T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ
EĞİTİM BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ
ANABİLİM DALI
BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ
BİLİM DALI

Selim ASLAN

YÜKSEK LİSANS TEZİ

Danışman
Doç. Dr. Ahmet Naci ÇOKLAR

Konya–2019

T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ
EĞİTİM BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ
ANABİLİM DALI
BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ
BİLİM DALI

BİLİŞİM TEKNOLOJİLERİ ALANINDAKİ MESLEK LİSESİ ÖĞRENCİLERİNİN SİBER GÜVENLİĞE YÖNELİK BİLGİ DÜZEYLERİNİN BELİRLENMESİ

Selim ASLAN

YÜKSEK LİSANS TEZİ

Danışman
Doç. Dr. Ahmet Naci ÇOKLAR

Konya–2019

BİLİMSEL ETİK SAYFASI

T. C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ
Eğitim Bilimleri Enstitüsü Müdürlüğü

BİLİMSEL ETİK SAYFASI

Öğrencinin		
	Adı Soyadı	Selim ASLAN
	Numarası	128305011016
	Ana Bilim/ Bilim Dalı	Bilgisayar ve Öğretim Teknolojileri Anabilim Dalı / Bilgisayar ve Öğretim Teknolojileri Eğitimi Bilim Dalı
	Programı	Tezli Yüksek Lisans ■ Doktora □
	Tezin Adı	Bilişim Teknolojileri Alanındaki Meslek Lisesi Öğrencilerinin Siber Güvenliğe Yönelik Bilgi Düzeylerinin Belirlenmesi

Bu tezin proje safhasından sonuçlanmasına kadarki bütün süreçlerde bilimsel etiğe ve akademik kurallara özenle riayet edildiğini, tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada başkalarının eserlerinden yararlanılması durumunda bilimsel kurallara uygun olarak atıf yapıldığını bildiririm.

Selim ASLAN

YÜKSEK LİSANS TEZİ KABUL FORMU

T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ
Eğitim Bilimleri Enstitüsü Müdürlüğü

KONYA

EĞİTİM BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ KABUL FORMU

Öğrencinin		
	Adı Soyadı	Selim ASLAN
	Numarası	128305011016
	Ana Bilim Dalı	Bilgisayar ve Öğretim Teknolojileri Anabilim
	Bilim Dalı	Bilgisayar ve Öğretim Teknolojileri Bilim Dalı
	Programı	Tezli Yüksek Lisans
	Tez Danışmanı	Doç.Dr. Ahmet Naci ÇOKLAR
	Tezin Adı	Bilişim Teknolojileri Alanındaki Meslek Lisesi Öğrencilerinin Siber Güvenliğe Yönelik Bilgi Düzeylerinin Belirlenmesi

Yukarıda adı geçen öğrenci tarafından hazırlanan Bilişim Teknolojileri Alanındaki Meslek Lisesi Öğrencilerinin Siber Güvenliğe Yönelik Bilgi Düzeylerinin Belirlenmesi başlıklı bu çalışma 30/05/2019 tarihinde yapılan savunma sınavı sonucunda oybirliği/oyçokluğu ile başarılı bulunarak, jürimiz tarafından yüksek lisans tezi olarak kabul edilmiştir.

	Ünvanı Adı Soyadı	İmza
Danışman	Doç.Dr. Ahmet Naci ÇOKLAR	
Jüri Üyesi	Doç.Dr. Y. Levent ŞAHİN	
Jüri Üyesi	Dr. Öğr. Üyesi Şemseddin GÜNDÜZ	

Necmettin Erbakan Üniversitesi Eğitim Bilimleri Enstitüsü Ahmet Keleşoğlu Eğitim Fak 42090 Meram Yeni Yol **Meram/KONYA**
Tel : 0 332 324 76 60
Faks : 0 332 324 55 10
Elektronik Ağ: https://www.konya.edu.tr/egitimbilimlerenstitusu
E- Posta: ebil@konya.edu.tr

ÖNSÖZ-TEŞEKKÜR

Günümüzde hızla gelişen bilişim teknolojilerinin insanların hayatlarını kolaylaştıran özelliklerinin yanı sıra birçok tehdidi de barındırdığı göz ardı edilemeyecek bir gerçektir. İnsanların interneti ne kadar çok kullandığı, e-ticaret, e-devlet, e-okul, sosyal medya gibi uygulamaların sayısal verilerinden çok daha net anlaşılmaktadır. Ağa bağlanan bir cihazın da dünya üzerindeki tüm cihazlarla bağlantıya geçtiği düşünüldüğünde, siber dünyadaki tüm kötü niyetli insanların da hedefi haline geldiği görülmektedir. Bu tehlikelerden korunabilmek için bireylerin siber güvenlik bilgi düzeylerinin yeterli olması ve gelişen teknoloji göz önünde bulundurulduğunda güncellenmesi gerekmektedir.

Geleceğimizin teminatı olan çocuklarımızın bu tehlikelerden korunmasının önemi düşünüldüğünde, araştırmamızın merkezinde yer alan Bilişim Teknolojileri alanındaki öğrencilerin, hem bu teknolojiyi en çok kullanan hem de bu teknolojileri geliştirecek olan bireyler olması sebebiyle siber güvenlik bilgi düzeylerinin belirlenmesinin kayda değer olduğu düşünülmektedir.

Bu çalışmamın verilerini toplamak amacıyla yardımlarını talep ettiğim meslektaşlarım olan değerli öğretmenlere, saygıdeğer yöneticilerime teşekkürlerimi sunar, çalışma hayatlarında başarılar dilerim.

Yüksek lisans sürecimin her noktasında ilgisini, desteğini, engin görüşlerini benden esirgemeyen kıymetli hocam Sayın Doç. Dr. Ahmet Naci ÇOKLAR'a teşekkürü bir borç bilir, onu tanıma ve çalışma fırsatı yakalamaktan dolayı onur duyduğumu belirtmek isterim.

Son olarak yüksek lisans fikrimin doğuşundan itibaren son ana kadar her aşamada desteği ve değerli görüşleri ile güç veren, yolumu aydınlatan, adeta beni tamamlayan hayat arkadaşım sevgili eşime sonsuz teşekkürlerimi sunarım.

Selim ASLAN

Konya, 2019

T. C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ
Eğitim Bilimleri Enstitüsü Müdürlüğü

Öğrencinin		
	Adı Soyadı	Selim ASLAN
	Numarası	128305011016
	Ana Bilim / Bilim Dalı	Bilgisayar ve Öğretim Teknolojileri Anabilim Dalı / Bilgisayar ve Öğretim Teknolojileri Eğitimi Bilim Dalı
	Programı	Tezli Yüksek Lisans ■ Doktora □
	Tez Danışmanı	Doç.Dr. Ahmet Naci ÇOKLAR
	Tezin Adı	Bilişim Teknolojileri Alanındaki Meslek Lisesi Öğrencilerinin Siber Güvenliğe Yönelik Bilgi Düzeylerinin Belirlenmesi

ÖZET

Günümüz eğitim politikası incelendiğinde, Mesleki ve Teknik Anadolu Liselerinin Bilişim Teknolojileri alanı için belirlenen öğretim programında siber güvenlik eğitiminin Ağ İşletmenliği dalında bir dersin modülünde ve ortak dersler içerisinde yer alan bir dersin modülünde yer aldığı görülmektedir. Alanı gereği bilişim teknolojilerini en çok kullanan öğrenciler olması ve bu teknolojileri ileride geliştirecek bireyler olması sebebiyle Bilişim Teknolojileri alanındaki öğrencilerin aldıkları eğitimler neticesinde siber güvenlik bilgilerinin hangi düzeyde olduğunun incelenmesinin değerli olduğu düşünülmektedir.

Bu araştırmanın amacı, meslek liselerinde bilişim teknolojileri alanındaki öğrencilerin kişisel siber güvenliğe yönelik bilgi düzeylerinin belirlenmesidir.

Bu bağlamda, Konya ili Meram, Selçuklu ve Karatay merkez ilçelerindeki meslek liselerinin Bilişim Teknolojileri alanındaki 305 öğrenciden veri toplanmıştır. Veri toplamak amacıyla Erol vd. (2015) tarafından geliştirilen Kişisel Siber Güvenliği Sağlama Ölçeği kullanılmıştır.

Veriler analiz edildiğinde genel siber güvenlik bilgi düzeyinin orta seviyede olduğu görülmektedir. Ayrıca farklı değişkenler açısından incelendiğinde, siber

güvenlik eğitimi alan öğrencilerin genel siber güvenlik bilgi düzeylerinin, almayan öğrencilere göre daha yüksek olduğu ortaya çıkmıştır. Öğrencilerin sınıf düzeylerine göre genel siber güvenlik bilgi düzeylerinde ise anlamlı bir farklılık görülmemiştir. Siber mağduriyet yaşama durumlarına göre incelendiğinde de genel siber güvenlik bilgi düzeylerinde anlamlı bir farklılık görülmemektedir. Öğrencilerin genel siber güvenlik bilgi düzeyleri ile algıladıkları kişisel siber güvenlik bilgi seviyeleri arasında istatistiksel olarak anlamlı bir fark bulunduğu, öğrencilerin belirttiği siber güvenlik bilgi seviyeleri arttıkça genel siber güvenlik bilgi düzeylerinin de doğru orantılı olarak arttığı görülmektedir.

Anahtar Kelimeler: Siber güvenlik, bilişim teknolojileri, meslek lisesi, bilgisayar güvenliği, bilgi güvenliği, veri güvenliği, siber güvenlik eğitimi, bilişim suçları, siber suç

T. C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ
Eğitim Bilimleri Enstitüsü Müdürlüğü

Öğrencinin		
	Adı Soyadı	Selim ASLAN
	Numarası	128305011016
	Ana Bilim / Bilim Dalı	Bilgisayar ve Öğretim Teknolojileri Anabilim Dalı / Bilgisayar ve Öğretim Teknolojileri Eğitimi Bilim Dalı
	Programı	Tezli Yüksek Lisans ■ Doktora □
	Tez Danışmanı	Doç.Dr. Ahmet Naci ÇOKLAR
	Tezin İngilizce Adı	Determination of Knowledge Levels of Vocational High School Students in the Field of Information Technologies for Cyber Security

SUMMARY

When today's education policy is examined, it is seen that cyber security education is included in the module of a course in the field of Network Management and in a module of common courses in the curriculum of Vocational and Technical Anatolian High Schools. Due to the fact that there are students who use information technologies as a requirement of their field and they will develop these technologies in the future It is considered that it is valuable to examine the level of cyber security knowledge as a result of the trainings taken by the students in the field of Information Technologies.

The aim of this research is to determine the level of knowledge of personal cyber security in the field of information technologies in vocational high schools.

In this context, the students in the field of Information Technologies of vocational high schools in Meram, Selçuklu and Karatay central districts of Konya were selected. Data were collected from 305 students. In order to collect data, Personal Cyber Security Ensuring Scale developed by Erol et al. (2015) was used.

When the data are analyzed, it is seen that the level of general cyber security knowledge is at the middle level. In terms of different variables, it was found out that

general cyber security knowledge level of the students receiving cyber security education was higher than the students who did not. There was no significant difference in general cyber security knowledge level of students according to their grade level. When it is analyzed according to cyber victimization situations, there is no significant difference in general cyber security knowledge levels. It is seen that there is a statistically significant difference between the students' level of general cyber security knowledge and the level of personal cyber security knowledge they perceive As the level of cyber security knowledge that students stated increases, the level of general cyber security knowledge also increases in direct proportion.

Keywords: Cyber security, information technologies, vocational high school, computer security, information security, data security, cyber security training, cyber crime

KISALTMALAR VE SİMGELER

BİAK: Bilişim ve İnternet Araştırma Komisyonu

BİT**:** Bilgi ve İletişim Teknolojileri

BM: Birleşmiş Milletler

BÖTE: Bilgisayar ve Öğretim Teknolojileri Eğitimi

BT: Bilişim Teknolojileri

BTK: Bilgi Teknolojileri ve İletişim Kurumu

HBÖGM: Hayat Boyu Öğrenme Genel Müdürlüğü

ITU: International Telecommunication Union

İTÜ: İstanbul Teknik Üniversitesi

MEB: Milli Eğitim Bakanlığı

MEGEP: Mesleki Eğitimi Geliştirme Projesi

ODTÜ: Ortadoğu Teknik Üniversitesi

TDK: Türk Dil Kurumu

TEF: Teknik Eğitim Fakültesi

TF: Teknoloji Fakültesi

TÜBİSAD: Türkiye Bilişim Sanayicileri Derneği

TÜİK: Türkiye İstatistik Kurumu

USGF: Uluslararası Siber Güvenlik Federasyonu

USGS: Ulusal Siber Güvenlik Stratejisi

İÇİNDEKİLER

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

BÖLÜM 1

GİRİŞ

Bu bölümde araştırma konusu, araştırma problemini net olarak belirten problem durumu, problem cümlesi, araştırmanın amacı, alt problemler, araştırmanın önemi, varsayımlar ve sınırlılıklar yer almaktadır.

1.1. Problem Durumu

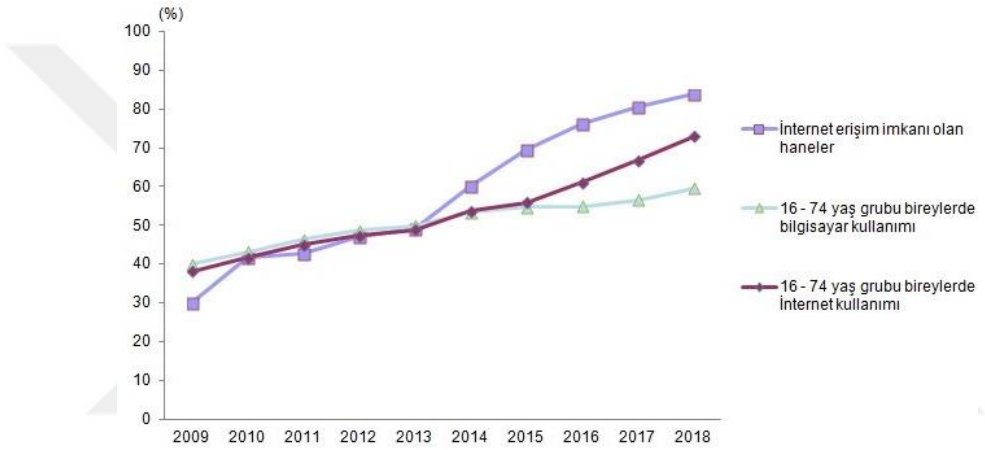
Bilişim güvenliği, dijital ortamda depolanan bilgilerin üçüncü şahıslar tarafından ele geçirilmesini önlemek, bilgi transferi sırasında bilginin bütünlüğünün ve yapısının bozulmadan aktarılmasını sağlamak, sistemlere yetkisiz kişilerin erişmesini engellemek, sistemin sürekli olarak erişilebilir olmasını sağlamak için verilmesi gereken uğraşların tümüdür (Resmi Gazete, 2013). Özellikle 1980'li yıllardan itibaren etkilerini yoğun bir şekilde hissettirmeye başlayan küreselleşme olgusunun da etkisiyle beraber 20. yüzyılın son çeyreği, sosyal ve ekonomik yaşamda çok önemli değişikliklerin yaşandığı bir dönem olmuştur. Bu değişikliklerin en önemlilerinden biri, dünya tarihinin son üç yüz yılına damgasını vuran sanayi toplumundan, bilgi toplumuna geçiş süreci olarak değerlendirilmektedir (Şahin, Çetin ve Yıldırım, 2009). Bu çalışmada da bahsedilmekte olan bilgi toplumu kavramı bilişim teknolojilerinin gelişimine paralel olarak ortaya çıkmıştır. Sanayi devrimi dünyada nasıl bir etki yarattı ise, bilgi toplumuna geçiş de o denli önemli bir olgu olarak karşımıza çıkmaktadır. 20. yüzyıldan günümüze ilerleyen teknolojik gelişmeler ve bilişim teknolojileri de günümüz bilgi çağının ve değişen toplum yapısıyla ortaya çıkan bilgi toplumunun zeminini oluşturmuştur (Çalık ve Çınar, 2009).

2009-2018 Türkiye İstatistik Kurumu (TÜİK) Hanehalkı Bilişim Teknolojileri Kullanım Verilerine göre ise, 2018 yılında, Bilgisayar ve İnternet kullanımı 2018 yılında 16-74 yaş grubundaki bireylerde sırasıyla %59,6 ve %72,9 olarak açıklanmıştır. Bu oranlar 2017 yılında sırasıyla %56,6 ve %66,8 idi. Bilgisayar ve İnternet kullanım oranları 16-74 yaş grubundaki erkeklerde %68,6 ve %80,4 iken, kadınlarda %50,6 ve %65,5 olmuştur. Bu araştırma sonuçlarına göre

haneler, 2018 yılı Nisan ayında hanelerin %83,8'i evden İnternete erişim imkânına sahip oldu. Bu oran 2017 yılının aynı ayında %80,7 olarak açıklanmıştır (TÜİK, 2018).

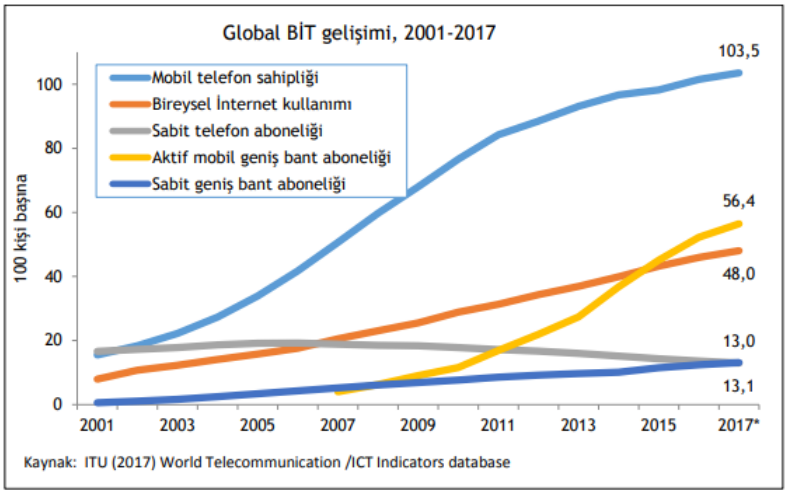
TÜİK tarafından verilen aşağıdaki oranlar incelendiğinde (Şekil 2) Türkiye'de internet kullanım oranlarının işletmelere göre ve hane halkına göre sürekli artış gösterdiği ve %100'e yaklaştığı ifade edilebilir.

Şekil-1: TÜİK, Hanehalkı Bilişim Teknolojileri Kullanım Araştırması, 2018



Akkoyunlu vd. (2018) tarafından yapılan bir diğer araştırmada da benzer şekilde yıllara göre bilgi ve iletişim teknolojileri (BİT) kullanım durumunda sürekli bir gelişim olduğu ifade edilmektedir (Şekil 3).

Şekil- 2: Yıllara göre BİT Kullanım Durumunun Gelişimi (Akkoyunlu vd., 2018)

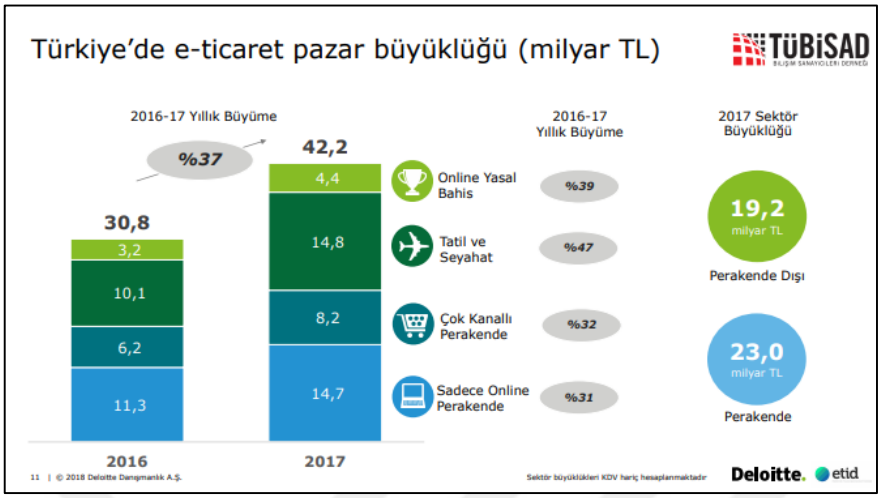


Sosyal medya ile ilgili istatistiklere bakıldığında ise, 2010 yılında dünyada 1 milyara yakın sosyal medya kullanıcısı bulunurken bu rakamın 2017 yılında 2,46 milyara yükseldiği görülmektedir. 2021 yılına kadar ise dünyada 3 milyar insanın sosyal medya kullanıcısı olması beklenmektedir (Statista, 2018). 2017 dijital istatistik sonuçlarına göre Türkiye'de toplamda 48 milyon sosyal medya kullanıcısı bulunmaktadır. Bu rakam ülkenin %60'lık dilimine denk gelmektedir. Zamansal açıdan irdelendiğinde Türkiye'de internet kullanımı bilgisayar veya tablette günlük ortalama 6 saat 46 dakika; telefonda 2 saat 59 dakika; herhangi bir cihazdan sosyal medya kullanımı 3 saat 1 dakika ve televizyon izleme oranı ise 2 saat 14 dakikadır. Türkiye'deki ağ sitelerinin kullanım oranları ise Youtube %57, Facebook %56, Instagram %45 ve Twitter %44'tür (We are Social, 2017). Oranlara bakıldığında sosyal medyanın ne kadar yoğun kullanıldığı anlaşılmaktadır. Bu kadar çok kullanıcının yer aldığı ve çok uzun süreler bu ortamlarda kalındığı göz önünde bulundurulduğunda siber suçlara maruz kalma tehdidinin çok ciddi boyutlara ulaştığı görülmektedir.

Sosyal ağlar, sanal zorbalık, içerik toplayıcılık ve intihal suçlarının yanı sıra öğrenciler, bilgisayar ve internet kullanımı sırasında zararlı yazılımlara (virüs, casus yazılım, Truva atları) maruz kalmakta, bazı belgeleri kaybedilmekte ve yazılım ayarlarını bozabilmektedirler. Kötü niyetli kişiler ile temas kurma, pornografik içerikler ve suç örgütleri öğrencilerin maruz kaldığı diğer durumlardır (Canbek ve Sağıroğlu, 2007). Görüldüğü üzere, ağda bağlı bulunmak aslında her türlü bilişim suçuna maruz kalma riskini de doğurmaktadır. Bu denli tehlikeli bir ortama karşı tedbir alınması da önemli konulardan biri olarak karşımıza çıkmaktadır.

Türkiye Bilişim Sanayicileri Derneği (TÜBİSAD) tarafından Türkiye'de e-ticaret pazarını uluslararası standartlara göre ölçümleyen "Türkiye e-Ticaret 2017 Pazar Büyüklüğü" raporuna göre (Şekil 4), Türkiye'de e-ticaret hacmi yüzde 37 büyüyerek 42,2 milyar TL'ye ulaşmıştır (TÜBİSAD, 2018).

Şekil-3: TÜBİSAD Türkiye'de E-Ticaret Pazar Büyüklüğü



Yukarıdaki şekilden de anlaşılacağı üzere, bilişim teknolojileri ve internet kullanımına bağlı olarak e-ticaret pazarındaki büyüme de görülmektedir.

Türkiye Cumhuriyeti vatandaşlık numarası ve kişisel şifre ile giriş yapılabilen e-devlet portalında; bilgilendirme hizmetleri, entegre elektronik hizmetler, ödeme işlemleri, kurum ve kuruluşlara kısa yollar ile kurumlar arası bilgi ve belge paylaşımı gibi işlemler yapılabilmektedir (turkiye.gov.tr, 2017a). E-devlet portalında 2017 itibariyle 73 kamu kurum ve kuruluşu, 58 ilde 196 belediye ile 9 yerel hizmet belediye kurumu ve 11 özel şirket hizmet vermektedir (turkiye.gov.tr, 2017b). Ülkemizde e-devlete erişim artma eğilimindedir. Ayrıca vatandaşların e-devlet hizmetlerine duyduğu memnuniyet de yüksektir ve memnuniyet oranı %88,7 olarak ifade edilmektedir. Yine TÜİK' in araştırmasına göre özel sektörde e-devlet kullanım oranı %81,4 ile oldukça yüksektir (2016-2019 Ulusal E-Devlet Stratejisi ve Eylem Planı (Taslak), 2015).

Bilgi toplumuna geçiş süreci eğitim öğretim hayatında da kendisini göstermiş, yapılan istatistiklere göre Türkiye'de Google'da en çok aranan 10 isim arasından 7. sırada e-Okul sistemi yer almaktadır. e-Okul, Milli Eğitim Bakanlığı (MEB) tarafından Milli Eğitim Bakanlığı Bilişim Sistemleri (MEBBİS) projesi kapsamında 2007 yılının Ocak ayında kullanıma açılmış olan bir okul yönetim bilgi sistemi web yazılımıdır.

Bir öğrencinin okula kaydından başlayıp, mezuniyetine kadar olan tüm süreci içeren bir sistem Bilgi İşlem Dairesi Başkanlığı tarafından geliştirilmektedir. Devlet ve özel ilköğretim okulları, anaokulları, özel eğitim kurumları, ortaöğretim kurumları e-okul sisteminde işlem yapmaktadır. e-okul sistemi üzerinden öğrenci kaydı, nakil işlemleri, not girişleri, devamsızlık işlemleri, sınav bilgileri, merkezî olarak yapılacak sınavların (TEOG, DPY-B vb.) başvuru ve tercih işlemleri, belge işlemleri (takdir, teşekkür, onur vb.), haftalık ders programı girişleri, alınan belgeler, e-karne, şube yazılı ortalamaları, duyurular ve birçok modül üzerinden bilgi girişleri T.C. Milli Eğitim Bakanlığı'na erişilebilmektedir. Bu kadar geniş kullanım alanına sahip olması da siber mağduriyet açısından dikkat edilmesi gereken bir sistem olarak görülmesine sebep olmaktadır.

Ayrıca e-okulda veliler, öğrencilerin okul durumlarının takibi yapabilsin diye açılmış olan e-okul Veli Bilgilendirme Sistemi (e-okul VBS) bulunmaktadır. Bu sistemde öğrencinin devamsızlıkları, ders programı, davranış notları, sınav tarihleri, okul tarafından yapılan duyurular, merkezî sınavların giriş belgeleri veya tercih sonuçları gösterilir. e-Okul öğrenci girişi için de e-okul sisteminden aynı işlemler yapılarak öğrenciler kendi notlarını ve daha fazlasını görebilir. Bu yönüyle de veli ve öğrencileri bu bilişim sistemini kullanmaya yöneltmektedir. Dolayısıyla öğrenci, öğretmen ve veli olarak düşünüldüğünde bu sistemin Türkiye'deki çok önemli bir kesimi ilgilendirdiği ve güvenliğinin önem arz ettiği ifade edilebilir.

Verilen örneklerde de görüldüğü üzere, bilişim sistemleri yaşamda pek çok alanda kendini göstermekte ve bir tercihten çok zorunluluk haline dönüşmektedir. İnternetin her kurum ve kuruluş için vazgeçilemez bir imkân olması nedeniyle resmi kurum ve kuruluşların bilişim sistemleri bu ağa bağlanmış ve suç işlemeye meyilli kişilerin saldırılarına karşı hedef olmaya başlamıştır. Örnek olarak bugüne kadar güvenliğin en üst seviyede tutulduğu bilinen kurumlar olan Amerika Birleşik Devletleri Savunma Bakanlığı (Pentagon), NATO, NASA ile bazı askeri ve endüstriyel araştırma laboratuvarlarının bilişim sistemlerine sızılmış, pek çok değerli veri çalınmış ya hack eyleminin kurbanı olmuş, şirketin ana sunucularına giren

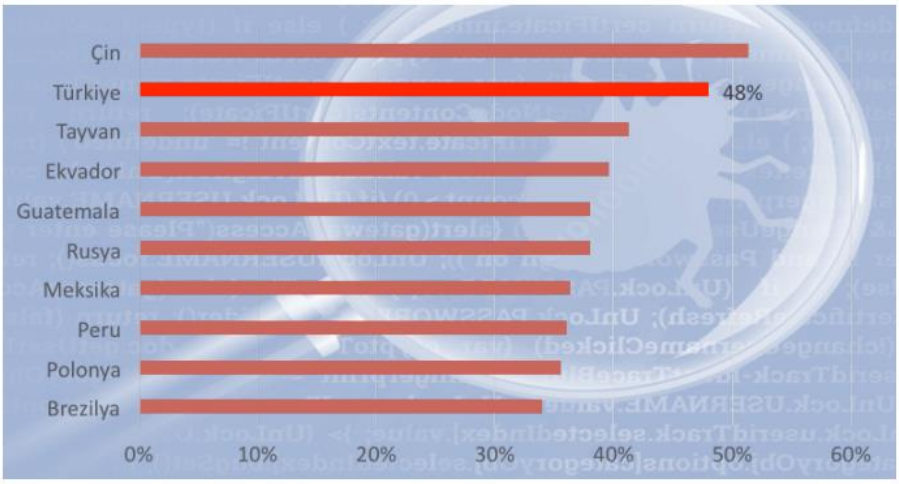
bilgisayar korsanları kullanıcıların iki gün boyunca Microsoft'un sitelerine girememesine yol açmıştır (Alaca, 2008).

5.Uluslarası Siber Suçlar Çalıştayı'nda siber suçlarla mücadele kapsamında 2018 yılında; bilişim sistemleri ihlali, oltalama (phishing), ödeme sistemlerinin kötüye kullanılması, çocukların cinsel istismarı ve yasadışı bahis gibi 54.374 bilişim suçunun işlendiği ve bu suçlara karışan 18.330 kişinin yakalanarak adli makamlara intikal ettirildiği değerlendirmelerinde bulunulmuştur (5. Uluslararası Siber Suçlar Çalıştay Raporu, 2018).

Bilişim Güvenliği ve Bilişim Suçlarına Karşı Mücadele Derneği tarafından yapılan bir değerlendirmede, Türkiye'de bilişim alanında, sosyal medyada işlenen suçların başı çektiği, sosyal medyada nefret söylemi, sahte profil açarak kişisel verilerin ifşa edilmesi ve sosyal medya hesaplarının ele geçirilmesi bu suçlardan bazıları olduğu belirtilmiştir. Şirketlerin sunucularına girilerek kurumsal verilerin şifrelenmesi, şifrelenen bu verilerin yüksek bedellerle şirket sahiplerine satılması, rakip şirketlerin internet sitelerine servisi engellemeye yönelik ataklar, kurum içi veri hırsızlığı, başkası adına online fatura ödeme ve bunu tahsil etme ile ön ödeme dolandırıcılığı, sanal ortamda para aklama, kimlik hırsızlığı da diğer bilişim suçları olarak belirtilmiştir (Anadolu Ajansı, 2017).

Ülkemizde siber suçlarla ilgili sonuçlar yukarıdaki verilerde görülmekle birlikte dünya genelinde diğer ülkeler ve Türkiye'nin bu ülkeler arasındaki yeri de incelenmiştir. Bir güvenlik şirketi olan Havelsan'ın Siber Güvenlik Bülteni'nde yer alan istatistiklere göre tüm ülkelere kötücül yazılım bulaşma oranı aşağıdaki şekilde verilmektedir.

Şekil- 4: Kötücül Yazılım Bulaşma Oranı (Havelsan, 2017)



Şekil 5 incelendiğinde dünya genelinde, neredeyse her iki kötücül yazılımından birinin Türkiye'deki bilişim sistemlerine bulaştığı görülmektedir. Bu yüksek oranla ülkemiz, dünya genelinde Çin'in ardından ikinci sırada yer almaktadır.

Bazı kötücül yazılımlardan etkilenme oranları sadece Türkiye özelinde aşağıdaki tabloda verilmektedir (Tablo 1).

Tablo - 1: 2016 Yılına Ait Türkiye Siber Güvenlik İstatistikleri Geneli (Havelsan, 2017)

Konu	Sıra	Yüzde
Kötücül Yazılım Bulaşma Oranı	2.	% 48
DDoS Saldırı Yapan ya da Yaptırılan (Zombi) Bilgisayarın Bulunduğu Ülkeler	3.	% 10,24
Sazan Avlama Tabanlı Kötücül Barındırma Oranı	10.	% 1
Banka Truva Atı Kurbanları	4.	% 2,77
Fidye Yazılım Ülke Dağılımı	4.	% 6
'HummingBad' Mobil Kötücül Yazılım Hedefleri	5.	% 6

Tablo 1'e bakıldığında, Türkiye'nin belirtilen kötücül yazılımlardan etkilenme oranı, diğer ülkelere göre iyi bir konumda olmadığı görülmektedir.

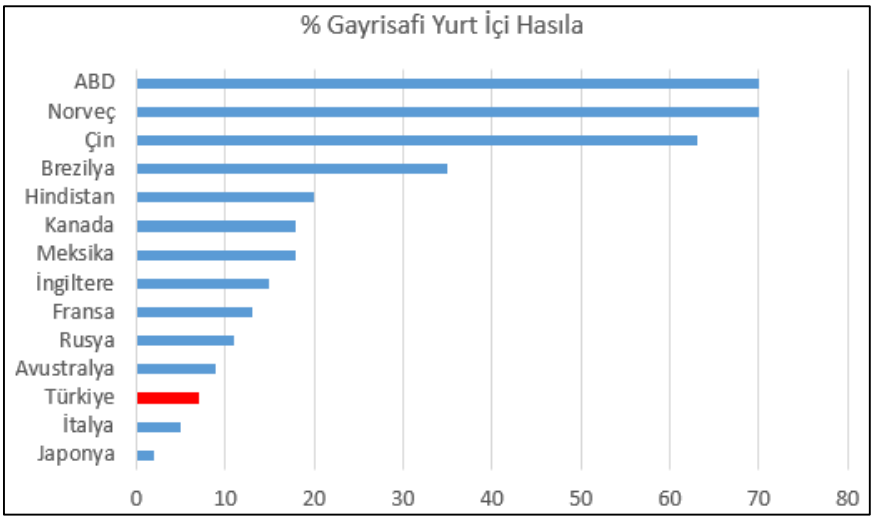
Genelde sıralamada ilk beşte yer alan Türkiye'nin, siber saldırılardan çok fazla etkilendiği söylenebilir.

Dünya genelinde duyulmuş zararlı yazılımlar ve sebep olduğu zararlar ise siber güvenliğin önemini ifade eden bir başka konudur. Bu konuda örnekler aşağıda şekilde verilebilir (Ünver ve Canbay, 2010).

- "I Love You" adlı virüsün dünya çapında yaklaşık 45 milyon bilgisayara bulaştığını ve yaklaşık 10 milyar USD'lik zarara,
- "Nimda" kurtçuğunun dünya çapında yaklaşık 3 milyar USD'lik, "Love Bug"ın ise 10 milyar USD'lik zarara,
- "MyDoom" adlı truva atının 4,8 milyar USD civarında zarara sebep olmuştur.
- "Sapphire/Slammer" solucanının 2003'te internete bağlı bilgisayarların %90'ına 10 dakika içinde bulaşmıştır.
- 2008 yılında geliştirilen siber casusluk amaçlı kullanılan "Regin Virüsü" 2014 yılında fark edilmiş ve Rusya, Sudi Arabistan, İrlanda, Belçika, İran gibi pek çok ülkeye yayılmıştır.

Siber saldırıların sonucunda ortaya çıkan mali boyutlara bakıldığında, sadece Türkiye'nin değil, bu suç türünün tüm dünyanın en önemli sorunlarından biri olduğu görülmektedir. Şekil 6'da siber suçların ülkelere maliyeti, her ülkenin gayrisafi yurt içi hasılalarına göre oranı verilmektedir.

Şekil - 5: Siber Suçların Ülkelere Maliyeti (Her Ülkenin Gayrisafi Yurt İçi Hasılasına Göre) (Havelsan, 2017)



Şekil 6 incelendiğinde Almanya, ABD, Çin gibi gelişmiş ülkelere siber suçların maliyetinin çok yüksek olduğu görülmekle beraber, Türkiye'nin her ne kadar alt sıralarda olduğu görülse de, %7'lik oranın hiç de göz ardı edilmeyecek bir rakam olduğu açıktır. Çünkü TÜİK verilerine göre, 2018 yılı ilk çeyreğinde gayrisafi yurtiçi hasıla (GSYH) 792 milyar 691 milyon TL olarak açıklanmıştır (TÜİK, 2018). Bu miktarın %7'sine bakıldığında, siber suçların ülkemize maliyetinin 55 milyar 488 milyon TL olduğu ortaya çıkmaktadır. Küresel bağlamda düşünüldüğünde ise 10 milyar dolarlık bir zarar olduğu ifade edilebilir. Siber suçların günümüzde geldiği nokta, bu büyük rakamlarla daha net anlaşılmaktadır.

Yapılan araştırmalar bilişim suçlarının faillerinin genel olarak; işten çıkarılma veya işteki çeşitli hoşnutsuzluklar, politik amaç gütmeleri, sadece eğlenmek istemeleri, cinsel tatmin isteği, ciddi psikolojik rahatsızlıklar, öfke ve intikam alma duygusu (vandalizm, sabotajlar, yağma gibi), mali zorluklar ve para sağlama isteği, bilgisayarı aşabilme duygusu (operatör makine ilişkisinden kaynaklanan sorunlar da dahil) sebepleriyle suç işlediklerini göstermektedir (Alaca, 2008). Bu ifadeye bakıldığında, siber suçların sadece mali boyutlar açısından değerlendirmek eksik olur. Siber suç işleyenlerin sebepleri incelendiğinde, mali boyutun yanında, insanları psikolojik açıdan yıpratmak da olduğu görülmektedir.

Bu ana kadar verilen bilgiler ve istatistikler ışığında internetin çok uzun zaman geçirildiği, sağladığı kolaylıklar ile önem taşıyan ya da mahrem bilgilerin bulunduğu, hayatın her alanında yeri geldiğinde zorunlu olarak kullanıldığı bir ortam veya kavram olduğu ifade edilebilir. Hayatın merkezinde yer alan bu ortamdan gelebilecek tehlikelerin ne denli büyük boyutlu olabileceğini her yıl düzenlenen raporlar, yapılan istatistikler, akademik çevreler ispatlayıp ortaya koymuşken, bu tehlikelerden korunma yolu da denilebilecek siber güvenlik konusu önem kazanmaktadır.

Birleşmiş Milletlerin (BM) haberleşme, bilgi ve iletişim teknolojileri alanındaki yetkili organı olan Dünya Telekomünikasyon Birliği (ITU) tarafından siber güvenlik, "siber uzayda organizasyon ve kullanıcıların varlıklarını korumak

amacıyla kullanılan araçlar, politikalar, güvenlik kavram ve önlemleri, kurallar, risk yönetimi yaklaşımları, eylemler, eğitimler, uygulamalar ve teknolojilerin bütünü" olarak tanımlanmıştır. Siber uzayda organizasyon ve kullanıcıların varlıklarını, bireyler, bilgi işlem donanımları, altyapılar, uygulamalar, hizmetler, haberleşme sistemleri ve siber uzayda iletilen ve/veya saklanan bilgiler oluşturmaktadır (ITU, 2008).

Öğrencilerin bilgi güvenliği farkındalığı üzerine yapılan bir araştırmaya göre, araştırmaya katılan öğrencilerin bilgi ve bilgisayar güvenliği konusundaki farkındalık düzeyleri konusunda ulaşılan sonuçlar öğrencilerin güvenli şifre kullanımı, çevrimiçi güvenli iletişim, kötücül yazılım denetlemesi yapma, belge koruma, kişisel bilgisayar güvenliği, güvenlik duvarı ve filtreleme yazılımları kullanımı, çevrimiçi arkadaş edinme ve internetin güvenli bir alan olup olmadığı konularındaki farkındalık düzeylerinin çok düşük olduğunu göstermektedir. Öğrencilerin, interneti sadece bir eğlence aracı olarak görmedikleri, izinsiz müzik ve program edinmenin yanlış olduğu, başkalarına ait alanlarda izinsiz işlem yapmanın sakıncalı olduğu, orijinal olmayan yazılım kullanımının sakıncalı olduğu, dosya paylaşım sitelerinin kullanımının etik olmadığı, sohbet odaları ve tanımadığı kişilerle iletişim kurmanın güvenli olmadığı, çevrim içi uygunsuz ortamlara girmenin sakıncalı olduğu konularında orta düzeyde bir farkındalık düzeyine sahip oldukları saptanmıştır (Tekerek ve Tekerek, 2013).

Farklı meslek gruplarına uygulanan siber güvenlik farkındalık ölçeğinde ise 501 katılımcıdan 157'si öğretmen olarak belirlenmiş ve sonuçlar incelendiğinde öğretmenlerin farkındalık düzeylerinin diğer meslek gruplarından farklı çıkmadığı belirlenmiştir (Mart, 2012).

Elâzığ Fırat Üniversitesi Teknik Eğitim Fakültesi Bilgisayar Eğitimi Bölümü ile Teknoloji Fakültesi Yazılım Mühendisliği bölümünde ve Meslek Liseleri Bilişim Teknolojileri Bölümlerinde yapılan bir araştırmada, ortaöğretim bilişim bölümü öğrencilerinin bilişim suçları hakkında bilgi sahibi olma oranları %45 iken, üniversitede ise %59,3 olarak bulunmuştur (Özdemir vd., 2013).

Örnek verilen çalışmalarda öğretmenlerin ve öğrencilerin farkındalık düzeylerinin orta seviyede olduğu görülmektedir. Bu denli önemli olan bir konuda ortaya çıkan seviyenin yeterli olmadığı görülmektedir. Bu açıdan geleceğimizin teminatı olan gençler içerisinde bilişim teknolojilerini en çok kullanan ve bu teknolojileri geliştirecek olan öğrenciler olması sebebiyle orta öğretim kurumlarında bilişim teknolojileri alanındaki öğrencilerin siber güvenlik konusundaki farkındalıklarını belirlemek önemli görülmüş ve araştırılmıştır.

1.2. Amaç

Bu araştırmanın amacı meslek liselerinde bilişim teknolojileri alanındaki öğrencilerin kişisel siber güvenliğe yönelik bilgi düzeylerinin belirlenmesidir. Bu amaca yönelik olarak aşağıdaki alt amaçlara yanıtlar aranmıştır.

1.2.1. Alt Amaçlar

1. Mesleki ve Teknik Anadolu Liseleri Bilişim Teknolojileri alanındaki öğrencilerin kişisel siber güvenliğe yönelik farkındalık düzeyleri nedir?

2. Mesleki ve Teknik Anadolu Liseleri Bilişim Teknolojileri alanındaki öğrencilerin kişisel siber güvenliğe yönelik farkındalık düzeyleri

   a. Siber güvenlik konusunda eğitim alma durumları,

   b. Sınıf düzeyleri (10 ve 12. sınıf),

   c. Siber güvenlik konusunda mağduriyet yaşama durumları

   d. Siber güvenlik konusundaki bilgi yeterlik düzeyi (az, orta, yüksek) değişkenlerine göre farklılık göstermekte midir?

1.3. Önem

Yaşadığımız çağa baktığımızda, durmaksızın gelişen teknoloji ile birlikte dünya üzerindeki hemen hemen tüm insanların hayatlarının dijital platforma aktarıldığını görmekteyiz. Bu yönü ile özellikle teknoloji ile bağı olanlara ek olarak, bu konuda çok yoğun bağı olmayan insanların da bir şekilde kişisel bilgileri dijital

dünyada bulunabilmektedir. Buna devlet kanalıyla dijital platforma aktarılan bilgiler, sosyal medya aracılığı ile paylaşılan resimler örnek olarak verilebilir. Dolayısıyla birebir dijital dünya ile irtibata geçmeyen insanlar, dolaylı yoldan kendilerini o ortamlarda görebilmektedirler. Bu bağlamda hızla yayılan ve halen genişlemeye devam eden bu dünyanın güvenliğinin de tüm insanlığı ilgilendirdiğini göz ardı edilemez. Maslow'un ihtiyaçlar hiyerarşisine göre en temel ihtiyaçlardan ikincisi olan güvenlik ihtiyacının, günümüzde siber güvenliği de kapsadığını söylemek mümkündür.

Artık günümüzde gelişen teknoloji ile birlikte devletlerin de en kritik organlarını dijital mecralara taşımaları, siber tehditlerle karşı karşıya kalmalarına zemin hazırlamıştır. Devletlerin bile zaman zaman siber mağduriyeti yaşadığı çağımızda, bireylerin bu konuda ne kadar tehlikede olduğu ortadadır. Dolayısıyla dijital platformu az veya çok farklı düzeyde kullanan her insanın kişisel siber güvenliği konusunda bilinçlenmesi bir zorunluluktur. Günümüzde siber mağduriyet yaşayan insanları yakın çevremizde olsun haber kanallarında olsun sık sık görebilmekteyiz. Yaşanan mağduriyetlerin sosyolojik, psikolojik boyutları görüldükçe ne kadar tehditkâr oldukları da anlaşılabilir. Araştırmanın evrenini oluşturan öğrencilerin seçilmesinin ise iki temel sebebi bulunmaktadır. Birincisi, öğrenciler arasında bilişim teknolojilerini en çok kullanan bireyler olmaları, siber tehditlerle karşı karşıya kalma olasılıklarını diğer öğrencilere oranla daha çok arttırmaktadır. İkincisi ise meslek icabı bu teknolojileri geliştirecek bireyler olmaları onları diğer insanlardan ayırmaktadır. Siber güvenlik yeterlilik düzeyleri ne kadar yüksek olursa geliştirecekleri teknolojiler de siber tehditlere karşı o kadar dirençli olacaktır. Bu teknolojileri kullanacak bireyleri de siber tehlikelerden koruyabilecektir. Bu faktörlerden dolayı Meslek liselerinin Bilişim Teknolojileri alanındaki öğrencilerin siber güvenlik konusundaki yeterlilik düzeyleri araştırmaya değer görülmüştür.

1.4. Sınırlılıklar

Mesleki ve Teknik Anadolu liselerinde bilişim teknolojileri alanındaki öğrencilerin aldıkları eğitimlerin kişisel siber güvenliklerine yansıması bağlamında değerlendirildiği bu araştırma;

- 2017-2018 öğretim yılı Konya Merkez İlçelerinde Bilişim Teknolojileri alanında öğrencileri bulunan Mesleki ve Teknik Anadolu Liseleri ile
- Bilişim Teknolojileri alanında eğitim gören 10. ve 12.sınıf öğrenciler ile sınırlıdır.

1.5. Tanımlar

Bilişim: İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimidir.

İnternet: Bilgisayar ağlarının birbirine bağlanması sonucu ortaya çıkan, herhangi bir sınırlaması ve yöneticisi olmayan uluslararası bilgi iletişim ağıdır.

Bilişim Teknolojileri: Dünyadaki tüm cihazların birbirine bağlandığı siber ortam, iletişim amacıyla kullanılan tüm aygıtlar, bu alanda hizmet veren bireyler, verilerin işlenmesi, aktarılması, depolanması için kullanılan geleneksel anlamda donanım ve yazılım gibi birçok faktöre sahip olan kavramdır.

Siber Güvenlik: Verilere, bilgisayarlara veya mobil cihazlara yapılan herhangi bir saldırıyı önlemek veya azaltmak için alınan önlemlerin adıdır. Siber güvenlik sadece gizliliği ve mahremiyeti korumakla kalmaz, hayati önem taşıyan verilerin kalitesi ve güvenliği için kullanılabilirliğini ve bütünlüğünü içerir.

Siber Suç: Verilerin işlenmesi, dağıtılması, depolanması için kullanılan bir sistemde, izinsiz, yasadışı olarak gerçekleştirilen her türlü eyleme verilen addır.

BÖLÜM 2

KURAMSAL ÇERÇEVE

Bu bölümde araştırmanın anlaşılmasına ışık tutacak kuramsal çerçeveye yer verilmiştir.

2.1. Bilişim

Bilgisayar teknolojisindeki gelişim sonrasında insanların bilgiye ulaşma yöntemleri ve sürelerinde çok ciddi değişimler meydana gelmiştir. Bilginin durağan ve sabit yapısı ortadan kalkmış, hiç durmaksızın gelişen ve değişen bir yapıya bürünmüştür. Bilgisayar teknolojisine paralel olarak iletişim teknolojisi de adeta bir evrim geçirmiş ve zaman içinde bugün ki halini almıştır. Tarihsel açıdan yakın ve kısa bir zamanda gerçekleşen bu değişim "Bilişim" kavramını da hayatımıza entegre etmiştir. Türk Dil Kurumu (TDK) bilişim kavramını, "insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi" olarak açıklamaktadır (TDK, 2019).

Bir sistemin çalışmasına destek olmak amacıyla verileri kaydeden, analiz eden, gerekli birimlere gönderen, hesaplayan ve interaktif olarak hizmet veren donanım ve yazılımlara bilişim denir (Çakır ve Eryılmaz, 2014).

Verinin, mesajın ve ilgili tüm kavramların yönlendirilmesi, gruplandırılması, kaydedilmesi, analiz edilmesi ve dağıtılması için kullanılan metotlardır. Ayrıca veriyi kaynağından alıp istenilen hedeflere gönderen, insanların veriyi kullandıkları zamanda ve mekanda yardımcı ya da ana unsur olarak görev alan teknolojiler, faaliyetler, sistemler, süreçlerdir (Aydın, 1992).

Bireylerin iş alanında sosyal alanda dolayısıyla her alanda kullandıkları bilginin, bilgisayar gibi teknolojik cihazlar vasıtasıyla belli kurallar çerçevesinde düzenlenmesi, algoritma adı verilen problem çözme adımlarının oluşturulması,

verinin depolanması, ihtiyaç duyulduğunda tekrar kullanılabilmesi bilimine bilişim denir (Dülger, 2004).

2.2. Bilişim Teknolojileri

Bilişim Teknolojileri (BT), bilgisayar alanındaki ilerlemeler neticesinde ortaya çıkmış, bilgileri depolamak, aktarmak ve analiz etmek amacıyla kullanılan donanım ve yazılım araçlarını kapsayan bir kavramdır. Bilgisayar ve teknolojik diğer cihazların gelişimiyle doğru orantılı bir şekilde ilerleyen sistemler, bilgilerin eğitim amacıyla karşı tarafa aktarılması sürecinde, bu sürecin oluşturulması, uygulanması ve değerlendirilmesi aşamalarında eğitimcilere kolaylıklar sağlamaktadır (Gülbahar ve Kalelioğlu, 2018).

Günümüzde BT, sadece bilgisayar donanımlarının bir araya getirilmesi ya da yazılımların geliştirilmesinden çok daha kapsamlı bir alandır. Güncel bir anlayışla BT, dünyadaki tüm cihazların birbirine bağlandığı siber ortam, iletişim amacıyla kullanılan tüm aygıtlar, bu alanda hizmet veren bireyler, geleneksel anlamda donanım ve yazılım gibi birçok faktöre sahiptir (Çakır ve Eryılmaz, 2014).

Verilerin elde edilmesinde, analiz edilmesinde, kaydedilmesinde, istenilen ortamlara aktarılmasında ve tüm bireylerin faydalanması için kullanılan her türlü teknolojiler, fiziksel cihazlar ya da düşünce sistemleri bilişim teknolojileri kapsamına girmektedir (Yüzer ve Okur, 2015).

Bilişim teknolojileri, bilgiyi oluşturmak, depolamak, değiştirmek ve bilgiden yararlanmak için kullanılan teknolojinin bütün formlarını (iş verileri, ses, konuşmalar, fotoğraflar, hareketli resimler, multimedya, sunumlar vb.) içine alan bir terimdir. Aynı zamanda iletişim ve bilgisayar ifadelerini içeren uygun bir kelime, genellikle bilgi devrimi olarak adlandırılan bir teknolojidir (Thing, 2001).

2.3. İnternet

İnternet ilk olarak 1960'lı yıllarda Amerika Birleşik Devletleri'nde askerî amaçlı bir proje ile ortaya çıkmıştır. Günümüzde İnternetin temelini oluşturan bu

projedeki ağa zamanla yeni bilgisayarların eklenmesiyle ağ üzerinden iletişim giderek arttırılmış ve çok sayıda kullanıcının yararlandığı elektronik mektup, tartışma listeleri, forumlar, dosya transfer hizmetleri gibi yeni kullanım alanları ortaya çıkmıştır**.** Siviller arasındaki İnternet ise ilk olarak Mart 1989'da, yüksek enerji fiziği konusunda dünyanın çeşitli yerlerinde araştırmalar yapan kişiler arasında, etkin ve kolay bir haberleşme platformu olarak kullanılması amacıyla Tim Berners Lee tarafından Avrupa Parçacık Fiziği laboratuvarlarında geliştirilmeye, 1991 yılında ise etkin bir şekilde kullanılmaya başlanmıştır.

İngilizce olan inter kelimesinin anlamı "arasında, birbiriyle" şeklinde çevrilmektedir. Net kelimesi ise "ağ" anlamına gelmekte olup internetin kelime anlamı ağlar arasında olarak düşünülebilir. Özellikleri arasında etkileşimli olması ön plana çıkmaktadır. Bir başka ifadeyle, kullanıcının isteklerine göre bilgi akışı şekillenir (Vural, 2006).

İnternet kavramı, TDK 'da genel ağ olarak belirtilmiş ve bilgisayar ağlarının birbirine bağlanması sonucu ortaya çıkan, herhangi bir sınırlaması ve yöneticisi olmayan uluslararası bilgi iletişim ağı olarak açıklanmıştır (TDK, 2019).

İnternet, dünyaya dağılmış binlerce küçük bölgesel ağdan oluşan sistemdir. Birçok bilgisayarı ve ağa bağlı cihazları birbirine bağlamanın bir yolu, kullanıcılarının yazıcı ve belge gibi kaynakları, genellikle sunucu adı verilen merkezi bir bilgisayar aracılığıyla paylaşabilmelerini sağlamanın bir yoludur (Rigdon, 2016).

Günümüzde çok büyük bir kapsama ulaşan internet, teknoloji ve iletişim alanındaki etkileriyle çağımızın en önemli gelişmesidir. Bilginin kolay ulaşılabilir ve dağıtılabilir olması sebebiyle dünya tarihinin en fazla bilgi birikimi bu süreçte meydana gelmiştir. İnternet aynı zamanda insanları, şirketleri, toplumu ve dolayısıyla tüm uygarlığı değiştirme özelliğine de sahiptir. Bu özelliğiyle de internetin dönüşüm gücünden bahsedilebilir (Nakilcioğlu, 2007).

2.4. Siber Güvenlik

BT'deki ağ yapısı, insanların tüm dünyayla iletişime geçmesine olanak sağlamaktadır. Bu kadar çok kişiye ulaşabilme potansiyeli art niyetli insanları da bu mecraya çekmektedir. Kullanılan teknoloji, gereken güvenlik özellikleriyle donatılmamışsa, dijital ortamda saklanan verilerin ele geçirilmesi ya da yok edilmesi ihtimali bulunmaktadır (Adalı, 2001).

Siber güvenlik, siber-uzay ve aktif siber-uzay sistemlerde fiilen haksızlığa uğranmasına neden olaylardan korunmak için kullanılan kaynakların, işlemlerin ve yapıların listesinden oluşan bir organizasyon ve koleksiyondur (Craigen vd., 2014).

Siber güvenlik, verilere, bilgisayarlara veya mobil cihazlara yapılan herhangi bir saldırıyı önlemek veya azaltmak için alınan önlemlerin adıdır. Siber güvenlik sadece gizliliği ve mahremiyeti korumakla kalmaz, hayati önem taşıyan verilerin kalitesi ve güvenliği için kullanılabilirliğini ve bütünlüğünü içerir (An Introduction to Cyber Security, 2017).

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı tarafından hazırlanan 2016-2019 Ulusal Siber Güvenlik Stratejisi'nde siber güvenlik kavramı, bilişim teknolojilerinin oluşturduğu sanal ortamı kötü niyetli insanlardan korunmasını, bu ortamlarda yer alan verilerin gizlilik, bütünlük ve erişilebilirliğinin sağlanmasını, bu kötü niyetli insanların davranışlarının ortaya çıkarılmasını, saldırıların belirlenmesini, bu belirlenen saldırılara karşı alınacak önlemlerin hayata geçirilmesini, son olarak saldırıdan önceki güvenli haline tekrar getirilmesini kapsamaktadır. Sanal ortam ismiyle anılan bilişim teknolojilerinin oluşturduğu yapıya siber uzay ismi de verilmektedir. Aynı raporda siber uzay ile ilgili dünyadaki tüm bilişim aygıtlarının ve bağlantı kurabilmeleri için oluşturulan ağların meydana getirdiği dijital ortam ifadesi yer almaktadır (USGS, 2016).

Bilişim güvenliği ve bilgi güvenliği olarak da adlandırılan siber güvenlik kavramı, Canbek ve Sağıroğlu (2006) tarafından dijital ortamlarda bilgilerin

depolanması, aktarılması ve analiz edilmesi süreçlerinde verilerin yapısı bozulmadan, yasadışı erişimlerden korunarak, güvenli bir ortamda yer alması için atılan adımlar olarak açıklanmıştır.

Siber güvenlik, dijital platformlarda bireylerin, şirketlerin ya da kurumların verilerini herhangi bir şekilde gerçekleşebilecek saldırılara karşı önlem almak için kullanılan programlar, aygıtlar, güvenlik prosedürleri, yönergeler, faaliyetler, eğitimler ve bu amaçla kullanılabilecek tüm teknolojilerin bütününe verilen addır (Topaloğlu, 2016).

2.5. Siber Güvenlik Unsurları

Literatür incelendiğinde siber güvenliğin sağlanması için, genel olarak teknolojik yöntemler, kişisel önlemler, eğitim ve farkındalık olmak üzere 3 temel unsur ön plana çıkmaktadır. Bu başlık altında, belirtilen unsurların açıklamaları ve alt boyutları bu konuda yapılan çalışmalar çerçevesinde aktarılmaktadır.

2.5.1. Teknolojik Yöntemler

Yazılım geliştiriciler tarafından ortaya çıkarılan uygulamalar ile siber güvenliğin sağlanması amaçlanmaktadır. Bu uygulamalar da önleme ve saldırı tespit yazılımları olarak isimlendirilmektedir. Literatür incelendiğinde aşağıdaki yazılımların siber güvenliği sağlamak için kullanıldıkları görülmektedir (Gökmen, 2014; Şahinaslan vd., 2009; Özüdoğru, 2011; Daş vd., 2012; Çeliktaş, 2016; Ghosh ve Turrini, 2010; Saini vd., 2012).

2.5.1.1. Kriptografi

Önemli görülen verilerin belirli metotlarla şifrelenerek izinsiz erişim gerçekleştiğinde anlaşılmasını engelleyecek biçimde kodlanması ve yalnızca alıcı tarafından kodlama çözülerek okunabilecek formata gelmesi için geliştirilen teknolojiye verilen addır. Şifreleme yöntemleri çok uzun bir geçmişe dayanmaktadır. Her ne kadar gelişen teknolojiyle birlikte şifreleme yöntemleri de gelişmiş olsa da art niyetli insanlar için de saldırı yöntemleri gelişmiştir. Gizliliği önemli olduğu düşünülen bilgilerin en güncel ve daha önce güvenirliği denenmiş şifreleme

yöntemleri ile saklanması elzemdir. Saldırganların da mevcut şifreleme algoritmalarını kırabilmek amacıyla çalıştıkları bilinmektedir. Dolayısıyla gelişen teknolojiyle bazı algoritmaların çok kısa sürede kırıldığı görülmektedir. Bu nedenle en güncel ve gelişmiş algoritmalar tercih edilmeli ve belli periyotlarla kontrol edilmelidir (Özbilgin ve Özlü, 2010).

Dijital platformlarda yer alan verilerin güvenle saklanması, taşınması ya da işlenmesi için kriptografik yöntemler kullanılmaktadır. Çağımızın hızla gelişen ve büyüyen bir kavramı olan internetle birlikte, bu ortamlardaki güvenlik sıkıntıları da aynı oranda büyüdüğü bilinmektedir. Bahsedilen güvenlik sorunlarının engellenebilmesi amacıyla Kriptografi teknolojileri kullanılabilecek yöntemler olarak karşımıza çıkmaktadır. Bu alanda yapılan uygulamaların güncel bir şekilde araştırılması ve kullanılan teknolojilere uygulanabilmesi gerekmektedir (Akleylek vd., 2011).

2.5.1.2. Güvenlik Duvarı (Firewall)

Güvenlik duvarları, ağlara güvenlik açısından çeşitli hizmetler sunar. Güvenilir ağ adresleri sağlarlar ve belirtilen güvenlik politikasına uymayan trafiği filtrelerler (Dubrawsky, 2003).

Firmaların ya da bireylerin kullandıkları bilişim teknolojileriyle ağa bağlandıklarında, ağdaki diğer cihazlardan veya internetten gelebilecek tehlikelerden korunmasını sağlayacak teknolojidir. Bilişim teknolojisiyle ağdaki diğer cihazlar arasında bir köprü görevi yapan, kullanıcı internete bağlandığında oradan gelebilecek tehlikeleri karşılayan, bertaraf eden sistemlerdir. Dışardan gelen verilerin ilk karşılandığı ara birimdir. Aynı zamanda internet protokolleriyle uyumlu olarak çalışır. Güvenlik duvarları gelen tehlikelere karşı korumakla birlikte, internette kullanılan protokolleri de uygulayarak doğru yöntemlerin kullanılması amacıyla da kullanılır. Güvenlik duvarları standart prosedürler uygulaması için çalışabildiği gibi, grafiksel ara yüzü kullanılarak istenildiği ayarlar ile de yapılandırılabilir (Karaaslan vd., 2004).

2.5.1.3. Yedekleme (Backup)

Dijital ortamdaki önemli olduğu düşünülen verilerin bir saldırı, arıza ya da kaza sonucu kaybedilmesini engellemek amacıyla belli aralıklarla harici bellek aygıtlarına (flash bellek, taşınabilir sabit disk, CD, DVD vb.) kaydedilerek saklanması teknolojisidir. Düzenli yedekleme yapılan bir bilişim sisteminde herhangi bir sebeple meydana gelebilecek veri kaybı hiçbir sorun teşkil etmeyecektir. Çünkü harici bir aygıta yedeklenen veriler halen kullanılabilir durumda kalacaktır.

2.5.1.4. Antivirüs Yazılımları

Ağdan ya da harici bir aygıttan (flash bellek, harici sabit disk, DVD vb.) gelebilecek kötücül yazılımlardan (virüs, Truva atı, solucan vb.) bilişim sistemini koruyan yazılımlardır. Antivirüs programlarının kurulmasının yanında, aynı zamanda güncel tutulması da bir o kadar önemlidir. Sürekli gelişen bilişim dünyasında, zararlı yazılımlar da gelişmekte ve değişmektedir. Yeni türeyen kötücül yazılımların da antivirüs programı tarafından algılanıp engellenebilmesi için o yazılımın programa tanıtılması gerekmektedir. Bu da antivirüs programlarının sürekli güncellenmesi ile sağlanabilir. Çünkü antivirüs şirketleri sürekli araştırma geliştirme çalışmalarına devam etmekte ve veritabanlarına yeni kötücül yazılımları dahil etmektedirler. Güncelleme işlemi de bilgisayardaki antivirüs programının merkez veritabanına bağlanarak yeni eklenen verileri alması ile gerçekleşir. Böylece son geliştirilen kötücül yazılımları da tanıyıp engelleyebilir.

Sunucu olmayan bilgisayarlarda siber tehditlerden korunmak için tercih edilen teknolojilerin en popüler olanı antivirüs programlarıdır. Bilgisayar ya da farklı bir bilişim cihazına yüklenen antivirüs programları, sistemde fark edilen zararlı yazılımları etkisiz hale getirmek amacıyla kullanılır (Arıkan ve Benzer, 2018).

2.5.1.5. IPS/IDS Teknolojileri

Saldırı Tespit Sistemleri (IDS), cihazların bağlandığı ağda ve cihazın dijital ortamında oluşan veri akışını takip ederek tehlikeli yazılımları tespit ederek kullanıcıya mesaj, eposta gibi seçilen bir iletişim yöntemiyle bilgi veren uyarı sistemleridir. Bununla birlikte ağ cihazlarına ya da güvenlik duvarına istenilen

kuralları yazmak suretiyle saldırıları engellemeye çalışır. Saldırı Engelleme Sistemleri(IPS) ise, cihazların bağlandığı ağda ve cihazın dijital ortamında oluşan veri akışını takip ederek tehlikeli yazılımları tespit eden ve saldırının geldiği ya da istenmeyen ağ trafiğini engelleyen sistemlerdir. IPS sistemlerinin arka planında saldırı tespit yazılımları olduğuna dikkat edilmelidir. Dolayısıyla IDS'nin bir çeşidi olduğu söylenebilir (Karaarslan, 2005).

2.5.1.6. Anti-spam Yazılımları

Anti-spam yazılımları, kontrol dışı olarak adlandırılan mailler aracılığıyla gelen tehlikelerden korumak ve spam ile yoğunlaştırılmak istenen veri trafiğini düzenlemek amacıyla önleyici adımlar atan sistemlerdir (Doğan vd., 2016).

Siber uzaydaki art niyetli kişilerce gönderilmek istenen spam postaları engellemek üzere geliştirilmiş olan anti-spam yazılımlar, bu saldırganların karşısındaki engellerden biridir. Bu tür yazılımlar bazı özel algoritmalar yardımıyla gelen postaları filtrelerler ve spam olduğunu tespit ettikleri postaların kullanıcıya ulaşmasını önleyebilirler (Alataş, 2007).

2.5.1.7. İçerik Filtreleme Yazılımları

Şiddete yönlendiren ifadeler ve görseller, toplumda kin duygusu oluşturacak paylaşımlar, cinsel içerikli görseller kullanıcılar için negatif duygular oluşturabilmektedir (Çubukcu ve Bayzan, 2013). İçerik filtreleme yazılımları da bu tür zararlı içerikleri tespit ederek engelleyen yazılımlardır. Telekomünikasyon İletişim Başkanlığı tarafından yönetilen servis sağlayıcılar ile yapılan çalışmalar neticesinde ortaya çıkan "Güvenli İnternet Hizmeti" Bilgi Teknolojileri ve İletişim Kurulu aracılığıyla yürütülmektedir. Bu proje ile Türkiye genelinde özellikle çocukların zararlı içeriklere maruz kalması engellenmeye çalışılmaktadır (Çubukcu ve Bayzan, 2013).

2.5.1.8. Kayıt Takip Yazılımları

Bilişim sistemine giriş yapan kullanıcıların oturum bilgilerini (kullanıcı adı, şifre vb.), giriş yaptıkları bilgisayarın bilgilerini (IP, MAC adresi vb.) ve zaman

bilgisini kaydeden sistemlerdir. Sistemde ya da verilerde kullanıcılardan kaynaklanan bir sorun meydana geldiğinde, tutulan bu kayıtlardan kimin, ne zaman ve hangi bilgisayardan giriş yaptığı tespit edilmesi prensibiyle çalışır.

2.5.1.9. Özel Sanal Ağlar (VPN)

Özellikle alışveriş merkezleri gibi toplu kullanım alanlarında internet hizmeti vermek amacıyla oluşturulan ağlar üzerinde daha güvenli iletişim kurabilmek amacıyla kurulan ağlara özel sanal ağlar (VPN) adı verilmektedir. İletilen bilgilerin internet ortamında korunabilmesi için şifreleme yöntemleri kullanılmaktadır. Özel sanal ağı kullanan kullanıcıların artması halinde güvenliği sağlayabilmek için daha etkili prosedürler kullanmak gerekmektedir (Karaaslan vd., 2004).

2.5.1.10. Bal Küpü

Bal küpleri ile ayıların tuzağa gelmesi sağlanmaktaydı. Günümüz bilişim dünyasında ise bal küpleri, saldırganları üzerine çekmek için kullanılmaktadırlar. Bal küpü sistemleri zararlı aktiviteyi ya da saldırganı durdurmakta aktif görev almazlar. Bal küpleri, izinsiz yapılmış girişlerin veya zararlı aktivitelerin tespitinde kullanılmasına ek olarak asıl amaçları saldırganın veya zararlı aktivitenin kullanmış olduğu metot ve araçlar hakkında bilgi edinmektir (Song vd., 2012).

2.5.2. Kişisel Önlemler

Her bireyin siber uzay adı verilen bilişim teknolojilerinin yer aldığı sistemden gelebilecek tehlikelere karşı alabileceği önlemler vardır. Bu önlemler neticesinde birçok zararlı yazılım ya da art niyetli kişilerin saldırılarından korunmak mümkün hale gelmektedir. Çok basit ya da zaman kaybı olarak görülebilen önlemler kimi zaman ciddi zararlara uğramaktan bireyleri koruyabilmektedir. Aşağıdaki maddelerde literatür incelenerek derlenmiş önlemler yer almaktadır.

(Gökmen, 2014; Karakoç, 2011; Çetin, 2014; Yavanoğlu vd., 2012) tarafından yapılan çalışmalarda aşağıdaki önlemlerden bahsedilmektedir.

- Flash disk, harici disk gibi veri depolama aygıtlarının her kullanımın ardından virüs programları ile taranması gerekmektedir.

- Şifrelerin güvenlik seviyelerini arttırmak amacıyla harf, rakam, özel karakterlerin kombinasyonlarıyla oluşturulmasına özen gösterilmelidir.
- Şifrelerin unutulması halinde kullanılan yöntemlerden biri olan hatırlatma sorularının başkaları tarafından kolay bir şekilde bilinemeyecek şekilde oluşturulmasına dikkat edilmelidir.
- Dijital ortamlarda kullandığımız tüm şifrelerin birbirinden farklı olması güvenlik için önemlidir.
- Mail hesaplarımıza gelebilecek kimlik doğrulama maillerine dikkat edilmeli, sahte olma ihtimali göz ardı edilmemelidir. Tehlikeli görülen mailler hiç açılmadan silinmelidir.
- Kablosuz ağlara bağlanan kullanıcıların mutlaka son şifreleme yöntemi ile giriş yapması gerekmektedir. Ağ kullanılmadığı durumlarda bağlantının kesilmesine dikkat edilmelidir.
- Sosyal medyada kimlik, adres, telefon gibi kişisel bilgiler paylaşılmamalı; paylaşılan görseller ya da bilgilerin de sadece arkadaşların erişimine izin verecek şekilde düzenlenmesi gerekmektedir.
- Ev dışında kişisel bilgisayar kullanıldığında, başından ayrılmak gerekiyorsa oturum kapatılmalı, özellikle şifre ile korunması sağlanmalıdır.
- Web sitelerini görüntülemek için kullandığımız tarayıcıların sürekli güncel tutulması ve güvenlik ayarlarının yapılandırılması zorunludur. Gezilen sitelerin başında güvenli sertifika olduğunu gösteren “https” ifadesi olmasına dikkat edilmelidir.
- Kullanılan bilgisayarların güncel bir antivirüs programıyla korunması ve mail hesapları için de anti-spam yazılımlarının bulunması, belli periyotlarla bu yazılımların güncellenmesi gerekmektedir.
- Aynı şekilde kullanılan işletim sisteminin de belli aralıklarla güncellenmesi, lisanslı işletim sistemlerinin tercih edilmesi önemlidir.

- İnternette veya başka bir bilgisayarla gerçekleştirilen veri trafiğini kontrol ederek tehlikeli yazılımların sistemimize erişimini engelleyen güvenlik duvarının aktif olmasına özen gösterilmelidir.
- İşletim sistemi özelliklerinde yer alan dosya paylaşımı, uzak masaüstü bağlantısı gibi dışardan erişimi mümkün kılan özelliklerin ihtiyaç dışında kapalı olmasına özen gösterilmelidir.
- Çoğunlukla zararlı yazılım göndermek için tercih edilen web sitelerindeki reklamlara itibar edilmemeli, mail hesabımıza gelen postanın göndericisini tanımıyorsak açmadan silinmelidir.
- Kullanıcıların bir sonraki deneyimlerinde kolaylık ve hız sağlamak amacıyla tarayıcılar belli bilgileri hafızalarında tutarlar. Bunların belli aralıklarla silinmesi, izinsiz erişimle başkalarının eline geçmesine engel olabilmektedir.
- E-ticaret sistemlerinde ya da bankacılık sistemlerinde bilgi girişi yapılırken ekran klavyesi kullanılmalıdır. Tuş kaydedici gibi zararlı yazılımlardan korunmak için önemli bir yöntemdir.
- Web ortamında açılan herhangi bir oturumdan tarayıcı kapatılarak değil güvenli çıkış yöntemiyle çıkılmalıdır.
- Önemli görülen bilgilerin sıkıştırma programları kullanılarak sıkıştırılması ve şifrelenmesi güvenlik açısından önemlidir.
- Sistemde meydana gelebilecek herhangi bir arıza durumunda tüm sistemi kaybetme riskine karşı belli aralıklarla işletim sistemi özelliklerinden biri olan geri yükleme noktası oluşturulmalıdır.
- Normalde indirilmesi yasal olmayan Crack, MP3 gibi dosyaların bulunduğu siteler pek çok tehlikeli yazılımın da merkezi olabilmektedir. Bu tür sitelerdeki linklere, reklamlara itibar edilmemeli, hatta ziyaret edilmemelidir.

- Piyasada pek çok şirket tarafından geliştirilen tarayıcı bulunmaktadır. Güvenlik açısından en gelişmiş olanları tercih edilmeli ve güncellemeleri zamanında yapılmalıdır.

- Çerez adı verilen yöntemle web siteleri kullanıcılardan bilgi toplamaktadır. Art niyetli kişiler de bu tür bilgilere erişmektedir. O nedenle güvenilmeyen siteleri çerez kaydetme istekleri reddedilmeli, tarayıcı ayarlarından da kaydetme seçenekleri iptal edilmelidir.

- Alışveriş merkezleri, internet kafeler gibi ortak ağ kullanılan ortamlarda, şifre gerektiren işlemlerin yapılmaması gerekmektedir.

- Web siteleri ziyaret edilirken pop-up pencere şeklinde karşımıza çıkan evet, hayır, tamam gibi butonlara okumadan tıklanmamalıdır.

- Art niyetli insanlar zararlı yazılımların isimlerini genel olarak kullanılan dosya türlerinden vermektedirler. Örneğin "Ornek.txt.exe" isminde zararlı bir yazılım "Ornek.txt" şeklinde göründüğünden dolayı kullanıcıların dikkatinden kaçabilmektedir. İnternetten, mailden ya da taşınabilir bir bellekten gelebilecek bu tür dosyaların uzantıları kontrol edilmelidir.

- Her türlü saldırı ihtimali akılda tutulmalı ve verilerin zarar görmemesi adına düzenli bir şekilde yedeklenmelidir.

- Teknolojinin gelişmesiyle zararlı yazılımlar da gelişip değişmektedir. Bu tür tehlikelerden korunma yollarını öğrenmek ve sürekli kendimizi geliştirmek için teknik forumlar ziyaret edilmeli, dergiler, ilgili çalışmalar okunmalıdır.

2.5.3. Eğitim ve Farkındalık

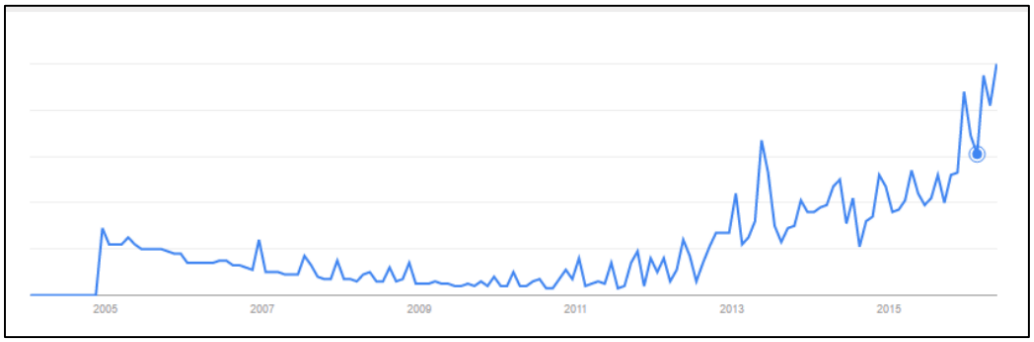
Siber tehditlerden korunmak amacıyla birçok yöntem ve uygulama geliştirilmesine rağmen insanlar her zaman için en kolay hedefler olmaktadır. Çünkü sistemleri koruma teknolojileri gelişse de bu sistemleri insanların kullanıyor olması orada meydana gelebilecek açıkları yok edememektedir. Dolayısıyla insanın zafiyeti ya da art niyeti sistemi saldırılara karşı savunmasız bırakabilmektedir. Bu bağlamda, bireylerin siber güvenlik farkındalıkları ve

eğitimleri en önemli saç ayaklarından biri olarak karşımıza çıkmaktadır. Kullanıcılar bilinçli ya da bilinçsiz olarak kullandıkları sistemleri saldırıların hedefi yapabilmektedir (Emiral, 2004).

Siber tehditlerden korunmanın en iyi yöntemi bu alana çok para harcamak ya da tüm teknolojileri bir arada kullanmaktan öte insanların siber güvenlik konusundaki farkındalıklarını arttırmak ve ihtiyaç duyulan doğru teknolojiyi kullanmaktır. Siber tehlikelerden tamamen korunmak mümkün olmasa da doğru teknolojiyi yerinde ve zamanında kullanmak, ayrıca insana bağlı açıkları kapatabilmek için gerekli siber güvenlik eğitimlerini almalarını sağlamak tehlike seviyesini en aza indirgeyebilir (Şahinaslan vd., 2009).

Topaloğlu (2016) tarafından yapılan çalışmada yer alan Google Trend tarafından paylaşılan grafikte, Türkiye'de siber güvenlik teriminin arama motorlarında indekslenme eğilimi verilmektedir. Grafikten de anlaşıldığı üzere, son yıllarda siber güvenlik farkındalığı gözle görülür bir şekilde artmıştır.

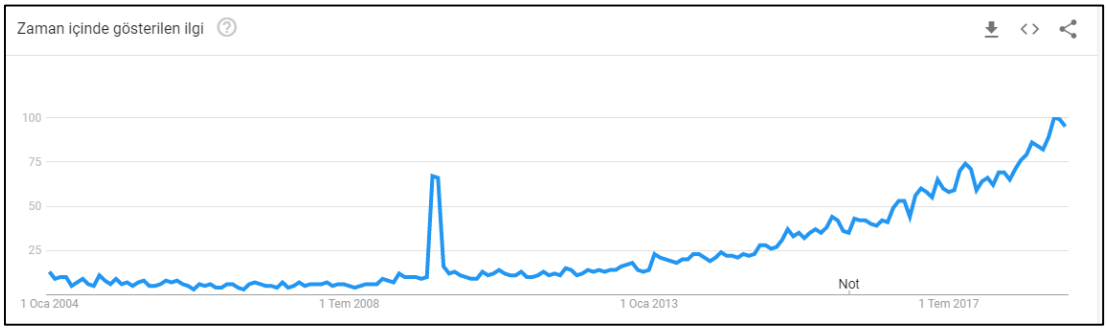
Şekil-6: Türkiye'de Siber Güvenlik Terimi Aramalarının Eğilimi



2.5.3.1. Dünyada Siber Güvenlik Eğitimi

Dünya'daki siber güvenliğe olan ilginin 2004 ile 2016 yılları arasındaki değişimi Google Trend 'den sağlanan eğilim grafiği ile Şekil 8'de gösterilmiştir. Şekil 8'den de anlaşılacağı üzere insanların siber güvenliğe olan ilgisi her geçen yıl artış göstermektedir.

Şekil - 7: Dünyada Siber Güvenliğe Olan İlginin Değişimi (Google Trends, 2019)



Grafikte 2009 yılı ekim ayına denk gelen tepe noktasının ortaya çıkması ABD Başkanı Barack Obama tarafından ekim ayının Ulusal Siber Güvenlik Bilinçlendirme Ayı olarak açıklanması ve dolayısıyla insanlarda meydana gelen farkındalık ile arama motorunda bu konuyu daha çok arama eğilimlerinden kaynaklanmaktadır (Sevri ve Topaloğlu, 2016).

Dünya genelinde siber güvenlik konusunda insanların daha çok bilinçlenmesini sağlamak amacıyla dikkat çekici faaliyetler hayata geçirilmektedir. Görsel içeriklerle zenginleştirilen, çeşitli sloganlarla dikkat çeken uygulamalar hem ABD'de hem de AB ülkelerinde kullanılmaktadır (Ünver, 2012).

Yapılan araştırmalar neticesinde siber güvenli eğitimlerindeki gelişmişlik açısından Amerika, Avrupa, Okyanusya, Asya ve Afrika olarak sıralandığı elde edilmiştir. Gelişmiş ülkelerde bilişim teknolojilerinin de daha çok geliştiği ve kullanıldığı düşünüldüğünde, siber tehditler de bu ülkelerde daha fazla olabilmektedir. Dolayısıyla bu ülkelerin siber güvenlik konusunda yetişmiş bireylere daha çok ihtiyacı olduğu görülmektedir. Bu ihtiyaca bağlı olarak da siber güvenlik eğitim programlarının sayısı doğru orantılı bir şekilde ortaya çıktığı gözlenmiştir. Aşağıdaki tabloda çeşitli kıtalardan bazı ülkelere yer verilmiş ve buralardaki eğitim programlarının sayıları paylaşılmıştır (Orakcı vd., 2016).

Tablo-2: Bazı Ülkelerde Siber Güvenlik Eğitim Programları

Ülkeler	Önlisans	Lisans	Yüksek Lisans	Doktora	Sertifika
USA	13	46	23	3	25
Kanada	-	3	1	-	13
İngiltere	-	23	14	1	-
Almanya	-	-	1	-	-
Hollanda	-	1	1	-	-
İtalya	-	3	-	-	-
İsveç	-	1	-	-	-
Hindistan	-	1	4	-	-
Avusturalya	-	5	6	1	-

Çin ülkedeki yetenekli hackerları ulusal çapta siber güvenliğe ilgi duyan öğrencilerden oluşan yaz ve kış kampları ile bulmakta ve sonrasında milli çıkarlarına uygun şekilde istihdam edebilmek için donanımlı bir eğitim programından geçirmektedir. Dünyada özel şirketlerin de düzenlediği siber güvenlik yarışmaları bulunmaktadır (TÜBİSAD, 2017).

Dünyada bu alanda okutulan dersler ve müfredat, alanın doğası gereği multidisipliner olarak şekillenmiştir. Programlarda bilişim, hukuk, eğitim ve sosyal açıdan birçok ders yer almıştır. Kıta ülkelerinin program sayılarına ek olarak bu programlarda yaygın olarak okutulan dersler de incelenmiştir. Dersler alanlarına göre gruplandırılarak aşağıdaki şekliyle sunulmuştur (Orakcı vd., 2016).

- Adli bilişim ve temelleri (Adli gereksinimler ve analizler, Adli mülakat)
- Bilişim suçları analizi ve tespiti (Siber suçlar, Suç araştırmaları, Saldırı tespiti ve analizi, Hacker, pedofil ve internet sapıklarının izlenmesi ve profillerinin çıkarılması)
- Bilişim teknolojileri yönüyle hukuk (Ceza hukuku, Siber hukuk)
- Kriminoloji (Kriminal prosedürler)
- Bilgisayar donanım, yazılım ve programlama (Ağ temelleri, bilgisayar güvenliği, işletim sistemleri, güvenlik mimarisi)

2.5.3.2. Türkiye'de Siber Güvenlik Eğitimi

Türkiye'de Siber Güvenlik Kurulu tarafından Ulusal Siber Güvenlik Stratejisi ve Eylem Planı hazırlanmış ve 20 Kasım 2012 yılında resmi gazetede yayınlanarak yürürlüğe girmiştir. Türkiye'nin bu konudaki önemli adımlarından ilki olarak karşımıza çıkmasından dolayı dikkate değerdir. 2016-2019 yılında yayınlanan Ulusal Siber Güvenlik Stratejisi eylem planında, eğitim ve farkındalık ile ilgili aşağıdaki eylemler yer almaktadır (USGS, 2016).

- Tüm toplum nezdinde siber güvenlik farkındalığının oluşturulması hem eğitim kurumlarının hem de yazılı ve görsel medyanın bu konuda çalışma yapması,
- Öncelikle kurum yöneticilerinin siber güvenlik konusunda bilinçlendirilmesi için çalışma yapılması,
- Siber güvenlik alanında yeterli düzeyde bilgiye sahip personelin yetiştirilmesi, bu alanda uzmanlaşmak isteyen tüm bireylerin teşvik edilmesi,

Güvenli İnternet Merkezi, toplumdaki ağa bağlı bilişim teknolojisi kullanıcılarının ve özellikle genç nüfusun, bu teknolojiler hakkında bilgi sahibi olması ve işlevsel kullanabilmesi amacıyla; bilinçlendirme çalışmaları, eğitimler, projeler düzenlemek üzere 2017 yılında Bilgi Teknolojileri ve İletişim Kurumu bünyesinde sosyal sorumluluk bilinciyle kurulmuştur. İnternet birçok risk taşımaktadır ki siber güvenlik bilgisi olmayan bireyler bu risklere karşı savunmasız bir şekilde bulunmaktadır. Toplumun her ferdini siber tehditlere karşı korumanın yanında korunma yöntemlerini öğretmek daha da elzemdir. Bu nedenle teknoloji çağında geleceğimizin teminatı olan çocukların internetin faydalarından istifade eden, zararlarından korunan, siber güvenlik konusunda farkındalıkları üst düzeyde bireyler olarak yetiştirilmesi gerekmektedir. Bu bağlamda yapılacak tüm çalışmaların her vatandaşa özellikle de gençlerimize, yarınlarımızın daha huzurlu olabilmesi için önem arz etmektedir (Güvenli İnternet Merkezi, 2017).

Türkiye'de siber güvenlik konusundaki farkındalığın devlet nezdinde politika olarak karşımıza çıkması ve eyleme dönüşmesi 2012 yılına denk gelmektedir. Bilgi Teknolojileri ve İletişim Kurumu (BTK), Ulusal Siber Güvenlik Stratejisi Eylem

Planı kapsamında ve toplumdan, kurumlardan gelen istekler neticesinde siber güvenlik konusunda farkındalığın arttırılması için çalışmalar yapmaktadır. Söz konusu çalışmalarda; siber uzaydan gelen tehlikeler, farkındalığı artırma, kişisel güvenlik önlemleri, kurumsal güvenlik politikaları, güvenli sosyal medya ve mobil cihazlarda bilgi güvenliği konularında sunumlar yer almaktadır. Kurumun yetkileri arasında yer alan siber güvenlik mevzuat çalışmaları ile ilgili bilgilendirme çalışmaları yapılmaktadır. Bunun yanında kurum personeli tarafından siber güvenlik ile ilgili uzmanlık tezi, makale, rapor çalışmaları da yapılmaktadır. (BTK, 2017).

MEB Hayat Boyu Öğrenme Genel Müdürlüğü tarafından düzenlenen kurslar ile Bilgi Güvenliği Bilinçlendirme Eğitimi verilmekte olup, siber güvenlik farkındalığını arttırma çalışmaları yapılmaktadır (HBÖGM, 2016).

MEB, 2023 Eğitim Vizyonu Belgesinde siber güvenlik eğitimlerine de yer vermiştir. Belgede İlkokul derslerinin kazanımlarında siber güvenlik ile ilgili olan güvenli internet, siber güvenlik, siber zorbalık ve veri güvenliği gibi kavramların bulunduğu ve çocukların bu konudaki kazanımlarının takip edileceği, gerekli görüldüğünde güncelleştirmeler yapılacağı ifadesine yer verilmiştir (MEB, 2018).

Bilgi Teknolojileri ve İletişim Kurumu, Bilgi Güvenliği Derneği, Gazi Üniversitesi, T.C. Ulaştırma ve Altyapı Bakanlığı, ODTÜ, İTÜ iş birliği ile her yıl düzenlenen Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı'nda (ISCTurkey), bilgi güvenliğini sağlama yöntemleri, saldırı tespit yöntemleri, şifreleme, siber tehditlere yönelik çözüm önerileri vs. bilişim güvenliğine yönelik Uluslararası bilgi güvenliği ve kriptoloji ile ilgili bilgi verilmektedir (ISCTurkey, 2018).

MEB ile Uluslararası Siber Güvenlik Federasyonu (USGF) arasında yapılan anlaşma kapsamında, (USGF) ortaöğretimde siber güvenlik ile ilgili eğitimlerin seçmeli ders vasıtasıyla verilmesi için bir çalışma başlatıldığı görülmektedir. Siber tehditlerden korunabilmek ve Türkiye'ye karşı düzenlenecek siber saldırıları bertaraf etmek amacıyla "siber ordu" projesi de irdelenmiş, bu doğrultuda Uluslararası Siber Güvenlik Federasyonu (USGF) tarafından geliştirilen diğer projeler de gündeme

alındığı ifade edilmektedir. Ortaöğretimde verilecek siber güvenlik eğitiminin içeriğinin de hazır olduğu ve yetkililerle paylaşıldığı ifade edilmektedir (USGF, 2019).

Türkiye'de lisans düzeyinde siber güvenlik eğitimi bulunmamakla birlikte, yüksek lisans ve doktora düzeyinde bu eğitimlerin verildiği görülmektedir. Milli Savunma Üniversitesi, Şehir Üniversitesi, Yaşar Üniversitesi, Gazi Üniversitesi, İstanbul Teknik Üniversitesi, Bahçeşehir Üniversitesi, Gebze Teknik Üniversitesi bünyesinde yüksek lisans programları; Medipol Üniversitesi, Gazi Üniversitesi, İstanbul Teknik Üniversitesi bünyesinde doktora programları yer almaktadır. Bunun yanında Polis Akademisi, Gazi Üniversitesi, Mustafa Kemal Üniversitesi, Hacettepe Üniversitesi, Fırat Üniversitesi bünyesinde ise Adli Bilişim eğitim programları verilmektedir (Önaçan ve Atan, 2016).

Ülkemizde pek çok sektörde siber güvenlik ile ilgili farkındalığı arttırmak için çalışmalar mevcut iken, burada konumuz gereği genellikle eğitim alanında yapılan faaliyetlere yer verilmiştir. Yine bu kapsamda İl ve İlçe Milli Eğitim Müdürlüklerinin, okulların kendi bünyelerinde siber güvenlik çalışmaları yaptığı da gözlenmektedir. Tüm bu çalışmalar gençlerimizi internetin tehlikeli yönlerine karşı korumak, bilinç geliştirmelerine yardımcı olmak amacıyla düzenlenmektedir.

2.5.3.3. Mesleki ve Teknik Anadolu Liselerinde Siber Güvenlik Eğitimi

Bilişim teknolojileri alanı, bilgisayar sistemlerinin yazılım ve donanım kurulumu yanında alanın altında yer alan ağ işletmenliği, bilgisayar teknik servisi, veritabanı programcılığı ve web programcılığı dallarının yeterliklerini kazandırmaya yönelik eğitim ve öğretim verilen alandır. Ağ İşletmenliği dalı, bilgisayar sistemlerinin donanım ve yazılım kurulumu, ağ sistemlerinin kurulumu, yönetimi ve ağ ortamı üzerinde yaşanabilecek sorunlar, çözüm yolları ve geniş ağ sistemleri yönetimine yönelik eğitim ve öğretim verilen daldır. Bilgisayar Teknik Servisi dalı, bilgisayar sistemlerinin donanım ve yazılımı, kurulumu, bakım ve arıza giderme işlemleri ve bilgisayar ile kontrol edilebilen sistemler kurmaya yönelik eğitim ve öğretim verilen daldır. Veritabanı Programcılığı dalı, bilgisayar sistemlerinin

donanım ve yazılım kurulumu, veri tabanı ve programlama dilinin kurulumu, veri tabanının oluşturulması ve yönetimi, yazılım geliştirme, hata giderme, bakım ve yedek almaya yönelik eğitim ve öğretim verilen daldır. Web Programcılığı dalı, bilgisayar sistemlerinin donanım ve yazılım olarak kurulumu bilgilerinin yanında, web sayfası tasarımına ve programlama dilleri yardımıyla etkileşimli web uygulamaları hazırlanmasına yönelik eğitim ve öğretim verilen daldır (MEB, 2011).

Bilişim Teknolojileri alanında eğitim gören öğrencilerin meslek olarak bu alanı seçmelerinden dolayı diğerlerine göre daha fazla bilgi sahibi olmaları, geliştirdikleri bilişim teknolojilerinde de siber güvenlik yöntemlerini kullanmaları beklenmektedir. Bu konuda Milli Eğitim Bakanlığı'nın Çerçeve Öğretim Programında, Programlama Temelleri dersine Bilişim Etiği ve Bilgi Güvenliği modülü eklenmiştir. Modülün amaçlanan öğrenme kazanımları aşağıda belirtilmiştir (MEGEP, 2018).

- Etik ve bilişim etiği kavramlarını açıklar.
- Bilgi güvenliği yönetimi temel kavramlarını açıklar.
- Temel Güvenlik Prensiplerini açıklar.
- Siber suçlar ve istismarları açıklar.
- Bilişim hukukunu açıklar.

Ağ İşletmenliği dalında Ağ Sistemleri ve Yönlendirme dersinde okutulan Ağ Güvenliği modülünün amacı, gerekli ortam sağlandığında; ağın sorunsuz ve güvenli çalışması için güvenlik önlemlerini alarak güvenlik araçlarını kullanabilmek, sorunsuz ve güvenli çalışan kablosuz ağ yapılandırabilmek olarak tanımlanmıştır (MEGEP, 2018).

Alandaki tüm dersler incelendiğinde bu iki ders dışında siber güvenlik ile ilgili bir eğitim verilmediği görülmektedir. Ağ Sistemleri ve Yönlendirme dersi sadece Ağ İşletmenliği dalını seçen öğrencilerin aldığı bir ders olduğu için, alandaki tüm öğrencileri kapsamamaktadır. Sadece Programlama Temelleri dersi ortak dersler içinde yer almakta ve 10.sınıfta tüm alan öğrencileri bu dersi almaktadır. Dolayısıyla bu dersin içeriğinde yer alan Bilişim Etiği ve Bilgi Güvenliği modülü Bilişim

Teknolojileri alanındaki öğrencilerin siber güvenlik eğitimi adına aldıkları tek kaynak olarak karşımıza çıkmaktadır.

2.6. Siber Suç

Literatür incelendiğinde, net bir tanımlamanın bulunmadığı kavram olarak karşımıza çıkan siber suç, "bilgisayar suçları", "bilişim suçları", "internette işlenen suçlar" şeklinde de ifade edildiği görülmektedir. Bu kavramlar için yapılan açıklamalara bakıldığında, birbirine benzer ifadelerin yer aldığı anlaşılmaktadır. Uluslararası araştırmalarda özellikle hukuk alanında kullanımına sık karşılaşılan bu Avrupa Konseyi Siber Suç Sözleşmesi'nde de kendine yer bulan bir kavram olarak "siber suç" ifadesini kullanmanın daha doğru olacağı düşünülmektedir (Turhan, 2006).

Genel olarak ifade edilmek istenirse, siber uzay denilen bilişim teknolojilerinin oluşturduğu ortamda işlenen suçlara siber suç adı verilmektedir.

Ancak bu ifadenin açıklamaya muhtaç olduğu, siber suçların özellikleri ile ilgili herhangi bir ibarenin yer almadığı görülmektedir. Bu nedenle siber suç, bilişim teknolojilerini kullanarak, yine bir bilişim teknolojisine zarar vermek amacıyla siber uzayda yapılan eylemler olarak tanımlanabilir (Turhan, 2006).

ABD'de yapılan araştırmalara bakıldığında, siber suçları yerine bilişim suçları ifadesi de kullanılmakta olup on iki madde şeklinde açıklanmaktadır. Bunlar ise sahip olunan varlıklara karşı yapılan hırsızlıklar, dijital ortamdaki bilgilere ya da verilen hizmetlere karşı yapılan eylemler, yetkisiz giriş, veri dolandırıcılığı, bireylerin hatasından kaynaklanan durumlar, gasp, gizli bilgilere karşı eylemler, sabotajlar, nakit birikimlere karşı hırsızlıklar, evrak sahteciliği, banka ve kredi kartlarına karşı eylemler, dijital ortamda kullanılan şifrelere yönelik eylemler olarak karşımıza çıkmaktadır (Ergün, 2008).

Bilgisayar suçları ya da siber suçlar gibi farklı ifadeler kullanılan bu suç türüne uygun yapılan en kapsamlı açıklama Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu tarafından Paris'te yapılmıştır. Bu açıklamaya göre bilişim suçları;

verilerin işlenmesi, dağıtılması, depolanması için kullanılan bir sistemde, izinsiz, yasadışı olarak gerçekleştirilen her türlü eyleme verilen addır (BİAK, 2012).

Dijital ortamdaki varlıklar denildiğinde akla, burada saklanan ve işlenen bilgiler, hizmet sunmak amacıyla kullanılan tüm cihazlar, bu cihazların yazılım ve donanımları gelmektedir. Örneğin bir işletmedeki çalışanların eposta adresleri ve şifreleri, o personelin dijital varlığı olarak görülmektedir. Siber uzayda bulunan yazılımdan ya da insandan kaynaklanan hatalar aracılığıyla, tanımlanan varlıklara izinsiz erişim, bilgilerin silinmesi, değiştirilmesi ya da ele geçirilmesi gibi eylemler siber suç olarak ifade edilmektedir (Önaçan ve Atan, 2016).

Literatürde yapılan araştırmalar ışığında, bilişim teknolojileri kullanılarak bilişim sistemlerine karşı hizmeti devre dışı bırakma ya da bozma amaçlı ataklar ve bilişim teknolojileri kullanılarak insanların maddi ve manevi zarar görmesine yol açmak olmak üzere siber suçu iki boyutta tanımlamanın doğru olacağı görülmektedir.

Bilgisayar suçlarının genel olarak iki kısımda incelenebileceği görülmektedir. Bunlardan ilki direk bilişim teknolojilerine karşı işlenen suçlardır. Burada suçun hedefinde bir bilişim sistemi bulunmakta olup, onun hizmetini durdurmak, geciktirmek, bozmak amaçlanmaktadır. İkincisi de bilişim teknolojilerinin araç olarak kullanılması ile gerçekleştirilen kanun dışı eylemlerdir. Bu kısımda, geleneksel suç olarak ifade edilen suçların, teknolojinin gelişmesiyle birlikte herhangi bir bilişim sistemi aracılığıyla işlenmesi karşımıza çıkmaktadır (BİAK, 2012).

2.6.1. Siber Suç Çeşitleri

Literatürde kabul görmüş olan McConnel International adlı Amerikan global politika ve teknoloji danışmanlık firmasının 2000 yılında yayınladığı raporda siber suçlar aşağıdaki gibi sınıflandırılmıştır (McConnell International, 2000).

- Veri Suçları
    - Verilere Müdahale Edilmesi
    - Verilerin Değiştirilmesi
    - Veri Hırsızlığı

- Ağ Suçları
    - Ağ Engellenmesi
    - Ağ Sabotajı
- Yetkisiz Erişim Suçları
    - Yetkisiz Erişim
    - Virüs Yayılması
- İlgili Suçlar
    - Bilgisayarla İlgili Sahtekârlıklar
    - Bilgisayarla İlgili Dolandırıcılık

İnternet Üst Kurulu tarafından yapılan sınıflandırmaya göre siber suçlar aşağıdaki gibi listelenmektedir (Turhan, 2006).

- Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim
    - Yetkisiz Erişim
    - Yetkisiz Dinleme
    - Hesap İhlali
- Bilgisayar Sabotajı
    - Mantıksal Bilgisayar Sabotajı
    - Fiziksel Bilgisayar Sabotajı
- Bilgisayar Yoluyla Dolandırıcılık
    - Banka Kartı Dolandırıcılığı
    - Girdi/Çıktı Program Hileleri
    - İletişim Servislerini Haksız ve Yetkisiz Olarak Kullanma
- Bilgisayar Yoluyla Sahtecilik
- Bir Bilgisayar Yazılımının İzinsiz Kullanımı
- Diğer Suçlar
    - Kişisel Verilerin Suiistimali
    - Sahte Kişilik Oluşturma ve Kişilik Taklidi
    - Yasadışı Yayınlar

Siber suçlar, geleneksel suçlarda olduğu gibi çeşitlilik göstermekte ve bu suçların da kendi içinde bir sınıflandırması yapıldığı görülmektedir. Yukarıdaki sınıflandırmalar ve bu alanda yapılmış olan diğer çalışmalar dikkate alındığında bu çalışmada siber suçlar; veri suçları, bilişim ağlarına yönelik suçlar, yetkisiz erişim suçları, dolandırıcılık, sahtecilik, yasadışı yayınlar, müstehcenlik, lisans haklarına aykırı kullanım olmak üzere geniş kapsamlı değerlendirilmektedir (Turhan, 2006; Nacar, 2010; Güvenli Web, t.y.; Altınok ve Vural, 2011).

2.6.1.1. Veri Suçları

Dijital ortamda saklanan bilgilerin ele geçirilmesi, değiştirilmesi, silinmesi gibi eylemler temel manada veri suçları kapsamına girmektedir. Ele geçirilen bilgilerle, bu bilginin asıl sahibinin ya da çalınan bilgiyle ilişkili bir başka kişinin mağdur edilmesi halinde işlenen suça veri suçu denir. Ayrıca çalınan bilgiler kullanılarak bir kişinin ya da kesimin bundan haksız yere gelir sağlaması durumunda da veri suçu ortaya çıkmaktadır (Turhan, 2006). Verilerin değiştirilmesi, bilişim sistemlerinde bulunan bilgilerin veri güvenliğinin tahrip edilmesi, bozulması ve değiştirilmesi suçudur. Özellikle sahtekârlık ve dolandırıcılık suçlarında kullanılır.

Verilere müdahale edilmesi, siber uzayda bilgi aktarılırken birilerinin etkilemesi yönlendirmesine ilişkin suçtur. Bu suçun ortaya çıkması için, bilgiler aktarılırken alıcı ve gönderici dışında transfere müdahil olan kişilerin bu verilerin iletimini durdurması, başka bir hedefe yönlendirmesi ya da ele geçirilmesi gerekmektedir (Nacar, 2010).

Veri sızıntılarına örnek olarak tarihe geçmiş bazı vakalar da şu şekildedir (platinbilisim.com.tr, 2019).

- 2014 yılında JPMorgan Chase şirketine yapılan siber saldırıda 83 milyon müşterinin dijital varlıklarının çalınması,
- 2015 yılında Anthem Sigorta adlı şirketin bilişim sistemlerine yapılan saldırıda 78 milyon müşterinin bilgilerinin çalınması
- Türkiye'de devlet kurumlarına ait sunuculardan 54 milyon seçmenin bilgilerinin çalındığını Rus hacker grubu tarafından duyurulması,
- 2013'te Japonya'da Yahoo adlı siteden 22 milyon kullanıcının eposta bilgilerinin çalınması,
- 2014 yılında Kore Kredi Bürosu'nda çalışan bir personelin 104 milyon kullanıcı bilgisini USB bellek ile çalınması

2.6.1.2. Bilişim Ağlarına Yönelik Suçlar

Ağ engellenmesi ve ağ sabotajı bilişim ağlarına yönelik suçlar olarak karşımıza çıkmaktadır. Ağ engellenmesi, ağa bağlı bir bilişim cihazının ağın tamamına ya da belli bir bölümüne erişimine engel olunması şeklinde işlenen bir suç çeşididir. Bu genellikle ele geçirilen bilgisayarlardan sürekli o cihaza veri gönderilmesi yoluyla cihazın gerçek kişilere ya da cihazlara cevap verememesinden kaynaklanan erişim sorunudur. Bu yönteme DDOS saldırısı adı verilmektedir. Siber suçların işlenme yöntemleri başlıklı konuda bu yöntem de incelenmektedir.

Ağ sabotajı, fiziksel olarak ağa ya da ağ sistemine gerçekleştirilen bir saldırı çeşididir. Bu direk fiziksel bir müdahale olabildiği gibi elektromanyetik alan kullanılarak da tahrip edilebilmektedir.

2.6.1.3. Yetkisiz Erişim Suçları

Bilişim sistemlerine yetkisiz giriş ve virüs adı verilen zararlı yazılımların yayılması olmak üzere bu suç türünü ikiye ayırmak mümkündür. Sisteme yetkisiz giriş Türk Ceza Kanunu (TCK)'nun 243.maddesinde, "bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden" ifadesiyle belirtilmiş ve suç olduğu açıklanmıştır. Dijital ortamdaki her türlü veriye erişmek, verilerin bulunduğu sisteme girmesine izin verilen kişilerce mümkündür. Yetkili bireyler dışında sisteme izinsiz girmek, bu verilere erişmek ve silmek ya da yönlendirmek suretiyle zarar vermek tüm dünyada suç olarak kabul görülmektedir (Turhan, 2006).

Zararlı yazılımlardan biri olan virüsler, bulaştığı sistemlere hasar vermek amacıyla geliştirilen uygulamalardır. Harici bellekler, epostalar, web sitelerinden indirilen veriler ile sistemlere bulaşan virüsler, verilerin silinmesine, bozulmasına neden olmakla birlikte, sistemin düzgün çalışmasını da engelleyebilmektedir. Bu programlar "exe" uzantılı uygulama dosyalarına kendilerini ekleyen, durmadan kendini çoğaltarak sisteme yayılabilen, sistemin çalışmasını yavaşlatan özellikleri vardır. Virüslerin bilişim sistemlerine ciddi zararları olmaktadır. Gelen bir mailin okunması ya da burada yer alan bir linke tıklanmasıyla, internetten bir verinin

indirilmesiyle, virüs bulunan bir uygulamanın çalıştırılmasıyla bilgisayarlara bulaşmaktadırlar (Yıldız, 2014).

2.6.1.4. Dolandırıcılık

Bireylerin kandırılması için bilişim teknolojilerinden faydalanmak suretiyle işlenen suçlardır. TCK'da ise dolandırıcılık suçuna "Hileli davranışlarla bir kimseyi aldatıp onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlamak" şeklinde yer alan bir ifadeyle yer verilmiştir. Bilişim sistemine yetkisiz erişim ile verilerin kopyalanması, banka ve kredi kartlarının klonlanması, bu veri ve kopyalar vasıtasıyla insanların banka hesaplarından başkalarının zimmetlerine para aktarılması ya da başkalarını kandırmak amacıyla kullanılması bu suç türüne giren eylemler olarak karşımıza çıkmaktadır (Altınok ve Vural, 2011).

2.6.1.5. Sahtecilik

Başkalarının maddi varlıklarını ele geçirmek ve bir başkasına haksız kazanç sağlamak amacıyla, bilişim teknolojilerini kullanarak senet, çek gibi sahte belge oluşturmak ya da bilişim sistemlerinde tutulan belgeler üzerinde izinsiz değişiklik yapmaktır (Turhan, 2006). Gerçek bir web sitesinin kopyasını yaparak insanları kandırmak, başka kişiler adına web sitesi oluşturarak ya da sosyal medya hesapları açarak o isim üzerinden mesajlar göndermek, spam adı verilen sahte mailler göndermek, oltalama adı verilen yöntemlerle insanları tuzağa düşürmek, sahte belge düzenlemek, sahte bilet satmak gibi eylemler bilişim teknolojileri kullanılarak gerçekleştirilen sahtecilik suçlarına örnek verilebilir (Altınok ve Vural, 2011).

2.6.1.6. Yasadışı Yayınlar

Ülkemizin bölünmez bütünlüğünü, vatandaşların huzurunu hedef alan, terör materyalleri kapsamına giren içerikleri yayınlayan web siteleri, özel ya da tüzel kişilere karşı hakaret içeren ifadelerin bulunduğu içerikler, pornografik adı verilen toplumun ahlak düzenini bozacak nitelikte içerikler bu suçun kapsamına girmektedir (Digisophia, 2014).

Bilişim teknolojileri kullanılarak devletler tarafından yasa dışı olarak kabul görmüş içeriklerin yayınlanması ve bilişim ağları üzerinden dağıtılması bu suçun kapsamındadır. Yasa koyucular tarafından kanunda suç olarak yer verilen bu araçlar; mailler, web siteleri, insanların birbiriyle iletişiminde kullandığı teknolojiler, ses ya da görüntü kaydeden her türlü teknolojik aygıt olarak kabul edilmektedir (Bilek, 2012).

2.6.1.7. Müstehcenlik

Müstehcen kelimesi Türk Dil Kurumunda; "açık saçık, edepsizce olan, çirkin ve uygunsuz" olarak açıklanmaktadır. Bu tanımdan yola çıkarak bu suçun ahlakla yakından ilgili olduğu açıktır. Türk Ceza Kanunu (TCK)'nun 226.maddesinde müstehcenlik suçunun hangi eylemleri kapsadığı açıklanmış ve bu cezaları da belirtilmiştir. Bu kanun maddelerine göre; "şiddet kullanılarak, hayvanlarla, ölmüş insan bedeni üzerinde veya doğal olmayan yoldan yapılan cinsel davranışlara ilişkin yazı, ses veya görüntüleri içeren ürünleri üreten, ülkeye sokan, satışa arz eden, satan, nakleden, depolayan, başkalarının kullanımına sunan veya bulunduran kişiler hakkında bir yıldan dört yıla kadar hapis cezası var iken bunları çocukların görmesini, dinlemesini ve izlemesini sağlayan bireylere altı yıldan on yıla kadar hapis ve beş bin güne kadar adlî para cezası" şeklinde açıklanmıştır. (Karaca ve Beyaznar, 2010).

Müstehcenlik suçu altında çocuk pornografisi de bulunmaktadır. Bu konuya da ayrıca değinmek önem arz etmektedir. Karar verme ehliyeti bulunmayan yaştaki bireylerin uygunsuz vaziyetteki görsellerin ya da gayri ahlaki davranışlarının yer aldığı videoların bilişim teknolojileri kullanılarak dağıtılması, bilişim sistemlerinde bulundurulması ya da yayınlanması siber suç olarak görülmektedir. Çocuk pornografisi olarak adlandırılması için bu içeriklerde yer alan bireylerin 15 yaşından küçük olması gerekmektedir (Bilek, 2012).

Küçük yaştaki çocukların gerçek görüntüleri ile ya da onları temsil eden animasyonlar ile pornografik adı verilen ahlaka aykırı içeriklerin oluşturulmasına çocuk pornografisi adı verilmektedir. Bu içerikleri kapsayan her türlü dijital ürünün

yayınlanması, satılması, gönderilmesi, bulundurulması tüm ülkeler tarafından kabul görmüş bir suçtur (İlbaş, 2009).

2.6.1.8. Lisans Haklarına Aykırı Kullanım

Geliştirilen bir yazılım Fikir ve Sanat Eserleri Kanunu tarafından koruma altına alınmaktadır. Yazılıma sahip olan kişi ya da kurumun izni olmadan kullanılması, kopyalanması, başka bilgisayarlara aktarılması, satılması suç olarak görülmektedir. Bir yazılım yasal yollardan satın alındığında sahibi tarafından bir kopyası verilmektedir. Bu yazılımın birden fazla bilgisayara kopyalanması, satılması ya da kiralanması kanunen yasaktır (Altınok ve Vural, 2011).

Turhan (2006)'a göre yazılımların izinsiz kullanılması, kanun maddesiyle korunan bir teknolojik ürünün izinsiz bir şekilde kopyalanmasını, sahibinin bilgisi ve rızası dışında elde edilen yazılım ürünlerinin çoğaltılmasını, satılmasını ve kullanımını kapsar. Belirtilen suç unsuru; lisans haklarına aykırı kullanma, çoğaltma ve kiralama şeklinde gerçekleşmektedir.

2.6.1.9. Diğer Suçlar

Satışı yasak olan ürünlerin internet yoluyla kolaylıkla satılabilmesi yasadışı faaliyette bulunan insanları bu alana çekmektedir. Silah, insan, uyuşturucu, organ, çocuk ticaretinin bilişim teknolojileri aracılığıyla yapılması nispeten daha kolay ve yakalanması güç olmasından dolayı genellikle siber suçların içerisine girmektedir (Budak, 2015).

2.6.2. Siber Suçların İşlenme Yöntemleri

Bir önceki konuda bilgi verilen siber suçların hangi yöntemlerle işlendiği de önemli bir konu olarak karşımıza çıkmaktadır. Bu yöntemlerin bilinmesi, siber güvenlik farkındalığının oluşması ve siber mağduriyetin engellenmesi açısından önemli bir olgu olarak karşımıza çıkmaktadır. Ancak, hızla gelişen teknolojiyle birlikte siber suçların işlenme yöntemleri de değişmekte ve karşımıza çok farklı şekillerde çıkabilmektedir. Ayrıca yöntemin bilinmesi de her zaman suçluyu ele vereceği anlamına gelmemektedir.

Geleneksel olarak ifade edilen suçlardan siber suçların farklı olması özellikle işlenme yöntemlerinin çok çeşitlilik göstermesi ve suçluların tespit edilmesinin zorluğundan kaynaklanmaktadır (Dülger, 2004). Çağımızın teknolojik gelişiminin hızıyla doğru orantılı olarak siber suçların da işlenme şekilleri farklılaşmakta, fark edilmesi ve engellenmesi zorlaşmaktadır (Orta, 2015). Burada günümüze kadar en çok karşılaşılan yöntemlere değinilmiştir.

2.6.2.1. Ağ Solucanları (Network Worms)

Virüslerle benzerliği bulunan ağ solucanları, siber uzayda internet ağları arasında gezinen, sadece bir bilişim teknolojisine zarar vermek üzere programlanmamış, herhangi bir tetiklemeye gerek kalmadan aktif olabilen ve kendini bilgisayarlara kopyalayabilen zararlı yazılımlardır. Ağ solucanları bilişim sistemlerine zarar verebileceği gibi, truva atı adı verilen zararlı programcıklar da sistemlere yerleştirebilir (Turhan, 2006).

2.6.2.2. Bilişim Korsanlığı (Hacking)

Bilişim cihazlarının yönetimini ve kullanıcılarla iletişimini sağlayan işletim sistemlerini geliştiren yazılımcılar, istenildiğinde sisteme müdahale etmek ve koruyabilmek amacıyla arka kapı adı da verilen sisteme gizli giriş yolları bırakmaktadırlar. Bilişim korsanı denilen art niyetli kişiler de bu arka kapıları tespit ederek, oradan sisteme giriş yapmaktadırlar. Bu açığı tespit ettikten sonra sistemin güvenliğini sağlayan kişiler ya da teknolojiler bu durumu fark edene kadar istediği verilere ulaşıp manipüle edebilmektedirler. Genellikle diğer siber suç yöntemlerinde ağ solucanı, virüs gibi zararlı yazılımlar kullanılırken bu yöntem de bilişim korsanı eylemi kendisi yapmaktadır. Sisteme erişim esnasında giriş kodlarını bulmayı kolaylaştırmak ve hızlandırmak amacıyla bazı yazılımlardan yardım alsalar da, sisteme giriş yaptıktan sonra verilere erişim, kopyalama, dağıtım, bozma gibi eylemleri kendileri yapmaktadır (Alaca, 2008).

2.6.2.3. Bukalemun Tekniği (Chameleon)

Adından da anlaşılacağı üzere, kendini gizleme tekniğine dayanan bu suç işleme yönteminde, zararlı yazılım kendini normal bir program gibi gösterirken çeşitli yöntemlerle çoklu oturum bulunan işletim sistemlerinde hesap bilgilerini gizlenmiş bir dosyaya kaydeder. Ardından sistemin bir süre durdurulacağına yönelik ifadelerle kullanıcıları aldatır ve bu esnada bukalemun yazılımını yöneten kişi, kaydedilen dosyaya erişerek hesap bilgilerini elde eder (Aydın, 1992).

2.6.2.4. Çöpe Dalma (Scavenging)

Bu yöntem hem fiziksel hem de dijital olarak çöpleri karıştırma esasına dayanır. Fiziksel olarak yazıcı gibi çıktı birimlerinden alınan verilerin çöplerde bulunmasıyla elde edilmesine dayanır. Dijital olarak ise sistemden silinerek çöp kutusuna gönderilen dosyalara erişim şeklinde elde edilebilirken, kurtarma programları vasıtasıyla silinen verilerin geri getirilmesiyle de yapılmaktadır (Yazıcıoğlu, 1997).

Son bahsedilen yöntem ile özellikle tamire gönderilen bilişim cihazları üzerinde, kurtarma programları ile kişilerin özel bilgileri elde edilmektedir. Cihazlar teknik servislere gönderilmeden önce depolama aygıtları çıkarılmalıdır. Depolama aygıtları ile gönderilmek zorunda kalınırsa özel verilerinin tamamen silinmiş olmasına dikkat edilmelidir. Verilerin silinmiş olsa da özel yöntem ve programlarla geri getirilebildiği unutulmamalıdır (Bilek, 2012).

2.6.2.5. Truva Atları (Trojan)

Tarihteki truva atı olayına benzerliğinden dolayı bu isim konulmuştur. Truva atının zararsız olarak düşünülmesi ve şehre alınması, ardından içinden askerlerin çıkması olayı ile bu suç türü aynı mantığa dayanmaktadır. Burada da zararsız olduğu düşünülen bir yazılımın indirilmesinin ardından bu yazılıma daha önceden dahil edilmiş zararlı kodların bilgisayara yayılması şeklinde gerçekleşir. Zararlı yazılımlarını sistemlere bulaştırmak isteyen kişiler, özellikle faydalı olan yazılımlara bunları eklerler ve kullanıcıların bu faydalı yazılımları bilgisayarlarına indirmelerini, başkalarıyla paylaşmalarını fırsat bilirler (Dülger, 2004).

Truva atı adı verilen yazılımlar ilk bakışta faydalı olduğu düşünülen fakat esasında bilişim teknolojilerine girdiklerinde zarar vermek için kodlanmış yazılımları da içinde barındıran programlardır. Mail yoluyla, lisansı olmayan programların kayıt dışı kullanılması için geliştirilen "crack" adı verilen programlar içine eklenerek ya da ücretsiz yararlı programlar vasıtasıyla bilgisayarlara bulaştırılmaya çalışılır. Sisteme bir kez bulaştıktan sonra, açıkları bulmaya çalışır ve sahibinin isteklerine yanıt verir (Altınok ve Vural, 2011).

Truva atları bulaştıkları sistemde bulunan sunucu kısmı ve truva atını yöneten kişinin bilgisayarında bulunan istemci kısmı olmak üzere iki bölümden oluşmaktadır. Zarar verilmek istenen sistemlerdeki kısmı boyut olarak çok küçüktür ve bu nedenle tespit edilmesi oldukça güçtür. İstemci adı verilen kısım kullanılarak bu sunucu ile iletişim sağlanır. Bu noktadan sonra truva atını yöneten kişinin istediği veriler sunucu kısım vasıtasıyla hedef sistemden kaynağa gönderilir (Değirmenci, 2002).

2.6.2.6. Virüsler

Virüs adı verilen zararlı yazılımlar, girdikleri sistemde bulunan uygulamaları bozarak, hedef alınan sistemlere maksimum hasarı vermek üzere geliştirilmişlerdir. Virüsler, internetten indirilen verilerle, mail yoluyla ya da harici bir depolama aygıtıyla sistemlere bulaşırlar. Bir kez girdikten sonra da kendilerini çoğaltarak yayılırlar. Uygulamaları çökerterek, depolama aygıtlarına yayılarak sistemi kullanılamaz hale getirirler (Alaca, 2008). Bir bilgisayar virüsü, kendini yürütülebilir dosyalara ekleyerek yayılan, kendi kendini sistem alanlarına kopyalayan bir bilgisayar programıdır. Uygulama veri dosyalarını etkileyen virüs türleri de vardır. Makro içeren bu virüsler, kendilerini yaymak için makro dilleri ile oluşturulmaktadır (Nachenberg, 1997).

Genellikle bir bilgisayar virüsü ana makineye zarar verir. Bilgisayarın işletim sistemi ve dosya sistemi gibi farklı bileşenlerinde hasarlara yol açabilir. Bu bileşenlere sistem sektörleri, dosyalar, makrolar, yardımcı dosyalar ve kaynak dosyalar örnek verilebilir. İnternetin sürekli birbirine bağlı olan dünyası virüsler için kolay bir hedef haline gelmektedir çünkü virüsler dünyaya daha hızlı yayılmak için

internet bağlantısını kullanmaktadır. Virüslerin erken teşhisi bunlardan kaynaklanan zararların en aza indirgenmesi için önemlidir (Desai, 2008).

Ağ solucanları ve virüsler genellikle birbirleriyle karıştırılır. Farkları ise virüslerin çalışabilmesi için kullanıcıya ihtiyaç duymaları, solucanların ise kullanıcı müdahalesine gerek duymadan kendilerinden aktif olmalarıdır. Bu açıdan değerlendirildiğinde ağ solucanlarının daha zararlı olduğu düşünülebilir (Ermeydan, 2018).

2.6.2.7. İstemdışı Elektronik Postalar (Spam)

Spam, özellikle reklam amaçlı tercih edilmekte olup, toplumun mümkün olduğu kadar fazla kesimine istenilen mesajların ulaştırılabilmesi için bilişim teknolojileri kullanan kişilerin isteği dışında mail yoluyla gönderilmesi mantığına dayanmaktadır (İnternet Üst Kurulu, 2005).

Spam, kullanıcının çevrimiçi güvenini baltalıyor, üretkenliğini azaltıyor, bilgisayar virüslerini yayıyor ve tüm taraflar için maliyetleri arttırıyor. Bu durumla mücadele etmek için uluslararası iş birliği çok önemli bir konu olarak karşımıza çıkmaktadır (OECD, 2004).

İstenmeyen epostalar, alıcıları için oldukça sıkıntı vericidir, aynı zamanda bir güvenlik tehdidi de sunar. Örneğin, gönderilen spamlar, kullanıcının oturum açma kimlik bilgilerini elde etmek isteyen sahte bir web sitesine bağlantı içerebilir. Kötü amaçlı yazılım yüklemek isteyebilir (DeBarr ve Wechsler, 2009).

2.6.2.8. Oltalama (Phishing)

Oltalama ismi, yem kullanılarak balık yakalama felsefesinden hareketle konulmuştur. Bu yöntemde temel amaç kişilerin gerçek zannettikleri ama sahte içeriklere inanmaları ve bilgilerini girmeleridir. Böylece bu bilgiler ele geçirilmiş olup kötü niyetle kullanılmaktadır. Ağa bağlı bilişim teknolojisi kullanan kişiler, çalıştıkları bankaların ya da kullandıkları mail servislerinin web siteleri gibi kişisel veri isteyen sitelerin kopyalarına inanması ile bilgilerini bu sahte sitelere

girebilmektedirler. Bu aşamada kopya siteleri yapan kişiler bu verileri ele geçirerek söz konusu kişilere zarar vermektedirler. Günümüzde sıkça görülmesi ve tehlikeli olması sebebiyle dikkat edilmesi gereken suç yöntemlerinin başında gelir (Turhan, 2006).

Bu yöntemde dolandırıcılar tarafından en çok tercih edilen teknik, bankaların ve e-ticaret sitelerinin kopyalarını yaparak insanları aldatmaktır. Mail yoluyla bu sahte sitelerin linkleri kullanıcılara gönderilir ya da arama motorlarından kopya sitelerin tıklanması beklenir. Birebir kopyası olduğu için kullanıcılar sahte olduğunu anlayamazlar. Dolayısıyla güvenle kullanıcı adı, şifrelerini ya da kredi kartı bilgilerini bu kopya sitelere girerler ve dolandırıcılar tarafından bu bilgiler çalınmış olur (Ünver vd., 2011).

Oltalama yöntemi ile aldatılan kullanıcıların sistemlerine bulaştırılan zararlı yazılımların barındığı sunucular üzerine 2016 ilk çeyreğinde yapılan bir araştırmada içinde zararlı yazılımlar bulunduran dünya genelindeki sunucuların %1'inin Türkiye'de hizmet verdiği görülmektedir (Havelsan, 2017).

Şekil-8: Sazan Avlama Tabanlı Saldırıların Gerçekleştirildiği Sunucuların Yer Aldığı Ülkelerin Oranı (Havelsan, 2017)

Ülke	Ocak'16	Şubat'16	Mart'16
ABD	77,7%	71,5%	62,4%
Çin	5,0%		13,7%
Güney Kore	3,4%		
Almanya	2,3%	2,1%	1,7%
İzlanda	1,8%	4,9%	3,3%
Hollanda	1,8%	0,9%	1,7%
Rusya Federasyonu	1,1%	2,3%	1,9%
Fransa	1,1%	2,8%	1,2%
Kanada	0,9%	2,8%	1,7%
Ukrayna	0,5%		
Ingiltere		3,5%	1,7%
İtalya		1,2%	
Türkiye		0,9%	1,0%

2.6.2.9. Veri Aldatmacası (Data Diddling)

Bu yöntem, işlenen verilerin bozulması, dijital ortamlarda tutulan bilgilerin bazı yazılımlar aracılığıyla değiştirilmesi, mevcut verilere yenilerinin eklenmesi, bazı verilerin silinmesi veya verileri kontrol eden mekanizmalardan saklanması amaçlarıyla kullanılabilmektedir (Alaca, 2008). Bu suç, sistemlere yetkisiz erişim ile işlenebileceği gibi sistemi kullanma yetkisi olan kişilerce de işlenmektedir. Bunlar; bilgileri oluşturan, analiz eden, düzenleyen, aktaran kişiler olabilir. Ancak, işletim sisteminde bulunan açıkları kullanarak giren, sisteme bir vasıtayla zararlı yazılım yükleyen kişilerce de güvenlik unsurlarını bertaraf ederek bu yöntemle suç işleyebilirler (Değirmenci, 2002).

2.6.2.10. Gizli Kapılar (Trap Doors)

Bilişim cihazıyla kullanıcı arasında arayüz görevi yapan, sistemi yönetmek için kullanılan işletim sistemlerini geliştiren yazılımcılar, bu sistemleri oluştururken ileride sistemde meydana gelebilecek bir probleme karşı güvenlik yöntemlerini atlayarak sisteme ulaşılması için gizli kapı adı verilen boşluklar bırakırlar. Gizli kapılar bu açıklara verilen isimdir (Yazıcıoğlu, 1997).

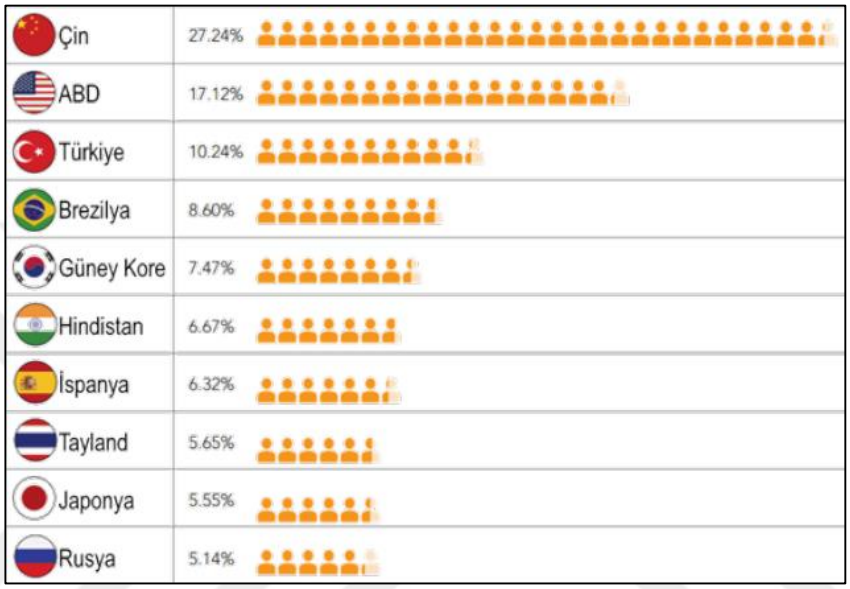
Gizli kapılar yapı itibarıyla truva atıyla benzerlik göstermektedir. Ancak gizli kapılar bizzat sistem geliştiricisi tarafından bırakılabilirken kimi zaman da kullanıcı tarafından kurulan bir program ile de bırakılabilir. Truva atları ise kullanıcının bilgisi dışında sisteme girmektedir. Bu özellikleriyle truva atları ve gizli kapılar birbirinden ayrılmaktadır (Keleştemur, 2018).

2.6.2.11. Hizmet Dışı ve Dağıtık Hizmet Dışı Bırakma (DoS, DDoS)

Sunucu bilgisayarların belli bir bant genişlikleri vardır. Bu bant genişliğini aşan istekle karşılaştığında yanıt veremez duruma gelir. Bu durumu kullanarak yapılan bir saldırı çeşidinde, hedef alınan sunucuya gönderilen yoğun istekler neticesinde sunucunun çalışamaz duruma gelmesi amaçlanmaktadır. Bu saldırı tek bir kaynaktan yapılırsa buna hizmet dışı bırakma (DoS) denir. Sunucunun o yönden gelen trafiği engellemesi ile saldırı önlenebildiği için, saldırganlar genellikle çok sayıda bilgisayarla sunucuya yüklenmektedir. Bu şekilde yapılan saldırıya da dağıtık hizmet dışı bırakma (DDoS) adı verilir. Saldırıya katılan tüm bilgisayarların bilinçli

olabildiği gibi zombi adı verilen bilgisayarlarla da bu saldırılar yapılabilmektedir. Zombi bilgisayar ise, gerçek kullanıcının farkında olmadan kötücül yazılım vasıtasıyla art niyetli kişilerce kullanılan bilgisayarlara verilen addır.

Şekil - 9: DDoS Saldırı Yapan veya Yaptırılan (Zombi) Bilgisayarların Bulunduğu Ülkeler (2016) (Havelsan, 2017)



Yukarıdaki şekilde DDoS saldırılarının en çok gerçekleştirildiği 10 ülke görülmektedir. ABD ve Çin'den sonra en çok saldırının yapıldığı üçüncü ülkenin Türkiye olduğu ortaya çıkmaktadır. Bir başka ifadeyle, her 10 DDoS saldırısından biri Türkiye'den kaynaklanmaktadır (Havelsan, 2017). Bu istatistikler saldırıyı gerçekleştiren bilgisayarların bulunduğu ülkeleri göstermektedir. Ancak bu bilgisayarlar "zombi" diye tabir edilen başkaları tarafından yönetilen bilgisayarlar da olabileceği gerçeği göz ardı edilmemelidir.

2.6.2.12. Tarama (Scanning)

Tarama yöntemi, bir döngü yardımıyla belirli bir düzende oluşturulan verileri tek tek bilişim teknolojilerine girerek olumlu yanıt bekleyen, hangi verilerden yanıt aldığını tespit ederek o verileri kaydeden bir işlem dizisidir. Örneğin, belirli bir IP aralığından hangilerini kullanan bilişim cihazları olduğunu tespit etmek için o aralıktaki tüm IP numaralarına sırasıyla sinyal gönderilir ve geri dönüş alınan

sinyaller raporlanır. Bunun sonucunda hangi IP numaralarının kullanıldığı belirlenmiş olur (Alaca, 2008).

2.6.2.13. Salam Tekniği (Salami Techniques)

Çok sayıda banka hesabından, çok küçük miktarda paranın özellikle virgülden sonraki kısmın dolandırıcılığı yapan kişilerin hesabına aktarılması şeklinde gerçekleştirilen bir yöntemdir. Bu işlemin yapılması için genellikle truva atı kullanılmaktadır (Altınok ve Vural, 2011).

Bu yöntemdeki temel esas, bu para transferinin çok küçük miktarlarda yapılmasıdır. Çünkü banak hesaplarının sahipleri ya da banka çalışanları, hesaplardaki bu çok küçük değişimleri fark etmemeleri amaçlanmaktadır. Her ne kadar bir hesaptan eksilen miktar küsuratlar seviyesinde olmasına karşın çok sayıda hesaptan bu işlem gerçekleştirildiği için toplamda transferlerin yapıldığı hesapta çok yüksek miktarda haksız kazanç sağlanmaktadır (Dülger, 2004).

2.6.2.14. Mantık Bombaları (Logic Bombs)

Mantık bombaları, bilişim cihazlarında ya da ağlarda, zararlı yazılım geliştirilirken belirlenen özel bir tarihte veya istenilen bir koşul oluştuğunda zarar vermesi için tasarlanan yazılımlardır. Öncesinde belirlenen özel durum gerçekleşmeden pasif durumda bulunur ki bu hali truva atları ile benzer özelliktedir. Aktif hale geldiğinde ise sistemi yıkıcı etkileri vardır. Mantık bombalarına her yıl 26 Nisan'da çalışan Chernobil isimli zararlı yazılım örnek olarak verilebilir (Bilek, 2012).

Mantık bombaları, zarar verme amacıyla yazılan kodların en basit örneğidir. Genellikle daha büyük bir programa gömülmüş bağımsız kod parçaları şeklindedirler (Brunnstein, 1999). Bu özelliğinden dolayı fark edilmesi zordur. Sistem içerisinde pasif halde çok uzun zaman fark edilmeden durabilir. Geliştirilirken belirlenen koşul gerçekleştiğinde aktif hale geçer ve sisteme zarar verir (Ermeydan, 2018).

2.6.2.15. Web Sayfası Hırsızlığı ve Web Sayfası Yönlendirme

Bir web sitesinin yayınlanabilmesi için öncelikle alan adı alınması gerekmektedir. Bir servis sağlayıcı aracılığıyla alınan alan adları, o sitenin adresi olur ve tarayıcıya o adres girildiğinde web sitesi bilgisayarda görüntülenir. Servis sağlayıcıda çalışan kötü niyetli insanlar aracılığıyla ya da servis sağlayıcının sistemlerine bilgisayar korsanları tarafından girilmesiyle web sayfalarına ait tescil bilgileri ele geçirilmekte ve kendi adlarına aktarılmaktadır. Böylece bu alan adı gerçek sahiplerine yüksek ücretlerle satılmaya çalışılmaktadır.

Web sayfası yönlendirme, web sitelerinin bulunduğu sunucuların IP adresleri ve alan adlarının tutulduğu DNS adı verilen sunucularda yasadışı bir şekilde alan adlarına karşılık gelen IP adresleri değiştirilir ve başak bir sunucuya yönlendirilmesi sağlanır (Alaca, 2008). Normalde bir kullanıcı tarayıcısına ziyaret etmek istediği web sitesinin adını yazdığında sistem onu DNS sunucusuna yönlendirir. Burada tarayıcıya yazılan alan adına karşılık gelen IP adresi bulunur ve o adrese yönlendirme yapılır. Eğer burada kanun dışı bir şekilde IP adreslerinde değişiklik yapıldıysa, o zaman yönlendirme olması gereken adrese değil dolandırıcının istediği adrese yapılır.

2.6.2.16. Süper Darbe (Super Zapping)

İşletim sistemleri normal düzeninde çalışırken meydana gelebilecek bir arızadan dolayı kilitlenirse, süper darbe adı verilen yazılım ile sistem üzerindeki tüm güvenlik adımları aşılarak sisteme girilmesi ve tekrar çalışır hale getirilmesi sağlanır (Nacar, 2010).

Bu program geliştirilme amacı doğrultusunda kullanıldığında çok işlevsel olmaktadır. Bozulan bir sistemin düzeltilmesi için kilit bir görev üstlenmektedir. Gerekli düzenlemelerin yapılabilmesi için öncelikle sistemde bulunan güvenlik protokollerinin geçilmesi gerekmektedir. Bu işlem de süper darbe programı ile yapılmaktadır. Ancak bu program art niyetli kişilerce kullanılırsa, güvenlik adımlarını geçerek sisteme yetkisiz giriş yapmalarına neden olabilmektedir. Bu nedenle oldukça tehlikeli bir yazılım haline dönüşmektedir (Turhan, 2006).

2.6.2.17. Gizlice Dinleme (Sniffing)

Bir internet ağı üzerinde iletilen verilerin gizlice ele geçirilmesi olayına gizlice dinleme (sniffing) denmektedir. Gizlice dinleme amaçlı geliştirilen yazılımlar, ağda transfer edilen verileri gizlice elde ederek istenilen yerlere yönlendirirler (Alaca, 2008). Bu yöntemde temel amaç, ağ trafiğinde iletilmekte olan verilerin ele geçirilmesidir. Alıcı ve vericinin fark etmemesi için, asıl veriye dokunulmaz ve bir kopyası başka adrese yönlendirilir (Ermeydan, 2018).

BÖLÜM 3

İLGİLİ ARAŞTIRMALAR

Araştırma kapsamında değerlendirilebilecek ve bu konuda yapılan araştırmalar Türkiye ve Dünya genelinde yapılan araştırmalar olarak iki farklı bakış açısı ile ele alınmıştır.

3.1. Türkiye'de Yapılan Araştırmalar

Süslü ve Oktay (2018) tarafından yapılan doktora tezinin temel amacı, lise öğrencilerinde siber zorbalık ve siber mağduriyette benlik saygısı, anne, baba ve akranlarla ilişkilerin yordayıcılığını incelemektir. Ayrıca lise öğrencilerinin siber zorbalık ve siber mağduriyet davranışlarında cinsiyet, yaş, okul türü, anne/baba eğitim durumu, bilgisayar/cep telefonu/tablete sahip olma, interneti kullanma sıklığı ve internete bağlandıkları yer açısından anlamlı bir fark olup olmadığı araştırılmıştır. Araştırmanın modeli ilişkisel tarama modelidir. Bu araştırmada, araştırma grubu İstanbul ili, Kadıköy ve Maltepe ilçelerinde devlet ve özel okullarda liseye devam eden 1085 öğrenciden (554 kız, 531 erkek) oluşturmaktadır.

Araştırmadan elde edilen sonuçlara göre, erkek öğrencilerin siber zorbalık puanlarının kız öğrencilerden daha yüksek olduğu, siber mağduriyet puanlarında cinsiyet açısından anlamlı bir fark olmadığı, 16 yaş grubunda bulunan öğrencilerin siber zorbalık puanlarının diğer yaş gruplarındaki öğrencilerden daha yüksek olduğu ve siber mağduriyet puanlarında yaş açısından anlamlı bir fark olmadığı görülmüştür. Öğrencilerin öğrenim gördükleri okul türüne bağlı olarak, siber zorbalık puanlarında anlamlı bir fark olmadığı, siber mağduriyet puanları açısından ise devlet okulunda öğrenim gören öğrencilerin siber mağduriyet puanlarının özel okul öğrencilerinin puanlarından daha yüksek olduğu sonucu elde edilmiştir. Öğrencilerin anne ve baba eğitim durumuna göre siber zorbalık puanlarında anlamlı bir fark olmadığı görülmüştür. Siber mağduriyet puanlarında ise annenin eğitim durumuna göre anlamlı bir fark olmadığı ancak babanın eğitim durumuna göre anlamlı bir fark olduğu bulunmuştur. Öğrencilerin bilgisayar, cep telefonu ve tablete sahip olmalarına bağlı olarak siber zorbalık ve siber mağduriyet puanlarında anlamlı bir fark olmadığı

görülmüştür. Ayrıca interneti kullanma süreleri açısından günde 3 saatten fazla internet kullanan öğrencilerin siber zorbalık ve siber mağduriyet puanlarının daha yüksek olduğu bulunmuştur. Öğrencilerin internete bağlandıkları yer açısından siber zorbalık puanlarında anlamlı bir farklılık görülmemiştir. Siber mağduriyet puanları açısından ise internete cep telefonundan bağlanan öğrencilerin internete evden bağlanan öğrencilerden daha yüksek puanları olduğu sonucu elde edilmiştir.

Özel (2013) tarafından yapılan yüksek lisans tezinde lise öğrencileri arasında görülen siber zorbalığın ve siber mağduriyetin, depresyon ve benlik saygısıyla olan ilişkisi, ilişkisel tarama yöntemiyle incelenmiştir. Araştırma İstanbul İli, Fatih İlçesinde bulunan 15 lisede dokuz, 10, 11 ve 12. sınıflarda okuyan öğrencilerle gerçekleştirilmiştir. Araştırmanın örneklemini 623'ü (% 47.1) kız, 701'i (% 52.9) erkek olmak üzere toplam 1324 öğrenci oluşturmaktadır. Öğrencilerin yaşları 13 ile 19 arasında değişmekte olup, yaş ortalaması 15.71'dir. Araştırmada Kişisel Bilgi Formu, Siber Zorbalık Ölçeği, Siber Mağduriyet Ölçeği, Beck Depresyon Ölçeği ve Rosenberg Benlik Saygısı Ölçeği kullanılmıştır.

Siber zorbalık ve siber mağduriyetin yaygınlığı incelendiğinde, araştırmaya katılan erkek öğrencilerin %30'unun, kız öğrencilerin ise %27'sinin siber zorbalık yaptığı görülmektedir. Erkek öğrencilerin, kız öğrencilerden daha fazla siber zorbalık yapmasına karşın siber mağduriyet açısından kız ve erkek öğrenciler arasında anlamlı bir fark görülmemektedir. Cinsiyet türlerine göre siber mağdur olma oranı kız öğrencilerde %26.50 erkek öğrencilerde %26.52 olarak bulunmuştur. İnternet kullanım süresi, depresyon düzeyi ve benlik saygısının, siber zorbalığı ve siber mağduriyeti yordayıp yordamadığı incelendiğinde, depresyon, benlik saygısı ve internet kullanım sürelerindeki artışın, siber zorbalıktaki pozitif yöndeki artışı açıkladığı görülmüştür. Bununla birlikte depresyon ve internet kullanım süresindeki artışın yanı sıra benlik saygısı puanındaki azalma, siber mağduriyetteki artışı anlamlı düzeyde açıklamaktadır.

Serin (2012) tarafından yapılan doktora tezinin temel amacı, ergenlerde siber zorbalık /siber mağduriyet yaşantılarını ve bu davranışlara ilişkin öğretmenlerin ve eğitim yöneticilerinin farkındalık düzeylerini incelemektir. Araştırma, İstanbul

ilindeki 74 resmi ilköğretim okulunun 5, 6, 7 ve 8. sınıflarında eğitim-öğretim gören 2226'sı kız, 2065'i erkek olmak üzere toplam 4291 öğrenci ile bu okullarda görevli 230'u kadın, 497'si erkek olmak üzere toplam 727 müdür ve müdür yardımcısı, 506'sı kadın, 410'u erkek olmak üzere toplam 916 öğretmen ile yürütülmüştür.

Araştırma sonucunda öğrencilerin %26,52'sinin siber zorbalığa bir şekilde karıştığı görülmüştür. Öğrencilerin %9.42'sinin siber zorbalık yaptıkları, %11,79'unun siber mağdur oldukları ve %5.31'inin ise hem siber zorba hem de siber mağdur oldukları bulunmuştur. Siber zorbalık davranışlarında bulunma / siber zorbalık davranışlarına maruz kalma yaygınlığı cinsiyete göre incelendiğinde, kız öğrencilerin erkek öğrencilerden hem daha az siber zorbalık davranışlarında bulundukları hem de daha az siber mağdur oldukları belirlenmiştir. İnternete internet kafeden giren çocukların; internete ev, okul ve arkadaşının evinden giren çocuklardan daha fazla siber zorbalık davranışları gösterdikleri, internete günde beş saat ve daha fazla bağlı kalan öğrencilerin internete bundan daha az süre ile bağlanan öğrencilerinden daha fazla siber zorbalık davranışlarında bulundukları ve daha fazla siber mağdur oldukları bulunmuştur. Araştırma sonuçlarına göre düşük sosyo-ekonomik çevredeki okullarda okuyan öğrenciler orta ve üst sosyo-ekonomik çevredeki okullarda okuyan öğrencilerden daha fazla siber mağduriyet yaşamaktadırlar. Okul yöneticilerinin %53,2'si, öğretmenlerin %47,6'sının daha önceden "siber zorbalık" şeklinde bir kavramı duydukları, yöneticilerin %58,7'sinin ve öğretmenlerin %58,3'ünün ise bu kavramın tanımını bildikleri görülmüştür. Okul yöneticilerinin %51,7'sinin, öğretmenlerin %65,4'ünün siber zorbalığa karşı herhangi bir önleyici çalışmada bulunmadıkları görülmüştür. Araştırma sonucunda elde edinilen bulgulara göre, okul yöneticilerinin %6,3'ünün, öğretmenlerin ise %7,6'sının siber zorbalığa maruz kaldıkları bulunmuştur.

Budak (2015) tarafından yapılan araştırmanın amacı, Mesleki ve Teknik liselerdeki bilişim bölümü öğrencilerinin siber suç farkındalıklarını araştırmaktır. Betimsel tarama modeli kullanılan bu araştırmada 2013-2014 eğitim-öğretim yılında Erzurum'da Mesleki ve Teknik Liselerin bilişim bölümlerinde okuyan toplam 269 öğrenciye yerli-yabancı kaynaklardan yararlanılarak ve uzman görüşlerine

başvurularak oluşturulan “Ortaöğretim Kurumlarında Siber Suç Farkındalık Anketi” uygulanmıştır.

Sonuçlar incelendiğinde öğrencilerin siber farkındalık durumlarının sınıf durumu, interneti kullanma yılı ve İnternette saldırıya uğrama durumu ile anlamlı bir farklılık göstermediği ancak cinsiyet ile anlamlı bir farklılık gösterdiği görülmüştür. Öğrencilerin internetteki rahatlık seviyelerinin sınıf durumu ve İnterneti kullanma yılı ile anlamlı bir farklılık göstermediği ancak cinsiyet ve İnternette saldırıya uğrama durumu ile anlamlı bir farklılık gösterdiği görülmüştür. Öğrencilerin İnternette alınan önlem seviyelerinin sınıf durumu, İnterneti kullanma yılı ve İnternette saldırıya uğrama durumu ile anlamlı bir farklılık göstermediği ancak cinsiyet ile anlamlı bir farklılık gösterdiği görülmüştür.

Bilişim teknolojilerinin gelişmesiyle ortaya çıkan etik sorunlar ve bilgisayar meslek dersi almış veya almakta olan ortaöğretim öğrencilerinin bilişim teknolojilerini etik olmayan şekilde kullanımlarının incelenmesini amaçlayan bu araştırma Zeybek (2011) tarafından yapılmıştır.

Araştırma sonucunda; kız öğrencilerin erkek öğrencilere göre bilişim teknolojilerini daha etik kullandıkları ortaya çıkmıştır. Ailelerinin gelir düzeyleri 2001 TL ve üzeri olan öğrencilerin bilişim teknolojilerini daha etik dışı amaçlarla kullandıkları tespit edilmiştir. Öğrencilerin bilişim teknolojilerini etik kullanımları ile öğrenim görmekte oldukları sınıf düzeyleri arasında Toplumsal Etki, Ağ Doğruluğu, Fikri Mülkiyet ve Güvenlik-Kalite faktörleri açısından anlamlı bir farklılık görülmüştür. Bilişim Teknolojileri ve Elektrik Elektronik Teknolojileri alanlarında öğrenim görmekte olan öğrenciler Çocuk Gelişimi ve Eğitimi ile Grafik ve Fotoğraf alanlarında öğrenim görenlere göre daha etik dışı görüş bildirmişlerdir. Benzer şekilde Grafik dalı öğrencileri ve henüz dal seçimi yapmamış olan öğrenciler, Endüstriyel Bakım Onarım, Veritabanı Programcılığı, Web Programcılığı ve Güvenlik Sistemleri dal öğrencilerine kıyasla daha etik görüş bildirmişlerdir. Kişisel bilgisayara sahip olmayan öğrenciler, kendine ait bilgisayarı olanlara göre daha etik görüş bildirirken, kaldığı yerde internet olmayan öğrenciler, olanlara göre daha etik görüş bildirmiştir. Öğrencilerden bilgisayar kullanım düzeylerini “çok iyi” olarak

belirtenler ile internet kullanım düzeylerini “çok iyi” olarak belirtenlerin, bilişim teknolojilerini daha etik dışı amaçlarla kullandıkları sonucuna varılmıştır. Ayrıca öğrencilerin internete bağlı kalma süresi arttıkça bilişim teknolojilerini etik dışı amaçlarla kullanımlarının da arttığı görülmüştür. Araştırma sonuçlarına göre; dosya transferi yapamayan öğrenciler, yapabilenlere göre daha etik görüş bildirirken, internetten dosya indirebilen öğrenciler Fikri Mülkiyet faktörü için daha etik dışı görüş bildirmişlerdir. Bunlara ek olarak hiç program yazamayan öğrenciler bilişim teknolojilerini en etik şekilde kullanırken, çeşitli programlama dillerinde program yazabilme düzeyini “çok iyi” olarak ifade etmiş olan öğrenciler bilişim teknolojilerini en etik dışı amaçlarla kullanmaktadırlar.

Güldüren vd. (2016) tarafından yapılan bu çalışmanın amacı, ortaöğretim kurumlarında öğrenim gören öğrencilerin bilgi güvenliği farkındalık düzeylerini belirlemeye yönelik bir ölçek geliştirmektir. Araştırma, ortaöğretim kurumlarında öğrenim gören 607 öğrenciyle gerçekleştirilmiştir.

Geliştirilen ölçek üzerinde yapılan analizler sonucunda, öğrencilerin bilgi güvenliği farkındalıklarına ilişkin ortalama puanlarının, cinsiyete göre anlamlı bir farklılık gösterdiği belirlenmiştir. Elde edilen veriler ölçeğin tamamı ve alt faktörlerinde bilgi güvenliği farkındalığı ölçeğinden elde edilen puan ortalamalarının erkeklerin kızlardan daha fazla olduğu belirlenmiştir. Bu doğrultuda çalışmada, ölçek alt faktörlerinden alınan ortalama puanlar incelendiğinde ortalamalar arasında farklılığın en çok saldırı ve tehditler alt faktöründe olduğu ve kişisel verilerin korunması alt faktöründe ise bu ortalama puanlar arasındaki farklılığın en az olduğu sonucuna ulaşılmıştır.

İlköğretim ve lise öğrencilerinin bilgi ve bilgisayar güvenliği farkındalık düzeyleri ortaya çıkarılmaya çalışılan bir diğer araştırma Tekerek ve Tekerek (2013) tarafından yapılmıştır. Araştırma kapsamında Kahramanmaraş ili, il merkezi, ilçe, kasaba ve köylerinde öğrenim gören 2449 öğrenciye, geliştirilen bilgi ve bilgisayar güvenliği farkındalık ölçeği uygulanmış ve elde edilen veriler istatistik analiz programı kullanılarak değerlendirilmiştir.

Sonuç olarak öğrencilerin etik konulardaki bilgi güvenliği farkındalık düzeylerinin yeterli seviyede olduğu bulunmuştur. Ancak öğrencilerin kurallar ve bilgi gerektiren konularda farkındalık düzeylerinin düşük olduğu gözlenmiştir. Bu da bilgi ve bilgisayar güvenliği farkındalık eğitim ve etkinliklerinin yetersiz kaldığı düşüncesini ortaya çıkarmaktadır. Eğer bu konudaki ilgili derslerin sayısı artırılırsa öğrencilerin bilgi ve bilgisayar güvenliği farkındalıkları arttırılabilir ve bunun sonucunda internetin zararlı etkileri kontrol edilebilir.

Çeliktaş (2016) tarafından yapılan yüksek lisans tezinde siber güvenlikle ilgili Türkiye adına örnek teşkil ettiği düşünülen devletler ve uluslararası örgütlerin hâlihazırdaki durumları, yapmış oldukları çalışmalar, tatbikatlar, siber güvenlik strateji belgeleri, eylem planları incelenmiş, bu sayede ulusal siber güvenlik bilinç ve farkındalık seviyelerinde artış olması amaçlanmıştır.

Teknolojik olarak daha gelişmiş ve e-devlet, e-finans, e-ticaret gibi alanlara daha bağımlı olan ülkelerin kritik altyapı sektörlerinde güvenlik açıkları daha fazla olduğundan siber saldırılara daha fazla maruz kaldıkları görülmüştür.

Karacı vd. (2017) tarafından yapılan araştırmada siber güvenlik, bilgi kaynaklarının korunmasını ve kişinin kendisi de dâhil 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.

Üniversite öğrencilerinin, bilgi güvenliğine yönelik kazanımları ve farkındalıkları belirlenerek, demografik özelliklerine göre farklılık gösterip göstermediği araştırılan, genel güvenlik bilgileri ile farkındalıkları arasındaki ilişkiler incelenen bu araştırma Erdoğmuş (2017) tarafından yapılmıştır.

Afyon Kocatepe Üniversitesi öğrencilerine uygulanan bir anket aracılığı ile derlenen verilerin analiz edilmesi sonucunda, bilgi güvenliği kazanımlarının cinsiyet, yaş ve internet kullanım yıllarına göre, bilgi güvenliği farkındalıklarının ise yaş, bölüm, sınıf ve internet ortamını güvenli bulup bulmamalarına göre anlamlı bir farklılık gösterdiği tespit edilmiştir. Diğer taraftan, kurulan modelden elde edilen sonuçlar bilgi güvenliği farkındalığı üzerinde en fazla etkiye sahip olan alt boyutun "İnternet Güvenliği" olduğunu göstermektedir.

Yapılan araştırmalar incelendiğinde, Türkiye'de siber güvenlik ile ilgili araştırmaların siber güvenlik farkındalıkları, siber mağduriyet ve siber zorbalık, siber suç farkındalığı konularına yöneldiği ve daha çok cinsiyet, internet kullanım süresi, yaş ve eğitim durumu açısından ortaya çıkan farklılıkların incelendiği görülmektedir. Analizler incelendiğinde, siber güvenlik bilgi düzeylerinin yeterli seviyede olduğu sonucuna ulaşılmıştır. Siber güvenlik bilgi düzeylerinin cinsiyete, yaşa, eğitimlerine göre anlamlı bir farklılık gösterdiği ortaya çıkmaktadır. Siber mağduriyetin ise cinsiyete ve yaşa göre farklılık göstermezken, internet kullanım süresine göre farklılık gösterdiği tespit edilmiştir.

3.2. Dünyada Yapılan Araştırmalar

Slusky ve Partow (2012) tarafından yapılan araştırmada, 2011 yılında Los Angeles'ta California Eyalet Üniversitesi İşletme ve Ekonomi Fakültesi öğrencileri arasında bilgi güvenliği anketi uygulanarak öğrencilerin farkındalık düzeyleri ölçülmüştür. Anket sonuçlarına göre, öğrencilerin kullandıkları uygulamaların özelliklerini, bilgisayarda karşılaşabilecekleri riskleri ve bunlara karşı alınabilecek önlemleri bildikleri gözlenmiştir. Farkındalık düzeylerinin yüksek olduğu belirlenmiş ancak ortaya çıkan sorunların bilgi eksikliğinden değil sahip oldukları bu bilgiyi gerçek dünyada kullanamadıklarından kaynaklandığı görülmüştür.

Kim (2013) tarafından yapılan araştırmada, güvenlik zincirinin en zayıf halkası olarak son kullanıcıların görülmesinden hareketle, öğrencilerin bilgi güvenliğini geliştirmek için güvenlik kontrollerini doğru bir şekilde uygulamaları gerektiği belirtilmiş ve bu konudaki bilgi düzeyleri irdelenmiştir. Anket sonuçları, üniversite öğrencilerinin Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) Özel Raporu tarafından önerilen bilgi güvenliği konularının çoğunu anladıklarını göstermektedir. Üniversitelerin, bilgi güvenliği eğitimlerini arttırmaları ve öğrencileri bu eğitimlere katılmaya teşvik etmeleri önerilmektedir.

Öğrencilerin siber zorbalıkla başa çıkmalarının anlaşılmasını amaçlayan bu araştırma Parris vd. (2011) tarafından yapılmıştır. Bu araştırmanın, araştırmacılara ve profesyonellere siber zorbalığın olumsuz etkilerini hafifletme ve önleme yollarını belirleme konusunda fayda sağlayabileceği belirtilmiştir. Niteliksel yöntemler siber zorbalıkla başa çıkmanın derinlemesine incelenmesini sağlamak için kullanılmıştır. Sonuçlar, üç temel başa çıkma yöntemi olduğunu gösteriyor ki bunlar da reaktif başa çıkma, önleyici başa çıkma ve siber zorbalığın önlenmesinin imkansız olduğu şeklindedir. Reaktif başa çıkma, mesajları silerek ya da yok sayarak siber zorbalık durumundan kaçınmayı içerir. Önleyici başa çıkma stratejileri ise şahsen konuşma, güvenlik ve farkındalığı içermektedir. Bazıları da siber zorbalığı azaltmanın yolunun olmadığı görüşlerini bildirdiler. Bu stratejiler yorumlanmış, ortaya çıkan bulgular

bilgi güvenliği eğitiminin arttırılması ve yeni bir model ortaya çıkarma gerekliliğini göstermiştir (Parris vd., 2011).

McCrohan vd. (2010) tarafından yapılan çalışmada, siber tehdit eğitimi ve farkındalık oluşturmanın kullanıcı güvenliği davranışlarındaki değişiklikler üzerindeki etkisini belirlemeye yönelik bir çalışmanın sonuçlarını sunmaktadır. Denekler rastgele, zayıf şifre seçimleri nedeniyle siber tehditlerle ilgili iki tanıtım dersinden birine atanmıştır. Düşük bilgi koşulu, şifreler ve bilgisayar güvenliği ile ilgili yüzeysel bir bilgiler içerirken, yüksek bilgi koşulu kişilerin e-ticaret kullanımına yönelik tehditler hakkında çok ayrıntılı ve özel bilgiler içermektedir. İki hafta boyunca süren çalışmalar sonucunda, düşük bilgi sınıfındaki öğrencilerde güvenli şifre oluşturma konusunda istatistiksel olarak bir fark bulunmadığı tespit edilmiştir. Yüksek bilgi düzeyindeki sınıflarda bulunan öğrencilerde ise %36 oranında daha güçlü şifre oluşturabildikleri gözlenmiştir. Sonuç olarak, kullanıcılar e-ticarete yönelik tehditler konusunda ve uygun güvenlik uygulamaları konusunda eğitildiğinde, kendileri ve istihdam edildikleri şirketler için çevrimiçi güvenliği arttırmak için davranışlarının değiştirilebileceği görülmüştür.

İngiltere'de bir işletme kolejindeki lisans ve lisansüstü eğitim gören öğrencilerin bilgi güvenliği konusundaki tutumlarını incelemek için Kim (2014) tarafından yapılan bir araştırmada uygulanan anket sonuçlarına göre, üniversite öğrencilerinin bilgi güvenliği bilinçlendirme eğitiminin önemini ve ihtiyacını anladıklarını ancak birçoğunun bu eğitimlere katılmadığını göstermiştir. Bilgi güvenliği düzeylerinin düşük olduğu gözlenmekle birlikte bazı konularda bilgi sahibi oldukları ve bunları çok çeşitli web kaynaklarından öğrendikleri anlaşılmaktadır.

North vd. (2006) tarafından ABD'de lise ve üniversite öğrencileri arasında bilgisayar güvenliği ve etik farkındalığı üzerine yapılan çalışmada, ankete bilgisayar teknolojisi kurslarına katılan 465 öğrenci katılmıştır. 21 sorudan oluşan bir anket uygulanmıştır. Anket, katılımcının bilgisayar güvenliği konusundaki farkındalığını ve etik bilgisayar kullanımı farkındalığını ölçmek amacıyla iki bölümden oluşmaktadır. Genel olarak, katılımcıların çoğunluğunun bilgisayar güvenliği ve etik

konusunda tatmin edici bir farkındalığa sahip olduğu görülmüştür. Ancak bilgisayar güvenliği konusunda %20 ile %52 arasında bilinç eksikliği, etik kuralların ihlali konusunda ise %14 ile %24 arasında bir fark ortaya çıkmıştır. Bu sonuçlar, üniversite kullanıcıları için güvenlik ve etik bilinçlendirme eğitiminin gerekli olduğunu göstermektedir.

Dünya genelinde öğrenciler üzerindeki siber güvenlik farkındalık düzeyleri üzerine yapılan çalışmalar incelendiğinde, genellikle siber güvenlik bilgi düzeylerinin yüksek olduğu sonucuna ulaşıldığı görülmektedir. Bilgi güvenliği konusunda eksik olduğu görülen bir araştırmada ise, yine aynı öğrencilerin bilgi güvenliği eğitiminin önemli olduğu görüşünü savundukları tespit edilmiştir. Bu sonuçtan da eğitimleri eksik olsa da farkındalıklarının yüksek olduğu sonucu çıkarılabilir.

BÖLÜM 4

YÖNTEM

4.1. Araştırma Modeli

Araştırmada nicel yöntem kullanılmış olup, nicel boyutu ile araştırmanın modeli tarama modelinde desenlenmiştir. Tarama modeli, araştırmanın konusunun geçmişte ya da halen var olan durumuyla ilgili hipotezleri test etmek ya da soruları cevaplamak için veri toplamayı ya da betimlemeyi sağlayan bir araştırma modelidir (Karasar, 2010). Araştırmanın amaçlarına uygun olarak tarama modellerinden tekil ve ilişkisel tarama modelleri kullanılmıştır.

4.2. Evren ve Örneklem

Araştırmanın evrenini 2017-2018 eğitim öğretim yılı Konya ili Merkez ilçeleri olan Karatay, Selçuklu ve Meram İlçelerinde bulunan ve Bilişim Teknolojileri Alanında 10 ve 12. sınıflarda öğrencisi bulunan Mesleki ve Teknik Anadolu Liseleri oluşturmaktadır. Araştırma kapsamında rastsal olarak her bölgeden 2 okul örnekleme dahil edilmiş ve bu okullardaki öğrencilerden veri toplanmıştır. Katılımcı olarak 10.sınıfların belirlenmesi, öğrencilerin Bilişim Teknolojileri alanını 10.sınıfa geçtiklerinde seçmeleri ve meslek derslerini henüz görmemiş olmalarından kaynaklanmaktadır. 12.sınıf belirlenme sebebi ise, tüm meslek derslerini görmüş olmalarıdır. Araştırmacı tarafından 310 katılımcıdan veri toplanmış olup, 3 adet ölçek yarım bırakıldığı için, 2 adet ölçek tamamı tek bir seçenek olarak işaretlendiği için geçersiz sayılmış ve sonuç olarak 305 adet katılımcının verileri değerlendirilmiştir.

Tablo - 3: Katılımcılara Ait Demografik Bilgiler

Değişkenler	Değerler	n	%
Sınıf	10. sınıf	181	59,3
	12.sınıf	124	40,7
Siber Güvenlik Eğitim Durumu	Aldım	61	20,0
	Almadım	244	80,0
Sosyal Ağ Kullanma Durumu	Kullanıyorum	296	97,0
	Kullanmıyorum	9	3,0
Siber Mağduriyet Yaşama Durumu	Evet	43	14,1
	Hayır	262	85,9
Siber Güvenlik Bilgi Düzeyi	Az	80	26,2
	Orta	195	63,9
	Yüksek	30	9,8
Toplam		305	100

Tablo 3 incelendiğinde, araştırmaya katılan öğrencilerin 181'inin (%59) 10.sınıf, 124'ünün (%41) ise 12.sınıf olduğu görülmektedir. Siber güvenlik eğitim durumları incelendiğinde ise, 244 (%80) katılımcının eğitim almadığı anlaşılmaktadır. Katılımcıların 296'sı (%97), neredeyse tamamı sosyal ağ kullandığını belirtmiştir. Siber mağduriyet yaşama durumları incelendiğinde ise, 43 (%14) katılımcının siber mağduriyet yaşadığını ifade ettiği görülmektedir. Siber güvenlik bilgi düzeyleri açısından ise katılımcıların yarısından fazlasının (%63,9), orta düzeyde bilgiye sahip olduğunu belirttiği anlaşılmaktadır. Yine aynı konuda katılımcıların sadece %9'u yüksek düzeyde bilgi sahibi olduğunu belirtmiştir.

4.3. Veri Toplama Aracı ve Verilerin Toplanması

Araştırmada veri toplamak amacı ile (Erol vd., 2015) tarafından geliştirilen Kişisel Siber Güvenliği Sağlama Ölçeği kullanılmıştır (Ek-1). 810 kullanıcı ile geliştirilen ölçekte 25 madde yer alıp, bu maddeler 5 faktörlü bir yapıya sahiptir. Ölçeğin güvenirliği için Cronbach Alpha değeri .735 olarak hesaplanmıştır.

4.4. Verilerin Analizi

Verilerin bilgisayara aktarılmasında kişisel siber güvenlik sağlama ölçeğindeki maddeler "1-Hiçbir Zaman", "2-Nadiren", "3-Ara Sıra", "4-Sık Sık" ve "5-Her Zaman" olacak şekilde puanlanmıştır. Ters madde olduğu belirtilen 5, 7, 12, 13, 17, 18, 19, 20, 24, 25 numaralı maddeler tersten puanlanmıştır. Öğrencilerin kişisel siber güvenliği sağlama düzeylerine yönelik görüşlerini yorumlamak için n (alınabilecek en yüksek değer – alınabilecek en küçük değer) / değerlendirme aralığı ((7 – 1) / 3) formülü uygulanarak aşağıdaki şekilde bir değerlendirme koşulları belirlenmiştir (Tablo 4).

Tablo-4: Öğrencilerin Kişisel Siber Güvenliklerini Sağlama Düzeylerini Değerlendirme Ölçütleri

Değerlendirme Aralığı	Değerlendirme Kriteri
1.00 – 2.33	Düşük
2.34 – 3.66	Orta
3.67 – 5.00	Yüksek

Verilerin analizinde betimsel istatistiklerden (aritmetik ortalama, standart sapma, yüzde, frekans) ek olarak, siber güvenliğe yönelik eğitim alma, sınıf düzeyi, sosyal ağ kullanma ve siber güvenlik konusunda mağduriyet yaşama değişkenlerine göre farklılıkları belirlemek için bağımsız örneklem t testi kullanılmıştır. Siber güvenlik yeterlik düzeyine göre öğrencilerin kişisel siber güvenlik bilgi düzeylerini incelemek için de tek yönlü varyans analizi (ANOVA) yapılmıştır. Hangi gruplar arasında farklılık olduğunu belirlemek amacıyla post hoc testlerinden yararlanılmış, grupların homojenliği sağlaması durumunda ($p>.05$) post hoc testlerinden Scheffe testi, homojenliği sağlamaması durumunda ($p<.05$) ise post hoc testlerinden Dunnett C gruplar arasındaki farklılığı belirlemek amaçlı kullanılmıştır.

Tüm verilerin analizlerinde istatistiksel çözümlemelerde SPSS 22.0 (Statistical Package fort he Social Sciences) paket programından yararlanılmış, anlamlılık düzeyi .05 olarak alınmıştır.

BÖLÜM 5

BULGULAR VE YORUMLAR

Mesleki ve Teknik Anadolu Liselerinin Bilişim Teknolojileri alanında eğitim gören öğrencilerin kişisel siber güvenliğe yönelik bilgi düzeylerinin ve bu bilgi düzeyinin sınıf, siber güvenlik eğitimi, sosyal ağ kullanma, siber mağduriyet yaşama ve kişisel siber güvenlik bilgi düzeylerine göre farklılıklarının araştırıldığı bu çalışmadan elde edilen bulgular başlıklar halinde verilmiştir.

5.1. Öğrencilerin Kişisel Siber Güvenliğe Yönelik Bilgi Düzeyleri

Öğrencilerin kişisel siber güvenliğe yönelik bilgi düzeylerini öğrenmek için katılımcılardan ölçek formu ile veri toplanmıştır. 305 öğrenciden elde edilen verilerin analiz sonuçları aşağıda verilmiştir (Tablo 5).

Tablo- 5: Öğrencilerin Kişisel Siber Güvenliğe Yönelik Bilgi Düzeyleri

Sıra No	Madde ve Faktör	$\bar{X}$	ss	Durum
1	İnternet şifrelerimin tümünün aynı olmasına dikkat ederim	3,02	1,419	Orta
2	E- posta ile gelen kimlik doğrulama mesajlarını (kullanıcı adı, şifre vb. istekler) cevaplarım	2,92	1,495	Orta
3	Tanımadığım kişiler ile web kamerası kullanarak sesli ve görüntülü iletişim kurarım	4,28	1,214	Yüksek
4	İnternet ortamında gerektiğinde kişisel bilgilerimi (TC No,Doğum tarihi,Gsm No vb.)paylaşırım	4,19	1,116	Yüksek
5	Tanımadığım kişilerden gelen e-posta eklerini açarım	3,97	1,155	Yüksek
6	Sosyal paylaşım sitelerinde kişisel bilgilerime yer veririm	3,77	1,075	Yüksek
7	İnternet üzerinden yer bildirimi yaparım	3,58	1,236	Orta
8	Sosyal ağlarda yer alan reklamlar üzerinden alışveriş yaparım	4,34	,974	Yüksek
9	Unutmamak için akılda kalan kolay bir şifre belirlerim	3,59	1,478	Orta
10	Banka, online alışveriş sitesi gibi sitelerden gelen e postalara (kart numarası, şifre vb. istekler) itibar ederim ve yanıtlarım	4,14	1,214	Yüksek
Faktör 1: Kişisel Gizliliği Koruma		**3,77**	**0,574**	**Yüksek**
11	İnternet üzerinden yapılan para ve kontör isteklerini dikkate almam.	3,80	1,532	Yüksek
12	Tanımadığım kişilerden gelen sosyal ağ arkadaşlık isteğini kabul etmem.	3,18	1,430	Orta
13	Güvenmediğim sitelere üye olmam	3,87	1,473	Yüksek
14	Güvenmediğim sitelerden dosya indirmem	3,62	1,493	Orta

Faktör2: Güvenilmeyenden Kaçınma		**3,61**	**0,997**	**Orta**
15	Web sayfalarında güvenlik bağlantılarını (https://) ve sertifikalarını kontrol ederim	2,85	1,317	Orta
16	Kullandığım yazılımları güncellerim.	3,77	1,192	Yüksek
17	Bilgisayarımda antivirus yazılımı bulundururum	3,64	1,485	Orta
18	Şifrelerimi belirlerken basit dizilimler kullanmaktan kaçınırım	4,18	1,154	Yüksek
19	Web tarayıcımın güvenlik ayarlarını düzenlerim	2,90	1,309	Orta
Faktör3: Önlem Alma		**3,46**	**0,852**	**Orta**
20	İnternet bankacılığı işlemlerini şahsi bilgisayarımdan yaparım.	3,17	1,644	Orta
21	Online alışveriş işlemlerini şahsi bilgisayarımdan yaparım	3,76	1,421	Yüksek
Faktör4: Ödeme Bilgilerini Koruma		**3,46**	**1,344**	**Orta**
22	Şahsi bilgisayarım dışında kullanılan bilgisayarlarda bilgilerimin kalmamasına dikkat ederim	4,55	0,920	Yüksek
23	Web geçmişimi temizlerim	3,77	1,247	Yüksek
24	Sosyal ağ - e-posta gibi hesaplarda işim bittiğinde oturumu kapatırım	3,49	1,426	Orta
25	İnternette kullandığım (eposta, sosyal ağ vb.)şifreleri değiştiririm	3,36	1,233	Orta
Faktör5: İz Bırakmama		**3,79**	**0,733**	**Yüksek**
GENEL SİBER GÜVENLİK BİLGİ DÜZEY ORTALAMASI		**3,66**	**0,458**	**Orta**

Tablo 5 incelendiğinde, öğrencilerin genel siber güvenlik bilgi düzeylerinin orta seviyede ($\overline{X}$=3.66) olduğu belirlenmiştir. Kişisel gizliliği koruma boyutunda bilgi düzeylerinin yüksek olduğu ($\overline{X}$=3.77) görülmektedir. Bu faktörün maddeleri incelendiğinde, internette kullandığı şifrelerin tümünün aynı olmaması($\overline{X}$=3.02), e-posta ile gelen kimlik doğrulama mesajlarını cevaplamama ($\overline{X}$=2.92), internet üzerinden yer bildirimi yapmama ($\overline{X}$=3.58), akılda kalması için kolay şifre kullanmama ($\overline{X}$=3.59) konularında bilgi düzeylerinin orta seviyede olduğu görülmüştür. Bu faktörün diğer maddelerinde bilgi düzeylerinin yüksek olduğu belirlenmiştir.

Öğrencilerin güvenilmeyenden kaçınma boyutunda bilgi düzeylerinin orta seviyede olduğu ($\overline{X}$=3.61) görülmektedir. Bu faktörün maddeleri incelendiğinde ise, internet üzerinden para ve kontör isteklerini dikkate almama ($\overline{X}$=3.80) ve güvenmedikleri sitelere üye olmama ($\overline{X}$=3.87) konularında bilgi düzeylerinin yüksek

olduğu tespit edilmiştir. Faktörün diğer maddelerinde ise orta düzeyde bilgi sahibi oldukları anlaşılmaktadır.

Ölçeğin bir diğer faktörü olan önlem alma boyutunda ise ($\overline{X}$=3.46), bilgi düzeylerinin orta seviyede oldukları görülmektedir. Bu faktörün alt maddelerine bakıldığında ise, kullandıkları yazılımları güncelleme ($\overline{X}$=3.77) ve şifre belirlerken basit dizilimler kullanmaktan kaçınma ($\overline{X}$=4.18) konularında yüksek bilgi düzeyinde oldukları belirlenmiştir. Faktörün diğer maddelerinde orta seviyede bir bilgi düzeyine sahip oldukları görülmektedir.

Öğrencilerin ödeme bilgilerini koruma boyutunda ($\overline{X}$=3.46) orta düzeyde bilgi sahibi oldukları ortaya çıkmıştır. Alt maddeler incelendiğinde, online alışveriş için şahsi bilgisayarlarını tercih etme konusunda ($\overline{X}$=3.76) bilgi düzeylerinin yüksek olduğu gözlenmektedir.

Son olarak iz bırakmama boyutunda öğrenciler ($\overline{X}$=3.79) yüksek bilgi düzeyine sahip oldukları görülmektedir. Bu faktörün maddelerine bakıldığında ise, sosyal ağ veya e-posta gibi hesaplarda işleri bittiklerinde oturum kapatma ($\overline{X}$=3.49) ve internette kullandıkları şifreleri değiştirme ($\overline{X}$=3.36) konularında orta seviyede bilgi düzeylerinin olduğu belirlenmiştir. Faktörün diğer maddelerinde bilgi düzeylerinin yüksek olduğu gözlenmektedir.

5.2. Farklı Değişkenler Açısından Öğrencilerin Kişisel Siber Güvenliğe Yönelik Bilgi Düzeyleri

Öğrencilerin kişisel siber güvenliğe yönelik bilgi düzeyleri sınıf, siber güvenlik eğitimi, siber mağduriyet yaşama durumu, kişisel siber güvenlik bilgi düzeyi değişkenlerine göre incelenmiştir. Her değişken açısından sonuçlar başlıklar halinde verilmiştir.

5.2.1. Eğitim Alma Durumlarına Göre Öğrencilerin Kişisel Siber Güvenlik Bilgi Düzeyleri

Katılımcıların siber güvenlik eğitimi alma durumlarının kişisel siber güvenliğe yönelik bilgi düzeylerine etkisi aşağıdaki tabloda istatistiki olarak verilmektedir (Tablo 6).

Tablo - 6: Eğitim Alma Durumlarına Göre Öğrencilerin Kişisel Siber Güvenlik Bilgi Düzeyleri

Faktörler	Eğitim Alma Durumu	N	$\bar{X}$	Ss	Sd	t	p
Kişisel Gizliliği Koruma	Aldım	61	3,83	0,592	303	0,469	0,365
	Almadım	244	3,76	0,570			
Güvenilmeyenden Kaçınma	Aldım	61	3,61	1,019	303	0,021	0,983
	Almadım	244	3,61	0,994			
Önlem Alma	Aldım	61	3,75	0,871	303	3,006	0,003*
	Almadım	244	3,39	0,834			
Ödeme Bilgilerini Koruma	Aldım	61	3,49	1,406	303	0,181	0,857
	Almadım	244	3,45	1,331			
İz Bırakmama	Aldım	61	3,93	0,784	303	1,762	0,079
	Almadım	244	3,75	0,717			
Genel Siber Güvenlik Bilgi Düzey Ortalaması	Aldım	61	3,77	0,524	303	2,067	0,040*
	Almadım	244	3,64	0,438			

* p<.05

Tablo 6 incelendiğinde, öğrencilerin siber güvenlik eğitimi alma durumlarına göre genel siber güvenlik bilgi düzeylerinde ($t_{(303)}$=2.067; p<.05) anlamlı bir farklılık görülmektedir. Bu analizden yola çıkarak, siber güvenlik eğitimi alan öğrencilerin ($\bar{X}$=3.77) genel siber güvenlik bilgi düzeylerinin, almayan öğrencilere göre ($\bar{X}$=3.64) daha yüksek olduğu söylenebilir.

Tablo 6'daki veriler incelendiğinde, katılımcıların siber güvenlik eğitimi alma durumlarına göre önlem alma boyutunda ($t_{(303)}$=3.006; p<.05), anlamlı bir farklılık görülmektedir. Bu sonuca göre, siber güvenlik eğitimi alan bireylerin önlem alma konusunda ($\bar{X}$=3.75), eğitim almayanlara göre ($\bar{X}$=3.39) daha yüksek bilgi düzeyine sahip oldukları belirlenmiştir.

Bununla birlikte, öğrencilerin siber güvenlik eğitimi alma durumlarına göre, kişisel gizliliği koruma ($t_{(303)}$=0.469; p>.05), güvenilmeyenden kaçınma ($t_{(303)}$=0.021; p>.05), ödeme bilgilerini koruma ($t_{(303)}$=0.181; p>.05) ve iz bırakmama ($t_{(303)}$=1.762; p>.05) boyutlarında anlamlı bir farklılık görülmemektedir.

5.2.2. Sınıf Düzeylerine Göre Öğrencilerin Kişisel Siber Güvenlik Bilgi Düzeyleri

Katılımcıların sınıf düzeylerinin kişisel siber güvenlik bilgi düzeylerine etkisi tüm faktörler açısından incelenmiş ve ortaya çıkan veriler Tablo 7'de gösterilmiştir.

Tablo - 7: Sınıf Düzeylerine Göre Öğrencilerin Kişisel Siber Güvenlik Bilgi Düzeyleri

Faktörler	Sınıf Düzeyi	N	$\bar{X}$	Ss	Sd	t	p
Kişisel Gizliliği Koruma	10. sınıf	181	3,79	0,565	303	,726	,469
	12.sınıf	124	3,75	0,588			
Güvenilmeyenden Kaçınma	10. sınıf	181	3,53	0,967	303	-1,708	,089
	12.sınıf	124	3,73	1,032			
Önlem Alma	10. sınıf	181	3,41	0,887	303	-1,345	,180
	12.sınıf	124	3,54	0,796			
Ödeme Bilgilerini Koruma	10. sınıf	181	3,34	1,362	303	-1,913	,057
	12.sınıf	124	3,64	1,302			
İz Bırakmama	10. sınıf	181	3,81	0,721	303	,687	,492
	12.sınıf	124	3,75	0,753			
Genel Siber Güvenlik Bilgi Düzey Ortalaması	10. sınıf	181	3,64	0,456	303	-,998	,319
	12.sınıf	124	3,69	0,462			

* p<.05

Tablo 7 incelendiğinde, öğrencilerin sınıf düzeylerine göre genel siber güvenlik bilgi düzeylerinde ($t_{(303)}$=-0.998; p>.05) anlamlı bir farklılık görülmemiştir. Kişisel gizliliği koruma boyutunda 10.sınıf düzeyinde bulunan öğrencilerin ortalama puanları ($\bar{X}$=3.79) ile 12.sınıf düzeyinde bulunan öğrencilerin ortalama puanları ($\bar{X}$=3.75) arasında istatistiki olarak anlamlı bir fark yoktur. Güvenilmeyenden kaçınma boyutunda ise 10.sınıf düzeyinde bulunan öğrencilerin ortalama puanları $\bar{X}$=3.53 iken, 12.sınıf düzeyinde bulunan öğrencilerin ortalama puanları $\bar{X}$=3.73 olup

anlamlı bir fark görülmemektedir. Önlem alma boyutunda, 10.sınıf düzeyinde bulunan öğrencilerin ortalama puanları ($\overline{X}$=3.41) ile 12.sınıf düzeyinde bulunan öğrencilerin ortalama puanları ($\overline{X}$=3.54) arasında anlamlı bir fark yoktur. Ödeme bilgilerini koruma boyutunda, 10.sınıf düzeyindeki öğrencilerin ortalama puanları $\overline{X}$=3.34 iken, 12.sınıf düzeyindeki öğrencilerin ortalama puanları $\overline{X}$=3.64 olup aralarında anlamlı bir fark bulunmamaktadır. İz bırakmama boyutunda, 10.sınıf düzeyindeki öğrencilerin ortalama puanları ($\overline{X}$=3.81) ile 12.sınıf düzeyinde bulunan öğrencilerin ortalama puanları ($\overline{X}$=3.75) istatistiksel olarak farklılaşmamaktadır.

Bu analizden yola çıkarak, öğrencilerin Bilişim Teknolojileri alanını seçmiş oldukları 10.sınıftan itibaren 12.sınıfa kadar almış oldukları meslek derslerinin genel siber güvenlik bilgi düzeylerine anlamlı bir etkisinden söz edilememektedir.

5.2.3. Siber Mağduriyet Yaşama Durumlarına Göre Öğrencilerin Kişisel Siber Güvenlik Bilgi Düzeyleri

Öğrencilerin siber mağduriyet yaşama durumlarına göre kişisel siber güvenlik düzeylerine etkisi incelenmiş ve ortaya çıkan bulgular Tablo 8'de verilmektedir.

Tablo - 8: Siber Mağduriyet Yaşama Durumlarına Göre Öğrencilerin Kişisel Siber Güvenlik Bilgi Düzeyleri

Faktörler	Siber Mağduriyet	N	$\overline{X}$	Ss	Sd	t	p
Kişisel Gizliliği Koruma	Yaşadım	43	3,63	0,673	303	0,726	,469
	Yaşamadım	262	3,80	0,554			
Güvenilmeyenden Kaçınma	Yaşadım	43	3,55	0,891	303	-1,708	,089
	Yaşamadım	262	3,62	1,015			
Önlem Alma	Yaşadım	43	3,43	0,766	303	-1,345	,180
	Yaşamadım	262	3,47	0,867			
Ödeme Bilgilerini Koruma	Yaşadım	43	3,89	1,232	303	-1,913	,057
	Yaşamadım	262	3,39	1,351			
İz Bırakmama	Yaşadım	43	3,86	0,705	303	0,687	,492
	Yaşamadım	262	3,77	0,738			
Genel Siber Güvenlik Bilgi Düzey Ortalaması	Yaşadım	43	3,64	0,492	303	-0,998	,319
	Yaşamadım	262	3,67	0,453			

* p<.05

Tablo 8 incelendiğinde, öğrencilerin siber mağduriyet yaşama durumlarına göre genel siber güvenlik bilgi düzeylerinde ($t_{(303)}$= -0.998; p>.05) anlamlı bir farklılık görülmemektedir. Kişisel gizliliği koruma boyutunda, siber mağduriyet yaşayan öğrencilerin ortalama puanları ($\overline{X}$=3.63) ile yaşamayan öğrencilerin ortalama puanları ($\overline{X}$=3.80) arasında anlamlı bir fark bulunmamaktadır. Güvenilmeyenden kaçınma boyutunda ise, siber mağduriyet yaşayan öğrencilerin ortalama puanları $\overline{X}$=3.55 iken, yaşamayan öğrencilerin ortalama puanları $\overline{X}$=3.62 olup aralarında istatistiksel olarak bir fark görülememektedir. Önlem alma boyutunda, siber mağduriyet yaşayan öğrencilerin ortalama puanları $\overline{X}$=3.43 iken, yaşamayan öğrencilerin ortalama puanları $\overline{X}$=3.47 olup anlamlı bir farktan söz edilememektedir. Ödeme bilgilerini koruma boyutunda ise, siber mağduriyet yaşayan öğrencilerin ortalama puanları ($\overline{X}$=3.89) ile yaşamayan öğrencilerin ortalama puanları ($\overline{X}$=3.39) arasında anlamlı bir fark bulunmamaktadır. Son olarak iz bırakmama boyutunda, siber mağduriyet yaşayan öğrencilerin ortalama puanları $\overline{X}$=3.86 olarak belirlenmiştir. Siber mağduriyet yaşamayan öğrencilerin ortalama puanları ise $\overline{X}$=3.77 'dir. Bu değerler karşılaştırıldığında anlamlı bir fark görülmemektedir.

Sonuç olarak Tablo-8'e göre, genel siber güvenlik bilgi düzeyinde, siber mağduriyet yaşayan öğrenciler ($\overline{X}$=3.64) ile yaşamayan öğrenciler ($\overline{X}$=3.67) arasında anlamlı bir farktan söz edilememektedir. Dolayısıyla siber mağduriyet yaşama durumlarının, bireylerin kişisel siber güvenlik bilgi düzeylerine anlamlı bir etkisi görülmemektedir.

5.2.4. Siber Güvenlik Yeterlik Düzeyine Göre Öğrencilerin Kişisel Siber Güvenlik Bilgi Düzeyleri

Öğrencilerin kişisel siber güvenlik yeterlik düzeylerinin, genel siber güvenlik bilgi düzeylerini etkileyip etkilemediğini belirlemek amacıyla kişisel siber güvenlik yeterlik seviyelerine göre gruplama yapılmıştır. Bu gruplamada 3 adet kişisel siber güvenlik yeterlik düzeyi belirlenmiş ve tek yönlü varyans analizine (ANOVA) uygun hale getirilmiştir (Tablo 9).

Tablo-9: Siber Güvenlik Yeterlik Düzeyine Göre Öğrencilerin Kişisel Siber Güvenlik Bilgi Düzeyleri

	Yabancı Dil Düzeyi	N	$\bar{X}$	Ss
Kişisel Gizliliği Koruma	A-Az	80	3,79	0,585
	B-Orta	195	3,77	0,563
	C-Yüksek	30	3,79	0,633
Güvenilmeyenden Kaçınma	A-Az	80	3,43	1,102
	B-Orta	195	3,68	0,952
	C-Yüksek	30	3,64	0,964
Önlem Alma	A-Az	80	3,09	0,769
	B-Orta	195	3,50	0,840
	C-Yüksek	30	4,19	0,593
Ödeme Bilgilerini Koruma	A-Az	80	2,96	1,320
	B-Orta	195	3,51	1,323
	C-Yüksek	30	4,45	0,884
İz Bırakmama	A-Az	80	3,62	0,768
	B-Orta	195	3,79	0,702
	C-Yüksek	30	4,21	0,687
Genel Siber Güvenlik Bilgi Düzeyi	A-Az	80	3,50	0,461
	B-Orta	195	3,68	0,423
	C-Yüksek	30	3,96	0,507

Tablo 9'dan görüleceği üzere, öğrencilerin genel siber güvenlik bilgi düzeylerine yönelik görüşleri, kişisel siber güvenlik yeterlik seviyelerinden etkilendiği, kişisel siber güvenlik yeterlik seviyesi arttıkça, öğrencilerin genel siber güvenlik bilgi düzeyi de artmaktadır. Öğrencilerin kendilerinin sahip olduğunu düşündüğü ve ölçekte az, orta, yüksek şeklinde görüş belirttikleri kişisel siber güvenlik farkındalık düzeylerinin genel siber güvenlik bilgi düzeylerini etkilediği görülmektedir.

Fakat gruplar arasındaki farklılığı belirlemek için tek yönlü varyans analizi (ANOVA) işlemi gerçekleştirilmiştir (Tablo 10).

Tablo - 10: Öğrencilerin Genel Siber Güvenlik Bilgi Düzeyleri İle Kişisel Siber Güvenlik Bilgi Seviyesi Arasındaki Farklılığa Yönelik Analiz Sonuçları

	Varyansın Kaynağı	Kareler Toplamı	Sd	Kareler Ort.	F	p	Fark
Kişisel Gizliliği Koruma	Gruplararası	.030	2	.015	.045	.956	-
	Gruplariçi	100.324	302	.332			
	Toplam	100.354	304				
Güvenilmeyenden Kaçınma	Gruplararası	3,774	2	1,887	1,908	,150	-
	Gruplariçi	298,719	302	,989			
	Toplam	302,493	304				
Önlem Alma	Gruplararası	27,072	2	13,536	21,065	,000	A-B, A-C, B-C
	Gruplariçi	194,057	302	,643			
	Toplam	221,129	304				
Ödeme Bilgilerini Koruma	Gruplararası	49,303	2	24,651	14,880	,000	A-B, A-C, B-C
	Gruplariçi	500,301	302	1,657			
	Toplam	549,603	304				
İz Bırakmama	Gruplararası	7,558	2	3,779	7,308	,001	A-C, B-C
	Gruplariçi	156,179	302	,517			
	Toplam	163,738	304				
Genel Siber Güvenlik Bilgi Düzeyi	Gruplararası	4,935	2	2,467	12,609	,000	A-B, A-C, B-C
	Gruplariçi	59,093	302	,196			
	Toplam	64,027	304				

Tablo 10'daki veriler doğrultusunda öğrencilerin genel siber güvenlik bilgi düzeyleri ile kişisel siber güvenlik bilgi seviyeleri arasında istatistiksel olarak anlamlı bir fark bulunduğu ifade edilebilir ($F_{(2-302)}$=12.609, p<.05). Önlem alma boyutu ile kişisel siber güvenlik bilgi seviyeleri arasında da anlamlı bir fark bulunmaktadır ($F_{(2-302)}$ = 21.065, p<.05). Benzer şekilde ödeme bilgilerini koruma boyutu ile kişisel siber güvenlik bilgi seviyeleri karşılaştırıldığında da anlamlı bir fark oluştuğu gözlenmektedir ($F_{(2-302)}$ = 14.880, p<.05). Son olarak iz bırakmama boyutu ile kişisel siber güvenlik bilgi seviyeleri arasında da yine aynı şekilde anlamlı bir fark bulunmaktadır ($F_{(2-302)}$ = 7.308).

Bununla birlikte kişisel gizliliği koruma boyutu ile kişisel siber güvenlik bilgi seviyeleri karşılaştırıldığında anlamlı bir farklılık bulunmadığı görülmektedir ($F_{(2-302)}$ = 0.045, p>.05). Güvenilmeyenden kaçınma boyutu ile kişisel siber güvenlik bilgi seviyeleri arasında da anlamlı bir farklılık gözlenmemiştir ($F_{(2-302)}$ = 1.908, p>.05).

Bu sonuçlar yorumlandığında, öğrencilerin kişisel siber güvenlik bilgi seviyelerine göre kişisel gizliliği koruma ve güvenilmeyenden kaçınma açısından istatistiksel olarak anlamlı bir fark bulunmadığı söylenebilir.

Çoklu karşılaştırma testlerinden Scheffe testi ile yapılan analiz sonuçlarına göre, genel siber güvenlik bilgi düzeyinde kişisel siber güvenlik bilgi seviyeleri bakımından az ve orta düzey grupları arasında farklılık olduğu görülmektedir. Bir başka ifadeyle, kişisel siber güvenlik bilgi seviyeleri az olan öğrenciler ($\overline{X}$=3.50) ile orta düzeyde olan öğrenciler ($\overline{X}$=3.68) arasında anlamlı derecede farklılık oluşmaktadır. Yine genel siber güvenlik bilgi düzeyinde kişisel siber güvenlik bilgi seviyeleri açısından az ile yüksek düzey grupları arasında da anlamlı bir farklılık görülmektedir. Farklı bir şekilde ifade etmek gerekirse, kişisel siber güvenlik bilgi seviyeleri az olan öğrenciler ($\overline{X}$=3.50) ile yüksek düzeyde olan öğrenciler ($\overline{X}$=3.96) arasında anlamlı bir fark bulunmaktadır. Son olarak genel siber güvenlik bilgi düzeyinde kişisel siber güvenlik bilgi seviyeleri açısından orta ile yüksek düzey grupları arasında da anlamlı bir farklılık görülmektedir. Bir başka deyişle, kişisel siber güvenlik bilgi seviyeleri orta düzeyde olan öğrenciler ($\overline{X}$=3.68) ile yüksek düzeyde olan öğrenciler ($\overline{X}$=3.96) arasında anlamlı bir fark bulunmaktadır. Bu sonuçlar yorumlandığında, öğrencilerin kişisel siber güvenlik bilgi seviyesi arttıkça genel siber güvenlik bilgi düzeylerinde anlamlı bir artış olduğu görülmektedir.

Önlem alma boyutunda kişisel siber güvenlik bilgi seviyeleri bakımından az ve orta düzey grupları arasında farklılık olduğu görülmektedir. Bir başka ifadeyle, kişisel siber güvenlik bilgi seviyeleri az olan öğrenciler ($\overline{X}$=3.09) ile orta düzeyde olan öğrenciler ($\overline{X}$=3.64) arasında anlamlı derecede farklılık oluşmaktadır. Yine önlem alma boyutunda kişisel siber güvenlik bilgi seviyeleri açısından az ile yüksek düzey grupları arasında da anlamlı bir farklılık görülmektedir. Farklı bir şekilde ifade etmek gerekirse, kişisel siber güvenlik bilgi seviyeleri az olan öğrenciler ($\overline{X}$=3.09) ile yüksek düzeyde olan öğrenciler ($\overline{X}$=4.19) arasında anlamlı bir fark bulunmaktadır. Son olarak önlem alma boyutunda kişisel siber güvenlik bilgi seviyeleri açısından orta ile yüksek düzey grupları arasında da anlamlı bir farklılık görülmektedir. Bir

başka deyişle, kişisel siber güvenlik bilgi seviyeleri orta düzeyde olan öğrenciler ($\overline{X}$=3.64) ile yüksek düzeyde olan öğrenciler ($\overline{X}$=4.19) arasında anlamlı bir fark bulunmaktadır. Bu sonuçlar yorumlandığında, öğrencilerin kişisel siber güvenlik bilgi seviyesi arttıkça önlem alma bakımından genel siber güvenlik bilgi düzeylerinde anlamlı bir artış olduğu görülmektedir.

Ödeme bilgilerini koruma boyutunda kişisel siber güvenlik bilgi seviyeleri az ve orta düzey grupları arasında farklılık olduğu görülmektedir. Bir başka ifadeyle, kişisel siber güvenlik bilgi seviyeleri az olan öğrenciler ($\overline{X}$=2.96) ile orta düzeyde olan öğrenciler ($\overline{X}$=3.51) arasında anlamlı derecede farklılık oluşmaktadır. Yine ödeme bilgilerini koruma boyutunda kişisel siber güvenlik bilgi seviyeleri açısından az ile yüksek düzey grupları arasında da anlamlı bir farklılık görülmektedir. Farklı bir şekilde ifade etmek gerekirse, kişisel siber güvenlik bilgi seviyeleri az olan öğrenciler ($\overline{X}$=2.96) ile yüksek düzeyde olan öğrenciler ($\overline{X}$=4.45) arasında anlamlı bir fark bulunmaktadır. Son olarak ödeme bilgilerini koruma boyutunda kişisel siber güvenlik bilgi seviyeleri açısından orta ile yüksek düzey grupları arasında da anlamlı bir farklılık görülmektedir. Bir başka deyişle, kişisel siber güvenlik bilgi seviyeleri orta düzeyde olan öğrenciler ($\overline{X}$=3.51) ile yüksek düzeyde olan öğrenciler ($\overline{X}$=4.45) arasında anlamlı bir fark bulunmaktadır. Bu sonuçlar yorumlandığında, öğrencilerin kişisel siber güvenlik bilgi seviyesi arttıkça ödeme bilgilerini koruma bakımından genel siber güvenlik bilgi düzeylerinde anlamlı bir artış olduğu görülmektedir.

İz bırakmama boyutunda kişisel siber güvenlik bilgi seviyeleri az ve yüksek düzey grupları arasında farklılık olduğu görülmektedir. Bir başka ifadeyle, kişisel siber güvenlik bilgi seviyeleri az olan öğrenciler ($\overline{X}$=3.62) ile yüksek düzeyde olan öğrenciler ($\overline{X}$=4.21) arasında anlamlı derecede farklılık oluşmaktadır. Yine ödeme bilgilerini koruma boyutunda kişisel siber güvenlik bilgi seviyeleri açısından orta ile yüksek düzey grupları arasında da anlamlı bir farklılık görülmektedir. Farklı bir şekilde ifade etmek gerekirse, kişisel siber güvenlik bilgi seviyeleri orta düzeyde olan öğrenciler ($\overline{X}$=3.79) ile yüksek düzeyde olan öğrenciler ($\overline{X}$=4.21) arasında anlamlı bir fark bulunmaktadır. Bu sonuçlar yorumlandığında, öğrencilerin kişisel

siber güvenlik bilgi seviyesi arttıkça iz bırakmama bakımından genel siber güvenlik bilgi düzeylerinde anlamlı bir artış olduğu görülmektedir.

BÖLÜM 6

SONUÇLAR VE TARTIŞMA

Bu çalışmada, meslek liselerinin Bilişim Teknolojileri alanında eğitim gören öğrencilerin siber güvenliğe yönelik bilgi düzeylerinin belirlenmesi amaçlanmıştır. Öğrencilerin eğitim alma durumları, sınıf düzeyleri, siber mağduriyet yaşama durumları ve siber güvenlik yeterlilik düzeyleri açısından siber güvenliğe yönelik bilgi düzeyleri incelenmiştir. Bu konuyla ilgili veri toplamak amacıyla Erol vd. (2015) tarafından geliştirilen Kişisel Siber Güvenliği Sağlama Ölçeği kullanılmıştır. Kişisel gizliliği koruma, güvenilmeyenden kaçınma, önlem alma, ödeme bilgilerini koruma ve iz bırakmama faktörleri bakımından siber güvenlik bilgi düzeyleri araştırılmıştır.

Bu amaçla, Konya ili Meram, Selçuklu ve Karatay merkez ilçelerindeki meslek liselerinin Bilişim Teknolojileri alanındaki 305 öğrenciden veri toplanmıştır.

Bu ölçekteki sınırlar çerçevesinde öğrencilerin soruları anlayarak doğru cevaplar verdikleri varsayılmıştır. Elde edilen bulgular, Bilişim Teknolojileri alanında verilen eğitimlerin siber güvenlik bilgi düzeylerine olan etkisi hakkında bize bilgi vermektedir. Böylelikle, öğrencilerin kişisel siber güvenliklerini arttırabilmek için atılabilecek adımlar, verilebilecek eğitimler ile ilgili bireysel ve devlet nezdinde fikir edinilmektedir.

Sonuçlar analiz edildiğinde, öğrencilerin genel siber güvenlik bilgi düzeylerinin orta seviyede olduğu ortaya çıkmıştır. Tekerek ve Tekerek (2013) tarafından ilköğretim ve lise öğrencilerinin bilgi ve bilgisayar güvenliği farkındalık düzeyleri üzerine yapılan çalışmada, öğrencilerin bilgi güvenliği farkındalık düzeylerinin yeterli seviyede olduğu bulunmuştur. Bu çıkarımın bizim yaptığımız çıkarımla aynı doğrultuda olduğu görülmektedir. Alt boyutlar açısından incelendiğinde, güvenilmeyenden kaçınma, önlem alma ve ödeme bilgilerini koruma boyutunda orta düzeyde bilgi sahibi oldukları görülmektedir. Kişisel gizliliği koruma

ve iz bırakmama boyutunda ise yüksek düzeyde bilgi sahibi oldukları tespit edilmiştir.

Siber güvenlik eğitimi alma durumları açısından bulgular analiz edildiğinde, çalışmaya katılan 305 öğrenciden 61 öğrencinin (%20) siber güvenlik eğitimi aldıkları görülmektedir. Siber güvenlik eğitimi alan öğrencilerin, genel siber güvenlik bilgi düzeylerinin almayan öğrencilere göre daha yüksek olduğu sonucuna ulaşılmıştır. Şahinaslan vd. (2009) tarafından bilgi güvenliği farkındalık eğitimi ile ilgili yapılan çalışmada, bireylere yapılacak bilgi güvenlik bilinçlendirme faaliyetlerinin bilgi güvenliği sağlamada çok büyük katkılar sağlayacağı sonucu da bu çıkarımı desteklemektedir. Öğütçü (2010) tarafından yapılan çalışmada, güvenlik eğitimi alan grubun korumacı davranış puanı güvenlik eğitim almayan gruptan daha yüksek olduğu, dolayısıyla açıkça eğitimin bireylerde farkındalığı arttırdığını gösterdiği sonucuna ulaşılmıştır. Bu sonucunda bizim sonuçla aynı doğrultuda olduğu görülmektedir. Yayla (2018) tarafından öğretmenlerin bilgi güvenliği farkındalığının incelenmesi ile ilgili yapılan çalışmada, öğretmenlerin bilgi güvenliği farkındalıklarının, bilgi güvenliği eğitimi alan öğretmenlerin almayan öğretmenlere göre daha yüksek düzeyde olduğu belirlenmiştir. Bu sonuç da bizim sonuçlarımızla tutarlılık göstermektedir. Karacı vd. (2017) tarafından üniversite öğrencilerinin siber güvenlik davranışlarının incelenmesi ile ilgili yapılan çalışmada, internet-bilgisayar güvenlik eğitimi alan veya bu konuda iş deneyimi olan öğrencilerin siber güvenlik davranışlarının daha olumlu olduğu ortaya konulmuştur. Bizim yaptığımız çıkarımla aynı doğrultuda olduğu görülmektedir.

Bununla birlikte Akgün ve Topal (2015) tarafından yapılan çalışmada, öğrencilerin sorulara verdikleri yanıtlar bilişim güvenliği ve etikle ilgili bir ders alıp almamaları açısından bir farklılık göstermediği belirtilmiştir. Gökmen (2014) tarafından BÖTE öğretmen adaylarının bilişim güvenliği eğitimi verebilme yeterliliklerinin incelenmesi ile ilgili yapılan çalışmada, BÖTE öğretmen adaylarının %30,4'ünün siber güvenlik eğitimi aldıklarını, ancak aldıkları bu eğitimlerin bilişim güvenliği bilgilerini değiştirmediğini belirtmiştir. Mevcut alınan eğitimlerin farkındalık oluşturmadığı dikkat çekici bir husus olmakla birlikte, bunu eğitim

içeriklerinin yetersizliğine, davranışa dönüşecek etkililikte olmamasına bağlayabiliriz. Gökmen (2014) tarafından bu konuyla ilgili yapılan çıkarım da bizim görüşümüzü destekler niteliktedir. Adayların bilişim güvenliği bilgilerinin bir farklılık göstermemesi, aldıkları derslerin veya eğitimlerin içerik, yöntem ve konular itibarıyla yetersiz olmasından kaynaklanabileceği düşünülmektedir. Nitekim bu sonuçlar, bilişim güvenliği konusunda iyi hazırlanmış eğitimlerin şart olduğunu ve bilişim güvenliğine yönelik verilen eğitimlerin içerik, kapsam, süreç, farkındalık ve değerlendirme bakımında düzenlenmesinin gerekli olduğunu göstermektedir (Gökmen, 2014).

Sınıf düzeyi değişkeni açısından bakıldığında, çalışmaya katılan 305 öğrenciden 181 öğrencinin 10.sınıf öğrencisi, 124 öğrencinin de 12.sınıf öğrencisi olduğu görülmektedir. Bu değişkene göre sonuçlar analiz edildiğinde, genel siber güvenlik bilgi düzeyleri arasında anlamlı bir fark bulunmamaktadır. Öğrencilerin 10. ve 11.sınıfta aldıkları Bilişim Teknolojileri alan derslerinin siber güvenlik bilgi düzeylerine bir katkısı olmadığı anlaşılmaktadır. Ayrıca yaşları açısından değerlendirildiğinde, aralarındaki iki yıllık farktan dolayı 12.sınıftaki öğrencilerin mental açıdan daha gelişmiş oldukları düşünüldüğünde, bu gelişimin de siber güvenlik bilgi düzeylerinde bir farklılığa yol açmadığı sonucuna ulaşılabilir. Bostan ve Akman (2011) tarafından yapılan çalışmada, yaşın artması ile bilgisayar güvenliği konusundaki hassasiyetin azaldığı, web güvenliği konusundaki farkındalığın da arttığı analiz edilmiştir. Bu iki zıt sonucun genel siber güvenlik bilgi düzeyi bağlamında birbirlerini dengelediği, bu nedenle de herhangi bir farklılığın oluşmadığı söylenebilir. Bu açıdan bakıldığında yapılan analizlerle tutarlılık gösterdiği sonucuna ulaşılabilir. Budak (2015) tarafından yapılan Erzurum ili meslek liselerindeki bilişim öğrencilerinin siber suç farkındalığı ile ilgili çalışmada, sınıf türü ile öğrencilerin siber suçları algılamaları, internetteki rahatlık seviyeleri ve internette aldıkları önlem seviyeleri arasında anlamlı bir farkın olmadığı sonucuna ulaşılmıştır. Bu sonucun bizim yaptığımız çıkarımla aynı doğrultuda olduğu görülmektedir. Zeybek (2011) tarafından yapılan çalışmada, öğrencilerin bilişim teknolojilerini kullanımlarının etik açıdan değerlendirilmesi yapılmıştır. Sonuçlar analiz edildiğinde öğrencilerin bilişim teknolojilerini kullanım davranışlarının

internette önlem alma faktörü açısından yaşlarına göre herhangi bir farklılık göstermediği belirtilmiştir. Bu sonuç ile bizim çıkardığımız sonuç arasında tutarlılık bulunmakla beraber, aynı çalışmada sınıf düzeyine göre öğrencilerin bilişim teknolojilerini kullanım davranışlarının internette önlem alma açısından farklılık gösterdiğine değinilmiştir.

Siber mağduriyet yaşama durumları açısından bulgulara bakıldığında, çalışmaya katılan öğrencilerden 262 öğrencinin siber mağduriyet yaşamadığı, 43 öğrencinin ise yaşadığı görülmektedir. Verilen cevaplar analiz edildiğinde, genel siber güvenlik bilgi düzeylerinin siber mağduriyet yaşama durumlarına göre anlamlı bir farklılık bulunmadığını göstermektedir. Bir başka ifadeyle, siber mağduriyet yaşayanlar ile yaşamayanlar arasında genel siber güvenlik bilgi düzeyleri arasında bir fark olmadığı görülmektedir. Bu sonuç, siber mağduriyet yaşayan öğrencilerin kişisel siber güvenliklerini geliştirmek için ya da internette önlem almak için bir çabası olmadığını göstermektedir. Budak (2015) tarafından yapılan çalışmada, öğrencilerin herhangi siber saldırıya uğraması siber suçlara karşı farkındalıklarını değiştirmemektedir. Aynı şekilde siber suçlara maruz kalan öğrencilerin internette aldıkları önlem seviyelerinde bir değişiklik olmadığı sonucu bu görüşü desteklemektedir. Ama aynı zamanda Slonje vd. (2013) tarafından yapılan çalışmada, siber zorbalığa maruz kalan bireylerin sonraki bilişim teknolojileri deneyimleri ile ilgili olarak daha dikkatli davranacakları sonucuna ulaşmıştır. Sadece bildikleri kişilerle çevrimiçi iletişim kuracaklarını, şifrelerini, kullanıcı adlarını ve eposta adreslerini değiştireceklerini, tanımadıkları kişilerden gelen mesajları okumayacaklarını belirtmişlerdir. Buradan yola çıkarak siber mağduriyete uğrayan kişilerin diğerlerine göre daha çok önlem alacakları sonucu bizim yaptığımız birinci çıkarımla farklılık göstermektedir. Bu farklılık, siber mağduriyete uğrayan kişilerin yeterli siber güvenlik bilgisine sahip olmadıkları için mağduriyet sonrasında bilişim teknoloji kullanımı davranışlarında nasıl bir değişiklik yapacaklarını bilmemelerinden kaynaklanabilir. Bu çıkarımla birlikte siber güvenlik eğitiminin önemi de bir kez daha karşımıza çıkmaktadır.

Siber güvenlik yeterlik düzeyi açısından sonuçlar incelendiğinde, çalışmaya katılan 305 öğrenciden 80 öğrencinin siber güvenlik yeterlik düzeylerini “Az”, 195 öğrencinin “Orta”, 30 öğrencinin de “Yüksek” olarak belirttiği görülmektedir. Bulgular analiz edildiğinde, siber güvenlik yeterlik düzeyi az olan öğrenciler ile orta düzeyde olan öğrenciler arasında anlamlı bir farklılık bulunmuştur. Ayrıca, siber güvenlik yeterlik düzeyi az olan öğrenciler ile yüksek düzeyde olan öğrenciler arasında da anlamlı bir farklılık bulunmuştur. Son olarak siber güvenlik yeterlik düzeyi orta olan öğrenciler ile yüksek olan öğrenciler arasında da fark bulunduğu gözlenmiştir. Sonuç olarak siber güvenlik yeterlik düzeyi arttıkça, genel siber güvenlik bilgi düzeylerinin de arttığı görülmektedir. Buradan yola çıkarak, siber güvenlik eğitimi verilerek bilgi düzeyleri arttırıldığında, bireylerin bilişim teknolojilerini kullanım davranışlarında da olumlu yönde farklılık oluşacağı görülmektedir. Nitekim üniversite öğrencileri arasında bilgi güvenliği bilincini incelemek ve farklı faktörlerin onu nasıl etkilediğini analiz etmek için yapılan çalışmada, algılanan bilgi güvenliği bilinci ile genel bilgi güvenliği düzeyinde istatistiksel olarak doğrusal bir oran olduğu belirtilmiştir. Bu sonucun bizim sonucumuzla aynı doğrultuda olduğu görülmektedir (Farooq vd., 2015). Akgün ve Topal (2015) tarafından yapılan çalışmada, öğrencilerin bilişim güvenliği bilgi düzeyleri iyi olmasına rağmen bilişim güvenliği farkındalıklarının düşük olduğu sonucuna ulaşılmıştır. Örneğin, güvenli şifre oluşturma yöntemlerini bilmelerine rağmen, kullandıkları şifreleri basit yöntemlerle belirledikleri görülmüştür. Çıkan bu sonucun bizim çalışmamızla farklılık gösterdiği görülmektedir. Bu farklılık, bireylerin güvenlik önlemleri hakkında bilgi sahibi olmalarına karşın, siber tehditlerin ciddiyeti konusunda yeterli bilgiye sahip olmamalarından kaynaklanabilir. Bir başka ifadeyle, siber dünyada ciddi bir zarara uğramayacaklarını düşünmelerinden dolayı güvenlik yöntemlerini bilmelerine rağmen kullanmadıkları düşünülebilir. Aksoğan vd. (2018) tarafından yapılan çalışmada siber güvenlik ve bilgi güvenliği farkındalığı kazandırılmasına yönelik eğitimlerin verilmesinin gerekli olduğu sonucuna ulaşılmıştır.

BÖLÜM 7

ÖNERİLER

Araştırma doğrultusunda yapılan öneriler uygulamaya ve yapılacak araştırmalar dönük olarak iki başlıkta verilmiştir.

7.1. Uygulamaya Yönelik Öneriler

Araştırmadan elde edilen sonuçlara bağlı olarak uygulamaya dönük aşağıdaki önerilerde bulunulabilir.

- Bilişim Teknolojileri alanında eğitim gören öğrencilerin hem teknolojiyi en çok kullanan bireyler olması hem de bu teknolojileri üretecek geliştirecek bireyler olması açısından siber güvenlik bilgi düzeylerinin en üst seviyede olması gerekmektedir. Mevcut eğitim programına bakıldığında Ağ İşletmenliği dalındaki Ağ Sistemleri ve Yönlendirme dersinin Ağ Güvenliği modülünde verilen içeriğin ve ortak dersler içerisinde okutulan Programlama Temelleri dersinin Bilgi Güvenliği ve Etik modülünde verilen içeriğin tüm sınıf düzeylerine aktarılması ve Bilişim Teknolojileri alanındaki tüm öğrencilere verilmesi gerekmektedir.
- Ayrıca bilişim teknolojilerinin sürekli gelişen ve değişen doğası göz önüne alındığında siber tehditlerin de şekil ve yöntem değiştirdiği ve geliştiği bilinmektedir. Dolayısıyla siber güvenlik eğitimlerinin bir kereye mahsus olmak yerine belli periyotlarla düzenli bir şekilde verilmesi önerilebilir.
- Siber güvenlik eğitim içeriklerinin farkındalık oluşturacak etkililikte ve uygulamaya yönelik olarak geliştirilmesi gerekmektedir. Bunun yanında, eğitim içeriklerinin gelişen teknolojiyle aynı paralelde geliştirilmesi ve güncellenmesi gerekmektedir.
- Bilişim Teknolojileri öğretmenlerinin siber güvenlik bilgi düzeyleri belirli periyotlarla ölçülebilir, ihtiyaç duyulan eğitimler öğretmenlerin seminer dönemlerinde verilerek gelişimleri sağlanabilir. Çünkü eğitimcilerin bilgi düzeyleri ve buna paralel verecekleri eğitimler, öğrencilerin siber güvenlik bilgi düzeylerine doğrudan etki eden bir faktör olduğu düşünülmektedir.

- Öğrencilerde farkındalığı arttırmak ve geliştirdikleri uygulamaların güvenlik seviyelerini yükseltmeye yardımcı olmak adına, zafiyet tarama ve sızma testlerinin ürettikleri teknolojilere uygulanması önerilebilir. Buna ek olarak, yapılan testler sonucu en güvenli uygulamalara okul bazında yapılacak etkinliklerle ödüller vermek suretiyle teşvik edilebilir, farkındalık arttırılabilir.

7.2. Araştırmaya Yönelik Öneriler

Araştırma sonucunda yapılacak yeni araştırmalar için aşağıdaki önerilerde bulunulabilir.

- Bilişim Teknolojilerinde eğitim gören öğrencilerin siber güvenlik farkındalık düzeyleri orta düzeyli bulunmuştur. Öğrencilerin siber güvenlik düzeylerini belirleyecek nitel araştırmalar ile ihtiyaç analizi çıkarılabilir.
- Bilişim Teknolojileri konusunda eğitim gören öğrencilere eğitim verilerek, bu eğitimlerin etkililiğini belirlemeye yönelik araştırmalar yapılabilir.
- Siber güvenlik eğitimi konusunda öğrencilerin farkındalıklarının projelerine nasıl yansıdığını belirleyecek araştırmalar yapılabilir. Benzer şekilde öğrencilere proje geliştirme süreçlerinde siber güvenlik boyutunda değerlendirme kriterleri de eklenebilir.
- Bilişim Teknolojileri alanında eğitim veren öğretmenlerin siber güvenlik bilgi düzeylerini ölçen çalışmaların yapılması önerilebilir.
- Bilişim Teknolojilerinde eğitim gören ya da mezun olan öğrencilerin geliştirdiği uygulamaları, zafiyet tarama ve sızma testleri ile inceleyip sonuçları analiz edecek araştırmalar yapılabilir.

BÖLÜM 8

KAYNAKÇA

Adalı, E. (2001). İnternet Suçları. *Bilişim ve İnternet Teknolojilerinin Ceza Hukuku Açısından Doğurduğu Yeni Sorunlar*. 35-39.

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

Akkoyunlu, B., İşman, A., ve Odabaşı, H. F. (2018). *Eğitim Teknolojileri Okumaları 2018.* Sakarya: Sakarya Üniversitesi

Akleylek, S., Yıldırım, H. M., ve Tok, Z. Y. (2011). Kriptoloji ve Uygulama Alanları: Açık Anahtar Altyapısı ve Kayıtlı Elektronik Posta. *Akademik Bilişim 2011*. Malatya.

Aksoğan, M., Bayer, H., Gülada, M. O., ve Çelik, E. (2018). İletişim Fakültesi Öğrencilerinin Siber Güvenlik Farkındalığı: İnönü Üniversitesi Örneği. *Kesit Akademi Dergisi*, 271-288.

Alaca, B. (2008). *Ülkemizde bilişim suçları ve internetin suça etkisi (Antropolojik ve Hukuki boyutları ile)*. Ankara Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara.

Alataş, Ş. (2007). Phishing: İnternet Denizinin Popüler Avlanma Yöntemi. *XII. Türkiye İnternet Konferansı.* Ankara.

Altınok, E., ve Vural, A. F. (2011). Bilişim Suçları. *Kamu İç Denetçileri Derneği*(8), 74-84.

An Introduction to Cyber Security. (2017). https://www.skillsforcare.org.uk/Documents/Topics/Digital-working/An-Introduction-to-Cyber-Security.pdf, Erişim Tarihi: 16.03.2019

Anadolu Ajansı. (2017). https://www.aa.com.tr/tr/turkiye/turkiyede-en-cok-bilisim-sucu-sosyal-medyada-isleniyor/818513, Erişim Tarihi: 06.03.2019

Arıkan, S. M., ve Benzer, R. (2018). Bir Güvenlik Trendi: Bal Küpü. *Acta Infologica, 2*(1), 1-11.

Aydın, E. D. (1992). Bilişim Sistemlerinde Güvenlik, Güvenirlik, Mahremiyet ve Bilişim Suçları. *Marmara İletişim Dergisi*, 109.

BİAK. (2012). *T.B.M.M. Bilişim ve İnternet Araştırma Komisyonu Raporu.* Türkiye Büyük Millet Meclisi, Ankara. https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss381.pdf, Erişim Tarihi: 27.03.2019

Bilek, B. T. (2012). *Bilişim Suçları ve Üniversite Lisans Öğrencilerinin Bilişim Suçlarına Yönelik Görüşleri.* Yüksek Lisans Tezi, Gazi Üniversitesi, Bilişim Enstitüsü Bilgisayar Eğitimi ABD, Ankara.

Bostan, A., ve Akman, İ. (2011). Bilişim Güvenliği : Kullanıcı Açısından bir Durum Tespiti. *IV. Ağ ve Bigli Güvenliği Sempozyumu*, 51-56. Ankara.

Brunnstein, K. (1999). From AntiVirus to AntiMalware Software and Beyond: Another Approach to the Protection of Customers from Dysfunctional System Behaviour. *22nd National Information Systems Security Conference.* Hamburg: University of Hamburg.

BTK. (2017, 12 5). Bilgi Teknolojileri ve İletişim Kurumu: https://www.btk.gov.tr/farkindalik-calismalari, Erişim Tarihi: 15.03.2019

Budak, Ö. S. (2015). *Bilişim Öğrencilerinin Siber Suç Farkındalığı: Erzurum İli Mesleki ve Teknik Liseler Örneği.* Yüksek Lisans Tezi, Atatürk Üniversitesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi ABD, Erzurum.

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

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

Craigen, D., Diakun-Thibault, N., and Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*.

Çakır, H., ve Eryılmaz, S. (2014). *Eğitimciler İçin Bilişim Teknolojileri.* Ankara: Pegem Akademi.

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

Çeliktaş, B. (2016). *Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme.* Yüksek Lisans Tezi, Karadeniz Teknik Üniversitesi, Uluslararası İlişkiler ABD, Trabzon.

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

Çubukcu, A., ve Bayzan, Ş. (2013). Türkiye'de Dijital Vatandaşlık Algısı ve Bu Algıyı İnternetin Bilinçli, Güvenli ve Etkin Kullanımı ile Artırma Yöntemleri. *Middle Eastern & African Journal of Educational Research,* 148-174.

Daş, R., Kara, Ş., ve Gündüz, M. Z. (2012). Casus Yazılımların Bilgisayar Sistemlerine Bulaşma Belirtileri ve Çözümleri. *5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı.* Ankara: ODTÜ.

DeBarr, D., and Wechsler, H. (2009). Spam Detection using Clustering, Random Forests, and Active Learning. *Sixth Conference on Email and Anti-Spam*.

Değirmenci, O. (2002). *Bilişim Suçları.* Yüksek Lisans Tezi, Marmara Üniversitesi, Sosyal Bilimler Enstitüsü Hukuk ABD, İstanbul.

Desai, P. (2008). *Towards an Undetectable Computer Virus.* San Jose State University, The Faculty of the Department of Computer Science, California.

Digisophia. (2014). İnternet ve Bilişim Suçları: http://www.digisophia.com/Article/Details/65, Erişim Tarihi: 01.04.2019

Doğan, A., Söylemez, İ., ve Özcan, U. (2016). Importance of Information Systems For Organizations in Terms of Disaster Recovery. *International Conference on Research in Education and Science (ICRES).* Muğla.

Dubrawsky, I. (2003). Firewall Evolution - Deep Packet Inspection. *Security Focus, 1*(5).

Dülger, M. V. (2004). *Bilişim Suçları.* Ankara: Seçkin Yayıncılık.

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

Erdoğmuş, A. (2017). *Üniversite Öğrencilerinin Bilgi Kazanımlarının, Farkındalıkları Üzerindeki Etkilerinin Analizi: Afyon Kocatepe Üniversitesi Örneği.* Afyon Kocatepe Üniversitesi, İnternet ve Bilişim Teknolojileri Yönetimi ABD, Afyonkarahisar.

Ergün, İ. (2008). *Siber Suçların Cezalandırılması ve Türkiye'de Durum.* Ankara: Adalet Yayınevi.

Ermeydan, D. (2018). *Türk Ceza Kanunu'nda Bilişim Suçları.* Yüksek Lisans Tezi, Çağ Üniversitesi, Sosyal Bilimler Enstitüsü Kamu Hukuku ABD, Mersin.

Erol, O., Şahin, Y. L., Yılmaz, E., ve Haseski, H. İ. (2015). Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması. *International Journal of Human Sciences, 12*(2), 75-91.

Farooq, A., Isoaho, J., Virtanen, S., and Isoaho, J. (2015). Information Security Awareness in Educational Institution: An Analysis of Students' Individual Factors. *IEEE Trustcom/BigDataSE/ISPA.*

Ghosh, S., and Turrini, E. (2010). *Cybercrimes: A Multidisciplinary Analysis.* Heidelberg.

Google Trends. (2019). https://trends.google.com.tr/trends/explore?date=all&q=cyber%20security, Erişim Tarihi: 13.04.2019

Gökmen, Ö. F. (2014). *Bilgisayar ve Öğretim Teknolojileri Eğitimi Öğretmen Adaylarının Bilişim Güvenliği Eğitimi Verebilme Yeterliklerinin İncelenmesi.* Yüksek Lisans Tezi, Sakarya Üniversitesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi, Sakarya.

Gülbahar, Y., ve Kalelioğlu, F. (2018). Bilişim Teknolojileri ve Bilgisayar Bilimi: Öğretim Programı Güncelleme Süreci. *Milli Eğitim*(217).

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

Güvenli İnternet Merkezi. (2017). http://gim.org.tr/hakkimizda.php, Erişim Tarihi: 16.03.2019

Güvenli Web. t.y. Bilişim Hukuku ve Bilişim Suçları: https://www.guvenliweb.org.tr/dosya/0B0m7.pdf, Erişim Tarihi: 27.03.2019

Havelsan. (2017, Mart). Havelsan Siber Güvenlik Bülteni. (8).

HBOGM. (2016). Hayat Boyu Öğrenme Genel Müdürlüğü Kurs Programı: https://hbogm.meb.gov.tr/modulerprogramlar/kurslar/Bili%C5%9Fim%20Teknolojileri_Bilgi%20G%C3%BCvenli%C4%9Fi%20Bilin%C3%A7lendirme%20E%C4%9Fitimi%20Kurs%20Program%C4%B1.pdf, Erişim Tarihi: 15.03.2019

İlbaş, Ç. (2009). *Bilişim Suçlarının Sosyo-Kültürel Seviyelere Göre Algı Analizi.* Yüksek Lisans Tezi, Başkent Üniversitesi, statistik ve Bilgisayar Bilimleri ABD, Ankara.

İnternet Üst Kurulu. (2005). *İnternet Üst Kurulu Spam Bildirgesi.* Ankara: T.C. Ulaştırma ve Altyapı Bakanlığı.

ISCTurkey. (2018). Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı: https://www.iscturkey.org/index.html, Erişim Tarihi: 16.03.2019

ITU. (2008). Overview of Cybersecurity, ITU-T Recommendations: http://handle.itu.int/11.1002/1000/9136-en?locatt=format:pdf&auth, Erişim Tarihi: 14.03.2019

Karaarslan, E. (2005). Kampüs Ağ Yönetimi. *Akademik Bilişim 2005.* Gaziantep.

Karaaslan, E., Teke, A., ve Şengonca, H. (2004). Bilgisayar Ağlarında Güvenlik Politikalarının Uygulanması. *Meslek Yüksek Okullarında Bilgi Güvenliği Eğitimi Ege Ü. Meslek Yüksek Okulları Sempozyumu.* İzmir.

Karaca, A., ve Beyaznar, B. (2010). İnternette Müstehcenlik: Nerede Başlar ve Nerede Biter? *XII. Akademik Bilişim Konferansı Bildirileri, I,* 63-71. Muğla.

Karacı, A., Akyüz, H. İ., ve Bilgici, G. (2017). Üniversite Öğrencilerinin Siber Güvenlik Davranışlarının İncelenmesi. *Kastamonu Eğitim Dergisi.* Kastamonu.

Karakoç, M. A. (2011). Bilişim Suçlarına Genel Bakış, Bilişim Suçlarını Önleme Çalışmaları ve Güvenli İnternet Kullanımı. *Suç Önleme Sempozyumu* (s. 423). Bursa: Bursa Emniyet Müdürlüğü Yayınları.

Karasar, N. (2010). *Bilimsel Araştırma Yöntemi: Kavramlar, İlkeler, Teknikler.* Ankara: Nobel Yayın Dağıtım.

Keleştemur, S. A. (2018). *Siber İstihbaratın Kamu Güvenliği İçin Rolü ve Önemi.* Yüksek Lisans Tezi, İstanbul Gedik Üniversitesi, Siyaset Bilimi ve Kamu Yönetimi ABD, İstanbul.

Kim, E. B. (2013). Information Security Awareness Status of Business College: Undergraduate Students. *Information Security Journal, 22*(4).

Kim, E. K. (2014). Recommendations for information security awareness training for college students. *Information Management & Computer Security,* 115-126.

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

McConnell International. (2000). *Cyber Crime and Punishment?*. http://www.iwar.org.uk/law/resources/cybercrime/mcconnell/CyberCrime.pdf, Erişim Tarihi: 06.04.2019

McCrohan, K. F., Engel, K., and Harvey, J. W. (2010). Influence of Awareness and Training on Cyber Security. *Journal of Internet Commerce, 9*(1).

MEB. (2011). *Bilişim Teknolojileri Alanı Çerçeve Öğretim Programı.* Ankara: Milli Eğitim Bakanlığı.

MEB. (2018). *2023 Eğitim Vizyonu Belgesi.* Milli Eğitim Bakanlığı.

MEGEP. (2018). Bilişim Teknolojileri Alanı 10.Sınıflar İçin Çerçeve Öğretim Programı: http://www.megep.meb.gov.tr/dokumanlar/ 10.SINIF%20(2018-2019)/10%20%C3%87%C3%96P/B%C4%B0L%C4%B0%C5%9E%C4%B0M%20TEKNOLOJ%C4%B0LER%C4%B0_%C3%87%C3%96P_10.pdf, Erişim Tarihi: 15.03.2019

Nacar, F. B. (2010). *Avrupa Birliği Ülkeleri ve Türkiye'de Bilişim Suçlarının Ceza Hukukundaki Uygulamaları.* Atılım Üniversitesi, Sosyal Bilimler Enstitüsü Avrupa Birliği ABD, Ankara.

Nachenberg, C. (1997). Computer Virüs Coevolution. *Communication Of The ACM, 40*(1).

Nakilcioğlu, İ. H. (2007). *İletişimden Bilişime: İnternet Kültüründen Kesitler.* Afyonkarahisar Kocatepe Üniversitesi, Radyo-TV Yayımcılığı Programı, Kütahya.

North, M. M., George, R., and North, S. M. (2006). Computer security and ethics awareness in university environments: a challenge for management of information systems. *44th Annual Southeast Regional Conference,* (s. 434-439). Florida.

OECD. (2004). Organisation for Economic Co-operation and Development: http://www.oecd.org/internet/oecdtaskforcetocoordinatefightagainstspam.htm, Erişim Tarihi: 11.04.2019

Orakcı, M., Kök, İ., ve Çakır, H. (2016). Adli Bilişim Eğitiminin Gereksinimi ve Genel Olarak Değerlendirilmesi. *Bilişim Teknolojileri Dergisi, 9*(2), 137-145.

Orta, M. (2015). *Bilişim Suçlarında Adli Analiz.* Doktora Tezi, Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü Kamu Hukuku ABD, Konya.

Öğütçü, G. (2010). *E-Dönüşüm Sürecinde Kişisel Bilişim Güvenliği Davranışı ve Farkındalığının Analizi.* Yüksek Lisans Tezi, Başkent Üniversitesi, İstatistik ve Bilgisayar Bilimleri ABD, Ankara.

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

Özbilgin, İ. G., ve Özlü, M. (2010). Yazılım Geliştirme Süreçleri ve ISO 27001 Bilgi Güvenliği Yönetim Sistemi. *Akademik Bilişim 2010.* Muğla.

Özdemir, S., Kalkan, Ö. K., Türkoğlu, A., Varol, N., ve Tokdemir, M. (2013). Elazığ'da Üniversite ve Lisede Öğrenim Gören Bilgisayar Bölümü Öğrencilerinin Adli Bilişim Suçlarına Yaklaşımları. *NWSA-Medical Sciences,* 16-25.

Özel, S. (2013). *Lise öğrencileri arasında siber zorbalık, siber mağduriyet, depresyon ve benlik saygısı ilişkisi.* Yüksek Lisans Tezi, Fatih Üniversitesi, Eğitim Bilimleri ABD, İstanbul.

Özüdoğru, U. (2011). *Siber Suçlar ve Mücadele Yöntemleri: Dünya Uygulamaları ve Türkiye İçin Çözüm Önerileri.* Bilişim Uzmanlığı Tezi, Bilgi Teknolojileri ve İletişim Kurumu, Ankara.

Parris, L., Varjas, K., Meyers, J., and Cutts, H. (2011). High School Students' Perceptions of Coping With Cyberbullying. *Sage Journals, 44*(2), 284-306.

platinbilisim.com.tr. (2019). Siber Güvenlik Farkındalığı: https://www.platinbilisim.com.tr/Uploads/DigerDosya/sb-farkindalik.pdf, Erişim Tarihi: 14.03.2019

Resmi Gazete. (2013, 06 20). *Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna ilişkin Karar*(28683).

Rigdon, J. C. (2016). *Dictionary of Computer and Internet Terms.* Cartersville: Eastern Digital Resources.

Saini, H., Rao, Y. S., and Panda, T. C. (2012). Cyber-Crimes and their Impacts: A Review. *International Journal of Engineering Research and Applications (IJERA), 2*(2).

Serin, H. (2012). *Ergenlerde siber zorbalık/siber mağduriyet yaşantıları ve bu davranışlara ilişkin öğretmen ve eğitim yöneticilerinin görüşleri.* Doktora Tezi, İstanbul Üniversitesi, Eğitim Bilimleri ABD, İstanbul.

Sevri, M., ve Topaloğlu, N. (2016). Cyber Security Education in Turkey. *International Conference on Education in Mathematics, Science & Technology (ICEMST).*

Slonje, R., Smith, P. K., and Frisen, A. (2013). The nature of cyberbullying, and strategies for prevention. *Computers in Human Behavior*, 26-32.

Slusky, L., and Partow, P. (2012). Students Information Security Practices and Awareness. *Journal of Information Privacy and Security, 8*(4).

Song, Y., Zhu, X., Hong, Y., Zhang, H., and Tan, H. (2012). A Mobile Communication Honeypot Observing System. *2012 Fourth International Conference on Multimedia Information Networking and Security.* Nanjing, China.

Statista. (2018). Number of social media users worldwide from 2010 to 2021 (in billions): https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

Süslü, D. P., ve Oktay, A. (2018). Lise Öğrencilerinde Siber Zorbalık ve Siber Mağduriyetle İlişkili Bazı Değişkenlerin İncelenmesi. *İlköğretim Online, 17*(4), 1877-1895.

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

Şahinaslan, E., Kandemir, R., ve Şahinaslan, Ö. (2009). Bilgi Güvenliği Farkındalık Eğitim Örneği. *XI. Akademik Bilişim Konferansı.* Şanlıurfa.

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

T.B.M.M. (2012). *Bilişim ve İnternet Araştırma Komisyonu Raporu.* Türkiye Büyük Millet Meclisi, Ankara. T.B.M.M.: https://www.tbmm.gov.tr/ sirasayi/donem24/yil01/ss381.pdf, Erişim Tarihi: 27.03.2019

T.C. İçişleri Bakanlığı (2018). *5. Uluslararası Siber Suçlar Çalıştay Raporu*. https://www.icisleri.gov.tr/5-uluslararasi-siber-suclar-calistayi, Erişim Tarihi: 01.03.2019

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı (2015). *2016-2019 Ulusal E-Devlet Stratejisi ve Eylem Planı (Taslak)*. http://www.edevlet.gov.tr/2016-2019-ulusal-edevletstratejisiveeylemplanitaslagi.pdf, Erişim Tarihi: 15.12.2017

TDK. (2019). Türk Dil Kurumu: http://www.tdk.gov.tr/index.php?option=com_gts&kelime=B%C4%B0L%C4%B0%C5%9E%C4%B0M, Erişim Tarihi: 16.03.2019

TDK. (2019). Türk Dil Kurumu: http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5c8cfc90251f79.27591881, Erişim Tarihi: 16.03.2019

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

Thing, L. (2001). *Encyclopedia of Technology Terms.* Indianapolis: Que Publishing.

Topaloğlu, N. (2016). Türkiye'de Siber Güvenlik Eğitiminin Durumu. *International Conference on Education in Mathematics, Science & Technology*. Muğla: Isres Publishing.

Turhan, O. (2006). *Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar).* Planlama Uzmanlığı Tezi, Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, Ankara.

turkiye.gov.tr. (2017a). Sık Sorulan Sorular: https://www.turkiye.gov.tr/bilgilendirme?konu=sikcaSorulanlar, Erişim Tarihi: 05.01.2019

turkiye.gov.tr. (2017b). Tüm Hizmetler: https://www.turkiye.gov.tr/hizmetler, Erişim Tarihi: 03.01.2019

TÜBİSAD. (2017). *Türkiye'nin Siber Güvenlik Stratejisine Yönelik Değerlendirme.* Türkiye Bilişim Sanayicileri Derneği.

TÜBİSAD. (2018). Türkiye e-Ticaret 2017 Pazar Büyüklüğü: http://www.tubisad.org.tr/tr/images/pdf/tubisad_2018_e-ticaret_sunum_tr.pdf

TÜİK. (2018). Girişimlerde Bilişim Teknolojileri Kullanım Araştırması 2017: www.tuik.gov.tr/PdfGetir.do?id=21779.

TÜİK. (2018). HaneHalkı Bilişim Teknolojileri Kullanım Araştırması 2016: www.tuik.gov.tr/PdfGetir.do?id=21779.

TÜİK. (2018). Dönemsel Gayrisafi Yurt İçi Hasıla I. Çeyrek: Ocak - Mart 2018: http://www.tuik.gov.tr/HbPrint.do?id=27826

USGF. (2019). Uluslararası Siber Güvenlik Federasyonu Resmi İnternet Sitesi: https://www.usgf.org.tr/haber/uluslararasi-siber-guvenlik-federasyonu-ve-meb-arasinda-protokol-yapildi-/, Erişim Tarihi: 15.03.2019

USGS. (2016). *2016-2019 Ulusal Siber Güvenlik Stratejisi.* Ankara: T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı.

Ünver, M. (2012). Ulusal Siber Güvenliğin Sağlanmasında Farkındalık Çalışmaları. *Mimar Mühendisler Degisi*(60).

Ünver, M., ve Canbay, C. (2010, Mart). *Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik.* http://www.emo.org.tr/ekler/a9a502d6e646c25_ek.pdf, Erişim Tarihi: 14.03.2019

Ünver, M., Canbay, C., ve Mirzaoğlu, A. G. (2011). *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler.* Ankara: Bilgi Teknolojileri ve İletişim Kurumu.

Vural, B. A. (2006). *Bilgi İletişim Teknolojileri ve Yansımaları.* Ankara: Nobel Yayın Dağıtım.

We are Social. (2017). We are Social: https://wearesocial.com/special-reports/digital-in-2017-globaloverview_ .

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

Yayla, H. G. (2018). *Fatih Projesi Uygulanan ve Uygulanmayan Okullardaki Öğretmenlerin Bilgi Güvenliği Farkındalığının İncelenmesi.* Yüksek Lisans Tezi, Ankara Üniversitesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi ABD, Ankara.

Yazıcıoğlu, Y. (1997). *Bilgisayar Suçları Kriminolojik Sosyolojik ve Hukuki Boyutları İle.* İstanbul: Alfa Yayınları.

Yıldırım, A., ve Şimşek, H. (2006). *Sosyal Bilimlerde Nitel Araştırma Yöntemleri.* Ankara: Seçkin Yayıncılık.

Yıldız, M. (2014). *Siber Suçlar ve Kurum Güvenliği.* Ankara: T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı.

Yüzer, V., ve Okur, R. (2015). *Temel Bilgi Teknolojileri-I.* Eskişehir: Anadolu Üniversitesi.

Zeybek, G. (2011). *Bilgisayar Meslek Dersi Alan Ortaöğretim Öğrencilerinin Bilişim Teknolojilerini Kullanımlarının Etik Açıdan Değerlendirilmesi.* Yüksek Lisans Tezi, Selçuk Üniversitesi, Eğitim Programı ve Öğretimi Bilim Dalı, Konya.

BÖLÜM 9

EKLER

EK-1: Kişisel Siber Güvenliği Sağlama Ölçeği

Bilişim Teknolojileri Alanındaki Öğrencilerin Kişisel Siber Güvenliğe Yönelik Bilgi Düzeylerinin Belirlenmesi

Değerli Öğrenciler,

Necmettin Erbakan Üniversitesi, Eğitim Bilimleri Enstitüsü, Bilgisayar ve Öğretim Teknolojileri Eğitimi ABD'da yüksek lisans yapmaktayım. Tezim kapsamında siz öğrencilerin değerli görüşlerine gereksinim duymaktayım. Tez araştırmamın genel amacı bilişim teknolojileri alanında öğrenim gören öğrencilerin kişisel siber güvenliğe yönelik bilgi düzeylerini belirlemektir. Maddelere verilecek doğru veya yanlış cevap yoktur. Maddeleri size en uygun şekilde içtenlikle cevaplamanız önemlidir. Her bir ifade için size uygun gelen seçeneği X ile işaretleyiniz. Verdiğiniz bilgiler sadece yapmakta olduğum yüksek lisans tezim için kullanılacak, araştırma kapsamında gizli tutulacak ve hiçbir kişi ya da kurumla paylaşılmayacaktır. Formda bulunan maddeleri boş bırakmadan, hepsini cevaplamanız formun geçerliliği açısından önemlidir.

Ölçekleri doldurmak yaklaşık 15 dakikanızı alacaktır.

Sağladığınız katkı ve ayırdığınız değerli zaman için teşekkür ederim.

Selim ASLAN
Yüksek Lisans Öğrencisi
İletişim: selimaslan42@gmail.com

KİŞİSEL BİLGİLER

---

1. **Sınıfınız nedir?**
   ( ) 10. Sınıf ( ) 12. Sınıf
2. **Siber Güvenlik Konusunda eğitim aldınız mı?**
   ( ) Evet ( ) Hayır
3. **Sosyal ağ kullanma durumunuz?**
   ( ) Kullanıyorum ( ) Kullanmıyorum
4. **Hiç siber mağduriyet yaşadınız mı?**
   ( ) Evet ( ) Hayır
5. **Kişisel siber güvenlik bilgi düzeyinizin nedir?**
   ( ) Az ( ) Orta ( )Yüksek

KİŞİSEL SİBER GÜVENLİK BİLGİ DÜZEYİ BELİRLEME ÖLÇEĞİ

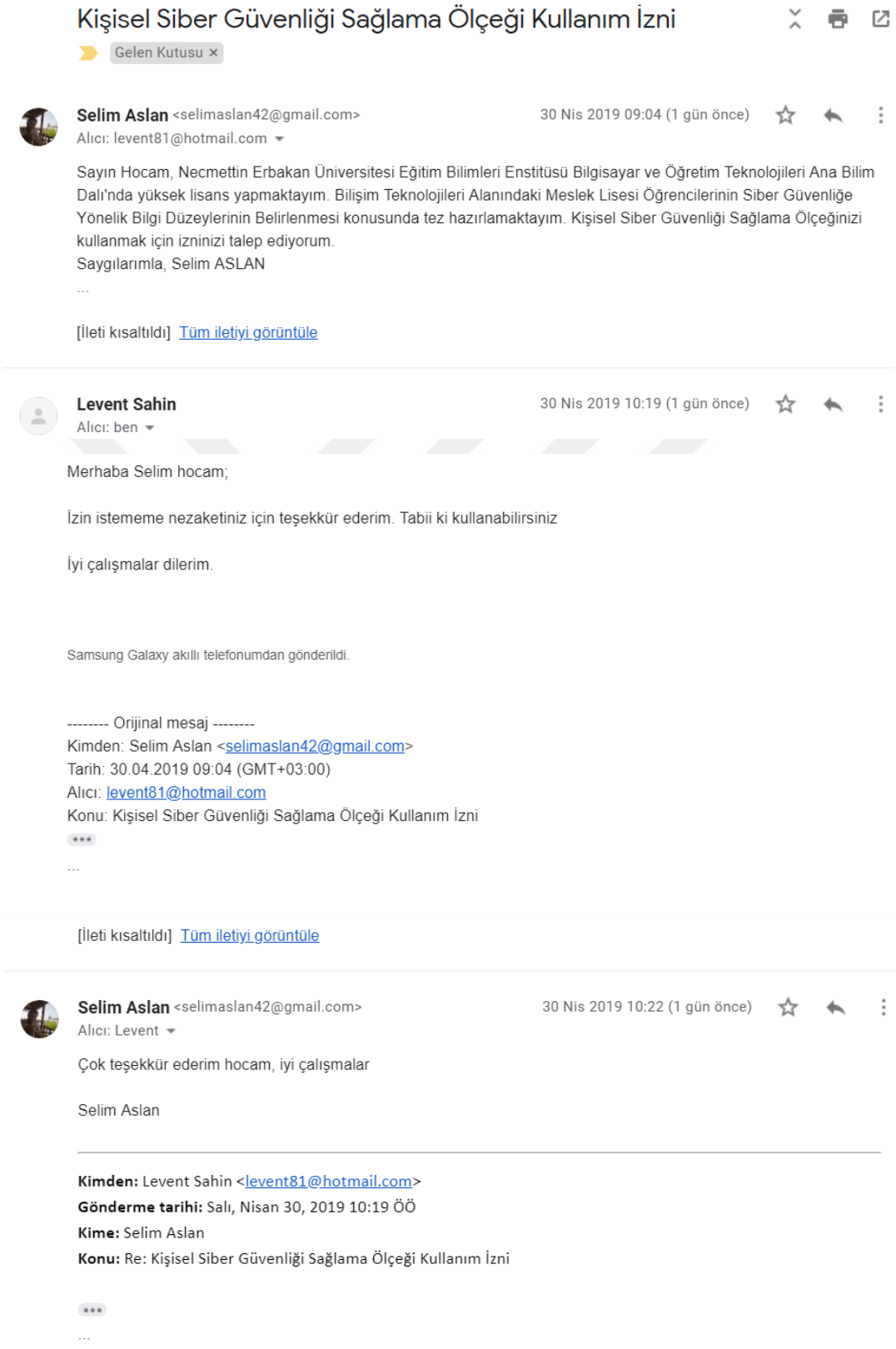
Bu ölçeğin amacı, öğrencilerin kişisel siber güvenlik bilgi düzeylerini belirlemektir.

Lütfen doğru yanıtı X ile işaretleyiniz.		**Hiçbir Zaman**	**Nadiren**	**Ara Sıra**	**Sık Sık**	**Her Zaman**
1	Web sayfalarında güvenlik bağlantılarını (https://) ve sertifikalarını kontrol ederim.					
2	Kullandığım yazılımları güncellerim.					
3	Bilgisayarımda antivirus yazılımı bulundururum.					
4	Şifrelerimi belirlerken basit dizilimler kullanmaktan kaçınırım.					

Lütfen doğru yanıtı X ile işaretleyiniz.		**Hiçbir Zaman**	**Nadiren**	**Ara Sıra**	**Sık Sık**	**Her Zaman**
5	İnternet şifrelerimin tümünün aynı olmasına dikkat ederim.					
6	Web tarayıcımın güvenlik ayarlarını düzenlerim.					
7	E- posta ile gelen kimlik doğrulama mesajlarını (kullanıcı adı, şifre vb. istekler) cevaplarım.					
8	Şahsi bilgisayarım dışında kullanılan bilgisayarlarda bilgilerimin kalmamasına dikkat ederim.					
9	İnternet üzerinden yapılan para ve kontör isteklerini dikkate almam.					
10	Tanımadığım kişilerden gelen sosyal ağ arkadaşlık isteğini kabul etmem.					
11	Güvenmediğim sitelere üye olmam.					
12	Tanımadığım kişiler ile web kamerası kullanarak sesli ve görüntülü iletişim kurarım.					
13	İnternet ortamında gerektiğinde kişisel bilgilerimi (TC No,Doğum tarihi,Gsm No vb.)paylaşırım.					
14	Web geçmişimi temizlerim.					
15	İnternet bankacığı işlemlerini şahsi bilgisayarımdan yaparım.					
16	Online alışveriş işlemlerini şahsi bilgisayarımdan yaparım.					
17	Tanımadığım kişilerden gelen e-posta eklerini açarım.					
18	Sosyal paylaşım sitelerinde kişisel bilgilerime yer veririm.					
19	İnternet üzerinden yer bildirimi yaparım.					
20	Sosyal ağlarda yer alan reklamlar üzerinden alışveriş yaparım.					
21	Sosyal ağ - e-posta gibi hesaplarda işim bittiğinde oturumu kapatırım.					
22	Güvenmediğim sitelerden dosya indirmem.					
23	İnternette kullandığım (eposta, sosyal ağ vb.)şifreleri değiştiririm.					
24	Unutmamak için akılda kalan kolay bir şifre belirlerim.					
25	Banka, online alışveriş sitesi gibi sitelerden gelen e postalara (kart numarası, şifre vb. istekler) itibar ederim ve yanıtlarım.					

Teşekkür Ederim.

EK-2: Ölçek Kullanım İzni



Kişisel Siber Güvenliği Sağlama Ölçeği Kullanım İzni

Gelen Kutusu ×

Selim Aslan <selimaslan42@gmail.com> 30 Nis 2019 09:04 (1 gün önce)
Alıcı: levent81@hotmail.com

Sayın Hocam, Necmettin Erbakan Üniversitesi Eğitim Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Ana Bilim Dalı'nda yüksek lisans yapmaktayım. Bilişim Teknolojileri Alanındaki Meslek Lisesi Öğrencilerinin Siber Güvenliğe Yönelik Bilgi Düzeylerinin Belirlenmesi konusunda tez hazırlamaktayım. Kişisel Siber Güvenliği Sağlama Ölçeğinizi kullanmak için izninizi talep ediyorum.
Saygılarımla, Selim ASLAN
...

[İleti kısaltıldı] Tüm iletiyi görüntüle

Levent Sahin 30 Nis 2019 10:19 (1 gün önce)
Alıcı: ben

Merhaba Selim hocam;

İzin istememe nezaketiniz için teşekkür ederim. Tabii ki kullanabilirsiniz

İyi çalışmalar dilerim.

Samsung Galaxy akıllı telefonumdan gönderildi.

-------- Orijinal mesaj --------
Kimden: Selim Aslan <selimaslan42@gmail.com>
Tarih: 30.04.2019 09:04 (GMT+03:00)
Alıcı: levent81@hotmail.com
Konu: Kişisel Siber Güvenliği Sağlama Ölçeği Kullanım İzni
...

[İleti kısaltıldı] Tüm iletiyi görüntüle

Selim Aslan <selimaslan42@gmail.com> 30 Nis 2019 10:22 (1 gün önce)
Alıcı: Levent

Çok teşekkür ederim hocam, iyi çalışmalar

Selim Aslan

Kimden: Levent Sahin <levent81@hotmail.com>
Gönderme tarihi: Salı, Nisan 30, 2019 10:19 ÖÖ
Kime: Selim Aslan
Konu: Re: Kişisel Siber Güvenliği Sağlama Ölçeği Kullanım İzni

...

EK-3: Ölçek Uygulamak İçin Alınan İzin Belgesi

T.C. MERAM KAYMAKAMLIĞI

Meram Mesleki ve Teknik Anadolu Lisesi Müdürlüğü

Sayı: 35571482-355.01-

Konu: Anket Uygulama İzni – Selim ASLAN

İLGİLİ MAKAMA

Necmettin Erbakan Üniversitesi Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı Bilgisayar ve Öğretim Teknolojileri Eğitimi Bilim Dalı Yüksek Lisans Programı'nda eğitim görmekte olan Selim ASLAN'ın "Bilişim Teknolojileri Alanındaki Meslek Lisesi Öğrencilerinin Siber Güvenliğe Yönelik Bilgi Düzeylerinin Belirlenmesi" konulu tezi için kullanacağı anket çalışmalarını okulumuz Meram Mesleki ve Teknik Anadolu Lisesi bünyesinde yürütmesine izin verilmiştir.

Bilgilerinize arz ederim.

20/04/2018

Ömer Faruk KARABULUT

Meram Mesleki ve Teknik Anadolu Lisesi

Okul Müdürü