Kasım 2017 Cilt:25 No:6 Kastamonu Eğitim Dergisi 2079-2094

Üniversite Öğrencilerinin Siber Güvenlik Davranışlarının İncelenmesi[1]

Investigation of Cyber Security Behaviors of University Students

Abdulkadir KARACI
Kastamonu Üniversitesi, Mühendisilik Mimarlık Fakültesi,Bilgisayar Mühendisliği Bölümü, Kastamonu, Türkiye.

Halil İbrahim AKYÜZ, Göksel BİLGİCİ
Kastamonu Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, Kastamonu, Türkiye.

Makale Geliş Tarihi: 10.02.2017 ***Yayına Kabul Tarihi: 10.08.2017***

Özet

Siber güvenlik, bilgi kaynaklarının korunmasını ve kişinin kendisi de dahil olmak üzere diğer varlıkların korunmasını kapsamaktadır. Bu çalışmada, bilişim teknolojileri ile ilgili bir bölümde öğrenim gören üniversite öğrencilerinin siber güvenlik davranışları farklı değişkenler açısından incelenmiştir. Çalışma gurubunu bir devlet, bir vakıf üniversitesinin Bilgisayar Mühendisliği ile Bilgisayar ve Öğretim Teknolojileri Öğretmenliği (BÖTE) bölümlerinde öğrenim gören toplam 170 öğrenci oluşturmaktadır. Verilerin toplanmasında Siber Güvenlik Ölçeği (SGÖ) kullanılmıştır. Çalışmanın sonuçlarına göre öğrencilerin siber güvenliğe yönelik davranışlarının siber güvenliği sağlayacak düzeyde olduğu görülmektedir. Faktörlere göre daha ayrıntılı bir inceleme yapıldığında, öğrenciler kişisel gizliliklerini koruyabilmektedirler. Ayrıca güvenilmeyen uygulamalardan kaçınmakta ve güvenlik için önlem alabilmektedirler. Bunun yanı sıra kredi kartı veya banka kartı gibi ödeme bilgilerini koruyabilmekte ve İnternet üzerinde gezinirken arkalarında iz bırakmamaktadırlar. Erkek ve kızların siber güvenlik davranışları arasında anlamlı bir farklılık yoktur. Kişisel güvenliği koruma faktörü açısından BÖTE bölümünde kızlar, Bilgisayar Mühendisliği bölümünde ise erkekler daha olumlu siber güvenlik davranışına sahiptirler. İnternet-bilgisayar güvenlik eğitimi alan veya bu konuda iş deneyimi olan öğrencilerin siber güvenlik davranışları daha olumludur. Farklı sınıflarda öğrenim gören öğrencilerin siber güvenlik davranışları arasında anlamlı bir farklılık bulunmamaktadır. Meslek lisesinden mezun olan öğrencilerin iz bırakmama faktörü açısından genel/düz liseden mezun olan öğrencilere göre daha dikkatli oldukları görülmektedir.

Anahtar Kelimeler*: siber güvenlik, güvenli İnternet, bilgi güvenliği*

Abstract

Cyber security is a concept that involves the safety of information resources and the protection of all kinds of entities including individuals. This study examines the cyber

1. Bu çalışma ICITS 2017 Sempozyumunda sözlü bildiri olarak sunulmuştur.

security behaviors of undergraduate students who study in Information and Communication Technologies (ICT)-related programs. The sample consists of 170 students of Computer Engineering and Computer Education and Instructional Technologies (CEIT) from one public and one private universities. The Cyber Security Scale (CSS?) was employed for measuring students' cyber security behaviors. Results indicate that the level of student behaviors are adequate for ensuring cyber security. Detailed factor analysis reveals that students can protect their personal and private information. They also avoid using threatening applications and take measures regarding security. Moreover, they protect payment information of credit or debit cards and do not leave digital footprints while browsing the Internet. No significant difference was found between genders in terms of cyber security behavior. With respect to the protection of personal security factor, female students in CEIT and male students in Computer Engineering demonstrated more positive cyber security behaviors. Students with previous training or work experience in the fields of Internet/computer security showed more positive cyber security behaviors. There is no significant difference in students' cyber security behaviors across study years. Vocational high school graduates are more cautious than regular high school graduates in terms of avoiding leaving digital footprints.

***Keywrods**: Cyber security, secure Internet, information security*

1. Giriş

Internet ve bilgisayar kullananların sayısı dünyada ve Türkiye'de hızla artmaktadır. Türkiye İstatistik Kurumu'nun 18 Ağustos 2016'da yayınladığı rapora göre 2016 yılında Türkiye' de İnternet kullanım oranı 16-74 yaş grubundaki bireylerde %61,2'dir. Bu oran 2012 yılında %47,4'dür (TUİK, 2016). Bu açıdan bakıldığında İnternet kullanım oranı son beş yılda %13,8 oranında artmıştır. İnternet kullanımının giderek artması, sınırsız, denetimsiz ve yasaksız her türlü bilgiye ve kişilere erişimin kolaylığı, çok olumlu gelişmelerin yanında bazı olumsuz sonuçların doğmasına da neden olabilmektedir. Yasal olmayan, şiddet ve cinsellik içeren sitelere kolay erişim, tehlikeli insanlarla iletişim, oyunlara aşırı bağımlılık başta gelen riskler arasındadır. Öte yandan uyuşturucu kullanımı ve terör gibi yasal olmayan yollara destek arayanlar Internet'i propaganda aracı olarak kullanmaktadırlar (Çelen, Çelik, Seferoğlu, 2011; Mert, Bülbül, Sağıroğlu, 2012).

Siber güvenlik terimi, bilgi güvenliği terimi ile sık sık birbirinin yerine kullanılır. Siber güvenlik ve bilgi güvenliği arasında önemli bir örtüşme olmasına rağmen, bu iki kavram tamamen benzer nitelikte değildir. Siber güvenlik, yalnızca bilgi kaynaklarının korunmasını değil, aynı zamanda kişinin kendisi de dahil olmak üzere diğer varlıkların korunmasını da kapsayarak geleneksel bilgi güvenliği sınırlarının ötesine geçer (Solms ve Niekerk, 2013). Siber güvenlik sadece İnternet güvenliğini değil tüm iletişim altyapılarını kapsayan geniş bir kavramdır (Hekim ve Başıbüyük, 2013).

Siber güvenlik, "siber ortamda, kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünüdür" şeklinde tarif edilebilir. Siber saldırı, "hedef seçilen şahıs, şir-

ket, kurum, örgüt, gibi yapıların bilgi sistemlerine veya iletişim altyapılarına yapılan planlı ve koordineli saldırılardır". Siber savaş, "Aynı saldırıların ülke veya ülkelere yönelik yapılmasıdır". Siber savaşta hedef ülkelerin güvenlik, sağlık, enerji, haberleşme, su ve kanalizasyon, bankacılık ve kamu hizmetleri gibi kritik altyapıları saldırı alanı olarak seçilmektedir (Yılmaz ve Sağıroğlu, 2013).

Internet kullanıcıları genel olarak zararlı yazılımlar ile ilgili güvenlik önlemlerinin farkındadırlar fakat İnternet üzerinden oluşabilecek tehlikeler hakkında farkındalıkları yetersizdir (Erol, Şahin, Yılmaz ve Haseki, 2015). Akamai (2016)'nin raporuna göre kaynak IP adreslerine en fazla saldırı gerçekleşen ilk beş ülke; %16 (115478) ile Çin, %10 (72598) ile ABD, %5 (43400) ile Türkiye, %5 (36472) ile Brezilya ve %4 (31692) ile Güney Kore'dir. Bu sıralamaya bakıldığında Türkiye 3. sırada yer almaktadır. Ülke olarak bilişim altyapılarına ve İnternete olan bağımlılığımız artmakta ve buna bağlı olarak siber alanda taşıdığımız risklerimiz de giderek büyümektedir. Bu yüzden siber güvenlik son yıllarda en fazla tartışılan konulardan birisi haline gelmiştir. Ancak siber güvenlik konusu Türkiye'de gereken önemi görmemekte, sadece sansasyonel olaylar ertesinde gündeme gelmektedir (Hekim ve Başıbüyük, 2013).

Mobil cihazların artması ve "nesnelerin İnterneti" kavramının uygulanması ile insanoğlu tamamen fiziksel dünyanın dışında bir siber-dünyada yaşamaya başlamıştır. Siber dünyanın bu beklenmedik genişlemesi, her türlü siber saldırı karşısında savunmasız kalmasına neden olmaktadır. Bugün, siber saldırganların ve siber saldırıların sayısı artmasına rağmen saldırganların bilgi düzeyleri azalmaktadır (Göztepe ve ark., 2014). Yılmaz, Şahin ve Akbulut (2016), Milli Eğitim Bakanlığı'na bağlı okullarda görev yapan öğretmenlerin dijital veri güvenliği farkındalıklarını araştırdıkları çalışmada, öğretmenlerin dijital veri güvenliği farkındalıklarının oldukça yüksek olduğunu belirtmişler. Farkındalıkların, günlük bilgisayar kullanım süresi, günlük İnternet kullanım süresi, cinsiyet, ve farklı teknolojilere sahip olma durumlarına göre farklılaştığını; öğrenim kademesi, branş, mesleki kıdem ve öğrenim durumu açısından farklılaşmadığını ifade etmişlerdir. Gökmen, Akgün (2016), BÖTE öğretmen adaylarının bilişim suçlarıyla ilgili tecrübelerini ve bilişim güvenliği dersi içeriğine yönelik görüşlerinin tespit etmek için gerçekleştirdikleri nitel araştırmaya göre, öğrencilerinin çoğunluğunun bilişim güvenliği ile ilgili bir ders almadığını, bilişim güvenliği hakkında bazı teknik konularda bilgi sahibi olmadıklarını ve bilişim güvenliği öğretebilme konusunda da yetersiz olduklarını belirtmişlerdir. Siber güvenliğin sağlanması için öncelikle bu konu da bilgi sahibi olması gerekenler bilgisayar konusunda eğitim veren bilişim teknolojileri öğretmenleri ve birçok firmada uzman görüşüne başvurulan bilgisayar mühendisleridir. Bilişim teknolojileri öğretmen adayları ve bilgisayar mühendisi adaylarının siber güvenlik düzeylerinin ortaya konulması önemlidir.

Kuru ve Ocak (2016), Türkiye'deki kamu çalışanlarının siber güvenlik ve siber uzay unsurları konusundaki farkındalıklarını araştırdıkları çalışmada, çalışanların siber güvenlik ve siber savaş hakkında yeterli bilgiye sahip olduğunu belirtmişlerdir. Elde etikleri bulgular, siber savunma politikasının diğer devlet kurumlarıyla koor-

dineli olarak planlanması ve deneyimlerin paylaşılması gerektiğini açıkça göstermektedir. Ayrıca kamu görevlilerinin siber güvenlikle ilgili eğitim ve öğretimlerini en önemli mesele olarak görmüşlerdir. Kariyerleri süresince yeterli eğitim verilmesi gerektiğini ve üniversitelerin müfredatıyla ilgili düzenlemelerin yapılması için bir an önce harekete geçilmesinin gerekliliğini vurgulamışlardır.

Akın ve ark. (2013), siber durum farkındalığını artırmaya yönelik bayrağı yakala (BY) yarışmalarını ayrıntılı olarak incelemiş ve bu kapsamda kurum içi farkındalık çalışması uygulamışlardır. Siber güvenlik alanında çalışan ve gerçek sistemlere saldırı yapma imkanı olmayan personel için düzenlenecek bayrağı yakalama yarışmaları ile bilgi düzeyi ve farkındalığın artırılabileceğini öne sürmüşlerdir. Yılmaz ve Sağıroğlu (2013), siber güvenlik konusunda uygulanması önerilen evrensel kuralları, siber kaynakların risk analizini, tehdit ve hazırlık seviyelerinin neler olduğunu ve siber tehdit araçlarını incelemişlerdir. Önaçan ve Atan (2016), kurum ve devletlerin siber uzaydaki saldırılardan maddi ve manevi etkilendiği ve zarara uğradığını, bu tür zararlardan korunabilmek için siber güvenlik farkındalığının artırılması, bilgi ve bilinç seviyesinin yükseltilmesi gerektiğini vurgulamışlardır. Bunun için de hem son kullanıcıların bilgilendirilmesi ve bilinçlendirilmesini hem de siber güvenlik alanında nitelikli, uzman personel ihtiyacının karşılanmasını sağlayacak eğitim ihtiyacının ortaya çıktığını belirtmişlerdir.

Güldüren ve ark. (2016), ortaöğretim kurumlarında öğrenim gören öğrencilerin bilgi güvenliği farkındalık düzeylerini belirlemeye yönelik çalışmada, öğrencilerin cinsiyetlerine göre bilgi güvenliği farkındalıkları arasında anlamlı bir farklılığın olduğunu tespit etmişlerdir.

Gökmen ve Akgün(2016), eğitim fakültesinde öğrenim gören öğretmen adaylarının bilişim suçlarıyla ilgili deneyimlerini ve bilişim güvenliği dersi içeriğinde yer alması gereken konulara yönelik görüşlerini tespit etmişlerdir. Ayrıca öğretmen adaylarının birçoğunun bilişim güvenliğinin tanımı ve kapsamı konusunda yetersiz bilgiye sahip olduklarını belirtmişlerdir. Çiftci ve Sakallı (2016), sınıf öğretmeni adaylarının dijital vatandaşlık düzeyleri ile siber zorbalık eğilimleri arasında düşük düzeyde, pozitif yönlü ve anlamlı bir ilişki olduğu bulmuşlardır. Ayrıca kız sınıf öğretmeni adaylarının siber zorbalık tutum düzeylerinin, erkek sınıf öğretmeni adaylarından daha yüksek olduğunu tespit etmişlerdir. Peker (2015) ortaokul öğrencilerinin yaşadığı suçluluk, üzüntü, kızgınlık gibi negatif duyguların artmasıyla birlikte siber zorbalık davranışlarının da artacağını ifade etmiştir.

Bu araştırmanın amacı Bilgisayar ve Öğretim Teknolojileri Eğitimi (BÖTE) ve Bilgisayar Mühendisliği bölümlerinde okuyan üniversite öğrencilerinin siber güvenlik ile ilgili davranışlarını bazı değişkenlere göre incelemek ve sonuçları değerlendirmektir.

Bu amaca bağlı olarak araştırmanın problem cümlesi aşağıdaki gibidir.

- BÖTE ve Bilgisayar Mühendisliğinde öğrenim gören öğrencilerin siber güvenlik davranışları nasıldır?

Araştırmanın alt problemleri ise aşağıdaki şekilde belirlenmiştir.

- Kız ve erkek öğrencilerin siber güvenlik davranışları arasında anlamlı fark var mıdır?
- Bilgisayar ya da İnternet güvenliğine yönelik alınan eğitim veya iş deneyimine göre siber güvenlik davranışları arasında anlamlı fark var mıdır?
- Öğrencilerin öğrenim görmekte olduğu sınıfa göre siber güvenlik davranışları arasında anlamlı fark var mıdır?
- Öğrencilerin mezun olduğu lise türüne göre siber güvenlik davranışları arasında anlamlı fark var mıdır?
- Internet kullanım yılına göre siber güvenlik davranışları arasında anlamlı fark var mıdır?

2. Yöntem

Araştırma nicel araştırma yöntemlerinden tarama araştırmasına göre desenlenmiştir. Tarama araştırmaları, bir grubun belli özelliklerini belirlemek için verilerin toplanmasını amaçlayan çalışmalardır (Büyüköztürk, vd., 2008).

Çalışma Grubu

Araştırmanın çalışma grubunu 2016-2017 öğretim yılı güz döneminde Kastamonu Üniversitesi Bilgisayar Mühendisliği, Bilgisayar ve Öğretim Teknolojileri Eğitimi (BÖTE) bölümleri ile Ahmet Yesevi Üniversitesi Bilgisayar Mühendisliği bölümünde öğrenimlerini sürdüren 170 öğrenci oluşturmaktadır. Çalışma grubunun demografik dağılımları Tablo 1'de verilmiştir.

Tablo 1. Çalışma Grubunun Bölüm ve Cinsiyete Göre Dağılımı

Bölüm	Cinsiyet		Toplam
	Kız	Erkek	Öğrenci Sayısı
Bilgisayar Mühendisliği	34	46	80
B.Ö.T.E	25	35	60
Bilgisayar Mühendisliği Uzaktan Eğitim	8	22	30
Toplam Öğrenci Sayısı	67	103	170

Veri Toplama Aracı

Veri toplamada kullanılan ölçme aracı iki bölümden oluşmaktadır. Birinci bölümünü cinsiyet, bölüm, sınıf, mezun olunan lise türü, kaç yıldır İnternet kullanıldığı ve bilgisayar güvenliği ya da İnternet güvenliğine yönelik alınan eğitim veya iş deneyimine ilişkin soruların yer aldığı kişisel bilgi bölümü oluşturmaktadır. İkinci

bölümünde ise Erol vd. (2015) tarafından geliştirilen "Siber Güvenlik Ölçeği (SGÖ)" yer almaktadır. Toplam 25 madde bulunan 5'li likert tipindeki ölçek, "Kişisel Gizliliği Koruma", "Güvenilmeyenden Kaçınma", "Önlem Alma", "Ödeme Bilgilerini Koruma" ve "İz Bırakmama" olmak üzere 5 faktörden oluşmaktadır. Ölçeğin cronbach-α güvenirlik katsayısı 0.735'dir. Faktörlere göre ise sırasıyla 0,763; 0,771; 0,704; 0,829 ve 0,557 şeklinde ortaya konulmuştur.

Verilerin Analizi

Ölçeklerin istatistiksel anlaşılırlığını artırmak için 5'li likert ölçeklerde puan aralıkları "kesinlikle katılmıyorum (1,0-1,80)", "katılmıyorum (1,81-2,60)", "kararsızım (2,61-3,40)", "katılıyorum (3,41-4,20)" ve "kesinlikle katılıyorum (4,21-5,0)" şeklinde kategorize edilebilmektedir (Yenilmez, 2008; Özyurt, 2015). Bu nedenle bu çalışmadaki SGÖ için puan aralıkları "Hiçbir zaman (1,0-1,80)", "Nadiren (1,81-2,60)", "Ara sıra (2,61-3,40)", "Sık sık (3,41-4,20)" ve "Her zaman (4,21-5,0)" olacak şekilde belirlenmiştir.

Verilerin analizinde kullanılacak istatistiksel testlerin belirlenmesi amacıyla faktörlerin basıklık ve çarpıklık katsayıları hesaplanmıştır. Çarpıklık katsayısı -0,456, basıklık katsayısı ise -0,451 olarak bulunmuştur. Çarpıklık ve basıklık katsayılarının -1 ile +1 sınırları içinde kalması, puanların normal dağılım sergilediğini göstermektedir (Huck, 2012; Çaka, Doğan ve Şahin, 2016). Ayrıca Kolmogorov-Smirnov normallik testi sonuçlarına göre p>,05 bulunduğundan verilerin normal dağılım gösterdiği tespit edilmiştir. Buna göre veri analizinde bağımsız örneklem t-testi ve tek yönlü varyans analizi (ANOVA) kullanılmıştır.

3. Bulgular ve Tartışma

Öğrencilerin Siber Güvenlik Davranışları

Öğrencilerin SGÖ'den aldığı ortalama puanlar Tablo 2'de gösterilmektedir.

Tablo 2. Öğrencilerin SGÖ'den aldıkları puan ortalamaları

Faktör	N	Minimum	Maksimum	Ortalama
Kişisel Gizliliği Koruma	170	2,30	5,00	3,9824
Güvenilmeyenden Kaçınma	170	1,00	5,00	4,0529
Önlem Alma	170	1,40	5,00	3,6800
Ödeme Bilgilerini Koruma	170	1,00	5,00	4,1588
İz Bırakmama	170	1,75	5,00	3,9250
Siber Güvenlik Ölçeği	170	2,71	4,90	3,9598

Tablo 2'de görülen ortalama puanlar Yenilmez (2008) tarafından belirlenen puan aralıklarına göre "Sık sık" aralığına denk gelmektedir. Bu tablodaki ortalama puanlara göre tüm alt boyutlar da ve ölçeğin tamamında öğrencilerin siber güvenlikle ilgili maddelere olumlu cevap verdikleri görülmektedir. Buna göre, öğrencilerin siber gü-

venliğe yönelik davranışlarının siber güvenliği sağlayacak düzeyde olduğu söylenebilir. Alt faktörlere göre daha ayrıntılı bir inceleme yapıldığında, öğrenciler kişisel gizliliklerini koruyabilmektedirler. Ayrıca güvenilmeyen uygulamalardan kaçınmakta ve güvenlik için önlem alabilmektedirler. Bunun yanı sıra kredi kartı, banka kartı gibi ödeme bilgilerini koruyabilmekte ve İnternet üzerinde gezinirken arkalarında iz bırakmamaktadırlar. Bu sonuçlar Yılmaz ve ark. (2016) tarafından elde edilen sonuçlarla benzer iken Gökmen ve Akgün (2016) tarafından elde edilen sonuçlarla farklılık göstermektedir. Yılmaz ve ark. (2016), Milli Eğitim Bakanlığı'na bağlı okullarda görev yapan öğretmenlerin dijital veri güvenliği farkındalıklarını incelemişler ve öğretmenlerin dijital veri güvenliği farkındalıklarının oldukça yüksek olduğunu belirtmişlerdir. Gökmen ve Akgün (2016) ise eğitim fakültesinde öğrenim gören öğretmen adaylarının bilişim suçu işledikleri, bilişim suçuna maruz kaldıkları, bilişim suçu konusunda bilgilerinin olmadığı ve bir bilişim suçuyla karşılaştıklarında ne yapabileceklerini bilmediklerini tespit etmişlerdir. Ayrıca öğretmen adaylarının birçoğunun bilişim güvenliğinin tanımı ve kapsamı konusunda yetersiz bilgiye sahip olduklarını ifade etmişlerdir. Bu farklılık çalışma grubunun bilişim teknolojileri ile ilgili bir bölümde öğrenim gören öğrencilerden oluşmasından kaynaklanabilir.

Öğrencilerin siber güvenlik davranış düzeylerini belirlemek amacıyla ölçekten alınan puanlar faktörlere göre ayrı ayrı incelenmiştir. Bu inceleme sonucuna göre puan kategorileri ve frekansları Tablo 3'te gösterilmiştir.

Tablo 3. Katılımcıların siber güvenlik davranış düzeyi

Dilsel İfade	Faktör 1		Faktör 2		Faktör 3		Faktör 4		Faktör 5		Tamamı		Siber Güvenlik Düzeyi
	n	%	n	%	n	%	n	%	n	%	n	%	
Hiçbir zaman Nadiren	3	1,76	20	11,76	22	12,94	21	12,35	5	2,94	0	0,00	Olumsuz davranış
Arasıra	24	14,12	7	4,12	44	25,88	13	7,65	34	20,00	29	17,06	Belirsiz
Sıksık Her zaman	143	84,12	143	84,12	104	61,18	136	80,00	131	77,06	141	82,94	Olumlu davranış

Tablo 3'deki veriler incelendiğinde öğrencilerin %82,94'ünün siber güvenlik davranış düzeyi olumlu iken %17,06'sı belirsizdir. Olumsuz davranış gösteren öğrenci ise bulunmamaktadır. Bu durum öğrencilerin BÖTE ve bilgisayar mühendisliği bölümü öğrencileri olmasından kaynaklanabilir. Faktör 1(kişisel gizliliği koruma), Faktör 2 (güvenilmeyenden kaçınma) ve Faktör 4 (ödeme bilgilerini koruma)'e göre siber güvenlik davranışı olumlu olan öğrencilerin yüzdesi %80 ve daha fazladır. Bu açıdan bakıldığında öğrencilerin büyük bir çoğunluğunun kişisel gizliliklerini ve ödeme bilgilerini koruyabildikleri, ayrıca güvenilmeyen ortamlardan kaçınabildikleri görülmektedir. Olumsuz siber güvenlik davranışlarına sahip öğrencilerin oranı ise sırayla %1,76, %11,76 ve %12,35'tir. Ek olarak öğrencilerin %77,06'sı İnternette dolaşırken arkasında iz bırakmazken (Faktör 5), %2,94'ü iz bırakmaktadır. Arkasında ara sıra iz bıraktığını belirten yani aslında iz bırakıp bırakmadığının farkında olmayan öğrenci-

lerin oranı ise %20'dir. Bunun yanı sıra öğrencilerin %61,18'i güvenlik önlemi alırken (Faktör 3), %12,94'ü almamaktadır. Ara sıra güvenlik önlemi alan öğrencilerin sayısı ise %25,88'dir.

Siber Güvenlik Davranışlarının Cinsiyete Göre İncelenmesi

Cinsiyete göre siber güvenlik davranışları arasında fark olup olmadığına bağımsız örneklem t-testi ile bakılmıştır. Sonuçlar Tablo 4'de verilmiştir.

Tablo 4. Cinsiyete Göre Siber Güvenlik Davranış Puanlarının Karşılaştırılması

Faktör	Cinsiyet	N	Ort.	Std. Sap.	t	sd	p
Kişisel Gizliliği Koruma	Kız	67	3,9269	,48604	1,060	168	,291
	Erkek	103	4,0184	,58824			
Güvenilmeyenden Kaçınma	Kız	67	4,1493	1,10616	-,913	168	,363
	Erkek	103	3,9903	1,11140			
Önlem Alma	Kız	67	3,5672	,76799	1,479	168	,141
	Erkek	103	3,7534	,82377			
Ödeme Bilgilerini Koruma	Kız	67	3,9776	1,17239	1,768	168	,079
	Erkek	103	4,2767	1,01152			
İz Bırakmama	Kız	67	3,8993	,65143	,403	168	,687
	Erkek	103	3,9417	,68349			
Siber Güvenlik ölçeği	Kız	67	3,9040	,50022	1,143	168	,255
	Erkek	103	3,9961	,52184			

Tablo 4 incelendiğinde cinsiyete göre siber güvenlik davranış puanları arasında tüm faktörlerde istatistiksel olarak anlamlı bir farklılık yoktur (p>,05).

Tablo 5 incelendiğinde BÖTE bölümünde öğrenim gören kız öğrencilerin kişisel gizliliği koruma faktörü puanları erkek öğrencilerden daha yüksektir. Bilgisayar mühendisliği Bölümü öğrencileri için ise tam ters bir durum söz konusudur. Başka bir ifade ile kişisel güvenliği koruma açısından bilgisayar mühendisliği bölümünde erkekler daha olumlu siber güvenlik davranış düzeyine sahiptir.

Tablo 5. Cinsiyete Göre Kişisel Gizliliği Koruma Faktörü Puanlarının Bölümler Bazında Karşılaştırılması

Bölüm	Cinsiyet	N	Ort.	Std. S.	t	sd	p
BÖTE	Kız	25	4,1000	,49497	-2,741	58	,008*
	Erkek	35	3,7257	,53925			
Bilgisayar Mühendisliği	Kız	34	3,7706	,47516	3,420	78	,001*
	Erkek	46	4,1870	,58027			

**p<0,05*

Yukarıdaki tabloya göre ayrıca, cinsiyete göre siber güvenlik davranışları arasında fark olup olmadığına bölümler bazında ayrı, ayrı bakıldığında her iki bölümde de kişisel gizliliği koruma alt boyutunda istatistiksel olarak anlamlı bir farklılık bulunmuştur (p<,05).

Siber Güvenlik Davranışlarının Bilgisayar ya da İnternet Güvenliğine Yönelik Alınan Eğitim veya İş Deneyimine Göre İncelenmesi

Siber güvenlik davranışlarının alınan bilgisayar-İnternet güvenlik eğitimi ya da iş deneyimine göre değişip değişmediğini belirlemek amacıyla bağımsız örneklem t-testi uygulanmıştır. Güvenlik eğitimi alan ve almayan öğrencilerin puanlarına uygulanan bağımsız örneklem t-testi analizi Tablo 6'da verilmiştir.

Tablo 6. Siber Güvenlik Davranışlarının Bilgisayar ya da İnternet Güvenliğine Yönelik Alınan Eğitim veya İş Deneyimine Göre Değişimi

Faktör	Güvenlik Eğitimi	N	Ort.	Std. Sap.	t	sd	p
Kişisel Gizliliği Koruma	Alan	58	4,143	,466	2,794	168	,006*
	Almayan	112	3,899	,573			
Güvenilmeyenden Kaçınma	Alan	58	4,064	1,181	,099	168	,921
	Almayan	112	4,046	1,074			
Önlem Alma	Alan	58	3,920	,613	2,864	168	,005*
	Almayan	112	3,555	,864			
Ödeme Bilgilerini Koruma	Alan	58	4,319	,980	1,390	168	,167
	Almayan	112	4,075	1,129			
İz Bırakmama	Alan	58	4,064	,658	1,974	168	0,050
	Almayan	112	3,852	,666			
Siber Güvenlik ölçeği	Alan	58	4,102	,495	2,649	168	,009*
	Almayan	112	3,886	,509			

**p<0,05*

Güvenlik eğitimi veya iş deneyimine sahip olan öğrenciler ile sahip olmayan öğretmen adaylarının siber güvenlik davranışları arasında kişisel gizliliği koruma, önlem alma faktörleri ve ölçeğin tümüne ait puanları arasında istatistiksel olarak anlamlı bir fark bulunmuştur (p<,05). İnternet-bilgisayar güvenlik eğitimi alan veya bu konuda iş deneyimi olan öğrencilerin siber güvenlik davranışları daha olumludur. Ayrıca yine bu öğrenciler kişisel gizli bilgilerini ve güvenliklerini korumak için önlem alma konusunda daha bilinçlidirler.

Siber Güvenlik Davranışlarının Sınıfa Göre Değişimi

Çalışma grubu öğrencilerinin öğrenim gördükleri sınıflara göre SGÖ puan ortalamaları Tablo 7'de verilmiştir.

Tablo 7. Sınıflara Göre SGÖ Puan Ortalamaları ve Tek Yönlü Varyans Analizi (ANOVA) Sonuçları

Puan	Sınıf	N	$\overline{X}$	ss	Var. K.	KT	Sd	KO	F	p
Kişisel Gizliliği Koruma	1	32	3,9187	,62961	G.Arası	,936	3	,312	1,030	,381
	2	43	3,9558	,55947	G.İçi	50,291	166	,303		
	3	54	3,9426	,55239	Toplam	51,227	169			
	4	41	4,1122	,46594						
Güvenilmeyenden Kaçınma	1	32	1,265	,223	G.Arası	3,889	3	1,296	1,056	,370
	2	43	,9365	,142	G.İçi	203,884	166	1,228		
	3	54	1,217	,165	Toplam	207,774	169			
	4	41	,985	,153						
Önlem Alma	1	32	3,431	,865	G.Arası	3,007	3	1,002	1,562	,201
	2	43	3,772	,842	G.İçi	106,545	166	,642		
	3	54	3,659	,685	Toplam	109,552	169			
	4	41	3,804	,845						
Ödeme Bilgilerini Koruma	1	32	4,000	1,288	G.Arası	1,827	3	,609	,514	,673
	2	43	4,081	1,101	G.İçi	196,884	166	1,186		
	3	54	4,259	,850	Toplam	198,712	169			
	4	41	4,231	1,183						
İz Bırakmama	1	32	3,968	,6772	G.Arası	2,130	3	,710	1,601	,191
	2	43	3,895	,7201	G.İçi	73,602	166	,443		
	3	54	3,796	,6086	Toplam	75,731	169			
	4	41	4,091	,6702						
Siber Güvenlik Ölçeği	1	32	3,837	,5428	G.Arası	1,343	3	,448	1,717	,166
	2	43	3,974	,4887	G.İçi	43,292	166	,261		
	3	54	3,917	,5027	Toplam	44,635	169			
	4	41	4,095	,5178						

**p<0,05*

Sınıf değişkenine göre SGÖ puanları arasında anlamlı ilişki olup olmadığını belirlemek için tek yönlü varyans analizi(ANOVA) uygulanmıştır. Analiz sonucunda farklı sınıflarda öğrenim gören öğrencilerin SGÖ ve her bir alt faktör puanları arasında istatistiksel olarak anlamlı bir ilişki bulunamamıştır (p>,05).

Siber Güvenlik Davranışlarının Mezun Olunan Lise Türüne Göre İncelenmesi

Siber güvenlik davranışlarının mezun olunan lise türüne göre değişimini belirlemek için ANOVA testi uygulanmıştır. Test sonuçları Tablo 8'de verilmiştir.

Tablo 8. SGÖ Puanlarının Mezun Olunan Lise Türüne Göre Ortalamaları ve ANOVA Testi Sonuçları

f, $\overline{X}$ ve s Değerleri					ANOVA Sonuçları					
Puan	Lise Türü	N	$\overline{X}$	ss	Var.K.	KT	Sd	KO	F	p
Kişisel Gizliliği Koruma	Teknik Lise	23	3,956	,5061	G.Arası	,187	3	,062	,203	,894
	Genel/Düz Lise	47	4,031	,4886	G.İçi	51,040	166	,307		
	Anadolu Lisesi	65	3,976	,6161	Toplam	51,227	169			
	Meslek Lisesi	35	3,942	,5457						
Güvenilmeyenden Kaçınma	Teknik Lise	23	3,902	1,140	G.Arası	6,353	3	2,118	1,745	,160
	Genel/Düz Lise	47	3,909	1,261	G.İçi	201,421	166	1,213		
	Anadolu Lisesi	65	4,011	1,122	Toplam	207,774	169			
	Meslek Lisesi	35	4,421	,746						
Önlem Alma	Teknik Lise	23	3,800	,793	G.Arası	1,780	3	,593	,914	,436
	Genel/Düz Lise	47	3,523	,967	G.İçi	107,772	166	,649		
	Anadolu Lisesi	65	3,704	,728	Toplam	109,552	169			
	Meslek Lisesi	35	3,765	,705						
Ödeme Bilgilerini Koruma	Teknik Lise	23	4,239	1,214	G.Arası	,296	3	,099	,083	,969
	Genel/Düz Lise	47	4,159	1,011	G.İçi	198,415	166	1,195		
	Anadolu Lisesi	65	4,115	1,092	Toplam	198,712	169			
	Meslek Lisesi	35	4,185	1,118						
İz Bırakmama	Teknik Lise	23	4,043	,615	G.Arası	4,692	3	1,564	3,655	,014*
	Genel/Düz Lise	47	3,707	,770	G.İçi	71,039	166	,428		
	Anadolu Lisesi	65	3,907	,662	Toplam	75,731	169			
	Meslek Lisesi	35	4,171	,464						
Siber Güvenlik ölçeği	Teknik Lise	23	3,988	,492	G.Arası	1,110	3	,370	1,411	,242
	Genel/Düz Lise	47	3,866	,619	G.İçi	43,525	166	,262		
	Anadolu Lisesi	65	3,943	,481	Toplam	44,635	169			
	Meslek Lisesi	35	4,097	,408						

** p<,05*

Yukardaki tablo incelendiğinde istatistiksel olarak anlamlı ilişki sadece iz bırakmama faktör puanları arasında bulunmuştur F(3, 166)=3,655; p<,05). Bu ilişkinin hangi gruplar arasında olduğunu tespit etmek için Tukey testi uygulanmıştır. Tukey testi sonucunda meslek lisesinden ($\overline{X}$=4,171) mezun olan öğrencilerin bu alt faktörde genel/düz liseden ($\overline{X}$=3,707) mezun olan öğrencilerden daha olumlu davranış gösterdiği görülmektedir. Bu durumun sebebi öğrencilerin meslek lisesinde eğitim görürken daha fazla İnternet ve İnternet teknolojileri ile iç içe olmaları olabilir.

Siber Güvenlik Davranışlarının İnternet Kullanım Yılına Göre İncelenmesi

Siber güvenlik davranışlarının İnternet kullanım yılına göre değişimini belirlemek için ANOVA testi uygulanmıştır. Test sonuçları Tablo 9'de verilmiştir.

Tablo 9. SGÖ Puanlarının İnternet Kullanım Yılına Göre Ortalamaları ve ANOVA Testi Sonuçları

Puan	Yıl	N	$\overline{X}$	ss	Var. K.	KT	Sd	KO	F	p
	3-4	8	4,012	,448	G.Arası	2,424	4	,606	2,049	,090
	5-6	24	3,854	,566	G.İçi	48,803	165	,296		
Kişisel Gizliliği Koruma	7-8	48	3,845	,551	Toplam	51,227	169			
	9-10	23	4,017	,595						
	>10	67	4,110	,521						
	3-4	8	3,593	1,202	G.Arası	3,061	4	,765	,617	,651
	5-6	24	3,875	1,242	G.İçi	204,712	165	1,241		
Güvenilmeyenden Kaçınma	7-8	48	4,156	,859	Toplam	207,774	169			
	9-10	23	4,076	1,040						
	>10	67	4,089	1,234						
	3-4	8	3,300	,821	G.Arası	7,878	4	1,970	3,196	,015*
	5-6	24	3,350	,851	G.İçi	101,674	165	,616		
Önlem Alma	7-8	48	3,550	,795	Toplam	109,552	169			
	9-10	23	3,852	,693						
	>10	67	3,877	,778						
	3-4	8	3,375	1,529	G.Arası	17,959	4	4,490	4,098	,003*
	5-6	24	3,812	1,231	G.İçi	180,753	165	1,095		
Ödeme Bilgilerini Koruma	7-8	48	3,937	1,248	Toplam	198,712	169			
	9-10	23	4,282	1,074						
	>10	67	4,492	,682						
	3-4	8	3,812	,593	G.Arası	1,103	4	,276	,610	,656
	5-6	24	4,031	,692	G.İçi	74,628	165	,452		
İz Bırakmama	7-8	48	3,822	,710	Toplam	75,731	169			
	9-10	23	4,021	,568						
	> 10	67	3,940	,677						
	3-4	8	3,618	,514	G.Arası	3,665	4	,916	3,691	,007*
	5-6	24	3,784	,567	G.İçi	40,969	165	,248		
Siber Güvenlik Ölçeği	7-8	48	3,862	,451	Toplam	44,635	169			
	9-10	23	4,050	,493						
	>10	67	4,102	,503						

** p<,05*

Tablo 9 incelendiğinde, İnternet kullanım yılına göre, önlem alma (F(4, 165)=3,196; p<,05), ödeme bilgilerini koruma (F(4, 165)=4,098; p<,05) ve SGÖ puanları (F(4, 165)=3,691; p<,05) arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmüştür. Farklılığın kaynağının hangi gruplar arasında olduğunu bulmak için Tukey testi uygulanmıştır. Önlem alma faktörüne göre 10 yıldan fazla İnternet kullanan öğrencilerin () siber güvenlik davranış düzeyleri 5-6 yıldır İnternet kullananlara göre () göre daha olumludur. Benzer şekilde ödeme bilgilerini koruma faktörü açısından 10 yıldan fazla İnternet kullananların () siber güvenlik davranış düzeyleri 3-4 yıl () ve 7-8 yıldır ()

İnternet kullananlara göre daha yüksektir. SGÖ puanlarına göre 3-4 yıldır () İnternet kullanan öğrencilerin siber güvenlik davranış düzeyleri, 9-10 yıldır() ve 10 yıl üzeri() İnternet kullanan öğrencilerden daha düşüktür. Dolayısıyla İnternet kullanım tecrübesi artıkça siber güvenlik davranış düzeyleri yükselmektedir.

4. Sonuç ve Öneriler

Bu çalışmada, Bilgisayar Mühendisliği ve BÖTE bölümlerinde öğrenim gören üniversite öğrencilerinin siber güvenlik davranışları çeşitli değişkenler açısından incelenmiştir. Ortalama puanlar incelendiğinde öğrencilerin siber güvenliğe yönelik davranışlarının yeterli düzeyde olduğu görülmektedir. Bu açıdan bakıldığında öğrenciler kişisel gizliliklerini koruyabilmektedirler. Ayrıca güvenilmeyen uygulamalardan kaçınmakta ve güvenlik için önlem alabilmektedirler. Bunun yanı sıra kredi kartı, banka kartı gibi ödeme bilgilerini koruyabilmekte ve İnternet üzerinde gezinirken arkalarında iz bırakmamaktadırlar. Kişisel güvenliği koruma açısından BÖTE bölümünde kızlar, bilgisayar mühendisliği bölümünde ise erkekler daha olumlu siber güvenlik davranışlarına sahiptirler.

İnternet-bilgisayar güvenlik eğitimi alan veya bu konuda iş deneyimi olan öğrencilerin siber güvenlik davranışları daha olumludur. Bu öğrenciler kişisel bilgilerini korumak ve güvenliklerini sağlamak için önlem alma konusunda daha bilinçlidirler. Bu durum göz önüne alındığında üniversite öğrencilerinin siber güvenlik davranış düzeylerini olumlu yönde artırmak ve farkındalık oluşturmak için siber güvenlik ile ilgili derslerin öğretim programına eklenmesi faydalı olabilir. Hatta bu durum bir adım daha öteye götürülerek bütün bölümlerde siber güvenlik ile ilgili bir ders okutulması zorunlu hale getirilebilir.

Sınıflar arasında siber güvenlik davranışları önemli bir farklılık göstermemektedir. Bunun nedeni öğrencilerin üniversite öğrenimleri boyunca siber güvenlikle ilgili olarak herhangi bir ders kapsamında eğitim almamaları olabilir. Meslek lisesinden mezun olan öğrencilerin siber güvenlik davranışlarının İnternette gezinirken arkalarında iz bırakmama açısından genel/düz liseden mezun olan öğrencilere göre daha olumlu olduğu görülmektedir. Bu durumda öğrencilerin meslek lisesinde eğitim görürken İnternet ve İnternet teknolojileri ile ilgili dersleri daha yoğun almaları etkili olabilir. İnternet kullanım yılı arttıkça siber güvenlik davranışları daha olumlu olmaktadır. Ayrıca İnternet kullanım yılı arttıkça öğrenciler siber güvenlik için daha fazla önlem almakta ve İnternet üzerinde alış veriş yaparken ödeme bilgilerini koruma konusunda daha hassas davranmaktadırlar. Farklı bir ifade ile İnternet deneyimi siber güvenlik davranışını olumlu yönde etkilemektedir.

Kuru ve Ocak (2016), kamu görevlilerine siber güvenlikle ilgili olarak kariyerleri süresince yeterli eğitim verilmesi ve üniversitelerin müfredatıyla ilgili gerekli düzenlemelerin tereddüt edilmeden gözden geçirilmesi gerektiğini öne sürmüşlerdir. Bu açıdan bakıldığında kamu kurumlarında siber güvenlikle ilgili eğitim verilebilmesi

için bilgisayar mühendislerinin ve bilişim teknolojileri öğretmenlerinin bu konuda iyi bir eğitim almaları çok önemli ve elzemdir. Ayrıca Önaçan ve Atan (2016) kurum ve devletlerin siber uzaydaki saldırılardan maddi ve manevi etkilendiklerini veya zarara uğradıklarını, bu tür zararlardan korunabilmek için siber güvenlik farkındalığının artırılması, bilgi ve bilinç seviyesinin yükseltilmesi gerektiğini vurgulamışlardır. Bunu gerçekleştirmek için bilgisayar mühendislerinin, bilişim teknolojileri öğretmenlerinin hatta lisans düzeyinde öğrenim gören herkesin kaliteli ve ayrıntılı bir siber güvenlik eğitimi alması gerekmektedir. Bunu gerçekleştirebilmek için üniversitelerin müfredatı acilen güncellenmelidir.

5. Kaynaklar

Akamai (2016). State of the Internet / Security Report. Erişim tarihi: 22.04.2016, https://www.akamai.com/us/en/multimedia/documents/state-of-the-İnternet/q4-2016-state-of-the-İnternet-security-report.pdf

Akın, O., Çınar, I., Karaman , M., Bilekyigit, F., Siber Durum Farkındalığını Artırmada Etkili Bir Yöntem: Bayrağı Yakala(Capture the Flag) , ISCTURKEY 2013 : International Conference on Information Security and Cryptology, 23-24 Mayıs, Ankara, 1-6, 2013.

Büyüköztürk, Ş., Çakmak, E. K., Akgün, Ö. E., Karadeniz, Ş., & Demirel, F. (2008). Bilimsel araştırma yöntemleri. *Ankara: Pegem Akademi*.

Çaka, C., Doğan, E., Şahin, Y. L., Sosyal Ağ Kullanan Öğrencilerin Çevrimiçi Bilgi Arama Stratejilerinin İncelenmesi, Trakya Üniversitesi Eğitim Fakültesi Dergisi, 6(1), 1-13, 2016.

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

Erol, O., Şahin, Y. L., Yılmaz, E., Haseski, H.l İ. (2015). Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması. International journal of human sciences, 12:2, 75-91.

Gökmen, Ö. F., Akgün, Ö. E., Öğretmen Adaylarının Bilişim Suçlarına Yönelik Deneyimleri ve Bilişim Güvenliği Ders İçeriğine Yönelik Görüşleri, Mustafa Kemal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 13(33), 178-193, 2016.

Göztepe, K., Kılıc, R., Kayaalp, A., Cyber Defense In Depth: Designing Cyber Security Agency Organization For Turkey, Journal of Naval Science and Engineering, 10(1), 1-24, 2014.

Güldüren, C., Çetinkaya, L., Keser, H., Ortaöğretim Öğrencilerine Yönelik Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması, İlköğretim Online, 15(2), 682-695, 2016.

Hekim, H., Başıbüyük, O., Siber suçlar ve Türkiye'nin siber güvenlik politikaları, Uluslararası Güvenlik ve Terörizm Dergisi, 4(2), 135-158, 2013.

Huck, S. W. (2012). Reading statistics and research (6th edt.). Boston: Pearson.

Kuru, H., Ocak, M. A., Determination of cyber security awareness of public employees and consciousness-rising suggestions, Journal of Learning and Teaching in Digital Age, 1(2), 57-65, 2016.

Mert, M., Bülbül. H.İ. & Sağıroğlu. Ş. (2012).Milli Eğitim Bakanlığına Bağlı Okullarda Güvenli İnternet Kullanımı. TUBAV Bilim Dergisi, 5(4), 1-12.

Önaçan, M. B. K., Atan, H., Siber Güvenlikte Lisansüstü Eğitim: Deniz Harp Okulu Örneği, Trakya University Journal of Engineering Sciences, 17(1), 13-21, 2016.

Özyurt Ö., Özyurt, H. (2015). A Study For Determining Computer Programming Students' Attitudes Towards Programming And Their Programming Self-Efficacy, Journal of Theory and Practice in Education, 11(1), 51-67.

Peker, A., Negatif Duygunun Siber Zorbalık ve Mağduriyete İlişkin Yordayıcı Rolünün İncelenmesi , K. Ü. Kastamonu Eğitim Dergisi, 23 (4), 1633-1646, 2015.

Sakallı, H., Çiftci, S., Sınıf Öğretmeni Adaylarının Dijital Vatandaşlık Düzeyleri İle Siber Zorbalık Eğilimleri Arasındaki İlişkinin İncelenmesi: Adnan Menderes Üniversitesi Örneği, Eğitim Teknolojisi Kuram Ve Uygulama, 6(2), 2016.

Solms, R. V., Niekerk J., V., From information security to cyber security, Computers & Security, Volume 38, Pages 97–102, October 2013.

TUİK (2016). http://www.tuik.gov.tr/PreIstatistikTablo.do?istab_id=41 Erişim Tarihi: 24.3.2017

Yenilmez, K. (2008). Open primary education school students' opinions about mathematics television programmes. Turkish Online Journal of Distance Education, 9(4), 176-189.

Yılmaz, E., Şahin Y. L., Akbulut, Y., Öğretmenlerin Dijital Veri Güvenliği Farkındalığı, Sakarya University Journal of Education, 6(2), 16-45, 2016.

Yılmaz, S. ve Sağıroğlu, Ş., Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri, 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 20-21 Eylül, Ankara, 158-166, 2013.

Extended Abstract

Cyber security is a concept that involves ensuring the safety of information resources and the protection of all kinds of entities including individuals. This study aims to examine the cyber security behaviors of undergraduate students of Computer Engineering and Computer Education and Instructional Technologies (CEIT) programs in terms of a number of variables and to evaluate the results.

The research question is given below:

- *How are the cyber security behaviors of CEIT and Computer Engineering students?*

The sub-problems of the study are stated below:

- *Is there a significant difference in the cyber security behaviors of female and male students?*
- *Do students' cyber security behaviors vary by previous training or work experience in the fields of Internet/computer security?*
- *Do students' cyber security behaviors vary by their study year?*
- *Do students' cyber security behaviors vary by the kind of high school they graduated from?*
- *Do students' cyber security behaviors vary by previous Internet experience?*

The study employs a survey research design which is a type of quantitative research methods. The sample consists of 170 students of Computer Engineering and Computer Education and Instructional Technologies (CEIT) from one public and one private universities. A 5 point Likert scale developed by Erol et al. (2015) and consisted of 5 factors and 25 items was employed for data collection. The sub-factors of the scale consist of Protection of Personal Privacy (Factor

1), Avoiding the Threatful (Factor 2), Taking Precautions (Factor 3), Protection of Payment Information (Factor 4) and Avoiding Leaving Digital Footprints (Factor 5). The average scores obtained from the scale was interpreted as 'Never' for scores between 1 and 1.80; 'Seldom' for 1.81 and 2.60; 'Occasionally' for 2.61 and 3.40; 'Frequently' for 3.41 and 4.20 and 'Always' for 4.21 and 5.0. Results indicate that the level of student behaviors are adequate for ensuring cyber security. Detailed factor analysis reveals that students can protect their personal and private information. They are also able to avoid using threatening applications and take precautions regarding security. Moreover, they can protect payment information of credit or debit cards and do not leave digital footprints while browsing the Internet. No significant difference was found between genders in terms of cyber security behavior. With respect to the protection of personal privacy factor, female students in CEIT and male students in Computer Engineering demonstrated more positive cyber security behaviors.

Students with previous training or work experience in the fields of Internet/computer security showed more positive cyber security behaviors. In other words, these students demonstrated higher levels awareness about protecting personal information and providing security. Therefore, adding cyber security courses in curricula may be helpful for increasing levels of cyber security behaviors and awareness. Furthermore, cyber security lessons may become compulsory for every program. There is no significant difference in students' cyber security behaviors across study years. Vocational high school graduates are more cautious than regular high school graduates in terms of avoiding leaving digital footprints.