T.C.

SAKARYA ÜNİVERSİTESİ
EĞİTİM BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ
ANABİLİM DALI
BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ
BİLİM DALI

LİSE ÖĞRENCİLERİNİN SİBER ZORBALIK DUYARLILIĞININ RİSKLİ DAVRANIŞ, KORUMACI DAVRANIŞ, SUÇA MARUZİYET VE TEHLİKE ALGISI İLE İLİŞKİSİ VE ÇEŞİTLİ DEĞİŞKENLER AÇISINDAN İNCELENMESİ

YÜKSEK LİSANS TEZİ

HÜSEYİN KINAY

HAZİRAN 2012

SAKARYA ÜNİVERSİTESİ
EĞİTİM BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ
ANABİLİM DALI
BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ
BİLİM DALI

LİSE ÖĞRENCİLERİNİN SİBER ZORBALIK DUYARLILIĞININ RİSKLİ DAVRANIŞ, KORUMACI DAVRANIŞ, SUÇA MARUZİYET VE TEHLİKE ALGISI İLE İLİŞKİSİ VE ÇEŞİTLİ DEĞİŞKENLER AÇISINDAN İNCELENMESİ

YÜKSEK LİSANS TEZİ

HÜSEYİN KINAY

DANIŞMAN:

YRD. DOÇ.DR. M. BARIŞ HORZUM

ORTAK DANIŞMAN:

DOÇ.DR. O. TOLGA ARICAK

HAZİRAN 2012

BİLDİRİM

Hazırladığım tezin tamamen kendi çalışmam olduğunu, akademik ve etik kuralları gözeterek çalıştığımı ve her alıntıya kaynak gösterdiğimi taahhüt ederim.

İmza

Hüseyin Kınay

JÜRİ ÜYELERİNİN İMZA SAYFASI

'Lise Öğrencilerinin Siber Zorbalık Duyarlılığının Riskli Davranış, Korumacı Davranış, Suça Maruziyet Ve Tehlike Algısı İle İlişkisi Ve Çeşitli Değişkenler Açısından İncelenmesi' başlıklı yüksek lisans tezi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim/bilim Dalında jürimiz tarafından kabul edilmiştir.

Başkan .....

Doç. Dr. Mustafa KOÇ

Üye .....

Yrd. Doç. Dr. Mübin KIYICI

Üye.....

Yrd. Doç. Dr. Tuncay AYAS

Ortak Danışman.....

Doç. Dr. O. Tolga ARICAK

Danışman.....

Yrd. Doç. Dr. Mehmet Barış HORZUM

Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım.

13/07/2012

Yrd. Doç. Dr. Mehmet Barış HORZUM

Enstitü Müdür V.

ÖNSÖZ

Teknolojinin insan hayatına olan etkisi arttıkça her türlü ihtiyacı gidermek için geliştirilen uygulamaların da güvenlik açıklarının arttığını görmekteyiz. Ayrıca hayatın her alanına giren, tercihlerimizde bize yardımcı olan yeni bir web dünyası ile birlikte bilgiye kolay yoldan ulaşmak ve ihtiyacının bir tıkla giderilmesini isteyen bir nesil yetişmektedir. Gençlerin çoğu bilgisayar başına oturduğunda istediği bilgiye ulaşmak için her türlü siteyi gezmekte, kendisine sunulan uygulamaları denemektedir. Özellikle öğrencilerimden birçoğunun sosyal paylaşım sitelerinde kişisel bilgilerini paylaştığını gördüğümde böyle bir çalışmanın gerekliliğini hissettim. Araştırmam boyunca desteğini esirgemeyen danışman hocam Yrd. Doç. Dr. M. Barış Horzum'a, siber zorbalık konusuyla tanışmamı sağlayan ve beni ekibine dâhil eden eşdanışmanım Doç. Dr. O. Tolga Arıcak'a ve ekip arkadaşım Öğr. Gör. Taşkın Tanrıkulu'ya teşekkürü bir borç bilirim.

Hüseyin Kınay

20.06.2012

ÖZET

LİSE ÖĞRENCİLERİNİN SİBER ZORBALIK DUYARLILIĞININ RİSKLİ DAVRANIŞ, KORUMACI DAVRANIŞ, SUÇA MARUZİYET VE TEHLİKE ALGISI İLE İLİŞKİSİ VE ÇEŞİTLİ DEĞİŞKENLER AÇISINDAN İNCELENMESİ

Kınay, Hüseyin

Yüksek Lisans Tezi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı, Bilgisayar ve Öğretim Teknolojileri Öğretmenliği

Danışman: Yrd. Doç. Dr. M. Barış Horzum

Ortak Danışman: Doç. Dr. O. Tolga Arıcak

Haziran, 2012. xvi+81 Sayfa

Bu araştırma, günümüzde oldukça önemli olan ve özellikle gençler ve çocuklarda oldukça sık karşılaşılan bilgi güvenliği ile alakalı davranışları tespit etmek, bilgi güvenliği konusuna dikkat çekmek ve siber zorbalık duyarlılığının bilgi güvenliği ile ilişkisini incelemek amacıyla yapılmıştır.

Araştırma, genel tarama modeli türlerinden ilişkisel tarama modeline göre yürütülmüştür. İlişkisel tarama modelinin yanında kesitsel modelden de yararlanılmıştır. Araştırmanın bağımlı değişkenleri riskli davranış, tehlike algısı, suça maruziyet, korumacı davranış ve siber zorbalığa ilişkin duyarlılıktır, bağımsız değişkenleri ise cinsiyet, yaş, internet kullanım süresi, öğrenim görülen alan ve güvenlik eğitimi alıp almama durumudur. Araştırmanın katılımcılarını İstanbul ilinde çeşitli ortaöğretim okullarında okuyan 180'i erkek, 188'i kadın 368 öğrenci oluşturmaktadır.

Araştırmada elde edilen veriler, pearson korelasyon analizi, t-test, tek yönlü ANOVA ve aşamalı regresyon analizi yapılarak incelenmiştir. Araştırma sonuçlarına göre tehlike algısı ve suça maruziyetin siber zorbalığa ilişkin duyarlılığı anlamlı düzeyde yordadığı görülmüştür. Araştırma sonucunda erkek öğrencilerin kadın öğrencilere göre bilgisayar ve internet kullanımında daha fazla riskli davranış gösterdiği aynı zamanda daha korumacı davrandığı da görülmektedir. Bununla birlikte erkek

öğrencilerin kadın öğrencilere göre daha çok suça maruz kaldığını ve tehlike algılarının da daha yüksek olduğu ortaya çıkmıştır. Son olarak Siber zorbalığa ilişkin duyarlılıkta ise kadın öğrencilerin erkek öğrencilere göre daha duyarlı olduğu görülmektedir. Ayrıca öğrencilerin yaşları arttıkça riskli davranış puanlarının arttığı ortaya çıkmıştır. Sosyal bilimler alanını seçen öğrencilerin bütün ölçek puan türlerinde en yüksek puanları aldıkları bulunmuştur. Daha önce güvenlik eğitimi alan öğrencilerin riskli davranış puanları almayan öğrencilere göre daha yüksektir. Ayrıca korumacı davranış puanlarında da güvenlik eğitimi almış öğrencilerin puanları, güvenlik eğitimi almamış öğrencilerin puanlarına göre daha yüksektir. Araştırmaya katılan lise öğrencilerinden interneti günlük ortalama olarak 1 saatten az kullanan öğrencilerin Riskli Davranış Puanı, Korumacı Davranış Puanı, Suça Maruziyet Puanı ve Tehlike Algısı Puanları en düşük olmasına rağmen Siber zorbalığa ilişkin duyarlılıklarının en yüksek olduğu bulunmuştur.

Anahtar Kelimeler: Siber zorbalık duyarlılığı, bilgi güvenliği, aşamalı regresyon analizi

ABSTRACT

AN ANALYSIS OF THE RELATION BETWEEN CYBERBULLYING SENSIBILITY AND RISK BEHAVIOUR, CONSERVATIVE BEHAVIOUR, EXPOSURE TO OFFENCE AND RISK PERCEPTION AND IN RELATION TO VARIOUS VARIABLES OF LYCEE STUDENTS

Kınay, Hüseyin

Master Thesis, Computer Education and Instructional Technology Department, Computer Education and Instructional Technology

Supervisor: Assist. Prof. Dr. M. Barış Horzum

Co-Advisor: Assoc. Prof. Dr. O. Tolga Arıcak

June, 2012. xvi+81 Pages

This research is conducted to identify behaviors associated with information security which are very important today and quite frequently encountered in especially children and adolescents and to draw attention to the issue of information security and to examine the relationship between information security and cyberbullying sensibility.

The research was carried out according to general survey models correlational survey model type. Besides the correlational model, cross-sectional model was also benefited. Dependent variables of research are risk behaviour, risk perception, exposure to offence, conservative behaviour and sensibility against cyberbullying, independent variables are gender, age, internet usage time, education field and to have a security training. 368 students including 180 male and 188 female students who are studying various secondary schools of Istanbul province are participants of this research.

Data which was obtained in this study were analyzed with pearson correlational test, t-test, one way ANOVA and stepwise regression analysis. As a result of the research, concerning risk perception and exposure to offence are both significant predict of sensibility against cyberbullying. Result of the research, male

students behave more conservative but also more risky behaviour than female students in the use of computers and the internet. However, male students exposed to a crime and risk perception turned out to be higher than female students. Finally, female students are more sensitive than male students in the cyber-bullying sensibility. Also, as the age of students' scores increased risky behavior emerged. Students who are taking the social sciences, received the highest scores of all kind of scale points. Students who had a security training have higher risky and conservative behaviour scores. Although lycee students who participated in research and used the internet less than 1 hour per day on average have lowest scores of risky behaviour, conservative behaviour, exposure to offence and risk perception, cyberbullying sensibility scores are the highest.

Keywords: Cyberbullying sensibility, information security, stepwise regression analysis

İÇİNDEKİLER

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

BÖLÜM I: GİRİŞ

Güvenlik insanlar için her zaman gereksinim duyulan ihtiyaçlardan biridir. İnsanlar kişisel bilgilerini ya da eşyalarını güvenli yerlere koymaya çalışırlar. Bilgi ise güvenle saklanması ve korunması gereken bir nesnedir. Bize ait bilgilerin başkaları tarafından bilinmesi bilgi güvenliğini zedeler ve tehlike altına girebiliriz.

Bilginin korunacak temel nitelikleri ISO/IEC 27001 bilgi güvenliği standardında şu şekilde bahsedilmektedir (Şahinaslan ve diğ., 2009):

Gizlilik: Bilginin yetkili olmayan kişiler, varlıklar ve süreçler tarafından erişilemez ve ifşa edilemez niteliği,

Doğruluk, **Bütünlük ve Özgünlük**: Bilginin doğruluk, bütünlük ve kendisine has özelliklerinin korunması,

Kullanılabilirlik (**erişilebilirlik**): Bilginin yetkili kişiler (görevi gereği) tarafından istenildiğinde ulaşılabilir ve kullanılabilir olma özelliğidir.

Bilgi güvenliği bu sayılan özelliklerin güvenliğinin sağlanması anlamını taşımaktadır. Bilgi güvenliğini, kişiler, şirketler ve hatta ülkeler göz ardı edememekte ve gün geçtikçe de önemi artmaktadır. Yaklaşık olarak 10-15 yıl kadar önce bilgi güvenliği çok deneyimli, yazılım bilgisi güçlü insanlar tarafından sağlanabiliyordu. Bilinen hacker sayısı sınırlıydı.

Bilgi ve iletişim teknolojilerinin hızla gelişmesi, beraberinde insanları teknolojiye ve internete bağımlı hale getirdi. Bireyler artık internet sayesinde bilgiye hızlıca ulaşabilir, bankacılık işlemlerimizi kısa sürede yapabilir, yol durumunu öğrenebilir, uzaktan eğitim alabilir ve daha pek çok işlem yapılabilir hale geldi. İnternetin sağladığı bu avantajların yanında bazı güvenlik zaaflarını da beraberinde getirdi. Kötü niyetli bazı kişiler interneti kullanarak zarar vermeye başladılar. Bazen suçlular, bilgisayar ve yazılım becerileri yüksek bireyler arasından çıkarken bazen de

internetten bulduğu birkaç programla arkadaşına zarar vermeye çalışan lise öğrencileri arasından çıktığı görülmüştür.

Sanal dünyayı zarar vermek amacıyla kullanan bireyler sadece kişiler için tehdit unsurları olmakla kalmayıp aynı zamanda şirketler içinde büyük sorunlar oluşturabilir. Gelişen teknolojiyle birlikte şirketler daha büyük ağlar, daha karmaşık sistemler ve yazılımlar kullanmaya başlamışlar ve işlemlerinin çok büyük kısmını bilgisayar sistemleri üzerine kurmuşlardır. Bu büyüme arttıkça hâkimiyet kurmak zorlaşmış ve güvenlik zafiyetleri ortaya çıkmaya başlamıştır (Burlu, 2010).

Web 1.0 teknolojilerinin sağlayabildiği tek yönlü iletişimden sonra web 2.0 teknolojilerinin katılımcı ve kolay kullanımı desteklemesi ile bilgi paylaşımı hızla artmaktadır. Yeterli internet ve bilgisayar süpervizyonuna sahip olmayan son kullanıcıların (end-user) paylaştığı değerli bilgiler bilgi güvenliği konusuna dikkat çekmektedir. İnternette başka kullanıcılara zarar vermeye yönelik saldırılar gün geçtikçe artarken saldırganlar tarafından ihtiyaç duyulan teknik, bilgi ve yetenekler giderek azalmaktadır.

Kaçakçılık ve Organize Suçlarla Mücadele (KOM) Daire Başkanlığı'nın 2011 raporuna göre yıl içerisinde ülkemizde bilişim suçlarıyla ilişkili 3901 olay gerçekleşmiş ve 4157 şüpheli şahıs hakkında işlem yapılmıştır. Bu olaylardan, banka ve kredi kartı dolandırıcılığı 1819, interaktif banka dolandırıcılığı 148, bilişim sistemlerine karşı işlenen suçlar 1791, internet aracılığıyla nitelikli dolandırıcılık 112 ve diğer olaylar 31 kez işlenmiştir. Şüpheli sayısı ise banka ve kredi kartı dolandırıcılığında 1503, interaktif banka dolandırıcılığında 348, bilişim sistemlerine karşı işlenen suçlarda 898, internet aracılığıyla nitelikli dolandırıcılıkta 285 diğer olaylarda ise 123 kişi hakkında işlem yapılmıştır (KOM, 2011). Bu bilgilerin gençlerde ve çocuklarda ne durumda olduğunun araştırılıp ortaya konulması da önemlidir.

CSI ve FBI kurumlarının 2008 yıllarında ortak yaptıkları bir çalışmanın sonuçlarına göre (Richardson, 2008; Akt. Eminağaoğlu ve Gökşen, 2009) ABD'deki 522 kurumun (devlet veya özel) %49'unda virüs, truva atı, solucan vb. zararlı kod saldırısı yaşanmıştır. Dünya genelinde Symantec tarafından yapılmış bir araştırmaya göre 2008 yılı boyunca saptanan tüm saldırıların nerdeyse %90'ı kullanıcıya ait kritik bilgilerin çalınması amacını taşımaktadır (Eminağaoğlu ve Gökşen, 2009).

Klavyeden basılan tuşların kaydedilmesi yolu ile çevrim içi banka hesap bilgilerinin çalınmasına yönelik tehditler, saldırıların %76'sını oluşturmaktadır ki bu oran 2007 yılında %72 olarak saptanan oranla kıyaslandığında, bir senede yaşanan artışı açıkça ortaya koymaktadır (Symantec,2009).

Symantec tarafından sunulan 2009 raporunda Türkiye'de bir önceki yıla göre spam mail sayısı 12 kat artarak bölgesinde ikinci sıraya yükselmiştir. Aynı raporda sunulan başka bir bilgi de 2008 yılında virüs gibi zararlı kodların üretildiği ve yayılma kaynağı olarak çıktığı ülkeler arasında Türkiye, bulunduğu bölge (Avrupa-Orta Doğu) itibariyle ikinci sırada yer almaktadır (Symantec, 2009). Raporda bahsedilen 2007 ve 2008'de Dünya genelinde zararlı kodların türlerine göre ülkeler arası sıralama Tablo 1, Dünya geneli ve Avrupa-Orta Doğu bölgesinde spam e-posta oranları ve sıralamaları Tablo 2 ve truva atı, virüs, arka kapı ve solucan tipinde zararlı kod saldırılarında ilk 3 sıradaki ülkeler Tablo 3'de yer almaktadır.

Tablo 1. 2007 ve 2008'de Dünya Genelinde Zararlı Kodların Türlerine Göre Ülkeler Arası Sıralama

2008 Tüm Saldırı Türleri Dünya Sıralaması	2007 Tüm Saldırı Türleri Dünya Sıralaması	Ülke	2008 yılı tüm saldırı türleri içinde oranı	2007 yılı tüm saldırı türleri içinde oranı	Zararlı Kod	Spam Yayıcı Sistem	Phishing (Oltalama) Web siteleri	Bot sistemler	Tüm Saldırılar Geneli
1	1	ABD	23	20	1	3	1	2	1
2	2	Çin	9	11	2	4	6	1	2
3	3	Almanya	6	7	12	2	2	4	4
4	4	İngiltere	5	4	4	10	5	9	3
5	5	Brezilya	4	3	16	1	16	5	9
6	6	İspanya	4	3	10	8	13	3	6
7	7	İtalya	3	3	11	6	14	6	8
8	8	Fransa	3	4	8	14	9	10	5
9	9	Türkiye	3	2	15	5	24	8	12
10	10	Polonya	3	2	23	9	8	7	17

Tablo 2. Dünya Geneli ve Avrupa-Orta Doğu Bölgesinde Spam E-posta Oranları ve Sıralamaları

2008 Avrupa ve Ortadoğu Sıralaması (spam)	2007 Avrupa ve Ortadoğu Sıralaması (spam)	2008 yılı Dünya geneli spam sıralaması	Ülkeler	2008 Avrupa ve Ortadoğu Spam Oranları (%)	2007 Avrupa ve Ortadoğu Spam Oranları (%)
1	1	2	Rusya	14	10
2	2	3	Türkiye	13	4
3	3	6	İngiltere	7	15
4	4	7	Almanya	6	9
5	5	8	İtalya	6	6
6	6	9	Polonya	6	10
7	7	10	İspanya	5	6
8	8	13	Fransa	5	6
9	9	19	Romanya	3	1
10	10	20	Hollanda	3	1

Tablo 3. Truva Atı, Virüs, Arka kapı ve Solucan Tipinde Zararlı Kod Saldırılarında İlk 3 Sıradaki Ülkeler

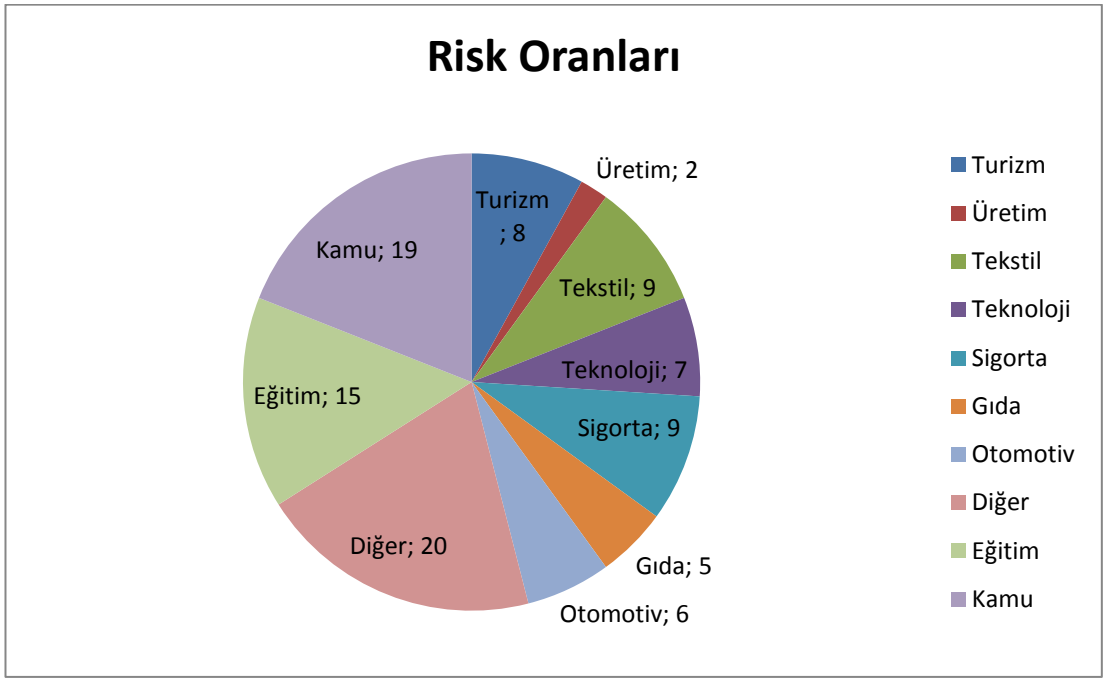
Sıralama	Zararlı kod türlerinde ilk 3 sıra (Avrupa ve Ortadoğu bölgesi geneli)			
	Arka Kapı	Truva Atı	Virüs	Solucan
1	İngiltere	İngiltere	Mısır	Suudi Arabistan
2	İspanya	Fransa	Türkiye	İngiltere
3	Fransa	Almanya	İngiltere	İspanya

Tablo 1, 2 ve 3'te yer alan bilgiler yabancı kuruluşların çalışmalarının sonuçlarını içermektedir. Türkiye'de de bu konu ile ilgili yapılan bazı çalışmalar bulunmaktadır. Ülkemizde yapılan çalışmalardan biri Koç.net şirketinin yapmış olduğu 1025 internet kullanıcısı ve 850 şirketin kapsandığı araştırmadır. Bu araştırmada (Eminağaoğlu ve Gökşen, 2009):

- İnternet erişimlerinde %65 oranında güvenlik duvarı kullanılmadığı;
- Web sunucularının %43'ünün bilgileri kolaylıkla çalınabilir, ana sayfaları değiştirilebilir veya başka bir adrese yönlendirilebilir durumda olduğu;

- İnternet kullanıcılarının sadece %30'unun casus yazılımlara karşı önlem aldığı;
- Alan adı hizmeti veren sunucuların %22'sinde ki açıklardan dolayı şirketlerin e-posta hesapları ele geçirilebilir veya çalışanların internet üzerinden yaptığı bankacılık şifreleri çalınabilir durumda olduğu;
- Tüm açıkların %19'unu kritik açıklar, %28'ini orta düzey açıklar olduğu saptanmıştır.

Bu araştırma sonucunda elde edilen bulgular araştırma kapsamında ki kullanıcıların yarısına yakınının bilgi güvenliği açısından risk altında olduğunu göstermektedir. Sektörlere göre risk oranları aşağıda Şekil 2'de yer almaktadır (Koç.net, 2005; Akt. Eminağaoğlu ve Gökşen, 2009).



Şekil 1. Sektörlere Göre Risk Oranları

Şekil 1'de verilen oranlara bakıldığında "Eğitim" sektörünün tüm risklerin %15'ini içerdiği görülmektedir. Eğitim sektöründe bulunan bu risk daha çok çocukları ve gençleri etkilemektedir. Ayrıca çocukların ve gençlerin internet ve bilgisayar kullanımında gerek ebeveynlerinden gerekse okullarından yeterli bilgi almamaları onları bilinçsiz bir kullanıma sürükleyebilmektedir. Çocuklar ve gençler siber

ortamlarda gezinirken bilgisayara, kendilerine ve ebeveynlerine verebilecekleri zararları düşünmeyebilmektedirler. Örnek olarak indirdikleri bir oyunda virüs, casus yazılım gibi zararlı yazılımlar bulunabilir ve bunun farkında olmayabilirler (Canbek ve Sağıroğlu, 2007).

WorldTracker tarafından sunulan en çok arama yapılan 200 anahtar sözcüğün 82'si pornografi ile ilgilidir. Web sitelerin %12'sinin pornografi içerikli site olduğu göz önüne alınırsa bu tür içeriklere çocukların ve gençlerin erişimi oldukça sakıncalıdır (Canbek ve Sağıroğlu, 2007). Bu sitelerin kullanım sıklığını bilen kötü niyetli kişilerde zararlı yazılımlarını özellikle bu sitelerde deneyebilmektedir.

Conference Board ve TNS şirketinin 10.000 ev sahibi üzerinde yaptığı ankette katılımcıların %41'inin okul çağında çocuğu olduğu ve bu ailelerin %56'sı çocuğunun kendi yaşına uygun içeriğe sahip sitelere girdiğini düşünürken, geriye kalan katılımcıların ise çocuklarının kişisel bilgilerinin ve kimlik bilgilerinin çalınmasından endişe ettikleri görülmüştür (Chai, Bagchi-Sen, Morrell, Rao ve Upadhyaya, 2006).

Çocukların ve gençlerin bilgisayar ve internet kullanımı esnasında karşılaşabilecekleri sorunlar genel olarak şu şekilde sıralanabilir (Canbek ve Sağıroğlu, 2007):

- Teknik zararlar: Çocukların bilgisayarlara zararlı yazılımlar bulaştırması, bilgisayarı bozması gibi zararlardır. Teknik zararlar sonucunda bilgisayarda bulunan belgeler, dosyalar ve diğer bilgiler zarar görebilir ya da yazılım ve sürücü ayarları bozulabilir.
- Fiziksel, sosyal ve psikolojik zararlar: İnternet ve bilgisayarın aşırı derecede kullanımı, oyun oynamak gibi aktiviteler çocukları ve gençleri asosyal birer birey haline getirebilmektedir.
- Hayati zararlar: Zararlı sitelere erişim, çocuk istismarına ve pedofili gibi durumlara neden olmaktadır.

Bu zararlardan korunabilmek ve güvenli bir teknoloji kullanımı oluşturabilmek amacıyla bir siber güvenlik kültürünün oluşturulması önemli bir durumdur. OECD tarafından 25 Temmuz 2002 tarihinde kabul edilmiş dokuz ilke siber güvenlik kültürünün oluşturulması konusunda kabul görülen ilkelerdir. Bu dokuz ilkeden biri

de “bilgi sistemlerinin ve şebekelerin güvenliğinin gerekliliği ve güvenliğin artırılması için neler yapılabileceğine dair farkındalıktır” (Ulaşanoğlu ve diğ, 2010).

Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı (2011) tarafından bilişim suçları ile mücadele ile ilgili çeşitli çalışmalar ve projeler yürütülmektedir. Avrupa ülkeleri arasındaki işbirliğinin artırılması amacıyla Avrupa Konseyi tarafından yürütülen “Cybercrime@IPA-Güney Doğu Avrupa’da Siber Suçlara Karşı Bölgesel İşbirliği” başlıklı projede ülkemiz adına KOM Daire Başkanlığı yer almaktadır. Projede Arnavutluk, Bosna-Hersek, Hırvatistan, Karadağ, Kosova, Makedonya, Sırbistan ve Türkiye yararlanıcı olarak yer almaktadır. Proje kapsamında yararlanıcı olarak yer alan ülkelerde internet üzerinden para akışı, kolluk kuvvetleri servis sağlayıcıları arası işbirliği, internet veri trafiğinin ve içeriğinin tespiti, bilişim suçları alanındaki uzman kolluk ve savcılık birimleri arası işbirliği konulu çalışma toplantıları gerçekleştirilmiştir.

Bilgi ve internet güvenliğine yönelik farkındalık oluşması açısından Avrupa Komisyonu 2004 yılından bu yana her yıl Şubat ayında “Safer Internet Day” ismiyle etkinlik düzenlemektedir. Bu etkinlik “Safer Internet Programı” içerisinde yer alan INSAFE ve INHOP gibi kurumsallaşmış hareketler tarafından desteklenmektedir (Ulaşanoğlu ve diğ, 2010). Ülkemizde de güvenli internet çalışmaları 2011 yılı Ağustos ayında başlatılmış ve kullanıcıların seçebileceği profiller oluşturulmuştur. Kullanıcılar seçtikleri profillere göre internet kullanımlarını güven altına alabilmektedirler.Bu çalışmalara ek olarak Ulusal Bilgi Güvenliği Kapısı (www.bilgiguvenligi.gov.tr), Bilgimi Koruyorum Projesi (www.bilgimikoruyorum.org.tr) TUBİTAK tarafından oluşturulmuş ve halen desteklenmekte olan uygulamalardır.

İnternet kullanıcılarının bilgisayarlarını ve kişisel bilgilerini koruyacak bilgi güvenliği bilgisine sahip olmadığı için güvenlik tehditlerine karşı kırılganlık gösterebilmektedirler. Bu nedenle internet kullanıcılarını ev kullanıcıları ve ev kullanıcısı olmayan kullanıcılar olarak ikiye ayırmak gerekir. Ev kullanıcısı olmayan kullanıcılar internete ticari bir alandan, kurumsal bir alandan ya da akademik bir alandan erişen kullanıcılardır. İnternete ticari, kurumsal ya da akademik bir alandan giren kullanıcılar zorunlu olarak bilgi güvenliğine karşı duyarlı olmak zorundadır (Kritzinger ve von Solms, 2010). Ev kullanıcısı olmayan diğer kullanıcıların çoğu bilgi güvenliği farkındalığı eğitiminden geçirilmektedir. Eğitimden geçirilmeseler

bile birçok kurum bünyesindeki bilgi işlem merkezleri ile güvenlik sağlanması konusunda kullanıcılarına hizmet sunmaktadır. Diğer taraftan ev kullanıcıları, internet erişimini kişisel ihtiyaçları için gerçekleştiren ve bilgi güvenliğini kendisi sağlaması gereken kullanıcılardır. Bilgi güvenliğinden habersiz olan ev kullanıcıları siber ortamlarda nasıl bir risk altında olduklarını bilememektedir. Ev kullanıcılarının önemli bir bölümünü de çocuklar ve gençler oluşturmaktadır. Ev kullanıcılarının karşılaştıkları riskler aşağıda yer almaktadır (Kritzinger ve von Solms, 2010):

- Ev kullanıcılarının %95'i internet ataklarına maruz kalmaktadır.
- 3 milyon bilgisayar Koobface isimli sosyal ağdan etkilenmiştir.
- 2010 yılında spam maillerin %30-40 seviyelerinde olduğu rapor edilmiştir.
- Her gün 23.500 web sitesi zararlı yazılımlardan etkilenmiş olarak keşfedilmektedir.
- İş amaçlı gönderilen maillerin %89,7'si spam içermektedir.
- Bunlara ek olarak ev kullanıcıları internet üzerinden alışkın olmadıkları tehditler ile karşılaşmakta ve gerekli korumayı bilmedikleri için tehditlere karşı koyamamaktadır (Furnell et al., 2008b).

Yukarıdaki bilgiler incelendiğinde bilgi güvenliği konusu gittikçe önem kazanmaktadır. Yapılan araştırmalar ve ortaya çıkan istatistiklerde bunu destekler niteliktedir. Gençlerin ve çocukların teknolojiden uzaklaşmalarını istemeden teknolojiyi doğru ve etkili kullanmaları esas amaç olmalıdır. Bu nedenle bu araştırmanın amacı özellikle gençler ve çocuklarda görülen bilgi güvenliği ile alakalı davranışları tespit etmek, bilgi güvenliği konusuna dikkat çekmek ve siber zorbalık duyarlılığının bilgi güvenliği ile ilişkisini incelemektir.

1.1. PROBLEM CÜMLESİ

Lise öğrencilerinin riskli davranış, korumacı davranış, suça maruziyet ve tehlike algısı ile siber zorbalık duyarlıkları arasında ilişki var mıdır?

1.2. ALT PROBLEMLER

Bu araştırmada aşağıdaki sorulara cevap aranmıştır.

1. Riskli davranış, korumacı davranış, suça maruziyet ve tehlike algısı siber zorbalığa ilişkin duyarlılığı yordamakta mıdır?

2. Lise öğrencilerinin sanal ortamlardaki riskli davranışları, suça maruziyet algıları, korumacı davranışları, tehlike algıları ve siber zorbalığa ilişkin duyarlıkları cinsiyete göre farklılık göstermekte midir?

3. Lise öğrencilerinin sanal ortamlardaki riskli davranışları, suça maruziyet algıları, korumacı davranışları, tehlike algıları ve siber zorbalığa ilişkin duyarlıkları yaşa göre farklılık göstermekte midir?

4. Lise öğrencilerinin sanal ortamlardaki riskli davranışları, suça maruziyet algıları, korumacı davranışları, tehlike algıları ve siber zorbalığa ilişkin duyarlıkları öğrenim gördükleri alanlarına göre farklılık göstermekte midir?

5. Lise öğrencilerinin sanal ortamlardaki riskli davranışları, suça maruziyet algıları, korumacı davranışları, tehlike algıları ve siber zorbalığa ilişkin duyarlıkları güvenlik eğitimi alıp almamalarına göre farklılık göstermekte midir?

6. Lise öğrencilerinin sanal ortamlardaki riskli davranışları, suça maruziyet algıları, korumacı davranışları, tehlike algıları ve siber zorbalığa ilişkin duyarlıkları internet kullanım süresine göre farklılık göstermekte midir?

1.3. ÖNEM

Gençler arasında popüler olan sosyal ağlar ve internet kullanımının artması bilgi paylaşımını kolaylaştırmıştır. Bunu değerlendiren ve bilinçsiz kullanıcıların bilgilerini kolaylıkla ele geçiren kötü niyetli kişiler ise giderek artmaktadır. İnternet ve diğer siber ortamlarda yapılan davranışlar ve tutumlar kontrol edilmezse istenmeyen sonuçlar verebilmektedir. Gençlerin bilgi güvenliği davranışlarını tespit etmek, siber ortamlarda yapılan davranışlara dikkat çekmek, istenmeyen ruhsal ve sağlık problemlerini engellemek için bu araştırma önemlilik arz etmektedir.

Bu araştırma;

- Lise öğrencileri arasında bilgi güvenliği davranışlarını ortaya çıkarması ve siber zorbalık duyarlılığı ile bilgi güvenliği algısı arasındaki ilişkiyi araştıran ilk çalışmalardan biri olması sebebiyle **özgün**,
- Bilgi güvenliği ve siber zorbalık gibi giderek önemi artan konuları içermesi nedeniyle **güncel**,
- Bilgi güvenliği konusunda farkındalığı ölçmesi ve siber zorbalık konusuna dikkat çekmesi açısından **gerekli,**

- Bulgularıyla lise öğrencileri arasında bilgi güvenliği davranışlarını ve siber zorbalık duyarlılığını göstermesi ve öneriler getirmesi açısından **işlevsel** olarak görülebilir.

1.4. SINIRLILIKLAR

Bu araştırma aşağıdaki nitelikleri içermesi açısından sınırlılıklara sahiptir. Bunlar;

1. Araştırma da uygun örnekleme yöntemi kullanılmıştır.
2. Araştırma İstanbul ilinde bulunan araştırmanın yapıldığı dersaneler ile sınırlıdır.

1.5. TANIMLAR

Bilgi Güvenliği: Bilginin gizlilik, doğruluk ve kullanılabilirlik özelliklerinin güvenliğinin sağlanmasıdır.

Siber Zorbalık Duyarlılığı: İnternet, cep telefonu gibi siber araçların kullanımı esnasında zorbaca davranışlara maruz kalmaya yol açabilecek davranışlardan uzak durma, bu türlü tehditlerin varlığından haberdar olma ve tedbir alma, tehdit oluşturabilecek uyarıcıları fark etmeye yönelik dikkati yüksek tutma davranışları olarak tanımlanabilir (Tanrıkulu, 2011).

1.6. SİMGELER VE KISALTMALAR

CMK: Ceza Muhakemeleri Kanunu

OECD: Ekonomik Kalkınma ve İşbirliği Örgütü (İngilizce: Organisation for Economic Co-operation and Development)

TCK: Türk Ceza Kanunu

DDOS: Dağıtılmış Hizmeti Engelleme Saldırısı (Distributed Denial of Service)

USB: Evrensel Seri Veriyolu (Universal Serial Bus)

BÖLÜM II: ARAŞTIRMANIN KURAMSAL ÇERÇEVESİ VE İLGİLİ ARAŞTIRMALAR

2.1. ARAŞTIRMANIN KURAMSAL ÇERÇEVESİ

2.1.1. Bilgi

Akolaş'a (2004) göre olayların sonuçlarıyla ilgili verilerin bir takım dönüştürme sürecinden geçirilip, kullanıcı için anlamlı hale getirilmesi durumunda bilgi oluşur. Başka bir tanımda, üzerinde kesin bir yargıya varılmış her türlü ses, görüntü ve metne bilgi denir ve kaynağını veriler oluşturur (Yozgat, 1998).

Bilginin yer aldığı belli başlı ortamlar (Şahinaslan ve diğ., 2009).;

Fiziksel ortamlar; Kâğıt, tahta, pano, faks, Çöp/Atık kağıt kutuları, Dolaplar vb.

Elektronik ortamlar; Bilgisayarlar, mobil iletişim cihazları, e-posta, USB, CD, Disk, Disket vb. manyetik ortamlar.

Sosyal ortamlar; Telefon görüşmeleri, muhabbetler, yemek araları, toplu taşıma araçları vb sosyal aktiviteler.

Tanıtım platformları; İnternet siteleri, broşürler, reklamlar, sunular, eğitimler, video ya da görsel ortamlar.

2.1.2. Bilgi Güvenliği

Bilgi güvenliği genel olarak bilginin bir varlık olarak tehditlerden korunması olarak tanımlanabilir (Ulaşanoğlu ve diğ., 2010). Ayrıca bilgi güvenliğini " teknolojinin doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda istenmeyen kişiler ve gruplar tarafından elde edilmesini önleme" olarak tanımlanır (Dülger, 2004). Bilgi güvenliğinin kapsamı hızla gelişme gösterdiği için Türk Standartları Enstitüsü, TS ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemi Standardını benimsemiş, bilgi güvenliğini gizlilik, bütünlük ve kullanılabilirlik başlıkları altında kabul etmiştir.

İnsan hayatını kolaylaştıracak teknolojik gelişmeler diğer yanda uygunsuz kullanım, bireylerdeki risk algısının zafiyeti, bilgi güvenliği tehditlerinden habersizliği karşısında bir takım olumsuzlukları, kötü amaçlı kullanımları ve bir takım telafisi güç bilgi güvenliği risklerini de bünyesinde taşımaktadır (Şahinaslan ve diğ., 2009).

Bilgi teknolojileri alanında yapılan yatırımlar sonucunda yazılım veya donanıma ilişkin açıklar üzerinden bilginin sömürülmesi ya da uygunsuz kullanımı zorlaşsa da bu açıklar yerine insan faktörünü kullanarak bilgiler üzerinde bir takım çıkarlar elde etme gayreti yoğunlaşmış durumdadır (Şahinaslan ve diğ., 2009). Bu çalışmada bilgi güvenliğinin riskli davranış, korumacı davranış, tehlike algısı ve suça maruziyet boyutları incelenmiştir.

2.1.2.1. Riskli davranış

Ortak kullanımına açık bilgisayarlarda şifre gerektiren işlemler veya bankacılık işlemleri yapmak, şifrelerin paylaşılması, kolay şifreler kullanılması ya da şifreleri yazılı olarak kolay ulaşılabilecek yerlere koymak, bilgisayardaki dosyaları ağda yazılabilir olarak açmak sanal ortamlarda yapılan riskli davranışlar olarak kabul edilebilir.

Erdur-Baker (2010) riskli internet davranışları ve siber zorbalık ile ilişkisini incelediği araştırmada, riskli internet davranışlarını; internette tanışılan birisine buluşma teklif etme ve kabul etme, internette tanımadığı insanlarla kişisel bilgilerini paylaşma olarak açıklamıştır.

Dowell ve arkadaşları (2009) tarafından riskli internet davranışları, internet üzerinde kişisel bilgileri paylaşmak, internette tanıştığı biriyle iletişime geçmek ve yüzyüze buluşmak, pornografik, madde kullanımına ya da intihara özendirici sitelere girmek, internette başkası hakkında kaba yorumlar yazma ve onun utanmasına neden olmak şeklinde açıklamıştır.

Ybarra ve arkadaşları (2007) tarafından yapılan araştırmada katılımcıların en çok yaptığı riskli davranışların kişisel bilgilerini internette paylaşmak, en az yaptığı riskli davranışın ise internette tanıştığı birisiyle cinsel konular hakkında konuşmak olduğunu bulmuştur. Riskli internet davranışı olarak bireylerin hesaplarına ait şifrelerini başkalarıyla paylaşma davranışına ilişkin Schrock ve Boyd (2008) yaptığı araştırmada, katılımcılar şifrelerini arkadaşlarının güvenlerini kazanmak için ve teknik destek almak için paylaştıklarını belirtmişlerdir.

2.1.2.2. Korumacı davranış

Bilgi ve iletişim teknolojilerini kullanırken bilgi güvenliğini sağlamak için çeşitli korumacı davranışlar bulunmaktadır. Bunlar, bilgisayarda lisanslı yazılımlar kullanmaya çalışmak ve lisanslı anti virüs yazılımı kullanmak, güvenlik duvarı ve casus yazılım engelleyici programlar kullanmak, geçici internet dosyalarını silmek, e-posta filtreleme programları kullanmak, bankacılık işlemleri sırasında e-imza, sanal klavye ya da şifre üreten programlar kullanmak, kolay tahmin edilemeyecek şifreler seçmek, bilgisayarın ele geçirilme ihtimaline karşı önemli dosyaları şifrelemek, bilgisayardan ayrılmadan önce bilgisayarı kilitlemek (Lock), ziyaret edilen web sitelerin SSL sertifikasına sahip olma durumunu kontrol etmek ve sertifikası olmayan siteleri gezmemeye çalışmak, şifreleri belirli periyotlarla değiştirmek, kullanılan antivirüs, işletim sistemi ve diğer yazılımların güncellendiğinden emin olmak gibi davranışlar bilgi ve iletişim teknolojilerini kullanırken korumacı davranışlar olarak adlandırılabilir (Öğütcü, 2010).

2.1.2.3. Tehlike algısı

Bilişim teknolojilerini kullanırken bu teknolojilerden ne derecede olumsuz etkilenebileceğine ilişkin ve ortaya çıkabilecek duruma karşı bireylerde oluşan algıya tehlike algısı diyebiliriz. Bireylerin, bilişim teknolojilerini kullanırken karşılarına çıkabilecek tehlikelere karşı oluşturduğu algı olarak da düşünebiliriz.

2.1.2.4. Suça maruziyet

Bilişim teknolojilerini kullanırken kötü niyetli kişiler tarafından mağdur edilme durumu suça maruz kalmak olarak nitelendirilebilir. Bireyler, zararlı yazılımlar, çevrimiçi alışveriş ya da bankacılık işlemleri, kişisel bilgilerin paylaşımı, kumar içerikli sitelere girmek, sosyal ağlar veya arkadaşlık sitelerine girmek gibi nedenlerden dolayı bilişim suçuna maruz kalabilirler.

2.1.3. Bilgi Güvenliği ve Tehditler

Bunca değerli bilginin bulunduğu bir ortamda, kısa sürede kötü niyetli kullanıcılar da boy göstermiş ve çeşitli amaçlarla diğer sistemlere karşı saldırılarda bulunmaya başlamıştır. CERT (Computer Agency Response Team) tarafından yapılan

istatistiklere göre saldırılar gün geçtikçe artmaktadır (Stallings, 2010). Bu saldırıları çeşitlerini şu şekilde sıralayabiliriz:

2.1.3.1. Dijital saldırılar:

Özel veya tüzel kişilerin sahip oldukları değerlere veya bilgilere izinsiz erişmek, zarar vermek, maddi/manevi kazanç sağlamak için bilgi iletişim teknolojilerini kullanılarak yapılan her türlü hareket olarak nitelendirilebilir. Dijital saldırılar aktif ve pasif saldırılar olmak üzere ikiye ayrılır (Stallings, 2010).

2.1.3.1.1. Pasif saldırılar

Pasif saldırılar iletişimi gizli olarak dinleme ve bunu göstermeye dayalıdır. Buradaki amaç, aktarılan veriyi bir şekilde öğrenmektir. İki çeşit pasif saldırı tipi vardır. Bunlar, paket içeriklerini görüntüleme ve trafik analizidir.

Paket içeriğini görüntüleme saldırısı, anlaşılması kolay bir saldırı şeklidir. İstenmeyen kişilerin, gönderdiğimiz paket içeriklerini görebilmesi anlamına gelir. Elektronik postada veya transfer edilen bir dosyada, hassas ve önemli bilgiler olabilir. Bu tür iletişimlerin içeriklerinin başka biri tarafından öğrenilmesine karşı tedbir almak gerekir.

Trafik analizi saldırısı ise, daha karmaşık bir saldırıdır ve ustalık gerektirir. Aktarılan veriler bir şekilde maskelenir ve veriler hedefe ulaştığında açılmaz. Buna encapsulation yani kapsülleme denir. Kapsülleme kullanıldığı halde saldıran kişi paketlerin kalıplarını gözlemleyebilir. Bu sayede iletişimde olan kişileri, paketlerin frekanslarını ve uzunluklarını tespit etmesi mümkündür. Bu şekilde mevcut iletişim yapısı hakkında çeşitli detaylar da tahmin edilir. Pasif saldırılarla veriler üzerinde değişiklik yapılamasa da korunulması gereken saldırılardır (Stallings, 2010).

2.1.3.1.2. Aktif saldırılar

Aktif saldırıların özelliği, veri akışı üzerinde değişikler yaparlar ve yanlış veriler üretirler. Aktif saldırıları maskeleme, tekrar oynatma, değiştirme ve hizmet aksatma olarak kategorileştirebiliriz.

Maskeleme, bir paketin içeriğinin değiştirilmesine denir. Örneğin, üretilen bir paketin sistemde daha yetkili bir paketmiş gibi hareket etmesidir.

Tekrar oynatma, verilerin o verilerle ilgili ilişkili ve sıralı iletimlerin, yetkisiz etkiler üretmek için pasif olarak yakalanmasıdır. Basitçe anlatmak gerekirse verilerin bir bölümünün veya tamamının değiştirilmesi, paketlerin tekrar sıraya sokulması, geciktirilmesi gibi yetkisiz etki sağlamak için kullanılmasıdır.

Hizmet aksatma, iletişim kanalları engelleme veya kısıtlama anlamına gelir. Bu saldırıların amacında belirli bir hedef vardır. Bütün ağı kesintiye uğratmak yada yavaşlatmak da hizmet aksatma saldırılarına girer. Ağ performansını etkilemek için çok fazla ve sürekli paket gönderilir.

Saldırılara karşı mümkün olduğunca kısa bir sürede tespit edilip, sebebiyet verecekleri zarardan korunmak gerekir. Tespit edilmenin saldırılardan korunma konusunda yıldırıcı bir etkisi bulunmaktadır (Stallings, 2010).

2.1.3.2. Riskler ve tehditler

Bilgi güvenliği konusunda gerek saldırganlar tarafından gerekse doğal yollardan oluşan riskler ve tehditleri şu şekilde sıralayabiliriz (Şahinaslan ve diğ., 2009).

1. Doğal tehditler; yangın, sel, yıldırım vb doğal afetler ve bunların bilgiler üzerinde oluşturabilecekleri tehditler.
2. Zararlı yazılımlar; virüsler, trojan'lar (truva atları), casus yazılımlar (spyware, spyware cookie), spam, exploit, keylogger, botnet, sniffer, phishing vb
3. Sosyal mühendislik
4. Güvenlik açıkları ve Fiziksel Güvenlik
5. Korsanlar ve Erişim; Korsanlar ve bilgi erişimine yönelik tehditler
   Bunların dışında;
6. Hizmetin engellenmesi saldırıları da bulunmaktadır. (Ulaşanoğlu ve diğ., 2010)

2.1.3.2.1. Zararlı Yazılımlar

Zararlı yazılımlar; yaşam döngüsü, kendi kendine çoğalma, özerklik, bulaşma mekanizması, ayrık veya virüs özelliği taşıma ve korunma mekanizması özellikleri

açısından farklı kategorilere ayrılabilir. Kendi kendine çoğalıp bilgisayara zarar verdikleri gibi, belli bir amaç için çalışanları ya da kullanıcısı tarafından yönetilen ve istendiği zaman hedef sistemin koruma ağını yok etmeye ayarlanmış olanlarda vardır. Zararlı yazılımlar bilgisayar virüsleri, solucanlar (worm), Truva atı (trojan), klavye izleme (keylogger) yazılımları, ticari tanıtım yazılımları (adware) ve casus yazılımlar (spyware) olarak ana başlıklar halinde sıralanabilir (Ulaşanoğlu ve diğ., 2010).

Truva Atı (Trojan)

Truva atı tarihi bir olaydan kaynaklanarak ismini almış, şehir içine alınmış bir atın içinden çıkan askerlerin şehri kuşatmasından bu isimle anılmaktadır. İngilizce trojan olarak geçen Truva atı yazılımları yararlı gibi gözüken programların içine gizlenmiş zararlı kodlar barındırmaktadır. Genellikle e-postalara ekli olarak gelen dosyalar ile bilgisayara bulaşmaktadır. Solucanlar ve virüsler gibi kendi başlarına işlem yapamazlar. Truva atları kullanıcıların hareketlerine bağlı olarak çeşitli zararlar verirler. Kendilerini kopyalayıp çoğalsalar bile kurbanın Truva atını çalıştırması gerekir (Ulaştırma Bakanlığı, 2005). Kullanıcıların özellikle P2P (Kazaa, Elite gibi) türü indirme programlarından, warez sitelerinden, torrentlerden ve diğer dosya paylaşımı yapan sitelerden indirdikleri programlar, müzik dosyaları, oyunlar ve diğer yazılımların içeriklerinde trojan barınabilir.

Truva atlarıyla sistemi arka kapıdan (backdoor) yöneten bilgisayar korsanları, sistemin yapısını değiştirebilir, kullanıcıların şifre ve diğer kişisel bilgilerine ulaşabilir (Ulaşanoğlu ve diğ., 2010).

Arka Kapı Yazılımları (Backdoor)

Bilgisayara uzaktan erişmeyi sağlayan ve kimlik doğrulama süreçlerini aşan yöntemler arka kapı olarak adlandırılmaktadır. Bir sisteme bir kez sızan kötü niyetli kişiler aynı sisteme tekrar girmek isterler. Bu iş için en çok kullanılan yöntem portu açık tutmaktır. Arka kapılar bazen sistemi geliştiren kişiler tarafından da oluşturulduğu için çeşitli açıklar ortaya çıkmaktadır. Programcı tarafından kasıtlı olarak bırakılan arka kapılar da bulunmaktadır (Turhan, 2006).

Solucanlar (Worm)

Solucanlar bilgisayar ağları arasında herhangi bir zarar vermeden dolaşabilen, kullanıcılardan bağımsız olarak kendilerini aktif hale getirebilen kopyalarını ağa

bağlı diğer bilgisayarlara bulaştırabilen programlardır (Ulaşanoğlu ve diğ., 2010). Virüslerden daha hızlı yayılmaları, bilgisayarın işlemcisini aşırı derecede yormaları ve internet hızını yavaşlatmaları bakımından solucanlar tehlikelidir. Bilinen ilk solucan Robert Morris tarafından yazılmıştır. Günümüzde ise yaklaşık olarak 16 milyon bilgisayara yayılarak bulaştığı bilgisayara zarar vermeyen ve sadece yönetici haklarına sahip olmayan çalışan "Conficker" solucanının ne yapacağı bilinmemektedir.

Solucanlar keşif ve yerleşme aşamaları sonunda sistemlere yerleşir. Keşif aşamasında kırılgan sistemler taranır, yerleşme aşamasında ise çalışan kodun transferi gerçekleşir (Sperotto ve diğ., 2010).

Bilgisayar solucanları; e-posta, anında mesajlaşma (Instant Messaging), İnternet ve ağ solucanları olarak dört grupta incelenebilir (Canbek ve Sağıroğlu, 2007). E-posta solucanları, adından anlaşılacağı gibi e-posta üzerinden sisteme bulaşan ve hızla yayılmaya çalışan solucan türüdür. Genellikle bir fotoğraf ya da metin dosyası olarak e-postaya eklenirler. Bulaştıkları kullanıcının adres defterinde bulunan e-postalara da kopyalarını yollarlar. Anında mesajlaşma solucanları, Microsoft Messenger, IRC, ICQ, KaZaA gibi mesajlaşma hizmetleri sayesinde yayılırlar. Genellikle kullanıcıyı bir internet adresine yönlendirmeye çalışırlar. İnternet solucanları, sadece internete bağlı olan bilgisayarlara bulaşırlar. Güvenlik açığı olan, internete bağlı bilgisayara bulaşır ve kendini hızla yaymaya çalışır. W32/Blaster ve W32/Deloder tarzı solucanlar internet solucanlarına örnek verilebilir. Son olarak ağ solucanları ise, ağ üzerinde paylaşılan bir klasöre faydalı bir program ya da dosya gibi gözükerek yerleşirler. Bu tür dosyaların kullanıcı tarafından çalıştırılması ile sisteme bulaşırlar.

Virüsler

Bilgisayarlara zarar vermek üzere hazırlanmış daha çok e-postalar ve taşınabilir aygıtlarla bulaşan virüsler bilgisayarların çalışmasını engelleyebilmekte, bilgilerinin kaybolmasına, bozulmasına veya silinmesine neden olabilmektedir. Bilgisayara yerleşerek daha yavaş çalışmasına neden olurlar, ayrıca virüsler çalıştırılabilen programlara kendini ekleyebilen, yerleştiği programların yapısını değiştirebilen ve kendi kendini çoğaltabilen programlardır (Ünver ve diğ, 2010).

Virüsler bilgisayarın ekranında çalışmaya engel oluşturacak mesajlar gibi zararsız etkilerinin yanında, önemli dosyaları silmek veya yönetici hesabı elde ederek sistemi

tamamen çalışmaz hale getirmek gibi yıkıcı etkileri de mevcuttur. Virüsleri diğer zararlı yazılımlardan ayıran en önemli özellik kullanıcı etkileşimine ihtiyaç duymasıdır. Bir dosyanın açılması, bir e-postanın okunması, bir sistemin önyükleme yapılmasıyla veya virüslü bir programın çalıştırılmasıyla kullanıcının haberi olmadan virüsler yayılabilir (Peikari ve Fogie, 2002).

Antivirüs şirketleri virüslere karşı önlem almak için hayvanat bahçesi (zoo), bal çanağı (honetpot) diye adlandırılan laboratuvarlarda gelecekte çıkması muhtemel virüsler için çeşitli çalışmalar yapmaktadır.

Bilgisayar virüsleri;

- Dosya virüsleri
- Önyükleme virüsleri
- Makro virüsleri
- Betik virüsleri olarak sınıflandırılabilir.

Dosya virüsleri, işletim sisteminde bulunan dosya sistemini kullanır ve yayılmak için çeşitli dizinlere kendilerini kopyalarlar. Önyükleme virüsleri, sabit disk veya disketin "Ana Önyükleme Kaydını" değiştirerek bilgisayarın açılışına gizlenir ve her açılışta çalışırlar. Makro virüsleri, ofis programları gibi güçlü makro desteği kullanabilen belgelerin açılmasıyla çalışırlar. Betik virüsü, Visual Basic, Javascript, BAT, PHP gibi betik dilleri kullanılarak yazılır. Betik virüsü Windows veya Unix tabanlı dosyalara veya programlara bulaşabilir. Betik desteği olan HTML, Help dosyaları veya Windows INF dosyalarına yerleşerek karşımıza çıkabilirler (Canbek ve Sağıroğlu, 2007).

Casus Yazılım (Spyware)

Casus yazılımlar olarak da geçen bu tür yazılımlar kullanıcının bilgisi dışında kullanıcıyla ilgili bilgileri aktarmak için kullanılır. Casus yazılımlar yüzünden istenmeyen sayıda mail alma, bilgisayar ekranında aniden beliren reklamlar, kaldırılamayan programlar oluşarak bilgisayarlar için yük oluştururken, kullanıcılar içinse risk oluşturmaktadır.

Bir casus yazılım sisteme yerleştikten sonra kurulduğu makinadan silmeye karşı direnç göstermektedir. Bazı casus yazılımlar kurulumları sırasında kullanıcılara Uç Kullanıcı Lisans Anlaşmasını (EULA- End User License Agreement) onaylatmakta

ve kaldırılmamalarını garanti altına almaya çalışmaktadır. Genellikle rutin programları kaldırma usullerinin dışında teknikler kullanmak gerekmektedir (Canbek ve Sağıroğlu, 2007).

Casus Yazılım Belirtileri

Casus yazılımlar sisteme girdiklerinde gizlice çalışırlar ve çoğu kez amaçlarına ulaşırlar. Bir bilgisayarda casus yazılım olup olmadığını anlamanın bazı yolları vardır.

- Bilgisayarınızın her zamanki hızı düşüyorsa ya da kısa süreli olarak duraklıyorsa,
- İnternet üzerinde sörf yaparken istemediğiniz sitelerle karşı karşıya geliyorsanız,
- İnternet tarayıcınızda varsayılan olarak ayarladığınız arama motoru yerine başka bir arama motoru çalışıyorsa,
- İnternet tarayıcınızın Sık Kullanılanlar veya Yer imi bölümlerine istemediğiniz bağlantılar eklenmişse,
- İnternet tarayıcınıza anasayfa olarak kaydettiğiniz varsayılan siteniz yerine başka bir sayfa açılıyor, değiştirmeye çalıştığınız halde değişmiyorsa,
- Tarayıcınıza eklenmiş olan daha önce görmediğiniz araç çubukları (toolbar) varsa,
- Masaüstünüzde daha önce görmediğiniz bir program simgesi varsa,
- İnternete bağlantınız olmadığı halde sizin de isminizi içeren reklamlar açılıveriyorsa,
- İnternet sayfanızda navigasyon tuşlarını çalıştıramıyor ya da kapatmak istediğiniz bir pencere pasif haldeyse,
- Bilgisayarınızda çalışmadığınız halde sabit disk hareketini gösteren işaret yanıp sönüyorsa,
- CD sürücünüz istemediğiniz halde açılıp kapanıyorsa,
- Rastgele hata mesajları alıyorsanız,

Sisteminizde büyük ihtimalle casus yazılım bulunmaktadır (Canbek ve Sağıroğlu, 2008).

Casus Yazılımların Bulaşma Teknikleri

Casus yazılımlar bilgisayarlara bulaşmak için çeşitli teknikler kullanmaktadır. Genellikle oldukça faydalı ve işe yarayacak gibi gösterilmeye çalışan ve "bedava" olduğu vurgulanan programlar aracılığıyla bulaşmaktadır.

Casus yazılımların sisteme sızabilmek için kullandığı ve aslında oldukça kötü denebilecek nitelikte olan bir tekniği de sahte pencere ve diyaloglar kullanmaktır. Bu yöntemde bireylerin hoşuna gidebilecek resim, canlandırma, animasyon gibi etkileyici özellikleri olan pencereler kullanılmaktadır (Canbek ve Sağıroğlu, 2008).

2.1.3.2.2. Hizmetin engellemesi saldırıları (Ddos)

Bu tür saldırılar kurumlara, şirketlere ve devlete ait siteleri işlem göremez hale getirmek ve hizmeti aksatmak amacıyla bireysel ya da grup halinde yapılır. Saldırı boyunca sisteme aşırı şekilde yüklenme yapılır. Bireysel saldırılarda yeterli yüklenme yapılamadığında grup halinde saldırı tekniği denenir. Kötü niyetli kullanıcılar kendilerine ait bir saldırı grubu oluşturamazlar ise botnet veya zombie denilen daha önce ele geçirilmiş bilgisayarlara saldırıda kullandıkları programları kurarlar ve masum kullanıcıları bile saldırıya ortak ederler. Ddos saldırılarına örnek olarak Anonymous grubunun ülkemize yaptığı saldırılar gösterilebilir. Bu saldırılarda kullanılan Low Orbit Ion Cannon programı saldırıdan önce siber ortamlarda hızla yayılmaktadır. Gruba katılmak isteyen kullanıcılardan sadece paylaşılan linklere tıklanması istenmektedir. Bu saldırılara katılmak bu nedenle oldukça kolaydır.

Botnet

Merkezi bir kontrol noktası (Command and Control) tarafından bağlanmış tehlikeli bilgisayarlar ya da zombi adı verilen yığınların oluşturduğu ağdır. Command and Control (C ve C) noktasına bağlanmış bilgisayarlar sahiplerinden izinsiz olarak bazen bir saldırı için bazen de elektronik oylama gibi amaçlar için kullanılmaktadır. Kontrol altına alınmış bilgisayarlara zombi, zombilerden oluşan topluluğa ise botnet denilmektedir.

Günümüzde en çok bilinen botnet 300.000 bilgisayarı yönetme kapasitesine ulaştığı varsayılan Srizbi isimli botnettir. Srizbi'den sonra 180.000 civarında bilgisayarı yöneten Torpig, 150.000 civarında bilgisayarı kontrol eden Rustog gelmektedir (Ulaşanoğlu ve diğ., 2010). Botnet'ler saatlik olarak internet üzerinden

kiralanmaktadır. Bu nedenle kötü niyetli kişilerin fazla çaba sarfetmeden zarar verebilmelerini kolaylaştırmaktadır.

2.1.3.2.3. Sosyal mühendislik

Sosyal Mühendislik Türleri

1. Oltalama (Phishing)
2. Nijeryan Mektupları
3. Zincir E-postalar (Hoax)

Yemleme-Oltalama (Phishing)

İnternet kullanıcılarının kandırılması veya ikna edilmesi suretiyle kişisel bilgiler ve bankacılık bilgileri gibi önemli bilgilerinin ele geçirilmesini için kullanılan dolandırıcılık yöntemidir (Turhan, 2006). Bu teknik daha çok banka gibi tüzel bir kişilikten gelmiş gibi gösterilen ve hikaye edilmiş güzel bir mail ile yapılmaktadır. Gönderilen mail de kullanıcının hesap bilgileri ve şifresi istenmektedir. Kullanıcı mail bilgilerini kontrol etmeden bankaya güvenerek istenilen bilgileri verebilmektedir. Symantec (2009) tarafından yayınlanan rapora göre yemleme-oltalama (phishing) tekniğinde daha çok hedef finans sektörüdür (%74). Daha sonra sırasıyla Internet Servis sağlayıcıları (%9), Perakende Pazar (%6), Sigortacılık (%3), İnternet Toplumu (%2), Telekomünikasyon (%2) gelmektedir. Oltalama yöntemi son dönemlerde özellikle sosyal paylaşım sitelerinde gençleri ve çocukları etkilemektedir.

Bu tür dolandırıcılıklara engel olabilmek için TC kimlik numarası, banka hesap bilgileri, şifre gibi önemli kişisel bilgilerin kullanıldığı arayüzlere dikkat etmek gerekir. Özellikle SSL sertifikası olmayan sitelerde bankacılık işlemleri ve diğer şifre gerektiren işlemler yapılmamalıdır.

Ulaşanoğlu ve arkadaşları (2010) tarafından belirlenmiş Oltalama yöntemine karşı yapılması gerekenler aşağıda listelenmiştir.

- Bankalardan geldiği düşünülen e-postalardaki linklere tıklanarak gidilen sayfada bankacılık işlemleri yapılmamalıdır. Bu tür işlemler için bankalar tarafından sunulan sanal klavye, tek kullanımlık SMS ile şifre edinme gibi çözümleri kullanmak güvenlidir.

- Oltalama yöntemi sadece bankacılık sitelerinde değil diğer arkadaşlık, sohbet, alışveriş ve ulaşımla ilgili sitelerde de kullanılmaktadır. Bu yüzden böyle sitelerden gelen maillere de dikkat etmek gerekir.
- Https ile başlayan sitelerde alışveriş yapmaya özen gösterilmelidir.
- ATM cihazları kullanırken dikkatli olunmalı, bu makineler üzerine mikro kamera, kart okuyucu, sahte tuş takımı gibi düzenekler yerleştirilebilmektedir.
- Bankadan geldiği belirtilen e-postalar üzerinde bankanın linki bile olsa internet adresinin elle girilmesi ve bankanın kendi sitesine erişim yapıldığına dikkat etmek gerekir.

Nijeryan Mektupları

Nijeryalı mektupları olarak bilinen dolandırıcılık içeren mektuplar çoğu zaman hikaye bir durumu anlatan e-postalardan oluşmaktadır. Ticari bir faaliyet için ortaklık teklif eden ya da zor bir durumda olduğu ve banka hesabına erişemediği için yardım isteyen bir içeriği vardır.

Zincir E-postalar (Hoax)

Zincir e-postalar birçok kullanıcının birbirine gönderdiği, içinde bir yardım ya da ulusal bir destek istenen iletilerdir. Kullanıcıların vicdani değerlerini sömüren, ahlaki göreve çağıran ya da toplumsal bir yanlışa dikkat çekmeye çalışan içerikleri vardır. E-postalar tanıdık kişilerden geldiği için kullanıcılar farkında olmadan maili açarlar ve başka insanlara göndermeye devam ederler. Bu sırada mail adresleri birikmeye devam eder.

Bu sosyal mühendislik türünün temel amacı mesajların mümkün olduğu kadar çok kişiye ulaşmasını sağlayarak e-posta adreslerinin toplanmasını sağlamaktır. Bu şekilde ele geçirilen e-posta adresleri üçüncü kişilere ya da şirketlere bir ücret karşılığında satılmakta ya da spam ya da reklam göndermede kullanılmaktadır (Schryen, 2007).

2.1.3.3. Saldırılara karşı alınabilecek önlemler

2.1.3.3.1. Zararlı yazılımlara karşı alınabilecek önlemler

Zararlı yazılımlara karşı alınması gereken önlemler kullanıcı kaynaklı tedbirler ve zararlı yazılımlara karşı kullanılan programların sağladığı korumalar olarak incelenebilir. Canbek ve Sağıroğlu (2008) tarafından zararlı yazılımlara karşı alınacak bazı önlemler listelenmiştir. Bunlar;

1. Kullanıcıların işletim sistemi ve güvenlik açıklarını takip etmeleri gerekir.
2. Kullanılan işletim sistemi ve programların yamaları ve güncellemeleri düzenli bir şekilde kurulmalıdır. Otomatik olarak açık olsa bile işletim sisteminin ve programların websiteleri ziyaret edilebilir.
3. Antivirüs programının güncel olması ve düzenli aralıklarla bilgisayarın ve kullanılan harici disklerin tam taramadan (full scan) geçmesi gerekir.
4. Lisans yazılım kullanılmalıdır. Kullanıcıların birçoğu lisanslı yazılım ücretleri yüksek olduğu için tercih etmemektedirler. En azından antivirüs yazılımlarının lisanslı olması casus yazılımlar ve diğer zararlı yazılımlara karşı koruyacaktır.
5. P2P programları, warez ve crack siteleri zararlı yazılımların bulundurmaktadır. Bu tür sitelerden ve P2P programlarından indirilen resim, müzik, video ve diğer yazılımlar mümkünse kullanılmamalı, gerekli durumlarda lisanslı antivirüs programlardan geçirilmeli ya da sanal makine kullanılarak test edilmelidir.
6. Bilgisayarınızın Boot sıralamasına dikkat etmek gerekir. Boot sıralamasında hard-disk seçilmelidir. Bu şekilde istediğimiz dışında USB, CD-DVD ya da ağ üzerinden boot edilmemiş olur. Kon-boot gibi programlar USB, CD-DVD üzerinden boot edilerek kullanıldığında bilgisayarı şifresiz olarak açabilmektedir.
7. Internet Explorer internet tarayıcıları içinde bilgisayar korsanları tarafından en çok saldırıya açık tarayıcıdır. Kullandığımız tarayıcıyı değiştirmek ve güncellemelerine dikkat ederek sürekli güncellenmelidir.
8. Zararlı web sitelerin kullandığı bir başka teknikte çerezlerdir. Tarayıcının çerez ayarlarını
    a. Birinci parti çerezleri sor
    b. Üçüncü parti çerezleri engelle
    c. Oturum çerezlerine her zaman izin ver şeklinde değiştirilmelidir.
9. ActiveX ve Java betiklemeyi devre dışı bırakmak bu tür ortamlara saldıran zararlı yazılımları durdurabilir.
10. İnternet kafeler, üniversiteler, oteller gibi ortak kullanıma açık bilgisayarlarda şifre gerektiren veya bankacılık işlemleri gibi önemli işlemler yapılmamalıdır.

11. İnternet üzerinden alışveriş yapılırken dikkat edilmeli, SSL sertifikası bulunan ya da güvenli protokolleri bulunan siteler tercih edilmelidir.
12. Düzenli aralıklarla kredi kartı dökümleri incelenmelidir.
13. İnternet kullanım kotası periyodik olarak kontrol edilmelidir.
14. Şifre veya önemli kişisel belgelerin bulunduğu not, dosya ya da klasörler 3. şahısların ulaşabileceği yerlere atılmamalı, çöpe atılacaksa öğütücüden geçirilmelidir.
15. Posta yolu ile gelen mektup ve belgeleri koruyunuz ve posta kutunuzu düzenli bir şekilde boşaltınız.
16. Dizüstü bilgisayarınızın kasasına isminizi ya da şirket ismini yapıştırınız. Dizüstü bilgisayarı belli edecek şekilde çantalar kullanılmamalı ve araba içine görünür şekilde bırakılmamalıdır. Seyahatlerde kargo bölümü yerine el bagajı olarak alınmalıdır.
17. İnternetten gezinirken yada çalışırken karşımıza çıkan ekranları okumadan karar vermemeli, hemen kurtulmak için rastgele tıklanma yapılmamalıdır. Çünkü kötü niyetli kişiler bu tür ekranlara kullanıcıların hemen X tuşuna bastıklarını bildikleri için istedikleri siteye yönlendirme yapabilmektedir. Bu nedenle Alt+F4 tuşunu kullanmak gerekir.
18. Çocuklara, gençlere ve çevremize bilgisayar ve internet güvenliği ile ilgili bilgiler verilmeli, özellikle ortak kullandığınız bilgisayarlarda dikkat edilmelidir. Kişinin yapmadığı hataları çevresindeki insanlara güvenerek yaşayabilir.
19. Şüpheli gözüken e-posta eklentileri asla açılmamalıdır. .vbs, .shs, .scr, .exe, .bat, .com, .pif, .lnk, .shb, .vb, .wsh, .wsf, .wsc, .sct ve .hta uzantılı dosyalara dikkat etmeli, tanıdık birinden gelse bile açılmamalıdır. Bu uzantılar başka belge gibi görünerek kişileri kandırabilmektedir.
20. Outlook gibi bazı e-posta araçlarında "mesaj ön izleme" penceresi kapatılabilir. Bu seçenek nedeniyle iletiler listeden seçildiği an kendiliğinden açılmaktadır.
21. Göndereni, konusu ve büyüklüğünden şüphe duyduğunuz postaları açmayınız.
22. Mümkün oldukça e-postalar "salt-metin (in text only)" olarak açılmalıdır. Bu sayede içinde bulunan linkler ve yönlendirmeler çalışmayacaktır.

23. Sosyal mühendislik ya da toplum mühendisliği konusunda duyarlı olunmalıdır. Bu konuyla ilgili site, dergi gibi kaynaklar takip edilebilir.
24. Şifre ve önemli bilgiler kimseyle paylaşılmamalıdır. Bunları bir kâğıda ya da bilgisayardaki bir yere yazmak da oldukça tehlikelidir.
25. İnternete gönderdiğiniz dosyalarda size ait bilgilerin olduğunu unutmayınız. Örneğin bir Word dosyasında isim, şirket ve e-posta adresi otomatik olarak ekleniyor olabilir. Bu tür bilgilerin kimin eline geçeceğini kestiremeyiz bu nedenle bu bilgilerin silinmesinde fayda vardır.
26. Windows işletim sisteminde dosya yönetim programı olan Windows gezgini programında "gizli dosyaları göster seçeneği" etkinleştirilerek gizli olan klasör ve dosyalar gösterilmelidir. Ayrıca "bilinen dosya türlerinin uzantılarını gösterme (hide file extension for known file types)" seçeneği kaldırılmalıdır. Bu seçenekler aktifken zararsız gibi görünen resim.jpg dosyası resim.jpg.exe şeklinde gözükecektir.
27. Bu işleme rağmen uzantısı gösterilmeyen .shs (Shell scrap object) dosyaları için sistem kütüğünde HKEY_CLASSES_ROOT\ShellScrap anahtarında bulunan "NeverShowExt" değerini; .shb (Document Shortcut)" dosyaları için sistem kütüğünde HKEY_CLASSES_ROOT\DocShortcut anahtarında bulunan "NeverShowExt" değeri silinmelidir.
28. Bilgisayarda bulunan kişisel veriler ve dosyalar düzenli olarak yedeklenmelidir.
29. İşletim sisteminin çökmesi ihtimaline karşılık sistemi daha önceki haline getirmeye yarayan denetim noktaları ya da sistem kalıp dosyası oluşturulmalıdır.
30. Makinenin günlük kullanımında yönetici hesabı kullanılmamalıdır. Tam erişimli bu hesapla ileri seviye işler yapılmalıdır. Bu seçenek kullanılmak istendiğinde "Run As" seçeneği kullanılabilir.
31. Bilgisayar terk edilirken şifreli ekran koruyucu ayarları yapılmış olarak ya da kilitleme (lock) yapılarak terk edilmelidir.

    Bunların dışında,
32. İnternet bankacılığı ya da şifre gerektiren işler kullanılırken sanal klavye, dijital imza seçenekleri kullanılmalıdır. Unutulmamalıdır ki keylogger sayesinde klavyeden basılan her tuş kötü niyetli bir kişiye gidebilir.

33. Kullanılan harici hard-disk yada büyük bellekli flash diskler bilgisayar ile aynı fiziksel ortamda tutulmamalıdır. Unutulmamalıdır ki bir bilgisayarı çalmak kolay olmasa da küçük bellekleri çalmak daha kolaydır.
34. Klavyeye takılacak bir aygıtla fiziksel bir keylogger oluşturulabilir bu nedenle bilgisayarımıza takılmış aygıtları kontrol etmeliyiz.
35. Sosyal ağlar kullanılırken kişisel bilgiler, fotoğraf paylaşımı yapılmamalıdır. Profil ayarları yapılmalı, tanınmayan kişilerden gelen davetiyeler ve özellikle uygulamalar kabul edilmemelidir.
36. Telefon sim kartlarının kopyalanabildiği unutulmamalıdır. Bu yüzden konuşma dökümleri kontrol edilmeli tanınmayan numaralar varsa GSM şirketinden yardım istenmelidir.

2.1.3.2.3. Hizmetin engellemesi saldırılarına karşı alınabilecek önlemler

Hizmetin engellemesi saldırıları daha çok kurumlara ve sistemlere karşı yapılan saldırılardır. Bu nedenle bu tür saldırılara karşı kişisel olarak önlem almak mümkün değildir. Bir sistemden veri çalmaya ya da paketler üzerinde değişiklik yapmaya karşı ağı tarayan sistemler hizmeti engelleme saldırılarına karşı etkili değildirler. İmza tabanlı giriş denetleme sistemleri, sistemden talep edilen paketleri ve sorguları kontrol ederken hizmeti engelleme saldırılarında paket çalmaya yönelik bir girişim olmadığı için uyarı vermeyecektir. Hizmeti engelleme saldırılarında IP Akış Tabanlı Giriş Denetleme Sistemleri kullanılmalıdır. Bu sistemler yapılan saldırıları durduramasa da sistemde bulunan trafiğin akış şemasını çizerek saldırının yoğunlaştığını haber verebilirler. Hangi IP numaraları üzerinden saldırının gerçekleştiğini göstererek saldırı yapan makinenin bağlı olduğu BOTNET'i de keşfetme imkânı tanımaktadır.

2.1.3.2.3. Sosyal mühendislik saldırılarına karşı alınabilecek önlemler

Sosyal mühendislik saldırılarına karşı aşağıdaki önlemler sıralanabilir;

1. İçeriğinde ahlaki, milli ya da vicdani bir göreve çağıran e-posta, uygulama ya da resim ile karşılaşıldığında bunun bir sosyal mühendislik oyunu olduğunu düşünerek istenilen davranışı yapmamak,

2. Bankaların ya da çeşitli kurumların bizden şifre ve kullanıcı adı gibi bilgileri mail yoluyla istemeyeceği unutulmamalıdır, bu şekilde gelen maillere itibar edilmemelidir.
3. Bilinmeyen bir numaradan gelen mesaj ya da çağrıya karşı meraklanıp yanıt verilmemelidir. Bu tarz çağrılara cevap vermek telefon faturamızı şişirecek sonuçlar doğurabilir.
4. İnternet sayfaları arasında gezinirken adres çubuğunda yazılı adres kontrol edilmeli, özellikle bankacılık işlemleri sırasında HTTPS ile başlayan adresler kullanılmalıdır.
5. Tanımadığımız bir kimseden gelen ve durumunu uzun bir şekilde anlatarak bize para ya da şirket ortaklığı teklif ettiği maillere itibar edilmemelidir.
6. Sosyal ağlarda tanımadığımız kişilerden gelen arkadaşlık teklifleri, uygulamalar, video görünümlü uygulamalar kabul edilmemelidir.
7. Hayır demenin bireyin temel hakkı olduğu unutulmamalı ve siber ortamlarda karşılaştığımız uygunsuz tekliflere hayır denmelidir.
8. Kendisini çalıştığımız şirkette ya da kurumda görevli olduğunu ve bazı değişiklikler için şifremize ihtiyaç duyduğunu söyleyen insanlara itibar edilmemelidir. Sosyal mühendisliğin en yaygın olan şekli yakınlarımıza güvenmekten kaynaklanmaktadır.

Şifre Güvenliği

Şifre güvenliğini sağlamaya yönelik kurallardan bazıları aşağıda şekilde özetlenebilir;

Şifre Seçimi; şifreler başkaları tarafından kolayca tahmin edilemeyen, kullanıcı hakkında özel bilgileri (doğum tarihi, çocuk bilgisi, araç plaka numarası vb) içermeyecek, içerisinde büyük küçük harflerin, sayıların ve özel karakterlerin karışımından oluşmalı. Şifre karakter boyutu en az 8 karakter olarak belirlenmelidir.

Koruma; Şifreler kâğıt ortamlar üzerine yazılmamalı, başkalarıyla paylaşılmamalı, şifrelerin tutulduğu ortamların güvenliği sağlanmalı, güvenliğinden şüphe edilen durumlarda yetkililer bilgilendirilmeli ve gerekiyorsa şifre değiştirilmelidir.

Gizlilik; Kullanıcılar şifrelerini gizli tutmalı ve kimseyle paylaşmamalı, şifre güvenliğinden şüphelendiği durumlarda derhal şifrelerini değiştirmeli, gerekiyorsa yetkililere haber vermelidir.

Düzenli Gözden Geçirme; Şifreler düzenli olarak kritiklik durumuna göre en fazla üç ayda bir gözden geçirilip değiştirilmelidir (Şahinaslan ve diğ., 2009).

2.1.4. Bilişim suçlarının hukuktaki yeri

1982 Anayasasında haberleşme hürriyetini düzenleyen 22. Maddede,

"Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır. Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmi dört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar. İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir." denmektedir. Bu çerçevede CMK 135 kapsamında bir mahkeme kararı olması durumunda belli bir süre ve belli bir kişi için e-posta gibi kayıtların izlenmesi mümkün olabilmektedir (Ulaşanoğlu ve diğ, 2010).

Ayrıca TCK'nın 243-246. Maddelerinde bilişim sistemine girme, sistemi engelleme, bozma, verileri yok etme veya değiştirme, tüzel kişiler hakkında güvenlik tedbiri uygulanması, banka ve kredi kartlarının kötüye kullanılması kapsamında suçlar yer almaktadır (TCK, 2004).

Bilişim sistemine girme

MADDE 243. - (1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

Sistemi engelleme, bozma, verileri yok etme veya değiştirme

MADDE 244. - (1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur.

Banka veya kredi kartlarının kötüye kullanılması

MADDE 245. - (1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis cezası ve adlî para cezası ile cezalandırılır.

(2) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan yedi yıla kadar hapis cezası ile cezalandırılır.

Tüzel kişiler hakkında güvenlik tedbiri uygulanması

MADDE 246. - (1) Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

2.1.5. Zorbalık

Zorbalık kavramı ilk olarak Olweus (1999) tarafından tanımlanmış ve bazı özellikleri barındırdığı vurgulanmıştır. Bu özellikler taraflar arasında "eşit olmayan güç

dengesinin olması" ve bunun "sürekli" olması ayrıca "bilerek yapılması" olarak sayılabilir. Zorbalık günümüzde sadece fiziksel ya da geleneksel zorbalık olarak kalmamıştır. Teknolojinin getirdiği olanaklar ve gençlerin ve çocukların bu teknolojiyi daha yaygın kullanmaya başlaması, geleneksel zorbalık kavramını genişletmiştir. Teknoloji üzerinden zorbalık yapmaya imkan tanıyan bu yeni kavram siber zorbalık olarak tanımlanmaktadır (Ayas ve Horzum, 2010).

2.1.6. Siber zorbalık

Belsey'in (2007) tanımladığı siber zorbalık, bilgi ve iletişim teknolojilerini bir birey yâda gruba tekrar ederek ve düşmanca zarar verme amacıyla kullanmaktır.

Hinduja ve Patchin'e (2005) göre internetin olanaklarını kullanarak isteyerek ve sürekli zarar verme olarak tanımlanmaktadır.

Siber zorbalık fiziksel ortamda gerçekleştirilen zorbalık türlerine benzemektedir. Temel fark internet veya cep telefonu gibi sanal iletişimin gerçekleşebildiği bilgi ve iletişim teknolojilerinin aracı olarak kullanılmasıdır (Baker Erdur ve Kavşut, 2007). Ayrıca, başkalarının e-postalarını izinsiz okuma veya kişisel şifrelerini kullanma, utandırıcı mesajlar gönderme, mağdurun utandırıcı resimlerini çekme ve bunları yayma gibi eylemleri içermektedir (Baker Erdur ve Kavşut, 2007).

Yine siber zorbalığın tanımıyla ilgili Arıcak'ın çeşitli tanımları bulunmaktadır. Arıcak'a (2011) göre siber zorbalık, "bilgi ve iletişim teknolojilerini kullanarak bir birey ya da gruba, özel ya da tüzel bir kişiliğe karşı yapılan teknik ya da ilişkisel tarzda zarar verme davranışlarının tümüdür". Ayrıca Arıcak (2011) tarafından yapılan sınıflandırmada siber zorbalığı elektronik zorbalık ve elektronik iletişim zorbalığı olarak ikiye ayırmaktadır. İlki olayın daha çok teknik yönünü içermektedir, diğeri ise olayın daha çok psikolojik yönünü içeren elektronik iletişim (e-iletişim) zorbalığıdır (e-communication bullying). Elektronik zorbalık kişilerin şifrelerini ele geçirmek, web sitelerini heklemek, spam içeren mailler göndermek gibi teknik olayları içerir. E-iletişim zorbalığı ise bilgi ve iletişim teknolojilerini kullanarak kişileri sürekli rahatsız etme, alay etme, isim takma, dedikodu yayma, internet üzerinden kişiye hakaret etme ya da kişinin rızası olmadan fotoğraflarını yayınlama gibi davranışları içerir. Bu davranışlar duyguları etkilemektedir. Siber zorbalık, "akran tacizinin" elektronik bir formuna dönüşmekte ve okul sınırlarını da aşarak çocukların evdeki odalarına kadar girmiştir.

Siber zorbaca davranışlarla ilgili olarak pek çok sınıflama yapılmaktadır. Nocentini ve arkadaşlarına (2010) göre ise siber zorbaca davranışlar; yazılı ve sözlü davranışlar (telefonla rahatsız edici çağrı yapma, yazılı mesaj gönderme, e-mail göndererek tehdit ve hakaret etme, chat odasında hakaret etme, blog veya sosyal paylaşım sitelerinde mesaj veya yorum yazma), görsel davranışlar (internet ya da cep telefonu aracılığı ile resim ya da video paylaşma, gönderme), dışlama (çevrimiçi bir gruptan atma ve dışlama), sahte kimlik geliştirerek kişisel bilgileri ele geçirme, başka birinin ismini ve bilgilerini kullanarak, hesap açma veya yorumlar yapma olarak sınıflandırılabilir.

Siber zorbalığın içerdiği davranışlar araştırmacılar tarafından şu şekilde belirlenmiştir (Anderson, 2010; Siegle, 2010; Walker, 2009; Willard, 2007):

a. **Hakaret Etme:** Çevrimiçi ortamlarda tartışma, kaba, tehdit dolu ve saldırganlık içeren ifadeler kullanma, onurunu zedeleyici sözler sarfetme,
b. **Bıktırma:** Sürekli olarak can sıkıcı, iğrenç, müstehcen, aşağılayıcı mesajlar ve iletiler gönderme,
c. **İftira:** Gerçeğe aykırı bir şekilde bir kişinin itibarını zedelemek veya ilişkilerini bozmak için hakkında dedikodu yapma, söylenti yayma,
d. **Taklit Etme:** Kişiyi utanılacak bir duruma sokmak, itibarını zedelemek, küçük düşürmek, diğer insanlarla olan ilişkilerini bozmak amacıyla onun yerine geçerek, taklit ederek ya da bilgilerini kullanarak tehlikeli nitelikte mesajlar gönderme, forumlarda ya da sosyal paylaşım sitelerinde yorumlar yapma,
e. **İfşa Etme:** Bireyi utandırmak, rezil etmek amacıyla kişisel bilgilerini ya da resim veya görüntülerini paylaşma,
f. **Hile Yapma:** Birini kandırarak kişisel bilgilerini ele geçirme ve sosyal mühendislik yapma,
g. **Dışlama:** Bilerek çevrimiçi bir gruptan atma veya iletişim kurmasını engelleme, dışlama,
h. **Sanal Taciz:** Tekrar eder nitelikte taciz, tehdit içeren veya korku vermeye yönelik cep telefonu veya internet aracılığı ile yazılı veya sözlü mesaj, e-mail gönderme,
i. **Sexting:** Kişilere çıplak resimler veya pornografik görüntüler gönderme,

Ayrıca siber zorbalık Anderson'a (2010) göre şu davranışları da içermektedir.

1. Bireyin hesaplarını, şifre veya kullanıcı adı gibi özel bilgilerini ele geçirerek ona zarar vermeye çalışma,
2. Bireyin teknolojik araçlarını işlemez hale getirme veya kullanmasını engelleme,
3. Kişisel blog, web sitesi veya hesaplarını ele geçirme, bu bilgileri kullanma veya kontrol etmesini engellemektir.

2.1.6.1. Geleneksel zorbalık ve siber zorbalık arasındaki farklar

Geleneksel zorbalık ve siber zorbalık, kişilik algısı, aileyle olan ile ilişkiler gibi özellikler bakımından benzerlikler göstermekle birlikte sosyallik, yaygınlık ve zorbalık için yapılan davranışların niteliği bakımından farklılıklar göstermektedir (Katzer, Fetchenhauer, ve Belschak, 2009). İki türün benzer özeliklerine bakıldığında güç dengesinin olmaması, tekrarlayan davranışlar olması ve saldırganlık içermesi (Dooley, Pyżalski, ve Cross, 2009; Grigg, 2010) ve birbirini besleyen (Jose, Kljakovic, Scheib ve Notter, 2012) davranışlar olmakla beraber, geleneksel zorbalık ve siber zorbalık şu nitelikler bakımından birbirinden ayrılmaktadır (Ayas ve Horzum, 2010):

1. Siber zorbalık, teknoloji üzerinden yapılması bakımından geleneksel zorbalıktan ayrılmaktadır.
2. Siber zorbaca davranışlarda bulunan kişiler, geleneksel zorbalıktan farklı olarak kim oldukları bilinmeden bu davranışları gerçekleştirebilirler.
3. Geleneksel zorbalık sadece olayın gerçekleştiği yerde bulunup, olaya yakın ve şahit olan kişiler öğrenirken, siber zorbalık olayları sanal ortamlarda olduğu için tüm dünyadan öğrenilebilmektedir.
4. Siber zorbaca davranışlarda cinsellik kolayca ve daha çok kullanılabilmektedir.
5. Geleneksel zorbalığa maruz kalan kişiler davranışın meydana geldiği alandan ayrıldıktan sonra zorbalardan kurtulabilmesine rağmen siber mağdurların zorbaca davranışlardan kurtulabilecekleri bir alan bulunmamaktadır.

Dooley ve diğ. (2009) yaptığı araştırmaya göre cinsiyet açısından geleneksel zorbalık ve siber zorbalığa bakıldığında geleneksel zorbalık erkeklerde kadınlara göre daha yaygınken siber zorbaca davranışlar için anlamlı bir farklılık bulunmamıştır.

Schneider ve arkadaşları tarafından (2012) yapılan başka bir araştırmada siber zorbalığa maruz kaldığını söyleyen öğrencilerin % 59,7'i geleneksel zorbalığa da maruz kaldığını belirtmektedir. Geleneksel zorbalığa maruz kaldığını söyleyenlerin ise % 36,3'ü siber zorbalığa da maruz kaldığını belirtmiştir.

Başka bir araştırma ise, okullarda siber zorbalığın geleneksel zorbalığa göre daha az görüldüğünü fakat okul dışında siber zorbalığın öğrenciler arasında geleneksel zorbalıktan daha fazla görüldüğünü tespit etmişlerdir (Smit ve diğ., 2008).

Li (2005) tarafından yapılan bir çalışmada, öğrencilerin %54'ünün geleneksel zorbalık mağduru olduğu ve %25'inden fazlasının da aynı zamanda siber zorbalık yaptığı bulunmuştur. Bu çalışma göstermektedir ki, öğrencilerin %30'undan fazlası geleneksel zorbalık yapmakta ve bunların yaklaşık %15 inin elektronik iletişim araçlarını kullanarak da siber zorbalık yapmaktadır. Yine, siber zorbalık mağdurlarının %60'ının kadın, siber zorbaların %52'den fazlasının ise erkek olduğu gözlenmiştir.

2.1.6.2. Siber zorbalık için kullanılan araçlar

Siber zorbalık için en yaygın kullanılan araçlar, e-mail, tartışma grupları (listserv), cep telefonu veya web kameraları, SMS veya anlık mesajlaşma (Msn, gtalk vb.) araçları, sosyal paylaşım siteleri, sohbet odaları, bloglar, çevrimiçi kişisel anket yapmaya olanak sağlayan siteler, MMS, video klipleri, ve MUDs (multi-user domains- bireylerin farklı kimlikler alabilmesini sağlayan sanal ortamlar) sayılabilir (Shariff ve Gouin 2005).

Bu araçlar kullanılarak yapılan davranışlar ise % 20.2 oranında çevrimiçi bir gruptan dışlama, % 20.1 oranında internette dedikodu veya söylenti yayma, utandırmaya çalışma veya taciz etme, % 16.8 oranında başkaları hakkında yorumlar gönderme, % 18.1 oranında başkalarının e-mail hesaplarını ele geçirmek gibi davranışlar ve % 14.5 oranında birine zorla bir şey yaptırma ve bunu cep telefonu veya diğer kayıt cihazları ile kayıt altına alma ve siber ortamlarda yayma oluşturmaktadır. (Calvete ve diğ., 2010). Başka bir çalışmada ise siber zorbaca davranışlar arasında en yaygın olanların

isim takma, dedikodu yapma ve söylenti çıkarma olduğu belirtilmektedir (Dehue, Bolman, ve Völlink, 2008).

NCH (National Children's Home) ve Tesco Mobile (2005) tarafından 11 ile 19 yaş arasındaki 770 çocuk arasında gerçekleştirilen bir anketin sonuçlarına göre ise, her beş çocuktan birisi e-posta, sohbet odası ya da cep telefonu mesajı aracılığı ile siber zorbalığa uğradığını bildirmişledir.

2.1.6.3. Siber zorbalığın nedenleri ve risk faktörleri

Öğrencilerin neden siber zorbalık yaptığına dair Raskauskas ve Stoltz (2007) tarafından yapılan bir araştırmada öğrencilerden, % 38'si eğlence amaçlı, % 25'i intikam almak amacıyla, %6'sı kendilerini kötü hissettikleri bir zamanda olmalarından dolayı yaptıklarını belirtmişlerdir. % 31'i ise bu konuda herhangi bir fikirlerinin olmadığını söylemişlerdir.

Arıcak (2009) tarafından psikiyatrik problemlerin siber zorbalığın bir yordayıcısı olup olmadığı konusunda yapılan araştırmada, herhangi bir zorbalık yapmamış ve zorbalığa maruz kalmamış kişilerin, saf-mağdurlardan ve zorba-mağdurlardan anlamlı düzeyde daha düşük psikiyatrik belirtiler gösterdiği bulunmuştur. Ayrıca düşmanca duygular ve psikotik belirtilerin siber zorbalığı anlamlı olarak yordayan iki temel değişken olduğu anlaşılmıştır. Aynı zamanda kişiler arası duyarlılık ve psikotik belirtiler siber zorbalığa uğrama ve siber zorba olma olasılığını da anlamlı düzeyde açıklamaktadır.

Araştırmacılar tarafından öfke ve saldırganlık ile siber zorbaca davranışlar arasında da ilişki olduğu bulunmuştur. Siber zorbaca davranışlar gösterenlerin ve siber mağdurların, öfke ve saldırganlık düzeyi daha yüksektir (J. W. Patchin ve Hinduja, 2010b; Schultze-Krumbholz ve Scheithauer, 2009).

Başka bir araştırmada yalnızlık içinde olanlar ile özsaygısı düşük bireylerde, akran iyimserlik derecesi, sosyal kabul edilebilirliği ve karşılıklı arkadaşlık ilişkisine sahip olma düzeyleri düşük olanlar daha fazla siber zorbaca davranış göstermektedir (Schoffstall ve Cohen, 2011).

Mason (2008), siber zorbaca davranışları meydana getiren durumları şu şekilde özetlemektedir;

1. Tepkisizlik Etkisi: Siber zorbaca davranışlarda bulunan bireyler sanal ortamlarda kim olduklarının bilinemeyeceğini ve bu sebeple cezalandırılmayacaklarını veya toplum tarafından kınanmayacaklarını düşünmektedirler. Bu fiziksel olarak görünmezlik ve engellenmeme durumu siber zorbalara siber ortamlarda güç sağlamaktadır. Bu sebeple gerçek hayatta bastırılmış karakterlerinin zorbaca özellikleri bu ortamlarda açığa çıkmaktadır. Gerçek tepki almıyor olmak, sorumlu tutulamayacağını düşünmek, zarar vermenin kolay olması özellikle ergenlere bu davranışlar konusunda özgürlük hissi oluşturmaktadır.
2. Bireyin özelden sosyale kimlik değişimi: Bireyler, internetin onlara kendi kimliklerinden uzaklaşma fırsatı verip özgürleştirdiğini hissetmektedirler. Siber ortamlar bireylere kendi özel fikirlerini ya da kimliklerini, bir çevrimiçi grup içinde kolayca ifade etme ve kendilerini gizleme olanağı sunmaktadır. Bu sebeple siber ortamlar, bireylerin kendilerini kontrolsüz şekilde serbest bırakmalarına, daha düşüncesiz, daha akıldışı ve daha agresif davranmalarına neden olabilmektedir.
3. Çocuk ve aileler arası zayıf bağlar: Siber ortamlar gençlere yetişkinlerin bilgisi ve kontrolünden uzak bir ortam oluşturmaya imkan sağlamaktadır. Birçok ergen siber zorbalıkla ilgili problemlerini bir yetişkine anlatmakta zorluk çektiğini belirtmektedir. Gençlerin yaşadığı problemleri ailesine, öğretmenine ya da bir büyüğüne anlatamaması siber zorbaca davranışlara maruz kalmalarına davetiye çıkarmaktadır.

Dowell ve arkadaşlarına (2009) göre;

- Siber ortamlarda tanımadığı kişilerle, kişisel bilgilerini paylaşma,
- Pornografik motifler veya şiddet içeren sitelere girme,
- Telefon veya internet aracılığı ile tanıştığı kişilere buluşma teklif etme veya buluşma teklifini kabul etme,
- İntiharı veya kendi kendine zarar vermeyi özendirici, belli bir grubu aşağılayıcı web sitelerine girme,
- İnternetten yasal olmayan materyaller indirme ve video paylaşım sitelerinde uygunsuz görüntü veya resimleri paylaşma

gibi riskli davranışlarda bulunmak siber zorbalığa maruz kalmayı artırmaktadır. Bu tür davranışları kadınlara göre erkeklerin daha çok yaptığı ve internette tanışılan biri

ile yüz yüze buluşma, yasak veya uygunsuz içerikli web sitelerine girme, sosyal paylaşım sitelerine ulaşımı sağlayan kullanıcı adı ve şifreleri başkaları ile paylaşmanın en yaygın riskli davranışlar olduğu görülmüştür (Erdur-Baker ve Tanrıkulu 2010).

2.1.6.4. Siber zorbalığın etkileri

Araştırmacılar siber zorbalığa maruz kalmış bireylerde yoğun üzüntü ve depresyon hali, intihar düşüncesi, korku ve utanç duyguları, aşırı gerginlik ve uyarılmışlık hali, internet ve diğer çevrimiçi araçlara olan ilginin azalması, çeşitli davranış problemleri, okulla ilgili sorumluluklardan uzak durma, zararlı madde kullanımına başlama ya da meyil etme gibi sorunların ortaya çıktığını söylemektedir (Mason, 2008; Morales, 2011; Schneider ve diğ., 2012).

Goebert, Else, Matsu, Chung-Do ve Chang (2011) ise, siber mağdurlarda madde kullanma olasılığının yaklaşık 2,5 kat, depresyon olasılığının 2 kat, intihar girişiminin kadınlarda 3,2 kat, erkeklerde ise 4,5 kat daha yüksek olduğunu söylemektedir. Eğer siber zorbaca davranışlar yetişkinler tarafından gençlere ve çocuklara yapılıyor ise daha tehlikeli sonuçlar oluşabilmektedir (Anderson, 2010).

Yine Hinduja ve Patchin'e göre (2005) zorbalığa maruz kalan gençlerde depresyon, düşük benlik saygısı, korku, üzüntü, hayal kırıklığı, utanç vb. gibi duygular yoğun olarak görülmektedir. Aynı araştırmacılara göre siber mağdur olan bireylerde ortaya çıkabilecek en büyük etki intihar düşüncesidir. Geleneksel zorbalık ile karşılaştırıldığında siber zorbalığa maruz kalmış bireylerde daha yüksek oranda intihar düşüncesi görülmektedir (Hinduja ve Patchin, 2010).

Ülkemizdeki yazılı basına yansıyan okul şiddeti haberlerindeki bilgi ve iletişim teknolojilerinin etkisini inceleyen bir tarama çalışması, benzer olayların ülkemizde de yaşandığını ve son yıllarda gazetelerde bu tür haberlerde artış olduğunu bulmuştur. Erdur-Baker, Yerin-Güneri ve Akbaba-Altun (2006), tarafından gerçekleştirilen çalışmaya göre, sanal ortamda gerçekleşen ve sonra fiziksel ortama taşınan şiddetin kadın-erkek arkadaş sorunu, chat odasında cinsiyetini farklı belirtme, chat odasında cinsel taciz ya da cinsel ilişki teklifi, chat odasında tartışma, hakaret ve tehdit gibi nedenlerden kaynaklandığını göstermektedir.

Başka bir araştırmada siber zorbalığa maruz kalan gençlerde kendini savunma güçsüzlüğü ve siber zorbalığın boyutlarına göre öfke, üzüntü gibi negatif duygular, güvenlik kaygısı, çeşitli kişilik problemleri ve ilişki sorunları görülebilmektedir (Spears, Slee, Owens, ve Johnson, 2009). Bu tür sorunlar yaşayan öğrencilerin okula gitme veya görünmeye karşı korku geliştirdikleri (Hinduja ve Patchin, 2009; Kowalski, Limber and Agatson, 2008; Morales, 2011), siber mağduriyetin tekrar yaşanması olasılığının verdiği yoğun baskı ile evde veya okulda konsantrasyon sağlamada sorunlar yaşadıkları anlaşılmaktadır. Bu nedenle duygusal problemlerin yanında okul başarısında da sorunların yaşandığı gözlenmektedir (Mason, 2008; Wong-Lo, Bullock ve Gable, 2011).

Price ve Dalgleish'in (2010), yaptığı araştırmaya göre siber mağdur olan öğrencilerin %78'inde özgüven kaybı, %70'inde özsaygı kaybı, %42'sinde arkadaş ilişkilerinde bozulma, %35'inde okul başarısında düşüş, %28'inde okul etkinliklerine katılmada isteksizlik ve %19'unda ise aile ilişkilerinde bozulma olduğu tespit edilmiştir. Ayrıca siber zorbalığın kadın öğrencileri erkek öğrencilere göre daha fazla etkilediği de anlaşılmıştır. Aynı araştırmada mağdurların % 75'inde üzülme, % 54'ünde aşırı üzüntü ve keder, % 72'sinde öfke ve kızgınlık, % 58'sinde hüsran ve yıkılma, % 48'inde utanç ve korku ve % 29'unda ise dehşete kapılma gibi duygusal etkiler olduğu tespit edilmiştir.

Siber zorbalığa maruz kalan bireylerin sıklıkla başka bireylere zorbaca davranışlar göstermeye başladığı da bilinmektedir. Siber zorbalarla ilgili yapılan araştırmalar zorbaların daha önce kendilerinin de bu tür zorbalığa maruz kaldığını göstermektedir (Katzer ve diğ., 2009; Schneider ve diğ., 2012; Vandebosch ve Van Cleemput, 2009; Yilmaz, 2011).

2.1.6.5. Siber zorbalığı önleme ve müdahale eğitimi

Diamanduros ve arkadaşlarının (2008) siber zorbalığı önlemek için yapmış olduğu çalışmalarda önleme programları için öncelikle şu konulara değinmektedirler;

1. Teknolojinin öğrencilerin hayatındaki yeri ve siber zorbalığın hangi yollarla yapıldığını anlamak,
2. Siber zorbalık sonucu oluşacak tehlikeleri bilmek,
3. Siber zorbalığın tam olarak kim tarafından yapıldığının bilenemeyebileceğini anlamak,

4. Siber zorbalığın geleneksel zorbalıktan daha kapsamlı daha yaygın ve hızlı gerçekleştiğini ve çok çeşitli dijital araçlarla günün her anında yapılabileceğini anlamak,
5. Öğrencilerin siber zorbalığa maruz kalmaları durumunda internet veya bilgi teknolojilerini kullanmalarının ebeveynleri tarafından kısıtlanacağı endişesi ile bunu anlatmaktan çekindiklerinin farkında olunmasıdır.

Hazırlanacak önleme ve müdahale programlarında ise şu konular işlenebilir (Diamanduros ve diğ., 2008);

1. Bireyin kendini güvende hissetmesinin kendisinin bir insani hakkı olduğunu bilmesi,
2. Siber zorbalık kavramının ne olduğunun açıklanması,
3. Siber zorbalığın hangi araçlarla ve nasıl gerçekleşebildiği,
4. Siber zorbalığın yaygınlık oranları ve ilgili istatistiki bilgilerin verilmesi,
5. Siber zorbalığa maruz kalmış bireylerin düşünceleri ve mağdurlar üzerindeki etkileri,
6. Her türlü elektronik iletişimin başkaları tarafından izlenebileceğinin bilinmesi,
7. Siber zorbalığın hukuki yaptırımları,
8. Siber zorbalığa neden karşı durulmalı ve mücadele edilmesi gerektiğinin anlatılması,
9. Siber zorbalığa maruz kalma durumunda neler yapılmalı ve yetişkinlerle olan ilişkilerin sağlamlaştırılması,
10. Siber zorbalığa şahit olunması durumunda yapılması gerekenler,
11. Bilgi güvenliği ilkesinin unutulmaması ve kişisel bilgilerin paylaşımından kaçınma,
12. İnternet ve siber güvenliğin farkında olunması ve sanal ortamlarda davranış kurallarının neler olduğu,
13. İnternet veya bilgi teknolojilerinin kullanımının bazı sorumluluklarının olduğu ve bunları kullanırken başkalarına saygılı olunması gerektiği,

Gençlerin ve çocukların siber zorbalığa maruz kalmalarını önlemenin en önemli yollarından birisi zorbaca bir davranış karşısında ergenlerin bunu bir yetişkine anlatmalarını sağlamaktır. Genellikle çocuklar ve gençler yaşadıkları mağduriyeti ya arkadaşlarına anlatmakta ya da kimseye bundan söz etmemektedir. Bu nedenle

özellikle aileler, öğretmenler ve okul yöneticileri bu sorunun farkında olamamaktadırlar (Slonje ve Smith, 2008). Maruz kalmayı önlemede en iyi yol, rahatsız edici davranışı engelleyen dijital önlemleri alma veya bunu bir yetişkine bildirmektir (Smith ve diğ., 2008).

Siber zorbalıkla mücadele için teknoloji kullanımı konusunda çeşitli önlemler alınmalı, farkındalık oluşturacak teknikler geliştirilmelidir. Medya okuryazarlığının gençler arasında sağlanması, siber zorbalara verilecek olan yaptırımlar için hukuki eksikliklerin giderilmesi, güvenli internet kullanımının sağlanması, yeterli kuralların oluşturulması ve denetleme birimlerinin kurulması gerekmektedir. Bununla birlikte ailelerin, eğitimcilerin ve gençlerin video, hareketli animasyonlarla zenginleştirilmiş eğitsel yazılımlarla ile eğitimler alması sağlanmalıdır (Jäger, Amado, Matos, ve Pessoa, 2010).

Geleneksel zorbalıkla mücadelede etkili olan bazı etkinlikler siber zorbalıkla mücadelede de yardımcı olabilir. Bunlar pozitif okul iklimi oluşturma, özgür sınıf kuralları geliştirme ve çatışma çözme eğitimleri gibi davranışlar olabilir (Cowie ve Colliety, 2010; Grigg, 2010). Okul içinde oluşturulan etkili bir özgür ortam ve öğrenciler arası yardım sisteminin kurulması geleneksel zorbalıkla mücadeleye olan etkisini gösteren bir araştırmanın sonuçlarına göre öğrencilerin zorbalık karşısında pasif izleyici olarak kalmayı anlamlı derecede azalttığı, zorbalık karşısındaki empatik ve bilişsel düzeyi yükselttiği ve öğrenciler arasındaki mağdur sayısını azalttığı görülmüştür. Siber zorbalıkla mücadele kapsamında kullanılacak böyle bir davranışın özellikle öğrencilerin siber zorbalık karşısında seyirci olarak kalmasının azaltılması ve bu sorunla mücadele konusunda çok önemlidir. Siber zorbalığın ve saldırganlığın azaltılması konusunda akran desteği etkili bir araç olabilir (Cowie ve Colliety, 2010; Smith ve diğ., 2008).

Başka bir araştırmaya göre internet ve bilgi teknolojilerinin kullanımı konusunda bir takım kurallar belirleyen ailelerde çocukların siber mağdur olma oranları daha düşük olmaktadır (Mesch, 2009). Çevrimiçi ortamlarda yapılan davranışlardan örneğin 13 yaşından küçükler için uygun olmayan sosyal paylaşım sitelerine girişimin engellenmesi gibi filtreleme ve sınırlama getiren ebeveynlerin siber mağdur olan çocuklarının oranı böyle davranmayan ebeveynlere göre daha düşük çıkmıştır. Ayrıca internet ve sanal ortamlardaki davranışlar için çeşitli kurallar koyan ailelerin bunu çoğu kez bilinçsizce yaptığı görülmüştür. Aileler çocuklarının siber zorbalığa

maruz kalıp kalmadığı konusunda bilgi sahibi değildirler. Dehue ve diğerlerinin (2008) yaptığı araştırmada siber zorbaca davranışlarda bulunduğunu belirten ergenlerin oranı %17,3 iken, ailelerin ancak %4,8'nin bu tip davranışların farkında olduklarını söylemişlerdir. Ayrıca siber zorbalığa maruz kaldığını belirtenlerin oranı %22,9 iken ailelerin ancak %11,8'i bunu bildiklerini söylemişlerdir.

Siber zorbalığın tanımlanması ve önlenmesi için aileler için aşağıda çeşitli öneriler sıralanmıştır (Siegle, 2010):

1. Gerçek yaşamda kişiler arası iletişimde kullandığımız tüm kuraları siber ortamlar ve cep telefonu ile iletişim içinde de kullanmak;
2. Okulun bilgi teknolojilerinin güvenli kullanımını içeren bir eğitimi programı olduğundan emin olmak;
3. Gençleri internetin ve teknolojinin uygun kullanımı hakkında eğitmek; özellikle teknolojinin hatalı kullanımının hangi problemlere yol açabileceğini açıklamak
4. Bilgi teknolojilerinin uygun şekilde kullanılmasında model olmak: Çocukların yanında başkaları hakkında şaka ve taciz içeren çevrimiçi davranışlarda bulunmamak,
5. Çocuk ve gençlerin siber ortamlardaki davranışlarını takip etmek; bu takip çocuklardan ve gençlerden bilgi almak, çevrimiçi davranışlarının neler olduğu hakkında konuşmak olabileceği gibi bazı takip ve güvenlik programları ile de olabilir. Çocukların ve gençlerin internette neler yaptığını kontrol etmek için çeşitli filtreleme ve kayıt programları kullanılabilir.
6. Çocukların teknolojiyi kullanırken yapmış olduğu davranışlara dikkat edilmeli, çocuk siber araçları kullanırken çekingen davranmaya ya da bazı takıntılar göstermeye başlamışsa siber zorbalığın mağduru ya da faili olabilir.
7. Başkalarına saygılı olma, insani değerleri bilmek gibi değerler eğitimi vermek ve güçlenmesini sağlamak
8. Çocuklarla onları teşvik eden bir iletişim ortamı oluşturmak onları deneyimlerimize ihtiyaç duydukları an soru sormaya istekli hale getirecektir. Araştırmalar öğrencilerin çevrimiçi ortamlarda diğer insanlarla olan etkileşimlerin konuşulmasının önemli olduğunu göstermiştir. Aileler çeşitli sorularla siber zorbalık konusunda çocuğunun durumunu öğrenebilir.

Örneğin:

- Diğer çocuklar sanal ortamlarda seninle çatışıyorlar ya da tartışıyorlar mı? Bunu mail yoluyla, anında mesajlaşmayla ya da cep telefonuyla mı yapıyorlar?
- İnternette birilerinin senin hakkında yazdıklarını diğer insanların görüp, bunları gerçek olarak düşünmeleri seni ilgilendiriyor mu?
- İnternette fiziksel ya da kişisel güvenliğini tehdit edici bir davranış ile karşılaştın mı?
- Sanal ortamlarda yapılan fiziksel ya da kişisel tehditlerin hukuki olarak suç olduğunu biliyor musun?
- Sanal ortamlarda yaşadığın bir olay gerçek hayatını da etkiledi mi?
- Sanal ortamlarda herhangi biri sana cinsel içeriği olan bir davranışta bulundu mu? Bunu nasıl yaptı ve nasıl başa çıkabildin?
- Seni sıkmadan, rahatsız etmeden sana nasıl yardımcı olabilirim?

Diamanduros ve arkadaşları (2008) tarafından siber zorbalığın tespit edildiği durumlarda takip edilecek süreçte yapılması gerekenler şu şekilde sıralanmıştır:

1. Özellikle hukuki süreç için siber zorbalığın gerçekleştiğine dair delilleri saklamak ve korumak,
2. Eğer mağdur tarafından önemli bir karışıklık, şiddet ya da intihar endişesi anlatılmışsa, şiddet varsa ya da herhangi bir tehlikeli durum ortaya çıkabilecekse emniyet birimleriyle irtibat geçilmeli,
3. Oluşan değerlendirme sonucunda müdahale seçeneklerini belirlemek ve uygun müdahaleyi kararlaştırmak,
4. Siber zorbaca davranışta bulunanlar bazen sahte bir kimlik ya da rumuz kullanabildiği için suçlunun kimliğini tespit etmek için teknik destek almak,
5. Mağdurlara ve ailelerine destek olunacağının güvencesini vermek, ihtiyaç duyuluyorsa teknik destek sağlamak, emniyet güçlerinin müdahalesi veya hukuki yaptırımlar gibi olanakların kullanımı konusunda danışmanlık önermek,
6. İnternet servis sağlayıcısından siber zorbalığı durdurmak için irtibata geçmek ve saldırının durdurulmasını isteme, eğer zorbalık telefon aracılığı ile yapılıyorsa rahatsız eden numarayı ve kim tarafından kullanıldığını tespit

etme, numarayı engelleme, gerekiyorsa telefon numarası ve e-mail adresini değiştirme ve teknoloji kullanma konusunda gerekli danışmanlığı sağlamak,

7. Zorba tespit edilebiliyorsa ailesi ile irtibata geçmek, sağlık sorunları olup olmadığını araştırmak, arabuluculuk konusunda danışmanlık önermek, tespit edilen failin neden böyle davrandığı ile ilgili altta yatan başka neden varsa bunları araştırmak ve çözümler konusunda çalışmalar yapmak.

2.1.7. Siber zorbalık duyarlılığı

Tanrıkulu ve diğ. (2011) göre siber zorbalık duyarlılığı, internet, cep telefonu gibi siber araçların kullanımı esnasında zorbaca davranışlara maruz kalmaya yol açabilecek davranışlardan uzak durma, bu türlü tehditlerin varlığından haberdar olma ve tedbir alma, tehdit oluşturabilecek uyarıcıları fark etmeye yönelik dikkati yüksek tutma davranışları olarak tanımlanabilir.

2.2. İLGİLİ ARAŞTIRMALAR

Ülkemizde bilgi güvenliği konusunda yapılan araştırmalar genellikle sistemlerin güvenliğini sağlamak üzerine yapılmıştır. Bu çalışmalardan bazıları şöyledir;

Arslan (2009) tarafından yapılan yüksek lisans tezinde Web tabanlı uzaktan eğitim sistemlerinde bilgi güvenliğinin sağlanması konusu işlenmiştir. Uzaktan eğitim sistemi olan WELANIMAL sisteminin kullanımından önce bilgi güvenliği testleri yapılmış ve gerekli düzenlemelere gidilmiştir.

Kumaş (2009) tarafından yapılan başka bir araştırmada bilgi güvenliği kapsamında ISO 27000 standardı, risk yönetimi model ve metodolojilerinin uygulanması ele alınmıştır. Türkiye şartlarında bilgi güvenliği kavramı ile ilgili durum değerlendirilmesi yapılmış, özel olarak e-devlet kapısı projesi ile ilgili eksiklikler ve gözlemler tariflenmiştir. Türkiye kamu yapısına ve özel sektöre göre uygun metodolojiler üretilmeye çalışılmıştır. Üretilen metodolojilerin e-devlet kapısı projesi özelinde nasıl çalıştığı aktarılmıştır.

Vardal (2009) tarafından yapılan araştırmada ise güvenlik ile ilgili standartlar ve kullanım örnekleri karşılaştırmalı olarak incelenmiş ve yükseköğretim kurumları için bilgi güvenlik yönetim sistemi modeli önerilmiştir. Önerilen Bilgi Güvenlik Yönetim Sistemi (ÖBGYS) güvenlikte en zayıf halka olan insan faktörünün güçlendirilmesi ve üniversiteler için kullanımı kolay olan talimat ve ipuçlarını sunmaktadır. Çalışma

sonucunda bilgi güvenliğinin üniversiteler için önemli olduğunu ve önerilen insan merkezli modelin kolaylıkla uygulanabilir olduğu görülmüştür.

Çifçi (2010) tarafından yapılan çalışmada ise 9.sınıf öğrencilerin sanal zorbalık ve empatik eğitim düzeyleri arasında ilişki olup olmadığı incelenmiştir. Araştırma sonucuna göre, 9. Sınıf öğrencilerinin sanal zorbalık düzeyleri ile empatik eğitimleri arasında istatistiksel olarak anlamlı bir ilişki saptanmamıştır.

Topcu (2008) tarafından yapılan çalışmada ise siber zorbalık ve empati düzeyi arasındaki ilişkinin toplumsal cinsiyete bağlı olarak incelenmiştir. Ayrıca siber zorbalığı yordamada geleneksel zorbalığın, bilgi ve iletişim araçları kullanım sıklığının ve internet kullanımında aile denetiminin rolü incelenmiştir. Araştırma sonuçlarında katılımcıların %55,2'sinin geleneksel zorbalık yaptığını, %47,6'sının ise siber zorbalık yaptığını göstermiştir. Erkeklerin hem geleneksel zorbalık deneyiminde hem de siber zorbalık deneyiminde kadınlara göre daha yüksek puanlar aldığı ortaya çıkmıştır. Ayrıca geleneksel zorbalık deneyiminin ve bilgi ve iletişim teknolojilerini sık kullanmanın siber zorbalık deneyimini yormada başarılı değişkenler olduğunu işaret etmiştir. Araştırma bulgularından bir başkası da empati düzeyi yüksek olan kadınlar daha az geleneksel ve siber zorbalık yaptıklarını, empati düzeyi düşük olan erkekler ise daha sık geleneksel ve siber zorbalık yaptıklarını rapor etmişlerdir.

Çetinkaya (2010) tarafından yapılan başka bir çalışmada ise, ilköğretim ikinci kademe öğrencilerinin siber zorbalık davranışlarına maruz kalma ve siber zorbalık davranışlarını uygulama yaygınlıklarını ve bu yaygınlığın cinsiyete göre değişimi incelenmiştir. Araştırma sonucunda erkek öğrencilerin kadın öğrencilere göre daha fazla siber zorbalık davranışlarına maruz kaldığı ve daha fazla siber zorbalık davranışlarını uyguladığı tespit edilmiştir.

Eroğlu (2011) tarafından yapılan araştırmada, riskli internet davranışları, içsel ve dışsal koşullu öz-değer alanlarının siber zorbalık/mağduriyet üzerindeki etkisi incelenmiştir. Ayrıca araştırmada siber zorbalık ve mağduriyetin cinsiyete, yaşa ve ailenin aylık gelirine göre farklılaşıp farklılaşmadığı da incelenmiştir. Araştırma sonuçlarında riskli internet davranışları ve dışsal öz-değer alanları siber zorbalığı/mağduriyeti pozitif, içsel öz-değer alanları ise negatif yönde yordamakta

olduğu görülmüştür. Ayrıca siber zorbalık ve mağduriyetin yalnızca cinsiyete göre farklılaştığı, yaşa ve ailenin aylık gelirine göre farklılaşmadığı görülmüştür.

Chai ve diğ., (2006) tarafından 6-9. sınıflarda okuyan öğrenciler üzerinde yapılan çalışmada sosyal bilişsel ve özyeterlilik ile bilgi güvenliği davranışı arasındaki ilişki incelenmiş ve bilgi güvenliğine karşı özyeterliliği gelişmiş öğrencilerin antivirüs yazılımının güncellenmesi, kimliği belirsiz kişilerden gelen maillerin açılmaması ve kişisel bilgilerin internette paylaşılmaması gibi bilgi güvenliği davranışlarını gösterdikleri bulunmuştur.

Albrechtsen (2007) tarafından kullanıcıların bilgi güvenliği üzerine görüşlerinin alındığı çalışmada,

- Kullanıcıların bilgi güvenliği konusunda motive oldukları ama birçok bilgi güvenliği davranışını yapmadıkları
- Yüksek seviyeli bilgi güvenliği davranışının güvenlik ile fonksiyonellik arasında çatışma oluşturduğu
- Bilgi güvenliği davranışını teşvik etmek için hazırlanan dokümanların davranış ve farkındalık üzerine çok küçük bir etkisi olduğu görülmüştür.

Kullanıcılar, kullanıcı-içerikli yaklaşımların farkındalık ve davranışı etkilemede daha verimli bulduklarını söylemişlerdir.

Alanyazın taraması sonucunda, öğrencilerin bilgi güvenliği ile alakalı konuları okullarından, ailelerinden ya da arkadaşlarından öğrenirlerse bilgi güvenliğini sağlamada bireysel farkındalıklarını güçlendirebilecekleri görülmüştür.

Ayrıca bilgi güvenliğinin eğitim kurumları, gençler ve çocuklar için önemine yeterince değinilmediği görülmektedir. Alanyazında bilgi güvenliği davranış ve algısının işletmeler ve çalışanlar üzerinde yoğunlaşıldığı görülmüştür.

Siber zorbalık duyarlılığı konusunun alanyazında yeni bir kavram olmakla beraber, siber zorbalığın birçok değişkenle birlikte incelendiği ama bilgi güvenliği davranış ve algısı ile birlikte incelenmediği görülmüştür.

Siber zorbalığın bilgi ve iletişim teknolojileri kullanılarak yapılan bir zorbalık çeşidi olduğu, gençlerin ve çocukların kişisel bilgilerini sanal ortamlarda bilinçsizce

paylaşabildikleri görülmüştür. Bu nedenle bilgi güvenliği davranış ve algısının siber zorbalık duyarlılığı ile ilişkisi olduğu düşünülmektedir.

BÖLÜM III: YÖNTEM

Bu bölümde araştırmanın modeli, evren ve örneklemi, veri toplama aracı, verilerin toplanması ve verilerin analizi ile ilgili bilgiler verilecektir.

3.1. ARAŞTIRMA MODELİ

Araştırma, genel tarama modeli türlerinden ilişkisel tarama modeline göre yürütülmüştür. Tarama (survey) modelleri, bir grubun belirli özelliklerini belirlemek için verilerin toplanmasını amaçlayan çalışmalardır (Büyüköztürk ve diğ., 2010). Bu tür araştırmalar, çok sayıda obje ya da denek üzerinde ve belirli bir zaman kesiti içinde yapılmaktadır (Kaptan, 1993). İlişkisel tarama modeli, iki ya da daha çok değişken arasındaki birlikte değişimin olup olmadığını ve bunun derecesini belirlemeyi sağlayan bir modeldir (Karasar, 2009). Araştırmada ilişkisel tarama modeline uygun olarak bilgi güvenli algıları arasındaki ilişki incelenmiştir. Araştırmada, ilişkisel tarama modelindenin yanında kesitsel tarama modeli de kullanılarak veri toplanmıştır. Kesitsel tarama türünde yapılan araştırmalarda tanımlanacak olan değişkenlerin özelliklerine uygun olarak bir seferde ölçüm yapılır (Fraenkel, Wallen, ve Hyun, 2011). Bu nedenle araştırmada kullanılan ölçekler örneklem üzerinde bir kez uygulanmıştır.

3.2. EVREN VE ÖRNEKLEM

Araştırma evreni olarak İstanbul ilinde bulunan ortaöğretim okulları belirlenmiş ve araştırma 2010-2011 Bahar yarıyılında İstanbul'daki çeşitli ortaöğretim kurumlarında okuyan 400 öğrenci üzerinde yapılmıştır. Araştırmaya katılan 32 öğrencinin ölçeklerinin eksik olduğu ve okunmadan işaretlendiği tespit edilmiş ve araştırmanın dışında tutulmuştur. Bu yüzden 368 öğrenci araştırmanın katılımcılarını oluşturmaktadır. Milli Eğitim Bakanlığının 2011-2012 öğretim yılı Örgün Eğitim istatistiklerine göre İstanbul ili Genel liselerinde 533646 öğrenci okumaktadır. Bu araştırmada Olasılık dışı örnekleme yöntemlerinden uygun örnekleme yöntemi seçilmiştir. Özdamar (2001) içerdiği denek sayısı 10.000 den az olan evrenleri sınırlı

evren, içerdiği denek sayısı 10.000'den fazla olan evrenleri ise sınırsız evren olarak nitelemiştir. Krejci ve Morgan (1970) değerlendirmelerin oranlara göre yapılacağı araştırmalarda evren hacminin büyüklüğüne karşılık örneklem büyüklüğüne nasıl karar verileceğine ilişkin 100.000 ve üzeri evrenlerde güvenirliğin % 95 ve p değerinin %5 olduğu hesaplamalarda örneklem büyüklüğünün 384 olduğunu belirtmişlerdir. Bu bilgilere dayanarak araştırma için seçilen örneklem büyüklüğüne karar verilmiştir.

Örneklemin cinsiyet, yaş, öğrenim görülen alan, güvenlik eğitimi alıp almadığı ve internet kullanım süresine göre dağılım tablosu Tablo 4'te yer almaktadır.

Tablo 4. Örneklem Grubunun Cinsiyet, Yaş, Alan, Güvenlik, Eğitimi, İnternet Kullanım Süresine Göre Dağılım Tablosu

		Sayı	Yüzde
Cinsiyet	Erkek	180	48,9
	Kadın	188	51,1
Yaş	15	29	7,9
	16	100	27,2
	17	129	35,1
	18	92	25
	19	18	4,9
Öğrenim Görülen Alan	Sosyal Bilimler	62	16,8
	Fen Bilimleri	203	55,2
	Eşit Ağırlık	103	28
Güvenlik Eğitimi Alıp Almadığı	Evet	56	15,2
	Hayır	312	84,8
İnternet Kullanım Süresi	1 saate kadar	104	28,3
	1-3 saat arası	211	57,3
	3 saatten fazla	53	14,4
	Toplam	368	100

3.3. VERİ TOPLAMA ARAÇLARI

Araştırmada veri toplama aracı olarak güvenlik algısı ile ilgili olarak Öğütçü (2010) tarafından geliştirilen ölçekler ve siber zorbalık duyarlılığı ile ilgili olarak Tanrıkulu, Kınay ve Arıcak (2011) tarafından geliştirilen "Siber Zorbalığa İlişkin Duyarlılık Ölçeği" kullanılmıştır. Öğütçü tarafından geliştirilen ölçekler sırasıyla Riskli Davranış Ölçeği, Korumacı Davranış Ölçeği, Suça Maruziyet Ölçeği ve Tehlike Algısı Ölçeğidir.

Bu ölçeklerden Riskli Davranış Ölçeği Öğütçü (2010) tarafından geliştirilen toplam 20 maddeden (1, 2, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 28, 29, 30, 32, 33 ve 36

numaralı maddelerden) oluşan bir ölçektir. . Bu ölçek 5'li Likert tipindedir. "Her Zaman" seçeneği 5, "Sık sık" seçeneği 4, "Bazen" seçeneği 3, "Nadiren" seçeneği 2 ve "Hiçbir Zaman" seçeneği 1 puan olacak şekilde puanlama yapılmıştır. Ölçekten alınacak en düşük puan 20, en yüksek puan ise 100'dür. Katılımcıların alacağı puan yükseldikçe riskli davranış gösterme oranının arttığı anlaşılmaktadır.

Korumacı Davranış Ölçeği de Öğütçü (2010) tarafından geliştirilmiş, toplam 20 maddeden (3, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 34, 35, 37, 38, 39, 40 ve 41 numaralı maddelerden) oluşan bir ölçektir. Bu ölçek de 5'li Likert tipindedir. "Her Zaman" seçeneği 5, "Sık sık" seçeneği 4, "Bazen" seçeneği 3, "Nadiren" seçeneği 2 ve "Hiçbir Zaman" seçeneği 1 puan olacak şekilde puanlama yapılmıştır. Ölçekten alınacak en düşük puan 20, en yüksek puan ise 100'dür. Katılımcıların alacağı puan yükseldikçe korumacı davranış gösterme oranının arttığı anlaşılmaktadır.

Suça Maruziyet Ölçeği de Öğütçü (2010) tarafından geliştirilmiş, toplam 15 maddeden (42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55 ve 56 numaralı maddelerden) oluşan bir ölçektir. Bu ölçek de 5'li Likert tipindedir. "Her Zaman" seçeneği 5, "Sık sık" seçeneği 4, "Bazen" seçeneği 3, "Nadiren" seçeneği 2 ve "Hiçbir Zaman" seçeneği 1 puan olacak şekilde puanlama yapılmıştır. Ölçekten alınacak en düşük puan 15, en yüksek puan ise 75'dir. Puanlar yükseldikçe suça ya da olumsuz bilişim tecrübesine daha yüksek derecede maruz kalındığı, puanlar düştükçe daha düşük derecede suça maruz kalındığı anlaşılmaktadır.

Tehlike Algısı Ölçeği de Öğütçü (2010) tarafından geliştirilmiş, toplam 25 maddeden (62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85 ve 86 numaralı maddelerden) oluşan bir ölçektir. Bu ölçek de 5'li Likert tipindedir. Bu ölçekteki maddeler " Çok tehlikeli" seçeneği 5 puan, "Tehlikeli" seçeneği 4 puan, "Az Tehlikeli" seçeneği 3 puan, "Tehlikesiz" seçeneği 2 puan ve "Fikrim Yok" seçeneği ise 1 puan alınarak hesaplanmıştır. Katılımcıların alacağı en yüksek puan 125, en düşük puan ise 25'dir. Puanlar yükseldikçe cevaplayıcının ilgili teknolojileri daha tehlikeli bulduğu, azaldıkça ise ilgili teknolojileri daha az tehlikeli bulduğu anlaşılmaktadır (Öğütcü, 2010). Ayrıca Öğütçü tarafından ölçekler hakkında yapılan geçerlik ve güvenirlik çalışmalarına şu şekilde değinilmiştir (Öğütcü, 2010).

> "Anket soruları taslak olarak hazırlandıktan sonra, Ocak-Şubat 2010 tarihleri arasında Başkent Üniversitesi İstatistik ve Bilgisayar Bilimleri Bölümü öğretim üyeleri, Türkiye Bilişim Güvenliği Derneği Başkanlığı,

> Emniyet Genel Müdürlüğü, Bilişim Suçları Şube Müdürü ve bilgi güvenliği uzmanları tarafından incelenmiştir.
>
> Yapılan öneriler doğrultusunda anket formuna ilişkin gerekli düzenlemeler yapılmış ve Akademik Bilişim 2010 konferansı öncesi düzenlenen Güvenlik Kursu'nda konusunda uzman 39 katılımcıya ve 23 akademisyene uygulanmıştır. Yapılan testlerde anketin geçerlilik güvenilirliği incelenmiş ve Cronbach alfa değeri 0,9345 olarak hesaplanmıştır. Buna göre anketin uygulanabileceğine karar verilmiştir."

Tanrıkulu, Kınay ve Arıcak tarafından geliştirilen siber zorbalık duyarlılığı ölçeği ise 14 madde ve tek faktörden oluşmaktadır. Bu tek faktör toplam varyansın %27.70'ini açıklamaktadır. Tek faktör altındaki faktör yükleri .32 ile .73 arasında değişmektedir. Elde edilen bu tek faktörlü yapı, doğrulayıcı faktör analizi ile test edilmiş, modelin kabul edilebilecek düzeyde olduğu görülmüştür (χ^2/sd= 2.06 ve RMSEA= .078). Ölçekteki sorular "Evet" seçeneği 3 puan, "Bazen" seçeneği 2 puan, "Hayır" seçeneği 1 puan olacak şekilde hesaplanmıştır. Ölçekten elde edilecek maksimum puan 42, en düşük puan ise 14'tür.

3.4. VERİLERİN TOPLANMASI

Kullanılacak ölçekler 2011 Mayıs ayında sosyo-ekonomik düzeyler dikkate alınarak İstanbul ilinde bulunan çeşitli dershanelerde okuyan ortaöğretim öğrencilerine uygulanmıştır. Ölçekler öğrencilere bir ders saatinde uygulanmış ve ortalama 20 dakika süre verilmiştir. Veriler toplandıktan sonra 32 öğrencinin ölçekleri eksik veya okumadan işaretlediği tespit edilmiş ve bu veriler araştırmadan çıkarılmıştır.

3.5. VERİLERİN ANALİZİ

Araştırmada verilerin analizi için bilgi güvenliği ölçek puanlarının arasındaki ilişki için Pearson korelasyon testi, Siber Zorbalığa İlişkin Duyarlılık Ölçeğinin diğer ölçekler tarafından nasıl yordandığına bakmak için Regresyon Analizi, ikili gruplar için t-testi ve ikiden fazla gruplar için ANOVA yapılmıştır. Veriler SPSS 17.0 programıyla çözümlenmiş ve anlamlılık düzeyi .05 kabul edilmiştir.

BÖLÜM IV: BULGULAR VE YORUM

Araştırmada ilk olarak Riskli Davranış, Korumacı Davranış, Tehlike Algısı, Suça Maruziyet ve Siber Zorbalığa İlişkin Duyarlılığın birbirleri arasındaki ilişkisine bakılmıştır. Bu ilişkileri incelemek için yapılan Pearson korelasyon testi sonuçları Tablo 5'te yer almaktadır.

Tablo 5. Riskli Davranış, Korumacı Davranış, Tehlike Algısı, Suça Maruziyet ve Siber Zorbalığa İlişkin Duyarlılık Puanlarının Pearson Korelasyon Tablosu

		Riskli Davranış Ölçeği Puanı	Korumacı Davranış Ölçeği Puanı	Suça Maruziyet Ölçeği Puanı	Tehlike Algısı Ölçeği Puanı	Siber Zorbalığa İlişkin Duyarlılık Ölçeği Puanı
Riskli Davranış Ölçeği Puanı	Pearson Korelasyonu	1				
Korumacı Davranış Ölçeği Puanı	Pearson Korelasyonu	.52**	1			
Suça Maruziyet Ölçeği Puanı	Pearson Korelasyonu	.71**	.28**	1		
Tehlike Algısı Ölçeği Puanı	Pearson Korelasyonu	.28**	.36**	.34**	1	
Siber Zorbalığa İlişkin Duyarlılık Ölçeği Puanı	Pearson Korelasyonu	-.16**	.10*	-.17**	.24**	1

**. Korelâsyon 0.01 düzeyinde anlamlıdır (2-kuyruklu).

*. Korelâsyon 0.05 düzeyinde anlamlıdır (2-kuyruklu).

Tablo 5 incelendiğinde riskli davranış puanı ile korumacı davranış puanı arasında pozitif yönlü, orta derecede ve anlamlı bir ilişki ($r = 0.52$, $p = 0.00$) bulunmuştur. Yine riskli davranış puanı ile suça maruziyet puanı arasında pozitif yönlü, yüksek derecede ve anlamlı bir ilişki ($r = 0.71$, $p = 0.00$) olduğu görülmektedir. Bunun yanında riskli davranış puanı ile tehlike algısı puanı arasında pozitif yönlü, düşük derecede ve anlamlı bir ilişki ($r = 0.28$, $p = 0.00$) olduğu ortaya çıkmıştır. Bununla

birlikte riskli davranış puanı ile siber zorbalığa ilişkin duyarlılık puanı arasında negatif yönlü, düşük derecede ve anlamlı bir ilişki (r = -0.16, p = 0.00) bulunmuştur. Tüm bu bulgular ışığında riskli davranış puanı arttığında korumacı davranış, suça maruziyet ve tehlike algısının arttığını, azaldığında ise bu puanların azaldığını göstermektedir. Bunun yanında riskli davranış puanı arttığında siber zorbalık duyarlılığının azaldığı görülmektedir.

Korumacı davranış puanı ile suça maruziyet puanı arasında pozitif yönlü, düşük derecede ve anlamlı (r = 0.28, p = 0.00), tehlike algısı puanı arasında pozitif yönlü, düşük derecede ve anlamlı (r = 0.36, p = 0.00) ve siber zorbalığa ilişkin duyarlılık puanı arasında pozitif yönlü, düşük derecede ve anlamlı (r = 0.10, p = 0.04) bir ilişki olduğu bulunmuştur. Tüm bu bulgular ışığında korumacı davranış puanı arttığında suça maruziyet, tehlike algısı ve siber zorbalık duyarlılığının arttığını, azaldığında ise bu puanların azaldığı söylenebilir.

Suça maruziyet puanı ile tehlike algısı puanı arasında pozitif yönlü, düşük derecede ve anlamlı bir ilişki (r = 0.34, p = 0.00) olduğu bulunmuştur. Bunun yanında, suça maruziyet puanı ile siber zorbalığa ilişkin duyarlılık puanı arasında negatif yönlü, düşük derecede ve anlamlı bir ilişki (r = -0.17, p = 0.00) bulunmuştur. Bu bulgular suça maruziyet puanının artmasının tehlike algısını arttırdığını, siber zorbalığa ilişkin duyarlılığı azalttığını göstermektedir. Tehlike algısı puanı ile siber zorbalığa ilişkin duyarlılık puanı arasında pozitif yönlü, düşük derecede ve anlamlı bir ilişki (r = 0.24, p = 0.00) olduğunu ortaya çıkarmıştır.

Riskli davranış, korumacı davranış, suça maruziyet ve tehlike algısı puanlarının siber zorbalığa ilişkin duyarlılık puanını yordayıp yordamadığını test etmek için aşamalı (stepwise) regresyon analizi yapılmıştır. Gerçekleştirilen aşamalı regresyon analizinden elde edilen veriler Tablo 6'da yer almaktadır.

Tablo 6. Siber Zorbalığa İlişkin Duyarlılığı Yordayan Değişkenler

	R	R^2	β	t	F	p
Yordayıcı Değişkenler	.24	.05			22.23	.00
Tehlike Algısı			.23	4.71		.00
Yordayıcı Değişkenler	.35	.12			26.88	.00
Tehlike Algısı			.33	6.45		.00
Suça Maruziyet			-.28	-5.45		.00

Tablo 6 incelendiğinde tehlike algısının ve suça maruziyet puanlarının birlikte siber zorbalığa ilişkin duyarlılığın varyansına katkılarının anlamlı olduğu görülmektedir (R^2 = .12, F=26.88, p< .05). Tehlike algısının tek başına siber zorbalığa ilişkin duyarlılık varyansının %5'ini açıkladığı (R^2=.5, F=22.23, p<.05), her iki değişkenin birlikte siber zorbalığa ilişkin duyarlılık varyansının %12'sini açıkladığı bulunmuştur. Buna göre siber zorbalığa ilişkin duyarlılığın anlamlı yordayıcısı olarak tehlike algısı ve suça maruziyet gösterilebilir. Tehlike algısı analizin birinci setinde yordama da anlamlıyken, yordamanın ikinci setinde suça maruziyet ile birlikte varyansı yordama da yine anlamlı çıkmıştır. Tüm bu bulgular siber zorbalığa yönelik duyarlılıkta riskli davranış, korumacı davranış, tehlike algısı ve suça maruziyetin önemli değişkenler olduğunu ancak bunlardan tehlike algısı ve suça maruziyetin daha çok ön plana çıktığını ortaya koymaktadır.

Araştırmada cinsiyet, yaş, öğrenim görülen alan, güvenlik eğitimi ve internet kullanım süresi sırasıyla Riskli Davranış, Korumacı Davranış, Suça Maruziyet, Tehlike Algısı, Siber Zorbalığa İlişkin Duyarlılık ölçeklerinden aldığı puanlara göre anlamlı farklılık oluşturup oluşturmadığına bakılmıştır. Bu değişkenlerden öncelikle cinsiyete ilişkin t-testi analizi sonuçları Tablo 7'de yer almaktadır.

Tablo 7. Cinsiyete İlişkin Riskli Davranış Puanı, Korumacı Davranış Puanı, Suça Maruziyet Puanı, Tehlike Algısı Puanı, Siber Zorbalığa İlişkin Duyarlık Puanlarının T-testi Sonuçları Tablosu

Faktörler	Cinsiyet	N	$\overline{X}$	S	sd	t	p
Riskli Davranış Puanı	Kadın	188	44.38	9.45	366	9.65	.00
	Erkek	180	57.5	15.7			
			54.78	14.49	366	3.87	.00
Korumacı Davranış Puanı	Kadın	188					
	Erkek	180	60.82	15.39			
Suça Maruziyet Puanı	Kadın	188	20.57	8.00	366	9.83	.00
	Erkek	180	39.33	24.36			
Tehlike Algısı Puanı	Kadın	188	67.33	15.90	366	3.60	.00
	Erkek	180	73	14.10			
Siber zorbalığa ilişkin Duyarlılık Puanı	Kadın	188	36.33	6.13	366	3.70	.00
	Erkek	180	33.86	6.62			

Tablo 7 incelendiğinde araştırmaya katılan öğrencilerin cinsiyetlerine göre Riskli Davranış Puanı ($t_{(366)}$= 9.65), Korumacı Davranış Puanı ($t_{(366)}$= 3.87), Suça Maruziyet Puanı ($t_{(366)}$= 9.83), Tehlike Algısı Puanı ($t_{(366)}$= 3.60) ve Siber Zorbalığa İlişkin Duyarlılık Puanına ($t_{(366)}$= 3.70) göre istatistiksel olarak anlamlı bir farklılık olduğu ($p<.05$) bulunmuştur. Anlamlı farklılık bulunan faktörler sırasıyla incelendiğinde araştırmaya katılan erkek öğrencilerin ($\overline{X}$=57.5) riskli davranış puanlarının kadın öğrencilere ($\overline{X}$=44.38) göre daha yüksek olduğu, yine erkek öğrencilerin ($\overline{X}$=60.82) korumacı davranış puanlarının kadın öğrencilere ($\overline{X}$=54.78) göre daha yüksek olduğu, erkek öğrencilerin ($\overline{X}$=39.33) suça maruziyet puanlarının kadın öğrencilere ($\overline{X}$=20.57) göre yüksek olduğu ve erkek öğrencilerin ($\overline{X}$=73) tehlike algısı puanlarının kadın öğrencilere göre ($\overline{X}$=67.33) yüksek olduğu bulunmuştur. Bu sonuçlardan farklı olarak kadın öğrencilerin ($\overline{X}$=36.33) siber zorbalığa ilişkin duyarlılık puanlarının erkek öğrencilere ($\overline{X}$=33.86) göre daha yüksek olduğu bulunmuştur. Bu bulgular ışığında erkek öğrencilerin kadınlara göre bilgi güvenliği konusunda riskli davranış

sergileme oranlarının arttığı bununda tehlike algısı, suça maruziyeti arttırdığı söylenilir.

Araştırmada öğrencilerin yaşlarına göre Riskli Davranış Puanı, Korumacı Davranış Puanı, Suça Maruziyet Puanı, Tehlike Algısı Puanı, Siber Zorbalığa İlişkin Duyarlık Puanları arasında fark olup olmadığını görebilmek için ANOVA testi yapılmıştır. Analiz sonucunda elde edilen betimsel bulgular Tablo 8'de Anova sonuçları ise Tablo 9'da yer almaktadır.

Tablo 8. Yaşa İlişkin Riskli Davranış Puanı, Korumacı Davranış Puanı, Suça Maruziyet Puanı, Tehlike Algısı Puanı, Siber Zorbalığa İlişkin Duyarlılık Puanlarının Betimleyici Tablosu

		N	$\overline{X}$	SS.
Riskli Davranış Ölçeği Puanı	15	29	45.31	10.50
	16	100	46.14	10.82
	17	129	47.87	13.01
	18	92	59.26	16.02
	19	18	63.27	14.14
	Toplam	368	50.80	14.45
Korumacı Davranış Ölçeği Puanı	15	29	56.86	14.32
	16	100	56.83	14.87
	17	129	56.35	15.24
	18	92	60.65	16.38
	19	18	59.16	11.04
	Toplam	368	57.73	15.22
Suça Maruziyet Ölçeği Puanı	15	29	20.62	6.48
	16	100	20.76	8.60
	17	129	22.96	13.36
	18	92	46.36	24.81
	19	18	58.16	20.10
	Toplam	368	29.75	20.26
Tehlike Algısı Ölçeği Puanı	15	29	71.20	10.72
	16	100	68.24	16.79
	17	129	66.62	14.89
	18	92	74.93	14.58
	19	18	78.94	9.21
	Toplam	368	70.10	15.29
Siber zorbalığa ilişkin Duyarlılık Ölçeği	15	29	37.31	4.00

Puanı	16	100	36.35	6.49
	17	129	35.34	6.15
	18	92	32.56	7,10
	19	18	36.33	5,13
	Toplam	368	35.12	6,48

Tablo 9. Yaşa İlişkin Riskli Davranış Puanı, Korumacı Davranış Puanı, Suça Maruziyet Puanı, Tehlike Algısı Puanı, Siber Zorbalığa İlişkin Duyarlılık Puanlarının ANOVA Sonuçları Dağılım Tablosu

Faktörler		Kareler Top.	sd	Kareler Ort.	F	p
Riskli Davranış Puanı	Gruplararası	13536.9	4	3384.2	19.45	.00
	Gruplariçi	63153.6	363	173.9		
	Toplam	76690.5	367			
Korumacı Davranış	Gruplararası	1168.90	4	292.22	1.26	.28
Puanı	Gruplariçi	83902.5	363	231.13		
	Toplam	85071.4	367			
Suça Maruziyet Puanı	Gruplararası	56377.11	4	14094.278	54.27	.00
	Gruplariçi	94266.87	363	259.688		
	Toplam	150643.9	367			
Tehlike Algısı Puanı	Gruplararası	5495.176	4	1373.794	6.20	.00
	Gruplariçi	80357.69	363	221.371		
	Toplam	85852.86	367			
Siber zorbalığa ilişkin	Gruplararası	924.129	4	231.032	5.77	.00
Duyarlılık Puanı	Gruplariçi	14524.868	363	40.013		
	Toplam	15448.997	367			

Öğrencilerin yaşlarına göre yapılan ANOVA analizi sonucunda riskli davranış puanları [$F_{(4,363)}$= 19.45], suça maruziyet puanları [$F_{(4,363)}$= 54.27], tehlike algısı puanları [$F_{(4,363)}$= 6.20] ve siber zorbalığa ilişkin duyarlılık puanlarında [$F_{(4,363)}$= 5.77] istatistiksel olarak anlamlı fark bulunmuştur ($p < .05$). Korumacı davranış puanında ise [$F_{(4,363)}$= 1.26] anlamlı bir farklılık bulunamamıştır ($p > .05$). Farklılık bulunan faktörlerde farklılığın hangi yaşlarda olduğunu bulabilmek için çoklu karşılaştırma testlerinden Tukey HSD testi kullanılmıştır.

Riskli davranış puanında 18 ve 19 yaşındakiler 15, 16 ve 17 yaşındakilere göre anlamlı derecede yüksek puana sahip bulunmuştur. Bunun yanında riskli davranış puanlarında diğer yaş grupları açısından anlamlı farklılık bulunmamaktadır. Suça Maruziyet puanında 19 yaşındakiler 15, 16, 17 ve 18 yaşındakilere, 18 yaşındakiler 15, 16 ve 17 yaşındakilere göre anlamlı derecede yüksek puana sahip bulunmuştur. Bunun yanında suça maruziyet puanında diğer yaş grupları açısından anlamlı

farklılık bulunmamaktadır. Tehlike Algısı Puanında 18 ve 19 yaşındakiler 16 ve 17 yaşındakilere göre daha yüksek puana sahip bulunmuştur. Bununla birlikte tehlike algısı puanlarında diğer yaş grupları açısından anlamlı farklılık bulunmamaktadır. Son olarak Siber zorbalığa ilişkin Duyarlılık Puanında ise 15, 16 ve 17 yaşındakiler 18 yaşındakilere göre daha yüksek puana sahip olduğu bulunmuştur. Bu bulgular ışığında öğrencilerin yaşları arttıkça teknoloji konusundaki güvenlerinin artması nedeniyle bilgi güvenliği konusunda riskli davranış sergileme oranlarının arttığı bununda tehlike algısı, suça maruziyeti arttırdığı söylenebilir.

Araştırmada öğrencilerin öğrenim gördükleri alana göre Riskli Davranış Puanı, Korumacı Davranış Puanı, Suça Maruziyet Puanı, Tehlike Algısı Puanı ve Siber Zorbalığa İlişkin Duyarlık puanları arasında fark olup olmadığını görebilmek için ANOVA testi yapılmıştır. Analiz sonucunda elde edilen betimsel bulgular Tablo 10'da ANOVA sonuçları ise Tablo 11'de yer almaktadır.

Tablo 10. Alana İlişkin Riskli Davranış Puanı, Korumacı Davranış Puanı, Suça Maruziyet Puanı, Tehlike Algısı Puanı, Siber Zorbalığa İlişkin Duyarlılık Puanlarının Betimleyici Tablosu

		N	$\overline{X}$	SS.
Riskli Davranış Ölçeği Puanı	Sosyal Bilimler	62	57.33	17.33
	Fen	203	49.98	14.56
	Eşit Ağırlık	103	48.48	10.91
	Toplam	368	50.80	14.45
Korumacı Davranış Ölçeği Puanı	Sosyal Bilimler	62	62.35	14.32
	Fen	203	57.74	15.91
	Eşit Ağırlık	103	54.93	13.74
	Toplam	368	57.73	15.22
Suça Maruziyet Ölçeği Puanı	Sosyal Bilimler	62	45.12	25.46
	Fen	203	29.13	19.89
	Eşit Ağırlık	103	21.71	9.77
	Toplam	368	29.75	20.26
Tehlike Algısı Ölçeği Puanı	Sosyal Bilimler	62	78.06	12.37
	Fen	203	70.62	14.55
	Eşit Ağırlık	103	64.30	16.04
	Toplam	368	70.10	15.29
Siber zorbalığa ilişkin duyarlılık ölçeği puanı	Sosyal Bilimler	62	36.17	5.46
	Fen	203	36.10	5.63
	Eşit Ağırlık	103	32.56	7.84
	Toplam	368	35.12	6.48

Tablo 11. Alana İlişkin Riskli Davranış Puanı, Korumacı Davranış Puanı, Suça Maruziyet Puanı, Tehlike Algısı Puanı, Siber Zorbalığa İlişkin Duyarlılık Puanlarının ANOVA Sonuçları Dağılım Tablosu

Faktörler		Kareler Top.	sd	Kareler Ort.	F	p
Riskli Davranış Puanı	Gruplararası	3338.98	2	1669.49	8.30	.00
	Gruplariçi	73351.53	365	200.96		
	Toplam	76690.5	367			
Korumacı Davranış	Gruplararası	2132.52	2	1066.26	4.69	.01
Puanı	Gruplariçi	82938.90	365	227.23		
	Toplam	85071.4	367			
Suça Maruziyet Puanı	Gruplararası	21384.04	2	10692.02	30.19	.00
	Gruplariçi	129259.9	365	354.13		
	Toplam	150643.9	367			
Tehlike Algısı Puanı	Gruplararası	7451.66	2	3725.83	17.34	.00
	Gruplariçi	78401.20	365	214.79		
	Toplam	85852.86	367			
Siber zorbalığa ilişkin	Gruplararası	940.99	2	470.49	11.83	.00
Duyarlılık Puanı	Gruplariçi	14508.00	365	39.74		
	Toplam	15448.99	367			

Öğrencilerin öğrenim gördükleri alanlarına göre yapılan ANOVA analizi sonucunda riskli davranış puanlarında [$F_{(2,365)}$= 8.30], suça maruziyet puanlarında [$F_{(2,365)}$= 30.19], tehlike algısı puanlarında [$F_{(2,365)}$= 17.34], siber zorbalığa ilişkin duyarlılık puanlarında [$F_{(2,365)}$= 11.83] ve korumacı davranış puanında [$F_{(2,365)}$= 4.69] istatistiksel olarak anlamlı bir farklılık bulunmuştur ($p<0.05$). Farklılık bulunan faktör puanlarında farklılığın hangi alanlarda olduğunu bulabilmek için çoklu karşılaştırma testlerinden Tukey HSD testi kullanılmıştır.

Riskli davranış puanında Sosyal Bilimler alanında öğrenim gören öğrencilerin Fen ve Eşit Ağırlık alanında öğrenim gören öğrencilere göre daha yüksek puana sahip olduğu bulunmuştur. Fen ve Eşit Ağırlık alanında öğrenim gören öğrenciler arasında riskli davranış puanı açısından anlamlı farklılık yoktur. Korumacı davranış puanında Sosyal Bilimler alanında öğrenim gören öğrencilerin Eşit Ağırlık alanında öğrenim gören öğrencilere göre daha yüksek puana sahip olduğu bulunmuştur. Diğer alanlar arasında korumacı davranış puanına göre anlamlı bir fark bulunmamıştır. Suça Maruziyet puanında Sosyal Bilimler alanında öğrenim gören öğrencilerin Eşit Ağırlık ve Fen alanlarında öğrenim gören öğrencilere, Fen alanında öğrenim gören öğrencilerin Eşit Ağırlık alanında öğrenim gören öğrencilere göre daha yüksek puana sahip olduğu bulunmuştur. Tehlike algısı puanında Sosyal Bilimler alanında öğrenim

gören öğrencilerin Fen ve Eşit Ağırlık alanında öğrenim gören öğrencilere , Fen alanında öğrenim gören öğrencilerin Eşit Ağırlık alanında öğrenim gören öğrencilere göre daha yüksek puana sahip olduğu bulunmuştur. Siber zorbalığa ilişkin duyarlılık puanında Sosyal Bilimler ve Fen alanlarında öğrenim gören öğrencilerin Eşit Ağırlık alanında öğrenim gören öğrencilere göre daha yüksek puana sahip olduğu bulunmuştur. Bu bulgular ışığında sosyal bilimler alanında öğrenim gören öğrencilerin bilgi güvenliğinde daha çok problemli davranış sergiledikleri söylenebilir.

Araştırmada öğrencilerin önceden güvenlik eğitimi alıp almamalarına göre Riskli Davranış Puanı, Korumacı Davranış Puanı, Suça Maruziyet Puanı, Tehlike Algısı Puanı ve Siber Zorbalığa İlişkin Duyarlık puanları arasında fark olup olmadığını görebilmek için t-testi yapılmıştır. Analiz sonucunda elde edilen betimsel bulgular Tablo 12'de yer almaktadır.

Tablo 12. Güvenlik Eğitimine İlişkin Riskli Davranış Puanı, Korumacı Davranış Puanı, Suça Maruziyet Puanı, Tehlike Algısı Puanı, Siber Zorbalığa İlişkin Duyarlılık Puanlarının T-testi Sonuçları Dağılım Tablosu

Faktörler	Güvenlik Eğitimi	N	$\overline{X}$	S	sd	t	p
Riskli Davranış Puanı	Evet	56	55.16	13.10	366	2.46	.014
	Hayır	312	50.01	14.56			
Korumacı Davranış Puanı	Evet	56	62.30	15.21	366	2.45	.015
	Hayır	312	56.91	15.10			
Suça Maruziyet Puanı	Evet	56	28.71	18.73	366	.41	.677
	Hayır	312	29.94	20.54			
Tehlike Algısı Puanı	Evet	56	68.35	15.09	366	.92	.353
	Hayır	312	70.41	15.33			
Siber Zorbalığa İlişkin	Evet	56	34.55	7.29	366	.71	.473
Duyarlılık Puanı	Hayır	312	35.23	6.33			

Öğrencilerin güvenlik eğitimi alıp almamalarına göre Riskli Davranış Puanı, Korumacı Davranış Puanı, Suça Maruziyet Puanı, Tehlike Algısı Puanı ve Siber Zorbalığa İlişkin Duyarlık puanlarında farklılık olup olmadığını anlamak için yapılan t-testi sonucuna göre riskli davranış puanı ($t_{(366)}$= 2.46) ve korumacı davranış puanlarında ($t_{(366)}$= 2.45), istatistiksel olarak anlamlı farklılık ($p< .05$) bulunmuştur. Bunun yanında suça maruziyet puanı ($t_{(366)}$=.41), tehlike algısı puanı ($t_{(366)}$=.92) ve siber zorbalığa ilişkin duyarlık ($t_{(366)}$= .71) puanlarında güvenlik eğitimi alıp

almamasına göre anlamlı bir farklılık (p> .05) bulunamamıştır. Anlamlı farklılık bulunan faktörlerden riskli davranış puanında güvenlik eğitimi aldığını ifade eden öğrencilerin ($\overline{X}$=55,16) güvenlik eğitimi almadığını ifade eden öğrencilere göre ($\overline{X}$=50,01) istatistiksel olarak anlamlı derecede daha fazla riskli davranış gösterdikleri bulunmuştur. Korumacı davranış puanında da güvenlik eğitimi aldığını ifade eden öğrencilerin ($\overline{X}$=62,30) güvenlik eğitimi almadığını ifade eden öğrencilere göre ($\overline{X}$=56,91) istatistiksel olarak anlamlı derecede daha fazla korumacı davranış gösterdikleri bulunmuştur.. Bu bulgular ışığında güvenlik eğitimi alan öğrencilerin riskli ve korumacı davranış sergileme oranlarının yüksek olduğu söylenebilir.

Araştırmada öğrencilerin internet kullanım süresine göre Riskli Davranış Puanı, Korumacı Davranış Puanı, Suça Maruziyet Puanı, Tehlike Algısı Puanı ve Siber Zorbalığa İlişkin Duyarlık puanları arasında fark olup olmadığını görebilmek için ANOVA testi yapılmıştır. Analiz sonucunda elde edilen betimsel bulgular Tablo 13'de ANOVA sonuçları ise Tablo 14'de yer almaktadır.

Tablo 13. İnternet Kullanım Süresine İlişkin Riskli Davranış Puanı, Korumacı Davranış Puanı, Suça Maruziyet Puanı, Tehlike Algısı Puanı, Siber Zorbalığa İlişkin Duyarlılık Puanlarının Betimleyici Tablosu

		N	$\overline{X}$	SS.
Riskli Davranış Ölçeği Puanı	1 saate kadar	104	43.71	12.93
	1-3 saat arası	211	53.10	14.46
	3 saatten fazla	53	55.54	12.38
	Toplam	368	50.80	14.45
Korumacı Davranış Ölçeği Puanı	1 saate kadar	104	53.24	16.85
	1-3 saat arası	211	59.18	14.04
	3 saatten fazla	53	60.79	14.79
	Toplam	368	57.73	15.22
Suça Maruziyet Ölçeği Puanı	1 saate kadar	104	21.65	13.24
	1-3 saat arası	211	32.08	21.39
	3 saatten fazla	53	36.37	22.42
	Toplam	368	29.75	20.26
Tehlike Algısı Ölçeği Puanı	1 saate kadar	104	66.61	18.15
	1-3 saat arası	211	70.48	13.94
	3 saatten fazla	53	75.45	12.59
	Toplam	368	70.10	15.29
Siber Zorbalığa İlişkin Duyarlılık Ölçeği Puanı	1 saate kadar	104	35.85	7.19
	1-3 saat arası	211	35.14	5.93
	3 saatten fazla	53	33.62	7.00
	Toplam	368	35.12	6.48

Tablo 14. İnternet Kullanım Süresine İlişkin Riskli Davranış Puanı, Korumacı Davranış Puanı, Suça Maruziyet Puanı, Tehlike Algısı Puanı, Siber Zorbalığa İlişkin Duyarlılık Puanlarının ANOVA Sonuçları Dağılım Tablosu

Faktörler		Kareler Top.	sd	Kareler Ort.	F	p
Riskli Davranış Puanı	Gruplararası	7540.33	2	3770.16	19.90	.00
	Gruplariçi	69150.18	365	189.45		
	Toplam	76690.5	367			
Korumacı Davranış	Gruplararası	3039.93	2	1519.96	6.76	.00
Puanı	Gruplariçi	82031.49	365	224.74		
	Toplam	85071.4	367			
Suça Maruziyet Puanı	Gruplararası	10295.533	2	5147.76	13.38	.00
	Gruplariçi	140348.45	365	384.51		
	Toplam	150643.9	367			
Tehlike Algısı Puanı	Gruplararası	2812.42	2	1406.21	6.18	.00
	Gruplariçi	83040.43	365	227.50		
	Toplam	85852.86	367			
Siber zorbalığa ilişkin	Gruplararası	175.26	2	87.63	2,094	.12
Duyarlılık Puanı	Gruplariçi	15273.73	365	41.48		
	Toplam	15448.99	367			

Öğrencilerin internet kullanım sürelerine ilişkin Riskli Davranış Puanı, Korumacı Davranış Puanı, Suça Maruziyet Puanı, Tehlike Algısı Puanı ve Siber Zorbalığa İlişkin Duyarlık Puanları arasında farklılık olup olmadığını anlamak için ANOVA testi yapılmıştır. Yapılan test sonucunda öğrencilerin riskli davranış puanı [$F_{(2,365)}$= 19,9], korumacı davranış puanı [$F_{(2,365)}$= 6,76], suça maruziyet puanı [$F_{(2,365)}$= 13,38] ve tehlike algısı puanında [$F_{(2,365)}$=6,181] anlamlı farklılık ($p< .05$) görülmüştür. Siber zorbalığa ilişkin duyarlılık puanlarında ise internet kullanım sıklığına göre anlamlı bir farklılık görülmemiştir ($F_{(2,365)}$= 2,09; $p>0.05$). Hangi gruplar arasında anlamlı farklılık oluşup oluşmadığını anlamak için çoklu karşılaştırma testlerinden Tukey HSD testi yapılmıştır. Ortaya çıkan sonuçlara göre günde ortalama olarak 1-3 saat arası internet kullananlar ve 3 saatten fazla internet kullananların riskli davranış puanları, korumacı davranış puanları ve suça maruziyet puanları günde 1 saatten az internet kullananlara göre anlamlı derecede yüksek bulunmuştur. Tehlike algısı puanına göre ise günlük 3 saatten fazla internet kullananların puanları 1 saatten az internet kullananların puanlarına göre anlamlı derecede yüksek bulunmuştur. Bu bulgular ışığında öğrencilerin internet kullanım sürelerinin artmasının bilgi güvenliği konusunda riskli davranış göstermelerini arttırdığı ve bilgi güvenliğinde daha çok problemli davranış sergiledikleri söylenebilir.

BÖLÜM V: SONUÇ, TARTIŞMA VE ÖNERİLER

5.1. SONUÇ VE TARTIŞMA

Siber zorbalığa ilişkin duyarlılığı yordayan değişkenlere bakıldığında tehlike algısının ve suça maruziyetin anlamlı yordayıcı olduğu ortaya çıkmıştır. Bu açıdan bilgi ve iletişim teknolojilerinin tehlikelerini bilen ya da internet ve bilgisayar üzerinden zorbalığa ya da saldırıya maruz kalmış bireylerde siber zorbalığa ilişkin duyarlılık düzeyi yüksek olduğu düşünülmektedir. Gençlerin teknolojik araçların avantajlarının yanında doğurduğu tehlikeleri de bilmesi önem arz etmektedir. Sanal zorbalık olayları daha çok evlerde yaşanmasından dolayı bu olayların önlenmesinde ailelere daha fazla görev düşmektedir. Özellikle günümüzde okullarda teknoloji kullanımını temel alan projelerin yaygınlaşması ve her öğrencinin bir tablet bilgisayarı olacağı düşünüldüğünde bu araçların kullanılmasına yönelik eğitimler verilirken amacı doğrultusunda kullanıma yönelik bilgiler verilmesi oldukça önemlidir (Ayas ve Horzum, 2012: 14).

Araştırma sonucunda erkek öğrencilerin kadın öğrencilere göre bilgisayar ve internet kullanımında daha fazla riskli davranış gösterdiği aynı zamanda daha korumacı davrandığı da görülmektedir. Bununla birlikte erkek öğrencilerin kadın öğrencilere göre daha çok suça maruz kaldığını ve tehlike algılarının da daha yüksek olduğu ortaya çıkmıştır. Son olarak Siber zorbalığa ilişkin duyarlılıkta ise kadın öğrencilerin erkek öğrencilere göre daha duyarlı olduğu görülmektedir. Yapılan araştırmalar erkeklerin kadınlara göre daha problemli internet kullanımı sergilediklerini desteklemektedir (Çelik ve Odacı, 2012; Horzum, 2011; Kelleci ve diğ.,2009; Öztürk ve Özmen, 2011). Buna göre cinsiyetin riskli davranış, korumacı davranış ve siber zorbalığa ilişkin duyarlılıkta önemli bir faktör olduğu düşünülmektedir. Horzum'a (2011) göre bunun sebebi olarak ülkemizde bilgisayar ve internet gibi araçların erkek oyuncağı olarak görülmesi ve erkeklerin internet kafeleri daha kolay kullanmaları gösterilebilir.

Öğrencilerin yaşlarına ilişkin yapılan istatistiksel işlem sonucunda öğrencilerin yaşları arttıkça riskli davranış puanlarının arttığı ortaya çıkmıştır. Bununla birlikte en

çok suça maruz kalmış öğrencilerde 19 yaş grubu öğrencilerdir. Siber zorbalığa ilişkin duyarlılık puanında ise yaş faktörünün küçük yaşlarda daha yüksek olduğu ve en yüksek duyarlılık gösteren grubun 15 yaş olduğu bulunmuştur. Orhan ve Akkoyunlu (2004) tarafından ilköğretim öğrencileri üzerinde yapılan çalışmada, öğrencilerin yaşları büyüdükçe internet kullanma oranında artış olduğu, oyun amaçlı kullanımın yaş büyüdükçe azaldığı bunun yerine bilgiye ulaşma, haberleşme gibi amaçların aldığı görülmüştür. Buna göre yaşın internet kullanımında önemli bir faktör olduğu ve ilerleyen yaşlarda internet kullanım amacının değiştiği düşünülmektedir.

Öğrencilerin öğrenim gördükleri alanlara göre yapılan istatistiksel işlem sonucunda sosyal bilimler alanını seçen öğrencilerin bütün ölçek puan türlerinde en yüksek puanları aldıkları bulunmuştur. Yine araştırmaya katılan öğrencilerin güvenlik eğitimi alıp almama durumlarına göre yapılan istatistiksel işlem sonucunda riskli ve korumacı davranış puanlarında anlamlı farklılık görülmüştür. Daha önce güvenlik eğitimi alan öğrencilerin riskli davranış puanları almayan öğrencilere göre daha yüksektir. Ayrıca korumacı davranış puanlarında da güvenlik eğitimi almış öğrencilerin puanları, güvenlik eğitimi almamış öğrencilerin puanlarına göre daha yüksektir. Bu nedenle güvenlik eğitimi almış öğrencilerin internet ve bilgisayar güvenliği konusunda bilgi sahibi oldukları ama riskli davranış göstermeye devam ettikleri düşünülmektedir. Bunun sebebi olarak öğrencilerin sahip olduğu güvenlik bilgisinin ona zarar gelmesini engelleyebilecek nitelikte olduğu düşüncesi gösterilebilir.

Araştırmaya katılan lise öğrencilerinden interneti günlük ortalama olarak 1 saatten az kullanan öğrencilerin Riskli Davranış Puanı, Korumacı Davranış Puanı, Suça Maruziyet Puanı ve Tehlike Algısı Puanları en düşük olmasına rağmen Siber zorbalığa ilişkin duyarlılıklarının en yüksek olduğu bulunmuştur. Bu sonuçlara dayanarak, öğrencilerin internet kullanım sürelerine ebeveynler tarafından öğrencilerin akademik başarılarını, fiziki ve psikolojik gelişimlerini etkilemeden izin verilmesi gerektiği düşünülmektedir.

5.2. ÖNERİLER

Araştırma sonucunda bilgi ve iletişim teknolojilerine olan tehlike algısının ve suça maruziyetin, siber zorbalığa ilişkin duyarlılığın yordayıcı modellerinden biri olduğu

ortaya çıkmıştır. Bu model siber zorbalığa ilişkin duyarlılığın %12'sini açıklamaktadır. Geriye kalan %88'lik bölümün açıklanması için birçok ve farklı değişkenler araştırmacılar tarafından denenebilir.

Araştırmada sosyal bilimler alanında öğrenim gören öğrencilerin riskli davranışları sergilemelerinin diğer alanlara göre fazla olmasının nedenlerini incelemek üzere daha derinlemesine araçları kullanım amaçları ve bilgi güvenliğinin en çok hangi durumlarda ve koşullarda gerçekleştiğini ortaya koyan çalışmalar yürütülebilir.

Yine lise öğrencilerinin günlük ortalama internet kullanım süreleri 1 saati geçtiğinde bilgi güvenliği konusunda problemler yaşındığı ortaya çıkmıştır. İnternetin 1 saatten fazla kullanımlarında kullanım amacının dışına çıkılabilmektedir. Bu yönüyle öğrencilerin internet kullandığı alanlar olan ev, okul ve internet kafelerde özel koruma programları ile internet kullanım saatleri denetlenebilir.

Bu araştırmada gençlerin bilgi güvenliği ve siber zorbalık konularında var olan durumları tarama modeli yoluyla ortaya koyulmaya çalışılmıştır. Mevcut durumun dışında bilgi güvenliği farkındalığı, bilgi güvencesi (information assurance) gibi konular hakkında gençler ve yetişkinlere eğitimler verilebilir. Bu eğitimler ve eğitimlerde uygulanan programların yeterlilikleri ölçülebilir. Farklı alanlarda çalışan akademisyenlerden oluşan araştırma grupları multidisipliner bir çalışmayla bilgi ve iletişim teknolojilerini tanımanın ve yeniliğe bakış açısının bilgi güvenliği konusu üzerine olan etkilerini inceleyebilirler.

Ayrıca, bilgi güvenliği farkındalığı ve siber zorbalığa ilişkin duyarlılık kazandırmak için dinamik olarak hazırlanmış, kullanıcıların etkin olarak katıldığı interaktif siteler ve yazılımlar hazırlanabilir. Bu yazılımlar içinde testler, örnekler ve çeşitli olaylar kullanılarak alıştırmalar hazırlanabilir. Bu yazılımlar yeni risklere ve sosyal ağlara göre güncel tutulmalı ve kullanıcıları aktif halde tutabilmelidir. Ayrıca Bilgisayar ve Öğretim Teknolojileri Öğretmenliği programlarında bilgi güvenliğine yönelik bu tür yazılımların hazırlanması proje olarak verilebilir. 8. sınıflarda seçmeli ders olarak alınan İlköğretim Medya Okuryazarlığı (2008) dersinin içeriğinde "İnternet Kullanıyorum" ve "İnternet Dost Mu? Düşman Mı?" başlıklı ünitelerde "İnternette bilgiye erişim, haber okuma, sohbet, e-posta, uzaktan eğitim, oyun gibi etkinlikleri uygulamalı olarak gerçekleştirir" ve "İnternetin olumlu özelliklerinin yanı sıra olumsuz etki ve özelliklerini tanıyarak hayata geçirir." kazanımları bulunmaktadır.

Bu kazanımların yanında bilgi güvenliğinin sağlanması, kişisel bilgileri korumanın önemi, siber zorbalık kavramı, siber zorbalığın risk faktörleri ve etkileri gibi konularda programa eklenebilir.

Bu araştırma lise öğrencilerinin bilgi güvenliği farkındalığını ve siber zorbalık duyarlılıklarını incelemek için yapılmıştır. Gelecek araştırmalarda farklı örneklemler seçilerek sonuçlarının tutarlılığı karşılaştırılabilr. Bilgi güvenliği konusunda sadece gençlerin değil, yetişkinlerin özellikle de şirketlerde ve kamu çalışanlarında bilgi güvenliği farkındalığını ölçen araştırmalar yürütülebilir.

Bireylerin kişisel bilgilerini paylaştığı alanlarda hazırlanacak olan talimatlar ve öneriler, bilgileri paylaşmadan önce bilgi güvenliğine dikkat çekebilir. Örneğin; "Birazdan yazacağınız bilgileri istediğiniz dışında insanların da okuyabileceğini ve bu bilgilerin sürekli saklı kalacağını unutmayınız." gibi uyarı yazılarının sitelerde ve diğer paylaşım alanlarında kullanılması bilgi güvenliği farkındalığını artıracağı düşünülmektedir.

Kullanıcıların bilgi güvenliği konusunda kötü niyetli insanları sorumlu tutmaktan öte, çocuklara ve gençlere bilgi güvenliği ve siber zorbalığa ilişkin duyarlılık kazandırma konusunda eğitim verilmelidir. Bu eğitim teknik konuları içermekle birlikte özellikle psikolojik boyutu da unutulmamalıdır. Gençlerin ve çocukların karşılaştıkları siber zorbalık gibi vakalarda çaresiz kalabildikleri göz önüne alındığında psikolojik destek vermenin önemi görülmektedir.

Ülkemizde bilgi güvenliğini zedeleyebilecek her türlü saldırıda alınması gereken önlemleri içeren çeşitli programlar ve seminerler ile çocuklar ve gençler bilgilendirilebilir. Bu sayede bilgi ve iletişim teknolojilerinin zararlarından korunma yolları gösterilirken, güvenlik uzmanı gibi nitelikli insan gerektiren işlere karşı sempati oluşturulabilir. Gelecekte her türlü işlemin siber ortamlarda yapılabileceği düşünülürse siber saldırıların ve hatta siber savaşların yapılacağı da kaçınılmaz olabilecektir. Bu nedenle ülkemizin siber güvenlik, bilgi güvenliği ve diğer güvenlik alanlarında yetişmiş insan gücüne ihtiyacı olacaktır. Bu yetişmiş insan gücü sayesinde milli yazılımlar ve kodlar yazılabilecektir.

Bununla birlikte siber zorbalık konusunda daha önce yapılan çalışmalar çocukların ve gençlerin siber zorba ve siber mağdur olma durumlarını ölçmektedir (Akbulut,

Sahin ve Eristi, 2010; Arıcak ve diğ., 2008; Arıcak, 2009; Ayas, 2011; Ayas ve Horzum, 2012; Aydoğan, Dilmaç ve Deniz, 2009; Dilmaç 2009; Dilmaç ve Aydoğan, 2010; Dursun ve Akbulut, 2010; Erdur-Baker ve Kavsut ,2007; Erdur-Baker ve Tanrıkulu, 2009; Erdur-Baker, 2010; Eroğlu ve Peker, 2011; Topçu, Erdur-Baker ve Çapa –Aydın, 2008). Bu araştırma siber zorbalığa ilişkin duyarlılığı ölçen ilk çalışmalardan biridir. Gelecek araştırmalarda siber zorbalığa ilişkin duyarlılığın öz yeterlilik, sosyal zeka, motivasyon, teknolojiye karşı tutum gibi değişkenler ile birlikte incelenebilir. Ayrıca siber zorbalık konusunda kurulacak bir kurul geliştirilmiş anket ve test maddelerini birleştirerek en ideal siber zorba ve mağdur ölçeklerini oluşturabilir. Böyle bir çalışma siber zorbalığa ilişkin hazırlanacak ortak bir müdahale eğitimini de beraberinde getirecektir.

KAYNAKÇA

Akbulut, Y., Sahin, Y. L., ve Erişti, B. (2010a). Cyberbullying victimization among Turkish online social utility members. *Educational Technology & Society, 13* (4), 192–201.

Akolaş, A. (2004). Bilişim Sistemleri ve Bilişim Teknolojisinin Küreselleşme Olgusu ve Girişimcilik Üzerine Yansımaları. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *12*, 29–43.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, *26*(4), 276–289. doi:16/j.cose.2006.11.004

Anderson, W. L. (2010). Cyber Stalking (Cyber Bullying) - Proof and Punishment. *Insights to a Changing World Journal*, *4*, 18-23.

Arıcak, T.; Siyahhan, S.; Uzunhasanoglu, A.; Sarıbeyoglu, S.; Cıplak, S.; Yılmaz, N. ve Memmedov, C. (2008).Cyberbullying among Turkish Adolescents. *Cyberpsychology & Behavior*, *11*(3), 253-261.

Arıcak, O. T. (2009). Psychiatric symptomatology as a predictor of cyberbullying among university students. *Eurasian Journal of Educational Research*, *34*, 167-184.

Arıcak, O.T. (2011). Siber zorbalık: gençlerimizi bekleyen yeni tehlike. *Kariyer Penceresi (Fatih Üniversitesi Aylık Bülteni)*, *2*(6),10-12.

Ayas, T. (2011). Lise öğrencilerinin sanal zorba ve mağdur olma yaygınlığı. *XI. Ulusal Psikolojik Danışma ve Rehberlik Kongresi*, 3–5 Ekim, İzmir.

Ayas, T. ve Horzum, M.B. (2011). İlköğretim öğrencilerinin sanal zorba ve mağdur olma durumu. *İlköğretim Online, 11*(2), 369-380,

Ayas T. ve Horzum M. B. (2010). Sanal Zorba / Kurban Ölçek Geliştirme Çalışması, *Akademik Bakış Dergi,19*, 3-5.

Ayas, T. ve, Horzum M.B. (2012). İlköğretim Öğrencilerinin Sanal Zorba ve Mağdur Olma Durumu. *İlköğretim Online Dergisi*,*11*(2), 369-380.

Aydoğan, D., Dilmaç, B. ve Deniz, M. E. (2009). İlköğretim Öğrencilerinde Sosyal Destek ve Siber Zorbalığın İncelenmesi. *18. Ulusal Eğitim Bilimleri Kurultayı*, 1-3 Ekim, İzmir.

Baker Erdur, Ö. ve Kavşut, F. (2007). Akran Zorbalığının Yeni Yüzü: Siber Zorbalık. *Eğitim Araştırmaları*, *27*, 31.

Belsey. B. (2007). Cyberbullying. www.cyberbullying.ca (Erişim tarihi 23.04.2012)

Burlu, K. (2010). *Bilişimin Karanlık Yüzü*. Ankara: Nirvana Yayınları.

Calvete, E., Orue, I., Estévez, A., Villardón, L., ve Padilla, P. (2010). Cyberbullying in adolescents: Modalities and aggressors' profile. *Computers in Human Behavior*, *26*(5), 1128-1135. doi:10.1016/j.chb.2010.03.017

Canbek, G., ve Sağıroğlu, Ş. (2007). Çocukların ve gençlerin bilgisayar ve internet güvenliği. *Politeknik Dergisi*, *10*(1), 33.

Canbek, G., ve Sağıroğlu, Ş. (2008). Casus yazılımlar: Bulaşma yöntemleri ve önlemler. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, *23*(1), 165.

Canbek, G., ve Sağıroğlu, S. (2007). Kötücül Ve Casus Yazılımlar: Kapsamlı Bir Araştırma. *Journal of the Faculty of Engineering ve Architecture of Gazi University*, *22*(1), 121–136.

Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., ve Upadhyaya, S. (2006). Role of Perceived Importance of Information Security: An Exploratory Study of Middle School Children's Information Security Behavior. *Issues in Information Science and Information Technology (IISIT)*, 3(61),127-135.

Cowie, H., ve Colliety, P. (2010). Cyberbullying: sanctions or sensitivity? *Pastoral Care in Education*, *28*(4), 261-268. doi:10.1080/02643944.2010.528017

Çelik, Ç., ve Odacı, H. (2012). Kendilik Algısı ve Benlik Saygısının Problemli İnternet Kullanımı Üzerindeki Yordayıcı Rolü. *E-Journal Of New World Sciences Academy (NWSA)*,*7*(1), 433-441.

Çetinkaya, B.(2010). *İlköğretim İkinci Kademe Öğrencilerinde Siber Zorbalığın Yaygınlığı*. Basılmamış Yüksek lisans Tezi. Selçuk Üniversitesi Eğitim Bilimleri Enstitüsü. Konya

Çifçi, S.(2010). *Dokuzuncu Sınıf Öğrencilerinin Sanal Zorbalık Düzeyleri ile Empatik Eğilim Düzeyleri Arasındaki İlişki*. Basılmamış Yüksek Lisans Tezi. Gaziosmanpaşa Üniversitesi Sosyal Bilimler Enstitüsü. Tokat.

Dehue, F., Bolman, C., ve Völlink, T. (2008). Cyberbullying: Youngsters' Experiences and Parental Perception. *CyberPsychology and Behavior*, *11*(2), 217-223. doi:10.1089/cpb.2007.0008

Diamanduros, T., Downs, E., ve Jenkins, S. J. (2008). The role of school psychologists in the assessment, prevention, and intervention of cyberbullying. *Psychology in the Schools*, *45*(8), 693-704. doi:10.1002/pits.20335

Dilmaç, B. ve Aydoğan, D. (2010). Values as a Predictor of Cyber-bullying Among Secondary School Students. *International Journal of Human and Social Sciences, 5*(3), 185-188.

Dilmaç, B.(2009) Cyber bullying: a Preliminary Report on College Students. *Kuram ve Uygulamada Eğitim Bilimleri*, *9*(3), 1307-1325.

Dursun, Ö. Ö., & Akbulut, Y. (2010). Investigation of cyberbullying victimization and communication styles in a hybrid learning environment. Paper presented at IODL & ICEM International Joint Conference and Media Days, Eskisehir, Turkey.

Dooley, J. J., Gradinger, P., Strohmeier, D., Cross, D., ve Spiel, C. (2010). Cyber-Victimisation: The Association Between Help-Seeking Behaviours and Self-Reported Emotional Symptoms in Australia and Austria. *Australian Journal of Guidance and Counselling*, *20*(2), 194-209. doi:10.1375/ajgc.20.2.194

Dowell, E.B., A.W. Burgess ve D.J. Cavanaugh, (2009), Clustering of Internet Risk Behaviors in a Middle School Student Population, *Journal Of School Health*, *79*(1), 547-553.

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

Eminağaoğlu, M., ve Gökşen, Y. (2009). Bilgi Güvenliği Nedir, Ne Değildir, Türkiyede Bilgi Güvenliği Sorunları ve Çözüm Önerileri. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *11*(4), 01–15.

Erdur-Baker, Ö (2010), "Cyberbullying and its correlation to traditional bullying, gender and frequent and risky usage of internet-mediated communication tools", *New Media & Society, 12*, 109-125.

Erdur-Baker, Ö. ve Tanrıkulu, İ. (2010), Psychological consequences of cyberbullying experiences among Turkish secondary school children, *Procedia-Social And Behavioral Sciences, 2*, 2771-2776.

Erdur-Baker, Ö., Yerin-Güneri, O. ve Akbaba-Altun, S. (2006). Bilgi ve iletişim teknolojileri çocukları ve gençleri nasıl etkiliyor? MEB, 1. Şiddet ve Okul: Okul ve Çevresinde Çocuğa yönelik Şiddet ve Alınabilecek Tedbirler. Uluslarası Katılımlı Sempozyum. İstanbul.

Erdur-Baker, Ö. ve Kavşut, F. (2007). Akran Zorbalığının Yeni Yüzü: Siber Zorbalık. *Eğitim Araştırmaları, 27*, 31-42.

Erdur-Baker, Ö., ve Tanrıkulu, İ. (2009). Cyber bullying in Turkey: Its correlates and links to depressive symptoms. *Journal of eHealth Technology and Application*, *7*, 16-23.

Eroğlu,Y. ve Peker, A.(2010). Aileden ve arkadaştan alınan sosyal destek ve siber mağduriyet.Yapısal eşitlik modeliyle bir inceleme. *Akademik Bakış, 27*,1-20

Fraenkel, J., Wallen, N., ve Hyun, H. (2011). *How to Design and Evaluate Research in Education* (8th ed.). McGraw - Hill Humanities / Social Sciences / Languages. San Francisco.

Furnell S, Tsaganid i V, Phippen A. (2008b). Security beliefs and barriers for novice Internet users. *Computers & Security*, *27*, 235.e40.

Goebert, D., Else, I., Matsu, C., Chung-Do, J., ve Chang, J. (2011). The Impact of Cyberbullying on Substance Use and Mental Health in a Multiethnic Sample. *Maternal & Child Health Journal*, 15, 282-1286.

Grigg, D. W. (2010). Cyber-Aggression: Definition and Concept of Cyberbullying. *Australian Journal of Guidance and Counselling*, *20*(2), 143-156. doi:10.1375/ajgc.20.2.143

Hinduja, S. ve Patchin, J. W. (2005). Research summary: Cyberbullying victimization. Preliminary findings from an online survey of Internet-using adolescents. (http://cyberbullying.us).

Hinduja, S., ve Patchin, J. W. (2010). Bullying, Cyberbullying, and Suicide. *Archives of Suicide Research*, *14*(3), 206-221. doi:10.1080/13811118.2010.494133

Horzum, M.B. (2011). İlköğretim Öğrencilerinin Bilgisayar Oyunu Bağımlılık Düzeylerinin Çeşitli Değişkenlere Göre İncelenmesi. *Eğitim ve Bilim*, *36*(159), 56-68.

Talim ve Terbiye Kurulu.(2008). İlköğretim Medya Okuryazarlığı Dersi Ders Kitabı Ünitelendirilmiş Yıllık Plan. Ankara.

Jäger, T., Amado, J., Matos, A., ve Pessoa, T. (2010). Analysis of Experts' and Trainers' Views on Cyberbullying. *Australian Journal of Guidance and Counselling*, *20*(2), 169-181. doi:10.1375/ajgc.20.2.169

Jose, P. E., Kljakovic, M., Scheib, E., ve Notter, O. (2012). The Joint Development of Traditional Bullying and Victimization With Cyber Bullying and Victimization in Adolescence. *Journal of Research on Adolescence*, 22,

301–309. doi: 10.1111/j.1532-7795.2011.00764.x

Kaçakcılık ve Organize Suçlar Daire Başkanlığı.(2011). *Kaçakcılık ve Organize Suçlarla Mücadele 2011 Raporu*. Ankara: KOM Yayınları.

Kaptan, S.(1993). *Bilimsel Araştırma ve İstatistik Teknikleri*. Ankara: Rehber Yayınevi.

Karasar, N. (2009). *Bilimsel araştırma yöntemi*. Ankara: Nobel Yayınevi.

Katzer, C., Fetchenhauer, D., ve Belschak, F. (2009). Cyberbullying: Who Are the Victims? *Journal of Media Psychology: Theories, Methods, and Applications*, *21*(1), 25-36. doi:10.1027/1864-1105.21.1.25

Keith, S. ve Martin, M. E. (2005). Cyber-bullying: Creating a culture of respect in a cyber world. *Reclaiming Children and Youth*, *13*, 224-228.

Kelleci M, Güler N, Sezer H, Gölbaşı Z.(2009). Lise Öğrencilerinde İnternet Kullanma Süresinin Cinsiyet Ve Psikiyatrik Belirtiler İle İlişkisi. *TAF Prev Med Bull*. *8*(3), 223-230.

Kowalski, R. M., Limber, P. ve Agatston, P.W. (2008), *Bullying In The Digital Age*, Blackwell Publishing, Boston.

Krejcie, V. ve Morgan, W.(1970). Determining Sample Size for Research Activities. *Educational and Psychological Measurement.30*: 607-610.

Kritzinger, E., ve von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, *29*(8), 840–847. doi:16/j.cose.2010.08.001

Kumaş, E.(2009). *Bilgi Güvenliğinin Sağlanmasında Risk Yönetimi: E-Devlet Kapısı Uygulaması*. Basılmamış Yüksek Lisans Tezi. Kırıkkale Üniversitesi Fen Bilimleri Enstitüsü. Kırıkkale.

Li, Q. (2005). New bottle but old wine: A research of cyber bullying in schools. Computers in Human Behavior. (01.11.2006). www.elsevier.com/locate/comphumbeh.

Li, Q. (2005a). Gender and CMC: A review on conflict and harassment. *Australian Journal of Educational Technology*, *21*, 382-406.

Mason, K. L. (2008). Cyberbullying: A preliminary assessment for school personnel. *Psychology in the Schools*, *45*(4), 323-348. doi:10.1002/pits.20301

Mesch, G. S. (2009). Parental Mediation, Online Activities, and Cyberbullying. *CyberPsychology & Behavior*, *12*(4), 387-393. doi:10.1089/cpb.2009.0068

Milli Eğitim Bakanlığı. (2012). *Milli Eğitim İstatistikleri 2011-2012 Örgün Eğitim*. Ankara

Morales, M. (2011). Cyberbullying. *Journal of Consumer Health On the Internet*, *15*(4), 406-419. doi:10.1080/15398285.2011.623593

NCH ve Tesco Mobile (2005). Putting u in the picture-Mobile bullying survey of 2005. www.stoptextbully.com.

Nelson, M. (2003). School bullies going high tech. (29.11.2005) http://canoe.ca/NewsStand/-LondonFreePress/2003/09/02/174030.

Nocentini, A., Calmaestra, J., Schultze-Krumbholz, A., Scheithauer, H., Ortega, R., ve Menesini, E. (2010). Cyberbullying: Labels, Behaviours and Definition in Three European Countries. *Australian Journal of Guidance & Counselling*, *20*(2), 129–142. doi:10.1375/ajgc.20.2.129

Orhan, F., ve Akkoyunlu, B. (2004). İlköğretim Öğrencilerinin İnternet Kullanımları Üzerine Bir Çalışma. *Hacettepe Üniversitesi Eğitim Fakültesi*, 26, 107.

Öğütcü, G. (2010). *E-Dönüşüm Sürecinde Kişisel Bilişim Güvenliği Davranışı ve Farkındalıklarının Analizi*. Basılmamış Yüksek lisans tezi. Başkent Üniversitesi Fen Bilimleri Ensitütü. Ankara.

Özdamar. K.(2010). *Modern Bilimsel Araştırma Yöntemleri*. Eskişehir. Kaan Kitabevi.

Öztürk, E., ve Özmen, S. (2011). Öğretmen Adaylarının Problemli internet kullanım davranışlarının, kişilik tipi, utangaçlık ve demografik değişkenlere göre incelenmesi. *Kuram Ve Uygulamada Eğitim Bilimleri*, *11*(4), 1785.

Patchin, J. W., ve Hinduja, S. (2010b). Traditional and Nontraditional Bullying Among Youth: A Test of General Strain Theory. *Youth & Society*, *43*(2), 727-751. doi:10.1177/0044118X10366951

Peikari, C . Fogie, S. (2002). *Maximum Wireless Security*, ABD: Sams Publishing.

Price, M., ve Dalgleish, J. (2010). Cyberbullying Experiences, impacts and coping strategies as described by Australian young people. *Youth Studies Australia*, *29*(2), 51-59

Raskauskas, J. ve A.D. Stoltz. (2007). "Involvement in traditional and electronic bullying among adolescents", *Developmental Psychology*, *43*, 564-575.

Schneider, S. K., O'Donnell, L., Stueve, A., ve Coulter, R. W. S. (2012). Cyberbullying, School Bullying, and Psychological Distress: A Regional Census of High School Students. *American Journal of Public Health*,

102(1), 171-177. doi:10.2105/AJPH.2011.300308

Schoffstall, C. L., ve Cohen, R. (2011). Cyber Aggression: The Relation between Online Offenders and Offline Social Competence. *Social Development*, *20*(3), 587-604. doi:10.1111/j.1467-9507.2011.00609.x

Schryen, G. (2007), *Anti-Spam Measures: Analysis and Design*. ABD: Springer Science Business Media.

Schultze-Krumbholz, A., ve Scheithauer, H. (2009). Social-Behavioral Correlates of Cyberbullying in a German Student Sample. *Zeitschrift für Psychologie / Journal of Psychology*, *217*(4), 224-226. doi:10.1027/0044-3409.217.4.224

Shariff, S. (2005). Cyber-dilemmas in the new millennium: School obligations to provide student safety in a virtual school environment. *McGill Journal of Education*, *40*(3).

Shariff, S. ve. Gouin, R (2005), "Cyberdilemmas: Gendered Hierarchies, Free Expression and Cyber-Safety in Schools", http://www.oii.ox.ac.uk/microsites/cybersafety/?view=papers, Erişim Tarihi: 30.01.2012.

Siegle, D. (2010). Cyberbullying and Sexting: Technology Abuses of the 21st Century. *Gifted Child Today*, *33*(2), 14-16.

Slonje, R., ve Smith, P. K. (2008). Cyberbullying: Another main type of bullying? *Scandinavian Journal of Psychology*, *49*(2), 147-154. doi:10.1111/j.1467-9450.2007.00611.x

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., ve Tippett, N. (2008). Cyberbullying: its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry*, *49*(4), 376-385. doi:10.1111/j.1469-7610.2007.01846.x

Spears, B., Slee, P., Owens, L., ve Johnson, B. (2009). Behind the Scenes and Screens. *Zeitschrift für Psychologie / Journal of Psychology*, *217*(4), 189-196. doi:10.1027/0044-3409.217.4.189

Sperotto, A.; Schaffrath, G.; Sadre, R.; Morariu, C.; Pras, A.; Stiller, B. (2010) .An Overview of IP Flow-Based Intrusion Detection , *Communications Surveys and Tutorials IEEE*. *12*(3), 343 – 356.

Stallings, W. (2010). *Cryptography and Network Security: Principles and Practice* (5th ed.). Prentice Hall.

Şahinaslan, E.,Kandemir, R.,Şahinaslan, Ö.(2009). Bilgi Güvenliği Farkındalık Eğitim Örneği. *Akademik Bilişim Konferansı*. Şanlıurfa,189-194.

T.C. Ulaştırma Bakanlığı İnternet Üst Kurulu.(2005). İnternet Üst Kurulu SPAM Bildirgesi, Ankara.

Tanrıkulu, T., Kınay, H, Arıcak, O.T.,(2011).Siber Zorbalığa İlişkin Duyarlılık Ölçeği. *XI. Ulusal PDR Kongresi*. 3-5 Ekim. Efes/İzmir.

Topcu, Ç. (2008). *The Relationship Of Cyberbullying to Empathy, Gender, Traditional Bullying, Internet Use and Adult Monitoring*. Basılmamış Yüksek lisans Tezi. Orta Doğu Teknik Üniversitesi Sosyal Bilimler Enstitüsü. Ankara.

Topçu, Ç., Erdur-Baker, Ö., ve Çapa-Aydin, Y. (2008). Examination of cyberbullying experiences among Turkish students from different school types. *CyberPsychology & Behavior, 11* (6), 643-648.

Turhan, O., 2006, Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar), Planlama Uzmanlığı Tezi, Ankara, Türkiye.

Türk Ceza Kanunu.(2004). http://www.tbmm.gov.tr/kanunlar/k5237.html Erişim tarihi: 23.04.2012.

Ulaşanoğlu, M.E., Yılmaz, R.,Tekin M.A.(2010). *Bilgi Güvenliği Riskler ve Öneriler*. Bilgi Teknolojileri ve İletişim Kurumu Raporu. Ankara.

Ural, A., Kılıç İ.,(2006). Bilimsel Araştırma Süreci ve SPSS ile Veri Analizi. *Detay Yayıncılık*. Ankara.s.38

Ünver, M., Canbay, C., (2010). Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik, *Elektrik Mühendisleri Odası Dergisi*. *48*(438) - ISSN 0013-5402, s. 94-103.

Vandebosch, H., ve Van Cleemput, K. (2009). Cyberbullying among youngsters: profiles of bullies and victims. *New Media & Society, 11*(8), 1349-1371. doi:10.1177/1461444809341263

Walker, Jenny, L., (2009), *The Contextualized Rapid Resolution Cycle Intervention Model for Cyberbullying,* Basılmamış Doktora Tezi, Arizona State Üniversitesi.

Wıllard, Nancy (2007), *Cyberbullying And Cyberthreats:Responding To The Challenge Of Online Social Agression, Threats, And Distress*, Champaign Research Press, Illinois.

Wong-Lo, M., Bullock, L. M., ve Gable, R. A. (2011). Cyber bullying: practices to face digital aggression. *Emotional and Behavioural Difficulties*, *16*(3), 317-

325. doi:10.1080/13632752.2011.595098

Yilmaz, H. (2011). Cyberbullying in Turkish middle schools: An exploratory study. *School Psychology International*, *32*(6), 645-654. doi:10.1177/0143034311410262

Yozgat, U. (1998).*Yönetim Bilişim Sistemleri*, İstanbul. Beta Yayınevi.

EKLER

Tezde Kullanılan Ölçekler

Yönerge: Aşağıdaki ifadeleri kullanma sıklığınıza göre cevaplayınız. Yanıtınız yalnızca evet ise her zaman, yalnızca hayır ise hiçbir zaman ifadelerinden birini işaretleyebilirsiniz.

	Her Zaman	**Sık Sık**	**Bazen**	**Nadiren**	**Hiçbir Zaman**
1. Msn Messenger,Gtalk,Skype ve benzeri sohbet programlarını kullanırım					
2. Bir iletişim aracı olarak elektronik posta(e-mail) kullanırım					
3. Birden fazla elektronik posta adresi kullanırım					
4. Kurumsal e-posta adresimi günlük işlerde de kullanırım					
5. Internette e-posta gruplarına üye olurum					
6. Facebook, twitter ve benzeri sosyal ağ sitelerini kullanırım					
7. Sosyal ağlarda gönderilen uygulama davetlerini kabul ederim					
8. İnternet bankacılığı kullanırım					
9. İnternet üzerinden alışveriş yaparım					
10. E-vatandaşlık (turkiye.gov.tr) hizmetleri veren web sayfalarını kullanırım					
11. İnternet üzerinden oyun oynarım					
12. İnternet üzerinden müzik, film, program ve dosya indiririm / kaydederim.					
13. İnternet üzerinden video / film izlerim.					
14. İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (Gsm No, adres, e-posta) paylaşırım.					
15. İnternet ortamında gerektiği durumlarda özlük bilgilerimi paylaşırım. (ad, soyad, doğ. tarihi vb.)					
16. Bilgisayarımda orijinal (lisanslı) yazılım kullanmaya dikkat ederim.					
17. Virüs temizleme, casus yazılım önleme v.b. programları kullanırım					
18. Güvenlik duvarı, reklam önleyici vb. programlar kullanırım.					
19. İçerik filtreleme programları kullanırım					
20. E-posta filtreleme programları kullanırım.					
21. İzleme yazılımları kullanarak internet üzerinde yapılan etkinlikler hakkında bilgi sahibi olurum.					
22. Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim.					
23. Herkesin kullanımına açık bir bilgisayardan ayrılmadan önce geçici internet dosyalarını ve Web gezinti geçmişlerini silerim.					
24. Dosyalarımı şifrelerim.					
25. İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım.					
26. Elektronik / Mobil imza kullanırım					
27.İnternet sitelerine girerken genellikle sık kullanılanlar listesini kullanırım.					

28. Sohbet (chat) yaparken dosya transferi yaparım.					
29. Bilgisayarımdaki dosyaları paylaşıma açarım.					
30. Halka açık internet erişimi olan yerlerde internet bankacılığı kullanırım					
31. İnternette karşılaştığım bilişim suçlarını ilgili makamlara iletirim.					
32. Parolalarımı başkalarıyla paylaşırım.					
33.Parolalarımı yazılı olarak kolay ulaşabileceğim yerlerde saklarım.					
34. Bilgisayarım şifre ile açılır.					
35. Bilgisayarımda otomatik olarak kullan özelliğini kapatırım.					
36. Tanımadığım kişilerden gelen e-postaları açarım, gelen ekleri indiririm.					
	Her Zaman	**Sık Sık**	**Bazen**	**Nadiren**	**Hiçbir Zaman**
37.Girdiğim sitelerin SSL (Güvenlik)sertifikası olup olmadığına dikkat ederim.					
38. Parolalarımı sık sık değiştiririm.					
39. Kablosuz modem şifremi değiştiririm.					
40.Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım					
41. Kullandığım programların güncellemelerini düzenli olarak yaparım.					
42. Bilgisayar virüsleri nedeniyle sorun yaşadım.					
43. Online alışverişten dolayı maddi zarara uğradım.					
44. Kredi kartım kopyalandı.					
45. Kişisel bilgilerimi internette paylaştığım için sıkıntı yaşadım.					
46. Elektronik bankacılık kullandığım için maddi zarara uğradım.					
47.Kişisel bilgilerim iznim olmadan üçüncü şahıslarla paylaşıldı/internette yayınlandı.					
48. İnternet üzerindeki hesaplarıma ait kullanıcı adım ve şifrem ele geçirildi.					
49. İnternette kimliği belirsiz kişiler tarafından şahsıma yönelik hakaret, tehdit, ahlaksız teklif aldım.					
50. Kumar içerikli siteler nedeniyle zarara uğradım.					
51. Sosyal ağ siteleri nedeniyle zarara uğradım.					
52. Arkadaşlık siteleri nedeniyle zarara uğradım.					
53. İnternette gezerken isteğim dışında şiddet ya da pornografik içerikli yayınlarla karşılaştım.					
54. Bilgisayarımdaki dosyalarım çalındı / silindi.					
55. Adıma sahte hesaplar açıldı.					
56. İnternet üzerinden yaptığım yazışmalar isteğim ve bilgim dışında başkaları tarafından izlendi / kaydedildi.					
57.Bilgisayar ve internet güvenliği ile ilgili hukuki gelişmeleri takip ediyorum					
58. Karşılaştığım bir bilişim suçunu nereye bildireceğimi biliyorum					
59.Kişisel bilgilerimin başkaları tarafından kötü amaçlarla kullanılabileceğini biliyorum.					
60. Kredi kartı kullanarak alışveriş yaptığımda kredi kartı bilgilerimin karşı tarafça saklanması benim için önemli değildir.					

61. Hacker olmak isterdim.					
YÖNERGE : Aşağıdaki davranışları ve teknolojilerin kullanımını ne derecede tehlikeli bulduğunuzu işaretleyiniz.	**Çok Tehlikeli**	**Tehlikeli**	**Az Tehlikeli**	**Tehlikesiz**	**Fikrim Yok**
62. Virüs yazılımları					
63. Virüs koruma programları					
64. Casus yazılımlar (Keylogger, Screenlogger, Trojanvb.)					
65. Dosya paylaşım programları (Ares, Limewire vb.)					
66. ActiveX, Javascript vb. mobil kodlar.					
67. Web tarayıcıları (İnternet Explorer, Mozilla Firefox,Google Chrome v.b.)					
68. Sohbet programları (Messenger , ICQ vb.)					
69. İstenmeyen Spam / Junk e-postalar					
70. Online oyunlar					
71. USB / Harici Bellekler					
72. MS Office Uygulamaları (Word, Excel vb.)					
73. Klavye kullanımı					
74. Kopya / Kırık / Korsan program kullanımı					
75. Müzik/ Resim/ Film gibi materyallerin herhangi bir bedel ödemeden indirilmesi					
76. Reklam içerikli e-postaların açılması					
77. Elektronik bankacılık kullanımı					
78. İnternet ortamında yabancılarla sohbet / bilgi paylaşımı					
79. İnternetten alışveriş yapılması					
80. Pornografik içerikli sitelere girilmesi					
81. Kumar , bahis sitelerine girilmesi					
82. Sosyal ağlara üye olunması (Facebook , twitter vb.)					
	Çok Tehlikeli	**Tehlikeli**	**Az Tehlikeli**	**Tehlikesiz**	**Fikrim Yok**
83. Bluetooth kullanımı					
84. Kablosuz modem kullanılması					
85. İnternetten kontör yüklenmesi					
86. Kırık veya ücretsiz güvenlik programı kullanımı					
87. Bina girişlerinde güvenlik birimine nufüs cüzdanı veya sürücü belgesinin teslim edilmesi					
88. Kargo, GSM operatörü vs. gibi kuruluşlara nufüs cüzdanı bilgilerinin verilmesi					
89. Vatandaşlık numarasının başka şahıslar tarafından bilinmesi					

Siber Zorbalık Duyarlılık Ölçeği

Bu ankette günlük hayatta, internet, cep telefonu vb. dijital araçları kullanırken gerçekleşen bazı davranışlara ve düşüncelere yer verilmiştir. Sonuçlar bilimsel amaçla kullanılacaktır. Yanıtlarınızın samimi olması araştırmamızın güvenilir olması için önemlidir. Bu yüzden eğer anketi doldurmak istemiyorsanız lütfen bunu öğretmeninize söyleyiniz. Eğer dolduracaksınız tüm maddeleri okuyup yanıtlayınız. Her maddenin yanında **"Hayır", " Bazen" ve "Evet"** şeklinde 3 seçenek sunulmuştur. Aşağıdaki ifadelerle ilgili davranışlarınız bu seçeneklerden hangisine denk geliyorsa ilgili yeri **(X)** ile işaretleyiniz.

	Hayır	Bazen	Evet
1. Bilgisayarımda güncel bir virüs programı bulundurmaya dikkat ederim.			
2. İnternete girdiğimde bilgilerimin başkaları tarafından çalınabileceğini göz önünde tutarım.			
3. Sosyal paylaşım sitelerinde (Facebook,twitter vb.) özel bilgilerimin başkaları tarafından kötü amaçlı olarak kullanılabileceğini göz önünde bulundururum.			
4. Gerçek yaşamda sorun yaşadığım insanlarla sanal ortamlarda da karşılaşmamaya çalışırım.			
5. Sanal ortamlarda başkalarının bana zarar vermemesi için bazı tedbirler alma ihtiyacı hissettiğim olur.			
6. Sanal ortamlardayken bir bilgisayar korsanının (hacker, cracker, lamer) benim için de tehlike oluşturabileceğini göz önünde bulundururum.			
7. Bana zarar vermek isteyen birisinin bunu internet, cep telefonu vb. aracılığıyla da yapabileceğini düşünürüm.			
8. İnternetteki e-posta, forum siteleri vb. üyelik şifrelerimi kimseyle paylaşmam			
9. Sanal ortamlarda küfür veya hakarette bulunan kişilerle iletişimimi keserim.			
10. Görülmesini istemediğim bir resim ya da görüntümün benden habersiz olarak yayılabileceği tehlikesini düşündüğüm olur.			
11. Sanal ortamlardaki iletişimde hakkımda gerçek olmayan söylentilerin de yayılabileceğini düşünürüm.			
12. İnternete girdiğimde internetin aynı zamanda başkalarına zarar verme amacıyla kullanılabileceğini aklımda tutarım.			
13. Benimle ilgili doğru olmayan bir bilginin internette yayılması durumunda ne yapacağımı düşündüğüm olur.			
14. E-posta ya da cep telefonundan kısa mesaj (SMS) yoluyla tehdit alabileceğim kişilerle sanal ortamlarda iletişimde bulunmam			

Araştırmamıza destek olduğunuz için teşekkür ederim.

Arş.Gör. Hüseyin Kınay

Bilgisayar ve Öğretim Teknolojileri

Fatih Üniversitesi, Büyükçekmece Kampüsü

ÖZGEÇMİŞ

Hüseyin Kınay: 1985 Konya Doğumludur. İlk, orta ve lise öğrenimini Konya'da tamamladıktan sonra 2003 yılında Atatürk Üniversitesi Bilgisayar ve Öğretim Teknolojileri Öğretmenliğini kazandı. 2010 yılında Sakarya Üniversitesi Eğitim Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Eğitiminde yüksek lisansa başlamıştır. Ayrıca Fatih Üniversitesinde araştırma görevlisi olarak çalışmaktadır. Araştırma alanları bilgi güvenliği, siber zorbalık ve bilgisayar destekli yabancı dil öğrenimidir.