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

ÖĞRETMEN ADAYLARININ SİBER GÜVENLİK FARKINDALIKLARININ İNCELENMESİ

Yasemin ÖZBEK

YÜKSEK LİSANS TEZİ

Danışman
Dr. Öğr. Üyesi Şemseddin GÜNDÜZ

Konya-2019

BİLİMSEL ETİK SAYFASI

Öğrencinin	Adı Soyadı	Yasemin ÖZBEK
	Numarası	148305011004
	Ana Bilim Dalı	Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı
	Bilim Dalı	Bilgisayar ve Öğretim Teknolojileri Eğitimi Bilim Dalı
	Programı	Tezli Yüksek Lisans
	Tezin Adı	Öğretmen Adaylarının Siber Güvenlik Farkındalıklarının İncelenmesi

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.

02/08/2019

Yasemin ÖZBEK

T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ
Eğitim Bilimleri Enstitüsü Müdürlüğü

KONYA

EĞİTİM BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ KABUL FORMU

Öğrencinin		
	Adı Soyadı	Yasemin ÖZBEK
	Numarası	148305011004
	Ana Bilim Dalı	Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı
	Bilim Dalı	Bilgisayar ve Öğretim Teknolojileri Eğitimi Bilim Dalı
	Programı	Tezli Yüksek Lisans
	Tez Danışmanı	Dr. Öğr. Üyesi Şemseddin GÜNDÜZ
	Tezin Adı	Öğretmen Adaylarının Siber Güvenlik Farkındalıklarının İncelenmesi

Yukarıda adı geçen öğrenci tarafından hazırlanan Öğretmen Adaylarının Siber Güvenlik Farkındalıklarının İncelenmesi başlıklı bu çalışma 09/07/2019 tarihinde yapılan savunma sınavı sonucunda oybirliği/oyçokluğu ile başarılı bulunarak, jürimiz tarafından yüksek lisans tezi olarak kabul edilmiştir.

	Ünvanı Adı Soyadı	İmza
Danışman	Dr. Öğr. Üyesi Şemseddin GÜNDÜZ	
Jüri Üyesi	Doç. Dr. Ahmet Naci ÇOKLAR	
Jüri Üyesi	Doç. Dr. Hüseyin ÖZÇINAR	

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/egitimbilimlerienstitusu
E- Posta: ebil@konya.edu.tr

TEŞEKKÜR

Yüksek lisans eğitim ve tez çalışması sürecinde tecrübesi ve bilgisi ile bana yol gösteren, danışmanım Dr. Öğr. Üyesi Şemseddin GÜNDÜZ' e teşekkürlerimi sunarım.

Tez dönemim boyunca yardım ve desteğini hiç esirgemeyen, Dr. Öğr. Üyesi Murat GÜLER' e, Doç. Dr. Ahmet Naci ÇOKLAR' a, Doç. Dr. Hüseyin ÖZÇINAR' a, verilerin elektronik ortama aktarılma sürecinde yardımlarını esirgemeyen kardeşim Büşra ÖZBEK' e, beni motive eden sevgili amcam Erol ÖZBEK' e ve tez çalışmamı düzenlememe yardımcı olan arkadaşım M. Uğur ÖZEN' e teşekkür ederim.

Hayatımın her anında yanımda olan, başaracağıma hep inanan, sevgi, sabır, anlayış ve desteklerini hiçbir zaman esirgemeyen annem Nejla ÖZBEK, babam Hanifi ÖZBEK'e teşekkür ederim.

Yasemin ÖZBEK

T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ
Eğitim Bilimleri Enstitüsü Müdürlüğü

Öğrencinin		
	Adı Soyadı	Yasemin ÖZBEK
	Numarası	1483050110004
	Ana Bilim Dalı	Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı
	Bilim Dalı	Bilgisayar ve Öğretim Teknolojileri Eğitimi Bilim Dalı
	Programı	Tezli Yüksek Lisans
	Tez Danışmanı	Dr. Öğr. Üyesi Şemseddin GÜNDÜZ
	Tezin Adı	Öğretmen Adaylarının Siber Güvenlik Farkındalıklarının İncelenmesi

ÖZET

Bu araştırmanın amacı, eğitim fakültelerinde öğrenim gören öğretmen adaylarının kişisel siber güvenlik sağlama durumlarını incelemektir. Bu amaç doğrultusunda öğretmen adaylarının demografik özellikleri ile kişisel siber güvenlik sağlama durumları arasındaki ilişki analiz edilmiştir. Araştırmanın örneklemini 2017-2018 eğitim öğretim yılında Necmettin Erbakan Üniversitesi'nde öğrenim gören 270 erkek ve 509 kadın olmak üzere 809 öğretmen adayı oluşturmaktadır.

Çalışmada ilişkisel tarama yöntemi kullanılmıştır. Araştırma sonucunda öğretmen adaylarının kişisel siber güvenlik farkındalıklarının orta düzeyde olduğu bulunmuştur. Erkek öğretmen adaylarının kişisel siber güvenlik farkındalıklarının kadın öğretmen adaylardan daha fazla olduğu görülmüştür. Öğretmen adaylarının akademik başarıları ve öğrenim gördükleri sınıf düzeylerine göre kişisel siber güvenlik farkındalıkları arasında anlamlı bir farklılık bulunmamıştır. İnterneti daha sık kullananların az internet kullananlardan kişisel siber güvenlik farkındalık düzeylerinin daha yüksek olduğu söylenebilir.

Anahtar Kelimeler: Siber güvenlik, Öğretmen adayı, Siber saldırı, Farkındalık

T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ
Eğitim Bilimleri Enstitüsü Müdürlüğü

Öğrencinin		
	Adı Soyadı	Yasemin ÖZBEK
	Numarası	1483050110004
	Ana Bilim Dalı	Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı
	Bilim Dalı	Bilgisayar ve Öğretim Teknolojileri Eğitimi Bilim Dalı
	Programı	Tezli Yüksek Lisans
	Tez Danışmanı	Dr. Öğr. Üyesi Şemseddin GÜNDÜZ
	Tezin Adı	Öğretmen Adaylarının Siber Güvenlik Sağlama Durumları Arasındaki İlişki

ABSTRACT

The aim of this study is to investigate the personal cybersecurity status of prospective teachers studying in faculties of education. For this purpose, the relationship between teacher candidates' demographic characteristics and their personal cybersecurity status were analyzed. The sample of the study consists of 809 prospective teachers, 270 of them are male and 509 of them are female who was studying at Necmettin Erbakan University in the 2017-2018 academic year.

The correlational survey model was used in the study. As a result of the research, it was found that the prospective teachers' personal cybersecurity awareness was at a moderate level. Also, it was seen that personal cybersecurity awareness levels of male prospective teachers were higher than female prospective teachers. There was no significant difference among the prospective teachers' personal cybersecurity awareness according to their academic standing and school grade. It can be asserted that those who use the Internet more frequently, have higher levels of personal cybersecurity awareness than less frequent users.

Keywords: Cybersecurity, Prospective teacher, Cyber attack, Awareness

KISALTMALAR VE İMGELER

BİT: Bilgi ve İletişim Teknolojileri

BÖTE: Bilgisayar ve Öğretim Teknolojileri Eğitimi

PDR: Psikolojik Danışmanlık ve Rehberlik

TDK: Türk Dil Kurumu

TÜİK: Türkiye İstatistik Kurumu

TİB: Telekomünikasyon İletişim Başkanlığı

UDHB: Ulaştırma Denizcilik ve Haberleşme Bakanlığı

WEB: World Wide Web

İÇİNDEKİLER

TABLOLAR LİSTESİ

BÖLÜM 1

GİRİŞ

Bu bölümde araştırmanın problem durumu ile ilgili açıklamalar yapılmış, buna bağlı olarak amaçlar ve alt amaçlar belirlenmiş, araştırmanın önemi vurgulanmış, araştırmaya engel olan sınırlılıklardan bahsedilmiş, alanyazın taramaları da dikkate alınarak araştırma kapsamında yer alan kavramlarla ilgili terimler açıklanmıştır.

1.1. Problem Durumu

Değişen ve gelişen teknolojiler büyük bir hızla hayatımıza girmektedir. Internet ve bilgisayar kullananların sayısı dünyada ve Türkiye'de hızla artmaktadır. Türkiye İstatistik Kurumu'nun 8 Ağustos 2018 tarihinde güncellediği verilere göre 2018 yılında Türkiye' de İnternet kullanım oranı 16-74 yaş aralığındaki kişilerde %63,2'dir. Bu oran 2004 yılında %9,9'dur (TUİK, 2018). Bu açıdan bakıldığında İnternet kullanım oranı on dört yılda %53,3 kadar artmıştır. En etkili kitle iletişim aracı olan internet, sağladığı çeşitli faydalarla birçok alanda etkinliğini göstermiştir. Bilgisayar aracılığı ile yapılan uzaktan eğitim, çeşitli bankacılık işlemlerinin vakitten kazanacak şekilde yapılabilmesi, türlü seçenekler ile alışveriş yapma olanağının olması, iletişimin çok çeşitli şekillerde yapılması ve bilgiye ulaşmada büyük bir hız ve kolaylık sağlaması, internetin başlıca avantajlarındandır.

İnternetin faydalı yanlarının olduğu kadar tehlikeli yanlarının da olduğu görülmüştür. İnternet, kötü niyetli kişilerin etkinliklerini sürdürmek için kullanım alanı haline gelmiştir (Kara, 2013). İnternet kullanımının hızlı bir şekilde artması, belli bir sınır ve engelleme olmadan, her türlü bilgiye ulaşmada kolaylığın olması, olumlu gelişmelerin yanında birtakım olumsuz sonuçların ortaya çıkmasına da sebep olabilmektedir. Siber saldırılar, illegal, şiddet ve cinsel içerikli web sayfalarına kolay erişim sağlama, kötü niyetli kişilerle iletişim kurma, oyun bağımlılığı sıkça karşılaşılan tehlikeli durumlardan bazılarıdır.

Bilgi ve İletişim Teknolojileri (BİT) kullanılarak dünyada hedef seçilen bir birey, kurum, bina, sistem ve kritik altyapıları hedef alan ve bunların istenilen şekilde hizmet vermesini engellemeye, işleyişini bozmaya veya bilgilere izinsiz erişim, bilgininin bütünlüğünü bozmaya dönük saldırılar siber saldırı olarak

adlandırılmaktadır (Şahinaslan, Kantürk, Şahinaslan, Borandağ 2009). Bulunduğumuz zaman içerisinde bireysel siber saldırılardan öte bir takım grupların beraber harekete geçtiği ve devletlerin bile birbirlerine siber savaş açtığı duruma gelinmiştir (Şahinaslan, Kandemir, Şahinaslan 2009).

Ülkelerin yaşayacağı siber saldırılar ülkedeki hayatı kesintiye uğratmaya hatta durdurmaya kadar getirebilecek boyuttadır. Bireysel ve ulusal açıdan birçok bilgi paylaşımının yapıldığı ve birçok bilgi paylaşımı yapılan bilişim araçları kullanılarak ortaya çıkan siber saldırılara karşı güvenliğin sağlanması gerekmektedir.

1.2. Araştırmanın Amacı

Araştırmanın amacı, eğitim fakültelerinde öğrenim görmekte olan öğretmen adaylarının kişisel siber güvenlik farkındalıklarını incelemektir. Bu amaçla aşağıdaki sorulara cevap aranmıştır.

1. Öğretmen adaylarının kişisel siber güvenlik farkındalıkları ne düzeydedir?
2. Öğretmen adaylarının cinsiyetlerine göre kişisel siber güvenlik farkındalıkları arasında anlamlı bir farklılık var mıdır?
3. Öğretmen adaylarının öğrenim görmekte oldukları bölümlere göre kişisel siber güvenlik farkındalıkları arasında anlamlı bir farklılık var mıdır?
4. Öğretmen adaylarının öğrenim gördüğü sınıf kademesine göre kişisel siber güvenlik farkındalıkları arasında anlamlı bir farklılık var mıdır?
5. Öğretmen adaylarının internet kullanım sıklıklarına göre kişisel siber güvenlik farkındalıkları arasında anlamlı bir farklılık var mıdır?
6. Öğretmen adaylarının not ortalamalarına göre kişisel siber güvenlik farkındalıkları arasında anlamlı bir farklılık var mıdır?

1.3. Araştırmanın Önemi

Her geçen gün teknolojinin ilerlemesiyle birlikte ortaya çıkan siber mağduriyet artmaktadır. Yapılan araştırmalar sonucu Türkiye'nin siber saldırılara en çok uğrayan 4. ülke olması (Bozdemir, 2016), son zamanlarda dijital ortamda artan kişisel/gizli bilgilerin çalınası, tehlikenin büyüklüğünü de gözler önüne sermektedir. Yapılan

araştırmalar ışığında siber ortamı en çok çocukların ve gençlerin kullandığı tespit ediliştir.

Ülkemizde bilişim sistemleri ve internet kullanım oranımız giderek artmaktadır. Bundan ötürü de siber ortamlardaki karşılaşabileceğimiz tehlikeler de çoğalmaktadır. Bundan dolayı siber güvenlik kavramı güncelliğini koruyarak son zamanların en çok tartışılan konulardan birisi haline gelmiştir. Birçok riske rağmen siber güvenlik kavramı, ülkemizde çok da önemsenmemekte, bunun sonucunda da maddi manevi kayıplar artmaktadır (Hekim ve Başıbüyük, 2013).

Siber güvenlik konusunda bireylere siber güvenlik farkındalığının kazandırılması ve bu farkındalığı etkileyebilecek bireye dayalı özelliklerin ortaya konulması açısından en çok mağduriyetin yaşandığı gruplardan biri olan üniversite gençliği olduğu düşünülmüştür. Bundan dolayı da örneklemimiz üniversite gençliği içerisinden öğretmen adayları olarak seçilmiştir. Çalışmada öğretmen adaylarının kişisel siber güvenlik farkındalıkları derinlemesine incelenmiştir.

1.4. Sınırlılıklar

1. Araştırma, Konya ili sınırları içerisinde, 2017-2018 eğitim öğretim yılında eğitim fakültelerinde öğrenim görmekte olan öğrencilerin görüşleriyle sınırlandırılmıştır.

2. Araştırma, değişkenleri ölçmek için geliştirilen ölçeklerle toplanan bilgilerle sınırlandırılmıştır.

3. Araştırma verileri tek bir zamanda kesitsel olarak toplanmıştır.

1.5. Tanımlar

Siber: Bilgisayar ve sistemleri birbirine bağlayan ağlarla ilgisi olan kavramları tanımlamak amacıyla kullanılır (Yaşar, 2014).

Siber Ortam: Bilişim sistemleri ve bunları birbirine bağlayan ağlardan oluşan ortam olarak adlandırılır (AFAD Sözlüğü, 2019).

Siber Saldırı: Siber ortamlarda bulunan teknolojilerin ve sistemlerin, güvenlik ilkelerinden herhangi birini yok etmek amacıyla, yine bu ortam içerisinde bulunan herhangi bir kişi ya da bilişim sistemleri aracılığı ile yapılan, bilerek ve isteyerek yapılan faaliyetlerdir (T.C Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 2016).

Siber Savaş: Bilişim teknolojileri aracılığı ile bir ülkenin hedef seçtiği başka bir ülkeye düzenlediği saldırı hareketleri olarak tanımlanmıştır (Yazıcı, 2011).

Siber Güvenlik: Siber alemi oluşturan bilgi ve iletişim sistemlerinin saldırılardan korunmasını, verilerin çeşitli boyutlarıyla incelenmesini, saldırıların ortaya çıkarılmasını, bunun sonucunda da önlem alma ve zarar görmemesi içi yapılan çalışmalar olarak tanımlanmıştır (T.C Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 2016).

Hacking: Bilgisayar ve ağ sistemlerine izinsiz giriş yapmakla birlikte, çeşitli bilgilere ulaşıp bu bilgileri çalma, zarar verme gibi eylemlere hacking adı verilir (TDK, 2019).

Hacker: Hacking eylemi gerçekleştiren kişilere hacker denilmektedir.

BÖLÜM 2

KURAMSAL ÇERÇEVE

Bu bölümde, siber, siber ortam, siber saldırı, siber savaş, siber güvenlik, bilgi güvenliği, siber saldırı çeşitleri, yakın geçmişte yaşanmış siber saldırılar ülkelerin siber saldırı konusunda aldığı tedbirler, hacking ve hacker, siber güvenlikle ilgili yurtiçi ve yurtdışında yapılan çalışmalar ile ilgili kavramlar ele alınmıştır.

2.1. Siber ve Siber Ortam

Siber terimi sibernetik kökeninden gelmektedir. Sibernetik, canlılar veya makineler arasındaki iletişim disiplinini inceleyen bilim dalıdır (Wikizero, 2019a). Siber, Bilgisayar ve bilgisayarları birbirine bağlayan ağlarla ilgisi olan kavramları tanımlamak amacıyla kullanılır (Yaşar, 2014). Başka bir tanımlama ise siber, çeşitli çalışmalardan hareketle bilgisayar ve buna bağlı sistemlerden oluşan ve bilişim kelimesiyle eş değer kullanılan bir kavram olarak da kullanılmaktadır.

Siber ortam, bilişim sistemleri ve bunları birbirine bağlayan ağlardan oluşan ortam olarak adlandırılır (AFAD Sözlüğü, 2019). Yapılan araştırmalardan yola çıkarak siber ortam kavramının son zamanlarda siber uzay olarak da kullanıldığı görülmüştür.

2.2. Siber Güvenlik

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığına göre siber güvenlik; "Siber alemi oluşturan bilişim sistemlerinin saldırılardan korunmasını, verilerin gizlilik, bütünlük ve erişilebilirliğinin boyutlarının ele alınmasını, saldırıların ortaya çıkarılmasını, bunun sonucunda da önlem alma ve zarar görmemesi içi yapılan çalışmalar olarak tanımlanmıştır (T.C Ulaştırma Bakanlığı, 2016).

Siber alemde, kurum, kuruluş ve kişisel kullanıcıların verilerini korumak amacıyla kullanılan araç gereç, yönetmelik, rehber, faaliyetler ve teknolojilerin tamamına siber güvenlik denilmektedir

Yakın bir zamana kadar bireysel sıkıntılara yol açan siber saldırılar artık ülke güvenliğini tehdit edebilecek duruma gelmiştir. Derian (2000) bu durumu; "taklit

(imitasyon) ve simülasyona ait yeni teknolojiler ile izleme yetenekleri ve hızın artması ile gerçek ve sanal savaş arasındaki alanın (gap), coğrafi mesafelerin ve kronolojik sürenin kısalması (collapse)" olarak ifade etmiştir. Gerçekleşen bu değişimler ile savunma sanayi teknolojileri sayesinde savaşın niteliği ve tanımı günden güne değişmeye başlamıştır (Çiftçi, 2013).

Günümüz teknoloji çağında, hayatımızın büyük bir kısmını dijital ortamlarda yaşamaktayız. Kişiler, devletler, kamu kurumları, sosyal platformlar, özel şirketler de dijital ortamda bir hayat sürmektedir. Dijital dönüşümün giderek arttığı dünyada yeni tehdit artık dijital dünya üzerinden gelmektedir. Son yıllarda yaşanan siber saldırılar, siber güvenlik kavramının önemini ortaya koymuştur. Bunun sonucunda da siber güvenlik nasıl sağlanır sorusuna cevap arayanlar da artmıştır. İnternetin çok fazla kullanıldığı bir ortamda verilerin güvenliği ve korunması da güçleşmeye başlamıştır. Siber güvenlik, kötü niyetli kişiler, kurumlar veya yazılımlardan, verilerin korunması anlamına gelmektedir.

Uluslararası siber güvenlik kuruluşu Arbor Networks'ün araştırmasına göre, günümüzde saldırı boyutları son 11 yıla göre 60 kat arttı (Hürriyet Gazetesi, 2018). Bilgi ve iletişim teknolojilerinin kullanımı gün geçtikçe artmaktadır. Siber ortamı oluşturan sistemlerinin saldırılardan korunmasını, bu ortamlarda yer alan verilerin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, ve bunların önlenmesi amacıyla yapılan çalışmalar siber güvenlik olarak adlandırılır (UDHB, 2016).

Saldırıların hedefinde bilgi olmasından dolayı, önceleri 'Bilgi Güvenliği' olarak kullanılan kavramın siber güvenliği de kapsadığına dair düşüncelerin olduğu, ancak zamanla bunun tersi olan durumun yaygınlaştığı, siber güvenliğin bilgi güvenliğini de kapsadığı görülmüştür (Şenol, 2017).

Siber güvenlik, her yıl şirketler, kurumlar kuruşlar ve devletler için daha önemli bir konu haline gelmeye başladı. Bilgisayar korsanlarının her geçen gün daha donanımlı hale gelmelerinden ve şirketlerin güvenlik açıklarını bulmalarından ötürü, bütün sektörlerden firmalar, kurumlar, kuruluşlar bu tehditle yüz yüze gelmektedir (Akçadağ Alagöz, 2012).

Siber saldırılardan dolayı birçok firma ve kuruluş hem veri kayıpları hem de maddi kayıplar verebilmektedir. Bunların en büyük sebepleri arasında, birçok şirketin yeni teknolojilere ayak uydurmayıp eski teknolojiler kullanması olarak gösterilebilir. Çünkü günümüzde eski ve basit yapıdaki sistemler yerini yeni ve karmaşık sistemlere bıraktı. Güvenlik sistemlerinin güncellenmemesi ve eski teknolojilerin kullanılıyor olması, hackerların işinin daha da kolaylaştırmaktadır (Alp, 2018).

Bilişim dünyasında kuruluşların siber güvenlik konusuna öncelikli olarak düşünmeleri ve böylece güvenlik sistemlerini geliştirmeleri, bu saldırılardan korunmalarını sağlayacak çalışmaların başında gelmektedir. Sistemler karmaşıklaştıkça siber güvenliğe ayrılan harcamalar da bununla orantılı olarak artmaktadır (STM Savunma Teknolojileri Mühendislik ve Tic. A.Ş., 2016).

Amerika Birleşik Devletleri, 2016 yılında siber güvenlik çalışmaları için 14 milyar dolarlık bir bütçe ayırırken, 2017'de ise bu bütçeyi yüzde 35 artırarak, 19 milyar dolar seviyelerine getireceğini açıkladı (Alkan,2016). 2015 yılında siber güvenliğe 250 milyon dolarlık bütçe ayıran J.P. Morgan Kurumu, 2016'da bu bütçeyi ikiye katlayarak 500 milyon dolara çıkardı. Bunların yanı sıra Bank of Amerika, Citibank ve Wells Fargo da siber güvenlik için bütçeler ayıran kurumlar arasında yer almaktadır. Cybersecurity Ventures Şirketinin 2017 ile 2021 yıllarını içine alan süreçte siber güvenlik alanındaki ürün ve hizmetlere harcanacak olan paranın 1 milyar dolar ayırdığını belirtmektedir (Morgan, 2019).

Aytekin (2015) tarafından yapılan çalışmanın amacı, siber sorunlara karşı kişi, kurum, kuruluş ve devlet düzeyinde hazırlanacak olan strateji eylem planlarında farkındalık oluşturulmasıdır. Siber güvenlik stratejimizin güncelliğini koruması, eksikliklerin yanlışlıkların ortaya çıkarılması ve siber güvenliği sağlamakla sorumlu olan kurum ve kuruluşları bilinçlendirmek amacıyla yapılmıştır.

Özbay (2015) tarafından yapılan araştırmanın amacı, siber saldırıları ve bunlara yönelik olarak savunma yöntemlerinin incelemek ve bunların ulusal güvenliği artırmak amacıyla nasıl kullanılabileceğini araştırmaktır. Araştırma sonucunda saldırı potansiyellerinin tespit edilip bunlara uygun önlemlerin alınması gerektiği vurgulanmıştır. Benzer bir çalışma Yılmaz, Ulus ve Gönen (2015) tarafından yapılmıştır. Buna göre, teknolojiye bağlı güvenlik sorunlarının ortaya çıkışı, ülkemizde ve dünyada bilgi toplumuna geçiş aşamaları, bilişim sistemleri ile

oluşturulan kritik altyapı sistemleri, bu sistemlere karşı tehditler araştırılmış ve bunlarla ilgili bilgi aktarılmıştır.

Ünver (2009) çalışmasında siber güvenlik konusunu incelemiştir. Bu kapsamda bilgi teknolojileri ve elektronik uygulamaları hakkında bilgi vermek ve bu araçlara yapılabilecek olan siber saldırı ve tehditler hakkında bilgi vererek korunma yollarına değinip, Bilgi Teknolojileri ve İletişim Kurumunun siber güvenlik konusundaki çalışmaları ile ilgili de bilgi verilmiştir. Başka bir çalışmada ise Çeliktaş (2016) Türkiye'deki siber güvenlik kavramına ilişkin inceleme ve değerlendirme yapmaktır. Buna göre, siber güvenlik kavramının alt boyutlarını iyi bir şekilde anlamak ve yaşanmış siber saldırı örneklerinden ders çıkarmak gerekmektedir. Bundan dolayı, kişilerin ve kurumların yeterli seviyede bilinç ve farkındalık düzeyine ulaşıp, uluslararası örgütler ve devletler düzeyinde yürütülen siber güvenlik çalışmalarını inceleyerek, ulusal siber güvenlik politika ve eylem planlarını oluşturmak, devletlerin siber güvenlik ile ilgili yürütmesi gerektiği asıl amaçları arasında olmalıdır.

Ada (2018) tarafından yapılan siber güvenlikle ilgili yapılan çalışmanın amacı, NATO'nun ve NATO üyesi ülkelerin uyguladığı siber güvenlik stratejileri incelenerek, Türkiye'nin uyguladığı siber güvenlik stratejisine katkılar sağlamaktır. İncelemeler sonrasında, ülkemizin stratejik planına önemli katkı sağlayacağı değerlendirilen noktalar belirlenmiştir. Tarhan (2018)' nın araştırmasının amacı, siber güvenlik ile ilgili tüm yaklaşımları geçmişten günümüze kadar incelemektir. Buna göre, siber ortam çalışmanın temelinde yer alacak; siber ortamda ortaya çıkan siber güvenlik kavramı da incelenecektir. Çalışmada siber güvenliğin uluslararası ilişkiler içerisine nasıl dâhil edildiği ve nasıl analiz edildiği vurgulanmaktadır. Aynı şekilde Okoye (2017) 'nin yaptığı çalışmada, siber güvenlikle ilgili olarak genel bir tarama yapılmış ve incelenmiştir. Bundan dolayı siber güvenlikle ilgili anahtar kelimeleri kullanarak (bilgi güvenliği, veri güvenliği, siber güvenlik, vb.) yaptığı araştırmada toplam 112 yayına ulaşmıştır.

2.2.1. Bilgi Güvenliği

Bilgi güvenliği, ortamlarda bulunan her türlü bilginin, göndericiden alıcıya ulaşana iletişimi esnasında zarar görmeden, kaybolmadan ya da başka kişilerin eline geçmeden ulaşma sürecidir (Canberk ve Sağıroğlu, 2006).

Bilişim teknolojileri geliştikçe bilgi güvenliğini sağlamak zorlaşmıştır. Çünkü teknoloji geliştikçe zararlı ve kötücül yazılımlar da gelişmektedir ve böylece önlem almak da zorlaşmaktadır.

Bilgi güvenliği, temel bileşenlerden oluşmaktadır. Bunlar, gizlilik (confidentiality), bütünlük (integrity), doğruluk (reliability), ulaşılabilirlik (availability) ve kanıt (proof) tır (Özseven, 2012).

- ✓ **Gizlilik (Confidentiality)** : Bilgilere sadece yetkili kişilerin erişiminin izin verildiği anlamına gelmektedir. Yetkisi olmayanlar bilgiye kesinlikle erişemez (Özkan, 2004).
- ✓ **Bütünlük (Integrity**) : Bilgi, bütün süreçlerde eksiksiz olarak sağlanmaktadır anlamına gelmektedir. Bilginin geçerli ve güvenilir olması sağlanması gerekmektedir.
- ✓ **Doğruluk (Relianility)** : İşlem gören bilginin kontrol dışı durumda olup bozulmasını engellemektir (Güngör, 2015).
- ✓ **Ulaşılabilirlik (Availability)** : Saklanmakta olan bilginin yetkili kişilerce istenilen zaman erişebilmesi demektir.
- ✓ **Kanıt (Proof)** : Saklanmakta olan bilginin tam ve bozulmadan kaldığının güvence edilmesi demektir (Tuğ İlçin, Adak, Çakır, 2014).

2.2.2. Siber Güvenlik İle İlgili Yurtiçinde Alınan Tedbirler

Telekomünikasyon İletişim Başkanlığı (TİB) tarafından, Türkiye'de internetin bilinçli ve güvenli kullanımıyla ilgili olarak birtakım çalışmalar ortaya konmuştur. Buna göre ülkemizde birçok yerde internetin güvenli ve bilinçli kullanımıyla ilgili seminerler vermişlerdir. Ayrıca bu konuya hizmet etmek için yayın yapan ilk internet sitesi yetişkinler için "Güvenli Web" ve çocuklar için "Güvenli Çocuk" web sayfalarını tasarlamışlardır (Bayzan ve Özbilen, 2011).

Siber güvenlik çalışmaları kapsamında ülkemizde Siber Güvenlik Kurulu kurulmuştur. Bu kurul, 3842 sayılı resmi gazetede yayınlanan bakanlar kurulu kararı ile kurulmuştur. Kuruluşundan kısa bir süre sonra ülkemizin ilk Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nı yayınlamıştır. Eylem planında bazı kritik altyapılar ele alınmıştır. Buna göre: "Bilginin gizliliği, bütünlüğü veya erişilebilirliği zarara uğradığında, ekonomik kayıplar olduğunda, siber güvenlik açıkları olduğunda düzeni kuracak veya iyileştirecek sistemleri mevcut altyapılar"

olarak belirtilmektedir. Bu plana göre çeşitli kurum ve kuruluşların bilişim sistemlerine ait siber güvenliğin sağlanması ve yaşanacak olumsuz olayların yaşanma ihtimalini azaltmak amacıyla kurumlara görev paylaşımı yapılmıştır. Bu plan 7 başlık altında birleşmiştir. Bu başlıklara göre; siber güvenlikle ilgili kanun düzenlenmesi, ulusal siber güvenlik altyapılarını saldırılardan korunabilecek seviyeye getirilmesi, siber güvenlikle ilgili yerli ve son teknoloji ürünlerin üretilmesi gibi konulara değinilmiştir (Ulusal Siber Güvenlik Stratejisi, 2013).

Siber Güvenlik Kurulunun almış olduğu kararlara göre kamu kurum ve kuruluşlarının daha güvenli bir ağ kullanmaları için, güvenli ağ alt yapısı oluşturulana kadar ağ iletiminin internete kapalı, siber saldırılara karşı daha dayanıklı ve güvenli olacak bir sanal ağ üzerinden yapılması planlanmıştır. Bu sayede siber güvenliğin daha çok sağlanması, çeşitli kamu uygulamalarının güvenle kullanılabilmesi amacıyla 2016/28 Sayılı Başbakanlık Genelgesi ile Kamu Sanal Ağı (KamuNet)' in kurulmasına karar verilmiştir (Başbakanlık Genelgesi, 2016).

Günümüzde çokça kullandığımız e-ticarete yönelik olarak 6563 sayılı kanun düzenlenmiştir. Bu kanuna göre, e ticaret iletişimini ve bu iletişimle yapılan sözleşmeleri, sözleşme dışına çıkanlara yönelik olarak yaptırımları, e ticarette kullanılan internet sağlayıcıların görev ve sorumluluklarını ortaya koyar (6563 Sayılı Kanun, 2014).

2.2.3. Siber Güvenlik İle İlgili Yurtdışında Alınan Tedbirler

1999 yılında Kosova Savaşı sırasında NATO ve NATO üyesi ülkelere yapılan siber saldırılar sonrasında NATO ‘ da “siber savunma” konusu önemli hale geldi. İlk siber saldırıların ardından 2002 yılında düzenlenen Prag Zirvesi ile NATO Siber Savunma Programı yapıldı. Bu program kapsamında, siber saldırıları bulmak ve bunları önlemek için NATO Bilgisayar Olaylarına Müdahale Birimi (NCIRC) kuruldu (Check, 2015).

2001 yılında imzalanıp, 2004 yılında yürürlüğe giren ve Budapeşte sözleşmesi olarak bilinen sözleşme, siber suçlarla ilgili olarak imzalanan ilk sözleşme özelliğini taşımaktadır. Sözleşme maddeleri; siber suçlarla mücadele etmek, siber dolandırıcılık ve telif haklarının ihlali gibi konuları kapsamaktadır (Council of Europe, 2001).

Rusya ve Çin'in siber güvenlik stratejileri incelendiğinde bu ülkelerin bu konuda uluslararası iş birliği olduğu görülmektedir. Çin, Rusya, Kazakistan, Kırgızistan, Tacikistan ve Özbekistan'ın katıldığı ve 16 Ağustos 2007 tarihinde düzenlenen 7. Devlet Başkanları Konsey Toplantısı'nda Şanghay İşbirliği Örgütü bilgi güvenliği ile ilgili bir eylem planını kabul edilmiştir (Sofaer, Clark ve Diffie, 2010).

2.3. Siber Saldırı

Siber ortamlarda bulunan teknolojilerin ve sistemlerin, güvenlik ilkelerinden herhangi birini yok etmek amacıyla, yine bu ortam içerisinde bulunan herhangi bir kişi ya da bilişim sistemleri aracılığı ile yapılan, bilerek ve isteyerek yapılan faaliyetlerdir (T.C Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 2016).

Bilişim teknolojileri vasıtasıyla hedef alınan birey, kurum, şirket, sistemler.. vs. hedef alan ve bunların işleyişini bozan, engelleyen, izinsiz olarak bilgiye erişen ve bilgi bütünlüğünü bozan saldırılardır (Şahinaslan ve Şahinaslan 2012).

Sanal ortam, üzerinde yapılan faaliyetler açısından çok geniş kapsamlı bir alana yayılmıştır. Bundan dolayı güvenlik olarak da birçok saldırının etkisi altında kalmaktadır. Siber saldırı, siber ortamdaki olanaklar kullanılarak, bilgisayar sistemleri, yazılım ya da iletişim sistemlerine yapılan kötü niyetli eylemler olarak tanımlanabilir (Yayla, 2014).

Tanımdan hareketler siber saldırılar şu şekilde sıralanabilir:

- ✓ E-postalar vasıtasıyla programlara zararlı virüsler yerleştirerek hedeflenen sistemlere gönderme,
- ✓ Bilişim Teknolojileri kullanılarak yasal olmayan yollarla kişisel bilgilerin alınması,
- ✓ Kamu ve özel kurum-kuruluşların saygınlıklarını kaybetmek ve psikolojik zarar vermek amacıyla web sitelerinin ele geçirilmesi,
- ✓ Kamu kurum ve kuruluşların web sitelerine aşırı yüklenerek sistemlerin çalışamaz duruma gelmesi, olarak sıralanabilir (Ercan, 2015).

Uygulama biçimi bakımından siber saldırılar iki farklı şekilde gerçekleşir. Birincisi, virüslü e-postalar ve spam mesajları ile kişisel bilgi ve şifrelerin ele geçirilmesi, çeşitli web sitelerine yapılan dijital saldırılardır. İkinci ise kişiyi aşağılamak, küçük düşürmek, psikolojisini bozmaya yönelik operasyonlar yapmaktır.

Siber saldırının birçok amacı olmakla birlikte genel bir çatı altında ikiye ayrılabilir:

- ✓ **Bilgiye Yönelik:** İzinsiz erişim, değiştirme, ortadan kaldırma, gizli bilgileri ortaya çıkarma.
- ✓ **Sisteme Yönelik:** İzinsiz erişim, çalışamaz hale getirme, hizmetin engellenmesi (Soğukpınar, ve Küçük, ty)

Bilgisayar ve internet sistemleri alanında uzman, bilgisayar korsanı (hacker) olarak tabir edilen, çeşitli bilişim sistemlerine zarar vermek amacıyla yapılan saldırılara siber saldırı denilmektedir (Milliyet Gazetesi, 2017).

2.3.1. Siber Saldırı Çeşitleri

Siber saldırılar, günlük yaşamdaki zorbalığın çevrimiçi ortamdaki yaşanma halidir. Saldırıların ortak amacı, kişi, kurum veya kuruluşları maddi veya manevi olarak zor duruma düşmesini sağlamaktır. Kişisel siber güvenliği sağlama boyutları ile bakıldığında Kişisel Gizliliği Koruma, Güvenilmeyenden Kaçınma, Ödeme Bilgilerini Koruma, Önlem Alma ve İz Bırakmama olarak 5'e ayırabiliriz. Yapılan saldırılar ve güvenlik tedbirleri tek bir boyutta keskin sınırlar içinde ele alınamaz ancak ağırlıklı özelliği sonucunda bu şekilde gruplandırılabilir.

2.3.1.1. Kişisel Gizliliği Koruma

Kişisel gizliliği koruma boyutunu ele aldığımızda, kişisel bilgileri tehdit eden yazılımlar aşağıda sıralanmıştır:

- ✓ **Arka Kapı (Backdoor):** Güvenlik engellerini aşıp uzaktan erişim ile sisteme zarar verirler. Bilgisayar sistemlerindeki açıkları kullanırlar.
- ✓ **Truva Atı (Trojan Horse):** Orijinal yazılım gibi görünen, kullanılmaya başlayınca da bilgisayar sistemlerine zarar veren zararlı yazılımlardır (Canberk, ve Sağıroğlu, 2007). Zararlı olan program dosyalarının çalıştırılması sonucu aktifleşirler ve kopyalama yoluyla çoğalır ve bulaşırlar. Program aktifleşmediği

sürece bilgisayara zarar veremez. Bunun sonucunda internet hızı düşer, bilgisayarlardaki dosyalara zarar verirler.

- ✓ **Virüs:** Zararlı yazılım türlerinden en çok bilineni olan virüsler, uygulama dosyaları aracılığıyla internetten üzerinden veya taşınabilir bellekler ile bilgisayarlara bulaşırlar ve işlevlerine göre sistemlere zarar verirler, çabuk yayılırlar ve hızla çoğalırlar (Çalışkan, 2013). Bilgisayarın çalışmasını engelleyerek çeşitli dosyalara zarar vererek kullanılmaz hale getirir ve veri kaybına sebep olurlar. Virüs geliştiriciler zarar verme, bilgi çalma gibi çeşitli amaçlarla virüsleri tasarlarlar (İlbaş, 2009).

- ✓ **Casus Yazılımlar (Spyware):** Bilgisayar kullanıcıların kişisel bilgilerini çalarak zarar veren yazılımlardır. Ayrıca bilgisayar sistemlerine zarar vererek bilgisayarın yavaşlamasına, donmasına da sebep olabilir (Gülmüş, 2010).

2.3.1.2. Güvenilmeyenden Kaçınma

Güvenilmeyenden kaçınma boyutunu ele aldığımızda, genel olarak güvenliğimizi tehdit eden yazılımlar aşağıda sıralanmıştır:

- ✓ **Mesaj Sağanakları (Spam**): Kullanıcının istediği dışında gelen e-postalardır. Özellikle firmaların ve kurum, kuruluşların reklamlarından oluşur. Genellikle zararsızdır ama içlerine saklanan solucanlarla zararlı hale gelebilir (Yavanoğlu, 2012).

2.3.1.3. Ödeme Bilgilerini Koruma

Ödeme bilgilerini koruma boyutunu ele aldığımızda, ödeme bilgilerini tehdit eden yazılımlar aşağıda sıralanmıştır:

- ✓ **Klavye Dinleme Sistemleri (Keylogger):** Klavye ile girilen tüm bilgileri hafızasında tutup kişisel bilgileri çalan zararlı yazılımlardır. Banka şifreleri, kredi kartı bilgileri, TC Kimlik numarası gibi önemli bilgileri çalan yazılımlardır. Maddi manevi zarar verebilirler.
- ✓ **Password Atakları:** Kullanıcıların şifrelerini ele geçiren yazılımlardır.

2.3.1.4. Önlem Alma

Önlem alma boyutunu ele aldığımızda, önlem almak için kullandığımız yazılımlar aşağıda sıralanmıştır:

- ✓ **Dijital İmzalar:** Kullanıcılara özel olan, ağ üzerinden işlem yaparken daha güvenli hale gelmesini sağlayan yazılımlardır.
- ✓ **Anti-Virüs:** Sistemlerdeki virüsleri tespit edip, durumlarına göre temizleme, yayılma ya da virüs bulaşmış dosyaları onarmak amacıyla tasarlanan yazılımlardır. Virüs koruma uygulamalarının kullanılması ve düzenli güncellenmesi gerekmektedir. Zararlı kodların sistemlere çeşitli şekillerde bulaşabileceği bu nedenle dijital sistemleri virüsten korumak amacıyla antivirüslerin kullanılması gerektiği belirtilmiştir. Farklılaşan tehditlere göre bu uygulamaların belirli zamanlarda güncellenmesi gerektiğini vurgulanmıştır (Vardal, 2009).
- ✓ **Firewall (Güvenlik Duvarı) :** Bilgisayarlarda internet trafiğini kontrol eden ve veri iletimi sırasında zararlı yazılımlara karşı sistemleri korumaya yardımcı olan yazılımlardır. İnternet üzerinde gelen yetkisiz kaynak erişimin engeller (Şahinaslan vd. 2013). Diğer bir tanımla, yerel ağı, internetten gelebilecek her türlü tehdide karşı bilgisayarı koruyan yazılımlardır (Çakar, 2005).

2.3.1.5. İz Bırakmama

İz bırakmama boyutunu ele aldığımızda, iz bırakmadan güvenliğimizi tehdit eden yazılımlar aşağıda sıralanmıştır:

- ✓ **Solucan (Worm):** E-postalarla gönderilen ek dosyalarının çalıştırılması sonucu bilgisayar sistemlerine yerleşen ve başka e-posta kullanıcıların sistemlerine bulaşan zararlı yazılımdır (Yaşar ve Çakır, 2015). Solucanlar güvenliği düşük web sitelerinden de bulaşabilmektedirler. Bir kez bilgisayara bulaştığında otomatik olarak kendiliğinden bulaşırlar ve dijital ayak izimizin raporunu oluştururlar.

- ✓ **Kök Kullanıcılar (Rootkit):** Sitemlere zarar veren saldırganın kimliğini gizler ve böylece bulunmasını zorlaştırır (Keleştemur, 2015).
- ✓ **Servis Reddetme (Dos/DDos Attack):** Denial of Service ve Distributed Denial of Service kelimelerinin kısaltılmasıdır. Dos, Dağınık Servis Engelleme anlamına gelmektedir. Sistemlere çok fazla istek göndererek sistemleri bozan veya zarar veren yazılımlardır. Bunlardan dolayı sistemler hizmet dışı kalırlar. İnternet kullanıcılarının belirli bir sisteme girmesi engellenir. DDos, Dos saldırılarının bir türü olup daha çok zarar verendir. Dos, tek bilgisayardan

yapılabildiği gibi DDos için binlerce veya yüzbinlerce bilgisayardan yapılır (Başaran, 2016).

- ✓ **Mantık Bombaları (Logic Bomb):** Güvenli olarak bilinen programlara entegre edilir ve istenilen olayın gerçekleşmesiyle veya istenilen zamanın gelmesiyle aktifleşen kötü yazılımlardır. Örnek olarak 26 Nisan da aktifleşen Çernobil Virüsü verilebilir (Başaran, 2016).
- ✓ **Oltalama (Phissing):** Çeşitli kurum, kuruluş veya firmaların web sayfalarını veya e-posta isimlerini taklit ederek bilgisayar kullanıcıların kişisel, önemli ve özel bilgilerini (kredi kartı bilgileri, banka şifreleri, anne kızlık soyadı, TC Kimlik no, Doğum yeri ve tarihi..vs) çalmayı hedefleyen kötü yazılımlardır (Çubukçu ve Bayzan 2013).
- ✓ **Spoofing (Aldatma) Atakları:** Güvenli ve bilinen bir adres, e-posta, web sayfası ismi..vb yerine geçerek sanki orijinalmiş gibi davranarak kullanıcıların dikkatini çekmeden sistemlere zarar veren yazılımlardır (Kaspersky, 2019).
- ✓ **Sniffing (Paket Dinleyici):** Güvenliği zayıf olan ağ iletimlerini takip ederek kullanıcıların önemli kişisel bilgilerini ele geçiren yazılımlardır (Ulaşanoğlu vd.,2010).
- ✓ **Sosyal Mühendislik (Social Engineering):** Yalan ve abartılı söylemlerle ve karşı tarafı inandırıp kişisel bilgileri kendisi aracılığıyla öğrenip kullanma durumudur (Aslay, 2017).

2.3.2. Yakın Geçmişte Yaşanmış Siber Saldırılar

Geçtiğimiz yıl Ekim ayında ABD'ye yapılan saldırı sonucunda ABD'nin %70 i 4-5 saat süreyle internetsiz kaldı. Birçok siteyi de etkileyen saldırı, belli başlı büyük şirketleri de belli süreliğine kullanım dışı bıraktı. Saldırıyı "New World Hackers" isimli bir hacker grubu saldırıyı üstlenmiştir (Arıman, 2017).

Estonya'da 27 Nisan günü Ping yoğunluyla başlayan siber saldırılar, hızlı bir şekilde DDOS (*Distributed Denial of Service)* saldırısına dönüştü. Bu saldırıya göre, ilk olarak birçok bilgisayar ele geçirildi ve zombi bilgisayar hâline getirildi. İkinci olarak ele geçirilen bu zombi bilgisayarlardan *Botnet* adı verilen bir ağ oluşturuldu ve belirlenen web sayfalarına aşamalı bir biçimde saldırmaları sağlanmıştır (Yener, 2015).

Rusya Federasyonu tarafından 2008 yılında Gürcistan'ı hedef alarak siber saldırılar planlanmıştır. Yapılan siber saldırılar, Gürcistan ile Rusya Federasyonu arasında dünyadaki ilk hibrit savaş örneği olarak gösterilmektedir (Goble, 2009). Siber saldırılar, 7 Ağustos 2008 gecesinden itibaren "DDoS" saldırıları şeklinde başlamıştır. Bu saldırılarda kullanılan siteler incelendiğinde, sitelerin ABD'den çalınan kredi kartlarının Rusya Federasyonu ve Türkiye'de açıldığı belirlenmiş, ayrıca saldırı için gönderilen SPAM e-postaların oluşturulduğu da tespit edilmiştir (Bıçakçı, 2012).

1990 yılında Körfez Savaşı için ABD siber savaşçıları ve askerleri ile birlikte çalışarak, Irak'ın hava savunma sistemlerini nasıl yok edeceklerini incelemişlerdir. İnceleme sonucunda bazı komutanlar, ilk olarak hava savunma sistemlerinin yok edilmesi gerektiğini, böylece havadan gelecek tehlikeye karşı savunması bozulan Irak'ı, bombalamanın daha kolay olacağı tahmininde bulunmuştur. Bu nedenle saldırılar hava savunma sistemlerine doğru başlatılmıştır. ABD Ordu İstihbarat birimi Irak ordusunun iletişim sistemleri üzerinde çalışarak, telsiz frekanslarını tespit etmiştir. Operasyon başladıktan sonra Irak iletişim sistemi gizlice dinlenmiş ve askerlerle iletişime geçilmiştir. Irak Savaşı, savaşların klasik yöntemler yerine, siber saldırılar ile yürütülebileceğini, önemli olanın siber ortam güvenliğinin sağlanması gerektiğini ve bu konuda bilinçli olunması gerektiği, bundan dolayı da savaş kazanılabileceğini gösteren, ilk büyük savaştır (Kara 2013).

2014 yılında Sony Pictures firmasına siber saldırı yapılmıştır. Farklı bir şirket, 24 kasım Sony Pictures firmasına karşı nerden geldiği tespit edilemeyen siber saldırı düzenlemiştir. Siber saldırıda firmanın gösterime girecek olan filmleri, bazı film senaryoları, firma içi özel elektronik posta ve yazışmaları da kapsayan 100 terabayt büyüklüğünde olduğu tahmin edilmekte olan veri bir hacker grubu tarafından çalınmıştır. Siber saldırı sonucunda çalınan filmler izinsiz olarak internette yayınlanmıştır. Sony firması, kendisine yapılan bu saldırı nedeniyle milyonlarca dolar zarara uğramıştır (Cieply ve Barnes, 2014).

2009'da İran'a karşı hedef alındığı öne sürülen saldırı da kullanılan virüsün adıyla anılan Stuxnet saldırısı bu faaliyetin 2009'da ABD tarafından İran'ın Natanz nükleer yakıt zenginleştirme tesislerine karşı düzenlendiği düşünülmektedir (Şenol, 2012)

30 Ocak 2009 tarihinde birçok ülkenin bilgisayar sistemine yayılan ve çok ciddi zararlar veren 'Conficker' ismindeki virüs, ülkemizde de zararlara yol açmış bunun sonucunda İstanbul'da Atatürk Havalimanı'nın çalışan bilgisayarları büyük ve olumsuz bir şekilde etkilemiştir (Şenol, 2012).

5 Ağustos 2008'de Bakü-Tiflis-Ceyhan boru Erzincan'da dolaylarında bir patlama olmuştur. Patlama sonucunda PKK terör örgütü saldırıyı üstlenmiştir. Araştırma sonucunda ise patlamanın nedeninin bir siber saldırı sonucunda gerçekleştiği ortaya çıkmıştır (Aydoğmuş, 2014).

2.3.3. Hacking ve Hacker

Bilgisayar ve ağ sistemlerine izinsiz giriş yapmakla birlikte, çeşitli bilgilere ulaşıp bu bilgileri çalma, zarar verme gibi eylemlere hacking adı verilir. Başka bir ifade ile sistemlerdeki engelleri aşarak sızma faaliyetlerine hacking adı verilir (Harris, 2006).

Hacking eylemi gerçekleştiren kimselere hacker denilmektedir Şahsi bilgisayarlara veya çeşitli kurum veya kuruluşlara ait bilgisayarlara veya ağlara izinsiz giriş yapan kişilere denir (Yeğen, 2011). Bilgisayar korsanı adı da verilmektedir. Bilgisayar ve iletişim teknolojileri konusundaki bilgisini izinsizce bilgisayar sistemlerine sızarak kullanan kişilerdir (TDK, 2019).

Hackerlar sistemdeki açıklardan faydalanarak, çeşitli uygulamaların şifresini kırabilir, sistemlere izinsiz erişebilir ve eriştikleri ortamlardan bilgi çalabilirler (Mitnick ve Simon, 2005).

Hedeflerine ve etkin oldukları alanlara göre bilinen siyah, beyaz ve gri şapkalı olmak üzere üç farklı hacker grubu vardır (Elbahadır, 2011).

2.3.3.1. Siyah Şapkalı Hackerlar

Siyah şapkalı hackerlar, hacker türleri arasında en tehlikeli ve zararlı olan hackerlardır. Her türlü sistemin açığını tespit edip sisteme girebilirler. Sisteme girdikleri zaman da sistemi çökertebilir veya sisteme zarar verebilirler.

2.3.3.2. Beyaz Şapkalı Hackerlar

Beyaz şapkalı hackerlar, hacker türleri arasında en zararsız hatta yararlı denebilecek olan hackerlardır. Bir sisteme sızınca bu sisteme zarar vermez, güvenlik açıklarını

tespit edip sistem yöneticilerine bildirirler. Bunun sonucunda da sistemdeki açığı kapatmaya çalışırlar. Kamu kurum ve kuruluşları veya özel şirketler de beyaz şapkalı hackerlardan faydalanmaktadır.

2.3.3.3. Gri şapkalı Hackerlar

Duruma göre beyaz veya siyah hacker grubuna dahil olabilen, sistem açıklarını tespit eden hacker çeşididir. Sistem açıklarını tespit ederken sistemlere izinsiz giriş yaptıkları için beyaz sayılamazlar, siyah hacker çeşidinin bir özelliğinin yansıttığından dolayı bunlara, gri hacker çeşidi adı verilmiştir.

2.4. Siber Savaş

Siber savaş, bilişim teknolojileri aracılığı ile bir ülkenin hedef seçtiği başka bir ülkenin, bilgi ve iletişim teknolojileri üzerinden düzenlenen saldırı faaliyetleri olarak tanımlanmıştır (Aslay, 2017). Başka bir tanımlama ise, bir devletin başka bir devletin bilgisayar ve ağ teknolojilerine saldırmak suretiyle sistemlerde kesinti yapmak ve bunlara zarar vermek amacıyla yapılan faaliyetlerdir (Wikizero, 2019b). Bu açıklamalardan yola çıkarak, siber savaş, siber saldırılar bütünüdür denilebilir.

BÖLÜM 3

İLGİLİ ALANYAZIN

Bu bölümde siber güvenlikle ilgili yurtiçinde ve yurtdışında yapılan çalışmalara yer verilmiştir.

3.1. Siber Güvenlik İle İlgili Yurtiçinde Yapılan Çalışmalar

Öğütçü (2010) tarafından yapılan çalışmanın amacı bireylerin internet ve bilgi teknolojilerini kullanımlarına ilişkin davranışlarını belirleyerek farkındalıklarını ve algılarını ölçmektir. Araştırmanın örneklemi güvenlik konusunda uzman 39 katılımcı ve 23 akademisyenden oluşmaktadır. Araştırma sonucunda katılımcıların farkındalık oranlarının çok yüksek olmadığı, kişisel koruma davranışların tam olarak gelişmediği görülmektedir. Konuyla ilgili olarak eğitim gören kişilerin eğitim görmeyenlere oranla farkındalıklarının daha yüksek olduğu görülmektedir.

Yılmaz ve Sağıroğlu (2013) tarafından yapılan çalışmada siber güvenlik konusunda uygulanması tavsiye edilen kurallar, siber kaynaklara uygulanabilecek olan tehditlerin ve bunlar karşısındaki önlemlerin neler olduğu ile ilgili incelemeler sunulmuştur. Araştırma sonucuna göre, siber güvenliğin sağlanabilmesi için karşılaşılabilecek tehditlerin tespiti yapılmalı, tehditler karşısında çözüm önerileri sunulup, gereken önlemler alınmalıdır.

Gökmen (2014) tarafından yapılan araştırmanın amacı, Bilgisayar ve Öğretim Teknolojileri Eğitimi bölümü öğretmen adaylarının bilişim güvenliği bilgilerini ve bu konuya yönelik eğitim verebilme yeterliliklerini ortaya koymaktır. Katılımcılar, ülke genelindeki çeşitli üniversitelerin Eğitim Fakültelerinde Bilgisayar ve Öğretim Teknolojileri Eğitimi bölümlerinde 3. ve 4. sınıfta okuyan 375 öğrenciden oluşmaktadır. Araştırma sonucunda, Bilgisayar ve Öğretim Teknolojileri Eğitimi öğretmen adayların bilgilerinin ve yeterliliklerinin beklenen seviyede olmadığı ortaya çıkmıştır.

Yaşar ve Çakır (2015) tarafından yapılan çalışmanın amacı, kurumların siber saldırılara karşı siber güvenliklerini korumaları açısından yardımcı olup kurumsal bazda yapılabilecekleri inceleyip açıklamaktır. Çalışmada görüşme ve veri analizi gibi veri toplama yöntemleri kullanılmıştır. Çalışma sonucunda kurumların siber güvenlik konusunda yeteri kadar farkındalığa sahip olmadığı tespit edilmiştir.

Akgün ve Topal (2015) tarafından yapılan çalışmanın amacı, eğitim fakültelerinde öğrenim gören öğrencilerin bilişim güvenliği farkındalıklarını ortaya koymaktadır. Araştırmada tarama modeli kullanılmıştır. Katılımcılar, Sakarya Üniversitesi Eğitim Fakültesi son sınıfta öğrenim gören ve farklı bölümlerden toplam 217 öğrenci oluşmaktadır. Araştırma sonuçlarına göre bilişim güvenliği konuları ile ilgili farkındalıklarının yeterli olmadığı ortaya çıkmıştır. Cinsiyete, bilgisayar - internet kullanım yılı gibi bazı konularda anlamlı farklılıklar olduğu bulunmuştur. Bilişim güvenliği eğitimi alan ve almayanlar katılımcılar arasında anlamlı farklılık bulunmamıştır. Araştırma sonucunda öğretmen adayları için geniş kapsamlı bir bilişim güvenliği eğitimi verilmesi önerilmektedir.

Sertçelik (2015)'e göre insanların siber uzay ile olan ilişkisi arttıkça siber uzay da güvenlik meselesi de yeni bir boyut kazanmaktadır. Gerçekleşen bir takım siber saldırıları algılamamız siber güvenliği algılamamız açısından önemini ortaya koymaktadır. Siber güvenlik, bilgisayar sistemleri ve teknoloji ile iç içe geçmiş olduğundan ve teknik boyutları birçok farklı çalışmanın konusunu oluşturduğundan siber güvenliğin teknik özellikleri incelenmemiştir. Sınırları belli olmayan siber uzayda güvenlik konusu ise kişi, kurum, kuruluş, ulusal, uluslararası düzeyde bir ihtiyaçtır. Çalışmada bu ihtiyaca dikkat çekmek amaçlanmıştır.

Erol (2016) tarafından yapılan çalışmanın amacı, siber güvenlik farkındalık yeterlilik düzeyinin ölçülmesine yönelik yetenek tabanlı dinamik bir model geliştirmek ve bu model ile ilgili değerlendirmeler yapmaktır. Araştırma sonucunda, geliştirilen modelin siber güvenlik farkındalığının arttırılmasına olumlu katkılar sağlayacağı gözlemlenmiştir.

Karacı ve Akyüz (2017) tarafından yapılan çalışmanın amacı, Bilgisayar Mühendisliği ile Bilgisayar ve Öğretim Teknolojileri Öğretmenliği (BÖTE) bölümlerinde öğrenim gören üniversite öğrencilerinin siber güvenlik davranışlarını farklı değişkenler açısından incelemektir. Çalışmanın sonuçlarına göre öğrencilerin siber güvenliğe yönelik davranışlarının siber güvenliği sağlayacak düzeyde olduğu görülmektedir. Katılımcılar, kişisel gizliliklerini koruyabilmektedirler. Ayrıca güvenilmeyen uygulamalardan kaçınmakta ve güvenlik için önlem alabilmektedirler. Cinsiyet ile siber güvenlik davranışları arasında anlamlı bir farklılık olmadığı görülmüştür.

Ünal ve Ergen (2018) tarafından yapılan çalışmanın amacı, kişilerin siber ortamda gerçekleştirdikleri faaliyetlerde siber güvenlikle ilgili davranışları ölçülmüştür. Araştırmanın katılımcıları, İstanbul'da yaşayan 18 yaş üzeri 335 bireyden oluşmaktadır. Veriler, internet ortamında anket yoluyla toplanmıştır. Siber güvenlik davranışının demografik faktörlere göre farklılaşıp farklılaşmadığı incelenmiştir. Araştırma sonucunda kadınların yazılım güncelleme sıklığının erkeklerden yüksek olduğu, özel sektör çalışanlarında cihaz güvenliği davranışı sıklığının kamu çalışanlarından yüksek olduğu ortaya çıkmıştır. Çıkan sonuçlara göre sonraki çalışmalarda kişilerin siber güvenlik davranışına neden olan etmenlerin araştırılması önerilmektedir.

3.2. Siber Güvenlik İle İlgili Yurtdışında Yapılan Çalışmalar

Pusey ve Sadera (2011) tarafından yapılan araştırmanın amacı, öğretmen adaylarının bilişim güvenliği ve bilişim etiği konusunda bilgilerini ve bu konular ile ilgili eğitim verebilme durumlarını ortaya çıkarmaktır. Araştırma kapsamında 318 öğretmen adayına bilişim güvenliği ve etiği konularına yönelik 75 konuyu içeren sorulardan oluşan bir anket uygulanmıştır. Araştırma sonucunda, öğretmen adaylarının bilişim güvenliği ve etiği konusunda yetersiz bilgiye sahip oldukları ve bu konuda eğitim verecek yeterlilikte olmadığı sonucuna ulaşılmıştır.

Kruger, Flowerday, Drevin ve Steyn (2011) tarafından yapılan çalışmanın amacı, kültürel etmenlerin siber güvenlik farkındalığı üzerinde etkisini incelemektir. Çalışmada, Anadil, mezun olunan okul, yaşanılan yer gibi kültürel etmenlerin siber güvenlik üzerinde etkisi incelenmiştir. Güney Afrika'nın iki üniversitesindeki 180 katılımcıya; phishing, casus yazılım, virüs, solucan, spam şifre, sosyal mühendislik gibi saldırılar hakkında bilgilerini ölçen test yapılmıştır. Katılımcıların virüs, spam, casus yazılım ve şifre konularında bilgi sahibi oldukları ancak sosyal mühendislik ve onunla ilgili konularda pek bilgi sahibi olmadıkları gözlenmiştir. Araştırma sonucunda, siber güvenlik farkındalık programı planlanırken kültürel etmenlerin de değerlendirilmesi gerektiği önerilmiştir.

Shehri (2012) tarafından yapılan çalışmanın amacı, kişilerin siber güvenlik davranışlarını incelemektir. Araştırma farklı kültür ve bilgi birikimine sahip 35 ülkeden 200 kullanıcı üzerinde uygulanmıştır. Araştırma sonucunda katılımcılardan bazılarının iyi düzeyde olmasına karşın bu bilgiyi kullanamadığı ve buna göre davranmadıklarını ortaya çıkarmıştır.

Agamba ve Keengwe (2012) tarafından yapılan çalışmanın amacı, öğretmen adaylarının siber suçlarını önlemede tedbir alma davranışlarını incelemektir. Araştırmada 19 öğretmen adayına siber suç farkındalığı ve siber suçlarını önlemeye yönelik görüşlerini içeren 20 soruluk bir anket uygulanmıştır. Araştırma sonucunda öğretmen adaylarının bilişim suçu bilgisinin, siber güvenlikle ilgili yazılım kullanma farkındalığının yüksek düzeyde olduğu ortaya çıkmıştır. Ancak öğretmen adaylarının siber suçları önlemek için gerekli tedbirleri almadıkları ortaya çıkmıştır.

Desai (2013) tarafından yapılan çalışmada, idarecilerin siber güvenlik alanında gerekli yatırım yapmak ve bu alanda çalışmak ve önlem almak için yeterli düzeyde bilgilerinin olmadıklarını belirtmiştir. Ayrıca çalışmada kurum ve kuruluşların hızla artan siber tehditlerle mücadelede yetersiz kaldığı ve bu alanda yapılan eğitimlere de gereken hassasiyetin vermediğini vurgulamıştır.

Mil (2015) tarafından yapılan çalışmanın amacı, Sosyal Güvenlik Kurumu'nun siber güvenlik açısından uygulamaları incelenmiş ve değerlendirmiştir. Araştırma sonucundan Sosyal Güvenlik Kurumun siber güvenlik ile ilgili belgeleri olmasına rağmen bu belgelerdeki kuralların hepsinin uygulanmadığı ortaya çıkmıştır. Çıkan sonuçlardan hareketle, siber güvenlik ile ilgili belgelerinde yer alan kuralların ve sorumlulukların ilgili kişilere eğitim verilerek öğretilmesi gerektiğinin üzerinde durulmuştur.

Tomlin (2016) tarafından yapılan çalışmanın amacı, kuruluşların siber güvenlik farkındalık durumlarını incelemektir. Araştırma sonucunda siber güvenlik durumlarını kontrol edebildikleri araçların, siber güvenlik farkındalık düzeylerini artırdığını ve tehditlere karşı korunmaya yardımcı olacağını tespit etmiştir.

BÖLÜM 4

YÖNTEM

Bu bölümde araştırmanın modeli, araştırma evreni ve örneklemi, veri toplama araçları, verilerin toplanması ve çözümlenmesinde kullanılan istatistiksel yöntem ve teknikler yer almaktadır.

4.1. Araştırmanın Modeli

Bu araştırmada, öğretmen adaylarının kişisel siber güvenlik durumlarını incelemek amacıyla, bir ölçme aracı kullanılmıştır. Araştırmada tarama modeli kullanılmıştır. Tarama modeli, çok sayıda katılımcı ya da nesneden oluşan bir evrende tahminlerde bulunarak bir yargıya varmak amacıyla evrende veya örneklemde gerçekleştirilen, araştırmacının bağımsız değişkenler üzerinde hiçbir etkisisin olmadığı araştırma desenlerine denir (Büyüköztürk, 2002).

Bu araştırma, öğretmen adaylarının kişisel siber güvenlik konusundaki davranışları ve buna etki eden bazı değişkenlerle karşılaştırma yapmaya olanak tanıyan bir araştırmadır. Tarama modelinin olduğu çalışmalarda, tekil veya ilişkisel adı verilen tarama çeşitleri kullanılabilmektedir.

Tekil tarama modeli, katılımcıların demografik bilgilerinin, araştırmayı amaçlanan konuyla ilgili olarak, görüşleri, düşünceleri, davranışlarını saptamak amacıyla kullanılır (Büyüköztürk, 2002). İlişkisel tarama modeli ise, iki veya daha fazla değişken arasında olumlu veya olumsuz ilişkilerin durumunu, bir ilişki durumu varsa da bunun derecesini belirleyip sebep sonuç ilişkisini bulmak amacıyla kullanılır (Büyüköztürk, Çakmak, Akgün, Karadeniz ve Demirel, 2008).

Bu araştırmada, eğitim fakültelerinde okuyan öğrencilerin, cinsiyet, öğrenim gördüğü sınıf, not ortalaması, öğrenim gördüğü bölüm, gelecek hakkındaki düşünceler ve internet kullanma sıklığı gibi değişkenlerin kişisel siber güvenlik sağlama biçimleri ile ilişkisi incelenmiştir. Araştırmaya katılan katılımcıların, değişkenlerle ilgili algıların belirlenmesi için tekil tarama kullanılmıştır.

4.2. Evren ve Örneklem

Araştırmanın evreni, 2017-2018 eğitim-öğretim yılında Konya ilinde eğitim fakültelerinde öğrenim görmekte olan öğrencilerden oluşmaktadır. Örneklem ise, 2017-2018 eğitim-öğretim yılında Konya ilinde eğitim fakültelerinde öğrenim görmekte olan rastgele seçilen 809 öğrenciden oluşmaktadır. Araştırmaya katılan öğretmen adaylarının cinsiyete göre dağılımları Tablo 1'de gösterilmiştir.

Tablo 1 : Araştırmanın Katılımcılarına Ait Demografik Bilgiler

Cinsiyet	N	%
Erkek	270	33,4
Kadın	539	66,6
Toplam	809	100

Tablo 1 incelendiğinde araştırmaya katılan öğrenciler cinsiyetleri açısından erkek öğrenciler örneklemin %33,4 (n=270), kız öğrenciler %66,6'sını (n=539) oluşturmaktadır. Araştırmaya katılan öğretmen adaylarının öğrenim gördükleri bölüme göre dağılımları Tablo 2'de gösterilmiştir.

Tablo 2 : Araştırmanın Katılımcılarına Branş/Bölüm Bilgileri

Branş/Bölüm	N	%
Türkçe Eğitimi	131	16,2
Matematik Eğitimi	105	13
Bilgisayar ve Öğretim Teknolojileri Eğitimi	237	29,3
Sosyal Bilgiler Eğitimi	63	7,8
Psikolojik Danışmanlık ve Rehberlik Eğitimi	39	4,8
Sınıf Eğitimi	234	28,9
Toplam	809	100

Tablo 2 incelendiğinde araştırmaya katılan öğretmen adaylarının %16,2'si Türkçe (n=131), %13'ü Matematik (n=105), %29,3'ü Bilgisayar ve Öğretim Teknolojileri Eğitimi (n=237), %7,8'i Sosyal Bilgiler (n=63), %4,8'i Psikolojik Danışmanlık ve Rehberlik (n=39) ve %28,9'u Sınıf Öğretmenliği bölümlerinde

(n=234) öğrenim görmektedir. Araştırmaya katılan öğrencilerin öğrenim gördükleri sınıf kademesine göre dağılımları Tablo 3'te gösterilmiştir.

Tablo 3 : Katılımcıların Öğrenim Gördükleri Sınıf Kademesine Göre Bilgileri

Sınıf Kademesi	N	%
1. Sınıf	229	28,3
2. Sınıf	243	30,0
3. Sınıf	221	27,3
4. Sınıf	116	14,3
Toplam	809	100

Tablo 3 incelendiğinde araştırmaya katılan öğretmen adaylarının %28,3'ü 1. Sınıf (n=229), %30'u 2. Sınıf (n=243), %27,3'ü 3. Sınıf (n=221), %14,3'ü 4. Sınıfta (n=116) öğrenim görmektedir. Araştırmaya katılan öğrencilerin internet kullanım sıklığına göre dağılımları Tablo 4'te gösterilmiştir.

Tablo 4 : Katılımcıların İnternet Kullanma Sıklığına Göre Bilgileri

İnternet Kullanma Sıklığı	N	%
Az	80	9,9
Orta	229	28,3
Yüksek	198	24,5
Çok Yüksek	302	37,3
Toplam	809	100

Tablo 4 incelendiğinde araştırmaya katılan öğretmen adaylarının %9,9'u az (n=80), %28,3'ü orta (n=229), %24,5'i yüksek (n=198), %37,3'ü çok yüksek düzeyde (n=302) internet kullanmaktadır.

4.3. Veri Toplama Araçları ve Verilerin Toplanması

Araştırmanın amacı, öğretmen adaylarının kişisel siber güvenlik davranışlarının farklı değişkenlere göre belirlenmesi ve incelenmesidir. Araştırma verileri bir ölçme aracı ve kişisel bilgiler formu ile toplanılmıştır.

4.3.1. Kişisel Bilgiler Formu

Araştırmacı tarafından hazırlanan kişisel bilgiler formunda, demografik bilgiler yer almaktadır. Öğretmen adayının; cinsiyet, öğrenim gördüğü sınıf, öğrenim gördüğü bölüm, not ortalaması, internet kullanım sıklığı ile ilgili bilgiler toplanmıştır.

4.3.2. Kişisel Siber Güvenliği Sağlama Ölçeği

Erol ve Arkadaşları tarafından geliştirilen "Kişisel Siber Güvenliği Sağlama Ölçeği", Uzman görüşü doğrultusunda 54 maddeden oluşan ölçek 29 madde atılarak 25 maddeye düşürülmüştür. Ölçek 5'li likert tipi olarak hazırlanmıştır ve her bir madde, 1-Hiçbir zaman 2-Nadiren 3-Ara sıra 4-Sık sık ve 5-Her zaman arası değerler almaktadır. 5 faktörden oluşmaktadır. (1. alt boyut: Kişisel Gizliliği Koruma, 2. alt boyut: Güvenilmeyenden Kaçınma, 3. alt boyut: Önlem Alma, 4. alt boyut: Ödeme Bilgilerini Koruma ve 5. alt boyut İz Bırakmama) Ayrıca ölçekte yer alan 10 madde ters madde olarak belirlenmiştir. Ölçeğin yapı geçerliliğinin test edilmesi için açımlayıcı faktör analizi yapılmıştır. Faktör analizi sonucunda oluşan ölçeğin tamamında ve faktör analizi sonucu belirlenen her alt boyutta ölçek maddelerinin güvenilirlik analizi yapılmıştır. Ölçeğin iç tutarlılık katsayısının hesaplanması için Cronbach Alpha katsayısı (α) kullanılmıştır. Buna göre ölçeğin tamamı için güvenilirlik kat sayısı 0.735; 1. alt boyut Kişisel Gizliliği Koruma için 0.763; 2. alt boyut Güvenilmeyenden Kaçınma için 0.771; 3. alt boyut Önlem Alma için 0.704; 4. alt boyut Ödeme Bilgilerini Koruma için 0.829; 5. alt boyut İz Bırakmama için ise 0.557 olarak bulunmuştur (Erol, Şahin, Yılmaz, Haseski; 2015).

4.4. Verilerin Analizi

Verilerin elektronik ortama aktarılmasında beşli likert tipinden oluşan kişisel siber güvenliği sağlama ölçeğinin maddelerin puanlanmasında 1-Hiçbir zaman 2-Nadiren 3-Ara sıra 4-Sık sık ve 5-Her zaman arası değerler almaktadır. Ölçekte ters maddeler bulunduğundan yorumlamayı kolaylaştırmak için 10 maddeye (M5, M7, M13, M12, M18, M17, M19, M20, M24 M25) tersten puanlama yapılmıştır. Çalışmanın amaçlarını test etmek için IBM SPSS 23 programı kullanılarak analizler yapılmıştır. Aşağıda uygulanan istatistiksel analizler sırasıyla açıklanmıştır.

4.5. Ölçeklerin Geçerlilik ve Güvenilirlik Analizleri

Araştırma hipotezlerinin test edilebilmesi için araştırmada kullanılan ölçeklerin seçilen örneklemde teorik olarak geliştirilen yapısına uygun olup olmadığının yani geçerliliğinin ve ölçülmek istenen yapıların ne kadar az hata ile doğru olarak ölçüldüğünün yani güvenilirliğinin incelenmesi gerekmektedir (Büyüköztürk, 2002). Araştırma da kullanılan ölçeklerin geçerlilik ve güvenilirlik analizlerinin sonuçları her ölçek için ayrı ayrı aşağıda gösterilmiştir.

Kişisel Siber Güvenliği Sağlama Ölçeği

Ölçeğin beş faktörünün güvenilirliğini değerlendirmek için Cronbach Alfa iç tutarlılık katsayıları hesaplanmıştır. Kişisel Gizliliği Koruma boyutu için (M5-M7-M12-M13-M17-M18-M19-M20-M24-M25 maddeler) $\alpha = 0,66$ olarak bulunmuştur. Ödeme Bilgilerini Koruma boyutu için (M15-M16) için güvenilirlik katsayısı $\alpha = 0,64$ olarak bulunmuştur. Güvenilmeyenden Kaçınma boyutu için (M9-M10-M11-M22) $\alpha = 0,70$ olarak bulunmuştur. İz Bırakmama boyutu için (M8-M14- M21-M23) $\alpha = 0,56$ olarak bulunmuştur. Önlem Alma boyutu için (M1-M2-M3-M4-M6) $\alpha = 0,61$ olarak bulunmuştur Güvenilirlik katsayısı için 0.70 seviyesine ulaşılması arzu edilmektedir (Büyüköztürk, 2018). Yeni ölçekler için bu seviye 0.60 lara kadar çekilebilmektedir. Bu haliyle siber güvenlik sağlama ölçeği boyutlarının asgari düzeyde güvenilir kabul edilebileceği değerlendirilmiştir.

Öğretmen adaylarının kişisel siber güvenlikle ilgili genel durumlarını ve 25 madde üzerinden durumlarını belirlemek için betimsel istatistiklerden aritmetik ortalama, yüzde ve frekanstan yararlanılmıştır. Bu açıdan öğretmen adayların kişisel siber güvenlikle ilgili maddeler, alt boyut ortalama puanları ve ölçek geneli ortalama puanları 1 ile 5 arasındadır. Öğretmen adaylarının kişisel siber güvenlik düzeyleri çok düşük, düşük, orta, yüksek ve çok yüksek olmak üzere 5 farklı kategoride değerlendirilmiştir. Bu kapsamda 5 ayrı grup bulunmasından dolayı değerlendirme aralığı için (en yüksek puan – en düşük puan)/ grup sayısı ((5-1)/5=0,80) formülü ile gruplar arası değerlendirme aralıkları belirlenmiştir. Öğretmen adaylarının kişisel siber güvenlik yeterliliklerinin değerlendirme ölçütü olarak Tablo 5'teki gibi bir değerlendirme aralığı benimsenmiştir.

Tablo 5 : Öğretmen Adaylarının Kişisel Siber Güvenlik Yeterliliklerini Değerlendirme Ölçütü

Değerlendirme Aralığı	Değerlendirme Ölçütü
1,00 - 1,79	Çok Düşük Düzey
1,80 - 2,59	Düşük Düzey
2,60 - 3,39	Orta Düzey
3,40 - 4,19	Yüksek Düzey
4,20 - 5,00	Çok Yüksek Düzey

Tablo 4'e göre 1,00-1,79 aralığı çok düşük düzey, 1,80-2,59 aralığı düşük düzey, 2,60-3,39 aralığı orta düzey, 3,40-4,19 aralığı yüksek düzey, 4,20-5,00 aralığı çok yüksek düzey olarak belirlenmiştir.

Diğer yandan öğretmen adaylarının kişisel siber güvenliği sağlaması açısından genel durumları bazı değişkenler açısından incelenmiştir. Bu amaçla farklılığı ve ilişkiyi belirlemeye yönelik istatistiklerden de faydalanılmıştır. Öğretmen adaylarının kişisel siber güvenlik düzeylerinin cinsiyet ve gelecekle ilgili algıları açısından farklılığını belirlemek için bağımsız gruplar arası t-testi (Independent Sample t-Test); öğrenim gördüğü bölüm, öğrenim gördüğü sınıf kademesi, internet kullanım sıklığı, not ortalamaları açısından farklılığını belirlemek için ise tek yönlü varyans analizi (One Way ANOVA) kullanılmıştır. Ayrıca tek yönlü varyans analizinde gruplar arasında farklılığı belirlemek için post-hoc testlerinden de yararlanılmıştır.

BÖLÜM 5

BULGULAR VE YORUMLAR

Öğretmen adaylarının kişisel siber güvenlik sağlama durumlarının araştırıldığı bu araştırmada alt amaçlar da dikkate alınarak bulgular başlıklar halinde verilmiştir.

5.1.Kişisel Siber Güvenliği Sağlama Durumlarından Kaynaklanan Farklılıkların Analizi

Öğretmen adaylarının öğrenim gördükleri sınıflara göre kişisel siber güvenliği sağlama ölçeğinden aldıkları puanların ortalamaları ve standart sapmaları Tablo 6' da gösterilmiştir.

Öğretmen adaylarının kişisel siber güvenliği sağlama ölçeğinden aldıkları puanların ortalamalarına göre 1 madde çok düşük derecesinde bulunmuştur. Bu madde, şöyle belirtilmektedir. "Tanımadığım kişilerle web kamerası kullanarak sesli ve görüntülü iletişim kurarım." Bu maddeden alınan puan ortalaması 1,61 ve standart sapması 1,23 olarak bulunmuştur.

Öğretmen adaylarının kişisel siber güvenliği sağlama ölçeğinden aldıkları puanların ortalamalarına göre 7 madde düşük derecesinde bulunmuştur. Bu maddelerden, bazıları şöyle belirtilmektedir. "Banka, online alışveriş siteleri gibi sitelerden gelen e-postalara (kart no, şifre vb. istekler) itibar ederim ve yanıtlarım." maddesinden alınan puanlardan oluşan ortalama 2,14 Standart Sapma 1,28 olarak bulunmuştur. "İnternet ortamında gerektiği zaman kişisel bilgilerimi (TC No, Doğum Tarihi, GSM No vb.) paylaşırım" maddesinden alınan puanlardan oluşan ortalama 2,29 Standart Sapma 1,24 olarak bulunmuştur. "Sosyal ağlarda yer alan reklamlar üzerinden alışveriş yaparım." maddesinden alınan puanlardan oluşan ortalaması 1,89 standart sapması 1,09 olarak bulunmuştur.

Öğretmen adaylarının kişisel siber güvenliği sağlama ölçeğinden aldıkları puanların ortalamalarına göre 6 madde orta derecesinde bulunmuştur. Bu maddelerden, bazıları şöyle belirtilmektedir. "E-posta ile gelen kimlik doğrulama mesajlarını (kullanıcı adı, şifre vb. istekler) cevaplarım." maddesinden alınan puanlardan oluşan ortalama 3,19 Standart Sapma 1,36 olarak bulunmuştur. "İnternette kullandığım hesapların (e-posta, sosyal ağ vb.) şifrelerini değiştiririm."

maddesinden alınan puanlardan oluşan ortalaması 3,13 standart sapması 1,20 olarak bulunmuştur.

Tablo 6 : Öğretmen Adaylarının Kişisel Siber Güvenlik Sağlama Durumları

	N	x̄	SS	
1. Web sayfalarında güvenlik bağlantılarını (https://) ve sertifikalarını kontrol ederim.	809	2,76	1,24	Orta
2. Kullandığım yazılımları güncellerim.	809	3,54	1,17	Yüksek
3. Bilgisayarımda anti-virüs yazılımı bulundururum.	809	3,81	1,32	Yüksek
4. Şifrelerimi belirlerken basit dizilimler kullanmaktan kaçınırım.	809	3,87	1,18	Yüksek
5. İnternet şifrelerimin tümümün aynı olmasına dikkat ederim.	809	3,21	1,3	Orta
6. Web tarayıcımın güvenlik ayarlarını düzenlerim.	809	3,12	1,25	Orta
7. E-posta ile gelen kimlik doğrulama mesajlarını (kullanıcı adı, şifre vb. istekler) cevaplarım.	809	3,19	1,36	Orta
8. Şahsi bilgisayarım dışında kullandığım bilgisayarlarda bilgilerimin kalmamasına dikkat ederim.	809	4,37	1,04	Çok Yüksek
9. İnternet üzerinden yapılan para ve kontör isteklerini dikkate almam.	809	4,18	1,39	Yüksek
10. Tanımadığım kişilerden gelen sosyal ağ arkadaşlık isteklerini kabul etmem.	809	4	1,28	Yüksek
11. Güvenmediğim sitelere üye olmam.	809	4,3	1,24	Çok Yüksek
12. Tanımadığım kişilerle web kamerası kullanarak sesli ve görüntülü iletişim kurarım.	809	1,61	1,23	Çok Düşük
13. İnternet ortamında gerektiği zaman kişisel bilgilerimi (TC No, Doğum Tarihi, GSM No vb.) paylaşırım.	809	2,29	1,24	Düşük
14. Web geçmişini temizlerim.	809	3,77	1,16	Yüksek
15. İnternet bankacılığı işlemlerimi şahsi bilgisayarımdan yaparım.	809	3,72	1,37	Yüksek
16. Online alışveriş işlemlerini şahsi bilgisayarımdan yaparım.	809	3,69	1,35	Yüksek
17. Tanımadığım kişilerden gelen e-posta eklerini açarım.	809	2,11	1,13	Düşük
18. Sosyal paylaşım sitelerinde kişisel bilgilerime yer veririm.	809	2,46	1,14	Düşük
19. İnternet üzerinden yer bildirimi yaparım.	809	2,57	1,24	Düşük
20. Sosyal ağlarda yer alan reklamlar üzerinden alışveriş yaparım.	809	1,89	1,09	Düşük
21. Sosyal ağ, e-posta gibi hesaplarda işim bittiğinde oturumu kapatırım.	809	3,89	1,27	Yüksek
22. Güvenmediğim sitelerden dosya indirmem.	809	3,77	1,33	Yüksek
23. İnternette kullandığım hesapların (e-posta, sosyal ağ vb.) şifrelerini değiştiririm.	809	3,13	1,2	Orta
24. Unutmamak için akılda kalan kolay bir şifre belirlerim.	809	3,02	1,39	Orta
25. Banka, online alışveriş siteleri gibi sitelerden gelen e-postalara (kart no, şifre vb. istekler) itibar ederim ve yanıtlarım.	809	2,14	1,28	Düşük
Kişisel Gizliliği Koruma Alt Boyutu	809	2,24	0,72	Düşük
Ödeme Bilgilerini Koruma Alt Boyutu	809	3,15	0,87	Orta
Güvenilmeyenden Kaçınma	809	4,16	1,03	Yüksek
İz Bırakmama	809	3,64	0,81	Yüksek
Önlem Alma	809	3,93	0,83	Yüksek
Genel	809	3,38	0,47	Orta

"Web sayfalarında güvenlik bağlantılarını (https://) ve sertifikalarını kontrol ederim." maddesinden alınan puanlardan oluşan ortalaması 2,76 standart sapması 1,24 olarak bulunmuştur.

Öğretmen adaylarının kişisel siber güvenliği sağlama ölçeğinden aldıkları puanların ortalamalarına göre 13 madde yüksek derecesinde bulunmuştur. Bu maddelerden, bazıları şöyle belirtilmektedir. "Şifrelerimi belirlerken basit dizilimler kullanmaktan kaçınırım." maddesinden alınan puanlardan oluşan ortalama 3,87 Standart Sapma 1,18 olarak bulunmuştur. "Tanımadığım kişilerden gelen sosyal ağ arkadaşlık isteklerini kabul etmem." maddesinden alınan puanlardan oluşan ortalama 4,00 Standart Sapma 1,28 olarak bulunmuştur. "Sosyal ağ, e-posta gibi hesaplarda işim bittiğinde oturumu kapatırım." maddesinden alınan puanlardan oluşan ortalaması 3,89 standart sapması 1,27 olarak bulunmuştur.

Öğretmen adaylarının kişisel siber güvenliği sağlama ölçeğinden aldıkları puanların ortalamalarına göre 2 madde çok yüksek derecesinde bulunmuştur. Bu maddeler, şöyle belirtilmektedir. "Şahsi bilgisayarım dışında kullandığım bilgisayarlarda bilgilerimin kalmamasına dikkat ederim." maddesinden alınan puanlardan oluşan ortalaması 4,37 standart sapması 1,04 olarak bulunmuştur. "Güvenmediğim sitelere üye olmam." maddesinden alınan puanlardan oluşan ortalaması 4,30 standart sapması 1,24 olarak bulunmuştur.

Öğretmen adaylarının kişisel siber güvenliği sağlama ölçeğinin "Kişisel Gizliliği Koruma Alt Boyutu" ndan aldıkları puanların ortalama ve standart sapmalarına göre düşük derecesinde puanlar alınmıştır. Bu alt boyuttan alınan puanların ortalaması 2,24 ve standart sapması 0,72 olarak bulunmuştur.

Öğretmen adaylarının kişisel siber güvenliği sağlama ölçeğinin "Ödeme Bilgilerini Koruma Alt Boyutu" ndan aldıkları puanların ortalama ve standart sapmalarına göre orta derecesinde puanlar alınmıştır. Bu alt boyuttan alınan puanların ortalaması 3,15 standart sapması 0,87 olarak bulunmuştur.

Öğretmen adaylarının kişisel siber güvenliği sağlama ölçeğinin "Güvenilmeyenden Kaçınma Alt Boyutu" ndan aldıkları puanların ortalama ve standart sapmalarına göre yüksek derecesinde puanlar alınmıştır. Bu alt boyuttan alınan puanların ortalaması 4,16 standart sapması 1,03 olarak bulunmuştur.

Öğretmen adaylarının kişisel siber güvenliği sağlama ölçeğinin "İz Bırakmama Alt Boyutu" ndan aldıkları puanların ortalama ve standart sapmalarına göre yüksek

derecesinde puanlar alınmıştır. Bu alt boyuttan alınan puanların ortalaması 3,64 standart sapması 0,81 olarak bulunmuştur.

Öğretmen adaylarının kişisel siber güvenliği sağlama ölçeğinin "Önlem Alma Alt Boyutu" ndan aldıkları puanların ortalama ve standart sapmalarına göre yüksek derecesinde puanlar alınmıştır. Bu alt boyuttan alınan puanların ortalaması 3,93 standart sapması 0,83 olarak bulunmuştur.

Öğretmen adaylarının kişisel siber güvenliği sağlama ölçeğinden genel olarak aldıkları puanların ortalama ve standart sapmalarına göre orta derecesinde puanlar alınmıştır. Bu ölçekten alınan puanların ortalaması 3,38 standart sapması 0,47 olarak bulunmuştur.

5.2. Kişisel Siber Güvenliği Sağlama Üzerinde Cinsiyete Göre Kaynaklanan Farklılıkların Analizi

Kişisel siber güvenliği sağlama durumlarının cinsiyete göre anlamlı bir farklılık gösterip göstermediğinin test edilmesi için bağımsız örneklem t testi yapılmıştır. Analiz sonrasında elde edilen bulgular Tablo 7' de sunulmuştur.

Kadın Öğretmen adaylarının kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "Kişisel Gizliliği Koruma" faktöründen aldıkları puanların ortalaması 2,10 Standart sapması ,67 olarak bulunmuştur. Erkek öğretmen adaylarının aynı ölçeğin aynı alt faktöründen aldıkları puanlarının ortalaması 2,52 ve standart sapması ,73 olarak bulunmuştur. Gruplar arasında anlamlı bir fark olup olmadığını belirlemek için bağımsız örneklem t-testi yapılmıştır ($t= -7,93$; $p<.05$). Buna göre erkek öğretmen adaylarının kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "Kişisel Gizliliği Koruma" konusunda farkındalık düzeylerinin kadın öğretmenlerden daha fazla oldukları söylenebilir.

Kadın Öğretmen adaylarının kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "Ödeme Bilgilerini Koruma" faktöründen aldıkları puanların ortalaması 3,04 Standart sapması ,83 olarak bulunmuştur. Erkek öğretmen adaylarının aynı ölçeğin aynı alt faktöründen aldıkları puanlarının ortalaması 3,37 ve standart sapması ,90 olarak bulunmuştur.

Tablo 7 : Öğretmen Adaylarının Cinsiyetlerine Göre Kişisel Siber Güvenlik Durumları

	Cinsiyet	N	x̄	S.S.	t	p
Kişisel Gizliliği Koruma	Kadın	539	2,10	,67	-7,93	0,00
	Erkek*	270	2,52	,73		
Ödeme Bilgilerini Koruma	Kadın	539	3,04	,83	-5,24	0,00
	Erkek*	270	3,37	,90		
Güvenilmeyenden Kaçınma	Kadın*	539	4,29	1,00	5,23	0,00
	Erkek	270	3,90	1,03		
İz Bırakmama	Kadın	539	3,63	,82	-0,62	0,54
	Erkek*	270	3,66	,81		
Önlem Alma	Kadın	539	3,91	,85	-1,35	0,18
	Erkek*	270	3,99	,80		
Kişisel Siber Güvenliği Sağlama	Kadın	539	3,35	,47	-3,87	0,00
	Erkek*	270	3,48	,48		

Gruplar arasında anlamlı bir fark olup olmadığını belirlemek için bağımsız örneklem t-testi yapılmıştır (t= -5,24; p<.05). Buna göre erkek öğretmen adaylarının kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "Ödeme Bilgilerini Koruma" konusunda farkındalık düzeylerinin kadın öğretmenlerden daha fazla oldukları söylenebilir.

Kadın Öğretmen adaylarının kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "Güvenilmeyenden Kaçınma" faktöründen aldıkları puanların ortalaması 4,29 Standart sapması 1,00 olarak bulunmuştur. Erkek öğretmen adaylarının aynı ölçeğin aynı alt faktöründen aldıkları puanlarının ortalaması 3,90 ve standart sapması 1,03 olarak bulunmuştur. Gruplar arasında anlamlı bir fark olup olmadığını belirlemek için bağımsız örneklem t-testi yapılmıştır (t= 5,23; p<.05).

Buna göre kadın öğretmen adaylarının kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "Güvenilmeyenden Kaçınma" konusunda farkındalık düzeylerinin kadın öğretmenlerden daha fazla oldukları söylenebilir.

Kadın Öğretmen adaylarının kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "İz Bırakmama" faktöründen aldıkları puanların ortalaması 3,63 Standart sapması ,82 olarak bulunmuştur. Erkek öğretmen adaylarının aynı ölçeğin aynı alt faktöründen aldıkları puanlarının ortalaması 3,66 ve standart sapması ,81 olarak bulunmuştur. Gruplar arasında anlamlı bir fark olup olmadığını belirlemek için bağımsız örneklem t-testi yapılmıştır ($t= -0,62$; $p>.05$). Buna göre erkek öğretmen adaylarının kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "İz Bırakmama" konusunda kadın öğretmenlerden istatistiksel olarak anlamlı bir farklılık göstermediği söylenebilir.

Kadın Öğretmen adaylarının kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "Önlem Alma" faktöründen aldıkları puanların ortalaması 3,91 Standart sapması ,85 olarak bulunmuştur. Erkek öğretmen adaylarının aynı ölçeğin aynı alt faktöründen aldıkları puanlarının ortalaması 3,99 ve standart sapması ,80 olarak bulunmuştur. Gruplar arasında anlamlı bir fark olup olmadığını belirlemek için bağımsız örneklem t-testi yapılmıştır ($-1,35$; $p>.05$). Buna göre erkek öğretmen adaylarının kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "Önlem Alma" konusunda kadın öğretmenlerden istatistiksel olarak anlamlı bir farklılık göstermediği söylenebilir.

Kadın Öğretmen adaylarının kişisel siber güvenliği sağlama ölçeğinden aldıkları puanların ortalaması 3,35 Standart sapması ,47 olarak bulunmuştur. Erkek öğretmen adaylarının aynı ölçeğin aynı alt faktöründen aldıkları puanlarının ortalaması 3,48 ve standart sapması ,48 olarak bulunmuştur. Gruplar arasında anlamlı bir fark olup olmadığını belirlemek için bağımsız örneklem t-testi yapılmıştır ($t= -3,87$; $p<.05$). Buna göre erkek öğretmen adaylarının kişisel siber güvenliği sağlama konusunda farkındalık düzeylerinin kadın öğretmenlerden daha fazla oldukları söylenebilir.

5.3. Kişisel Siber Güvenliği Sağlama Üzerinde Öğrenim Gördüğü Bölüme Göre Kaynaklanan Farklılıkların Analizi

Öğretmen adaylarının öğrenim gördükleri sınıflara göre kişisel siber güvenliği sağlama ölçeğinden aldıkları puanların ortalamaları ve standart sapmaları Tablo 8' de gösterilmiştir.

Öğretmen adaylarının öğrenim gördükleri bölüme göre kişisel siber güvenliği sağlama ölçeğinin "Kişisel Güvenliği Koruma" faktöründe aldıkları puanların ortalama ve standart sapmalarına göre en yüksek ortalama ($\bar{x}$= 2,67) Sosyal Bilgiler Eğitimi en düşük ortalama ($\bar{x}$= 1,98) Matematik Eğitimi olarak bulunmuştur.

Öğretmen adaylarının öğrenim gördükleri bölüme göre kişisel siber güvenliği sağlama ölçeğinin "Ödeme Bilgilerini Koruma" faktöründe aldıkları puanların ortalama ve standart sapmalarına göre en yüksek ortalama ($\bar{x}$= 3,38) Bilgisayar ve Öğretim Teknolojileri Eğitimi, en düşük ortalama ($\bar{x}$= 2,80) Matematik Eğitimi olarak bulunmuştur.

Öğretmen adaylarının öğrenim gördükleri bölüme göre kişisel siber güvenliği sağlama ölçeğinin "Güvenilmeyenden Kaçınma" faktöründe aldıkları puanların ortalama ve standart sapmalarına göre en yüksek ortalama ($\bar{x}$= 4,37) Matematik Eğitimi, en düşük ortalama ($\bar{x}$= 3,81) Sosyal Bilgiler Eğitimi olarak bulunmuştur.

Öğretmen adaylarının öğrenim gördükleri bölüme göre kişisel siber güvenliği sağlama ölçeğinin "İz Bırakmama" faktöründe aldıkları puanların ortalama ve standart sapmalarına göre en yüksek ortalama ($\bar{x}$= 3,73) Sınıf Eğitimi, en düşük ortalama ($\bar{x}$= 3,51) Matematik Eğitimi olarak bulunmuştur.

Öğretmen adaylarının öğrenim gördükleri bölüme göre kişisel siber güvenliği sağlama ölçeğinin "Önlem Alma" faktöründe aldıkları puanların ortalama ve standart sapmalarına göre en yüksek ortalama ($\bar{x}$= 4,62) Sosyal Bilgiler Eğitimi, en düşük ortalama ($\bar{x}$= 3,73) Matematik Eğitimi olarak bulunmuştur.

Öğretmen adaylarının öğrenim gördükleri bölüme göre kişisel siber güvenliği sağlama ölçeğinin genelinden aldıkları puanların ortalama ve standart sapmalarına göre en yüksek ortalama ($\bar{x}$= 3,48) Bilgisayar ve Öğretim Teknolojileri Eğitimi, en düşük ortalama ($\bar{x}$= 3,21) Matematik Eğitimi olarak bulunmuştur.

Tablo 8 : Öğretmen Adaylarının Öğrenim Gördükleri Bölümlere Göre Kişisel Siber Güvenlik Durumları

	Öğrenim Gördüğü Bölüm	N	x̄	S.S.
Kişisel Gizliliği Koruma	Türkçe	131	2,14	0,69
	Matematik	105	1,98	0,55
	Bilgisayar ve Öğretim Teknolojileri E.	237	2,24	0,74
	Sosyal Bilgiler	63	2,67	0,80
	Psikolojik Danışmanlık ve Rehberlik	39	2,35	0,77
	Sınıf Öğretmenliği	234	2,28	0,69
Ödeme Bilgilerini Koruma	Türkçe	131	2,97	0,86
	Matematik	105	2,80	0,79
	Bilgisayar ve Öğretim Teknolojileri E.	237	3,38	0,80
	Sosyal Bilgiler	63	3,31	1,04
	Psikolojik Danışmanlık ve Rehberlik	39	2,82	0,99
	Sınıf Öğretmenliği	234	3,20	0,81
Güvenilmeyenden Kaçınma	Türkçe	131	4,09	1,16
	Matematik	105	4,37	0,83
	Bilgisayar ve Öğretim Teknolojileri E.	237	4,16	0,97
	Sosyal Bilgiler	63	3,81	0,83
	Psikolojik Danışmanlık ve Rehberlik	39	4,29	0,99
	Sınıf Öğretmenliği	234	4,17	1,03
İz Bırakmama	Türkçe	131	3,59	0,76
	Matematik	105	3,51	0,73
	Bilgisayar ve Öğretim Teknolojileri E.	237	3,67	0,81
	Sosyal Bilgiler	63	3,56	1,03
	Psikolojik Danışmanlık ve Rehberlik	39	3,53	0,91
	Sınıf Öğretmenliği	234	3,73	0,80
Önlem Alma	Türkçe	131	3,80	0,88
	Matematik	105	3,74	0,74
	Bilgisayar ve Öğretim Teknolojileri E.	237	4,22	0,71
	Sosyal Bilgiler	63	4,62	0,97
	Psikolojik Danışmanlık ve Rehberlik	39	4,02	0,70
	Sınıf Öğretmenliği	234	3,87	0,87
Kişisel Siber Güvenliği Sağlama	Türkçe	131	3,22	0,51
	Matematik	105	3,21	0,34
	Bilgisayar ve Öğretim Teknolojileri E.	237	3,48	0,42
	Sosyal Bilgiler	63	3,41	0,67
	Psikolojik Danışmanlık ve Rehberlik	39	3,33	0,43
	Sınıf Öğretmenliği	234	3,41	0,47

Katılımcıların öğrenim gördüğü bölüme göre Kişisel Siber Güvenliği Sağlama durumlarının anlamlı bir farklılık olup olmadığını incelemek üzere tek yönlü varyans analizi yapılmıştır.

Öğretmen adaylarının öğrenim gördükleri bölümlerine göre kişisel siber güvenliği sağlama puanları arasında fark olup olmadığını belirlemek için tek yönlü varyans analizi yapılmıştır. Analiz sonuçları Tablo 9' da gösterilmiştir.

Tablo 9 : Öğretmen Adaylarının Öğrenim Görmekte Olan Bölüme Göre Farklılıklara Yönelik Tek Yönlü Varyans Analizi

Değişken		Kareler Toplamı	s.d.	Kareler Ortalaması	F	p	Fark
Kişisel Gizliliği Koruma	Gruplar arası	21,27	5	4,22	8,45	0,00	Matematik-Sosyal* / Matematik-Sınıf*
	Gruplar içi	404,33	803	0,504			Türkçe-Sosyal * / Matematik-BÖTE*
	Toplam	425,6	808				BÖTE-Sınıf* / Sosyal*- Sınıf Ö.
Ödeme Bilgilerini Koruma	Gruplar arası	36,27	5	7,25	10,01	0,00	Türkçe-BÖTE*/ Matematik BÖTE*
	Gruplar içi	576,47	803	0,718			Matematik-Sosyal* / Matematik-Sınıf*
	Toplam	612,75	808				BÖTE*-PDR / Sosyal*-PDR
Güvenilmeyenden Kaçınma	Gruplar arası	13,7	5	2,74	2,59	0,02	Matematik* -Sosyal
	Gruplar içi	849,65	803	1,05			
	Toplam	863,36	808				
İz Bırakmama	Gruplar arası	5,18	5	1,03	1,55	0,17	
	Gruplar içi	537,27	803	0,669			
	Toplam	542,46	808				
Önlem Alma	Gruplar arası	32,98	5	6,59	9,93	0,00	Türkçe-BÖTE* / Matematik-BÖTE*
	Gruplar içi	533,3	803	0,664			BÖTE-Sosyal */ BÖTE*- Sınıf
	Toplam	566,28	808				
Kişisel Siber Güvenliği Sağlama (Genel Durum)	Gruplar arası	6,79	5	1,35	6,13	0,00	Türkçe-BÖTE* / Matematik-BÖTE*
	Gruplar içi	177,76	803	0,221			Matematik-Sınıf*
	Toplam	184,55	808				

Öğretmen adaylarının kişisel siber güvenlik ölçeğinin "Kişisel Gizliliği Koruma" alt boyut puanlarının öğrenim gördükleri bölümlere göre farklılaşıp farklılaşmadığını belirlemek için tek yönlü varyans analizi yapılmış ve gruplar arasında istatistiksel açıdan anlamlı bir farklılık bulunmuştur ($F=8,45$; $p<.05$). Bu farklılığın hangi gruplar arasında olduğunu belirlemek için TUKEY testi yapılmıştır. Buna göre Sosyal Bilgiler bölümünde öğrenim gören öğretmen adaylarının Türkçe, Matematik, Sınıf öğretmenliği bölümünde öğrenim gören öğretmen adaylarının, Bilgisayar ve Öğretim Teknolojileri Eğitimi ve Matematik bölümünde öğrenim gören öğretmen adaylarından, kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "Kişisel Gizliliği Koruma" konusunda farkındalık düzeylerinin daha fazla oldukları söylenebilir.

Öğretmen adaylarının kişisel siber güvenlik ölçeğinin "Ödeme Bilgilerini Koruma" alt boyut puanlarının öğrenim gördükleri bölümlere göre farklılaşıp farklılaşmadığını belirlemek için tek yönlü varyans analizi yapılmış ve gruplar arasında istatistiksel açıdan anlamlı bir farklılık bulunmuştur ($F=10,10$; $p<.05$). Bu farklılığın hangi gruplar arasında olduğunu belirlemek için TUKEY testi yapılmıştır. Buna göre Bilgisayar ve Öğretim Teknolojileri Eğitimi bölümünde öğrenim gören öğretmen adaylarının Türkçe, Matematik ve Psikolojik Danışmanlık ve Rehberlik bölümünde öğrenim gören öğretmen adaylarından, Sosyal Bilgiler bölümünde öğrenim görmekte olan öğretmen adaylarının Matematik ve Psikolojik Danışmanlık ve Rehberlik bölümünde öğrenim görmekte olan öğretmen adaylarından, Sınıf Öğretmenliği bölümünde öğrenim görmekte olan öğretmen adaylarının Matematik bölümünde öğrenim gören öğretmen adaylarından, kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "Ödeme Bilgilerini Koruma" konusunda farkındalık düzeylerinin daha fazla oldukları söylenebilir.

Öğretmen adaylarının kişisel siber güvenlik ölçeğinin "Güvenilmeyenden Kaçınma" alt boyut puanlarının öğrenim gördükleri bölümlere göre farklılaşıp farklılaşmadığını belirlemek için tek yönlü varyans analizi yapılmış ve gruplar arasında istatistiksel açıdan anlamlı bir farklılık bulunmuştur ($F=2,59$; $p<.05$). Bu farklılığın hangi gruplar arasında olduğunu belirlemek için TUKEY testi yapılmıştır. Buna göre Matematik bölümünde öğrenim görmekte olan öğretmen adaylarının Sosyal Bilgiler bölümünde öğrenim görmekte olan öğretmen adaylarından kişisel

siber güvenliği sağlama ölçeğinin alt boyutlarından olan "Güvenilmeyenden Kaçınma" konusunda farkındalık düzeylerinin daha fazla oldukları söylenebilir.

Öğretmen adaylarının kişisel siber güvenlik ölçeğinin "İz Bırakmama" alt boyut puanlarının öğrenim gördükleri bölümlere göre farklılaşıp farklılaşmadığını belirlemek için tek yönlü varyans analizi yapılmış ve gruplar arasında istatistiksel açıdan anlamlı bir farklılık bulunmamıştır ($F=1,55$; $p>.05$). Buna göre öğretmen adayları arasında kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "İz Bırakmama" konusunda anlamlı bir farklılık bulunmamıştır.

Öğretmen adaylarının kişisel siber güvenlik ölçeğinin "Önlem Alma" alt boyut puanlarının öğrenim gördükleri bölümlere göre farklılaşıp farklılaşmadığını belirlemek için tek yönlü varyans analizi yapılmış ve gruplar arasında istatistiksel açıdan anlamlı bir farklılık bulunmuştur ($F=9,93$; $p<.05$). Bu farklılığın hangi gruplar arasında olduğunu belirlemek için TUKEY testi yapılmıştır. Buna göre Bilgisayar ve Öğretim Teknolojileri Eğitimi bölümünde öğrenim görmekte olan öğretmen adaylarının Türkçe, Matematik ve Sınıf öğretmenliği bölümünde öğrenim görmekte olan öğretmen adaylarından, Sosyal Bilgiler bölümünde öğrenim görmekte olan öğretmen adaylarının Bilgisayar ve Öğretim Teknolojileri Eğitimi bölümünde öğrenim görmekte olan öğretmen adaylarından, kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "Önlem Alma" konusunda farkındalık düzeylerinin daha fazla oldukları söylenebilir.

Öğretmen adaylarının kişisel siber güvenlik ölçeğinin öğrenim gördükleri bölüme göre farklılaşıp farklılaşmadığını belirlemek için tek yönlü varyans analizi yapılmış ve gruplar arasında istatistiksel açıdan anlamlı bir farklılık bulunmamıştır ($F=6,13$; $p<.05$). Bu farklılığın hangi gruplar arasında olduğunu belirlemek için TUKEY testi yapılmıştır. Buna göre Bilgisayar ve Öğretim Teknolojileri Eğitimi bölümünde öğrenim görmekte olan öğretmen adaylarının Türkçe ve Matematik bölümünde öğrenim görmekte olan öğretmen adaylarından, Sınıf Öğretmenliği bölümünde öğrenim görmekte olan öğretmen adaylarının Matematik bölümünde öğrenim görmekte olan öğretmen adaylarından, kişisel siber güvenliği sağlama konusunda farkındalık düzeylerinin daha fazla oldukları söylenebilir.

5.4. Kişisel Siber Güvenliği Sağlama Üzerinde Öğrenim Gördüğü Sınıf Kademesine Göre Kaynaklanan Farklılıkların Analizi

Öğretmen adaylarının öğrenim gördükleri sınıf kademesine göre kişisel siber güvenliği sağlama ölçeğinden aldıkları puanların ortalama ve standart sapması Tablo 10' da gösterilmiştir.

Tablo 10 : Öğretmen Adaylarının Öğrenim Gördüğü Sınıf Kademesine Göre Kişisel Siber Güvenlik Durumları

	Sınıf	N	x̄	SS
Kişisel Gizliliği Koruma	1	229	2,10	,71
	2	243	2,36	,75
	3	221	2,22	,71
	4	116	2,32	,65
Ödeme Bilgilerini Koruma	1	229	3,15	,79
	2	243	3,03	,93
	3	221	3,27	,83
	4	116	3,18	,91
Güvenilmeyenden Kaçınma	1	229	4,21	,96
	2	243	4,07	1,10
	3	221	4,19	1,06
	4	116	4,21	,94
İz Bırakmama	1	229	3,62	,83
	2	243	3,58	,83
	3	221	3,71	,81
	4	116	3,67	,76
Önlem Alma	1	229	3,99	,85
	2	243	3,80	,87
	3	221	4,03	,77
	4	116	3,90	,79
Kişisel Siber Güvenliği Sağlama (Genel Durum)	1	229	3,36	,42
	2	243	3,35	,52
	3	221	3,43	,46
	4	116	3,40	,49

Öğretmen adaylarının öğrenim gördükleri sınıflara göre kişisel siber güvenliği sağlama ölçeğinin "Kişisel Güvenliği Koruma" faktöründe aldıkları puanların ortalama ve standart sapmalarına göre en yüksek ortalama ($\bar{x}$= 2,36) 2. sınıf kademesi, en düşük ortalama ($\bar{x}$= 2,10) 1. sınıf kademesi olarak bulunmuştur.

Öğretmen adaylarının öğrenim gördükleri sınıflara göre kişisel siber güvenliği sağlama ölçeğinin "Ödeme Bilgilerini Koruma" faktöründen aldıkları puanların ortalama ve standart sapmalarına göre en yüksek ortalama ($\bar{x}$= 3,27) 3. sınıf kademesi, en düşük ortalama ($\bar{x}$= 3,03) 2. sınıf kademesi olarak bulunmuştur.

Öğretmen adaylarının öğrenim gördükleri sınıflara göre kişisel siber güvenliği sağlama ölçeğinin "Güvenilmeyenden Kaçınma" faktöründen aldıkları puanların ortalama ve standart sapmalarına göre en yüksek ortalama ($\bar{x}$= 4,21) 1. ve 4. sınıf kademeleri, en düşük ortalama ($\bar{x}$= 4,07) 2. sınıf kademesi olarak bulunmuştur.

Öğretmen adaylarının öğrenim gördükleri sınıflara göre kişisel siber güvenliği sağlama ölçeğinin "İz Bırakmama" faktöründen aldıkları puanların ortalama ve standart sapmalarına göre en yüksek ortalama ($\bar{x}$= 3,71) 3. sınıf kademeleri, en düşük ortalama ($\bar{x}$= 3,58) 2. sınıf kademesi olarak bulunmuştur.

Öğretmen adaylarının öğrenim gördükleri sınıflara göre kişisel siber güvenliği sağlama ölçeğinin "Önlem Alma" faktöründen aldıkları puanların ortalama ve standart sapmalarına göre en yüksek ortalama ($\bar{x}$= 4,03) 3. sınıf kademeleri, en düşük ortalama ($\bar{x}$= 3,80) 2. sınıf kademesi olarak bulunmuştur.

Öğretmen adaylarının öğrenim gördükleri sınıflara göre kişisel siber güvenliği sağlama ölçeğinden genel olarak alınan puanların ortalama ve standart sapmalarına göre en yüksek ortalama ($\bar{x}$= 3,43) 3. Sınıf kademeleri, en düşük ortalama ($\bar{x}$= 3,35) 2. sınıf kademesi olarak bulunmuştur.

Katılımcıların öğrenim gördüğü sınıf kademesine göre Kişisel Siber Güvenliği Sağlama durumlarının anlamlı bir farklılık olup olmadığını incelemek üzere tek yönlü varyans analizi yapılmıştır.

Öğretmen adaylarının öğrenim gördükleri sınıf kademesine göre kişisel siber güvenliği sağlama puanları arasında fark olup olmadığını belirlemek için tek yönlü varyans analizi yapılmıştır. Analiz sonuçları Tablo 11' de gösterilmiştir.

Tablo 11 : Öğretmen Adaylarının Öğrenim Gördüğü Sınıf Kademesine Göre Tek Yönlü Varyans Analizi

Değişken		Kareler Toplamı	s.d.	Kareler Ortalaması	F	p	Fark
Kişisel Gizliliği Koruma	Gruplar arası	8,63	3	2,87	5,55	0,01	1-2* 1-4*
	Gruplar içi	416,97	805	,518			
	Toplam	425,60	808	-			
Ödeme Bilgilerini Koruma	Gruplar arası	6,74	3	2,24	2,98	0,03	2-3*
	Gruplar içi	606,01	805	,753			
	Toplam	612,75	808	-			
Güvenilmeyenden Kaçınma	Gruplar arası	3,11	3	1,039	0,97	0,41	
	Gruplar içi	860,24	805	1,069			
	Toplam	863,36	808	-			
İz Bırakmama	Gruplar arası	2,43	3	0,81	1,21	0,31	
	Gruplar içi	540,03	805	,671			
	Toplam	542,46	808	-			
Önlem Alma	Gruplar arası	7,14	3	2,38	3,43	0,02	2-3*
	Gruplar içi	559,14	805	,695			
	Toplam	566,28	808	-			
Kişisel Siber Güvenliği Sağlama (Genel Durum)	Gruplar arası	1,03	3	,346	1,51	,209	-
	Gruplar içi	183,51	805	,228			
	Toplam	184,55	808	-			

Öğretmen adaylarının kişisel siber güvenlik ölçeğinin "Kişisel Gizliliği Koruma" alt boyut puanlarının öğrenim gördükleri sınıf kademelerine göre farklılaşıp

farklılaşmadığını belirlemek için tek yönlü varyans analizi yapılmış ve gruplar arasında istatistiksel açıdan anlamlı bir farklılık bulunmuştur (F=5,55; p<.05). Bu farklılığın hangi gruplar arasında olduğunu belirlemek için TUKEY testi yapılmıştır. Buna göre 2. ve 4. Sınıfta öğrenim gören öğretmen adaylarının 1. sınıfta öğrenim gören öğretmen adaylarından kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "Kişisel Gizliliği Koruma" konusunda farkındalık düzeylerinin daha yüksek oldukları söylenebilir.

Öğretmen adaylarının kişisel siber güvenlik ölçeğinin "Ödeme Bilgilerini Koruma" alt boyut puanlarının öğrenim gördükleri sınıf kademelerine göre farklılaşıp farklılaşmadığını belirlemek için tek yönlü varyans analizi yapılmış ve gruplar arasında istatistiksel açıdan anlamlı bir farklılık bulunmuştur (F=2,98; p<.05). Bu farklılığın hangi gruplar arasında olduğunu belirlemek için TUKEY testi yapılmıştır. Buna göre 3. Sınıfta öğrenim gören öğretmen adaylarının 2. Sınıfta öğrenim gören öğretmen adaylarından kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "Ödeme Bilgilerini Koruma" konusunda farkındalık düzeylerinin daha yüksek oldukları söylenebilir.

Öğretmen adaylarının kişisel siber güvenlik ölçeğinin "Güvenilmeyenden Kaçınma" alt boyut puanlarının öğrenim gördükleri sınıf kademelerine göre farklılaşıp farklılaşmadığını belirlemek için tek yönlü varyans analizi yapılmış ve gruplar arasında istatistiksel açıdan anlamlı bir farklılık bulunmuştur (F=0,97; p>.05). Buna göre çeşitli kademelerde öğrenim gören öğretmen adaylarından kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "Güvenilmeyenden Kaçınma" konusunda anlamlı bir farklılık bulunmamaktadır.

Öğretmen adaylarının kişisel siber güvenlik ölçeğinin "İz Bırakmama" alt boyut puanlarının öğrenim gördükleri sınıf kademelerine göre farklılaşıp farklılaşmadığını belirlemek için tek yönlü varyans analizi yapılmış ve gruplar arasında istatistiksel açıdan anlamlı bir farklılık bulunmuştur (F=1,21; p>.05). Buna göre çeşitli kademelerde öğrenim gören öğretmen adaylarından kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "İz Bırakmama" konusunda anlamlı bir farklılık bulunmamaktadır.

Öğretmen adaylarının kişisel siber güvenlik ölçeğinin "Önlem Alma" alt boyut puanlarının öğrenim gördükleri sınıf kademelerine göre farklılaşıp farklılaşmadığını

belirlemek için tek yönlü varyans analizi yapılmış ve gruplar arasında istatistiksel açıdan anlamlı bir farklılık bulunmuştur (F=3,43; p<.05). Bu farklılığın hangi gruplar arasında olduğunu belirlemek için TUKEY testi yapılmıştır. Buna göre 3. Sınıfta öğrenim gören öğretmen adaylarının 2. Sınıfta öğrenim gören öğretmen adaylarından kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "Önlem Alma" konusunda farkındalık düzeylerinin daha yüksek oldukları söylenebilir.

Öğretmen adaylarının kişisel siber güvenlik ölçeğinin öğrenim gördükleri sınıf kademelerine göre farklılaşıp farklılaşmadığını belirlemek için tek yönlü varyans analizi yapılmış ve gruplar arasında istatistiksel açıdan anlamlı bir farklılık bulunmamıştır (F=1,51; p>.05). Buna göre öğretmen adaylarının kişisel siber güvenliği sağlama ölçeğinin öğrenim gördüğü sınıf kademesine göre anlamlı bir fark bulunmamıştır.

5.5. Kişisel Siber Güvenliği Sağlama Üzerinde İnternet Kullanma Sıklığından Kaynaklanan Farklılıkların Analizi

Öğretmen adaylarının internet kullanım sıklığına göre kişisel siber güvenliği sağlama ölçeğinin "Kişisel Güvenliği Koruma" faktöründe aldıkları puanların ortalama ve standart sapmalarına göre en yüksek ortalama ($\bar{x}$= 2,41) çok yüksek sıklıkta kullanım, en düşük ortalama ($\bar{x}$= 2,12) orta sıklıkta kullanım olarak bulunmuştur.

Öğretmen adaylarının internet kullanım sıklığına göre kişisel siber güvenliği sağlama ölçeğinin "Ödeme Bilgilerini Koruma" faktöründe aldıkları puanların ortalama ve standart sapmalarına göre en yüksek ortalama ($\bar{x}$= 3,22) çok yüksek sıklıkta kullanım, en düşük ortalama ($\bar{x}$= 2,12) az sıklıkta kullanım olarak bulunmuştur.

Öğretmen adaylarının internet kullanım sıklığına göre kişisel siber güvenliği sağlama ölçeğinin "Güvenilmeyenden Kaçınma" faktöründe aldıkları puanların ortalama ve standart sapmalarına göre en yüksek ortalama ($\bar{x}$= 4,23) orta sıklıkta kullanım, en düşük ortalama ($\bar{x}$= 3,89) az sıklıkta kullanım olarak bulunmuştur.

Tablo 12 : Öğretmen Adaylarının İnternet Kullanma Sıklığına Göre Kişisel Siber Güvenlik Durumları

	İnternet Kullanım Sıklığı	N	x̄	SS
Kişisel Gizliliği Koruma	Az	80	2,14	,86
	Orta	229	2,12	,68
	Yüksek	198	2,20	,59
	Çok Yüksek	302	2,41	,76
Ödeme Bilgilerini Koruma	Az	80	2,91	,92
	Orta	229	3,11	,79
	Yüksek	198	3,18	,82
	Çok Yüksek	302	3,22	,92
Güvenilmeyenden Kaçınma	Az	80	3,89	1,15
	Orta	229	4,23	1,00
	Yüksek	198	4,15	1,06
	Çok Yüksek	302	4,19	,99
İz Bırakmama	Az	80	3,47	1,02
	Orta	229	3,70	,80
	Yüksek	198	3,66	,75
	Çok Yüksek	302	3,62	,80
Önlem Alma	Az	80	3,69	1,06
	Orta	229	3,93	,82
	Yüksek	198	3,91	,77
	Çok Yüksek	302	4,02	,80
Kişisel Siber Güvenliği Sağlama (Genel Durum)	Az	80	3,22	,63
	Orta	229	3,36	,46
	Yüksek	198	3,37	,42
	Çok Yüksek	302	3,45	,46

Öğretmen adaylarının internet kullanım sıklığına göre kişisel siber güvenliği sağlama ölçeğinin "İz Bırakmama" faktöründe aldıkları puanların ortalama ve

standart sapmalarına göre en yüksek ortalama ($\bar{x}$= 3,70) orta sıklıkta kullanım, en düşük ortalama ($\bar{x}$= 3,47) az sıklıkta kullanım olarak bulunmuştur.

Öğretmen adaylarının internet kullanım sıklığına göre kişisel siber güvenliği sağlama ölçeğinin "Önlem Alma" faktöründe aldıkları puanların ortalama ve standart sapmalarına göre en yüksek ortalama ($\bar{x}$= 4,02) çok yüksek sıklıkta kullanım, en düşük ortalama ($\bar{x}$= 3,69) az sıklıkta kullanım olarak bulunmuştur.

Öğretmen adaylarının internet kullanma sıklığına göre kişisel siber güvenliği sağlama puanları arasında fark olup olmadığını belirlemek için tek yönlü varyans analizi yapılmıştır. Analiz sonuçları Tablo 13' te gösterilmiştir.

Öğretmen adaylarının kişisel siber güvenlik ölçeğinin "Kişisel Gizliliği Koruma" alt boyut puanlarının internet kullanım sıklığına göre farklılaşıp farklılaşmadığını belirlemek için tek yönlü varyans analizi yapılmış ve gruplar arasında istatistiksel açıdan anlamlı bir farklılık bulunmuştur ($F=8,40$; $p<.05$). Bu farklılığın hangi gruplar arasında olduğunu belirlemek için TUKEY testi yapılmıştır. Buna göre öğretmen adaylarından internet kullanma sıklığı çok yüksek olanın az, orta ve yüksek olandan, kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "Kişisel Gizliliği Koruma" " konusunda farkındalık düzeylerinin daha yüksek oldukları söylenebilir.

Öğretmen adaylarının kişisel siber güvenlik ölçeğinin "Ödeme Bilgilerini Koruma" alt boyut puanlarının internet kullanım sıklığına göre farklılaşıp farklılaşmadığını belirlemek için tek yönlü varyans analizi yapılmış ve gruplar arasında istatistiksel açıdan anlamlı bir farklılık bulunmuştur ($F=2,94$; $p<.05$). Bu farklılığın hangi gruplar arasında olduğunu belirlemek için TUKEY testi yapılmıştır. Buna göre öğretmen adaylarından internet kullanma sıklığı çok yüksek olanın az olandan, kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "Ödeme Bilgilerini Koruma" " konusunda farkındalık düzeylerinin daha yüksek oldukları söylenebilir.

Tablo 13 : Öğretmen Adaylarının İnternet Kullanma Sıklığına Göre Tek Yönlü Varyans Analizi

Değişken		Kareler Toplamı	s.d.	Kareler Ortalaması	F	p	Fark
Kişisel Gizliliği Koruma	Gruplar arası	12,92	3	4,3	8,4	0	Az- Çok Yüksek*
	Gruplar içi	412,68	805	0,513			Orta- Çok Yüksek*
	Toplam	425,6	808				Yüksek-Çok Yüksek*
Ödeme Bilgilerini Koruma	Gruplar arası	6,65	3	2,21	2,94	0,032	
	Gruplar içi	606,09	805	0,753			Az-Çok Yüksek*
	Toplam	612,75	808				
Güvenilmeyenden Kaçınma	Gruplar arası	7,16	3	2,38	2,24	0,082	
	Gruplar içi	856,19	805	1,06			
	Toplam	863,36	808				
İz Bırakmama	Gruplar arası	3,3	3	1,01	1,64	0,178	
	Gruplar içi	539,16	805	0,67			
	Toplam	542,46	808				
Önlem Alma	Gruplar arası	7,07	3	2,35	3,39	0,018	
	Gruplar içi	559,21	805	0,695			Az-Çok Yüksek*
	Toplam	566,28	808				
Kişisel Siber Güvenliği Sağlama (Genel Durum)	Gruplar arası	3,8	3	1,26	5,64	0,001	
	Gruplar içi	180,75	805	0,22			Az-Çok Yüksek*
	Toplam	184,55	808				

Öğretmen adaylarının kişisel siber güvenlik ölçeğinin "Güvenilmeyenden Kaçınma" alt boyut puanlarının internet kullanım sıklığına göre farklılaşıp farklılaşmadığını belirlemek için tek yönlü varyans analizi yapılmış ve gruplar arasında istatistiksel açıdan anlamlı bir farklılık bulunmamıştır ($F=2,24$; $p>.05$). Buna

göre öğretmen adaylarının internet kullanma sıklığına göre kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "Güvenilmeyenden Kaçınma" konusunda anlamlı bir fark bulunmamıştır.

Öğretmen adaylarının kişisel siber güvenlik ölçeğinin "İz Bırakmama" alt boyut puanlarının internet kullanım sıklığına göre farklılaşıp farklılaşmadığını belirlemek için tek yönlü varyans analizi yapılmış ve gruplar arasında istatistiksel açıdan anlamlı bir farklılık bulunmamıştır ($F=1,64$; $p>.05$). Buna göre öğretmen adaylarının internet kullanma sıklığına göre kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "İz Bırakmama" konusunda anlamlı bir fark bulunmamıştır.

Öğretmen adaylarının kişisel siber güvenlik ölçeğinin "Önlem Alma" alt boyut puanlarının internet kullanım sıklığına göre farklılaşıp farklılaşmadığını belirlemek için tek yönlü varyans analizi yapılmış ve gruplar arasında istatistiksel açıdan anlamlı bir farklılık bulunmuştur ($F=3,39$; $p<.05$). Bu farklılığın hangi gruplar arasında olduğunu belirlemek için TUKEY testi yapılmıştır. Buna göre öğretmen adaylarından internet kullanma sıklığı çok yüksek olanın az olandan, kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "Önlem Alma" " konusunda farkındalık düzeylerinin daha yüksek oldukları söylenebilir.

Öğretmen adaylarının kişisel siber güvenlik ölçeğinden aldıkları puanların internet kullanım sıklığına göre farklılaşıp farklılaşmadığını belirlemek için tek yönlü varyans analizi yapılmış ve gruplar arasında istatistiksel açıdan anlamlı bir farklılık bulunmuştur ($F=5,64$; $p<.05$). Bu farklılığın hangi gruplar arasında olduğunu belirlemek için TUKEY testi yapılmıştır. Buna göre öğretmen adaylarından internet kullanma sıklığı çok yüksek olanın az olandan, kişisel siber güvenliği sağlama " konusunda farkındalık düzeylerinin daha yüksek oldukları söylenebilir.

5.6. Kişisel Siber Güvenliği Sağlama Üzerinde Not Ortalamasından Kaynaklanan Farklılıkların Analizi

Öğretmen adaylarının öğrenim gördükleri sınıf kademesine göre kişisel siber güvenliği sağlama ölçeğinden aldıkları puanların ortalama ve standart sapması Tablo 14' te gösterilmiştir.

Tablo 14 : Öğretmen Adaylarının Not Ortalamalarına Göre Kişisel Siber Güvenlik Durumları

	Not Ortalaması	N	$\bar{x}$	S.S.
Kişisel Gizliliği Koruma	Düşük	182	2,36	,74
	Orta	425	2,21	,71
	Yüksek	202	2,20	,71
Ödeme Bilgilerini Koruma	Düşük	182	3,13	,93
	Orta	425	3,14	,84
	Yüksek	202	3,18	,87
Güvenilmeyenden Kaçınma	Düşük	182	4,00	1,05
	Orta	425	4,17	1,06
	Yüksek	202	4,27	,92
İz Bırakmama	Düşük	182	3,58	,83
	Orta	425	3,66	,78
	Yüksek	202	3,64	,86
Önlem Alma	Düşük	182	3,92	,82
	Orta	425	3,93	,85
	Yüksek	202	3,97	,81
Kişisel Siber Güvenliği Sağlama (Genel Durum)	Düşük	182	3,38	,45
	Orta	425	3,38	,49
	Yüksek	202	3,39	,47

Öğretmen adaylarının not ortalamalarına göre kişisel siber güvenliği sağlama ölçeğinin "Kişisel Güvenliği Koruma" faktöründe aldıkları puanların ortalama ve standart sapmalarına göre en yüksek ortalama ($\bar{x}$= 2,36) düşük derece not ortalaması, en düşük ortalama ($\bar{x}$= 2,20) yüksek derece not ortalaması olarak bulunmuştur.

Öğretmen adaylarının not ortalamalarına göre kişisel siber güvenliği sağlama ölçeğinin "Ödeme Bilgilerini Koruma" faktöründe aldıkları puanların ortalama ve standart sapmalarına göre en yüksek ortalama ($\bar{x}$= 3,18) yüksek derece not ortalaması, en düşük ortalama ($\bar{x}$= 3,13) düşük derece not ortalaması olarak bulunmuştur.

Öğretmen adaylarının not ortalamalarına göre kişisel siber güvenliği sağlama ölçeğinin "Güvenilmeyenden Kaçınma" faktöründe aldıkları puanların ortalama ve standart sapmalarına göre en yüksek ortalama ($\bar{x}$= 4,27) yüksek derece not ortalaması, en düşük ortalama ($\bar{x}$= 4,00) düşük derece not ortalaması olarak bulunmuştur.

Öğretmen adaylarının not ortalamalarına göre kişisel siber güvenliği sağlama ölçeğinin "İz Bırakmama" faktöründe aldıkları puanların ortalama ve standart sapmalarına göre en yüksek ortalama ($\bar{x}$= 3,66) orta derece not ortalaması, en düşük ortalama ($\bar{x}$= 3,58) düşük derece not ortalaması olarak bulunmuştur.

Öğretmen adaylarının not ortalamalarına göre kişisel siber güvenliği sağlama ölçeğinin "Önlem Alma" faktöründe aldıkları puanların ortalama ve standart sapmalarına göre en yüksek ortalama ($\bar{x}$= 3,97) yüksek derece not ortalaması, en düşük ortalama ($\bar{x}$= 3,92) düşük derece not ortalaması olarak bulunmuştur.

Öğretmen adaylarının not ortalamalarına göre kişisel siber güvenliği sağlama ölçeğinden genel olarak aldıkları puanların ortalama ve standart sapmalarına göre en yüksek ortalama ($\bar{x}$= 3,39) yüksek derece not ortalaması, en düşük ortalama ($\bar{x}$= 3,38) düşük ve orta derece not ortalaması olarak bulunmuştur.

Öğretmen adaylarının not ortalamalarına göre kişisel siber güvenliği sağlama puanları arasında fark olup olmadığını belirlemek için tek yönlü varyans analizi yapılmıştır. Analiz sonuçları Tablo 15' te gösterilmiştir.

Öğretmen adaylarının kişisel siber güvenlik ölçeğinin "Kişisel Gizliliği Koruma" alt boyut puanlarının not ortalamasına göre farklılaşıp farklılaşmadığını belirlemek için tek yönlü varyans analizi yapılmış ve gruplar arasında istatistiksel açıdan anlamlı bir farklılık bulunmamıştır ($F=3,05$; $p>.05$). Buna göre öğretmen adaylarından not ortalamalarının kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "Kişisel Gizliliği Koruma" konusunda anlamlı bir farklılık bulunmamıştır.

Öğretmen adaylarının kişisel siber güvenlik ölçeğinin "Ödeme Bilgilerini Koruma" alt boyut puanlarının not ortalamasına göre farklılaşıp farklılaşmadığını belirlemek için tek yönlü varyans analizi yapılmış ve gruplar arasında istatistiksel açıdan anlamlı bir farklılık bulunmamıştır ($F=,217$; $p>.05$). Buna göre öğretmen adaylarından not ortalamalarının kişisel siber güvenliği sağlama ölçeğinin alt

boyutlarından olan "Ödeme Bilgilerini Koruma" konusunda anlamlı bir farklılık bulunmamıştır.

Tablo 15 : Öğretmen Adaylarının Not Ortalamalarına Göre Tek Yönlü Varyans Analizi

Değişken		Kareler Toplamı	s.d.	Kareler Ortalaması	F	p	Fark
Kişisel Gizliliği Koruma	Gruplar arası	3,2	2	1,6	3,05	0,048	
	Gruplar içi	422,4	806	0,524			
	Toplam	425,6	808				
Ödeme Bilgilerini Koruma	Gruplar arası	0,33	2	0,165	0,217	0,805	
	Gruplar içi	612,42	806	0,76			
	Toplam	612,75	808				
Güvenilmeyenden Kaçınma	Gruplar arası	7,23	2	3,61	3,4	0,034	Düşük-Yüksek*
	Gruplar içi	856,12	806	1,06			
	Toplam	863,36	808				
İz Bırakmama	Gruplar arası	0,904	2	0,452	0,673	0,511	
	Gruplar içi	541,56	806	0,672			
	Toplam	542,46	808				
Önlem Alma	Gruplar arası	0,311	2	0,156	0,222	0,801	
	Gruplar içi	565,97	806	0,702			
	Toplam	566,28	808				
Kişisel Siber Güvenliği Sağlama (Genel Durum)	Gruplar arası	0,01	2	0,005	0,021	0,979	
	Gruplar içi	184,54	806	0,229			
	Toplam	184,55	808				

Öğretmen adaylarının kişisel siber güvenlik ölçeğinin "Güvenilmeyenden Kaçınma" alt boyut puanlarının not ortalamasına göre farklılaşıp farklılaşmadığını

belirlemek için tek yönlü varyans analizi yapılmış ve gruplar arasında istatistiksel açıdan anlamlı bir farklılık bulunmuştur (F=3,40; p<.05). Buna göre öğretmen adaylarından not ortalamalarının kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "Güvenilmeyenden Kaçınma" konusunda anlamlı bir farklılık bulunmamıştır. Bu farklılığın hangi gruplar arasında olduğunu belirlemek için TUKEY testi yapılmıştır. Buna göre öğretmen adaylarından not ortalaması çok yüksek olanların az olanlardan, kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "Önlem Alma" konusunda farkındalık düzeylerinin daha yüksek oldukları söylenebilir.

Öğretmen adaylarının kişisel siber güvenlik ölçeğinin "İz Bırakmama" alt boyut puanlarının not ortalamasına göre farklılaşıp farklılaşmadığını belirlemek için tek yönlü varyans analizi yapılmış ve gruplar arasında istatistiksel açıdan anlamlı bir farklılık bulunmamıştır (F=,673; p>.05). Buna göre öğretmen adaylarından not ortalamalarının kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "İz Bırakmama" konusunda anlamlı bir farklılık bulunmamıştır.

Öğretmen adaylarının kişisel siber güvenlik ölçeğinin "Önlem Alma" alt boyut puanlarının not ortalamasına göre farklılaşıp farklılaşmadığını belirlemek için tek yönlü varyans analizi yapılmış ve gruplar arasında istatistiksel açıdan anlamlı bir farklılık bulunmamıştır (F=,222; p>.05). Buna göre öğretmen adaylarından not ortalamalarının kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "Önlem Alma" konusunda anlamlı bir farklılık bulunmamıştır.

Öğretmen adaylarının kişisel siber güvenlik ölçeğinden genel olarak alınan puanlarının not ortalamasına göre farklılaşıp farklılaşmadığını belirlemek için tek yönlü varyans analizi yapılmış ve gruplar arasında istatistiksel açıdan anlamlı bir farklılık bulunmamıştır (F=3,05; p>.05). Buna göre öğretmen adaylarından not ortalamalarının kişisel siber güvenliği sağlama konusunda anlamlı bir farklılık bulunmamıştır.

BÖLÜM 6

SONUÇ VE TARTIŞMA

Öğretmen adaylarının kişisel siber güvenlik farkındalıklarının incelendiği bu araştırmada kişisel siber güvenliğin cinsiyet, öğrenim gördüğü bölüm, öğrenim gördüğü sınıf kademesi, not ortalaması, internet kullanma sıklığına göre değiştiği tespit edilmiştir.

Öğretmen adaylarının kişisel siber güvenliği sağlama ölçeğinden genel olarak aldıkları puanların ortalama ve standart sapmalarına göre orta derecesinde puanlar alınmıştır. Bu ölçekten alınan puanlardan oluşan ortalama 3,38 Standart Sapma 0,47 olarak bulunmuştur. Öğretmen adaylarının kişisel siber güvenliği sağlama ölçeğinden aldıkları puanların ortalama ve standart sapmalarına göre çok düşük derecesinde puan alınmıştır. Bu madde, şöyle belirtilmektedir. "Tanımadığım kişilerle web kamerası kullanarak sesli ve görüntülü iletişim kurarım." maddesinden alınan puanlardan oluşan ortalama 1,61 Standart Sapma 1,23 olarak bulunmuştur. Öğretmen adaylarının kişisel siber güvenliği sağlama ölçeğinden aldıkları puanların ortalama ve standart sapmalarına göre çok yüksek derecesinde puanlar alınmıştır. Bu maddeler, şöyle belirtilmektedir. "Şahsi bilgisayarım dışında kullandığım bilgisayarlarda bilgilerimin kalmamasına dikkat ederim." maddesinden alınan puanlardan oluşan ortalama 4,37 Standart Sapma 1,04 olarak bulunmuştur. "Güvenmediğim sitelere üye olmam." maddesinden alınan puanlardan oluşan ortalama 4,30 Standart Sapma 1,24 olarak bulunmuştur.

Kişisel siber güvenliği sağlama durumlarına göre bulguların, araştırmaya katılan öğretmen adayların cinsiyet bilgileri dikkate alınarak ele alındığında:

Araştırmaya göre erkek öğretmen adaylarının kişisel siber güvenliği sağlama konusunda kadın öğretmen adaylarından daha yüksek farkındalığa sahip oldukları ortaya çıkmıştır. Kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "Kişisel Gizliliği Koruma" faktöründen aldıkları puanlar incelendiğinde erkek öğretmen adaylarının kadın öğretmen adaylarından daha yüksek farkındalığa sahip oldukları ortaya çıkmıştır. Kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "Ödeme Bilgilerini Koruma" faktöründen aldıkları puanlar incelendiğinde erkek öğretmen adaylarının kadın öğretmen adaylarından daha yüksek farkındalığa sahip oldukları ortaya çıkmıştır. Kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından

olan "Güvenilmeyenden Kaçınma" faktöründen aldıkları puanlar incelendiğinde kadın öğretmen adaylarının erkek öğretmen adaylarından daha yüksek farkındalığa sahip oldukları ortaya çıkmıştır. Kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "İz Bırakmama" faktöründen aldıkları puanlar incelendiğinde kadın ve erkek öğretmen adayları arasında anlamlı bir farklılık bulunmamıştır. Kişisel siber güvenliği sağlama ölçeğinin alt boyutlarından olan "Önlem Alma" faktöründen aldıkları puanlar incelendiğinde kadın ve erkek öğretmen adayları arasında anlamlı bir farklılık bulunmamıştır. Benzer şekilde Gökmen ve Akgün (2015) yaptığı çalışmada BÖTE erkek öğretmen adaylarının bilişim güvenliği bilgilerinin kadın öğretmen adaylarının bilişim güvenliği bilgilerine göre daha yüksek olduğu sonucuna ulaşılmıştır. Yiğit ve Seferoğlu (2019) tarafından yapılan çalışmada kadın ve erkek öğrencilerin siber güvenlik sağlama durumları arasında anlamlı bir farklılık bulunmamıştır. Ancak siber güvenlik alt boyutlarına incelendiğinde ise kişisel gizliliği koruma ve güvenilmeyenden kaçınma konularında kadın öğrencilerin erkek öğrencilerden daha duyarlı olduğu tespit edilmiştir. Mart (2012) tarafından yapılan çalışmada ise Kadın katılımcıların erkek katılımcılara oranla bilişim güvenliği farkındalığının daha yüksek olduğu gözlenmiştir.

Kişisel siber güvenliği sağlama durumlarına göre bulguların, araştırmaya katılan öğretmen adayların öğrenim gördükleri bölüm bilgileri dikkate alınarak ele alındığında:

Araştırmaya katılan katılımcıların bölümlerinin farklı olmasından dolayı, kişisel siber güvenlik farkındalıklarının bölümlere göre anlamlı farklılık olup olmadığının incelenmesini gerekli kılmıştır. Buna göre Bilgisayar ve Öğretim Teknolojileri Eğitimi bölümünde öğrenim görmekte olan öğretmen adaylarının Türkçe bölümünde öğrenim görmekte olan öğretmen adaylarından, Bilgisayar ve Öğretim Teknolojileri Eğitimi bölümünde öğrenim görmekte olan öğretmen adaylarının Matematik bölümünde öğrenim görmekte olan öğretmen adaylarından, Sınıf Öğretmenliği bölümünde öğrenim görmekte olan öğretmen adaylarının Matematik bölümünde öğrenim görmekte olan öğretmen adaylarından, kişisel siber güvenliği sağlama konusunda farkındalık düzeylerinin daha yüksek olduğu ortaya çıkmıştır.

Kişisel siber güvenliği sağlama ölçeğinin alt boyutları dikkate alındığında Bilgisayar ve Öğretim Teknolojileri bölümünde öğrenim gören adayların genel olarak

boyutlarda da daha duyarlı oldukları görülmektedir. Özellikle Kişisel Gizliliği Koruma, Ödeme Bilgilerini Koruma, Önlem Alma alt boyutlarında duyarlı oldukları görülmektedir. Buna etken olarak öğrenim gördüğü bölüm ile siber güvenlik konusunun yakın ilişki içinde olması olarak gösterilebilir. Yine alt boyutlar dikkate alındığında Sosyal Bilgiler bölümünde öğrenim gören adayların genel olarak Kişisel Gizliliği Koruma, Ödeme Bilgilerini Koruma, Güvenilmeyenden Kaçınma alt boyutlarında duyarlı oldukları görülmektedir. Yine alt boyutlar dikkate alındığında Matematik bölümünde öğrenim gören adayların genel olarak duyarlılıklarının düşük oldukları görülmektedir. Yiğit ve Seferoğlu (2019) tarafından yapılan çalışmada BÖTE öğrencilerinin kişisel siber güvenlik konusunda lojistik programı, Psikolojik danışmanlık rehberlik ve okul öncesi öğrencilerininkine göre daha duyarlı olduğu; bilgisayar programcılığı öğrencilerinin de kişisel siber güvenlik konusunda lojistik bölümü öğrencilerinden daha duyarlı olduğu ortaya çıkmıştır. Bulgulardan hareketle bilişim ile ilgili veya buna yakın bölümlerde kişisel siber güvenlik farkındalığının daha yüksek olduğu ortaya çıkmıştır. Öğretim programı içerisinde bilişim yoğunluğu olması ve bu alana olan yatkınlıktan kaynaklı olarak yüksek çıktığı söylenebilir.

Kişisel siber güvenliği sağlama durumlarına göre bulguların, araştırmaya katılan öğretmen adayların öğrenim gördükleri sınıf kademesi dikkate alınarak ele alındığında:

Araştırmaya göre öğretmen adaylarının öğrenim gördüğü sınıf kademesine göre inceleme yapıldığında anlamlı bir farklılık olmadığı saptanmıştır.

Kişisel siber güvenliği sağlama ölçeğinin alt boyutları dikkate alındığında, 2. ve 3. Sınıf kademesinde öğrenim gören öğretmen adaylarının daha yüksek farkındalığa sahip oldukları görülmüştür. Buna göre, 2. Sınıfta öğrenim gören öğretmen adaylarının Kişisel Gizliliği Koruma alt boyutunda, 3. Sınıfta öğrenim gören öğretmen adaylarının Ödeme Bilgilerini Koruma ve Önlem Alma alt boyutlarında daha yüksek farkındalığa sahip oldukları ortaya çıkmıştır. Karacı, Akyüz ve Bilgici (2017) tarafından yapılan çalışmada öğrencilerin öğrenim gördüğü sınıf kademelerine göre anlamlı bir farklılık bulunmamıştır. Seferoğlu ve Yiğit (2019) tarafından yapılan çalışmada öğrencilerin öğrenim gördüğü sınıf kademesine göre anlamlı farklılıklar bulunmuştur. Buna göre 3. sınıf ve 4. sınıf öğrencilerin siber güvenlik sağlama durumları önlisans öğrencilerine göre daha duyarlı olarak

tespit edilmiştir. Benzer bir şekilde 4. sınıf öğrencileri de 1. sınıf öğrencilerinden siber güvenlik konusunda daha duyarlı olduğu ortaya çıkmıştır. Bulgulardan hareketle sınıf kademesi dolayısıyla yaş arttıkça deneyim de artacağı için üst sınıfta öğrenim gören öğretmen adaylarının alt sınıfta öğrenim görenlere göre kişisel siber güvenlik konusunda farkındalık düzeylerinin daha yüksek olduğu söylenebilir.

Kişisel siber güvenliği sağlama durumlarına göre bulguların, araştırmaya katılan öğretmen adaylarının internet kullanma sıklığı dikkate alınarak ele alındığında:

Araştırmaya göre öğretmen adaylarından internet kullanma sıklığı çok yüksek olanın az olandan, kişisel siber güvenliği sağlama konusunda daha yüksek farkındalığa sahip oldukları ortaya çıkmıştır.

Kişisel siber güvenliği sağlama ölçeğinin alt boyutları dikkate alındığında, internet kullanma sıklığı çok yüksek olan öğretmen adaylarının farkındalık düzeylerinin daha yüksek olduğu görülmüştür. Buna göre Kişisel Gizliliği Koruma, Ödeme Bilgilerini Koruma, Önlem Alma alt boyutlarında internet kullanma sıklığı çok yüksek olan öğretmen adaylarının farkındalık düzeylerinin daha yüksek olduğu gözlenmiştir. Mart (2012) tarafından yapılan çalışmada katılımcıların internet kullanma sıklığı ile bilişim güvenliği sağlama durumları arasında anlamlı bir farklılık bulunmamıştır. Akgün ve Topal (2015) tarafından yapılan çalışmada ortalamanın üstünde internete bağlanan katılımcıların daha çok korsan yazılım kullandıkları tespit edilmiştir. Seferoğlu ve Yiğit (2019) tarafından yapılan çalışmada genel olarak internet kullanım düzeyleri arasında anlamlı bir farklılık bulunmamıştır. Karacı, Akyüz ve Bilgici (2017) tarafından yapılan çalışmada İnternet kullanım düzeyi artıkça siber güvenlik davranış düzeylerinin arttığı sonucuna ulaşmıştır. Ulaşılan bulgulara göre internet kullanma sıklığı arttıkça, öğretmen adayları kişisel siber güvenlik açısından daha çok önlem almakta ve özellikle internetten yapılan alış verişlerde ödeme bilgilerini koruma konusunda farkındalık düzeyleri yükselmektedir. Sonuç itibariyle öğretmen adaylarının internette geçirdiği süre arttıkça kişisel siber güvenlik farkındalığı artmaktadır.

Kişisel siber güvenliği sağlama durumlarına göre bulguların, araştırmaya katılan öğretmen adaylarının not ortalamaları dikkate alınarak ele alındığında:

Araştırmaya göre öğretmen adaylarından not ortalamalarının kişisel siber güvenliği sağlama konusunda anlamlı bir farklılık bulunmamıştır.

Kişisel siber güvenliği sağlama ölçeğinin alt boyutları dikkate alındığında, sadece Güvenilmeyenden Kaçınma alt boyutunda yüksek not ortalaması olan öğretmen adaylarının düşük not ortalaması olan öğretmen adaylarına göre farkındalık düzeylerinin daha yüksek olduğu görülmüştür. Buradan hareketle yüksek not alan öğrencilerin güvenmedikleri konusunda daha temkinli yaklaştıkları görülmektedir.

BÖLÜM 7

ÖNERİLER

Yapılan araştırmada elde edilen bulgular sonucunda aşağıdaki öneriler getirilmiştir:

- ✓ Bilgisayar ile ilgili olmayan bölümlerde öğrenim gören öğretmen adaylarının kişisel siber güvenlik davranışları istenilen düzeyde olmadığı görülmüştür. Günümüzdeki bütün meslek alanları bilişim teknolojileri ile bir ilişki içerindedir. Bundan dolayı özellikle bilgisayar ile bir ilişkisi olmayan bölümlerin siber güvenlik konusunun ders içeriklerinde yer alması veya tamamen bir ders olarak eklenmesi önem arz etmektedir. Ayrıca öğrenim görülen sınıf kademesine göre bakıldığında kişisel siber güvenlik konusunda 3. ve 4. Sınıf öğrencilerinin 1. ve 2. sınıf öğrencilerine göre farkındalık düzeylerinin daha yüksek olduğu görülmüştür. Bu kısımda da 1. Sınıftan itibaren her sınıf kademesinde siber güvenlikle ilgili eğitimlerin verilmesi konusunun dikkate değer olduğu görülmektedir.
- ✓ İnternet kullanma sıklığı arttıkça kişisel siber güvenlik farkındalıkları da artmaktadır. Bundan dolayı interneti az kullananların hangi uygulamaları veya web sitelerini kullandıkları tespit edilip, o sitelerde kişisel siber güvenliği sağlama ile ilgili kamu spotlarının paylaşılması gerekmektedir.
- ✓ Erkek öğretmen adaylarının kişisel siber güvenlik farkındalığı kadın öğretmen adaylarından daha yüksek çıkmıştır. Buna göre kadın öğretmen adaylarının internet kullanımı teşvik edilerek kişisel siber güvenliği sağlama farkındalıkları arttırılabilir.
- ✓ Bu araştırmada nicel araştırma yöntemleri kullanıldığı için ileriye dönük araştırmalarda nitel araştırma yöntemleri de kullanılarak öğretmen adaylarının siber güvenlik bilinç, farkındalık ve davranışları ayrıntılı bir biçimde incelenebilir.
- ✓ Bu çalışmada sadece öğretmen adayları incelenmiştir. Diğer programlarda öğrenim gören öğrenciler, farklı meslek grupları, farklı yaş grupları için de bu konu araştırılmalıdır.
- ✓ Bu çalışma sadece Konya ili ile sınırlı kaldığı için Türkiye geneli daha kapsamlı bir çalışma yapılmalıdır. Araştırmaya katılımı arttırmak için web siteleri oluşturulmalı, kitle iletişim alanlarıyla duyurular yapılmalıdır.

- ✓ Araştırmada kullanılan ölçek kişisel siber güvenliği sağlama durumlarını 5 alt boyutta ele almıştır. Gelecek araştırmalarda bu konuda yeni ve kapsamı daha geniş ölçekler geliştirilmesi faydalı olacaktır.

KAYNAKÇA

Ada, M. (2018). *NATO Üyesi ülkelerin siber güvenlik stratejileri açısından incelenmesi*, Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü, Ankara

Afet ve Acil Durum Yönetimi Başkanlığı. (2019). *Siber Ortam Nedir?* , Açıklamalı Afet Yönetimi Terimleri Sözlüğü, https://www.afad.gov.tr/tr/23792/Aciklamali-Afet-Yonetimi-Terimleri-Sozlugu?kelime=siber+ortam Erişim Tarihi: 12.06.2019

Agamba, J. and Keengwe, J. (2012). *Pre-Service teachers' perceptions of information assurance and cyber security*. International Journal of Information and Communication Technology Education, 8(2), 94-101. DOI: 10.4018/jicte.2012040108.

Akçadağ Alagöz, E. (2012, 20 Temmuz). *Sürekli Artan Önemi Işığında Siber Güvenlik.* Bilge İnsanlar Stratejik Araştırmalar Merkezi. http://www.bilgesam.org/incele/1207/-surekli-artan-onemi-isiginda-siber-guvenlik/#.XS7-9egzbIV adresinden edinilmiştir.

Akgün, Ö. E. ve Topal, M. (2015*). Eğitim fakültesi son sınıf öğrencilerinin bilişim güvenliği farkındalıkları: Sakarya Üniversitesi Eğitim Fakültesi Örneği,* Sakarya Üniversitesi Eğitim Dergisi, 5(2) s98-121

Alkan, H. (2016). *ABD'nin Siber Güvenliği İçin 19 Milyar Dolar*. https://www.techinside.com/abdnin-siber-guvenligi-icin-19-milyar-dolar/, Erişim Tarihi: 26.03.2019

Alp, Ö. (2018). *Akıllı şehirlerde siber güvenlik*, Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul

Arıman, M. (2017). *2016'da Yaşanan En Büyük Siber Saldırılar*. https://ceotudent.com/2016-da-yasanan-en-buyuk-siber-saldirilar, Erişim Tarihi: 17 Mayıs 2018.

Aslay, F. (2017). *Siber saldırı yöntemleri ve Türkiye'nin siber güvenlik mevcut durum analizi*, International Journal of Multidisciplinary Studies and Innovative Technologies, 1(1) , ss24-28

Aydoğmuş, A. (2014). *Hackerler Erzincan'daki Petrol Boru Hattını Patlattı*. https://www.teknolojioku.com/guncel/hackerlar-erzincandaki-petrol-boru-hattini-patlatti-5a28f85b18e540630d1d8dea, Erişim Tarihi: 26 Mayıs 2019.

Aytekin, A. (2015). *Türkiye'nin siber güvenlik stratejisi ve eylem planının değerlendirilmesi*, Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü, Ankara

Başaran, A. (2016). *Siber Savaş Cephesinden Notlar*. İstanbul: Arion yayınevi.

Bayzan, Ş. Ve Özbilen, A. (2011). *"Aplication examples of safer use of the ınternetin the world and ınvestigation of awareness activities in turkey suggestions for turkey"*, cilt 7, no.2, 5th International Computer & Instructional Technologies Symposium, Fırat University, Elazığ , ss. 22-24

Bıçakcı, S. (2012*) "NATO'nun gelişen tehdit algısı: 21. yüzyılda siber güvenlik", uluslararası ilişkiler*, Cilt 10, Sayı 40 (Kış 2014), s. 101-130.

Bozdemir, M. (Mayıs 2016). *Türkiye en çok siber saldırıya uğrayan 4. Ülke*. (http://www.iha.com.tr/haber-bozdemir-turkiye-en-cok-siber-saldiriya-ugrayan-4-ulke-559751/ , Erişim Tarihi: 17 Mayıs 2016.

Büyüköztürk Ş (2002). *Sosyal Bilimler İçin Veri Analizi El Kitabı: İstatistik, Araştırma Deseni, SPSS Uygulamaları ve Yorum* 1. Baskı, Pegem Akademi, Ankara

Büyüköztürk Ş., Akgün, Ö. E., Demirel, F., Karadeniz, Ş., Kılıç ve Çakmak, E. (2008). *Bilimsel Araştırma Yöntemleri.* 1. Baskı, Pegem Akademi, Ankara

Canbek, G. ve Sağıroğlu, Ş. (2006). *Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme.* Politeknik Dergisi, 9(3), 165-174.

Canberk, G. ve Sağıroğlu, Ş.(2007), *Kötücül ve casus yazılımlar: kapsamlı bir araştırma,* Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 22(1) ss121–136

Check, T. (2015). *Book Review: analyzing the effectiveness of the tallinn manual's jus ad bellum doctrine on cyberconflict: a nato-centric approach*, Cleveland State University, ss495-512

Cieply, M. and Barnes, B. (2014), *Sony cyberattack, first a nuisance, swiftly grew ınto a firestorm,* https://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html?_r=0 , Erişim Tarihi: 15.04.2019

Council of Europe, (2011), *Convention on cybercrime*, European Treaty Series - No. 185

https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561 Erişim Tarihi: 01.06.2019

Czosseck, C. Ottis, R. and Ziolkowski, K. (2012). 4th International Conference on Cyber Conflict . NATO CCD COE Publications.

Çakar, H. (2005). *Bilgisayar ağ güvenliği ve güvenlik duvarları*, Yüksek Lisans Tezi, Fırat Üniversitesi Fen Bilimleri Enstitüsü, Elazığ

Çalışkan, E. (2013), *Zararlı yazılımların etkisinde Dijital adli delillerin güvenilirliği* yüksek lisans tezi, İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul

Çeliktaş, B. (2016), *Siber güvenlik kavramının gelişimi ve türkiye özelinde bir değerlendirme,* Yüksek Lisans Tezi, Karadeniz Teknik Üniversitesi, Sosyal Bilimler Enstitüsü, Trabzon

Çiftçi, H. (2013), *Her Yönüyle Siber Savaş*, 1.Baskı, TÜBİTAK Yayınları, Ankara

Çubukçu, A. ve Bayzan, Ş. (2013*) Türkiye'de dijital vatandaşlık algısı ve bu algıyı internetin bilinçli, güvenli ve etkin kullanımı ile artırma yöntemleri.* Middle Eastern & African Journal of Educational Research, 5, 148-174

Derian, J. D. (2000). "*Virtuous war/virtual theory*", International Affairs, 76(4), s.771–788.

Desai, D. (2013). *Beyond location: Data security in the 21st century*. Communications of the ACM, 56(1), 34-36. doi:10.1145/2398356.2398368

Elbahadır, H. (2011). *Haching İnterface*, Kodlab Yayınevi, İstanbul

Ercan, M. (2015), *Kritik alt yapıların kornasına ilişkin belirlenen siber güvenlik stratejileri*, Yüksek Lisans Tezi, Gebze Teknik Üniversitesi, Kocaeli

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.

Erol, S. E. (2016). *Siber güvenlik farkındalığı için yetenek tabanlı dinamik model,* Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimler Enstitüsü, Ankara

Furnell, S. M., Jusoh A. and Katsabas (2005). D. *The challenges of understanding and using security : A survey of end-users. Computers & Security,vol.25,no.5, s.27 - 35, 2005.*

Goble A. P. (2009), *Defining victory and defeat: the ınformation war between russia and georgia,* In the Guns of August 2008: Russia War in Georgia", edited by Svantee E. Cornell and S. Frederick Starr (Armonk, N.Y.: M.E. Sharpe)

Gökmen, Ö. F. (2014). *Bilgisayar ve öğretim teknolojileri eğitimi öğretmen adaylarının bilişim güvenliği eğitimi verebilme yeterliliklerinin incelenmesi,* Yüksek Lisans Tezi, Sakarya Üniversitesi Eğitim Bilimleri Enstitüsü, Sakarya

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

Gülmüş, M. (2010). *Kurumsal bilgi güvenliği yönetim sistemleri ve güvenliği*, Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul

Güngör, M. (2015), *Ulusal Bilgi Güvenliği: Strateji ve kurumsal yapılanma,* uzmanlık tezi, Bilgi Toplumu Dairesi Başkanlığı

Hansen, L., and Nissenbaum, H. (2009). *Digital disaster, cyber security, and the copenhagen school*. International Studies Quarterly, 53, 1155-1175.

Hekim, H. ve Başıbüyük, O. (2013*). Siber suçlar ve Türkiye'nin siber güvenlik politikaları,* Uluslararası Güvenlik ve Terörizm Dergisi, 4(2) s135-158

Hürriyet Gazetesi. (2018). *Siber güvenlik nedir?*. http://www.hurriyet.com.tr/teknoloji/siber-guvenlik-nedir-40975739, Erişim Tarihi: 19.05.2019

İlbaş, Ç. (2009). *Bilişim suçlarının sosyo-kültürel seviyelere göre algı analizi,* yüksek lisans tezi, Başkent Üniversitesi, Fen Bilimleri Enstitüsü, Ankara

Kamu Kurum ve Kuruluşlarının KamuNet'e Dâhil Edilmesi ile İlgili 2016/28 Sayılı Başbakanlık Genelgesi. (2016). T.C. Resmi Gazete, 29907, 03 Aralık 2016.

Kara, M. (2013). *Siber saldırılar - siber savaşlar ve etkileri.* Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul

Karacı, A., Akyüz, H. İ. ve Bilgici, G. (2017). *Üniversite öğrencilerinin siber güvenlik davranışlarının incelenmesi,* Kastamonu Eğitim Dergisi, 25(6) s12-27

Keleştemur, A. (2015), *Siber İstihbarat*, 1.Baskı, Level Yayınevi, Kocaeli.

Kruger, H.A, Flowerday, S., Drevin, L. and Steyn, T. (15-17 August 2011). *An Assessment of the role of cultural factors in ınformation security awareness*. Information Security South Africa Conference. Johannesburg, South Africa. DOI:10.1109/ISSA.2011.6027505.

Küçük A. ve Soğukpınar İ. (2019) Siber Saldırılar ve Farkındalık Eğitimi için bir Öneri, http://cigicigi.com/CA.pdf . Erişim Tarihi: 13.06.2019.

Mil, H. İ. (2015) *Sosyal güvenlik kurumundaki siber güvenlik yönetimi uygulamalarının incelenmesi ve değerlendirilmesi,* Dicle Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Nisan 2015 YIL-7 S.13 sh.398-416.

Milliyet Gazetesi. (2017). *Siber saldırı nedir?*. http://www.milliyet.com.tr/sibel-saldiri-nedir--teknoloji-haber-1991343/, Erişim Tarihi: 19.06.2019

Mitnick, Kevin D and Simon, William L. (2005). *Aldatma Sanatı*. (Çeviren: Nejat Eralp Tezcan). Ankara. Odtü Yayıncılık.

Morgan, S. (2019). *Cybersecurity market report sponsored by secure anchor* Cybersecurity Ventures' 2019. https://cybersecurityventures.com/cybersecurity-market-report/ , Erişim Tarihi: 15.06.2019

Necmettin Erbakan Üniversitesi (2018). T*ez hazırlama ve yazma klavuzu*. Konya: Necmettin Erbakan Üniversitesi Eğitim Bilimleri Enstitüsü

Nissenbaum, H. (2005). *Where computer security meets national security*. Ethics and Information Technology, 2, 61-73.

Okoye, S. (2017). *Strategies to Minimize the Effects of Information Security Threats on Business Performance*, College of Management and Technology, Walden University, Doctoral Study 2017

Öğütçü, G. (2010). *E-Dönüşüm sürecinde küresel bilişim güvenliği davranışı ve farkındalığının analizi,* Yüksek Lisans Tezi, Başkent Üniversitesi Fen Bilimleri Enstitüsü, Ankara

Özbay, R. (2015). *Aktif siber savunma teknikleri ve performans analizi.* Yüksek Lisans Tezi, Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü, Afyon

Özkan, Ö. (2004). *Veri güvenliğinde saldırı ve savunma yöntemleri,* Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü, Isparta.

Özseven T. (2012). *Bilgisayar Ağları*, Murathan Yayınevi, ss. 227-259

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

Ryan H. (2006), *Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem*, Indiana 2006 ("Harris"), sf. 4.

Schatz, D., Bashroush, R., and Wall, J. (2017). *Towards a more representative definition of cyber security*. Journal of Digital Forensics Journal of Digital Forensics, Security and Law, 12(2). Erişim: 8 Nisan 2018, https://commons.erau.edu/jdfsl/vol12/iss2/8

Sertçelik, A. (2015). *Siber olaylar ekseninde siber güvenliği anlamak,* Medeniyet Araştırmaları Dergisi, 2(3) s25-42

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

Sofaer, A. D., Clark, D., and Diffie, W. (2010). *Cyber security and ınternational agreements. ın committee on deterring cyberattacks (Ed.),* Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (pp. 179-206). Washington, DC: The National Academies Press.

Solms, V., and Niekerk, V. (2013). *From ınformation security to cyber security*. Computers & Security 38, 97-102.

STM Savunma Teknolojileri Mühendislik ve Tic. A.Ş. (2016). 2016 Temmuz-Eylül Dönemi Siber Tehdit Durum Raporu. https://www.stm.com.tr/documents/file/Pdf/Siber%20Tehdit%20Durum%20Raporu%20Temmuz%20-%20Eylul%202016.pdf , Erişim Tarihi: 15.03.2019

Şahinaslan E., Kantürk A., Şahinaslan Ö. ve Borandağ E. (2009). *Kurumlarda bilgi güvenliği farkındalığı, önemi ve oluşturma yöntemleri,* Akademik bilişim konferansı, 11-13 Şubat 2009.

Şahinaslan, E., Kandemir, R. ve Şahinaslan, Ö. (2009). *Bilgi güvenliği farkındalık eğitim örneği*. 11. Akademik Bilişim Konferansı, 11-13 Şubat 2009.

Şahinaslan, E. ve Şahinaslan, Ö. (2012). *Akıllı yapılarda siber güvenlik*. IV İstanbul Bilişim Kongresi, Bahçeşehir Üniversitesi.

Şahinaslan E., Kantürk A., Şahinaslan Ö. ve Borandağ E. (2013). *Güvenli bir toplum için son kullanıcı siber güvenliği,* Akademik bilişim konferansı, 23-25 Ocak 2013.

Şenol, M. (2012). *Siber Savaş, Silahlı Kuvvetler Dergisi*, Gnkur. ATASE Yayınları. Sayı:413, Ankara

Şenol, M. (2017). *Türkiye'de siber saldırılara karşı caydırıcılık,* Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 3(2), S:1-9

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2013). *Ulusal siber güvenlik stratejisi ve 2013-2014 eylem planı*. T.C. Resmi Gazete, 28683, 20 Haziran 2013.

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2016). *2016-2019 Ulusal Siber Güvenlik Stratejisi*. http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf , Erişim Tarihi: 17 Mayıs 2017.

Tarhan, K. (2018). *Uluslararası güvenliğin bir bileşeni olarak siber güvenlik,* Yüksek Lisans Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya

Tomlin M. (2015*) Advancing small business cyber maturity: an application of the nıst cybersecurity framework*. Master's thesis, Royal Holloway, University of London, 2015.

Tuğ İlçin, E., Adak Ş.F. ve Çakır H. (2014). *Bilişim güvenliği tedbirleri ve tkdk kurumunda uygulama örneği,* Bilişim Teknolojileri Dergisi, Cilt: 7, Sayı: 1 (2014) s11-18

Türk Dil Kurumu (2019). *Bilgisayar Korsanı (hacker) Nedir?* , Güncel Türkçe Sözlük, http://sozluk.gov.tr/ Erişim Tarihi: 12.06.2019

Türkiye Cumhuriyeti Anayasası (2014). *6563 Sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun*. http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6563.pdf adresinden edinilmiştir.

Türkiye İstatistik Kurumu, *Türkiye'nin internet kullanım alışkanlıkları* (9 Ağustos 2018) https://www.guvenliweb.org.tr/haber-detay/turkiyenin-internet-kullanimaliskanliklari -tuik-2018, Erişim Tarihi: 06.04.2019.

Ulaşanoğlu, M. E., Yılmaz, R. ve Tekin, M.A. (2010). *Bilgi güvenliği: riskler ve öneriler,* Bilgi Teknolojileri Ve İletişim Kurumu, Ankara, http://docplayer.biz.tr/632957-Bilgiguvenligi-riskler-ve-oneriler.html (12.01.2016).

Ünal, A. N. ve Ergen, A. (2018). *Siber uzayda yeterince güvenli davranıyor muyuz? istanbul ilinde yürütülen nicel bir araştırma*, Manisa Celal Bayar Üniversitesi Sosyal Bilimler Dergisi, 16(2), s191 – 216

Ünver, M. (2009). *Ulusal ve uluslararası boyutlarıyla siber güvenlik,* Elektrik Mühendisliği, 438. sayı, Mart 2010 s.94-103

Vardal, N. (2009). *Yükseköğretimde bilgi güvenliği: bilgi güvenlik yönetim sistemi için bir model önerisi ve uygulaması*, Doktora Tezi, Gazi Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara

Wikizero. (2019a). Siber,. https://www.wikizero.com/tr/Siber, Erişim Tarihi: 17.04.2019

Wikizero. (2019b). Siber,. https://www.wikizero.com/tr/Siber_sava%C5%9F, Erişim Tarihi: 17.04.2019

Yaşar, H. (2014). *Kurumsal siber güvenliğe yönelik tehditler ve mücadele yöntemleri: eylem planı örneği*, Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü, Ankara

Yaşar, H. ve Çakır, H (2015). *Kurumsal siber güvenliğe yönelik tehditler ve önlemleri*, Düzce Üniversitesi Bilim ve Teknolojileri Dergisi, 3(2015) s488-507.

Yaşar, H. ve Çakır, H.(2007), *Kurumsal siber güvenliğe yönelik tehditler ve önlemleri*, Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 3(2015) ss488-507

Yavanoğlu, U, Sağıroğlu Ş ve Çolak, İ. (2012). *Sosyal ağlarda bilgi güvenliği tehditleri ve alınması gereken önlemler,* Politeknik Dergisi, 15(1) s15-27

Yayla, M. (2014). *Siber savaş ve siber ortamdaki kötü niyetli hareketlerden farkı*, Hacettepe Hukuk Fakültesi Dergisi, 4(2), ss. 181–200

Yazıcı, A. (2011). *Güvenli Bilgi Paylaşımı ve SAHAB,* http://www.emo.org.tr/ekler/fad64faae21db53_ek.pdf , Erişim Tarihi: 17.04.2019

Yener, Y. (2015). *8. Yılında estonya saldırılarına çok boyutlu bir bakış*. https://siberbulten.com/siber-saldirilar-2/8-yilinda-estonya-saldirilarina-cok-boyutlu-bir-bakis/ , Erişim Tarihi: 18 Mayıs 2018.

Yılmaz, E. N., Ulus H. İ. Ve Gönen S. (2015). *Bilgi toplumuna geçiş ve siber güvenlik*, Bilişim Teknolojileri Dergisi, Cilt: 8, Sayı: 3(2015) s133-146

Yılmaz, S., ve Sağıroğlu, Ş. (2013). *Siber güvenlik risk analizi, tehdit ve hazırlık seviyeleri.* 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara, 20-21 Eylül, 158-166.

Yiğit, M. F. ve Seferoğlu, S. S. (2019). *Öğrencilerin siber güvenlik davranışlarının beş faktör kişilik özellikleri ve çeşitli diğer değişkenlere göre incelenmesi*, Mersin Üniversitesi Eğitim Fakültesi Dergisi, 15(1): 186-215

Yüksek Planlama Kurulu. (2005). *E-Dönüşüm Türkiye projesi 2005 yılı eylem planı.* http://www.edevlet.gov.tr/2015/10/13/e-donusum-turkiye-projesi-2005-yili-eylem-plani/, Erişim Tarihi: 25.05.2019.

EKLER

EK-1: Veri Toplama Araçları

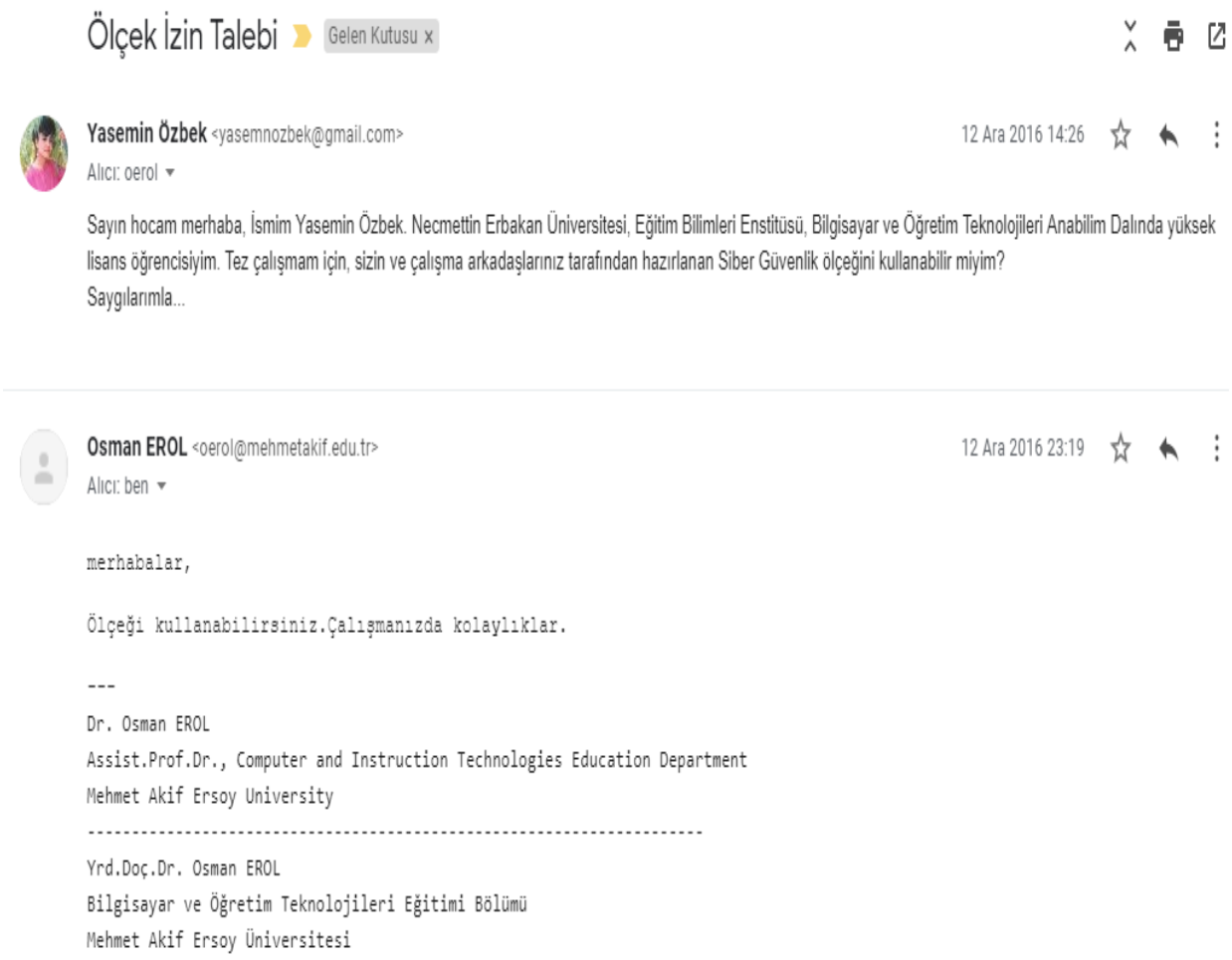
Kişisel Bilgiler Formu

1. Cinsiyet: ( ) Kız ( ) Erkek
2. Sınıf: ( ) 1 ( ) 2 ( ) 3 ( ) 4
3. Akademik Not Ortalaması (4'lük sisteme göre): …….
4. İnternet kullanma sıklığınız (günde) (1-Hiçbir zaman, 5- Her zaman):
   ( ) 1 ( ) 2 ( ) 3 ( ) 4 ( ) 5
5. Kendinizi Nasıl Tanımlarsınız? ( ) İçedönük ( ) Dışadönük
6. Gelecekle ilgili düşünceniz: ( ) İyimser ( ) Kötümser

Kişisel Siber Güvenliği Sağlama Ölçeği

Kişisel Siber Güvenliği Sağlama Ölçeği	**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 anti-virüs yazılımı bulundururum.					
4. Şifrelerimi belirlerken basit dizilimler kullanmaktan kaçınırım.					
5. İnternet şifrelerimin tümümün 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 kullandığım bilgisayarlarda bilgilerimin kalmamasına dikkat ederim.					
9. İnternet üzerinden yapılan para ve kontör isteklerini dikkate almam.					
10. Tanımadığım kişilerden gelen sosyal ağ arkadaşlık isteklerini kabul etmem.					
11. Güvenmediğim sitelere üye olmam.					
12. Tanımadığım kişilerle web kamerası kullanarak sesli ve görüntülü iletişim kurarım.					
13. İnternet ortamında gerektiği zaman kişisel bilgilerimi (TC No, Doğum Tarihi, GSM No vb.) paylaşırım.					
14. Web geçmişini temizlerim.					
15. İnternet bankacılığı işlemlerimi 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 hesapların (e-posta, sosyal ağ vb.) şifrelerini değiştiririm.					
24. Unutmamak için akılda kalan kolay bir şifre belirlerim.					
25. Banka, online alışveriş siteleri gibi sitelerden gelen e-postalara (kart no, şifre vb. istekler) itibar ederim ve yanıtlarım.					

Ek- 2: Ölçek Kullanım İzni



Ölçek İzin Talebi Gelen Kutusu x

Yasemin Özbek <yasemnozbek@gmail.com> 12 Ara 2016 14:26

Alıcı: oerol

Sayın hocam merhaba, İsmim Yasemin Özbek. Necmettin Erbakan Üniversitesi, Eğitim Bilimleri Enstitüsü, Bilgisayar ve Öğretim Teknolojileri Anabilim Dalında yüksek lisans öğrencisiyim. Tez çalışmam için, sizin ve çalışma arkadaşlarınız tarafından hazırlanan Siber Güvenlik ölçeğini kullanabilir miyim?
Saygılarımla...

Osman EROL <oerol@mehmetakif.edu.tr> 12 Ara 2016 23:19

Alıcı: ben

merhabalar,

Ölçeği kullanabilirsiniz.Çalışmanızda kolaylıklar.

Dr. Osman EROL
Assist.Prof.Dr., Computer and Instruction Technologies Education Department
Mehmet Akif Ersoy University

Yrd.Doç.Dr. Osman EROL
Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü
Mehmet Akif Ersoy Üniversitesi

ÖZGEÇMİŞ

Adı Soyadı:	Yasemin ÖZBEK	İmza:	
Doğum Yeri:	Niğde		
Doğum Tarihi:	27.09.1991		
Medeni Durumu:	Bekar		

Öğrenim Durumu

Derece	Okulun Adı	Program	Yer	Yıl
İlkokul	Çamlıbel İlkokulu		Kıbrıs	2002
Ortaokul	Mustafa Kemal İlköğretim Okulu		İskenderun	2005
Lise	İskenderun Lisesi	Fen Bilimleri	İskenderun	2009
Lisans	Necmettin Erbakan Üniversitesi	Bilgisayar ve Öğretim Teknolojileri Eğitimi	Konya	2014
Yüksek Lisans	Necmettin Erbakan Üniversitesi	Bilgisayar ve Öğretim Teknolojileri Eğitimi	Konya	2019

Becerileri:	Kodlama, Programlama
İlgi Alanları:	Teknoloji, Zeka Oyunları
İş Deneyimi	Milli Eğitim Bakanlığı/Öğretmen/2016-
E-posta	yasemnozbek@gmail.com
Adres	İskenderun