

YAKIN DOĞU ÜNİVERSİTESİ
EĞİTİM BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ
ANABİLİM DALI

ÖĞRENCİLERİN GÜVENLİ İNTERNET KULLANIMINA YÖNELİK
ÖZ-YETERLİK ALGILARININ BELİRLENMESİ

YÜKSEK LİSANS TEZİ

Mehmet KARABULUT

Lefkoşa

Mayıs, 2017

YAKIN DOĞU ÜNİVERSİTESİ
EĞİTİM BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ
ANABİLİM DALI

ÖĞRENCİLERİN GÜVENLİ İNTERNET KULLANIMINA YÖNELİK
ÖZ-YETERLİK ALGILARININ BELİRLENMESİ

YÜKSEK LİSANS TEZİ

Mehmet KARABULUT

Danışman

Yrd. Doç. Dr. Erinç Erçağ

Lefkoşa
Mayıs, 2017

JÜRİ ÜYELERİNİN ONAY SAYFASI

Eğitim Bilimleri Enstitüsü Müdürlüğü'ne

Mehmet Karabulut'un "Öğrencilerin Güvenli İnternet Kullanımına Yönelik Öz-Yeterlik Algılarının Belirlenmesi" Başlıklı tezi 25/05/2017 Tarihinde, aşağıdaki jüri tarafından Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı'nda YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Başkan : Prof. Dr. Nadire Çavuş

Üye : Yrd. Doç. Dr. Sezer Kanbul

Danışman : Yrd. Doç. Erinç Erçağ

Onay

Yukarıdaki İmzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım

...../...../.....

Doç. Dr. Fahriye Altınay

Enstitü Müdürü

ÖNSÖZ

Bilişim Teknolojileri kullanımının her geçen gün yaygınlaştığı ve internet teknolojisinin hayatın her alanında kullanıldığı günümüz dünyasında internet ve bilişim teknolojilerinin faydaları olduğu gibi zararlarının da olabileceği unutulmaması gereken bir gerçektir. Dijital dünyada yer alan risk unsurlarının bilinmesi, kullanıcıların mevcut risk unsurlarına ilişkin yeterliliklerinin belirlenmesi oldukça önem arz etmektedir.

Öğrencilerin güvenli internet kullanımına yönelik öz-yeterlik algılarını ölçmeyi amaçlayan bu çalışmaya başladığım günden itibaren bu zorlu süreçte yoğun çalışma programına rağmen her daim yardımlarını, fikirlerini ve desteğini esirgemeyen danışmanım Yrd. Doç. Dr. Erinç Erçağ' a teşekkür ederim. Önerileriyle bana yol gösteren ve çalışmamı şekillendiren Yard. Doç. Dr. Sezer Kanbul' a ve Doç. Dr. Nadire Çavuş'a teşekkürlerimi sunuyorum.

Araştırmam boyunca bana zaman ayıran ve yardımlarını esirgemeyen tüm arkadaşlarıma çok teşekkür ederim

Ayrıca eğitim hayatım boyunca benden desteğini hiç esirgemeyen her daim yanımda olan Annem, Babam ve kardeşlerime teşekkürlerimi sunarım.

Mayıs 2017

Mehmet Karabulut

ÖĞRENCİLERİN GÜVENLİ İNTERNET KULLANIMINA YÖNELİK ÖZ-YETERLİK ALGILARININ BELİRLENMESİ

KARABULUT, Mehmet

Yüksek Lisans, Bilgisayar Ve Öğretim Teknolojileri Eğitimi Anabilim Dalı

Tez Danışmanı: Yrd. Doç. Dr. Erinç Erçağ

Mayıs 2017, 104 Sayfa

ÖZET

Bu çalışma öğrencilerin güvenli internet kullanımına yönelik öz-yeterlik algılarını ölçmek amacıyla yapılmıştır. Araştırma 2016 - 2017 öğretim yılında KKTC Millî Eğitim Bakanlığı bünyesinde yer alan Mesleki Teknik Ortaöğretim Dairesi ve Genel Ortaöğretim Dairesine bağlı liselerde bulunan öğrenciler ile yapılmıştır.

Araştırma nicel bir çalışma olarak yapılmış ve lise öğrencilerinin güvenli internet kullanımına yönelik öz-yeterlik algılarını ölçmek amacıyla anket uygulanmıştır. Araştırma KKTC de bulunan 30 adet lisede öğrenim gören 880 adet öğrenciye uygulanmıştır. Araştırmada betimsel araştırma yöntemlerinden genel tarama yöntemi kullanılmıştır. Araştırma sonucunda elde edilen verilerin çözümlenmesinde; frekans (f), yüzdelik (%), aritmetik ortalama ($\bar{X}$), standart sapma (SS), bağımsız iki örneklem testi (two-independent sample test), bağımsız örneklem için Kruskal-Wallis testi (K-independent sample test) analiz teknikleri kullanılmış çıkan sonuçlar tablolar oluşturularak yorumlanmıştır.

Araştırmada kullanılan ölçek doğrultusunda katılımcıların güvenli internet kullanımına yönelik öz-yeterlik algıları 4 boyutta incelenmiştir. Araştırmanın birinci boyutunda çalışmaya katılan öğrencilerin sosyal ağ (sosyal medya) güvenliği konusunda yeterlilikleri incelenmiştir. Ankette yer alan ifadeler verdikleri yanıtlar doğrultusunda öğrencilerin sosyal ağ (sosyal medya) güvenliği konusunda tamamen yeterli oldukları bulgusuna ulaşılmıştır. Ancak araştırmanın ikinci boyutu olan zararlı yazılımlar konusunda yeterlilikleri orta düzeyde olduğu yöneltelen sorulara verdikleri cevaplar sonucunda belirlenmiştir. Araştırmanın üçüncü boyutunu oluşturan web güvenliği ve sosyal

mühendislik konusunda öğrenciler kendilerini orta düzeyde yeterli gördüklerini bildirmişlerdir. Araştırmanın dördüncü boyutunda bilgisayar güvenliğine ilişkin sorulara öğrenciler yeterli olduklarını bildirmişlerdir.

Çalışma sonucunda öğrencilerin düzenli kullanım gösterdikleri sosyal medya, sosyal ağlar konusunda yeterli olduklarını, bilgisayar güvenliği, web güvenliği ve sosyal mühendislik konularında orta düzeyde yeterli olduklarını, bunun da temel sebebinin bilgi eksikliği olduğu düşünülmektedir.

Anahtar Kelimeler: Güvenli İnternet, Bilişim Güvenliği, Öz-yeterlik Algısı, KKTC, Öğrenci

SELF-EFFICACY AND PERCEPTIONS OF STUDENTS WHO STUDY AT TRNC STATE SCHOOLS TOWARDS SAFE INTERNET USE

KARABULUT, Mehmet

Master, Computer Education and Instructional Technology

Thesis Supervisor: Assistant professor Erinç Erçağ

May 2017, 104 Pages

ABSTRACT

This study was held with the aim of measuring the self-sufficiency perceptions of students in terms of safe Internet use. The research was done among the high school students of the Department of General Secondary Education and Technical and Vocational Secondary Education at TRNC Ministry of Education in 2016-2017 academic year.

As a quantitative study, the research has applied a questionnaire to the high school students in order to measure their self-sufficiency perceptions related to the safe Internet use. The study was applied to 880 students who study at 30 high schools in TRNC as the scope of the study. The general screening method was used which is one of the descriptive research methods. For the analysis of the data acquired as a result of the research; frequency (f), percentage (%), arithmetic average ($\bar{X}$), standard deviation (SS), two-independent sampling test and for independent sampling Kruskal-Wallis test analysis (K-independent sample test) technique were used and consequently the results were interpreted by making tables.

According to the scale used in the research, the self-sufficiency perceptions of participants were analyzed in 4 dimensions in terms of safe Internet use. On the first dimension, the sufficiency of students on social networks (or media) was analyzed in terms of their security. Regarding their answers for the statements on the questionnaire; it is found out that the students are completely sufficient on social media in terms of their security. Whereas; their answers on the second dimension of the research show that they are sufficient on harmful software on the medium security. The students stated that, they are on the middle security level in terms of social engineering and web security on the third dimension of the

research. Lastly, the fourth dimension includes questions related to computer security and they stated themselves as sufficient.

As a result of the research, the students are sufficient in terms of social networks, social media which they use regularly on the other hand; they have middle security about the social engineering, web security and computer security and the main reason of this can be thought as lack of information.

Key Words: Safe (Secure) Internet, Information Security, Self-Sufficiency, TRNC, Student

YAKIN DOĞU ÜNİVERSİTESİ
EĞİTİM BİLİMLERİ ENSTİTÜSÜ
YÜKSEK LİSANS TEZ ÇALIŞMASI
ETİK BEYANI

Yakın Doğu Üniversitesi Bilimsel Araştırma ve Yayın Etiği Yönergesini okuduğumu ve anladığımı ve Yakın Doğu Üniversitesi Eğitim Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmada;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik kurallarına uygun olarak sunduğumu,
- Tez çalışmada yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde ve ortaya çıkan sonuçlarda herhangi bir değişiklik yapmadığımı,
- Tez olarak sunduğum bu çalışmanın özgün olduğunu,

bildirir, aksi bir durumda bu konuda hakkımda yapılacak tüm yasal işlemleri ve aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim. / / 20....

İMZA

Mehmet Karabulut

İÇİNDEKİLER

ÖNSÖZ.....	ii
ÖZET	iii
ABSTRACT	v
İÇİNDEKİLER.....	viii
TABLolar.....	xii
ŞEKİLLER	xiii
BÖLÜM I	1
GİRİŞ.....	1
1.1. Araştırmanın Problemi	1
1.2. Araştırmanın Amacı	6
1.3. Araştırmanın Önemi	7
1.4. Araştırmanın Sınırlılıkları	8
1.5. Kısaltmalar	9
1.6. Tanımlar	10
BÖLÜM II.....	11
KAVRAMSAL TEMELLER VE İLGİLİ ARAŞTIRMALAR	11
2.1. KAVRAMSAL TEMELLER.....	11
2.1.1. Öz-Yeterlik Algısı	11
2.1.1.1. Bilgisayar Kullanımına Yönelik Öz-yeterlik Algısı.....	12
2.1.1.2. İnternet Kullanımına Yönelik Öz-yeterlik Algısı.....	12
2.1.2. Güvenli İnternet.....	13
2.1.2. Bilgi Güvenliği	15
2.1.3. Bilişim Güvenliği	16
2.1.4. Bilişim Suçları	18
2.1.5. Sosyal Medya Güvenliği	19
2.1.6. Bilişim Güvenliğini Tehdit Eden Yazılım Temelli Unsurlar	22

2.1.6.1. Virüsler	22
2.1.6.2. Solucanlar (Worms).....	23
2.1.6.3. Truva Atı (Trojan)	23
2.1.6.4. Casus Yazılımlar (Spyware).....	24
2.1.6.5. Fidyeye Yazılımları (Ransomware)	24
2.1.6.5.1. Şifreleyici Fidyeye Yazılımları (Crypto Ransomware)	25
2.1.6.5.2. Kilitleyici Fidyeye Yazılımları (Locker Ransomware).....	26
2.1.6.6. Tuş Kaydediciler (Keylogger)	27
2.1.6.7. Reklam Yazılımları (Adware)	27
2.1.6.8. Sosyal Mühendislik Saldırıları	27
2.1.6.8.1. Oltalama (Pshing)	28
2.1.6.8.2. İstenmeyen E-Postalar (Spam)	28
2.1.7. İnternet de Yer alan İçerik Temeli Suçlar	29
2.1.7.1. Sanal Dolandırıcılık.....	29
2.1.7.2. Pornografi	31
2.1.7.3. Çocuk İstismarı.....	31
2.1.7.4. Siber Zorbalık.....	32
2.1.8. Bilişim Korsanları (Hacker)	33
2.1.8.1. Beyaz Şapkalı Hacker.....	33
2.1.8.2. Siyah Şapkalı Hacker.....	34
2.1.8.3. Gri Şapkalı Hacker	34
2.1.8.4. Lamer.....	34
2.2. İLGİLİ ARAŞTIRMALAR.....	35
2.2.1. Bilişim Teknolojileri Kullanımına Yönelik Öz-Yeterlik Algısı.....	35
2.2.2. Güvenli İnternet Kullanımına Yönelik Araştırmalar.....	36
2.2.3. Güvenli İnternet Kullanımında Ebeveyn Denetimine Yönelik Araştırmalar	38
2.2.4. Siber Zorbalık Konusunda Yapılan Araştırmalar	40
2.2.5. İnternet ve Sosyal Medya Bağımlılığına Yönelik Araştırmalar	41
BÖLÜM III.....	41
YÖNTEM.....	41

3.1. Araştırma Modeli.....	41
3.2. Evren Örneklem.....	41
3.2.2. Öğrencilerin Liselere Göre Dağılımı.....	42
3.2.5. Araştırmaya Katılan Öğrencilerin Demografik Bilgileri.....	43
3.2.3. Öğrencilerin İnternet Erişim Yerlerine Göre Dağılımı.....	44
3.2.4. Öğrencilerin Haftalık İnternet Kullanım Sürelerine Göre Dağılımı.....	45
3.3. Veri Toplama Aracı.....	46
3.4. Verilerin Analizi.....	46
BÖLÜM IV	44
BULGULAR VE YORUMLAR	44
4.2. Lise Öğrencilerinin Güvenli İnternet Kullanımına Yönelik Öz-yeterlik Algılarına İlişkin Bulgular	44
4.2.1. Sosyal Ağ (Sosyal Medya) Güvenliğine Yönelik Öz-Yeterlik Algıları.....	44
4.2.2. Zararlı Yazılımlara Yönelik Öz-Yeterlik Algıları.....	46
4.2.3. Web Güvenliği Ve Sosyal Mühendislik Konusuna Yönelik Öz-yeterlik Algıları	47
4.2.4. Bilgisayar Güvenliği Konusuna Yönelik Öz-yeterlik algıları	49
4.2.5. Öğrencilerin Güvenli İnternet Kullanımlarının Cinsiyet Faktörüne Göre Değerlendirilmesi.....	50
4.2.6. Öğrencilerin Güvenli internet kullanımına yönelik öz-yeterlik algılarının sınıf düzeyine göre farklılık var mı?	51
4.2.7. Öğrencilerin Güvenli İnternet Kullanımlarının İlçelere Göre Değerlendirilmesi	52
4.2.8. Öğrencilerin Güvenli İnternet Kullanımlarına yönelik öz-yeterliklerinin İnternet Kullanım Sürelerine Göre Değerlendirilmesi	53
BÖLÜM V	59
SONUÇ VE ÖNERİLER	59
5.1. Sonuçlar	59

5.1.1. Öğrencilerin sosyal ağ (sosyal medya) güvenliğine yönelik öz-yeterlik algıları	59
5.1.2. Öğrencilerin zararlı yazılımlara yönelik öz-yeterlik algıları	60
5.1.3. Öğrencilerin web güvenliği ve sosyal mühendislik konusunda öz-yeterlik algıları	60
5.1.4. Öğrencilerin bilgisayar güvenliğini konusunda öz-yeterlik algıları	61
5.1.5. Öğrencilerin genel itibari ile güvenli internet kullanımına yönelik öz-yeterlik algıları	62
5.1.6. Öğrencilerin güvenli internet kullanımına yönelik öz-yeterlik algıları cinsiyete göre sonuçları	62
5.1.7. Öğrencilerin güvenli internet kullanımına yönelik öz-yeterlik algıları bulundukları ilçelere göre sonuçlar	63
5.1.8. Öğrencilerin güvenli internet kullanımına yönelik öz-yeterlik algılarının Sınıf Düzeylerine Göre Sonuçları	63
5.2. Öneriler	63
5.2.1. Öğrencilere Yönelik Öneriler	63
5.2.2. Öğretmenlere Yönelik Öneriler	63
5.2.3. Akademisyenlere Yönelik Öneriler	63
KAYNAKÇA	65
EK 1. Öğrencilerin Güvenli İnternet Kullanımına Yönelik Öz-Yeterlik Algıları Ölçeği ...	79
EK 2. Genel Ortaöğretim Dairesinden Alınan İzin Belgesi	82
EK 3. Mesleki Teknik Öğretim Dairesinden Alınan İzin Belgesi	83
ÖZGEÇMİŞ	84

TABLOLAR

Tablo 1. Katılımcıların tabakalara göre öğrenci dağılımı.....	42
Tablo 2. KKTC’de Bulunan Liselerin Dağılımı	43
Tablo 3. Öğrencilerin Demografik Bilgilerine Göre Dağılımı	44
Tablo 4. İnternet’e Erişim Ortamlarına Göre Dağılım	45
Tablo 5. İnternet kullanım sürelerine göre dağılım	46
Tablo 6. Beşli Derecelendirmede Kullanılan Sınırlar	47
Tablo 7. Sosyal Ağ (Sosyal Medya) Güvenliği boyutuna İlişkin Ortalama Verileri	44
Tablo 8. Zararlı Yazılımlar Boyuna İlişkin Ortalama Verileri	46
Tablo 9. Web Güvenliği ve Sosyal Mühendislik Boyutu	48
Tablo 10. Bilgisayar Güvelliği Boyutuna İlişkin Ortalama Verileri	49
Tablo 11. Güvenli İnternet Kullanım Öz-Yeterliğinin Cinsiyete Göre Mann-Whitney testi sonuçları	50
Tablo 12. Öğrencilerin Güvenli İnternet Kullanımına Yönelik Öz-Yeterlik Algılarının Sınıf Düzeyinde Değerlendirilmesi	51
Tablo 13. Öğrencilerin Güvenli İnternet Kullanımlarına Yönelik Öz-Yeterlik Algılarının İlçeler Göre Değerlendirilmesi	52
Tablo 14. Öğrencilerin Güvenli İnternet Kullanımlarına Yönelik Öz-Yeterlik Algılarının Haftalık İnternet Kullanımlarına ilişkin değerlendirilmesi	53

ŞEKİLLER

Şekil 1. Sosyal Medya Kullanım Oranları (F. Kılıç, 2016).....	20
Şekil 2. Şifreleyici Fidyeye Yazılımı (Bhardwaj ve diğerleri, 2016).....	26
Şekil 3. Kilitleyici Fidyeye Yazılımı (“Locker Ransomware”, 2016)	26

BÖLÜM I

GİRİŞ

Bu bölümde araştırmanın problemi, araştırmanın amacı, sınırlılıklara ve sayıtlarına yer verilmektedir.

1.1. Araştırmanın Problemi

Bilişim çağını yaşamakta olduğumuz bugün, bilgi ve iletişim teknolojilerinin (BİT) hızlı gelişimi ile dijital dünya şeklini almıştır. Dijital dünya; insan yaşamını kolaylaştırırken kendisine ait sosyal ortamı, iş çevresi, yasası ve yaptırımları olan günümüz dünyası içerisinde oluşturulmuş ayrı bir dünya olarak tanımlanabilmektedir (Aydın, 2013; Bozkurt, 2013; Erdoğan ve Bahtiyar, 2014).

20.yy.'ın son dönemleri BİT alanında gelişmenin ve yeniliklerin başlangıç dönemi olarak ifade edilebilir. 20.yy.'ın en önemli buluşu olan internet teknolojisiyle bireylerin bilgiye erişimi hızlanırken, anlık erişimle birlikte zaman ve mekân kısıtlamasının ortadan kalkması, sosyal ağ ortamlarının insanların sosyalleşmesini sağlaması, gelişim sürecinde en büyük etkenler olarak görülmektedir (Akca, Sayımer, Salı ve Başak, 2014)

21.yy'a gelindiğinde insanların bilginin yoğun olarak kullanıldığı döneme geçiş yaptıkları görülmektedir. Bu dönem BİT alanında yeniliklerin ve gelişmelerin en çok yaşandığı dönem olarak kabul edilmektedir. 21.yy toplum ve bilim adamları tarafından bilgi çağı olarak kabul görmüştür (İşman, 2011). Bu dönemde internet teknolojisinin yapısında meydana gelen gelişmeler ile web 1.0'ın mevcut sistemi olan tek yönlü iletişim yerini Web 2.0 teknolojisinin sunduğu çift yönlü iletişime bırakmıştır (Aghaei, Nematbakhsh ve Farsani, 2012; Kırık, 2014)

İnternet Teknolojisinin sürekli olarak gelişmesi ve yaygınlaşması ile beraber, bireysel veya kurumsal kullanımda bilgi edinme, aktarma, tanıtımların kolay şekilde gerçekleştirilebilmesi, meydana gelen gelişmelerin takip edilebilmesi vb. gibi uygulamalar insan yaşamında etkili olmaya başlamıştır (Akgün ve Topal, 2015).

İnternet insan yaşamına dair birçok farklı alanda etkin şekilde kullanılmaktadır. Evlerde, iş yerlerinde, devlet hizmetlerinde, askeri alanda, sağlık sektöründe vb. gibi birçok alanda kendine yer edindiği gibi eğitim alanında kullanılan e-kitaplar, bloglar, çevrimiçi eğitim araçları ile daha yenilikçi ve kalıcı öğrenmenin sağlanmasında internet önemli rol oynamaktadır (Bedir, 2012). Kişisel kullanımda mobil araçların kullanımının artması ile sosyal medya kullanımı yaygınlaşmaya başlamıştır (O’Keeffe ve Clarke-Pearson, 2011).

İnternet teknolojisinin yaşamımızda etkin şekilde yer alması ile kullanıcı sayısı her geçen yıl daha da artmaktadır. Bu artış daimi olarak araştırmalara konu olmaktadır (Aslan, 2016; Topal ve Akgün, 2015; Yılmaz, Şahin, Haseski ve Erol, 2014).

İnternet kullanımına yönelik Türkiye İstatistik Kurumu (2013) yılında yayınladığı raporunda çocukların ortalama internet kullanmaya başlama yaşı 8 yaş olarak tespit edilmiştir. Araştırmada 6-10 yaş arası internet kullanım oranı %36,9 iken 11-15 yaş gurubunda ise %65,1 olarak tespit edilmiştir (Türkiye İstatistik Kurumu, 2013).

Sosyal medya ortamları bilinçsiz kullanıcılara yönelik birçok tehlikenin barındığı ortamlar olarak ifade edilebilir. Bu konuda bilinçlendirilmemeleri ve denetlenmemeleri halinde istenmeyen durumlarla karşılaşılması muhtemeldir.

Sosyal paylaşım platformlarında çocuk ve genç kullanıcıların yoğun olarak varlık göstermesi bu risk unsurlarının yayılmasında önemli bir etken olarak kabul edilebilmektedir. Çağıltay, Karakuş, Kurşun ve Kaşıkçı (2011) yaptıkları çalışmada elde ettikleri bulgulara göre çocukların %44’ü olan sosyal ortamların güvenli alanlar olduğuna inanırken %40’ı güvenli bir alan olmadığını bilmektedirler. %16 oranında bir grup ise konuya yönelik fikirlerinin olmadığını belirtmişlerdir.

We Are Social firmasının 2017 yılı dünya çapında yapılan araştırma sonucunda elde edilen bilgiler incelendiğinde 7,476 milyar dünya nüfusunun 3,773 milyarı aktif internet kullanıcısı olduğu tespit edilmiştir. Aynı araştırmanın 2016 yılı verileri ise 7,395 milyar insan nüfusunun 3,419’ u aktif internet kullanıcısı olarak kayıt altına alınmıştır (We Are Social, 2017). Burada bizlere kullanıcı sayısında dünya çapında kayda değer bir artış olduğu açıkça göstermektedir.

Türkiye İstatistik Kurumu (TÜİK) (2016) yılı verilerinde Türkiye nüfusunu 79,814,871 olarak tespit edilmiştir. Bu rakamın %61,2'si internet kullanıcısı olarak tespit edilmiştir. We Are Social raporunda internet kullanımı ise 46,28 milyon (%58) olarak tespit edilmiştir Türkiye'de 42 milyon (%53) aktif sosyal medya kullanıcısı olduğu We Are Social'ın raporu ile tespit edilmiştir (Türkiye İstatistik Kurumu, 2016; We Are Social, 2017)

Kıbrıs'a yönelik araştırmalar incelendiğinde ise Güney Kıbrıs Rum Yönetiminde internet kullanım oranları We Are Social raporunda 0,93 milyon olarak tespit edilmiştir. Kuzey Kıbrıs Türk Cumhuriyeti' de ise Bilgi Teknolojileri Haberleşme Kurumu (BTHK)'nın paylaştığı olduğu raporda bu sayı sabit geniş bant internet kullanımında 111,670 olarak belirlenmiştir. Akıllı telefonların yaygınlaşması ile mobil internet kullanımı artış göstermektedir. Kuzey Kıbrıs Türk Cumhuriyeti'nde belirlenen mobil internet kullanıcısı 313,218 olarak tespit edilmiştir (Bilgi Teknolojileri Ve Haberleşme Kurumu, 2015).

BİT ve İnternet'in günümüzde çok yoğun şekilde yaşam döngüsünde yer alması ve hızlı gelişiminin insan yaşamına yönelik birçok faydalı etkileri olmasına karşın zararlı etkileri 'de azımsanmayacak miktardadır. Kurumsal ve kişisel anlamda her alanda kullanılabilmesi bu teknolojiyi kötü amaçlı kullanıcılar için önemli bir araç haline getirebilmektedir (Akgün ve Topal, 2015). BİT 'in bilinçsiz kullanımı sonucunda kullanıcılar birçok farklı olumsuz içerikler ile karşılaşabilmektedir.

Aydın (2011) lise öğrencilerine yönelik yapmış olduğu "Liselerde Bilgisayar ve İnternet Kullanımının Eğitim ve Öğretimdeki olumsuz etkileri" konulu yüksek lisans tez çalışmasında öğrencilerin %78,2'sinin pornografik içeriklerle, %43,2' sinin kumar, %6.8' inin uyuşturucu madde, %25'inin ırkçılık, terör propagandaları ve %25'inin çeşitli sapkın akımlara yönelik içerikler ile karşılaştıklarını tespit etmiştir.

İnternet üzerinde denetimsizliğin getirdiği bir sorun olarak; erken yaşta kullanıcıların yasal olmayan cinsel içerikli veya şiddet içerikli sitelere rahat ulaşabilmesi, istem dışı reklamlar yolu ile yönlendirilebilmeleri bir diğer risk unsuru olarak uyuşturucu ticareti veya terör yandaşlarının interneti propaganda ortamı olarak kullanmaları interneti tehlikeli bir ortam haline getirmektedir (Çelen, Çelik ve Seferoğlu, 2011).

Karakuş ve diğerleri (2014) yaptıkları çalışmada Türkiye ve Avrupa’da çocukların güvenli internet kullarımlarını incelemişlerdir. Çalışma verileri incelendiğinde internet ortamında cinsel içerikler ile karşılaştığını belirten öğrencilerin oranı Türkiye’de %11 iken Avrupa’da %15,5 olarak belirlenmiştir. Araştırmaya katılan ve bu soruyu yanıtsız bırakan öğrencilerin oranı %85,6 olarak belirlenmiştir. Araştırmaya Türkiye’den katılan çocuklardan %48,2, Avrupa’dan katılan çocukların %27,1’i karşılaştığı cinsel içeriklerden rahatsızlık duyduğunu belirtmiştir.

İnternet üzerinde yer alan tehditlerin daha rahat incelenmesi aşamasında güvenlik yazılım üreten firmalar tespit edilen zararlı durumları raporlamakta ve sonuçları çevrim içi ortamda yayınlamaktadır. Burada amaç güvenlik zafiyetlerinin tespiti ve bu konuda kullanıcıları bilgilendirerek bu zararların en düşük seviyeye indirgenmesine katkı sağlamaktır.

Kaspersky Lab (2016) raporu incelendiğinde dünyadaki birçok çevrimiçi kaynaktan yapılan 758,044,650 siber saldırının engellendiği belirtilmiştir. Ayrıca 2,871,965 cihazda çevrimiçi bankacılık yoluyla para çalmayı hedefleyen Malware tespit edilmiş ve temizlenmiştir. Kaspersky antivirüs programı ile toplam 4,071,588 zararlı ve potansiyel olarak istenmeyen yazılım tespit edilmiştir. Web antivirüs sistemi ile toplamda 69,277,280 istenmeyen yazılım tespiti yapılmıştır. 2016 yılı özellikle fidye yazılımlarının yılı olarak belirtilmiştir. 1,445,434 kullanıcı bilgisayarı fidye yazılımları tarafından hedef alınmıştır.

Trend Labs (2016) verileri incelendiğinde çevrimiçi bankacılık yolu ile dolandırıcılık tehdidi dikkat çekmektedir. Trend Labs tarafından tespit edilen 11,516.00 çevrimiçi dolandırıcılık girişimi tespit edilmiştir. Bu rakam ile Türkiye Avrupa ülkeleri arasında birinci sırada bulunmaktadır. Ayrıca Trend Micro antivirüs tarafından 2016 yılı içerisinde 691.126,00 zararlı web sitesini ve bu sitelere yönelik yapılan 10.998,33 zararlı tıklamayı tespit edip önlemiştir. Türkiye genelinde 25.943,549 spam e-posta tespit edilmiştir. Tespit edilen zararlı yazılımların toplam miktarı ise 2.548,326 olarak tespit edilmiştir. Mobil uygulama sektöründe yapılan incelemelerde toplamda 658.799,00 şüpheli yazılım indirilmiştir. İndirilen uygulamalar arasında 10.747,00 mobil virüs tespit edilmiştir.

İnternet teknolojisinin kullanıcılara sağladığı en büyük kolaylıklardan bir tanesi bilgi paylaşımıdır. Bilinçli kullanıcılar için oldukça avantajlı sayılan bu sistem aynı zamanda birçok sorunu içinde barındırmaktadır. Özellikle genç kullanıcılar açısından bu problemlerin başında internet ortamında güvenlik sorunu ve internet ortamında bilgilerin gizliliğinin sağlanması sorunu gelmektedir (Johnson ve diğerleri, 2012).

BİT ve İnternet yetişkinlerde olduğu kadar çocuk yaşta kullanıcılar arasında da önemli oranda kullanım alanına sahiptir. Günümüzde çocuklar erken yaşta internet kullanmaya başladıkları gibi kullanıcıların yarısından fazlası sosyal paylaşım platformlarında hesap edinmektedir (Karakuş ve diğerleri, 2014).

Staksrud, Ólafsson ve Livingstone (2013) 25 ülkeden 1000 kişi ile yaptıkları çalışmada sosyal ağ sitelerini kullanan çocukların cinsel içerikli mesaj alma ihtimallerini %46 olarak tespit etmişlerdir. Ayrıca web ortamında cinsel içerikli medyalarla karşılaşma ihtimalleri ise %55 olarak tespit edilmiştir.

Erken yaşta kullanıcıların sosyal medya kullanımlarında karşılaşılabilecekleri tehlikelerden bir tanesi de sosyal medyanın kontrolsüz ve aşırı kullanımından kaynaklanan sosyal medya bağımlılığı olarak ifade edilebilir. Sosyal medya bağımlılığı olarak değerlendirilen durumlarda kullanıcılar sosyal medya ortamlarında ne kadar zaman geçirdiklerini unutmakta ve gerçek yaşamda sorumluluklarını aksatabilmektedir. Bunun yanında gerçek sosyal çevreleri ile ilişkilerini geri plana atarak sanal sosyal ortamlarındaki arkadaş sayısına odaklanmaktadırlar. Sosyal medya bağımlılığı genellikle çevresi ve ailesi ile iletişim zorluğu yaşayan bireylerde görülen bir problem olarak ifade edilebilir (Kırık, Arslan, Çetinkaya ve Gül, 2015)

Akbulut (2013) bu konuda denetim yetersizliğinden dolayı meydana gelen sorunlardan korunmaya yönelik yapılması gerekenleri “Çocukların internet etkinliklerinin niteliğini, zamanını, yerini ve süresini belirli bir süreci tamamlayana kadar denetlemesini gerektirmektedir. Bu süreç içerisinde mümkün olduğunca internet etkinliklerinin çocuk ile birlikte zaman geçirme süreci olarak değerlendirilmesi daha doğru bir yönelim olacaktır “şeklinde ifade etmiştir.

BİT alanında yer alan ve tehdit oluşturan unsurlara karşı önlem alınmasında okullarda görev yapan bilişim öğretmenlerine önemli görevler düşmektedir (Gökmen, 2014). İnternetin yaşamın her aşamasında yoğun olarak kullanılması güvenlik zaafiyetlerini de beraberinde getirmektedir. Kullanıcıların konuya yönelik öz-yeterliklerinin denetlenmesi bilinçlendirme aşamasında yapılması gerekenlere kaynak oluşturacağı düşünülmektedir.

Bu bağlamda Dünyada ve Türkiye’de yapılan çalışmalar incelendiğinde önemli derecede yol alındığı görülmektedir. Ancak ülkemizde güvenli internet kullanımı konusu üzerinde yeterince durulmamış olması yapılan araştırmalar sonucunda ortaya koyulan bir gerçek olarak karşımıza çıkmaktadır. Yapılan araştırma sonucunda akademik anlamda tek bir çalışma Erçağ (2014) yılında yapmış olduğu “Otantik Öğrenme Yaklaşımıyla Tasarlanan Sanal Öğrenme Ortamlarının Öğretmenlerin Güvenli İnternet Kullanımına Yönelik Başarısına, Memnuniyetine ve Öz-Yeterlik Algısına Etkisi” konulu doktora tezidir. Araştırmanın öğretmenlere yönelik olması açısından düşünüldüğünde öğrencilere yönelik yapılan bir çalışma bulunmaması bu alanda bilimsel, akademik çalışmaların yapılması gerekliliğini ortaya koymaktadır.

Bu aşamada öğrencilerin güvenli internet kullanımına yönelik öz-yeterlik algılarının nasıl olduğu araştırmanın problemi oluşturmaktadır.

1.2. Araştırmanın Amacı

Bu araştırmanın amacı KKTC MEB bakanlığına bağlı Mesleki Teknik Öğretim Dairesi ile Genel Ortaöğretim dairesine bağlı bulunan liselerdeki öğrencilerin güvenli internet kullanımına yönelik öz-yeterlik algılarının değerlendirilmesidir. Bu bağlamda araştırmanın amacına ulaşması için aşağıdaki alt amaçlara yanıt aranmıştır.

- Öğrencilerin sosyal ağ (sosyal medya) güvenliğine yönelik öz-yeterlik algı düzeyleri nasıldır?
- Öğrencilerin zararlı yazılımlara yönelik öz-yeterlik algı düzeyleri nelerdir?
- Öğrencilerin web güvenliği ve sosyal mühendislik konusunda öz-yeterlik algı düzeyleri nasıldır?
- Öğrencilerin bilgisayar güvenliğini konusunda öz-yeterlik algı düzeyleri nasıldır?

- Öğrencilerin güvenli internet kullanımına yönelik öz-yeterlik algıları cinsiyete göre farklılık var mı?
- Öğrencilerin güvenli internet kullanımına yönelik öz-yeterlik algılarında sınıf düzeyine göre farklılık var mı?
- Öğrencilerin güvenli internet kullanımına yönelik öz-yeterlik algılarında bulundukları ilçelere göre farklılık var mı?
- Öğrencilerin güvenli internet kullanımına yönelik öz-yeterlik algılarının internet kullanım sürelerine göre farklılık var mı?

1.3. Araştırmanın Önemi

Endüstri toplumundan bilgi toplumuna geçişte en önemli etken 21. Yüzyıla damgasını vuran en önemli buluş olarak gösterilen internet olarak ifade edilebilir. Bugün mobil teknolojilerin de internete erişim sağlayabilmesi teknolojinin ve internetin insan yaşamındaki kullanım alanını ve önemini daha da arttırmıştır (Gök, 2012).

Günümüzde medyadan, ekonomiye, sağlık alanı, devlet daireleri, alış-veriş, sosyal ortamlar, turizm, eğitim sektörü, sanayi vb. daha birçok alanda internet kullanımı, işlerimizi hızla ve kolaylıkla yapabilmemizi sağlamaktadır. İnternet teknolojileri bilgiye hızlı erişim, çevrimiçi iletişim imkânları ile insanlara geniş bir özgürlük sağlamaktadır (Tercan, Sakarya ve Çoklar, 2012).

İnternet kullanımının hızla yaygınlaşması ile internet ortamında risk unsurlarının artmasına ortam sağlamıştır. İnternet üzerinde yer alan risk unsurları genel itibari ile çocukları hedef almaktadır. Aydın (2013) yapmış olduğu çalışmada internetin getirdiği riskleri zorbalık, cinsel içerikli mesajlar, tanınmayan kişilerle etkileşim, pornografi ve kişisel bilgilerin kötüye kullanımı olarak tanımlamaktadır.

Livingstone, Kirwil, Ponte ve Staksrud (2013) Avrupa Çevrimiçi Çocuklar (EU Kids Online) projesi kapsamında 9-16 yaş Aralığında 25,142 kişi ile yaptıkları araştırma sonucunda çocukların %55' inin internet ortamında kendilerini rahatsız eden içeriklerle karşılaştıkları bulgusuna ulaşmışlardır. Araştırmada elde edilen bulgular detaylandırıldığında ise çocukların %58'i kendilerini rahatsız eden unsurları Pornografi,

şiddet vb. içerikler olarak tanımlarken çocukların %42' si ise davranış ve temas içerikli riskler (virüsler, saldırgan davranışlar, istenmeyen mesajlar, uygunsuz resim ve mesajlar) olarak belirtilmiştir.

Dünyada internet üzerinden işlenen suçlar bilişim suçları yasası kapsamında değerlendirilirken KKTC'de bilişim yasası bulunmamasından dolayı yaşanan mağduriyetlere yönelik resmi kayıt bulunamamıştır. Bilişim Güvenliği ve İnternetin bilinçli kullanımına yönelik çalışmaların önemli oranda bir gereklilik arz ettiği ülkemizde, bu alandaki araştırmaların az olması önemli bir eksiklik oluşturmaktadır.

Mevcut risk unsurları göz önünde bulundurulduğunda bu araştırma ile KKTC' de bulunan liselerdeki öğrencilerin “Güvenli İnternet Kullanımı” konusunda öz-yeterliklerinin araştırılması ve değerlendirilmesi araştırmanın önemini açıkça vurgulamaktadır.

1.4. Araştırmanın Sınırlılıkları

- Araştırma 2015 -2016 öğretim yılı ile,
- KKTC Millî Eğitim Bakanlığına Bağlı Genel Orta Öğretim ve Mesleki Teknik Orta Öğretim dairesine bağlı bulunan liselerdeki öğrenciler ile,
- Araştırmada veri toplamak amacı ile kullanılan anket ile,
- Araştırma gönüllü katılımcılar ile sınırlıdır.

1.5. Kısaltmalar

BIT	Bilgi ve İletişim Teknolojileri
FBI	Federal Soruşturma Bürosu
TÜİK	Türkiye İstatistik Kurumu
HHBTK	Hane Halkı Bilişim Teknolojileri Kullanımı Araştırması
BTHK	Bilgi Teknolojileri Haberleşme Kurumu
MEB	Millî Eğitim Bakanlığı
KKTC	Kuzey Kıbrıs Türk Cumhuriyeti
MTOÖ	Mesleki Teknik Ortaöğretim
GOÖ	Genel Ortaöğretim
BÖTE	Bilgisayar ve Öğretim Teknolojileri Eğitimi

1.6. Tanımlar

Öz-Yeterlik Algısı: Bireyin herhangi bir alanda karşılaşacağı problemlerin üstesinden gelebileceğine dair bilgi ve yeteneklerine olan inancı olarak tanımlanabilmektedir.

Güvenli İnternet: İnternet teknolojisinin barındırdığı tehlikelerden korunarak güvenli bir şekilde kullanımının sağlanması olarak tanımlanabilir.

Sosyal Medya Bağımlılığı: Sosyal Medyanın aşırı ve kontrolsüz kullanımı sonucunda ortaya çıkan sağlık problemi olarak tanımlanabilir.

Zararlı Yazılım: İnternet ortamında yer alan ve zarar vermek amacı ile hazırlanmış olan programlardır.

Sosyal Mühendislik: Hırsızlık ve zarar vermek amacı ile yazılan bilgisayar yazılımlarıdır. Genelde saldırının gerçekleştirilmesinde kullanılan araçlar e-mail hesapları ve sosyal medya araçlarıdır. Sosyal Mühendislik yazılımlarını diğer kötü amaçlı yazılımlardan ayıran ise hedef olarak insan faktörünün seçilmesidir.

BÖLÜM II

KAVRAMSAL TEMELLER VE İLGİLİ ARAŞTIRMALAR

Bu bölümde araştırmanın kavramsal çerçevesi ve konu ile ilgili araştırmalar açıklanmaya çalışılmıştır.

2.1. KAVRAMSAL TEMELLER

2.1.1. Öz-Yeterlik Algısı

Öz-yeterlik sosyal bilişsel kuramın temelini oluşturan en önemli kavram olarak görülmektedir. Sosyal Bilişsel Teori temelinde yeteneklerin kullanılabilmesi için alana dair sahip olunan bilgi birikimine yönelik bireyin kendine olan inancı konusuna dayanmaktadır (Bandura, 2011, 2012; Bolat, 2011).

Bandura (1994) yapmış olduğu çalışmada bir konuya yönelik öz-yeterliğin yüksek olması halinde bireyin o konuda başarılı olmak için elinden gelen tüm çabayı göstereceğini, diğer taraftan öz-yeterliği düşük olan bireylerin ise bahsi geçen konuda başarılı olmak adına çok fazla çaba göstermeyeceğinden dolayı, karşılaşılabilecek zorluklar karşısında kendi yeteneklerine yeteri kadar güvenemeyeceğini ve vazgeçme eğiliminin yüksek olacağından bahsetmektedir.

Öz-yeterlik algısı insan davranışlarının anlaşılması ve değerlendirilmesinde önemli bir yeri olduğundan dolayı herhangi bir işi yapmaya ilişkin performansı etkilediği, karşılaşılan zorlukların aşılmasında önemli bir etken olarak görülebilir (Balay, Kaya ve Çevik, 2014).

Öz-yeterlik kişilerin performansına doğrudan etkili bir durumdur. Farklı alanlarda farklı türevleri bulunan öz-yeterlik algısının temelde özelliği bireylerin herhangi bir konuda etkinliği ile ilgili bir durum olarak değerlendirilebilir. Bireylerin etkin faaliyette oldukları bir konuda karşılaşılabilecekleri problemlerin üstesinden gelmekte zorlanmadıkları yapılan çalışmalarda (Baş, 2011; Bayırtepe ve Tüzün, 2007; Kurbanoglu, 2004) ortaya koyulmaktadır.

Eğitim alanı açısından ele alındığında öz-yeterlik inancı öğrenmenin gerçekleşmesi sürecinin duyuşsal boyutunu tanımlamada yer alan önemli değişkenlerden biri olarak gösterilmektedir. Öğrenci merkezli öğrenme yaklaşımlarının yaygınlaşması ile birlikte önem kazanmıştır (Tuncer ve Tanaş, 2011). İnternetin eğitim alanındaki uygulama alanının genişlemesi ile birlikte, internet üzerindeki aktiviteleri organize etme ve uygulama konusunda bireylerin kendilerine olan inançları olarak tanımlanan internet öz-yeterliği kavramı ön plana çıkmaktadır (Akın, Kaya, Akın, Sahranç ve Uğur, 2014; Kuo, Walker, Schroder ve Belland, 2014).

2.1.1.1. Bilgisayar Kullanımına Yönelik Öz-yeterlik Algısı

Bilgisayar kullanımına yönelik öz-yeterlik algısı yüksek olan bireylerin bilgisayar uygulamaları ve etkinlikleri konusunda daha etkin katılım göstermektedirler. Aynı zamanda bilgisayar öz-yeterliği yüksek olan bireyler bilgisayar konusunda karşılaşılabilecekleri sorunların üstesinden gelmekte daha başarılı olmaktadır (Bayırtepe ve Tüzün, 2007).

Tekerek, Ercan, Udum ve Saman (2012), Bilgisayar ve Öğretim Teknolojileri Eğitimi bölümünde (BÖTE) öğrencilerinin bilgisayar öz-yeterliklerini değerlendirmeye yönelik yaptıkları çalışma sonucunda BÖTE öğrencilerinin bilgisayar kullanımına yönelik öz-yeterlik algılarının yüksek olduğunu tespit etmişlerdir.

Timur, Yılmaz ve Timur (2013) farklı bölümlerde öğrenim görmekte olan öğretmen adaylarına yönelik yaptıkları çalışma sonucunda bilgisayar kullanım öz yeterliliklerinin bölümlere göre farklılık gösterdiği bulgusuna ulaşmışlardır.

2.1.1.2. İnternet Kullanımına Yönelik Öz-yeterlik Algısı

İnternet Öz-yeterliği yüksek olan bireyler internet kullanımı konusunda bilinçli ve dikkatli kullanıcılar olarak internetten kaynaklanan risklere karşı gerekli önlemleri alabilmekte böylelikle interneti etkin şekilde kullanabilmektedir. İnternet öz-yeterliği düşük olan bireylerde ise bu durumun tersi söz konusudur (Sırakaya, 2011).

Balay ve diğerleri (2014) 290 öğretmen ile yaptıkları çalışma sonucunda internet kullanımına ilişkin tutumları orta derecede yeterli olan öğretmenlerin eğitsel internet

kullanımına yönelik algıları ise yeterli düzeyinde olduğu tespit edilmiştir. İnternet kullanımına yönelik alınacak pozitif bir tutumun eğitsel internet kullanımına yönelik öz-yeterlik algılarında’ da artış gösterdiğini tespit etmişlerdir.

Kahraman, Yılmaz, Erkol ve Yalçın (2013) yaptıkları çalışmada öğretmenlerin bilgisayar kullanım deneyimlerinin eğitsel amaçlı internet kullanım düzeyleri konusunda önemli sonuçlara ulaşmışlardır. Araştırmada 4 yıl ve üzeri bilgisayar kullanım deneyimine sahip öğretmen adaylarının eğitsel amaçlı internet kullanımına yönelik öz-yeterlik algıları 1 yıllık internet kullanıcısı olan öğretmenlere göre daha yüksek olduğu belirlenmiştir.

Sonuç olarak bilişim teknolojileri alanında karşılaşılan problemlerin üstesinden gelebilmek ve çözüm üretebilmek için bilgisayar ve internet kullanımına yönelik yeterli düzeyde öz-yeterliğe sahip olmak ile mümkün olacağı söylenebilir.

2.1.2. Güvenli İnternet

İnternetin hızlı gelişimi ve yaygınlaşması ile paralel olarak her geçen gün artış gösteren riskler göz önünde bulundurulduğunda “Güvenli İnternet” konusunun önemini artırdığı söylenebilir. Güvenli internet, kullanıcıların internet ortamında yer alan zararlı yazılımlardan ve istenmeyen içeriklerden arındırılmış şekilde interneti kullanabilmeleri olarak tanımlanmaktadır (Mert, Bülbül ve Sağıroğlu, 2012).

Güvenli internet kavramı olarak bakıldığında kişisel verilerin internet ortamında yer alan tehlikelerden korunması olarak açıklanabilir. İnternet ortamında yer alan tehlikeler konusunu Aslan (2016) çalışmasında “İnternet’te bireyleri kişisel, sosyal ve psikolojik yönden olumsuz şekilde etkileyerek bireylerin iyi olma hallerine zarar verecek nitelikteki içerik ve iletiler” şeklinde belirtmiştir.

İnternet teknolojisi hayatımızı kolaylaştıran bir yapı olduğu gibi, özellikle çocuk ve genç kullanıcılar olmak üzere genelde tüm kullanıcılara yönelik tehlikeler barındırmaktadır. Fiziksel dünyada işlenen suçlar sanal dünyada da işlenebilmekte ve bunun yapılabilmesi için aynı fiziksel ortamda bulunmaları dahi gerekmemektedir. Dolandırıcılık, zorbalık, istismar, kişisel hakların ihlali ve siber terörizmde dâhil olmak üzere birçok suç internet üzerinde

işlenebilmektedir (Hekim ve Başbüyük, 2013)□. Özellikle internet ortamında yer alan sosyal ağ siteleri bilinçsiz kullanıcılara yönelik birçok tehlike barındırmaktadır. Kullanıcıların sosyal ağ ortamlarında gerekli güvenlik ayarlarını yapamamaları durumunda kişisel bilgilerinin çalınarak kötü amaçlarla kullanılması, illegal internet sitelerinde yayımlanması gibi birçok riski de beraberinde getirmektedir. Aynı zamanda kullanıcıların bilgisayarlarında interneti güvenli şekilde kullanabilmeleri için güncel ve lisanslı antivirüs kullanmaları önem arz etmektedir (Çavus ve Ercağ, 2014).

İnternet ortamında yer alan tehdit unsurlarının bilinçsiz kullanıcıları hedef alması bu konuda önlemler alınmasını gerekli kılmıştır. Bu aşamada öncelikli olarak çevrimiçi ortamlarda çocukları bekleyen risk unsurlarının belirlenmesi gerekliliği ön plana çıkmaktadır. (Canbek ve Sağiroğlu, 2007) yaptıkları çalışmada çocuk ve genç kullanıcıların internet ortamında karşılaşılabilecekleri risk unsurlarını aşağıdaki şekilde sıralamışlardır:

- Pornografik öge, düşmanlık, öfke ve şiddet ihtiva eden yasa dışı içeriklere internet üzerinde maruz kalabilme,
- Çevrimiçi ortamlarda, kendilerini veya ailelerini tehlikeye atacak adres, kredi kartı numarası, evde o an kimin ya da kaç kişinin bulunduğu bilgisi gibi bilgileri üçüncü şahıslara, eposta veya sohbet programları vasıtasıyla iletebilme,
- İnternet üzerinden ebeveynlerinin kredi kartı ile haber vermeden alışveriş yapabilmeye
- Kendisinden yaşça büyük ve kötü niyetli kişilerle ve suç örgütleri ile haberleşebilme olarak ifade edilebilir.

İnternet teknolojisinin sağlamakta olduğu kolaylıklardan sorunsuz yararlanılabilmesi güvenli internet kullanımı konusunda bilinçli kullanıcılar olmakla mümkün olabildiği gibi ülkelerin internet ortamında işlenmekte olan suçlara yönelik yasal yaptırımlar oluşturmaları gerekmektedir.

İnternet ortamında güvenliğin sağlanması amacıyla yapılan çalışmalara bakıldığında ABD çocukları internetin zararlarından koruyabilmek amacıyla 2000 yılında “Çocukların İnternetin Zararlarından Korunması Yasası” CIPA olarak bilinen yasayı onaylamıştır. Amaç

okul ve kütüphanelerde çocukları internetin zararlarından koruyacak güvenlik programlarını zorunlu hale getirmektir (Akca, Sayımer, Salı ve Başak, 2014).

Avrupa da internet ortamında işlenen suçların önüne geçmek amaçlı çalışmalar sonucunda 2001 yılında 47 ülke tarafından imzalanan Avrupa Konseyi Siber Suçlar Sözleşmesi yürürlüğe girmiştir (Ceylan, 2013; Henkoğlu ve Yılmaz, 2013)□.

Dünyada internetin güvenli kullanımına yönelik yapılan çalışmalara paralel olarak Türkiye ‘de girişimler hızlandırılmıştır. Türkiye’de 04.05.2007 tarihli 5651 sayılı kanun “İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Kanunu“ ile sanal ortamda olan suçlarla mücadelede önemli bir adım atılmıştır (Bayzan ve Özbilen, 2012). Dünyada 2004 yılında kutlanmaya başlayan güvenli internet günü etkinlikleri 2010 yılı itibari ile Türkiye’de kutlanmaya başlanmıştır. Bilgi Teknolojileri ve İletişim Kurumu (BHK) öncülüğünde faaliyet gösteren www.guvenlinet.org, www.guvenliweb.org.tr ve çocuklara yönelik hizmet veren www.guvenlicocuk.org.tr siteleri Türkiye’de güvenli internet kullanımına yönelik atılmış önemli adımlar olarak gösterilebilir (Çubukcu ve Bayzan, 2013).

2.1.2. Bilgi Güvenliği

“Bilgi” geçmişten günümüze en değerli varlık olma niteliğini sürdürmektedir. Değerinden ötürü bilginin güvenliği önemli bir sorun olarak değerlendirilmektedir. İnternet ile gelen sosyal alanların artması, iletişim alanlarının çoğalması ile internet ortamında bulunan veri miktarında önemli oranda artış meydana gelmiştir. Bu alanlara erişim yaşının gün geçtikçe aşağı çekilmesi ile birlikte bilgi güvenliğinin sağlanmasına yönelik kurumsal ve kişisel ihtiyaç üst seviyeler çıkmıştır (Arıtürk, 2014).

Bilgi güvenliğinin ne olduğuna dair tanımlamalara bakıldığında (Moğol, 2016) yapmış olduğu tez çalışmasında bilgi güvenliğini “bilgiye yetkisiz erişim, kullanım, açığa çıkarma, bozulma, değişiklik, inceleme, teftiş, kayıt veya imha durumlarına karşı savunma uygulaması” şeklinde tanımlamıştır.

Bilginin güvenliğini sağlanması amacı ile kullanılacak bilişim teknolojilerinin güvenliğini amacı ise bu teknolojiyi kullanacak olan kişi ve kurumların karşılaşabilecekleri tehdit ve tehlikelerin analizlerinin yapılması ve gerekli önlemlerin alınmasının sağlanması olarak tanımlanmaktadır (Canbek ve Sağıroğlu, 2006).

Mccumber güvenlik bileşenleri tanımlamasında özellikle üç ana madde üzerinde durulmuştur. Bunlar sırasıyla; gizlilik, bütünlük ve kullanılabilirlik 'dir. Bu üç madde Mccumber' in geliştirmiş olduğu " bilginin karakteristiği" grubunun altında yer alan temel maddelerdir (Henkoğlu ve Yılmaz, 2013).

- **Gizlilik:** Bilgiye erişimin sadece yetki sahipleri ile sınırlandırılması, yetkisi olmayan kişilerin bilgiyi ifşa etmelerinin engellenmesi olarak tanımlanabilir (Hekim ve Başbüyük, 2013).
- **Bütünlük:** Bilginin yetkisi olmayan kişilerce silinmesi, değiştirmesi veya bilgiye hasar verilmesi eylemlerine karşın bilginin korunması olarak ifade edilebilir (Mehmet Tekerek, 2008).
- **Kullanılabilirlik:** Bilgiye ihtiyaç duyulduğunda ulaşılabilmesi durumudur. Bu durum bilgi sisteminde sorun olması halinde veya sisteme yönelik bir riskin olması durumunda dâhil bilgiye erişimin sağlanabilmesi olarak tanımlanabilir (Güngör, 2015).

Bilgi güvenliğini sağlanmasında güvenlik sistemlerinin yeterliği konusunun ardından bu sistemleri yöneten insan faktörünün yeterliği son derece önemli bir durumdur. Özellikle kurumsal bilgi güvenliği alanında büyük önem arz etmektedir (Canbek ve Sağıroğlu, 2007; Yılmaz, Yılmaz ve Sezer, 2014) Bu aşamada verilen eğitimlerin içeriği ve etkinliği önem kazanmaktadır.

2.1.3. Bilişim Güvenliği

Bilişim teknolojileri günümüzde her alanda hemen hemen her amaca yönelik kullanılan araçlardır. Bireysel veya kurumsal tüm bilgileri bilişim teknolojileri aracılığı ile internet ortamında tutulurken bilgilerimizin ne kadar güvende olduğu sorusu göz ardı edilemeyecek bir sorun olarak karşımıza çıkmaktadır.

İnternet teknolojisi ilk zamanlarında iletişim amaçlı kurulmuş bir sistemken kullanıcı sayısının artması internetin iletişimden ziyade bir paylaşım ortamı halini almasını sağladı. Zamanla ekonomik ve ticari amaçlı kullanımın artması, internetin her alanda kullanılabilir olmasının yanında milyarlarca varan kullanıcı kitlesi ile haksız kazanç başta olmak üzere sistemlere yetkisizi erişim, bilgi hırsızlığı, terör propagandası, illegal kumar siteleri, çocuk istismarı vb. sorunların yaygınlaşmasına sebep olmuştur (Öğün ve Kaya, 2013).

Gökmen (2014) yılında hazırlamış olduğu yüksek lisans tezinde Bilişim Güvenliğinin sağlanması konusunda önerileri şu şekilde sıralamaktadır:

- Taşınabilir bellekler her kullanışta virüs taramasından geçirilmelidir.
- Bütün şifrelerin harf, rakam ve simgelerden oluşan karmaşık bir şifre olmasına özen gösterilmelidir.
- Kullanılan şifrelerin unutulması durumunda sorulacak gizli soru ve cevapların kontrol edilerek kolay bulunabilecek cevaplar olmadığına dikkat edilmelidir.
- Kullanılan her hesap için şifreler farklı olmalıdır.
- E-postalara gelebilecek kimlik bilgilerinin doğrulama mesajlarına itibar edilmemeli ve güvenli olmayan e-postalar açılmadan silinmelidir.
- Kablosuz ağ (wireless) kullanıcıları son şifreleme metodu kullanmalı, şifresiz kablosuz ağ kullanımlardan kaçınmalı ve kablosuz ağ kullanılmadığı durumlarda ağ bağlantısı kapatılmalıdır.
- Sosyal paylaşım sitelerinde tüm adres, telefon, okul, sınıf, kimlik bilgileri paylaşılmamalı; bilgiler, fotoğraflar, videolar sadece arkadaşların görebileceği şekilde belirlenmeli; hatta bilgiler gizli tutulmalıdır.
- Bilgisayar başında olunmadığı durumlarda bilgisayar açık bırakılmamalı ve bilgisayarlara parola koyularak güvenlik sağlanmalıdır.
- Kullanılan web tarayıcısı sürekli güncellemeli, güvenlik ayarları yapılmalı ve internette gezinirken tarayıcının adres çubuğunda HTTPS:// yazıldığına dikkat edilmelidir.
- Lisanslı işletim sistemi kullanılmalı ve işletim sistemi sürekli güncellenmelidir.

- Başka bilgisayarlardan gelen verileri kontrol eden ve zararlı yazılımların girişini engelleyen güvenlik duvarı aktif edilmelidir.
- Dosya paylaşımları, uzak masaüstü bağlantısı ve otomatik çalıştır özelliği kapatılmalıdır.
- Web sitelerinde cazip gelen reklamlara tıklanmamalı, tanınmayan kişilerden gelen e-postalara açılmamalı ve görülen her program bilgisayara kurulmamalıdır.
- Web tarayıcısında özellikler sekmesi kullanılarak geçici internet dosyalar, tanımlama bilgileri, form bilgileri ve parolalar geçmişi belli aralıklarla silinmelidir.
- İnternet bankacılığını kullanırken veya internet üzerinden alışveriş yaparken şifre istenen formlarda ekran klavyesi kullanılmalıdır.
- Üye girişi yapılan herhangi bir siteden güvenli çıkış yapılmalıdır.
- Sıkıştırma programları yardımıyla önemli olan belgeler sıkıştırılmalı ve şifrelenmelidir.

Bilişim güvenliğini sağlayabilme konusunda okullarda bu eğitimi verecek olan öğretmenlerin ve öğretmen adaylarının yeterliliklerinin belirlenmesi konusunda yapılan çalışmalar dikkat çekmektedir.

2.1.4. Bilişim Suçları

Kelime anlamı olarak bakıldığında bilişim suçları kelimesi suçun ilk olarak faaliyet gösterdiği Amerikan doktrinde “computer crime” olarak geçmektedir. Aynı doktrinde bilişim suçları kelimesine karşılık gelen “crime against computer” (bilgisayara karşı işlenen suç), “computer-assisted crime” (bilgisayar yardımıyla işlenen suç), “computer-related crime” (bilgisayarla bağlantılı suç) terimleri de kullanılmaktadır. Ülkemizde ise bilişim suçları, sanal suçlar, bilgisayar suçları, siber suç, terimleri kullanılmaktadır (Türkiye Büyük Millet Meclisi, 2012).

Bilek, (2012) yaptığı çalışmada bilişim suçlarını “Genel olarak elektronik bilgi işlem kayıtlarına yasadışı yollarla erişilmesi veya bu kayıtların yasal olmayan şekilde silinmesi, değiştirilmesi veya bu tür kayıtlara girilmesi” olarak tanımlamıştır.

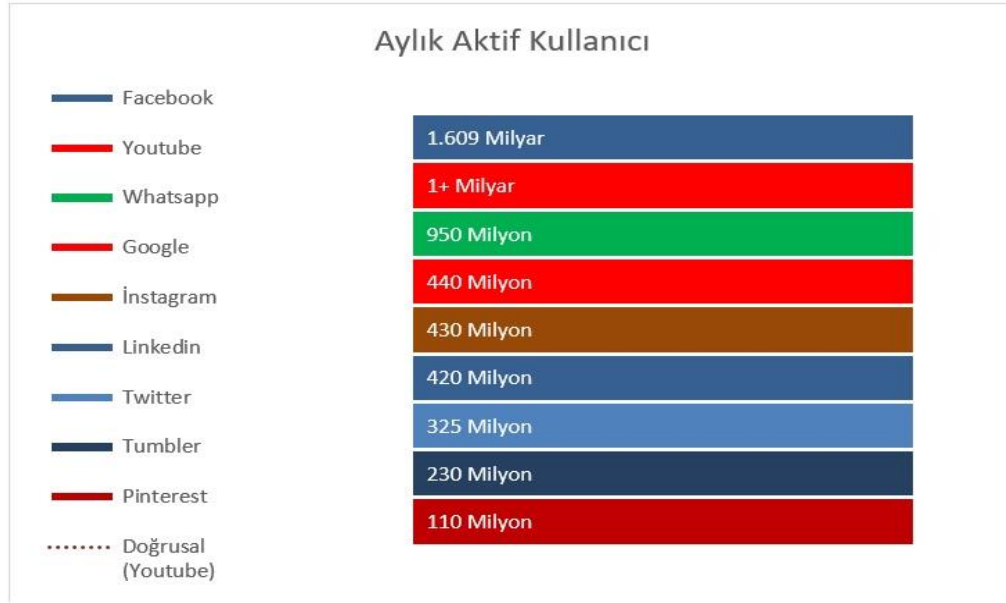
İnternetin küresel çapta kullanım alanının olması ceza kanunlarında yer alan klasik suçların işlenmesinde araç olarak kullanılabilmesinin yanında denetimde yetersizliğin getirisi olarak kendine özgü yeni suçların yaratılabildiği bir ortam olabilmektedir (Koç ve Kaynak, 2010).

Bilişim teknolojileri kullanım alanı her geçen gün genişlerken bilişim teknolojileri kullanımını tehdit eden unsurlar da her geçen gün artmaktadır. Bu artış ile ülkemizde ve dünyada bilişim suçlarının yaşanma sıklığında da artış yaşanmaktadır (Gökmen ve Akgün, 2016). İnternet ortamında gerçekleşen suçlarda en çok karşılaşılan suçların başında sistemlere zarar verme, dolandırıcılık, bilgi hırsızlığı ve pornografi gelmektedir (Yıldırım, 2014).

2.1.5. Sosyal Medya Güvenliği

Web 2.0 ile gelen ve internetin bu kadar hızlı yayılmasında en büyük etken sosyal medya araçları olarak gösterilebilir. Sosyal medya araçları kullanıcıların normal yaşamda olduğu gibi sosyal ortamlar oluşturmalarına imkân sağlamaktadır. Bu ortamlarda insanlar gruplar oluşturarak zaman ve mekân sınırlaması olmaksızın bilgi paylaşımında bulunabilmektedirler (Tanrıverdi ve Sağır, 2014).

Sosyal Medya araçlarının günümüzde bu kadar yaygınlaşması ve tüm kullanıcılara hitap etmesi kullanımını zorunlu hale getirmektedir (Çalı ve Altunbaş, 2012). Sosyal medya platformları, insanlara sunduğu mesajlaşma sistemleri, blog oluşturma ve yayınlama, web ortamlarının tasarlanabilmesi, sosyal ağ platformları ile profil oluşturma ve paylaşma vb. daha birçok olanak ile yaşam döngüsünde önemli yer edinmiştir (Oğuz, 2016). Günümüzde sosyal medya kullanım oranları dikkat çekici düzeylere ulaşmıştır. Şekil 2’de aylık olarak belirlenen aktif kullanıcı oranları verilmiştir.



Şekil 1. Sosyal Medya Kullanım Oranları (Kılıç, 2016)

Sağladığı imkânlar ile yetişkinlerin olduğu kadar gençlerin ve çocukların ilgisini çekmekte ve etkilemektedir (Demir, 2016). Sosyal medya içerdiği birçok risk unsuruna rağmen bilinçli kullanılması durumunda insan hayatını kolaylaştıran, gelişime katkı sağlayan bir yapı olarak gösterilebilir.

Tanrıverdi ve Sağır, (2014) yılında yapmış oldukları çalışmada sosyal medyanın bilinçli kullanılması halinde sağlayacağı faydaları “öğrenmeyi destekler, grup çalışmaları için uygun bir ortam oluşturur ve üst düzey düşünme becerisini geliştirir. Sosyal ağlar öğrencilerde iletişim becerilerini geliştirip paylaşımı ve sosyal aidiyeti kuvvetlendirirken, arkadaş desteğini de güçlendirir ve birlikte öğrenmeye katkı sağlar” şeklinde tanımlamışlardır. Sosyal medyanın faydalı şekilde kullanılabilmesi barındırdığı risklerden korunulabildiği sürece mümkün olacaktır. Erdoğan ve Bahtiyar (2014) sosyal medya kullanımını güvenli hale getirilmesi amacıyla bazı önerilerde bulunmuşlardır. Bunlar;

- Sosyal ağınıza dikkatlice seçin. Kullanmayı planladığınız siteyi değerlendirin ve gizlilik politikasını anladığınızdan da emin olun.

- Sosyal ağın insanların yayınladıkları içerikleri izleyip izlemediğini öğrenin. Bu web sitesine kişisel bilgiler vereceksiniz, bu nedenle kredi kartı bilgilerinizi gireceğiniz bir siteyi seçerken kullandığınız koşulların aynılarını kullanın.
- Çocukların gizlilik politikalarında belirtilen yaş sınırlarına uygun olarak bu ortamları kullanmaları aileleri tarafından sağlanmalıdır.
- Gizlilik ayarlarının son güncel hali kullanıldığından emin olunmalıdır.
- Bir anti-virüs programı kullanılmalıdır. Bu program zararlı yazılımlardan korunmada yararlı olacaktır.
- Özellikle resim paylaşımında iki kere düşünülmelidir. Ailenin veya yakınların görmesini istenmediği resimler sosyal ağlara yüklenmemelidir.
- Bir sosyal ağ ziyaret edildikten sonra tarayıcıların tuttuğu çerezler silinmelidir.
- Tatil planları, özellikle tarihleri sosyal ağ üzerinden paylaşılmamalıdır.
- Bilgisayar yazılımları özellikle de web sunucuları güncel tutulmalıdır.
- Bir yabancından bağlantı isteği alındığında en güvenli yöntem bu bağlantı isteğini reddetmektir.
- Sosyal ağ sitesinden ayrıldığında çıkış yapıldığından emin olunmalıdır.
- Hangi sebeple olursa olsun Spam maillere cevap verilmemeli, linklerine tıklanmamalıdır.
- Link tarayıcı kullanın. Link tarayıcı o linkin ait olduğu ilgili sitenin zararlı bir site olup olmadığını sıyanan web uygulamasıdır. ‘Urlvoid’, ‘Mywot’ bu bağlamda örnek sitelerdir.
- Kısaltılmış linkleri mutlaka kontrol edin. Bazı zararlı linkler kullanıcıya kısa bir link olarak gösterilir ve bu sayede zararlı link bir nevi gizlenmiş olur. Kullanıcı şüphelendiği kısa linkin yönlendirdiği gerçek linki mutlaka kontrol etmelidir. Gerçek linkleri kontrol eden siteler vardır. ‘Sucuri’ bu örneklerden bir tanesidir.

Sosyal ağlar kullanıcılar tarafından en çok kullanılan ortamlardır. Sosyalleşme amacı ile oldukça popüler kullanıma sahiptir. Arkadaş ve aile çevresi ile bağlantı kurmayı kolaylaştıran sosyal ağ ortamları sağladığı araçlar ile sanal sosyal yaşamın temeli olarak tanımlanabilir. Bir bilişim korsanı için bilgi edinme adresi sosyal ağ ortamları gösterilebilir.

Kullanıcıların paylaştıkları kişisel bilgiler bilişim korsanlarına başka hesaplara erişim için gerekli veriyi sağlayabilecek kaynak olabilmektedir (Wazid, Katal, Goudar ve Rao, 2013).

Sosyal paylaşım sitelerinin genelinde üyelik için 13 yaş sınırı bulunmaktadır. Karakuş ve diğerleri, (2014) yaptıkları çalışmada araştırmaya katılan çocuklarının üçte biri 13 yaşından küçük olmakla birlikte facebook, Twitter gibi sosyal paylaşım sitelerinde üyelikleri bulunduğunu ve %46'sının profillerinde kişisel bilgilerini “Herkes Açık” şekilde paylaştıkları bulgusuna ulaşmışlardır. Bu durum çocukların internet kullanımlarının denetlenmesi aşamasında eksiklikler olduğu şeklinde yorumlanabilir. Ebeveynlerin çocuklarının internet kullanımlarını denetlemesi çocuk istismarı olaylarının önüne geçilmesinde önem teşkil etmektedir.

2.1.6. Bilişim Güvenliğini Tehdit Eden Yazılım Temelli Unsurlar

İnternetin yaygın olarak kullanılması hayatımızda büyük kolaylıklar sağlamaktadır. Yaygın olarak kullanımı bilişim korsanlarının zarar verebilme potansiyellerini arttırmaktadır. İnternet üzerinde yer alan risklerden korunmada en önemli unsur her zaman bilinçli kullanıcı olmaktan geçmektedir. Bilişim güvenliği farkındalığına sahip olan bireyler aşağıda tanımlanmış olan unsurlara karşı önlem almada başarı sağlayabilirler.

2.1.6.1. Virüsler

Virüsler bilgisayarlara zarar verme amaçlı oluşturulmuş kod parçacıklarıdır. Genel olarak bilgisayar programlarına eklenen bu küçük kod parçaları kendi kendini çoğaltarak yayılma özelliğine sahiptir. Sistemi çalışmasını kısa süreliğine durdurmak gibi basit etkileri olduğu gibi önemli ölçülerde zarara yola açabilen virüsler de mevcuttur (Öğütçü, 2010).

Virüsler yeni bir problem değildir. Geçmişten günümüze önemli düzeyde gelişmeler sağlanmış ve geçmişte virüs tasarımları oldukça zahmetli önemli düzeyde programlama bilgisi isteyen bir işken bugün çok fazla programlama bilgisi gerekmeksizin isteğe göre virüsler hazırlanabilmektedir (DeFranco, 2011).

Bayzan, (2011) yılında yapmış olduğu çalışmada, bilgisayar virüslerini “bilgisayarın çalışmasını engelleyecek, verileri kaydedecek, bozacak veya silecek ya da kendilerini

internet üzerinde diğer bilgisayarlara yayarak yavaşlamalara veya başka sorunlara neden olacak şekilde tasarlanmış yazılımlar” şeklinde tanımlamıştır.

Günümüzde internet üzerinde dolanan çok fazla sayıda ve farklı etkilere sahip virüsler bulunmaktadır. Virüslerin yaygınlaşma sürecinin bilişim teknolojileri gelişim sürecine paralel olduğu söylenebilir. Virüslerin aktif olabilmesi için kullanıcıların etkileşimine ihtiyaç duyuyor olmaları önemli bir dikkat noktasıdır (Can ve Akbaş, 2014). İnsan gücüne ihtiyaç duyması virüsleri diğer zararlı yazılımlardan ayıran en önemli özelliktir (Can ve Akbaş, 2014; Ögütçü, 2010).

Bilgisayar virüsleri etkiledikleri fonksiyona göre çeşitlilik gösterebilmektedir. Boot Sektör Virüsü bilgisayarların ‘boot’ (Açılış) sekmesine bulaşan virüslerdir. Bilgisayar açılırken işletim sisteminin başlangıcında çalışmakta ve sisteme hasar vermektedir. Dosya virüsleri çalıştırılabilir dosyalara bulaşmaktadır. Böylelikle dosyalar her çalıştığında virüsler aktif hale getirilmektedir. Makro virüsleri Word, Excel, PowerPoint gibi ofis programları ile bulaşarak ofis belgelerine hasar veren virüslerdir (Gökmen, 2014).

2.1.6.2. Solucanlar (Worms)

Yapıları virüsleri andırsa da aralarındaki fark insan etkileşimidir. Virüsler aktif olabilmek için kullanıcının çalıştırması gerekmektedir. Fakat aynı durum solucanlar için gerekli değildir. Solucanlar sisteme girdikten sonra kendi kendine çoğalmaya başlarlar. Sistemde oluşacak yavaşlık ve kasma problemleri bu durumun ortaya çıkmasında en önemli etkidir (Öğün ve Kaya, 2013). Solucanlar sisteme sızması halinde çok hızlı yayılabilme özelliğine sahip programlardır. Bilgisayarlarda bulunan e-posta programları sayesinde çok daha hızlı yayılabilmektedir. Eposta programlarında yer alan kişi listesinde bulunan herkese birer eposta gönderilerek yayılma işlemi tamamlanmış olur (Can ve Akbaş, 2014; Gökmen, 2014; Öğün ve Kaya, 2013).

2.1.6.3. Truva Atı (Trojan)

Truva atları kullanıcıları ihtiyaç duyduğu yazılım veya güvenli bir dosya görüntüsü ile aldatarak bilgisayarlara sızmaktadır. Bu yazılımların özelliği aktif olması için insan

etkileşimine ihtiyaç duymamalarıdır. Truva atının genel amacı sistemlerin yetkisiz kişilerce uzaktan yönetilebilmesi amacı ile arka kapı açabilmesidir (Güngör, 2015). Truva atı bilgisayar sistemlerini yetkisiz kullanımlara açarak finansal veriler, kişisel bilgiler şifreler ve benzeri verilerin kopyalanmasına olanak sağlamaktadır (Kim, Jeong, Kim ve So, 2011).

Truva atı yöntemi bilgi hırsızlı, yetkisiz erişim, dolandırıcılık ve daha birçok suçun faaliyetinde en sık kullanılan yöntemdir. Truva atları kendilerini kopyalayabilme özelliğine sahip değildir (Can ve Akbaş, 2014). Bu özellik Truva atının işlevleri ve amacında gereklilik arz etmemektedir. Güvenlik önlemlerinin aşılarda saldırıana sisteme erişim yolu açmak Truva atının görevidir.

2.1.6.4. Casus Yazılımlar (Spyware)

Casus yazılımlar birçok işlevi bulunan yazılımlardır. Yayılma prensipleri de farklılık göstermektedir. Genel olarak internet de yer alan programların deneme sürümlerinin içine yerleşmekte veya yerleştirilmektedir. Kullanıcılar deneme sürümü programları yüklerken harici programlar kurulacağı kullanıcıya bildirilmektedir. Fakat bildiri yöntemleri itibari ile bazen seçenekler halinde kullanıcı tercihleri sorulurken bazense kullanıcı sözleşmelerinde yasal maddeler arsına sıkıştırılarak bildiri sunulduğundan dikkat çekmemektedir. Uzayan maddeler çok okunmadığından kolayca sisteme yerleşebilmektedirler (Öğün ve Kaya, 2013).

Casus yazılımların birçok etkisi bulunmaktadır. Kullanıcılara ait şifrelerin çalınması, bilgisayarların istem dışı yapılandırılması ve bazı programların engellenerek sisteme müdahale edilmesi, internet browser içerisine istem dışı eklentiler kurularak istem dışı sayfalara yönlendirme yapılması ve daha birçok etkiye sahiptir (Gökmen, 2014; Kim ve diğerleri, 2011; Öğün ve Kaya, 2013; Türkiye Büyük Millet Meclisi, 2012).

2.1.6.5. Fidyeye Yazılımları (Ransomware)

Fidyeye Yazılımları dijital şantaj veya dijital gasp yazılımları olarak da bilinirler. Bu tür virüsler zararlı kodları barındıran kötü amaçlı yazılımları kullanarak sistemlere bulaşırlar. Kurbanların dikkatini çekebilmek amacıyla ücretsiz yazılımlar, eposta ekleri, maddi kazanç

belirten reklamlar vb. araçlar kullanılmaktadır (Bhardwaj, Avasthi, Sastry ve Subrahmanyam, 2016).

FBI (Federal Bureau of Investigation) tarafından yapılan açıklamada fidye yazılımlarından dolayı oluşan maddi zararın tahmini olarak 1 Milyar doların üstünde olduğunu belirtmişlerdir. Fidye yazılımları şifreleme işlemini tamamladıkları anda kullanıcıya dijital ortamda kullanılmakta olan bitcoin veya türevi para birimleri üzerinden ödeme yapabilecekleri yönlendirici linkler ile uyarı mesajı yayınlar. Bitcoin kullanılmasının sebebi takip edilememesi olarak tanımlanabilir. Ödemeler genellikle iz sürme durumunu ortadan kaldırmak maksadı ile TOR (The Onion Routing) tarayıcı üzerinden yapılmaktadır (Hampton ve Baig, 2015).

Fidye Yazılımları (Ransomware) genelde iki türde bulunur. Bunlar Crypto Ransomware (Şifreleyici Fidye Yazılımları) ve Locker Ransomware (Kilitleyici Fidye Yazılımları) olarak ayrılmaktadır (Bhardwaj ve diğerleri, 2016).

2.1.6.5.1. Şifreleyici Fidye Yazılımları (Crypto Ransomware)

Genel amacı kullanıcıların kişisel verilerini şifreleyerek şantaj ile para gasp etmek olarak tanımlanabilmektedir. Şekil 2' de şifreleyici fidye yazılımına ait ekran görüntüsü yer almaktadır (Bhardwaj ve diğerleri, 2016). Fidye yazılımlarının popüler yayılma yöntemlerinden bir tane si e-postalar ile gönderilen elektronik faturalardır. Genelde kullanıcın dikkatini çekebilmek amacıyla fatura miktarları yüksek tutularak kullanıcın faturayı inceleme gereksinimini teşvik etmektedirler.



Şekil 2. Şifreleyici Fidyeye Yazılımı (Bhardwaj ve diğerleri, 2016)

2.1.6.5.2. Kilitleyici Fidyeye Yazılımları (Locker Ransomware)

Kilitleyici fidye yazılımlarının farkı dosyaları şifrelemek yerine sisteme erişimi sınırlandırmaktadır. Kullanıcıya sadece klavyenin numerik tuş takımını açık bırakarak (bunun sebebi ödeme aşamasında kullanıcının hesap numaralarını girebilmesidir) diğer tüm fonksiyonları kilitlemektedir. Aşağıda kilitleyici fidye yazılımına ait örnek bir görüntü verilmiştir (Bhardwaj ve diğerleri, 2016; Hampton ve Baig, 2015).



Şekil 3. Kilitleyici Fidyeye Yazılımı ("Locker Ransomware", 2016)

2.1.6.6. Tuş Kaydediciler (Keylogger)

Keylogger (Tuş Kaydedici)' ler kullanıcıların klavye üzerinde bastıkları tüm tuşları kaydeden ve yazılımı tasarlayan bilişim korsanına doküman olarak göndermektedir. Keylogger' in amacı kullanıcılara ait kullanıcı adı, şifre, hesap numaraları ve daha birçok bilginin ele geçirilmesini sağlamaktır (Öğün ve Kaya, 2013). Günümüzde ilkel yani sadece klavye de basılan tuşları kaydeden Keylogger yerine klavyeden girilen veriler, sistem kayıt dosyaları, sosyal medyada yapılan sohbet kayıtlarından bilgisayar ekran görüntülerine kadar her türlü bilgiyi sızdıran yazılımlar mevcuttur (Çıtak, 2016).

2.1.6.7. Reklam Yazılımları (Adware)

Bu yazılımlar özel olarak pazarlama ve reklam amaçlı üretilen özel bir casus yazılım (Spyware) türü olarak bilinmektedir. Reklam yazılımları kullanıcı bilgilerini elde edebilmek için çeşitli yöntemler kullanır. Örnek olarak, bir web sitesine girdiğinizde size eksik eklenti uyarısı verebilir ve bu eklentinin kurulumunu onaylamanızı talep edebilir. Kullanıcı “kabul ediyorum” seçeneğini tıkladığı an eklentinin bulunduğu web sitesi ile sizin girmiş olduğunuz web sitesi arasında gizlenen reklam yazılımı (adware) gerekli kullanıcı bilgilerini edinmektedir (Kim ve diğerleri, 2011).

2.1.6.8. Sosyal Mühendislik Saldırıları

Bilgi güvenliği alanında yer alan en önemli sorun olarak tanımlanabilir. Sosyal mühendislik saldırılarının önemi bilgi güvenliği alanında önemli bir unsur olan insan faktörünü hedef almasıdır (Can ve Akbaş, 2014). Kurumsal veri hırsızlığında çok kullanılan bir yöntem olan sosyal mühendislik saldırıları bilgi edinme aracı olarak insanların zayıf oldukları duygusal yapılarını kullanmaktadır (İnanç, yardım etme, vicdan vb.). Şirket çalışanı olarak davranma sohbet, bilgi edinme talebi, şifre kaybı gibi hileler ile saldırgan istediği bilgileri elde etmektedir. Sonuç olarak gerçekleştirilen saldırılar ile mağduriyetler yaratmaktadırlar (Can ve Akbaş, 2014; Vural ve Sağiroğlu, 2008).

Sosyal mühendislik saldırılarında önemli bir yöntem ise sosyal medya üzerinden gerçekleştirilmektedir. Bu tür olayların senaryosu gereği hedef olarak seçilen bireyler

hakkında bilgi sosyal medya platformları üzerinden toplanarak (bu işlemler açılan sahte hesaplar ile gerçekleştirilmektedir) şifrelerin ele geçirilmesi amacı ile özel olarak tasarlanmış internet sitelerine yönlendirilmekte sonuç olarak istenilen bilgiler elde edilmektedir (www.bthaber.com, 2016).

2.1.6.8.1. Oltalama (Pshing)

Oltalama saldırıları genelde kitle e-posta atakları ile başlamaktadır. Bu e-postalar hedef alınan okuyucuları içeriğinde barındırdığı linklere yönlendirir. Bu tür saldırılar genelde balık avına benzetilir. Balık avında olduğu gibi balıkçı oltayı atar ve yemi yutmasını bekler, kimlik avcıları ise birçok mail gönderir ve birçok okuyucunun bu e-postalarda bulunan linkleri ziyaret etmeleri beklenir. Genelde bu linkler şirket logosu taşıyan legal e-posta olarak görünür. Örnek olarak ünlü bir şirketin logosu olabilir. Okuyucu elektronik postanın içinde bulunan logo ve legal görüntünün cazibesine kapılır fakat link e tıkladığında olanlar beklediği gibi olmaz (Almomani, Gupta, Atawneh, Meulenberg ve Almomani, 2013).

Oltalama saldırıları genel olarak bilgisayar ve internet güvenliği bilinci zayıf olan bireyleri hedef alan saldırılardır. İnternet bankacılığı sistemlerini hedef alan bu tür saldırılar en çok 2006 yıllarında çok kullanılmıştır. Geçmişte olduğu kadar yoğun olmasa da günümüzde hala etkin bir saldırı yöntemi olarak kullanılabilir.

2.1.6.8.2. İstenmeyen E-Postalar (Spam)

Spam e-postalar kullanıcıların e-posta adreslerine gelen resim, metin, videolar vb. içeriklere sahip olan zararlı e-postalardır. Spam e-postalar işletmelerin e-posta sunucuları olduğu kadar, e-posta servisi sağlayıcılar (Gmail, yahoo, Hotmail vb.) için çok ciddi problem olabilmektedir (Li, Hsu, Wang, Chen ve Chen, 2014).

Kullanıcıların dikkatlerini çekebilmek amacı ile genelde ‘Tebrikler Kazandınız, Şu kadar para sizi bekliyor veya pornografik içerikler, sanal arkadaşlık istekleri vb.’ gibi mesajlar kullanılabildiği gibi e-posta ile gelen ve bu tür mesajları barındıran linklere

tıklamaktadırlar. Açılan sayfalarda kullanıcı kişisel bilgilerini girdiği an itibari ile e-posta adreslerine istenmeyen e-postalar gelmeye başlar (Gökmen, 2014; Li ve diğerleri, 2014).

2.1.7. İnternet de Yer alan İçerik Temeli Suçlar

2.1.7.1. Sanal Dolandırıcılık

Bilişim teknolojileri kullanılarak yapılan dolandırıcılığın diğer dolandırıcılıklarla ortak yanı suçu işleyen kişinin maddi kazanç sağlarken işlenen suçtan mağdur olan kişilerin ciddi zarara uğratılmasıdır. Burada fark suçun işleniş şekli ve kullanılan teknik ve yöntemler olarak açıklanabilir.

Bilişim Teknolojilerinin araç olarak kullanılması ile işlenen dolandırıcılık suçu; sistemlere izinsiz erişim, hedef alınan sistemdeki verilerin değiştirilerek sahte veriler girilmesi, verilere zarar verilmesi ve hedef sistemde bulunan verilerin silinerek imha edilmesi sonucunda maddi çıkar elde etme veya başkalarına haksız kazanç sağlamak amacı ile işlenen suçlardır (Bilek, 2012). Dolandırıcılık alanında en etkin yöntemlerden biri de sahte kredi kartı basımıdır. Kredi kartı basımında “Card Generator (Kart Üretim Programı)” isimli programları kullanmaktadırlar (Koç ve Kaynak, 2010).

Dolandırıcılar kullanıcılara “Bankamız hesap sahiplerinin güvenliği için kişisel bilgilerinizin güncellenmesi gerekmektedir” benzeri sahte mesajlar atarak kullanıcılara ait şifre, kimlik bilgisi gibi bilgileri talep edebilirler. Bu dolandırıcılıkta sık kullanılan bir metot olarak karşılaşılmaktadır (Kubovič, 2016).

Sanal dolandırıcılık yöntemlerinden bir diğeri ise sosyal ağ dolandırıcılığıdır. Bu yöntem sosyal ağ siteleri aracılığı ile e-posta adreslerine erişilmekte ve e-posta adresleri ile kişilere ait sosyal medya hesapları ele geçirilmektedir. Daha sonra arkadaş listelerinde bulunan kişilere sahte mesajlar göndererek maddi yardım talebinde bulunmaktadırlar

Erzurum Emniyet Müdürlüğü (2013) sanal dolandırıcılığa karşı alınması gereken önlemleri şu şekilde sıralamışlardır;

- Güvenliğinden emin olmadığımız sitelerden kesinlikle alışveriş yapılmamalıdır.

- Telefonla bankadan aradığını söyleyen her kişiye kişisel bilgiler verilmemelidir. Bu bilgiler başkalarına geçtikten sonra ciddi zarar verebilmektedir.
- Telefonunuza gelen her mesaja itibar etmeyin. Ciddi telefon ücretleriyle karşı karşıya kalılabilmektedir.
- Telefonla ürün satmak isteyen şirketlere itibar edilmemesi gerekmektedir. Gözle görülmeyen ürünler kapınıza geldiğinde hayal kırıklığına uğranmakta ve kredi kart bilgilerinin güvensiz ellere geçmesine sebep olmaktadır.
- İnternet bankacılığı işlemleri yapılan bilgisayarın kişisel bilgisayarımız olması ve zararlı yazılımlara karşı her zaman güncel Antivirüs programları kullanılması hesap bilgilerimizin hackerlerin eline geçmesini engelleyecektir.
- İnternet üzerinden araç veya emlak alımı yapılacaksa aracı veya emlağı görmeden telefondaki sese aldanarak şahsa para yatırılmamalıdır. İnternette çok sayıda sahte profilli dolandırıcı mevcuttur.
- Mesajla gelen şu telefon numarasını arayın hediye kazandınız şu tutarda para kazandınız şeklindeki mesajlara itibar etmeyin. Bu mesajlarla aranan telefon numaraları ya çok tutarlı telefon numaraları yahut kişisel bilgilerinizi ele geçirmeye çalışan dolandırıcılarla karşılaşacaksınız.
- ATM'den para çekme işlemlerinde kesinlikle kart giriş yuvası para çıkış haznesi ve herhangi bir kamera düzeneği olup olmadığı kontrol edilerek işlem gerçekleştirmektedir.
- Facebook, Twitter vb. sosyal ağlara üyelik yaparken kişisel bilgilerimizin kesinlikle yazılmaması gerekmektedir. Bu sitelere paylaşımda bulunulurken nerede olduğumuz ne yaptığımız ve evimizin resimlerini paylaşmamak gerekmektedir. Bu tür bilgiler ve paylaşımlar evimize gelecek hırsızlara davetiye çıkarmaktadır. Ayrıca bu tür sosyal paylaşım sitelerinde paylaşılan telefon numarası, doğum günü, çocuklarımızın ismi vb. bilgiler kimlik hırsızlığı açısından dolandırıcılar açısından son derece önemlidir.

2.1.7.2. Pornografi

İnternet ortamında kullanıcıları tehdit eden önemli sorunlardan bir tanesi ve önemli bir sorun pornografi 'dir. Burada hedef alınan kitlenin yetişkinlere oranla çocuklar olması bu suçun önemini açıkça öne çıkartmaktadır. Bu suçu işleyenler küçük yaşta çocukları kullanmaktan çekinmemektedirler. Diğer tarafta internet üzerinden kadın ticareti, pornografik video içerikli sitelerin oluşturulması ve internet ortamında yayılması vb. daha birçok alanda suç faaliyetlerini yürütmektedirler (Yıldırım, 2014).

İnternet birçok işlevin gerçekleşmesini kolaylaştıran bir yapıya sahip olması cinsel içerikli müstehcenlik içeren materyallerin üretimini ve dağıtımını kolaylaştırmakla birlikte maliyetini de azaltmaktadır. Teknolojinin sağladığı bu ortam zararlı internet içeriklerinden biri olan pornografik malzemelerin hazırlanması ve dağıtılmasında önemli bir role sahiptir (Bilek, 2012).

2.1.7.3. Çocuk İstismarı

İnternet kullanımının denetlenmesi en çok bu aşamada önem kazanmaktadır. Çocukların internet ortamında istenmeyen cinsel içerikli videolar, resimler vb. içeriklere maruz kalmaları olarak tanımlanabilir.

Çocuk İstismarına yönelik Türkiye ve Dünyada birçok çalışma yapılmış ve yapılmaya da devam etmektedir. Amerika Birleşik Devletleri (ABD)'nin 2002 yılında Pennsylvania eyaletinde İnternet ve Çocuk Pornografisi kanunu başsavcılık onayı ile kabul edilmiş ve yürürlüğe girmiştir. 2004 yılında bazı Avrupa Birliği ülkeleri tarafından internet üzerinde çevrimiçi çocuk istismarının önüne geçmek, yanlışlıkla erişimin engellenmesi amacı ile farklı ISS ile çalışmalar yapılmıştır. Kanada'da 2006 yılında 8 İnternet Servis Sağlayıcı (ISS) tarafından herhangi bir yasal zorunluluk olmaksızın tamamıyla gönüllülük esasına dayanarak çevrim içi ortamlarda çocuk istismarını önlemeye yönelik çalışmalar yapılmıştır (Bayzan ve Özbilen, 2012).

İnternet ortamında yer alan risklerden korunmada en önemli rol ebeveynlere düşmektedir. Çocukların internet ortamındaki faaliyetleri, paylaşımlarını denetleme görevi

öncelikli olarak ebeveynlerin görevi olmaktadır. Bunun gerçekleştirilebilmesi için ebeveynlerin bilinçli yaklaşım sergilemeleri oldukça önemli bir etken olarak karşımıza çıkmaktadır (Kalyon ve diğerleri, 2016). Gerekli ilgi ve denetimin sağlanmaması durumunda çocukların internet ortamında birçok tehlike ile karşılaşabilecekleri bir gerçektir. Bu tehlikelerin başında da çocuk istismarı gelmektedir.

Çocukların yasal olmayan içeriklere maruz kalmaları gelişim çağında sorunlara neden olabilmektedir. pedofili hastaları sosyal ağ ortamlarında çocuk yaş seviyesinde profil açarak çocuklara pornografik içerikli resim, video dosyaları göndermesi ve cinsel içerikli sohbetlere girmesi ve buluşmalar ayarlayarak fiziksel istismara yönelme gibi yöntemler çocukların internet ortamında Karşı karşıya oldukları tehlikelere sadece bir örnek olarak gösterilebilir (Kır, 2013). Çubukcu ve Bayzan (2013) yapmış oldukları çalışmada cinsel istismarın nedenini “internet ortamında kendini farklı kişilik ve yaş gruplarında gösteren yabancı kişilerle bilinçsiz bir şekilde sonucunu düşünmeden kurulan arkadaşlıklar” şeklinde tanımlamışlardır.

İnternet ortamı pedofili (sübyancı) hastalarının yaşlarını, fiziksel görünümelerini gizleyerek çocuklarla iletişime geçmelerine olanak sağlamaktadır. Daha ilginç olan bir durum ise pedofili hastalarının birbirleri ile iletişime geçerek aralarında bilgi paylaşımında bulundukları gerçeğidir (*Çocuk İstismarına Yönelik Rapor*, 2016).

Çocuk pornografisi çoğunlukla istismarının bir sonucu olarak karşımıza çıkmaktadır. İnternete sansür uygulama türleri ülkelere göre farklılık gösterse de başta Avrupa ülkeleri olmak üzere dünya ülkeleri çocuk pornografisine karşı ortak olarak sansür uygulamaktadır (Köse ve Özen, 2010).

2.1.7.4. Siber Zorbalık

BİT gelişimi yaşamı kolaylaştırmanın yanında bazı sorunları da beraberinde getirmektedir. Bu sorunlardan bir tanesi de klasik zorbalık eylemlerinin bilişim teknolojileri kullanılarak internet ortamında gerçekleşmeye başlaması ile gündeme gelen siber zorbalıktır. Bayram ve Sayılı (2013) çalışmasında siber zorbalığı “sanal ortamda modern iletişim

araçları kullanılarak başkalarına kasıtlı olarak hakaret edilmesi, aşağılanması, dışlanması, onların tehdit, teşhir ya da rahatsız edilmesi” olarak tanımlamıştır

Siber zorbalık girişimlerinin belirlenmesi amacıyla birçok çalışma yapılmıştır (Baştürk Akca, Sayımer ve Ergül, 2015; Cicioğlu, 2014; Eroğlu ve Güler, 2015; Peker, 2013). Siber zorbalık genel olarak tüm yaş gruplarını kapsayan genel bir sorun olmasının yanında özellikle üniversite öğrencilerinin genişleyen sosyal çevreleri ve sanal sosyal çevrelerinden dolayı siber zorbalığa daha çok maruz kalmaktadırlar (Söylemez ve Balaman, 2015).

Siber zorbalık davranışı küfür, hakaret, içerikli mesajlar, cinsel içerikli resim, video veya mesajlar olabildiği gibi başkalarına ait kişisel bilgi, fotoğraf veya videoların izinsiz paylaşımı, şantaj ve benzeri hareketler olarak tanımlanabilmektedir (Cicioğlu, 2014). Siber zorbalık konusunda birçok araştırma yapılmıştır. Eroğlu ve diğerleri (2016)’nın yaptıkları araştırmada siber zorbalık konusunda cinsiyet konusunda fark olduğu bulgusuna ulaşmışlardır (Eroğlu, Aktepe, Akbaba, Işık ve Özkorumak, 2015).

2.1.8. Bilişim Korsanları (Hacker)

Günümüzde hacker denildiğinde akla gelen bilişim teknolojilerini zarar vermek amacı ile kullanan, bilişim dünyasının tehlikeli insanlarıdır (Yegen, 2014). Türkçede “bilişim korsanı” olarak ifade edilen hackerler bilgisayar, ağ sistemleri ve yazılım kodlama konusunda ileri seviyede kullanıcılardır (S. Çakır ve Kesler, 2012). Hackerler bilişim dünyasının üst düzey yeteneklere sahip oyuncularını tanımlanabilirler. Çok eski bir terim olarak bilinmemesine rağmen hackerlerin kökeni ilk bilgisayarlara kadar dayanır. Hackerler faaliyetlerine göre kendi içlerinde türleri bulunmaktadır (Uçkan, 2012).

2.1.8.1. Beyaz Şapkalı Hacker

Beyaz Şapkalı Hacker genelde güvenlik uzmanı, güvenlik danışmanı olarak çalışan sistemlere yönelik saldırıları veya olası siber tehdit durumlarını raporlayarak bildiren legal çalışanlardır (Yegen, 2014).

2.1.8.2. Siyah Şapkalı Hacker

Hackerler arasında en tehlikelisi olarak tanımlanabilir. Amaçları sistemlere izinsiz erişim sağlayarak veri hasarına neden olmanın yanında veri hırsızlığı olabildiği gibi sistem işlevini engelleme veya sisteme zarar verme gibi faaliyetleri bulunan hacker türüdür (Kara, 2013).

2.1.8.3. Gri Şapkalı Hacker

Hacker türleri arasında farklı bir tür olarak yer alırlar. Legal veya illegal çalışacakları çıkarları doğrultusunda belirlenen hacker türüdür. Yasal sınırlarda çalışan gerekli gördüklerinde bu yasal sınırları tanımayan tehlikeli sayılabilecek hackerlerdir (Kara, 2013; A. F. Kılıç, 2014).

2.1.8.4. Lamer

Hackerlere özenen sempatizan olarak tanımlayabileceğimiz hacker türüdür. Tehlikeli olmalarının sebebi ne yaptıklarına dair bir fikirleri olamayan kararsız çalışan hackerler olmasıdır (A. F. Kılıç, 2014; Yegen, 2014).

2.2. İLGİLİ ARAŞTIRMALAR

İnternet teknolojisinin güvenli kullanımına yönelik yapılan araştırmalar, uygulamaların geliştirilmesi aşamasında kullanılabilecek önemli veri toplama araçları olarak kabul edilebilir. Bu bölümde internetin güvenli kullanımına yönelik geçmişten günümüze yapılan çalışmalar ve sonuçlarına değinilmiştir.

2.2.1. *Bilişim Teknolojileri Kullanımına Yönelik Öz-Yeterlik Algısı*

Bilişim Teknolojileri kullanımında önemli bir unsur olan öz yeterlik konusunda birçok araştırma yapılmıştır. Öz yeterlilik konusu bireylerin bir işi başarabilme, üstesinden gelebilmeye yönelik kendilerine olan inançları olarak tanımlanmaktadır. Bilişim teknolojileri kullanımına yönelik öz yeterlik algıları ile ilgili araştırmalara bakıldığında,

Seferoğlu ve Akbıyık (2005) ilköğretim öğretmenlerinin bilgisayar öz-yeterlik algılarını ölçmek amacıyla bir çalışma yapmışlardır. Çalışma sonucunda araştırmaya katılan 51 ilköğretim öğretmenin bilgisayarla yönelik öz yeterlilik algılarının orta düzeyde olduğunu orta düzeyde olduğu tespit etmişlerdir. Ayrıca bilgisayar kullanımını çalıştıkları kurumlarda düzenlenen kurslarda öğrenen öğretmenlerin %46'sının öz yeterlilik algılarının düşük düzeyde olduğu belirlenmiştir. Bilgisayar kullanımını öğrencilik dönemlerinde öğrenen (%28) ve deneme yanılma yöntemi ile öğrenen (%20) öğretmenlerin öz yeterlilik algıları ise yüksek seviyede olduğu tespit edilmiştir.

Gürcan, (2005) Üniversitelerde öğrenim gören 500 öğrenci ile yaptığı bilgisayar öz yeterlik algısı ve öğrenme stratejileri konulu çalışmasında öğrenme stratejileri ile bilgisayar öz yeterlik algısı arasında anlamlı bir bağ tespit etmişlerdir. Araştırma sonucunda öğrenme stratejilerini üst düzeyde kullanabilen öğrencilerde bilgisayar öz yeterliliğinin yerleşik ve yüksek olabileceğini belirtmiştir.

Kahraman, Yılmaz, Erkol ve Altun-Yalçın (2013) eğitim fakültelerinde öğrenim görmekte olan 294 öğretmen adayı ile gerçekleştirdikleri araştırma sonucunda öğretmen adaylarının eğitsel internet kullanımına yönelik yaptıkları çalışmada bilgisayar kullanım deneyimleri ile öz-yeterlik algıları arasında önemli oranda farklılık tespit edilmiştir.

Araştırmada Bir yıldan beri aktif olarak bilgisayar kullanan öğretmen adaylarının öz yeterlik ortalaması 65,1 olarak belirlenmiştir. İki yıllık bilgisayar kullanım geçmişi olan öğretmen adaylarının puan ortalamaları 84,1 olarak belirlenmiştir. Üç yıllık tecrübesi olan öğretmen adaylarının puan ortalamaları 96,1 iken bilgisayar konusunda dört yıl ve üzeri deneyime sahip öğretmen adaylarının öz yeterlik skor ortalamaları 103,4 olarak tespit edilmiştir. Bilgisayar kullanımına yönelik deneyimleri ile eğitsel internet kullanım öz-yeterlikleri arasında anlamlı bir ilişki olduğu sonucuna ulaşmışlardır. Öğretmen adaylarının bilgisayar kullanımına yönelik deneyimleri arttıkça eğitsel internet kullanımına yönelik öz-yeterlik inanç düzeylerinin arttığını saptamışlardır.

Yalnız, (2014) üniversite öğrencilerinin akademik öz-yeterlikleri ile olumlu ve olumsuz duygulanım arasındaki ilişkiyi incelemek amacı ile 286 üniversite öğrencisi ile çalışma yapılmıştır. Çalışma sonucunda akademik öz-yeterlik ile olumlu duygulanım arasında olumlu yönde bir ilişki tespit edilirken, olumsuz duygulanım arasında negatif yönde bir ilişki saptanmıştır. Öğrencilerin olumlu duygulanımlarının yüksek olması akademik öz-yeterliklerini olumlu yönde etkilerken, olumsuz duygulanımlarının ise akademik öz-yeterliklerini olumsuz yönde etkilediği saptanmıştır.

2.2.2. Güvenli İnternet Kullanımına Yönelik Araştırmalar

İnternetin güvenli kullanımına yönelik yapılan çalışmaların genel önceliği, çocuk ve gençlerin internetin zararlı yönünden korunmasını sağlamak olduğu görülmektedir.

ABD’de çeşitli dönemlerde çeşitli düzenlemeler yapılmıştır. Bunlara örnek olarak, 1998 yılında yürürlüğe giren Çocukların Online Mahremiyetinin Korunması Yasası (Children’s s Online Privacy Protection Act) ile internet ortamında çocuklardan bilgi toplama olanaklarını sınırlandırırken, riskli içerik barındıran web sitelerinin işaretlenmesini gerekli kılmaktadır (Valcke, De Wever, Van Keer ve Schellens, 2011). 2000 yılına gelindiğinde Çocukların İnternette korunması Yasası (Children’s İnternet Protection Act) ile okullar ve kütüphanelerde çocukların çevrim içi ortamda yer alan tehlikeli içeriklerden korunmasını sağlamak amacıyla yapılmış bir diğer çalışmadır (Yetim, 2015).

Türkiye’de 2007 yılında kabul edilen 5651 sayılı “İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun” Başta çocukların çevrimiçi ortamlarda tehlikeli içeriklerden korunmasını amaçlarken, bilişim yoluyla işlenen suçların önüne geçmeyi de amaçlamaktadır (Köse ve Özen, 2010).

Demirel, Yörük ve Özkan (2012) yaptıkları çocuklar ve gençlere yönelik verilen güvenli internet hizmeti ve ebeveyn görüşlerini değerlendirmeye yönelik çalışmada tek başına devletin yürüttüğü güvenli internet hizmetinin yeterli olmadığını bunun sebebinin de bu hizmete yönelik ebeveynlerin, gençlerin ve çocukların yeterli bilgiye sahip olmadıkları belirtilmektedir. Bu nedenle önemli önceliğin çocukların, gençlerin ve ebeveynlerin konuya yönelik bilinçlendirilmelerinin gerekliliği olarak belirtilmiştir. Araştırmada elde edilen bulgular bu durumu açıkça göstermektedir. Araştırmaya katılan ebeveynlerin Güvenli internet hizmetinden haberdar olama durumlarına bakıldığında katılımcıların %68,4’ü uygulamadan haberdar olduğunu belirtirken %31,6’sı ise haberdar olmadığını belirtmişlerdir. Buna rağmen uygulamanın kullanım durumuna bakıldığında tam tersi bir durum karşımıza çıkmaktadır. Evde güvenli internet filtresi kullanan ebeveynlerin oranı %36,9 iken kullanmayanların oranı %63,1 olarak tespit edilmiştir.

Carvalho (2013) yaptığı araştırmada çocuklara yöneltilen “En az bir kez bilgi güvenliği saldırısı kurbanı oldun mu?” sorusuna 640 çocuktan %8’i “Evet” derken %40’ı ise “Hayır” cevabı verirken %52’si “Bilmiyorum” cevabını vermiştir. Aynı araştırmada çocuklara yöneltilen “Hiç bilgi güvenliği ile ilgili eğitim aldınız veya daha önce duydunuz mu?” sorusuna çocukların %96,5’i “Hayır” cevabını vermişlerdir.

Tekerek ve Tekerek (2013) ilköğretim ve lise düzeyinde öğrenim gören 2449 öğrenci ile yaptıkları çalışmada öğrencilere araştırmacılar tarafından geliştirilmiş olan bilgi güvenliği farkındalık ölçeği uygulanmıştır. Araştırma sonuçları incelendiğinde öğrenciler güvenli şifre kullanımı, çevrimiçi güvenli iletişim, kötücül yazılım denetlemesi yapma, belge koruma, kişisel bilgisayar güvenliği güvenlik duvarı ve filtreleme yazılımlarının kullanımı konularında farkındalıklarının düşük olduğu belirlenmiştir. Bu durum

araştırmacılara göre bilgi ve bilgisayar güvenliği konusunda farkındalık yaratmaya yönelik eğitimlerin yetersizliğinden kaynaklanan bir durum olarak ortaya çıkmaktadır.

Karakuş ve diğerleri (2014) yaptıkları çalışmada Türkiye ve Avrupa'daki çocukların internet kullanım alışkanlıkları ve güvenli internet kullanımlarına değinmişlerdir. Çalışma sonucunda çocukların internet kullanımı konusunda kendilerine güvendiklerini ancak internet kullanımına yönelik beceriler konusunda yetersiz kaldıkları bulgusuna ulaşmışlardır. Bu durum çocukların internet ortamında karşılaşılabilecekleri olumsuzlukların üstesinden gelme eğilimlerine ciddi derecede etki etmektedir.

Erçağ (2014) öğretmenlere yönelik yapmış olduğu çalışmada öğretmenlerin eğitim öncesinde uygulanan ön test sonucunda güvenli internet kullanımına yönelik öz-yeterlik ve algı düzeylerinin yeterli olduğu sonucuna varmıştır. Otantik öğrenme yöntemi ile yapılan eğitimler sonucunda öğretmenlerin güvenli internet kullanımına yönelik öz-yeterlik ve algı düzeylerinde belirgin bir artış sağlandığı elde edilen önemli bir bulgudur.

Beder ve Ergun (2015) ortaokul öğrencilerinin güvenli internet kullanım durumlarını belirlemek amacıyla bir çalışma yapmışlardır. 503 ortaokul öğrencisi ile yapılan araştırmada 8. Sınıf öğrencilerinin bilinç düzeylerinin 6. Sınıf öğrencilerine göre daha düşük çıkmış olması önemli bir bilgi olarak belirtilmiştir. Çocukların “Yazılımsal Tehdit” unsurlarına yönelik soruları cevaplamada kararsızlık ifade etmeleri çocukların güvenli internet kullanımı konusunda riskleri arttırmaktadır. Çalışmada ayrıca “Telif Hakları ihlali” ve “Sorun Olabilecek Paylaşımlar” konularında bilinç düzeyleri düşük olarak belirlenmiştir.

2.2.3. Güvenli İnternet Kullanımında Ebeveyn Denetimine Yönelik Araştırmalar

Mitchell, Finkelhor ve Wolak (2005) 1.049 kişi ile yaptıkları çalışmada özellikle 10-15 yaş arası çocuk sahibi olan ailelerin %36.9'u internet filtresi kullandıkları 16-17 yaş arası çocuk sahibi olan ailelerin ise %22.8'i internet filtresi ve engelleme programları kullandıkları tespit edilmiştir. Ailelerin %84'ü çocuklarının internet ortamında karşılaşılabilecekleri cinsel içerikli materyallerden korunmalarını sağlamayı amaçlamaktadırlar.

Canbek ve Sağıroğlu (2007) yapmış oldukları çalışma ile internet kullanımında karşılaşılabilecek tehditler ve alınması gerek önlemler konusunda öneriler sunmuşlardır. Çocukların internet riskleri konusunda bilinçlendirilmesi aşamasında ebeveyn denetiminin yetersizliğine dikkat çekilirken ebeveynlerin internet kullanımına uzak olmaları bu duruma sebep olarak gösterilmektedir. Ebeveynlerin bilinçlendirilmesinin yanında çocuk ve gençlerin kullanıcıların internet ortamında yer alan risk unsurlarına yönelik müfredatta düzenlemeler yapılarak bilinçlendirilmesinin sağlanabileceği belirtilmektedir.

Demirel ve diğerleri (2012) yaptıkları çalışmada katılan ebeveynlerin %38.5'i bilgisayar ve internet kullanımını çocuklarının eğitiminde olumsuz bir etken olarak görürken, %75.3'ü internetin çocukları için güvensiz bir ortam olarak görmektedir. Araştırmacıların elde ettiği bir diğer bulgu ise katılımcıların %68.4'ünün Türkiye'de hizmet veren Bilgi Teknolojileri ve İletişim kurumu (BTK)' nun kullanıcılarına sunduğu güvenli internet hizmetinden haberdar olduklarını ancak %36.9'unun bu hizmeti kullandığını belirlemişlerdir.

İnternetin güvenli kullanılmasında kullanıcıların çevresindeki bütün faktörlere görevler düşmektedir. Aile, Okul, Arkadaş her bir faktörün görevi internet kullanımında kullanıcının karşılaşılabileceği zararların önüne geçmektir. İnternetin güvenli kullanımına yönelik yapılan araştırmalarda özellikle ebeveyn denetiminin önemli bir unsur olduğu sıkça karşılaşılan bir bulgu olarak karşımıza çıkmaktadır. İnternet kullanımında ebeveyn denetiminde karşılaşılan sorun bilinçsiz ebeveynlerin evde internet kullanımını etkin şekilde denetleyebildikleri yanılgısına düşmeleridir (Akbulut, 2013).

Karakuş ve diğerleri (2014) yaptıkları çalışmada Türkiye'de 1018 ebeveyn ve çocuğa ulaşmışlardır. Çalışmada ebeveynlerin %9'unun çocukların cinsel içerikli mesaj aldığını ve %2'sinin benzeri mesajlar gönderdiklerini belirtmişlerdir. Aynı araştırmada çocukların %12'si cinsel içerikli mesaj aldıklarını ve %3'ü mesaj gönderdiklerini belirtmişlerdir. Araştırmaya katılan çocukların %85,6'sı ise soruları yanıtlamamışlardır. Araştırmacılar bu durumun geleneksel ve kültürel yapının çocuklar üzerinde oluşturduğu etkiye bağlamışlardır. Ebeveynler arasında önemli bir oran çocuklarının karşılaştıkları riskler konusunda habersiz oldukları elde edilen önemli bir bulgudur.

Güvenli internet kullanımı konusunda ebeveyn görüşlerine yönelik bir diğer araştırma Kırık (2014) yaptığı nitel araştırmada elde edilen sonuçlar incelendiğinde, araştırmaya katılan ailelere yöneltilen “Çocuğunuz internet başındayken hangi hareket / davranışlarda bulunuyorsunuz?” sorusuna %48 oranında bir kısım çocukları internet başındayken kendiışleri ile ilgilendiklerini belirtmiştir. Ailelerin denetimi internetin zararlarından çocukların korunmasında önemli bir etkindir.

2.2.4. Siber Zorbalık Konusunda Yapılan Araştırmalar

Siber zorbalık, internetin güvenli kullanımı konusunda gündeme gelen bir diğer önemli sorun olarak karşımıza çıkmaktadır. Siber zorbalık konusunda yapılan araştırmalar incelendiğinde çocuk, genç, yetişkin her düzeyde internet kullanıcısına yönelik bir sorun olduğu görölmektedir.

Agatston, Kowalski ve Limber (2007) yaptıkları çalışmada öğrencilerin anlık mesajlaşma yöntemi ile okul saatlerinde siber zorbalık yapıldığını fakat okullarda mobil cihaz kullanımının yasak olmasından dolayı çok fazla gerçekleşmediğini belirtmişlerdir. Siber zorba davranışlara okul saatleri dışında kalan süreçte daha fazla yaşandığı öğrencilerden edinilen bir diğer bilgi olarak dikkat çekmektedir. Dikkat çeken bir diğer unsur ise araştırmaya katılan lise öğrencilerinin büyük çoğunluğu ve ortaokul seviyesindeki bazı öğrencilerin okullarda sosyal ağlara yönelik uygulanan filtrelerin aşılmasına yönelik bilgi sahibi olduklarını belirtmeleri olmuştur.

Arslan, Savaser, Hallett ve Balci (2012) yaptıkları çalışmadır. 2. 3. ve 4. Sınıf olmak üzere toplamda 372 öğrenci ile yapılan çalışmada katılımcıların %27’ si siber zorbalık mağduru, %18’i saldırgan ve %15’i ise saldırgan/mağdur durumunda oldukları tespit edilmiştir. Araştırmada erkeklerin kızlara göre daha fazla siber zorbalık yaptıkları tespit edilmiştir.

Yenilmez ve Seferoğlu (2013) öğretmenlerin internet kullanım süreleri ile sanal zorbalık konusunda bilgi sahibi olma durumları arasındaki ilişkiye dikkat çekmektedirler. Katılımcılara yöneltilen “Sanal zorbalık yalnızca yetişkinler tarafından yapılır” düşüncesine interneti ayda bir kullanan öğretmenlerin %45’i katıldıklarını bildirirken, %54,5’i bu

düşünceye katılmadıklarını bildirmişlerdir. İnterneti her gün kullanan öğretmenlerin %9,9'u bu düşünceye katıldıklarını bildirirken %75,6'sı bu düşünceye katılmadıklarını bildirmişlerdir. Bu durum interneti sürekli kullanan öğretmenlerin sanal zorbalık konusunda daha bilinçli olduklarını göstermektedir.

Baştürk Akca ve diğerleri (2015) yaptıkları çalışmada ortaokul öğrencilerinin siber zorbalık deneyimlerini değerlendirmişlerdir. Sonuçlar incelendiğinde araştırmaya katılan öğrencilerin %9,5'lik kısmı siber mağdur, %7'si siber zorba ve %7,5'nin ise siber mağdur/zorba olduğu bulgusuna ulaşmışlardır. Burada önemli nokta %7,5'lik zorba/mağdur bulgusudur. Her iki durum yani hem mağdur hem zorba durumunda olan gençlerdir. Bununun anlamı mağdur olan gençlerin karşılık verme, misilleme yapmak amacı ile siber zorbalık yaptığıdır.

Eroğlu ve diğerleri (2015) 160 kişi ile yaptıkları çalışmada katılımcıların %6,9'u siber zorba, %8,7'si siber mağdur olarak tespit edilmiştir. Cinsiyet faktörüne yönelik bulgular dikkat çekmektedir. Siber zorba durumunda olan katılımcıların %63,9'u Bayan, %36,4'ü erkektir. Siber mağdur durumunda olan katılımcıların %71,4'ü bayan, %28,6'sı ise erkektir. Her iki durumda da cinsiyet farkı önemli bir bulgudur. Siber zorba/mağdur durumunda olan katılımcıların oranı ise %67,5 olarak tespit edilmiştir. Her iki durumda olan katılımcıların %42,6'sı bayan, %57,4'ü ise erkektir. Araştırmada elde edilen sonuçlara göre mağduriyetinden dolayı misilleme yapanların oranları oldukça dikkat edilmesi gereken bir durumdur.

2.2.5. İnternet ve Sosyal Medya Bağımlılığına Yönelik Araştırmalar

İnternet ve sosyal medya bağımlılığı, bilişim teknolojilerinin kontrolsüz ve bilinçsiz kullanımı sonucunda karşılaşılabilecek risk unsurlarından bir tanesi olarak ifade edilebilir. İnternet bağımlılığının tanımlanmasında en büyük etken olarak internet başında aşırı zaman geçirilmesi gösterilebilir (Günüç ve Kayrı, 2010). İnternet ve sosyal medya bağımlılığına ilişkin yapılan araştırmalar durumun ciddiyetini öne sürmektedir.

Gökçearslan ve Günbatır (2012) lise öğrencilerinin internet bağımlılık düzeylerini belirlemeye yönelik yaptıkları çalışma sonucunda araştırmaya katılan öğrencilerin %2,33' ü

internet bağımlısı, %17,45' i bağımlılık eşiğinde bulunan yani risk altında oldukları tespit edilmiştir. Araştırmada internet ve sosyal ağ kullanımı kullanım süresinin anlamlı düzeyde etkisinin olduğu belirtilmiştir.

Yılmaz ve diğerleri (2014) 2853 lise öğrencisi ile internet bağımlılık düzeylerini belirlemeye yönelik yapmış olduğu çalışmada katılımcıların büyük çoğunluğunun orta düzeyde bağımlı olduklarını, %16'sının ise yüksek düzeyde bağımlı olduklarını belirlemişlerdir. Araştırmaya katılan erkek öğrencilerin kız öğrencilere göre daha yüksek düzeyde bağımlı oldukları ise elde edilen diğer bir önemli bulgudur.

Kır ve Sulak (2014) eğitim fakültesinde öğrenim gören 337 öğrenci ile yaptıkları çalışma sonucunda %10,1 bağımlılığın eşiğinde yani risk grubunda olduğu, %1,2 oranında öğrencilerin ise internet bağımlısı olarak tespit edilmişlerdir.

Kırık (2014) internetin aile ve çocuk ilişkisinde yerini ölçmek amacıyla 0-6 yaş gurubunda çocuğu olan 50 aileyle yüz yüze görüşme yapmışlardır. Araştırmaya katılan ailelerin %28'i internetin bağımlılık yarattığı fikrini savunmuşlardır. Katılımcıların %18'i bireylere ve topluma zarar verdiğini savunmuşlardır.

BÖLÜM III

YÖNTEM

Bu bölümde, araştırma modeli, veri toplama aracı, verilerin toplanması ve toplanan verilen çözümlemesine yönelik bilgiler verilecektir.

3.1. Araştırma Modeli

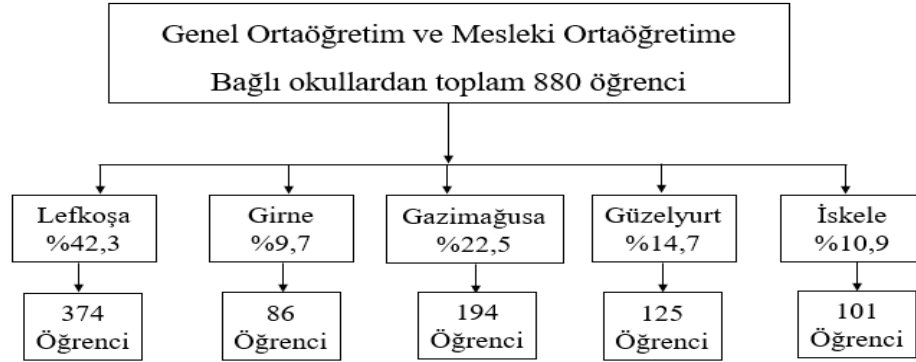
Bu araştırma, KKTC’de bulunan liselerde öğrenim görmekte olan öğrencilerin güvenli internet kullanımına yönelik öz-yeterlik algılarını değerlendirmeyi amaçlayan betimsel bir çalışmadır.

Bu çalışmada betimsel araştırma yöntemlerinden genel tarama modeli uygulanmıştır. Büyüköztürk (2012) genel tarama modelini “bir grubun belirli özelliklerini belirlemek için verilerin toplanmasını amaçlayan çalışmalar tarama (survey) araştırması” olarak tanımlamaktadır.

3.2. Evren Örneklem

Araştırma evrenini Kuzey Kıbrıs Türk Cumhuriyeti Millî Eğitim Bakanlığı Genel Ortaöğretim dairesi ve Mesleki Teknik Ortaöğretim dairelerine bağlı 30 lisede öğrenim görmekte olan 2568 öğrenci, örneklemi ise bu öğrencilerden seçkisiz tabakalı örneklem yöntemi ile seçilen 880 öğrenciler oluşturmaktadır. Öğrenciler 30 liseden rastgele gönüllülük esasına dayanarak seçilmiştir. Örneklem belirlenmesinde Büyüköztürk, Çakmak, Akgün ve Karadeniz (2008) örneklem hesaplamaları baz alınarak belirlenmiş ve anket uygulanmıştır.

Araştırma evrenini oluşturan okullardan Lefkoşa, Girne, Gazimağusa, Güzelyurt, Lefke, İskele ve karpaz olmak üzere bölgesel olarak ayrı ayrı tabakalar oluşturulmuştur. Oluşturulan tabakalara bağlı olarak anket uygulanacak öğrenci sayısı belirlenmiştir. Araştırma için belirlenen 880 öğrenciden 374 öğrenci (%42,3) Lefkoşa, 86 öğrenci (%9,7) Girne, 194 öğrenci (%22,5) Gazimağusa, 125 öğrenci (%14,7) Güzelyurt, 101 öğrenci (%10,9) İskele ilçelerinde öğrenim görmektedirler. Tablo 1’de tabakalara göre öğrenci sayıları verilmiştir.



Tablo 1. Katılımcıların tabakalara göre öğrenci dağılımı

Tabakalara ayrılan bölgelerde bulunan Ortaöğretim dairesine bağlı bulunan liselere “Öğrencilerin Güvenli İnternet Kullanımına Yönelik Öz-Yeterlikleri Algıları” konulu anket uygulanmıştır.

3.2.2. Öğrencilerin Liselere Göre Dağılımı

Araştırmaya katılan öğrencilerin öğrenim görmekte oldukları liselere göre dağılımları Tablo 2’de verilmiştir.

OKULLAR	N	%
20 Temmuz Fen Lisesi	33	3,7
Bülent Ecevit Anadolu Lisesi	33	3,7
Değirmenlik Lisesi	33	3,7
Lefkoşa Anadolu Güzel Sanatlar Lisesi	33	3,7
Lefkoşa Türk Lisesi	33	3,7
Türk Maarif Koleji	34	3,8
Sedat Semavi Endüstri Meslek Lisesi	35	4,0
Haydarpaşa Ticaret Lisesi	35	4,0
Atatürk Meslek Lisesi	35	4,0
Haspolat Meslek Lisesi	35	4,0
Hala Sultan İlahiyat Koleji	35	4,0
Lefkoşa	374	42,3
Cumhuriyet Lisesi	31	3,5
Gazimağusa Türk Maarif Koleji	31	3,5

Namık Kemal Lisesi	31	3,5
Polatpaşa Lisesi	31	3,5
Dr. Fazıl Küçük Endüstri Meslek Lisesi	23	2,8
Gazimağusa Ticaret Lisesi	23	2,8
Gazimağusa Meslek Lisesi	24	2,9
Gazimağusa	194	22,5
19 Mayıs Türk Maarif Koleji	29	3,3
Anafartalar Lisesi	29	3,3
Lapta Yavuzlar Lisesi	28	3,1
Girne	86	9,7
Güzelyurt Türk Maarif Koleji	22	2,6
Kurtuluş Lisesi	22	2,6
Lefke Gazi Lisesi	22	2,6
Cengiz Topel Endüstri Meslek Lisesi	30	3,5
Güzelyurt Meslek Lisesi	29	3,4
Güzelyurt	125	14,7
Bekirpaşa Lisesi	29	3,2
Erenköy Lisesi	29	3,2
Karpaz Meslek Lisesi	22	2,3
İskele Ticaret Lisesi	21	2,2
İskele	101	10,9

Tablo 2. KKTC’de Bulunan Liselerin Dağılımı

Tablo 2’de öğrencilerin KKTC’de Milli Eğitim ve Kültür Bakanlığı’na bağlı bulunan liselere göre dağılımı görülmektedir. Tablo 2 incelendiğinde en yoğun katılımın %4,0 (N=35) öğrenci sayısı ile Sedat Semavi Endüstri Meslek Lisesi, Haydarpaşa Ticaret Lisesi, Atatürk Meslek Lisesi, Haspolat Meslek Lisesi ve Hala Sultan İlahiyat Koleji olarak belirlenmiştir. Lefkoşa ilçesinde bulunan ve genel orta öğretim dairesine bağlı bulunan okullar ise %3,8 (N=33) ile en yoğun katılımlı liseler olarak görülmektedir

3.2.5. Araştırmaya Katılan Öğrencilerin Demografik Bilgileri

Bu bölümde, araştırmaya katılan öğrencilerin cinsiyetleri, yaşları, ilçelere göre dağılımına ilişkin frekans (f) ve yüzde (%) değerleri tablolar halinde verilmiştir.

		N	%
Bağlı Oldukları Ortaöğretim Dairelerine Göre Dağılımı	Genel Ortaöğretim Dairesi	531	60,3
	Mesleki Teknik Ortaöğretim Dairesi	349	39,7
	Toplam	880	100
Cinsiyete Göre Dağılım	Kız	516	58,6
	Erkek	364	41,4
	Toplam	880	100,0
Yaşlara Göre Dağılım	14-17	716	81,4
	18-20	164	18,6
	Toplam	880	100,0
Sınıf Düzeylerine Göre Dağılım	9. Sınıf	220	25,0
	10. Sınıf	219	24,9
	11. Sınıf	220	25,0
	12. Sınıf	221	25,1
	Toplam	880	100,0

Tablo 3. Öğrencilerin Demografik Bilgilerine Göre Dağılımı

Tablo 3'e bakıldığında araştırmaya katılan öğrencilerin %60,3 (N=531) Genel Ortaöğretime bağlıken %39,7 (N=349) Mesleki Teknik Ortaöğretime bağlı okullarda öğrenim görmektedir. Dağılıma bakıldığında genel ortaöğretime bağlı okulların katılımının ağırlıkta olduğu görülmektedir. Cinsiyete göre dağılıma bakıldığında araştırmaya katılan 880 öğrencinin %58,6 (N=516) kız, %41,4 (N=364)'ü erkek öğrencilerden oluşmaktadır. Araştırmaya katılan öğrencilerde kız öğrencilerin çoğunlukta olduğu görülmektedir. Yaş aralıklarına göre bakıldığında araştırmaya katılan öğrencilerin %81,4 (N=716) 14 ile 17 yaş Aralığında, %18,6 (N=164) ise 18 ile 20 yaş arasında oldukları tespit edilmiştir.

Sınıf Düzeylerine göre öğrencilerin sınıf düzeyi incelendiğinde öğrencilerin %25 (N=220) 9. Sınıf, %24,9'u (N=219) 10. Sınıf, %25'i (N=220) 11. Sınıf ve %25,1'i (N=221) 12. Sınıf da öğrenim görmektedirler.

3.2.3. Öğrencilerin İnternet Erişim Yerlerine Göre Dağılımı

Araştırmaya katılan öğrencilerin internete erişim sağladıkları ortamlara göre dağılımları Tablo 4' de verilmiştir.

Tablo 4. İnternet’e Erişim Ortamlarına Göre Dağılım

		N	%
Kişisel Bilgisayardan Erişenler	Evet	505	57,4
	Hayır	375	42,6
	Toplam	880	100
Okuldan Erişenler	Evet	86	9,8
	Hayır	794	90,2
	Toplam	880	100
İnternet Kafeden Erişenler	Evet	73	8,3
	Hayır	807	91,7
	Toplam	880	100
Cep Telefonu İle Erişenler	Evet	764	86,8
	Hayır	116	13,2
	Toplam	880	100

Tablo 4’de görüldüğü gibi araştırmaya katılan öğrencilerin %57,4’ü (N=505) internete kendi kişisel bilgisayarlarından erişim sağlamaktadır. %41,6’sı (N=375) ise internet erişimi için farklı ortamlardan yararlanmaktadır. İnternet erişiminde farklı ortamlardan yararlanma durumları incelendiğinde katılımcıların %9,8’inin internet erişimini okuldan sağlarken, %8,3’ ünün ise internet eriminde internet kafelerden yararlandıkları tespit edilmiştir. Araştırmada internet erişiminde en çok kullanılan aracın ise cep telefonları olduğu belirlenmiştir. Araştırmada internet erişimini cep telefonundan sağlayanların oranı %86,8 olarak tespit edilmiştir.

Karakuş ve diğerleri (2014) yaptıkları çalışmaya katılan öğrencilerin %60,1’inin internete okuldan erişim sağlarken, Katılımcıların %51,5’ inin ise internet erişimin internet kafelerden sağladıkları tespit edilmiştir.

3.2.4. Öğrencilerin Haftalık İnternet Kullanım Sürelerine Göre Dağılımı

Araştırmaya katılan öğrencilerin haftalık internet kullanım sürelerine göre dağılımları Tablo 5’de görülmektedir.

Tablo 5. İnternet kullanım sürelerine göre dağılım

	F	%
4 Saatten Az	136	15,5
4-12	251	28,5
13-27	174	19,8
28 Saatten Fazla	319	36,3
Toplam	880	100,0

Tablo 5’e bakıldığında araştırmaya katılan öğrencilerin %15,5’i haftada en fazla 4 saat internet kullandıklarını bildirirken %28,5’i 4 ile 12 saat arasında, %19,8’ i 13 ile 27 saat ve %36,1’i ise haftada 28 saatten fazla internet kullandıkları görülmektedir.

3.3. Veri Toplama Aracı

Araştırmada öğrencilere yönelik demografik bilgilerin toplanması amacı ile anketin ilk bölümünde kişisel bilgi formu eklenmiştir. İkinci bölümde güvenli internet kullanımına yönelik öz-yeterlik algılarını ölçmek amacı ile Çavuş ve Erçağ (2014) tarafından geliştirilen “Öğrencilerin Güvenli İnternet Kullanımına Yönelik Öz-Yeterlik Algıları Ölçeği” kullanılmıştır. Kullanılan ölçek 5’li likert tipinde olup; “Tamamen Yetersizim”, “Yetersizim”, “Orta Düzeyde Yeterliyim”, “Yeterliyim” ve “Tamamen Yeterliyim” şeklinde düzenlenmiştir. Anket “Tamamen Yetersizim” ‘den “Tamamen Yeterliyim” seçeneğine doğru 1’den 5’e doğru verilen sayısal değerler ile puanlandırılmıştır. Ölçek katılımcıların güvenli internet kullanımına yönelik öz-yeterliklerini “Sosyal Ağlarda Güvenlik (Sosyal Medya Güvenliği)”, “Zararlı Yazılımlar”, “Web Güvenliği ve Sosyal Mühendislik” ve “Bilgisayar Güvenliği” olmak üzere 4 alt boyutta değerlendirmektedir. Ölçekte sosyal ağlarda güvenlik konusuna ilişkin 12, zararlı yazılımlar konusuna ilişkin 8, web güvenliği ve sosyal mühendislik konusuna ilişkin 9 ve bilgisayar güvenliğine ilişkin 6 soru yer almaktadır. Yapılan analizler sonucunda cronbach alpha iç güvenirlik katsayısı 0.843 olarak hesaplanmıştır.

3.4. Verilerin Analizi

Anket uygulamaları sonucunda araştırmaya katılan 880 öğrenciden elde edilen bilgiler uzman denetiminde “Statistical Package For Social Science” (SPSS) 24 programı ile oluşturulan veri tabanına aktarılmış ve istatistiksel analizler yapılmıştır. Araştırma sonunda elde edilen verilerin çözümlenmesinde; frekans (f), yüzdelik (%), aritmetik ortalama ($\bar{X}$), standart sapma (SS), bağımsız değişkenler arasında farklılık olup olmadığını analiz etmek için Kruskal-Wallis testi (K-independent sample test) analiz teknikleri kullanılmış çıkan sonuçlar tablolar oluşturularak yorumlanmıştır.

Anket sonuçlarının çözümlenmesi aşamasında 5’ li derecelendirme sisteminde kullanılan sınırlar Tablo 6’de verilmiştir.

Tablo 6. Beşli Derecelendirmede Kullanılan Sınırlar

Ağırlıklar	Sınırlar	Öz-yeterlik Algıları
1	1.00- 1,79	Tamamen Yetersizim
2	1,80- 2,59	Yetersizim
3	2,60- 3,39	Orta Düzeyde Yeterliyim
4	3,40- 4,19	Yeterliyim
5	4,20- 5,00	Tamamen Yeterliyim

BÖLÜM IV

BULGULAR VE YORUMLAR

Bu bölümde, araştırma sonunda elde edilen veriler ile yapılan istatistik sonuçlarının yorumlanmasına yer verilmiştir.

4.2. Lise Öğrencilerinin Güvenli İnternet Kullanımına Yönelik Öz-yeterlik Algılarına İlişkin Bulgular

Lise öğrencilerinin internetin güvenli kullanımına yönelik öz-yeterlik algılarını gösteren anket sonuçları 4 boyut altında incelenecektir.

4.2.1. Sosyal Ağ (Sosyal Medya) Güvenliğine Yönelik Öz-Yeterlik Algıları

Araştırmada kullanılan “Lise Öğrencilerinin Güvenli İnternet Kullanımına Yönelik Öz-yeterlikleri” anketinin birinci boyu olan sosyal ağ (sosyal medya) güvenliği boyutunda yer alan ifadelerle ilişkin elde edilen verilerin Ortalama ($\bar{X}$) ve Standart Sapma (SS) verileri Tablo 7’de verilmiştir.

Tablo 7. Sosyal Ağ (Sosyal Medya) Güvenliği boyutuna İlişkin Ortalama Verileri

	($\bar{X}$)	SS
1. Sosyal paylaşım ağlarında paylaştığım bilgileri, istemediğim kişilerden gizleyebilme	4,47	0,92
2. Sosyal paylaşım ağlarında tanımadığım/istemediğim kişilerden gelen istekleri engelleyebilme	4,65	0,79
3. Sosyal paylaşım ağlarında kişisel bilgilerimi, istemediğim kişilerden gizleyebilme	4,49	0,89
4. Sosyal paylaşım ağlarında güvenlik tehlikesi açısından paylaştığım bilgileri koruyabilme	4,18	1,02
5. Sosyal paylaşım ağlarındaki şifremin çalınması durumunda gerekli başvuruları ilgili yerlere yapabilme	3,94	1,21
6. Sosyal paylaşım ağlarında video, fotoğraf gibi kişiliğime zarar vermeyecek bilgiyi paylaşabilme	4,37	1,98
7. Sosyal paylaşım ağlarında başkalarının kişiliğine zarar vermeyecek bilgiyi paylaşabilme	4,24	1,11

8. Facebook, Twitter gibi sosyal paylaşım ağlarını güvenli bir şekilde kullanabilme	4,49	0,89
9. Sosyal ağlarda paylaşılan virüslü videolardan korunabilme	3,97	1,19
10. Sosyal paylaşım ağlarında güvenlik açıklarına karşı tedbir alabilme	3,95	1,15
11. Sosyal paylaşım ağlarında fotoğraf albümlerimin çalınmasını engelleyebilme	3,64	1,29
12. Sosyal paylaşım ağlarında güçlü şifre oluşturabilme	4,31	1,07
Sosyal Ağlarda Güvenlik Genel Ortalama	4,22	0,69

Tablo 7'e bakıldığında **Sosyal Ağlarda (Sosyal Medyada) Güvenlik** boyutu altında yöneltilen sorulara verilen cevapların 4.00 ortalamasının üzerinde olduğu, derecelendirme sınırlarına göre Tamamen Yeterliyim seçeneğini öne çıkardıkları görülmektedir. Genç kullanıcıların sosyal ağlarda güvenliklerini sağlama yönünde yeterli bilince sahip olduklarını düşünceleri ve bu konuda kendilerine güvenmeleri yeterli öz-yeterliğe sahip olduklarını göstermektedir. Ancak 5. Madde 'de yöneltilen “*Sosyal paylaşım ağlarındaki şifrenin çalınması durumunda gerekli başvuruları ilgili yerlere yapabilme*” ($\bar{X}=3,93$, $SS=1.20$), 9. Madde “*Sosyal ağlarda paylaşılan virüslü videolardan korunabilme*” ($\bar{X}=3,96$, $SS=1.19$), 10. Madde “*Sosyal paylaşım ağlarında güvenlik açıklarına karşı tedbir alabilme*” ($\bar{X}=3,94$, $SS=1.14$) ve 11. Madde “*Sosyal paylaşım ağlarında fotoğraf albümlerimin çalınmasını engelleyebilme*” ($\bar{X}=3,63$, $SS=1.28$) konularında katılımcıların verdikleri cevapların ortalamalarının diğer maddelere göre daha düşük olduğu belirlenmiştir. Katılımcıların genel durumunun **Sosyal Ağlarda (Sosyal Medyada) Güvenlik** konusunda tamamen yeterli olduklarını gösterirken bazı katılımcıların bu konuda ikilemde oldukları dikkat çekmektedir.

Tablo 7' de son olarak “Sosyal Ağlarda Güvenlik” boyutunda öğrencilerin genel ortalamaları verilmiştir. Elde edilen veriler incelendiğinde araştırmaya katılan öğrencilerin “Sosyal Ağlarda Güvenlik” konusunda verdikleri yanıtlar $\bar{X}=4,2246$ (Tamamen Yeterliyim) sonucunu ortaya çıkarmaktadır.

Akgün ve Topal (2015) yaptıkları çalışmada katılımcıların %60'ından fazlasının sosyal ağ ortamlarında kişisel bilgilerin korunması konusunu önemsedikleri aynı zamanda bu amaçla gerekli düzenlemelerin yapılması ve gizlilik, güvenilirlik ayarlamalarının

yapılması konusunda kendilerini yeterli derecede duyarlı olarak gördüklerini tespit etmişlerdir.

4.2.2. Zararlı Yazılımlara Yönelik Öz-Yeterlik Algıları

Araştırmada kullanılan “Lise Öğrencilerinin Güvenli İnternet Kullanımına Yönelik Öz-yeterlikleri” anketinin ikinci boyutu olan zararlı yazılımlar boyutunda yer alan ifadelere ilişkin elde edilen verilerin Ortalama ($\bar{X}$) ve Standart Sapma (SS) verileri Tablo 14’de verilmiştir.

Tablo 8. Zararlı Yazılımlar Boyuna İlişkin Ortalama Verileri

Zararlı Yazılımlar	$\bar{X}$	SS
13. Zararlı yazılımların bilgisayara bulaşmasını engelleyebilme	3,62	1,22
14. Tuş Kaydedici (Keylogger) şifrelerimi koruyabilme	3,21	1,34
15. Zararlı yazılımlar bilgisayara bulaştığı zaman temizleyebilme	3,59	1,29
16. Virüslerin bilgisayara bulaşmaması için gereken güvenlik önlemlerini alabilme	3,76	1,22
17. Solucanlara (Worm) karşı korunabilme	3,24	1,32
18. Truva Atlarının (Trojan) bilgisayara bulaşmaması için gereken güvenlik önlemlerini alabilme	3,15	1,35
19. Casus Yazılımlara (Spyware) karşı korunabilme	3,22	1,36
20. Microsoft Security Essentials programını kullanabilme	3,40	1,34
Zararlı Yazılımlar Genel Ortalama	3,40	1,02

Tablo 8’deki sonuçlar ***Zararlı Yazılımlar*** boyutuna yönelik ortalamaları göstermektedir. Tablo 14 incelendiğinde ortalamanın 4 ün altında olduğu görülmektedir. Katılımcıların 13. Madde “*Zararlı yazılımların bilgisayara bulaşmasını engelleyebilme*” ($\bar{X}$ =3,61, SS=1.22), 15. Madde “*Zararlı yazılımlar bilgisayara bulaştığı zaman temizleyebilme*” ($\bar{X}$ =3,58, SS=1.28) ve 16. Madde “*Virüslerin bilgisayara bulaşmaması için gereken güvenlik önlemlerini alabilme*” ($\bar{X}$ =3,76, SS=1.22), ifadelerine verdikleri yanıtlar sonucunda, “Yeterliyim” seçeneği ortaya koyarken Madde 14 “*Tuş Kaydedici (Keylogger) şifrelerimi koruyabilme*” ($\bar{X}$ =3,20, SS=1.34), Madde 17 “*Solucanlara (Worm) karşı*

korunabilme” ($\bar{X}=3,24$, $SS=1.31$), Madde 18 “*Truva Atı 'nın (Trojan) bilgisayara bulaşmaması için gereken güvenlik önlemlerini alabilme*” ($\bar{X}=3,15$, $SS=1.35$), Madde 19 “*Casus Yazılımlara (Spyware) karşı korunabilme*” ($\bar{X}=3,21$, $SS=1.35$) ve Madde 20 “*Microsoft Security Essentials programını kullanabilme*” ($\bar{X}=3,39$, $SS=1.34$) ifadelerine verdikleri yanıtların ortalaması derecelendirme sisteminde “Orta Düzeyde Yeterliyim” seçeneğini ortaya koymaktadır. Kullanıcıların zararlı yazılımlar konusunda tamamen yeterli olmadıkları bilgi eksiklikleri olduğu ve bu nedenle kendilerini tamamen yeterli görmediklerini söyleyebiliriz.

Tablo 8’e bakıldığında öğrencilerin zararlı yazılımlar konusunda verdikleri yanıtların genel ortalaması ($\bar{X}=3,39$, $SS= 1,01$) “Orta Düzeyde Yeterliyim” seçeneğini öne çıkarmaktadır. Öğrencilerin zararlı yazılımlar konusunda orta düzeyde yeterlilik düzeyinde olmaları bilişim teknolojileri kullanımında risk altında olduklarını açıkça göstermektedir. Öğrencilerin zararlı yazılımlar konusunda bilgi eksiklikleri siber dünyanın barındırdığı risk unsurlarına karşı savunmasız olduklarını göstermektedir. Zararlı Yazılımlar konusunda önlem almada orta düzeyde yeterli olan öğrencilerin internet ve sosyal medya ortamlarında risk altında olacaklardır.

Çakır ve Kesler, (2012) Anadolu Üniversitesi öğrencileri ile yaptıkları çalışmada katılımcılara yöneltilen “Bilgisayar virüsleri ile ilgili temel bilginiz ne düzeyde” sorusuna verilen cevaplara bakıldığında katılımcıların %41’i konuya yönelik az bilgiye sahip olduklarını bildirmişlerdir.

4.2.3. Web Güvenliği Ve Sosyal Mühendislik Konusuna Yönelik Öz-yeterlik Algıları

Araştırmada kullanılan “Lise Öğrencilerinin Güvenli İnternet Kullanımına Yönelik Öz-yeterlikleri” anketinin üçüncü boyutu olan web güvenliği ve sosyal mühendislik boyutunda yer alan ifadelerle ilişkin elde edilen verilerin Ortalama ($\bar{X}$) ve Standart Sapma (SS) verileri Tablo 9’de verilmiştir.

Tablo 9. Web Güvenliği ve Sosyal Mühendislik Boyutu

Web Güvenliği Ve Sosyal Mühendislik	$\bar{X}$	SS
21. İnternet’te güvenli alış-veriş yapabilme	3,59	1,36
22. Gereksiz (Spam) e-postalara karşı önlem alabilme	3,78	1,28
23. Kameralı kalemler, kameralı gözlükler gibi sosyal mühendislik donanımlarından korunabilme	3,14	1,37
24. İnteraktif bankacılık işlemlerini yaparken güvenlik önlemlerini alabilme	3,31	1,34
25. Aldatmaca (Hoax) e-posta yöntemi konusunda gereken önlemleri alabilme	3,33	1,33
26. Phishing (Oltalama/sahte) e-postalarına karşı kendini koruyabilme.	3,45	1,33
27. Gizli parola oluşturabilme	4,14	1,19
28. HTTP ile HTTPS arasındaki farkı ortaya koyabilme	3,05	1,41
29. E-posta ile yapılan sosyal mühendislik saldırılarına karşı korunabilme	3,28	1,35
Web Güvenliği Ve Sosyal Mühendislik Genel Ortalama	3,45	0,94

Tablo 9 incelendiğinde araştırmaya katılan öğrencilerin 21. Madde de yöneltilen “İnternet’te güvenli alış-veriş yapabilme” ifadesine ($\bar{X}$ =3,58, SS=1.36), Madde 22 “Spam (gereksiz) e-postalara karşı önlem alabilme” ($\bar{X}$ =3,77, SS=1.27), Madde 26 “Phishing (Oltalama/sahte) e-postalarına karşı kendini koruyabilme” ($\bar{X}$ =3,44, SS=1.33) ve Madde 27 “Gizli Parola Oluşturabilme” ($\bar{X}$ =4,13, SS=1.18) verdikleri yanıtlar ile “Yeterliyim” düzeyinde bir fikir ortaya koymuşlardır. Ortalama sonuçlarına göre öğrencilerin tam yeterli bilgiye sahip olmadıklarını bilgi eksiklikleri olduğu görülmektedir. Madde 23 “Kameralı kalemler, kameralı gözlükler gibi sosyal mühendislik donanımlarından korunabilme ” ($\bar{X}$ =3,13, SS=1.36), Madde 24 “ İnteraktif bankacılık işlemlerini yaparken güvenlik önlemlerini alabilme ” ($\bar{X}$ =3,31, SS=1.34), Madde 25 “Hoax (Aldatmaca) e-posta yöntemi konusunda gereken önlemleri alabilme” ($\bar{X}$ =3,33, SS=1.33), Madde 28 “HTTP ile HTTPS arasındaki farkı ortaya koyabilme” ($\bar{X}$ =3,04, SS=1.40) ve Madde 29 “E-posta ile yapılan sosyal mühendislik saldırılarına karşı korunabilme” ($\bar{X}$ =3,27, SS=1.34), konusunda yeterlilik düzeyi “Orta Düzeyde Yeterliyim” olarak tespit edilmiştir.

Tablo 9'a bakıldığında öğrencilerin **Web Güvenliği Ve Sosyal Mühendislik** konusunda işaretledikleri yanıtların “Yeterliyim”, ($\bar{X}=3,45$, $SS= ,94$) düzeyinde olduğu görülmektedir

4.2.4. Bilgisayar Güvenliği Konusuna Yönelik Öz-yeterlik algıları

Araştırmada kullanılan “Lise Öğrencilerinin Güvenli İnternet Kullanımına Yönelik Öz-yeterlikleri” anketinin dördüncü ve son boyutu olan bilgisayar güvenliği boyutunda yer alan ifadelerle ilişkin elde edilen verilerin Ortalama ($\bar{X}$) ve Standart Sapma (SS) verileri Tablo 10'da verilmiştir.

Tablo 10. Bilgisayar Güvelliği Boyutuna İlişkin Ortalama Verileri

Bilgisayar Güvenliği	$\bar{X}$	SS
30. Kişisel dosyalarımı koruyabilme	4,33	1,01
31. Windows işletim sistemine şifre koyabilme	4,13	1,12
32. Bilgisayar için gerekli giriş güvenlik önlemlerini alabilme	4,14	1,11
33. Güvenlik yazılımlarını gerektiğinde güncelleyebilme	4,00	1,13
34. Dosyaları şifreleyebilme	3,96	1,25
35. Bilgi kaybının yaşanmaması için dosyaları belirli aralıklarla yedekleyebilme	3,78	1,29
Bilgisayar Güvenliği Genel Ortalaması	4,06	0,89

Tablo 10' da yapılan analiz sonucu elde edilen ortalama verileri incelendiğinde öğrencilerin iyi düzeyde olduğu söylenebilir. Öğrenciler Madde 30 “*Kişisel Dosyalarımı Koruyabilme*” ($\bar{X}=4,32$, $SS=1.01$), ifadesine verdikleri cevaplar ile “Tamamen Yeterli Oldukları yönünde fikir bildirmişlerdir. Madde 31 “*Windows işletim sistemine şifre koyabilme*” ($\bar{X}=4,13$, $SS=1.12$), Madde 32 “*Bilgisayar için gerekli giriş güvenlik önlemlerini alabilme*” ($\bar{X}=4,14$, $SS=1.11$), Madde 33 “*Güvenlik yazılımlarını gerektiğinde güncelleyebilme*” ($\bar{X}=4,00$, $SS=1.13$), Madde 34 “*Dosyaları Şifreleyebilme*” ($\bar{X}=3,96$, $SS=1.25$) ve 35. Madde “*Bilgi kaybının yaşanmaması için dosyaları belirli aralıklarla yedekleyebilme*” ($\bar{X}=3,78$, $SS=1.29$) ifadelerine verdikleri cevapların analizleri sonucunda öğrencilerin maddelerde belirtilen konularda yeterli olduklarını düşündükleri fakat kendilerini tamamen yeterli görmedikleri sonucuna varılmaktadır.

Tablo 10'a bakıldığında öğrencilerin Bilgisayar Güvenliği konusunda verdikleri yanıtların ortalamasının “Yeterliyim”, ($\bar{X}=4.05$, $SS=,89$) düzeyinde olduğu görülmektedir. Öğrencilerin bilgisayar güvenliğini sağlamada tam yeterli olduklarını düşünememeleri önemli bir sorun olarak değerlendirilmelidir.

4.2.5. Öğrencilerin Güvenli İnternet Kullanımlarının Cinsiyet Faktörüne Göre Değerlendirilmesi

Araştırmaya katılan öğrencilerin güvenli internet kullanımına yönelik öz-yeterlik algılarının cinsiyete göre farklılık durumları Tablo 11’de görülmektedir.

Tablo 11. Güvenli İnternet Kullanım Öz-Yeterliğinin Cinsiyete Göre Mann-Whitney testi sonuçları

	Cinsiyet	N	Sıra Ortalaması
Sosyal Ağlarda Güvenlik (Sosyal Medyada Güvenlik)	Kız	516	422,37
	Erkek	364	466,20
	Toplam	880	
Zararlı Yazılımlar	Kız	516	386,04
	Erkek	364	517,70
	Toplam	880	
Web Güvenliği Ve Sosyal Mühendislik	Kız	516	397,80
	Erkek	364	501,04
	Toplam	880	
Bilgisayar Güvenliği	Kız	516	412,37
	Erkek	364	480,37
	Toplam	880	

Tablo 11’de Lise Öğrencilerinin Güvenli İnternet Kullanımına Yönelik Öz-Yeterlik Algılarının’ cinsiyet değişkenine göre değerlendirildiğinde önemli bazı farklar görülmektedir. Araştırma ölçeğini oluşturan 4 boyutun sıra ortalamasına bakıldığında erkek katılımcıların kızlara göre yeterlilik düzeyleri daha yüksek olduğu görülmektedir.

Elde edilen bulgular M Tekerek ve Tekerek, (2013) çalışmalarında elde edilen bulgular ile zıtlık göstermektedir. Yapılan çalışmada bilgi güvenliği konusunda kızların erkek öğrencilerden daha iyi olduklarını tespit etmişlerdir.

Bir diğer araştırmada Timur ve diğerleri (2013) tarafından bilgisayar kullanım öz-yeterliliğine yönelik yapılan çalışmadır. Araştırmada katılımcıların cinsiyetleri ile bilgisayar kullanım öz-yeterliliği arasında anlamlı bir farklılık bulamamışlardır.

4.2.6. Öğrencilerin Güvenli internet kullanımına yönelik öz-yeterlik algılarının sınıf düzeyine göre farklılık var mı?

Lise öğrencilerinin güvenli internet kullanımına yönelik öz-yeterlikleri algılarını ölçmek üzere uygulanan anket verilerine ilişkin yapılan Independent-Sample T testi sonucunda elde edilen veriler Tablo 12’de verilmiştir.

Tablo 12. Öğrencilerin Güvenli İnternet Kullanımına Yönelik Öz-Yeterlik Algılarının Sınıf Düzeyinde Değerlendirilmesi

	Sınıfınız	N	$\bar{X}$	SS
Sosyal Ağlarda (Sosyal Medya) Güvenlik	9	220	4,17	0,69
	10	219	4,20	0,63
	11	220	4,32	0,60
	12	221	4,21	0,80
Zararlı Yazılımlar	9	220	3,42	1,05
	10	219	3,43	0,91
	11	220	3,40	1,03
	12	221	3,35	1,07
Web Güvenliği ve Sosyal Mühendislik	9	220	3,47	0,95
	10	219	3,52	0,86
	11	220	3,41	0,95
	12	221	3,40	0,10
Bilgisayar Güvenliği	9	220	4,00	0,90
	10	219	4,08	0,82
	11	220	4,08	0,92
	12	221	4,07	0,92

Tablo 12 incelendiğinde “Zararlı Yazılımlar” boyutunda 11 ve 12. Sınıf düzeyinde “Orta Düzeyde Yeterliyim” sonucuna ulaşılırken 9. Ve 10. Sınıf düzeylerinde “Tamamen Yeterliyim” sonucuna ulaşılmıştır. “Sosyal Ağ (Sosyal Medya) Güvenliği”, “Web Güvenliği ve Sosyal Mühendislik” ve “Bilgisayar Güvenliği” Konularında ise katılımcıların yeterli düzeyde bilgiye sahip oldukları belirlenmiştir. Genel anlamda bir farklılık bulunamamıştır.

Yapılan diğer çalışmalarda Berkant ve Efendioğlu (2010); Gökmen ve Akgün (2015); Sırakaya (2011) sınıf düzeyine göre anlamlı bir farklılık elde edilememiştir.

4.2.7. Öğrencilerin Güvenli İnternet Kullanımlarının İlçelere Göre Değerlendirilmesi

Lise öğrencilerinin güvenli internet kullanımına yönelik öz-yeterlikleri algılarını ölçmek üzere uygulanan anket verilerine ilişkin yapılan Kruskal-Wallis testinde Girne ilçesinin diğer ilçelere göre daha düşük düzeyde yeterliliğe sahip olduğu görülmektedir. Test sonucuna ilişkin veriler Tablo 13’da verilmiştir.

Tablo 13. Öğrencilerin Güvenli İnternet Kullanımlarına Yönelik Öz-Yeterlik Algılarının İlçeler Göre Değerlendirilmesi

	Okulunuzun bulunduğu ilçe	N	Sıra Ortalaması
Sosyal Ağlarda (Sosyal Medyada) Güvenlik	Lefkoşa	374	455,81
	Girne	86	391,68
	Gazimağusa	194	445,77
	Güzelyurt	125	411,06
	İskele	101	453,08
	Toplam	880	
Zararlı Yazılımlar	Lefkoşa	374	449,81
	Girne	86	400,56
	Gazimağusa	194	427,26
	Güzelyurt	125	408,76
	İskele	101	509,75
	Toplam	880	
Web Güvenliği ve Sosyal Mühendislik	Lefkoşa	374	453,10
	Girne	86	430,89
	Gazimağusa	194	424,13
	Güzelyurt	125	430,67
	İskele	101	447,17
	Toplam	880	
Bilgisayar Güvenliği	Lefkoşa	374	458,36
	Girne	86	399,85
	Gazimağusa	194	410,43
	Güzelyurt	125	428,21
	İskele	101	485,81

Toplam	880
---------------	-----

Tablo 13’a bakıldığında Girne ilçesinin “Sosyal Ağlarda Güvenlik (Sosyal Medyada Güvenlik)” ve “Bilgisayar Güvenliği” boyutlarında yeterliliği diğer ilçelere göre düşük olduğu tespit edilmiştir. Çalışma kapsamına alınan ilçelerin güvenli internet kullanımına yönelik öz-yeterlik algıları yeterli düzeyde olduğu analizler sonucunda tespit edilmiştir.

M Tekerek ve Tekerek (2013) yaptıkları çalışmada öğrencilerin bilgi ve bilgisayar güvenliğine ilişkin bulguları yerleşim yeri değişkenine göre anlamlı bir farklılık tespit edilmiştir.

4.2.8. Öğrencilerin Güvenli İnternet Kullanımlarına yönelik öz-yeterliklerinin İnternet Kullanım Sürelerine Göre Değerlendirilmesi

Öğrencilerin Güvenli internet kullanım düzeylerinin, haftalık internet kullanım süreleri ile arasında fark olup olmadığına ilişkin bulgular Tablo 14’ de verilmiştir.

Tablo 14. Öğrencilerin Güvenli İnternet Kullanımlarına Yönelik Öz-Yeterlik Algılarının Haftalık İnternet Kullanımlarına ilişkin değerlendirilmesi

	Haftalık İnternet Kullanım Süresi	N	Sıra Ortalaması
Sosyal Ağlarda Güvenlik (Sosyal Medyada Güvenlik)	4 saatten az	136	353,01
	4-12	251	439,10
	13-27	174	435,39
	28+	319	481,69
	Toplam	880	
Zararlı Yazılımlar	4 saatten az	136	409,86
	4-12	251	442,73
	13-27	174	412,71
	28+	319	466,97
	Toplam	880	
Web Güvenliği ve Sosyal Mühendislik	4 saatten az	136	375,79
	4-12	251	448,01
	13-27	174	425,55
	28+	319	470,33
	Toplam	880	
	4 saatten az	136	407,94

Bilgisayar	4-12	251	442,47
Güvenliği	13-27	174	427,89
	28+	319	459,71
Toplam		880	

Tablo 14’ ye bakıldığında haftalık internet kullanım süreleri 4 saatten az olan kullanıcıların sosyal ağ güvenliği (sosyal medya güvenliği), web güvenliği ve sosyal mühendislik konularında yeterli düzeyde öz-yeterlik ve algıya sahip olmadıkları görülmektedir. Zararlı yazılımlar ve bilgisayar güvenliği konularında katılımcıların yeterli düzeyde öz-yeterlik algısına sahip oldukları görülmektedir. Haftalık internet kullanım süreleri 28 saatten fazla olan öğrencilerin ise güvenli internet kullanımına yönelik öz-yeterlik algılarının yüksek olduğu tespit edilmiştir.

Durmuş ve Başarmak (2014) yaptıkları araştırmada internet kullanım sürelerinin eğitsel internet kullanım düzeyleri ile doğrudan ilişkili olduğu bulgusuna ulaşmışlardır. Araştırmada internet kullanım süreleri 8 saatten fazla olan bireylerin eğitsel internet kullanım öz-yeterlik düzeylerinin yüksek olduğu belirlenmiştir.

Özdemir ve Akar (2011) Anakara ve İstanbul illerinde öğrenim gören 336 lise öğrencisi ile yaptıkları çalışmada internet kullanım süreleri 5 saatin üstünde olan öğrencilerin daha fazla siber zorbalık yaptıklarını tespit etmişlerdir.

BÖLÜM V

SONUÇ VE ÖNERİLER

Bu bölümde lise öğrencilerinin güvenli internet kullanımına yönelik öz-yeterlik algılarına ilişkin uygulanan anketin sonuçlarına yer verilmiş ve Araştırma sonucunda elde edilen bulgular tartışılmıştır.

5.1. Sonuçlar

Bilişim teknolojilerinin her an, her yerde, her konuda ve her yaşta kullanım alanı bulabilmesi teknolojinin hayatın olmazsa olmazı durumunda olduğunu göstermektedir. Her yaşta kullanıcı profiline sahip olması “sanal dünyada ne kadar güvende olunabilir?” Sorusunu gündeme getirmektedir. Bu bölümde araştırma sonuçları alt amaçlara göre açıklanmıştır.

5.1.1. Öğrencilerin sosyal ağ (sosyal medya) güvenliğine yönelik öz-yeterlik algıları

Araştırma sonucunda KKTC’ de öğrenim görmekte olan lise öğrencilerinin sosyal ağlarda güvenlik konusunda öz-yeterlik algılarının tamamen yeterli düzeyde oldukları tespit edilmiştir. Araştırma sonuçları incelendiğinde katılımcıların sosyal ağ kullanımında gerekli güvenlik önlemlerini alabilecek düzeyde yeterliliğe sahip oldukları belirlenmiştir. Ancak ankette sosyal ağlarda güvenlik boyutu altında araştırılan faktörlerde kullanıcıların yeterlilik düzeyleri olması gerekenin altında olduğu belirlenmiştir.

Sosyal ağlarda yer alan tehlikeler göz önünde bulundurduğunda gerekli önlemlerin alınabilmesi hususunda bilinçli olmak önemli bir konudur. Sosyal ağlarda güvenlik konusunda, H. Çakır, Hava, Gülen ve Özüdoğru (2015) Yaptıkları çalışmada araştırmaya katılan öğretmen adaylarının genel olarak sosyal ağ güvenliğine yönelik orta düzeyde farkındalığa sahip oldukları bulgusuna ulaşmıştır.

Günümüzün internet teknolojisinin sağladığı en büyük kolaylıklardan biri olan sosyal medya ortamları yeterli güvenlik bilgisi olmaksızın kullanılmaları halinde birçok soruna yol açabilmektedir. Siber zorbalık (Siber taciz), kimlik hırsızlığı, çocuk istismarı vb. durumlar

ile karşılaşılması ve önüne geçilebilmesi aşamasında kullanıcıların bilgi düzeyleri oldukça büyük önem arz etmektedir.

5.1.2. Öğrencilerin zararlı yazılımlara yönelik öz-yeterlik algıları

Araştırma sonucunda katılımcıların zararlı yazılımları konusunda bilgi düzeyleri orta düzeyde yeterli olduğu görülmektedir. Çocuk ve gençlerin internet kullanımlarında güvenlik en önemli sorun olarak karşımıza çıkmaktadır. Güvenlik önlemlerini alabilmek, ancak bilinçli kullanıcı olabilmekle mümkündür. Araştırma sonucunda öğrencilerin virüs ve diğer zararlı yazılımlardan korunma konusunda yeterli bilgiye sahip olmadıklarını göstermektedir. Bilişim teknolojilerinin yoğun olarak kullanılmakta olduğu günümüzde bu durum olması gerekenin durumun çok gerisindedir.

Akgün ve Topal (2015) yaptıkları çalışmada öğrencilerin antivirüsler ve zararlı yazılımları engelleyebilme konularında dikkate değer düzeyde farkındalığın düşük olduğunu belirtmişler ve öğrencilerin bilgi eksikliklerine dikkat çekmektedirler. Özellikle katılımcıların toplamda %50,5'i bilişim güvenliğini sağlamak amacıyla kullanılan yazılımların bulunması ve kullanılması konusunda yeterliliklerinden emin olamamaktadır.

Gökmen ve Akgün (2015) yaptıkları 375 BÖTE öğrencisi ile yaptıkları çalışmada katılımcıların %13,1'i antivirüs programı kullanmadıklarını, %11,5'sinin ise güncelleme zamanları ile ilgili bilgilerinin olmadığını belirtmişlerdir.

Günümüzde yaşanan zararlı yazılım mağduriyetlerinin çokluğu göz önüne alındığında güvenlik yazılımlarının kullanımı ve güncelliği önemini arttırmaktadır.

5.1.3. Öğrencilerin web güvenliği ve sosyal mühendislik konusunda öz-yeterlik algıları

İnternet kullanıcılarının internet ortamında güvenliği sağlayabilmeleri ve sosyal mühendislik saldırılarına karşı önlem alabilmeleri için bu konularda yeterli bilgi birikimine

ve öz-yeterliliğe sahip olmaları gerekmektedir. Lise öğrencilerine yönelik yapılan araştırmanın web güvenliği ve sosyal mühendislik konularında katılımcıların yeterli düzeyde bilgi sahibi olup olmadıkları konusunda kararsız oldukları belirlenmiştir.

Kruger, Drevin, Flowerday ve Steyn (2011) yapmış oldukları çalışma sonucunda katılımcıların %47'si sosyal mühendislik ve sosyal mühendislik ile bağlantılı kavramların ne olduğunu bilmediklerini tespit etmişlerdir. Tekerek ve Tekerek (2013) yapmış oldukları çalışma sonucunda öğrencilerin internet ortamında güvenli şifre kullanımları konusunda yeterliliklerinin alt düzeyde olduğunu tespit etmişlerdir. Akgün ve Topal (2015) yaptıkları çalışmada katılımcıların 71,6'sı nasıl güvenli şifre oluşturabilecekleri konusunda bilgi sahibi olduklarını belirtmişlerdir.

5.1.4. Öğrencilerin bilgisayar güvenliğini konusunda öz-yeterlik algıları

Araştırma sonucunda araştırmaya katılan öğrencilerin bilgisayar güvenliği konusunda yöneltilen ifadelere verdikleri cevaplar ile yeterli düzeyde bilgi sahibi olduklarını belirtmişlerdir. Bilişim çağını yaşadığımız düşünüldüğünde bilgisayar güvenliğine yönelik elde edilen bulgular beklentileri karşılamamaktadır. Günümüzde çocuklar internet teknolojisi ile büyümektedirler. Teknoloji yerlisi olarak da tanımlanabilen (DeFranco, 2011) yeni nesil kullanıcıların bilgisayar kullanımı ve güvenliğine yönelik bilgi düzeyinin yüksek olması beklenmektedir.

Çakır ve Kesler (2012) Anadolu üniversitesi BÖTE 32 öğrenci ve diğer bölümlerden 1.2.3 ve 4. Sınıflardan 32 öğrenci olmak üzere toplamda 64 öğrenci ile çalışma yapmışlardır. Anketler böte ve diğer bölümler olmak üzere 2 kategoride değerlendirilmiştir. Çalışma sonuçları incelendiğinde antivirüs kullanım oranları Böte öğrencilerinde %69'u lisanssız %25'i lisanslı antivirüs programları kullanırken %6' sı antivirüs programı kullanmamaktadır. Diğer bölümlerden katılımcıların %53' ü lisanssız %38'i lisanslı antivirüs programı kullanırken %9' unun antivirüs programı kullanmadıkları belirlenmiştir.

Katılımcıların lisanssız antivirüs programı kullanımlarının yoğunlukta olması Kişisel bilgisayar güvenliği, kişisel veri güvenliği ve internet güvenliği konusundaki bilgi eksikliklerini ortaya koymaktadır.

Yılmaz ve diğerleri (2014) 124 üniversite öğrencisi ile yaptıkları karma araştırma sonucunda öğrencilerin bilişim güvenliğini sağlama konusunda yeterli düzeyde yeterliliğe sahip olmadıkları bulguna ulaşmışlardır. Bu konuya yönelik temel sorunun ise öğrencilere verilen bilişim teknolojileri derslerinde bilişim ve internet güvenliğine yönelik yeterli düzeyde yer verilmemesi bilgilerin güncel olmaması olarak gösterilebilir.

5.1.5. Öğrencilerin genel itibari ile güvenli internet kullanımına yönelik öz-yeterlik algıları

İnternet teknolojisinin yaygın olarak kullanıldığı günümüzde kullanıcıların güvenli internet kullanımına yönelik bilgi düzeyleri internetin zararlı yönlerinden korunmada önemli bir yere sahiptir. KKTC’ de lise öğrencilerin güvenli internet kullanımına yönelik öz-yeterlik algılarının betimlemek amacıyla yapılan çalışma sonucunda öğrencilerin sosyal ağ güvenliği (sosyal medya güvenliği) konusunda yeterli düzeyde bilgi sahibi oldukları tespit edilmiştir. Ancak web güvenliği ve sosyal mühendislik, zararlı yazılımlar ve bilgisayar güvenliği konusunda tamamen yeterli olmamakla birlikte günümüz bilişim gereksinimlerine göre beklenenin altında olduğu tespit edilmiştir.

Araştırma sonuçları Gökmen ve Akgün (2016) yaptıkları çalışmada öğretmenlerin bilişim suçları konusunda yeterli bilgiye sahip olmadıklarını ve bilişim suçuyla karşılaşmaları halinde yapmaları gerekenler konusunda bilgi sahibi olmadıklarını tespit etmişlerdir.

5.1.6. Öğrencilerin güvenli internet kullanımına yönelik öz-yeterlik algıları cinsiyete göre sonuçları

Analiz sonuçları incelendiğinde araştırma kapsamında değerlendirilen dört boyutta da erkek öğrencilerin kız öğrencilere göre daha yüksek öz-yeterlik algısına sahip oldukları tespit edilmiştir. Araştırma sonuçları Gökmen ve Akgün (2014) BÖTE öğretmen adaylarına yönelik yaptıkları çalışmada erkek öğretmen adaylarının bilişim teknolojileri güvenliği bilgi düzeylerinin bayan öğretmen adaylarına göre daha yüksek olduğu tespit edilmiştir.

Bilişim teknolojileri kullanımının cinsiyete göre farklılıklar gösterdiği yapılan araştırmalar incelendiğinde görülmektedir. Beder ve Ergun (2015) ortaokul öğrencilerine yönelik yaptıkları çalışmada elde edilen bulgularda kız öğrencilerin bilinç düzeylerinin daha yüksek olduğunu tespit etmişlerdir. Yılmaz, Şahin ve Akbulut (2016) çalışmalarında elde ettikleri bulgular ile uyushmaktadır.

5.1.7. Öğrencilerin güvenli internet kullanımına yönelik öz-yeterlik algıları bulundukları ilcelere göre sonuçlar

Araştırma sonuçlarına bakıldığında öğrencilerin güvenli internet kullanımlarına yönelik öz-yeterlik algılarının ilcelere farklılık göstermemektedir. Ancak sadece Girne bölgesi, güvenli internet kullanımına yönelik öz-yeterlikler ve algılar konusunda diğer ilcelere göre düşük düzeyde yeterliğe sahip oldukları tespit edilmiştir.

Tekerek ve Tekerek (2013) yaptıkları çalışmada katılımcıların bilgi güvenliği farkındalık düzeylerinin yerleşim yerlerine göre farklılık gösterdiği bulgusuna ulaşmışlardır.

5.1.8. Öğrencilerin güvenli internet kullanımına yönelik öz-yeterlik algılarının Sınıf Düzeylerine Göre Sonuçları

Araştırma sonuçları incelendiğinde 11 ve 12. Sınıf öğrencilerinin zararlı yazılımlar konusunda yeterli düzeyde bilgi sahibi olmadıkları belirlenmiştir. Zararlı yazılımlar konusunda yeterli bilgi sahibi olunmaması halinde güvenlik önlemlerinin alınması mümkün olmamaktadır. Tuncer ve Tanaş (2011) bilgisayar öz-yeterliğine yönelik yaptıkları

alıřmada sınıf dzeylerine iliřkin anlamlı bir farklılık olmadığı bulgusuna ulařmıřlardır. Beder ve Ergun (2015) problemlı internet kullanımına ynelik yaptıkları alıřmada sınıf dzeylerine gre anlamlı derecede farklılık olduėunu tespit etmiřlerdir.

5.2. Öneriler

Öğrencilerin güvenli internet kullanımına yönelik öz-yeterlik algılarının belirlenmesi amacıyla yapılan çalışmanın bulguları incelendiğinde öğrencilerin güvenli internet kullanımına yönelik yeterli öz-yeterlik ve algıya sahip olmadıkları belirlenmiştir. Bu durumun nedenlerini maddeler halinde belirtecek olursak;

5.2.1. Öğrencilere Yönelik Öneriler

- Sosyal medya platformlarında tanımadıkları kişilerden gelen bildirimleri ve mesajları kabul etmemeleri
- Sosyal Medya platformlarında geçirdikleri sürelere dikkat edilerek kontrollü kullanımın sağlanması,
- Birden fazla sosyal medya hesabı kullanılması halinde farklı hesaplar için farklı şifreler oluşturmaları
- Kişisel bilgisayarlarda lisanslı ve güncel antivirüs kullanımına dikkat edilmesi
- Kişisel profil ayarlarını sadece arkadaşlarının görebilecekleri şekilde ayarlamaları
- Hiç kimse ile şifre paylaşımında bulunmamaları,
- Kullanılan işletim sisteminin gerekli güncellemelerinin daimî kontrol edilmesi ve gerekli güncellemelerin yapılması,
- Hakaret, taciz gibi rahatsızlık verici paylaşımlardan kaçınmaları, Böyle bir durum ile karşılaşıldığında ise ilgili platformun yöneticileri ile irtibata geçilmesi,
- Bilinçli kullanıcı olmaksızın çevrimiçi alışverişlerden uzak durmaları,
- Çevrimiçi alışveriş yaparken kişisel bilgi, kredi kartı şifresi vb. bilgilerin kesinlikle verilmemesi önerilebilir.

5.2.2. Öğretmenlere Yönelik Öneriler

- Öğrencilere internetin güvenli kullanımına yönelik eğitimlerin verilmesi aşamasında öğretmenlerin farklı öğretim yöntemlerini kullanmaları önerilir.
- Bilişim teknolojileri öğretmenlerinin internet riskleri, sosyal medyanın güvenli kullanımı ve kişisel bilgisayar güvenliği ile ilgili daha geniş bilgiye yer vermeleri önerilir.

5.2.3. Akademisyenlere Yönelik Öneriler

- Araştırma öğrencilerin öz-yeterlik algılarının değerlendirmek amacı ile yapılmıştır. Öğrencilerin yeterliklerine yönelik kendi görüşleri değerlendirilmiştir. Deneysel çalışmalar yapılarak bulguların değerlendirilmesi,
- Güvenli internet kullanımına yönelik konuların ders kitaplarında yer almasına rağmen çalışmamızın sonucunda öğrencilerin tamamen yeterli olmamaları bilişim teknolojileri öğretmenlerinin güvenli internet kullanımına yönelik eğitim verebilme yeterliliklerinin araştırılması, gerekli kılınmaktadır.

5.2.4. Kurumlara Yönelik Öneriler

- Şu an tasarı halinde olan bilişim suçlarının ivedi olarak ele alınması ve çalışmaların hızlandırılması,
- Bilgi teknolojileri ve haberleşme kurumunun Kuzey Kıbrıs Türk Cumhuriyeti’nde bilişim teknolojileri kullanımına yönelik araştırmaları yapmaları aynı zamanda Kuzey Kıbrıs Türk Cumhuriyeti’nde bilişim suçlarından yaşanan mağduriyetlere yönelik araştırmaların yapılması gereklilik arz etmektedir.

KAYNAKÇA

- Agatston, P. W., Kowalski, R. ve Limber, S. (2007). Students' Perspectives on Cyber Bullying. *Journal of Adolescent Health*, 41(6 SUPPL.), S59-60. doi:10.1016/j.jadohealth.2007.09.003
- Aghaei, S., Nematbakhsh, M. A. ve Farsani, H. K. (2012). Evolution of the World Wide Web : From Web 1.0 to Web 4.0. *International journal of Web & Semantic Technology*, 3(1), 1–10. doi:10.5121/ijwest.2012.3101
- Akbulut, Y. (2013). Çocuk ve Ergenlerde Bilgisayar ve İnternet Kullanımının Gelişimsel Sonuçları. *Trakya Üniversitesi Eğitim Fakültesi Dergisi*, 3(2).
- Akca, E. B., Sayımer, İ., Salı, J. B., & Başak, B. E. (2014). Okulda siber zorbalığın nedenleri, türleri ve medya okuryazarlığı eğitiminin önleyici çalışmalarındaki yeri. *Elektronik Mesleki Gelişim Ve Araştırmalar Dergisi*, 2(2), 17-30.
- Akgün, Ö. E. ve Topal, M. (2015). Eğitim fakültesi son sınıf öğrencilerinin bilişim güvenliği farkındalıkları: Sakarya Üniversitesi Eğitim Fakültesi örneği. *Sakarya University Journal of Education*, 2(5), 98–121.
- Ahmet, A., Merve, K., Ümran, A., SAHRANÇ, Ü., & Erol, U. (2014). İnternet Öz-yeterliği Ölçeği Türkçe Formunun Geçerlik ve Güvenirliği (The Validity and Reliability Studies of Turkish Version of the Internet Self-efficacy Scale)..... Doi: 10.14686/BUEFAD. 201428191. *BARTIN ÜNİVERSİTESİ EĞİTİM FAKÜLTESİ DERGİSİ*, 3(2), 404-415.
- Almomani, A., Gupta, B. B., Atawneh, S., Meulenberg, A., & Almomani, E. (2013). A survey of phishing email filtering techniques. *IEEE communications surveys & tutorials*, 15(4), 2070-2090.
- Arıtürk, M. (2014). Bilgi farkındalığı ve bilgi güvenliğinin karşılaştırılması.

- Arslan, S., Savaser, S., Hallett, V., & Balci, S. (2012). Cyberbullying among primary school students in Turkey: Self-reported prevalence and associations with home and school life. *Cyberpsychology, Behavior, and Social Networking*, 15(10), 527-533.
- Aslan, A. (2016). *Türkiye’de Çocukların Güvenli İnternet Kullanımında 2010-2015 Yılları Arasındaki Değişmeler Ve Uygulamaların Yansımaları*. Atatürk Üniversitesi.
- Aydın, İ. (2013). Çocuk, İnternet ve Etik. *Gençlik Araştırmaları Dergisi*, 2(1), 98.
- Aydın, Y. (2011). Liselerde bilgisayar ve internet kullanımının eğitim ve öğretimdeki olumsuz etkileri [Negative effects of computer and internet usage in education and training at high schools]. *Unpublished Masters Thesis*. Marmara University, İstanbul, Turkey.
- Balay, R., Kaya, A. ve Çevik, M. (2014). Öğretmenlerin İnternete Yönelik Tutumları ve Eğitsel İnternet Kullanım Öz-Yeterlik İnanç Düzeyleri. *Dergi Karadeniz*.
- Bandura, A. (2011). Social cognitive theory. *Handbook of social psychological theories*, 2012, 349-373.
- Bandura, A. (2012). On the Functional Properties of Perceived Self-Efficacy Revisited. *Journal of Management*, 38(1), 9–44. doi:10.1177/0149206311410606
- Baş, G. (2011). İlköğretim Öğretmenlerinin Eğitsel İnternet Kullanımı Öz-Yeterlik İnançlarının Farklı Değişkenler Açısından İncelenmesi. *Eğitim Teknolojisi Kuram ve Uygulama*, 1(2), 35–51. doi:10.17943/ETKU.13173
- Baştürk Akca, E. B., Sayımer, İ. ve Ergül, S. (2015). Ortaokul Öğrencilerinin Sosyal Medya Kullanımları Ve Siber Zorbalık Deneyimleri: Ankara Örneği. *Global Media Journal TR Edition*, 5(10), 71–86.
- Bayırtepe, E., & Tüzün, H. (2007). Oyun-tabanlı öğrenme ortamlarının öğrencilerin bilgisayar dersindeki başarıları ve öz-yeterlik algıları üzerine etkileri. *Hacettepe Üniversitesi Eğitim Fakültesi Dergisi*, 33(33).

- Bayram, N. ve Saylı, M. (2013). Üniversite Öğrencileri Arasında Siber Zorbalık Davranışı. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, 1(73), 107–116.
- Bayzan, Ş. (2011). Dünyada İnternetin Güvenli Kullanımına Yönelik Uygulama Örnekleri ve Türkiye'de Bilinçlendirme Faaliyetlerinin İncelenmesi ve Türkiye İçin Öneriler. *İletişim Uzmanlığı Tezi, Bilgi Teknolojileri ve İletişim Kurumu, Ankara*.
- Bayzan, Ş. ve Özbilen, A. (2012). Dünyada İnternetin Güvenli Kullanımına Yönelik Uygulama Örnekleri Ve Türkiye’de Bilinçlendirme Faaliyetlerinin İncelenmesi Ve Türkiye İçin Öneriler. *New World Sciences Academy*, 7(2), 521–531.
- Beder, A. ve Ergun, E. (2015). Ortaokul Öğrencilerinin Güvenli İnternet Kullanım Durumlarının Belirlenmesi. *Eğitim Bilimleri Ve Uygulama*, 14(27), 23–41
- Berkant, H. G. ve Efendioğlu, A. (2010). Sınıf Öğretmenliği Bölümü Öğrencilerinin Bilgisayarla İlgili Öz-Yeterlik Algıları ve Bilgisayar Destekli Eğitim Yapmaya İlişkin Tutumları. 9. *Ulusal Sınıf Öğretmenliği Eğitimi Sempozyumu* içinde (ss. 951–955). Elazığ.
- Bhardwaj, A., Avasthi, V., Sastry, H. ve Subrahmanyam, G. V. B. (2016). Ransomware Digital Extortion: A Rising New Age Threat. *Indian Journal of Science and Technology*, 9(14). doi:10.17485/ijst/2016/v9i14/82936
- Bilek, B. T. (2012). Bilişim suçları ve üniversite lisans öğrencilerin bilişim suçlarına yönelik görüşleri. *Yüksek lisans tezi, Gazi Üniversitesi, Bilişim Enstitüsü, Ankara*.
- Bilgi Teknolojileri Ve Haberleşme Kurumu. (2015). 2015 Elektronik Haberleşme Sektörü 3 Aylık Veriler Raporu. www.bthk.org. 29 Nisan 2016 tarihinde <http://www.bthk.org>/ adresinden erişildi.
- Bolat, O. İ. (2011). Öz Yeterlilik ve Tükenmişlik İlişkisi: Lider-Üye Etkileşiminin Aracılık Etkisi/The Relationships Between Self-Efficacy and Burnout: Mediating Effects of Leader-Member Exchange. *Ege Akademik Bakis*, 11(2), 255.

- Büyüköztürk, Ş., Çakmak, E., Akgün, Ö. ve Karadeniz, Ş. (2008). Bilimsel araştırma yöntemleri. *Ankara: Pegem Akademi*.
- Canbek, G., & SAĞIROĞLU, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. *Politeknik Dergisi*, 9(3).
- Canbek, G. ve Sağiroğlu, Ş. (2007). Çocukların ve Gençlerin Bilgisayar ve İnternet Güvenliği. *Politeknik Dergisi*, 10(1), 33–39. doi:10.2339/2007.10.1.33-39
- Carvalho, M. (2013). Early Security Adopters. *International Journal of Computer Applications*, 72(4).
- Ceylan, Y. (2013). Türkiye’de Çocukların Güvenliğine Yönelik “Güvenli İnternet” Uygulamasının Yazılı Basında Yankıları. *Akademik bakış Dergisi*, 37, 12.
- Cicioğlu, M. (2014). Öğrencilerin problemlı internet kullanımı ve siber zorbalık davranışlarına ilişkin görüşleri. *Yayımlanmamış Yüksek Lisans Tezi, Abant İzzet Baysal Üniversitesi, Bolu*.
- Çakır, H., Hava, K., Gülen, Ş. B. ve Özudoğru, G. (2015). Öğretmen adaylarının sosyal ağ sitelerinde güvenlik farkındalıklarının incelenmesi. *International Journal of Human Sciences*, 12(1), 887. doi:10.14687/ijhs.v12i1.3142
- Çakır, S., & Kesler, M. (2012). Bilgisayar Güvenliğini Tehdit Eden Virüsler ve Antivirüs Yazılımları. *XIV. Akademik Bilişim Konferansı Bildirileri*, 551-558.
- Çali, H. H., & Altunba, F. (2012). Güvenlik Hizmetlerinde Yönetişim Aracı Olarak Sosyal Medya Platformları. *Ekev Akademi Dergisi*.
- Çavus, N. ve Ercağ, E. (2014). The scale for the self-efficacy and perceptions in the safe use of the Internet for teachers: The validity and reliability studies. *British Journal of Educational Technology*, 47(1), 76–90. doi:10.1111/bjet.12217

- Çelen, F. K., Çelik, A., & Seferoğlu, S. S. (2011). Çocukların internet kullanımları ve onları bekleyen çevrim-içi riskler. *Akademik Bilişim*, 2-4.
- Çıtak, Ö. (2016). *Ethical Hacking* (1.). İstanbul: Level Kitap
- Çubukcu, A., & 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.
- DeFranco, J. F. (2011). Teaching Internet Security, Safety in Our Classrooms. *Techniques: Connecting Education and Careers (J1)*, 86(5), 52-55.
- Demir, Ü. (2016). Sosyal Medya Kullanımı Ve Aile İletişimi: Çanakkale'de Lise Öğrencileri Üzerine Bir Araştırma. *Selçuk Üniversitesi İletişim Fakültesi Akademik Dergisi*, 9(2), 27-50.
- Demirel, M., Yörük, M., & Özkan, O. (2012). Çocuklar İçin Güvenli İnternet: Güvenli İnternet Hizmeti ve Ebeveyn Görüşleri Üzerine Bir Araştırma-Safe Internet For Children: A Study on Safe Internet Service and Parental Views. *Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 4(7), 54-68.
- Durmuş, A., & Başarmak, U. (2014). Öğretmen adaylarının eğitsel internet kullanım öz-yeterlik inançları ve problemleri internet kullanım durumları arasındaki ilişkinin incelenmesi. *Ahi Evran Üniversitesi Kırşehir Eğitim Fakültesi Dergisi*, 15(3).
- Erçağ, E. (2014). *Otantik Öğrenme Yaklaşımıyla Tasarlanan Sanal Öğrenme Ortamlarının Öğretmenlerin Güvenli İnternet Kullanımına Yönelik Başarısına, Memnuniyetine Ve Öz Yeterlik Algısına Etkisi*. Yakın Doğu Üniversitesi, Lefkoşa.
- Erdoğan, G. ve Bahtiyar, Ş. (2014). Sosyal Ağlarda Güvenlik. *XVI. Akademik Bilişim, Mersin Üniversitesi, Mersin içinde* (ss. 5–7). <http://ab.org.tr/ab14/bildiri/200.pdf> adresinden erişildi.

- Eroğlu, Y., Aktepe, E., Akbaba, S., Işık, A. ve Özkorumak, E. (2015). Siber Zorbalık ve Mağduriyetin Yaygınlığının ve Risk Faktörlerinin İncelenmesi. *Eğitim ve Bilim*, 40(177), 93–107. doi:10.15390/EB.2015.3698
- Eroğlu, Y. ve Güler, N. (2015). Koşullu öz-değer, riskli internet davranışları ve siber zorbalık/mağduriyet arasındaki ilişkinin incelenmesi. *Sakarya University Journal of*. doi:dx.doi.org/10.19126/suje.56594
- Erzurum Emniyet Müdürlüğü. (y.y.). İnternetteki Sahtekarlıklar ve Dolandırıcılıklar. 2 Kasım 2016 tarihinde <http://www.erkurum.pol.tr/Duyurular/Sayfalar/Internetteki-Sahtekarlıklar-ve-Dolandiriciliklar-21102014.aspx> adresinden erişildi.
- Gökçearsan, Ş., & Günbatar, M. S. (2012). Ortaöğrenim öğrencilerinde internet bağımlılığı. *Eğitim Teknolojisi Kuram ve Uygulama*, 2(2), 10-24.
- Gökmen, Ö. F. (2014). *Bilgisayar ve öğretim teknolojileri eğitimi öğretmen adaylarının bilişim güvenliği eğitimi verebilme yeterliklerinin incelenmesi*. Sakarya Üniversitesi.
- Gökmen, Ö. F. ve Akgün, Ö. E. (2014). Bilgisayar ve Öğretim Teknolojileri Eğitimi Öğretmen Adaylarının Bilişim Güvenliği Bilgilerinin Çeşitli Değişkenlere Göre İncelenmesi. *Çukurova Üniversitesi Eğitim Fakültesi Dergisi*, 44(1), 61–84. doi:10.14812/cufej.2015.004
- Gökmen, Ö. F. ve Akgün, Ö. E. (2015). Bilgisayar ve Öğretim Teknolojileri Eğitimi Öğretmen Adaylarının Bilişim Güvenliği Eğitimi Verebilmeye Yönelik Yeterlilik Algılarının İncelenmesi. *Elementary Education Online*, 14(4), 1208–1221. doi:10.17051/ie.2015.04635
- Gökmen, Ö. F. ve Akgün, Ö. E. (2016). Öğretmen Adaylarının Bilişim Suçlarına Yönelik Deneyimleri Ve Bilişim Güvenliği Ders İçeriğine Yönelik Görüşleri. *Mustafa Kemal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 13(33), 178–193.

- Güngör, M. (2015). *Ulusal Bilgi Güvenliği: Strateji Ve Kurumsal Yapılanma*. Ankara: Türkiye Cumhuriyeti Kalkınma Bakanlığı.
- Günüç, S. ve Kayri, M. (2010). Türkiye’de İnternet Bağımlılık Profili ve İnternet Bağımlılık Ölçeğinin elıştırılması: Geçerlik- Güvenirlik Çalışması. *Hacettepe Üniversitesi Eğitim Fakültesi Dergisi*, 39, 220–232.
- Gürcan, A. (2005). Bilgisayar Öz yeterliliği ile Bilişsel Öğrenme Stratejileri Arasındaki ilişkiler. *Eğitim Araştırmaları Dergisi*, 19, 179–193.
- Hampton, N. ve Baig, Z. A. (2015). Ransomware: Emergence of the cyber-extortion menace. *Australian Information Security Management Conference, 2015*, 47–56. doi:10.4225/75/57b69aa9d938b
- Hekim, H., & Başbüyük, O. (2013). Siber Suçlar ve Türkiye’nin Siber Güvenlik Politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi*, 135-158.
- Henkoğlu, T. ve Yılmaz, B. (2013a). İnternet Erişim Özgürlüğünün Kısıtlanması : Türkiye Üzerine Bir Değerlendirme Restrictions of Internet Access Freedom : An Evaluation Study of Turkey Öz Giriş. *Bilgi Dünyası*, 14(5651), 215–239.
- Henkoğlu, T. ve Yılmaz, B. (2013b). Avrupa Birliği (AB) Bilgi Güvenliği Politikaları. *Türk Kütüphaneciliği*, 27(3), 451–471.
- Johnson, J., Gupta, S., Carlson, L., Rifon, N. J., Larose, R. ve Quilliam, E. T. (2012). Adult and Teen Internet Safety Perceptions and Behaviors : a Comparative Protection Motivation Theory Examination. *American Marketing Association* içinde (ss. 138–140). In Ama Winter Educators’ Conference Proceedings.
- Kahraman, S., Yılmaz, Z. A., Erkol, M. ve Yalçın, S. A. (2013). Öğretmen Adaylarının Eğitsel İnternet Kullanımı Öz Yeterlik İnançlarının İncelenmesi. *Elementary Education Online*, 12(4), 1000–1015.

- Kalyon, A., Balcı, İ. ve Şahin, M. (2016). İnternet bağımlılığının medyada yansımaları. *Journal of Human Sciences*, 13(2), 2520. doi:10.14687/jhs.v13i2.3631
- Kara, M. (2013). *Siber Saldırılar Siber Savaşlar ve Etkileri* (Doctoral dissertation, İstanbul Bilgi Üniversitesi).
- Karakuş, T., Çağıltay, K., Kaşıkçı, D., Kurşun, E., & Ogan, C. (2014). Türkiye ve avrupa'daki çocukların internet alışkanlıkları ve güvenli internet kullanımı. *Eğitim ve Bilim*, 39(171).
- Kaspersky Lab. (2016). *Kaspersky Security Bulletin: Overall Statistics for 2016*. Kaspersky Lab. https://kasperskycontenthub.com/securelist/files/2016/12/Kaspersky_Security_Bulletin_2016_Statistics_ENG.pdf adresinden erişildi.
- Kılıç, A. F. (2014). Bulut Bilişimde Gizlilik ve Güvenliğin Korunması: bilişimsel Savunma ve Hukuki Çerçeve Boyutlar.
- Kılıç, F. (2016). 2016 Sosyal Medya Kullanım Oranları. www.webtakibi.com. 27 Ocak 2017 tarihinde <http://www.webtakibi.com/2016-sosyal-medya-kullanim-oranlari/1316> adresinden erişildi.
- Kır, E. (2013). Çocuklara Yönelik Cinsel Taciz Ve İstismara Karşı Önleyici Eğitim Çalışmaları. İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 71(1), 785-800.
- Kır, İ. ve Sulak, Ş. (2014). Eğitim Fakültesi Öğrencilerinin İnternet Bağımlılık Düzeylerinin İncelenmesi. *Elektronik Sosyal Bilimler Dergisi*, 13(51), 150–167.
- Kırık, A. M. (2014). Aile ve Çocuk İlişkisinde İnternetin Yeri: Nitel Bir Araştırma. *Eğitim ve Öğretim Araştırmaları Dergisi*, 1(3).
- Kırık, A. M., Arslan, A., Çetinkaya, A., & Mehmet, G. Ü. L. (2015). A Quantitative Research On The Level Of Social Media Addiction Among Young People İn Turkey. *International Journal Of Science Culture And Sport (Intjcs)*, 3(3), 108-122.

- Kim, W., Jeong, O., Kim, C. ve So, J. (2011). The dark side of the Internet: Attacks, costs and responses. *Information systems*.
- Koç, S., & Kaynak, S. (2010). Bilişim suçları bağlamında yeni medya olarak internet ve kişisel güvenlik . *Akademik Bilişim Konferansı 2010*.
- Köse, G., & Özen, K. (2010). İnternet’te sansür üzerine bir değerlendirme. *S. Kurbanoglu ve diğeleri (Yay. Haz.), “Bilgi Yönetiminde Teknolojik Yakınsama ve Sosyal Ağlar, 2, 22-24*.
- Kruger, H. A., Drevin, L., Flowerday, S. ve Steyn, T. (2011). An assessment of the role of cultural factors in information security awareness. *2011 Information Security for South Africa* içinde (ss. 1–7). IEEE. doi:10.1109/ISSA.2011.6027505
- Kubovič, O. (2016). Çocuklar hangi dijital risklerle karşı karşıya? www.eset.com. 27 Ekim 2016 tarihinde <https://www.eset.com/tr/about/press/articles/article/cocuklar-hangi-dijital-risklerle-karsi-karsiya/> adresinden erişildi.
- Kuo, Y.-C., Walker, A. E., Schroder, K. E. E. ve Belland, B. R. (2014). Interaction, Internet self-efficacy, and self-regulated learning as predictors of student satisfaction in online education courses. *The Internet and Higher Education*, 20, 35–50. doi:10.1016/j.iheduc.2013.10.001
- Kurbanoglu, S. S. (2004). Öz-Yeterlik İnancı ve Bilgi Profesyonelleri İçin Önemi. *Bilgi Dünyası*, 5(2), 137–152.
- Labs., T. (2016). The Reign of Ransomware. 27 Ekim 2016 tarihinde <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/reports/rpt-the-reign-of-ransomware.pdf>
- Li, C. H., Hsu, F. H., Chen, S. J., Wang, C. S., Chen, Y. H., & Hwang, Y. L. (2014, September). Hawkeye: Finding spamming accounts. In *Network Operations and Management Symposium (APNOMS), 2014 16th Asia-Pacific*(pp. 1-4). IEEE.

- Livingstone, S., Kirwil, L., Ponte, C., & Staksrud, E. (2014). In their own words: What bothers children online?. *European Journal of Communication*, 29(3), 271-288.
- Locker Ransomware. (2016).www.knowbe4.com. 27 Ekim 2016 tarihinde <https://www.knowbe4.com/locker-ransomware> adresinden erişildi.
- Mert, M., Bülbül, H. İ., & Sağıroğlu, Ş. (2012). Milli eğitim bakanlığına bağlı okullarda güvenli internet kullanımı. *Türk Bilim Araştırma Vakfı Bilim Dergisi*, 5(4), 1-12.
- Mitchell, K. J., Finkelhor, D. ve Wolak, J. (2005). Protecting youth online: Family use of filtering and blocking software. *Child Abuse & Neglect*, 29(7), 753-765. doi:10.1016/j.chiabu.2004.05.008
- Moğol, Ş. H. (2016). *Importance Of Information Security Awareness*. Yıldırım Beyazıt University.
- O’Keeffe, G. S. ve Clarke-Pearson, K. (2011). The impact of social media on children, adolescents, and families. *American Academy of Pediatrics*, 127(4), 800-804. doi:10.1542/peds.2011-0054
- Oğuz, T. (2016). Çağdaş Narkisisos’lar: Facebook Kullanım Alışkanlıkları Ve Narsisizm. *Selçuk Üniversitesi İletişim Fakültesi Akademik Dergisi*, 9(2). Doi:10.18094/Si.33596
- Öğün, M. N. ve Kaya, A. (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler. *Güvenlik Stratejileri Dergisi*, 18(18). doi:10.17752/gsd.50236
- Öğütçü, G. (2010). *E-Dönüşüm Sürecinde Kişisel Bilişim Güvenliği Davranışı Ve Farkındalığının Analizi*. Başkent Üniversitesi.
- Özdemir, M., & Akar, F. (2011). Lise öğrencilerinin siber-zorbalığa ilişkin görüşlerinin bazı değişkenler bakımından incelenmesi. *Kuram ve Uygulamada Eğitim Yönetimi*, 4(4), 605-626.

- Peker, A. (2013). İnsani değerler yönelimli psiko-eğitim programının problemli internet kullanımı ve siber zorbalık üzerindeki etkisi. *University of Sakarya, Educational Science Institute, Sakarya*.
- Seferoğlu, S. S., & Akbıyık, C. (2005). İlköğretim öğretmenlerinin bilgisayara yönelik öz-yeterlik algıları üzerine bir çalışma. *Eğitim Araştırmaları Dergisi*, 19, 89-101.
- Sırakaya, M. (2011). *Öğretmen Adaylarının Problemli İnternet Kullanımı ve İnternet Öz-Yeterlik Düzeylerinin İncelenmesi*. Hacettepe Üniversitesi.
- Söylemez, M. ve Balaman, F. (2015). Bilişimin Etik Olarak Kullanımının Çeşitli Değişkenler Açısından İncelenmesi. *Elektronik Sosyal Bilimler Dergisi*, 54(14), 115–128.
- Staksrud, E., Ólafsson, K. ve Livingstone, S. (2013). Does the use of social networking sites increase children's risk of harm? *Computers in Human Behavior*, 29(1), 40–50. doi:10.1016/j.chb.2012.05.026
- Şiddeti Önleme ve Rehabilitasyon Derneği, Acıbadem Üniversitesi Suç ve Şiddetle Mücadele ve Uygulama ve Araştırma Merkezi. (2016). *Çocuk İstismarına Yönelik Rapor*. İstanbul. <http://imdat.org/wp-content/uploads/2016/05/Çocuk-İstismarina-Yönelik-Rapor.pdf> adresinden erişildi.
- Tanrıverdi, H., & Sağır, S. (2014). Lise Öğrencilerinin Sosyal Ağ Kullanım Amaçlarının Ve Sosyal Ağları Benimseme Düzeylerinin Öğrenci Başarısına Etkisi. *Adıyaman Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 2014(18).
- Tekerek, M. (2008). Bilgi Güvenliği Yönetimi. *KSÜ Fen ve Mühendislik Dergisi*, 11(1), 132–137.
- Tekerek, M., Ercan, O., Udum, M. S., & Saman, K. (2012). Bilişim teknolojileri öğretmen adaylarının bilgisayar öz-yeterlikleri. *Turkish Journal of Education*, 1(2). Doi.10.19128/turje.95804

- Tekerek, M. ve Tekerek, A. (2013). A Research on Students' Information Security Awareness. *Turkish Journal of Education*, 2(3).
- Tercan, İ., Sakarya, S. ve Çoklar, A. N. (2012). Çocukların Gözüyle Onların İnternet Kullanım Profilleri Ve Ailelerin Getirdiği Sınırlamalar: Anamur İlçe Örneği. *New World Sciences Academy*, 7(1), 305–312.
- Timur, B., Yılmaz, Ş. ve Timur, S. (2013). Öğretmen Adaylarının Bilgisayar Kullanımına Yönelik Öz-yeterlik İnançları. *Mersin Üniversitesi Eğitim Fakültesi Dergisi*, 9(1). doi:10.17860/EFD.88438
- Topal, M. ve Akgün, Ö. E. (2015). Eğitim Fakültesinde Okuyan Öğretmen Adaylarının Eğitim Amaçlı İnternet Kullanımı Öz-Yeterlik Algılarının İncelenmesi. *Kastamonu Eğitim Dergisi*, 23(1), 22.
- Tuncer, M. ve Tanaş, R. (2011). Eğitim Fakültesi Öğrencilerinin Bilgisayar Öz-Yeterlik Algılarının Değerlendirilmesi. *Adıyaman Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 4(6), 222–232. doi:10.14520/adyusbd.128
- Türkiye Büyük Millet Meclisi. (2012). *Bilgi toplumu olma yolunda bilişim sektöründeki gelişmeler ile internet kullanımının başta çocuklar, gençler ve aile yapısı üzerinde olmak üzere sosyal etkilerinin araştırılması amacıyla kurulan meclis araştırma komisyonu raporu*. Ankara.
- Türkiye İstatistik Kurumu. (2013). *06-15 Yaş Grubu Çocuklarda Bilişim Teknolojileri Kullanımı*. <http://www.tuik.gov.tr/PreHaberBultenleri.do?id=15866#> adresinden erişildi.
- Türkiye İstatistik Kurumu. (2016). *HaneHalkı Bilişim Teknolojileri Kullanım Araştırması*. www.tuik.gov.tr. Adresinden erişildi.

- Uçkan, Ö. (2012). Dijital Aktivizm mi? Aktivizm mi?. 20 Ekim 2016 tarihinde <https://spotdergi.wordpress.com/2012/05/30/dijital-aktivizm-mi-aktivizm-mi/> adresinden erişildi.
- Valcke, M., De Wever, B., Van Keer, H. ve Schellens, T. (2011). Long-term study of safe Internet use of young children. *Computers and Education*, 57(1), 1292–1305. doi:10.1016/j.compedu.2011.01.010
- Vural, Y., & Sağiroğlu, Ş. (2008). Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme. *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi*, 23(2).
- Wazid, M., Katal, A., Goudar, R. H., & Rao, S. (2013, April). Hacktivism trends, digital forensic tools and challenges: A survey. In *Information & Communication Technologies (ICT), 2013 IEEE Conference on* (pp. 138-144). IEEE.
- We Are Social. (2017). Digital in 2017. 10 Şubat 2017 tarihinde <https://wearesocial.com/special-reports/digital-in-2017-global-overview> adresinden erişildi.
- www.bthaber.com. (2016). Sosyal Medya ve Zararlı Yazılımlar: Riskler Nedir ve Nasıl Ele Alınmalıdır? 24 Eylül 2016 tarihinde <http://www.bthaber.com/guvenlik/sosyal-medya-ve-zararli-yazilimlar-riskler-nedir-ve-nasil-ele-alinmalidir/1/18980> adresinden erişildi.
- Yalnız, A. (2014). Akademik Öz-Yeterlik: Olumlu ve Olumsuz Duygulanımın Yordayıcı Rolü. *Eğitim ve Öğretim Araştırmaları Dergisi*, 3(2), 95-100.
- Yegen, C. (2014). Dijital Aktivizmin Bir Türü Olarak Hacktivizm ve "RedHack". *International Journal of Intermedia*, 1(1), 118.
- Yenilmez, Y. ve Seferoğlu, S. S. (2013). Sanal Zorbalık ve Öğretmenlerin Farkındalık Durumlarına Bir Bakış. *Eğitim ve Bilim*, 169(38), 420–432

- Yetim, S. (2015). Siber zorbalık, Türkiye ve ABD karşılaştırması (ABD v. Drew dosyası). *Türkiye Barolar Birliği Dergisi*, 120, 325-384.
- Yıldırım, A. (2014). İnternetin Görünen Yüzü. *Karamanoğlu Mehmetbey Üniversitesi Sosyal Ve Ekonomik Araştırmalar Dergisi*, 2014(3), 51-59.
- Yılmaz, E., Şahin, Y., Haseski, H. ve Erol, O. (2014). Lise öğrencilerinin internet bağımlılık düzeylerinin çeşitli değişkenlere göre incelenmesi: Balıkesir ili örneği. *Eğitim Bilimleri Araştırmaları Dergisi*, 4(1), 133–144. doi:10.12973/jesr.2014.41.7
- Yılmaz, E., Şahin, Y. L. ve AKbulut, Y. (2016). Öğretmenlerin Dijital Veri Güvenliği Farkındalığı. *Sakarya University Journal of Education*, 6(2), 26–45.
- Yılmaz, G. K., Yılmaz, R. ve Sezer, B. (2014). Üniversite Öğrencilerinin Güvenli Bilgi ve İletişim Teknolojisi Kullanım Davranışları ve Bilgi Güvenliği Eğitimine Genel Bir Bakış. *Bartın Üniversitesi Eğitim Fakültesi Dergisi*, 3(1), 176–176. doi:10.14686/BUEFAD.201416213

EK 1. Öğrencilerin Güvenli İnternet Kullanımına Yönelik Öz-Yeterlik Algıları Ölçeği

Değerli Öğrenciler,

Kuzey Kıbrıs Türk Cumhuriyeti sınırları içerisindeki orta öğretim ve mesleki teknik dairesine bağlı bulunan okullarda öğrenim gören öğrenciler için oluşturulan **“öğrencilerin güvenli İnternet kullanımına yönelik öz-yeterlik algılarını belirlemek” isimli** anketi size en yakın olan seçeneği işaretleyerek cevaplamanız beklenmektedir. Anket sonuçları sadece araştırma raporu için kullanılacaktır. Kesinlikle herhangi bir birime/kuruma vs. verilmeyecektir. Araştırmamıza katıldığınız için teşekkür ederiz.

Mehmet Karabulut

Yrd. Doç. Dr. ERİNÇ ERÇAĞ

Kişisel Bilgi Formu

- 1.Cinsiyetiniz: ☐ Kız ☐ Erkek
2. Yaşınız:
- 3.Okulunuz:
- 4.Okulunuzun bulunduğu ilçe:
☐ Lefkoşa ☐ Girne ☐ Gazimağusa ☐ Güzelyurt ☐ İskele
5. Sınıfınız:
6. İnternete bağlanmak için kullandığınız yöntem:
☐ ADSL ☐ 3G ☐ Wireless ☐ Modem ☐ Diğer (Lütfen belirtiniz) :
7. İnternete nereden erişim sağlıyorsunuz? (Birden fazla seçeneği işaretleyebilirsiniz.)
☐ Kişisel bilgisayarımdan ☐ Okulumdan ☐ İnternet kafeden
☐ Cep telefonumdan ☐ Diğer (Lütfen belirtiniz) :
8. İnternet erişimini hangi cihazlar aracılığı ile sağlıyorsunuz? (Birden fazla seçeneği işaretleyebilirsiniz.)
☐ Tablet ☐ PDA ☐ PC ☐ Laptop
9. Haftalık İnternet kullanma süreniz kaç saattir?
☐ 4 saatten az ☐ 4 ile 12 saat arası ☐ 13 ile 27 saat arası ☐ 28 saatten fazla

Lütfen her maddeye ilişkin yeterlik durumunuzu yanda verilen “Tamamen Yeterliyim” , “Yeterliyim”, “Orta Düzeyde Yeterliyim”, “Yetersizim”, “Tamamen Yetersizim” yazan seçeneklerden uygun olanını X işareti koyarak belirtiniz. Hiçbir maddeyi boş bırakmayınız.	Tamamen yeterliyim	Yeterliyim	Orta düzeyde yeterliyim	Yetersizim	Tamamen yetersizim
SOSYAL AĞLARDA GÜVENLİK (SOSYAL MEDYADA GÜVENLİK)					
1. Sosyal paylaşım ağlarında paylaştığım bilgileri, istemediğim kişilerden gizleyebilme					
2. Sosyal paylaşım ağlarında tanımadığım/istemediğim kişilerden gelen istekleri engelleyebilme					
3. Sosyal paylaşım ağlarında kişisel bilgilerimi, istemediğim kişilerden gizleyebilme					
4. Sosyal paylaşım ağlarında güvenlik tehlikesi açısından paylaştığım bilgileri koruyabilme					
5. Sosyal paylaşım ağlarındaki şifremin çalınması durumunda gerekli başvuruları ilgili yerlere yapabilme					
6. Sosyal paylaşım ağlarında video, fotoğraf gibi kişiliğime zarar vermeyecek bilgiyi paylaşabilme					
7. Sosyal paylaşım ağlarında başkalarının kişiliğine zarar vermeyecek bilgiyi paylaşabilme					
8. Facebook, Twitter gibi sosyal paylaşım ağlarını güvenli bir şekilde kullanabilme					
9. Sosyal ağlarda paylaşılan virüslü videolardan korunabilme					
10. Sosyal paylaşım ağlarında güvenlik açıklarına karşı tedbir alabilme					
11. Sosyal paylaşım ağlarında fotoğraf albümlerimin çalınmasını engelleyebilme					
12. Sosyal paylaşım ağlarında güçlü şifre oluşturabilme					
ZARARLI YAZILIMLAR					
13. Zararlı yazılımların bilgisayara bulaşmasını engelleyebilme					
14. Tuş Kaydediciler (Keylogger) şifrelerimi koruyabilme					
15. Zararlı yazılımlar bilgisayara bulaştığı zaman temizleyebilme					
16. Virüslerin bilgisayara bulaşmaması için gereken güvenlik önlemlerini alabilme					
17. Solucanlara (Worm) karşı korunabilme					
18. Trojan'lerin (TruvaAtı'nın) bilgisayara bulaşmaması için gereken güvenlik önlemlerini alabilme					
19. Spyware'lara (Casus Yazılımlara) karşı korunabilme					
20. Microsoft Security Essentials programını kullanabilme					
WEB GÜVENLİĞİ ve SOSYAL MÜHENDİSLİK					
21. İnternet'te güvenli alış-veriş yapabilme					
22. Spam (gereksiz) e-postalarına karşı önlem alabilme					
23. Kameralı kalemler, kameralı gözlükler gibi sosyal mühendislik donanımlarından korunabilme					
24. İnteraktif bankacılık işlemlerini yaparken güvenlik önlemlerini alabilme					
25. Hoax (Aldatmaca) e-posta yöntemi konusunda gereken önlemleri alabilme					
26. Phishing (Oltalama/sahte) e-postalarına karşı kendini koruyabilme.					
27. Güçlü parola oluşturabilme					
28. HTTP ile HTTPS arasındaki farkı ortaya koyabilme					
29. E-posta ile yapılan sosyal mühendislik saldırılarına karşı korunabilme					

BİLGİSAYAR GÜVENLİĞİ					
30. Kişisel dosyalarımı koruyabilme					
31. Windows işletim sistemine şifre koyabilme					
32. Bilgisayar için gerekli giriş güvenlik önlemlerini alabilme					
33. Güvenlik yazılımlarını gerektiğinde güncelleyebilme					
34. Dosyaları şifreleyebilme					
35. Bilgi kaybının yaşanmaması için dosyaları belirli aralıklarla yedekleyebilme					

EK 2. Genel Ortaöğretim Dairesinden Alınan İzin Belgesi



**KUZEY KIBRIS TÜRK CUMHURİYETİ
MİLLÎ EĞİTİM BAKANLIĞI
GENEL ORTAÖĞRETİM DAİRESİ MÜDÜRLÜĞÜ**

GOÖ.0.00.35-A/15/16-4881

07.12.2015

ı Mehmet Karabulut,

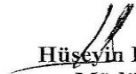
İlgi: 01.12.2015 tarihli başvurunuz.

Talim ve Terbiye Dairesi Müdürlüğü'nün TTD.0.00.03-12-15/1628 sayı ve 04.12.2015 tarihli uyarınca "Öğrencilerin Güvenli İnternet Kullanımına Yönelik Öz-Yeterlik Algıları" konulu anın gizlilik ve gönüllülük ilkelerine riayet edilerek uygulanması müdürlüğümüze uygun müştür.

Ancak çalışmayı uygulamadan önce çalışmaya katılacak olanların bağlı bulunduğu okul rlüğüyle istişarede bulunulup, çalışmanın hangi okulda ne zaman uygulanacağı birlikte malıdır.

Çalışmayı uyguladıktan sonra sonuçlarının Talim ve Terbiye Dairesi Müdürlüğü'ne ılması yasa gereğidir.

Bilgilerinize saygı ile rica ederim.


Hüseyin Kavaz
Müdür

EK 3. Mesleki Teknik Öğretim Dairesinden Alınan İzin Belgesi



**KUZEY KIBRIS TÜRK CUMHURİYETİ
MİLLİ EĞİTİM BAKANLIĞI
MESLEKİ TEKNİK ÖĞRETİM DAİRESİ MÜDÜRLÜĞÜ**

Sayı: MTÖ.0.00-13-15/ 3119

07 Aralık 2015

Sn. Mehmet Karabulut
Yakın Doğu Üniversitesi,

İlgili yazınızda, müdürlüğümüze bağlı okullarda öğrencilere yönelik olarak “Öğrencilerin Güvenli İnternet Kullanımına Yönelik Öz-Yeterlik Algıları” konulu anket uygulama istemiyle izin talebinde bulundunuz.

Talebinizle ilgili olarak Talim ve Terbiye Dairesi Müdürlüğü ‘nce yapılan incelemede, çalışmanın gizlilik ve gönüllük ilkelerine riayet edilerek uygulanması uygun görülmüştür. Ancak uygulanmadan önce ilgili okul müdürlükleri ile istişarede bulunup anketin ne zaman uygulanacağı birlikte saptanmalıdır. Keza, anket yapıldıktan sonra da sonuçlarının Talim ve Terbiye Dairesi Müdürlüğü’ ne de ulaştırması gerekmektedir.

Bilgi edinmenizi ve gereğini saygı ile rica ederim.


Ayhan Şirket
Müdür

AŞ/ZL

Tel (90) (392) 228 22 57
Fax (90) (392) 227 87 27
E-Mail meb@mebnet.net

Lefkoşa-KIBRIS

ÖZGEÇMİŞ

Adı, Soyadı: Mehmet Karabulut

Doğum Tarihi: 1 Nisan 1989

Akademik Düzey: Lisans

Adres: Cemal Hamit Sok. Aldora 3. Sitesi 25/6 Hamitköy/Lefkoşa

Medeni Durum: Bekar

Yabancı Dil: İngilizce

Eğitim

2013- 2017 Yakın Doğu Üniversitesi BÖTE Yüksek Lisans

2010 -2013 Yakın Doğu Üniversitesi BÖTE Lisans

2004 -2007 Sedat Semavi Endüstri Meslek Lisesi- Bilgisayar Donanım ve Yazılım Bölümü

Güvenli İnternet Kullanımı

ORIGINALITY REPORT

% 4	%	% 4	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

- 1** TUNCER, Murat and ÖZÜT, Aytaç. "Sınıf öğretmenleri adaylarının eğitsel internet kullanımına yönelik öz-yeterlik inançları", Erzincan Üniv. Fen Edebiyat Fak. Türk Dili ve Edebiyatı Bl., 2012. %**1**

Publication
- 2** KAHRAMAN, Sakıp, YILMAZ, Zeynel Abidin, ERKOL, Mehmet and YALÇIN ALTUN, Sema. "Investigation of pre-service teachers' self-efficacy beliefs of educational internet use", Öğretmen Eğitimi Akademisi-Maya Akademi, 2013. <%**1**

Publication
- 3** Bayzan, Şahin and Özbilen, Alper. "DÜNYADA İNTERNETİN GÜVENLİ KULLANIMINA YÖNELİK UYGULAMA ÖRNEKLERİ VE TÜRKİYE'DE BİLİNÇLENDİRME FAALİYETLERİNİN İ..", e-Journal of New World Sciences Academy (NWSA), 2012. <%**1**

Publication
- 4** KAŞIKCI, Duygu Nazire, ÇAĞILTAY, Kürşat, KARAKUŞ, Türkan, KURŞUN, Engin and <%**1**