İletişim Fakültesi Öğrencilerinin Siber Güvenlik Farkındalığı İnönü Üniversitesi Örneği

Article · March 2018

CITATIONS
0

READS
232

3 authors:

Harun Bayer

12 PUBLICATIONS **4** CITATIONS

SEE PROFILE

Mustafa Aksoğan

Malatya Turgut Özal Üniversitesi

13 PUBLICATIONS **4** CITATIONS

SEE PROFILE

Enes Celik

Kirklareli University

19 PUBLICATIONS **26** CITATIONS

SEE PROFILE

Kesit Akademi Dergisi
The Journal of Kesit Academy

ISSN: 2149 - 9225
Yıl: 4, Sayı:13, Mart 2018, s. 271-288

Mustafa AKSOĞAN
İnönü Üniversitesi, Akçadağ MYO, Bilgisayar Programcılığı, mustafa.aksogan@inonu.edu.tr
Harun BAYER
İnönü Ünv. - Bilgisayar Programcılığı - harun.bayer@inonu.edu.tr
Mehmet Ozan GÜLADA
İnönü Ünv. - İşletme Yönetimi - mehmet.gulada@inonu.edu.tr
Enes ÇELİK
Kırklareli Ünv. - Bilgisayar Programcılığı - enes.celik@kirklareli.edu.tr

İLETİŞİM FAKÜLTESİ ÖĞRENCİLERİNİN SİBER GÜVENLİK FARKINDALIĞI: İNÖNÜ ÜNİVERSİTESİ ÖRNEĞİ

Özet

Bu çalışma İletişim Fakültesinde öğrenim gören öğrencilerin siber suçlar ve siber güvenlik hakkındaki farkındalıklarını incelemek amacıyla yapılmıştır. Katılımcı grubunu İnönü Üniversitesi İletişim Fakültesinde, farklı bölüm ve sınıflarda öğrenim gören toplam 368 öğrenci oluşturmaktadır. Veri toplama aracı olarak araştırmacılar tarafından geliştirilen "Siber Güvenlik Farkındalığı Anketi" kullanılmıştır. Veriler betimleyici ve çıkarımsal istatistikler kullanılarak analiz edilmiştir. Araştırma sonuçlarına göre, öğrencilerin büyük çoğunluğunun siber güvenlik konusunda farkındalıklarının düşük olduğu ortaya çıkmıştır. Ayrıca, cinsiyete, yaşlara ve internette günlük geçirilen süreye göre verilen cevapların bazılarında anlamlı farklılıklar gözlemlenirken, katılımcıların okudukları bölüme göre verilen cevaplar arasında anlamlı bir fark bulunmamıştır.

Anahtar Kelimeler: Siber Tehdit, Siber Saldırı, Siber Güvenlik

CYBER SECURITY AWARENESS OF THE STUDENTS OF THE FACULTY OF COMMUNICATION: INONU UNIVERSITY SAMPLE

Abstract

This study was conducted to investigate the awareness of cybercrime and cyber security by students at the Faculty of Communication. The participant group consists

of 368 students who are studying in different departments and classes in Inonu University Faculty of Communication. The "Cyber Security Awareness Questionnaire" developed by the researchers was used as data collection tool. The data were analyzed using descriptive and meaningful statistics. The findings of the survey revealed, that there were important number of students at low levels of awareness. There were significant differences in some answers about awareness level of information security between gender, age and average internet usage daily but there weren't significant differences by their departmant. It is suggested to give inclusive and effective information security education to prospective student attending Faculty of Communication.

Keywords: Cyber Threat, Cyber Attack, Cyber Security

Giriş

Günümüzde teknolojik cihazların hızlı gelişimi ile birlikte internete bağlanan cihaz sayısının artması, sosyal medya uygulamaları sayısındaki artış, ticaret, sağlık, eğitim vb. işlemlerin internet ortamında gerçekleştirilebilmesi sayesinde internet kullanıcı sayısı da artmaktadır. Dijital pazarlama ajansı We Are Social ve Hootsuite işbirliği ile hazırlanan "Digital in 2017 Global Overview" raporuna göre Dünya nüfusunun %50'si (yaklaşık 3.77 milyar kişi), Türkiye nüfusunun ise %60'ı (yaklaşık 48 milyon kişi) aktif olarak internet kullanmaktadır. Aynı şirketin 2016 yılındaki "Digital in 2016" raporu ile karşılaştırıldığında aktif internet kullanıcı sayısı Dünya'da %10 artmıştır. Günümüzde özellikle akıllı telefonlar olmak üzere, tabletler, taşınabilir bilgisayarlar vb. cihazların internet bağlantısına sahip olması bu artışın sebeplerinden biri olarak gösterilebilir. Artık insanlar bu taşınabilir cihazlar sayesinde zaman ve mekân kısıtlaması olmadan internete bağlanarak; alış-veriş yapabilmekte, bankacılık, e-devlet vb. kritik işlemleri gerçekleştirebilmektedirler. İnternetin bu kadar kolay ulaşılabilir olması ve internet kullanıcı sayısındaki hızlı artış internet kullanıcılarından yasadışı yollarla yararlanmak isteyen kötü niyetli kişilere çok büyük fırsatlar sunmaktadır (Mann ve Sutton, 1998: 201). Başka bir deyişle internete bağlanabilen cihaz sayısındaki çeşitlilik ve bununla beraber internet kullanıcı sayısındaki artış, güvenlik ihlallerine maruz kalma riskini de arttırmaktadır (Aytekin, 2015: 3). Bu nedenle devletlerin bu risklere karşı önlemler almaları ve bu alana daha fazla yatırım yapmaları gerekmektedir.

Bilişim teknolojileri ile birlikte bilgiler sanal ortamlara taşınmış ve bu bilgiler bu ortamlarda dolaşır hale gelmiştir. Gereksiz kırtasiye masrafından kurtaran bu teknolojiler beraberinde en önemlisi güvenlik olan bilişim teknolojilerini yanlış kullanma, bireylerdeki risk algılarının az olması, siber tehditlerden habersiz olma gibi bazı riskleri de beraberinde getirmiştir. Yapılan araştırmalarda, insan faktörünü göz ardı ederek sadece donanımsal ve yazılımsal tedbirler ile bu tehditlerden korunmanın mümkün olmadığını görülmektedir (Mart, 2012: 35).

Bu kapsamda, araştırmada ilk olarak, siber tehdit, siber saldırı, siber savaş ve siber güvenlik konularında teorik alt yapı sunulmuş, daha sonrasında bu konuda yapılan benzer çalışmaların literatür özeti verilmiştir. Yapılan benzer çalışmalar hiç kuşkusuz konunun önemini kavramak açısından oldukça önemlidir. Araştırmanın uygulama kısmında, yöntem, hipotezler, veri top-

lama araçları, istatistiksel analizler ve sonrasında ortaya çıkan bulgular açıklanarak, sonuç ve değerlendirmeye gidilmiştir.

1. KURAMSAL AÇILIM

1.1. Siber Tehdit

Siber tehdit kavramı son yıllarda gittikçe önem kazanmıştır. Bu tehditler genellikle kötü amaçlı kişilerce bilişim suçu işlemek amacıyla yazılmış programlar kullanarak sistemlerin zafiyetlerinden yararlanarak, başka kişilere ait gizli bilgilerin elde edilmesi ile gerçekleştirilir (Gordon ve Ford, 2006: 13). Günümüzde siber tehdit sadece bilgisayar sistemlerine verilen zararlarla kalmamakta, aynı zamanda enerji, ulaşım, askeri, haberleşme, kontrol vb. sistemlere zarar verebilen bir savaş şekli olarak karşımıza çıkmaktadır (Aytekin, 2015: 19). Clarke ve Knake (2010: 74-85)'ye göre siber tehditleri oluşturan üç boyuttan söz edilebilir:

- İnternetin merkezi olmayan büyük bir ağ olması, adresleme sistemi, yönetim boşluğu, internetin çalışmasını sağlayan sistemlerin çoğunun şifresiz ve kolay erişilebilir olması ve zararlı yazılımların dağılma kolaylığı gibi internet zafiyetleri.
- Donanımsal ve yazılımsal hatalar.
- Önemli sistemlere çevrim içi erişim sağlanabilmesi.

Siber tehditler, öncelikle bilgi güvenliğinin temel ilkelerinden gizlilik, bütünlük ve erişilebilirlik işlevlerinden en az birini hedef alabilir. Gizlilik, bilginin sadece erişim yetkisi verilen kişiler tarafından görüntülenmesi veya yazılabilir hale getirilmesidir. Bütünlük, bilginin silinmemiş, kısmen veya tamamen değiştirilmemiş olmasıdır. Erişilebilirlik ise, saklanan bilginin yetkisi olan kişiler tarafından erişilebilir hale getirilmesidir (Goodrich ve Tamassia, 2011: 153). Siber ortamın güvenli olabilmesi için bilişim sistemlerinin temel malzemesi olan bilginin bu işlevlerinin sağlanması gerekmektedir(Aslay, 2017: 25).

1.2. Siber Saldırı

Bireyler ve uluslar için önemli bilgilerin elde edilmesine yönelik yapılan siber saldırı; hedeflenen kişi, şirket, kurum, örgüt gibi yapıların bilgi sistemlerine ya da iletişim altyapılarına, ticari, politik veya askeri amaçlı yapılan sistematik ve koordineli saldırılar olarak tanımlanabilir (Alkan, 2012: 14). 2016-2019 Ulusal Siber Güvenlik Stratejisi (2016: 8)'ne göre ise siber saldırı; bilişim sistemlerinin erişilebilirliğini kısıtlamak veya tamamen engellemek amacıyla, insanlar veya kötü amaçlı yazılımlar sayesinde sistemli, planlı ve kasten olarak yapılan işlemlerdir. Siber saldırılar, hackerlar, organize suç şebekeleri, casusluk amacı güden kişiler, dış istihbarat örgütleri veya düşman ülke tarafından koordineli olarak yapılabildiği gibi sistemi kullanan kişiler tarafından yanlışlıkla da yapılabilmektedir (Çeliktaş, 2016: 8). Siber saldırıları ciddi maddi zararlara yol açabilen ve tüm ülkelerin ortak bir sorunu olarak tanımlayan Güngör (2015: 42-43)'e, göre siber saldırıların özellikleri şunlardır:

- Özellikle internete bağımlı olarak çalışan sistemlerin saldırının niteliğine göre tamamen veya belli bir süreliğine işlevsiz kalabilmesi nedeniyle sonuçları yıkıcıdır.
- Maliyeti düşük bir saldırı yöntemidir.
- İnternet erişimini kullandığı için farklı coğrafi bölgelerden saldırılar gerçekleştirilebilir. Bu nedenle kimin tarafından yapıldığının bulunması oldukça zor hatta bazı durumlarda imkânsızdır.
- Saldırılar ani ve hızlı gerçekleştirildiği için önlem alınması zordur.

1.3. Siber Saldırı Yöntemleri

Günümüzde siber saldırılar çok çeşitli yöntemlerle gerçekleştirilmektedir. Belli başlı siber saldırı yöntemleri şunlardır (Çubukcu ve Bayzan, 2013: 154; Altunok ve Vural, 2016: 78; Kurt, 2005: 60-77; Aslay, 2017: 26; Hekim ve Başıbüyük, 2013: 143);

- Sistem güvenliğinin kırılıp içeri sızılması: Bilgisayar korsanları tarafından bilgi çalmak veya sistemi kullanılamaz duruma getirmek amacıyla, ustalık gerektiren ve yasa dışı olan eylemlerdir.
- Oltalama: Genellikle kişilerin banka hesapları, kredi kartı vb. değerli bilgilerini almak amacıyla, sahte logo ve web sayfaları kullanılarak e-posta gönderme işlemleridir.
- Truva atları: Bilişim sistemlere genellikle internet üzerinden bulaşan ve sistemin açıklarından yararlanarak programın yerleştirilmesini sağlayan kişilerin isteklerine cevap veren zararlı yazılımlardır.
- Veri aldatmacası: Basit, güvenli ve yaygın bir saldırı tekniği olup verilerin kasten yanlış girilmesi veya girildikten sonra değiştirilmesidir.
- Süper darbe: Sistemin arızalanması veya kilitlenmesi durumunda güvenlik kontrollerini atlatarak sisteme olumsuz yönde etki eden yazılımlardır. Bilgiye erişim için güvenlik sistemini devre dışı bırakmak amacıyla kullanılırlar.
- Mantık bombaları: Genellikle bilişim sistemlerini tamamen devre dışı bırakmak amacıyla, hedeflenen bilişim sistemindeki programların içerisine yerleştirilen zararlı kod parçalarıdır.
- Çöpe dalma: Sistem belleğinde bulunan fakat ihtiyaç duyulmadığı için silinmiş bilgi veya belgelerin gelişmiş yöntemler kullanılarak geri getirilmesidir.
- Yerine geçme: Bilişim sistemlerinde hile yapmak amacıyla, sisteme giriş yetkisi olmayan veya sınırlı giriş yetkisi olan kişilerin, yetkili bir kişinin kullanıcı adı ve parola bilgilerini kullanarak sızmasıdır.
- Web sayfası hırsızlığı ve yönlendirme: Bir web sayfasının çalınarak kullanılamaz hale getirilmesi, web sayfasında farklı içerikler sunulması, istenmeyen bir web sayfasına yönlendirilmesi gibi eylemlerin gerçekleştirilmesidir.

- İstem dışı alınan elektronik postalar: Kişilerin talepleri olmaksızın elektronik adreslerine gönderilen ve kötü yazılımın yayılmasına neden olan postalardır.
- Hizmeti engelleme: Sunucu bilgisayarla çok sayıda sahte bağlantı kurarak sunucuya aşırı iş yükü yüklemek ve gerçekten bağlantı kurmaya çalışan kullanıcılara cevap veremez hale gelmesini sağlama yöntemidir.
- Salam tekniği: Özellikle bankacılık işlemlerinde kullanılan ve işlemlerde virgülden sonraki kısmı başka bir hesap numarasına aktararak haksız kazanç ele etme yöntemidir.

Bu yöntemler kullanılarak, bilgiye yetkisiz erişim sağlanmakta, bu bilgiler silinmekte, değiştirilmekte, çalınmakta, üçüncü şahıslarla paylaşılmakta veya erişimi engellenmektedir.

1.4. Siber Savaş

Siber savaş kavramının genel bir tanımı olmamakla beraber Carr (2011: 39) siber savaşı; fiziksel mücadele etmeksizin savaşma ve düşmanın kanını dökmeden onu alt etmeye çalışma sanatı olarak açıklamıştır. Daha genel bir tanımla siber savaş, bir ülkenin başka bir ülkenin internet ve bilişim ağlarına zarar vermek veya geçici süre çalışmasını engellemek üzere gerçekleştirdiği sızma faaliyetleridir. Başka bir deyişle siber savaş; düşmanı psikolojik olarak çökertmek için teknolojik bilgileri çalmak, değiştirmek, çökertmek, kullanılmaz hale getirmek ya da yanlış yönlendirmektir (Karakuş, 2013: 1).

1.5. Siber Güvenlik

2016-2019 Ulusal Siber Güvenlik Stratejisi (2016: 7)'ne göre siber güvenlik bilişim sistemlerinin saldırılardan korunması, bu ortamlarda gerçekleştirilen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınması, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitler neticesinde tepki mekanizmalarının devreye alınarak sistemin yaşanan siber güvenlik olayı öncesine döndürülmesidir. Siber güvenlik; bilgi sistemlerini ve ağlarını işlemez hale getiren veya çalışmasını engelleyen tüm tehdit, saldırı ve tehlikelere karşı teknolojik sistemleri korumaya denilmektedir (Akleylek ve Tok, 2011). Hansen ve Nissenbaum (2009: 1160) ise siber güvenlik kavramının ilk defa 1990'lı yıllarda bilgisayar mühendisleri tarafından ağa bağlı bilgisayarlarla ilgili güvenlik sorunlarını ifade etmek amacıyla kullanıldığını ifade etmiştir. Siber güvenlik; siber ortamda kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, uygulamalar ve teknolojilerin bütününü kapsar (Alkan, 2012: 16).

2016-2019 Ulusal Siber Güvenlik Stratejisi (2016: 11)'de ulusal siber güvenliğin sağlanmasında göz önünde bulundurulacak ilkeler şu şekilde tanımlanmıştır:

- Siber güvenlik, risk yönetimini esas alan etkin ve sürekli değerlendirmeye ve iyileştirmeye dayalı yöntemler aracılığıyla sağlanır.
- Siber güvenliğin sağlanması için tüm paydaşların siber güvenlik risklerini bilmeleri, bu risklerin yönetilmesine ilişkin yaklaşımlarının kendileri kadar başkalarını da etkileyebileceğinin bilincinde olmaları gerekir.

- Risk yönetimi, teknik zaafların hızla giderilmesini, saldırı ve tehditlerin önlenmesini, fark edilmesini, yanıtlanmasını ve muhtemel zararın en aza indirgenmesini içerir.
- Siber güvenliğin sağlanması ve sürdürülmesinde; kamu, özel sektör, üniversiteler, sivil toplum kuruluşları ve bireyler dâhil tüm paydaşlar arasında işbirliğinin yanı sıra uluslararası işbirliği ve bilgi paylaşımı esas kabul edilir ve güven inşa edilir.
- Tüm paydaşlar, siber güvenliğin sağlanması için çalışırken, hukukun üstünlüğü, ifade özgürlüğü, temel insan hak ve hürriyetleri ile mahremiyetin korunması ilkelerini gözetir.
- Paydaşlar siber risklerin yönetimi ile ilgili sorumluluklarını yerine getirirken şeffaflık, hesap verilebilirlik ve etik değerleri göz önünde bulundurur.
- Alınan siber güvenlik önlemlerinin ilgili risklerle orantılı olması, olumlu ve olumsuz etkilerinin değerlendirilmesi ve dengelenmesi sağlanır.
- Siber güvenlik gereksinimlerinin karşılanmasında yerli ürün ve hizmet kullanımı teşvik edilir, bunların geliştirilmesi için araştırma ve geliştirme projeleri desteklenir, yenilikçilik anlayışı esas kabul edilir.

Günümüzde siber güvenlik, özellikle kritik altyapıların tamamı ile bilişim teknolojilerine bağlı olması neticesinde, bireyler, ülkeler ve uluslararası toplumlar için hayati bir öneme sahiptir (Ünver ve Canbay 2010: 96). Siber güvenlik, sadece yazılımlar ile sağlanamaz ve bu yüzden internet kullanıcılarının siber güvenlik hakkında bilgi sahibi olmaları, internet kaynaklı zararların en aza indirilmesi belki de ortadan kaldırılması için son derece önemlidir.

2. LİTERATÜR TARAMASI

Bu bölümde, siber tehdit, siber güvenlik ve benzer konulara ilişkin daha önce yapılan araştırmalara yer verilmiştir. Nitekim, araştırmada ele alınan konu ve alt konuların ilgili bilgi ve araştırma sonuçları belirlenerek araştırma probleminin tanımlanması ve benzer araştırmalara yer verilmesi oldukça önemlidir.

Siber farkındalık bugün dünyanın en dikkat çeken ve en hayati önem taşıyan konuları arasına girmiştir. Farkındalık noktasında yapılan bir araştırmada, "Kişisel Veri Güvenliği Farkındalığı Anketi" Antalya ilinde 526 kişiye uygulanmış ve 501 tanesi değerlendirmeye alınmıştır. Katılımcılara ait veri analizinde t testi, faktör analizi ve varyans analizi kullanılmıştır. Analiz sonuçlarına göre; katılımcıların bilgi güvenliği noktasında farkındalık düzeylerinin ortalamanın üstünde olduğu belirlenmiştir (Çetin; 2014). Yine yapılan başka bir araştırmada, Sakarya Üniversitesi Eğitim Fakültesinin farklı bölümlerinde eğitim gören 217 son sınıf öğrencisi ele alınmış, veri toplama aracı olarak araştırmacılar tarafından geliştirilen "Bilişim Güvenliği Anketi" kullanılmıştır. Veri analizi için ki-kare testi uygulanmış ve analizler sonucunda öğrencilerin çoğunun bilişim güvenliği konusunda farkındalıklarının olduğu belirlenmiştir (Akgün ve Topal, 2015).

Öğretmen adaylarının sosyal ağ sitelerinde güvenlik farkındalıklarını belirlemeye yönelik yapılan farklı bir araştırmada da, 2013-2014 akademik yılında Ahi Evran Üniversitesi Eğitim Fakültesinde öğrenim gören 909 öğretmen adayı üzerinde yapılmıştır. Veri toplama aracı olarak araştırmacılar tarafından geliştirilen "Sosyal Ağ Sitelerinde Güvenlik Farkındalığı Anketi" uygulanmış, verilerin analizinde t testi kullanılmıştır. Araştırma sonucunda katılımcıların parola konusunda yüksek güvenlik farkındalığına sahip oldukları ve anti-virüs programı kullandıkları görülmüştür (Çakır ve diğerleri, 2015). Bu konu da benzer bir araştırma da Yıldırım ve Varol (2013) tarafından yapılmıştır. Araştırma örneklemi Fırat Üniversitesi ve Bitlis Eren Üniversitesi öğrencileri ve akademisyenleri olmak üzere toplam 306 kişidir. Betimsel tarama modelinde gerçekleştirilen bu araştırma sonuçlarına göre katılımcıların çoğunun sosyal medyayı güvenli bulmadığı fakat anti-virüs programı kullanmadıkları görülmüştür.

Türkiye'nin farklı üniversitelerinde Bilgisayar Öğretim Teknoloji Eğitimi bölümünde öğrenim gören 312 öğrencinin katıldığı bir başka araştırmada, veriler internet üzerinden sunulan bir anket yardımı ile toplanmıştır. Analizler sonucunda katılımcıların birçoğu, sosyal medyayı güvenli bulmadıkları halde sosyal medya hesabı kullandıklarını belirtmişlerdir. Ayrıca katılımcıların büyük bir çoğunluğu internet üzerinde kullandıkları parola ve şifreleri değiştirmediklerini belirtmiştir. Bu durum katılımcıların parola güvenliği farkındalıklarının düşük olduğunu göstermektedir (Bilek, 2012). Yine eğitim hayatında, ilköğretim ve lise öğrencilerinin bilgi ve bilgisayar farkındalık düzeylerini ortaya çıkarmak amacıyla yapılan bir başka araştırmada, Kahramanmaraş ilinde öğrenim gören 2449 öğrencinin katılımıyla geçekleştirilmiştir. Veri toplama aracı olarak "Bilgi Güvenliği Farkındalığı Ölçeği" kullanılmış, veri analizi için t testi ve tek yönlü ANOVA analizi uygulanmıştır. Analizler sonucunda kız öğrencilerin erkek öğrencilere göre bilgi güvenliği farkındalıklarının daha fazla olduğu görülmüştür. Yine araştırma sonuçları öğrencilerin parola güvenliği farkındalıklarının çok düşük olduğunu ortaya koymuştur (Tekerlek ve Tekerlek, 2013).

Aslanyürek, (2016) tarafından yapılan bir başka araştırmada, ülkemizdeki internet kullanıcılarının internet güvenliği ve çevrimiçi gizlilik alanlarındaki ihlaller karşısında kanaatlerini ve farkındalıklarını değerlendirmek amaçlanmıştır. Bu amaçla 479 katılımcılı bir anket araştırması gerçekleştirilmiştir. İki bağımsız değişkeni olan verilere t testi, ikiden fazla bağımsız değişkeni olan verilere ANOVA analizi uygulanmıştır. Analizler sonucunda katılımcıların internet güvenliği farkındalıklarının yüksek olduğu ve güvenlik ihlallerine rağmen sosyal medya hesaplarını kullanmaktan vazgeçmedikleri görülmüştür.

Ege Üniversitesi İletişim Fakültesi öğrencilerinin internet ve sosyal medya kullanımlarına ilişkin yapılan bir araştırmada örneklem grubunu Ege Üniversitesi İletişim Fakültesinde öğrenim gören 319 öğrenci oluşturmuştur. Veriler araştırmacılar tarafından geliştirilen bir anket ile toplanmış, verilerin değerlendirilmesinde frekans analizi ile ANOVA analizi kullanılmıştır. Analizler sonucunda öğrencilerin büyük bir kısmının sosyal medya hesabına sahip olduğu, yarısından çoğunun her gün internete girdikleri, büyük bir çoğunluğunun da sosyal medya hesaplarından tanımadıkları kişiler ile görüşmedikleri görülmüştür (Vural ve Bat; 2010).

3. YÖNTEM

Bu araştırma belirlenen bir kitleden veri toplayarak kitlenin özelliklerini ortaya çıkarmak amacıyla yapılmıştır. Bu nedenle araştırmada kesitsel tarama modeli kullanılmıştır. Kesitsel araştırmalarda değişkenler betimlenmek üzere tek seferde ölçülür (Büyüköztürk ve diğerleri, 2011). Araştırma amacıyla araştırmacılar tarafından geliştirilen ankette farkındalık düzeyleri incelenerek katılımcıların siber güvenlikte dikkat ettikleri konular belirlenmeye çalışılmıştır. Araştırma sonunda elde edilen veriler SPSS 17 paket programı ile bilgisayara aktarılmış ve gerekli analizler yapılmıştır.

2.1. Araştırmanın Hipotezleri

Araştırma kapsamında iki ana hipotez test edilmektedir.

Ana Hipotezler

H_1: İnönü Üniversitesi İletişim Fakültesi öğrencilerinin siber güvenlik farkındalığı düşüktür.

H_0: İnönü Üniversitesi İletişim Fakültesi öğrencilerinin siber güvenlik farkındalığı yüksektir.

Alt Hipotezler

$H_{1.1}$: İnönü Üniversitesi İletişim Fakültesi öğrencilerinin siber güvenlik farkındalığı cinsiyete göre farklılık gösterir.

$H_{1.2}$: İnönü Üniversitesi İletişim Fakültesi öğrencilerinin siber güvenlik farkındalığı günlük internet kullanım süresine göre farklılık gösterir.

$H_{1.3}$: İnönü Üniversitesi İletişim Fakültesi öğrencilerinin siber güvenlik farkındalığı okudukları bölüme göre farklılık gösterir.

Katılımcılar

Bu araştırmanın evrenini, İnönü Üniversitesi İletişim Fakültesi Halkla İlişkiler ve Tanıtım ve Gazetecilik 1. ve 2. öğretim programlarında 2017-2018 akademik yılı güz döneminde eğitim gören toplam 394 lisans öğrencisi oluşturmaktadır. Anket evren kümesinin tamamına uygulanmış ancak yapılan incelemeler sonucunda hatalı ve eksik anketler çıkartılarak 368 anket değerlendirmeye tabi tutulmuştur. Bu öğrencilerin programlarına göre dağılımları şöyledir: Halkla İlişkiler ve Tanıtım 255, Gazetecilik 113.

2.2. Veri Toplama Aracı

Bu çalışmada veri toplama aracı olarak "Siber Güvenlik Farkındalığı Anketi" kullanılmıştır. Bu anket gerekli literatür çalışmaları ve konu ile ilgili anketler incelenerek araştırmacılar tarafından hazırlanmıştır. Anketin kapsam ve geçerliliği için ölçek 50 kişilik bir gruba uygulanmış geçerlilik ve güvenirlilik testleri yapıldıktan sonra güvenirlilik katsayısı düşük olan sorular anketten çıkarılmıştır. Sonuç olarak anketin güvenirlilik katsayısı (cronbach's alpha) 0,77 bulunmuştur. Güvenilirlik katsayısının 0,70 ve daha yüksek olması test puanlarının güvenilirliği için yeterli olarak görüldüğünden (Büyüköztürk, 2008: 171), geliştirilen ölçeğin güvenilir olduğu söylenebilir. Anket 9'u 2'li likert tipi, 7'si 5'li likert tipi, 7'si demografik ve kullanım özelliklerine ilişkin toplam 23 sorudan oluşmuştur. 2'li likert tipi hazırlanan soruların cevap seçenekleri "Evet" ve

"Hayır", 5'li likert tipi hazırlanan soruların cevap seçenekleri öğrencilerin "Kesinlikle Katılıyorum", "Katılıyorum", "Kararsızım", "Katılmıyorum" ve "Kesinlikle Katılmıyorum" şeklinde kendilerini yakın hissettikleri düzeyde yanıt verebilmeleri için düzenlenmiştir. Bulguların okunması ve yorumlanmasının kolay olması amacıyla "Kesinlikle Katılıyorum" ve "Kesinlikle Katılmıyorum" cevapları birleştirilerek "Katılıyorum" ve "Katılmıyorum" başlığı altında sunulmuştur. Anketteki sorular sosyal medya, siber saldırıya karşı önlemler, siber güvenlik farkındalığı, ülkemizin siber güvenlik farkındalığı ve savaş halleri olmak üzere 5 başlık altında toplanmıştır.

2.3. Verilerin Analizi

Veriler ankette yer alan sorulara verilen yanıtlara göre 5 ayrı başlık altında toplanmış, frekans ve yüzde değerleri ile betimlenmiştir. Siber güvenlik farkındalığının, cinsiyet, yaş ve internet ortamında geçirilen zamana göre farklılaşıp farklılaşmadığı ki-kare ile incelenmiştir.

3. Bulgular

Bulgular ankette yer alan maddelerin kategorilerine göre yukarda belirtilen 5 başlık altında sunulmuştur.

3.1.1. Sosyal Medya Sorularına Verilen Cevaplara Ait Bulgular

Katılımcıların sosyal medya ile ilgili verdikleri cevaplar Tablo 1'de sunulmuştur.

Tablo 1. Sosyal Medya Sorularına Verilen Cevaplara Ait Frekans ve Yüzdelikler

Soru		**f**	**%**
S4- Herhangi bir sosyal medya hesabı kullanıyor musunuz veya hiç kullandınız mı?	Evet	368	100
	Hayır	0	0
S9- Sosyal medyayı güvenli buluyor musunuz?	Evet	65	17,7
	Hayır	303	82,3
S12- Farklı sosyal medya hesaplarındaki şifreleriniz aynı mı?	Evet	149	40,5
	Hayır	219	59,5
S13- Sahte hesap kullandınız mı?	Evet	139	37,8
	Hayır	229	62,2
S14- Başkasına ait bir sosyal medya hesabını ele geçirmeye çalıştınız mı?	Evet	70	19,0
	Hayır	298	81,0
S15- Sosyal medya hesaplarında tanımadığınız kişilerden gelen teklifleri kabul ediyor musunuz?	Evet	180	48,9
	Hayır	188	51,1

Tablo 1'deki veriler incelendiğinde, öğrencilerin tamamının en az bir sefer sosyal medya hesabı kullandıkları görülmektedir. Bunun yanında öğrencilerin, %82,3'ünün sosyal medyayı güvenli

bulmadıkları, %48,9'unun sosyal medya hesaplarında tanımadıklarından gelen teklifleri kabul ettikleri ve %37,8'inin sahte bir hesap kullandıkları fakat sadece %19'unun bir başkasına ait sosyal medya hesabını ele geçirmeye çalıştığı görülmektedir. Öğrencilerin büyük kısmı sosyal medyayı güvenli bulmamasına rağmen, sosyal medyada tanımadığı kişilerden gelen teklifleri kabul edenlerin sayısı azımsanmayacak kadar fazladır. Ayrıca öğrencilerin %40,5'inin farklı sosyal hesaplarda kullandıkları şifrelerin aynı olduğunu görülmektedir. Bu duruma göre öğrencilerin şifre ve parola konusunda farkındalıklarının çok fazla olmadığını söylemek mümkündür.

3.1.2. Siber Saldırılara Karşı Önlemler Sorularına Verilen Cevaplara Ait Bulgular

Katılımcıların siber saldırılara karşı önlemler ile ilgili verdikleri cevaplar Tablo 2 ve Tablo 3'te sunulmuştur.

Tablo 2. Siber Saldırılara Karşı Önlemler Sorularına Verilen Cevaplara Ait Frekans ve Yüzdelikler

Soru		**f**	**%**
S18- Anti-virüs programları virüslere karşı yeterlidir	Katılıyorum	54	14,7
	Kararsızım	111	30,2
	Katılmıyorum	203	55,1
S19- Siber suç etkinliklerinin hızla arttığı günümüzde, etkili güvenlik önlemleri alınmalıdır	Katılıyorum	320	87
	Kararsızım	25	6,8
	Katılmıyorum	23	6,2

Tablo 2'deki veriler incelendiğinde öğrencilerin %55,1'i anti-virüs programlarının virüslere karşı etkili olmadığını, %87 gibi büyük bir çoğunluğunun da siber suçlara karşı etkili güvenlik önlemleri alınması gerektiğini düşündüğü ortaya çıkmaktadır. Bu sonuçlara göre öğrencilerin, siber saldırılara karşı virüs programına güvenmedikleri ve daha etkili önlemlerin alınması gerektiğini düşündükleri görülmektedir.

Tablo 3. Siber Saldırılara Karşı Önlemler Sorularına Verilen Cevaplara Ait Frekans ve Yüzdelikler

Soru		f	%
S11- Olası siber saldırılara karşı hangi önlemleri alıyorsunuz?	Virüs programı kullanıyorum	166	45,1
	Sık sık şifre değiştiriyorum	129	35,1
	Tek bir bilgisayardan internete giriyorum	46	12,5
	Maillerime güvenlik kodu ile giriyorum	113	30,7
	Bilgisayarımda başkalarının belleklerini kullanmıyorum	69	18,8
	Önlem almıyorum	81	22,0

Tablo 3'teki veriler incelendiğinde olası bir siber saldırıya karşı öğrencilerin %45,1'si virüs programı kullandıklarını, %35,1'i şifrelerini sık sık değiştiklerini, %12,5'i tek bir bilgisayardan internete girdiklerini, %30,7'si maillerine güvenlik kodu ile girdiklerini, %18,8'i bilgisayarında başkalarının belleklerini kullanmadıklarını belirtirken, %22'si herhangi bir önlem almadıklarını belirtmiştir. Tablo 2'de virüs programlarının etkili olmadığını söyleyen (%55,1) ve bu konuda kararsız olduklarını belirten öğrencilerin (%30,2) bu kadar fazla olmasına karşın, siber saldırılara karşı virüs programı kullandıklarını söyleyen (%45,1) öğrenci sayıları çelişmektedir. Bu durumda öğrencilerin siber saldırılara karşı etkili güvenlik önlemleri farkındalıklarının az olduğu ve bu konuda eğitimler düzenlenmesi gerektiği ortaya çıkmaktadır. Bunun yanında olası saldırılara karşı herhangi bir önlem almayanların sayısı da (%22) azımsanmayacak kadar çoktur.

3.1.3. Siber Güvenlik Farkındalığı Sorularına Verilen Cevaplara Ait Bulgular

Katılımcıların siber güvenlik farkındalığı ile ilgili verdikleri cevaplar Tablo 4 ve Tablo 5'te sunulmuştur.

Tablo 4. Siber Güvenlik Farkındalığı Sorularına Verilen Cevaplara Ait Frekans ve Yüzdelikler

Soru		f	%
S5- Siber güvenlik hakkında bilgi sahibi misiniz?	Evet	165	44,8
	Hayır	203	55,2
S6- Siber saldırıya maruz kaldınız mı?	Evet	41	11,1
	Hayır	327	88,9
S7- Veri hırsızlığının suç olduğunu biliyor musunuz?	Evet	300	81,5
	Hayır	68	18,5
S8- Karşılaştığınız bir siber suçu nereye bildireceğinizi biliyor musunuz?	Evet	129	35,1
	Hayır	239	64,9
S17- Siber güvenliğinizin sağlandığına inanıyor musunuz?	Evet	54	14,6
	Hayır	314	85,4

Tablo 4'deki veriler incelendiğinde öğrencilerin %55,2'si siber güvenlik hakkında bilgi sahibi olmadığını, %81,5'i veri hırsızlığının suç olduğunu bildiğini fakat %64,9'u bir siber suçu nereye bildireceklerini bilmediklerini, %85,4'ü siber güvenliklerinin sağlandığına inanmadıklarını belirtmiştir. Ayrıca %88'9'u bir siber saldırıya maruz kalmadığını belirtmiştir. Bu sonuçlara göre katılımcıların siber güvenlik hakkında yeterince bilgi sahibi olmadıkları ve bu konuda gerekli bilgilendirmelerin yapılması gerektiği görülmektedir.

Tablo 5. Siber Güvenlik Farkındalığı Sorularına Verilen Cevaplara Ait Frekans ve Yüzdelikler

Soru		f	%
S10- Siber tehdit sizce nedir?	Veri hırsızlığı	65	17,7
	Virüs bulaşması	12	3,3
	Bilgisayar korsanlarının bilgisayara girmesi	46	12,5
	Şifremin çalınması	10	2,7
	Kredi kartı bilgilerimin çalınması	3	0,8
	Hepsi	232	63,0

Tablo 5'deki veriler incelendiğinde öğrencilerin %17,7'si veri hırsızlığını, %12,5'i bilgisayara korsanların girmesini, %3,3'ü virüs bulaşmasını, %2,7'si şifrelerinin çalınmasını, sadece %0,8'i kredi kartı bilgilerinin çalınmasını siber tehdit olarak görürken, çoğunluğu olan %63'ü bunların hepsinin siber tehdit olduğunu belirtmiştir. Bu sonuçlara göre katılımcıların siber tehdit hakkındaki farkındalıklarının yeterli olduğu söylenebilir.

3.1.4. Ülkemizin Siber Güvenlik Farkındalığı Sorularına Verilen Cevaplara Ait Bulgular

Katılımcıların ülkemizin siber güvenlik farkındalığı ile ilgili verdikleri cevaplar Tablo 6'da sunulmuştur.

Tablo 6. Ülkemizin Siber Güvenlik Farkındalığı Sorularına Verilen Cevaplara Ait Frekans ve Yüzdelikler

Soru		f	%
S20- Ülkemizin siber güvenlik konusunda yeterli bilgiye sahip olduğunu düşünüyorum	Katılıyorum	72	19,5
	Kararsızım	131	35,6
	Katılmıyorum	165	44,9
S22- Siber güvenliğe devletin ciddi yatırımlar yapması gerektiğini düşünüyorum	Katılıyorum	305	83,9
	Kararsızım	43	11,7
	Katılmıyorum	20	4,4

Tablo 6'daki veriler incelendiğinde öğrencilerin %44,9'u ülkemizin siber güvenlik konusunda yeterli bilgiye sahip olmadığını düşünürken, %83,9'u siber güvenliğe devletin ciddi yatırımlar yapması gerektiğini belirtmiştir. Bu sonuçlara göre katılımcıların ülkemize siber güvenlik konusunda katılmadıkları görülmüştür.

3.1.5. Savaşlar İle İlgili Sorulara Verilen Cevaplara Ait Bulgular

Katılımcıların savaşlar ile ilgili verdikleri cevaplar Tablo 7 ve Tablo 8'de sunulmuştur.

Tablo 7. Savaşlar İle İlgili Sorulara Verilen Cevaplara Ait Frekans ve Yüzdelikler

Soru		f	%
S16- Siber savaşların kişiler üzerinde psikolojik etkisi olabileceğini düşünüyorum	Katılıyorum	309	83,9
	Kararsızım	45	12,2
	Katılmıyorum	14	3,9

Tablo 7'deki veriler incelendiğinde öğrencilerin %83,9'u siber savaşların psikolojik etkisi olabileceğini belirtmiştir.

Tablo 8. Savaşlar İle İlgili Sorulara Verilen Cevaplara Ait Frekans ve Yüzdelikler

Soru		f	%
S23- Günümüzde ülke olarak içerisinde bulunduğumuzu düşündüğünüz savaş hangisi/hangileridir?	Psikolojik Savaş	250	67,9
	Biyolojik Savaş	70	19,0
	Ekonomik Savaş	240	65,2
	Siber Savaş	219	59,5
	Silahlı Savaş	144	39,1
	Nükleer Savaş	74	20,1

Tablo 8'deki veriler incelendiğinde öğrencilerin %67,9'u psikolojik savaş, %65,2'si ekonomik savaş, %59,5'i siber savaş, %39,1'i silahlı savaş içerisinde bulunduğumuzu belirtirken sadece %19'u biyolojik savaş ve %20,1'i nükleer savaş içerisinde bulunduğumuzu belirtmiştir.

2.2.1. Cinsiyete Göre Verilen Cevapların Farklılık Gösterdiği Sorulara İlişkin Bulgular

Katılımcıların verdikleri yanıtlar cinsiyet değişkenine göre çaprazlandığında dağılımın anlamlı farklılık gösterdiği sorular Tablo 9'da verilmiştir.

Tablo 9. Cinsiyete Göre Ki-kare Testi Sonuçları

Soru		Kadın	Erkek	X^2	sd	p
		%	%			
S5- Siber güvenlik hakkında bilgi sahibi misiniz?	Evet	37,8	<u>54,1</u>	9,687	1	,002
	Hayır	<u>62,2</u>	45,9			
S8- Karşılaştığınız bir siber suçu nereye bildireceğinizi biliyor musunuz?	Evet	25,4	<u>47,8</u>	19,973	1	,000
	Hayır	<u>74,6</u>	52,2			
S15- Sosyal medya hesaplarında tanımadığınız kişilerden gelen teklifleri kabul ediyor musunuz?	Evet	<u>58,9</u>	41,1	19,121	1	,000
	Hayır	35,8	<u>64,2</u>			

Tablo 9'daki veriler incelendiğinde siber güvenlik hakkında bilgi sahibi olan erkeklerin (%54,1) kadınlara göre (%37,8) daha fazla bilgi sahibi oldukları görülmektedir. Karşılaşılan bir siber suçu nereye bildireceklerini bilen erkekler (%47,8) yine kadınlara göre (%25,4) daha fazladır. Bunlara karşın kadınlar (%58,9) erkeklere göre (%41,1) sosyal medya hesaplarında tanımadıkları kişilerden gelen teklifleri daha fazla kabul etmektedir.

2.2.2. Yaşlara Göre Verilen Cevapların Farklılık Gösterdiği Sorulara İlişkin Bulgular

Katılımcıların verdikleri yanıtlar yaş değişkenine göre çaprazlandığında dağılımın anlamlı farklılık gösterdiği sorular Tablo 10'da verilmiştir.

Tablo 10. Yaşlara Göre Ki-kare Testi Sonuçları

Soru		17-19	20-22	23-25	26 +	X^2	sd	p
		%	%	%	%			
S8- Karşılaştığınız bir siber suçu nereye bildireceğinizi biliyor musunuz?	Evet	34,3	30,2	43,8	56,0	9,163	3	,027
	Hayır	65,7	69,8	56,3	44,0			
S11- Virüs programı kullanıyorum	Evet	25,4	48,1	42,2	80	23,824	3	,000
	Hayır	74,6	51,9	57,8	20			

Tablo 10'daki veriler incelendiğinde karşılaşılan bir siber suçu nereye bildireceklerini bilen 26 ve üstü yaştaki öğrenciler (%56,0) 17-19 yaşlarındaki (%34,3), 20-22 yaşlarındaki (%30,2) ve 23-25 yaşlarındaki öğrencilere göre (%43,8) daha fazladır. Yine 26 ve üstü yaştaki öğrenciler (%80) 17-19 yaşlarındaki (%25,4), 20-22 yaşlarındaki (%48,1) ve 23-25 yaşlarındaki öğrencilere göre (%42,2) olası bir siber saldırılara karşı virüs programı kullandıklarını söylemektedir.

2.2.3. İnternet Ortamında Geçirilen Zamana Göre Verilen Cevapların Farklılık Gösterdiği Sorulara İlişkin Bulgular

Katılımcıların verdikleri yanıtlar internet ortamında geçirdikleri süreye göre çaprazlandığında dağılımın anlamlı farklılık gösterdiği sorular Tablo 11'de verilmiştir.

Tablo 11. İnternette Geçirdikleri Zamana Göre Ki-kare Testi Sonuçları

Soru		0-1 saat	2-4 saat	5-7 saat	8 + saat	X^2	sd	p
		%	%	%	%			
S5- Siber güvenlik hakkında bilgi sahibi misiniz?	Evet	7,1	44,5	46,7	75,0	41,934	3	,000
	Hayır	92,9	55,5	53,3	25,0			
S13- Sahte hesap kullandınız mı?	Evet	26,2	33,5	41,0	56,3	11,148	3	,011
	Hayır	73,8	66,5	56,3	43,8			
S23- Günümüzde içinde	Evet	47,6	54,3	63,8	79,2	12,890	3	,005

bulunduğumuz savaş hangisidir? (Siber Savaş)	Hayır	52,4	45,7	36,2	20,8

Tablo 11'deki veriler incelendiğinde siber güvenlik hakkında bilgi sahibi olan günde 8 saat ve üzeri internet kullanan öğrenciler (%75), 5-7 saat internet kullanan (%46,7), 2-4 saat internet kullanan (%44,5) ve 0-1 saat internet kullanan öğrencilere göre (%7,1) daha fazladır. Sahte hesap kullanan 8 saat ve üzeri internet kullanan öğrenciler (%56,3), 5-7 saat internet kullanan (%41), 2-4 saat internet kullanan (%33,5) ve 0-1 saat internet kullanan öğrencilere göre (%26,2) daha fazladır. Aynı şekilde günümüzde ülkemizin siber savaş içerisinde bulunduğunu düşünen 8 saat ve üzeri internet kullanan öğrenciler (%79,2), 5-7 saat internet kullanan (%63,8), 2-4 saat internet kullanan (%54,3) ve 0-1 saat internet kullanan öğrencilere göre (%47,6) daha fazladır.

Sonuç ve Değerlendirme

Siber güvenlik günümüzde yalnızca bireylerin değil aynı zamanda devletlerin önlem alması gereken ve bu doğrultuda ulusal güvenlik stratejilerini belirlemek zorunda kaldıkları bir kavram haline gelmiştir. Birçok devlet bu kavramın önemini anlayarak sadece ülke genelinde değil uluslararası platformlarda da siber güvenlik için gerekli yatırımları yapmaya başlamışlardır. Siber saldırıların zamanının bilinmemesi yani her an gerçekleşebileceği ve etkilerinin teknolojik anlamda yıkıcı olması devletlerin bu tedbirleri almasında önemli rol oynamıştır. Bu araştırmada üniversite öğrencilerinin siber güvenlik farkındalık düzeyleri ölçülmeye çalışılmış ve aşağıda sıralanan sonuçlara ulaşılmıştır.

Genel olarak sonuçlara bakıldığında öğrencilerin çoğunun bilişim güvenliği konusunda farkındalıklarının az olduğu ortaya çıkmıştır. Bu kapsamda araştırma hipotezlerinden "H_1: İnönü Üniversitesi İletişim Fakültesi öğrencilerinin siber güvenlik farkındalığı yüksektir" hipotezi reddedilerek, "H_2: İnönü Üniversitesi İletişim Fakültesi öğrencilerinin siber güvenlik farkındalığı düşüktür" hipotezi kabul edilmiştir. Çünkü ankette ele alınan birçok boyut açısından sorulara azımsanmayacak sayıda öğrenci kararsız ya da olumsuz yanıt vermiştir. Örneğin katılımcıların çok büyük bir çoğunluğu anti-virüs programlarının virüslere karşı yeterli olmadığını düşünürken, yine katılımcıların yaklaşık yarısı siber saldırılara karşı virüs programı kullandıklarını belirtmişlerdir. Aynı zamanda katılımcıların büyük bir çoğunluğu farklı sosyal medya hesaplarında aynı parolayı kullandıklarını belirtmiştir. Bu durumda katılımcıların parola güvenliği konusunda fazla bilgi sahibi olmadıklarını göstermektedir. Bununla birlikte, sosyal medyayı güvenli bulmayan katılımcıların sayısı azımsanmayacak kadar fazladır. Aynı zamanda sosyal medya hesaplarında tanımadığı kişilerden gelen teklifleri kabul ettiklerini ve sahte hesap kullandıklarını belirten katılımcı sayısı kayda değer sayıdadır.

$H_{1.1}$ alt hipotezi doğrultusunda siber güvenlik farkındalığının cinsiyete göre farklılaşıp farklılaşmadığı incelendiğinde erkek öğrencilerin kız öğrencilere oranla siber güvenlik hakkında daha fazla bilgi sahibi oldukları ve siber bir suçu nereye bildireceklerini bildikleri görülmektedir. Kadınların ise sosyal medyada tanımadıkları kişilerden gelen talepleri daha fazla kabul ettikleri görülmüştür.

$H_{1.2}$ alt hipotezi doğrultusunda siber güvenlik farkındalığının günlük internet kullanım sürelerine göre farklılaşıp farklılaşmadığı incelendiğinde, interneti daha fazla kullanan katılımcıların siber güvenlik hakkında daha fazla bilgi sahibi oldukları görülmüştür. Bunun yanında günlük internet kullanım süreleri daha fazla olan katılımcıların sahte hesap kullandıkları bir anlamda etik dışı davranış sergiledikleri görülmüştür.

$H_{1.3}$ alt hipotezi doğrultusunda siber güvenlik farkındalığının okudukları bölüme göre farklılaşıp farklılaşmadığı incelendiğinde ise, anlamlı bir farklılık saptanmamıştır. Bunun nedeni farklı bölümler olsa da okudukları fakültenin aynı olması ve bölüm derslerinin paralellik göstermesi olabilir.

Tüm bu sonuçlar ışığında siber güvenlik ve bilgi güvenliği farkındalığı kazandırılmasına yönelik eğitimlerin verilmesinin gerekli olduğu düşünülmektedir. Bu eğitimler ile siber saldırılar, siber güvenlik ve siber saldırılara karşı alınabilecek önlemler anlatılmalıdır. Gelecek araştırmalarda, fakülte öğrencilerinin bilişim güvenliğini ve farkındalığını arttırmak ve yeterli düzeyde bilgilendirmek için neler yapılabileceği ile ilgili araştırmalar yapılabilir.

KAYNAKLAR

2016-2019 Ulusal Siber Güvenlik Stratejisi (2016), T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf Erişim tarihi: 30.11.2017.

Akgün, Ö.E., Topal, M. (2015). Eğitim Fakültesi Son Sınıf Öğrencilerinin Bilişim Güvenliği Farkındalıkları: Sakarya Üniversitesi Eğitim Fakültesi Örneği. Sakarya University Journal of Education, 5(2), 98-121.

Akleylek, S., Tok, Z. (2011). Siber Güvenlikte Kriptoloji. Siber Güvenlik Çalıştayı, Ankara.

Alkan, M. (2012). Siber Güvenlik ve Siber Savaşlar. Siber Güvenlik Siber Savaşlar TBMM İnternet Komisyonu.

Altunok, E., Vural, A.F. (2016). Bilişim Suçları. Denetişim, 8, 74-84.

Aslanyürek, M. (2016). İnternet ve Sosyal Medya Kullanıcılarının İnternet Güvenliği ve Çevrimiçi Gizlilik ile İlgili Kanaatleri ve Farkındalıkları. Maltepe Üniversitesi İletişim Fakültesi Dergisi, 3(1), 80-106.

Aslay, F. (2017). Siber Saldırı Yöntemleri Ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi. International Journal Of Multidisciplinary Studies And Innovative Technologies, 1(1), 24-28.

Aytekin, A. (2015). Türkiye'nin Siber Güvenlik Stratejisi Ve Eylem Planının Değerlendirilmesi. Gazi Üniversitesi Bilişim Enstitüsü Yayımlanmamış Yüksek Lisans Tezi, Ankara.

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

Büyüköztürk, Ş. (2008). Veri Analizi El Kitabı, Pegem Yayınları, Ankara.

Büyüköztürk, Ş., Kılıç Çakmak, E., Akgün, Ö. E., Karadeniz, Ş. ve Demirel, F. (2012). Bilimsel araştırma yöntemleri (11. Baskı). Ankara: PegemA Yayıncılık.

Carr, J. (2011). Inside Cyber Warfare Mapping Te Cyber Underworld. O'Reilly Media. ISBN: 9781449382995

Clarke, R.A., Knake R.K. (2010). Cyber War: The Next Threat To National Security And What To Do About It. Harper Collins Publishers. ISBN: 9780061962233

Çakır, H., Hava, K., Gülen, Ş.B., Özüdoğru, G. (2015). Öğretmen adaylarının sosyal ağ sitelerinde güvenlik farkındalıklarının incelenmesi. International Journal of Human Sciences, 12(1), 887-902.

Çeliktaş, B. (2016). Siber Güvenlik Kavramının Gelişimi Ve Türkiye Özelinde Bir Değerlendirme. Karadeniz Teknik Üniversitesi Sosyal Bilimler Enstitüsü Yayımlanmamış Yüksek Lisans Tezi, Trabzon.

Çetin, H. (2014). Kişisel Veri Güvenliği Ve Kullanıcıların Farkındalık Düzeylerinin İncelenmesi. Akdeniz İ.İ.B.F. Dergisi, 29, 86-105.

Çubukcu, A., Bayzan, Ş. (2013). Türkiye'de Dijital Vatandaşlık Algısı Ve Bu Algıyı İnternetin Bilinçli, Güvenli Ve Etkin Kullanımı İle Artırma Yöntemleri. Middle Eastern & African Journal Of Education, 5, 148-174.

Hansen, L., Nissenbaum, H. (2009). Digital Disaster, Cyber Security And The Copenhagen School. International Studies Quarterly, 53(4), 1155-1175.

Hekim, H., Başıbüyük, O. (2013). Siber Suçlar Ve Türkiye'nin Siber Güvenlik Politikaları. Uluslararası Güvenlik ve Terörizm Dergisi, 4(2), 135-158.

Goodrich, M., Tamassia, R. (2011). Introduction To Computer Security: International Edition. Pearson. ISBN: 9780321702012

Gordon, S., Ford, R. (2006). On The Definition And Classification Of Cybercrime. Journal in Computer Virology, 2, 13-20.

Güngör, M. (2015). Ulusal Bilgi Güvenliği: Strateji VE Kurumsal Yapılanma. T.C. Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı Uzmanlık Tezi, Ankara.

Karakuş, C. (2013). Kritik Alt Yapılara Siber Saldırı, İstanbul Kültür Üniversitesi. http://ylt44.com/bilimsel/siber.html Erişim tarihi: 24/11/2017

Mann, D., Sutton, M. (1998). More Change in the Organization of Thieving. British Journal of Criminology, 38(2), 201-229.

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

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

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

Vural, Z.B., Bat, M. (2010). Yeni Bir İletişim Ortamı Olarak Sosyal Medya: Ege Üniversitesi İletişim Fakültesine Yönelik Bir Araştırma. Journal of Yasar University, 20(5), 3348-3382.

Yıldırım, N., Varol, A. (2013). Sosyal Ağlarda Güvenlik: Bitlis Eren ve Fırat Üniversitelerinde Gerçekleştirilen Bir Alan Çalışması. Bilgisayar Bilimleri ve Mühendisliği Dergisi, 6(1), 285-292.