim araçları, e-posta bombardımanı, veri trafiğinin izlenmesi, veri trafiğini izlerken gizlenme, sql kodlarının kullanılarak sistem kodlarına ulaşılması, bireylerin sahte adreslere yönlendirilmesi ve reklam bedelli yazılımlar gibi araçlar ve yöntemlerdir (Canbek, 2005).

Bilişim sistemlerine yönelik tehditlere ve gerçekleştirilen saldırılara karşı gerekli tedbirlerin alınması; yönetsel önlemler, teknoloji uygulamaları ve eğitim-farkındalık süreçlerinden oluşmaktadır. Prosedürler, yönergeler, talimatlar gibi yönetsel önlemeler; kriptografi, güvenlik duvarı, yedekleme gibi teknoloji uygulamaları ve güvenlik konusunda eğitimler bilişim güvenliğinin sağlanmasında önemli aşamalardır. Ulaşanoğlu, Yılmaz ve Tekin (2010) bilişim güvenliğini, bilgi ve bilginin işlenmesi, gönderilmesi, depolanmasında kullanılan her türlü teknolojik ortam ve aracın yetkisiz kişiler tarafından erişilmesi, değiştirilmesi, silinmesi, bozulması gibi her türlü tehdide karşı önlem alınması olarak tanımlamaktadır. Bilişim güvenliğini tehdit eden unsurlar incelendiğinde bunlar; kullanıcı tabanlı, yazılım tabanlı ve sosyal mühendislik olarak üçe ayrılmaktadır (Kınay, 2012). Her geçen gün bu üç unsurun zafiyetlerinden faydalanılarak bilişim sistemlerine karşı saldırılar gerçekleştirilmekte, saldırı yöntemleri farklılaşmakta ve bunun sonucunda maddi ve manevi zararlar oluşmaktadır. Dolayısıyla buradan hareketle özellikle okullarda çocuklara kendilerini ve bilişim sistemlerindeki bilgilerini koruyabilecekleri ve gerekli önlemleri alabilecekleri bilişim güvenliği eğitimlerinin verilmesi önem taşımaktadır.

Yapılan araştırmalarda bireylerin bilişim güvenliğini tehdit eden unsurlar konusunda farkındalıklarının ve bilgilerinin düşük düzeyde olduğu sonucuna ulaşılmıştır (Dijle, 2006; Dijle ve Doğan 2011; Karaoğlan-Yılmaz, Yılmaz ve Sezer, 2014; Pusey ve Sadera, 2011; Shehri, 2012; Tekerek ve Mart, 2010; Tekerek ve Tekerek, 2013). Yine yapılan araştırmalarda, bilişim suçları konusunda bilgilendirme ve gerekli önlemleri alma konusunda bilgilendirme faaliyetleri içerisinde olunması gerektiği vurgulanmıştır (Bilek, 2012; Dijle ve Doğan, 2011; İlbaş, 2009). Bilişim güvenliği konusuna yönelik gerçekleştirilen başka araştırmalarda da bireylere küçük yaşlardan itibaren eğitimlerin verilmesinin, bilişim güvenliğini sağlamaya yönelik derslerin okullarda okutulmasının, seminerler ve kitle iletişim araçlarıyla bilinçlendirme faaliyetlerinin yapılmasının gerekliliği üzerinde durulmuştur (Mart, 2012; Öğütçü, 2010). Uluslararası Eğitimde Teknoloji Topluluğu (International Society for Technology in Education-ISTE) öğretmenlerin, etik konuları uygulama ve örnek olma; teknolojinin sosyal etkileşimi sağlamasında sorumluluk sahibi olma; dijital bilginin ve teknolojinin güvenli ve etik kullanımını destekleme ve bu teknolojilerin güvenli kullanımını öğretme becerilerine sahip olmaları gerektiğini vurgulamaktadır (ISTE, 2008).

Ülkemizde Milli Eğitim Bakanlığı (MEB) bünyesinde teknolojinin güvenli kullanımına yönelik bilişim teknolojileri öğretmenlerinin özel alan yeterlilikleri belirlenmiştir. MEB tarafından belirlenen bilişim teknolojileri özel alan yeterliliklerinde, bilişim teknolojileri öğretmenlerinin; bilişim

Gönderildiği tarih: 14-04-2015 Kabul edildiği tarih: 22-09-2015

Elementary Education Online, 2015; 14(4): 1208-1221
İlköğretim Online, 2015; 14(4): 1208-1221. [Online]: http://ilkogretim-online.org.tr
doi: http://dx.doi.org/10.17051/io.2015.04635

teknolojileri, internet ve ağ teknolojilerinin yasal kurallarını bilme ve etik davranmaları gerektiği ifade edilmiştir. Bunun yanında bilişim teknolojileri öğretmenlerinin bu teknolojileri güvenli kullanabilmeleri, güvenlik tehditlerine karşı gerekli önlemleri alabilmeleri ve bilişim güvenliği konularını öğretebilme niteliklerine sahip olmaları gerektiği belirtilmiştir (MEB, 2008). Buradan hareketle öğrencilere bilişim teknolojilerinin bilinçli ve güvenli kullanımını öğretecek, onların güvenlik tehditlerine karşı gerekli önlemleri almalarını sağlayacak olan Bilişim Teknolojileri öğretmenlerine önemli görev ve sorumluluklar düşmektedir. Dolayısıyla bu çalışmanın amacı, okullarda istihdam edilecek olan Bilgisayar ve Öğretim Teknolojileri Eğitimi (BÖTE) bölümü öğretmen adaylarının bilişim güvenliği eğitimi verebilmeye yönelik yeterlilik algılarının tespit edilmesidir. Bu amaca yönelik olarak aşağıdaki araştırma sorularına yanıt aranmıştır:

1- Katılımcıların bilgisayar ve internet kullanım sürelerine, bilişim güvenliği ile ilgili bir eğitim alıp almamalarına ve virüs tarama yazılımı güncelleme sıklığına yönelik durumları nedir?
2- Katılımcıların bilişim güvenliğiyle ilgili "hakkında hiçbir şey duymadıklarını" belirttikleri konular nelerdir?
3- Katılımcıların bilişim güvenliğiyle ilgili "duydukları fakat ne anlama geldiğini bilmedikleri" konular nelerdir?
4- Katılımcıların bilişim güvenliğiyle ilgili "bildikleri fakat öğretebilecek yeterliliğe sahip olmadıklarını" düşündükleri konular nelerdir?
5- Katılımcıların bilişim güvenliğiyle ilgili bildikleri ve öğretebilecek yeterliliğe sahip olduklarını" düşündükleri konular nelerdir?

YÖNTEM

Araştırma Modeli

Bu araştırma kesitsel tarama modelinde yürütülmüştür. Tarama araştırmalarının amacı, bir konu veya olayla ilgili katılımcıların tutumlarını, görüşlerini veya yeterliliklerini belirlemektir. Tarama türü araştırmalarının genel amacı, mevcut durumun ortaya çıkarılmasıdır. (Büyüköztürk, Kılıç Çakmak, Akgün, Karadeniz ve Demirel, 2012). Buradan hareketle bu çalışmada, BÖTE öğretmen adaylarının bilişim güvenliği konuları öğretebilmeye yönelik yeterlilik algılarının belirlenmesi hedeflenmiştir.

Katılımcılar

Araştırmanın katılımcılarını, BÖTE bölümünün olduğu Sakarya Üniversitesi, Erzincan Üniversitesi, Amasya Üniversitesi ve Siirt Üniversitesi bölümünde okuyan ve gönüllü olarak araştırmaya katılan 375 öğrenci oluşturmuştur. Anketler BÖTE bölümü 3. ve 4. sınıfta öğrenim gören tüm öğrencilere uygulanmıştır. Katılımcıların öğrenim gördükleri üniversitelere ve sınıflarına göre dağılımı Tablo 1'de verilmiştir.

Tablo 1. *Katılımcıların Demografik Bilgiler*

Özellik	Özelliğin Alt Düzeyleri	Frekans	Yüzde
Cinsiyet	Kadın	173	46,1
	Erkek	202	53,9
Üniversite	Sakarya Üniversitesi	127	33,9
	Erzincan Üniversitesi	107	28,5
	Amasya Üniversitesi	83	22,1
	Siirt Üniversitesi	58	15,5
Sınıf	3	130	34
	4	245	66
Yaş	20	27	7,2
	21	96	25,6
	22	115	30,7
	23	86	22,9
	24	35	9,3
	25 ve üzeri	16	4,3
Toplam		375	100

Gönderildiği tarih: 14-04-2015 Kabul edildiği tarih: 22-09-2015

Elementary Education Online, 2015; 14(4): 1208-1221
İlköğretim Online, 2015; 14(4): 1208-1221. [Online]: http://ilkogretim-online.org.tr
doi: http://dx.doi.org/10.17051/io.2015.04635

Veri Toplama Aracı

Bu araştırmada veriler, Pusey ve Sadera'nın (2011) geliştirdiği "Bilişim Güvenliği Eğitimi Verebilme Yeterliliği Algısı" anketinin Türkçe'ye uyarlanan formu ile toplanmıştır. Türkçe'ye çevrilen anket kapsam geçerliliğinin incelenmesi adına alanda uzman 6 kişinin görüşüne sunulmuştur. BÖTE alanından doktora yapmış 3, Bilişim suçları konusunda doktora yapmış 1, Yönetim Bilişim Sistemleri alanında doktora eğitimi alan 1, Emniyet Müdürlüğü Bilişim suçları biriminde çalışan 1 emniyet mensubu olmak üzere 6 kişiden uzman görüşü alınmıştır. Uzman görüşleri doğrultusunda bazı maddelerin Türkçe çevirilerinde değişiklik yapılmış ve uzmanlar tarafından önerilen yeni maddeler eklenmiştir. Örneğin uzman görüşleri doğrultusunda günümüzde kullanımları artan "mobil teknolojilerin güvenliği" ve "5651 sayılı İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele kanunu" maddeleri ankete dâhil edilmiştir. Anket, likert tipi 4'lü derecelendirme özelliğine sahip demografik sorulardan ve toplam 76 maddeden oluşmaktadır. Pusey ve Sadera (2011) anketin 4'lü derecelendirmesini "Bu konu hakkında hiçbir şey duymadım", "Duydum. Fakat ne anlama geldiğini bilmiyorum", "Biliyorum. Fakat öğrencilerime öğretmem" ve "Biliyorum ve öğrencilerime öğretebilirim" şeklinde oluşturmuşlardır. Bu çalışmada da seçenekler bu şekilde kullanılmıştır. Pusey ve Sadera (2011) güvenirlik çalışması sonucu anketin iç tutarlık katsayısı Cronbach alfa değerini 0.99 olarak bulmuşlardır. Uyarlanan aracın güvenirlik çalışması sonucu iç tutarlık katsayısı Cronbach alfa hesaplanmış ve güvenirlik katsayısı 0.96 bulunmuştur. Bu değer anketin yüksek düzeyde güvenilir olduğunu göstermektedir.

Verilerin Analizi

Verilerin analizinde ankette yer alan her bir maddeye verilen yanıtların ortalama puanları hesaplanmıştır. Ortalama puan; 0 ile 1,49 arasında ise öğretmen adaylarının o konu hakkında bir şey duymadıkları, ortalama puan 1,50 ile 2,49 arasında ise öğretmen adaylarının duydukları fakat ne anlama geldiğini bilmedikleri, ortalama puan 2,50 ile 3,49 arasında ise öğretmen adaylarının bildikleri fakat öğretebilme yeterliliğine sahip olmadıklarını düşündükleri, ortalama puanı 3,50 ve üzeri ise öğretmen adaylarının bildiklerini ve öğrencilerine öğretebileceklerini düşündükleri şeklinde belirlenmiştir (Pusey ve Sadera, 2011). Maddeler ortalama puanları göz önüne alınarak araştırma sorularına uygun olarak yukarıda belirtilen yanıt gruplarına göre ayrı tablolar halinde verilmiştir.

BULGULAR VE YORUMLAR

Bu bölümde hedef kitlenin özellikleri betimlenerek araştırmanın bağlamının ortaya konması açısından BÖTE öğretmen adaylarının günlük bilgisayar ve internet kullanım sürelerine, bilişim güvenliğine yönelik bir kurs veya eğitim alıp almama durumuna, virüs tarama yazılımının güncellenme sıklığına ve bilişim güvenliğini öğretebilme yeterliliklerine yönelik bulgulara yer verilmiştir. Tablo 2'de günlük bilgisayar kullanım süresinin dağılımına, Tablo 3'te günlük internet kullanım süresinin dağılımına, Tablo 4'te bilişim güvenliğine yönelik bir kurs veya eğitim alınıp alınmama durumuna ve Tablo 5'da virüs tarama yazılımının güncellenme sıklığına yer verilmiştir. Ayrıca öğretmen adaylarının bilişim güvenliği eğitimi yeterlilikleri konularına yönelik anket maddelerine verdikleri cevapların ortalama değerleri Tablo 6, 7 ve 8'de sunulmuştur.

Tablo 2. *Günlük Bilgisayar Kullanım Süresi*

Günlük Bilgisayar Kullanım Süresi	Frekans	Yüzde
1-3 saat	153	40,8
4-6 saat	134	35,7
7 saat ve üzeri	88	23,5
Toplam	375	100

Tablo 2'deki bulgular dikkate alındığında BÖTE öğretmen adaylarının %40,8'i günlük 1 ile 3 saat, % 35,7'si günlük 4 ile 6 saat, %23,5'i ise günde 7 saat ve üzerinde bilgisayar kullandıklarını belirtmişlerdir. Buna göre öğretmen adaylarının günlük bilgisayar kullanım süresinin yoğun olarak günde 4-6 saat ile günde 1-3 saat arasında olduğu görülmektedir. Benzer şekilde Mart (2012)

Gönderildiği tarih: 14-04-2015 Kabul edildiği tarih: 22-09-2015

Elementary Education Online, 2015; 14(4): 1208-1221
İlköğretim Online, 2015; 14(4): 1208-1221. [Online]: http://ilkogretim-online.org.tr
doi: http://dx.doi.org/10.17051/io.2015.04635

araştırmasında katılımcıların yarısına yakının günlük bilgisayar kullanımın 4 saatten fazla olduğu sonucuna ulaşması, bu bulguları destekler niteliktedir.

Tablo 3. *Günlük İnternet Kullanım Süresi*

Günlük İnternet Kullanım Süresi	Frekans	Yüzde
1 saatten az	55	14,7
2-3 saat	163	43,5
4-6 saat	106	28,3
7 saat ve üzeri	51	13,6
Toplam	375	100

Tablo 3 incelendiğinde BÖTE öğretmen adaylarının %43,5'i günlük 2 ile 3 saat, % 28,3'ü günlük 4 ile 6 saat, %14,7'si günde 1 saatten az, %13,6'sı ise günde 7 saatten fazla internet kullandıklarını belirtmişlerdir. Bu bulgular BÖTE öğretmen adaylarının yarısına yakınının günde 2 ile 3 saat internette zaman geçirdiğini göstermektedir.

Tablo 4. *Bilişim Güvenliği Kursu veya Dersi Alma Durumu*

Bilişim güvenliği kursu veya dersi alma durumu	Frekans	Yüzde
Evet	114	30,4
Hayır	261	69,6
Toplam	375	100

Tablo 4'te de görüldüğü gibi BÖTE öğretmen adaylarının % 69,6'sı bilişim güvenliğini sağlamaya yönelik bir kurs veya ders almadıklarını belirtirken, % 30,4'ü bu konuda bir ders veya kurs aldıklarını belirtmişlerdir. Öğütçü (2010) gerçekleştirdiği çalışmasında, öğrencilerin %30,5'nin bilişim güvenliği eğitimi aldığı bulgusuna ulaşmıştır. Bu bulgular, bilişim güvenliğine yönelik zorunlu bir dersin olmadığı ve bu konuya yeterli önemin verilmediği düşüncesini doğurmaktadır. Ders aldığını belirtenlerin bir kısmının, dolaylı olarak bilişim güvenliğinden bahseden "İşletim sistemleri" vb. dersleri aldıkları düşünülmektedir. Ancak alındığı belirtilen eğitimlerin niteliği ile ilgili yeni araştırma bulgularına ihtiyaç duyulmaktadır.

Tablo 5. *Virüs Tarama Yazılımının Güncellenme Sıklığı*

Virüs tarama yazılımının güncellenme sıklığı	Frekans	Yüzde
Günlük	47	12,5
Haftalık	144	38,4
Yılda bir kez	61	16,3
Sadece kurduğum zaman	31	8,3
Kurulu virüs programım yok	49	13,1
Bilmiyorum	43	11,5
Toplam	375	100

Katılımcılara bilişim güvenliği konusunda duyarlılıklarının bir göstergesi olarak virüs tarama yazılımlarını güncelleme sorusu sorulmuştur. Tablo 5 incelendiğinde BÖTE öğretmen adaylarının %38.4'ü virüs tarama yazılımını haftada bir kez güncelliklerini, %12.5'i her gün güncelliklerini, %16.3'ü yılda bir kez güncelliklerini, %8.3'ü sadece kurdukları zaman güncelliklerini belirtmişlerdir. Ayrıca %13.1'i kurulu bir virüs programının olmadığını, %11.5'si güncelleme sıklığını bilmediklerini belirtmişlerdir. Bilişim güvenliğinin önemi ve virüs tarama yazılımlarının önemi dikkate alındığında adayların çok düşük oranının kurulu anti-virüs programlarının olmadığını belirtmeleri olumlu bir bulgu olarak görülmektedir. Bu bulgular, BÖTE öğretmen adaylarının çoğunun virüs tarama yazılımını günlük ve haftalık olmak üzere kısa zaman aralığında güncelliklerini göstermektedir. Diğer taraftan az sayıda da olsa anti-virüs yazılımı kullanmayan ve güncelleme duyarlılığı olmayan katılımcıların da olduğu dikkat çekmektedir.

Gönderildiği tarih: 14-04-2015 Kabul edildiği tarih: 22-09-2015

Elementary Education Online, 2015; 14(4): 1208-1221
İlköğretim Online, 2015; 14(4): 1208-1221. [Online]: http://ilkogretim-online.org.tr
doi: http://dx.doi.org/10.17051/io.2015.04635

BÖTE Öğretmen Adaylarının Hakkında Hiçbir Şey Duymadıkları Konular

BÖTE öğretmen adaylarının verdikleri yanıtlarda, ortalama değerin 1.49 ve altında olduğu hiçbir soru bulunmamaktadır. Bu bulgular, BÖTE öğretmen adaylarının bilişim güvenliği ile ilgili sorularda yer alan tüm konularla ilgili bir şeyler duyduklarını göstermektedir. Bu bulgunun nedeninin, adayların okudukları programda aldıkları derslerin içeriklerinden ve ayrıca öğrenim süreleri boyunca derslerde yapılan tartışmalar, arkadaşlarından, sosyal medyadan, ilgili yayınlardan ve medyadan öğrendikleri gizli öğretim programı (Kentli, 2009) olarak adlandırılan öğrenmelerden kaynaklanabileceği düşünülmektedir. Ancak katılımcıların bu çalışma sınırlılıkları kapsamında yer alan tüm konuları duymuş olmaları, bu konularla ilgili ve algıda seçici olduklarını göstermekle birlikte bu konuları bildikleri anlamına gelmemektedir.

BÖTE Öğretmen Adaylarının Duydukları Fakat Ne Anlama Geldiğini Bilmedikleri Konular

BÖTE öğretmen adaylarının duydukları fakat ne anlama geldiğini bilmedikleri konular Tablo 6'da verilmiştir.

Tablo 6. *BÖTE Öğretmen Adaylarının Duydukları Fakat Ne Anlama Geldiğini Bilmedikleri Konular*

Konular (*Tüm Yanıtlar İçin N=375)	$\overline{X}$	**SS**
Uygun Kullanım Politikası	2,49	1,13
Reklam Bedelli Yazılım (Adware)	2,49	1,04
Yapışkan Web Siteler	2,47	1,14
Türk Hukuk Sisteminde Bilişim Suçları Kanun Maddeleri	2,46	1,11
DoS Saldırısı (Denial of Service)	2,41	1,03
Nefret Grupları	2,23	1,09
Hacker'ların paylaştığı araçları kullananlar (Script Kiddies)	2,19	1,05
Kandırmacılık (Tricklers)	2,19	1,14
Sosyal Mühendislik	2,17	1,09
Arka kapılar (Back door)	2,14	1,13
Oltalama (Phishing)	1,97	1,07
Köle Bilgisayar (Zombi)	1,97	1,06
İçerik Toplayıcılık (Screen Scraping)	1,96	1,09
Bot ve Botnet	1,90	1,01
Spoofing	1,73	1,03
İntihal (Plagiarism)	1,70	0,96
Sniffing	1,67	1,01

Tablo 6 incelendiğinde, BÖTE öğretmen adaylarının duydukları fakat ne anlama geldiğini bilmedikleri konuların daha çok teknik bilgi gerektiren konular olduğu görülmektedir. Bulgular incelendiğinde BÖTE öğretmen adaylarının teknik bilgi gerektiren konuları bilmedikleri anlaşılmaktadır. Teknik konuların yanı sıra BÖTE öğretmen adaylarının İntihal'in ne anlama geldiğini bilmemeleri önemli bir bulgudur. Hâlbuki Associaton for Educational Communications and Technology (AECT, 2012) bilgi teknolojilerinin kullanılmasında özellikle etik kullanıma vurgu yapmaktadır. BÖTE öğretmen adaylarının, öğrencilerin bilişim güvenliğinin etik kullanımlarını sağlayacakları düşünüldüğünde, intihal'in ne olduğu bilmemeleri düşündürücü bir sonuç olarak görülmektedir. Bunun yanında öğretmen adaylarının günümüzde sıklıkla duyduğumuz oltalama, bot ve botnetler, sosyal mühendislik, DoS saldırıları ve reklam bedelli yazılımlar konularında bilgi sahibi olmamaları dikkate alınması gereken bir bulgu olarak görülmektedir. Çünkü yapılan araştırmalar, özellikle bu yöntemler kullanılarak saldırıların arttığını göstermektedir. Dolayısıyla öğretmen adaylarının bu konularda öğrencilerini bilgilendirecek yeterliliğe sahip olmaları ve öğrencileri bilgilendirmeleri bilişim güvenliğini sağlama açısından faydalı olacaktır.

BÖTE Öğretmen Adaylarının Bildikleri Fakat Öğrencilerine Öğretebilecek Yeterliliğe Sahip Olmadıklarını Düşündükleri Konular

BÖTE öğretmen adaylarının bildikleri fakat öğrencilerine öğretebilecek yeterliliğe sahip olmadıklarını düşündükleri konular Tablo 7'de verilmiştir.

Gönderildiği tarih: 14-04-2015 Kabul edildiği tarih: 22-09-2015

Elementary Education Online, 2015; 14(4): 1208-1221
İlköğretim Online, 2015; 14(4): 1208-1221. [Online]: http://ilkogretim-online.org.tr
doi: http://dx.doi.org/10.17051/io.2015.04635

Tablo 7. *BÖTE Öğretmen Adaylarının Bildikleri Fakat Öğrencilerine Öğretebilecek Yeterliliğe Sahip Olmadıklarını Düşündükleri Konular*

Konular (*Tüm Yanıtlar İçin N=375)	$\overline{X}$	**SD**
Şifreler	3,46	0,80
Kablosuz Aygıt Güvenliği	3,45	0,85
Çevrimiçi Oyunlar	3,44	0,84
Spam	3,44	0,82
Portlar	3,44	0,91
Güvenlik Ayarları	3,43	0,91
Güvenli Çocuk Portalları	3,41	0,86
Web kamera güvenliği	3,40	0,88
Korsan Yazılım	3,39	0,75
Sosyal Ağ Güvenliği	3,38	0,85
Mobil Teknoloji Güvenliği	3,36	0,90
Profil Denetimi	3,34	0,92
E-posta ekleri	3,32	0,93
Kaçak Yazılım Kullanma	3,29	0,82
Adil Kullanım	3,25	0,99
Şifreleme (Encryption)	3,25	0,93
Blog Güvenliği	3,24	0,95
Karalama / İftira / Hakeret	3,24	0,94
Çerezler (Cookies)	3,24	0,95
Erişim İzni	3,20	0,94
Son Kullanıcı Lisans Sözleşmesi	3,20	0,98
Zamanını doldurmuş eski teknojilerin elden çıkarılması	3,14	0,99
Ekran Kaydediciler (Screenlogger)	3,13	1,00
İnternet Filtreleri	3,13	0,95
Gizli Arşiv Dosyaları	3,12	0,96
Metin Mesaj Güvenliği	3,11	1,04
Siber Zorbalık	3,10	1,03
Önbelleğe Yüklenmiş Web Siteler	3,09	0,98
Spam Filtreleme	3,08	1,03
Değiştirilmiş Dijital Fotoğraflar	3,05	0,93
Reklam İçerikli Pencereler (Pop-Up Ads)	3,04	1,00
Sabit Diski olan Fotokopi makinelerinin ve tarayıcıların güvenliği	3,04	1,04
Yamalar	2,97	1,06
Casus Yazılım (Spyware)	2,91	0,98
Tuş Kaydediciler (Keylogger)	2,90	1,07
Bilişim Korsanlığı (Hacking)	2,89	0,94
Dijital Sertifikalar	2,88	0,98
Şifrelenmemiş e-mail	2,87	1,06
Çevrimiçi Kimlikler	2,78	1,08
Çalmak / Gasp / Hırsızlık (Hijack)	2,75	1,06
Vekil Sunucu (Proxy)	2,74	1,04
İzinsiz Yayınlama / Yasadışı Yayın	2,70	1,04
Kimlik Hırsızlığı	2,66	1,06
Takip Edilen Çerezler	2,64	1,13
MEB Bilgi ve Sistem Güvenliği Yönergesi	2,54	1,17
5651 sayılı internet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele kanunu	2,54	1,12
Filtre atlama	2,51	1,06
Çevrimiçi Kumar	2,50	1,14

Tablo 7'de BÖTE öğretmen adaylarının bildikleri fakat öğrencilerine öğretebilecek yeterliliğe sahip olmadıklarını düşündükleri konulara yer verilmiştir. Bilişim güvenliğinin sağlanmasında her konunun ayrı bir öneme sahip olduğu söylenebilir. BÖTE öğretmen adaylarının bu konuları

Gönderildiği tarih: 14-04-2015 Kabul edildiği tarih: 22-09-2015

Elementary Education Online, 2015; 14(4): 1208-1221
İlköğretim Online, 2015; 14(4): 1208-1221. [Online]: http://ilkogretim-online.org.tr
doi: http://dx.doi.org/10.17051/io.2015.04635

bilmelerine rağmen öğrencilerine öğretebilecek yeterliliğe sahip olmadıklarını düşünmeleri, BÖTE lisans öğretim programında bilişim güvenliği ve bilişim güvenliği eğitimine yönelik zorunlu bir dersin olmayışına bağlanabilir. Ayrıca, özellikle adayların şifreler, spam, güvenlik ayarları, sosyal ağ güvenliği, mobil teknoloji güvenliği, e-posta ekleri, çerezler, siber zorbalık, casus yazılım, tuş kaydedici yazılımlar gibi önemli konuları öğretebilecek yeterliliğe sahip olmadıklarını belirtmeleri, bilişim güvenliğine yönelik derslerin verilmesinin gerekli olduğunu göstermektedir. Öte yandan bu çalışmada adaylarının büyük çoğunluğunun (%69,6) bilişim güvenliğine yönelik bir ders veya kurs almadıklarına yönelik bulgu göz önüne alındığında (Tablo 5) adayların birçok konuda kendini yeterli görmemeleri doğal bir sonuç olarak görülmektedir.

BÖTE Öğretmen Adaylarının Bildikleri ve Öğrencilerine Öğretebilecek Yeterliliğe Sahip Olduklarını Düşündükleri Konular

BÖTE öğretmen adaylarının bildikleri ve öğrencilerine öğretebilecek yeterliliğe sahip olduklarını düşündükleri konular Tablo 8'de verilmiştir.

Tablo 8. *BÖTE Öğretmen Adaylarının Bildikleri ve Öğrencilerine Öğretebilecek Yeterliliğe Sahip Olduklarını Düşündükleri Konular*

Konular (*Tüm Yanıtlar İçin N=375)	$\overline{X}$	**SD**
Video ve Resim Gönderme	3,71	0,67
Güvenli İnternet Hizmeti	3,68	0,66
Yazılım Güncellemesi	3,60	0,71
Cep Telefonu Güvenliği	3,60	0,72
Taşınabilir Veri Depolama Aygıtlarının Güvenliği	3,58	0,83
Gizlilik	3,57	0,74
Dosya Paylaşım Güvenliği	3,56	0,75
Zararlı Yazılımlar (Virüs, Solucan, Truva atı vb.)	3,54	0,75
Güvenli Siteler	3,54	0,76
Telif Hakkı	3,53	0,80
Güvenlik Duvarı	3,52	0,78

Tablo 8'de BÖTE öğretmen adaylarının bildikleri ve öğrencilerine öğretebileceklerini düşündükleri konulara yer verilmiştir. Tablo 8 incelendiğinde adayların toplam 67 konu arasından sadece 11 konu hakkında kendilerini yeterli gördükleri anlaşılmaktadır. Bu bölümden mezun olacak adayların ilerde görev alacakları okullarda bilişim güvenliği konusunda rehberlik yapacakları göz önüne alındığında, kendilerini yeterli gördükleri konuların daha fazla sayıda olması beklenmektedir. Fakat yine de BÖTE öğretmen adaylarının güvenli internet hizmeti, güvenlik duvarı, yazılım güncellemesi, zararlı yazılımlar, dosya paylaşımı, taşınır belleklerin güvenli kullanımı vs. gibi konuları öğretebilecek yeterliliğe sahip olduklarını belirtmeleri yeterli olmasa da olumlu bir bulgu olarak görülmektedir.

SONUÇLAR VE TARTIŞMA

Bu araştırmanın en önemli sonuçları, BÖTE öğretmen adaylarının büyük bir oranın bilişim güvenliğine yönelik bir eğitim almadıklarının ve bilişim güvenliği eğitimi vermeye yönelik yeterliklerinin düşük olduğunun belirlenmesi olmuştur. Öğütçü (2010) de benzer biçimde üniversitede çalışan akademik ve idari personelin % 77,7'sinin bilişim güvenliğine yönelik bir eğitim almadıklarını belirlemiştir. Bu sonuçlardan yükseköğretim düzeyinde bile bilişim güvenliğine yönelik seminer, kurs veya eğitim gibi faaliyetlere yeterince önem verilmediği veya bu konuya yönelik bir girişimin olmadığı anlaşılmaktadır. BÖTE lisans programından mezun olacak öğretmen adaylarının okullarda bilişim teknolojilerinin etkili, bilinçli ve güvenli kullanımından sorumlu olacakları düşünüldüğünde, BÖTE öğretmen adaylarına bilişim güvenliğini sağlamaya dönük bir eğitimin verilmesinin, BÖTE lisans programında bilişim güvenliğine yönelik zorunlu bir dersin olmasının faydalı olacağı düşünülmektedir.

Gönderildiği tarih: 14-04-2015 Kabul edildiği tarih: 22-09-2015

Elementary Education Online, 2015; 14(4): 1208-1221
İlköğretim Online, 2015; 14(4): 1208-1221. [Online]: http://ilkogretim-online.org.tr
doi: http://dx.doi.org/10.17051/io.2015.04635

Son yıllarda gerçekleştirilen çalışmalar (Canbek ve Sağıroğlu, 2007; Marinos, 2013; Symantec, 2013) bilişim güvenliğini sağlamaya yönelik faaliyetlerin yapılmasının önemine vurgu yapmaktadır. Bu çalışmada araştırma kapsamında sorulan sorular dikkate alındığında, BÖTE öğretmen adaylarının duymadıkları bir bilişim güvenliği konusunun olmadığı sonucuna ulaşılmıştır. Pusey ve Sadera (2011) öğretmen adayları üzerinde gerçekleştirdikleri çalışmada adayların arka kapılar, filtre atlama, bot, yapışkan web siteler, hacker'ların paylaştığı araçları kullananlar (script kiddies), sniffing ve köle bilgisayar konularını duymadıkları sonucuna ulaşmışlardır. BÖTE bölümünün özelliği dikkate alındığında, öğretmen adayların duymadıkları konuların olmaması olumlu bir sonuç olarak değerlendirilmektedir.

BÖTE öğretmen adaylarının duydukları fakat ne anlama geldiğini bilmedikleri konular; reklam bedelli yazılım, uygun kullanım politikası, yapışkan web siteler, Türk hukuk sisteminde bilişim suçları kanun maddeleri, DoS saldırıları, nefret grupları, hacker'ların paylaştığı araçları kullananlar (script kiddies), sosyal mühendislik, arka kapılar, oltalama, köle bilgisayar, içerik toplayıcılık (screen scraping), bot ve botnet, spoofing, sniffing ve intihal'dir. Benzer şekilde Pusey ve Sadera (2011) öğretmen adaylarının duydukları fakat ne anlama geldiğini bilmedikleri konular içerisinde reklam bedelli yazılım, uygun kullanım politikası, oltalama, DoS saldırıları, sosyal mühendislik ve spoofing konularını gösteren sonuca ulaşmışlardır. Özelikle intihal, oltalama, bot ve botnet, sosyal mühendislik, DoS saldırıları, reklam bedelli yazılım günümüzde en sık karşılaşılan tehditler arasında bulunmakta ve yapılan çalışmalarda bu konuların önemine değinilmektedir (Djile ve Doğan, 2011; Marinos, 2013; Symantec, 2013). İntihal konusunda Ural ve Sulak'ın (2012) üniversite öğrencileri üzerinde gerçekleştirdiği çalışmalarında öğrencilerin kopyala-yapıştır yöntemini çok kullandıkları, referans göstermenin yaygın olmadığı, referans gösterirken uygun referans gösteriminin yapılmadığı tespit edilmiştir. Associaton for Educational Communications and Technology'nin (AECT, 2012) bilgi teknolojilerinin kullanılmasında özellikle etik kullanıma vurgu yapması bu konunun önemini göstermektedir. Benzer biçimde bu çalışmada, BÖTE öğretmen adaylarının çoğunlukla intihalin ne olduğunu bilmedikleri bulunmuştur. Bu bilgi eksikliğinin, intihalin yaygın bir şekilde yapılmasına sebebiyet verdiği düşünülmektedir.

Günümüzde önemli konulardan ve gerçekleştirilen saldırılardan biri de kullanıcıların sahte web sitelerine yönlendirilmesidir. Sahte web sitelerine yönlendirme, kullanıcıların bilinçsizliğinden yararlanılarak bir sosyal mühendislik saldırısı olan oltalama diye bilinen yöntem ile yapılmaktadır. Symantec raporunda (2013) her geçen yıl sosyal mühendislik saldırılarının arttığı ve en sık gerçekleşen saldırılardan birinin oltalama saldırısı olduğu görülmektedir. Benzer şekilde Marinos (2013) araştırmasında, en çok gerçekleştirilen saldırılar arasında oltalama yönteminin bulunduğunu belirtmektedir. Kruger, Flowerday, Drevin ve Steyn ise (2011) üniversite öğrencileri üzerinde gerçekleştirdikleri araştırmada öğrencilerin yarısının, sosyal mühendislik ve oltalamanın ne olduğunu bilmedikleri sonucuna ulaşmışlardır. Bu çalışmada ve Pusey ve Sadera'nın (2011) gerçekleştirdikleri çalışmada da öğretmen adaylarının sosyal mühendislik ve oltalama hakkında bilgi sahibi olmamaları tehlikenin boyutunu gözler önüne sermektedir. Ünver, Canbay ve Mirzaoğlu (2009) kötü niyetli kişilerin botnetler, oltalama, reklam bedelli yazılımlar, sosyal mühendislik, DoS saldırıları, sniffing ve spoofing yöntemlerini kullanarak sistemlere yetkisiz bir şekilde eriştiklerini, bu sistemleri çalışmaz hale getirdiklerini, bilgileri değiştirdiklerini, bilgileri yok ettiklerini ve ifşa ettiklerini vurgulamaktadır. Dolayısıyla bireylerin ve kurumların bu gibi kötü niyetli kişilerin açık hedefi haline gelebilme ihtimalleri dikkate alındığında, bu konuların ne kadar önemli olduğu ve bu gibi tehditlere karşı önlemlerin alınması gerektiği anlaşılmaktadır. Ayrıca son yıllarda bu saldırıların gittikçe artması, bu konularda eğitim verilmesinin gerekli olduğunu göstermektedir.

BÖTE öğretmen adaylarının bildiklerini fakat öğrencilerine öğretebilecek yeterliliğe sahip olmadıklarını düşündükleri konular: Şifreler, kablosuz aygıt güvenliği, spam, web kamera güvenliği, korsan yazılım, sosyal ağ güvenliği, mobil teknolojilerin güvenliği, şifreleme, çerezler, ekran kaydedici yazılımlar, güvenlik ayarları, siber zorbalık, reklam içerikli pencereler (Pop-up Ads), casus yazılım, tuş kaydedici yazılımlar ve 5651 sayılı bilişim suçları kanunu şeklinde tespit edilmiştir. Benzer şekilde Pusey ve Sadera (2011) öğretmen adaylarının bildikleri fakat öğrencilerine öğretebilecek yeterliğe sahip olmadıklarını düşündükleri konular içerisinde şifreler, kablosuz aygıt güvenliği, sosyal ağ güvenliği, reklam içerikli pencereler, siber zorbalık, web kamera güvenliği, spam, casus yazılım ve güvenlik ayarları konularını içeren sonuca ulaşmışlardır. Bu konular ile ilgili yapılan

Gönderildiği tarih: 14-04-2015 Kabul edildiği tarih: 22-09-2015

Elementary Education Online, 2015; 14(4): 1208-1221
İlköğretim Online, 2015; 14(4): 1208-1221. [Online]: http://ilkogretim-online.org.tr
doi: http://dx.doi.org/10.17051/io.2015.04635

çalışmalara bakıldığında, sosyal ağ kullanımı güvenliği açısından Horzum ve Ayas'ın (2011) ortaöğretim öğrencilerinin siber zorba ve mağdur olma düzeylerini belirlediği çalışmada siber zorbalığın ilerleyen yıllarda teknolojinin gelişmesi ve kullanımının artmasıyla daha fazla yaşanacağı görüşü dikkat çekmektedir. Bu nedenle öğrencilere, teknolojik araçların yanlış kullanılması durumunda bireylerin olumsuz etkilenebileceğine yönelik bilgilendirme çalışmalarının yapılmasının önemli olduğunu belirtmişlerdir. Sosyal ağların güvenli kullanımı konusunda Mert, Bülbül ve Sağıroğlu (2012) öğrenciler üzerinde gerçekleştirdikleri araştırmalarında, öğrencilerin büyük çoğunluğunun (%77) sosyal paylaşım sitesi hesabının olduğunu ve bu sitelerde doğum tarihi, telefon numarası, nerede olduklarına dair bilgileri paylaştıkları sonucuna ulaşmışlardır. Yine sosyal ağların güvenliği konusunda Yavanoğlu, Sağıroğlu ve Çolak ise (2012) yaptıkları çalışmalarında sosyal ağlarda kimlik avı, spam, bot saldırıları, oltalama, sahte linkler gibi güvenlik ihlallerinin olduğunu belirtmektedirler. Bu çalışmada, BÖTE öğretmen adaylarının sosyal ağların güvenliğini sağlama konusunda kendilerini yeterli görmemeleri ve yapılan çalışmalarda (Mert vd., 2012; Yavanoğlu vd., 2012) bireylerin sosyal ağ güvenliği konusunda uygun hareket etmemeleri bu konularda eğitime gereksinim olduğunu göstermektedir. BÖTE öğretmen adayları bu konuları öğretebilecek yeterliliğe sahip olmadıklarını belirtmişlerdir. Bunun olası nedeninin BÖTE lisans programlarında bilgisayar ve internet güvenliğine yönelik zorunlu bir dersin olmayışının ve adayların bilişim güvenliği konusunda bir eğitim almamalarının olduğu düşünülmektedir.

BÖTE öğretmen adaylarının öğretebilme yeterliliğine sahip olduklarını düşündükleri konular ise; güvenli internet hizmeti, yazılım güncellemesi, dosya paylaşım güvenliği, gizlilik, cep telefonu güvenliği, zararlı yazılımlar, güvenli siteler, telif hakkı ve güvenlik duvarıdır. Pusey ve Sadera (2011) kendi çalışmalarında sadece dört konuda öğretmen adaylarının yeterli olduğu sonucuna ulaşmıştır. Bu konular e-posta ekleri, cep telefonu güvenliği, intihal ve metin mesaj güvenliği olarak tespit edilmiştir. Pusey ve Sadera (2011) öğretmen adaylarının intihali öğretebilecek yeterliliğe sahip olmalarının nedeni olarak bu konuya eğitim ortamlarında yaygın bir şekilde değinmelerinin etkisinin olduğunu belirtmişlerdir. Bu araştırma sonuçlarında ise intihal katılımcıların duydukları fakat ne anlama geldiğini bilmedikleri bir konu olarak belirlenmiştir. Benzer şekilde Türkiye'de de bilişim güvenliği ile ilgili konulara önem vermenin ve yaygın bir şekilde bu konulara yer vermenin olumlu sonuçlar vereceği düşünülmektedir. Buradan anlaşılacağı üzere internet ortamında nasıl güvenli hareket edileceğine ve yapılması gereken güvenlik tedbirlerine yönelik bilgilendirmeler olumlu sonuçlar doğurmaktadır. Güvenli internet hizmeti konusunda Demirel, Yörük ve Özkan (2012) ebeveynlerin güvenli internet hizmetinden haberdar olma durumlarının yeterli olmadığı sonucuna ulaşmıştır. Bu açığın kapatılması açısından BÖTE öğretmen adaylarının bu konuyu öğrencilerine öğretebilecek yeterliliğe sahip olduklarını belirtmeleri güvenli internet hizmetinin kullanımı ve bu konuda öğrencilere bilgilendirme yapılması açısından olumlu bir sonuç olarak görülmektedir. Öğretmen adaylarının ileride görev alacakları okullarda bilişim güvenliği konusunda rehberlik yapacakları göz önüne alındığında, kendilerini yeterli gördükleri konuların daha fazla sayıda olması beklenmektedir. Fakat yine de BÖTE öğretmen adaylarının güvenli internet hizmeti, güvenlik duvarı, yazılım güncellemesi, zararlı yazılımlar, dosya paylaşımı, taşınır belleklerin güvenli kullanımı vs. gibi konuları öğretebilecek yeterliliğe sahip olduklarını belirtmeleri olumlu görülmektedir.

Genel olarak araştırma sonuçları dikkate alındığında BÖTE öğretmen adaylarının bilişim güvenliği konularını öğretebilmeye yönelik yeterlilik algılarının düşük olduğu görülmüştür. Benzer şekilde Pruitt-Mentle ve Pusey (2010) çok az öğretmenin temel güvenlik konularını öğrettikleri sonucuna ulaşmışlardır. Tekerek ve Tekerek'in (2013) öğrencilerin temel bilişim güvenliğini sağlama konularında farkındalıklarının çok düşük olduğu sonucuna ulaşmaları okullarda öğrencilere bilişim güvenliği konusunda eğitim verilmediğini veya öğretmenlerin bu konuda yeterli bilgiye sahip olmadıkları düşüncesini akla getirmektedir. Nitekim yurtdışında National Cyber Security Alliance (NCSA) (2011) tarafından gerçekleştirilen araştırmada öğrencilerin bilişim güvenliğine yönelik bilgilerin düşük düzeyde olmasının tespit edilmesi ve ülkemizde de internet kullanıcılarının, bireylerin interneti güvenli kullanma, bilişim güvenliğini sağlama, gelebilecek güvenlik tehditlerine karşı önlem alma konusunda bilgi düzeylerinin düşük olduğu (Dijle, 2006; Dijle ve Doğan 2011; Karaoğlan-Yılmaz vd., 2014; Kaşıkçı, Çağıltay, Karakuş, Kurşun ve Ogan, 2014; Mert vd., 2012; Tekerek ve Mart, 2010; Tekerek ve Tekerek, 2013) sonucuna ulaşılması bu düşünceyi doğrulamaktadır. Dolayısıyla bu sonuçlardan hareketle öğrencilerin bilişim teknolojilerini ve interneti kullanırken

Gönderildiği tarih: 14-04-2015 Kabul edildiği tarih: 22-09-2015

Elementary Education Online, 2015; 14(4): 1208-1221
İlköğretim Online, 2015; 14(4): 1208-1221. [Online]: http://ilkogretim-online.org.tr
doi: http://dx.doi.org/10.17051/io.2015.04635

karşılaşabilecekleri güvenlik tehditlerine karşı kendilerini nasıl koruyacaklarının öğretilmesi önemli bir konuma gelmektedir.

Sonuç olarak bu araştırmada BÖTE öğretmen adaylarının bilişim güvenliğine yönelik yeterli düzeyde kurs veya ders almadıkları, BÖTE öğretmen adaylarının bilişim güvenliği ile ilgili 17 konunun ne anlama geldiğini bilmedikleri, 48 konuyu öğretebilecek yeterliliğe sahip olmadıkları ve 11 konuyu öğretebilecek yeterliliğe sahip oldukları sonucuna ulaşılmıştır. BÖTE öğretmen adayların toplam 76 konudan sadece 11 konuyla ilgili kendilerini bu konuları öğretebilecek yeterliliğe sahip olduklarını belirtmeleri, adayların bilişim güvenliği eğitimi verebilme açısından yetersiz olduklarını göstermektedir. Bu sonuçlardan hareketle aşağıdaki öneriler sunulmuştur.

ÖNERİLER

BÖTE öğretmen yetiştirme programında bilişim güvenliği ve bilişim güvenliği eğitimi verebilmeye yönelik konulara ya da derslere yer verilmesinin yararlı olacağı düşünülmektedir. Bu tür derslerin BÖTE bölümü için zorunlu, diğer öğretmen yetiştirme programları için ise seçmeli olarak yer almasının bilişim teknolojilerini güvenli kullanma, güvenli kullanıma yönelik eğitim verme ve rehberlik yapma açılarından katkı sağlayacağı düşünülmektedir. Bunun yanında şu an çalışmakta olan öğretmenler için düzenlenecek seminerler ve kurslar ile öğretmenlerin bilişim güvenliğini sağlama ve öğrencilere rehberlik yapabilme bilgi ve becerileri artırılabilir. Bilişim güvenliğine yönelik verilecek eğitimlerin hedeflerinin, içeriğinin ve yönteminin belirlenmesinde tüm paydaşların görüşlerinin alınması ve bundan sonra harekete geçilmesi verimliliği artırabilir. Bu çalışmada geçen konu başlıkları ihtiyaç analizin yapılması ve bilişim güvenliği ders içeriğinin belirlenmesi çalışmaları için kullanılabilir. Çalışmada kullanılan anketin var olan durumun daha iyi anlaşılması için hedef kitlesi farklı başka araştırmalarda da kullanılması önerilmektedir. İleride yapılacak araştırmalarda bilişim güvenliği yeterliliği ile siber zorbalık ve siber suçlara maruz kalma, siber dünyanın sosyo-psikolojik özellikler üzerindeki olumlu ve olumsuz etkileri gibi konulara odaklanılmasının güvenli bilişim teknolojisi kullanımının önemine ve nasıl olması gerektiğine yönelik konularda katkı sağlayabileceği düşünülmektedir.

KAYNAKÇA

Association for Educational Communications and Technology. (2012). AECT Standarts. http://c.ymcdn.com/sites/aect.site-ym.com/resource/resmgr/AECT_Documents/AECT_Standards_adopted7_16_2.pdf adresinden 20.04.2014 tarihinde erişilmiştir.

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

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

Canbek, G. (2005). *Klavye dinleme ve önleme sistemleri analiz, tasarım ve geliştirme*. Yüksek lisans tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.

Canbek, G. ve Sağıroğlu Ş. (2007). Bilgisayar sistemlerine yapılan saldırı türleri: bir inceleme. *Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 23*(1-2), 1 – 12.

Çelik, L. (2007). Bilişim teknolojileri. B. Güneş (Ed.), *Bilgisayar-1* (5-24). Ankara: EDM Özel Eğitim Hizmetleri Yayıncılık.

Demir, E. (2006). *Birey ve aile yaşamına ilişkin konularda internet kullanımının etkisinin belirlenmesi*. Yüksek lisans tezi, Ankara Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.

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.

Gönderildiği tarih: 14-04-2015 Kabul edildiği tarih: 22-09-2015

Horzum, M.B. ve Ayas, T. (2011). Ortaöğretim öğrencilerinin sanal zorba ve mağdur olma düzeylerinin okul türü ve cinsiyet açısından incelenmesi. *Eğitim Bilimleri ve Uygulama, 10* (20), 139-159.

ISTE. (2008). *National Educational Standards for Teachers*. http://www.iste.org/docs/pdfs/nets-t-standards.pdf?sfvrsn=2 adresinden 23.12.2013 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.

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.

Kentli, F. D. (2009). Comparison of hidden curriculum theories. *Europian Journal of Educational Studies, 1(2), 83 – 88.*

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

Kruger, H.A, Flowerday, S., Drevin, L. ve Steyn, T. (2011). An assessment of the role of cultural factors in ınformation security awareness. *Information Security South Africa Conference*, 15-17 August 2011, Johannesburg, South Africa. DOI:10.1109/ISSA.2011.6027505.

Maheshwari, H., Hyman H.S. ve Agrawal, M. (2011). A comparison of cyber-crime definitions in India and the United States. R. Santanam, M. Sethumadanhavan ve M. Virendra. (Ed.), *Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives.* (33-45) Hershey: İnformation Science Reference.

Marinos, L. (2013). ENISA Threat Landscape 2013: Overview of current and emerging cyber-threats. Heraklion: European Union Agency for Network and Information Security Publishing. doi:10.2788/14231. www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats adresinden 15.06.2013 tarihinde erişilmiştir.

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

Mert, M., Bülbül, H.İ. ve Sağıroğlu, Ş. (2012). Milli Eğitim Bakanlığına bağlı okullarda güvenli internet kullanımı. *Türk Bilim Araştırma Vakfı Bilim Dergisi, 5*(4), 1-12.

Milli Eğitim Bakanlığı. (2008). Bilişim teknolojileri öğretmeni özel alan yeterlikleri. http://otmg.meb.gov.tr/alanbt.html adresinden 15.06.2013 tarihinde erişilmiştir.

National Cyber Security Alliance. (2011). The State of K-12 Cyberethics, cybersafety and cybersecurity curriculum in the United States. C:\Users\Sau\Downloads\Documents\2011_national_k12_study.pdf adresinden 28.03.2014 tarihinde erişilmiştir.

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

Pati, P. (t.y). Cyber crime, http://www.naavi.org/pati/pati_cybercrimes_dec03.htm adresinden 25.02.2014 tarihinde erişilmiştir.

Pruitt-Mentle, D. ve 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. ve Sadera, W.A. (2011). Cyberethics, cybersafety and cybersecurity: preservice teacher knowledge, preparedness and the need for teacher education to make a difference. *Journal of Digital Learning in Teacher Education, 28*(2), 82-88.

Richardson, R. (2008). CSI computer crime and security survey, http://www.sis.pitt.edu/jjoshi/courses/IS2150/Fall11/CSIsurvey2008.pdf adresinden 24.02.2014 tarihinde erişilmiştir.

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

Symantec. (2013). Internet security threat report 2013. http://www.symantec.com/content/en/us/enterprise/other_resources/bistr_main_report_v18_2012_21291018.en-us.pdf adresinden 24.02.2014 tarihinde erişilmiştir.

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' ınformation 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 26.12.2013 tarihinde erişilmiştir.

Ulaşanoğlu, M. E., Yılmaz, R. ve Tekin, M. A. (2010). *Bilgi güvenliği: Riskler ve öneriler*. Bilgi Teknolojileri ve İletişim Kurumu. Ankara.

Ural, M.N. ve Sulak, S.A. (2012). Plagiarism via Internet on undergraduate students in Turkey. *Journal of Educational and Instructional Studies, 2*(3), 2146-7463.

Ünver, M., Canbay, C. ve Mirzaoğlu, A. G. (2009). *Siber güvenliğin sağlanması: türkiye'de mevcut durum ve alınması gereken önlemler*. Bilgi Teknolojileri ve İletişim Kurumu. Ankara.

Yavanoğlu, U., Sağıroğlu, Ş. ve Çolak, İ. (2012). Sosyal ağlarda bilgi güvenliği tehditleri ve alınması gereken önlemler. *Politeknik Dergisi, 15*(1), 15-27.