Ege Eğitim Teknolojileri Dergisi
Journal of Ege Education Technologies
e-ISSN 2667-4270
Sayı 3, Cilt 1, Temmuz 2019, Sayfa 20- 27

Bilgisayar Teknolojileri Ve Bilişim Sistemleri Öğrencilerinin Bilişim Güvenliği Alanında Yeterliliklerinin İncelenmesi[1]

Onur KARA
Trakya Üniversitesi, Keşan Yusuf Çapraz Uygulamalı Bilimler Yüksekokulu, Bilgisayar Teknolojileri Ve Bilişim Sistemleri
onurkr22@gmail.com

Murat TOPALOĞLU
Trakya Üniversitesi, Keşan Yusuf Çapraz Uygulamalı Bilimler Yüksekokulu, Bilgisayar Teknolojileri Ve Bilişim Sistemleri
murattopaloglu@trakya.edu.tr

Geliş Tarihi: 07.11.2018 Kabul tarihi: 04.07.2019 Yayınlanma Tarihi: 30.07.2019

Özet
Bilişim teknolojileri hayatımızın her alanında kullanılmasıyla birlikte pek çok güvenlik problemine neden olmaktadır. Bu yüzden öğrencilerin, bilişim teknolojilerini güvenli kullanabilmesi önemli bir konu haline gelmiştir. Bu araştırma, Bilgisayar Teknolojileri ve Bilişim Sistemleri bölümü öğrencilerinin bilişim güvenliği yeterliliklerini belirlemek amacıyla gerçekleştirilmiştir.
Araştırmanın çalışma grubu Trakya Üniversitesinde lisans eğitimi gören 210 öğrenciden oluşmaktadır. Araştırma nicel araştırma yöntemlerinden tarama modeli ile gerçekleştirilmiştir. Veriler, Pusey ve Sadera'nın geliştirdiği "Bilişim Güvenliği Eğitimi Verebilme Yeterliliği Algısı" ölçeğinin Gökmen ve Akgün tarafından (Gökmen ve Akgün; 2015) Türkçe'ye uyarlanan formu ile toplanmıştır. Ölçek, 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; öğrencilerin büyük çoğunluğunun, bilişim güvenliğini sağlamaya yönelik bir kurs veya ders almadıkları tespit edilmiştir. Bunun yanında öğrencilerin birçoğunun, bilişim güvenliği bilgilerinin düşük düzeyde olduğu görülmüştür. Bu sonuçlardan yola çıkarak, Bilgisayar Teknolojileri ve Bilişim Sistemleri lisans programında bu konuya yönelik zorunlu bir dersin olmasının faydalı olacağı düşünülmektedir.

Anahtar Kelimeler: Bilişim Güvenliği, Farkındalık, Bilişim Güvenliği Yeterliliği

[1] Bu çalışma 12. Uluslararası Bigisayar ve Öğretim Teknolojileri Sempozyumunda sözlü olarak sunulmuştur.

Ege Eğitim Teknolojileri Dergisi
Journal of Ege Education Technologies

Volume 3, Issue 1, July 2019, Pages 20- 27

Investigation of Computer Technologies and Information Systems Students' Competences in Information Security

Abstract
Information technologies are used in every area of our life and cause many security problems. Therefore, the ability of students to use information technology safely has become an important issue. This research was carried out in order to determine the computer security competencies of students of Computer Technologies and Information Systems Department.
The study group of the study consisted of 210 students who had undergraduate education at Trakya University. The research was carried out using a survey model from quantitative research methods. The data were collected using a data collection tool adapted to Turkish by Gökmen and Akgün. (Gökmen and Akgün; 2015) . The survey consists of 76 questions with 7 questions and 4 rating features that measure information security knowledge. In the analysis of the data, Kruskal Wallis H-Test and Mann Whitney U-Test were used to determine whether the information security data of the candidates showed significant differences according to various variables while the percentage, frequency and mean values were used. According to the results, the majority of students haven't taken any course or lecture about information security. According to the results, the majority of students haven't taken any course or lecture about information security. Furthermore, students is not well enough in information security topics. Based on the results, it is thought that it will be useful to put a compulsory course for this subject to Computer Technologies and Information Systems Department

Keywords: Information Security, Awareness, Information Security Efficiacy

Giriş

Bilişim teknolojilerinde zaman içinde baş döndürücü hızda gelişmeler yaşanmıştır. Bu gelişmeler neticesinde farklı işlev ve amaçları bünyesinde barındıran teknolojileri adım attığımız her yerde görmemiz mümkündür. Bu teknolojileri kullananların, zaman ve mekân sınırlaması olmadan hızlı ve de kolay şekilde gerekli bilgiye ulaşabilmeyi mümkün kılmaktadır. Bilişim teknolojilerinin kullanım alanındaki sınırsızlığa yakın genişlik ve sunduğu imkânlar, bilişim teknolojilerinin bankacılık işlemlerinde, e-devlet uygulamalarında, uzaktan eğitimde, online yemek siparişi gibi çok fazla alanda rol almasına ve vazgeçilemez araçlar olmasına yol açmaktadır.

Bilişim teknolojilerinin kullanımın artmasıyla her alanda üretilen bilgi miktarında hızlı bir artış olmaktadır. Bilgi toplumunda hayatımızdaki pek çok işlemin kolaylaşmasıyla birlikte bilgi güvenliğine karşı çeşitli boyutlarda risk ve tehditler oluşmaktadır. Kullanıcıların oluşan bu risk ve tehditleri farkında olmamasında dolayı çoğunlukla maddi kayba uğramalarına ya da bilgilerinin değiştirilmesi, silinmesi ya da bilgilerine izinsiz olarak erişilmesi gibi istenmeyen bazı durumlara maruz kalabilmektedir. Bu teknolojiler vasıtasıyla işlenen suçlar bireylere, bireylerin mülkiyet haklarına, kurumlara, kurumların teknik sistemlerine karşı işlenebilmektedir (Pati, t.y). Bilgisayar ve internet kullanılarak bu teknolojiler vasıtasıyla gerçekleştirilen suçlara bilişim suçu denmektedir (Maheshwari, Hyman ve Agrawal (2011) .

Bilişim suçları farklı şekil ve yapılarda işlenebilmektedir. Ayrıca bu suçların işlenmesinde yöntemler farklılık gösterebilmektedir. Son yıllarda su, gıda, enerji ve sağlık hizmetleri gibi önemli altyapılara, bulut bilişim teknolojilerine, mobil teknolojilere ve sosyal ağlara yapılan suç teşkil eden saldırılar gün geçtikçe artmaktadır. (Marinos, 2013) Genel olarak bakıldığında bilişim teknolojilerinde suç teşkil eden durumları özetlemek mümkündür. Bunlar; casus yazılımlar, arka kapılar, zararlı yazılımlar, sistem aracı gibi kendini gösteren rootkitler, e-posta bombardımanı, uzaktan yönetim araçları, veri trafiğinin izlenmesi, veri trafiğini izlerken gizlenme, bireylerin sahte adreslere yönlendirilmesi, reklam bedelli yazılımlar ve de sql kodlarının kullanılarak sistem kodlarına ulaşılması gibi yöntem ve araçlardır. (Richardson, 2008; Canbek, 2005; Kaçakcılık ve Organize Suçlar Daire Başkanlığı, 2011)

Bilgi güvenliği açıklarına sebebiyet veren birçok etken olmasına rağmen yapılan analizler sonucunda kullanıcı davranışlarının ilk sıralarda olduğu görülmüştür (Adams ve Sasse, 1999; Maxion ve Reeder, 2005). Ayrıca kullanıcıların bilişim güvenliği konusundaki farkındalıklarının ve bilgilerinin düşük düzeyde olduğu anlaşılmıştır(Dijle ve Doğan 2011; Karaoğlan-Yılmaz, Yılmaz ve Sezer, 2014; Pusey ve Sadera, 2011; Shehri, 2012; Tekerek ve Mart, 2010; Tekerek ve Tekerek, 2013). Yapılan başka bir araştırmada kurumların ve kullanıcıların bilgi güvenliği konusunda bilgilendirme ve gerekli önlemleri alma konusunda eğitilmesi ve farkındalıklarının yükseltilmesi gerekli olduğu anlaşılmıştır.(Chou, Chan ve Wu, 2007; Wishart, Oades ve Morris, 2007). Son olarak da bilgi güvenliğinin kişiler üzerinde oluşturabileceği olası etkilerden ve bireylere küçük yaşlardan itibaren eğitiminin verilmesi gerektiği üzerinde durulmuştur. (Ceylan, 2013; Çelen, Çelik ve Seferoğlu, 2011; Demirel, Yörük ve Özkan, 2012; Öğün ve Kaya, 2013; Şahinaslan, Kandemir ve Şahinaslan, 2009; Vural ve Sağıroğlu, 2008)

Artan bilişim güvenliği tehditleri, Uluslararası Eğitimde Teknoloji Topluluğu standartları, kamu kurum ve özel sektörde verilerin çok önemli olduğu dikkate alındığında Bilgisayar Teknolojisi ve Bilişim

Sistemleri lisans öğrencilerinin bilişim güvenliği bilgilerinin incelenmesinin önemli olduğu düşünülmektedir.

Bu çalışmanın amacı, gelecekte iş hayatında ve okullarda istihdam edilecek olan Bilgisayar Teknolojileri ve Bilişim Sistemleri bölümü öğrencilerinin bilişim güvenliği konusunda yeterlilik algılarının tespit edilmesidir. Bu amaç doğrultusunda Bilişim güvenliği bilgilerinin yaş, cinsiyet, bilişim güvenliğine yönelik bir kurs veya ders alıp almama, günlük bilgisayar kullanım süresi, günlük internet kullanım süresi ve virüs taraması sıklığı değişkenlerine göre anlamlı bir farklılık gösterip göstermediği tespit edilmiştir.

YÖNTEM

Katılımcılar

Araştırmanın çalışma grubunu Trakya Üniversitesi Keşan Yusuf Çapraz Uygulamalı Bilimler Yüksekokulu Bilgisayar Teknolojisi ve Bilişim Sistemleri bölümü 1. 2. 3. ve 4. sınıfta okuyan 210 öğrenci oluşturmaktadır.

Veri Toplama Araçları

Araştırmada nicel araştırma yöntemlerinden tarama modeli kullanılmıştır. Araştırmanın başında ölçek aracılığıyla öğrencilerin bilişim güvenliği yeterliliklerine yönelik bilgiler toplanmıştır. Bu araştırmada veriler, Pusey ve Sadera'nın (2011) geliştirdiği "Bilişim Güvenliği Eğitimi Verebilme Yeterliliği Algısı" ölçeğinin Türkçe'ye uyarlanan formu ile toplanmıştır (Gökmen ve Akgün; 2015).

Veri Analizi

Araştırmada veri analizi SPSS 20 programı kullanılmıştır. Bu kapsamda öncelikle araştırmaya katılan 210 öğrencinin demografik özelliklerine ilişkin frekans dağılımı gerçekleştirilmiştir. Daha sonra ölçek verilerine faktör analizi uygulanmıştır ve faktörlerin ağırlık değerleri dikkate alınarak ölçekteki bazı değerler çıkarılmıştır. Bu işlemimin ardından kalan 60 soruya bağlı olarak saldırı yöntemleri, güvenlik, hırsızlık, casus yazılımlar, bilgi saklama, yasalar, güvenlik duvarı, şifreleme ve erişim izni olmak üzere dokuz adet faktör bulunmuştur. Daha sonra belirtilen dokuz alt boyuta ilişkin güvenilirlik analizleri gerçekleştirilmiştir. Alt boyutlara bağlı olarak yapılan güvenilirlik analizleri sonucunda Cronbach's Alpha değeri 0.961 olarak bulunmuştur. Bu durum bize güvenilirliğin iyi düzeyde olduğunu göstermektedir.

BULGULAR

Araştırmanın bu bölümünde, örneklem grubunu oluşturan öğrencilerin demografik özelliklerini (cinsiyeti, yaşı, günlük bilgisayar kullanım süresi, günlük internet kullanım süresi, bilişim güvenliği kursu/dersi alması ve kişisel bilgisayar virüs tarama güncelleme sıklığı) betimleyici frekans ve yüzde dağılımları çıkarılmış ve yorumlanmıştır. Örneklem grubunu oluşturan öğrencilerin 102'si (%48,6) kadın; 108'i (%51,4) erkek olmak üzere toplam 210 kişiden oluşmaktadır. Öğrencilerin 152'si (%72,4)

21-23 yaş aralığında olduğu, 102'si (%48,6) günde 1-3 saat bilgisayar kullandığı, 84'ü (%40,0) günde 4-6 saat internet kullandığı, 150'si (%71,4) bilişim güvenliği veya kursu almadığı, 60'ı (%28,6) virüs taramasını haftalık olarak yaptığı anlaşılmıştır.

Yapılan KMO ve Bartlett's testi sonucunda KMO değeri 0.896 olarak elde edilmiştir. Elde edilen değer bize veri seti için faktör analizi yapılabileceğini ifade etmektedir. Ayrıca Barlett's testinin değeri p< 0.05 olduğu ve değişkenler arasında faktör analizi yapmak için yeterli düzeyde ilişki olduğu sonucuna ulaştırmaktadır. Analiz sonucunda dokuz adet faktör bulunmuştur. Faktörler toplam varyansın %63.235'sini açıklamaktadır. Ayrıca buradaki faktörler için yapılan Kolmogorov-Smirnov normal dağılım test sonuçlarına göre tüm faktör değerlerinin p<0.05 koşulunu sağladığı görülmektedir. Bu durumda ölçeğin normal dağılım göstermediği ve parametrik testlerin uygulanmasının doğru olamayacağına karar verilmiştir. Bu durumda çözümlemeler non-parametrik teknikler kullanılarak yapılmıştır.

Ölçeklerden alınan puanların cinsiyete göre değişip değişmediğini belirlemek için bağımsız gruplar t-testinin parametrik olmayan alternatifi olarak Mann-Whitney U Testi uygulanmıştır.

Tablo 1. Mann-Whitney U Testi

	F1	F2	F3	F4	F5	F6	F7	F8	F9
Mann-Whitney U	3677,0	4955,0	3303,0	3803,0	4253,5	3906,5	3760,0	4188,0	3769,0
WilcoxonW	8930,0	10208,0	8556,0	9056,0	9506,5	9159,5	9013,0	9441,0	9022,0
Z	-4,163	-1,304	-4,939	-3,893	-2,866	-3,693	-3,895	-3,078	-3,802
Asymp. Sig. (2-tailed)	,000	,192	,000	,000	,004	,000	,000	,002	,000

Tablo 1'de yer alan değerlere göre F2 için ulaştığımız verilerde Asymp. Sig. (p) değeri 0,05'den büyük olduğundan dolayı bu hipotezler reddedilmez fakat diğer faktörlerin Asymp. Sig. değeri 0,05'den küçük olduğundan bu faktör için hipotez reddedilecektir. F2 de bulunan sorular için bay ve bayan öğrencilerin bilişim güvenliği yeterliliği değerlerinin ortancalarının eşit olmadığına karar verilmiştir.

Tablo 2. Bilişim Güvenliği Kursuna Gitme Düzeyi için Kruskal Wallis Tek Yönlü Varyans Analizi

	F1	F2	F3	F4	F5	F6	F7	F8	F9
Chi-Square	10,985	3,847	13,090	5,548	14,736	11,034	9,403	6,166	10,792
Df	1	1	1	1	1	1	1	1	1
Asymp. Sig.	,001	,050	,000	,019	,000	,001	,002	,013	,001

Tablo 2'de yer alan değerlere göre p<0,05 olduğundan katılımcıların bilişim güvenliği kursuna gitme düzeyi ile faktörler arasında anlamlı bir fark olduğu görülmüştür. Bu durum da tüm alt hipotezlerinin kabul edildiği anlamını vermektedir. Faktörlerin önem değerleri 0,05'ten küçük olduğu için bu

hipotezler kabul edilmeyecektir. Öğrencilerin bu faktördeki sorulara verdiği cevaplarda anlamlı farklılık bulunmamaktadır. Bilişim güvenliğine yönelik kurs alan öğrencilerin bilgi düzeylerinin, bu kursu almayan öğrencilerin bilgi düzeylerine göre bir fark oluşturmadığını görülmüşür. Ayrıca öğrencilerin almış oldukları kursların, öğrencilerin bilgilerini ve yeterliliklerini artıracak bir düzeyde ve içerikte olmadığı yönünde bir yorum yapılabilir. Ancak bu bulgunun daha iyi anlaşılabilmesi için öğrencilerin aldıkları kursun içeriğinin incelenmesi gerekmektedir.

Sonuç Tartışma ve Öneriler

BTBS öğrencilerinin bilişim güvenliği yeterliliklerinin incelendiği bu araştırmada öğrencilerin cinsiyet, yaş, günlük bilgisayar kullanım süresi, günlük internet kullanım süresi, bilişim güvenliği kursu veya dersi alması ve bilgisayarınızdaki virüs tarama yazılımını güncelleme sıklığı olmak üzere 6 adet demografik özellikleri kullanılmıştır. Araştırmaya katılanların çoğu erkek, yaş aralığı 21-23, günlük internet kullanım sıklığı 4-6 saat, günlük bilgisayar kullanım sıklığı 1-3 saat, bilişim güvenliği dersi veya kursu almadığı ve kişisel bilgisayarındaki virüs tarama yazılımını güncelleme sıklığının haftalık olduğu tespit edilmiştir.

Yapılan analizler sonucunda dokuz adet faktör bulunmuştur. Faktör analizlerinin ardından demografik özelliklerin faktörlere olan etkisini bulmak için fark testleri uygulanmıştır.

Araştırmanın sonuçlarına göre Bilgisayar Teknolojileri ve Bilişim Sistemleri bölümü öğrencilerinin, bilişim güvenliği bilgi düzeylerinin cinsiyete göre farklılaştığı görülürken Mart'ın (2012) bulgularında cinsiyet açısından bilgi düzeylerinin değişmediği ifade edilmiştir.

Günlük Bilgisayar kullanım süresine ve günlük internet kullanım süresine göre bilişim güvenliği bilgi düzeyleri incelendiğinde bir farklılaşma görülmemiştir. Bu bulguya benzer olarak Mart (2012) bilgi güvenliği farkındalığı ile bilgisayar ve internet kullanımı arasında bir fark olmadığı belirtilmiştir.

Araştırmanın bir başka sonucu, öğrencilerin bilişim güvenliği bilgilerinin düşük düzeyde olduklarıdır. Bilişim güvenliğini tehdit eden unsurların ve bilişim suçlarının günümüzde arttığı göz önüne alındığında, Bilgisayar Teknolojileri ve Bilişim Sistemleri öğrencilerinin bilgilerinin ve yeterliliklerinin beklenen düzeyde olmaması araştırmadan çıkarılabilecek en önemli sonuç olarak görülmektedir.

Alan yazında yapılan çalışma sonuçlarına göre bilişim güvenliği farkındalığı kazandırmaya yönelik bilgilendirme faaliyetlerinin yapılması ve eğitimlerin verilmesi gerekli olduğu belirtilmiştir(Bilek, 2012; İlbaş, 2009; Dijle ve Doğan, 2011; Gökmen, 2014). Öğütçü (2010) bireysel olarak herkesin kişisel bilişim güvenliği bilgi düzeylerini artırılması ve bununla birlikte tüm toplumun güvenli bilgisayar ve internet kullanımını sağlayacak eğitimlerin verilmesinin bir devlet politikası olması gerektiğini belirtmektedir.

Bu araştırmada Bilişim güvenliğine yönelik kurs alan öğrencilerin bilgi düzeylerinin, bu kursu almayan öğrencilerin bilgi düzeylerine göre bir fark oluşturmadığını görülmüşür. Bu yüzden öğrencilerin almış oldukları kursların, öğrencilerin bilgilerini ve yeterliliklerini artıracak bir düzeyde ve içerikte olmadığı yönünde bir yorum yapılabilir. Bu noktada bilişim güvenliği eğitimleri verilmeden önce hedef kitleye uygun konuları içeren ve ihtiyaçlara yönelik eğitim programının belirlenmesi faydalı olacaktır. Bu

konuda Şahinaslan ve diğer. (2009) temel bir bilişim güvenliği farkındalık eğitiminde; temel bilgi kavramları, bilginin korunacak nitelikleri, bilişim güvenliğine ilişkin güncel tehditler ve saldırılar, sosyal mühendislik, fiziksel güvenlik, şifre güvenliği, yasal düzenlemeler gibi konulara değinilmesi ve bu bilgilerin örneklerle zenginleştirilerek aktarılması gerektiğini belirtmektedirler.

Araştırma sonuçlarından yola çıkarak, Bilgisayar Teknolojileri ve Bilişim Sistemleri öğrencilerinin bu konularda yeterli bilgi sahibi olmalarını ve bilişim güvenliğini sağlamaları amacıyla Bilgisayar Teknolojileri ve Bilişim Sistemleri 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 çalışmalarının yapılması oldukça yararlı olacaktır.

Kaynakça

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

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

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

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

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

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

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

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

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

Gökmen, Ö. F. ve Akgün, Ö. E. (2015). Bilgisayar ve öğretim teknolojileri eğitimi öğretmen adaylarının bilişim güvenliği eğitimi verebilmeye yönelik yeterlilik algılarının incelenmesi. İlköğretim Online, 14(4), 1208-1221.

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

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

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

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.

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

Marinos, L. (2013). ENISA Threat Landscape 2013: Overview of current and emerging cyber-threats. Heraklion: European Union Agency for Network and Information Security Publishing. doi:10.2788/14231.

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

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

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

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

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

Richardson, R. (2008). CSI computer crime and security survey

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

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

Tekerek, M. ve Mart, İ. (2010). K8 düzeyi için davranışsal bilgisayar ve internet güvenliği farkındalığı, 4.uluslararası bilgi güvenliği ve kriptoloji konferansı bildirileri. 6-8 mayıs 2010, orta Doğu Teknik Üniversitesi. Ankara.

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

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

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