T. C.

SAKARYA ÜNİVERSİTESİ EĞİTİM BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ

ANABİLİM DALI

BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ BİLİM DALI

BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ ÖĞRETMEN ADAYLARININ BİLİŞİM GÜVENLİĞİ EĞİTİMİ VEREBİLME YETERLİKLERİNİN İNCELENMESİ

YÜKSEK LİSANS TEZİ

ÖMER FARUK GÖKMEN

DANIŞMAN

YRD. DOÇ. DR. ÖZCAN ERKAN AKGÜN

TEMMUZ 2014

T. C.

SAKARYA ÜNİVERSİTESİ EĞİTİM BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ

ANABİLİM DALI

BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ BİLİM DALI

BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ ÖĞRETMEN ADAYLARININ BİLİŞİM GÜVENLİĞİ EĞİTİMİ VEREBİLME YETERLİKLERİNİN İNCELENMESİ

YÜKSEK LİSANS TEZİ

ÖMER FARUK GÖKMEN

DANIŞMAN

YRD. DOÇ. DR. ÖZCAN ERKAN AKGÜN

TEMMUZ 2014

BİLDİRİM

Hazırladığım tezin tamamen kendi çalışmam olduğunu, akademik ve etik kuralları gözeterek çalıştığımı ve her alıntıya kaynak gösterdiğimi taahhüt ederim.

Ömer Faruk GÖKMEN

01.07.2014

'Bilgisayar ve Öğretim Teknolojileri Eğitimi Öğretmen Adaylarının Bilişim Güvenliği Eğitimi Verebilme Yeterliklerinin İncelenmesi' başlıklı bu yüksek lisans tezi, Bilgisayar ve Öğretim Teknolojileri Anabilim/bilim Dalında hazırlanmış ve jürimiz tarafından kabul edilmiştir.

Jüri Başkanı: Doç. Dr. Mübin KIYICI

Üye: Yrd. Doç. Dr. Hüseyin ÇALIŞKAN

Üye: Yrd. Doç. Dr. Özcan Erkan AKGÜN

Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım.

11.. / 07 / 2014

(imza)

Prof. Dr. İsmail GÜLEÇ

Enstitü Müdürü

ÖNSÖZ

Gittikçe artan teknoloji kullanımı pek çok sorunu beraberinde getirmektedir. Özellikle son yıllarda işlenen suçların sanal ortama kaydığını görmekteyiz. Ayrıca yapılan araştırmalarda, bilgisayar ve internet ortamında güvenliği tehdit eden unsurların ve yöntemlerin arttığı vurgulanmaktadır. Bu açıdan bakıldığında geleceğimizin teminatı çocukları bu gibi tehditlere karşı bilgilendirmek ve gerekli önlemleri almalarını sağlamak önemli bir husus olarak karşımıza çıkmaktadır. Dolayısıyla okullarda görev yapacak bilgisayar ve öğretim teknolojileri eğitimi öğretmen adaylarının bu konulara yönelik bilgilerinin ve bu konuları öğretebilme yeterliliklerinin ne düzeyde olduğunun araştırılması gerekmektedir. Nitekim alan yazında bu konuya yönelik az sayıda çalışma olduğu görülmüştür.

Araştırmam boyunca beni sabırla ve anlayışla karşılayan, hiçbir desteğini esirgemeyen, çalışmanın gerekliliğine vurgu yapan ve beni yönlendiren tez danışmanım Sayın Yrd. Doç. Dr. Özcan Erkan Akgün'e sonsuz ve gönülden teşekkür ederim. Ayrıca çalışmam boyunca her konuda bana manevi güç veren sevgili anneme, babama ve kardeşlerime çok teşekkür ederim. Çalışma ortamımda bana yardımcı olan ve desteklerini esirgemeyen çalışma arkadaşlarıma da teşekkürlerimi iletmeyi bir borç bilirim.

ÖZET

BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ ÖĞRETMEN ADAYLARININ BİLİŞİM GÜVENLİĞİ EĞİTİMİ VEREBİLME YETERLİLİKLERİNİN İNCELENMESİ

Gökmen, Ömer Faruk

Yüksek Lisans Tezi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı

Danışman: Yrd. Doç. Dr. Özcan Erkan AKGÜN

Temmuz, 2014. xvi + 110 Sayfa.

Bu araştırma, Bilgisayar ve Öğretim Teknolojileri Eğitimi bölümü öğretmen adaylarının bilişim güvenliği bilgilerini ve bilişim güvenliğine yönelik eğitim verebilme yeterliliklerini belirlemek amacıyla gerçekleştirilmiştir.

Araştırmanın çalışma grubunu Sakarya, Amasya, Erzincan ve Siirt Üniversitelerinin Eğitim Fakültesi Bilgisayar ve Öğretim Teknolojileri Eğitimi bölümü 3. ve 4. sınıfta okuyan 375 öğrenci oluşturmaktadır. Araştırma nicel araştırma yöntemlerinden tarama modeli ile gerçekleştirilmiştir. Veriler, Türkçe'ye uyarlanan veri toplama aracı ile toplanmıştır. Eğitim Fakültesi BÖTE bölümünden doktorasını tamamlamış 3, Yönetim Bilişim Sistemlerinde bilişim güvenliği konusunda doktora yapan 1, Bilişim suçları konusunda doktorasını tamamlamış 1 ve Sakarya Emniyet Müdürlüğü Bilişim suçları biriminde görev yapan 1 emniyet mensubu olmak üzere toplam 6 kişiden uzman görüşü alınarak düzeltmeler ve konuya yönelik eklemeler yapılmıştır. Uyarlanan anket, bilişim güvenliği bilgisini ölçen 7 soru ve 4'lü derecelendirme özelliğine sahip 76 maddeden oluşmaktadır. Verilerin analizinde yüzde, frekans ve ortalama değerlerinden yararlanılırken, adayların bilişim güvenliği bilgilerinin çeşitli değişkenlere göre anlamlı farklılıklar gösterip göstermediğini belirlemek için ise Kruskal Wallis H-Testi ve Mann Whitney U-Testi yapılmıştır.

Araştırma sonuçlarına göre Bilgisayar ve Öğretim Teknolojileri Eğitimi bölümü öğretmen adaylarının bilişim güvenliği bilgilerinin cinsiyete ve öğrenim görülen üniversiteye göre farklılaştığı görülürken; sınıfa, yaşa, günlük bilgisayar kullanım süresine, günlük internet kullanım süresine, bilgisayar sahiplik yılına ve bilişim

güvenliğin yönelik bir ders veya kurs alınıp alınmadığı durumuna göre farklılık göstermediği tespit edilmiştir. Ayrıca Bilgisayar ve Öğretim Teknolojileri Eğitimi bölümü öğretmen adaylarının büyük çoğunluğunun bilişim güvenliğine yönelik bir kurs veya ders almadıkları sonucuna ulaşılmıştır. Araştırmanın bir diğer sonucu, adayların bilişim güvenliği bilgilerinin düşük düzeyde olduğu ve bilişim güvenliği eğitimi verebilme konusunda az sayıda konuda yeterli olduklarıdır. Bilişim güvenliğini tehdit eden unsurların ve bilişim suçlarının günümüzde arttığı göz önüne alındığında, Bilgisayar ve Öğretim Teknolojileri Eğitimi öğretmen adayların bilgilerinin ve yeterliliklerinin beklenen düzeyde olmaması araştırmadan çıkarılabilecek en önemli sonuç olarak görülmektedir. Araştırma sonuçlarından yola çıkarak, Bilgisayar ve Öğretim Teknolojileri Eğitimi öğretmen adaylarının bu konularda yeterli bilgi sahibi olmalarını ve bilişim güvenliğini sağlamaları amacıyla Bilgisayar ve Öğretim Teknolojileri Eğitimi lisans programında bu konuya yönelik zorunlu bir dersin olmasının faydalı olacağı düşünülmektedir. Bunun yanında bilişim güvenliğini tehdit eden unsurlara karşı önleyici tedbirlerin uygulanmasına yönelik bilgilendirme faaliyetlerinin yapılması yararlı olacaktır.

Anahtar Kelimeler: Bilişim Güvenliği, Farkındalık, Bilişim Güvenliği Yeterliliği, BÖTE, Öğretmen Adayı

ABSTRACT

AN ANALYSIS OF COMPUTER EDUCATION AND INSTRUCTIONAL TECHNOLOGY STUDENT TEACHERS' EFFICIACY TO TEACH INFORMATION SECURITY

Gokmen, Omer Faruk

Master Thesis, Department of Computer Education and Instructional Technology

Supervisor: Assist. Prof. Dr. Ozcan Erkan AKGUN

July, 2014. xvi + 110 Pages.

This research was conducted to determine computer education and instructional technology department student teachers' knowledge of information security and efficiacy to teach information security.

Participants of this study consisted of 3 and 4. grade computer education and instructional technology student teachers from Sakarya, Amasya, Erzincan and Siirt Universities. Participants were consisted of 375 computer education and instructional technology student teachers. The study carried out with descriptive survey model which is one of the quantitative research methods. Data was collected with an information security survey which is adopted to Turkish language by the researches. The information security instrument was put into final form by taking opinions of 3 experts who have a PhD degree at computer education and instructional technology field, 1 expert who have a PhD degree on preventing cybercrime, 1 police officer working on preventing cybercrime and 1 PhD student working on information security from department of management information systems. The information security survey consists of 7 knowledge questions about information security and 76 likert type 4-point items on information security topics. While analyzing the data, frequency, percentage, and mean scores were calculated and to determine whether the student teachers' knowledge of information security differs according to the various variables, Mann Whitney U test and Kruskall Wallis test were applied.

According to the results, it was concluded that while computer education and instructional technology student teachers' information security knowledge differ with

gender and university, it doesn't differ with daily computer usage time, daily internet usage time, age, grade, computer ownership period and whether they enrolled a course o lecture about information security or not. Besides, most of computer education and instructional technology student teachers were concluded not to take any course or lecture about information security training. Another result of this study is that computer education and instructional technology student teachers' knowledge about information security level is low and efficiacy to teach information security is not well enough in many information security topics. Taking into account the factors that threat information security and cybercrime, the level of computer education and instructional technology student teachers' information security knowledge and the efficiacy to teach information technology topics being not at the expected level is the most important result of this study. Based on the results, it is thought that it will be useful for student teachers to put a compulsory course to computer education and instructional technology curriculum for the aim of providing information security and have adequate knowledge about cyber security. Furthermore, it will be useful to actualize informative and practical activities about applying prevention against information security breaches.

Keywords: Information Security, Awareness, Information Security efficiacy, CEIT, Student Teachers

İÇİNDEKİLER

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

BÖLÜM I

GİRİŞ

1980'li yıllardan itibaren küreselleşme olgusu etkisini yoğun bir şekilde göstermeye başlamış, 20. Yüzyılın son çeyreğinden itibaren sosyal, ekonomik ve toplumsal yaşamda çok önemli değişiklikler yaşanmıştır. Bu değişikliklerden en önemlisi sanayi toplumundan bilgi toplumuna geçiş süreci olmuştur. İnsanlık, sırasıyla tarım toplumundan sanayi toplumuna daha sonra da sanayi toplumundan bilginin ve nitelikli insanın önem kazandığı bilgi toplumuna geçiş sürecini yaşamıştır (Şahin, Çetin ve Yıldırım, 2009).

Bilgi toplumuna geçiş süreci, bilişim teknolojilerinde yaşanan gelişmelerle beraber hızlı bir şekilde devam etmiştir. Bilişim teknolojilerinde yaşanan gelişmeler sosyo-ekonomik hayat, devlet faaliyetleri, bankalar, eğitim, sağlık, ticaret, kamu kurum ve kuruluşları, işletmeler gibi toplumun her alanında değişimler meydana getirmektedir. Değişimler içerisindeki bilgi toplumunun bir parçası olan bilişim teknolojileri, insana ve topluma pek çok yararlar sağlamaktadır. Bu açıdan bakıldığında bilişim teknolojilerinin etkili ve yararlı şekilde kullanılması önemli görülmektedir (Çalık ve Çınar, 2009).

Günümüzde bilişim teknolojileri pek çok alanda kullanılmaktadır. Bilişim teknolojileri; evlerde, eğitimde, askeri alanda, imalatta, devlet hizmetlerinde, sağlık hizmetlerinde, ticarette, ofis otomasyonunda, veri tabanı yönetimde, mühendislik uygulamalarında, istatistikte, ticari uygulamalarda ve daha birçok yerde kullanılmakta ve her geçen gün kullanım alanı artmaktadır (Çelik, 2007). İnternet ve bilişim teknolojilerinin kullanım alanının artmasıyla beraber bireyler ve kurumlar çift yönlü ve kolay iletişim gerçekleştirme, gerekli bilgileri edinme, bilgi aktarma, tanıtım yapma, gelişmeleri takip etme vb. daha birçok imkâna kavuşmuştur. Bu fırsatlar, internet ve bilişim teknolojilerinin gelişimi ile web siteleri, bloglar,

forumlar, elektronik posta, haber grupları, sohbet odaları, video/ses konferansları, arama motorları ve bunun gibi daha birçok sistemi kapsamaktadır (Taş ve Kestellioğlu, 2011).

Bilişim teknolojilerinin sunduğu fırsatların artması kullanıldığı alanlarda önemli rol üstelenmelerini ve vazgeçilmez unsur olmalarını sağlamıştır. Örneğin işletmelerde gerçekleştirilen faaliyetlerde her geçen yıl bilişim teknolojilerinden yararlanma durumunda artış görülmektedir. Kimi zaman bilişim teknolojileri eksikliği veya bilişim teknolojilinin kullanımında yaşanan sorunlar nedeniyle işlerin yürümesinde sorunlar yaşanmaktadır. İşletmeler; müşteri isteklerine hızlı cevap verme, hizmet kalitesini artırma, işlemlerde kolaylık ve hız sağlama, satışları artırma, işlem ve nakliye masraflarını azaltma, küresel pazarlara açılma, rekabet gücünü artırma, yenilikleri takip etme ve daha birçok amacı gerçekleştirmek için bilişim teknolojilerini kullanmaktadırlar (Tekin, Zerenler ve Bilge, 2005). Bu amaçların gerçekleşmesi durumunda bilişim teknolojilerinin işletmelere; bilgi sağlama, iletişim, maliyeti azaltma, rekabet avantajı, pazarlara erişim gibi önemli faydaları olmaktadır. Dolasıyla bilişim teknolojilerinin zaman ve mekândan bağımsız olarak sağladığı hızlı, esnek ve düşük maliyet işletme içinde ve küresel boyutta devamlılık ve başarı için çok önemli görülmektedir (Güney ve Mutlu, 2008).

Bilişim teknolojilerinin her geçen gün daha fazla kullanılmaya başlanması, kullanım alanlarındaki uygulama sayısının artması, yaşamı elektronik ortama taşımış ve e'li yaşama geçilmiştir. Elektronik ortama geçiş ile sağlık, eğitim, ekonomi gibi sosyal kurumlar yeni yapılara dönüşmekte, ulusal ve yerel örgütlenmelerde köklü değişimler yaşanmaktadır. E-devlet, e-ticaret, e-ekonomi, e-belediye, e-öğrenme, e-sağlık ve daha birçok e'li yaşam alanlarının günümüzde kullanımı hızlıca artmaktadır (Dedeoğlu, 2006).

Kişisel bilgisayar kullanımının artması ve internet alt yapısının gelişmesiyle tüketiciler ve firmalar büyük bir pazarda buluşma imkânına kavuşmuştur. Ürün ve hizmetlerin sunulması, satılması, reklamının yapılması ve satın alınması işlemlerinin elektronik ortamdan gerçekleştirilmesi e-ticaret olarak adlandırılmaktadır (Erses, 2011). E-ticaretin kullanıcılara sunduğu faydalar; geniş ürün yelpazesi, maliyet düşüklüğü, müşteri ihtiyaçlarını tespit etme, ihtiyaçlara göre ürün oluşturma, taleplere hızlı cevap verme, herkese eşit erişim imkânı sunma, standart formatta üretici ve alıcı bilgileri içerme olarak görülmektedir (Aydın ve Sarısakal, 2003). E-

ticaret sayesinde firmalar düşük maliyetle, giriş engelleriyle karşılaşmaksızın bütün dünyaya açılma imkânı bulurken, kullanıcılar ise aracılara ihtiyaç duymadan hızlı bir şekilde mal ve ürünlere ulaşma olanağı bulmaktadırlar. Bu açıdan bünyesinde barındığı avantajlardan dolayı e-ticaretin hacmi giderek artmakta, sosyal ve ticari hayatta vazgeçilmez bir unsur olmaktadır (Özel, 2013). E-ticaretin yaygınlaşması kamu kurum/kuruluşlarda gerçekleştirilen işlerin hızlı bir şekilde elektronik ortamdan yapılmasına ve e-devletin doğmasına öncülük etmiştir. E-devlet zamansal kazanç sağladığından; maliyet ve kâğıt bağımlığını düşürdüğünden, verimliliği, memnuniyeti, vatandaşa sorgulama ve yanıt alma hizmeti sağladığından, hayat kalitesini artırdığından; karar almada kolaylık ve hız sağladığından kullanımı giderek artmaktadır. E-devlet uygulamaları sayesinde kamu kurum/kuruluşlarının, vatandaşların ve ticari kurumların birbirlerine karşı yükümlü olduğu hizmetler ve görevler elektronik ortamdan yürütülmektedir (Türkiye Bilişim Şurası (TBŞ), 2002). Kamu kurum/kuruluşlarında yapılması gereken işlemler artık e-devlet hizmeti ile hızlı ve rahat bir şekilde yapılmakta ve devlet kurumlarında olan yoğunluk giderek azaltmaktadır. E-devlet faaliyetlerinin artması, halk-belediye arasında iletişim ve bilgi alışverişi sağlayan e-belediyenin oluşmasını kaçınılmaz hale getirmiştir. Belediyenin sunduğu hizmetler, belediye projeleri, ihale ilanları, personel ilanları, istek iletebilme, borç sorgulama, ödemeleri görüntüleme ve daha birçok hizmet belediye web siteleri ile halka sunulmaktadır (Acılar, 2012). E-belediye hizmetiyle halk elektronik ortamdan belediye faaliyetlerini ve gelişmeleri takip edebilmektedir.

Ticari, devlet ve belediye faaliyetlerinin elektronik ortama kaymasıyla sağlık alanında da önemli değişiklikler yaşanmış ve e'li yaşam sağlık alanında da etkisini göstermeye başlamıştır. Hastalık tanısı konulması, hastaya ilişkin kayıtlar tutulması, hastalıkların tedavi edilmesi vb. daha birçok amacın gerçekleştirilmesi e-sağlık hizmetlerinden birkaçıdır (Dedeoğlu, 2006).

Bilişim teknolojilerindeki hızlı gelişmeler yukarıda bahsedilen alanlara etki ettiği gibi eğitim-öğretim faaliyetlerini de etkilemiştir. Internetin ve bilişim teknolojilerinin eğitim-öğretim faaliyetleri içeresinde kullanılmasıyla bilgisayar destekli eğitim, web tabanlı öğretim, internet destekli öğrenme, uzaktan eğitim gibi farklı öğrenme ortamları oluşmuştur. Akçakaya ve Tanrısever (2007) bilişim teknolojilerinin ve internetin sunduğu hizmetler ile eğitim faaliyetlerinin daha verimli gerçekleştiğini, daha fazla bilgi öğrenildiğini, zaman ve mekân sınırlaması olmadığını ve daha

başarılı sonuçlar alındığını belirtmişlerdir. Bilgisayarların eğitim-öğretimde kullanılması bilgisayar destekli öğretim sürecinin başlangıcı olarak kabul edilmektedir. Bilgisayar destekli eğitim ile öğrenme etkililiği artmakta, eğitim kalitesi yükselmekte ve ihtiyaçlar giderilmektedir. Bilgisayar destekli eğitimle farklı duyulara hitap edecek çoklu ortamlar sağlanarak öğretimin etkililiği ve başarısı artmaktadır. Bilgisayar destekli eğitim, mevcut geleneksel eğitim yöntemine göre daha etkili olmaktadır (Kaçar ve Doğan, 2007). Teknolojinin ilerlemesi, radyo, televizyon, bilgisayar, internet ve bilişim teknolojilerindeki hızlı gelişmeler eğitim-öğretim faaliyetlerini etkileyerek bireylerin zaman ve mekân sınırlaması olmaksızın yani uzaktan eğitim almalarına imkân tanımıştır. Uzaktan eğitim; her kademede eğitim verilmesini, eğitim maliyetlerini düşmesini, coğrafi olarak uzak bölgelerdeki geniş kitlere ulaşılmasını, öğrencilerin bireysel hızlarına göre öğrenmelerini sağlayan zaman ve mekândan bağımsız olarak öğrenci ve öğretmen arasında çift yönlü iletişimdir (Frank, Reich ve Humpreys, 2003; Akt. İşman, 2011). Uzaktan eğitim uygulamaları sayesinde birbirinden uzak olan öğretmen ve öğrenciler farklı ortamlardan görüntülü ve sesli iletişim kurabilmekte, bağımsız bireysel çalışma ortamlarına girebilmekte, sanal okul ve sanal sınıf ortamlarında eğitim alabilmektedirler (İşman, 2011). Uzaktan eğitimin eğitim-öğretim ve kamu kurum/kuruluşları tarafından yaygın bir şekilde kullanılmasıyla; fırsat eşitsizliği en aza indirilmekte, maliyet düşürülmekte, zengin bir eğitim ortamı sağlanmakta, bireysel ve bağımsız öğrenmeler gerçekleştirilmekte, hayat boyu öğrenme verilebilmekte, mekân ve zaman problemini ortadan kaldırılmaktadır (Kaya, 1996; Akt. Kaya, 2002). Günümüzde birçok ilköğretim, ortaöğretim, yükseköğretim ve kamu kurum/kuruluşlarında uzaktan eğitim sistemi bulunmakta ve her geçen gün uzaktan eğitim ile eğitim alan öğrenci sayısı artmaktadır.

Görüldüğü gibi bilişim teknolojilerinin ve internetin toplum hayatında, sosyal yaşamda, ticarette, kamu kurum/kuruluşlarda, eğitimde, sağlıkta, bankacılıkta vb. birçok alanda kullanılmasıyla insanlara pek çok faydası olmaktadır. Fakat elektronik ortamda bilgi aktarımının, iş ve işlemlerin artması beraberinde büyük bir tehlikeyi meydana getirmiştir. Bu hızlı gelişmeler neticesinde bilişim teknolojilerini tehdit eden veya bu teknolojiler kullanılarak işlenen bilişim suçları ortaya çıkmıştır (Yavuz ve Ulaş, 2013). Bilgi hırsızlığı ile başlayan bilişim suçları, ücretli hizmetlerin yerine ücretsiz hizmetlerin kullanılmaya başlanması ve internetin de hayatımıza girmesiyle

daha da belirgin hale gelmiştir. Internetin ve kişisel bilgisayarların yaygınlaşması, birçok kişiye ve ticari kuruluşlara ait bilgilerin kolay bir şekilde elde edilmesine sebebiyet vermiştir. Böyle bir ortam, kişilerin ve kurumların bilgilerine erişenlerin ve daha kötüsü bu bilgilere ulaşarak şantaj amaçlı kullananların hızlıca artmasına ve bilişim suçlarının yaygınlaşmasına neden olmuştur (Şamlı, 2010).

Günümüzde en çok karşılaşılan bilişim suçları bireylere, şirketlere ve toplumun büyük bir kısmına karşı işlenen suçlar olarak Tablo 1'de görülmektedir (Pati, t.y).

Tablo 1. En Çok Rastlanan Bilişim Suçları

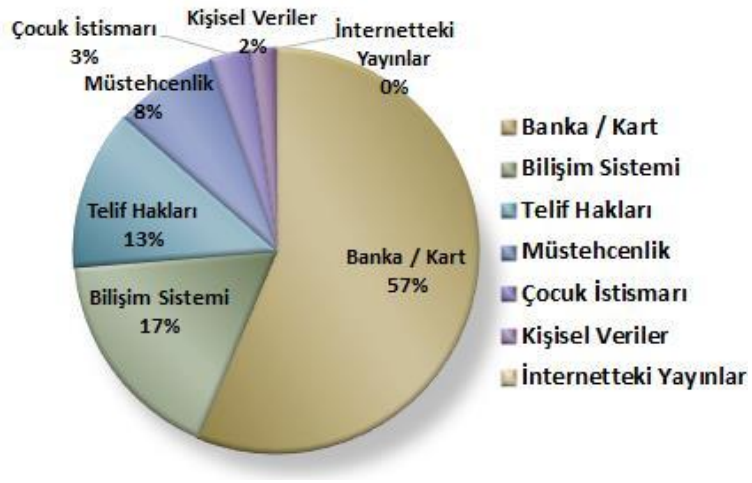
Bireylere ve Mülkiyet Haklarına Karşı İşlenen Suçlar	Organizasyonlara Karşı İşlenen Suçlar	Toplumun Büyük Bir Kısmına Karşı İşlenen Suçlar
e-posta ile taciz	Yetkisiz bilgi sahibi olma	Pornografi
Müstehcen malzemelerin dağıtılması	Hükümet kuruluşlarına karşı siber terörizm	Müstehcen görüntülerle gençlerin ahlaki yapısının bozulması
Siber takip	Korsan yazılım vb. dağıtımı	Mali suçlar
Bilgisayar sistemi üzerinden yetkisiz erişim	Bilgisayar sistemi üzerinden yetkisiz erişim	Kaçak eşya satışı
Ahlaksız teşhir		Çevrimiçi kumar
e-posta ile kandırma		Sahtecilik
Hile ve dolandırıcılık		Yasadışı ticaret
İftira		

ABD'de 2009 yılında Bilgisayar ve Güvenliği Enstitüsünün (Computer Security Enstitute) gerçekleştirdiği bilgisayar suçları ve güvenlik araştırmasında devlet şirketlerinde, mali tıbbi kurumlarda ve ayrıca üniversitelerde bilgisayar güvenliği uygulayıcılarının saldırı deneyimleri araştırılmıştır. Araştırma sonuçlarına göre; kötücül yazılım bulaşması, organizasyon içinde botlar/zombiler, Phishing (oltalama), dolandırıcılık, Denial of service (DoS) atakları, web sitesi tahrifatı, laptop veya mobil cihazların çalınması veya kaybolması, şifre koklama (Password sniffing) en çok gerçekleşen saldırılar olarak tespit edilmiştir (Richardson, 2009). Dünya genelinde araştırma yapan Symantec'in (2013), yayınladığı bilgi güvenliği tehdidi raporunda en fazla zararlı yazılım saldırılarına maruz kalan ülkeler sırasıyla ABD, Çin, Hindistan, Brezilya Almanya, Hollanda, İtalya ve İngiltere'dir. Spam saldırılarına en fazla Hindistan; Phishing (Oltalama), Bot ve web saldırılarına en

fazla ABD; ağ saldırılarına ise en fazla Çin maruz kalmıştır. ABD ve Çin'in saldırılara en fazla maruz kalmasında nüfusunun büyük çoğunluğunun interneti yaygın bir şekilde kullanması gösterilmektedir. Yine bu araştırmada, en fazla zararlı yazılım saldırısına maruz kalan web siteleri sırasıyla iş, teknoloji, blog, alışveriş, otomotiv, sağlık ve eğitim içerikli siteler olmuştur. En fazla zararlı yazılım bulunduran web siteler olarak pornografi, otomotiv ve askeri web siteler olarak tespit edilmiştir. Ayrıca günümüzde kullanımı artan Android işletim sistemine sahip mobil telefonlara yönelik saldırıların da her geçen gün arttığına yönelik sonuçlara ulaşılmıştır. Günden güne atan Phishing (Oltalama) saldırıları ise, en çok finans organizasyonlarını ve bilgi servislerini hedef almaktadır. E-mail yoluyla Phishing saldırıları sırasıyla en çok devlet ve kamu kurumlarında, finans kuruluşlarında ve eğitim sektöründe tespit edilmiştir. Güvenlik açığı en fazla olan tarayıcılara bakıldığında sırasıyla; Apple safari, Google Chrome, Microsoft Internet Explorer, Mozilla Firefox ve Opera olmuştur. Symantec'in her yıl gerçekleştirdiği araştırma sonuçları, her geçen gün tehdit sayısının ve çeşidinin arttığını göstermektedir. Marinos'un (2013) gerçekleştirdiği araştırma sonuçları da bu bulguları doğrular niteliktedir. Marinos (2013) araştırmasında kritik altyapılar, mobil bilişim, sosyal ağlar, bulut bilişim gibi alanlara yönelik saldırıların arttığını tespit etmiştir. Bu saldırılar en fazla; internetten kasıtlı veya kasıtsız indirilen programlar, zararlı yazılımlar, kod enjekte etme, Denial of service (DoS), Phishing (Oltalama), spam, veri ihlali, kimlik hırsızlığı, fiziksel zarar, bilgi sızdırma şeklinde gerçekleştirilmektedir. Bunlara ek olarak mobil teknolojilere yönelik tehditlerin de arttığı görülmektedir. Dekker, Karsberg ve Lakka (2013) 18 ülkede gerçekleştirdiği raporunda; gerçekleştirilen saldırıların % 50'sinin mobil telefon ve mobil internet üzerine olduğunu, % 37'sinin acil numaraların servis vermesini engelleme üzerine gerçekleştiğini belirtmiştir.

Ülkemizde yapılan araştırmalar ve çalışmalar incelendiğinde, Kaçakçılık ve Organize Suçlarla Mücadele (KOM) Daire Başkanlığı tarafından hazırlanan ve 2011 yılında yayınlanan rapora göre bilişim suçlarına yönelik toplam 3901 olay gerçekleşmiş ve 4157 şüpheli şahıs hakkında işlem yapılmıştır. Olay sayısına göre en fazla; banka ve kredi kartı dolandırıcılığı, bilişim sistemleri (sisteme girme, engelleme, bozma, verileri yok etme), internet bankacılığı, internet aracılığıyla nitelikli dolandırıcılık ve bunların dışında kalan müstehcenlik, kumar, gizlilik ihlali suçları işlenmiştir. Bilişim

suçlarının işlendiği suç unsurları ise; genelde CD ve DVD, kredi/banka kartı, bilgisayar, laptop, harddisk, flash disk, hafıza kartı, cep telefonu ve IMEI no değiştirilmiş cep telefonları olarak tespit edilmiştir. Ülkemizde 1990-2011 yılları arasında en çok işlenen ve davalık olan bilişim suçları Şekil 1'de görülmektedir (İlbaş ve Göksal, 2011: 165).



Şekil 1. En Çok İşlenen ve Davalık Olan Bilişim Suçları

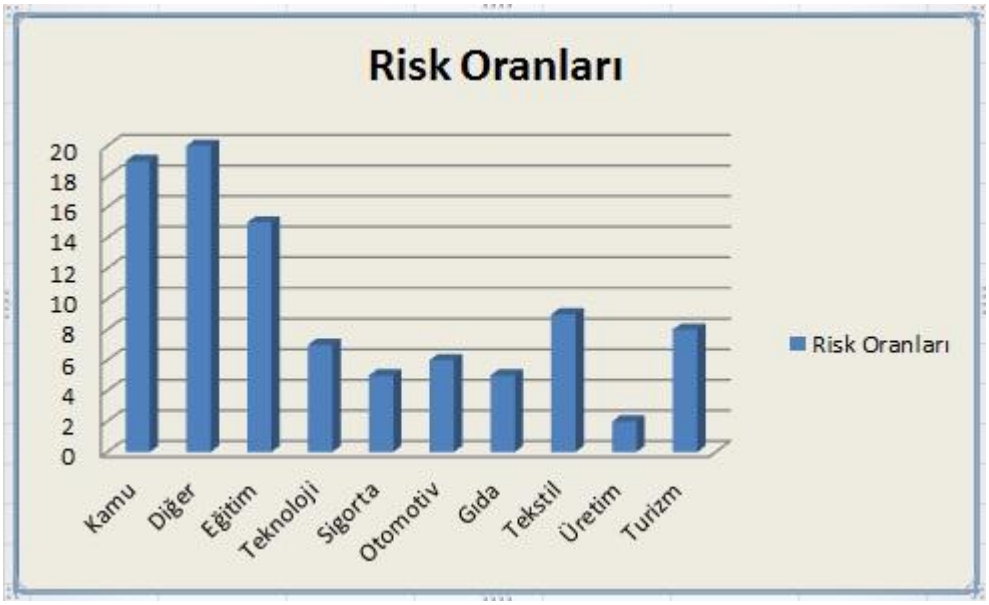
Yukarıda görülen bilişim suçları kötü niyetli kişiler, kurumlar ve hatta bazen devlet tarafından gerçekleştirilebilmektedir. Siber ortamda bireylerin, toplumların ve devletlerin güvenliği tehdit eden ve bilişim suçlarına neden olan çeşitli yöntemler ve araçlar bulunmaktadır. Virüsler, solucanlar, Truva atları gibi zararlı yazılımlar, köle bilgisayarlar, DoS saldırıları, Phishing (oltalama), klavye dinleme yazılımları, casus yazılımlar, ağ trafiğinin izlenmesi (sniffing), istem dışı elektronik postalar (spam), istem dışı gönderilen ticari tanıtım yazılımları (adware) ve bunlar gibi daha birçok yöntem ve araç kullanılmaktadır (Ünver, Canbay ve Mirzaoğlu, 2009).

Yine ülkemizde internet servis sağlayıcılarından olan Koc.net'in 2005 yılında 1025 internet kullanıcısı ve 850 şirket üzerinde yaptığı araştırmaya göre;

- Şirketlerin %43'ünün web sunucu bilgilerinin çalınabileceği veya farklı adreslere yönlendirilebileceği,
- ADSL abonelerinin %65'nin firewall (güvenlik duvarı) kullanmadıkları,

- Şirketlerin ADSL Anti-virüs kullanım oranı %85 iken anti-spyware kullanım oranı %30 olduğu,
- DNS sunucularındaki %24 olan açıklık nedeniyle şirket e-postalarının başkalarının eline geçebileceği veya bankacılık işlemlerinde şifrelerin çalınma riski görülebileceği,
- Her iki web sunucusundan birinin tehlike altında olduğu,
- Tüm açıkların %47'sinin orta ve yüksek seviyede olduğu tespit edilmiştir.

Araştırma sonunda ulaşılan bulgulara göre araştırmaya katılan kullanıcıların yarısına yakınının tehlike altında olduğu belirlenmiştir. Ayrıca bu sonuçlar kullanıcıların ve şirketlerin yeterli güvenlik önlemleri almadıklarını, bilgi güvenliğine yeterli önemi vermediklerini ve teknik konularda eksikliklerin olduğunu göstermektedir. Aynı araştırmanın sektörlere göre risk dağılımı ise Şekil 2'de verilmiştir.



Şekil 2. Sektörlere Göre Risk Oranlar

Şekil 2'den de anlaşılacağı üzere en fazla risk oranına sahip sektörlerden birini eğitim sektörü oluşturmaktadır (Koç.net, 2005). Eğitimdeki risk oranı dikkate alındığında idarecilerin ve öğretmenlerin yeterli güvenlik önlemleri almadıklarını/alamadıklarını, bilişim güvenliği konusunda yetersiz olduklarını düşündürmektedir. Ayrıca eğitimde risk oranın yüksek olması, okullarda bilişim güvenliği eğitiminin verilmediği veya öğrencilerin bilişim güvenliği bilgileri ile

davranışları arasındaki ilişkinin tutarlı olmadığı düşüncelerini doğurmaktadır. Bilişim teknolojilerini ve interneti sosyal yaşamda ve eğitimde yoğun kullanan bireylerin çeşitli tehlikelerle karşı karşıya kalmaları bu düşünceleri doğrular niteliktedir. Özelikle günümüzde kullanımı her geçen gün artan sosyal ağlar kullanıcılara yeni fırsatlar, iletişim, sosyalleşme, gelişmeleri takip etme gibi imkânlar sunarken pek çok tehdit ve tehlikeyi de beraberinde getirmiştir. Sosyal ağlarda mahremiyet ilkesine uyulmaması, kişisel bilgilerin paylaşılması ve kullanıcıların bilgisizliği bireylerin açık hedef haline getirilmesine ve çeşitli bilişim suçlarının sosyal ağlardan elde edilen bilgiler vasıtasıyla gerçekleşmesine sebep olmaktadır (Yavanoğlu ve Sağıroğlu, 2010). Ayrıca sosyal paylaşım siteleri, e-posta, metin mesajları ve sohbet odalarının teknolojik araçlarla (cep telefonu, tablet, bilgisayar) öğrenciler tarafından yaygın bir şekilde kullanılması internet üzerinden hakaret, tehdit ve küçük düşürücü sözler gibi zorbalık hareketlerinin sanal ortama taşınmasına sebebiyet vermiştir. Sanal zorbalığa maruz kalan kişiler korktuklarından ve durumu gerekli mercilere bildirmediklerinden bu suç türü giderek yaygınlaşmaktadır (Bayram ve Saylı, 2013).

Internet kullanımı ve web 2.0 teknolojilerinin gelişimiyle üçüncü kişilere ait web sitesi içeriklerinin bir başkası tarafından kendi web sitesinde kullanılması da fikri mülkiyet suçlarını oluşturmaktadır (Bozbel, 2011). İçerik toplayıcılık denen bu suç, kaynak gösterilmediğinden aynı zamanda intihal suçuna da girmektedir. Internette bulunan hazır ödev siteleri, ödev yaptırma siteleri, forum siteleri ve bloglar intihallerin yapılmasına sebebiyet veren siteler olarak ön plana çıkmaktadır. İntihal günümüzde internetin yaygın kullanımı ile giderek artan bir suç olmuştur. Yapılan bir araştırmaya göre öğrencilerin dönemlik bir ödevde %94 kopyala-yapıştır yaptıklarını, %50 sinin hiç referans göstermediklerini, %35'nin uygun referans göstermediklerini, %27'sinin kaynağın aynısını aldıklarını, %34'nün kısmen değişiklik yaptıklarını göstermektedir (Ural ve Sulak, 2012).

Sosyal ağlar, sanal zorbalık, içerik toplayıcılık ve intihal suçlarının yanı sıra öğrenciler bilgisayar ve internet kullanımı sırasında zararlı yazılımlara (virüs, casus yazılım, Truva atları) maruz kalmakta, bazı belgeleri kaybedilmekte ve yazılım ayarlarını bozabilmektedirler. Kötü niyetli kişiler ile temas kurma, pornografik içerikler ve suç örgütleri öğrencilerin maruz kaldığı diğer durumlardır (Canbek ve

Sağıroğlu, 2007b). Son zamanlarda internet üzerinden çocukların ahlaki yapılarını bozacak içeriklerin teşhir edilmesinde artış görülmektedir. Dünyanın önde gelen güvenlik sağlayıcılarından Bitdefender (2013) dünya üzerinde 19 bin ebeveyn üzerinde yaptığı araştırmasında; çocukların internet üzerinden porno içeriklerine ulaşma yaşının 6'ya kadar düştüğünü, flört etme yaşının 8'e kadar düştüğünü, çevrimiçi oyun ve anlık mesajlaşma uygulamalarının kullanımının gittikçe azaldığını, 12 yaşındaki çocukların sosyal ağ hesaplarının olduğunu, sosyal ağ hesaplarında yalan beyanların bulunduğunu tespit etmiştir.

Öğrencilerin bilişim güvenliği bilgisi, farkındalığı, davranışları ve tehlikelere maruz kalma durumlarıyla ilgili yapılan araştırmalar, öğretmenlerin ve öğrencilerin bilgi güvenliği konularına yönelik gerekli önlemleri almadıklarını ve bu konularda yeterli bilgi düzeyine sahip olmadıklarını göstermektedir (Tekerek ve Mart, 2010). Tekerek ve Tekerek (2013) gerçekleştirdikleri araştırmalarında; öğrencilerin etik konularda yeterli bilinç düzeyine sahip oldukları fakat kurallar ve bilgi gerektiren konularda farkındalık düzeylerinin düşük olduğu sonucuna ulaşmışlardır.

Yapılan araştırmaların sonuçları, bilişim sistemlerine yönelik tehditlerin artması ve bilişim suçlarının farklı boyutlara ulaşması kurumları ve bireyleri çeşitli tedbirler almaya yönlendirmiştir. Kurumların ve bireylerin bilişim güvenliği farkındalığını artırma ve bilişim suçlarını önlemeye yönelik çeşitli çalışmaları ve girişimleri bulunmaktadır. Uluslararası Standartlar Organizasyonu (ISO), Bilişim Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemlerini kurmak, geliştirmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için ISO/IEC 27000 standart serisi altında standartlar geliştirerek kuruluşların bilgi güvenlik yönetim gereksinimlerini ve gerekliliklerini karşılamaktadır (Peker, 2008). Ülkemizde TÜBİTAK aracılığıyla Devlet Planlama Teşkilatı (DPT) tarafından desteklenen "Bilgimi Koruyorum Projesi" adı altında bilgi güvenliği bilinçlendirme çalışmaları yürütülmektedir (Bilgimi Koruyorum, 2011). Ayrıca yine TÜBİTAK tarafından gerçekleştirilen "Ulusal Bilgi Güvenliği Kapısı" uygulamasında bilgi güvenliği ile ilgili güncel uyarılar, bilgilendirici rehberler, etkinlikler, kılavuzlar, güvenlik bildirileri, güvenlik saldırıları, konferanslar programları ve teknik yazılar yayınlanmaktadır. Uygulamaya içerik yönünden bilgi güvenliğiyle ilgilenen her kurum ve birey katkı yapabilmektedir (Ulusal Bilgi Güvenliği Kapısı, 2014). 2011

yılında başlatılan güvenli internet hizmetiyle kullanıcılar, çocuk ve aile profili seçeneklerini kullanarak internette zararlı içeriklere, dolandırıcılık sitelerine ve zararlı yazılımlara karşı güvenliklerini sağlayabilmektedirler (Güvenli Internet, 2012). 2013 yılında Muğla Fethiye İlçe Milli Eğitim ve Emniyet Müdürlüğünün ortak çalışması sonucu gerçekleştirilen projeyle, okullarda öğrencilere ve velilere seminerler verilmiş ve pano çalışmaları yürütülmüştür (Güvenli ve Bilinçli Internet Kullanım Projesi, 2013). Ayrıca her yıl bilişim güvenliğine yönelik ulusal ve uluslararası konferanslar düzenlenmektedir. 2008 yılından itibaren her yıl Ulaştırma, Denizcilik ve Haberleşme Bakanlığı himayesinde bilgi güvenliğini sağlama yöntemleri, saldırı tespit yöntemleri, şifreleme, siber tehditlere yönelik çözüm önerileri vs. bilişim güvenliğine yönelik Uluslararası bilgi güvenliği ve kriptoloji konferansı düzenlenmektedir (Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 2014). Bunların yanında web ortamında gerçekleşen suçlarla mücadele emek amacıyla Telekomünikasyon İletişim Başkanlığı tarafından 2007 tarihinde Bilgi İhbar Merkezi kurulmuştur. 5651 Sayılı Internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanununu uyarınca internet kullanıcıları sakıncalı gördükleri içerikleri bu merkez sayesinde ihbar edebilmektedirler (Telekomünikasyon İletişim Başkanlığı Internet İhbar Merkezi, 2010).

Yapılan çalışmalar, faaliyetler ve girişimler bilişim teknolojileri ve internet güvenliğine önem verildiğini göstermektedir. Fakat günümüzde bilişim teknolojileri ve internet üzerinden gerçekleştirilen saldırılar artmaya devam etmektedir. Günümüzde özellikle öğrencilerin bu saldırılara karşı nasıl önlem alacaklarını bilmeleri ve internet ortamında güvenli bir şekilde gezmeleri önemli bir konu olmaktadır. Dolayısıyla bilişim tehditlerine karşı önlem almada ve bilişim güvenliğinin sağlanmasında okullarda görev yapan bilişim teknolojileri öğretmenlerine büyük görev ve sorumluluklar düşmektedir. Uluslararası Eğitimde Teknoloji Topluluğu (International Society for Technology in Education-ISTE) yayınladığı Ulusal Eğitim Teknolojisi Standartlarında (The National Educational Technology Standards-NETs) öğretmenlerin, etik konularda model olma; bilginin ve teknolojinin kullanımında sosyal etkileşimden sorumlu olma; dijital bilginin ve teknolojinin güvenli, yasal ve etik kullanımını destekleme ve öğretme becerilerine sahip olmaları gerektiği ifade edilmektedir (ISTE, 2008). Ayrıca ülkemizde Milli

Eğitim Bakanlığı (MEB) tarafından belirlenen bilişim teknolojileri özel alan yeterliliklerinde, bilişim teknolojileri öğretmenlerinin etik ve güvenlik konularında sahip olmaları gereken özelliklere yer verilmiştir. Bilişim teknolojileri öğretmenlerinin; bilişim teknolojileri, internet ve ağ teknolojilerinde yasal kuralları bilme, etik davranma, güvenli kullanabilme, güvenlik tehditlerine karşı güvenlik stratejileri geliştirme ve bilişim güvenliği konularını öğretebilme niteliklerine sahip olmaları gerektiği belirtilmiştir (MEB, 2008). Bu bağlamda ISTE ve MEB'in belirlediği standartlar, bilişim suçlarında yaşanan artış ve güvenlik tehditleri dikkate alındığında, okullarda görev yapan bilişim teknolojileri öğretmenlerinin bilişim güvenliği seviyelerinin ve bilişim güvenliğine yönelik öğrencilerini bilgilendirme yeterliliklerinin ne düzeyde olduğunun önemli olduğu görülmektedir.

1.1 PROBLEM CÜMLESİ

Bu araştırmanın problem cümlesini "BÖTE öğretmen adaylarının bilişim güvenliği bilgilerinin ne düzeyde olduğu ve bilişim güvenliğine yönelik eğitim verebilme konusunda hangi konularda yeterli oldukları?" sorusu oluşturmaktadır.

1.2 ALT PROBLEMLER

BÖTE öğretmen adaylarının;

1. Bilişim güvenliği bilgileri ne düzeydedir?

2. Bilişim güvenliğine yönelik eğitim verebilme yeterlilikleri ne düzeydedir?

3. Bilişim güvenliği bilgileri

    a) Yaş,

    b) Cinsiyet,

c) Bilişim güvenliğine yönelik bir kurs veya ders alıp almama,

d) Sınıf,

e) Günlük bilgisayar kullanım süresi,

f) Günlük internet kullanım süresi,

g) Öğrenim görülen üniversite,

h) Bilgisayara sahip olma yılına göre anlamlı bir farklılık göstermekte midir?

1.3 ÖNEM

Çağımızda bilişim ve internet teknolojilerinin kullanımı her geçen gün artmaya devam etmektedir. Bilişim teknolojileri ve internet, birey ve toplum hayatında önemli değişiklikler meydana getirmekte ve günlük yaşamda vazgeçilmez unsur olmaktadırlar. Bilişim teknolojileri ve internet kullanımının yaygınlaşmasıyla bu teknolojilere yönelik veya bu teknolojiler vasıtasıyla işlenen suçlar ve tehditler giderek artmaktadır. Bireylerin bilinçsiz bilişim teknolojileri ve internet kullanımlardan faydalanan kötü niyetli kişilerin sayıları da artmaktadır. Dolayısıyla küçük yaşlardan itibaren bireylere bilişim güvenliğine karşı önlem alabilme ve güvenliği sağlama eğitimlerinin verilmesi gerekmektedir. Bu durumda hiç şüphesiz okullarda görev yapacak bilişim teknolojileri öğretmen adaylarına büyük iş düşmektedir. Bu çalışma, BÖTE öğretmen adaylarının bilişim güvenliği bilgilerini ve bilişim güvenliğine yönelik eğitim verebilme yeterliliklerini belirlemeye yönelik olduğu ve alan yazınında bu konuya yönelik bir çalışma bulunmadığı için özgün bir çalışmadır. Bilişim güvenliği konusunun giderek öneminin artması bakımından günceldir. Aynı zamanda bu çalışma, bilişim güvenliğine yönelik artan tehditler ve BÖTE öğretmen adaylarının öğrencilerini bu konularda bilgilendirebilme yeterliliklerinin belirlenmesi açısından gerekli görülmektedir.

1.4 SINIRLILIKLAR

Bu araştırma, 2013-2014 eğitim-öğretim yılında Sakarya, Erzincan, Amasya ve Siirt Üniversitelerinin BÖTE bölümünde 3. ve 4. sınıflarda okuyan 375 öğrenci üzerinden elde edilen veriler ile sınırlıdır.

1.5 TANIMLAR

Bilişim: Bilginin aktarılması, organize edilmesi, saklanması, tekrar elde edilmesi, değerlendirilmesi ve dağıtımı için gerekli kuram ve yöntemlerle bu bilgiyi kaynağından alıp kullanıcıya aktaran temel bilgi sistemleri, işlevleri ve süreçleri olarak tanımlanmaktadır (Aydın, 1992).

Bilişim Güvenliği: 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 tanımlanmaktadır (Ulaşanoğlu, Yılmaz ve Tekin, 2010).

Bilişim Suçu: Elektronik bilgilere ve verilere bilgisayar veya elektronik araçlar ile yasadışı yollarla erişilmesi, bilgilerin veya verilerin bu araçlar vasıtasıyla değiştirilmesi, silinmesi olarak tanımlamaktadır (Bilek, 2012).

1.6 KISALTMALAR

TBŞ: Türkiye Bilişim Şurası

ISO: International Organization for Standardization (Ulusal Standartlar Organizsyonu)

DPT: Devlet Planlama Teşkilatı

TDK: Türk Dil Kurumu

DOS: Denial of Service (Hizmet Kesintisi)

DDOS: Distributed Denial of Service

TBD: Türk Bilişim Derneği

SSUK: Siber Suç Uzmanları Komitesi

TCK: Türk Ceza Kanunu

NCSA: National Cyber Security Alliance (Ulusal Siber Güvenlik Birliği)

BTK: Bilgi Teknolojileri ve İletişim Kurumu

RAT: Remote Administration Tools (Uzaktan Yönetim Araçları)

MEB: Milli Eğitim Bakanlığı

TUİK : Türkiye İstatistik Kurumu

ISTE: International Society for Technology in Education (Uluslararası Eğitimde Teknoloji Topluluğu)

NETs: The National Educational Technology Standards (Ulusal Eğitim Teknolojisi Standartları)

SSL: Secure Sockets Layer (Güvenli Yuva Katmanı)

BÖLÜM II

ARAŞTIRMANIN KURAMSAL ÇERÇEVESİ VE İLGİLİ ARAŞTIRMALAR

Bu bölümde bilişim kavramı, bilişim teknolojileri, bilgi güvenliği, bilgi güvenliği ilkeleri, bilişim güvenliği, bilişim güvenliğini sağlamak için alınacak önlemler, bilişim güvenliği tehdit eden kullanıcı tabanlı ve yazılım tabanlı unsurlar, bilişim suçları, bilişim suçlarının sınıflandırılması, Türk hukuk sisteminde bilişim suçlarına yönelik bilgilere yer verilmiştir. Bunların yanında bilgi güvenliği, bilişim suçları, bilgi güvenliği farkındalığı, bilgi güvenliği davranışı, bilgisayar ve internet güvenliği ile ilgili yapılan araştırmalara yer verilmiştir.

2.1 ARAŞTIRMANIN KURAMSAL ÇERÇEVESİ

2.1.1 Bilişim Nedir?

Bilgisayar ve iletişim teknolojilerindeki gelişmeler sonucunda bilgi kavramının niteliği de değişmiştir. Teknolojilerin yaygın olarak kullanılmadığı dönemde durağan olan bilgi günümüzde kullanılan teknolojiler ile hareketli bir biçime dönüşmüştür. Bilişim kelimesi ilk kez Prof. Dr. Aydın Köksal tarafından kullanılmıştır. Bilimsel anlamda bilişim; bilgisayar, teknoloji ve iletişim ile yakın görülmektedir (İlbaş, 2009). Bilişim sözcüğü Fransızca informatiqe ile aynı kökten gelmektedir. Bu sözcük Türkçe' ye çevrilerek enformasyon olarak kullanılmıştır. Daha sonra yabancı kaynaklı sözcük değiştirilerek bilgi kökeninden gelen bilişim kelimesi uygun görülmüştür (Dülger, 2004).

Bilişim, bilgi ve bilginin otomatik olarak elektronik makineler vasıtasıyla düzenli ve mantıksal olarak işlenmesiyle ilgilenen bir yapısal bilim dalıdır (Pallı 2008). Bilişim kavramı Türk Dil Kurumu'nun (TDK) Genel Türkçe Sözlüğünde şöyle belirtilmiştir: "İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişimde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimidir." Erses'e göre (2011) bilişim, son yüzyılda meydana gelen bilgi ve iletişim teknolojileri ön plana çıkarılarak bilgisayar ve iletişim teknolojilerinin kullanılmasıyla bilginin işlenmesi, depolanması ve dağıtılmasıdır.

Aydın (1992) daha kapsamlı bir tanım yaparak bilişimi, bilginin aktarılması, organize edilmesi, saklanması, tekrar elde edilmesi, değerlendirilmesi ve dağıtımı için gerekli kuram ve yöntemlerle bu bilgiyi kaynağından alıp kullanıcıya aktaran temel bilgi sistemleri, işlevleri ve süreçleri olarak tanımlamıştır. Boğa ise (2011) bilişim kavramını, bilginin teknoloji vasıtasıyla işlenmesi, saklanması ve aktarılması olarak tanımlamıştır.

Bilişim, insanların teknik, sosyal ve ekonomik alanlarda kullandığı bilginin, bilgisayar aracılığıyla düzenli bir şekilde işlenmesi, bilginin bilgisayar ortamında depolanması ve kullanıcıların erişimine açık olması bilimidir (Dülger, 2004). Yukarıdaki tanımlar dikkate alındığında bilişim; bilgisayar ve iletişim teknolojilerini kapsayan, bilginin elektronik makineler aracılığıyla düzenli ve mantıksal biçimde işlenmesi anlamına gelmektedir (Pallı, 2008).

2.1.2 Bilişim Teknolojileri

İnsan yaşamının ve toplumsal yaşamın değişimi 19. yüzyılda gerçekleşen endüstri devrimi ile hızlanmıştır. Yirminci yüzyılın ikinci yarısından itibaren kullanılmaya başlanan bilgisayarlar ve ardından gelen iletişim teknolojileri bu değişim sürecini etkilemiştir. Özellikle son dönemde bilgi ve iletişim teknolojilerindeki gelişmeler artan bir ivmeyle devam etmekte ve her geçen gün yeni teknolojilerle karşılaşılmaktadır (Dedeoğlu, 2006). Bu teknolojiler ilk çıktıklarından itibaren birey ve sosyal yaşam üzerinde önemli etkiler meydana getirmektedirler. Bilgi ve iletişim teknolojilerindeki gelişmeler, internet ve internet teknolojilerinde çığır açan

platformlar bireylerin bu teknolojiler ile daha fazla vakit geçirmelerine ve bu teknolojilerin toplum hayatında önemli unsur olmalarına ortam sağlamıştır.

Internet ve internet teknolojisinin yaygınlaşması toplum üzerinde önemli etkilere neden olmuştur. Bilgisayarlar ve internet sayesinde toplumlar demokratikleşmekte, e-ticaret yaygınlaşmakta, bilgi farklı ortamlara yayılmakta, sosyal hareketlik artmakta ve bilgi kaynaklarına ulaşma kolaylaşmaktadır (Demir, 2006). Bilgisayar, bilgi, iletişim ve internet teknolojilerinin yaygın kullanımı sonucunda bireysel hayatta, toplum hayatında, sosyal ilişkilerde, eğitimde, ekonomide, ticarette, sağlıkta ve kamuda çok önemli değişiklikler meydana getirmeye devam etmektedir. Bilgisayar ve internet evde, işte, okulda ve daha birçok yerde sürekli kullanılmakta ve ihtiyaçların büyük bir çoğunluğu bu sayede karşılanmaktadır. Bilgisayar teknolojisinin gelişmesi ile beraber internetin de gelişmesi bireylerin yaşantısında bu iki teknolojiyi odak nokta haline getirmiştir. Internet, bilgisayar sistemleriyle bağlanan ve dünya üzerinde sürekli gelişip büyüme gösteren çok yaygın bir iletişim ağı olması itibariyle bireyler ve toplumlar üzerinde gözlenebilir değişimlere neden olmaktadır (Çalık ve Çınar, 2009).

Yapılan araştırmaların her geçen gün dünyada ve ülkemizde bilgisayar ve internet kullanımının artmaya devam ettiğini göstermektedir. Türkiye nüfusunun yüzde 45,7'si yani 36 milyonu internet kullanmaktadır. Ayrıca ülkemiz internet kullanımında 30 Haziran 2012 itibari ile Avrupa ülkeleri arasında beşinci sıradadır. 2012 itibari ile dünya nüfusunun yüzde 34,3'ü internete erişebilmektedir (Internet World Stats, 2012). Türkiye İstatistik Kurumu'nun (TUİK) yaptığı araştırmaya göre ise, 2013 yılında girişimlerde bilgisayar kullanımı % 92 iken hanelerde bilgisayar kullanımı % 49,9 olarak tespit edilmiştir. Internet erişimi ise girişimlerde % 90,8 iken hanelerde %48,9 olarak tespit edilmiştir. Bu istatistikler göz önüne alındığında ülkemizde bilgisayar ve internet kullanım oranının iyi seviyede olduğu görülmektedir.

Günümüzde bilgisayar, bilgi, iletişim, internet ve teknolojilerinin yoğun kullanımı sonucunda bilginin işlenmesini, depolanmasını ve dağıtılmasını temel alan bilişim teknolojileri kavramının sıklıkla kullanıldığını görmekteyiz. Bilişim teknolojisi, iletişim ve bilgisayar sistemleriyle bağlanabilen; bilginin toplanmasında, işlenmesinde, depolanmasında, ağ sistemleri vasıtasıyla bir yerden bir yere

gönderilip kullanıcıların hizmetine sunulmasında kullanılan iletişim ve bilgisayarlar dâhil bütün teknolojileri kapsayan teknolojilerdir (MEB, 2013). Çelik (2007) bilişim teknolojilerini, bilginin bilimsel yöntemlerle bilgisayar ve istatistiksel yaklaşımlar kullanılarak derlenmesi, sınıflandırılması, depolanması, işlenmesi olarak tanımlamıştır. Ünüvar ise (2006) bilişim teknolojilerini, eldeki verileri istenen formatta bilgilere dönüştürmek ve bu bilgileri istenen kişilere iletmek için bilgisayar donanım ve yazılımlarını, telekomünikasyon cihazlarını ve ağlarını kapsayan teknolojiler olarak tanımlamıştır. Bilgisayarlar, yazıcılar, optik okuyucular, veri tabanı programları, yazılımlar, telefonlar, internet sistemleri vb. bilişim teknolojileri araçlarıdır (Ünüvar, 2006).

Bilişim teknolojileri, sahip olduğu özellikler sayesinde günlük yaşamın bütünleşik bir parçası olmuştur. İnsan hayatında, ticarette, tarımda, sağlıkta, eğitimde işlemlerin hızlanmasına ve aynı zamanda kolaylaşmasına neden olmuştur. Ticarette; kurum ve müşteriler arasındaki bilgi yönetimini sağlamakta, kullanıcıların internette hangi linklere tıkladığı, hangi sayfada ne kadar kaldığı gibi bilgiler sisteme kaydedilerek kullanıcıların ilgi alanlarına göre seçenekler sunulmaktadır. Tarımda; üretim otomasyonu yapılmakta ve topraktan daha fazla verim almak için gelişmiş teknolojiler kullanılmaktadır. Sağlıkta; sağlık hizmetlerinin kalitesi izlenmekte, değerlendirmekte, iyileştirmeye katkı sağlamakta ve sağlık bakım maliyetinin düşürülmesinde etkin rol oynamaktadır. Eğitimde; bilgiye ulaşılmasında, bilginin üretiminde, bilginin yayılmasında, kalıcı öğrenmelerin gerçekleştirilmesinde, bireysel hıza göre eğitim verilmesinde, dönüt vermede, iletişim sağlamada, konuları tekrar etmede vazgeçilmez bir unsur olmaktadır (Çelik, 2007). Bilişim teknolojilerindeki gelişmeler devam etmekte, her gün yeni teknolojiler çıkmakta ve kullanım alanları artmaktadır. Bilişim teknolojileri denince akla bilgisayarlar, yazılımlar, cep telefonları, tabletler, banka kartları, internet, elektronik uygulamalar, akıllı telefonlar ve daha birçok cihaz ve sistem gelmektedir (Yaycı, 2007).

2.1.3 Bilgi Güvenliği

Sayısal birimler halindeki verilerin dönüştürme süreçlerinden geçirilip kullanıcılar için anlamlı hale getirmesine bilgi denir (Akolaş, 2004). Kağıt, tahta, bilgisayarlar, mobil iletişim cihazları, e-posta, USB, CD, DVD, hard disk, internet siteleri, video

ve görsel ortamlar bilginin başlıca bulunduğu ortamlardır (Şahinaslan, Kandemir ve Şahinaslan, 2009). Bilgi güvenliği; yazılı, sözlü ve elektronik ortamdaki bilginin her türlü tehditten korunmasıdır (Ulaşanoğlu, Yılmaz ve Tekin 2010). Bilgi güvenliğinin birçok boyutu olmasına rağmen temelde üç ilkeden bahsedilmektedir. Bunlar gizlilik, bütünlük ve sürekliliktir (Pro-G, 2003). Bu üç temel ilkeye alt bileşen olarak kayıt tutma, kimlik tespiti, güvenirlik ve inkar edememe bileşenleri de eklenebilmektedir (Tekerek, 2008).

2.1.3.1 Bilgi güvenliği ilkeleri

2.1.3.1.1 Bütünlük

Verilerin, yetkisiz kişiler tarafından veya tesadüfi bir şekilde değişmemesi, parçalanmaması veya kaybedilmemesidir (Gelbstein ve Kamal, 2002). Kötü niyetli kişilerin yaptıkları saldırılar, sistem kullanıcısını istemeden ve bilmeden bir dosyası silmesi, sisteme virüs bulaşması, önemli dosyalardaki bilgilerin değiştirilmesi veri bütünlüğü bozacak örneklerdir (Delialiağlu, 2011). Verilerin haberleşme sırasında izlediği yolların değişmemesi, yeni verilerin eklenmemesi, verilerin bir kısmının veya bütünün tekrar edilmediği, verinin sırasının değişmemesi durumunda veri bütünlüğü sağlanmış olur (Tekerek, 2008).

2.1.3.1.2 Gizlilik

Gizlilik, bilginin yetkisiz kişiler tarafından ele geçirilmesinin engellenmesidir. Gizlilik kalıcı ortamlar olan disk, CD, DVD, Harisi diskler vb. gibi ortamlarda bulunan bilgiler veya ağ üzerinden gönderilen bilgiler için geçerlidir (Pro-G, 2003). Bilgisayarda çalışırken kişilerin fark ettirmeden ekrandaki bilgileri görmeye ve okumaya çalışması, sosyal mühendislik yöntemi, klavye tuşlarının kaydedilmesi, başlıca gizlilik ihlalleridir.

2.1.3.1.3 Süreklilik

Kullanıcıların erişim izinleri olan verilere, verilerin tazeliğini yitirmeden zamanında ve güvenilir şekilde ulaşılmasıdır. Süreklilik, kurum içinden veya dışından

gelebilecek tehditlere karşı bilişim sistemlerinin korunmasını hedefler. Kötü amaçlı hackerlar, sistemdeki yazılım hataları, sistemin eğitimsiz ve bilinçsiz personel tarafından kullanımı, ortam şartlarındaki değişimler (ses, ışık, nem vb.) sistem sürekliliğini etkiler (Pro-G, 2003). Sistem sürekliliğini sağlamak için sistemin iç ve dış saldırılara karşı korunması, personelin bilgi ve becerisini artıracak eğitimlerin verilmesi, servisi aksatacak her hangi bir duruma karşı önceden çözümler üretilmesi gerekir (Delialioğlu, 2011).

2.1.3.1.4 Kayıt tutma

Kayıt tutma, bilgisayar sistemi veya ağı üzerinde gerçekleşen olayların daha sonra analiz etmek için kayıt altına alınmasıdır. Bu olaylar kullanıcı parolalarını yazılarak sisteme girmeleri, bir web sayfasına bağlanmaları ve gezinmeleri, e-posta göndermeleri vb. gibi sistem üzerinde yapılan faaliyetlerdir. Kayıt edilen olaylar üzerinde yapılacak analizler ile saldırı izine yönelik veya saldırı ihtimaline karşı sistem yöneticilerine uyarı mesajları gönderilir (Pro-G, 2003). Ayrıca bu saldırı kayıtlarının izi takip edilerek saldırganların kimliği tespit edilebilir (Tekerek, 2008).

2.1.3.1.5 Kimlik tespiti

Kimlik tespiti, sisteme girmek isteyen kişinin doğru kişi olduğundan emin olunmasıdır. Her hangi bir sisteme girerken parolanın istenmesi kimlik tespitine örnektir (Pro-G, 2003; Tekerek, 2008). Günümüzde hemen hemen bütün sistemler güvenlik için kimlik tespitini sağlayan uygulamaları barındırmaktadır. Bilgisayarda açılırken parola sorulması, telefonlarda pin kodunu sorulması, facebook msn gibi ortamlarda kullanıcı adı ve şifre istenmesi kimlik tespitlerine örnektir.

2.1.3.1.6 Güvenirlik

Sistemden beklenen davranış ile gerçekleşen davranış arasında tutarlılık olmasıdır. Sistemde yapılması gereken işlemin eksik veya fazla olmadan yapılması ve sistemin her çalıştığında aynı şekilde davranmasıdır (Pro-G, 2003).

2.1.3.1.7 İnkâr edememe

Bu hizmet sayesinde ne gönderici alıcıya bir mesaj gönderdiğini ne de alıcı göndericiden bir mesaj aldığını inkâr edebilir. Özellikle finans ve bankacılık sistemlerinde kullanılmaktadır. Gönderici ile alıcı arasındaki anlaşmazlıkların en aza indirilmesine yardımcı olur (Pro-G, 2003).

2.1.4 Bilişim Güvenliği

1990 yıllarından itibaren hızlı gelişen teknolojik gelişmeler sayesinde bilgisayarlar modern hayatın her alanına girmiştir. Günümüzde iletişim, para transferi, kamu hizmetleri, bankacılık, savunma sistemleri, eğitim ve daha birçok alanda bilgisayar ve bilgisayar ağ teknolojileri yoğun bir şekilde kullanılmaktadır. Teknolojideki bu olumlu gelişmeler aynı zamanda bu teknolojileri bir saldırıcı aracı ve açık bir hedef haline getirmiştir (Pro-G, 2003). Kötü niyetli bilişim korsanları güvenlik sistemlerini aşarak sisteme zarar verebilmekte, sistemin işleyişini bozabilmekte, sistemi çökertebilmekte ve kişilere zarar verebilmektedirler. Bilişim korsanları bu emellerine ulaşmak için çok farklı saldırı teknikleri uygulamaktadırlar (Canbek ve Sağıroğlu 2006). Son zamanlarda bilişim güvenliğine yönelik yapılan saldırı çeşitleri hızlı bir şekilde artmakta ve her geçen gün bilişim korsanları tarafından farklı saldırı türleri ortaya çıkmaktadır. Genel olarak bu saldırılar; virüs, solucan, Truva atı gibi zararlı yazılımlar, arka kapılar, casus yazılımlar, uzaktan yönetim araçları, botlar, saldırgan ActiveX, klavye dinleme sistemleri, tarayıcı soyma, rootkitler, eposta bombardımanı, sniffing, spoofing, aldatmaca, SQL enjeksiyon, phishing (oltalama), adware ve port tarayıcılar gibi her biri farklı amaçlara yönelik gerçekleştirilen saldırılardır (Canbek, 2005). Bu tür saldırılara maruz kalmamak ve bilişim güvenliğini sağlamak için çeşitli süreçler, politikalar ve ilkeler bulunmaktadır. Bilişim güvenliğinin öneminin kişiler ve kurumlarca bilinmesini sağlamak, bilgi güvenliği ilkelerini bilmek ve yürütmek, bilişim güvenliği farkındalığının artırılmasına yönelik faaliyetler yürütmek, bilgi güvenliği süreçlerini ve bilgi güvenliği politikalarını uygulamak bu tür saldırılara karşı alınabilecek önlemlerdir.

Bilişim güvenliği, bilgiyi işleme sürecinde kullanılan teknolojilerde, depolamada, iletişimde, kişilerin veya kurumların bilgisayar kaynaklarında bulunan her türlü formattaki bilginin ve verinin korunması disiplini olarak tanımlanmaktadır

(Gelbstein ve Kamal 2002). 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.

2.1.4.1 Bilişim güvenliği süreçleri

Bilişim güvenliği süreçleri önleme, saptama ve karşılık verme şeklinde 3 süreçten oluşur. Önleme sürecinde virüs tarama programlarının kurulu olması, bu programların ve işletim sisteminin güncellemelerinin yapılması, bilgisayarların şifre korumalı olması, şifrelerin tahmin edilmesini önlemeye yönelik zor şifrelerin oluşturulması, bu şifrelin gizli tutulması, internetten indirilen veya e-posta ile gelen dosyalara dikkat edilmesi, önemli belgelerin şifrelenerek korunması, önemli bilgi ve belgelerin düzenli bir şekilde yedeklerinin alınması alınabilecek önlemlerden bazılarıdır. Kısaca gerekli saldırılara karşı gerekli teknik ve donanımsal tedbirlerin alınması sürecidir. Alınan tedbirlere rağmen önleme sürecinde başarısız olunması halinde saptama süreci devreye girmektedir. Bu süreçte önlenemeyen saldırılar, bilinen veya yeni çıkmış saldırılar rapor edilerek uygun cevaplar verilir. Saptama sürecinde güvenlik duvarları, saldırı tespit sistemleri, ağ trafiği izleyiciler, ağ yoklayıcı algılayıcıları gibi teknolojiler ile sistemin bütün durumu ve hareketleri izlenip kayıt altında tutulur. Karşılık verme süreci ise, önleme sürecinde engellenemeyen ve saptama sürecinde belirlenmiş saldırılara en kısa zamanda cevap verecek eylemlerin gerçekleştirilmesidir (Canbek ve Sağıroğlu, 2006).

2.1.4.2 Bilişim güvenliğinin sağlanması

Bilişim güvenliğinin sağlanması yönetsel önlemler, teknoloji uygulamaları, eğitim ve farkındalık yaratma olmak üzere 3 temel unsurdan oluşur. Güçlü bir güvenlik altyapısı için bu üç unsuru bütünleştirilmesi ve her bir unsurun tam ve eksiksiz çalıştırması gerekmektedir.

2.1.4.2.1 Yönetsel önlemler

Yönetsel önlemler, güvenlik yönetimi ile ilgili bir dizi kuralın belirlenmesi ve uygulanması şeklindedir. Prosedürler, yönergeler, talimatlar ve politikalar yazıya dökülerek doküman şeklinde oluşturulur. Kurumun karşı karşıya kaldığı riskler tanımlanarak ve bunlara değer biçilerek bu risklerin belli bir seviyenin altında kalmasını sağlamak için mekanizmalar oluşturulur. Ayrıntıya girmeden kavramsal olarak güvenlik politikaları tanımlanır. Kurumlardaki bilgisayar yazılım ve donanımın nasıl kullanılacağına dair güvenlik standartları belirlenir, kurumsal bir standart uygulanmasında yaşanacak bir sıkıntıya karşı yol gösteren bir takım önerilerin yer aldığı yönergeler oluşturulur. Ayrıca belirli bir işi gerçekleştirmeye yardımcı olmak amacıyla hazırlanan ve atılacak adımların belirlendiği prosedürleri içeren dokümanlar hazırlanır (Pro-G, 2003).

2.1.4.2.2 Teknoloji uygulamaları

Bilişim güvenliğinin sağlanmasında çeşitli teknolojiler kullanılmaktadır. Genel anlamda bilişim güvenliğinin sağlanmasında kullanılan teknolojiler: kriptografi, güvenlik duvarları, yedekleme, saldırı tespit programları ve anti-virüs sistemleridir. Kriptografi, verinin matematiksel yöntemler ile kodlanarak başkalarının okuyamayacağı şekilde yalnızca istenen kişilere göndermek için kullanılan teknolojidir. Güvenlik duvarı, kurumların ağ güvenliği politikasının uygulanmasında başka bilgisayarlardan veya internet üzerinden gelebilecek saldırıları önleyen bir teknolojidir. Yedekleme, beklenmeyen bir saldırı veya afet sonucu önemli verileri kaybetmemek için düzenli aralıklar ile verilerin bellek üniteleri (flash bellek, taşınabilir hard disk, CD, DVD) üzerine yazılarak kaydetme ve saklama teknolojisidir. Saldırı tespit programları, bilgisayar ve bilgisayar ağı sistemlerinin faaliyetlerini izlemek ve olası saldırıları tespit etmek için kullanılan teknolojilerdir. Anti-virüs yazılımları, sisteme veya kişilere zarar verecek kötü amaçlı e-postaları veya dosyaları tanıyabilen ve temizleyebilen yazılımlardır (Pro-G, 2003).

2.1.4.2.3 Eğitim ve farkındalık

Bilişim güvenliğinin sağlanmasında yönetsel önlemlerin ve teknoloji uygulamalarının yanında en önemli unsur eğitim ve farkındalıktır. İnsan faktörü bilişim güvenliğini sağlamada en zayıf halka olarak görülmektedir. Kullanıcılar isteyerek veya istemeyerek sistemlerini, bilgi ağını veya kurumlarını tehditlere karşı açık bırakabilmektedir (Emiral, 2004). Burada önemli olan nokta sadece güvenlik teknolojilerini kullanmanın her zaman risklere karşı korunmanın en iyi yolu olmadığıdır. Risklere karşı korunma, güvenlik stratejilerinin ve çözümlerinin doğru yerde ve zamanda uygulanmasıyla ve insanların bilişim güvenliği konusunda bilinçlendirilmesiyle gerçekleşir (Eminağaoğlu ve Gökşen, 2009). Prosedür, politika, yönergeler ve talimatlar gibi yönetsel önlemler ile beraber gerekli güvenlik önlemlerini almanın yanında bilişim güvenliğinin nasıl sağlanacağı, nelerin yapılması gerektiği, risklere karşı hangi uygulamaların kullanılacağı bilgisi önemli konular olarak görülmektedir. Her ne kadar prosedürler, politikalar, yönergeler ve talimatlar oluşturulsa da son zamanlarda güvenlik teknolojileri geliştikçe kötü niyetli kişiler sistemlere erişebilmek için kullanıcıların zayıflıklarından yararlanmaya başlamışlardır. Dolayısıyla insan faktörüne bağlı olarak ortaya çıkan güvenlik risklerini en aza indirmek için farkındalık ve eğitim faaliyetlerine önem vermek gerekmektedir (Şahinaslan, Kantürk, Şahinaslan ve Borandağ, 2009). Yapılan çalışmalar; çevrimiçi erişim ve kullanım olanakların artmasıyla çevrimiçi risklerin de arttığını, bilişim güvenliği farkındalığının düşük olduğunu ve bu konularda bilinçlendirme çalışmalarının yapılması gerektiğini göstermektedir (Çelen, Çelik ve Seferoğlu, 2011). Çevrimiçi erişim ve kullanımın artmasıyla çocuklar ve gençler bilgisayar ve internet kullanırken çeşitli sorunlar ile karşılaşmaktadırlar. Bilgisayarlara virüsün bulaşması, casus yazılımların sisteme girmesi, yazılım ayarlarının bozulması, bilgisayarın çalışmaz hale gelmesi, aşırı oyun oynama, şiddet içerikli oyunlar oynama, önemli bilgilerin üçüncü şahıslara verilmesi, yabancı kişiler ile sohbet edilmesi, zararlı içeriklerle karşılaşma, pornografik öğeler maruz kalma, suç örgütleri ile haberleşme gibi durumlar çocukların ve gençlerin karşı karşıya kaldıkları tehlikelerdir (Canbek ve Sağıroğlu, 2007b). Çocukları bu gibi tehlikelerden korumak ve güvenli internet kullanımlarını sağlamak için ebeveynlere büyük iş düşmektedir. Demirel, Yörük ve Özkan'ın (2012) gerçekleştirdikleri bir araştırmanın sonuçlarına göre; ebeveynler, çocukların bilgisayar ve internet kullanımının,

derslerini olumsuz etkilediğini, interneti çocuklar için güvensiz bir ortam olduğunu belirtmişlerdir. Yine aynı araştırmanın sonuçlarına göre; ebeveynlerin Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından başlatılan güvenli internet hizmetinden haberdar olma durumların orta düzeyin biraz üstünde olduğu, internet filtresi kullanım oranının yetersiz olduğu ve güvenli internet hizmetinden yararlanma konusunda çok istekli olmadıkları görülmüştür. Bir diğer araştırma, öğrencilerin yüksek seviyede güvensiz internet kullandıklarını ve ebeveyn denetiminin, çocukların güvenli internet kullanımlarında önemli etkiye sahip olduğunu ortaya çıkarmıştır (Valcke, Schellens, Van Keer ve Gerarts, 2007). Yapılan araştırma sonuçları dikkate alındığında, ailenin çocuklarıyla yakın ilişkiler içinde olması ve en iyi denetimin ailede gerçekleşiyor olması nedeniyle çocuklara interneti doğru kullanmayı öğretmek, sağlıklı gelişimlerini sağlamak ve internetin olumsuz etkilerini en aza indirmek için ebeveynlere büyük görevler düşmektedir (Yalçın, 2006). Internette güvenliği sağlamak bilgili olmayı ve bilgi güvenliğini alışkanlık haline getirmeyi gerektirirken aynı zamanda bir süreçtir. Sürecin sağlıklı bir şekilde ilerlemesi için bilişim ve internet güvenliği konusunda eğitim ve bilinçlendirme faaliyetleri düzenlenmelidir. Bu eğitim sürecinde öğretmenler, öğrenciler, yöneticiler ve ebeveynler mutlaka yer almalıdır (Mert, Bülbül ve Sağıroğlu 2012).

Çocukların ve gençlerin bilişim güvenliği konularında yetersiz olmalarının yanında kurum ve kuruluşların da bilişim güvenliğini sağlamada yetersiz kaldığı noktalar bulunmaktadır. Özellikle kasıtlı saldırılar, teknik yazılım hataları, hırsızlık, bilginin tahrif edilmesi, teknolojinin eskimesi gibi güvenlik problemleri yaygın bir şekilde görülmektedir. Hizmet kesintisini önleme, ağ gizliliğini güvence altına alma, yüksek seviyede doğrulama mekanizmaları uygulama gibi konularda önlemler ve çalışmalar yetersiz olmaktadır. Mevcut prosedürlerde, belgelerde, politikalarda bilgi güvenliğine dair amaçlar bulunmamakta, birçok çalışan bilişim güvenliğini önemli bir konu olarak düşünmemekte ve kendilerini bu sorunların çözümünde bir unsur olarak görmemektedirler. Bu durumlar kurumlarda çalışan personelin bilişim güvenliği farkındalığına önem vermediklerini ve karşılaşılan tehditler göz önüne alındığında personelin bilişim güvenliği bilgisinin düşük olduğunu göstermektedir (Rezgui ve Marks, 2008). İnsan faktörü temel alınarak bireylerde bilişim güvenliği farkındalığının oluşturulması ve bireylere bilişim güvenliği konusuna yönelik eğitimlerin verilmesi önemli bir husus olarak görülmektedir. Bilişim güvenliği

farkındalığı oluşturmak ve artırmak için çeşitli faaliyetler yapılabilmektedir. Temel bilgisayar güvenliği, bilişim güvenliği temelleri, yazılım güvenliği, ağ güvenliği ve şifreleme gibi güvenlik dersleri ilkokul, ortaokul, lise ve üniversite müfredatında yer alması bilişim güvenliği farkındalığın artırmak için yapılabilecek önemli bir faaliyettir (Karaarslan ve Şengonca, 2003). Okullarda müfredata konacak bilişim güvenliği derslerinin yanında pek çok farklı yöntem bulunmaktadır. Bunlar;

- Internet tabanlı interaktif sanal eğitimler
- E-Learning eğitimleri
- Bilgi güvenliğine yönelik kitapçık, broşür, posterler
- Film gösterileri ve animasyonlar
- Güvenlikle ilgili sesli e-posta, videolar
- Bilgi güvenliğine yönelik skeçler, oyunlar
- Belli aralıklarla yapılan bilgi güvenliğine yönelik sunulardır (Şahinaslan, Kantürk, Şahinaslan ve Borandağ, 2009).

Bunlara ek olarak kullanıcılara bilgi güvenliği farkındalığını artıracak ve güvenlik yöntemlerini uygulamada yardımcı olacak video oyunlar ve simülasyonlar kullanılabilmektedir. Bilginin değeri, erişim kontrol mekanizmaları, sosyal mühendislik, şifre yönetimi, zararlı yazılım, veri güvenliği sağlama, fiziksel güvenlik, antivirüs koruma, veri yedekleme gibi konularda hazırlanan senaryolar kullanıcılar tarafından yürütülerek güvenliğin nasıl sağlanacağı öğreten video oyunlar yapılmaktadır (Cone, Irvine, Thompson ve Nguyen, 2007). Simülasyonlarla iyi oluşturulmuş bilgi güvenliği politikalarına olan ihtiyaç belirtilebilmekte, güvenlik politikalarını yürürlüğü koymak için kullanıcıların çeşitli yöntemleri uygulamasına izin verilebilmektedir. Ayrıca kimlik doğrulama, denetim, erişim kontrolü ve kötü niyetli kişiler tarafında sistemlere bulaştırılan zararlı yazılımlar simülasyonlar ile gösterilerek kullanıcılar bilinçlendirilmektedir (Irvine ve Thompson, 2003). Video oyunlar ve simülasyonların yanında bilişim güvenliğine yönelik uygulamalar geliştirilebilmekte veya programlar yazılabilmektedir. Örneğin; Küçük ve Soğukpınar (2013) kişilere ve kurumlara yönelik, içinde eğitim ve analiz amaçlı siber saldırı araçları bulunan ve derinlemesine güvenlik bilgisi sağlayan bir yazılım geliştirmişlerdir. Uygulamada ilk olarak belirlenen siber saldırı aracı ile ilgili bilgi verilmekte, ikinci bölümde siber saldırı kullanıcının bilgisayarında çalıştırılmakta,

üçüncü bölümde öğrenilen bilgiler ışığında problemler verilmekte ve bu problemlerin çözülmesi istenmekte, uygulamanın sonuç bölümünde ise kullanıcının bilgisine, problemlere verilen cevaplara göre güvenlik skoru ve öğrenme skoru gibi puanlar verilmektedir. Bu uygulama, bireylerin veya kurumların siber saldırılara karşı ne derece temkinli ve bilgili olduklarını tespit etme açısından oldukça yararlı görülmektedir. Buna benzer uygulamalar yapılmadan veya gerekli değerlendirmeler yapılmadan sadece bilişim güvenliği farkındalık eğitimini veya programını uygulayarak bireylerin bilişim güvenliğini otomatikman garanti altına alındığını belirtmek doğru bir yaklaşım olmayacaktır. Bilişim güvenliği farkındalık eğitimini veya programını değerlendirmek ve bilgi güvenliği alanını katkı sağlamak için eğitimin veya programın etkililiğini ölçmek ve geri bildirim almak gerekmektedir. Bilişim güvenliği farkındalığını ölçerken bireylerin konu hakkında doğru bilgi sahibi olup olmadıklarına, konuya yönelik düşüncelerine ve en önemlisi bir sorunla karşılaştıklarında gösterdikleri davranışlara yönelik değerlendirmeler yapılması daha yararlı olacaktır (Kruger ve Kearney, 2006). Özelikle bireylerin herhangi bir saldırı veya tehdit karşında davranışlarını belirlemek en doğru değerlendirme yöntemi olarak düşünülmektedir.

2.1.5 Bilişim Güvenliğini Sağlamak İçin Alınabilecek Önlemler

- Taşınabilir bellekler her kullanışta virüs taramasından geçirilmelidir.
- Bütün şifrelerin harf, rakam ve simgelerden oluşan karmaşık bir şifre olmasına özen gösterilmelidir.
- Kullanılan şifrelerin unutulması durumunda sorulacak gizli soru ve cevapların kontrol edilerek kolay bulunabilecek cevaplar olmadığına dikkat edilmelidir.
- Kullanılan her hesap için şifreler farklı olmalıdır.
- E-postalara gelebilecek kimlik bilgilerinin doğrulama mesajlarına itibar edilmemeli ve güvenli olmayan e-postalar açılmadan silinmelidir.
- Kablosuz ağ (wireless) kullanıcıları son şifreleme metodu kullanmalı, şifresiz kablosuz ağ kullanımlardan kaçınmalı ve kablosuz ağ kullanılmadığı durumlarda ağ bağlantısı kapatılmalıdır.

- Sosyal paylaşım sitelerinde tüm adres, telefon, okul, sınıf, kimlik bilgileri paylaşılmamalı; bilgiler, fotoğraflar, videolar sadece arkadaşların görebileceği şekilde belirlenmeli; hatta bilgiler gizli tutulmalıdır.
- Bilgisayar başında olunmadığı durumlarda bilgisayar açık bırakılmamalı ve bilgisayarlara parola koyularak güvenlik sağlanmalıdır.
- Kullanılan web tarayıcısı sürekli güncellemeli, güvenlik ayarları yapılmalı ve internette gezinirken tarayıcının adres çubuğunda HTTPS:// yazıldığına dikkat edilmelidir.
- Bilgisayarlarda kullanılan tüm yazılımların güncel tutulmasına dikkat edilmeli, lisanslı anti-virüs ve anti-spyware programları kurulmalı, bu programlar sürekli güncellenmelidir (Karakoç, 2011).
- Lisanslı işletim sistemi kullanılmalı ve işletim sistemi sürekli güncellenmelidir.
- Başka bilgisayarlardan gelen verileri kontrol eden ve zararlı yazılımların girişini engelleyen güvenlik duvarı aktif edilmelidir.
- Dosya paylaşımları, uzak masaüstü bağlantısı ve otomatik çalıştır özelliği kapatılmalıdır.
- Web sitelerinde cazip gelen reklamlara tıklanmamalı, tanınmayan kişilerden gelen e-postalara açılmamalı ve görülen her program bilgisayara kurulmamalıdır.
- Web tarayıcısında özellikler sekmesi kullanılarak geçici internet dosyalar, tanımlama bilgiler, form bilgiler ve parolalar geçmişi belli aralıklarla silinmelidir.
- Internet bankacılığını kullanırken veya internet üzerinden alışveriş yaparken şifre istenen formlarda ekran klavyesi kullanılmalıdır.
- Üye girişi yapılan her hangi bir siteden güvenli çıkış yapılmalıdır.
- Sıkıştırma programları yardımıyla önemli olan belgeler sıkıştırılmalı ve şifrelenmelidir.
- Bilgisayarda olabilecek zararlı bir gelişmeye karşı sistemi eski ayarlarına döndürebilmek için sistem geri yükleme noktası oluşturulmalıdır (Gelişken, 2009).

- MP3, Crack, Wares gibi siteler yasal olmadıklarının yanında birçok sayfasında casus yazılımlar bulunduğundan bu gibi siteleri ziyaret etmekten kaçınılmalıdır.
- Web tarayıcıların güvenlik özelliklerini dikkate alarak en güvenli web tarayıcısı kullanılmalı ve güncel tutulmalıdır.
- Çerezler zararlı web siteleri tarafından bilgi toplama amacıyla kullanılabileceğinden tarayıcınızın güvenlik ayarları; birinci parti çerezlerini sor, üçüncü parti çerezleri engelle, oturum çerezlerine her zaman izin ver şeklinde ayarlanmalıdır.
- Ortak paylaşımını olduğu internet kafeler, üniversite yerleşkeler gibi yerlerde şifre, kredi kartı vb. bilgilerinizi kullandığınız işlemler yapılmamalıdır.
- Internette gezinirken veya işletim sisteminde işlem yaparken karşınıza çıkan pencereleri okumadan "Evet", "Hayır", "Tamam" gibi düğmelere tıklanmamalıdır.
- "Ornek.txt.exe" isminde exe uzantılı zararlı bir dosya "Ornek.txt" olarak gözüktüğünden dosya yönetimimi bölümünden "bilinen dosya türlerini uzantılarını gösterme" seçeneğini kaldırmalıdır.
- Her ihtimale karşı düzenli aralıklarla sisteminizin ve önemli belgelerinizin yedeği alınmalıdır.
- Gelişen tehditlerden ve saldırı tekniklerinden haberdar olmak için teknik forumlara üye olunmalı, güvenlik ile ilgili çalışmalar okunmalı ve güncel güvenlik gelişmeleri sisteme uygulanmalıdır (Canbek ve Sağıroğlu, 2008).

2.1.6 Bilişim Güvenliğini Tehdit Eden Unsurlar

Bilişim güvenliğine yönelik tehditler kullanıcı tabanlı, yazılım tabanlı ve sosyal mühendislik olarak üçe ayrılmaktadır.

2.1.6.1 Kullanıcı tabanlı tehditler

2.1.6.1.1 Şifre ve gizli soru tahmini

Bir sisteme yetkisiz erişim sağlamak için en yaygın olarak kullanılan yöntem, kullanıcıların şifrelerini elde etmek için kullanılan gizli soru yanıtının tahmin

edilmesidir. Her hangi bir sisteme kayıt olunurken kullanıcıların şifrelerini unutma ihtimallerine karşı gizli soru ve yanıt ikilisinin tanımlanması istenmektedir. Telefon bankacılığı yapılırken banka yetkilileri tarafından istenen anne kızlık soyadı gizli soru ve yanıt ilişkisinin en yaygın örneklerinden biridir (İlbaş, 2009).

2.1.6.1.2 Omuz sörfü ve çöpe dalma

Omuz sörfü, kullanıcıların bilişim sistemlerinde veya internet ortamında şifrelerini yazarken gizlice izlenmesi, gözlenmesi; kullanıcıların şifrelerini yazdıkları not kâğıtları gibi araçların incelenmesi şeklinde olan bir yöntemdir (İlbaş, 2009). Kredi kartlarıyla alışveriş yapıldığı esnada veya yapıldıktan sonra kullanıcıların, başkaları tarafından gizlice izlenerek kredi kartı numaralarının ve şifrelerinin ele geçirilmesidir (Moore, 2011).

Çöpe dalma ise, bilişim sistemiyle gerçekleşen bir veri-işlem sonrası çıktı birimlerince kullanılan ve daha sonra çöpe atılan kâğıt, mürekkep şeriti vb. gibi malzemelerin üzerinde bulunan bilgilerin toplanmasıdır. Bu yöntem için fazla bilgi gerektirmediğinden çok kullanılan bir yöntemdir (Değirmenci, 2002).

Diğer yöntem ise bilişim sistemlerinin belleğinde bulunan ve ihtiyaç duyulmayarak silinen belgelerin gelişmiş programlar yardımıyla tekrar elde edilmesidir. Bu yöntem, genellikle programlama bilgileri orta seviyede olan, bilişim ve ağ sistemlerine nasıl erişeceğini iyi bilen kişiler tarafından gerçekleştirilmektedir (Değirmenci, 2002).

2.1.6.2 Yazılım tabanlı tehditler

2.1.6.2.1 Virüsler

Virüsler, biyolojik virüsler gibidir. İçine girdiği sistemi içten çökerterek sistemi kullanılmayacak hale getirirler ve bulunduğu sistemde kendini kopyalayarak diğer dosya ve sistemlere bulaşırlar. Virüsler veri depolama cihazları ve veri transfer yolları ile bulaşırlar. Veri depolama cihazlarına örnek olarak CD, DVD, USB Diskler ve harici hard disk verilebilir. Veri transfer yollarıyla bulaşmalarına örnek olarak ise, sohbet programlarından ve e-posta uygulamalarından gelen dosyalar örnek olarak gösterilebilir (Gelişken, 2009).

Virüsler, makine ve işletim sisteminin verdiği olanakları kullanarak kullanıcıların bilgisiz ve izni olmaksızın kendilerini bir programa veya bir dosyaya iliştirerek bilgisayardan bilgisayara atlayabilen bir bilgisayar kodu parçalarıdır. Bilgisayara, dosyaya, programlara gizli bir şekilde yerleşerek zarar verirler (Alaca, 2008; Boğa, 2011; Burlu, 2010). Virüsler, girdikleri programlara bir kopyalarını ekleyerek programların çalışmasını değiştiren, programların işlevleriyle oynayan, zararlı eylemlerde bulunan, ekranda tuhaf mesajlar görüntüleyen, sistemde anormal davranışlar yaratan, sabit disk üzerindeki verileri silen programlardır (Aydın, 1992). Virüsler üzerinde bulundukları programlar çalıştırılmaya başlandığı zaman çoğalırlar. Programlar gereğinden fazla hafıza alıyorsa, işletim sistemi donuyorsa veya hata veriyorsa, tarayıcı veya diğer programlar donuyorsa, disk sürücülerini ismi değişiyorsa bilgisayara virüsün bulaşmış olma ihtimali yüksektir (Burlu 2010).

Virüsler neye bulaştıklarına göre sınıflandırılabilirler. Boot virüsleri, disk üzerinde işletim sisteminin yüklenmesini sağlayan "boot" sektörlerine yerleşerek sistem açıldığında zarar veren virüslerdir. Dosya virüsleri, çalıştırılabilir dosyalara yani uzantısı ".exe", ".com", ".bat" vb. olan ve bu gibi dosyalar çalıştırılınca devreye giren virüslerdir. Bilgisayar açık kaldığı sürece bu virüsler kendilerini diğer dosyalara bulaştırmaktadırlar (Boğa, 2011; Burlu, 2010). Makro virüsler, Word, Excel ve Access gibi programlarının dokümanları ile bulaşan virüslerdir. Network virüsleri, e-posta ve ağ protokolleri ile diğer sistemlere bulaşan virüslerdir. Bunların dışında anti-virüs yazılımlarına karşı kendilerini gizleyen virüsler de bulunmaktadır (Burlu, 2011).

2.1.6.2.2 Truva atları (Trojans)

Truva atlarının bir diğer adı trojandır. Truva atları faydalı gibi görünen, kendisini programlayan bilişim korsanıyla sürekli iletişim halinde olan ve sistemin ele geçirilmesinde yardımcı olan zararlı yazılımlardır. İlk başta faydalı görünüp daha sonra zararlı oldukları anlaşıldığından dolayı Truva atlarına ikiyüzlü yazılım denmektedir. Truva atları sistemde sanal kapılar açarak bilişim korsanın sisteme sızmasını sağlarlar (Gelişken, 2009). Genellikle kullanıcıları cezbedecek programlar içerisine konulmakta, elektronik posta ile gönderilmekte ve farklı internet sayfalarında bulunan görsel öğeler ile kullanıcılara ulaştırılmaktadır. Truva atları

virüsler gibi zararlı yazılımlardır. Fakat virüslerin sahip olduğu çoğalma özelliğine sahip değillerdir. Truva atları sisteme girdikten sonra, kendilerini belleğe yüklerler, sistemin açıklarını tespit ederler ve bilişim korsanına sistem ile ilgili bilgiler gönderirler. Ayrıca gönderen kişinin isteklerine göre bilgilerde değişiklik yapabilir veya bilgileri silebilirler (Boğa, 2011). Truva atları internetten indirilen bedava dosya ve programlarla, işletim sistemini güncellenmemesi durumunda ortaya çıkan zayıflıklarla, otomatik çalıştır özelliğinin kullanılmasıyla, hareketli görsellerle ve e-posta yoluyla bulaşabilirler (Burlu, 2010).

2.1.6.2.3 Solucanlar (Worms)

Solucanlar, kendilerini otomatik olarak bir bilgisayardan diğer bir bilgisayara kopyalayan yazılımlardır. Solucanlarını virüslerden ayıran en önemli özellik, programın çalıştırılmasına gerek duymadan bulaşabilmeleridir. Solucanlar virüslerin alt kümeleri olarak adlandırılırlar. Solucanlar sisteme bir kez girdikten sonra kullanıcının yönlendirmelerine gerek kalmadan sistem içerisinde rahat bir şekilde ilerleyebilirler. En büyük özellikleri, hızlı bir şekilde ve büyük bir oranda çoğalmalarıdır. Örneğin solucanlar e-posta listesindeki kişilere bir kopyalarını gönderdikten sonra ulaşılan bilgisayarın e-posta listesindeki kişilere de bir kopya göndererek bu şekilde bir döngü içerisinde hızlı bir şekilde çoğalabilmektedirler. Solucanlar ağın yavaşlanmasına, ağın kilitlenmesine, web sayfaları görüntülenirken uzun süre beklenmesine neden olabilmektedirler (Boğa, 2011; Burlu, 2010). Ağ solucanları, internet solucanları, e-posta solucanları ve bilgisayar solucanları olmak üzere 4 çeşit solucan vardır (Canbek ve Sağıroğlu, 2007). Sisteme bulaşan solucanlar virüsler gibi sisteme zarar verebileceği gibi Truva atı bırakarak da sisteme zarar verebilirler. Solucanların temel çalışma prensibi kendilerini kısa sürede çoğaltmak ve ulaşabildiği tüm sistemlere yayılarak ağları ve bilgisayarları kullanılmaz hale getirmektir (Bilek, 2012).

2.1.6.2.4 Tuş kaydedici yazılımlar (Keylogger)

Bu yazılımlar, sistemde gizli bir şekilde çalışan, klavyeden basılan tuşları okuyup bunları metin haline getirerek kaydeden ve ağ üzerinden bilişim korsanlarına ileten yazılımlardır (Burlu, 2010; Gelişken, 2009). Keyloggerlar donanım ve yazılım

tabanlı olmak üzere iki türlüdür. Donanım olarak keylogger, ana kart ile klavye arasına yerleştirilen aparatlardır. Bu donanımlar günümüzde yaygın bir şekilde kullanılmamaktadır. Yazılım tabanlı olan Keyloggerlar her zaman gizli bir şekilde çalışırlar ve kullanıcılar sistemde bir keylogger olduğunu anlamazlar (Gelişken, 2009). Keyloggerlar, bir şirket yöneticisinin çalışanlarının mesai saatinde neler yaptıklarını öğrenmek ve iş dışında başka işlerle ilgilenmelerini önlemek, bir ebeveynin çocuklarının girdiği siteleri görmesini sağlamak, bir eşin karısının/kocasının internette kimlerle sohbet ettiğini öğrenmek amacıyla yazılan programlardır (Elbahadır, 2010). Fakat günümüzde bilişim korsanları tarafından bu gibi amaçların dışına çıkılarak kişilere ve sistemlere zarar vermek için kullanılmaktadırlar. Keyloggerlar, kendilerini programlayan ve sisteme yerleştiren bilişim korsanıyla sürekli iletişim halindedirler. Günümüzde keylogger, metin verileri göndermelerinin yanında görsel öğelerin ve videoların gönderilmesini de sağlamaktadırlar. Keyloggerlar internetten indirilen ücretsiz yazılımlar, resimler ve videolarla sisteme yerleşebilmektedirler (Gelişken 2009).

2.1.6.2.5 Ekran kaydedici yazılımlar (Screenlogger)

Kullanıcının fare ile her tıklama sonucunda belli bir piksel büyüklüğünde bir grafiği kaydederek kullanıcının belleğinde saklayan ve istenen bir zamanda uzaktaki bir sunucuya e-posta yoluyla gönderen yazılım türüdür (İlbaş, 2009). Internet bankacılığı sistemlerinde veya e-ticaret sitelerinde keylogger saldırılarına maruz kalmamak için web sitelerinin sağladığı sanal klavyeler screenlogger programların ortaya çıkmasına neden olmuştur. Screenlogger yazılımlarıyla, kötü niyetli kişiler sanal klavye kullanılan sistemlerde ekranda yapılan işlemleri takip ederek kullanıcıların bilgilerini elde edebilmektedirler.

2.1.6.2.6 Casus yazılım (Spyware)

Spyware, kullanıcılardan izinsiz sisteme kurulan, bilgisayar sistemini ele geçiren ve gizli bilgilere erişmek için kullanılan yazılımdır. Casus yazılım olarak telaffuz edilmektedir. Casus yazılımlar bilişim korsanları tarafından amaca uygun olarak geliştirilirler. Dolayısıyla bilişim korsanının tanımladığı işlemleri yaparlar. Bu gibi yazılımlar tarayıcı ayarlarını değiştirler, kişisel bilgileri öğrenirler, verilere ulaşırlar,

internette dolaşılan web sitelerini araştırırlar, kullanıcı adı ve şifreleri çalarlar ve sahte web sitelerine yönlendirme işlemlerini gerçekleştirirler. Bilgisayarda yapılan değişiklikleri bilgisayar her açıldığında değiştirirler. Casus yazılımlar kendilerini çoğaltmadan sistemin arka planında çalışırlar. Internetten indirilen bütün bedava veya reklam içerikli yazılımlarda casus yazılım bulunmaktadır. Bu gibi casus yazılımlardan korunmak için sisteme casus yazılım bulaşmadan önce bir anti-spyware programı kurmak gerekmektedir (Gelişken, 2009).

2.1.6.2.7 Reklam bedelli yazılım (Adware)

Reklamcılar ve pazarlamacılar tarafından kullanılan meşruluğu kesin olan özel bir Spyware (casus yazılım) tipidir. Reklam bedelli yazılım olarak adlandırılırlar. Adware yazılımlar, bilgisayara yasal olan bir yazılım kurulduğu sırada ana kurulum üzerinden bilgisayara yerleşirler. Ana yazılımın kurulumu sırasında kabul edilmesi gereken anlaşma şartlarının içine gömülüdürler. Kullanıcıların çoğu bu şartları okumadığı için Adware yazılımı kurduklarından habersizdirler. Adware'ler, Casus yazılımlar gibi çalışır. Bilgisayarda yapılan işlemleri izlerler ve reklam firmasına iletirler. Örneğin kullanıcıların internette nerelerde gezdiklerini, hangi siteleri ziyaret ettiklerini reklam firmasına bildirirler. Ayrıca sık sık ziyaret edilen web sayfalarına uygun olarak tarayıcıda kişileştirilmiş reklamlar görüntülerler (Miller, 2002/2003). Günümüzde Adware olarak dağıtılan reklam destekli programlar, oyunlar ve araçlar bulunmaktadır. Internetten bu gibi programlar, oyunlar veya araçlar indirilirken ve kurarken, casus yazılım bileşeni içeren yazılımlara hayır diyerek Spyware ve Adware kurumlarına karşı önlem alınabilmektedir (Miller, 2002/2003).

2.1.6.2.8 Çöp mail (Spam)

E-posta hesaplarına kullanıcıların isteği dışında gelen, reklam içerikli metinlerden ve resimlerden veya web siteleriyle ilgili bağlantılardan oluşan, göndereni belli olmayan sahte bilgilerle dolu e-postalara spam denir. Spam mesajları bir ödül kazandınız veya kolay bir şekilde nasıl para kazanacağınız içeren e-postalar olabilmektedir. Genelde spamlar herhangi bir zarar oluşturmazlar. Fakat spamlar içlerinde zararlı scriptler veya solucanlar bulundurabileceğinden zararlı olabilmektedirler. Kullanıcılar, sahte web sitelerine veya kötücül yazılım bulunduran sitelere bilgilerini verdikleri

durumda spam mesajlara maruz kalabilmektedirler. Spam mesajların içeriğinin, iletiyi gönderen kişinin ve mail adresinin garip olması sahte bir posta olduğunu göstermektedir. Spamlardan korunmak için güvenilmeyen kişilere veya web sitelerine e-posta adresleri verilmemeli ve spam filtreleme yazılımları kullanılması önerilmektedir (Gelişken, 2009).

2.1.6.2.9 DOS ve DDOS saldırıları

Bilişim korsanı sisteme sızmayı başaramadığı durumlarda sistemi çökertmesine veya sistem kaynaklarını harcayarak kullanıcıların sisteme erişmelerini engellemesine Denial of Service (DOS) saldırısı denir (Yılmaz, 2005). DOS saldırılarının amacı sisteme izinsiz giriş yapmak değildir. Amaç, hedef sistemlere erişmek isteyen kullanıcıların sisteme erişmesini engellemektir. DOS saldırısı, DOS sistemlerinin veya servislerinin aşırı yüklenmesi sonucu hizmet vermesi gereken kullanıcılara hizmet verememesidir. Saldırganlar, sistemin güvenlik açığını bulamadıklarında veya kullanılan yöntemler başarısız olduğunda DOS saldırısını kullanmaktadırlar (Burlu, 2010). DOS saldırıları, hizmet veren sunucunun işlemci, hafıza, bağlantı hızı, yedekleme gibi bileşenlerin kapasiteleri doldurularak hizmet vermelerini önleyerek gerçekleştirilmektedir (Delialioğlu, 2011). DOS saldırısı, tek noktadan ve sadece bir hedefe doğru gerçekleştirilir. Distributed Denial of Service (DDOS) saldırısı ise, saldırının çok noktadan tek bir hedefe doğru gerçekleştirilmesidir. Bilişim korsanları DDOS saldırısını gerçekleştirmek için bilgisayarlara virüs, solucan veya Truva atı gibi kötü amaçlı yazılımlarla bulaştırarak sistemlere sızarlar. Daha sonra bu bilgisayarlar kullanılarak istenen hedef bilgisayarlara saldırılar gerçekleştirilip, sistem hizmetlerini ve kullanıcıların sistemlere erişmelerini engellerler (Delialioğlu, 2011).

2.1.6.2.10 Köle bilgisayar (Zombi)

DDOS saldırılarında bilişim korsanları emellerini gerçekleştirmek için birden fazla sistemi ele geçirerek bu bilgisayarlara zombi denen yazılımlar yerleştirirler. Bilişim korsanları tek bir komutla bu bilgisayarları hedef sisteme yönlendirirler. Bu bilgisayarlara zombi yani köle bilgisayarlar denir. Bu saldırılarda köle bilgisayar sayıları yüzleri hatta binleri bulabilmektedir. Bilişim korsanları ele geçirdiği

sistemleri köleleştirmek için çeşitli yöntemler kullanırlar. Bu yöntemler doğrudan zombi yazılımı enjekte edilerek veya dolaylı olarak Truva atı gibi zararlı bir yazılımla bilgisayara zombi yazılımı indirilerek gerçekleştirilir (Elbahadır, 2010).

2.1.6.2.11 Mantık bombaları

Mantık bombaları, bilişim sisteminde önceden belirlenen durumlar meydana gelinceye kadar sisteme zararlı bir müdahalede bulunmayan fakat belirlenen tarih geldiğinde, yapılmaması gereken bir şey yapıldığında veya yapılması gereken bir şey yapılmadığında sisteme zarar veren bir çeşit Truva atı gibi ilk başta yararlı gözüken daha sonra zararlı yönleri ortaya çıkan programlardır (Alaca 2008; Boğa 2011). Mantık bombaları belirli şartlar oluşuncaya dek etkisiz bekleyen programlardır. Bu özellikleri sayesinde mayınlara benzetilirler. Mantık bombaları, kendilerini çoğaltacak şekilde yazılmayan ve yazımı için üst düzey programlama bilgisi gerektirmeyen programlardır (Atalıç-Taş 2010).

2.1.6.2.12 SQL enjeksiyon

SQL, veri tabanlarına ulaşmak ve işlem yapmak için diğer programlama dilleri ile beraber çalışarak kayıt ekleme, silme, listeleme, güncelleme gibi işlemlerin yapılmasını sağlayan bir yazılım dilidir. MySql, MsSql ve Oracle gibi pek çok veri tabanı SQL diliyle çalışmaktadır. Masaüstü programları ve Web yazılımları veri tabanı işlemlerini yaparken SQL komutlarını kullanırlar. SQL enjeksiyon saldırısı, web formları ya da veri girişi yapılan alanlara SQL komutları ve bazı karakterlerin ortak kullanımları ile yapılan saldırı türüdür. Veri tabanları ile çalışan web sitelerine yönelik gerçekleştirilen bu saldırılarda veri tabanı içinde bulunan kayıtlar görüntülenebilmekte, değiştirilebilmekte veya silinebilmektedir (Burlu 2010; Gündüz 2013).

2.1.6.2.13 Arka kapılar (Back doors)

Arka kapılar, bir sistemin yazılımını yapan kişi tarafından sistemde kalıcılığı sağlamak ve istenildiği zaman sisteme girmek için yazılımın içine gizli bir şekilde

yerleştirilen bir virüs programıdır. Arka kapılar, alan yazında tuzak kapılar veya gizli kapılar olarak da geçmektedir. Bu programın çalışması ile sistem yazılımını yapan kişi sisteme sızabilmektedir. Arka kapı olarak kullanılan pek çok program vardır. Truva atları bu programlardan biridir. Arka kapıların genel amacı sisteme veya kullanıcılara zarar vermek değil, kullanıcılar ait özel bilgilere ve programlara ulaşmaktır (Alaca, 2008; Boğa, 2011; Yılmaz, 2005). Arka kapılar genellikle sistemde ilerde oluşabilecek hatalara karşı sorunları gidermek için yazılımı yapan kişi tarafından oluşturulmaktadır. Fakat kötü niyetli kişiler tarafından bu kapılar tespit edilebildiğinden (Bilek, 2012) sistemlere gelebilecek ciddi zararlar karşı sistemin önceden bir yedeğini almak yararlı olacaktır (Yılmaz, 2005).

2.1.6.2.14 İzleme (Sniffing) ve Gizleme (Spoofing)

Bilgisayarlar bir ağ içerisinde birbirlerine veri gönderirler ve birbirleriyle iletişimi sağlarlar. Hedeflenen sistemlere sosyal mühendislik metotları ile sızmayı başaran bir bilişim korsanın yapacağı ilk iş sistemi izlemek ve bu izleme sırasında kendini gizlemek olacaktır. Bu izlemeyi gerçekleştirmek için sniffing yöntemini kullanırlar. Sniffing, kısaca veri trafiğini izlemektir. Bilişim korsanları, bu izleme sırasında kullanıcı bilgilerini, e-posta içeriklerini, transfer edilen dosyaları ve sistem bilgisini ele geçirebilirler (Elbahadır, 2010; Gündüz, 2013). Sniffing ağda olan biteni izlemeye imkân tanıdığından hem sistem yöneticileri hem de bilişim korsanları için kullanılabilecek önemli bir metottur (Gündüz, 2013).

Spoofing ise ağdaki bilgisayarlara kendisini ağdaki başka bir bilgisayarmış gibi tanıtarak ulaşılamayan bilgilere ulaşma işlemidir (Yılmaz, 2005). Ayrıca Spoofing, hedef sisteme sızan bir bilişim korsanının kendi güvenliğini sağlaması için kimlik bilgilerini gizleme ve sistem kayıtlarını silerek arkasında bıraktığı izleri silme işlemidir (Elbahadır, 2010). Kısacası Spoofing, bir kandırma ve gizlenme yöntemidir.

2.1.6.2.15 Web sayfası hırsızlığı ve web sayfası yönlendirme

IP adresi bilgisayarların birbirlerini tanımasını, birbirleriyle iletişim kurmasını ve veri iletimini sağlayan 32 bitlik verilerdir. IP adresleri xxx.xxx.xxx.xxx 4 haneli 8 bitlik rakamlar dizisinden oluşmaktadır (Elbahadır, 2010). Her bir web sayfasının kendine özgü bir IP adresi vardır. DNS ise IP adreslerinin tutulduğu bilgisayarları ve ağ hizmetlerini barındıran bir sistemdir (Alaca, 2008; Elbahadır, 210). Alan adları DNS veri tabanı sunucularında tutulur. Alan adları www.microsoft.com ve www.mynet.com.tr gibi adreslerdir. Bir web sitesine ulaşmak için alan adları tarayıcının adres çubuğuna yazılır. Örneğin tarayıcının adres çubuğuna www.microsoft.com yazıldığında web tarayıcısı alan adının DNS veri tabanlarında sorgular. Daha sonra web sayfasının bulunduğu sunucunun IP adresini öğrenir ve bu IP adresinden sayfayı tarayıcıya yükler. Bir kişi veya kurum bir web sayfası yayınlamak istediğinde alan adı hizmeti veren Servis Sağlayıcılara müracaat ederek uygun bir alan adı alır. Alan adını alan kişi veya kurum adını tescil etmiş olur. Yani isim hakkı o kişinin veya kurumun olur. Tescil edilmiş alan adları bilişim korsanları tarafından ele geçirilip değiştirilerek üçüncü kişilere yüksek ücretle satılması durumunda web sayfası hırsızlığı yapılmış olur (Alaca, 2008). Web sayfası yönlendirme ise, alan adlarının ve IP adreslerinin bulunduğu DNS sunucuların saldırı gerçekleştirilerek DNS sunucularında değişiklik yapıp kullanıcıları farklı web site adreslerin yönlendirmedir (Alaca, 2008). Bu yönlendirmeler sahte web sitelerine yapılır. Sahte web siteleri, internet ortamında yer edinmiş, tanınan ve sık bir şekilde erişilen web sitelerinin tasarımının kopyalanarak, benzer alan adı altında yayınlanan web siteleridir. Örneğin www.hotmail.c.com, www.hotmaij.com ve www.hot-mail.com gibi adresler www.hotmail.com sitesinin sahte web adresleridir (Gelişken, 2009). Bu yöntem özellikle internet bankacılığını kullanırken ve internetten alışveriş yapılırken gerçekleştirilir. Kullanıcılar ulaşmak istedikleri web sayfalarının adreslerini tarayıcının adres çubuğuna yazdıklarında farkına varmadan gerçek web sayfasına benzeyen bir sayfasına yönlendirilirler. Bilişim korsanları, kullanıcıların bu sayfalar üzerinde kullanıcı adı ve şifrelerini girmeleri ile kişinin sistemdeki bilgilerini, hesap bilgilerini ve kredi kartı bilgilerini ele geçirmiş olurlar (Boğa, 2011).

2.1.6.2.16 Rootkitler

Rootkitler, sistem yetkilileri ile çalışan hedef sistemin dosyalarını ve süreçlerini gizleyen ve değiştiren uygulamalardır (Burlu, 2010; Elbahadır, 2010). Rootkitler, sistem ele geçirildikten sonra bilişim korsanının sisteme istediği zaman girip çıkmasını sağlayan uygulamalardır (Burlu, 2010). Önceden derlenmiş ve içine Truva atları koyulan kurulmaya hazır programlardır (Yılmaz, 2005). Rootkitler'i diğer zararlı yazılımlardan ayıran en önemli özelliği sistem araçları ile yer değiştirerek kendilerini gizlemelidir. Güvenlik yazılımları Rootkitleri tespit etmede çok zorlanırlar (Elbahadır, 2010). Rootkitler, bir tarayıcının ya da çalışan bir uygulamanın sisteme gönderdiği sorguları sistemin yerine kendi cevap verir. Dolayısıyla herhangi bir güvenlik yazılımdan bir sorgu geldiğinde, Rootkitler gönderilecek cevaplara müdahale ederek gizliliklerini korumuş olurlar. Rootkitler dosyaları, kayıt defteri kayıtlarını (Registry) ve çalışan uygulamaların işlemlerini gizler, istenen işlemleri yönlendirirler ve arka kapı açarlar (Burlu, 2010; Elbahadır, 2010).

2.1.6.2.17 Botlar

Çok kullanılan bir DDOS saldırısıdır. Bot kelimesi Robot kelimesinden gelmektedir. Birçok botun bir arada hareket ederek saldırı yapmasına BOTNET denir (Burlu, 2010). Botlar; yazılımcılar tarafından geliştirilen, otomatik işlemler yapan, birtakım yönetimsel aygıtları el geçiren ve toplu saldırılar yapılmasında kullanılan yazılımlardır. Botlar kendilerine tanımlanmış komutlar ile bilgisayar kullanıcısı gibi davranış gösterirler. Botlar sahte web siteleri, sahte e-postalar ve taşınabilen dosyalar ile yayılabilmektedirler. Botlar genellikle çeşitli internet sitelerinde bulunan program veya virüslü dosyaları otomatik olarak indirirler ve kurarlar. Bu sayede korsanların ulaşamadığı bilgisayarlarda sanal insanlar gibi hareket eden botlar, gerekli işlemleri yürütürler veya korsanların sisteme erişmelerini sağlarlar (Gelişken, 2009).

2.1.6.2.18 Exploit

Kelime anlamı sömürmek, kötüye kullanmak, istismar etmektir (Burlu, 2010). Kişisel bilgisayarlar ve işletim sistemleri bugünkü çok kullanıcılı bir sistem olmadan

önce DOS gibi tek kullanıcılıydı. Tek kullanıcılı olduğu için tüm yönetimsel işlemler, tek kullanıcı hesabı altında yer alıyordu. Artan ihtiyaçlar ve gelişen teknoloji ile birlikte sistemi yöneten kullanıcı ile sıradan kullanıcıların olduğu çok kullanıcılı sistemlere geçildi. Bilişim korsanları için sıradan kullanıcı hesaplarının ele geçirilmesi kısıtlı ve yetersiz oluyordu. Dolayısıyla normal kullanıcı yetkilerinin sistem yetkilerine dönüştürülmesi gerekiyordu. Bilişim korsanlarının yetkisiz kullanıcı profiline yönetsel yetkiler kazandırmak için sistemin zayıflığından faydalanarak zarar verme işlevine exploiting, bunları yaparken kullandıkları uygulamalara exploit denir. Exploitler ileri seviye programlama bilgisi olan kullanıcılar tarafından yazılmaktadır (Elbahadır, 2010). Bu tip saldırılar, ileri seviye programlama bilgisi olan kullanıcılar tarafından yazılan programların, hacking konusunu fazla bilmeyen kişiler tarafından yapılması ile gerçekleşmektedir. Bu kişiler ”script kiddie” veya çaylak olarak adlandırılmaktadırlar. Internette ileri seviyede programlama bilgisi olan kullanıcılar tarafından yazılan bir sürü Exploit vardır. Herhangi bir Exploiti ele geçiren çaylak, güvenlik açığı olan sistemlere rahat bir şekilde saldırabilmektedir (Yılmaz, 2005).

2.1.6.2.19 Reklam içerikli pencereler (Pop-up Ads)

Bir web sitesinin sayfası yüklenirken, bu esnada kendiliğinden açılan reklam içerikli tarayıcı pencerelerine pop-up denir (Miller, 2002/2003). Internet kullanıcıların güvenilir bir internet sitesinde işlem yaparken açılan pencereler, kötü niyetler için kullanılabilmektedir. Bu tür pencereler sıradan reklam görüntüsü sunarken bazen de kullanıcılara bir şeyler vaat ederek onları sahte web sitelerine yönlendirebilmektedir. Ayrıca pop-up’ların içlerin bulunan kötücül yazılımlar, kullanıcıların sistemlerine bulaşarak kişisel verilerin ele geçirilmesinde kullanılabilmektedir (Ünver ve Mirzaoğlu, 2011). Kötü amaçlı yazılımlar yüklemek için oluşturulan Pop-up’lar bir web sitesinin, Google’da en üst sıralardan alt sıralara inmesine neden olabilmektedir.

2.1.6.2.20 Uzaktan yönetim araçları (RAT: Remote Administration Tools)

Bilişim korsanlarının kullanıcıların bilgisayarlarını tamamen kontrol altına almasını sağlayan çift taraflı çalışan programlardır. Bilişim korsanları, kendi bilgisayarlarında yüklü olan bir program ile kullanıcıların internetten indirdiği bu tür RAT programları

aktif ederek sisteme erişebilmektedirler. RAT programları Truva atları gibi davranmaktadırlar (Gelişken, 2009).

2.1.6.3 Sosyal mühendislik

Sosyal mühendislik, sıradan kullanıcılarla ilgili sistem hakkında elde edilemeyecek önemli bilgilerin ikna, etkileme, kandırma gibi yöntemlerle ele geçirilmesidir. Güvenliğin sağlanmasında en zor olan bu saldırı çeşididir. Çünkü hedef insandır (Elbahadır, 2010). Bu tür saldırılar, üst düzey programlama veya teknik bilgi sahibi olmayan kişiler tarafından bile gerçekleştirilebilmektedir. Bu saldırı türünün amacı, karşıdaki kullanıcıya kişinin kendini inandırmasıdır. Kişinin güveni kazanıldıktan sonra kullanıcı adı ve şifre gibi bilgiler istenerek saldırı gerçekleştirilmektedir. Bu saldırı türüne örnek olarak son zamanlarda telefonlara gönderilen kısa mesajlar veya internet ortamından elektronik postalar örnek gösterilebilir. Kişinin bir şey kazandığı inandırılarak kredi kartı bilgileri istenmekte veya bir programın kullanımının devamı için kişisel bilgiler istenmektedir (Delialioğlu, 2011). Bu gibi sosyal mühendislik saldırılarına maruz kalmamak için; bireyler bu konuda eğitilmeli, sosyal mühendislik konusunda bilgilendirme faaliyetleri verilmeli, sistem hakkında kritik bilgileri öğrenmek isteyenlere karşı neler yapılması gerektiği konusunda bilgilendirme yapılmalı, fiziksel güvenlik sağlanmalı, gerekirse en az iki aşamalı güvenlik doğrulaması yapılmalıdır (Elbahadır 2010). Aşağıda yaygın bir şekilde kullanılan sosyal mühendislik metotları verilmiştir.

2.1.6.3.1 Oltalama (Phishing)

Phishing, password (şifre) ve fishing (balık tutmak) sözcüklerinin birleşmesinden oluşmuştur. Bu saldırı, hedefe sahte e-posta gönderilerek şifre bilgilerinin çalınması ile gerçekleştirilir. Kullanıcılara gönderilen e-posta ile kullanıcılar gerçek web sayfası yerine ara yüzü gerçek web sayfasına benzeyen sahte bir siteye yönlendirilmektedir. Bu sayede sahte web sayfasına giren kullanıcıların kullanıcı adı, şifre, hesap bilgileri, kredi kartı vs. bilgilerine ulaşılmaktadır (Burlu, 2010; Delialioğlu, 2011). Kısaca bir internet sitesine benzer bir web sitesi kullanılarak kişilerin istenen bilgilerinin elde edilmesi ile yapılan bir aldatma yöntemidir (Türk Bilişim Derneği (TBD), 2006). Phishing saldırılarında doğrudan bir temas yerine

güvenilen bir banka ve firma adları kullanılarak kullanıcılara bir mail gönderilmektedir. ABD'de bir sene içerisinde 1,2 milyon bilgisayar kullanıcısı Phishing saldırısına maruz kalmış ve toplam 929 milyon dolar korsanlar tarafından ele geçirilmiştir. Bu kayıp şirketlerin yaklaşık olarak 2 milyon dolar kaybetmelerine neden olmuştur (Elbahadır, 2012). Symantec (2013) tarafından yayınlanan bir araştırmaya göre Phishing saldırılarının %69'u finans sektörüne, %27'si bilgi sistemlerine karşı yapılmaktadır. Son zamanlarda bilgi sistemlerinden olan sosyal paylaşım sitelerinde bu saldırıların arttığı görülmektedir. Bu tür saldırılara maruz kalmamak için özellikle hangi adrese yönlendirildiğine dikkat edilmelidir. Tarayıcının adres çubuğundaki adresin doğru adres olduğundan ve HTTPS güvenli protokolünün yazıldığından emin olunmalıdır (Burlu, 2010; Delialioğlu, 2011; Elbahadır, 2010).

2.1.6.3.2 Aldatmaca (Hoax)

Sahte içerikli e-postalar ile kullanıcılarda kayıtlı olan e-posta hesaplarını kişilere ve kuruluşlara gönderen bir sosyal mühendislik tekniğidir. Bu tür e-postalarda toplumda tepki yaratması amaçlanan yanlış bilgiler, inanılması zor olaylar, ünlü kişilerden geldiğini gösteren mesajlar, dini veya insanı konular içeren mesajlar ve genellikle duyarlılık anlamında herkese gönderilmesi istenen mesajlar bulunmaktadır (Canbek ve Sağıroğlu, 2007a; İlbaş, 2009; Burlu, 2010). Bu e-postalarda gönderilen linkin üzerine gelindiğinde gerçekte kötü amaçlı bir sitenin adresi görülmektedir. Dolayısıyla bu tür e-postalarda gönderilen linklerin kötü amaçlı bir siteye gidip gitmediği kontrol edilmeli veya bu tür e-postalara itibar edilmemelidir (Burlu, 2010; İlbaş, 2009).

2.1.7 Bilişim Suçu

Bilgi teknolojilerinde yaşanan gelişmeler sonucunda insanlık bilgisayar ve Internet gibi iki büyük imkâna kavuşmuştur. Fakat suç işlemeye meyilli kişi, gruplar ve örgütler bilişim teknolojileri kendi çıkarları için kullanabilmektedirler (Tulum, 2006). Toplumun düzenini tehdit eden, toplum tarafından yasaklanan ve toplum düzenini bozan işlerin yürütülmesine suç denir. Suçlar kişilere zarar vererek, kişilerin

mallarını gasp ederek, kurallara uymayarak ve ahlaki durumları hiçe sayarak gerçekleşmektedir. Bilişim suçu normal işlenen suçlara göre suçun işleniş şekli bakımından ayrılmaktadır. Normal suçlular silah kullanırken, siber suçlular bilgisayar teknolojilerini kullanılır. Bugün gördüğümüz birçok suç gerçek dünyadan siber ortama geçmiştir. Dolayısıyla bilişim suçları eskiden teknoloji olmadan işlenen suçların artık bilişim teknolojileri ile işlenmesi sonucu ortaya çıkmıştır (Brenner, 2010).

Bilişim suçunun tanımı ile ilgili farklı görüşler bulunmaktadır. Aydın (2002) bilişim sistemlerinin kötüye kullanılması ile ilgili olası geniş boyutlu hukuki bir tanımlamanın yapılabilmesinin zor olduğunu belirtmektedir. Genel anlamda bilişim suçu İngilizce'de sibersuç (cybercrime), dijital suç (digital crime), bilgisayarla ilgili suç (computer related crime), internet suçu (internet crime), bilgisayar suçu (computer crime) ve ileri teknoloji suç (hi-tech crime) gibi kelimelerle ifade edilmektedir. Bazen internet suçları ve bilgisayar suçları gibi kavramların kullanıldığı da görülmektedir (Pallı, 2008). Günümüzde bilgisayar, internet, cep telefonu, akıllı telefonlar, tabletler ve elektronik cihazlar ile bu suçlar işlenebilmektedir. Dolayısıyla genel anlamda bu cihazlar vasıtasıyla veya bu cihazlara yönelik gerçekleştirilen suçlara bilişim suçu denilmektedir.

Bilek (2002) bilişim suçunun; bilgisayar suçu, internet suçları, siber suçlar, teknoloji suçları gibi çok farklı adlarla anılabildiğini belirtirken, genel anlamda bilişim suçlarını elektronik bilgilere ve verilere bilgisayar veya elektronik araçlar ile yasadışı yollarla erişilmesi, bilgilerin veya verilerin bu araçlar vasıtasıyla değiştirilmesi, silinmesi olarak tanımlamaktadır. Elbahadır (2010) bilişim suçunu; bilgisayar, kredi kartı, elektronik bir cihaz, cep telefonu, bir bilgisayar programı gibi bilişim teknolojileri kullanılarak işlenen suçlar olarak tanımlamıştır. Dülger (2004) bilişim suçunu, verilere veya veri işleme ile bağlantısı olan sisteme karşı, bilişim sistemlerini kullanarak işlenen suçlar olarak tanımlamaktadır. Maheshwari, Hyman ve Agrawal (2011) ise, bilişim suçuna farklı bir açıdan yaklaşarak internet üzerinden bilgisayarı bir araç olarak kullanarak ya da bireyi hedef alarak işlenen suçlar olarak tanımlamışlardır.

Yapılan tanımlar incelendiğinde bilişim suçu geniş kapsamlı bir terim olarak kullanılmaktadır. Bu terimler sahtekârlık, hırsızlık, hasar, şantaj, topluma yönelik suçlar gibi, ortak paydaşı bilişim sistemi olan suçları kapsamaktadır. Dolayısıyla bilişim suçu terimi, bilişim ve bilişim sistemleriyle ilgili olarak her tür suç tipini kapsayabilmektedir (Aydın, 1992).

Günümüzde bilinen iftira, karalama, hakaret, kişisel bilgileri ifşa etme, kurumlara maddi kayıplar verme vb. gibi suçların bilişim sistemleriyle işlendiği ve her geçen gün arttığı görülmektedir. Buradan yola çıkarak bilişim suçu, teknolojik araçlar vasıtasıyla bireyleri veya kurumları hedef alan suçlar olarak tanımlanabilir. Ayrıca teknolojik cihazın çalışmasını engellemek veya teknolojik cihazı bozmak amacıyla gerçekleştirilen saldırılar da bilişim suçu kapsamına alınabilir.

2.1.8 Bilişim Suçlarının Sınıflandırılması

2.1.8.1 Yetkisiz erişim ve dinleme

Yetkisiz Erişim, bir bilgisayar sistemine ya da bilgisayar ağına izin alınmadan yani yetki olmaksızın erişmek ve sistemin iletişimini yetkisiz dinlemektir. Burada, suçun hedefi bir bilgisayar sistemi ya da ağıdır. "Erişim" sistemin bir kısmına, bütününe, sistem programlarına veya sistemin içerdiği verilere ulaşma anlamındadır. Bu sistemlere erişim bir kişi tarafından bilgisayara direkt olarak yakın bir yerden olabileceği gibi, uzak bir mesafeden örneğin bir modem hattı ya da başka bir bilgisayar sisteminden de olabilmektedir. Yetkisiz dinleme ise, bir bilgisayarı veya sistemleri veya özel telekomünikasyon sistemleri ile yapılan veri iletimini izin almadan dinlemektir. Teknik anlamda dinleme, iletişim içeriğinin bilgisayar sistemi veya elektronik cihaz kullanma yoluyla izlenmesi olarak tanımlanmaktadır (Gümüş, 2008).

2.1.8.2 Bilgisayar sabotajı

Bir bilgisayar ya da iletişim sisteminin fonksiyonlarına mantıksal ve fiziksel olarak zarar vermektir. Bilgisayar sabotajı, mantıksal zarar ve fiziksel zarar olmak üzere ikiye ayrılır. Mantıksal zarar, bilgisayarı veya sistemi engellenmek amacıyla

bilgisayar verilerinin veya programlarının sisteme girilmesi, yüklenmesi, değiştirilmesi, silinmesi veya ele geçirilmesidir. Bu bilgisayar ve sistemlere zarar vermek için virüsler, solucanlar, Truva atları vb. zararlı yazılımlar kullanılmaktadır. Bilgisayarlarda veya sistemlerde bulunan bilgiler ve veriler virüs, solucan veya Truva atları gibi kötücül yazılımlar ile değiştirilir, silinir veya çalışmaz hale getirilir. Fiziksel zarar ise bilgisayar ya da sistemin fonksiyonlarına zarar vermek amacı ile sistemin donanımsal araçlarını tahrif etmek veya kullanılmaz hale getirmektir (Gümüş, 2008).

2.1.8.3 Bilgisayar yoluyla dolandırıcılık

Bilgisayar yoluyla dolandırıcılık, bilgisayar ve iletişim teknolojilerini kullanılarak verilerin alınması, değiştirilmesi, silinmesi yoluyla kişilerin kendisine veya başkasına yasadışı mali kazanç sağlaması veya mağdura maddi ve manevi zarar verilmesidir (Boğa, 2011; Gümüş 2008). Bilgisayar yoluyla dolandırıcılık kredi kartlarının ve bankamatik kartlarının çalınması, çoğaltılması veya kopyalanması ile yapılmaktadır. Kredi kartları ve bankamatik kartları bilgilerine ulaşabilmek için genellikle bu kartların kullanımı sırasında manyetik kopyalama cihazları kullanılır. Ayrıca internet üzerinden çevrimiçi alışveriş sitelerinin kayıtlarının elde edilmesi veya kart sahiplerinin spam e-postalarla kandırılması şeklinde olabilmektedir (Boğa, 2011).

2.1.8.4 Bilgisayar yoluyla sahtecilik

Bilgisayar yoluyla sahtecilik, kişinin kendisine veya başkasına yasa dışı ekonomik menfaat sağlamak veya mağdura zarar vermek amacıyla bilgisayar, bilişim ve iletişim sistemlerini kullanarak sahte materyal (banknot, kredi kartı, senet, vs.) oluşturması veya dijital ortamda tutulan belgeler (formlar, raporlar vs.) üzerinde değişiklik yapması şeklindedir (Boğa, 2011; Gümüş 2008). Dijital ortamda bulunan her türlü bilginin üzerinde değişiklik yapmak sahteciliktir. Baskı teknolojilerinin gelişmesiyle evrak sahteciliğinde, sahte kimliklerde artış yaşanmaktadır. Resmi evraklar üzerinde yapılan değişikliklerle bireyler mağdur edilmekte ve zarar görmektedirler. Başkalarının adına e-posta gönderilerek veya web sayfası hazırlanarak ticari ve özel ilişkiler zedelenmektedir (Bilek, 2012). Özellikle

hayatımızda önemli yer edinen, her alanda kullanılan ve ticari amaçlı kullanımı artan sosyal ağlarda sahte hesap sayısında artış görülmektedir.

2.1.8.5 Bilgisayar yazılımının izinsiz kullanımı

Bilgisayar yazılımının izinsiz kullanımı, ulusal ve uluslararası telif sözleşmeleri ve yasalarla lisans hakkı korunan yazılım ürünlerinin yetkisiz olarak yani yasadışı yollarla kopyalanması, çoğaltılması, yayılması ve ticari anlamda kullanılmasıdır (Boğa, 2011). Fikir ve Sanat Eserleri Kanununda eser olarak kabul edilen bilgisayar yazılımlarının; resim, müzik ve görüntülerin; internet ortamından indirilen resim, müzik ve dokümanların lisans haklarına aykırı olarak kullanılması da bu kapsamda değerlendirilmektedir (Tulum, 2006). Film, müzik, oyun, program içerikli CD ve DVD'ler vs. her türlü eseri tamamen veya kısmen kopyalamak, çoğaltmak; çoğaltılmış nüshalarını kiralamak, ödünç vermek, satmak, kullanmak, dağıtmak da lisans haklarına aykırı eylemler kapsamına girmekte ve suç sayılmaktadır. Bunun yanı sıra, bu gibi çoğaltma ve kopyalama işlemlerini önleyen programları etkisiz hale getirmek veya bu programları etkisiz hale getirmek için program ve teknik donanım üretmek de suç kapsamına girmektedir (Atalıç.-Taş, 2010).

2.1.8.6 Yasadışı yayınlar

Alaca (2011) ve Gümüş (2008) yasadışı yayınları, kanun tarafından yasaklanmış her türlü materyalin web sayfaları, elektronik postalar, haber grupları, iletişim ortamları her türlü verinin bulundurulabileceği bellekler ve medya araçları ile dağıtılması ve yayınlanması olarak tanımlamışlardır. Yasadışı yayınlar üç şekilde olmaktadır. Birincisi; ülke güvenliğini ve huzurunu tehdit eden terör içerikli yayınlar ve web siteleridir (Bilek, 2012). İkincisi; çocukların, gençlerin ve toplumun ar ve hayâ duygularını inciten, ahlaki yapısını bozan, psikolojik ve sosyolojik bozuklara neden olan, toplum sağlığını bozan yayınlar ve web sayfalarıdır (Elbahadır, 2010). Üçüncüsü; bir kişiye, kuruma veya kuruluşlara yönelik hakaret, çirkin söz ve sövme içeren yayınlar ve web sayfalarıdır (Bilek, 2012; Elbahadır, 2010). Bu tür siteleri hazırlayanların asıl amacı Anayasa'ya aykırı olan düşüncelerini internet aracılığıyla belirli kişilere ve gruplara yaymaktır (Bilek, 2012).

2.1.8.7 Çocuk pornografisi (Pedophilia)

Çocuk pornografisi, bilgisayar sistemlerini kullanarak genellikle 18 yaş altındaki kız ve erkek çocukların cinsel istismarını içeren filmler, resimler ve videolardan oluşan uluslararası boyutta yasaklanmış zararlı içerikler bulunduran pornografi türüdür (Boğa 2011). Çocuk pornografisi, cinsel anlamda reşit olmayan bir kişinin cinsellik içeren görüntüleri olarak tanımlanmaktadır (Siber Suç Uzmanları Komitesi (SSUK), 2008). Bilişim suçları alanında, son zamanlarda bilgi ve iletişim teknolojilerindeki gelişmelerle birlikte çocuk pornografisi sıkça karşılaşılan bir suç olmuştur ve bu suçların geleceğin en büyük tehditlerinden birini oluşturacağı düşünülmektedir. Toplumun ahlaki yapısını bozan bu suçlar, ulusal ve uluslararası boyutta dünyayı tehdit eden unsurlar arasında başı çekmektedir. Teknolojik gelişmelerin devam etmesi ve internetin yaygınlaşması ile bu suçlar küresel bir kimlik kazanmış ve bu suçlarda çok hızlı gelişmeler yaşanmıştır (Uzunay ve Koçak, 2005). Bu zararlı içerikler; kötü niyetli kişiler tarafından internet ortamında bulunan çocuklara e-mail yoluyla, sosyal medya vasıtasıyla, tartışma gruplarıyla, akrandan akrana uygulamalarıyla, web siteleriyle, sohbet odalarıyla ve anlık mesajlar ile ulaştırılmaktadır (Cross, 2008). Temelde mesaj gönderme ve alma servisi sunan, resim ve videoları değiştirebilen her türlü internet aracı veya uygulaması bu suçların işlenmesinde kullanılabilmektedir. Bireylerle iletişim sağlamaya imkân tanıyan bu uygulamalar ve araçlar, kötü niyetli kişiler tarafından çevrimiçi ortamda çocukların karşısına çıkarılabilmektedir.

2.1.8.8 Internet bankacılığı dolandırıcılığı

Internet bankacılığı; bireylerin banka şubesine gitmeden internet erişim imkânı sunan bilgisayar, tablet veya akıllı telefon gibi teknolojik araçlar ile bankacılık işlemlerinin yapılması olarak tanımlanmaktadır (Boğa, 2011). Teknolojik gelişmeler, rekabet, müşteri memnuniyeti gibi etmenler nedeniyle internet bankacılığı hizmetleri hızlanmış, kolaylaşmış ve çeşitlenmiştir. Günümüzde hemen hemen bir banka şubesinde yapılabilecek işlemlerin tümü internet bankacılığı ile yapılabilmektedir. Para transferleri, ödemeler, havale, EFT, senet ödemeleri, SSK prim ödemeleri, trafik cezası ödemeleri, kredi kartı işlemleri, kredi kartı borçları ödeme, hesap açma, fatura ödeme gibi ve daha birçok işlem internet bankacılığının sunduğu olanaklardan

birkaçıdır. Internet bankacılığının bu gibi olanaklar sunması tabi ki güvenlik konusunu gündeme getirmiştir. Güvenlik probleminin çözümü için Secure Sockets Layer (SSL), SD Secure ve Secure Code gibi yüksek güvenlik önlemleri oluşturulmuştur (Çakmak, Güneşer ve Terzi, 2011). Bu yüksek güvenlik önlemlerine rağmen son zamanlarda internet şubeleri üzerinden Phishing, Keylogger veya e-posta aracılığıyla dolandırıcılık faaliyetleri artmıştır. Kötü niyetli kişiler, kullanıcıların güvenlik konusunda bilgi eksikliğinden ve kullanım hatasından yararlanarak banka sistemlerine sızmakta yüklü miktarda para elde edebilmektedirler (Boğa, 2011).

2.1.8.9 Dijital aktivizm

Dijital aktivizm bireylerin sosyal medya ve internet aracılığıyla sosyal veya politik konularda kamuoyu oluşturmaları ve eylemler tasarlamalarıdır. Tanım doğru bir amaca hizmet ediyor gibi gözükse de otorite aleyhinde devletin gizli bilgilerini yaymak veya kamuoyunu aldatarak kamuoyunun otoriteye karşı tavır almasını sağlamak bir suç oluşturmaktadır. Bu gibi ortamlar özgür iletişim ortamları olarak görülse de ülkenin milli birlik ve beraberliğine, güvenliğine zarar verecek yayınların veya paylaşımların yapılması uluslararası platformda ülke saygınlığını sarsabilmektedir (Bilek 2012). Web 2.0 teknolojileri ile birlikte kullanıcıların artık içerik tüketen konumdan içerik üreten konuma geçmeleri bu eylemlerin artmasında önemli gelişme olarak görülmektedir. Teknolojinin ilerlemesi, internet alanında yaşanan gelişmeler ve kullanıcıların internet ortamında düşüncelerini rahat bir şekilde paylaşabilmeleri bir takım sıkıntılara neden olabilmektedir. Kullanıcıların en çok içerik oluşturduğu ortamlar bloglar, forumlar, sohbet siteleri gibi sosyal medya araçları olduğundan bu ortamlar vasıtasıyla verilerde tahrifat yapılmakta ve manipüle edici içerikler yayınlanabilmektedir (Mavnacıoglu, 2009). Yalan yanlış bilgilerin ve kışkırtıcı içeriklerin paylaşılmasıyla toplumda bir karışıklık yaratılmakta, toplumun huzuruna gölge düşürülmektedir.

2.1.8.10 Siber terörizm

Siber terörizm, son zamanlarda gündeme gelen ve oldukça konuşulan yeni bir kavramdır (Moore 2011). Terör gruplarının propaganda faaliyetleri, haberleşmeler, taraftar kazanma, toplumda karışıklık oluşturma, bireyleri yönlendirme, terör

örgülerine yardım toplama, devleti kötüleme, hakaret gibi daha birçok eylemler bilişim ortamına taşınmakta ve bu eylemlerin ifa edilmesi yaygınlaşmaktadır (Boğa, 2011; Tulum, 2006). Siber terörizm; önceden planlanarak ve sahnelenerek kişilerin ve kurumların sistem güvenliğini ele geçirip politik amaçlar için toplumda bir korku hissi aşılamalarına denir. Genellikle ülkelerin kritik altyapıları hedef alınmaktadır. Bunlar elektrik sistemi, hava trafik kontrol sistemi, acil telefon sistemleri ve nükleer enerji sistemleri gibi sistemlerdir. Bilgisayar veya ağ sistemlerini etkisiz hale getiren, servislerin bozulmasından dolayı zararlara ve ölümlere neden olan kişilere siber terörist denmektedir. Günümüzde hemen hemen tüm bilgisayarlar ve bilişim sistemleri internete bağlı olduklarından bu araçların toplum içinde terör maksatlı kullanımı günden güne kolaylaşmaktadır (Moore, 2011).

2.1.9 Türk Hukuk Sisteminde Bilişim Suçları

01.06.2005 tarihinde yürürlüğe giren bilişim suçları kanun maddeleri, 5237 sayılı Türk Ceza Kanunu'nun (TCK) onuncu bölümünde bilişim alanında suçlar adı altında yer almaktadır. TCK'nın 243-246. maddelerinde bilişim sistemine girme, sistemi engelleme, sistemi bozma, verileri yok etme veya değiştirme, tüzel kişiler hakkında güvenlik tedbiri uygulanması, banka ve kredi kartlarının kötüye kullanılması kapsamında aşağıdaki suçlar bulunmaktadır (TCK, 2004).

2.1.9.1 Bilişim sistemine girme

MADDE 243. - (1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

2.1.9.2 Sistemi engelleme, bozma, verileri yok etme veya değiştirme

MADDE 244. - (1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur.

2.1.9.3 Banka veya kredi kartlarının kötüye kullanılması

MADDE 245. - (1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis cezası ve adlî para cezası ile cezalandırılır.

(2) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan yedi yıla kadar hapis cezası ile cezalandırılır.

2.1.9.4 Tüzel kişiler hakkında güvenlik tedbiri uygulanması

MADDE 246**.** - (1) Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

2.1.9.5 5237 sayılı Türk Ceza Kanunu'nda bilişim sistemleri aracılığıyla işlenen suçlar

TCK'da bulunan her suça bilişim sistemleri dâhil edilebilir. TCK'nın 103 nolu "Çocukların Cinsel İstismarı", 106 nolu "Tehdit", 226 nolu "Müstehcenlik", 107 nolu "Şantaj", 125 nolu "hareket", 133 nolu "Kişiler Arasında Konuşmaların Dinlenmesi ve Kayda Alınması", 134 nolu "Özel Hayatın Gizliliğini İhlal", 135 nolu "Kişisel Verilerin Kaydedilmesi", 136 nolu "Verileri Hukuka Aykırı olarak verme veya ele geçirme", 228 nolu "Kumar Oynanması için Yer ve İmkan Sağlama" maddeleri 5237 sayılı TCK'da Bilişim sistemleri aracılığıyla işlenebilecek suçlardır (Atalıç-Taş, 2010).

2.1.9.6 5651 sayılı İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi kanunu

Ulaştırma bakanlığı tarafından hazırlanıp 04.05.2007 tarihinde yürürlüğü konulan 5651 sayılı internet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkındaki kanunun amacı; erişim sağlayıcıların, yer sağlayıcıların, içerik sağlayıcıların yükümlülüklerine ve sorumluluklarına ilişkin usul ve esasları düzenleme ve kanuna uygun olmayan durumlarda erişimi engellemektir.

2.2 İLGİLİ ARAŞTIRMALAR

Bu bölümde bilişim suçları, bilgi güvenliği farkındalığı, bilgi güvenliği davranışları, internet güvenliği ve bilişim güvenliği ile ilgili yapılan alanyazındaki çalışmalara yer verilmiştir.

Bilek (2012) "Bilişim Suçları ve Üniversite Lisans Öğrencilerin Bilişim Suçlarına Yönelik Görüşleri" adlı yüksek lisans tezinde bilişim, bilişim suçu, bilgisayar gibi kavramlara değinmiş, internetin tarihi gelişimi ve suç kavramı üzerinde durmuştur. Türk Hukukundaki Bilişim suçlarından, bu suçlara yönelik düzenlemelerden, 2006-

2011 yılları arasındaki bilişim suçları verilerinden, bilişim suçları işleniş şekillerinden bahsedilmiştir. Araştırmada, nicel ve nitel veri toplama yöntemleri kullanılmıştır. Ceza ve Tevkif evleri Genel Müdürlüğü Yetişkin Eğitim Bürosunun görüşleri dikkate alınarak 30 mahkûm ile 19 sorudan oluşan nitel bir çalışma ve bununla birlikte Üniversite bilgisayar ve öğretim teknolojileri teknolojilerinde okuyan 312 öğrenciye 49 sorudan oluşan bilişim suçları konusunda bilgi düzeylerini ve tutumlarını ölçen nicel bir çalışma gerçekleştirilmiştir. Yapılan araştırmanın sonuçlarına göre; üniversite öğrencilerin bilişim suçları farkındalıklarının yüksek olmasına rağmen bir takım teknik konularda eksik oldukları ortaya çıkarılmıştır. Araştırmanın sonunda, bilişim suçlarıyla mücadele kanununun çıkarılması gerektiği, bilişim suçları konusunda uzman personelin yetiştirilmesi gerektiği, farkındalık düzeyinin her zaman yüksek tutulması gerektiği belirtilmiştir.

İlbaş (2009) "Bilişim Suçlarının Sosyo-kültürel Seviyelere Göre Algı Analizi" adlı yüksek lisans tezinde bilişim suçları algısının demografik faktörlere göre değişimini incelemiştir. Araştırmacını amacı; bazı bilişim suçlarını öğretim elemanlarının ve öğrencilerin ahlaki ve hukuksal düzenlemede nasıl gördüklerini belirlemektir. Araştırmanın veri toplama aracında; demografik bilgiler; teknoloji, internet, bilgisayar kullanımına yönelik ilgi; farklı ülkelerin hukuk sistemlerinde bilişim suçu sayılan 14 fiilin kişisel algı düzeyinde suç şiddeti açısı ve bazı bilişim suçu fiillerin ahlaki ve hukuksal açıdan suç olup olmadığına yönelik sorular bulundurulmuştur. Anket sonuçlarına göre en çok duyarlı olunan bilişim suçu konuları çocuk pornografisi, akademik aşırmacılık, özel hayatın gizliliği ve siber hırsızlık olmuştur. Araştırmanın sonunda araştırmacı, bilişim suçları ile mücadele için bilinçlendirici faaliyetlerin yapılması, bu faaliyetlerin yaygınlaştırılması ve toplumsal olarak bilgi ve algı düzeylerinin geliştirilmesi önerilerinde bulunmuştur.

Dijle (2006) "Türkiye'de Eğitimli İnsanların Bilişim Suçlarına Yaklaşımı" adı altında yüksek lisans tezi hazırlamıştır. Araştırmanın çalışma grubu öğretim elemanlarından ve öğrencilerden oluşmuştur. Bu çalışmada bilişim suçları çeşitli yönlerden incelenmiş, bilişim suçlarının kapsamı açıklanmış, bilişim suçları tanımlanmış, sınıflandırılmış ve hukuki boyutu üzerinde durulmuştur. Bilişim suçları ile mücadele alınması gereken önlemlerden bahsedilmiştir. Araştırma sonuçlarına göre bireylerin; konu ile ilgili yeterince bilgi sahibi olmadıkları ve internetten film, müzik vb. indirmenin suç olduğunu bilmedikleri tespit edilmiştir. Bunun nedenleri

olarak eğitimsizlik ve maddi yetersizlikler olarak belirtilmiştir. Araştırmada açık kaynak kodlu yazılımların kullanılması, bilişim suçları ile ilgili yasaların çıkarılması, uluslararası işbirliği yapılması, bilişim konularında uzman olan kişilerin bu konularda bilgilendirme faaliyetleri içerisine girmeleri gerektiği vurgulanmıştır.

Agamba ve Keengwe (2012) öğretmen adayları ile son kullanıcılar arasında bilişim suçlarını önlemede önleyici tedbir alma davranışlarını karşılaştıran bir çalışma gerçekleştirmişlerdir. 19 öğretmen adayına bilişim suçu farkındalığı ve bilişim suçlarını önlemeye yönelik görüşlerini içeren 20 soruluk bir anket uygulanmıştır. Öğretmen adaylarının bilişim suçu bilgisinin, bilişim suçlarının toplum üzerinde etkisinin ve güvenlik yazılımı kullanma farkındalığının iyi düzeyde olduğu tespit edilmiştir. Fakat öğretmen adaylarının bilişim suçlarını önlemek için gerekli önlemleri almadıkları ve son kullanıcılarla bilişim suçlarını önleme davranışları arasında anlamlı bir farklılık olmadığı tespit edilmiştir.

Dijle ve Doğan (2011) "Türkiye'de Bilişim Suçlarına Eğitimli İnsanların Bakışı" adlı çalışmasında Dünya'da ve Türkiye'de bilişim suçlarında yaşanan artışı ele almışlardır. Ayrıca eğitimli insanların (öğrenciler ve öğretim elemanları) bilişim suçu ve bilişim suçlarıyla mücadele konusunda görüşleri alınmıştır. 766 kişiden elde edilen verilere göre; katılımcıların %72,5'nin lisansız yazılım kullandıklarını, %29,6'sının internetten müzik, film, oyun indirmenin suç olduğunu bildiklerini, %34,9'nun maliyet düşüklüğü nedeniyle internetten indirme yaptıklarını, %35,6'sının bilişim suçu kavramını daha önce duymadıklarını, %75,3'ün internet bankacılığını güvenilir bulmadıklarını belirtmişlerdir. Bireylerin konuyla ilgili yeterli bilgiye sahip olmadıkları, öğrencilerin ve bilgisayar eğitimi almayanların bilişim suçu işleme oranının yüksek olduğu araştırmanın diğer sonuçlardandır. Araştırmada, bilişim suçu işleyenlerin aldıkları cezaların kamuoyuna duyurulmasının, bilişim suçlarının takibini gerçekleştirecek özel ve kamu kuruluşlarının kurulmasının, bilişim teknolojilerini iyi bilecek uzman personelin yetiştirilmesinin gerekli olduğu belirtilmiştir. Toplumun her kesimine bilişim suçları konusunda bilgilendirmelerin yapılması ve bilişim suçlarıyla nasıl mücadele edileceğinin anlatılması önerilmektedir.

Bilişim suçlarına yönelik çalışmalar genelde sosyal bilimler alanında yapılmaktadır. Bu konuya yönelik gerçekleştirilen araştırmalarda, bireylerin bazı konularda yeterli bilgiye sahip olmadıkları ve bazı eylemlerin suç olduğunu bilmedikleri ortaya çıkarılmıştır. Yapılan çalışmalarda bilişim suçlarına yönelik farkındalığın artırılmasının ve bilinçlendirme çalışmalarının gerçekleştirilmesinin gerekli olduğu belirtilmiştir.

Mart (2012) "Bilişim Kültüründe Bilgi Güvenliği Farkındalığı" adlı çalışmasında teknolojinin toplumda paylaşılmasıyla oluşan bilişim kültürü içinde bireylerin bilgi farkındalıklarını ölçen bir çalışma yapmıştır. Çalışma tarama modeli niteliğinde betimsel bir çalışmadır. Araştırmanın örneklerimini 2011-2012 yıllarında farklı meslek gruplarından (öğretmen, avukat, mühendis, sağlık personeli) oluşan 501 birey oluşturmuştur. Araştırmacı çalışmasında bilgi güvenliğini tehdit eden unsurlardan, bilişim teknolojilerinin doğuşundan ve gelişiminden, bilişim kültürünün nasıl oluştuğundan söz etmiştir. Bireylere, araştırmacı tarafından geliştirilen 60 sorudan ve 3 bölümden oluşan bilişim kültüründe bilgi güvenliği anketi uygulanmıştır. Birinci bölümde katılımcıların sosyo-demografik özelliklerini belirleyen 9, ikinci bölümde bilgi güvenliğini belirleyen 20, üçüncü bölümde teknoloji belirleyen 31 soru bulunmaktadır. Araştırma sonuçlarına göre katılımcıların bilgi güvenliği farkındalığı arasında yaşlarına, cinsiyetlerine ve mesleklerine göre anlamlı farklılık olduğu görülürken eğitim durumları, bilgisayar ve internet kullanım sürelerine göre anlamlı bir farklılık olmadığı görülmüştür. Katılımcıların bilişim kültürü ile bilgi güvenliği farkındalıkları arasında zayıf düzeyde, pozitif ve anlamlı bir ilişki olduğu tespit edilmiştir. Araştırmacı, küçük yaşlardan itibaren eğitimin verilmesi gerektiği, bilgi güvenliğinin zorunlu bir ders olarak okullarda yer alması gerektiği, seminerler, internet siteleri ve kitle iletişim araçları ile bilgi güvenliği farkındalık bilincinin oluşturulması gerektiği önerilerinde bulunmuştur.

Öğütçü (2010) "E-dönüşüm Sürecinde Kişisel Bilgi Güvenliği Davranışı ve Farkındalığın Analizi" adlı çalışmasında bireylerin bilişim güvenliğine yönelik risk içeren teknoloji kullanımlarını, kendilerini nasıl koruduklarını, her hangi bir bilişim suçuna maruz kalıp kalmadıklarını ve bazı bilişim teknolojilerini ne derece tehlikeli algıladıklarını araştırmıştır. Araştırmanın kuramsal çerçevesinde bilgi güvenliğine, bilgiyi koruma unsurlarına, bilgi güvenliğine yönelik tehditlere değinilmiştir. Araştırma kapsamında hazırlanan anket sorularına uzman görüşleri alınarak son şekli

verilmiştir. Anket, Başkent Üniversitesi öğrencileri, akademik personeli ve idari personel üzerinde uygulanmıştır. Anket formu; demografik sorular, katılımcıların bilişim teknolojileri ve bilgisayar güvenliği ile ilgili profillerinin belirlenmesine yönelik sorular, katılımcıların bilişim teknolojilerini yönelik risk içeren davranış profillerinin belirlenmesine yönelik sorular, bilişim tehditlerine yönelik korumacı davranış düzeylerini belirleyen sorular ve katılımcıların bilişim suçlarına maruziyet düzeylerinin belirlenmesine yönelik sorular olmak üzere beş bölümden oluşmuştur. Sonuçlara göre en büyük tehdidin bireyin bizzat kendisi olduğu, bireylerin bir sorun veya suç ile karşılaştıklarında hangi makama ileteceklerini bilmedikleri, konu ile güncel hukuki gelişmeleri takip etme oranın düşük olduğu, tehlike algısı arttıkça kendilerini koruma davranışlarının arttığı, risk içeren teknolojilerin kullanımı arttıkça suça maruziyet oranının da arttığı ortaya çıkmıştır. Araştırmanın sonunda bireylerin bilişim güvenliği farkındalığının artırılması gerektiği, riskleri en aza indirmenin şart olduğu, bu konularda çeşitli eğitimlerin ve kampanyaların düzenlenmesi gerektiği, bilişim savcılığı ve bilişim mahkemelerinin kurulması gerektiği belirtilmiştir.

Tekerek ve Tekerek (2013) ilköğretim ve lise düzeyinde öğrenim gören öğrencilerin bilgisayar ve internet güvenliği farkındalığını belirleyen bir çalışma gerçekleştirmişlerdir. Çalışmanın örneklemini Kahramanmaraş'ta öğrenim gören 2449 ilköğretim ve lise öğrencisi oluşturmuştur. Öğrencilere araştırmacı tarafından geliştirilen bilgi güvenliği farkındalığı ölçeği uygulanmıştır. Araştırmanın sonuçlarına göre öğrenciler güvenli şifre kullanımı, çevrimiçi güvenli iletişim, kötücül yazılım denetlemesi yapma, belge koruma, kişisel bilgisayar güvenliği, güvenlik duvarı ve filtreleme yazılımları kullanımı gibi konularda farkındalıklarının düşük olduğu görülmüştür. Ayrıca öğrenciler, bilgi güvenliği konusunda yeterli bilgiye sahip olmadıklarını belirtmişlerdir. Temel olarak öğrencilerin etik konularda yeterli bilinç düzeyine sahip oldukları fakat kurallar ve bilgi gerektiğinden konularda farkındalıklarının düşük olduğu belirlenmiştir. Bu sonuçlara göre öğrencilere, velilere ve öğretmenlere bilgi güvenliği farkındalıklarını artıracak eğitim faaliyetleri yürütülmesinin gerekli olduğu belirtilmiştir.

Tekerek ve Mart (2010) 8-14 yaşları arasında olan evrenden rastgele yöntemle 14 öğrenci seçerek bilgisayar ve internet güvenliği farkındalığını davranışsal düzeyde ölçen bir çalışma gerçekleştirmişlerdir. Görüşme yönteminin kullanıldığı çalışmada, öğrenciler sırasıyla pornografi, zararlı içerikli siteler, şiddet içerikli oyunlar, msn ve

sosyal ağlar, teknik zararlar konusunda tehlikelerle karşılaştıklarını belirtmişlerdir. Çalışmanın sonuçlarına göre; çocukların internette birçok risk ve tehlikeyle karşılaştıkları ve bunlara karşı gerekli farkındalığa sahip olmadıkları belirlenmiştir. Ayrıca yeterli bilincin oluşması için ebeveyn ve öğretmenlerin gerekli önlemleri almadıkları/alamadıkları görülmüştür.

Kınay (2012) lise öğrencilerinin siber zorbalık duyarlılığının riskli davranış, korumacı davranış, suça maruziyet ve tehlike algısı ile ilişkisini inceleyen bir araştırma gerçekleştirmiştir. Araştırmada bilgi güveniği, siber zorbalık ve bilgi güvenliği tehditlerine değinilmiştir. Çalışma genel tarama modeli türlerinden ilişkisel tarama modeli ile yürütülmüştür. Araştırmanın katılımcıları, İstanbul ilinde çeşitli ortaöğretim okullarında okuyan toplam 368 öğrenciden oluşmuştur. Araştırma sonuçlarına göre tehlike algısı ve suça maruziyetin siber zorbalığa ilişkin duyarlığı anlamlı düzeyde yordadığı görülmüştür. Erkek öğrenciler kadın öğrencilere göre bilgisayar ve internet kullanımında daha riskli davranış gösterdiği sonucuna ulaşılmıştır. Siber zorbalık duyarlık konusunda ise kadın öğrenciler erkek öğrencilere göre daha duyarlı olduğu sonucuna ulaşılmıştır. Bunların yanında erkek öğrencilerin kadın öğrencilere göre tehlike algılarının daha yüksek olduğu sonucuna ulaşılmıştır. Araştırmanın sonunda, gençlere bilgi güvenliği konusunda eğitimlerin verilmesi, bilgi güvenliği farkındalığı ve siber zorbalığa ilişkin duyarlık kazandırmak için kullanıcıların etkin olarak katıldığı interaktif sitelerin ve yazılımların hazırlanması önerilmiştir.

İlkan, İşçioğlu, Egelioğlu ve Doğanalp (2010) Akademik personelin bilgi güvenliği farkındalığını, bilgi güvenliği uygulamalarını ve bilgi güvenliği farkındalığına ve uygulamalarına karşı tutumlarını inceleyen bir araştırma gerçekleştirmişlerdir. Araştırmada; akademik personelin bilgi güvenliği farkındalığı ve uygulamalarına karşı tutumları yüksek çıkmıştır. Sonuçların yüksek çıkmasında, katılımcıların Bilgisayar ve Teknoloji Yüksekokulunda olmalarının etkili olduğu belirtilmiştir. Fakat katılımcılar, çalıştıkları kurumların politikalarından haberdar olma konusunda, şifre yönetiminde, bilgi depolamada, bilginin güvenli şekilde elden çıkarılmasında sıkıntılar yaşadıklarını belirtmişlerdir. Kısa dönemli eğitim uygulamaları ile bu sıkıntıların ortadan kaldırılabileceği önerilmiştir.

Pusey ve Sadera (2011) öğretmen adaylarının bilişim güvenliği ve bilişim etiği konusunda bilgilerini ve bu konuları öğretebilmeye yönelik durumlarını araştıran bir

çalışma gerçekleştirmişlerdir. 318 öğretmen adayına bilişim güvenliği ve etiği konularına yönelik 75 konuyu içeren sorulardan oluşan bir anket uygulanmıştır. Öğretmen adayları, kavramlardan %60'ı hakkında bilgilerinin olmadığını ya da az bilgiye sahip olduklarını, %4'ünü bildiklerini ve öğrencilerine öğretebileceklerini belirtmişlerdir. Araştırmada, öğretmen adaylarının bilişim güvenliği ve etiği konusunda sınırlı bilgilere sahip oldukları ve kendilerini bu konuları öğretmeye yetersiz buldukları sonucuna ulaşılmıştır. Öğretmen adaylarının bilişim güvenliği bilgilerini ve bilişim güvenliğine yönelik eğitim verebilme yeterliliklerini artırmak için bilişim güvenliğinin, lisans programlarında yer alması gerektiği vurgulanmıştır.

Kruger, Flowerday, Drevin ve Steyn (2011) kültürel faktörlerin bilişim güvenliği farkındalığı üzerinde etkisini inceleyen bir çalışma gerçekleştirmişlerdir. Anadil, mezun olunan okul, yaşanılan yer gibi kültürel faktörlerin bilişim güvenliği üzerinde etkisi incelenmiştir. Güney Afrika'nın iki farklı üniversitesindeki 180 katılımcıya; phishing, casus yazılım, virüs, solucan, spam şifre, sosyal mühendislik gibi saldırılar hakkında bilgilerini ve davranışlarını ölçen test uygulanmıştır. Katılımcıların virüs, spam, casus yazılım ve şifre konularını iyi bildikleri fakat sosyal mühendislik ve sosyal mühendislik kapsamındaki konuları iyi bilmedikleri görülmüştür. Katılımcıların büyük çoğunluğu sosyal mühendisliğin ne olduğunu bilmemelerine rağmen sosyal mühendislik saldırılarına karşı kişisel bilgilerini kolayca vermemeleri dikkat çeken bir sonuç olmuştur. Bu sonuç bireylerin bazı saldırı çeşitlerini bilmemelerine rağmen güvenli şekilde hareket ettiklerini göstermektedir. Çalışmada, bilişim güvenliği farkındalık programı geliştirilirken kültürel faktörlerin dikkate alınması gerektiği önerilmiştir.

Shehri (2012) farklı kültür ve bilgi birikimine sahip 35 ülkeden 200 kullanıcının internet kullanımlarını, bilişim güvenliği farkındalığını ve davranışlarını inceleyen bir araştırma gerçekleştirmiştir. Demografik bilgiler, kullanıcıların genel bilgisayar kullanımları, güvenlik davranışları, güvenlik farkındalığı sorularının bulunduğu dört bölümden oluşan sorular, forumlar ve e-posta aracılığıyla kullanıcılara ulaştırılmıştır. Lisans ve lisansüstü öğrenciler arasında güvenlik farkındalığı ve güvenlik davranışları arasında kayda değer bir farklılık olmadığı fakat güvenlik kursu alanların güvenlik konusunda iyi düzeyde farkındalığa ve bilgiye sahip oldukları tespit edilmiştir. Kullanıcıların bazı konularda iyi düzeyde farkındalığa sahip olmalarına rağmen buna uygun şekilde davranışlar sergilememeleri ve bazı güvenlik

konularında yeterli bilgiye sahip olmamaları araştırmanın dikkate alınması gereken en önemli sonuçlarındandır.

2.3 ALAN YAZIN TARAMASININ SONUCU

Yapılan çalışmalar incelendiğinde genellikle bireylerin bilişim suçları yaklaşımlarına ve algılarına, bilgi güvenliği farkındalığına ve davranışlarına yönelik araştırmaların yapıldığı görülmektedir. Bilişim güvenliğine yönelik az sayıda araştırma yapılmıştır. Araştırmalarda, bireylerin bir takım bilgi ve bilişim güvenliğini tehdit eden unsurlar konusunda farkındalıklarının ve bilgilerinin düşük düzeyde olduğu tespit edilmiştir (Dijle, 2006; Dijle ve Doğan 2011; Pusey ve Sadera, 2011; Shehri, 2012; Tekerek ve Mart, 2010; Tekerek ve Tekerek, 2013). Bireylerin farkındalıklarının ve bilgilerinin düşük düzeyde olması itibariyle okullarda küçük yaşlardan itibaren bilgi ve bilişim güvenliğine yönelik bilinçlendirme faaliyetlerine önem verilmesi gerekmektedir. Dolasıyla okullarda bilişim teknolojilerinin kullanımından ve öğretilmesinden sorumlu olacak BÖTE bölümü öğretmen adaylarının bilişim güvenliği bilgi seviyelerinin ne düzeyde olduğu ve hangi konularda yeterli oldukları önemli bir konu olarak karşımıza çıkmaktadır. Yurt dışında öğretmen adaylarının bilişim güvenliği bilgilerini ve bilişim güvenliğini yönelik eğitim verebilme yeterliliklerini inceleyen bir çalışma gerçekleştirilmiştir (Pusey ve Sadera, 2011). Ülkemizde bu konuya yönelik bir araştırma bulunmaması nedeniyle bu konuya yönelik bir araştırmanın gerçekleştirilmesi önemli görülmektedir.

BÖLÜM III

YÖNTEM

Bu bölümde araştırmanın modeli, çalışma grubu, veri toplama araçları, verilerin toplanması ve verilerin analizi ile ilgili bilgilere yer verilmiştir.

3.1 ARAŞTIRMA MODELİ

Bu çalışma, nicel araştırma yöntemlerinden tarama modeli ile gerçekleştirilmiştir. Tarama araştırmaları, bir konu veya olaya yönelik katılımcıların görüşlerinin, tutumlarının, becerilerinin, yeteneklerinin belirlendiği araştırma türü olarak bilinmektedir. Bu araştırma türünün amacı genelde var olan durumun fotoğrafını çekerek betimleme yapmaktır (Büyüköztürk, Kılıç Çakmak, Akgün, Karadeniz ve Demirel, 2012). Dolasıyla bu araştırmada, BÖTE öğretmen adaylarının bilişim güvenliği bilgileri ve bilişim güvenliğine yönelik eğitim verebilme yeterliliklerinin ne durumda olduğunun yani mevcut durumun ne olduğunun tespit edilmesi amaçlanmıştır.

3.2 ÇALIŞMA GRUBU

Bu araştırmanın çalışma grubunu, 2013-2014 eğitim-öğretim yılı Sakarya, Amasya, Erzincan ve Siirt Üniversitelerinin BÖTE bölümünde okuyan ve gönüllü olarak araştırmaya katılan 3. ve 4. sınıf öğrencileri oluşturmaktadır. Araştırma, bu üniversitelerin 3. ve 4. sınıflarında okuyan 375 lisans öğrencisi üzerinde

gerçekleştirilmiştir. Çalışma; ulaşım kolaylığı, para ve yeterli sayıda öğretmen adayına ulaşmak amacıyla belirtilen üniversitelerde gerçekleştirilmiştir. BÖTE lisans programında bulunan dersler ve araştırmanın konusu dikkate alındığında çalışmanın 3. ve 4. sınıflara uygulanması uygun görülmüştür. Çalışmanın yürütüldüğü üniversitelere ve öğrenci sayılarına Tablo 2'de yer verilmiştir.

Tablo 2. BÖTE Öğretmen Adaylarının Üniversite ve Sınıflarına Göre Dağılımları

Üniversiteler	3.Sınıf		4.Sınıf		Toplam	
	N	%	N	%	N	%
Sakarya Üniversitesi	10	3	117	31	127	34
Amasya Üniversitesi	45	13	38	10	83	22
Erzincan Üniversitesi	41	10	66	17	107	29
Siirt Üniversitesi	34	9	24	7	58	15
Toplam	130	35	245	65	375	100

Öğrencilerin yaş, cinsiyet günlük bilgisayar ve internet kullanım süreleri, sıklıkla kullandıkları bilgisayarın kime ait olduğu ve ne kadar zamandır bilgisayara sahip olduklarına yönelik bulgular ise tablo 3'te verilmiştir.

Tablo 3. BÖTE Öğretmen Adaylarının Demografik Özellikleri

Özellik	Gruplar	Frekans (f)	Yüzde (%)
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
Cinsiyet	Kadın	173	46,1
	Erkek	202	53,9
Günlük bilgisayar kullanım	1-3 saat	153	40,8

süresi	4-6 saat	134	35,7
	7 saat ve üzeri	88	23,5
Günlük internet kullanım süresi	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
Kişisel bilgisayara sahip olma yılı	2 yıl ve altı	47	125
	3 yıl	62	16,5
	4 yıl	66	17,6
	5 yıl	36	9,6
	6 yıl	22	5,9
	7 yıl	37	9,9
	8 yıl	33	8,8
	9 yıl ve üzeri	72	19,2
Sıklıkla kullanılan bilgisayarın sahibi	Kendim	361	96,3
	Anne ve Babam	1	0,3
	Üniversiteden Ödünç	2	0,5
	Internet Kafe	1	0,3
	Diğer	10	2,7

Tablo 2 ve Tablo 3'teki sonuçlara ek olarak araştırmaya katılan BÖTE öğretmen adaylarının tamamına yakının kişisel bilgisayarı bulunmaktadır.

3.3 VERİ TOPLAMA ARACI

Bu araştırmada veri toplama aracı olarak Pusey ve Sadera (2011) tarafından geliştirilen çoktan seçmeli sorulardan ve 4'lü derecelendirme özelliğine sahip olan maddelerden oluşan "Bilişim Güvenliği Bilgisi ve Bilişim Güvenliğini Yeterliliği" aracı kullanılmıştır (EK-1). Anket, uzman görüşü alınarak Türkçe'ye uyarlanmıştır. Ölçekte yer alan maddelerin kapsam geçerliliğini ve Türkçe çevirinin doğruluğunu sağlamak için uzman görüşü alınmıştır. Eğitim Fakültesi BÖTE bölümünden doktorasını tamamlamış 3, Yönetim Bilişim Sistemlerinde bilişim güvenliği konusunda doktora yapan 1, Bilişim suçları konusunda doktorasını tamamlamış 1 ve

Sakarya Emniyet Müdürlüğü Bilişim suçları biriminden 1 kişi olmak üzere toplam 6 kişiden uzman görüşü alınarak düzeltmeler ve eklemeler yapılmıştır. Uzmanlar genel olarak adayların bilişim güvenliği bilgilerini ölçen soruların ve bilişim güvenliği kavramlarına yönelik maddelerinin kapsamını yeterli bulduklarını belirtmişlerdir. Bununla beraber uzman görüşleri doğrultusunda günümüzde önemli hale gelen bilişim suçları ve mobil teknolojilerin güvenliği gibi maddelerin eklenmesi önerilmiştir. Veri toplama aracının ilk bölümünde BÖTE öğretmen adaylarının yaş, cinsiyet, sınıf, günlük bilgisayar ve internet kullanım süresi, sık kullanılan bilgisayarın sahibinin kim olduğu ve ne kadar zamandır kişisel bilgisayara sahip olduklarını belirleyen sorular bulunmaktadır. Veri toplama aracının ikinci bölümünde adayların bilişim güvenliği bilgilerini ölçen 7 çoktan seçmeli sorudan oluşan sorular bulunmaktadır. Bu sorularda adayların tahmin yürütmesini önlemek ve bilgilerinin ne olduğunu tam anlamıyla ölçmek amacıyla "bilmiyorum" seçeneğine de yer verilmiştir (Pusey ve Sadera 2011). Aracın üçüncü bölümünde; 4'lü derecelendirme özelliğine sahip olan ve 76 maddeden oluşan bilişim güvenliği ile ilgili maddeler bulunmaktadır. Pusey ve Sadera (2011) bu bölümdeki anketin 4'lü derecelendirmesini "Bu konu hakkında hiçbir şey duymadım", "Duydum. Fakat ne anlama geldiğini bilmiyorum", "Biliyorum. Fakat öğrencilerime öğretemem" ve "Biliyorum ve öğrencilerime öğretebilirim" şeklinde oluşturmuşlardır. Pusey ve Sadera (2011) güvenirlik çalışması sonucu anketin iç tutarlık katsayısı Cronbach alfa değerini 0,99 olarak bulmuşlardır. Bu çalışmada, uyarlanan aracın anket bölümünün güvenirlik çalışması sonucu, iç tutarlık katsayısı Cronbach alfa hesaplanmış ve güvenirlik katsayısı 0,96 bulunmuştur. Bu değer anketin yüksek düzeyde güvenilir olduğunu göstermektedir.

3.4 VERİLERİN TOPLANMASI

Araştırma kapsamında verilerin toplanması için Sakarya Üniversitesi Eğitim Bilimleri Enstitüsünden izin yazısı çıkarılmış ve bu izin yazısı diğer üniversitelerde verileri toplayacak öğretim elemanlarına gönderilmiştir (EK-2). Veri toplama aracı, Aralık ve Mart ayı arasında öğrencilere uygulanmıştır. Veriler toplandıktan sonra eksik veya rastgele doldurulan toplam 21 anket tespit edilerek araştırmadan çıkarılmıştır.

3.5 VERİLERİN ANALİZİ

BÖTE öğretmen adaylarının bilişim güvenliğine yönelik eğitim verebilme yeterliliklerinin tespit edildiği likert tipi anket bölümünde her madde için ortalama puanlar hesaplanmıştır. Sorulara verilen yanıtlar incelenirken ortalama puan 0 ile 1,49 arasında ise öğretmen adaylarının o konu hakkında bir şey duymadıklarını, ortalama puan 1,50 ile 2,49 arasında ise öğretmen adaylarının duyduklarını fakat ne anlama geldiğini bilmediklerini, ortalama puanı 2,50 ile 3,49 arasında ise öğretmen adaylarının bildiklerini fakat öğretebilme yeterliliğine sahip olmadıklarını düşündüklerini, ortalama puanı 3,50 ve üzeri ise öğretmen adaylarının ilgili konuları bildikleri ve öğrencilerine öğretebileceklerini düşündüklerini göstermektedir. (Pusey ve Sadera, 2011). Maddeler, ortalama puanlar göz önüne alınarak ayrı tablolar halinde verilmiştir.

BÖTE öğretmen adaylarının bilişim güvenliği bilgilerini ölçen 7 çoktan seçmeli sorular için toplam puan hesaplanmıştır. Adayların bilişim güvenliği toplam puanları incelendiğinde verilerin normal dağılım göstermediği görülmüştür. Dolasıyla verilerin analiz edilmesinde normallik varsayımının karşılanmadığı durumlarda ilişkisiz iki örneklem için Mann Whitney U-Testi kullanılmıştır (Büyüköztürk vd., 2012). Bu testle BÖTE öğretmen adaylarının bilişim güvenliği bilgisi toplam puanlarının; cinsiyet, sınıf ve bilişim güvenliğine yönelik eğitim alıp almama durumuna göre anlamlı farklılık gösterip göstermediği incelenmiştir. Yine normallik varsayımının karşılanmadığı durumlarda ikiden fazla ilişkisiz örneklem için Kruskal Wallis H-Testi kullanılmıştır (Büyüköztürk vd., 2012). Bu testle BÖTE öğretmen adaylarının bilişim güvenliği bilgisi toplam puanlarının; yaş, bilgisayara sahip olma yılı, günlük bilgisayar kullanım süresi, günlük internet kullanım süresi ve öğrenim görülen üniversiteye göre anlamlı bir farklılık gösterip göstermediği incelenmiştir. Verilerin analizinde IBM SPSS Statistics 22 programı kullanılmış ve anlamlılık düzeyi .05 olarak kabul edilmiştir.

BÖLÜM IV

BULGULAR VE YORUMLAR

Araştırmanın bu bölümde araştırma verilerinin analizinde elde edilen bulgulara ve bu bulgulara yönelik yorumlara yer verilmiştir.

4.1 BÖTE ÖĞRETMEN ADAYLARININ BİLGİSAYAR GÜNCELLEMESİNE, BİLİŞİM GÜVENLİĞİNE YÖNELİK EĞİTİM ALIP ALMAMA DURUMLARINA VE VİRÜS TARAMA YAZILIMININ GÜNCELLENME SIKLIĞINA YÖNELİK BULGULAR VE YORUMLAR

Tablo 4. Bilgisayarın Güncelleştirmesini Kimin Yaptığına Dair Bulgular

	Frekans (f)	Yüzde (%)
Kendim	355	94,7
Diğer	12	3,2
Kimse Yapmaz	8	2,1

Tablo 4 incelendiğinde BÖTE öğretmen adaylarının tamamına yakınının bilgisayarının güncellenmesini kendilerinin yaptığı görülmektedir. 8 kişi bilgisayarını güncelleştirmediği ve 12 kişi de başka birilerinin bilgisayarın güncelleştirmesini gerçekleştirdiğini belirtmişlerdir. Bu bulgulara göre, BÖTE öğretmen adaylarının okullarda bulunan laboratuvarlardaki bilgisayarların güncelleştirilmesinden sorumlu olacakları göz önüne alındığında, tamamına yakının

bu bilgisayarın güncelleştirme işini kendilerinin yaptıklarını belirtmeleri önemli bir bulgu olarak görülmektedir.

Tablo 5. Bilişim Güvenliğiyle İlgili Bir Kurs veya Ders Alma Durumlarına Yönelik Bulgular

	Frekans (f)	Yüzde (%)
Evet	114	30,4
Hayır	261	69,6

Tablo 5'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. Bilişim güvenliği eğitimi alanların %46'sı seçmeli Bilişimde güvenlik ve etik dersini aldıklarını, %19'u emniyet müdürlüğünün düzenlediği bilişim güvenliğine yönelik bilgilendirme toplantılarına katıldıklarını, %14'ü Cisco tarafından eğitim aldıklarını belirtmişlerdir. Öğütçü'nün (2010) gerçekleştirdiği çalışmasında, öğrencilerin %30,5'nin bilişim güvenliği eğitimi aldığı bulgusuna ulaşmıştır. Bu bulgular, bilişim güvenliğine yönelik bir dersin olmadığı ve bu konuya yeterli önemin verilmediği düşüncesini doğurmaktadır. Ayrıca yine bulgular, lisans programlarında bilişim güvenliğine yönelik zorunlu bir dersin olmadığını, bireylerin daha çok seçmeli dersler ve bilgilendirme toplantılarına katılarak bilgi sahibi olduklarını göstermektedir.

Tablo 6. Virüs Tarama Yazılımının Güncellenme Sıklığına Yönelik Bulgular

	Frekans (f)	Yüzde (%)
Günlük	47	12,5
Haftalık	144	38,4
Yılda bir kez	61	16,3
Sadece kurduğum zaman	31	8,3
Virüs programım yok	49	13,1
Bilmiyorum	43	11,5

Tablo 6 incelendiğinde BÖTE öğretmen adaylarının %38,4'ü virüs tarama yazılımını haftada bir kez olarak 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 belirtmişleridir. Bu bulgular, BÖTE öğretmen adaylarının virüs tarama yazılımını kısa zaman aralığında güncelliklerini göstermektedir.

4.2 BÖTE ÖĞRETMEN ADAYLARININ BİLİŞİM GÜVENLİĞİ BİLGİLERİNE YÖNELİK BULGULAR VE YORUMLAR

Bu bölümde BÖTE öğretmen adaylarının bilişim güvenliği bilgi sorularına verdikleri cevaplara yönelik bulgulara yer verilmiştir. Tablolarda soruların doğru cevapları * işareti ile belirtilmiştir.

BÖTE öğretmen adaylarının "Virüs taraması yapmadan e-posta ekini açmak … güvenlidir." sorusuna verdikleri cevaplar Tablo 7'de verilmiştir.

Tablo 7. E-Posta Ekini Açmaya Yönelik Bilgi Sorusu Bulguları

	Frekans (f)	Yüzde (%)
Güvenilir kaynaktan geldiği zaman	239	63,7
Bir banka veya ticari kuruluştan geldiği zaman	9	2,4
Konu satırı hakkınızda kişisel bilgi içerdiği zaman	9	2,4
Yukarıdakilerden hepsi	30	8,0
*Hiçbiri**	57	15,2
Bilmiyorum	31	8,3

*Doğru cevap**

BÖTE öğretmen adaylarının e-posta ekini açma sorusuna verdikleri cevaplar Tablo 7'de görülmektedir. Adaylarının yarısından fazlası (%63,7) güvenilir kaynaktan geldiği zaman virüs taraması yapmadan e-posta ekini açmanın güvenli olduğunu belirtmişlerdir. Adayların %15,2'si doğru cevap olan "hiçbiri" seçeneğini işaretlemişlerdir. Adayların %8,3'ü bilmediklerini belirtmişlerdir. Adayların %2,4'ü

bir banka veya ticari kuruluştan geldiği zaman, %2,4'ü konu satırı kendileri hakkında bilgi içerdiği zaman seçeneklerini işaretlemişlerdir. Bu bulgular, BÖTE öğretmen adaylarının e-posta eklerinin güvenliğine yönelik bilgi düzeylerinin düşük olduğunu göstermektedir.

BÖTE öğretmen adaylarının "E-Posta Ekinin İçinde Bulunan Bağlantıya (Linke) Tıklamak … Güvenlidir." sorusuna verdikleri cevaplar Tablo 8'de verilmiştir.

Tablo 8. E-Posta Eki İçindeki Bağlantıya Tıklamaya Yönelik Bilgi Sorusu Bulguları

	Frekans (f)	Yüzde (%)
Güvenilir kaynaktan geldiği zaman	239	63,7
Bir banka veya ticari kuruluştan geldiği zaman	15	4,0
Konu satırı hakkınızda kişisel bilgi içerdiği zaman	7	1,9
Yukarıdakilerden hepsi	31	8,3
*Hiçbiri**	61	16,3
Bilmiyorum	22	5,9

*Doğru cevap**

Tablo 8'de BÖTE öğretmen adaylarının e-posta eki içerisindeki bağlantıya tıklanması sorusuna verdikleri cevaplar görülmektedir. Adayların %63,7''si güvenilir kaynaktan geldiği zaman e-posta eki içinde bağlantıya tıklamanın güvenli olduğunu, %4'ü bir banka veya ticari kuruluştan geldiği zaman e-posta eki içinde bağlantıya tıklamanın güvenli olduğunu, %1,9'u konu satırı hakkınızda kişisel bilgi içerdiği zaman e-posta eki içinde bağlantıya tıklamanın güvenli olduğunu, %8,3'ü yukarıdaki seçeneklerin hepsinin güvenli bir yöntem olduğunu, %16,3'ü doğru cevap olan hiçbirinin güvenli olmadığını, %5,9'u bilmediklerini belirtmişlerdir. Bu bulgular, BÖTE öğretmen adaylarının e-posta eki içerisindeki bağlantıya tıklama güvenliğine yönelik bilgi düzeylerinin düşük olduğunu göstermektedir.

BÖTE öğretmen adaylarının Proxy sunucusunun görevine yönelik soruya verdikleri cevaplar Tablo 9'de verilmiştir.

Tablo 9. Proxy Sunucunun Görevine Yönelik Bilgi Sorusu Bulguları

	Frekans (f)	Yüzde (%)
Çocukları çevrimiçi müstehcen içerikten korur.	45	12,0
Çocukların okulda internet filtrelerini atlamalarına izin verir.	27	7,2
Web Siteleri için güvenli şifre oluşturur.	113	30,1
*Yukarıdakilerden hepsi**	60	16,0
Hiçbiri	21	5,6
Bilmiyorum	109	29,1

*Doğru cevap**

Tablo 9'da BÖTE öğretmen adaylarının Proxy sunucuların görevinin ne olduğuna yönelik soruya verdikleri cevaplar görülmektedir. Adayların %12'si çocukları çevrimiçi müstehcen içerikten koruduğunu, %7,2'si çocukların okulda internet filtrelerini atlamalarında izin verdiğini, %30,1'i web siteleri için güvenli şifre oluşturduğunu, %16'sı yukarıdaki seçeneklerin hepsini sağladığını, % 5,6'sı hiçbir seçeneğin Proxy sunucusunun görevi olmadığını, %29,1'i görevinin ne olduğunu bilmediklerini belirtmişlerdir. Proxy sunucusu ilk üç seçenekteki özellikleri gerçekleştirmektedir. Dolayısıyla bu bulgular, öğretmen adaylarının Proxy sunucusunu işlevleri konusunda eksik bilgiye sahip olduklarını göstermektedir. Ayrıca bilmiyorum seçeneğini işaretleyenlerin oranına bakıldığında (%29,1) konu hakkında bilgi sahibi olmayanların oranın beklenenden yüksek olduğu görülmektedir.

BÖTE öğretmen adaylarının Yeni pencerede (ekranda) açılan reklam pencerelerinin (Pop-up Ads) ne zaman görüntülendiğine yönelik soruya verdikleri cevaplar Tablo 10'da verilmiştir.

Tablo 10. Reklam Pencerelerine (Pop-Up Ads) Yönelik Bilgi Sorusu Bulguları

	Frekans (f)	Yüzde (%)
Web sitelerinde sörf yaparken görüntülenir.	146	38,9
Web sitelerini ziyaret ettikten sonra görüntülenir.	52	13,9
Internet tarayıcısı açıldığı zaman görüntülenir.	50	13,3
Yukarıdakilerden hepsi	73	19,5

*Hiçbiri**	14	3,7
Bilmiyorum	40	10,7

*Doğru cevap**

Tablo 10'da BÖTE öğretmen adaylarının reklam pencerelerinin (Pop-up Ads) görüntülenmesine yönelik soruya verdikleri cevaplar görülmektedir. Adayların %38.9'u web sitelerinde sörf yaparken görüntülendiğini, %13,9'u web sitelerini ziyaret ettikten sonra görüntülendiğini, %13,3'ü internet tarayıcısı açıldığı zaman görüntülendiğini, %19,5'i yukarıdaki seçeneklerde yapılan her işlemin bu pencerelerin görüntülenmesine neden olduğunu, %3,7'si yukarıdaki belirtilen işlemlerin bu pencerelerin görüntülenmesine neden olmadığını, %10,7'si bilmediklerini belirtmişlerdir. Reklam pencerelerin güvenli olmayan sitelerde gezinirken veya güvenli olmayan bir bağlantıya tıklanınca görüntülendiği göz önüne alındığında doğru olan "hiçbiri" seçeneğini işaretleyenlerin yüzdesinin (%3,7) düşük çıktığı görülmektedir.

BÖTE öğretmen adaylarının USB/Flash bellek gibi taşınabilir veri depolama aygıtları ne tür amaçlar için kullanılabileceğine yönelik soruya verdikleri cevaplar Tablo 11'de verilmiştir.

Tablo 11. Taşınabilir Veri Depolama Aygıtlarında Saklanan Verilere Yönelik Bilgi Sorusu Bulguları

	Frekans (f)	Yüzde (%)
Öğrenci isimleri, adresleri, test puanları gibi verileri	12	3,2
Öğrenci çalışmalar	65	17,3
Bireylerin eğitim planlari	8	2,1
Yukarıdakilerden hepsi	275	73,3
*Hiçbiri**	11	2,9
Bilmiyorum	4	1,1

*Doğru cevap**

Tablo 11'de USB/Flash bellek gibi taşınabilir aygıtların ne tür amaçlar için kullanılabileceğine yönelik soruya verdikleri cevaplar görülmektedir. Adayların büyük çoğunluğu (%73,3) bu taşınabilir aygıtların öğrencilerin kişisel bilgilerini,

öğrencilerin çalışmalarını ve bireylerin eğitim planları gibi verileri depolamak için kullanılabileceğini belirtmişlerdir. Çok düşük oranda aday (%2,9) doğru seçenek olan "Hiçbiri" şeçeneğini işaretlemişlerdir. Bu bulgular, adayların USB/Flash bellek gibi taşınabilir aygıtlar ile öğrencilerin kişisel bilgilerinin, çalışmalarının taşınmasının bir suç olduğunu bilmediklerini göstermektedir.

BÖTE öğretmen adaylarının Güvenlik duvarının görevine yönelik soruya verdikleri cevaplar Tablo 12'de verilmiştir.

Tablo 12. Güvenlik Duvarının Görevine Yönelik Bilgi Sorusu Bulguları

	Frekans (f)	Yüzde (%)
Bir bilgisayara izinsiz girişi önler.	84	22,4
Bilgisayardan gönderilen yetkisiz bir bilgiyi engeller.	92	24,5
*Yukarıdakilerden hepsi**	179	47,7
Hiçbiri	8	2,1
Bilmiyorum	12	3,2

*Doğru cevap**

Tablo 12'de BÖTE öğretmen adayların güvenlik duvarının görevine yönelik soruya verdikleri cevaplar görülmektedir. Adayların %22,4'ü güvenlik duvarının bir bilgisayara izinsiz girişi önlediğini, % 24,5'i bilgisayardan gönderilen yetkisiz bilgiyi engellediğini, %47,7'si iki seçeneği de gerçekleştirdiğini, %2,1'i hiçbirinin güvenlik duvarının görevi olmadığını, %3,2'si güvenlik duvarının görevinin ne olduğunu bilmediklerini belirtmişlerdir. Güvenlik duvarı, bir bilgisayara dışardan yetkisiz bir girişi ve izinsiz bilgi akışını önleyen bir yazılımdır. Dolayısıyla bu bulgular, bazı adayların güvenlik duvarının görevinin tam olarak ne olduğu konusunda eksik bilgilerinin olduğunu göstermektedir. Katılımcıların yaklaşık yarısı bu soruyu doğru cevaplamışladır.

BÖTE öğretmen adaylarının şifrelerin nasıl olması gerektiğine yönelik soruya verdikleri cevaplar Tablo 13'de verilmiştir.

Tablo 13. Şifrelerin Nasıl Olması Gerektiğine Yönelik Bilgi Sorusu Bulguları

	Frekans (f)	Yüzde (%)
Tüm hesaplar için aynı	57	15,2
*Küçük-büyük harflerin ve numaraların karışımı**	261	69,6
Gerçek kelimeler	11	2,9
Yukarıdakilerden hepsi	33	8,8
Hiçbiri	13	3,5

*Doğru cevap**

Tablo 13'te BÖTE öğretmen adaylarının şifrelerin nasıl olması gerektiği konusuna verdikleri cevaplar görülmektedir. Adaların büyük çoğunluğu (69,6) şifrelerin küçük-büyük harflerin ve numaraların karışımı olması, %15,2'si aynı olması, %2,9'u gerçek kelimelerden oluşması gerektiğini belirtmişlerdir. Bu bulgular, adayların çoğunun güvenli şifrelerin nasıl olması gerektiği konusunda bilgi sahibi olduklarını göstermektedir. Ancak yaklaşık %30'luk kesimin bu konuda bilgilendirmeye ihtiyaç duyduğu düşünülmektedir.

4.3 BÖTE ÖĞRETMEN ADAYLARININ BİLİŞİM GÜVENLİĞİNE YÖNELİK EĞİTİM VEREBİLME YETERLİLİĞİNE YÖNELİK BULGULAR VE YORUMLAR

Bu bölümde betimleyici istatistikten yararlanarak BÖTE öğretmen adaylarının bilişim güvenliği konularına yönelik verdikleri cevapların ortalama değerlerine yer verilmiştir. Bulguların yorumlanmasında Pusey ve Sadera'nın (2011) ölçütleri dikkate alınarak ortalama değeri 3,50 ve üzeri olan konular BÖTE öğretmen adaylarının öğretebileceklerini düşündükleri, ortalama değeri 2,50 ile 3,49 arasında olan konular BÖTE öğretmen adaylarının bildikleri fakat öğretebilecek yeterliliğe sahip olmadıklarını düşündükleri, ortalama değeri 2,49 ile 1,50 arasındaki konular BÖTE öğretmen adaylarının duydukları fakat ne anlama geldiğini bilmedikleri, ortalama değeri 1,49 ve altında olanlar konular ise BÖTE öğretmen adaylarının duymadıkları şeklinde değerlendirilmiştir. Bulgular ayrı tablolar halinde sunulmuştur.

4.3.1 BÖTE Öğretmen Adaylarının Hakkında Hiçbir Şey Duymadıkları Konular

BÖTE öğretmen adaylarının bilişim güvenliğine yönelik konularda ortalama değeri 1,49 ve altında hiçbir konu bulunmamıştır. Bu bulgular, BÖTE öğretmen adaylarının en azından ankette yer alan sorularla ile ilgili bir şeyler duyduklarını göstermektedir. Adayların duymadıkları konuların olmaması yeterli olmasa da olumlu bir bulgudur.

4.3.2 BÖTE Öğretmen Adaylarının Duydukları Fakat Ne Anlama Geldiğini Bilmedikleri Konular

Tablo 14. BÖTE Öğretmen Adaylarının Duydukları Fakat Ne Anlama Geldiğini Bilmedikleri Konular

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

Tablo 14 incelendiğinde BÖTE öğretmen adaylarının duydukları fakat ne anlama geldiğini bilmedikleri konuların daha çok teknik bilgi gerektiren konular olduğu görülmektedir. Bu bulgular, BÖTE öğretmen adaylarının teknik bilgi gerektiren konuların bazılarını bilmediklerini göstermektedir. Özellikle BÖTE öğretmen adaylarının İntihal'in ne anlama geldiğini bilmemeleri dikkat çeken bir bulgudur. Hâlbuki Associaton for Educational Communications and Technology (AECT, 2012) bilgi teknolojilerinin kullanılmasında özellikle etik kullanıma vurgu yapmaktadır. Bunun yanında öğretmen adaylarının günümüzde sıklıkla duyduğumuz bot ve botnetler, sosyal mühendislik, DoS saldırıları ve adware konularında bilgi sahibi olmamaları dikkate alınması gereken bulgular olarak görülmektedir.

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

Tablo 15. BÖTE Öğretmen Adaylarının Bildikleri Fakat Öğrencilerine Öğretebilecek Yeterliliğe Sahip Olmadıklarını Düşündükleri Konular

Konular	N	$\overline{X}$	SS
Şifreler	375	3,46	0,80
Kablosuz Aygıt Güvenliği	375	3,45	0,85
Çevrimiçi Oyunlar	375	3,44	0,84
Spam	375	3,44	0,82
Portlar	375	3,44	0,91
Güvenlik Ayarları	375	3,43	0,91
Güvenli Çocuk Portalları	375	3,41	0,86
Web Kamera Güvenliği	375	3,40	0,88
Korsan Yazılım	375	3,39	0,75
Sosyal Ağ Güvenliği	375	3,38	0,85
Mobil Teknoloji Güvenliği	375	3,36	0,90
Profil Denetimi	375	3,34	0,92
E-posta Ekleri	375	3,32	0,93
Kaçak Yazılım Kullanma	375	3,29	0,82
Adil Kullanım	375	3,25	0,99
Şifreleme (Encryption)	375	3,25	0,93

Blog Güvenliği	375	3,24	0,95
Karalama / İftira / Hakeret	375	3,24	0,94
Çerezler (Cookies)	375	3,24	0,95
Erişim İzni	375	3,20	0,94
Son Kullanıcı Lisans Sözleşmesi	375	3,20	0,98
Zamanını Doldurmuş Eski Teknolojilerin Elden Çıkarılması	375	3,14	0,99
Screenlogger (Ekran Kaydediciler)	375	3,13	1,00
İnternet Filtreleri	375	3,13	0,95
Gizli Arşiv Dosyaları	375	3,12	0,96
Metin Mesaj Güvenliği	375	3,11	1,04
Siber Zorbalık	375	3,10	1,03
Önbelleğe Yüklenmiş Web Siteler	375	3,09	0,98
Spam Filtreleme	375	3,08	1,03
Değiştirilmiş Dijital Fotoğraflar	375	3,05	0,93
Reklam İçerikli Pencereler (Pop-Up Ads)	375	3,04	1,00
Sabit Diski Olan Fotokopi Makinelerinin ve Tarayıcıların Güvenliği	375	3,04	1,04
Yamalar	375	2,97	1,06
Casus Yazılım (Spyware)	375	2,91	0,98
Tuş Kaydediciler (Keylogger)	375	2,90	1,07
Bilişim Korsanlığı (Hacking)	375	2,89	0,94
Dijital Sertifikalar	375	2,88	0,98
Şifrelenmemiş e-mail	375	2,87	1,06
Çevrimiçi Kimlikler	375	2,78	1,08
Hijack (Çalmak / Gasp / Hırsızlık)	375	2,75	1,06
Proxy (Vekil Sunucu)	375	2,74	1,04
İzinsiz Yayınlama / Yasadışı Yayın	375	2,70	1,04
Kimlik Hırsızlığı	375	2,66	1,06
Takip Edilen Çerezler	375	2,64	1,13
MEB Bilgi ve Sistem Güvenliği Yönergesi	375	2,54	1,17
5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Kanunu	375	2,54	1,12
Filtre Atlama	375	2,51	1,06
Çevrimiçi Kumar	375	2,50	1,14

Tablo 15'te BÖTE öğretmen adaylarının bildikleri fakat öğrencilerine öğretebilecek yeterliliğe sahip olmadıklarını düşündükleri konulara yer verilmiştir. Tablo 15 incelendiğinde her konunun ayrı bir öneme sahip olduğu görülmektedir. BÖTE öğretmen adaylarının bu konuları bilmelerine rağmen öğrencilerine öğretebilecek yeterliliğe sahip olmadıklarını belirtmeleri, BÖTE lisans öğretim programında bilişim güvenliğine 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, keylogger gibi önemli konuları öğretebilecek yeterliliğe sahip olmadıklarını belirtmeleri, bilişim güvenliğine yönelik eğitimlerin verilmesinin gerekli olduğunu göstermektedir. Dolayısıyla adaylarının büyük çoğunluğunun (%69,6) bilişim güvenliğine yönelik bir ders veya kurs almadıkları göz önüne alındığında, adayların birçok konuda kendini yeterli görmemeleri doğal bir sonuç olarak görülmektedir. Ayrıca öğretmen adaylarının öğretebilecek yeterliliğe sahip olmadıklarını belirtikleri konuların fazla olmasında, bu derste konuların güvenlikle ilgili boyutuna yeterince değinilmemesinin etkili olabileceği düşünülmektedir.

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

Tablo 16. BÖTE Öğretmen Adaylarının Bildikleri ve Öğrencilerine Öğretebilecek Yeterliliğe Sahip Olduklarını Düşündükleri Konular

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

Güvenlik Duvarı	375	3,52	0,78

Tablo 16'da BÖTE öğretmen adaylarının bildikleri ve öğrencilerine öğretebileceklerini düşündükleri konulara yer verilmiştir. Tablo 16 incelendiğinde adayların toplam 76 konu arasından sadece 11 konu hakkında kendilerini yeterli gördükleri anlaşılmaktadır. Bu bölümden mezun olacak adayların ileride görev alacakları okullarda diğer öğretmen ve öğrencilere rehberlik edecekleri ve güvenlik konusuna yönelik eğitim verecekleri göz önüne alındığında, yeterli oldukları 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 dikkate alınması gereken bir bulgu olarak görülmektedir.

4.4 ÇEŞİTLİ DEĞİŞKENLERE GÖRE BÖTE ÖĞRETMEN ADAYLARININ BİLİŞİM GÜVENLİĞİ BİLGİLERİNE İLİŞKİN BULGULAR VE YORUMLAR

Bu bölümde BÖTE öğretmen adaylarının bilişim güvenliği bilgilerinin; yaşa, cinsiyete, sınıfa, öğrenim görülen üniversiteye, bilişim güvenliğine yönelik bir ders veya kurs alınıp alınmama durumuna, günlük bilgisayar kullanım süresine, günlük internet kullanım süresine ve ne kadar süredir bilgisayara sahip olma durumuna göre anlamlı farklılık gösterip göstermediğine yönelik bulgulara yer verilmiştir.

4.4.1 Yaş Değişkenine İlişkin Bulgular ve Yorumlar

Tablo 17. Bilişim Güvenliği Bilgisinin Yaş Değişkenine Göre Kruskal Wallis Sonucu

Yaş	N	Sıra Ortalaması	sd	χ^2	p
20	27	206.00	5	7.45	.189
21	96	179.86			
22	115	180.50			

23	86	183.53
24	35	226.66
25 ve üzeri	16	199.84

Tablo 17 incelendiğinde, adayların bilişim güvenliği testinden aldıkları puanların, yaşlarına bağlı olarak anlamlı farklılık göstermemektedir [χ^2 (sd=5, n=375) =7.45, p>.05]. Bu bulgu, yaşın öğretmen adaylarının bilişim güvenliği bilgilerinde bir farklılığa neden olmadığını göstermektedir.

4.4.2 Cinsiyet Değişkenine İlişkin Bulgular ve Yorumlar

Tablo 18. Bilişim Güvenliği Bilgisinin Cinsiyete Göre U-Testi Sonucu

Cinsiyet	N	Sıra Ortalaması	Sıra Toplamı	U	p	*d*
Kadın	173	170.48	29492.50	14441.50	.002	0.15
Erkek	202	203.01	41007.50			

Öğretmen adaylarının bilişim güvenliği testinden aldıkları puanların Mann Whitney U-testi sonuçları Tablo 18'de verilmiştir. Tablo 18'de adayların bilişim güvenliği bilgi puanlarının cinsiyete göre anlamlı farklılık gösterdiği görülmektedir [U:14441.50, p<.05]. Ayrıca *d* = 0,15 hesaplanmıştır. Bu değer 0,2 den küçük olduğu için etki büyüklüğünün düşük seviyede olduğu söylenebilir (Green ve Salkind, 2008). Sıra ortalamaları dikkate alındığında, erkek öğretmen adaylarının kadın öğretmen adaylarına göre bilişim güvenliği bilgi puanlarının daha yüksek olduğu anlaşılmaktadır. Yani bilişim güvenliği açısından erkekler daha yeterlidir.

4.4.3 Bilişim Güvenliğine Yönelik Bir Eğitim Alıp Almama Değişkenine İlişkin Bulgular ve Yorumlar

Tablo 19. Bilişim Güvenliği Bilgisinin Bilişim Güvenliğine Yönelik Eğitim Alıp Almama Durumuna Göre U-Testi Sonucu

Grup	N	Sıra Ortalaması	Sıra Toplamı	U	p
Evet	114	194.21	22139.50	14169.50	.437

Hayır	261	185.29	48360.50

Tablo 19 incelendiğinde adaylarının bilişim güvenliği bilgi puanları, bu konuya yönelik herhangi bir eğitim alıp almama durumlarına göre anlamlı farklılık göstermemektedir [U:14169.50, p>.05]. Sıra ortalamalarına bakıldığında, bilişim güvenliğine yönelik eğitim alanlar ile almayanlar arasında çok büyük bir fark olmadığı görülmektedir. Bu bulgu, bilişim güvenliğine yönelik eğitim alan adayların bilgi düzeylerinin, bu eğitimleri almayan adayların bilgi düzeylerine göre bir farklılaşma oluşturmadığını göstermektedir. Ayrıca yine bu bulgulara göz önüne alınarak bilişim güvenliğine yönelik verilen eğitimlerin, adayların bilgilerini ve yeterliliklerini artıracak bir düzeyde ve içerikte olmadığı yönünde bir yorum yapılabilir. Ancak bu bulgunun daha iyi anlaşılabilmesi için katılımcıların aldıkları dersler olarak hangi dersleri belirtiklerinin tespit edilmesini sağlayacak nitel bulgulara ihtiyaç duyulmaktadır.

4.4.4 Sınıf Değişkenine İlişkin Bulgular ve Yorumlar

Tablo 20. Bilişim Güvenliği Bilgisinin Sınıf Değişkenine Göre U-Testi Sonucu

Sınıf	N	Sıra Ortalaması	Sıra Toplamı	U	p
3	130	182.73	23754.50	15239.50	.467
4	245	190.80	46745.50		

Tablo 20'de adayların bilişim güvenliği bilgilerinin sınıf değişkeni göre anlamlı farklılık oluşturup oluşturmadığına yönelik bulgulara yer verilmiştir. Tablo 20 incelendiğinde adayların bilişim güvenliği bilgilerinin sınıf düzeyine göre anlamlı farklılık oluşturmadığı görülmektedir [U:15239.50, p>.05]. Bu bulgu, sınıf düzeyinin öğretmen adaylarının bilişim güvenliği bilgilerinde bir farklılığa neden olmadığını göstermektedir. Bu bulgu, hali hazırdaki lisans programlarında bilişim güvenliğine yönelik bir dersin olmayışının bu sonucu doğurduğu şeklinde yorumlanabilir. Çünkü 3. ve 4. sınıftaki dersler arasında bilişim güvenliği bilgisi çıktılarını hedefleyen doğrudan bir ders bulunmaktadır.

4.4.5 Günlük Bilgisayar Kullanım Süresi Değişkenine İlişkin Bulgular ve Yorumlar

Tablo 21. Bilişim Güvenliği Bilgisinin Günlük Bilgisayar Kullanım Süresi Değişkenine Göre Kruskal Wallis Sonucu

Günlük Bilgisayar Kullanım Süresi	N	Sıra Ortalaması	sd	χ^2	p
1-3 saat	153	180.95	2	1.25	.536
4-6 saat	134	192.10			
7 saat ve üzeri	88	194.01			

Adayların günlük bilgisayar kullanım sürelerine göre bilişim güvenliği testinden aldıkları puanların Kruskall Wallis testi sonuçları Tablo 21'de verilmiştir. Tablo incelendiğinde, adayların bilişim güvenliği testinden aldıkları puanların, günlük bilgisayar kullanım süresine göre anlamlı farklılık göstermediği görülmektedir [χ^2 (sd=2, n=375) =1.25, p>.05.]. Bu bulgu, öğretmen adaylarının günlük bilgisayar kullanım süresinin adayların bilişim güvenliği bilgilerinde her hangi bir farklılaşma yaratmadığını göstermektedir. Yani bilgisayarı az yada çok kullanmak bilişim güvenliği farkındalığını değiştirmemektedir.

4.4.6 Günlük Internet Kullanım Süresi Değişkenine İlişkin Bulgu ve Yorumlar

Tablo 22. Bilişim Güvenliği Bilgisinin Günlük Internet Kullanım Süresi Değişkenine Göre Kruskal Wallis Sonucu

Günlük Internet Kullanım Süresi	N	Sıra Ortalaması	sd	χ^2	p
1 saatten az	55	175.38	3	2.59	.458
2-3 saat	163	187.39			
4-6 saat	106	199.67			
7 saat ve üzeri	51	179.32			

Tablo 22 incelendiğinde, adayların bilişim güvenliği testinden aldıkları puanların, günlük internet kullanım süresine göre anlamlı farklılık göstermediği görülmektedir [χ^2 (sd=3, n=375) =2.59, p>.05]. Bu bulgu, günlük internet kullanım süresinin

öğretmen adayların bilişim güvenliği bilgilerinde her hangi bir farklılaşma yaratmadığını göstermektedir.

4.4.7 Öğrenim Görülen Üniversitelere İlişkin Bulgu ve Yorumlar

Tablo 23. Bilişim Güvenliği Bilgisinin Öğrenim Görülen Üniversite Değişkenine Göre Kruskal Wallis Sonucu

Üniversiteler	N	Sıra Ortalaması	sd	χ^2	p	Anlamlı Fark	η^2
Erzincan	107	173.97	3	14.16	.003	Sakarya > Erzincan Sakarya > Siirt	0.53
Siirt	58	153.61				Amasya > Siirt	
Amasya	83	204.00					
Sakarya	127	205.07					

Tablo 23 incelendiğinde, adayların bilişim güvenliği testinden aldıkları puanların, öğrenim gördükleri üniversitelere göre anlamlı farklılık gösterdiği görülmektedir [χ^2 (sd=3, n=375) =14.16, p<.05]. Grupların sıra ortalamalarına bakıldığında, Sakarya Üniversitesinde okuyan öğrencilerin bilişim güvenliği bilgilerinin en yüksek değere sahip olduğu, bu üniversiteyi sırasıyla Amasya, Erzincan ve Siirt Üniversitelerinin takip ettiği görülmektedir. Anlamlı farklılığın hangi üniversiteler arasında olduğuna bakıldığında ise Sakarya Üniversitesi ile Erzincan Üniversitesi, Sakarya Üniversitesi ile Siirt Üniversitesi, Amasya Üniversitesi ile Siirt Üniversitesi arasında olduğu belirlenmiştir. Ayrıca η^2 = 0,53 hesaplanmıştır. Bu değer .14 den büyük olduğu için etki büyüklüğünün yüksek seviyede olduğu söylenebilir (Green ve Salkind, 2008). Bu bulgular, öğrenim görülen üniversitenin öğretmen adaylarının bilişim güvenliği bilgilerine etki ettiğini göstermektedir. İleride yapılacak çalışmalarda bu farklılığı oluşturan nedenleri belirlemeye yönelik çalışmalar yapılabilir.

4.4.8 Bilgisayar Sahiplik Yılı Değişkenine İlişkin Bulgu ve Yorumlar

Tablo 24. Bilişim Güvenliği Bilgisinin Bilgisayar Sahiplik Yılı Değişkenine Göre Kruskal Wallis Sonucu

Bilgisayara Sahip Olma Süresi	N	Sıra Ortalaması	sd	χ^2	p
2 yıl ve altı	47	179.09	7	7.94	.337
3 yıl	62	170.40			
4 yıl	66	172.35			
5 yıl	36	203.51			
6 yıl	22	220.45			
7 yıl	37	193.46			
8 yıl	33	198.27			
9 yıl ve üzeri	72	198.14			

Adayların bilgisayara sahip olma yıllarına göre bilişim güvenliği testinden aldıkları puanların Kruskall Wallis testi sonuçları Tablo 24'te verilmiştir. Tablo incelendiğinde, adayların bilişim güvenliği bilgi puanlarının, bilgisayara sahip olma yılına göre anlamlı farklılık göstermediği görülmektedir [χ^2 (sd=7, n=375) =7.94, p>.05]. Bu bulgu, öğretmen adaylarının bilgisayara sahip olma yıl süresinin bilişim güvenliği bilgilerinde her hangi bir farklılaşma yaratmadığını göstermektedir.

BÖLÜM V

SONUÇLAR, TARTIŞMA VE ÖNERİLER

5.1 SONUÇLAR VE TARTIŞMA

Bu araştırmada BÖTE öğretmen adaylarının bilişim güvenliği bilgileri ve bilişim güvenliğine yönelik eğitim verebilme yeterliliklerinin belirlenmesi amaçlanmıştır. Araştırmada, BÖTE öğretmen adaylarının tamamına yakınının kişisel bilgisayara sahip olduklarını, kişisel bilgisayara sahip olma yılının 2 ile 8 yıl arasında değiştiğini ve bilgisayar güncelleştirmelerini kendilerinin yaptıklarını gösteren sonuçlara ulaşılmıştır. Bu sonuçlar göz önüne alındığında, özellikle BÖTE öğretmen adaylarının okullarda bilgisayarların ve teknolojilerin kullanımından sorumlu olacakları düşünüldüğünde, bilgisayar güncelleştirmelerini kendilerinin yapabilmeleri beklenen bir durum olsa da önemli bir sonuç olarak görülmektedir.

Öğretmen adaylarının günlük bilgisayar kullanım süresi sonuçlarına bakıldığında, adaylarının büyük çoğunluğunun (% 76.5) günlük bilgisayar kullanım süresinin 4 saatinde üzerinde olduğu tespit edilmiştir. Mart (2012) farklı meslek gruplarından bireyler üzerinde gerçekleştirdiği çalışmasında da bireylerin günlük bilgisayar kullanımını 4 saatin üzerinde olduğu sonucuna ulaşmıştır. Benzer bir şekilde İlkan vd. (2010) akademik personel üzerinde gerçekleştirdiği çalışmasında akademik personelin günde 4 saat ve üzerinde bilgisayar kullandıkları sonucuna ulaşmışlardır. Yapılan araştırmalar dikkate alındığında, bireylerin günlük bilgisayar kullanım süresinin genellikle 4 saatten fazla olduğu görülmektedir.

Bu araştırmada, öğretmen adaylarının günlük internet kullanım süresi sonuçlarına bakıldığında ise 2-3 saat ile 4-6 saat arasında yoğunlaştığı sonucuna ulaşılmıştır.

Adayların okudukları bölüm ve aldıkları dersler göz önüne alındığında bu sonuçların beklenen seviyede olduğu düşünülmektedir. İlkan vd. (2010) gerçekleştirdikleri çalışmalarında akademik personelin günlük internet kullanım süresinin 1 ile 4 saat arasında yoğunlaştığını tespit etmişlerdir. 2013 yılında gerçekleştirilen bir proje sonuçlarına göre ise, öğrencilerin yarısı günde 1 saatten fazla zamanını internet ortamında geçirmektedirler (Güvenli ve Bilinçli Internet Kullanım Projesi, 2013). Mert vd. (2012) 8. sınıflar üzerinde gerçekleştirdikleri çalışmalarında, öğrencilerin günde internette geçirdikleri zamanının 30 dakika-1 saat aralığında en yüksek orana sahip olduğu tespit edilirken, bu saat aralığının üzerinde ve altındaki oranın düşük olduğu sonucuna ulaşmışlardır. Gerçekleştirilen araştırma sonuçları göz önüne alındığında günlük internet kullanım süresinin farklılık gösterdiği görülmektedir. Bu farklılık internet kullanım amaçlarına, ihtiyaçlara, internet bağlantısını olup olmamasına, mesleklere, cinsiyetlere vb. daha birçok duruma göre değişebileceğini düşündürmektedir. TUİK'in her yıl gerçekleştirdiği araştırma sonuçları incelendiğinde ise, ülkemizde her yıl internet erişiminin ve internet kullanımının arttığı görülecektir (TUİK, 2013). Ayrıca Internet World Stats (2012) istatistiklerinde Türkiye'nin internet kullanıcısı sayısında dünyada 5. sırada yer alması ülkemizde internet kullanımının arttığını destekler niteliktedir.

5.1.1 BÖTE Öğretmen Adaylarının Bilişim Güvenliği Bilgilerine Yönelik Sonuçlar ve Tartışma

BÖTE öğretmen adaylarının bilişim güvenliğine yönelik bir ders veya kurs alıp almadıklarına yönelik sonuçlara bakıldığında; adayların %69.6'sının bu konuya yönelik herhangi bir ders veya kurs almadıkları, %30.4'ünün bilişim güvenliğini sağlamaya yönelik eğitim aldıklarını belirtikleri görülmüştür. Öğütçü (2010) akademik personel, idari personel ve öğrenciler üzerinde gerçekleştirdiği araştırmasında, bireylerin %22.36'sının güvenlik eğitimi aldıkları, % 77.64'ünün ise güvenlik eğitimi almadıkları sonucuna ulaşmıştır. Aynı çalışmada öğrencilerin güvenlik eğitim alıp almadıklarına yönelik sonuçlar incelendiğinde ise, öğrencilerin %30.46'ünün güvenlik eğitimi aldıkları sonucuna ulaşılmıştır. Bu sonuçlar; bilişim güvenliğini sağlamaya yönelik eğitimlerin çok az olduğunu, güvenliği sağlamaya yönelik sistematik bir yaklaşımın olmadığını ve bireylerin bu konularda yeterli

düzeyde eğitim almadıklarını göstermektedir. Ayrıca öğretmen yetiştirme programlarına bakıldığında, bilişim güvenliğine yönelik bir dersin olmadığı görülmektedir. Clinton (2009) bireylerin güvenliğini sağlayacak uygulamaya dönük, etkili ve davranış değişikliği yaratacak eğitim programlarının yer alması gerektiğini ve bu konuya yönelik yatırımların yapılması gerektiğini belirtmektedir. Ayrıca eğitimcilerin kendilerini bu konularda hazırlamalarının bir ihtiyaç olduğunu vurgulamaktadır. Dolasıyla bireylerin bilişim teknolojilerini ve interneti güvenli bir şekilde kullanmalarını sağlayacak eğitimlerin, seminerlerin veya çalışmaların gerçekleştirilmesinin faydalı sonuçlar doğuracağı düşünülmektedir.

Bu çalışmada BÖTE öğretmen adaylarının bilişim güvenliği bilgi sorularına verdikleri cevaplar incelendiğinde, adayların bilgi düzeylerinin düşük olduğu sonucuna ulaşılmıştır. BÖTE öğretmen adaylarının bilişim güvenliği bilgileri; cinsiyet ve öğrenim görülen üniversiteye göre değiştiği tespit edilmiştir. BÖTE erkek öğretmen adaylarının bilişim güvenliği bilgilerinin kadın öğretmen adayların bilişim güvenliği bilgilerine göre daha yüksek olduğu sonucuna ulaşılmıştır. Benzer şekilde Mart (2012) gerçekleştirdiği araştırmasında katılımcıların bilgi güvenliği farkındalığının cinsiyete göre farklılaştığı sonucuna ulaşmıştır. Fakat Mart'ın (2012) araştırmasında kadın katılımcıların bilgi güvenliği farkındalığı erkek katılımcılara göre daha yüksek çıkmıştır. Mart (2012) araştırmasını mühendis, avukat vb. farklı meslek grubundan bireyler üzerinde gerçekleştirmesi bu farklılığın oluşmasında etkili olabileceği düşünülmektedir. Yine araştırma sonuçlarına göre, Sakarya Üniversitesinde okuyan BÖTE öğretmen adaylarının bilişim güvenliği bilgi düzeylerinin diğer üç üniversitede okuyan BÖTE öğretmen adayların bilgi düzeylerine göre daha yüksek çıktığı sonucuna ulaşılmıştır.

BÖTE öğretmen adaylarının bilişim güvenliği bilgilerinin; yaşa, bilgisayar sahiplik yılına, sınıf düzeyine, günlük bilgisayar kullanım süresine, günlük internet kullanım süresine ve bilişim güvenliğine yönelik bir ders veya kursun alınıp alınmadığı durumuna göre değişmediği sonucuna ulaşılmıştır. Bu çalışmada, yaşın öğretmen adaylarının bilişim güvenliği bilgileri üzerinde bir etkiye sahip olmadığı sonucuna ulaşılmıştır. Fakat Mart (2012) çalışmasında, yaşın bilgi güvenliği farkındalığına etki ettiği sonucuna ulaşmıştır. Mart (2012) çalışmasını 25 ve 45 üzeri farklı meslek grubundan mühendis, avukat, öğretmen vs. bireyler üzerinde gerçekleştirmesi bu sonucu doğurduğu düşünülmektedir. Bu çalışmada günlük bilgisayar ve internet

kullanım süresinin bilişim güvenliği konusunda farklılıklara yol açmadığı, Mart'ın (2012) çalışmasında da bulunmuştur. Bu sonuçlar, bilgisayar ve internette geçirilen sürenin bilişim güvenliği konusunda fazladan bir farklılık oluşturmadığını göstermektedir. Özellikle BÖTE öğretmen adaylarının bilişim güvenliği bilgilerinin, bilişim güvenliğine yönelik bir eğitim alıp almama durumlarına göre farklılık göstermemesi şaşırtıcı bir sonuç olarak görülmektedir. Bu çalışmada bilişim güveniğine yönelik eğitim aldıklarını belirten 114 adayın 53'ü yani yarısına yakını (%46) seçmeli ders olan "Bilişimde Güvenlik ve Etik" dersini aldıklarını, geriye kalanlar ise seminer ve kurs aldıklarını belirtmişlerdir. Dolayısıyla adayların bilişim güvenliği bilgilerinin "Bilişimde Güvenlik ve Etik" dersi, seminer ve kurs alanların almayanlara göre bir farklılık göstermemesi, bu derslerin veya eğitimlerin içerik, yöntem ve konular itirabiriyle yetersiz olmasından kaynaklanabileceği düşünülmektedir. Nitekim Bu sonuçlar, bilişim güvenliği konusunda iyi hazırlanmış eğitimlerin şart olduğunu ve bilişim güvenliğine yönelik verilen eğitimlerin içerik, kapsam, süreç, farkındalık ve değerlendirme bakımında düzenlenmesinin gerekli olduğunu göstermektedir.

5.1.2 BÖTE Öğretmen Adaylarının Bilişim Güvenliği Öğretebilme Yeterliliğine Yönelik Sonuçlar ve Tartışma

Bu çalışmada, BÖTE öğretmen adaylarının çalışma kapsamında yer alan tüm bilişim güvenliği kavramlarını duydukları sonucuna ulaşılmıştır. Pusey ve Sadera (2011) öğretmen adayları üzerinde gerçekleştirdiği çalışmasında adayların tüm bilişim güvenliği kavramlarından arka kapılar, filtre atlama, bot, yapışkan web siteler, script kiddies, sniffing, köle bilgisayar konularını duymadıkları sonucuna ulaşmışlardır. BÖTE lisans programı ve bölümün işlevi dikkate alındığında adayların duymadıkları konu olmaması önemli bir sonuç olarak görülmektedir. BÖTE öğretmen adaylarının duydukları fakat ne anlama geldiğini bilmedikleri konular; uygun kullanım politikası, adware, yapışkan web siteler, türk hukuk sisteminde bilişim suçları kanun maddeleri, DoS Saldırıları (Denial of Service), Nefret grupları, script kiddies, sosyal mühendislik, arka kapılar, phishing, köle bilgisayar, 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

uygun kullanım politikası, adware, phishing, DoS Saldırıları (Denial of Service), sosyal mühendislik ve spoofing konuları içeren sonuca ulaşmışlardır. Özelikle intihal, phishing, bot ve botnet, sosyal mühendislik, DoS saldırıları, adware günümüzde en sık karşılaşılan tehditler arasında bulunmakta ve yapılan çalışmalarda bu konuların önemine değinilmektedir (Djile ve Doğan, 2011; Marinos, 2013; Symantec, 2013). Örneğin; Ural ve Sulak (2012) üniversite öğrencileri üzerinde gerçekleştirdiği çalışmasında kopyala-yapıştır yönteminin çok kullanıldığını, referans göstermenin yaygın olmadığını, referans gösterirken uygun referans gösteriminin yapılmadığını tespit etmişlerdir. Bu çalışmada, BÖTE öğretmen adaylarının çoğunlukla intihalin ne olduğunu bilmedikleri bulunmuştur. Bu bilgi eksikliğinin intihal'in yaygın bir şekilde yapılmasına sebebiyet verdiği düşünülmektedir. Günümüzde önemli konulardan ve gerçekleştirilen saldırılardan biri de kullanıcıların sahte web sitelerine yönlendirilmesidir. Ayrıca Symantec firması (2013) her geçen yıl sosyal mühendislik saldırıların arttığını ve en sık gerçekleşen saldırının phishing saldırısı olduğunu tespit edilmiştir. Marinos (2013) da yaptığı çalışmasında da en çok gerçekleştirilen saldırılar arasında phishing yöntemi bulunmaktadır. Kruger, Flowerday, Drevin ve Steyn ise (2011) üniversite öğrencilerin yarısının, sosyal mühendislik ve phishing ne olduğunu bilmedikleri sonucuna ulaşmışlardır. Bu çalışmada ve Pusey ve Sadera'nın (2011) gerçekleştirdikleri çalışmada öğretmen adaylarının sosyal mühendislik ve phishing hakkında bilgi sahibi olmadıklarının belirlenmiş olması tehlikenin boyutunu gözler önüne sermektedir. Günümüzde bu saldırıların gittikçe artması bu konularda eğitim verilmesinin gerekli olduğunu göstermektedir. Bunun yanında Ünver, Canbay ve Mirzaoğlu (2009) kötü niyetli kişilerin botnetler, phishing, adware, 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.

BÖTE öğretmen adaylarının bildikleri fakat öğrencilerine öğretebilecek yeterliliğe sahip olmadıklarını düşündükleri bazı konular: şifreler, kablosuz aygıt güvenliği, spam, web kamera güvenliği, korsan yazılım, sosyal ağ güvenliği, mobil

teknolojilerin güvenliği, şifreleme, çerezler, screenlogger, güvenlik ayarları, siber zorbalık, reklam içerikli pencereler (Pop-up Ads), casus yazılım, tuş kaydediciler, 5651 sayılı billişim suçları kanunudur. 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 (Pop-up Ads), siber zorbalık, web kamera güvenliği, spam, casus yazılım ve güvenlik ayarları konularını içeren sonuca ulaşmışlardır. BÖTE lisans programlarında bilgisayar ve internet güvenliğine yönelik zorunlu bir dersin olmayışının, öğretmen adaylarının bu konuları öğretebilecek yeterliliğe sahip olmamalarına neden olduğu düşünülmektedir. Bu konularda yapılan çalışmalara bakıldığında, Horzum ve Ayas (2011) ortaöğretim öğrencilerin sanal zorba ve mağdur olma düzeylerini belirlediği çalışmasında sanal zorbalığın ilerleyen yıllarda teknolojinin gelişmesi ve kullanımının artmasıyla daha fazla yaşanacağı görüşünü dile getirmişledir. Bu nedenle öğrencilere, teknolojik araçların yanlış kullanılması durumunda bireylerin olumsuz etkilenebileceğine yönelik bilgilendirme çalışmalarının yapılmasının önemli olduğunu belirtmişlerdir. Mert vd. (2012) öğrenciler üzerinde gerçekleştirdiği araştırmasında öğrencilerin büyük çoğunluğunun (%77) sosyal paylaşım sitesi hesabının olduğunu ve bu sitelerde doğum tarihi, telefon numarası, nerede olduklarına dair bilgileri paylaştıkları sonucuna ulaşmışlardır. Yavanoğlu, Sağıroğlu ve Çolak ise (2012) sosyal ağların güvenliği konusunda yaptıkları çalışmalarında kimlik avı, spam, bot saldırıları, phishing, sahte linkler gibi güvenlik ihlallerinin olduğunu göstererek, bireylerin bu konularda nasıl tedbir alabileceklerine yönelik örnekler sunmuşlardır. Ayrıca yine bu çalışmada verilen örneklerden yararlanılarak bilinçlendirme ve bilgilendirme faaliyetleri içerisinde olunması gerektiği belirtilmiştir. Bu çalışmada, BÖTE öğretmen adaylarının sosyal ağlarının güvenliğini sağlama konusunda kendilerini yeterli görmemeleri ve yapılan çalışmalarda bireylerin sosyal ağ güvenliği konusunda uygun hareket etmemeleri bu konulara yönelik verilecek eğitimin faydalı olabileceğini göstermektedir.

BÖTE öğretmen adaylarının öğretebilme yeterliliğine sahip olduklarını belirtikleri 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) ise, sadece 4 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 intihal'i öğretebilecekleri sonucuna ulaşmalarının nedeninin, bu konuya eğitim ortamlarında yaygın bir şekilde değinmeleri olduğunu belirtmişlerdir. Buradan anlaşılacağı üzere internet ortamında nasıl güvenli hareket edileceğine ve gerekli güvenlik tedbirlerine yönelik bilgilendirmeler olumlu sonuçlar doğurmaktadır. BÖTE öğretmen adaylarının iki yıldır yürürlükte olan ve 6 milyon kullanıcıya ulaşan ayrıca yaygın bilgilendirme kampanyası yapılan güvenli internet hizmeti (Güvenli Internet, 2012) hakkında bilgi sahibi oldukları bu konuya yönelik öğrencilerini bilgilendirebilecek yeterliğe sahip oldukları sonucuna ulaşılmıştır. Nitekim Demirel vd. (2012) ebeveynlerin güvenli internet hizmetinden haberdar olma durumlarının yeterli olmadığı sonucuna ulaşması ve bu çalışmada BÖTE öğretmen adaylarının bu konuyu öğrencilerine öğretebilecek yeterliliğe sahip olduklarını belirtmeleri güvenli internet hizmetinin kullanımı ve bu konuda bilgilendirme yapılması açısından iyi bir sonuç olarak görülmektedir.

Bilişim güvenliğinin öğretilmesine yönelik çalışmalar incelendiğinde, Amerika Birleşik Devletleri'nde (ABD) National Cyber Security Alliance (NCSA) (2011) tarafından gerçekleştirilen araştırmada öğretmenlerin, yöneticilerin ve teknoloji koordinatörlerinin tamamına yakını okullarda bilişim güvenliğinin öğretilmesi gerektiğini belirtmişlerdir. Katılımcıların büyük çoğunluğu, bilişim güvenliğini sağlamaya yönelik verilmesi gereken eğitimlerin okullarda görev yapan teknoloji koordinatörleri tarafından verilmesi gerektiğini vurgulamışlardır. Yine aynı araştırmada, okullarda görev yapan öğretmenlerin son 12 ay içerisinde öğrencilere öğrettikleri bilişim güvenliği konularının yüzdelerinin düşük olduğu tespit edilmiştir (NCSA, 2011). Pruitt-Mentle ve Pusey (2010) bilişim güvenliğine yönelik öğretmen görüşlerinin neler olduğunu tespit ettiği araştırmasında, çok az öğretmenin temel internet becerilerini öğrettikleri sonucuna ulaşmıştır. Bu sonuca göre öğretmenlerin %25'ü şifre değiştirme, %14'ü antivirüs yazılımı kullanma, %12'si bilişim korsanlığı, %16 güvenlik duvarı, %33'ü sosyal ağların tehlikeleri, %39'u yabancılarla bilgi paylaşma, %33'ü özel hayata saygı gösterme konularında öğrencilerini bilgilendirmektedirler. Ülkemizde Tekerek ve Tekerek (2013) tarafından öğrencilerin bilgi güvenliği farkındalıkları üzerine gerçekleştirilen araştırmada, öğrencilerin güvenli şifre kullanımı, çevrimiçi güvenli iletişim, kötücül

yazılım denetlemesi yapma, belge koruma, kişisel bilgisayar güvenliği, güvenlik duvarı ve filtreleme yazılımı kullanma gibi konularda farkındalıklarının çok düşük olduğu sonucuna ulaşılmıştır. Ayrıca yine bu araştırmada öğrenciler, bilgi güvenliği konusunda yeterli bilgiye sahip olmadıklarını belirtmişlerdir. Dijle ve Doğan (2011) bilişim suçlarına yönelik gerçekleştirdiği araştırmasında, bireylerin bilişim suçları konularında yeterli bilince sahip olmadıklarını ve bunun yanında bilişim suçlarına neden olacak ihlallerin, öğrencilerde ve bilgisayar eğitimi almamış kişilerde daha yüksek olduğu sonucuna ulaşmışlardır. Valcke vd. (2007) ilköğretim öğrencilerinin güvenli internet kullanımına yönelik gerçekleştirdiği araştırmasında öğrencilerin yüksek düzeyde güvensiz biçimde internet kullandıklarını tespit etmiştir. Tekerek ve Mart (2010) 8-14 yaş grubu üzerinde gerçekleştirdiği araştırmasında çocukların internette birçok risk ve tehditle karşılaştıklarını fakat bu tehditlere karşı yeterli farkındalığa sahip olmadıklarını tespit etmişlerdir. Ayrıca yine bu araştırmada öğretmenlerin ve ebeveynlerin internette güvenliği sağlama konusunda yeterli bilinç düzeyine sahip olmadıkları sonucuna ulaşılmıştır.

Görüldüğü gibi yapılan araştırmalar göz önüne alındığında internet kullanıcılarının, bireylerin veya öğrencilerin interneti güvenli kullanma, bilişim güvenliğini sağlama, gelebilecek güvenlik tehditlerine karşı önlem alma konusunda farkındalıklarının ve bilgi düzeylerinin düşük olduğu anlaşılmaktadır (Dijle, 2006; Dijle ve Doğan 2011; Mert vd., 2012; Shehri, 2012; Tekerek ve Mart, 2010; Tekerek ve Tekerek, 2013; Valcke vd., 2007). Yine yapılan araştırmalarda, başta öğrencilere olmak üzere tüm bireylere bilgisayar ve internet güvenliğini sağlama konusunda bilgilendirici faaliyetlerin düzenlenmesinin gerekliliği üzerinde durulmaktadır (Dijle ve Doğan, 2011; Emiral, 2004; Mart 2012; Mert vd., 2010; Öğütçü, 2010; Pruitt-Mentle ve Pusey, 2010; Pusey ve Sadera 2011; Rezgui ve Marks, 2008; Richardson, 2009; Tekerek ve Mart, 2010; Tekerek ve Tekerek; 2013; Ünver ve Canbay, 2010). Çocuklara evde, okulda ve sokakta nasıl güvenli yaşayacakları öğretildiği gibi bilgisayar ve internet ortamında da gelebilecek tehditlere karşı kendilerini nasıl koruyacaklarının öğretilmesi önemli görülmektedir. Dolayısıyla bu konuda özellikle okullarda görev yapacak olan BÖTE öğretmen adaylarına büyük görevler ve sorumluklar düşmektedir. Bu çalışmada, okullarda görev yapacak BÖTE öğretmen adaylarının bilişim güvenliğini sağlama ve gerekli önlemleri alma konularına yönelik bilgilerinin ve yeterliliklerinin beklenen düzeyde olmadığı sonucuna ulaşılmıştır.

5.2 ÖNERİLER

Araştırma sonuçlarından yola çıkarak aşağıdaki öneriler geliştirilmiştir.

5.2.1 Araştırma Sonuçlarına Dayalı Öneriler

- BÖTE bölümü lisans programında bilişim teknolojileri ve internet güvenliğine yönelik kapsamlı ve uygulamaya yönelik bir dersin yer alması faydalı olacaktır.
- Öğrencilere karşılaşabilecekleri tehditlere karşı hangi yöntemleri nasıl uygulayabileceklerine yönelik eğitimler verilmelidir.
- Bilişim güvenliğini sağlamaya, sık karşılaşılan saldırıları önlemeye, internet ortamında güvenli bir şekilde gezinmeye yönelik web siteleri geliştirilebilir.
- Bilişim güvenliğini sağlama konusunda bireyleri işin içine katarak uygulanması gereken güvenlik yöntemleri seminerler veya kurslar yoluyla anlatılabilir.

5.2.2 İleride Yapılabilecek Araştırmalara Yönelik Öneriler

- Bu çalışma nicel araştırma yöntemlerinden tarama türü ile yürütülmüştür. Başka bir çalışmada nitel araştırma yöntemleri kullanarak öğretmen adaylarının bilişim güvenliği bilgileri ve farkındalıkları derinlemesine araştırılabilir.
- Öntest-sontest kontrol gruplu deneysel desen kullanılarak verilecek bir bilişim güvenliği eğitiminin, öğrencilerin bilgi düzeyleri ve gerekli tedbirleri alma konusunda ne kadar etkili olduğu araştırılabilir.
- Okullarda görev yapan Bilişim teknolojileri rehber öğretmenlerinin yeterlilikleri ve öğrencilerin bilgisayar ve internet güvenliğini sağlama konusunda ne tür faaliyetler içerisinde oldukları araştırılabilir.
- Bu çalışmada sadece BÖTE bölümü öğrencileri incelenmiştir. Diğer öğretmenlik programlarında okuyan öğrencilerde mevcut durum incelenebilir.

KAYNAKÇA

Acılar, A. (2012). Küçük Şehir Belediyelerinde Web Sitesi ve E-belediye Kullanımı: Bilecik Belediyesi Örneği. *Dumlupınar Üniversitesi Sosyal Bilimler Dergisi*, *1*(32), 125-142.

Agamba, J. ve Keengwe, J. (2012). Pre-Service Teachers' Perceptions of Information Assurance and Cyber Security. International Journal of Information and Communication Technology Education, *8*(2), 94-101. DOI: 10.4018/jicte.2012040108.

Akçakaya, V. ve Tanrısever, T. (8-10 Kasım 2007). Eğitimciler İçin Yeni Bir Web Aracı. *12. Türkiye'de Internet Konferansı Bildirileri Kitabı.* Bilkent Üniversitesi, Ankara.

Akolaş, A. (2004). Bilişim Sistemleri ve Bilişim Teknolojisinin Küreselleşme Olgusu ve Girişimcilik Üzerine Yansımaları. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *12*, 29–43.

Alaca, B. (2008). *Ülkemizde Bilişim Suçları ve Internetin Suça Etkisi (Antropolojik ve Hukuk Boyutları ile)*. Yüksek lisans tezi. Ankara Üniversitesi, Sosyal Bilimleri Enstitüsü, Ankara.

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.

Aydın, E. D. (1992). *Bilişim Suçları ve Hukukuna Giriş*. Ankara: Doruk Yayınevi.

Aydın, M. A. ve Sarısakal, M. N. (2003). E-ticaretin Yeni Yüzü Mobil Internet. *Havacılık ve Uzay Teknolojileri Dergisi, 1*(2), 83-90.

Bayram, N. ve Saylı, M. (2013). Üniversite Öğrencileri Arasında Siber Zorbalık Davranışı. *İstanbul Üniversitesi Hukuk Fakültesi Dergisi.* 71(1), 107-116..

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

Bilgimi Koruyorum. (2011). Bilgi Güvenliği - Hakkımızda. http://www.bilgimikoruyorum.org.tr/?bilgem-proje-hazirlayanlar-hakkinda adresinden 11.12.2013 tarihinde erişilmiştir.

Bitdefender. (2013). Case Study: Kids & Online Threats. http://www.guvenliweb.org.tr/istatistikler/files/Bitdefender-CaseStudy-Kids.pdf adresinden 17.12.2013 tarihinde erişilmiştir.

Boğa, U. (2011). *Bilişim Suçları İle Mücadele Yöntemleri.* Uzmanlık Tezi, Radyo Televizyon Üst Kurulu. Ankara.

Bozbel, S. (17-19 Kasım 2011). Internette Üçüncü Bir Kişiye Ait İçeriğin Bir Başkası Tarafından Kendi Program veya Web Sitesinde Kullanılması. *2. Uluslararası Bilişim Hukuku Kurultayı Bildiriler Kitabı.* İzmir.

Brenner, S.W. (2010). *Cybercrime: Criminal Threats from Cyberspace.* California: ABC-CLIO Publishing.

Burlu, K. (2010). *Bilişimin Karanlık Yüzü*. Ankara: Nirvana Yayınları.

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

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. (2008). Casus Yazılımlar: Bulaşma Yöntemleri ve Önlemler. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, *23* (1), 165-180.

Canbek, G. ve Sağıroğlu, Ş. (2007a). Kötücül Casus Yazılımlar Kapsamlı Bir Araştırma. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 22* (1), 121-136.

Canbek, G. ve Sağıroğlu, Ş. (2007b). Çocukların ve Gençlerin Bilgisayar ve Internet Güvenliği. *Politeknik Dergisi*. *10*(1), 33-39.

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

Clinton, L. (2009). Education's Critical Role in Cybersecurity. *EDUCAUSE Quarterly*, *32*(3), 60-61.

Cone, B.D., Irvine, C.E., Thompson, M.F. ve Nguyen, T.D. (2007). A Video Game for Cyber Security Training and Awareness. *Computers & Security*, 26, 63-72. DOI:10.1016/j.cose.2006.10.005

Cross, M.(2008). *Scene of Cybercrime*. (Second Edition). Burlington: Syngress Publishing, Inc.

Çakmak A.Ç., Güneşer M.T. ve Terzi H. (2011). Bankaların Müşterilerine Sunduğu Internet Bankacılığı Hizmetinin Müşteriler Tarafından Değerlendirilmesi: Karabük Şehir Merkezinde Uygulama. *Sosyal Bilimler Enstitüsü Dergisi. 31*, 1-30.

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

Çelen, F.K., Çelik, A. ve Seferoğlu, S.S. (2-4 Şubat 2011). Çocukların İnternet Kullanımları ve Onları Bekleyen Çevrim-içi Riskler. *13. Akademik Bilişim Konferansı Bildirileri,* İnönü Üniversitesi, Malatya.

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

Çoban, S. (7-9 Kasım 2012). Uzaktan ve Teknoloji Destekli Eğitimin Gelişimi. *17. Türkiye'de İnternet Konferansı Bildirileri,* Anadolu Üniversitesi, İletişim Bilimleri Fakültesi, Eskişehir.

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

Değirmenci, O. (2002). *Bilişim suçları*. Yayınlanmamış yüksek lisans tezi, Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul.

Dekker, M., Karsberg, C. ve Lakka, M. (2013). Annual Incident Reports 2012: Analysis of Article 13a Annual Incident Reports.

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2012 adresinden 24.12.2013 tarihinde erişilmiştir. Heraklion: European Union Agency for Network and Information Security Publishing ISBN 978-92-9204-066-6.

Delialioğlu, Ö. (2011). Bilişim Sistemleri Güvenliği ve İlgili Etik Kavramlar. A. Şentürk (Ed.), *Temel Bilgi Teknolojileri ve Bilgisayar Kullanımı* (509-538). Bursa: Ekin Yayınevi.

Demir, E. (2006). *Birey ve Aile Yaşamına İlişkin Konularda İnternet 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.

Demirli, C. ve Kütük, Ö.F. (2010) Anlamsal Web (Web 3.0) ve Ontolojilerine Genel Bir Bakış. *İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi,* 9(18), 95-105.

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

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

Dülger, M.V.(2004). *Türk Ceza Hukukunda Bilişim Suçları*. Yüksek lisans tezi. İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul.

Elbahadır, H. **(**2011). *Hacking Interface*. İstanbul: Kodlab Yayıncılık.

Eminağaoğlu, M. ve Gökşen, Y. (2009). Bilgi Güvenliği Nedir, Ne Değildir, Türkiye'de Bilgi Güvenliği Sorunları ve Çözüm Önerileri. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 11*(4), 1-15.

Erses, N.(2011). Bilişim Teknolojileri Temel Kavramları. A. Şentürk (Ed.), *Temel Bilgi Teknolojileri ve Bilgisayar Kullanımı* (1-55). Bursa: Ekin Yayınevi.

Emiral, F. (2004). Bilgi Güvenliği Bilincinin Genele Yayılması. http://www.denetimnet.net/UserFiles/Documents/50_45_1.pdf adresinden 05.12.2013 tarihinde erişilmiştir.

Gelbstein, E. ve Kamal, A. (2002). *Information Insecurity: A Survival Guide to the Uncharted Territories of Cyber-threats and Cyber-security* (Second Edition). New York: United Nations ICT Task Force and the United Nations Institute for Training and Research.

Gelişken, U. (2009). *10 Adımda Bilgisayar Güvenliği.* İstanbul: Kodlab Yayıncılık.

Green, S. B. ve Salkind, N. J. (2008). *Using SPSS for Windows and Macintosh: Analyzing and Understanding Data.* Upper Saddle River: Pearson; Prentice Hall.

Gümüş, Ç. (2008). *Bilişim Suçları ile Mücadelede Polisin Eğitimi.* Yüksek lisans tezi. Fırat Üniversitesi, Sosyal Bilimler Enstitüsü, Elazığ.

Güney, S. ve Mutlu, S. (2008). Bilişim Teknolojilerinin Girişimciliğe Etkileri. *Girişimcilik ve Kalkınma Dergisi*, *3*(1), 85-102.

Gündüz, M.Z. (2013). *Bilişim Suçların Yönelik IP Tabanlı Delil Tespiti*. Yüksek lisans tezi. Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elazığ.

Güvenli Internet. (2012). Güvenli Internet Hizmeti Nedir? http://guvenlinet.org.tr/tr/menu/12-Guvenli_Internet_Hizmeti_Nedir_.html adresinden 12.12.2013 tarihinde erişilmiştir.

Güvenli ve Bilinçli Internet Kullanım Projesi. (2013). http://fethiye.meb.gov.tr/meb_iys_dosyalar/2013_02/18110143_gvenlveblnlnternetkullanimprojesktapik.pdf adresinden 13.12.2013 tarihinde erişilmiştir.

Horzum, M.B. ve Ayas, T. (2011). Ortaöğretim Öğrencilerinin Sanal Zorba ve Mağdur Olma Düzeylerinin Okul Türü ve Cinsiyet Açısından İncelenmesi. *Eğitim Bilimleri ve Uygulama, 10* (20), 139-159.

Internet World Stats. (2012). Europe Internet Usage Stats Facebook Subscribers and Population Statistics, http://www.internetworldstats.com/stats4.htm adresinden 25.03.2014 tarihinde erişilmiştir.

Irvine, C.E. ve Thompson, M. (24-27 June 2003). Teaching Objectives of Simulation Game for Computer Security. *Informing Science & Information Technology Joint Conference*. Pori, Finland. 0779-0791.

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

İlbaş, Ç. ve Köksal, M.A. (17-19 Kasım 2011). Türkiye Bilişim Suçları Raporu: 1990-2011 Temmuz. *2. Uluslararası Bilişim Hukuku Kurultayı Bildiriler Kitabı.* İzmir.

İlkan, M., İşçioğlu, E., Egelioğlu, F. ve Doğanalp, A. (6-8 Mayıs 2010). Information Security Awareness of Academic Staff Members: An Example of Eastern Mediterranean University School of Computing and Technology, *4.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildirileri*, Orta Doğu Teknik Üniversitesi. Ankara.

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.

İşman, A. (2011). *Uzaktan Eğitim.* (4.Baskı). Ankara: Pegem Yayıncılık.

Kaçakcılık ve Organize Suçlar Daire Başkanlığı.(2011). *Kaçakcılık ve Organize Suçlarla Mücadele 2011 Raporu*. Ankara: KOM Yayınları.

Kaçar, A.Ö. ve Doğan, N. (31 Ocak - 2 Şubat 2007). Okul Öncesi Eğitimde Bilgisayar Destekli Eğitimin Rolü. *9. Akademik Bilişim Konferansı Bildirileri,* Dumlupınar Üniversitesi, Kütahya.

Karaarslan, E. ve Şengonca, H. (2003). *Meslek Yüksek Okullarında Bilgi Güvenliği Eğitimi. Ege Üniversitesi Meslek Yüksek Okulu Sempozyumu, Ege Üniversitesi, İzmir.*

Karakoç, M. A. (7-8 Ekim 2011). Bilişim Suçlarına Genel Bakış, Bilişim Suçlarını Önleme Çalışmaları ve Güvenli Internet Kullanımı. *Suç Önleme Sempozyumu,* Merinos Atatürk Kongre ve Kültür Merkezi, Bursa.

Karaman, S., Yıldırım, S. ve Kaban, A. (22-23 Aralık 2008). Öğrenme 2.0 Yaygınlaşıyor: Web 2.0 Uygulamalarının Eğitimde Kullanımına İlişkin

Araştırmalar ve Sonuçları. *14.Türkiye'de Internet Konferansı Bildirileri.* Orta Doğu Teknik Üniversitesi, Ankara.

Kaya, Z. (2002). *Uzaktan Eğitim.* Ankara: Pegem Yayımcılık.

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

Koc.net. (2005). *Rizikometre-Türkiye Internet Güvenliği Araştırma Sonuçları.* İstanbul: KoçNet A.Ş.

Küçük, A. ve Soğukpınar İ. (14-16 June 2013). Cyber Attacks and a Proposal for Awareness Training. *İlk Bildiriler Konferansı Bildirileri Kitabı,* TOBB Ekonomi ve Teknoloji Üniversitesi, Ankara.

Kruger, H.A ve Kearney, W.D. (2006). A Prototype for Assessing İnformation Security Awareness. *Computers & Security, 25,* 289-296. DOI:10.1016/j.cose.2006.02.008

Kruger, H.A, Flowerday, S., Drevin, L. ve Steyn, T. (15-17 August 2011). An Assessment of the Role of Cultural Factors in Information Security Awareness. *Information Security South Africa Conference*. 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. ISBN 978-92-79-00077-5 doi:10.2788/14231.

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

Mavnacıoglu, K. (7-9 Ekim 2009). Internette Kullanıcıların Oluşturduğu ve Dağıttığı İçeriklerin Etik Açıdan İncelenmesi: Sosyal Medya Örnekleri. *Medya ve Etik Sempozyumu Bildirileri Kitapçığı*, Fırat Üniversitesi İletişim Fakültesi, Elazığ.

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.

Miller, M. (2003). *Herkes İçin PC Güvenliği ve Bilgisayar Virüsleri.* (Çev. B. Erol). İstanbul: Alfa Yayınları. (Eserin orijinali 2002'de yayımlandı).

Milli Eğitim Bakanlığı. (2008). Bilişim Teknolojileri Öğretmeni Özel Alan Yeterlikleri. http://otmg.meb.gov.tr/alanbt.html adresinden 15.06.2013 tarihinde erişilmiştir.

Milli Eğitim Bakanlığı, (2013). Bilişim Teknolojisi Nedir? http://mebk12.meb.gov.tr/meb_iys_dosyalar/06/27/709216/icerikler/bilisim-teknolojisi-nedir_399424.html adresinden 12.12.2012 tarihinde erişilmiştir.

Moore, R. (2011). *Cybercrime: Investigating high-technology computer crime.* (Second edition). Burlington: Anderson Publishing.

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.* Başkent Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.

Özel, H.A. (2013). E-ticaret ve Türkiye'nin Bilgi Toplumundaki Yeri, *Akademik Bakış Dergisi,* 38. http://www.akademikbakis.org/38/13.pdf adresinden 06.12.2013 tarihinde erişilmiştir.

Pallı, H. (2008). *Türk Hukukunda ve Mukayesli Hukukta Bilişim Suçları.* Yüksek lisans tezi. Erciyes Üniversitesi, Sosyal Bilimler Enstitüsü, Kayseri.

Pati. (t.y). Cyber Crime. http://www.naavi.org/pati/pati_cybercrimes_dec03.htm adresinden 09.12.2013 tarihinde erişilmiştir.

Peker, D. (2008). Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin Uygulanmasında ISO/IEC 27001:2005 - Bilişim Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler standardı Sürüm 1.0. http://www.tbd.org.tr/usr_img/cd/kamubib12/raporlarPDF/RP1-ISO27001-2008.pdf adresinden 12.12.2013 tarihinde erişilmiştir.

Pro-G. (2003). Bilişim Güvenliği. Sürüm 1.1. Proje Bilişim Güvenliği ve Araştırma San. ve Tic. Ltd. Şti. http://www.pro-g.com.tr/whitepapers/bilisim-guvenligi-v1.pdf adresinden 07.01.2014 tarihine 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.

Rezgui, Y. ve Marks, A. (2008). İnformation Security Awareness in Higher Education: A Exploratory Study. *Computers & Security, 27*, 241-253. DOI:10.1016/j.cose.2008.07.008.

Richardson, R. (2009). 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.

Siber Suç Uzmanları Komitesi. (2008). *Avrupa Konseyi Siber Suçlar Sözleşmesi Taslağı* (3.Baskı). Ankara: Ankara Barosu Bilgi İşlem Merkezi Yayınları.

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 24.11.2013 tarihinde erişilmiştir.

Şahin, L., Çetin, B.I. ve Yıldırım, K. (2009). Bilişim Teknolojilerindeki Gelişmelerin İşletmelerin Strateji ve Maliyet Üzerine Etkileri. *Sosyal Siyaset Konferansları Dergisi, 56*(1), 547-573.

Şahinaslan, E., Kantürk, A., Şahinaslan., Ö. ve Borandağ, E. (11-13 Şubat 2009). Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri. *11. Akademik Bilişim Konferansı Bildirileri.* Harran Üniversitesi, Şanlıurfa.

Şahinaslan, E., Kandemir, R. ve Şahinaslan, Ö. (11-13 Şubat 2009). Bilgi Güvenliği Farkındalık Eğitim Örneği. *11. Akademik Bilişim Konferansı Bildirileri*. Harran Üniversitesi, Şanlıurfa.

Şamlı, R. (10-12 Şubat 2010). Türk ve Dünya Hukukunda Bilişim Suçları. *12. Akademik Bilişim Konferansı Bildirileri.* Muğla Üniversitesi, Muğla.

Taş, İ. E. ve Kestellioğlu, G. (2011). Halkla İlişkilerde Internetin Yeri ve Önemi. *Kahramanmaraş Sütçü İmam Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 1*(1), 73-92.

Taş, K. A. (2010). *Bilişim Suçları ve Adana İlinde 2006-2009 Yılları Arasında Meydana Gelen Bilişim Suçlarının Değerlendirilmesi.* Yüksek lisans tezi. Çukurova Üniversitesi, Sağlık Bilimleri Enstitüsü, Adana.

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

Tekerek, M. (2008). Bilgi Güvenliği Yönetimi. *Kahramanmaraş Sütçü İmam Üniversitesi Fen ve Mühendislik dergisi, 11*(1), 132-137.

Tekerek, M. ve Mart, İ. (6-8 Mayıs 2010). K8 Düzeyi İçin Davranışsal Bilgisayar ve Internet Güvenliği Farkındalığı, *4.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildirileri.* Orta Doğu Teknik Üniversitesi. Ankara.

Tekin, M., Zerenler, M. ve Bilge, A. (2005). Bilişim Teknolojileri Kullanımının İşletme Performansına Etkileri: Lojistik Sektöründe Bir Uygulama. *İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi, 4*(8), 115-129.

Telekomünikasyon İletişim Başkanlığı Internet İhbar Merkezi. (2010). http://ihbarweb.org.tr/index.html adresinden 13.12.2013 tarihinde erişilmiştir.

Tulum, İ. (2006). *Bilişim Suçları ile Mücadele.* Yüksek lisans tezi. Süleyman Demirel Üniversitesi, Sosyal Bilimler Enstitüsü, Isparta.

Türk Bilişim Derneği. (2006). *Bilişim Sistemleri Güvenliği El Kitabı Sürüm 1.0*. Ankara: Türkiye Bilişim Derneği Yayınları.

Türk Ceza Kanunu. (2004). http://www.tbmm.gov.tr/kanunlar/k5237.html adresinden 13.12.2013 tarihinde erişilmiştir.

Türk Dil Kurumu. (2013). Genel Türkçe Sözlüğü. http://tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.52ab0a9de06dc8.51022261 adresinden 13.12.2013 tarihinde erişilmiştir.

Türkiye Bilişim Şurası. (2002). E-devlet Çalışma Grubu Raporu. http://www.tbd.org.tr/usr_img/cd/kamubib12/diger/SuraRaporu.DOC adresinden 06.12.2013 tarihinde erişilmiştir.

Türkiye İstatistik Kurumu. (2013). Bilgi Toplumu İstatistikleri. http://www.tuik.gov.tr/UstMenu.do?metod=temelist adresinden 26.11.2013 tarihinde erişilmiştir.

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

Ulusal Bilgi Güvenliği Kapısı. (2014). Ulusal Bilgi Güvenliği Kapısı Hakkında, https://www.bilgiguvenligi.gov.tr/hakkimizda.html adresinden 11.12.2013 tarihinde erişilmiştir.

Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı. (2013), http://www.iscturkey.org/ adresinden 13.12.2013 tarihinde erişilmiştir.

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.

Uzunay, Y. ve Koçak M. (2005). Internet Üzerinden Çocuk Pornografisi ve Mücadele Yaşanan Sıkıntılar. *Polis Bilimleri Dergisi, 7* (1), 98-116.

Ünüvar, M. (2006). Örgütsel Değişimde Bilgi Teknolojilerinin Rolü. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 8*(4), 270-285.

Ünver, M. ve Canbay, C. (2010). Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik. *Elektrik Mühendisliği Dergisi, 438*, 94-103.

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

Ünver, M. ve Mirzaoğlu, A.G. (2011). Yemleme ("Phishing"). Bilgi Teknolojileri ve İletişim Kurumu. Ankara.

Valcke, M., Schellens, T., Van Keer, H. Ve Gerarts, M. (2007). Primary School Children's Safe and Unsafe Use of the Internet At Home and At School: An Exploratory Study. *Computers in Human Behavior, 23*, 2838-2850.

Wall, D.S. (2007). *Cybercrime: the Transformation of Crime in the Information Age*. Cambridge: Polity Press.

Yalçın, N. (9-11 Şubat 2006). İnterneti Doğru Kullanıyor Muyuz? İnternet Bağımlısı Mıyız? Çocuklarımız ve Gençlerimiz Risk Altında Mı? *IV. Bilgi Teknolojileri Kongresi Akademik Bilişim Bildiriler Kitabı*, Pamukkale Üniversitesi, Denizli.

Yavanoğlu, U. ve Sağıroğlu, Ş. (6-8 Mayıs 2010). Sosyal Ağlar ve Bilgi Güvenliği. *4.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildirileri,* Orta Doğu Teknik Üniversitesi, Ankara.

Yavanoğlu, U., Sağıroğlu, Ş. ve Çolak, İ. (2012). Sosyal Ağlarda Bilgi Güvenliği Tehditleri ve Alınması Gereken Önlemler. *Politeknik Dergisi, 15*(1), 15-27.

Yavuz, H. ve Ulaş, M. (20-21 Mayıs 2013). Adli Bilişime konu olan Bilişim Suçları ve Bilgi Güvenliği Farkındalık Tespiti. *1. International Symposium on Digital Forensics and Security Proceding Book.* Fırat Üniversitesi, Elazığ.

Yaycı, E. (2007). *Bilişim Suçları.* Yüksek lisans tezi. Gazi Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara.

Yılmaz, D.(2005). *Hacking: Bilişim Korsanlığı ve Korunma Yöntemleri.* (3.Baskı). İstanbul: Hayat Yayıncılık.

EKLER

EK-1. BİLİŞİM GÜVENLİĞİ BİLGİSİ VE BİLİŞİM GÜVENLİĞİNE YÖNELİK EĞİTİM VEREBİLME YETERLİLİĞİ ARACI

Değerli Öğrenci Arkadaşlarım;

Bu anket, bilişim güvenliği konusundaki bilgilerinizi ölçmek amacıyla hazırlanmıştır. Yüksek lisans tez çalışmamın veri toplama aracı olarak size uygulanmaktadır. Anketi doldururken adınız sorulmamaktadır. Vereceğiniz bilgiler bireysel olarak hiçbir kişi ya da kurumla paylaşılmayacaktır. Gerçek durumunuzu gösteren yanıtı işaretlemeniz çalışmanın geçerli sonuçlar vermesi açısından önemlidir. Katıldığınız için teşekkür ederim.

Arş. Gör. Ömer Faruk GÖKMEN
omerfarukgokmenn@gmail.com

Danışman:
Yrd. Doç. Dr. Özcan Erkan AKGÜN
ozcanakgun@gmail.com

---

1) Yaşınız: …

2) Cinsiyet: K ( ) E ( )

3) Sınıfınız: 1 ( ) 2 ( ) 3 ( ) 4 ( )

4) Günlük bilgisayar kullanım süreniz? ( )1-3 saat ( )4-6 saat ( )7-9 saat ( )10 saat ve üzeri

5) Günlük internet kullanım süreniz? ( )1 saatten az ( )1-3 saat ( )4-6 saat ( )7 saat ve üzeri

6) Sık kullandığınız bilgisayarın sahibi kim? ( ) Ben **( )**Annem babam **( )**Üniversiteden ödünç **( )**Internet kafe **( )**Diğer. Lütfen Belirtiniz ……

7) Ne kadar zamandır kendi bilgisayarınız var? ….. yıl

8) Bilgisayarınızın güncellemelerini kim yapar?

( ) Ben
( ) Diğer. Lütfen belirtiniz ….
( ) Kimse Yapmaz.

9) Bilişim güvenliği ile ilgili bir ders veya kurs aldınız mı?

( ) Evet. Yanıtınız evet ise lütfen dersi/kursu kısaca anlatınız (adı, kurs aldığınız yer, içeriği)……
( ) Hayır

10) Ne kadar sıklıkla virüs tarama yazılımını güncellersiniz?

( ) Günlük
( ) Haftalık
( ) Yılda bir kez
( ) Kurduğum zaman sadece
( ) Kurulu virüs programım yok
( ) Bilmiyorum

11. ve 17. sorularda boş bırakılan yere size göre gelmesi gereken doğru seçeneği işaretleyiniz.

11) Virüs taraması yapmadan e-posta ekini açmak … güvenlidir.

( ) Güvenilir kaynaktan geldiği zaman
( ) Bir banka veya ticari kuruluştan geldiği zaman
( ) Konu satırı hakkınızda kişisel bilgi içerdiği zaman
( ) Yukarıdakilerin hepsi
( ) Hiçbiri
( ) Bilmiyorum

12) E-posta ekinin içinde bulunan bağlantıya (linke) tıklamak … güvenlidir.

( ) Güvenilir kaynaktan geldiği zaman
( ) Bir banka veya ticari kuruluştan geldiği zaman
( ) Konu satırı hakkınızda kişisel bilgi içerdiği zaman
( ) Yukarıdakilerin hepsi
( ) Hiçbiri
( ) Bilmiyorum

13) Proxy sunucu …

( ) Çocukları çevrimiçi müstehcen içerikten korur
( ) Çocukların okulda internet filtrelerini atlamalarına izin verir.
( ) Web siteleri için güvenli şifre oluşturur.
( ) Yukarıdakilerin hepsi
( ) Hiçbiri
( ) Bilmiyorum

14) Yeni pencerede (ekranda) açılan reklam pencereleri (Pop-up Ads) …

( ) Web sitelerinde sörf yaparken görüntülenir
( ) Web sitelerini ziyaret ettikten sonra görüntülenir
( ) Internet tarayıcısı açıldığı zaman görüntülenir
( ) Yukarıdakilerin hepsi
( ) Hiçbiri
( ) Bilmiyorum

15) USB/ Flash bellek gibi taşınabilir veri depolama aygıtları aşağıdakilerden hangisi için kullanılabilir?

( ) Öğrenci isimleri, adresleri, test puanları gibi verileri
( ) Öğrenci çalışmaları
( ) Bireylerin eğitim planları
( ) Yukarıdakilerin hepsi
( ) Hiçbiri
( ) Bilmiyorum

16) Güvenlik duvarı …

( ) Bir bilgisayara izinsiz girişi önler
( ) Bilgisayardan gönderilen yetkisiz bir bilgiyi engeller.
( ) Yukarıdakilerin hepsi
( ) Hiçbiri
( ) Bilmiyorum

17) Şifreler … olmalıdır.

( ) Tüm hesaplar için aynı
( ) Küçük-büyük harfin ve numaraların karışımı
( ) Gerçek kelimeler
( ) Yukarıdakilerin hepsi
( ) Hiçbiri

Aşağıda bilişim güvenliği bilginizi ve bilişim güvenliğini öğretebilmenizi belirlemek amacıyla sorular sorulmaktadır. Size yöneltilen her soru için durumunuza en uygun seçeneğin karşısına (X) işareti koyunuz.				
	Bu konu hakkında hiçbir şey duymadım	Duydum. Fakat ne anlama geldiğini bilmiyorum	Biliyorum. Fakat öğrencilerime öğretemem	Biliyorum ve öğrencilerime öğretebilirim
Uygun Kullanım Politikası				
Reklam Bedelli Yazılım (Adware)				
Gizli Arşiv Dosyaları				
e-posta Ekleri				
Arka Kapılar (Back door)				
Bot ve Botnet				
Blog Güvenliği				
Filtre Atlama (Aşma)				
Önbelleğe Yüklenmiş Web Siteler				
Cep Telefonu Güvenliği				
Güvenli Internet Hizmeti				
Güvenli Çocuk Portalları				
Çerezler (Cookies)				
Sabit Diski Olan Fotokopi Makinelerinin ve tarayıcıların Güvenliği				
Telif Hakkı (Copyright)				
Siber Zorbalık				
Karalama / İftira / Hakaret				
DoS Saldırıları (Denial of Service)				
Değiştirilmiş Dijital Fotoğraflar				
Dijital Sertifikalar				
Zamanını Doldurmuş Eski Teknolojilerin Elden Çıkarılması				
Şifrelenmemiş E-mail				
Şifreleme (Encryption)				
Son kullanıcı Lisans Sözleşmesi				

Kaçak Yazılım Kullanma				
Korsan Yazılım (Lisanssız yazılım)				
5651 sayılı Internet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele kanunu				
Adil Kullanım				
Dosya Paylaşım Güvenliği				
Güvenlik Duvarları (Firewall)				
Çevrimiçi Kumar				
Bilişim Korsanlığı (Hacking)				
Nefret Grupları				
Milli Eğitim Bakanlığı Bilgi ve Sistem Güvenliği Yönergesi				
Çalmak / Gasp/ Hırsızlık (Hijack)				
Kimlik Hırsızlığı				
Internet Filtreleri				
Tuş Kaydediciler (Keylogger)				
Ekran Kaydediciler (Screenlogger)				
Zararlı Yazılımlar (Virüs, Solucan, Truva atı)				
Çevrimiçi Oyunlar				
Çevrimiçi Kimlikler				
Şifreler				
Yamalar				
Erişim İzni				
Oltalama (Phishing)				
İzinsiz Yayınlama / Yasa Dışı Yayın				
İntihal (Plagiarism)				
Screen Scraping (İçerik Toplayıcılık)				
Reklam İçerikli Pencereler (Pop-Up Ads)				
Taşınabilir Veri Depolama Aygıtları Güvenliği				
Portlar				
Video ve Resim Gönderme / Postalama				
Gizlilik				
Profil Denetimi				
Vekil Sunucu (Proxy)				
Hacker'ların Paylaştığı Araçları Kullananlar (Script				

Kiddies)				
Güvenli Siteler				
Güvenlik Ayarları				
Sniffing				
Sosyal Mühendislik				
Sosyal Ağ Güvenliği				
Yazılım Güncellemesi				
Spam (İstem Dışı alınan e-posta/Çöp posta)				
Spam Filtreleme				
Spoofing				
Casus Yazılım (Spyware)				
Yapışkan Web Siteler				
Metin Mesaj Güvenliği				
Takip Edilen Çerezler				
Kandırmacılık (Tricklers)				
Kablosuz Aygıt Güvenliği				
Web Kamera Güvenliği				
Köle Bilgisayar (Zombi)				
Türk Hukuk Sisteminde Bilişim Suçları Kanun Maddeleri				
Mobil Teknoloji Güvenliği				

EK-2. ANKET İZİN BELGESİ

T.C.
SAKARYA ÜNİVERSİTESİ
Eğitim Fakültesi

Sayı : 1408200 _044-1589

26 Aralık 2013

Konu :Anket Uygulama İzni

EĞİTİM BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

İlgi:19/12/2013 tarihli ve 67236739-044/741 sayılı yazı.

Üniversitemiz Eğitim Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı Ömer Faruk GÖKMEN'un Fakültemiz lisans öğrencilerine uygulamak istediği "Bilgisayar ve Öğretimi Teknolojisi Eğitimi Öğretmen Adaylarının Bilişim Güvenliği Bilgisi ve Bilişim Güvenliğine Yönelik Eğitim Verme Yeterlilikleri" başlıklı çalışmasını bizzat iştiraki ile yapması halinde uygun görülmüştür.

Gereğini bilgilerinize arz ve rica ederim.

Prof.Dr.Rahmi KARAKUŞ
Dekan

T.C.
SAKARYA ÜNİVERSİTESİ
EĞİTİM BİLİMLERİ ENSTİTÜSÜ

KAYIT	Tarih	31.12.2013	Ek		PARAF	Havale/Kayıt
	Sayı	044.949	-			Tarih / No
HAVALE						
AÇIKLAMA						Dosyasına

Başpınar Mah. Muammer Sencar Cad. No:23 54300 Hendek / SAKARYA
Telefon : (0 264) 614 10 33 Faks : (0 264) 614 10 34
e-posta : ef@sakarya.edu.tr Elektronik Ağ : www.sakarya.edu.tr

ÖZGEÇMİŞ VE İLETİŞİM BİLGİSİ

Ömer Faruk GÖKMEN, 1990 yılında Siirt'te doğdu. İlk ve orta öğrenimini Siirt'te tamamladı. 2008 yılında Siirt Anadolu Lisesinden mezun oldu. Aynı yıl Amasya Üniversitesi Bilgisayar ve Öğretim Teknolojileri Eğitimi Öğretmenliği bölümünü kazandı. 2012 yılında Amasya Üniversitesinden mezun oldu. Yine aynı yıl içerisinde Sakarya Üniversitesi Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı'nda yüksek lisans eğitimine başladı. 2014 yılının başından itibaren Sakarya Üniversitesi Bilgisayar ve Öğretim Teknolojileri Eğitimi bölümünde araştırma görevlisi olarak çalışmaktadır. Yabancı dili İngilizcedir.

E-posta : omerfarukgokmenn@gmail.com