T.C.
EGE ÜNİVERSİTESİ
Eğitim Bilimleri Enstitüsü

BİLGİ GÜVENLİĞİNE YÖNELİK ÖĞRENCİ, ÖĞRETMEN, VELİ VE OKUL YÖNETİCİLERİNİN FARKINDALIKLARININ İNCELENMESİ

Yüksek Lisans Tezi

Cansu ALTUNSABAN YERLİKAYA

Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı

İzmir
2019

T.C.
EGE ÜNİVERSİTESİ
Eğitim Bilimleri Enstitüsü

BİLGİ GÜVENLİĞİNE YÖNELİK ÖĞRENCİ, ÖĞRETMEN, VELİ VE OKUL YÖNETİCİLERİNİN FARKINDALIKLARININ İNCELENMESİ

Cansu ALTUNSABAN YERLİKAYA

Danışman : Prof. Dr. Mustafa Murat İNCEOĞLU

Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı
Bilgisayar ve Öğretim Teknolojileri Eğitimi Yüksek Lisans Programı

İzmir
2019

EGE ÜNİVERSİTESİ EĞİTİM BİLİMLERİ ENSTİTÜSÜ

ETİK KURALLARA UYGUNLUK BEYANI

EÜ Lisansüstü Eğitim ve Öğretim Yönetmeliğinin ilgili hükümleri uyarınca Yüksek Lisans/Doktora Tezi olarak sunduğum "Bilgi Güvenliğine Yönelik Öğrenci, Öğretmen, Veli ve Okul Yöneticilerinin Farkındalıklarının İncelenmesi" başlıklı bu tezin kendi çalışmam olduğunu, sunduğum tüm sonuç, doküman, bilgi ve belgeleri bizzat ve bu tez çalışması kapsamında elde ettiğimi, bu tez çalışmasıyla elde edilmeyen bütün bilgi ve yorumlara atıf yaptığımı ve bunları kaynaklar listesinde usulüne uygun olarak verdiğimi, tez çalışması ve yazımı sırasında patent ve telif haklarını ihlal edici bir davranışımın olmadığını, bu tezin herhangi bir bölümünü bu üniversite veya diğer bir üniversite başka bir tez çalışması içinde sunmadığımı, bu tezin planlanmasında yazımına kadar bütün safhalarda bilimsel etik kurallarına uygun olarak davrandığımı ve aksinin ortaya çıkması durumunda her türlü yasal sonucu kabul edeceğimi beyan ederim.

Cansu ALTUNSABAN YERLİKAYA

Cansu ALTUNSABAN YERLİKAYA tarafından Yüksek Lisans tezi olarak sunulan "Bilgi Güvenliğine Yönelik Öğrenci, Öğretmen, Veli ve Okul Yöneticilerinin Farkındalıklarının İncelenmesi" başlıklı bu çalışma EÜ Lisansüstü Eğitim ve Öğretim Yönetmeliği ile EÜ Eğitim Bilimleri Enstitüsü Eğitim ve Öğretim Yönergesi'nin ilgili hükümleri uyarınca tarafımızdan değerlendirilerek savunmaya değer bulunmuş ve 29 Kasım 2019 tarihinde yapılan tez savunma sınavında aday oybirliği/oyçokluğu ile başarılı bulunmuştur.

Jüri Üyeleri:			**İmza**
Jüri Başkanı	:	Prof. Dr. Mustafa M. İNCEOĞLU	.....
Raportör Üye	:	Doç. Dr. Tarık KIŞLA	.....
Üye	:	Dr. Öğr. Üyesi Nilüfer ATMAN USLU	.....

T.C
YÜKSEKÖĞRETİM KURULU
ULUSAL TEZ MERKEZİ

TEZ VERİ GİRİŞ FORMU

Referans No	10269178
Yazar Adı / Soyadı	CANSU ALTUNSABAN
T.C.Kimlik No	32116859296
Telefon	5549396157
E-Posta	cansu.altunsaban@gmail.com
Tezin Dili	Türkçe
Tezin Özgün Adı	BİLGİ GÜVENLİĞİNE YÖNELİK ÖĞRENCİ, ÖĞRETMEN, VELİ VE OKUL YÖNETİCİLERİNİN FARKINDALIKLARININ İNCELENMESİ
Tezin Tercümesi	EXAMINING THE AWARENESS OF STUDENTS, TEACHERS, PARENTS AND SCHOOL ADMINISTRATORS AIMED AT INFORMATION SECURITY
Konu	Eğitim ve Öğretim = Education and Training
Üniversite	Ege Üniversitesi
Enstitü / Hastane	Eğitim Bilimleri Enstitüsü
Anabilim Dalı	Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı
Bilim Dalı	
Tez Türü	Yüksek Lisans
Yılı	2019
Sayfa	117
Tez Danışmanları	PROF. DR. MUSTAFA MURAT İNCEOĞLU
Dizin Terimleri	
Önerilen Dizin Terimleri	Bilgi güvenliği, bilgi güvenliği farkındalığı, farkındalık eğitimi

03.12.2019

İmza:.....

ÖNSÖZ

Günümüzde teknoloji ürünlerinin kullanımının yaygınlaşması, insan yaşamını kolaylaştırmış, ancak birtakım olumsuzlukları da beraberinde getirmiştir. Söz konusu teknoloji ürünleri, gerekli önlemler alınmadığı takdirde, kötü niyetli kişilerin saldırılarına hedef olabilmekte ve bu durum sonucunda bilginin güvenliği tehdit altına girebilmektedir. Bu gibi durumların önüne geçilebilmesi adına kurumların üzerine düşen vazifeler olmakla birlikte, teknoloji ürünlerini kullanan bireylere de önemli vazifeler yüklenmektedir. Söz konusu teknoloji ürünlerinin doğru amaçla ve bilinçli bir şekilde kullanımı ile bilgi güvenliği farkındalığının edinilmiş olması, her bir bireyin başlıca yapması gerekenlerdendir.

Bilgi güvenliği farkındalığının son derece önem kazandığı bu dönemde, farkındalığın edinilmesi için, sürecin küçük yaşlardan itibaren başlaması gerekmektedir. Bu doğrultuda atılacak en önemli adım eğitim alanında olmalıdır. Mevcut bilgiler dahilinde, yapılan araştırmanın probleminin çıkış noktası, bilgi güvenliği farkındalığının öğrenciler üzerinde incelemesinin yapılması olmuştur. Fakat yalnızca öğrenciler üzerinde inceleme yapmak yetersiz kalacağı için, öğrencilerin velileri, öğretmenler ve okul yöneticileri üzerinde de yapılacak bir inceleme, bu alanda kapsamlı bir bilgi sağlayacak ve bu bilgi ile farkındalık eğitimine yönelik yapılacak çalışmalara temel oluşturabilecektir.

Bu bağlamda hem özel okulda hem devlet okulunda ayrıca hem ortaokul hem lise düzeyinde öğrenci, veli, öğretmen ve okul yöneticilerinin bilgi güvenliği farkındalıklarını inceleyen bir çalışma gerçekleştirilmiştir. Gerçekleştirilen çalışmanın sonuçlarının gerek literatüre gerekse bilgi güvenliği farkındalık eğitimlerine katkı sağlaması beklenmektedir.

İZMİR
10/07/2018

Cansu ALTUNSABAN YERLİKAYA

TEŞEKKÜR

Tez çalışmam süresince bilgi birikimi, deneyimleri ve kıymetli önerileriyle bana yol gösteren danışman hocam Sayın Prof. Dr. Mustafa Murat İNCEOĞLU'na, almış olduğum yüksek lisans eğitimi süresince derslerime giren tüm hocalarıma, yapmış olduğum çalışmaya gönüllü olarak katılıp destek veren tüm öğrenci, veli, öğretmen ve okul yöneticilerine, araştırmanın uygulama kısmında her türlü yardımı yapan Sayın Elif ÖZDEMİR'e, Sayın Çağdaş ÖZDEMİR'e ve Sayın Hayriye YILMAZ'a, çalışma boyunca bana destek olan arkadaşlarım Sayın Ezgi ATAŞ AVCI'ya ve Sayın Gönül ALTAY'a, yüksek lisans eğitimim süresince her koşulda hep yanımda olan, hoşgörü ve sevgiyle desteklerini asla esirgemeyen eşim Sayın Bülent YERLİKAYA'ya, annem Sayın Melahat ALTUNSABAN'a ve babam Sayın Adem ALTUNSABAN'a teşekkürü borç bilirim.

01/09/2019

Cansu ALTUNSABAN YERLİKAYA

İmza

ÖZGEÇMİŞ

Kişisel Bilgiler

Ad Soyad	Cansu ALTUNSABAN YERLİKAYA
Doğum Tarihi	03.01.1993
Doğum Yeri	Konak/İZMİR
Medeni Durumu	Evli
Uyruk	T.C.
E-posta	cansu.altunsaban@gmail.com

Eğitim Bilgileri

2015-2019	Yüksek Lisans Eğitimi (Tezli) Ege Üniversitesi Eğitim Fakültesi Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü
2010-2015	Lisans Eğitimi Ege Üniversitesi Eğitim Fakültesi Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü Mezuniyet Derecesi (3,68/4,00)-Bölüm Birinciliği
2017-devam	Lisans Eğitimi Anadolu Üniversitesi Açık Öğretim Fakültesi Sosyoloji Bölümü
2017-2019	Ön Lisans Eğitimi Atatürk Üniversitesi Açık Öğretim Fakültesi Çocuk Gelişimi Bölümü Mezuniyet Derecesi (2,74/4,00)
2011 - 2017	Lisans Eğitimi Anadolu Üniversitesi Açık Öğretim Fakültesi İşletme Bölümü Mezuniyet Derecesi (3,30/4,00)
2006 - 2010	Lise Eğitimi Teğmen Ali Rıza Akıncı Anadolu Lisesi Sayısal Bölüm Mezuniyet Derecesi (75,56/100)

İş Deneyimi

2019-devam	Bilset Okulları Bilişim Teknolojileri Öğretmeni
2015-2019	Özel Yeşeren Okulları Bilişim Teknolojileri Öğretmeni

Yayınlanan Makaleler

Aralık 2018 Jale İPEK, Gönül ALTAY, Cansu ALTUNSABAN, Mert ADSAY ve Hayrünnisa ERGİN, Yaratıcı Problem Çözme Sürecini Değerlendirme Ölçeği: Türkçe' ye Uyarlama Çalışması, Necatibey Eğitim Fakültesi Elektronik Fen ve Matematik Eğitimi Dergisi, Cilt 12 (2), 727-738.

Sunulan Bildiriler

Ağustos 2017 Cansu ALTUNSABAN and Jale İPEK, Relevant Problem Solving in Roboting Programming Education and Cooperative Learning, XIV.European Conference on Social and Behavioral Sciences- IASSR, Odessa, Ukraine, August 23-26 2017.

Mayıs 2017 Cansu ALTUNSABAN, Fırat SARSAR, Tarık KIŞLA, Beril CEYLAN ve Mustafa Murat İNCEOĞLU, Eğitsel Mobil Uygulamaların Tasarım İlkelerinin Öğrenme Üzerine Etkisine Yönelik Görüş Ölçeği, 11. Uluslararası Bilgisayar ve Öğretim Teknolojileri Sempozyumu- ICITS, Malatya, Türkiye, 24-26 Mayıs 2017.

Mayıs 2017 Beril CEYLAN, Fırat SARSAR, Cansu ALTUNSABAN, Yağmur DEMİR, Saniye KULELİ ve Gönül ALTAY, Öğretmenlerin Teknoloji Entegrasyonuna İlişkin Görüşlerinin Betimlenmesi, 11.Uluslararası Bilgisayar ve Öğretim Teknolojileri Sempozyumu- ICITS, Malatya, Türkiye, 24-26 Mayıs 2017.

Mayıs 2017 Jale İPEK, Cansu ALTUNSABAN, Gönül ALTAY, Hayrünnisa ERGİN ve Mert ADSAY, Yaratıcı Problem Çözme Sürecini Değerlendirme Ölçeği, 11. Uluslararası Bilgisayar ve Öğretim Teknolojileri Sempozyumu-ICITS, Malatya, Türkiye, 24-26 Mayıs 2017.

Temmuz 2018 Cansu ALTUNSABAN and Mustafa Murat İNCEOĞLU, Investigatıon of Research in The Field of Information Security in Turkey, Conference Paper: 10th International Conference on Education and New Learning Technologies, DOI: 10.21125/edulearn.2018.1022

İÇİNDEKİLER

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

EKLER LİSTESİ

SİMGELER VE KISALTMALAR LİSTESİ

Simgeler	Açıklama
df	Serbestlik derecesi
p	Anlamlılık düzeyi
t	t testi değeri
$\overline{X}$	Aritmetik ortalama

Kısaltmalar

BGFÖ	Bilgi güvenliği farkındalık ölçeği
CD	Compact disc/yoğun disk
DLOY	Devlet okulunda lise düzeyinde görev yapan okul yöneticisi
DLÖ	Devlet okulunda lise düzeyinde öğrenim gören öğrenci
DLÖT	Devlet okulunda lise düzeyinde görev yapan öğretmen
DLV	Devlet okulunda lise düzeyinde çocuğu olan veli
DOOY	Devlet okulunda ortaokul düzeyinde görev yapan okul yöneticisi
DOÖ	Devlet okulunda ortaokul düzeyinde öğrenim gören öğrenci
DOÖT	Devlet okulunda ortaokul düzeyinde görev yapan öğretmen
DOS	Disk operating system/disk işletim sistemi
DOV	Devlet okulunda ortaokul düzeyinde çocuğu olan veli
Dr.	Doktor
DVD	Digital versatile disc/çok amaçlı sayısal disk
MEB	Milli eğitim bakanlığı

MS	Microsoft
n	Örneklem sayısı
ÖLOY	Özel okulda lise düzeyinde görev yapan okul yöneticisi
ÖLÖ	Özel okulda lise düzeyinde öğrenim gören öğrenci
ÖLÖT	Özel okulda lise düzeyinde görev yapan öğretmen
ÖLV	Özel okulda lise düzeyinde çocuğu olan veli
ÖOOY	Özel okulda ortaokul düzeyinde görev yapan okul yöneticisi
ÖOÖ	Özel okulda ortaokul düzeyinde öğrenim gören öğrenci
ÖOÖT	Özel okulda ortaokul düzeyinde görev yapan öğretmen
ÖOV	Özel okulda ortaokul düzeyinde çocuğu olan veli
ss	Standart sapma
TÜBİTAK	Türkiye bilimsel ve teknolojik araştırma kurumu
yy.	Yüzyıl

ÖZET

BİLGİ GÜVENLİĞİNE YÖNELİK ÖĞRENCİ, ÖĞRETMEN, VELİ VE OKUL YÖNETİCİLERİNİN FARKINDALIKLARININ İNCELENMESİ

YERLİKAYA ALTUNSABAN, Cansu

Yüksek Lisans Tezi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı

Tez Danışmanı: Prof. Dr. Mustafa Murat İNCEOĞLU

Kasım 2019, 117 sayfa

Yapılan araştırmanın amacı, devlet okulları ve özel okullarda yer alan öğrencilerin, velilerin, öğretmenlerin ve okul yöneticilerinin bilgi güvenliği konusundaki farkındalıklarını araştırmak ve söz konusu bu paydaşların görüşlerinin, devlet okulları ile özel okullar arasında farklılık gösterip göstermediğini incelemektir. Araştırmada karma yöntem uygulanmış olup, araştırmanın çalışma grubunda, çalışmanın nicel yöntem uygulanan bölümünde kolay ulaşılabilir örnekleme yöntemi ile belirlenen 2 özel okul ve 2 devlet okulu içerisinden seçilen, ortaokul ve lise düzeyinden 50'şer öğrenci ve 30'ar öğretmen olmak üzere toplam 200 öğrenci ve 120 öğretmen yer almıştır. Nitel yöntem uygulanan bölümünde de her okuldan 3'er öğrenci, 3'er veli, 3'er öğretmen ve 1'er okul yöneticisi seçilmiş olup, toplamda 12 öğrenci, 12 veli, 12 öğretmen ve 4 okul yöneticisi araştırmaya katılmıştır. Araştırmanın veri toplama araçları öğrencilere ve öğretmenlere yönelik ayrı ayrı hazırlanan demografik bilgi anketleri, öğrencilere ve öğretmenlere yönelik ayrı ayrı geliştirilmiş olan Bilgi Güvenliği Farkındalık Ölçeği, öğrenci, öğretmen ve velilere yönelik ayrı ayrı geliştirilmiş olan yarı yapılandırılmış görüşme sorularıdır. Araştırmadan elde edilen verilerin analizinde anlamlılık düzeyi $p<0,05$ kabul edilmiştir. Devlet okulu ve özel okuldaki öğrenciler ve öğretmenlerin ölçek puanları arasında farklılık olup olmadığı incelenmesi için bağımsız örneklem t testi (independent sample t test) ve tek yönlü varyans analizi (ANOVA) uygulanmıştır. Nitel araştırma yöntemi doğrultusunda yapılan görüşmeler de betimsel analiz yöntemi ile yorumlanmıştır.

Gerçekleştirilen analizler sonucunda; okul türüne göre özel okulda öğrenim gören öğrencilerin, okul düzeyine göre ise ortaokulda öğrenim gören öğrencilerin farkındalık düzeylerinin daha yüksek olduğu görülürken, lisede öğrenim gören öğrencilerden özel okulda öğrenim gören öğrencilerin farkındalık düzeylerinin daha

yüksek olduğu, devlet okulunda öğrenim gören öğrencilerden de ortaokulda öğrenim gören öğrencilerin farkındalık düzeylerinin daha yüksek olduğu tespit edilmiştir. Ayrıca cinsiyete göre değerlendirildiğinde erkek öğrencilerin farkındalık düzeylerinin daha yüksek olduğu sonucuna ulaşılmıştır. Nicel verilerden ulaşılan özel okuldaki öğrencilerin farkındalık düzeylerinin daha yüksek olduğu sonucunun nitel verilerle desteklenebileceği görülmüştür. Ortaokul ve lise düzeyinde öğrenim gören öğrenciler arasındaki farkındalık düzeyi farklılığına yönelik ise sonuçların birbirini tam olarak desteklemediği görülmüştür.

Öğretmenler, okul seviyesine göre değerlendirildiğinde, lisede görev yapan öğretmenlerin farkındalık düzeyinin daha yüksek olduğu, özel okulda görev yapan öğretmenler içerisinde de devlet okulunda görev yapan öğretmenler içerisinde de lisede görev yapan öğretmenlerin farkındalık düzeyinin daha yüksek olduğu görülmüştür. Fakat bu sonucunun nitel verilerle tam olarak desteklenmediği görülmüştür. Öğretmenlerin cinsiyetine göre sonuçlar değerlendirildiğinde, erkek öğretmenlerin farkındalık düzeyinin daha yüksek olduğu görülmüştür. Ayrıca İnternette ve bilgisayarda daha uzun süre vakit geçiren öğretmenlerin farkındalık düzeylerinin daha yüksek olduğu sonucuna ulaşılmıştır.

Okul yöneticilerinin Bilgi Güvenliği Farkındalık Ölçeği analizleri değerlendirildiğinde, özel okulda görev yapan okul yöneticilerinin devlet okulunda görev yapan okul yöneticilerine göre farkındalık düzeylerinin daha yüksek olduğu görülmüştür. Nicel verilerden ulaşılan sonucun nitel verilerle desteklendiği görülmüştür.

Veliler ile yapılan görüşmeler sonucunda, velilerin önemli bir kısmının farkındalık düzeylerinin düşük olduğu, çocuklarını gözlemleme konusunda ve bilinçli kullanıma dair yönlendirmede yetersiz kaldıkları sonucuna ulaşılmıştır.

Bu sonuçlar doğrultusunda özel okullarda ve devlet okullarında yer alan öğrenci, veli öğretmen ve okul yöneticilerinin farkındalık düzeylerinin üst seviyeye çıkarılabilmesi için her bir hedef kitleye özgü seminerler düzenlenebileceği, yaşanılabilecek sorunlara yönelik alınması gereken önlemler konusunda bilinçlendirme sağlanabileceği önerilmiştir.

Anahtar sözcükler: Bilgi güvenliği, bilgi güvenliği farkındalığı, farkındalık eğitimi

EXTENDED ABSTRACT

EXAMINING THE AWARENESS OF STUDENTS, TEACHERS, PARENTS AND SCHOOL ADMINISTRATORS AIMED AT INFORMATION SECURITY

YERLİKAYA ALTUNSABAN, Cansu

MSc in Computer Education and Instructional Technology

Supervisor: Prof. Dr. Mustafa Murat İNCEOĞLU

November 2019, 117 pages

The aim of the research is to investigate the awareness of students, parents, teachers and school administrators in public and private schools about information security and to examine whether the opinions of these stakeholders differ between public and private schools. Mixed method was applied in the study. In the working group of the study, in the quantitative part of the study, 200 students and 120 teachers, 50 students and 30 teachers from secondary and high schools, selected from 2 private schools and 2 public schools determined by easily accessible sampling method. has taken place. In the qualitative part, 3 students, 3 parents, 3 teachers and 1 school administrators were selected from each school and a total of 12 students, 12 parents, 12 teachers and 4 school administrators participated in the study. The data collection tools of the research are demographic information questionnaires prepared for students and teachers, Information Security Awareness Scale developed for students and teachers separately, and semi-structured interview questions developed for students, teachers and parents. Significance level was accepted as $p < 0.05$ in the analysis of the data obtained from the research. Independent sample t test (ANOVA) and independent sample t test (ANOVA) were used to examine the difference between the scale scores of students and teachers in public and private schools. The interviews conducted in line with the qualitative research method were also interpreted with descriptive analysis method.

As a result of the analyzes performed; It is seen that the students who are educated in private schools according to the type of school, and the students who are educated in secondary school are higher than the school level, the students who are educated in the private school are more aware than the students who are educated in

high school and the students who are educated in the public school. levels were found to be higher. In addition, when evaluated according to gender, it was concluded that the awareness level of male students was higher. It was seen that the level of awareness of the students in the private school, which was obtained from quantitative data, was higher and could be supported by qualitative data. Concerning the difference of awareness level among the students in secondary and high school levels, the results did not fully support each other.

When the teachers were evaluated according to the school level, it was seen that the awareness level of the teachers working in high school was higher and that of the teachers working in the public school was higher among the teachers working in the public school. However, this result was not fully supported by qualitative data. When the results were evaluated according to the gender of the teachers, it was seen that the awareness level of male teachers was higher. Moreover, it was concluded that the awareness levels of the teachers who spent longer time on the Internet and computer were higher.

When the Information Security Awareness Scale analyzes of the school administrators were evaluated, it was seen that the school administrators working in the private school had higher awareness levels than the school administrators working in the public school. The results obtained from the quantitative data were supported by qualitative data.

As a result of the interviews with the parents, it was concluded that a significant portion of the parents had low levels of awareness and that they were inadequate in observing their children and directing them for conscious use.

In line with these results, it has been suggested that seminars specific to each target group can be organized in order to raise the awareness levels of students, parents, teachers and school administrators in private schools and public schools, and awareness raising can be provided for the problems to be experienced.

Key words: Information security, information security awareness, awareness training

BÖLÜM I
GİRİŞ

Problem Durumu

Sosyal, kurumsal ve toplumsal düzeyde gerçekleşen bilgi ve iletişim teknolojilerindeki gelişim ve teknolojideki değişimler ile mesafeler önemini yitirmiş, bilgi ve iletişim teknolojileri geri dönülmez bir etki ile günlük hayattaki yerini almıştır (Yıldırım ve Öner, 2004). Bu aşamada teknoloji, bireylerin hayatlarını değiştirmiştir (Davies, 2011). Bununla birlikte teknolojideki gelişmeler, bilgisayar ağlarının ve sistemlerinin, bir saldırı aracı haline, kullanılan sistemlerin de açık birer hedef haline gelmesine neden olmuş, söz konusu sistemlerde yer alan bilginin korunması tehlikeye girmiştir (Johnson, 2000).

Bir bireyin değerleri, sahip olduğu bilgiyle ölçülmektedir. Bir birey için büyük öneme sahip olan ve her ortamda yer alan bir varlığın korunabilmesi, güvenliğinin sağlanabilmesi gerekmektedir. Bilgi ve iletişim teknolojileri dikkate alınarak bilgi güvenliği; bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önleme şeklinde açıklanmaktadır (Canbek ve Sağıroğlu, 2006). Bilgi güvenliği aynı zamanda, bilginin tehditlere karşı uygun şekillerde korunması ve bir varlık türü olarak izinsiz veya yetkisiz bir biçimde erişimini, kullanımını, değiştirilmesini, ifşa edilmesini, ortadan kaldırılmasını ve el değiştirmesini önlemek olarak tanımlanabilir (ISO/IEC, 2013). Tehdit, bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini olumsuz yönde etkileme olasılığı olan tanımlı risklerdir. Tehditlerin bilgi varlıklarına etkisi, tehlikenin oluşma olasılığı, bilgi varlığı üzerindeki açık ve varlığın değeri ile doğru orantılıdır. Tehditler uygun ortam şartlarının oluşmasıyla bilgi sistemlerine zarar verecek kusurları içeren zafiyetlere, zafiyetler saldırganlar tarafından kullanıldığında güvenlik ihlallerine yol açarak bilgi sistemlerine zarar vermektedir (Blanding, 2004).

Bilgi güvenliği, bilginin gizliliği, bütünlüğü ve erişilebilirliğinin sağlanmasıdır. Gizlilik, bütünlük ve erişilebilirlik kavramları, bilgi güvenliğinin temel bileşenleri olarak değerlendirilmektedir (Fussell, 2005). Bu üç temel bileşen birbirinden bağımsız olarak değerlendirilmemektedir. Bir bilginin gizliliğinin sağlanmasıyla o bilginin erişilebilirliği engellememelidir. Ayrıca, erişilebilir bir

bilginin bütünlüğünün de sağlanması gereklidir. Eğer bir bilgi için gizlilik sağlanılıyor fakat bilgiye erişim engelleniyor ise, kullanılmaz durumda olan bu bilgi bir değer ifade etmeyecektir. Diğer yandan erişimi sağlanıp bütünlüğü sağlanmıyorsa kurumlar ve bireyler için yanlış ya da eksik bilgi söz konusu olacak ve olumsuz sonuçlara neden olabilecektir. Dolayısıyla bilgi güvenliği kavramı temel olarak bu üç bileşenin bir arada sağlanması demektir (Fussell, 2005).

Bilgi güvenliğine olan gereksinimin ortaya çıkma sebeplerinin anlaşılabilmesi için zamanında ve doğru bilgiyi edinmenin öneminin anlaşılması gereklidir. Bilgi güvenliğinin sağlanmasının temel amacı doğru kişinin kısa sürede doğruluğu kesin olan bilgiye ulaşımını garanti etmektir (Schneider, 2008).

Bilgi güvenliği ihlali olayları teknik nedenlerden kaynaklı olabildiği gibi, bireyler tarafından kaynaklanabilmektedir. Bireylerden kaynaklanan ihlaller genellikle bilinçsiz davranışların sonucu olmakla birlikte, kötü niyetli çalışanların bilgiyi dışarıya sızdırması, kötü amaçlı kullanımı veya yok etmesi de söz konusudur. Bilgi güvenliğini sağlamak için en önemli unsur olan insan faktörünün bilgi güvenliği konusunda eğitimi şarttır. Bu eğitim, bilginin, nasıl korunacağını, neden korunması gerektiğini öğretmelidir. Bireyler hatalı davranışlarının bilgi güvenliği üzerinde yaratabileceği etkiyi anlamalıdır. Bilgi güvenliğinin sağlanmasında ne kadar önlem alınmış olsa da insan faktörü göz ardı edilirse hiçbir önlem sonuç vermeyecektir. Çünkü bilgi güvenliği bilinci ve farkındalığı olmayan insanlar bu güvenlik sürecini aksatacaktır. Bu noktada, özellikle genç yaştaki kişiler bu durumdan daha kolay etkilenebilmekte, fakat bununla birlikte farkındalığın kazanılmasında genç yaşta verilen eğitim önem arz etmektedir. Genç yaştaki bireylerin eğitimi konusunda çalışma yapılabilmesi ve sonuç alınabilmesi için, söz konusu bireylerin ailelerinin, öğretmenlerinin ve okul yöneticilerinin konu ile ilgili bilgi birikimleri ve farkındalık düzeyleri de önemli bir faktördür. Verilen eğitimin, bireylerin yaşantılarında yer alan diğer kişiler tarafından pekiştirilmesi ve genç yaştaki bireylere eğitimi verecek olan kişilerin yeterli bilgi birikimine sahip olması, eğitim sürecinin verimli bir şekilde tamamlanmasını sağlayacaktır.

Amaç ve Önem

Tez kapsamında devlet okulu ve özel okulda ortaokul ve lise düzeyinde öğrenim gören öğrenciler, veliler, söz konusu okullarda görev yapan öğretmenler ve

okul yöneticilerinin bilgi güvenliği alanındaki farkındalıkları incelenecek olup, belirlenen çalışma grubunun bilgi güvenliği alanındaki görüşleri araştırılıp, devlet okulu ve özel okulda yer alan öğrenci, veli, öğretmen ve okul yöneticilerinin görüşleri karşılaştırılarak değerlendirilecek ve bu doğrultuda literatüre katkı sağlayacaktır.

Yapılan çalışma öğretim teknolojisi kapsamında değerlendirildiğinde, söz konusu kavramın içerisinde yer alan tüm basamaklar üzerinde etkili bir araştırma olduğu görülmektedir. Öğretim teknolojisi, belirlenmiş hedefler uyarınca, daha etkili bir öğretim elde etmek için öğrenme ve iletişim konusundaki araştırmaların ve ayrıca insan kaynakları ve diğer kaynakların beraber kullanılmasıyla tüm öğrenme-öğretme sürecinin sistematik bir yaklaşımla tasarlanması, uygulanması ve değerlendirilmesidir. Sürecin işleyişinde yer alan insan kaynaklarının (öğrenci, öğretmen, okul yöneticisi ve veliler) bilgi güvenliği farkındalık düzeyleri, ortaya konulacak ürünü doğrudan etkilemektedir. Bunun yanı sıra, tez sonucunda edinilen bulgular doğrultusunda, öğrencilere, öğretmenlere, velilere ve okul idarecilerine verilecek eğitim seminerlerine yönelik içerik geliştirme çalışmalarına katkı sağlanması da beklenmektedir.

Problem Cümlesi

Bu bilgiler doğrultusunda araştırmanın problem cümlesi; devlet okulu ve özel okulda ortaokul ve lise düzeyinde öğrenim gören öğrenci, öğrencilerin velileri, söz konusu okullarda görev yapan öğretmen ve okul yöneticilerinin bilgi güvenliği alanında farkındalıklarının ne düzeyde olduğu şeklinde belirlenmiştir.

Alt Problemler

Araştırma kapsamında ele alınan probleme yönelik belirlenen alt problemler şu şekildedir;

1. Öğrencilerin bilgi güvenliği farkındalıklarının düzeyi ve bu konuya ilişkin görüşleri nelerdir?

1.a. Öğrencilerin bilgi güvenliği farkındalık düzeyleri;

- Cinsiyet
- Okul düzeyi (ortaokul-lise)
- Okul türü (devlet okulu – özel okul)
- Bilgisayar kullanım süresi
- İnternet kullanım süresi

- Sosyal ağa üye olma durumuna göre anlamlı farklılık göstermekte midir?

1.b. Özel okulda ve devlet okulunda öğrenim gören öğrencilerin bilgi güvenliği farkındalığına yönelik görüşleri nelerdir?

2. Öğretmenlerin bilgi güvenliği farkındalıklarının düzeyi ve bu konuya ilişkin görüşleri nelerdir?

2.a. Öğretmenlerin bilgi güvenliği farkındalık düzeyleri;

- Cinsiyet
- Kaç yıldır öğretmenlik yapıldığı
- Okul düzeyi (ortaokul-lise)
- Okul türü (devlet okulu – özel okul)
- Bilgisayar kullanım süresi
- İnternet kullanım süresi
- Sosyal ağa üye olma durumuna göre anlamlı farklılık göstermekte midir?

2.b. Özel okulda ve devlet okulunda görev yapan öğretmenlerin bilgi güvenliği farkındalığına yönelik görüşleri nelerdir?

3. Okul yöneticilerinin bilgi güvenliği farkındalıklarının düzeyi ile özel okulda ve devlet okulunda görev yapan okul yöneticilerinin bilgi güvenliği farkındalığına yönelik görüşleri nelerdir?

4. özel okulda ve devlet okulunda öğrencisi bulunan velilerin bilgi güvenliği farkındalığına yönelik görüşleri nelerdir?

Sınırlılıklar

Araştırma İzmir İl'i Bornova İlçesi'nde yer alan 2 devlet okulu ve 2 özel okul ile sınırlıdır.

Sayıltılar

Araştırma kapsamında veri toplama araçları ile katılımcılara yöneltilen sorulara, katılımcıların samimi bir şekilde cevaplar verdiği varsayılmıştır.

Tanımlar

Bilgi Güvenliği: bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda,

istenmeyen kişiler tarafından elde edilmesini önleme şeklinde açıklanmaktadır (Canbek ve Sağıroğlu, 2006).

Bilgi Güvenliği Farkındalığı: bilgi güvenliği olgusunda risk oluşturan ögelere dair oluşturulabilecek tedbirlerden ve bireysel ya da kurumsal stratejilerin farkında olunması, bu hususta bilinçli tutumlar gösterilmesi biçiminde ifade edilmektedir (Siponen, 2000).

BÖLÜM II
İLGİLİ YAYIN VE ARAŞTIRMALAR

Bu bölümde bilgi, bilgi güvenliği, bilgi güvenliği öğeleri, bilgi güvenliği farkındalığı, bilgi güvenliği tehditleri ve bilgi güvenliğinin sağlanmasına yönelik alınması gereken önlemlere yönelik açıklamalar yer almaktadır.

2.1 Bilgi Güvenliği

2.1.1 Bilginin Tanımı

Sosyal, kurumsal ve toplumsal düzeyde bilgi; geçmişten itibaren organizasyonların ve bireylerin fikirlerini, hayatlarını, tutumlarını, gelişimlerini ve politikalarını oluşturan faktörlerin başında gelen, önemini hayatın çeşitli alanlarında, siyasette, sanat ortamında, çalışma hayatında, eğitimde vb. olmak üzere bugüne değin sürdüren bir olgudur (Odabaş, 2005; Demirtaş, 2013). Bilgi olgusunun devamlılığına ilk çağlardan itibaren öyküler, destanlar, masallar aracılık etmiş ve 12. yy. sonrasında da üniversiteler, okullar ve kitaplar etkin bir rol üstlenmiştir. Fakat, son zamanlarda etkileşim ve iş birliği durumunu oldukça kolaylaştıran informatik teknolojilerin yaşamımıza dahil olması ve süratli biçimde yayılmıştır. Böylece, bilginin yönetimi, çalışma verimliliğinin ve işleyişlerinin süratlendirilmesi, iş görenler ve öteki kuruluşlar ile hızlı biçimde iletişimi kolaylaştırmış, yaşamımız basit hale gelmiş, bilgideki üretim ve tüketimde artışlar meydana gelmiştir. Elektronik alanlarda bilginin kullanımı, aktarılması ve muhafazası basitleşerek, bilgiye, yer ve zamandan bağımsız biçimde istenilen yerde ve istenilen zamanda erişimi kolaylaşmıştır (Vural, 2007).

Bilgi olgusunun üretimi, saklanma, muhafaza, yararlanılma, paylaşma, yaygınlaşma, etkileşim ve artış hızı, teknolojiyle gelen süratli bilgi işleyişi ve iletişim vasıtalarıyla daha iyi bir hale gelmiştir. Günümüzde insanlar, gündelik hayatında dahi ihtiyaç duyduğu ve ihtiyacı olmayan çoğu bilgi ile karşı karşıya kalmaktadır. Bu kafa karıştıran durumdan uzaklaşmak adına bilgiye ulaşmada seçici metotlardan faydalanılarak, doğrudan erişilmesi hedeflenen bilgiye ulaştıracak metotlar bulunmalıdır. Diğer bir önemli husus da bilginin değeridir. Bilginin değerli ya da değersizliğini saptamak ya da değerini belirlemek, en az bilgi kadar önemlidir. Erişilen bilginin yorumlanmasında, bilginin niteliğini belirten nitelikler değerlendirilmelidir. Güncellik, doğruluk, konu ile alakalı olma, öz ve bütünlük, ihtiyaçlara uyum sağlama

hem fiziksel olarak hem idrak yoluyla erişme, sunulma biçimi vb. kriterler bilginin niteliğini saptayan faktörlerdendir (Canbek, 2005).

Zamanla oluşan teknolojik ilerleme ve farklılaşmayla birlikte bireylerle organizasyonların ileriye dair programları ve politikalarında bazı farklılıklar oluşturma gereksinimi ortaya çıkmış, bu gereksinime cevap hazırlamayanlarınsa özel yaşamlarında ya da içinde oldukları piyasada rekabet edemedikleri fark edilmiştir (Odabaş, 2005). Bu sebep ile; tarım toplumundan bilgi toplumuna geçiş ile beraber maddi bir değer ve güç şeklini alan bilgi kavramı, üretmeye ve kurumların ilerlemesine etkide bulunan önemli etmenlerden birisi olarak, bu değeri bulunduranların ellerindekini geliştirip, yeni normlar geliştirmesiyle beraber, rakip olanları saf dışı bırakmanın en önemli ögesi şekline bürünmüştür (Atılgan, 2009; Demirtaş, 2013).

Bilgi kavramının gelişmesinde, bilgiye gösterilen önemde oluşan artış neticesinde devamlı şekilde tekrar ifade edilmek durumunda kalınmış ve anlamı, yaşamın ihtiyaçları doğrultusunda şekillenmiştir. Hatta 1950'li yıllarda bilgi, organizasyonlar adına yalnızca bürokratik bir gereklilikken, 1990'larda rekabet üstünlüğü oluşturacak politik bir rezerv halini almıştır. Bu süreçte, düzenlemelerin en değerli hazinesi iş görenlerin bulundurduğu bilgi olmuş, bu sebep ile de yapısal yatırımların dışında birey yatırımı da önemsenerek, düzenleme bilgisinin haricinde iş görenlerin bilgilerini de geliştirmeye uğraşmışlardır (Atılgan, 2009).

Bilgi, bütün organizasyonlar ve bireyler adına gelişmeyle farklılaşmanın temeli şeklinde düşünüldüğünden ve eğitim yaşamından, iş yaşamına, özel yaşamdan, kurumsal yaşama değin her adımda pasif olmadığından, gerçek anlamında ifade etmek ve anlamak bu noktadan sonrasında geleceğe dair gelişimimizi oluşturmanın en önemli belirleyicisi şeklinde yorumlanmaktadır (Canbek ve Sağıroğlu, 2006; Durna ve Demirel, 2008). Bu bağlamda Çoban (1996) açısından bilgi; belirli şekilde yoğurulmuş ve alan bakımından anlamı bulunan, şimdiki ve ileride alınacak kararlar adına önemli olan, kavranan ya da reel değeri bulunan veri biçiminde ifade edilmiştir Özetle veri, tutumlara etki ettiğinde bilgi şeklini almaktadır. Ghaziri and Elias (2004) açısından bilgi kavramı, deneyim ya da çalışmayla edinilmiş değerdir. Bununla birlikte, kural ya da gerçeklerin birikimidir. Bilgi özgüldür, bir sorundan bir başka soruna aktarılamaz, belirli bir zaman içinde kullanılır ve sonrasında o bilgiye gereksinim olmayabilir. Bilgi; normlarla, inanışlarla ve güvenle ilişkilidir. Bilgi, başarılı tecrübeler ile gelişir

ve sonrasında da bu deneyim ustalığa evrilir (Güçlü ve Sotirofski, 2006). Bilgi kavramı daha detaylı tanımlanacak olursa, belirli bir düzen içerisindeki değerlerin, deneyimlerin, hedefe yönelik enformasyon ve uzman görüşünün, yeni deneyimler ve enformasyonun bir bütün haline getirilip değerlendirilebilmesi adına bir çerçeve ortaya koyan esnek bir bileşimdir. Bilgi, bilen kişinin beyninde oluşur ve orada uygulanmaya geçer. Kurumlarda sadece belgeler veya dolaplarda değil günlük çalışmada, süreçler içerisinde, uygulamalar ve normlarda da kendisini göstermektedir (Davenport ve Prusak, 2001). Kimi zaman bilgi net bir anlam taşımayabilir. Bir karar almak adına anlamı bulunan bilgi, diğer bir yorumlama bakımından ham data halinde bulunabilir. Bu nedenle, kullanan bireyle değişkenlik gösteren bilgi ve data birbirlerinin konumunda olacak biçimde faydalanılabilir. Bazı uzmanlar bakımından bilgi, hâlihazırdaki bir norm, kuruluşun üst idarecisi bakımından ham data anlamında olabilir (Demirtaş, 2013).

TDK güncel Türkçe sözlüğünde bilgi kavramı; kişi zihninin kavrayabileceği öge, hakikat ve kuralların tümünü, ilim, malumat, anlama, inceleme ve izlemeyle erişilen her çeşit hakikat, edinç, birey aklının işlemesi neticesinde meydana gelen fikir ürünüdür. Genellikle ve ilk sezgi durumunda zihinde kavranan ana fikirler şeklinde ifade edilmektedir (TDK, 2019).

2.1.2 Bilgi Güvenliği Kavramı

Her çeşit örgütsel düzenin, kuruluşun ya da bireysel olarak kişilerin; gündelik çalışma süreçleri bağlamında bilgiyle ilgili işler, ögeler ya da parçalar önemli bir şekilde konumlanmaktadır. Bu noktada, bazen kâğıt belgeler üstünde yazılı şekilde olan bilgi, bazen de informatik düzenleri ile elektronik ortamda muhafaza edilebilmektedir. Muhafaza edilen bilgiler, teknolojik araçlarla bir noktadan başka bir noktaya aktarılabilmekte veya bireyler arasında yazılı olmayan biçimde tanımlanmaktadır. Bu noktada başka bir ifadeyle bilginin saklandığı ortamlarda ya da aktarımı sırasında ne biçimde ve nerede saklı olur ise olsun, diğer kişilerin ulaşmasının önüne geçilmesi adına kesinlikle uygun biçimde muhafaza edilmelidir. Nitekim, işin özelliği ya da sürecin durumu nasıl olur ise olsun, teknolojiyle alakalı olsun ya da olmasın bütün süreçlerin idaresinde bilgi güvenliği kavramının da dinamik, devamlı ve başarılı biçimde oluşturularak idare edilmesi oldukça önemli bir ihtiyaçtır. İşlerin ve süreçlerin iyi idaresi eş zamanlı olarak bilgi güvenliği süreçlerinin de iyi idaresini

beraberinde getirmektedir. Bilgi güvenliği politikaları ve bu stratejileri idare edecek uygun metotları bulunmayan kuruluşlar, yalnızca güvenlik bakımından değil, düzensel ve diğer tüm iş süreçlerinin idaresi bakımından da önemli sorunlar, ekonomik ve/ya da manevi kayıplar ile karşı karşıya kalmaktadır (Tipton and Krause, 2007; Atılgan, 2009; Eminağaoğlu ve Gökşen, 2009; Aslandağ, 2010).

Dünyada küresel bir ağın bulunması, internet olgusunun yaşamımıza dahil olup süratli biçimde yaygın hale gelmesi, sosyal medya ve taşınabilir akıllı cihaz kullanım durumunun fazlalaşması, bilgiye istenilen ortamdan ve istenilen zamanda erişilebiliyor olunmasıyla beraber ortaya çıkan farklılık, üretilmekte ve kullanılmakta olan bilgi çeşitlerini ve biçimlerini farklılaştırmanın yanında meydana gelebilecek tehlike çeşitlerini de değiştirmiştir. Eskiden kendimizin, evlerimizin, çalışma yerlerimizin, araçlarımızın güvenliği başka bir ifadeyle fiziki güvenlik ön planda iken, bugün daha ziyade, bireysel haklar, fikri haklar, ticari değeri olan giziller vb. bireysel ya da kurumsal verilere diğer bireylerin erişmesinin önüne geçmeye dair tedbirler oldukça önem arz eden bir husus olmuştur. Tehlike kavramındaki bu farklılıkla beraber bundan böyle, "kart hesaplarımıza erişilir mi? Virüs bilgisayarlarımızı çökertir mi? Yatırım hesaplarımız korumalı mı? İş ortamındaki bilgisayarlar izinsiz erişime açık mı? Sosyal medya hesaplarım çalındı mı?" vb. soruların oldukça çok konuşulduğu ve yanıtlarının verilmesinin önemli olduğu bir devir başlamıştır (Mart, 2012; Çetin, 2014).

Bilgi güvenliği hususunun oldukça iyi kavranabilmesi adına önce, bilgi güvenliği olgusuna dair gereksinim ne sebeple oluştu? Bilgiler yok olur ya da diğer kişilerce ulaşılırsa ne çeşit problemler ile mücadele ederiz? Bilgi güvenliği hususunda kuruluşlar, kişiler ve halk ne çeşit sorunlarla karşı karşıya kalır? Vaktinde ve gerçek bilgiye ulaşmanın önemi nedir? vb. soruların cevaplanıp, bireysel ve kurumsal anlayış kapsamında üstüne yoğunlaşılarak, her insanın ya da her organizasyonun şahsi sistematiği kapsamında belirli politikalar izlemeleri mecburidir. Fakat genele bakıldığında bu hususun hayata geçirilemediği, hatta zaman ilerledikçe bilgileri oldukça fazla bir biçimde kendimizin bile paylaştığı olmaktadır. Şu durumu unutmamak önemlidir ki; bilginin muhafazası hususuna gerekli önemi göstermeyip, devamlı göz ardı edilmesi sonucunda önemli iş kayıpları, ekonomik ve manevi kayıplar ve hatta ölümler de dahil olmak üzere çeşitli bilgi güvenliği problemleri oluşmaktadır (Eminağaoğlu ve Gökşen, 2009).

Bilgi kavramı en basit açıklama ile para benzeri bir ögedir. Bireyler, kuruluşlar ve ülkeler bakımından bilgi kavramı, erişilmesi, eş zamanlı olarak da muhafazası güç bir ögedir (Canbek, 2005). Nitekim, bilginin, yalnızca güvenilir biçimde muhafazası ve istiflenmesi güvenlik açısından yeterli bir çözüm değildir. Artan ihtiyaçlar bakımından bilginin eş zamanlı olarak bir noktadan bir noktaya aktarılması da vazgeçilmez bir gereksinim olduğundan, bu aktarım sırasında da tedbirlerinin sağlanması önemlidir (Aslandağ, 2010).

Entelektüel bir servet olan bilginin sahibinin muhafazası da yaşamsal bir önem taşımaktadır. Bu muhafaza, hem bilginin kullanılması sırasındaki karışıklığı, dejenerasyonu ve doğru olmayan kullanımın önüne geçmenin yanında, bilgi olgusunu emek sarf ederek kazanan yasal ya da reel bireylerin haklarının muhafazasını da temin edecektir. Bu nedenle patent vb. haklar, entelektüel serveti muhafaza etmek adına ortaya çıkmıştır. Bu açıdan bakıldığında, bilgi güvenliği kavramının, oldukça detaylı ve farklı paydaşların dahil olmasıyla meydana getirilmesinin gerekli bir husus olduğunun farkına varılmıştır (Canbek, 2005). Bu denli detaylı önlemleri tek başına ortaya koymak olanaksız olduğundan, bireysel ve kurumsal dataların muhafazası konusunda gereken ilkeleri belirleyerek, suçlu olanların yargılanması konusunda hükümetlere de oldukça fazla görev yüklenmektedir.

Bilgi güvenliği olgusuyla alakalı kaynaklardaki ifadeler göz önüne alındığında, bilirkişilerin bulundurdukları bilgiler ve özel uzmanlık alanlarına dair bilgi güvenliği olgusuna ayrı çözümler tercih edilmesi ve hayata geçirilmesi önemlidir. Düşük maliyetli ve basit bir güvenlik çözümü bazı kuruluşlar adına eksik olabilirken, bu çözümün diğer bir kuruluş adına tam ve etkili olabileceği de göz önünde bulundurulmalıdır. Ayrıca, bilgi güvenliği olgusu, belirli bir süreci kapsayan bir uygulama olmanın ötesinde süreklilik arz eden bir incelemedir. Bilgi güvenliği olgusunun idaresi, kuruluşlar ve veriler bulunduğu müddetçe devamlı idare edilmesi, kontrol edilmesi gerekli bir hayat döngüsüdür (Eminağaoğlu ve Gökşen, 2009).

2.1.3 Bilgi Güvenliği Ögeleri

Bilgi güvenliği olgusu, “verinin bir nesne olması açısından zararlardan uzak tutulması, doğru teknolojinin, doğru amaç ile kullanımıyla bilginin tüm mecralarda, istenmeyen kişilerce ulaşılmasının önüne geçilmesi” şeklinde ifade edilmektedir (Canbek ve Sağıroğlu, 2006). Bilgiye sürekli ulaşımın olduğu bir mecrada, bilginin

göndericiden alıcıya değin gizlilik çerçevesinde, zarar görmeden, farklılaşmadan ve başkalarınca erişilmeden varlığının korunması ve güven içinde aktarılması süreci bilgi güvenliği şeklinde ifade edilebilir. Bilgi güvenliği olgusunun oluşturulmasında, uyulması ve gerçekleştirilmesi gerekli birden fazla güvenlik ögesi bulunur. İlk olarak üç temel kural olan gizlilik, bütünlük ve erişilebilirlik kurallarına uyulmasının ardından bu kurallara ilaveten kontrol edilebilecek giriş denetimi, güvenlik, inkâr edememe, güven duyulması, kimlik tespiti, kayıt altına alma kurallarına uyulması bilgi güvenliği olgusunun üst seviyede oluşturulması adına önemlidir (Sharp, 2004). Bu ögeler özetle şu şekilde açıklanmıştır.

a. Gizlilik: Sanal ortamlarda aktarılan bilginin; yetkisi ve izni bulunmayan bireyler ya da süreçlerce erişilse dahi anlamlı biçimde ulaşılmasının önüne geçilmesi şeklinde ifade edilebilir. Gizlilik olgusu, statik mecralar (DVD, teyp, disk, CD, gibi) ya da ağ üstünde bir ileticiden bir iletilene aktarılan aktif mecradaki veriler adına oluşturulmak mecburiyetindedir. Kötü niyetli ve saldırgan kişiler, yetkisi bulunmayan gizli verilere çoğu yöntem ile ulaşabilirler. Bu noktadaki amaç, onlar tarafından bu verilere ulaşılsa dahi kavranmasını ya da çözümünü güçleştirecek yollardan faydalanılarak aktarılan bilgiyi anlaşılamayacak ayrı bir biçim haline getirmektir. Gizlilik kuralının sürekliliğinde şifreleme prosedürleri ve steganografi yollarından yararlanılmaktadır.

b. Bütünlük: Bilginin ileticiden gönderildiği şekliyle zarar görmeden bir bütün olarak iletilene aktarılmasına garanti veren bir güvenlik ögesidir. Bilginin iletişim esnasında kullandığı yöntemlerde farklılaşmamış, yeni datalar dahil olmamış, belirli bir parçası veya tümü tekrarlanmamış ve yerleri değişmemiş biçimde iletilene aktarılarak bütünlüğü korunur. Bilginin bütünlüğünün devamlılığı adına özetleme (hashing) algoritmalarından yararlanılmaktadır.

c. Erişilebilirlik: İstenilen bilgiye, kullananların yetkisi çerçevesinde, vaktinde erişim sağlanması adına gereken tedbirlerin oluşturulması şeklinde ifade edilebilir. Erişilebilirlik, informatik düzenlerden faydalanan bireyler ya da süreçlerce oldukça önemlidir. İnformatik düzenlerden, kendilerinden umulan görevleri belirli bir vakit çerçevesinde gerçekleştirmeleri beklenir. Erişilebilirlik hizmeti, informatik sistemlerini, kurumun içinden ya da kurum dışından oluşabilecek erişilebilirliği azaltıcı tehditlerine (Denial of Service Attack-DOS) dair muhafazayı amaçlar. Bu

bileşenle, kullanıcılar, bağlantı yetkileri çerçevesinde olan verilere, güncel, vaktinde, süratli ve güvenlikli biçimde erişebilirler. Bilgisayar yazılımlarında bulunan uygunsuz şifrelemeler, düzenin hatalı, bilinçli olmayan ve eğitimsiz çalışan tarafından kullanımı ya da işlemesi, doğal afetler vb. sistem erişilebilirliğine negatif etki eden önemli etmenlerdir. Bilgi sistemine ulaşılabilirliğin devamlı olması adına fiziki tedbirler oluşturulmalı, casus önleyici yazılımlar, güvenlik duvarları, atak belirleyici sistemler, virüs önleyici programlar yüklenmeli ve güncel tutulmalıdır.

d. Kayıt (Log) altına alma/izlenebilirlik: Sanal mecrada oluşan hususların (bilgisayar üstünde oluşan herhangi bir etkinliğin) sonrasında çözümlemek adına kayıt oluşturmak şeklinde ifade edilebilir. Kullanıcının şifresini girerek sistemi açmak, internete girmek, mail atmak vb. kayıtlanması gerekli hususlardandır. Toplanan kayıtlar üstünde gerçekleştirilecek çözümleme neticesinde, bilinen atak çeşitlerinin ipuçlarına denk gelinirse ve atak ihtimali fazla bir etkinlik saptanırsa, saldırı belirleme sistemlerince alarm iletileri oluşturularak sistem idarecilerine uyarı gönderilir. Kayıtlama öğesi, atakların ve kötü niyetli ve saldırgan kişilerin saptanmasında önem taşımaktadır. Atağın gerçekleştirilmesinin sonrasında oluşturulan kayıtlar atak çeşidi ve saldırganın kimliğinin belirlenmesini kolaylaştırır. Kayıt oluşturulmayan bir düzenin güvenliğinden söz edilemeyeceği her daim göz önünde bulundurulmalıdır.

e. Kimlik tespiti (kanıt oluşturma ve doğrulama): Bilgi düzenlerinden hizmet sunan alıcının, söylediği birey olduğuna emin olunması şeklinde ifade edilebilir. Örnek olarak, giriş izinleri bulunan bir sanal mecraya ulaşan bireye sorulan parolalar, bilgisayar açılırken parola sorulması kullanıcının kimliğinin belirlenmesinde kullanılan metotlardır. Günümüzde kimlik belirlenmesi, bilgisayar bağlantıları ve başka düzenler adına da oldukça önemli bir hizmet şekline bürünmüştür. Tek kullanıma dayalı şifreler (one time password), akıllı kartlar, biletler, e-imza kartları, biyometrik araçlar kimlik belirlenmesinde faydalanılan teknolojilerdendir.

f. Güven olgusu: Bilgisayar düzenlerinin beklenen tutumuyla elde edilen neticeler arasındaki çelişki konusu şeklinde ifade edilebilir. Başka bir tanımla güven, herhangi bir veri düzeninden ne olması bekleniyor ise, düzenin ondan bekleneni gerçekleştirerek her çalıştığında da aynı neticeleri sunması şeklinde ifade edilebilir. Örnek olarak, ağ kapsamında bulunan merkezi distribütör anahtarın (switch) 24 saat

süresince sürekli işlemesi beklenmektedir. Güvenirlik olgusu, aygıtın işlediği vakit dilimiyle, işlemesi gerekli vakit dilimi mukayese edilerek oluşturulmaktadır.

g. İnkâr etmemek: Sanal mecralarda iletici ve iletilen arasındaki iletişimin inkâr edilmemesi adına gereken tedbirlerin oluşturulmasına yardımcı olan güvenlik ögesidir. Sağlanan güvenlik tedbirleri yardımıyla ileticiyle alıcı arasında meydana gelebilecek sürtüşmelerin, zararların minimuma düşmesi hedeflenir. Bu güvenlik ögesi, bilhassa gerçek zamanlı işlemi mecbur kılan finans ve bankacılık veri düzenlerinde çok işlevseldir. İnkâr edememe ögesi, açık anahtar sistemi ve e- imzadan faydalanılarak oluşturulmaktadır.

h. Giriş denetimi (Erişim listeleri): Bilgi düzenlerine ulaşmak adına kimlik belirlemesi gerçekleşmiş kullanıcı ya da programlara tanımlanan yetkilerin saptanması, bir rezerve ulaşmak adına bazı izinlerin alınması ya da verilmesi şeklinde ifade edilebilir.

i. Güvenlik: Bilgi sistemlerini risklerden uzak tutmak adına fiziki ya da teknik çözümlerdir. Bir bilgisayarın ya da yazılımın fonksiyonel alanına gömülü olduğu zaman kendisi ya da gömülü bulunduğu mecra adına istenilmeyen belirsiz ya da gerçek risk teşkil edecek faaliyet ya da hususların önüne geçme unsurudur.

2.1.4 Bilgi Güvenliği Farkındalığı

Bu kavram, bilgi güvenliği olgusunda risk oluşturan ögelere dair oluşturulabilecek tedbirlerden ve bireysel ya da kurumsal stratejilerin farkında olunması, bu hususta bilinçli tutumlar gösterilmesi biçiminde ifade edilmektedir (Siponen, 2000). Bilginin idaresi ve güvenliğinin oluşturulması oldukça karışık bir durum olduğu için, bu sürecin devamlılığının programlanması ile idaresi gereklidir. Bu programlama kapsamına eklenmesi gerekli en önemli öge olan kişi etmenine dayalı bilgi güvenliği tehlikelerini tamamı ile ortadan kaldırılamamaktadır. Fakat, iyi eğitimli ve dikkatli kişilerle, muhtemel güvenlik ihlalinin, kabul edilebilir bir düzeye getirilmesi kolaylaşabilmektedir (Vural, 2007; Keser ve Güldüren, 2015; Güldüren vd., 2016). Birey ve yönetim sorunlarından meydana gelen güvenlik ihlallerinin nedenleri incelendiğinde son kullananlardan ülke idaresine değin ayrı pozisyonlarda vazifelerini gerçekleştiren kuruluş ya da kişilerin ortak yetersizliklerinin eğitim ve farkındalıktan geçtiği belirtilmektedir (Vural vd., 2009). Bu husus, kişilerin olası bir sağlık problemi oluşmadan önce doktora gitmemeleri ile benzer durumdur. Nitekim,

kişiler ya da kuruluşlar bilgi güvenliği olgusunu riske sokan bir durum yaşamadan bilgi güvenliğine dair bilinç oluşturmaya çalışmamaktadır (Öztemiz ve Yılmaz, 2013). Bu durumun neticesi olarak yitirdiğimiz sağlığımız veya verilerimiz ne olur ise olsun bu noktadan dönütü bulunmayacağının farkında olunması önemlidir. Bu farkındalıkla, halkın bilgi güvenliği hususunda toplumsal ve iş yaşamlarındaki pozisyonlarına dair bilinçlendirmelerin fazlalaştırılması adına gereken eğitim ve seminerlerin gerçekleştirilmesi mecburidir. Nitekim, bilgi güvenliği bilinci bulunmayan kişiler bilgi güvenliği döngüsünün kötü bileşenleri şeklinde bu sürecin gecikmesine sebebiyet vereceklerdir (Mart, 2012).

Örnek olarak, vazifesi sebebi ile telefonda bazı bilgilerin paylaşılıp bazılarının paylaşılamayacağı hususunda bilinci bulunmayan bir personelden, telefon ile edinilecek bilgiler, siber saldırı gerçekleştirmek adına gereken istilaların bir parçası olabilmektedir. Üst düzeyde bilgi düzenleri güvenliği olgusunun oluşturulması adına kişi etmeni göz önünde bulundurulmalı ve direkt ya da dolaylı şekilde bağı olan bütün kişiler bilgi güvenliği hususunda bilinçlendirilmelidir (Vural vd., 2009).

Bilgi güvenliği bilinci bilhassa genç kişilerde oldukça önemlidir. Eckertova vd. (2013), çocuklar, bilhassa da gençlerin birbiriyle haberleşme olanağına sahip, her gün gelişen ve kullanımı adına devamlı çekici hal alan teknolojiyle sarılmıştır. Bu teknolojileri ya da teknolojik araçların ortak noktası internete bağlanmalarıdır. Fakat, iletişim bakımından önemli pratiklik olarak düşünülen bu ilerlemeler, eş zamanlı olarak gençleri türlü risklerle karşı karşıya bırakabilmektedir. Başka bir ifadeyle, teknoloji amaçlanan kişiye erişmek adına oldukça uygun bir vasıta da olmaktadır. Kimi zaman bir korkutma kimi zaman da sosyal ortamlarda bilinçsizce gerçekleştirilen bireysel veri paylaşımları, genç insanları tehlikeli ve zorlu bir duruma düşürebilmektedir. Bireyler sanal ortamda gerçek hayattakinden ayrı tutumlar sergilemekte, kolayca veri, fotoğraf ve video paylaşmaktadırlar. Fakat bu paylaşımlar kimi zaman bireyin yakın çevresinin ötesine geçebilmektedir. Çoğunlukla bu veriler suistimal edilmekte, daha sonra sorun olmaktadırlar (Güldüren vd., 2016).

Bintziou vd. (1999) bilgi güvenliğine dair eğitimin en uygun dönemin ortaokul çağları olduğunu belirtmektedirler. Bu dönemde, öğrenciler, bilgi ve iletişim teknolojileriyle ilk kez gerçek anlamda baş başa kalır ve muhafazaya gereksinim hisseder. Bu dönemlerde var olan sorunların farkında olup konu ile ilgili bir fikir

oluşturmaya başlamaktadır. Ancak gençlerin bu sorunlardan korunması adına genellikle teknik bakımdan, yaptıklarına engeller ya da kısıtlamalar getirilmektedir. Buna benzer tedbirler, problemi çözmek yerine tümüyle kompleks hale getirmekte ve internet ortamında hür olmak isteyen gençlerin beklentilerini gerçekleştirmemektedir. Bu durumun aksine, bilgi güvenliği hususunda onların eğitim süreçlerine bizzat katılarak, bilgi seviyelerini yükseltmeleri önemlidir. Böylece, bilinçlenmeleri artacak ve şahsi güvenliklerini oluşturmaları adına emek sarf edeceklerdir.

2.1.5 Bilgi Güvenliği Tehditleri

Tehdit kavramı, bilginin gizlilik, bütünlük ve erişilebilirliğine negatif etkide bulunma ihtimali olan tehlikelerdir (Blanding, 2004). Tehditler, bilgi sistemlerinde etkili olmak adına bilgi sistemleri üstünde bulunan zafiyetlerden faydalanırlar. Tehditlerin bilgiye etkisi, riskin gelişme ihtimali, bilginin varlığı üstündeki açıklar ve varlığın değeriyle paraleldir. Tehditler uygun ortam koşullarının meydana gelmesi ile bilgi sistemlerine zararı olacak noksanlıkları kapsayan zayıflıklara, zayıflıklar da kötü niyetli ve saldırgan kişilerce kullanıldığı zaman güvenlik bozukluklarına neden olarak bilgi sistemlerinde zarar meydana getirmektedirler.

Tehditler, kaynak bakımından ele alındığında;

a. Doğal felaketler ya da teknik sorunlarla alakalı tehditler,

b. Prosedüre dayalı eksiklerden kaynaklı tehditler,

c. İnsandan kaynaklı tehditler ve

d. Zararlı yazılımlar ile alakalı tehditler şeklinde belirtilebilir.

2.1.5.1 Doğal Felaketlerden Oluşan Tehditler

Doğal felaketler ve teknik sorunlar genelde öngörülemediklerinden önlenmesi oldukça güçtür. Bu tehditlere dair bütün önlemler önceden programlanmalı ve gerçekleştirilmelidir. Zelzele, yangın, sel, umulmadık sıcaklık farklılaşmaları, heyelan, fırtınalar, çığ vb. felaketler oluşabilecek tehditlere örnektir. Doğal felaket ve teknik sorunlarla alakalı tehditlere gösterilebilecek başka örnekler şu şekilde sıralanmıştır:

a. Güç rezervinde sorun olması,

b. Yangın söndürme düzenindeki sorunlar,

c. Telefon santrali bozukluğu,

d. Aktif aygıt (anahtar, yönlendirici gibi) bozuklukları,

e. Sunucu bilgisayarlarda meydana gelebilecek yazılım ya da donanım sorunları,

f. Kripto düzenlerdeki sorunlar (algoritmanın kötü olması, anahtar eksiklikleri gibi),

g. Havalandırma sorunları,

h. Kamera sistemleri sorunları,

i. Kapı çıkışları düzeninde oluşan sorunlar,

j. Terör saldırısı (kundaklama, bombalama gibi),

k. Başkaldırılar, protestolar, gösteriler ve

l. Veri depolama ağı ve yedekleme düzeninde oluşan sorunlardır.

Doğal felaketler ve teknik sorunlarla alakalı tehditlerden herhangi bir tanesinin oluşması genelde bütün bilgi sistemlerinin etkilenmesine ya da işlememesine neden olmaktadır. Bu çeşit tehditleri minimum düzeyde devam ettirmek adına kurumsallığa uygun afet planları oluşturulmalı ve afetten en az sürede ne şekilde kurtulacağı ile alakalı (disaster recovery) iş sürekliliği hususundaki incelemeler önceden hazırlanmalıdır (Blanding, 2004).

2.1.5.2 Prosedüral Aksaklıklarından Oluşan Tehditler

Bu tehdit çeşidi kurumsallaşma süreçlerini bitiremeyen işletmelerde gözlenir. Prosedüral aksaklıklar kendi içinde teknik ve yönetimsel olarak iki başlıkta incelenmektedir (Blanding, 2004).

Yönetimsel Prosedür Aksaklıkları:

a. Çalışanın işe alınması ve işinden çıkarılmasında güvenlik prosedürünün bulunmaması

b. Güvenlikle alakalı vazife ve işlerin paylaşımında aksaklıklar

c. Personellerin güvenlik ilke ve yöntemlerini bilmemeleri ya da bu hususta yetersiz bilgi sahibi olmaları

d. Vazifelerin paylaştırılması ve rotasyon yöntemlerinin bulunmaması

e. Acil durumlarda ya da afet zamanlarında kullanılacak *Bilgi Devamlılık Planları*nın bulunmaması

f. Güvenlik Stratejisi ve yöntemlerinin bulunmaması

g. Güvenlik farkındalığı eğitimlerinin düzenlenmesi ve gerçekleştirilmesine dair aksaklıklar

h. Bütün iş süreçlerinin belgelenmesine dair aksaklıklar.

Teknik Yöntem Aksaklıkları:

a. Bilgi yedekleme yöntemlerinin bulunmaması

b. Bilgisayar, bakım ve kurulum (yardım masası) yöntemlerinin aksaklığı

c. Bilgi dokümanlarının kayıt altına alınmaması ve revizyonunu devam ettirecek düzeneğin bulunmaması

d. Bilgi sistemleri takip etme yöntemlerinin bulunmaması

e. Ağ hizmetleri (e-mail, net, belge aktarımı gibi) kullanım yöntemlerinin bulunmaması

f. Etki sahası hizmet (Parola değiştirme, yeni hesap oluşturma vb.) yöntemlerinin yetersizliği

g. Server hizmetleri (dns, dhcp, etki alanı, vb.) programlama ve idare yönetim yetersizliği

h. Haberleşme kanallarının (ses, bilgi gibi) kontrolü ve idaresine dair yöntem yetersizliği.

2.1.5.3 İnsandan Kaynaklı Tehditler

Konu bilgi güvenliği ise genellikle, çeşitli standartlar, yazılımlar (güvenlik duvarları, yetkilendirme, anti virüs yazılımları, kapsamlı denetleme yazılımı, bilgi şifreleme, kimlik onaylaması gibi) ve donanımlar bularak, teknoloji esaslı çareler üretilerek, bu teknolojilerden yararlanan ve çalışanların bireyler olduğu gerçeği göz önüne alınmamıştır. Bu husus niyeti kötü olan bireylerin, güvenliğin en güçsüz parçası şeklinde düşündükleri kişilerin zaafları, dikkatsiz ve bilinçsiz tutumlarından faydalanmaya dair bazı metotlar bulmanın en önemli faktör olduğu belirtilmiştir (Vural, 2007; Öztemiz ve Yılmaz 2013; Keser ve Güldüren, 2015; Güldüren vd., 2016).

Bu durum, bilgi güvenliği probleminin kişilerden bağımsız, sadece teknoloji esaslı metotlarla çözülemeyeceğini (Güldüren vd., 2016) ve bu yüzden de halkın bilgi güvenliği hususunda farkındalık oluşturarak, bilinç seviyesinin yükselmesinin önemli olduğu neticesini ortaya koymaktadır. Böylece bilinçli olan kişiler hem bireysel hem de kurumsal bilgi güvenliği olgusuna oldukça etki edeceklerdir (Çetin, 2014).

Önceden informatik aygıtlarını yalnızca bu alanda çalışan bilirkişiler kullanmakta idi. Dolayısıyla bilgi güvenliği olgusunun, bilişim çalışanı olmayan

kişilerce zor kavranacağı şeklinde bir düşünce bulunmaktaydı. Bu sebeple bilişim personellerine, bu hususu teknik olmayan ifadelerle başka kişilere kolayca aktarmamalarının gerekliliği açıklanmıştır. Bugün, insanlar, herkesle haberleşme donanımına sahip, süratle gelişen ve kompleks hale gelen teknolojilerle çevrelendiğinden, bilgi güvenliği bilinci yalnızca belirli bir toplulukta değil, bütün kişilerce bilinmelidir. Böylece insanlar, bireysel verilerinin muhafazasında belirli bir farkındalık düzeyine gelerek, iş gördükleri kuruluşlar ve bulundukları devletlerin de bilgi güvenliği gözetim düzeninde önemli vazifeler alacaklardır (Aslandağ, 2010).

Tipton and Krause (2007), kuruluşlarda bilgi güvenliği hususunda meydana getirilen prensiplere ilk uyulması gereken toplulukların, idareciler ve bilişim personellerinin olduğunu, fakat tam aksine bu prensiplere en çok uymayan ve en tehlikeli aktivitelerin gerçekleştiği alanlarında en değerli ve saklı verilerden faydalanan, aktaran ve kayıt altına alan bu iki topluluktaki personellerin olacağını söylemişlerdir. Bu sebep ile kuruluştan bilgi güvenliği olgusuna zarar veren istilalar ya da bilmeden gerçekleştirilen davranışlar; dıştan gerçekleştirenlere kıyasla tehlikelerin ve kayıpların üst seviyede olmasına sebebiyet vermektedir (Eminağaoğlu ve Gökşen, 2009).

Bu bilgiler doğrultusunda, insandan kaynaklı tehditler kendi arasında iki başlıkta incelenebilir (Vural, 2007; Tekerek, 2008):

a) Bilinçli olmayan tutumlardan doğan tehditler

Bilinçli olmayan tutumlardan doğan tehditler; herhangi bir sistem üstünde yetkisi bulunan bir kullanıcı, bilgi sistemlerini bilinçli olmayan şekilde ya da bilgisiz, gereken eğitimi almadan işletmesi neticesinde verinin gizlilik, bütünlük ve erişilebilirlik prensiplerinin birine ya da birçoğuna uyulmamasına sebebiyet veren, bilinçsizce ya da önemsememe neticesinde gerçekleştirilen kullanıcı tutumlarıdır (Vural, 2007). En önemli anlaşmazlıklardan ve problemlerden biri, kuruluşların en değerli ticari gizillerin hafıza kartı, DVD, laptop ya da cep telefonu vb. kolayca çaldırılabilecek, kaybolabilecek cihazlarda, muhafaza tedbirleri sağlanmadan sıklıkla taşınması ve işletilmesidir. Daha da önemli olan, bu çeşit cihazlardan yararlanan bireylerin hemen hemen %70'lik kısmı söz konusu güvenlik tehlikelerinin ve aldıkları vazifelerin bilincinde olmamalarıdır (Eminağaoğlu ve Gökşen, 2009).

Program geliştiriciler, son kullanıcılar, sistem idarecileri vb. farklı seviyede bilgisi bulunan kişilerce istemsiz ya da önemsememe neticesinde gerçekleştirilen tutumlardan doğan bazı tehditler aşağıda belirtilmiştir (Canbek ve Sağıroğlu, 2006; Vural, 2007).

a. Güvenlik stratejilerine uyum göstermeme

b. Güvenlik tedbir ve denetlemelerini sağlamadan yazılım geliştirme

c. Temizlik yapan kişinin server fişini elektrikten çekmesi

d. Eğitimi gerçekleştirilmemiş personelin yapılandırma düzeniyle oynaması

e. İnformatik sistemlerin doğru kullanılmaması ya da idaresi

f. Eksik ya da yanlış yapılandırma

g. Erişim haklarının ayarlanmaması

h. Sistem kayıt durumunun (log) çözümlenmeden silinmesi ya da kayıt edilmemesi

i. Bilgisayarda bulunulmayan vakitlerde şifreli ekran koruyucu ayarlamama

j. Yanlış yedekleme ya da yedekleme yapmama

k. Gerekli olmayan servislerin kullanıma açılması

l. Anti-virüs sistemlerinin bilgisayarı kasıyor sebebiyle kaldırma

m. Bilmediği adreslerden alınan e-mailleri açma ya da e-maillerle istenilen sırları paylaşma

n. Parolasını unutanların parolalarını telefonla değiştirebilmesi

o. Parolaların masa üstünde küçük kâğıtlara yazılması ve

p. Sistemlerin başlangıç (default) düzenlerinde tutulması

b) Bilinçli tutumlardan doğan tehditler (sosyal mühendislik)

İnsandan kaynaklı diğer tehdit çeşidi çalışma ortamına öfkeli ya da küs olan ve hiç beklentisi bulunmayan problemli çalışanın vazifesini ve yetkilerine iyiye kullanmadan bilerek gerçekleştirdiği kötü tutumlardır. Bu bireyler bugün yerel istilacı (internal hacker) şeklinde isimlendirilmektedir. Bu saldırganların gerçekleştirdiği saldırılardan sonra kuruluşlar çok fazla zarara uğrarlar. Bilerek gerçekleştirilen kötü tutumlardan doğan bazı tehditler aşağıda belirtilmiştir (Blanding, 2004):

a. Yetkisi ve vazifesi olmayan bilgisayar ortamlarına sızmak ve gizli verilere ulaşmak

b. Vazifesinden ötürü bildiği üst seviyedeki yetkisi olan parolaları kuruluş dışına, çıkar uğruna söylemek

c. Veri tabanında bulunan bazı kayıtları yok etmek, farklılaştırmak ya da tamamı ile silmek

d. Güvenlik serverlarını (güvenlik duvarı, istila tespit sistemi, anti-virüs gibi) bilinçli hatalı yapılandırma ya da yok etme

e. Gerçekleştirilen kötü tutumların ipucu oluşturmaması adına güvenlik kayıtları ortamından yok edilmesi

f. Bilerek kötü uygulamaların bilgisayarlara sızdırılması vb. birçok durum söz konusu olmaktadır.

Bilerek gerçekleştirilen çoğu tutum suç içermektedir. Sayılan örneklerden görüldüğü üzere eğitimsizlik, bilinçli olmama, gönülsüzlük ve önemsememe, vazifesini iyiye kullanmama vb. birey hatalarından doğan durumlar, bilgi güvenliğine dair olan önemli tehditlerdendir.

- **Sosyal mühendislik**

Bilgisayar ve ağ güvenliği bakımından bu olgu, birey tutumundaki ögeleri güvenlik eksikleri şeklinde yorumlayıp, bu eksiklerden yararlanma yoluyla güvenlik süreçlerini geçerek sistem idarecisi veya kullanıcıların yetkilerine ulaşım yollarını içeren bir kavramdır. Sosyal mühendislik olgusunu ifade eden ve informatik alanda konuyla alakalı esas kaynaklardan birisi şeklinde benimsenen ‘Art Of Deception’ isimli kaynağın yazarı, Kevin Mitnick, bu kitabında birey ögesini ağ güvenliği olgusunun en güçsüz zinciri şeklinde ifade etmektedir (Mitnick, 2002).

İnformatik teknolojilerinin ilerlemesiyle orantılı informatik sistemlere dair istilalarda ve informatik suçlarında önemli artışlar görülmektedir. İnformatik sistemlerdeki ilerlemeler, işleyişi artan yeni aygıtlar (taşınabilir teknolojiler ve bilgisayarlar) yeni güvenlik risklerini de beraberinde getirmektedir. Bunun yanında, informatik teknolojisinde yer alan yeni aygıtlar (bilgisayar yazılımları, veri tabanı düzenleri) yeni istila metotlarının oluşmasına imkan vermektedir. İnformatik teknolojisinde oluşan süratli ilerleme, informatik suçlarının çeşitlenmesi ve yaygınlaşmasının daha yüksek düzeylerde bir artış göstermesine sebebiyet vermektedir.

Sosyal mühendislik metoduyla gerçekleştirilen izinsiz erişim denemesi, sadece bir kullanıcıya odaklanılması ya da kullanıcılara toplu biçimde odaklanılması biçiminde olmaktadır. Sadece bir kullanıcıya odaklanan izinsiz erişim denemeleri kapsamında; birebir (yüz yüze), telefon, e-mail ya da faks gibi iletişim organları kullanılmaktadır. Söz konusu iletişim organları, direkt, odaklanılan bireye yönelik olduğu gibi, kimliğin taklit edilmesi ile sistem idarecilerine yönelik de gerçekleştirilmektedir. İletişim araçlarının kitlesel amaçlar doğrultusunda amaçlandığında, genelde, aldatıcı internet sayfası ve kitlesel e-mail iletişim araçlarının bir araya getirilmesi tercih edilmektedir. Sahte e-posta, phishing dolandırmaları ve hoax e-mailleri yığınsal amaçları saptırmaya dair kullanılan metotlardandır (Mitnick, 2002).

2.1.5.4 Zararlı Yazılımlardan Oluşan Tehditler

Bilgi almak, etkileşim kurmak, eğlenmek gibi gereksinimlerimizi gidermek adına, yaşamın her alanında kullanılan mobil telefonlar, bilgisayarlar, taşınabilir bilgisayarlar, bugün dahi oldukça yaygın olan smart televizyonlar ile çalışan uygulamalar aracılığıyla işlerimizi yapmaktayız. Bu gereksinimlerimizi gideren, sistemlerin altyapısını meydana getiren, donanım ve yazılım teknikleri birbirlerini bütünlemektedir. Ancak tüm bu cihazların donanımının altyapısı gerek sürat gerekse de enerji harcaması bakımından gelişse de, gereksinimlerimize uygun çözümler, bu donanımın altyapısından faydalanan yazılımlarla oluşturulmaktadır. Gereksinimlerimizi gidermemiz konusunda faydası bulunan bir bilişim teknolojisi ürünü olan yazılımların olumlu yönde kullanılmaması, ne yazık ki, sıklıkla yaşanan bir durumdur (Çalışkan, 2013).

Zararlı yazılım veya malware (malicious software'in kısaltılmışı), bilgisayara girerek zarar oluşturmak, veri çalmak veya kullananları rahatsız etmek adına düzenlenmiş, istenmeyen yazılımların genel ismidir. Söz konusu yazılım, girdiği sistemin bozulmasına sebebiyet vermektedir (Canbek, 2005).

Zararlı yazılımlar amaçlarına göre oldukça farklı biçimlerde sisteme girmektedirler. Bu yollarda bazıları;

- Port, servis vb. sistemde bulunan eksik bir yerin fark edilmesi,
- Kullanıcının hataları ve bilinçsiz kullanımından faydalanarak,

- Zararlı yazılımın hedefteki bilgisayara kullanıcı aracılığıyla kurulumunun gerçekleşmesi sağlanarak (Ercan, 2015).

Zararlı yazılımların hedefleri gün geçtikçe farklılaşmıştır. Eskiden bu tür yazılımların uğrattıkları kayıplara bakıldığında, daha çok kişisel etkinlikler biçiminde olduğu gözlenmiştir. Bu etkinliklerden kimileri şöyledir:

- Kullananların hali hazırdaki belgeleri yok edilmiş,
- İşletim sistemi bozulmuş,
- Bilgisayar performansı azalmıştır.

Hâlbuki bugün zararlı yazılımlardan, ekonomik imtiyaz oluşturmak adına yararlanılmaktadır. İlerleyen teknoloji ile beraber, daha süratli ve kolay olduğundan, para aktarımı, internet üstünden yapılmaktadır. Bu yazılımlar, kullanıcının haberi olmadan ya da dikkatsiz olmasından yararlanarak bilgisayara girmekte ve internet bankacılığı parolaları, kredi kartı bilgileri vb. önemli bilgilere erişmektedir (Şahinaslan, 2013).

Zararlı yazılım şifrelerini bulan kötü niyetli ve saldırgan kişiler, ucunda paranın olmasından kaynaklı olarak, birbirleri ile çalışarak saldırıları planlamaktadırlar. Saldırılar planlı şekilde yapılmaktadır. Organize olan kötü niyetli ve saldırgan kişiler, güvenlik bilinci bulunmayan kullanıcılara yönelik, kurdukları planlar ile informatik sistemler üstünde zarar oluşturmak adına, plan yapmakta ve bu doğrultuda yazılımlar geliştirmektedirler (Gülmüş, 2010).

Bu yazılımlar, kullanıcıların dikkatli olmamasından yararlanılarak bilgisayara veya sisteme girebilmektedir. Sosyal mühendislik yöntemleriyle, kullanıcı anlamadan kabul ettirilmekte ve bu yazılımlar sisteme kurulmaktadır. Bu çeşit yazılımlar teknik tedbirlerin sağlanmadığı korumasız sistemlerde, kullanıcı etkinliği olmaksızın da yüklenebilmektedir. Bu bağlamda alınabilecek teknik tedbirlerden bazıları şu şekildedir:

- Anti-virüs yazılımının bulunması,
- Güvenlik duvarının aktif olması,
- Anti-malware yazılımların kurulması,
- İşletim sisteminin revize edilmiş olması önemlidir (Çalışkan, 2013).

Zararlı yazılımlar sebebi ile kullanıcıların yaşayabileceği bazı hususlar şu şekildedir:

- Bireysel, kurumsal veriler çalınıp, bu veriler diğer kişiler ile paylaşılabilir,
- İşletim sistemi ve yazılımların çalışmasına etki edebilir,
- Bilgisayarda bulunan belgeleri yok edebilir, kopya oluşturabilir, pozisyonlarını farklılaştırabilir ya da yeni belgeler oluşturabilir,
- Klavyeyle yazılan ve mouse ile gerçekleştirilen bütün her şeyi kaydedebilir,
- İstenmeyen internet sitelerine yönelten açılabilir sayfalar meydana getirebilir,
- Bilgi kaybına sebebiyet vermek adına bilgisayarda bulunan diski yeniden oluşturabilir,
- Sistem içinde kötü niyetli ve saldırgan kişilerin kullanması için güvenlik açıkları meydana getirebilir,
- İnternet kaynağını meşgul edebilir veya bilgisayarın ağır işlemesine sebebiyet verebilir.

Cisco aracılığıyla sunulan "2017 Siber Güvenlik Bildirgesi" kapsamında en çok rastlanan kötü içerikli yazılımlar, rakamları ile aşağıda gösterilmiştir (Cisco, 2017).

Şekil 2.1 2017 siber güvenlik bildirgesinde yer alan kötü içerikli yazılımlar

Ponemon Kurumu'nun bilgi ihlalleriyle alakalı 2010 yılındaki senelik bildirgesinde, 2010 senesinde zararlı yazılımlar sebebi ile bireysel bilgilerin yitirilmesiyle neticelenen durumlar, bütün olayların %24'lük kısmını meydana getirmektedir. Hizmetlerin sanal ortama aktarılması ve fazla olan internet tüketimi de önceki senelere kıyasla zararı arttırmaktadır (Civelek, 2011). Bu sebep ile kuruluşların gereken önlemleri alması, kullanıcıların da gerekli farkındalık eğitimleriyle bilgilendirilmeleri önemlidir.

Bilgi güvenliğine dair tehditlerden en bilinenleri zararlı veya kötü yazılımlar, ülkemizde ve dünyada çokça kullanılmakta ama kullanıcılar bu çeşit saldırıları ve

riskleri bilmemektedir. Hem kuruluşların hem de kullanıcıların bir zarar yaşamaması için bu konuya önem gösterilmelidir. Bu bağlamda kuruluşlar gereken özeni sağlayarak tedbirler almalı ve kullanıcı bilincinin oluşması adına seminerler gerçekleştirilmelidir (Canbek ve Sağıroğlu, 2007).

Bilgi güvenliğine dair tehditlerin en önemlilerinden zararlı yazılım çeşitleri tablo 2.1'de belirtilmiştir.

Tablo 2.1 Zararlı Yazılımların Temel Çeşitleri

Zararlı Yazılım Türleri (Malware)
Bilgisayar Virüsleri
Bilgisayar Solucanı (Worm)
Truva Atı (Trojans)
Arka Kapılar (Backdoor)
Ticari Tanıtım Yazılımları (Adware)
Klavye İzleme Yazılımları (Keylogger)
Casus Yazılımlar (Spyware)

i. Bilgisayar virüsleri

Virüsler üstünde ilk incelemeleri gerçekleştirmiş bulunan Dr. Frederick bakımından virüs kavramı, diğer uygulamaların içerisine kendisinin bir kopyasını dahil ederek giren bir bilgisayar yazılımı çeşididir (Canbek ve Sağıroğlu, 2006).

Başka bir ifadeyle; kullanıcının haberi olmadan bilgisayara giren, kendini kopya ederek artan, başka belge ve şifrelere dahil olan; sisteme, bilgisayara ve ağa zararı dokunan programların ismi bilgisayar virüsüdür (Yılmaz ve Salcan, 2008).

Bilgisayara giren virüslerin nasıl meydana geldiğini ve virüs yazılımı yapan bireylerin gayelerinin ne olabileceğini aşağıdaki gerekçelerle belirtmek mümkündür:

- İnceleme projesi çerçevesinde,
- Zarar oluşturma,
- Bazı kurumlarda zarar oluşturmak ve kurumların popülaritesini düşürmek,
- Siyasi ileti vermek,
- Ekonomik gelir kazanmak,
- Veri çalmak (Burlu, 2015).

En popüler kötü yazılım çeşitlerinden, virüsler, çoğunlukla kullanıcı aracılığıyla bir maile bakılması, taşınabilir hafıza kartlarının bilgisayarla bağlantısının sağlanması ya da internetten indirilen içinde virüs bulunan '*.exe' uzantısı olan bir belgenin bilgisayara kurulmasıyla girebilmektedir. Bu işlemleri yapan kişi, farkında olmadan virüs yazılımını bilgisayarına bulaştırmaktadır. Virüs yazılımlarını diğer kötü yazılımlardan farklı kılan niteliklerden en önemlisi birey etkileşimine gereksinim duymasıdır. Bilgisayara zararı olan kötü yazılımların aktif olabilmesi için, mutlaka bir kişi aracılığıyla çalıştırılması gerekmektedir (Gülmüş, 2010).

Genellikle e-mail ve taşınabilir cihazlarla sisteme giren virüs yazılımları, veri sistemlerinin işlemesini güç duruma sokmakta veya sistemlerin aksamasına sebebiyet vermektedir. Söz konusu bu kötü yazılımlar, uygulamayı tasarlayanın arzusu yönünde bilgi güvenliği olgusunu türlü biçimlerde riske sokmakta ve girdiği bilgisayarlarda belli bir hedefe dair etkinlik gerçekleştirmektedir. Verilerin yok olması, bozulması ya da silinmesi Bilgi güvenliği olgusuna dair söz konusu tehditlerin zararlarındandır. Bunun yanında virüs yazılımları uygulamalara kendilerini dahil edebilen, bu uygulamaların yapısını farklılaştırabilen ve kendisini kopyalayabilen özelliktedirler (Ünver ve Canbay, 2010).

Virüs yazılımları, hedefleri bakımından çeşitli biçimlerde sınıflandırılmaktadır: (Şahinaslan, 2013).

a) ***Dosya virüsleri;*** sürücü veya arşivlenmiş belgelere girerek çoğalan yazılımlardır.

b) ***Önyükleme(bootsector) virüsü;*** işletim sisteminin başlatılabilmesi için sabit diskte gereken belgelerin olduğu yere girerek sistemin çalışmasına engel olan virüslerdir

c) ***Makro virüsler;*** MS Office programları vb. içinde makro nitelik bulunduran uygulamalara giren kötü yazılımlardır.

d) ***Ağ virüsleri;*** yerel ağ üstünden paylaşılmakta olan belge ve sürücüler üstünden süratle ilerleyerek belgelerde zarar oluşturan yazılımlardır.

ii. Bilgisayar solucanı (worm)

1975'de John Brunner'in yazdığı "Şok Dalgası Binicisi (Shockwave Rider)" adlı eserinde, sistem üstünden kendisini yaygınlaştıran yazılım, solucan şeklinde

isimlendirilmiştir. Bu kitaptan hareketle bilgisayarda zarar oluşturan bu programlara bilgisayar solucanı ismi verilmiştir (Canbek, 2005).

Kötü yazılımlardan olan bu yazılım, kullanıcı işlevi olmadan kendisini bağımsız şekilde aktive edebilen, bilgisayarlara zararları dokunmadan bilgisayar bağlantıları arasında gezinebilen ve ağa dayalı öteki sistemlerde çoğalabilen yazılımlardır (Ulaşanoğlu vd., 2010).

Bu yazılımlar bilgisayar işletiminin çalışmasına engel olmakta ve bilgisayarın yavaş olmasına sebebiyet vermektedir. Bunun yanı sıra, virüslere kıyasla daha süratli yaygın hale gelmesi sebebi ile oldukça tehlikeli olmaktadır (Kınay, 2012).

Solucan yazılımların virüs yazılımlardan farklılaştığı noktalar şu şekildedir;

- Virüs yazılımları diğer uygulamaların içine girerek veya belgelere girerek kopyalanıp sayısı artmaktadır. Solucanlara bakıldığındaysa diğer bir programa bağlı olmamaktadır, yalnız da çalışabilmektedirler.
- Virüs yazılımları, e-mail, belge paylaşım ortamları ya da taşınabilir hafıza kartları üstünden bilgisayar ağları arasında yaygın olurken; solucan yazılımlar ağ aracılığıyla bulaşmaktadır.
- Virüs yazılımları kullanıcının zayıflıklarından faydalanarak bilgisayara bulaşırken; solucan yazılımlar sistemde bulunan boşluklardan faydalanmaktadır.
- Virüs yazılımlarının kullanıcıya gereksinimi varken, solucanlar buna gereksinim duymazlar (Çalışkan, 2013).

Solucanlar da kendi içinde farklı gruplarda toplanmaktadırlar. Bu gruplar: (Canbek ve Sağıroğlu, 2007):

a) ***E-mail solucanı:*** Solucan yazılımların en fazla kullanılan halidir. Genel olarak bir tek (bir resim veya metin belgesi) dosya olan e-mailde bulunurlar. Solucan kendi kendini çalıştırır ve kullanıcının adres defterini çoğaltır ve bu adreslere kendisini iletir. Solucan olan e-mail başlıkları, "3. Dünya savaşı başladı.", "Fidel Castro kaçırıldı.", "500$ para kazandınız." biçiminde ilgi çekicidir.

b) ***Anlık mesajlaşma solucanı:*** Anlık konuşma hizmetlerinden faydalanan bütün kullanıcılara, solucan girmiş bir belge ya da bir link atılarak kötü yazılımı bulunan solucanın yaygınlaşması kolaylaşır. Kullanıcılar linke tıkladığı zaman solucan bilgisayara inmiş olur ve aktif hale gelir. Böylece girdiği sistemin haberleşme ağında

bulunan bütün bağlantılara benzer türde iletiler gönderir. Böylece kendisini kopyalar ve yayılımını sürdürür.

c) ***İnternet solucanı:*** İnternetten gerçekleştirilen tarama neticesinde bilgisayarda bulunan güvenlik boşluklarından yararlanılarak sistemlere giren solucan türleridir. İnterneti kullanan bilgisayarların taraması yapılarak güncelleme gerçekleştirmemiş, güvenlik duvarı bulunmayan sistemleri saptar. Bulduğu sistemlerde kendisini çoğaltır ve yayılımını devam ettirir.

d) ***Ağ solucanı:*** Ağ üzerinden paylaşılan belgenin adını garip ve yararlı olacak biçime sokarak kullanıcıların bu belgeyi çalıştırmasını kolaylaştırır. Böylece çalıştırılan belge ile solucan sisteme girmiş olmaktadır.

iii. Truva atı (trojan)

Odysseia veya Odesa adlı Homeros'un meşhur eserinde bahsedildiği gibi Yunanlılar, Truva'yı fethetmek adına az sayıdaki askerin tahtadan üretilmiş bir at figürünün içine girerek, armağan edilerek kaleye girilmesini sağlamışlardır. Ata gizlenen askerler, gecenin geç saatlerinde içeriden kale kapılarını açmak suretiyle oranın sarılmasını kolaylaştırmışlardır (Canbek, 2005). Kötü yazılımlardan birisi olan bu Truva atı, adını, söz konusu tarihi olaydan esinlenilip almıştır. Yunanlıların hazırladıkları planın gerçekleşmesi adına atın, Truvalılarca içeriye ne şekilde sokulması gerekiyor ise bu kötü yazılımın da kullanıcı ile çalıştırılması gerekmektedir (Turhan, 2010).

Kötü niyetli ve saldırgan kişiler, zararlı kodları dahil ettikleri e-mail veya anlık iletileri seçtikleri kişilere iletmektedir. Böylece Truva atı, uzaktan erişim oluşturacak ana sisteme girmektedir. Saldırgan aracılığıyla belirtilmiş fonksiyonları, belli bir amaca dair gerçekleştirmesi açısından virüs yazılımlarından farklıdırlar (Çalışkan, 2013).

Bu yazılımın solucanlar ile benzer yanı, girdikleri bilgisayara arka kapılar dahil etmesi ve bilgisayara uzaktan erişimi gerçekleştirmesidir (Gülmüş, 2010).

Solucan yazılımlardan farklı olduğu yönler ise:

- Hangi yazılım ile sisteme girmişse o uygulama açılmadan aktif hale gelmez.
- Bilgisayarın işletimini doğrudan etkileyebilir.

- İzinli olmayan erişimleri yapabilecek bütün denetimleri ele alabilir (Yaşar, 2014).

Truva atları, bilgisayarın işleyişini bozabilmekte, kullanana özel parola ve bireysel verilere erişebilmektedir. Girdiği bilgisayarın açılması ile birlikte kendini sisteme dahil etmekte ve sistem boşluklarından yararlanarak istediklerini yapmaktadır (Turhan, 2010).

Bağımsız bir yazılımla kendini zararsız ve değişik tanıtarak, kullanıcının gereksinimi olan bir işlevi yapıyormuş gibi çalışan, esasen izinli olmayan erişimleri (bilgisayarın kamerasını kullanarak görüntüsü alma veya optik sürücünün kapağıyla oynama vb.) basitleştiren çeşitleri de vardır (Ünver vd., 2010).

Açıklandığı gibi, Truva atları görünürde kullanana faydası olan ama içinde kötü şifrelemelere sahip yazılımlardandır. Bu yazılımın verdiği kayıplar aşağıda yer almaktadır (Gülmüş, 2010);

- Bilgisayar denetimini ele alabilir ve böylece sistemin izlenmesini gerçekleştirebilir.
- Klavyenin tuşlarını izleyip çeşitli verilere sahip olabilir.
- Bilgileri silebilir veya üstüne veri ekleyebilir.
- Belgeleri tehlikeye sokabilir.
- Odaklanılan bilgisayarda uzaktan erişim gerçekleştirebilir.

Truva atının bilgisayara girmesi genellikle internet üstünden olmaktadır. E-mail ile, popüler oyunlar veya parasız uygulamalarla bilgisayara girmektedir. Bu sebep ile kullanıcılar mümkün mertebe bilinmeyen ve sunucularından emin olmadıkları mailleri açmamalı, parasız programa yönelmemeli ve lisansı bulunmayan yazılım kullanmamaya dikkat etmelidirler (Taş, 2010).

iv. Klavye izleme (key logger) yazılımları

Trojan türlerinden birisi de Key Logger, en sade ifade ile, klavye üzerindeki tuş eylemlerini izleyerek verileri karşı tarafa aktarmayı saklayan kötü yazılımlardır (Taş, 2010).

Ana görevi, kullanıcının klavye ile yazdığı bütün her şeyi algılayan bu yazılımlar, “screen scraper” (ekran kazıyıcı) ve “keycatcher” (tuş yakalayıcı) şeklinde de isimlendirilmektedir (Canbek, 2005).

Keylogger yazılımıyla kullanıcıya dair kişisel veriler kötü niyetli bireylere aktarılmaktadır. Aktarılan bu verilerden bazıları, internet bankacılık parolaları, kredi kartları bilgileri ve parolası, sosyal medya uygulamalarını dair parolalardır. Özetle keylogger yazılımının bulunduğu herhangi bir sistemde, kullanıcı aracılığıyla klavyeyle işlenilen bütün parolalar kötü niyetli ve saldırgan kişiler aracılığıyla bilinmektedir (Altun, 2014).

Say ve Sağıroğlu (2004), yaptıkları incelemede, kötü niyetli programların risk teşkil ettiği bireysel bilgi güvenliğinin sağlanabilmesi adına, alınması gereken tedbirler üstünde çalışmışlardır. İncelemeyi yapan kişilerce bulunan anti-casus programlarıyla bu yazılımlar belirlenmekte ve kendiliğinden yok edilmektedir. Aynı şekilde bu incelemede klavyeyi dinleyen sistemlerin belirlenmesinin oldukça güç olduğu ve vakit gerektirdiği belirtilmiştir.

Kullanıcılar bireysel bilgilerinin güvenliğini oluşturmak adına keylogger yazılımlarına yönelik tedbirler oluşturmalıdır. Bu tedbirlerden ikisi dijital imza ve sanal klavyedir. İnternet bankacılığı veya parola gerekli olan fonksiyonlarda sanal klavye veya dijital imzadan faydalanılmaktadır (Kınay, 2012). Ancak, sanal klavye olgusu "screenlogger"ın yazılımlarının bulunması ile birlikte yetersiz kalmıştır. Bulunan yeni çeşit casus programlarıyla ekrana yazılan tüm şeyler kaydedilmektedir (Taş, 2010). Bunun yanında, casus programlara dair uygulanan paket yazılımlar, klavye izleme düzenlerini tam anlamıyla belirleyememekte, dikkat dahi etmemektedir. Bu nedenlerden dolayı bu programlara yönelik kullanıcılar kendi önlemlerini kendileri oluşturmalı ya da klavye izlemesini engelleme programlarından yararlanmalıdırlar (Canbek ve Sağıroğlu, 2007).

Klavye izlemesini engelleyici yazılımdan kimileri şu şekildedir:

- Anti-keylogger
- Keylogger Hunter
- Advanced Anti Keylogger (Canbek, 2005).

v. Casus / köstebek (spyware) programlar

Bu yazılımlar, girdikleri bilgisayardaki kullanıcıya dair önemli verileri, kullanıcının gerçekleştirdiği fonksiyonları, bu bireylerin iznini almadan saldırganlara ileten yazılımlardır (Canbek, 2005).

Kullanıcının sistemine gizli bir şekilde kurulan bu programlar, kullanıcılarla alakalı veri elde etmelerinin yanında bu bireylerin bilgisayarı ve gezinme alışkanlıkları (girilen web pencereleri) ile alakalı da veri elde edip karşıya iletmektedir (Ünver vd., 2010). Bu sebep ile bu programlar bireylerin izni olmadan bilgisayara kurulduğunda, veri güvenliğine dair meydana gelen en önemli saldırılardan olmaktadır.

Casus programların bilgisayarlara etkileri şöyledir:

- Bilgisayar performansında görülür bir farklılık bulunuyor ise,
- İnternet sayfalarında beklenmeyen zamanlarda reklam sayfaları açılıyor ise,
- İnternet sayfalarında bulunan arama sistemi neticeleri farklılaşmışsa,
- Beklemediğiniz anlarda server ana sayfası normalden değişikse
- Serverda daha önce karşılaşılmayan görev çubukları görülüyorsa,
- İnternetin bulunmadığı durumlarda bile pop-up reklamları açılıyor ise,
- CD player beklemediğiniz zamanlarda açılıyor kapanıyor ise büyük ihtimalle sisteminizde casus bir program bulunmaktadır (Canbek, 2005).

Bu yazılımlar değişik metotlardan yararlanarak bilgisayara ya da sisteme girmektedir. Bu yazılımlar, yararlı ve işlevsel görünüp "parasız" olduğu üstünde durulan programlarla kullanıcının ilgisini çekmekte ve kullanıcıya kabul ettirerek bilgisayara yerleşmektedir (Kınay, 2012).

Bilgisayara giren casus programların ana gayesi, odaklandığı noktayla alakalı mümkün mertebe fazla veri elde etmektir. Bireysel verilere ulaşarak kullanıcıda zarar oluşturmayı amaçlayan kötü niyetliler haricinde, bu programlar ticari kurumlarca da sızdırılabilmektedir. Ticari kurumlar, bireylerin internet üstündeki aktivitelerini çözümleyerek eylemlerini belirlemekte ve reklamları kullanıcının gereksinimi paralelinde göstermektedir (Canbek ve Sağıroğlu, 2007).

Casus programlardan korunmak adına anti-virüs yazılımları yeterli değildir. Bu konuda bireylerde farkındalık yaratılmalı ve bu yazılımlara yönelik kullanılan anti-spware programlarının sistemlere yüklenmesi gerçekleştirilmelidir (Taş, 2010).

vi. İstem dışı ticari tanıtım (adware) yazılımları

Adware programlarının ana gayesi reklamları kullanıcılara sunmaktır. Üstünde çalıştıkları bilgisayarda bulunan bireysel ve istatistiki bilgileri kullananın izni ve haberi ile 3. kişilerle paylaşmaktadır (Turhan, 2010).

Adware yazılımları, bireye hususi reklamların göstermek adına girilen internet sitelerinin çeşitleriyle alakalı pazarlama bilgileri elde etmek adına dizayn edilmiştir. Bu yazılımlar, casus yazılımlardan farklıdır. Adware'ler izninizle veri elde eden programlar iken, casus programlarsa izinsiz veri elde etmektedir. Adware, veri toplamasını size belirtmediği müddetçe casus program şeklinde görülür (Kaspersky Resource Center, 2019).

vii. Mantık bombaları

Hedef bilgisayara kurulur ama işlevini gerçekleştirmesi adına programlanan saatin gelmesi veya belli koşulların iyileşmesini bekler (Taş, 2010).

Şartlar tamamlandığında mantık bombaları bilgisayarda zarar oluşturacak eylemlere başlamaktadır. Bu şartlar;

- Gün içinde belirli bir vakit,
- Herhangi bir zaman dizini,
- Belli bir kullanıcının bilgisayara girmesi vb. durumlardır (Gülmüş, 2010).

Önceden düzenlenen kötücül yazılımlar, kötü niyetli kişiler ve saldırganlar aracılığıyla emir gönderildiğinde harekete geçmektedir. Emir verilene değin bilgisayarda saklanır. Vakit gelince mantık bombaları bilgisayarda geri dönüşü olmayan zararlar oluşturmaktadır (Ercan, 2015).

viii. Arka kapılar (backdoor)

Arka kapı, veri sistemleri içinde bulunan kimlik onaylama süreçlerini bilgisayarda yer alan boşluklardan yararlanarak üstesinden gelen ve bilgisayarlara erişimi kolaylaştıran bir yaklaşımdır (Canbek, 2005).

Sistemi ilerleten yazılımcı aracılığıyla, test müddetince vakit kaybı yaşanmaması bakımından yok edilen parolalar, unutulan boşluklar halini almaktadır. Meydana gelen bu boşlukları gören saldırganlar bilgisayarlara girmekte ve bazı hasarlara sebebiyet vermektedir. Arka kapılar, genellikle Truva atlarıyla aynı sanılmaktadır. İki yazılım da kötü niyetli programlardandır, fakat farklı oldukları yer ise, Truva atları yararlı gibi kendilerini tanıtırken; arka kapılar, saklanarak bilgisayara yalnızca erişim sağlayan yazılımlardır (Turhan, 2010).

Arka kapı, esasında veri sistemlerine girmek adına yararlanılan saklı bağlantıdır. Bilgisayara arka kapıdan faydalanarak ulaşılması halinde bu ulaşım

kayıtları bilgisayarda fark edilmemektedir. Bütün bu sebeplerden ötürü arka kapıların, veri güvenliğine ve sistemlerine dair bir risk şekline dönüşmemesi için, izlemlere uygun biçimde programlar bulunmalı ve revize edilmelidir. Programlar kullanılmadan önce yazılımcısı aracılığıyla arka kapı yazılımları temizlenmelidir (Gülmüş, 2010).

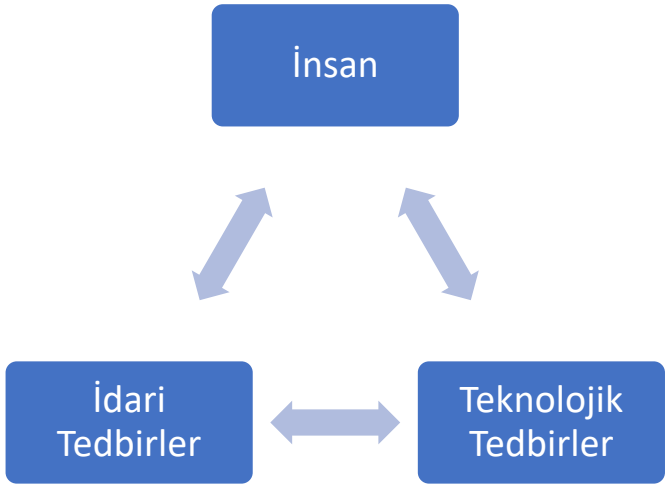
2.1.6 Bilgi Güvenliğinin Sağlanmasına Yönelik Önlemler

Bilgi güvenliği olgusu, verinin doğruluğunun ve bütünlüğünün sağlanması adına, verilere kötü niyetli bireylerin ulaşmasının önüne geçmek ve bu hususta gereken tedbirlerin sağlanması şeklinde ifade edilmektedir. Veri ve bilgisayar güvenliği birbirleri ile karıştırılan olgulardır. Bilgisayar güvenliği olgusu, veri güvenliği kavramının bir alt parçasıdır (Canbek ve Sağıroğlu, 2006; Marks, 2007).

Son zamanlarda veri ve bilgisayar güvenliğini riske sokan; birey, kuruluş ve firmalar üstünde ekonomik ve manevi hasarlara sebebiyet veren çeşitli saldırılar gerçekleşmektedir. Bu hasarların minimum seviyeye düşmesi için veri güvenliğine dair önlemlerin sağlanması bir mecburiyet şekline dönüşmüştür (Vural ve Sağıroğlu, 2007).

Bilgi güvenliği olgusu oldukça detaylı ve kompleks bir durumdur (Wright ve Kakalık, 2007). Veri güvenliğinin teminatı, aşağıdaki üç ana sürecin birlikte sağlanmasıyla mümkündür (Şekil 2.2).

Şekil 2.2 Veri güvenliği sürecindeki öğeler



- ***İdari tedbirler;*** doğru program, politika ve stratejilerin gerçekleştirilmesi,
- ***Teknolojik tedbirler;*** güvenlik duvarı, şifreleme, anti-virüs programları, yedekleme yapma, denetim vb. tedbirlerden yararlanılması,

- ***Farkındalık ve eğitim;*** kullanıcıların veri güvenliği hususunda farkında olmalarını sağlamak adına çeşitli farkındalık ve eğitim çalışmalarının uygulanmasıdır (Öztürk vd., 2016).

2.1.6.1 Teknolojik Bakımdan Sağlanacak Tedbirler

İnsan ögesinin olduğu her yerde olduğu üzere veri güvenliği hususunda eksiksiz bir güvenlikten bahsetmek mümkün değildir. Donanım, yazılım ve sistemle ilgili sağlanacak bütün teknolojik tedbirler, bilgilerin güvenliğine tam olmasa dahi mutlaka yarar sağlayacaktır (Gencer, 2015).

Veri teknolojilerindeki ilerlemeler ışığında veriye ve sistemlere dair gerçekleştirilen saldırılar her ilerleyen gün fazlalaşmaktadır. Bu saldırılar, verinin gizlilik, bütünlük ve erişilebilirliği hususunda önemli ve geri dönüşü zor hasarlara sebebiyet vermekte ve teknolojik tedbirlerin sağlanma mecburiyetini gündeme getirmektedir. Önceden ve zamanında sağlanacak güvenlik tedbirleriyle zararları tamamı ile yok etmek muhtemel olmasa dahi, bilgisayarda oluşturacağı hasarın etkisini hafifletecektir (Vural, 2007). Bu sebep ile yeni saldırı çeşitlerinin devamlı izlenmesi ve bu hususta Dünya'da ve ülkemizde gerçekleşen işlem ve incelemelerin araştırılması gereklidir. Bu incelemeler neticesinde saptanan boşlukların kapatılmasına yönelik önlemler kurumlarca sağlanması zorunludur. Böylece veri güvenliği ihlalinin önüne geçilmesi için yapılması gereken işler başlatılmış ve iş devamlılığı sağlanmış olacaktır (Gülmüş, 2010).

Saptanan teknik açıklarla alakalı risk tespiti gerçekleştirilirken, güvenlik ve kullanılabilirlik tutarlılığı göz önünde bulundurulmalıdır. O zamanki şartlarda sağlanacak tedbirler, sistemi kullanılabilirlikten uzaklaştıracak ise meydana gelen tehlikeye katlanılabilir. Fakat tehlikenin üzerinde durulmaması, söz konusu açığın meydana getirdiği tehlikenin var olduğu gerçeğini değiştirmemektedir. Sistemde meydana gelen bu teknik açıkların tehdit şeklinde değerlendirilmesi gerçekleştirilirken, üstünde durulması gerekli başka ögeler de vardır. Açığın teknik düzeyi olan "derece" ve bu açığın firma bakımından "önemi"dir. Örnek olarak; hiç çalışmayan bir sistemde olan teknik anlamda açık düzeyi oldukça fazla bulunmasına karşın, firma bakımından önemi az olabilmektedir veya tehlikeli bir yerde çalışan sistemde bulunan düşük dereceli bir açık firmada görevlerin sekteye uğramasına sebebiyet verdiğinden firma bakımından oldukça önemlidir (Dinçkan, 2008).

Konusu geçen bu teknik derecelendirme gerçekleşirken şekil 2.3'te bulunan ölçütler dikkate alınmalıdır (Muharremoğlu, 2013):

Şekil 2.3 Açıkların teknik bakımdan derecelendirilmesi

Seviye	Açıklama
Kritik 	Sisteme veya veritabanına direk erişim sağlanabilen, veri elde edilebilen, değiştirilebilen veya sistemi uzaktan devre dışı bırakabilecek açıklar.
Yüksek 	Sisteme veya veritabanına direk erişilemeyen ancak başka açıklarla birleştirilerek ve denemeler yapılarak verilere erişim yapılabilen açıklar.
Orta 	Tek başına kullanımı ile sistemleri etkilemeyen ancak başka yöntemlerle birleştirilip kullanıldığında güvenlik ihlali oluşturabilecek açıklar.
Düşük 	Sistem ve uygulamalar üzerinde konfigürasyon sıkılaştırılması yapılmamış, kötü niyetli kullanıcılara sistemler hakkında bilgi veren açıklar.
Bilgilendirme 	Sistemin ve altyapının daha güvenilir ve güvenli olmasını sağlayacak güvenlik önerileri.

Teknolojiden faydalanırken güvenliğin oluşturulması adına öncelikle yapılması gerekli mantık, güvenliğin aktif bir süreç olduğudur. Güvenlik ölçütleri ve rehberleri de bu düşünce ışığında düzenlenmekte ve ilerletilmektedir. Bu sebep ile bilgi güvenliğini olgusunun oluşturulması adına kullananların ve teknik çalışanların kendilerini devamlı ilerletmeleri ve yararlanılan teknolojilerin de bu ilerlemeler ışığında revize edilmesi önemlidir. Yalnızca teknolojiyle güvenliğin oluşturulması muhtemel değildir. Nitekim, bu teknolojiden yararlanan kişiler gereken düzeyde bilgiyi bulundurmaz ve yeterli desteği almaz ise yalnızca teknolojiden faydalanılması, bilgi güvenliği olgusunun oluşturulması halinde yeterli olmayacaktır (Vardal, 2009).

Bilgi güvenliği olgusunun oluşturulması adına teknik gereçlerin sağladığı teknolojiye dayalı çözümlerden virüslerden temizleme, ağ sorunlarını çözme, izinsiz erişmeleri kısıtlama vb. çoğunluk ile kullanılan metotlardandır (Civelek, 2011). Ancak teknolojik tedbirler bunlardan ibaret değildir.

Bilgi güvenliği olgusu gerek bireysel gerekse de kurumsal güvenliği kapsadığından, teknolojik tedbirlerin her iki olgu kapsamında sağlanması bilgi

güvenliği olgusunun oluşturulması bakımından oldukça önemlidir (Özenç, 2007). Bilgi güvenliği olgusuna dair sağlanacak teknolojik tedbirlerden bazıları şu şekildedir:

- Parola teknolojileri
- Dijital İmza
- Güvenlik Duvarı
- Yedekleme yapma
- Anti-virüs yazılımları
- Yazılım güvenliği
- Ağ güvenliği
- Web güvenliği
- Kullanan hesap güvenliği

2.1.6.2 İdari Bakımdan Sağlanacak Tedbirler

İdari tedbirler, bilgi güvenliği idaresiyle alakalı prensiplerin oluşturulması ve yürürlüğe konması biçiminde ifade edilebilmektedir (Yıldız, 2014).

Bilgi güvenliği sadece teknolojik tedbirlerin (anti-virüs yazılımları, firewall gibi) sağlanması ile oluşturulamaz. Bilgi güvenliği olgusu, iş süreçlerinin bir parçası şeklinde benimsenmeli, idare ve firma kültürü şeklinde incelenmelidir. Her firma mutlaka bilgi güvenliği olgusunu bulundurmalıdır. Kişisel ve firma düzeyinde düzenlenecek güvenlik stratejileri yazılı şekle dönüştürülmeli; iş görenlere ve ortaklarına iletilmelidir. Personellerin bu stratejileri bilmeleri ve onlar üstünde farkındalık oluşturması önemlidir. Fakat firmaların güvenlik stratejilerini bulundurması bilgi güvenliği olgusunun oluşturulması aşamasında yetersiz kalmaktadır. Bu hususta personellere de önemli vazifeler yüklenmektedir. Bilgi güvenliğinin farkında olan personeller ulaştıkları verileri muhafaza edecek, verinin güvenliğinin oluşturulması hususunda titiz davranacaklardır. Personellerin bilgi güvenliği stratejilerini önemsemesi ve gerçekleştirmesi konusunda üst idarenin rolü de etkilidir. Üst idarece onay görüp yayımlanan güvenlik stratejileri, bilgi güvenliği olgusunun önemini açıklamalı ve gereken vazifeleri saptamalıdır. Bu stratejiler iş paydaşlarını (müşteri, kurum, tedarikçi vb.) içerecek biçimde düzenlenmelidir (Doğantimur, 2009).

İdari tedbirler doğrultusunda ana süreçlerin tamamlanması gereklidir. Bu süreçler:

- Risk idaresi,
- Güvenlik stratejileri,
- Ölçütler, komutlar ve yöntemler ile
- Güvenlik kontrolleridir (Yıldız, 2014).

2.1.6.3 Eğitsel Bakımdan Sağlanacak Tedbirler

Yaşamın her alanında teknolojinin sağladığı olanaklardan yararlanan kişiler eş zamanlı olarak bilgi güvenliği olgusuyla yüz yüze gelmektedir. Bireyler, bilgi güvenliği olgusuna dair gerçekleştirilen tehditlerde en güçsüz zincir halini almış; bilgi güvenliği olgusunun oluşturulmasında birey etmeni, anahtar vazifesini üstlenmiştir. Bu anlamda olması muhtemel tehditlere yönelik bireylerde farkındalık oluşturulması, bilgi güvenliği olgusunun bilinmesine dair önlemlerin oluşturulması zorunlu bir hal almıştır (Mart, 2012).

Kurumsal anlamda bilgi güvenliği olgusu; yazılım, donanım, kişi, sistem vb. veri kaynaklarının dış ve iç tehditlere yönelik muhafaza edilmesi şeklinde ifade edilmektedir (Koç, 2008). Kurumsal anlamda bilgi güvenliği olgusunun oluşturulması hususunda dış kaynaklı oluşabilecek tehlikelere dair tedbirler oluşturulması ne denli önemli ise; kurumda oluşabilecek tehditlere dair tedbir oluşturulması da o denli önemlidir. Kurumda tehlike arz edebilecek en önemli öge çalışandır. Bilerek oluşan zararları bertaraf etmek adına firmalar öncelikle güvenilir çalışan almak ile işe başlamalıdır. Ayrıca çalışanın bilgi eksikliğinden doğan yanlışları minimuma düşürebilmek adına eğitim ve farkındalık çalışmalarının, firma içinde gerçekleştirilmesi önemlidir. Bilgi güvenliği idaresinin başarılı biçimde devam ettirilmesi, kişilerin bilgi güvenliği hususunda eğitilmesiyle mümkün olmaktadır (Eminağaoğlu ve Gökşen, 2009).

Güvenliğin en güçsüz zinciri şeklinde benimsenen insan etmeni çerçevesinde bulunan son kullanıcı aracılığıyla oluşan güvenlik aksaklıklarının, genel olarak bilinçlendirme ve farkındalık eksikliklerinden oluştuğu bilinmektedir (Vural ve Sağıroğlu, 2007).

Personeller, bilgi güvenliği olgusunun yalnızca teknolojik gereçler ile gerçekleştirildiğini sanmakta, problemin yalnızca güvenlik duvarı veya diğer teknolojiler ile gerçekleştirileceğini tasarlamaktadırlar. Bilinçlendirme çalışmalarının

ana gayelerinden birisi, her bir iş görenin, firmanın genel güvenliğine katkısının olacağının bilincini oluşturmaktır (Mitnick and Simon, 2016).

Üniversitelerde bulunan yönetici ve akademik çalışanlar ve öğrenciler, teknik topluluğa katılmayan kullanıcıları temsil etmektedir. Üniversitede gerçekleştirilecek bilinçlendirme eğitimlerinin ana gayesi, gerçekleştirilmesi gerekli ana güvenlik denetimleriyle alakalı kullanıcıyı bilinçlendirmek ve kullanıcının bilgi güvenliği olgusunu tehlikeye sokan tehditlerle alakalı genel bilgilendirmeyi gerçekleştirmektir (Vardal, 2009).

Güvenlik hususunda farkındalık eğitimlerinin ana gayesi, firmanın bilgi kaynaklarının muhafazasına katkıda bulunmak hedefi ile her bir personeli motive etmektir. Kazandırdıklarının yalnızca firmaya değil, eş zamanlı olarak kendilerine ve diğer personellere de getirisi olacağı üzerinde durulmalıdır. Bu verilerin muhafazasına etkisi olan personeller, esasında kendi verilerini de muhafaza ederler. Nitekim, firmalar her personel ile alakalı belli bireysel verileri barındırır (Mitnick and Simon, 2016).

Birçok konuda olduğu üzere, bilgi güvenliği olgusunun oluşturulmasında da istekli, eğitimli ve farkındalığı olan kişilerin bulunması önemlidir. Firmanın ana gayesi, bilgi güvenliğini olgusunun firma kültürüne dönüşümüne yardımcı olmaktır. Çok tecrübeli bir saldırgan aracılığıyla oluşabilecek hasardan daha tehlikeli olan bir husus bulunur ki, o da firmadaki kötü niyetli, eğitimsiz veya işini önemsemeyen çalışandır (Eminağaoğlu ve Gökşen, 2009).

Wenger, Metzger ve Dunn (2008) bakımından bilgi güvenliği olgusunun oluşturulmasının en önemli koşullarından biri, insan etmeninin bilinçlendirilmesidir. Bu farkındalıkla beraber, kişiler, verinin ne şekilde ve ne sebeple muhafaza edilmesi gerektiği hususunda bilinçleneceklerdir. Böylece hatalı tutumlarının nasıl neticeler getireceğini ve veri güvenliğine ne şekilde etki edeceğini kavrayacaklardır.

Mükemmel bir eğitim almış kişiler, güvenlik hususunda meydana gelebilecek aksaklıkların önüne geçebilmektedirler. Bu sebeple, kişilerde ve toplumda farkındalık yaratmak ve arttırmak oldukça önemlidir. Bu anlamda çeşitli medya araçlarıyla veya eğitim planlarının tertip edilmesiyle kişilerin bilinçlenme oranlarının artması sağlanabilir. İngiltere, güvenlik probleminin eğitimle çözülebileceği fikrinden yola

çıkarak, eğitim planlarına güvenli internet kullanımı konusunda mecburi bir ders dahil etmeyi tasarlamaktadır (Ulaşanoğlu vd., 2010).

Bilgi güvenliği olgusu üzerine yoğunlaşan kuruluşlar incelendiğinde birçoğu banka, maliye, büyük şirketler, yazılım şirketleri ve devlet kuruluşlarıdır. Halbuki bütün alanlarda ve kuruluşlarda bilgi güvenliği olgusunun yaygın hale gelmesi, uzun süreler devam etmesi ve vizyoner olmasının gerekli bir durum olduğu fikrinin kabullenilmesi önemlidir. Bu düşüncenin kökleşmesi ve yaygın hale gelmesi yalnızca halkın bilgi güvenliği hususunda farkındalık oluşturulmasıyla gerçekleşebilir. Bunun yanında kişilerin gündelik hayatlarında sıklıkla kullandıkları internet ve taşınabilir cihazlara bakıldığında, yalnızca iş için değil kişisel bakımdan da bilgi güvenliğine dair çözümlerin hızlı bir biçimde yayılmasının gerekliliği bilinmektedir (Swaminatha ve Elden 2003).

Gelecek yıllarda Dünya çapında ve ülkemizde, bilgi güvenliği olgusuna dair gerçekleşmesi muhtemel saldırılar, oldukça kompleks metotlara dayanacağı ve daha fazla insanı tehlikeye sokacağından, kurumsal veri güvenliği olgusuna dair gerçekleşen tehditleri konu edinen incelemelerin önemi daha iyi anlaşılacaktır. Bu incelemeler ışığında, tehditlere yönelik, kurumlarını ne şekilde muhafaza etmeleri gerektiğiyle alakalı kuruluşlarda ve kişilerde farkındalık oluşturulmalıdır (Vural ve Sağıroğlu, 2007).

BÖLÜM III
GEREÇ VE YÖNTEM

Bu bölümde araştırmanın yöntemi, çalışma grubu, veri toplama araçları, verilerin toplanması, verilerin istatistiksel analizi ve araştırmacının rolü açıklanmıştır.

3.1 Araştırmanın Yöntemi

Araştırmada nitel ve nicel araştırma yöntemlerinin bir arada bulunduğu karma yöntem kullanılmıştır. Karma yöntem araştırması, araştırmacı tarafından bir çalışmada ya da birbirini izleyen çalışmalarda nicel ve nitel yöntemler, yaklaşımlar ve kavramların birleştirilmesi olarak açıklanmaktadır (Creswell, 2003). Karma yöntem ile araştırma yapılarak, çeşitli metotlar aracılığıyla olaylar, bir çerçeve içinde sunulup, analiz edilip bir araya getirilmektir. Johnson ve Onwuegbuzie (2004) karma araştırma yönteminin temel ilkesinin, araştırmacının farklı strateji, yöntem ve yaklaşımları kullanarak çoklu veriler toplaması olarak ifade etmektedir. Bunun yanı sıra, Creswell (2006) karma yöntemin temel önermesinin nitel ve nicel yaklaşımların birlikte kullanılmasının, her iki yaklaşımın tek başına kullanılmasına kıyasla araştırma probleminin daha iyi anlaşılmasını sağlamak şeklinde açıklamaktadır. Karma araştırma yöntemi; çoğulcu, kapsamlı, tamamlayıcı ve araştırmacı için yöntem belirlemede ve çalışma hakkında tasarlama yapmada seçmeci bir yaklaşım sunar. Birçok araştırma problemi veya problemleri karma araştırma yöntemin sunduğu çözüm yollarıyla tam anlamıyla yanıtlandırılabilir (Johnson and Onwuegbuzie, 2004). Araştırmada karma yöntem olarak "Sıralı Açıklayıcı Desen" kullanılmıştır. Araştırma kapsamında karma yöntem kullanılarak elde edilecek nicel veriler, nitel veriler ile desteklenerek daha geniş kapsamlı bulgulara ulaşılabilecektir.

Araştırmanın nicel yöntem ile gerçekleştirilen bölümünde tarama araştırması uygulanmıştır. Tarama araştırmaları ile yapılan çalışmalarda hedef kitlenin görüşlerinin özellikleri betimlenmektedir. Bu araştırma türünde ne, nerede, nasıl, ne sürede, hangi sıklıkta ve düzeyde, vb. soruların yanıtları araştırılır. Tarama araştırmasının amacı, genel olarak araştırma konusuyla ilgili olan mevcut durumun fotoğrafının çekilmesi ile betimleme yapılmasıdır. Bu amaç doğrultusunda tarama araştırmasında genel olarak hedef kitlelerden araştırmacının belirlediği cevap seçenekleri aracılığıyla veri toplanmaktadır (Büyüköztürk vd., 2016). Araştırmada

tarama araştırması yöntemi kullanılmış ve bu doğrultuda ölçek ve anket uygulaması yapılmıştır.

3.2 Araştırmanın Çalışma Grubu

Araştırmanın çalışma grubunda, İzmir ili Bornova İlçesinde bulunan Suphi Koyuncuoğlu Ortaokulu, Süleyman Demirel Çok Programlı Anadolu Lisesi, Özel Yeşeren Ortaokulu ve Özel Yeşeren Anadolu Lisesi olmak üzere 2 devlet okulu ve 2 özel okuldan seçilen öğrenci, öğretmen, veli ve okul yöneticileri yer almıştır.

Araştırmanın nicel yöntem uygulanan bölümünde, kolay ulaşılabilir örnekleme yöntemi ile belirlenen, İzmir ili Bornova İlçesinde bulunan Suphi Koyuncuoğlu Ortaokulu, Süleyman Demirel Çok Programlı Anadolu Lisesi, Özel Yeşeren Ortaokulu ve Özel Yeşeren Anadolu Lisesi olmak üzere 2 devlet okulu ve 2 özel okuldan rastgele bir şekilde öğrenci, öğretmen ve okul yöneticileri seçilmiştir. Ortaokul ve lise düzeyinden 50'şer öğrenci ve 30'ar öğretmen olmak üzere toplam 200 öğrenci ve 120 öğretmen ile 4 okul yöneticisi gönüllük esasına dayalı olarak araştırmada yer almıştır.

Araştırmanın nitel yöntem uygulanan bölümünde, gönüllük esasına dayalı olarak, çalışma grubunda yer alan okullarda öğrenim gören öğrenciler ve bu öğrencilerin velileri içerisinden, her okuldan 3'er öğrenci ve 3'er veli seçilmiş olup, toplamda 12 öğrenci ve 12 veli araştırmaya katılmıştır. Belirlenen okullarda görev yapan öğretmenler ve okul yöneticileri içerisinden, her okuldan 3'er öğretmen ve 1'er okul yöneticisi seçilmiş olup, toplamda 12 öğretmen ve 4 okul yöneticisi çalışmada yer almıştır.

3.2.1 Öğrencilerin Demografik Bilgileri

Tablo 4.1 incelendiğinde, araştırmada yer alan öğrencilerin (n=200); %36'sının kadın, %64'ünün erkek, %50'sinin ortaokul, %50'sinin lise düzeyinde olduğu görülmektedir. 200 öğrencinin %71'inin kendi bilgisayarı olup, %28,5'inin kendine ait bilgisayarı bulunmamaktadır. Evde yer alan bilgisayarın konumu incelendiğinde, öğrencilerin (n=200), %55,6'sının kendi odasında, %18,7'sinin salonda, %12,1'inin oturma odasında, %9,6'sının başka bir aile bireyinin odasında, %4'ü ise diğer bir yerde yer aldığı görülmüştür. Bu verilere göre, öğrencilerin büyük bir çoğunluğu bilgisayarı kendi odasında ve ebeveynlerinin olmadığı bir ortamda kullandığı bulgusuna ulaşılmıştır. Velilerin internet ve bilgisayar kullanımına yönelik kısıtlamalarına bakıldığında, %36,1'inin süre kısıtlaması, %5,5'inin kullanılan programlara yönelik

kısıtlama, %7,3'ünün internette gezinilen siteye yönelik kısıtlama, %2,3'ünün maddi kısıtlama, %2,3'ünün diğer kısıtlamaları getirdiği %46,6'sının ise hiç kısıtlama getirmediği tespit edilmiştir. Bu bulgulara göre, velilerin çoğunluğunun herhangi bir kısıtlama getirmediği, kısıtlama getiren velilerin de genel olarak süre kısıtlaması getirdiği görülmektedir. Öğrencilerin (n=200) %32,1'i aile üyelerinden, %11,8'i arkadaşlarından, %2,1'i kitaplardan, %30,8'i internet kaynaklarından, %1,7'si diğer kaynaklardan yardım için faydalanırken, %21,5'i ise hiçbir kaynaktan yararlanmamaktadır.

Tablo 4.1 Öğrencilerin Demografik Bilgi Analizi Tablosu 1

		frekans	**yüzde**
Cinsiyet	**Kadın**	72	36
	Erkek	128	64
	Toplam	200	100
Sınıf düzeyi	**Ortaokul düzeyi**	100	50
	Lise düzeyi	100	50
	Toplam	200	100
Evde öğrencinin kendisine ait bilgisayarı var mı	**Var**	142	71
	Yok	57	28,5
	Toplam	199	99,5
Evde bilgisayarın konumu	**Kendi odası**	110	55,6
	Salon	37	18,7
	Oturma odası	24	12,1
	Başka bir aile bireyinin odası	19	9,6
	Diğer	8	4
	Toplam	198	100
Velinin internet ve bilgisayar kullanımına yönelik kısıtlamaları	**Süre kısıtlaması**	79	36,1
	Kullanılan programlara yönelik kısıtlama	12	5,5
	İnternette gezinilen siteye yönelik kısıtlama	16	7,3
	Maddi kısıtlama	5	2,3
	Hiçbiri	102	46,6
	Diğer	5	2,3
	Toplam	219	100
Bilgisayar kullanırken yardım için kime/neye başvuruluyor	**Aile üyeleri**	76	32,1
	Arkadaşlar	28	11,8
	Kitaplar	5	2,1
	İnternet kaynakları	73	30,8
	Hiçbiri	51	21,5
	Diğer	4	1,7
	Toplam	237	100

Tablo 4.2'de teknolojik cihazların hangi amaçlarla kullanıldığı incelendiğinde, öğrencilerin (n=200) %22,4'ünün haberleşme, %26,5'inin sosyal medyada gezinme, %24,7'sinin ders çalışma, %%22,4'ünün oyun oynama ve %3,6'sının diğer amaçlarla teknolojik cihazları kullandığı görülmüştür. Öğrencilerin (n=200) %54,5'inin teknolojik cihazları paylaşımlı kullandığı, %44,5'inin ise paylaşımlı kullanmadığı tespit edilmiştir. İnternette bir günde geçirilen süreye bakıldığında, %17 oranında 0-1

saat, %44 oranında 1-2 saat, %24 oranında 2-4 saat, %15 oranında 5 saatten fazla süre geçirildiği görülmüştür. Bilgisayarda bir günde geçirilen süreye bakıldığında, %55 oranında 0-1 saat, %22 oranında 1-2 saat, %11,5 oranında 2-4 saat, %8,5 oranında 5 saatten fazla süre geçirildiği tespit edilmiştir. Bilgisayarda bir haftada toplam geçirilen süreye bakıldığında, %23 oranında 0-1 saat, %12,5 oranında 1-2 saat, %22,5 oranında 2-4 saat, %21 oranında 5-10 saat, %19 oranında 10 saatten fazla süre geçirildiği görülmüştür. Öğrencilerin (n=200) %92'si en az bir sosyal ağa üye olduklarını, %8'i ise hiçbir sosyal ağa üye olmadığını ifade etmiştir. Öğrencilerin (n=200) üye oldukları sosyal ağlar ise %25,8'i Facebook, %9,8'i Twitter, %38,2'si Instagram, %19,6'sı Snapchat, %6,6'sı diğer sosyal ağlar şeklinde dağılmaktadır. E-posta hesabının olup olmadığı sorusuna ise %89 evet, %11 hayır cevabının verildiği görülmüştür.

Tablo 4.2 Öğrencilerin Demografik Bilgi Analizi Tablosu 2

		frekans	yüzde
Teknolojik cihazların hangi amaçlarla kullanıldığı	**Haberleşmek**	125	22,4
	Sosyal medyada gezinmek	150	26,9
	Ders çalışmak	138	24,7
	Oyun oynamak	125	22,4
	Diğer	20	3,6
	Toplam	558	100
Teknolojik cihazların paylaşımlı kullanımı	**Evet**	109	54,5
	Hayır	89	44,5
	Toplam	198	99
İnternette günde ne kadar süre geçirildiği	**0-1 Saat**	34	17
	1-2 Saat	88	44
	2-4 Saat	48	24
	5 Saatten fazla	30	15
	Toplam	200	100
Bilgisayarda günde ne kadar süre geçirildiği	**0-1 Saat**	110	55
	1-2 Saat	44	22
	2-4 Saat	23	11,5
	5 Saatten fazla	17	8,5
	Toplam	194	97
Bilgisayarda haftada ne kadar süre geçirildiği	**0-1 Saat**	46	23
	1-2 Saat	25	12,5
	2-4 Saat	45	22,5
	5-10 Saat	42	21
	10 Saatten Fazla	38	19
	Toplam	196	98
Sosyal ağa üyelik durumu	**Evet**	184	92
	Hayır	16	8
	Toplam	200	100
Üye olunan sosyal ağlar	**Facebook**	121	25,8
	Twitter	46	9,8
	Instagram	179	38,2
	Snapchat	92	19,6
	Diğer	31	6,6
	Toplam	469	100
E-posta hesabının olma durumu	**Evet**	178	89
	Hayır	22	11
	Toplam	200	100

Tablo 4.3 incelendiğinde, öğrencilerin (n=200) kullandıkları teknolojik cihazları en çok kullandıklarından en az kullandıklarına göre yaptıkları sıralamanın analizi görülmektedir. Bu analize göre en çok kullanılan teknolojik cihazın cep telefonu olduğu, en az kullanılan teknolojik cihazın ise masaüstü bilgisayar olduğu tespit edilmiştir.

Tablo 4.3 Öğrencilerin Demografik Bilgi Analizi Tablosu 3

Kullanım sıralaması (1 en çok, 4 en az)	Tablet	Laptop	Cep Telefonu	Masaüstü Bilgisayar
1	8	8	115	12
2	33	53	17	34
3	46	46	2	30
4	41	23	9	47

3.2.2 Öğretmenlerin Demografik Bilgileri

Tablo 4.4 incelendiğinde, araştırmada yer alan öğretmenlerin (n=120); %72,5'inin kadın, %27,5'inin erkek olduğu görülmektedir. Öğretmenlerin (n=120) %24,2'si 1-5 yıldır, %24,2'si 5-10 yıldır, %17,5'inin 10-15 yıldır, %10,8'inin 15-20 yıldır, %23,3'ünün 20 yıl ve üzerinde öğretmenlik mesleğini yapmaktadırlar. Kendinize ait bilgisayarınız var mı sorusuna öğretmenlerin (n=120) %94,2'si var, %5,8'i yok cevabını vermiştir. Teknolojik cihazları hangi amaçla kullandıklarına bakıldığında, %17,3 oranında haberleşme, %15,1 oranında sosyal medyada gezinme, %17,6 oranında iş ile ilgili çalışmaları yapma, %16,5 oranında e-mailleri inceleme, %13,9 oranında bankacılık işlemleri yapma, %4,7 oranında oyun oynama, %12,8 oranında e-devlet ile ilgili işlemler yapma, %2,2 oranında diğer amaçlar doğrultusunda kullanıldığı görülmüştür. Öğretmenlerin (n=120) %58,3'ünün teknolojik cihazları paylaşımlı olarak kullandığı, %41,7'sinin ise paylaşımlı kullanmadığı tespit edilmiştir. İnternette bir günde geçirilen süreye bakıldığında, %25,8 oranında 0-1 saat, %35,8 oranında 1-2 saat, %30 oranında 2-4 saat, %8,3 oranında 5 saatten fazla süre geçirildiği görülmüştür. Bilgisayarda bir günde geçirilen süreye bakıldığında, %35,8 oranında 0-1 saat, %40,8 oranında 1-2 saat, %16,7 oranında 2-4 saat, %6,7 oranında 5 saatten fazla süre geçirildiği tespit edilmiştir.

Tablo 4.4 Öğretmenlerin demografik bilgi analizi tablosu 1

		frekans	yüzde
Cinsiyet	**Kadın**	87	72,5
	Erkek	33	27,5
	Toplam	120	100
Öğretmenlik yapılan süre	**1-5 yıl**	29	24,2
	5-10 yıl	29	24,2
	10-15 yıl	21	17,5
	15-20 yıl	13	10,8
	20 yıl ve üstü	28	23,3
	Toplam	120	100
Kendisine ait bilgisayarı var mı	**Var**	113	94,2
	Yok	7	5,8
	Toplam	120	100
Teknolojik cihazların hangi amaçlarla kullanıldığı	**Haberleşmek**	111	17,3
	Sosyal medyada gezinmek	97	15,1
	İş ile ilgili çalışmaları yapmak	113	17,6
	E-mailleri incelemek	106	16,5
	Bankacılık işlemleri yapmak	89	13,9
	Oyun oynamak	30	4,7
	E-devlet ile ilgili işlemler yapmak	82	12,8
	Diğer	14	2,2
	Toplam	642	100
Teknolojik cihazların paylaşımlı kullanımı	**Evet**	70	58,3
	Hayır	50	41,7
	Toplam	120	100
İnternette günde ne kadar süre geçirildiği	**0-1 Saat**	31	25,8
	1-2 Saat	43	35,8
	2-4 Saat	36	30
	5 Saatten fazla	10	8,3
	Toplam	120	100
Bilgisayarda günde ne kadar süre geçirildiği	**0-1 Saat**	43	35,8
	1-2 Saat	49	40,8
	2-4 Saat	20	16,7
	5 Saatten fazla	8	6,7
	Toplam	120	100

Bilgisayarda bir haftada toplam geçirilen süreye bakıldığında, %5 oranında 0-1 saat, %12,5 oranında 1-2 saat, %21,7 oranında 2-4 saat, %37,5 oranında 5-10 saat, %23,3 oranında 10 saatten fazla süre geçirildiği görülmüştür. Sosyal medya ve internetin zararlı yönleri ile ilgili gündemi takip etme sorusuna %82,5 oranında evet, %16,7 oranında hayır cevabı, sosyal medya ve internetin zararlı yönleri ile ilgili öğrencileri bilgilendirme sorusuna ise %94,2 oranında evet, %5,8 oranında hayır cevabı verilmiştir. Sosyal medya veya internet aracılığıyla dolandırılma durumunun sorulduğu soruya öğretmenlerin (n=120) %10,8'i evet, %89,2'si hayır, sosyal medya veya e-posta hesabının başkaları tarafından ele geçirilme durumunun sorulduğu soruya da %10,8'i evet, %89,2'si hayır yanıtını vermiştir. Öğretmenlerin (n=120) %90,8'si

en az bir sosyal ağa üye olduklarını, %9,2'si ise hiçbir sosyal ağa üye olmadığını ifade etmiştir. Öğretmenlerin (n=120) üye oldukları sosyal ağlar ise %36'sı Facebook, %21,6'sı Twitter, %34'ü Instagram, %2,8'i Snapchat, %5,6'sı diğer sosyal ağlar şeklinde dağılmaktadır. E-posta hesabının olup olmadığı sorusuna ise %100 oranında evet cevabının verildiği görülmüştür (Tablo 4.5).

Tablo 4.5 Öğretmenlerin Demografik Bilgi Analizi Tablosu 2

		frekans	**yüzde**
Bilgisayarda haftada ne kadar süre geçirildiği	**0-1 Saat**	6	5
	1-2 Saat	15	12,5
	2-4 Saat	26	21,7
	5-10 Saat	45	37,5
	10 Saatten Fazla	28	23,3
	Toplam	100	100
Sosyal medya ve internetin zararlı yönleri ile ilgili gündemi takip etme	**Evet**	99	82,5
	Hayır	20	16,7
	Toplam	119	99,2
Sosyal medya ve internetin zararlı yönleri ile ilgili öğrencileri bilgilendirme	**Evet**	113	94,2
	Hayır	7	5,8
	Toplam	120	120
Sosyal medya veya internet aracılığıyla dolandırılma durumu	**Evet**	13	10,8
	Hayır	107	89,2
	Toplam	120	100
Sosyal medya veya e-posta hesabının başkaları tarafından ele geçirilme durumu	**Evet**	13	10,8
	Hayır	107	89,2
	Toplam	120	100
Sosyal ağa üyelik durumu	**Evet**	109	90,8
	Hayır	11	9,2
	Toplam	120	100
Üye olunan sosyal ağlar	**Facebook**	90	36
	Twitter	54	21,6
	Instagram	85	34
	Snapchat	7	2,8
	Diğer	14	5,6
	Toplam	250	100
E-posta hesabının olma durumu	**Evet**	120	100
	Hayır	0	0
	Toplam	120	100

Tablo 4.6 incelendiğinde, öğretmenlerin (n=120) kullandıkları teknolojik cihazları en çok kullandıklarından en az kullandıklarına göre yaptıkları sıralamanın analizi görülmektedir. Bu analize göre en çok kullanılan teknolojik cihazın cep telefonu olduğu, en az kullanılan teknolojik cihazın ise masaüstü bilgisayar olduğu tespit edilmiştir.

Tablo 4.6 Öğretmenlerin Demografik Bilgi Analizi Tablosu 3

Kullanım sıralaması (1 en çok, 4 en az)	Tablet	Laptop	Cep Telefonu	Masaüstü Bilgisayar
1	7	10	64	2
2	6	57	9	10
3	31	14	3	28
4	30	1	8	35

3.2.3 Okul Yöneticilerinin Demografik Bilgileri

Tablo 4.7 incelendiğinde, araştırmada yer alan okul yöneticilerinin (n=4); %50'sinin kadın, %50'sinin erkek olduğu görülmektedir. Okul yöneticilerinin (n=4) %25'i 5-10 yıldır, %25'i 10-15 yıldır, %50'sinin 20 yıl ve üzerinde öğretmenlik mesleğini yapmaktadırlar. Kendinize ait bilgisayarınız var mı sorusuna okul yöneticilerinin (n=4) %100'ü var cevabını vermiştir. Teknolojik cihazları hangi amaçla kullandıklarına bakıldığında, %19 oranında haberleşme, %9,5 oranında sosyal medyada gezinme, %19 oranında iş ile ilgili çalışmaları yapma, %19 oranında e-mailleri inceleme, %14,3 oranında bankacılık işlemleri yapma, %4,8 oranında oyun oynama, %14,3 oranında e-devlet ile ilgili işlemler yapma amaçları doğrultusunda kullanıldığı görülmüştür. Okul yöneticilerinin (n=4) %25'inin teknolojik cihazları paylaşımlı olarak kullandığı, %75'inin ise paylaşımlı kullanmadığı tespit edilmiştir. İnternette bir günde geçirilen süreye bakıldığında, %50 oranında 1-2 saat, %50 oranında 2-4 saat süre geçirildiği görülmüştür. Bilgisayarda bir günde geçirilen süreye bakıldığında, %25 oranında 0-1 saat, %25 oranında 1-2 saat, %50 oranında 5 saatten fazla süre geçirildiği tespit edilmiştir.

Tablo 4.7 Okul Yöneticilerinin Demografik Bilgi Analizi Tablosu 1

		frekans	yüzde
Cinsiyet	**Kadın**	2	50
	Erkek	2	50
	Toplam	4	100
Öğretmenlik yapılan süre	**1-5 yıl**	0	0
	5-10 yıl	1	25
	10-15 yıl	1	25
	15-20 yıl	0	0
	20 yıl ve üstü	2	50
	Toplam	4	100
Kendisine ait bilgisayarı var mı	**Var**	4	100
	Yok	0	0
	Toplam	4	100
Teknolojik cihazların hangi amaçlarla kullanıldığı	**Haberleşmek**	4	19
	Sosyal medyada gezinmek	2	9,5
	İş ile ilgili çalışmaları yapmak	4	19
	E-mailleri incelemek	4	19
	Bankacılık işlemleri yapmak	3	14,3
	Oyun oynamak	1	4,8
	E-devlet ile ilgili işlemleri yapmak	3	14,3
	Diğer	0	0
	Toplam	21	100
Teknolojik cihazların paylaşımlı kullanımı	**Evet**	1	25
	Hayır	3	75
	Toplam	4	100
İnternette günde ne kadar süre geçirildiği	**0-1 Saat**	0	0
	1-2 Saat	2	50
	2-4 Saat	2	50
	5 Saatten fazla	0	0
	Toplam	4	100
Bilgisayarda günde ne kadar süre geçirildiği	**0-1 Saat**	1	25
	1-2 Saat	1	25
	2-4 Saat	0	0
	5 Saatten fazla	2	50
	Toplam	4	100

Bilgisayarda bir haftada toplam geçirilen süreye bakıldığında, %25 oranında 0-1 saat, %50 oranında 5-10 saat, %25 oranında 10 saatten fazla süre geçirildiği görülmüştür. Sosyal medya ve internetin zararlı yönleri ile ilgili gündemi takip etme sorusuna %100 oranında evet cevabı, sosyal medya ve internetin zararlı yönleri ile ilgili öğrencileri bilgilendirme sorusuna da %100 oranında evet cevabı verilmiştir. Sosyal medya veya internet aracılığıyla dolandırılma durumunun sorulduğu soruya okul yöneticilerinin (n=4) %25'i evet, %75'i hayır, sosyal medya veya e-posta hesabının başkaları tarafından ele geçirilme durumunun sorulduğu soruya da %25'i evet, %75'i hayır yanıtını vermiştir. Okul yöneticilerinin (n=4) %75'i en az bir sosyal ağa üye olduklarını, %25'i ise hiçbir sosyal ağa üye olmadığını ifade etmiştir. Okul yöneticilerinin (n=4) üye oldukları sosyal ağlar ise %20'si Facebook, %30'u Twitter,

%30'u Instagram, %10'u Snapchat, %10'u diğer sosyal ağlar şeklinde dağılmaktadır. E-posta hesabının olup olmadığı sorusuna ise %100 oranında evet cevabının verildiği görülmüştür (Tablo 4.8).

Tablo 4.8 Okul Yöneticilerinin Demografik Bilgi Analizi Tablosu 2

		frekans	yüzde
Bilgisayarda haftada ne kadar süre geçirildiği	**0-1 Saat**	1	25
	1-2 Saat	0	0
	2-4 Saat	0	0
	5-10 Saat	2	50
	10 Saatten Fazla	1	25
	Toplam	4	100
Sosyal medya ve internetin zararlı yönleri ile ilgili gündemi takip etme	**Evet**	4	100
	Hayır	0	0
	Toplam	4	100
Sosyal medya ve internetin zararlı yönleri ile ilgili öğrencileri bilgilendirme	**Evet**	4	100
	Hayır	0	0
	Toplam	4	100
Sosyal medya veya internet aracılığıyla dolandırılma durumu	**Evet**	1	25
	Hayır	3	75
	Toplam	4	100
Sosyal medya veya e-posta hesabının başkaları tarafından ele geçirilme durumu	**Evet**	1	25
	Hayır	3	75
	Toplam	4	100
Sosyal ağa üyelik durumu	**Evet**	3	75
	Hayır	1	25
	Toplam	4	100
Üye olunan sosyal ağlar	**Facebook**	2	20
	Twitter	3	30
	Instagram	3	30
	Snapchat	1	10
	Diğer	1	10
	Toplam	10	100
E-posta hesabının olma durumu	**Evet**	4	100
	Hayır	0	0
	Toplam	4	100

Tablo 4.9 incelendiğinde, okul yöneticilerinin (n=4) kullandıkları teknolojik cihazları en çok kullandıklarından en az kullandıklarına göre yaptıkları sıralamanın analizi görülmektedir. Bu analize göre en çok kullanılan teknolojik cihazın cep telefonu olduğu, en az kullanılan teknolojik cihazın ise laptop olduğu tespit edilmiştir.

Tablo 4.9 Okul Yöneticilerinin Demografik Bilgi Analizi Tablosu 3

Kullanım sıralaması (1 en çok, 4 en az)	Tablet	Laptop	Cep Telefonu	Masaüstü Bilgisayar
1	0	0	2	0
2	0	1	0	1
3	0	1	0	0
4	0	0	0	0

3.3 Veri Toplama Araçları

Yapılan araştırmada kullanılan veri toplama araçları; öğrencilere yönelik demografik bilgi anketi, öğrencilere yönelik bilgi güvenliği farkındalık ölçeği, öğretmenlere yönelik demografik bilgi anketi, öğretmenlere yönelik bilgi güvenliği farkındalık ölçeği ve öğrencilere, velilere ve öğretmenlere yönelik görüşme sorularıdır.

3.3.1 Nicel Veri Toplama Araçları

3.3.1.1 Öğrencilere Yönelik Demografik Bilgi Anketi

Araştırma kapsamında öğrencilere uygulanan demografik bilgi anketi, araştırmacı tarafından hazırlanmıştır. Hazırlanan ankette; cinsiyet, sınıf düzeyi, kardeş sayısı, kiminle yaşanıldığı, kişinin kendisine ait bilgisayarı olup olmadığı, bilgisayar var ise evdeki konumu, velinin internet ve bilgisayar kullanımına yönelik kısıtlamaları, bilgisayar kullanımında yardım alınan kaynaklar, en çok kullanılan teknolojik cihazlar, teknolojik cihazların hangi amaçlarla kullanıldığı, kullanılan teknolojik cihazların paylaşımlı olarak kullanılıp kullanılmadığı, internette günde ne kadar vakit harcandığı, bilgisayarda günde ve haftada toplam kaç saat vakit harcandığı, herhangi bir sosyal ağa üye olunup olunmadığı, sosyal ağa üyelik durumu var ise hangi sosyal ağlara üye olunduğu ve e-posta hesabının olup olmadığı ile ilgili sorular bulunmaktadır (Ek 1).

3.3.1.2 Öğrencilere Yönelik Bilgi Güvenliği Farkındalık Ölçeği

Araştırma kapsamında belirlenen öğrencilere Güldüren vd. (2016) tarafından öğrencilere yönelik olarak geliştirilen "Bilgi Güvenliği Farkındalık Ölçeği" uygulanmıştır. Uygulanan ölçekte 5'li Likert tipi derecelendirme ölçeği kullanılmıştır ve ölçek maddelerinin seçenekleri "Kesinlikle Katılmıyorum (1)", "Katılmıyorum (2)", "Kısmen Katılmıyorum (3)", "Katılıyorum (4)" ve "Kesinlikle Katılıyorum (5)" şeklindedir. Ölçekte ters madde yer almamaktadır ve en yüksek puan 180, en düşük puan 36'dır. Ölçeğin geçerlilik ve güvenlik analizi Güldüren vd. (2016) tarafından

yapılmış olup yapı geçerliliği çalışmalarında ölçekte yer alan 36 madde 3 faktör altında toplanmış ve açıklayabildiği toplam varyans %47,34 olarak hesaplanmıştır. İlk faktör 'saldırı ve tehditler' olarak isimlendirilmiş ve açıklayabildiği toplam varyans %35,20'dir. İkinci faktör 'mahremiyet' olarak isimlendirilmiş ve açıklayabildiği toplam varyans %7,78'dir. Üçüncü faktör 'kişisel verilerin korunması' olarak isimlendirilmiş ve açıklayabildiği toplam varyans %4,40'dır. Madde analizlerinde, madde toplam puanları arasında güçlü bir korelasyonel ilişki belirlenmiştir. Ölçeğin tamamına ait Cronbach Alfa iç tutarlılık katsayısı 0,955, alt faktörlere ilişkin değerler saldırı ve tehditler alt faktörü için 0,954, mahremiyet alt faktörü için 0,890 ve kişisel verilerin korunması alt faktörü için 0,808 olarak hesaplanmıştır. Madde toplam korelasyonları ve iç tutarlılık katsayıları dikkate alındığında geliştirilen ölçeğin güvenilir olduğu değerlendirilmiştir (Güldüren vd., 2016).

3.3.1.3 Öğretmenlere Yönelik Demografik Bilgi Anketi

Araştırma kapsamında öğretmenlere uygulanan demografik bilgi anketi, araştırmacı tarafından hazırlanmıştır. Hazırlanan ankette; cinsiyet, kaç yıldır öğretmenlik mesleğinin yapıldığı, kişinin kendisine ait bilgisayarı olup olmadığı, en çok kullanılan teknolojik cihazlar, teknolojik cihazların hangi amaçlarla kullanıldığı, kullanılan teknolojik cihazların paylaşımlı olarak kullanılıp kullanılmadığı, internette günde ne kadar vakit harcandığı, bilgisayarda günde ve haftada toplam kaç saat vakit harcandığı, sosyal medya kullanımının ve internetin zararlı yönleri konusunda gündemin takip edilip edilmediği ve bu doğrultuda öğrencilerin bilgilendirilip bilgilendirilmediği, kişinin sosyal medya veya internet aracılığıyla dolandırılma durumunun olup olmadığı, kişinin sosyal medya veya e-posta hesaplarının başkaları tarafından hiç ele geçirilip geçirilmediği, herhangi bir sosyal ağa üye olunup olunmadığı, sosyal ağa üyelik durumu var ise hangi sosyal ağlara üye olunduğu ve e-posta hesabının olup olmadığı ile ilgili sorular bulunmaktadır (Ek 2).

3.3.1.4 Öğretmenlere Yönelik Bilgi Güvenliği Farkındalık Ölçeği

Araştırma kapsamında belirlenen okullarda görev yapan öğretmenler ve okul yöneticilerine de gönüllük esasına dayalı olarak, Çetinkaya vd. (2017) tarafından öğretmenlere yönelik olarak geliştirilen "Bilgi Güvenliği Farkındalık Ölçeği" uygulanmıştır. Uygulanan ölçekte 5'li Likert tipi derecelendirme ölçeği kullanılmıştır ve ölçek maddelerinin seçenekleri "Kesinlikle Katılmıyorum (1)", "Katılmıyorum

(2)", "Kısmen Katılıyorum (3)", "Katılıyorum (4)" ve "Kesinlikle Katılıyorum (5)" şeklindedir. Ölçekte ters madde yer almamaktadır ve en yüksek puan 240, en düşük puan 48'dir. Ölçeğin geçerlilik ve güvenilirlik analizi Çetinkaya vd. (2017) tarafından yapılmış olup, yapı geçerliliği çalışmalarında ölçekte yer alan 48 madde üç faktör altında toplanmış ve açıklayabildiği toplam varyans %61,74 olarak hesaplanmıştır. İlk faktör 'mobil cihazlar, mahremiyet ve iletişim' olarak isimlendirilmiş ve açıklayabildiği toplam varyans %50,05'dir. İkinci faktör 'saldırı ve tehditler' olarak isimlendirilmiş ve açıklayabildiği toplam varyans %6,49'dur. Üçüncü faktör 'genel güvenlik' olarak isimlendirilmiş ve açıklayabildiği toplam varyans %5,20'dir. Madde analizlerinde, madde toplam puanları arasında güçlü bir korelasyonel ilişki belirlenmiştir. Ölçeğin tamamına ait Cronbach Alfa iç tutarlılık katsayısı 0,980, alt faktörlere ilişkin değerler mobil cihazlar, mahremiyet ve iletişim alt faktörü için 0,967, saldırı ve tehditler alt faktörü için 0,969 ve genel güvenlik alt faktörü için 0,926 olarak hesaplanmıştır. Madde toplam korelâsyonları ve iç tutarlılık katsayıları dikkate alındığında geliştirilen ölçeğin güvenilir olduğu değerlendirilmiştir (Çetinkaya vd., 2017).

3.3.2 Nitel Veri Toplama Araçları

Araştırmada, nitel veri toplama aracı olarak öğrencilere, öğretmenlere ve velilere yönelik yarı yapılandırılmış görüşme soruları kullanılmıştır.

Yapılan araştırmada, çalışma grubuna yönelik görüşme soruları hazırlanırken ilk olarak, araştırmanın problemi ve alt problemleri analiz edilmiş ve konu ile ilgili alanyazın taraması yapılmıştır. Bu doğrultuda hangi türde verilere gereksinim olduğu değerlendirilmiştir. Yapılan değerlendirme sonucunda görüşme soruları, soruların yöneltildiği katılımcının anlayabileceği bir şekilde yalın bir anlatımla yazılmış ve bir soru havuzu oluşturulmuştur. Yazılan sorular içerisinden yapılan çalışma için en uygun olanları seçilmiştir. Seçilen sorular, araştırmanın evreninde yer alan öğrenci, veli, öğretmen ve okul yöneticisine uygulanmış, bir deneme çalışması yapılmıştır. Yapılan çalışma neticesinde soruların anlaşılabilir olduğu görülmüştür (Ek 3, Ek 4, Ek 5).

3.4 Verilerin Toplanması

Araştırma kapsamında elde edilen veriler, çalışmada yer alan katılımcıların onayı ile toplanmıştır (Ek 6).

Araştırmada uygulanan nicel yöntem doğrultusunda okullarda veri toplama araçları uygulanmıştır. Öğrencilere anket ve ölçek uygulaması yapılırken, araştırmacının kendisinin yanı sıra dersin öğretmeni de sınıfta yer almıştır. Uygulama esnasında öğrencilerin soruları yanıtlaması için sessiz bir ortam sağlanmış olup, süre konusunda esnek davranılmıştır. Böylece öğrencilerin, soruları, acele etmeden, anlayarak ve sağlıklı bir şekilde yanıtlamaları sağlanmıştır. Benzer şekilde öğretmen ve okul öneticilerine anket ve ölçek uygulaması yapılırken, zaman kısıtlaması olmamasına dikkat edilmiş, söz konusu katılımcının boş dersi olması, veli görüşmesinin olmaması vb. etmenler göz önünde bulundurulmuştur.

Araştırmada uygulanan nitel yöntem doğrultusunda öğrenci, veli, öğretmen ve okul yöneticileri ile yarı yapılandırılmış görüşme soruları uygulanmıştır. Yapılan görüşmeler boş sınıf, kütüphane, müdür odası vb. bir ortamda, katılımcı ve araştırmacı yalnızken gerçekleştirilmiş olup, verilerin gizliliği ön planda tutulmuştur.

Yapılan çalışmada elde edilen tüm veriler, bizzat araştırmacı tarafından toplanmıştır. Çalışma grubunda yer alan tüm katılımcılara uygulanan anket ve ölçekler, araştırmacının gözetiminde gerçekleşmiştir. Anket ve ölçeklere dair tüm açıklamalar araştırmacı tarafından yapılmış, sorulan tüm sorulara araştırmacı yanıt vermiştir. Böylelikle başka bir kişinin yanlış bir yönlendirmesinin önüne geçilmiş, sorulara müdahale etmediğinden emin olunmuştur. Bununla birlikte katılımcıların hepsinin yönergeleri doğru bir şekilde anlaması sağlanmış ve tek bir kişinin yönlendirmesi ile verilerin güvenirliği elde edilmiştir. Nitel verilerin toplanmasında da benzer şekilde araştırmacının kendisi katılımcılarla birebir görüşme gerçekleştirmiş ve yapılan görüşmeler kayıt altına alınmıştır. Görüşmeler esnasında katılımcıların samimiyetle cevap vermelerinin sağlanması için, görüşme öncesi bir konuşma yapılmış ve güven ortamının oluşması sağlanmıştır. Nitekim görüşme yapılıp ses kaydı alınsa dahi, istemedikleri takdirde görüşme kaydının silinebileceği, istemedikleri bilgilerin kullanılmayacağı ve istedikleri anda araştırmadan çıkabilecekleri katılımcılara ifade edilmiştir.

3.5 Verilerin Analizi

Çalışma grubuna uygulanan anketten elde edilen verilerin analizinde aritmetik ortalama, yüzde, standart sapma ve frekans kullanılmıştır.

Bilgi güvenliği farkındalığı ölçeğinde likert tipi derecelendirme vardır ve ölçekte ters madde yer almamaktadır. Ölçek toplam puanı ve alt faktörlere ilişkin puanlar attıkça, katılımcıların bilgi güvenliği farkındalığı artmaktadır. Yapılan analizlerde ölçek puanlarının normal dağılım gösterdiği görülmüştür. Bu doğrultuda, devlet okulu ve özel okuldaki öğrenciler ve öğretmenlerin ölçek puanları ve arasında farklılık olup olmadığı incelenmesi için bağımsız örneklem t testi (independent sample t test) ve tek yönlü varyans analizi (ANOVA) uygulanmıştır. Araştırmadan elde edilen veriler SPSS 24.0 programıyla analiz edilmiş olup, istatistiksel olarak anlamlılık düzeyi $p<0,05$ kabul edilmiştir.

Nitel araştırma yöntemi doğrultusunda yapılan görüşmeler ses kaydı ve form yardımı ile kaydedilmiştir. Kaydedilen görüşmeler yazıya dökülmüştür. Görüşmeler betimsel analiz yöntemi ile analiz edilmiştir.

BÖLÜM IV

BULGULAR

Bu bölümde yapılan araştırmada elde edilen verilerin analizi gerçekleştirilmiştir.

4.1 Öğrencilerin Bilgi Güvenliği Farkındalık Düzeyleri ve Bu Konuya İlişkin Görüşleri

Araştırma kapsamında yer alan 200 öğrenciye demografik bilgi anketi ve bilgi güvenliği farkındalık ölçeği uygulanmış, 12 öğrenci ile de yüz yüze görüşme yapılmıştır. Elde edilen verilerden ulaşılan bulgular aşağıda yer alan başlıklarda altında açıklanmıştır.

4.1.1 Öğrencilerin Bilgi Güvenliği Farkındalık Düzeyleri

Araştırmada yer alan öğrencilerin (n=200) Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) puan ortalamaları değerlendirildiğinde, kişisel verilerin korunması alt boyutu ortalamasının 23,02±5,53, saldırı ve tehditler alt boyutu ortalamasının 52,97±19,40, mahremiyet alt boyutu ortalamasının 39,17±10,37, BGFÖ genel puan ortalamasının 115,15±30,48 olduğu görülmektedir (Tablo 4.10).

Tablo 4.10 Öğrencilerin BGFÖ Puanlarına İlişkin Betimsel İstatistikler

Alt Boyutlar	n	$\overline{X}$	ss	Max	Min
Kişisel Verilerin Korunması	200	23,02	5,56	30	6
Saldırı ve Tehditler	200	52,97	19,40	95	19
Mahremiyet	200	39,17	10,37	55	11
BGFÖ genel puan	200	115,15	30,48	180	36

4.1.1.1 Öğrencilerin Bilgi Güvenliği Farkındalık Düzeylerinin Cinsiyete Göre Değerlendirilmesi

Araştırmada yer alan öğrencilerin (n=200) cinsiyete göre BGFÖ puan ortalamaları değerlendirildiğinde, saldırı ve tehditler alt boyutunda kadın ve erkek öğrenciler arasında istatistiksel olarak anlamlı fark olduğu tespit edilmiştir ($p<0,05$). Elde edilen verilere göre erkek öğrencilerin farkındalık düzeylerinin daha yüksek olduğu görülmektedir. Kişisel verilerin korunması alt boyutu, mahremiyet alt boyutu ile ölçek genel puan ortalamalarında kadın ve erkek öğrenciler arasında istatistiksel olarak anlamlı fark olmadığı görülmüştür ($p>0,05$) (Tablo 4.11).

Tablo 4.11 Öğrencilerin Cinsiyete Göre BGFÖ Bağımsız Örneklem T Testi Sonuçları

Alt Boyutlar	Cinsiyet	n	$\overline{X}$	ss	df	t	p
Kişisel Verilerin Korunması	Kadın	72	23,76	4,78	173,482	1,525	0,129
	Erkek	128	22,59	5,89			
Saldırı ve Tehditler	Kadın	72	47,07	17,67	198	-3,306	**0,001***
	Erkek	128	56,29	19,60			
Mahremiyet	Kadın	72	39,21	10,13	198	0,044	0,965
	Erkek	128	39,14	10,55			
BGFÖ genel puan	Kadın	72	110,04	27,81	198	-1,788	0,075
	Erkek	128	118,02	31,62			

*p<0.05 (Anlamlılık düzeyi)

4.1.1.2 Öğrencilerin Bilgi Güvenliği Farkındalık Düzeylerinin Okul Düzeyine (Ortaokul-Lise) Göre Değerlendirilmesi

Araştırmada yer alan öğrencilerin (n=200) okul düzeyine göre BGFÖ puan ortalamaları değerlendirildiğinde, kişisel verilerin korunması alt boyutunda ortaokul ve lisede öğrenim gören öğrenciler arasında istatistiksel olarak anlamlı fark olduğu tespit edilmiştir (p<0,05). Elde edilen verilere göre ortaokulda öğrenim gören öğrencilerin farkındalık düzeylerinin daha yüksek olduğu görülmektedir. Saldırı ve tehditler alt boyutu, mahremiyet alt boyutu ile ölçek genel puan ortalamalarında ise ortaokul ve lisede öğrenim gören öğrenciler arasında istatistiksel olarak anlamlı fark olmadığı görülmüştür (p>0,05) (Tablo 4.12).

Tablo 4.12 Öğrencilerin Okul Düzeyine Göre BGFÖ Bağımsız Örneklem T Testi Sonuçları

Alt Boyutlar	Okul düzeyi	n	$\overline{X}$	ss	df	t	p
Kişisel Verilerin Korunması	Ortaokul	100	24,29	4,46	179,783	3,340	**0,001***
	Lise	100	21,74	6,20			
Saldırı ve Tehditler	Ortaokul	100	51,98	17,21	189,275	-0,721	0,472
	Lise	100	53,96	21,40			
Mahremiyet	Ortaokul	100	40,47	8,21	174,567	1,789	0,075
	Lise	100	37,86	12,06			
BGFÖ genel puan	Ortaokul	100	116,74	26,34	185,959	0,737	0,462
	Lise	100	113,56	34,17			

*p<0.05 (Anlamlılık düzeyi)

Araştırmada yer alan ve özel okulda öğrenim gören öğrencilerin (n=100) okul düzeyine göre BGFÖ puan ortalamaları değerlendirildiğinde, ölçek alt boyutları ile ölçek genel puan ortalamalarında ortaokul ve lisede öğrenim gören öğrenciler arasında istatistiksel olarak anlamlı fark olmadığı görülmüştür (p>0,05) (Tablo 4.13).

Tablo 4.13 Özel Okulda Öğrenim Gören Öğrencilerin Okul Düzeyine Göre BGFÖ Bağımsız Örneklem T Testi Sonuçları

Alt Boyutlar	Okul düzeyi	n	$\overline{X}$	ss	df	t	p
Kişisel Verilerin Korunması	Ortaokul	50	24,70	3,39	83,918	1,541	0,127
	Lise	50	23,38	5,24			
Saldırı ve Tehditler	Ortaokul	50	51,88	16,07	90,868	-0,401	0,689
	Lise	50	53,40	21,43			
Mahremiyet	Ortaokul	50	40,78	8,14	88,015	-0,370	0,712
	Lise	50	41,52	11,56			
BGFÖ genel puan	Ortaokul	50	117,40	24,01	89,908	-0,157	0,876
	Lise	50	118,30	32,72			

*p<0.05 (Anlamlılık düzeyi)

Araştırmada yer alan ve devlet okulunda öğrenim gören öğrencilerin (n=100) okul düzeyine göre BGFÖ puan ortalamaları değerlendirildiğinde, kişisel verilerin korunması ve mahremiyet alt boyutunda ortaokul ve lisede öğrenim gören öğrenciler arasında istatistiksel olarak anlamlı fark olduğu tespit edilmiştir (p<0,05). Elde edilen verilere göre ortaokulda öğrenim gören öğrencilerin farkındalık düzeylerinin daha yüksek olduğu görülmektedir. Saldırı ve tehditler alt boyutu ile ölçek genel puan ortalamalarında ortaokul ve lisede öğrenim gören öğrenciler arasında istatistiksel olarak anlamlı fark olmadığı görülmüştür (p>0,05) (Tablo 4.14).

Tablo 4.14 Devlet Okulunda Öğrenim Gören Öğrencilerin Okul Düzeyine Göre BGFÖ Bağımsız Örneklem T Testi Sonuçları

Alt Boyutlar	Okul düzeyi	n	$\overline{X}$	ss	df	t	p
Kişisel Verilerin Korunması	Ortaokul	50	23,84	5,31	93,253	3,098	**0,003***
	Lise	50	20,10	6,68			
Saldırı ve Tehditler	Ortaokul	50	52,08	18,44	98	-0,608	0,545
	Lise	50	54,52	21,58			
Mahremiyet	Ortaokul	50	40,16	8,35	89,341	2,962	**0,004***
	Lise	50	34,20	11,52			
BGFÖ genel puan	Ortaokul	50	116,08	28,72	98	1,129	0,262
	Lise	50	108,82	35,26			

*p<0.05 (Anlamlılık düzeyi)

4.1.1.3 Öğrencilerin Bilgi Güvenliği Farkındalık Düzeylerinin Okul Türüne Göre Değerlendirilmesi

Araştırmada yer alan öğrencilerin (n=200) okul türüne göre BGFÖ puan ortalamaları değerlendirildiğinde, kişisel verilerin korunması alt boyutu ve mahremiyet alt boyutunda özel okul ve devlet okulunda öğrenim gören öğrenciler arasında istatistiksel olarak anlamlı fark olduğu tespit edilmiştir (p<0,05). Elde edilen verilere göre özel okulda öğrenim gören öğrencilerin farkındalık düzeylerinin daha yüksek olduğu görülmektedir. Saldırı ve tehditler alt boyutu ile ölçek genel puan ortalamalarında ise özel okul ve devlet okulunda öğrenim gören öğrenciler arasında istatistiksel olarak anlamlı fark olmadığı görülmüştür (p>0,05) (Tablo 4.15).

Tablo 4.15 Öğrencilerin Okul Türüne Göre BGFÖ Bağımsız Örneklem T Testi Sonuçları

Alt Boyutlar	Okul Türü	n	$\overline{X}$	ss	df	t	p
Kişisel Verilerin Korunması	Özel Okul	100	24,06	4,45	178,083	2,713	**0,007***
	Devlet Okulu	100	21,97	6,29			
Saldırı ve Tehditler	Özel Okul	100	52,64	18,86	198	-0,240	0,811
	Devlet Okulu	100	53,30	20,01			
Mahremiyet	Özel Okul	100	41,15	9,96	198	2,751	**0,006***
	Devlet Okulu	100	37,18	10,45			
BGFÖ genel puan	Özel Okul	100	117,85	28,56	198	1,255	0,211
	Devlet Okulu	100	112,45	32,20			

*p<0.05 (Anlamlılık düzeyi)

Araştırmada yer alan ve ortaokulda öğrenim gören öğrencilerin (n=100) okul türüne göre BGFÖ puan ortalamaları değerlendirildiğinde, kişisel verilerin korunması alt boyutu, mahremiyet alt boyutu, saldırı ve tehditler alt boyutu ve ölçek genel puan ortalamalarında özel okul ve devlet okulunda öğrenim gören öğrenciler arasında istatistiksel olarak anlamlı fark olmadığı görülmüştür (p>0,05) (Tablo 4.16).

Tablo 4.16 Ortaokulda Öğrenim Gören Öğrencilerin Okul Türüne Göre BGFÖ Bağımsız Örneklem T Testi Sonuçları

Alt Boyutlar	Okul Türü	n	$\overline{X}$	ss	df	t	p
Kişisel Verilerin Korunması	Özel Okul	50	24,74	3,39	83,255	1,010	0,316
	Devlet Okulu	50	23,84	5,31			
Saldırı ve Tehditler	Özel Okul	50	51,88	16,07	98	-0,058	0,954
	Devlet Okulu	50	52,08	18,44			
Mahremiyet	Özel Okul	50	40,78	8,14	98	0,376	0,708
	Devlet Okulu	50	40,16	8,35			
BGFÖ genel puan	Özel Okul	50	117,40	24,01	98	0,249	0,804
	Devlet Okulu	50	116,08	28,72			

*p<0.05 (Anlamlılık düzeyi)

Araştırmada yer alan ve lisede öğrenim gören öğrencilerin (n=100) okul türüne göre BGFÖ puan ortalamaları değerlendirildiğinde, kişisel verilerin korunması alt boyutu ve mahremiyet alt boyutunda özel okul ve devlet okulunda öğrenim gören öğrenciler arasında istatistiksel olarak anlamlı fark olduğu tespit edilmiştir (p<0,05). Elde edilen verilere göre özel okulda öğrenim gören öğrencilerin farkındalık düzeylerinin daha yüksek olduğu görülmektedir. Saldırı ve tehditler ile ölçek genel puan ortalamalarında ise özel okul ve devlet okulunda öğrenim gören öğrenciler arasında istatistiksel olarak anlamlı fark olmadığı görülmüştür (p>0,05) (Tablo 4.17).

Tablo 4.17 Lisede Öğrenim Gören Öğrencilerin Okul Türüne Göre BGFÖ Bağımsız Örneklem T Testi Sonuçları

Alt Boyutlar	Okul Türü	n	$\overline{X}$	ss	df	t	p
Kişisel Verilerin Korunması	Özel Okul	50	23,38	5,24	98	2,731	**0,007***
	Devlet Okulu	50	20,10	6,68			
Saldırı ve Tehditler	Özel Okul	50	53,40	21,43	98	-0,260	0,795
	Devlet Okulu	50	54,52	21,58			
Mahremiyet	Özel Okul	50	41,52	11,56	98	3,172	**0,002***
	Devlet Okulu	50	34,20	11,52			
BGFÖ genel puan	Özel Okul	50	118,30	32,72	98	1,394	0,167
	Devlet Okulu	50	108,82	35,26			

*p<0.05 (Anlamlılık düzeyi)

4.1.1.4 Öğrencilerin Bilgi Güvenliği Farkındalık Düzeylerinin Bilgisayar Kulanım Süresine Göre Değerlendirilmesi

Araştırmada yer alan öğrencilerin (n=200) bilgisayarda günde kaç saat vakit geçirdiklerine göre BGFÖ puan ortalamaları değerlendirildiğinde, ölçek alt boyutları ile ölçek genel puan ortalamalarında istatistiksel olarak anlamlı fark olmadığı görülmüştür (p>0,05) (Tablo 4.18).

Tablo 4.18 Öğrencilerin Bilgisayarda Günde Kaç Saat Vakit Geçirdiklerine Göre BGFÖ ANOVA Testi Sonuçları

Alt Boyutlar	Bilgisayar Kullanım Süresi	n	$\overline{X}$	ss	df	X^2	p	Fark
Kişisel Verilerin Korunması	0-1 saat[1]	110	22,92	5,01	3	0,453	0,715	-
	1-2 saat[2]	44	23,84	5,82				
	2-4 saat[3]	23	22,35	6,34				
	5 saat ve üstü[4]	17	23,35	6,98				
Saldırı ve Tehditler	0-1 saat[1]	110	51,03	20,21		1,385	0,249	-
	1-2 saat[2]	44	54,43	17,22				
	2-4 saat[3]	23	59,22	20,84				
	5 saat ve üstü[4]	17	56,18	17,62				
Mahremiyet	0-1 saat[1]	110	38,16	10,25		1,131	0,338	-
	1-2 saat[2]	44	40,59	10,45				
	2-4 saat[3]	23	41,87	11,20				
	5 saat ve üstü[4]	17	39,06	10,54				
BGFÖ genel puan	0-1 saat[1]	110	112,10	30,22		1,199	0,311	-
	1-2 saat[2]	44	118,86	29,43				
	2-4 saat[3]	23	123,44	33,78				
	5 saat ve üstü[4]	17	118,59	32,18				

*p<0.05 (Anlamlılık düzeyi)

Araştırmada yer alan öğrencilerin (n=200) bilgisayarda haftada toplam kaç saat vakit geçirdiklerine göre BGFÖ puan ortalamaları değerlendirildiğinde, ölçek alt boyutları ile ölçek genel puan ortalamalarında istatistiksel olarak anlamlı fark olmadığı görülmüştür (p>0,05) (Tablo 4.19).

Tablo 4.19 Öğrencilerin Bilgisayarda Haftada Kaç Saat Vakit Geçirdiklerine Göre BGFÖ ANOVA Testi Sonuçları

Alt Boyutlar	Bilgisayar kullanım süresi	n	$\overline{X}$	ss	df	F	p	Fark
Kişisel Verilerin Korunması	0-1 saat[1]	46	22,48	5,60	4	0,423	0,792	-
	1-2 saat[2]	25	23,20	5,89				
	2-4 saat[3]	45	22,91	5,01				
	5-10 saat[4]	42	23,98	4,68				
	10 saat ve üstü[5]	17	23,05	6,62				
Saldırı ve Tehditler	0-1 saat[1]	46	51,67	21,02		1,546	0,191	-
	1-2 saat[2]	25	45,92	18,73				
	2-4 saat[3]	45	53,13	19,47				
	5-10 saat[4]	42	57,14	17,95				
	10 saat ve üstü[5]	17	55,58	18,64				
Mahremiyet	0-1 saat[1]	46	37,15	11,27		2,097	0,083	-
	1-2 saat[2]	25	38,32	9,33				
	2-4 saat[3]	45	38,18	10,59				
	5-10 saat[4]	42	43,05	8,77				
	10 saat ve üstü[5]	17	39,76	10,88				
BGFÖ genel puan	0-1 saat[1]	46	111,30	32,04		1,622	0,170	-
	1-2 saat[2]	25	107,44	28,91				
	2-4 saat[3]	45	114,22	29,71				
	5-10 saat[4]	42	124,17	28,56				
	10 saat ve üstü[5]	17	118,40	31,82				

*p<0.05 (Anlamlılık düzeyi)

4.1.1.5 Öğrencilerin Bilgi Güvenliği Farkındalık Düzeylerinin İnternet Kulanım Süresine Göre Değerlendirilmesi

Araştırmada yer alan öğrencilerin (n=200) internette günde kaç saat vakit geçirdiklerine göre BGFÖ puan ortalamaları değerlendirildiğinde, ölçek alt boyutları ile ölçek genel puan ortalamalarında istatistiksel olarak anlamlı fark olmadığı görülmüştür (p>0,05) (Tablo 4.20).

Tablo 4.20 Öğrencilerin İnternette Günde Kaç Saat Vakit Geçirdiklerine Göre BGFÖ ANOVA Testi Sonuçları

Alt Boyutlar	İnternet Kullanım Süresi	n	$\overline{X}$	ss	df	F	p	Fark
Kişisel Verilerin Korunması	0-1 saat[1]	34	23,91	5,18	3	1,593	0,192	-
	1-2 saat[2]	88	22,53	5,20				
	2-4 saat[3]	48	24,04	5,85				
	5 saat ve üstü[4]	30	21,77	6,16				
Saldırı ve Tehditler	0-1 saat[1]	34	52,32	18,93		0,051	0,985	-
	1-2 saat[2]	88	53,56	19,00				
	2-4 saat[3]	48	52,46	20,76				
	5 saat ve üstü[4]	30	52,80	19,75				
Mahremiyet	0-1 saat[1]	34	37,35	10,50		1,653	0,178	-
	1-2 saat[2]	88	38,97	13,36				
	2-4 saat[3]	48	41,81	10,24				
	5 saat ve üstü[4]	30	37,57	10,14				
BGFÖ genel puan	0-1 saat[1]	34	113,59	30,59		0,297	0,827	-
	1-2 saat[2]	88	115,06	29,44				
	2-4 saat[3]	48	118,31	33,02				
	5 saat ve üstü[4]	30	112,13	30,19				

*p<0.05 (Anlamlılık düzeyi)

4.1.1.6 Öğrencilerin Bilgi Güvenliği Farkındalık Düzeylerinin Sosyal Ağa Üye Olma Durumuna Göre Değerlendirilmesi

Araştırmada yer alan öğrencilerin (n=200) sosyal ağa üyelik durumlarına göre BGFÖ puan ortalamaları değerlendirildiğinde, ölçek alt boyutları ile ölçek genel puan ortalamalarında sosyal ağa üye olan ve olmayan öğrenciler arasında istatistiksel olarak anlamlı fark olmadığı görülmüştür (p>0,05) (Tablo 4.21).

Tablo 4.21 Öğrencilerin Sosyal Ağa Üyelik Durumuna Göre BGFÖ Bağımsız Örneklem T Testi Sonuçları

Alt Boyutlar	Sosyal Ağa Üyelik	n	$\overline{X}$	ss	df	t	p
Kişisel Verilerin Korunması	Evet	184	23,07	5,44	16,794	0,446	0,661
	Hayır	16	22,31	6,65			
Saldırı ve Tehditler	Evet	184	53,41	19,26	198	1,083	0,280
	Hayır	16	47,94	20,85			
Mahremiyet	Evet	184	39,23	10,42	198	0,317	0,752
	Hayır	16	38,38	10,14			
BGFÖ genel puan	Evet	184	115,72	30,17	198	0,892	0,373
	Hayır	16	108,63	34,14			

*p<0.05 (Anlamlılık düzeyi)

4.1.2 Öğrencilerin Bilgi Güvenliği Farkındalığına Yönelik Görüşleri

Çalışmaya katılan 12 öğrenci ile yarı yapılandırılmış görüşme sorularıyla yüz yüze görüşme gerçekleştirilmiştir. Görüşmede öğrencilere 15 adet soru yöneltilmiş ve öğrencilerin görüşme esnasında verdikleri cevaplar analiz edilmiştir.

Kendinize ait bilgisayar, cep telefonu veya tabletiniz var mı sorusunda; özel okulda ortaokul düzeyinde öğrenim göre öğrencilerden ÖOÖ1'in kendisine ait

bilgisayar, cep telefonu ve tableti olduğu, ÖOÖ2'nin bilgisayar ve tableti olduğu, ÖOÖ3'ün de cep telefonu ve tableti olup kendisine ait bilgisayarı olmayıp annesinin bilgisayarını kullandığı, yapılan görüşmelerde tespit edilmiştir. Devlet okulunda ortaokul düzeyinde öğrenim gören öğrencilerden DOÖ1'in cep telefonu ve tableti olup, bilgisayarının olmadığı, DOÖ2'nin bilgisayarı ve cep telefonu olduğu, DOÖ3'ün de bilgisayar, cep telefonu ve tableti olduğu sonucuna ulaşılmıştır. Özel okulda lise düzeyinde öğrenim gören öğrencilerden ÖLÖ1'in cep telefonu ve tableti olup bilgisayarı ise ortak kullandığı, ÖLÖ2'nin cep telefonu ve bilgisayarı olduğu, ÖLÖ3'ün de cep telefonu ve tableti olup bilgisayarı ortak bir şekilde kullandıkları bulgusuna varılmıştır. Devlet okulunda lise düzeyinde öğrenim gören öğrencilerden DLÖ1 ve DLÖ2'nin bilgisayar, cep telefonu ve tableti olduğu, DLÖ3'ün de bilgisayar ve cep telefonu olduğu tespit edilmiştir.

Eğer varsa evinizde yer alan bilgisayar hangi odada bulunmaktadır sorusuna; özel okulda ortaokul düzeyinde öğrenim gören ÖOÖ1 "arka odada ablamla birlikte kullanıyoruz, tableti de salonda kullanıyorum", ÖOÖ2 "genelde salonda veya kendi odamda kullanıyorum", ÖOÖ3 "tableti genellikle salonda kullanıyorum, annemin dizüstü bilgisayarını ise odamda kullanıyorum" cevaplarını vermişlerdir. Devlet okulunda ortaokul düzeyinde öğrenim gören DOÖ1'in evinde bilgisayar bulunmamakta, DOÖ2 ve DOÖ3 kendi odasında bilgisayarı kullandıklarını ifade etmişlerdir. Özel okulda ve devlet okulunda lise düzeyinde öğrenim gören öğrenciler de (ÖLÖ1, ÖLÖ2, ÖLÖ3, DLÖ1, DLÖ2 ve DLÖ3) bilgisayarlarını kendi odalarında kullandıklarını belirtmişlerdir.

Eğer varsa teknolojik cihazları (tablet, cep telefonu vb.) hangi amaçlar (haberleşme, oyun, sohbet/chat, ders çalışma vb.) doğrultusunda kullanıyorsunuz sorusuna, özel okulda ortaokul düzeyinde öğrenim gören ÖOÖ1 tableti oyun oynamak için, cep telefonunu birileri ile mesajlaşmak için, bilgisayarı da powerpoint sunusu hazırlamak ve video izlemek için ÖOÖ2 araştırma ve oyun oynamak için, ÖOÖ3 tableti oyun oynamak için, cep telefonunu arama yapmak ve müzik dinlemek için yanıtlarını vermişlerdir. Devlet okulunda ortaokul düzeyinde öğrenim gören DOÖ1 oyun oynamak ve ders çalışmak için, DOÖ2 oyun oynamak, video izlemek ve sosyal medyada gezinmek için, DOÖ3 ders çalışmak, sosyal medyada gezinmek ve film izlemek için kullandıklarını ifade etmişlerdir. Özel okulda lise düzeyinde öğrenim

gören öğrencilerden ÖLÖ1 tableti pek kullanmadığını, cep telefonunu sosyal medyaya bakmak ve haberleşmek için, diz üstü bilgisayarı da ders çalışmak için, ÖLÖ2 cep telefonunu ödev yapmak için, bilgisayarı proje ve performans ödevleri yapmak, film izlemek ve oyun oynamak için, ÖLÖ3 ise haberleşmek, ders çalışmak, sosyal medyaya bakmak ve oyun oynamak için kullandığını belirtmişlerdir. Devlet okulunda lise düzeyinde öğrenim gören DLÖ1 ödev yapmak, oyun oynamak ve bir şeyler araştırmak için, DLÖ2 ödev yapmak, oyun oynamak, internette dolaşmak ve sosyal medyada gezinmek için, DLÖ3 sohbet etmek, ders çalışmak ve oyun oynamak teknolojik cihazları kullandıklarını dile getirmişlerdir.

Eğer varsa evde bilgisayar kullanımınıza yönelik bir kısıtlama mevcut mu? Kısıtlama mevcut ise, bu konuda ne düşünüyorsunuz? Sizce, neden veliniz size böyle kısıtlamalar getiriyor sorusunda; özel okulda ortaokul düzeyinde öğrenim gören ÖOÖ1 ve ÖOÖ3 herhangi bir kısıtlama olmadığını, ÖOÖ2 ise oyun oynamak için 1 saat izni olup, araştırma yapma, ödev yapma vb. amaçlara yönelik izin verildiğini belirtmiş ve ailesinin kısıtlama yapmasını haklı bulup "bazen kendimi kaybettiğim için ailem kısıtlama getiriyor" diyerek gerekçesini açıklamıştır. Devlet okulunda ortaokul düzeyinde öğrenim gören DOÖ2 ve DOÖ3 kısıtlama yapılmadığını, DOÖ1 ise ailesinin kısıtlama yaptığını, tehdit içeren oyunları oynamasına izin verilmediğini ve zaman kısıtlaması getirdiklerini dile getirmiştir. Ailesinin bu tutumuna yönelik "haklılık payları da var haksızlık payları da var…haklı oldukları konu derslerimi iyi getirmem için haksızlıklarıysa şey boşu boşuna, zamanım varken zamanın doldu diyolar" düşüncesini ifade etmiştir. Özel okulda lisede öğrenim gören ÖLÖ1 kısıtlama olmadığını, ÖLÖ2 kısıtlama olduğunu, hafta sonları oyun oynayabildiğini, hafta içi sadece ödev için bilgisayarı kullanabildiğini, ÖLÖ3 ise günlük 2 saatlik bilgisayar kullanma hakkı olduğunu belirtmiştir. Ailelerinin tutumlarını, ÖLÖ2 "bilgisayarla zaman kaybedip derslerime yoğunlaşamayacağım için…haklılar", ÖLÖ3 ise "haklılar annem uyarmazsa bırakamıyorum, annem uyarınca bırakabiliyorum" diyerek açıklamışlardır. Devlet okulunda lise düzeyinde öğrenim gören DLÖ2 ve DLÖ3 herhangi bir kısıtlama yapılmadığını, DLÖ1 ise günde en fazla 1 saat bilgisayar başında oturabildiğini ifade etmiş ve ailesinin bu tutumunu haklı bulup kendisinin daha sosyal olmasını sağladığını dile getirmiştir.

Öğretmenleriniz güvenli bilgisayar ve İnternet kullanımı hakkında size ne gibi yönlendirmede bulunuyor sorusunda; özel okulda ortaokul düzeyinde öğrenim gören ÖOÖ1 yönlendirmede bulunulduğunu, ÖOÖ2 bilgisayar başında çok kalmamak gibi yönlendirmelerde bulunulduğunu, ÖOÖ3 süre konusunda yönlendirmelerde bulunulduğunu belirtmişlerdir. Devlet okulunda ortaokul düzeyinde öğrenim gören DOÖ1 telefonun güvenli kullanımı konusunda yönlendirmede bulunulduğunu, DOÖ2 kötü amaçlı yazılımlara girmeme, bilinmeyen yerlerden uygulama indirmeme gibi yönlendirmelerde bulunulduğunu, DOÖ3 sadece bilişim dersi kapsamında yönlendirmede bulunulduğunu ifade etmiştir. Özel okulda lise düzeyinde öğrenim gören ÖLÖ1 yönlendirmede bulunulduğunu, şifrelerle ilgili vs., seminerler düzenlendiğini, ÖLÖ2 seminerler verildiğini, ÖLÖ3 ise "bu konuda aslında pek bir şey söylemiyorlar sadece internet başında fazla vakit geçirmememizi söylüyorlar" diyerek düşüncesini belirtmiştir. Devlet okulunda lise düzeyinde öğrenim gören DLÖ1 bilgisayarları boş yere kullanmayın, oyun vb. gibi amaçlarla kullanmayın şeklinde yönlendirmelerde bulunulduğunu, DLÖ2 olumsuz şeylere girmeyin şeklinde yönlendirmelerde bulunulduğunu, DLÖ3 ise yönlendirmede bulunulmadığını dile getirmiştir.

Arkadaşlarınızdan bilgisayar kullanımı konusunda yardım alıyor musunuz? Cevabınız evet ise, arkadaşlarınız ne gibi yardımda bulunuyor sorusunda; özel okulda ortaokul düzeyinde öğrenim gören ÖOÖ1 bazen yardım istediğini, bir yeri (program) açarken nasıl açacağını sorabildiğini, ÖOÖ2 okul dışında yardım isteğinde bulunmadığını, okul içerisinde bilişim derslerinde arkadaşlarından yardım talebinde bulunduğunu, ÖOÖ3 bir iki kez oyun yükleme konusunda yardım aldığını belirtmiştir. Devlet okulunda ortaokul düzeyinde öğrenim gören DOÖ1 babasından yardım aldığını, DOÖ2 oyun indirme konusunda nadiren arkadaşlarından yardım aldığını, DOÖ3 bir program indirme gibi konularda arkadaşlarından yardım aldığını ifade etmiştir. Özel okulda lise düzeyinde öğrenim gören ÖLÖ1 ve ÖLÖ2 yardım almadıklarını, ÖLÖ3 ise Word programını kullanırken, bir uygulamayı açarken vs. yardım aldığını dile getirmiştir. Devlet okulunda lise düzeyinde öğrenim gören DLÖ1 ve DLÖ3 bazen yardım aldıklarını, DLÖ2 ise yardım almadığını belirtmiştir.

Bilgi güvenliği kavramını daha önce duydunuz mu? Bu konuda bir bilginiz var mı sorusunda; özel okulda ortaokul düzeyinde öğrenim gören ÖOÖ1, ÖOÖ2 ve ÖOÖ3

bilgi güvenliği kavramını daha önce hiç duymadığını belirtmiştir. Devlet okulunda ortaokul düzeyinde öğrenim gören DOÖ1 bilgi güvenliği kavramını duyduğunu ve "kendimize ait olan eee TC kimlik numaramız gibi özel şeylerimizin korunması" şeklinde bu kavramı açıklamıştır. DOÖ2 bilgi güvenliği kavramını daha önce hiç duymadığını, DOÖ3 ise duyduğunu ama ne anlama geldiğini bilmediğini ifade etmiştir. Özel okulda lise düzeyinde öğrenim gören ÖLÖ1 bilgi güvenliği kavramını duyduğunu ve bu kavramın "kişisel bilgilerimizi güvenlik altında tutmak" şeklinde açıklanabileceğini, ÖLÖ2 bilgi güvenliği kavramını duyduğunu ve bu kavramın "sosyal medya hesaplarındaki bilgileri korumak" olarak tanımlanabileceğini, ÖLÖ3 ise daha önce bu kavramı duymadığını dile getirmiştir. Devlet okulunda lise düzeyinde öğrenim gören öğrenciler olan DLÖ1, DLÖ2 ve DLÖ3 bilgi güvenliği kavramını daha önce hiç duymadıklarını ve ne anlama geldiği hakkında fikir sahibi olmadıklarını belirtmişlerdir.

Eğer varsa bilgisayarınızda veya kullandığınız diğer teknolojik cihazlarda (tablet/ipad, cep telefonu vb.) antivirüs programı yüklü mü sorusunda; özel okulda ortaokul düzeyinde öğrenim gören ÖOÖ1 ve ÖOÖ2 antivirüs programının yüklü olduğunu, ÖOÖ3 ise telefon ve tablette yüklü olup bilgisayarda yüklü olmadığını ifade etmiştir. Devlet okulunda ortaokul düzeyinde öğrenim gören DOÖ1 ve DOÖ2 antivirüs programının yüklü olduğunu, DOÖ3 ise cep telefonumda olmadığını, sadece bilgisayarında yüklü olduğunu belirtmiştir. Özel okulda lise düzeyinde öğrenim gören ÖLÖ1 sadece bilgisayarında antivirüs programının yüklü olduğunu, telefonunda olmadığını, ÖLÖ2 ve ÖLÖ3 ise antivirüs programının yüklü olduğunu dile getirmiştir. Devlet okulunda lise düzeyinde öğrenim gören DLÖ1 ve DLÖ3 antivirüs programının yüklü olduğunu, DLÖ2 de bilgisayarında yüklü olup cep telefonunda yüklü olmadığını söylemiştir.

Antivirüs programlarının gerekliliği ve işlevi hakkında neler düşünüyorsunuz sorusunda; özel okulda ortaokul düzeyinde öğrenim gören ÖOÖ1 "bilgisayara virüs girmesin diye", ÖOÖ2 "bilgisayarı internet korsanlarından korumak için", ÖOÖ3 "…oyun yüklerken bu oyun zararlı diyo, yükletmiyor" diyerek antivirüs programlarının gerekliliğine yönelik açıklama yapmışlardır. Devlet okulunda ortaokul düzeyinde öğrenim gören DOÖ1 "bazı uygulamalarda virüs olursa diye o virüsleri kaldırmak için", DOÖ2 "bilgisayar virüs kapmasın diye, virüs kaptıysa da onları

silmek için", DOÖ3 "gelen virüsleri tespit etmek için" şeklinde açıklama yapmışlardır. Özel okulda lise düzeyinde öğrenim gören ÖLÖ1 "e-posta kullanımında, flash vs.'den gelebilecek virüslerden koruyor", ÖLÖ2 "flash bellekler veya internet siteleri virüslü olabiliyor, virüs bulaşabiliyor, bu virüslerden telefonumuzu ve bilgisayarımızı korumak için", ÖLÖ3 "bilgisayara ve telefona virüs bulaşmaması için koruyor, kalkan gibi" diyerek antivirüs programlarının gerekliliğini açıklamışlardır. Devlet okulunda lise düzeyinde öğrenim gören DLÖ1 "oyun vs. yüklerken virüs bulaşmasın diye", DLÖ3 "güvenmediğimiz bir dosyayı indirmeyelim diye, bilgisayarı korumak için" şeklinde açıklama yaparken DLÖ2 bilgisi olmadığını ifade etmiştir.

Eğer varsa bilgisayarınızda şifresi kaldırılmış (cracklenmiş) program kullanıyor musunuz? Bu şekilde lisanssız program kullanmanın zararları hakkındaki yorumunuz nedir sorusunda; özel okulda ortaokul düzeyinde öğrenim gören öğrenciler bu şekilde program kullanmadıklarını belirtmişlerdir. Zararlarına yönelik ise ÖOÖ1 "sorun çıkabilir…bilgisayarı kullanamayabiliriz", ÖOÖ2 "hesabım çalınabilir", ÖOÖ3 "virüs kapabilir telefon" açıklamalarını yapmışlardır. Devlet okulunda ortaokul düzeyinde öğrenim gören DOÖ1 konu ile ilgili bilgi sahibi olmadığını, DOÖ2 bu şekilde program kullanmadığını ve bu konuda bilgi sahibi olmadığını, DOÖ3 de lisanssız program kullanmadığını, ama bu programların kullanılması sonucunda bilgisayarın virüs kapabileceğini belirtmiştir. Özel okulda lise düzeyinde öğrenim gören öğrenciler bu şekilde program kullanmadıklarını belirtmişlerdir. Zararlarına yönelik olarak, ÖLÖ1 bilgi sahibi olmadığını, ÖLÖ2 "..korsan oluyor, o da iyi bir şey değil", ÖLÖ3 "üretim firması için zararlı korsan olduğundan" şeklinde açıklama yapmışlardır. Devlet okulunda lise düzeyinde öğrenim gören öğrenciler bu şekilde program kullanmadıklarını, bu programları zararları için ise DLÖ1 "yasal olmayan yollardan indirilen programlar bence haksızlık oluyor" ve DLÖ3 "güvenilmeyen program, bilgisayar bozulabilir" şeklinde açıklama yaparken DLÖ2 bir bilgisi olmadığı ifade etmiştir.

Herhangi bir sosyal medya hesabına üye misiniz sorusunda; özel okulda ortaokul düzeyinde öğrenim gören ÖOÖ1 instagram, facebook ve snapchat, ÖOÖ2 hayır ÖOÖ3 instagram ve facebook sosyal medya hesaplarına üye olduklarını dile getirmişlerdir. Devlet okulunda ortaokul düzeyinde öğrenim gören DOÖ1 facebook ve instagram, DOÖ2 facebook, twitter, snapchat ve instagram, DOÖ3 facebook ve

instagram sosyal medya hesaplarına üye olduklarını belirtmişlerdir. Özel okulda lise düzeyinde öğrenim gören ÖLÖ1 facebook, snapchat ve instagram, ÖLÖ2 facebook, twitter ve instagram, ÖLÖ3 facebook, snapchat ve instagram sosyal medya hesaplarına üye olduklarını söylemişlerdir. Devlet okulunda lise düzeyinde öğrenim gören DLÖ1 instagram, DLÖ2 instagram, DLÖ3 facebook, twitter ve instagram sosyal medya hesaplarına üye olduklarını ifade etmişlerdir.

Sosyal medya kullanımının ve İnternet'in zararlı yönleri konusunda bilgi sahibi misiniz? Cevabınız evet ise, bu konudaki düşünceleriniz nelerdir sorusuna; özel okulda ortaokul düzeyinde öğrenim gören ÖOÖ1 "bağımlılık yapabilir", ÖOÖ2 "çektiğim bir fotoğraf başkası tarafından çalınabilir", ÖOÖ3 "..kötü şeyler izliyolar…snapchatte uygunsuz şeyler yapıyolar.." şeklinde yanıt vermişlerdir. Devlet okulunda ortaokul düzeyinde öğrenim gören DOÖ1 tanınmayan kişilere karşı güvenlik önlemi alma, DOÖ2 yanlış ve gereksiz kullanım, DOÖ3 ise sosyal medya ve internetin doğru kullanılmamasının zararlı olabileceğini belirtmişlerdir. Özel okulda lise düzeyinde öğrenim gören ÖLÖ1 "vakit kaybına ve dikkatin dağılmasına yol açıyor", ÖLÖ2 "internet sitelerinde bazen uygunsuz şeyler çıkabiliyor..onun dışında insanları kandırmak çok yaygın işte sosyal medya hesabından işte kandırılabiliyorlar insanları", ÖLÖ3 "internetteki her kişiye güvenemezsiniz mesela, çünkü sanal kişiler oluyolar ve gerçekte tanımadığın için güvenin de olmamalı sonuçta yani iyi biri gibi gözüken biri çok kötü biri de olabilir" diyerek bu konudaki düşüncelerini dile getirmişlerdir. Devlet okulunda lise düzeyinde öğrenim gören DLÖ1 uygunsuz şeyler olduğunu, DLÖ2 zaman kaybına yol açtığını, DLÖ3 de bilinmeyen şeylere yönelim olabileceğini ifade etmişlerdir.

Sosyal medya kullanımının ve İnternet'in zararlı yönleri doğrultusunda yaşadığınız kötü bir tecrübe (sosyal medya hesabının başkasının eline geçmesi, dolandırıcılık vb.) var mı sorusunda; özel okulda ortaokul düzeyinde öğrenim gören ÖOÖ1 kendisinin başına gelmediğini, arkadaşının hesabının çalındığını, ÖOÖ2 böyle bir şey yaşamadığını, ÖOÖ3 ise instagram ve bir oyun hesabının çalındığını dile getirmiştir. Devlet okulunda ortaokul düzeyinde öğrenim gören DOÖ1 kendisinin değil, dayısının başına böyle bir olay geldiğini, DOÖ2 babasının hesabının çalındığını, DOÖ3 ise böyle bir şey yaşamadığını belirtmiştir. Özel okulda lise düzeyinde öğrenim gören ÖLÖ1 "yok ama bir arkadaşımın instagram hesabı çalınmıştı. Fotoğraflarına

uygunsuz shoplar yapıp hesabında paylaşmıştı" diyerek kendisinin böyle bir olay yaşamadığını ancak arkadaşının başına böyle bir olay geldiğini, ÖLÖ2 ve ÖLÖ3 ise böyle bir olay yaşamadığını ifade etmiştir. Devlet okulunda lise düzeyinde öğrenim gören DLÖ1 e-posta hesabının çalındığını ve sonrasında hesabı geri alabildiğini, DLÖ2 sosyal medya hesabının bir kez çalındığını, DLÖ3 ise bu şekilde bir olayı daha önce hiç yaşamadığını söylemiştir.

Sosyal medya kullanımının ve İnternet'in zararlı yönlerine yönelik olarak ne gibi önlemler alınmalı? Siz bu konuda herhangi bir önlem alıyor musunuz sorusunu; özel okulda ortaokul düzeyinde öğrenim gören ÖOÖ1 "güçlü şifreler koyuyorum", ÖOÖ2 "şifreyi çok bilinmedik bir şekilde ayarlayabiliriz", ÖOÖ3 "tanımadığımız kişileri takip etmemeliyiz…oyunlarda ise yaş sınırına uyulmalı" şeklinde cevaplamışlardır. Devlet okulunda ortaokul düzeyinde öğrenim gören DOÖ1 "paylaşımlarda dosyayı indirmeden önce antivirüs programından emin oluyorum sonra fecebookta falan paylaşım yaparken yakın çevreme gönder butonuna basıp sadece tanıdığım insanlara gönderiyorum", DOÖ2 "bilgilerimizi korumalıyız…şifrelerimizi kimsenin bilmeyeceği şekilde koymalıyız, kimseye söylememeliyiz", DOÖ3 "kaliteli, güçlü şifre koyuyorum" diyerek soruyu yanıtlamışlardır. Özel okulda lise düzeyinde öğrenim gören ÖLÖ1 "kendimi kısıtlamaya çalışıyorum, sosyal medya hesaplarında şifrelerimi güvenli şeyler yapmaya çalışıyorum ve bilgilerimi daha çok korumaya çalışıyorum", ÖLÖ2 "daha az vakit ayırabiliriz, şifremizi daha güçlü seçebiliriz tanımadığımız insanlarla sosyal medya üzerinden konuşmayabiliriz", ÖLÖ3 "ben her şeye çabucak inanmıyorum çok araştırıyorum mesela önüme bir yazı geldiğinde işte araştırıyorum acaba bunu onaylarsam nolur diye..toplumlara da, yani özellikle genç ve çocuk kitlelerine bu konuda seminerler düzenlenmeli bence yani bunun zararlarını, internetin zararlarını ve nasıl kullanılacağı konusunda bilgilendirme yapılmalı bence" şeklinde alınması gerek önlemlere yönelik açıklama yapmışlardır. Devlet okulunda lise düzeyinde öğrenim gören DLÖ1 "önleme gerek yok yapan zaten bir şekilde yapıyor", DLÖ2 "başkalarına şifremizi vermemeliyiz", DLÖ3 "antivirüs programı yüklemeliyiz…gerektiğinden fazla girmemeliyiz" diyerek soruyu cevaplandırmışlardır.

4.2 Öğretmenlerin Bilgi Güvenliği Farkındalık Düzeyleri ve Bu Konuya İlişkin Görüşleri

Araştırma kapsamında yer alan 120 öğretmene demografik bilgi anketi ve bilgi güvenliği farkındalık ölçeği uygulanmış, 12 öğretmen ile de yüz yüze görüşme yapılmıştır. Elde edilen verilerden ulaşılan bulgular aşağıda yer alan başlıklarda altında açıklanmıştır.

4.2.1 Öğretmenlerin Bilgi Güvenliği Farkındalık Düzeyleri

Araştırmada yer alan öğretmenlerin (n=120) BGFÖ puan ortalamaları değerlendirildiğinde, genel güvenlik alt boyutu ortalamasının 45,84±9,52, saldırı ve tehditler alt boyutu ortalamasının 40,71±14,89, mobil cihazlar, mahremiyet ve iletişim alt boyutu ortalamasının 57,98±16,74, BGFÖ genel puan ortalamasının 144,53±37,12 olduğu görülmektedir (Tablo 4.22).

Tablo 4.22 Öğretmenlerin BGFÖ Puanlarına İlişkin Betimsel İstatistikler

Alt Boyutlar	n	$\overline{X}$	ss	Max	Min
Genel Güvenlik	120	45,84	9,52	65	13
Saldırı ve Tehditler	120	40,71	14,89	85	17
Mobil Cihazlar, Mahremiyet ve İletişim	120	57,98	16,74	90	18
BGFÖ genel puan	120	144,53	37,12	240	48

4.2.1.1 Öğretmenlerin Bilgi Güvenliği Farkındalık Düzeylerinin Cinsiyete Göre Değerlendirilmesi

Araştırmada yer alan öğretmenlerin (n=120) cinsiyetine göre BGFÖ puan ortalamaları değerlendirildiğinde, saldırı ve tehditler alt boyutu puan ortalamasında kadın ve erkek öğretmenler arasında istatistiksel olarak anlamlı fark tespit edilmiştir ($p<0,05$). Erkek öğretmenlerin farkındalık düzeyinin daha yüksek olduğu görülmüştür. Genel güvenlik alt boyutu, mobil cihazlar, mahremiyet ve iletişim alt boyutu ve ölçek genel puan ortalamalarında ise gruplar arasında istatistiksel olarak anlamlı fark olmadığı görülmüştür ($p>0,05$) (Tablo 4.23).

Tablo 4.23 Öğretmenlerin Cinsiyete Göre BGFÖ Bağımsız Örneklem T Testi Sonuçları

Alt Boyutlar	Cinsiyet	n	$\overline{X}$	ss	df	t	p
Genel Güvenlik	Kadın	87	45,23	9,52	118	-1,145	0,255
	Erkek	33	47,46	9,48			
Saldırı ve Tehditler	Kadın	87	39,02	13,75	118	-2,040	**0,044***
	Erkek	33	45,15	16,97			
Mobil Cihazlar, Mahremiyet ve İletişim	Kadın	87	57,01	15,75	118	-1,024	0,308
	Erkek	33	60,52	19,13			
BGFÖ genel puan	Kadın	87	141,26	34,17	118	-1,572	0,119
	Erkek	33	153,12	43,37			

*p<0.05 (Anlamlılık düzeyi)

4.2.1.2 Öğretmenlerin Bilgi Güvenliği Farkındalık Düzeylerinin Kaç Yıldır Öğretmenlik Yapıldığına Göre Değerlendirilmesi

Araştırmada yer alan öğretmenlerin (n=120) görev sürelerine göre BGFÖ puan ortalamaları değerlendirildiğinde, genel güvenlik alt boyutu, mobil cihazlar, mahremiyet ve iletişim alt boyutu, saldırı ve tehditler alt boyutu ve ölçek genel puan ortalamalarında gruplar arasında istatistiksel olarak anlamlı fark olmadığı görülmüştür (p>0,05) (Tablo 4.24).

Tablo 4.24 Öğretmenlerin Görev Sürelerine Göre BGFÖ ANOVA Testi Sonuçları

Alt Boyutlar	Görev süresi	n	$\overline{X}$	ss	df	F	p	Fark
Genel Güvenlik	1-5 yıl[1]	29	45,72	9,99	4	0,582	0,676	-
	5-10 yıl[2]	29	44,69	9,41				
	10-15 yıl[3]	21	44,43	10,99				
	15-20 yıl[4]	13	48,62	7,33				
	20 yıl ve üstü[5]	28	46,93	9,09				
Saldırı ve Tehditler	1-5 yıl[1]	29	40,79	13,99		0,326	0,860	-
	5-10 yıl[2]	29	40,76	12,52				
	10-15 yıl[3]	21	43,24	15,74				
	15-20 yıl[4]	13	41,39	15,40				
	20 yıl ve üstü[5]	28	38,36	17,66				
Mobil Cihazlar, Mahremiyet ve İletişim	1-5 yıl[1]	29	60,45	15,80		0,331	0,857	-
	5-10 yıl[2]	29	57,21	17,15				
	10-15 yıl[3]	21	57,05	15,79				
	15-20 yıl[4]	13	60,00	14,02				
	20 yıl ve üstü[5]	28	55,96	19,61				
BGFÖ genel puan	1-5 yıl[1]	29	146,97	35,90		0,170	0,953	-
	5-10 yıl[2]	29	142,66	35,36				
	10-15 yıl[3]	21	144,71	37,48				
	15-20 yıl[4]	13	150,00	34,10				
	20 yıl ve üstü[5]	28	141,25	42,98				

*p<0.05 (Anlamlılık düzeyi)

4.2.1.3 Öğretmenlerin Bilgi Güvenliği Farkındalık Düzeylerinin Okul Düzeyine (Ortaokul-Lise) Göre Değerlendirilmesi

Araştırmada yer alan öğretmenlerin (n=120) okul düzeyine göre BGFÖ puan ortalamaları değerlendirildiğinde, saldırı ve tehditler alt boyutu, mobil cihazlar, mahremiyet ve iletişim alt boyutu ve ölçek genel puan ortalamalarında ortaokul ve lisede görev yapan öğretmenler arasında istatistiksel olarak anlamlı fark tespit edilmiştir (p<0,05). Lisede görev yapan öğretmenlerin farkındalık düzeyinin daha yüksek olduğu görülmüştür. Genel güvenlik alt boyutu puan ortalamasında ise gruplar arasında istatistiksel olarak anlamlı fark olmadığı görülmüştür (p>0,05) (Tablo 4.25).

Tablo 4.25 Öğretmenlerin Okul Düzeyine Göre BGFÖ Bağımsız Örneklem T Testi Sonuçları

Alt Boyutlar	Okul düzeyi	n	$\overline{X}$	ss	df	t	p
Genel Güvenlik	Ortaokul	60	44,61	8,90	118	-1,452	0,149
	Lise	60	47,12	10,03			
Saldırı ve Tehditler	Ortaokul	60	37,72	15,24	118	-2,273	**0,025***
	Lise	60	43,80	13,98			
Mobil Cihazlar, Mahremiyet ve İletişim	Ortaokul	60	54,71	18,81	118	-2,212	**0,029***
	Lise	60	61,36	14,18			
BGFÖ genel puan	Ortaokul	60	137,03	38,80	118	-2,288	**0,024***
	Lise	60	152,27	33,92			

*p<0.05 (Anlamlılık düzeyi)

Araştırmada yer alan ve özel okulda görev yapan öğretmenlerin (n=60) okul düzeyine göre BGFÖ puan ortalamaları değerlendirildiğinde, saldırı ve tehditler alt boyutu puan ortalamasında ortaokul ve lisede görev yapan öğretmenler arasında istatistiksel olarak anlamlı fark tespit edilmiştir (p<0,05). Lisede görev yapan öğretmenlerin farkındalık düzeyinin daha yüksek olduğu görülmüştür. Genel güvenlik alt boyutu, mobil cihazlar, mahremiyet ve iletişim alt boyutu ve ölçek genel puan ortalamalarında ise gruplar arasında istatistiksel olarak anlamlı fark olmadığı görülmüştür (p>0,05) (Tablo 4.26).

Tablo 4.26 Özel Okulda Görev Yapan Öğretmenlerin Okul Düzeyine Göre BGFÖ Bağımsız Örneklem T Testi Sonuçları

Alt Boyutlar	Okul düzeyi	n	$\overline{X}$	ss	df	t	p
Genel Güvenlik	Ortaokul	30	44,50	8,74	58	-0,822	0,414
	Lise	30	46,47	9,76			
Saldırı ve Tehditler	Ortaokul	30	34,33	14,82	58	-2,594	**0,012***
	Lise	30	43,57	12,66			
Mobil Cihazlar, Mahremiyet ve İletişim	Ortaokul	30	55,97	19,83	58	-1,063	0,292
	Lise	30	60,87	15,65			
BGFÖ genel puan	Ortaokul	30	134,80	39,59	58	-1,657	0,103
	Lise	30	150,90	35,56			

*p<0.05 (Anlamlılık düzeyi)

Araştırmada yer alan ve devlet okulunda görev yapan öğretmenlerin (n=60) okul düzeyine göre BGFÖ puan ortalamaları değerlendirildiğinde, mobil cihazlar,

mahremiyet ve iletişim alt boyutu puan ortalamasında ortaokul ve lisede görev yapan öğretmenler arasında istatistiksel olarak anlamlı fark tespit edilmiştir (p<0,05). Lisede görev yapan öğretmenlerin farkındalık düzeyinin daha yüksek olduğu görülmüştür. Genel güvenlik alt boyutu, saldırı ve tehditler alt boyutu ve ölçek genel puan ortalamalarında ise gruplar arasında istatistiksel olarak anlamlı fark olmadığı görülmüştür (p>0,05) (Tablo 4.27).

Tablo 4.27 Devlet Okulunda Görev Yapan Öğretmenlerin Okul Düzeyine Göre BGFÖ Bağımsız Örneklem T Testi Sonuçları

Alt Boyutlar	Okul düzeyi	n	$\overline{X}$	ss	df	t	p
Genel Güvenlik	Ortaokul	30	44,71	9,20	58	-1,216	0,229
	Lise	30	47,79	10,44			
Saldırı ve Tehditler	Ortaokul	30	41,00	15,15	58	-0,768	0,446
	Lise	30	44,03	15,46			
Mobil Cihazlar, Mahremiyet ve İletişim	Ortaokul	30	53,48	17,18	58	-2,134	**0,037***
	Lise	30	61,86	12,75			
BGFÖ genel puan	Ortaokul	30	139,19	38,54	58	-1,566	0,123
	Lise	30	153,69	32,70			

*p<0.05 (Anlamlılık düzeyi)

4.2.1.4 Öğretmenlerin Bilgi Güvenliği Farkındalık Düzeylerinin Okul Türüne (Devlet Okulu-Özel Okul) Göre Değerlendirilmesi

Araştırmada yer alan öğretmenlerin (n=120) okul türüne göre BGFÖ puan ortalamaları değerlendirildiğinde, genel güvenlik alt boyutu, saldırı ve tehditler alt boyutu, mobil cihazlar, mahremiyet ve iletişim alt boyutu ve ölçek genel puan ortalamalarında gruplar arasında istatistiksel olarak anlamlı fark olmadığı görülmüştür (p>0,05) (Tablo 4.28).

Tablo 4.28 Öğretmenlerin Okul Türüne Göre BGFÖ Bağımsız Örneklem T Testi Sonuçları

Alt Boyutlar	Okul Türü	n	$\overline{X}$	ss	df	t	p
Genel Güvenlik	Özel Okul	60	45,48	9,24	118	-0,411	0,682
	Devlet Okulu	60	46,20	9,86			
Saldırı ve Tehditler	Özel Okul	60	14,44	1,86	118	-1,297	0,197
	Devlet Okulu	60	15,24	1,97			
Mobil Cihazlar, Mahremiyet ve İletişim	Özel Okul	60	17,88	2,31	118	0,288	0,774
	Devlet Okulu	60	15,65	2,02			
BGFÖ genel puan	Özel Okul	60	38,18	4,93	118	-0,493	0,623
	Devlet Okulu	60	36,28	4,68			

*p<0.05 (Anlamlılık düzeyi)

Araştırmada yer alan ve ortaokulda görev yapan öğretmenlerin (n=60) okul türüne göre BGFÖ puan ortalamaları değerlendirildiğinde, genel güvenlik alt boyutu, saldırı ve tehditler alt boyutu, mobil cihazlar, mahremiyet ve iletişim alt boyutu ve ölçek genel puan ortalamalarında gruplar arasında istatistiksel olarak anlamlı fark olmadığı görülmüştür (p>0,05) (Tablo 4.29).

Tablo 4.29 Ortaokulda Görev Yapan Öğretmenlerin Okul Türüne Göre BGFÖ Bağımsız Örneklem T Testi Sonuçları

Alt Boyutlar	Okul Türü	n	$\overline{X}$	ss	df	t	p
Genel Güvenlik	Özel Okul	30	44,50	8,74	59	-0,091	0,928
	Devlet Okulu	30	44,71	9,20			
Saldırı ve Tehditler	Özel Okul	30	34,33	14,82	59	-1,737	0,088
	Devlet Okulu	30	41,00	15,15			
Mobil Cihazlar, Mahremiyet ve İletişim	Özel Okul	30	55,97	19,83	59	0,523	0,603
	Devlet Okulu	30	53,48	17,18			
BGFÖ genel puan	Özel Okul	30	134,80	39,59	59	-0,439	0,662
	Devlet Okulu	30	139,19	38,54			

*p<0.05 (Anlamlılık düzeyi)

Araştırmada yer alan ve lisede görev yapan öğretmenlerin (n=60) okul türüne göre BGFÖ puan ortalamaları değerlendirildiğinde, genel güvenlik alt boyutu, saldırı ve tehditler alt boyutu, mobil cihazlar, mahremiyet ve iletişim alt boyutu ve ölçek genel puan ortalamalarında gruplar arasında istatistiksel olarak anlamlı fark olmadığı görülmüştür (p>0,05) (Tablo 4.30).

Tablo 4.30 Lisede Görev Yapan Öğretmenlerin Okul Türüne Göre BGFÖ Bağımsız Örneklem T Testi Sonuçları

Alt Boyutlar	Okul Türü	n	$\overline{X}$	ss	df	t	p
Genel Güvenlik	Özel Okul	30	46,47	9,76	57	-0,504	0,616
	Devlet Okulu	30	47,79	10,44			
Saldırı ve Tehditler	Özel Okul	30	43,57	12,66	57	-0,127	0,899
	Devlet Okulu	30	44,03	15,46			
Mobil Cihazlar, Mahremiyet ve İletişim	Özel Okul	30	60,87	15,65	57	-0,267	0,790
	Devlet Okulu	30	61,86	12,75			
BGFÖ genel puan	Özel Okul	30	150,90	35,56	57	-0,313	0,755
	Devlet Okulu	30	153,69	32,70			

*p<0.05 (Anlamlılık düzeyi) **p<0.01 (Anlamlılık düzeyi)

4.2.1.5 Öğretmenlerin Bilgi Güvenliği Farkındalık Düzeylerinin Bilgisayar Kullanım Süresine Göre Değerlendirilmesi

Araştırmada yer alan öğretmenlerin (n=120) bilgisayarda günde kaç saat vakit geçirdiklerine göre BGFÖ puan ortalamaları değerlendirildiğinde, genel güvenlik alt boyutu, mobil cihazlar, mahremiyet ve iletişim alt boyutu ve ölçek genel puan ortalamalarında gruplar arasında istatistiksel olarak anlamlı fark tespit edilmiştir (p<0,05). Mobil cihazlar, mahremiyet ve iletişim alt boyutu ile ölçek genel puan ortalamalarında, günde 0-1 saat bilgisayar kullanan grup ile günde 5 saatten fazla bilgisayar kullanan grup arasında anlamlı farklılık yer almaktadır. Farkındalık düzeyi en yüksek olan grubun ise günde 5 saatten fazla bilgisayar kullanan grup olduğu görülmüştür. Saldırı ve tehditler alt boyutunda ise gruplar arasında istatistiksel olarak anlamlı fark olmadığı tespit edilmiştir (p>0,05) (Tablo 4.31).

Tablo 4.31 Öğretmenlerin Bilgisayarda Günde Kaç Saat Vakit Geçirdiklerine Göre BGFÖ ANOVA Testi Sonuçları

Alt Boyutlar	Bilgisayar Kullanım Süresi	n	$\overline{X}$	ss	df	F	p	Fark
Genel Güvenlik	0-1 saat[1]	43	42,72	8,99	3	3,038	**0,032***	-
	1-2 saat[2]	49	47,31	9,49				
	2-4 saat[3]	20	46,75	9,59				
	5 saat ve üstü[4]	8	51,38	8,75				
Saldırı ve Tehditler	0-1 saat[1]	43	37,47	11,72		2,184	0,094	-
	1-2 saat[2]	49	41,67	15,98				
	2-4 saat[3]	20	41,05	15,76				
	5 saat ve üstü[4]	8	51,38	17,82				
Mobil Cihazlar, Mahremiyet ve İletişim	0-1 saat[1]	43	53,26	15,02		3,251	**0,024***	1-4
	1-2 saat[2]	49	58,90	16,70				
	2-4 saat[3]	20	60,45	17,64				
	5 saat ve üstü[4]	8	71,50	16,79				
BGFÖ genel puan	0-1 saat[1]	43	133,44	29,94		3,379	**0,021***	1-4
	1-2 saat[2]	49	147,88	38,79				
	2-4 saat[3]	20	148,25	39,93				
	5 saat ve üstü[4]	8	174,25	39,02				

*p<0.05 (Anlamlılık düzeyi)

Araştırmada yer alan öğretmenlerin (n=120) bilgisayarda haftada toplam kaç saat vakit geçirdiklerine göre BGFÖ puan ortalamaları değerlendirildiğinde, genel güvenlik alt boyutu (p<0,05), mobil cihazlar, mahremiyet ve iletişim alt boyutu (p<0,05) ve ölçek genel (p<0,05) puan ortalamalarında gruplar arasında istatistiksel olarak anlamlı fark tespit edilmiştir. Genel güvenlik alt boyutunda, haftada toplam 1-2 saat bilgisayar kullanan grup ile haftada toplam 2-4 saat, 5-10 saat ve 10 saatten fazla bilgisayar kullanan gruplar arasında anlamlı farklılık yer almaktadır. Farkındalık düzeyi en yüksek olan grubun ise haftada toplam 10 saatten fazla bilgisayar kullanan grup olduğu görülmüştür. Mobil cihazlar, mahremiyet ve iletişim alt boyutu ile ölçek genel puan ortalamalarında, haftada toplam 1-2 saat bilgisayar kullanan grup ile haftada toplam 10 saatten fazla bilgisayar kullanan gruplar arasında anlamlı farklılık yer almaktadır. Farkındalık düzeyi en yüksek olan grubun ise haftada toplam 10 saatten fazla bilgisayar kullanan grup olduğu görülmüştür. Saldırı ve tehditler alt boyutunda ise gruplar arasında istatistiksel olarak anlamlı fark olmadığı tespit edilmiştir (p>0,05) (Tablo 4.32).

Tablo 4.32 Öğretmenlerin Bilgisayarda Haftada Kaç Saat Vakit Geçirdiklerine Göre BGFÖ ANOVA Testi Sonuçları

Alt Boyutlar	Bilgisayar kullanım süresi	n	$\overline{X}$	ss	df	F	p	Fark
Genel Güvenlik	0-1 saat[1]	6	46,50	9,42	4	6,623	**0,000***	2-3, 2-4, 2-5
	1-2 saat[2]	15	35,27	8,96				
	2-4 saat[3]	26	46,08	7,72				
	5-10 saat[4]	45	47,33	8,81				
	10 saat ve üstü[5]	28	48,75	9,21				
Saldırı ve Tehditler	0-1 saat[1]	6	43,17	8,77		1,041	0,389	-
	1-2 saat[2]	15	35,40	12,90				
	2-4 saat[3]	26	39,92	12,73				
	5-10 saat[4]	45	40,16	16,89				
	10 saat ve üstü[5]	28	4,64	15,09				
Mobil Cihazlar, Mahremiyet ve İletişim	0-1 saat[1]	6	57,00	8,03		2,761	**0,031***	2-5
	1-2 saat[2]	15	47,73	13,48				
	2-4 saat[3]	26	57,58	16,86				
	5-10 saat[4]	45	57,47	17,33				
	10 saat ve üstü[5]	28	64,86	16,35				
BGFÖ genel puan	0-1 saat[1]	6	146,67	22,67		3,016	**0,021***	2-5
	1-2 saat[2]	15	118,40	27,73				
	2-4 saat[3]	26	143,58	32,89				
	5-10 saat[4]	45	144,96	40,05				
	10 saat ve üstü[5]	28	158,25	37,24				

*p<0.05 (Anlamlılık düzeyi)

4.2.1.6 Öğretmenlerin Bilgi Güvenliği Farkındalık Düzeylerinin İnternet Kullanım Süresine Göre Değerlendirilmesi

Araştırmada yer alan öğretmenlerin (n=120) internette günde kaç saat vakit geçirdiklerine göre BGFÖ puan ortalamaları değerlendirildiğinde, genel güvenlik alt boyutu (p<0,05), mobil cihazlar, mahremiyet ve iletişim alt boyutu (p<0,05), saldırı ve tehditler alt boyutu (p<0,05) ve ölçek genel (p<0,05) puan ortalamalarında gruplar arasında istatistiksel olarak anlamlı fark tespit edilmiştir. Genel güvenlik alt boyutu puan ortalamalarında, günde 0-1 saat internette vakit geçiren grup ile günde 2-4 saat internette vakit geçiren grup arasında anlamlı farklılık yer almaktadır. Farkındalık düzeyi en yüksek olan grubun ise günde 2-4 saat internette vakit geçiren grup olduğu görülmüştür. Mobil cihazlar, mahremiyet ve iletişim alt boyutu ile ölçek genel puan ortalamalarında, günde 0-1 saat internette vakit geçiren grup ile günde 2-4 saat internette vakit geçiren grup arasında ve günde 0-1 saat internette vakit geçiren grup ile günde 5 saatten fazla internette vakit geçiren grup arasında anlamlı farklılık yer almaktadır. Farkındalık düzeyi en yüksek olan grubun ise günde 5 saatten fazla internette vakit geçiren grup olduğu görülmüştür (Tablo 4.33).

Tablo 4.33 Öğretmenlerin İnternette Günde Kaç Saat Vakit Geçirdiklerine Göre BGFÖ ANOVA Testi Sonuçları

Alt Boyutlar	İnternet Kullanım Süresi	n	$\overline{X}$	ss	df	F	p	Fark
Genel Güvenlik	0-1 saat[1]	31	41,26	9,07	3	3,876	**0,011***	1-3
	1-2 saat[2]	43	46,33	8,14				
	2-4 saat[3]	36	48,56	9,18				
	5 saat ve üstü[4]	10	48,20	13,32				
Saldırı ve Tehditler	0-1 saat[1]	31	34,58	15,27		3,072	**0,031***	-
	1-2 saat[2]	43	41,02	11,52				
	2-4 saat[3]	36	43,78	15,60				
	5 saat ve üstü[4]	10	47,30	19,32				
Mobil Cihazlar, Mahremiyet ve İletişim	0-1 saat[1]	31	50,61	16,36		4,434	**0,005***	1-3, 1-4
	1-2 saat[2]	43	57,70	13,73				
	2-4 saat[3]	36	61,47	17,47				
	5 saat ve üstü[4]	10	69,40	19,07				
BGFÖ genel puan	0-1 saat[1]	31	126,45	37,12		4,587	**0,005***	1-3, 1-4
	1-2 saat[2]	43	145,05	27,50				
	2-4 saat[3]	36	153,81	38,90				
	5 saat ve üstü[4]	10	164,90	47,77				

*p<0.05 (Anlamlılık düzeyi)

4.2.1.7 Öğretmenlerin Bilgi Güvenliği Farkındalık Düzeylerinin Sosyal Ağa Üye Olma Durumuna Göre Değerlendirilmesi

Araştırmada yer alan öğretmenlerin (n=120) sosyal ağa üyelik durumlarına göre BGFÖ puan ortalamaları değerlendirildiğinde, ölçek alt boyutları ile ölçek genel puan ortalamalarında sosyal ağa üye olan ve olmayan öğrenciler arasında istatistiksel olarak anlamlı fark olmadığı görülmüştür (p>0,05) (Tablo 4.34).

Tablo 4.34 Öğretmenlerin Sosyal Ağa Üyelik Durumuna Göre BGFÖ Bağımsız Örneklem T Testi Sonuçları

Alt Boyutlar	Sosyal Ağa Üyelik	n	$\overline{X}$	ss	df	t	p
Genel Güvenlik	Evet	109	45,61	9,79	118	-0,855	0,394
	Hayır	11	48,18	6,05			
Saldırı ve Tehditler	Evet	109	40,28	15,05	118	-0,982	0,328
	Hayır	11	44,91	13,04			
Mobil Cihazlar, Mahremiyet ve İletişim	Evet	109	57,52	16,96	118	-0,931	0,354
	Hayır	11	62,46	14,22			
BGFÖ genel puan	Evet	109	143,41	37,87	118	-1,333	0,304
	Hayır	11	155,55	27,67			

*p<0.05 (Anlamlılık düzeyi)

4.2.2 Öğretmenlerin Bilgi Güvenliği Farkındalığına Yönelik Görüşleri

Çalışmaya katılan 12 öğretmen ile yarı yapılandırılmış görüşme sorularıyla yüz yüze görüşme gerçekleştirilmiştir. Görüşmede öğretmenlere 13 adet soru yöneltilmiştir. Öğretmenlerin görüşme esnasında verdikleri cevaplar analiz edilmiştir.

Kaç yıldır öğretmenlik mesleğini icra ediyorsunuz sorusunda; özel okulda ortaokul düzeyinde görev yapan ÖOÖT1 3 yıldır, ÖOÖT2 2 yıldır, ÖOÖT3 5 yıldır,

devlet okulunda ortaokul düzeyinde görev yapan DOÖT1 19 yıldır, DOÖT2 2 yıldır, DOÖT3 9 yıldır, özel okulda lise düzeyinde görev yapan ÖLÖT1 5 yıldır, ÖLÖT2 2 yıldır, ÖLÖT3 3 yıldır ve devlet okulunda lise düzeyinde görev yapan DLÖT1 7 yıldır, DLÖT2 16 yıldır, DLÖT3 28 yıldır öğretmenlik yaptığını söylemiştir.

Kendinize ait bilgisayar, cep telefonu, tablet vb. teknolojik cihazlarınız var mı sorusuna, özel okulda ortaokul düzeyinde görev yapan ÖOÖT1 bilgisayarı, cep telefonu ve tableti olduğunu, ÖOÖT2 cep telefonu, masaüstü bilgisayarı ve diz üstü bilgisayarı olduğunu, ÖOÖT3 bilgisayarı ve cep telefonu olduğunu söylemişlerdir. Devlet okulunda ortaokul düzeyinde görev yapan DOÖT1, bilgisayarı ve cep telefonu, DOÖT2 bilgisayarı ve cep telefonu, DOÖT3 bilgisayarı, cep telefonu ve tableti olduğunu belirtmiştir. Özel okulda lise düzeyinde görev yapan ÖLÖT1, ÖLÖT2 ve ÖLÖT3 bilgisayar ve cep telefonu sahibi olduklarını ifade etmişlerdir. Devlet okulunda lise düzeyinde görev yapan DLÖT1, DLÖT2 ve DLÖT3 kendilerine ait bilgisayar, cep telefonu ve tableti olduğunu dile getirmişlerdir.

Eğer varsa teknolojik cihazları (tablet, cep telefonu vb.) hangi amaçlar (haberleşme, oyun, sohbet/chat, iş, e-devlet vb.) doğrultusunda kullanıyorsunuz sorusuna; özel okulda ortaokul düzeyinde görev yapan ÖOÖT1 iş (deney araştırma, video indirme vs.), haberleşmek ve sosyal medyada gezinmek için, ÖOÖT2 haberleşmek, e-mailleri kontrol etmek ve sosyal medyada dolaşmak için, ÖOÖT3 haberleşmek, iş ile ilgili şeyleri yapmak ve e-mail kontrolü yapmak için yanıtını vermişlerdir. Devlet okulunda ortaokul düzeyinde görev yapan DOÖT1 bilgisayarı eğitim materyalleri üretmek ve mesleki işleri yapmak için, cep telefonunu haberleşmek, sosyal medyada dolaşmak, bankacılık işlemleri ve e-devlet işlemleri yapmak için, DOÖT2 haberleşmek, sohbet etmek, iş, e-devlet işlemlerini yapmak ve film izlemek için, DOÖT3 bilgi edinmek, araştırmak, haberleşmek ve sosyal medyada gezinmek için kullandıklarını belirtmişlerdir. Özel okulda lisede görev yapan ÖLÖT1 gündemi takip etmek, haberleşmek ve okul işlerini halletmek için, ÖLÖT2 mesleğe yönelik çalışmalar yapmak, haberleşmek, sosyal medyada dolaşmak ve gündemi takip etmek için, ÖLÖT3 haberleşmek ve iş için teknolojik cihazları kullandıklarını söylemişlerdir. Devlet okulunda lise düzeyinde görev yapan DLÖT1 mesleği ile ilgili işler yapmak, haberleşmek, bankacılık işlemlerini yapmak, e-mailleri kontrol etmek ve sosyal medyada gezinmek için, DLÖT2 sosyal medyada gezinmek, internete

girmek ve bilgiye erişmek için, DLÖT3 bilgi alışverişi yapmak, haberleşmek, oyun oynamak, sohbet etmek, sosyal medyada dolaşmak ve e-devlet ile ilgili işlemleri yapmak için kullandıklarını ifade etmişlerdir.

Bilgi güvenliği kavramını daha önce duydunuz mu? Bu konuda bir bilginiz var mı sorusuna özel okulda ortaokul düzeyinde görev yapan ÖOÖT1 "bilgilerin, sosyal medya hesaplarının korunması diye biliyorum", ÖOÖT2 "sanıyorum paylaştığımız bilgilerin ne kadar, kimlerle, nasıl paylaşıldığı ve bunun kalıcılığıyla ilgili, biraz daha doğru insanlara mı gidiyo diye biliyorum", ÖOÖT3 "bilgilerimin nasıl bende saklı olabileceğine dair bir kavram" şeklinde yanıt vermişlerdir. Devlet okulunda ortaokul düzeyinde görev yapan DOÖT1 "var olan bilgilerinizin..cihazlarınıza kaydedilmesi veya internet ortamına taşınması konusunda onların nasıl korunabileceği yolunda bazı adımlar atılması ve önlemler alınması diye biliyorum", DOÖT2 "kişisel bilgilerimizin internet ortamında paylaşılması konusundaki gizlilik", DOÖT3 "kişisel verilerin korunması ile ilgili yapılacak işlemler" diyerek açıklama yapmışlardır. Özel okulda lise düzeyinde görev yapan ÖLÖT1, ÖLÖT2 ve ÖLÖT3 bu kavramı duyduklarını fakat çok fazla bilgi sahibi olmadıklarını dile getirmişlerdir. Devlet okulunda lise düzeyinde görev yapan DLÖT1 bu kavramı daha önce duymadığını, DLÖT2 "kişisel verilerin korunması veya firma açısından kurum bilgilerinin korunması", DLÖT3 "duydum ama çok bilgi sahibi değilim kişisel bilgilerin korunması, bilgilerin kötü amaçlı kişilerin eline geçmesinin engellenmesi denilebilir" şeklinde düşüncelerini ifade etmişlerdir.

Eğer varsa evinizde kullandığınız teknolojik cihazlarda antivirüs yazılım mevcut mu? Antivirüs programlarının gerekliliği hakkında neler düşünüyorsunuz sorusunu; özel okulda ortaokul düzeyinde görev yapan ÖOÖT1 antivirüs programının yüklü olduğunu ve "internet bankacılığında şifrelerimin korunduğunu, saklandığını biliyorum, bir şey indirmek istediğimde o programın onu frenlediğini biliyorum", ÖOÖT2 telefonda olmadığını fakat bilgisayarında antivirüs programı olduğunu ve "gerekli olduğunu düşünüyorum, çünkü bir siteye girdiğimiz zaman çok fazla virüslü içerikler olabiliyor spam tarzı şeyler gelebiliyor işte bildirimler gelebiliyor bunlarda zararlı", ÖOÖT3 bilgisayarında antivirüs programı olduğunu ve "dışarıdan gelebilecek kötü amaçlı yazılımlara engel olmak için..ancak antivirüs programlarının yeterli olduğunu da düşünmüyorum hala bir saldırıya uğradığımı düşünüyorum" şeklinde

yanıtlamışlardır. Devlet okulunda ortaokul düzeyinde görev yapan DOÖT1 antivirüs programının yüklü olduğunu ve "korsan veya zarar verici yazılımlar var ister istemez devamlı internet ortamında olduğumuz için bu kötü niyetli yazılımlar veya kişileri engellemek için antivirüs programlarının olması gerektiğini düşünüyorum" DOÖT2 antivirüs programının yüklü olduğunu ve "internetten ve diğer kişilerden gelecek zararlı yazılımları engellemek için", DOÖT3 "windows'un kendi yazılımı var ayrıca bir program kullanmıyorum" ve "bilgisayarda bulunan bilgilerin ele geçirilmesi konusunda faydalı olabilir..gerekli bir program ama bilinçli kullanmak gerekiyor" şeklinde cevap vermişlerdir. Özel okulda lise düzeyinde görev yapan ÖLÖT1 antivirüs programı kullanmadığını ve "kişisel bilgilerimizin kötü niyetli kişilerin eline geçmemesi için kullanılabilir", ÖLÖT2 antivirüs programının yüklü olduğunu ve "arada çerezler çıkabiliyor, bilgisayara virüs girebiliyor", ÖLÖT3 "yok, ama apple marka olduğu için kullanmıyorum, ama virüslerden korunulması için kullanılmalı" diyerek soruyu yanıtlamışlardır. Devlet okulunda lise düzeyinde görev yapan DLÖT1 antivirüs programını kullandığını ve "kesinlikle gerekli, özellikle internetin bu kadar yaygın kullanıldığı, internet üzerinden bu kadar alışveriş yapıldığı..online işlem yapıldığı, önemli işlemlerin yapıldığı bu devirde antivirüssüz bir bilgisayar düşünemiyorum", DLÖT2 antivirüs programının yüklü olduğunu ve "kesinlikle gerekli, bilgilerin korunması açısından ve bilgisayarın sürekli çalışabilir durumda kalması açısından gerekli" DLÖT3 antivirüs programının yüklü olduğunu ve "gerekli olduğunu düşünüyorum" diyerek düşüncelerini ifade etmişlerdir.

Eğer varsa bilgisayarınızda şifresi kaldırılmış (cracklenmiş) program kullanıyor musunuz? Bu şekilde lisanssız program kullanmanın zararları hakkındaki yorumunuz nedir sorusuna ÖOÖT1 "hayır…suç diye biliyorum" ÖOÖT2 "kullanmıyorum...doğru olmayabilir, bilgiler gidebilir ve bir yandan da lisansın amacı sonuçta emek verilerek bir program oluşturulmuş nasıl ki korsan CD gibi geliyor biraz bana hani bir kişinin telif hakları olmadan onu kullanabilme çok etik gelmiyor bana açıkçası", ÖOÖT3 "hayır, bilmiyorum" şeklinde yanıt vermişlerdir. Devlet okulunda ortaokul düzeyinde görev yapan DOÖT1 "kullanıyorum...bilgisayarın güvenliğini düşürüyor ister istemez, bilgisayara ulaşım imkanını artırıyor diye düşünüyorum size ait değil kuruma ait değil, bu durumda genel ait bir program haline dönüşüyor, haliyle bir güvenlik zafiyeti oluşuyor heralde", DOÖT2 "kullanıyorum…detaylı bilgim yok",

DOÖT3 “evet kullanıyorum…kişisel verileri ele geçirmek olabilir, reklam virüsleri bulaşabilir” diyerek düşüncelerini açıklamışlardır. Özel okulda lise düzeyinde görev yapan ÖLÖT1 “evet kullanıyorum…kişisel verilerin başka kişilerin eline geçebilmesi gibi zararları olabilir”, ÖLÖT2 “kullanıyorum…bilgiler ele geçirilebilir ama bunun için bir şey yapmıyorum maalesef”, ÖLÖT3 “hayır kullanmıyorum…bu konuda pek fikrim yok” diyerek fikirlerini dile getirmişlerdir. Devlet okulunda lise düzeyinde görev yapan DLÖT1 “kullanıyorum…lisanslı ürünler güncellenebildiği için daha güvenli olabileceğini düşünüyorum”, DLÖT2 “kullanıyorum…zararları olma ihtimali yüksek...bilgilerin güvenliği riske atılmış oluyor”, DLÖT3 “hayır kullanmıyorum…yasal sorumluluğu var…onun haricinde dışarıdan müdahale edilmesi daha kolay olabilir” şeklinde konuyla ilgili yorumlarını yapmışlardır.

Herhangi bir sosyal medya hesabına üye misiniz sorusuna tüm öğretmenler evet cevabını vermişlerdir. Öğretmenlerin üye oldukları sosyal medya hesapları; özel okulda ortaokul düzeyinde görev yapan ÖOÖT1 facebook, twitter ve instagram, ÖOÖT2 instagram ve snapchat, ÖOÖT3 facebook ve instagram, devlet okulunda ortaokul düzeyinde görev yapan DOÖT1 facebook, twitter ve instagram, DOÖT2 facebook ve instagram, DOÖT3 facebook, özel okulda lise düzeyinde görev yapan ÖLÖT1 facebook, twitter ve instagram, ÖLÖT2 twitter ve instagram, ÖLÖT3 facebook, twitter, snapchat ve instagram, devlet okulunda lise düzeyinde görev yapan DLÖT1 facebook ve instagram, DLÖT2 facebook ve instagram, DLÖT3 facebook ve instagram şeklindedir.

Sosyal medya kullanımının ve İnternet’in zararlı yönleri konusunda gündemi takip eder misiniz sorusuna; özel okulda ortaokul düzeyinde görev yapan ÖOÖT1 “konu ile ilgili yazıyla karşılaşırsam okuyorum” ÖOÖT2 “evet takip ediyorum…mesleğimle de ilgili olarak çocuklar nasıl kullanıyor Türkiye’de neler oluyor Dünya’da neler oluyor bunlarla ilgili araştırmalar yapıyorum”, ÖOÖT3 “evet takip ediyorum ama kaçırdığım şeyler oluyordur” şeklinde yanıt vermişlerdir. Devlet okulunda ortaokul düzeyinde görev yapan DOÖT1 “haberlerden..sivil toplum kuruluşları bunların vermiş olduğu çerçevede bilgi sahibiyim”, DOÖT2 “özellikle araştırmam karşıma çıkarsa bakarım”, DOÖT3 “gündemi takip ederim” diyerek düşüncelerini açıklamışlardır. Özel okulda lise düzeyinde görev yapan ÖLÖT1 “sosyal medyada karşılaştıkça okumaya çalışıyorum”, ÖLÖT2 “gündemde karşıma çıkarsa

okuyorum özel olarak bir araştırma yapmıyorum bunun için", ÖLÖT3 "evet gündemi takip ederim" cevaplarını vermişlerdir. Devlet okulunda lise düzeyinde görev yapan DLÖT1 "haber sitelerinden denk geldiğim olaylara bakıyorum", DLÖT2 "evet ederim", DLÖT3 "karşılaştığımda mutlaka okurum" şeklinde açıklama yapmışlardır.

Sosyal medya kullanımının ve İnternet'in zararlı yönleri konusunda öğrencilerinizi bilgilendirir misiniz sorusuna; özel okulda ortaokul düzeyinde görev yapan ÖOÖT1 "evet…sınıfta özellikle sosyal medya konusuna değiniyorum ara ara…tanımadığı kişileri eklememeleri gerektiğini, arkadaşlık isteklerini kabul etmemelerini veya onlardan bir link geldiğinde tıklamamaları gerektiğini söylüyorum", ÖOÖT2 "siber zorbalık ve doğru internet kullanımı konusunda öğrencilerimi bilgilendiriyorum", ÖOÖT3 "evet yönlendirmeye çalışıyorum elimden geldiğince, genelde bu tarz konular geçtiğinde derste bilgilendirme yapıyorum veya rehberlik derslerinde öğrencilere bu konuda bilgi veriyorum" şeklinde cevap vermişlerdir. Devlet okulunda ortaokul düzeyinde görev yapan DOÖT1 "ders kapsamında kazanım da var bilim, teknoloji, teknolojinin kullanımı, zararları veya işte güvenlik...gibi konularda bilgilendirme yapıyorum", DOÖT2 "tabii gördüğüm bildiğim konularda tabi muhakkak bilgilendiririm veya çocuklardan gelen dönütler çerçevesinde yorum yapabilirim", DOÖT3 "zaman zaman bilgilendirme yapıyorum" diyerek düşüncelerini ifade etmişlerdir. Özel okulda lise düzeyinde görev yapan ÖLÖT1 "konusu açıldıkça bildiğim kadarıyla bilgilendirme yapıyorum", ÖLÖT2 "hayır, kendim bile hâkim değilken öğrencilere böyle bir bilgilendirme yapmıyorum", ÖLÖT3 "bilgilendiririm" yanıtını vermişlerdir. Devlet okulunda lise düzeyinde görev yapan DLÖT1 "tabi, kendim takip ettiğim kadarıyla bilgilendirmeye çalışıyorum internet kültürünün oluşması açısından", DLÖT2 "yeri gelince konuştuğum olur ama çok fazla bilgi verdiğim söylenemez", DLÖT3 "zamanı kullanım açısından yönlendirme yapıyorum" şeklinde konu ile ilgili fikirlerini dile getirmişlerdir.

Hiç sosyal medya ya da İnternet aracılığıyla dolandırıldınız mı sorusuna özel okulda ortaokul ve lise düzeyinde, devlet okulunda da lise düzeyinde görev yapan öğretmenler hayır cevabını vermiştir. Devlet okulunda ortaokul düzeyinde görev yapan DOÖT2 ve DOÖT3 hayır cevabını vermiş, DOÖT1 ise "kredi kartı ile ilgili bir hareketlilik olmuştu...internet bankacılığından mı mobil uygulamadan mı böyle bir

durum gerçekleşti bu konuda bilgimiz yok" şeklinde açıklama yaparak daha önce dolandırılma olayını yaşadığını belirtmiştir.

Hiç sosyal medya ya da elektronik posta hesaplarınız başkaları tarafından ele geçirildi mi sorusuna tüm öğretmenler hayır cevabını vermiştir.

Sosyal medya kullanımının ve İnternet'in zararlı yönlerine yönelik olarak ne gibi önlemler alınmalı? Siz bu konuda herhangi bir önlem alıyor musunuz sorusuna; özel okulda ortaokul düzeyinde görev yapan ÖOÖT1 "tanımadığım kişileri eklemiyorum, linklerine tıklamıyorum, toplu mesajlar geldiğinde açmıyorum", ÖOÖT2 "tanımadığım kişileri eklemiyorum, herkese açık gönderi paylaşmıyorum", ÖOÖT3 "tanımadığım insanlarla iletişime geçmiyorum, antivirüs programının güvenli işaretinin olduğu sitelere giriyorum" şeklinde yanıt vermişlerdir. Devlet okulunda ortaokul düzeyinde görev yapan DOÖT1 "bilinçli paylaşımlar yapıyorum, sitelere girerken paylaştığım şahsi bilgilerime bilhassa dikkat ediyorum", DOÖT2 "vakti dikkatli kullanmalıyız…onun dışında bilinçli şekilde kullanımı konusunda bilgim yok", DOÖT3 "kendimizi kontrol etmeliyiz..gerçekten amaca yönelik kullanmalıyız" diyerek fikirlerini dile getirmişlerdir. Özel okulda lise düzeyinde görev yapan ÖLÖT1 "kişisel bilgelerimizi, daha özel şeyleri paylaşmamaya dikkat edebiliriz, arkadaş listemizi daha tanıdığımız kişilerden oluşturabiliriz şifrelerimizi düzenli olarak değiştirebiliriz", ÖLÖT2 "önlem almıyorum, çok uzun zamandır şifremi dahi değiştirmedim", ÖLÖT3 "maillere karşı dikkatliyim, çok spam olarak mail geliyor, hiçbirini açmadan siliyorum" şeklinde açıklama yapmışlardır. Devlet okulunda lise düzeyinde görev yapan DLÖT1 "çok bilmediğim web sitelerine kolayca girmem, çok fazla reklam yayınlayan...çerezlerime olabildiğince bakmaya çalışırım, her sitede olabildiğince şifrelerimi kaydetmem, antivirüs, internet security programlarını kullanmaya çalışıyorum, bilmediğim kaynaklardan dosya yüklemiyorum, herhangi bir tanımadığım kişiden dosya alışverişi yapmıyorum", DLÖT2 "antivürüsün yanı sıra güvenlik duvarı kullanarak önlem almaya çalışıyorum", DLÖT3 "internet sitelerinde açılan reklam pencerelerine girmemeye özen gösteririm...bilmediğim mesaj, e-posta filan bunları açmam" diyerek düşüncelerini açıklamışlardır.

Sosyal medya kullanımının ve İnternet'in zararlı yönlerine yönelik olarak alınması gereken önlemler konusunda öğrencilerinizi yönlendiriyor musunuz sorusuna; özel okulda ortaokul düzeyinde görev yapan ÖOÖT1 kendi aldığı önlemleri

öğrencilerine aktardığını dile getirmiş, ÖOÖT2 "gerek kendi almış olduğum önlemler gerek öğretmen arkadaşlarımın da paylaşımları doğrultusunda öğrencileri almaları gereken önlemler almaları konusunda yönlendirme yapıyorum", ÖOÖT3 "konusu geçtiği zaman yönlendire yapıyorum" diyerek cevap vermişlerdir. Devlet okulunda ortaokul düzeyinde görev yapan DOÖT1 "olumsuz örnekleri, haberleri işte videoları vb. gündeme getirip dersin içerisinde bilgilendirme ve farkındalık oluşturuyoruz", DOÖT2 "hayır, hiç olmadı", DOÖT3 "tabii yönlendiriyorum" diyerek fikirlerini ortaya koymuşlardır. Özel okulda lise düzeyinde görev yapan ÖLÖT1 konusu açıldıkça bilgilendirdiğini ifade etmiş, ÖLÖT2 "yapmadım kendim de yapmıyorum", ÖLÖT3 "tanımadığınız kişiler yazarsa cevap vermek zorunda değilsiniz" şeklinde uyarılarda bulunduğunu belirtmişlerdir. Devlet okulunda lise düzeyinde görev yapan DLÖT1 "konu geçerse bilgilerimi aktarmaya çalışıyorum", DLÖT2 "bu konuda bir soru olduğu zaman cevap veriyorum" şeklinde yanıt verirken, DLÖT3 öğrencilerden bir paylaşım gelirse bilgi birikimi doğrultusunda bilgilendirme yaptığını ifade etmiştir.

4.3 Okul Yöneticilerinin Bilgi Güvenliği Farkındalık Düzeyleri ve Bu Konuya İlişkin Görüşleri

Araştırma kapsamında yer alan 4 okul yöneticisine demografik bilgi anketi ve bilgi güvenliği farkındalık ölçeği uygulanmış, ayrıca 4 okul yöneticisi ile yüz yüze görüşme de yapılmıştır. Elde edilen verilerden ulaşılan bulgular aşağıda yer alan başlıklarda altında açıklanmıştır.

4.3.1 Okul Yöneticilerinin Bilgi Güvenliği Farkındalık Düzeyleri

Araştırmada yer alan okul yöneticilerinin (n=4) BGFÖ puan ortalamaları değerlendirildiğinde, genel güvenlik alt boyutu ortalamasının 50,75±8,88, saldırı ve tehditler alt boyutu ortalamasının 56,00±17,21, mobil cihazlar, mahremiyet ve iletişim alt boyutu ortalamasının 64,25±22,63, BGFÖ genel puan ortalamasının 171,00±48,45 olduğu görülmektedir (Tablo 4.35).

Tablo 4.35 Okul Yöneticilerinin BGFÖ Puanlarına İlişkin Betimsel İstatistikler

Alt Boyutlar	n	$\overline{X}$	ss	Max	Min
Genel Güvenlik	4	50,75	8,88	65	13
Saldırı ve Tehditler	4	56,00	17,21	85	17
Mobil Cihazlar, Mahremiyet ve İletişim	4	64,25	22,63	90	18
BGFÖ genel puan	4	171,00	48,45	240	48

Araştırmada yer alan okul yöneticilerinin (n=4) BGFÖ puan ortalamaları değerlendirildiğinde, genel güvenlik alt boyutunda özel okulda lise düzeyindeki okul yöneticisinin, saldırı ve tehditler alt boyutunda özel okulda ortaokul düzeyindeki okul yöneticisinin, mobil cihazlar, mahremiyet ve iletişim alt boyutunda özel okulda ortaokul düzeyindeki okul yöneticisinin, ölçek genel puanlarında ise özel okulda ortaokul düzeyindeki okul yöneticisinin en yüksek puanı aldığı ve farkındalık düzeyinin en yüksek olan okul yöneticisi olduğu tespit edilmiştir. Bu bulgulara ve tablo 4.36'ya göre özel okulda görev yapan okul yöneticilerinin devlet okulunda görev yapan okul yöneticilerine göre farkındalık düzeylerinin daha yüksek olduğu görülmektedir.

Tablo 4.36 Okul Yöneticilerinin Okul Türü ve Okul Düzeyine Göre BGFÖ Puan Tablosu

Alt Boyutlar			**Puan**
Genel Güvenlik	Özel Okul	Ortaokul	57
		Lise	59
	Devlet Okulu	Ortaokul	47
		Lise	40
Saldırı ve Tehditler	Özel Okul	Ortaokul	74
		Lise	66
	Devlet Okulu	Ortaokul	48
		Lise	36
Mobil Cihazlar, Mahremiyet ve İletişim	Özel Okul	Ortaokul	84
		Lise	81
	Devlet Okulu	Ortaokul	56
		Lise	36
BGFÖ genel puan	Özel Okul	Ortaokul	215
		Lise	206
	Devlet Okulu	Ortaokul	151
		Lise	112

4.3.2 Okul Yöneticilerinin Bilgi Güvenliği Farkındalığına Yönelik Görüşleri

Çalışmaya katılan 4 okul yöneticisi ile yarı yapılandırılmış görüşme sorularıyla yüz yüze görüşme gerçekleştirilmiştir. Görüşmede okul yöneticilerine 13 adet soru yöneltilmiştir. Okul yöneticilerinin görüşme esnasında verdikleri cevaplar analiz edilmiştir.

Kaç yıldır öğretmenlik mesleğini icra ediyorsunuz sorusuna; özel okulda ortaokul düzeyinde okul yöneticiliği yapan ÖOOY 8 yıldır, devlet okulunda ortaokul düzeyinde okul yöneticiliği yapan DOOY 20 yıldır, özel okulda lise düzeyinde okul yöneticiliği yapan ÖLOY 34 yıldır, devlet okulunda lise düzeyinde okul yöneticiliği yapan DLOY 15 yıldır cevabını vermişlerdir.

Kendinize ait bilgisayar, cep telefonu, tablet vb. teknolojik cihazlarınız var mı sorusunu; özel okulda ortaokul düzeyinde okul yöneticiliği yapan ÖOOY bilgisayar ve cep telefonu, devlet okulunda ortaokul düzeyinde okul yöneticiliği yapan DOOY masaüstü bilgisayar, diz üstü bilgisayar, cep telefonu ve tablet, özel okulda lise düzeyinde okul yöneticiliği yapan ÖLOY diz üstü bilgisayar ve cep telefonu, devlet okulunda lise düzeyinde okul yöneticiliği yapan DLOY bilgisayar, cep telefonu ve tablet sahibi oldukları yönünde yanıtlamışlardır.

Eğer varsa teknolojik cihazları (tablet, cep telefonu vb.) hangi amaçlar (haberleşme, oyun, sohbet/chat, iş, e-devlet vb.) doğrultusunda kullanıyorsunuz sorusuna; özel okulda ortaokul düzeyinde okul yöneticiliği yapan ÖOOY oyun oynamak, e-mail ile haberleşmek, iş ve çaldığı enstrüman için, devlet okulunda ortaokul düzeyinde okul yöneticiliği yapan DOOY iş, haberleşmek, bankacılık işlemleri ve sosyal medyada gezinmek için, özel okulda lise düzeyinde okul yöneticiliği yapan ÖLOY iş, haberleşmek ve e-mailleri incelemek için, devlet okulunda lise düzeyinde okul yöneticiliği yapan DLOY iş, haberleşme ve devlet işleri için kullandıklarına dair açıklama yapmışlardır.

Bilgi güvenliği kavramını daha önce duydunuz mu? Bu konuda bir bilginiz var mı sorusunda; özel okulda ortaokul düzeyinde okul yöneticiliği yapan ÖOOY bilgisi olduğunu, bu konu ile ilgili bir seminere gittiğini söylemiştir. Devlet okulunda ortaokul düzeyinde okul yöneticiliği yapan DOOY bilgisi olduğunu bilginin güvenliğinin, bilginin saklanma koşullarının son derece önemli olduğunu bu doğrultuda mümkün olduğunca uygulamaları gerçekleştirmeye çalıştığını dile getirmiştir. Özel okulda lise düzeyinde okul yöneticiliği yapan ÖLOY bilgi güvenliği kavramını duyduğunu, okul kapsamında bu konuya yönelik bir kulüp kurulduğunu belirtmiştir. Devlet okulunda lise düzeyinde okul yöneticiliği yapan DLOY "duymadım, ama kişisel verilerin korunumu durumunu biliyorum..ama tam olarak bu kavram ile ilgili bilgim yok" diyerek soruya yanıt vermiştir.

Eğer varsa evinizde kullandığınız teknolojik cihazlarda antivirüs yazılım mevcut mu? Antivirüs programlarının gerekliliği hakkında neler düşünüyorsunuz sorusunda; özel okulda ortaokul düzeyinde okul yöneticiliği yapan ÖOOY teknolojik cihazlarında söz konusu programların mevcut olduğunu, çok fazla dosya indiren, kaynağı belli olmayan sitelerden film vb. indirmeler yapan kişilerin mutlaka

kullanması gerektiğini ifade etmiştir. Çerezler, casus yazılımların çok fazla olduğunu, e-maillerde eklerde de virüs olabildiğini belirtip antivirüs programlarının önemli olduğunu söylemiştir. Devlet okulunda ortaokul düzeyinde okul yöneticiliği yapan DOOY kullandığı teknolojik cihazlarda antivirüs programlarının mevcut olduğunu, antivirüs programlarının işlevselliğine yönelik olarak her programın amaca hitap etmediğini düşünmekle birlikte son derece gerekli olduğunu ifade edip, bilgisayarda ilk uyarıyı antivirüs programlarının verdiğini ve bu şekilde saldırılara karşı önlemler alınabildiğini dile getirmiştir. Özel okulda lise düzeyinde okul yöneticiliği yapan ÖLOY kullandığı cihazlarda antivirüs programı olduğunu ve bu programın son derece gerekli olduğunu düşündüğünü belirtmiştir. Devlet okulunda lise düzeyinde okul yöneticiliği yapan DLOY antivirüs programının bilgisayarında mevcut olduğunu, bu programın bilgisayarı virüslerden korumak için kullandığı ama konu ile ilgili başka bir bilgisi olmadığını ifade etmiştir.

Eğer varsa bilgisayarınızda şifresi kaldırılmış (cracklenmiş) program kullanıyor musunuz? Bu şekilde lisanssız program kullanmanın zararları hakkındaki yorumunuz nedir sorusuna; özel okulda ortaokul düzeyinde okul yöneticiliği yapan ÖOOY önceden var olduğunu ama artık çoğunlukla lisanslı kullandığını, lisanssız ürünlerde programı tüm özellikleri ile kullanmanın söz konusu olmayabildiğini, ayrıca hem çok sık güncelleme yapmak gerektiği hem virüs tehlikesi ile karşı karşıya kalındığını dile getirmiştir. Devlet okulunda ortaokul düzeyinde okul yöneticiliği yapan DOOY böyle bir program kullanmadığını, lisanssız ürün kullanmanın garantisi olmayan ikinci el bir ürün kullanmak gibi olduğunu düşündüğünü belirtmiştir. Özel okulda lise düzeyinde okul yöneticiliği yapan ÖLOY lisanssız program kullanmadığını belirtmiş ve bu durumu haksız bir kullanım olarak nitelendirmiştir. Devlet okulunda lise düzeyinde okul yöneticiliği yapan DLOY "lisanssız program kullanıp kullanmadığımı bilmiyorum ama genelde kullanmıyorum diye biliyorum" diyerek ve bu programlar ile virüslere karşı bilgisayarın korunmasında problem olabileceğini dile getirip soruyu yanıtlamıştır.

Herhangi bir sosyal medya hesabına üye misiniz sorusunda; özel okulda ortaokul düzeyinde okul yöneticiliği yapan ÖOOY şu an için herhangi bir sosyal medya hesabına üyeliğinin bulunmadığını ama geçmişte kullanmış olduğunu belirtmiştir. Devlet okulunda ortaokul düzeyinde okul yöneticiliği yapan DOOY

üyeliklerinin olduğunu, özel okulda lise düzeyinde okul yöneticiliği yapan ÖLOY twitter ve instagram, devlet okulunda lise düzeyinde okul yöneticiliği yapan DLOY ise facebook, instagram ve twitter üyeliklerinin olduğunu ifade etmişlerdir.

Sosyal medya kullanımının ve İnternet'in zararlı yönleri konusunda gündemi takip eder misiniz sorusuna; özel okulda ortaokul düzeyinde okul yöneticiliği yapan ÖOOY "gündemi takip ederim..hem gerekli önlemleri alabilmek için hem de mesleğimiz doğrultusunda öğrencileri doğru bir şekilde yönlendirebilmek için gündemi takip ederim" cevabını vermiştir. Devlet okulunda ortaokul düzeyinde okul yöneticiliği yapan DOOY "hem kendim çocuk sahibi olduğum için hem de öğrencilerimin sorumluluğunu taşıdığım için takip etmek durumundayım" sözleri ile gündemi takip ettiğini ifade etmiştir. Özel okulda lise düzeyinde okul yöneticiliği yapan ÖLOY ve devlet okulunda lise düzeyinde okul yöneticiliği yapan DLOY gündemi takip ettiklerini dile getirmişlerdir.

Sosyal medya kullanımının ve İnternet'in zararlı yönleri konusunda öğrencilerinizi bilgilendirir misiniz sorusuna; özel okulda ortaokul düzeyinde okul yöneticiliği yapan ÖOOY bilgilendirdiği yönünde yanıt vermiştir. Devlet okulunda ortaokul düzeyinde okul yöneticiliği yapan DOOY "siber suçlar, bilgisayar kullanımı, şifreler, hackerlar bu işten gelebilecek zararlarla ilgili öğrencilerimizi 2 defa toplu olarak seminer hazırladık bilgilendirdik..birbirlerine akran zorbalığının siber suçlarla bağlantısı, çünkü cep telefonu üzerinden yapılan bir takım şeyler var, bu konularda özellikle il emniyet müdürlüğünden gelen ekipler tarafından çok detaylandırılmış örnek çalışmayla öğrencilerimizi bilgilendirdik" diyerek soruyu cevaplamıştır. Özel okulda lise düzeyinde okul yöneticiliği yapan ÖLOY "bilgilendiriyoruz ve konu ile ilgili farkındalık çalışmaları yapıyoruz" şeklinde açıklama yapmıştır. Devlet okulunda lise düzeyinde okul yöneticiliği yapan DLOY ise öğrencileri bilgilendirmeye ve aşırı kullanımı önlemeye çalıştıklarını ifade etmiştir.

Hiç sosyal medya ya da İnternet aracılığıyla dolandırıldınız mı sorusuna; devlet okulunda ortaokul düzeyinde okul yöneticiliği yapan DOOY ve özel okulda lise düzeyinde okul yöneticiliği yapan ÖLOY hayır cevabını vermişlerdir. Özel okulda ortaokul düzeyinde okul yöneticiliği yapan ÖOOY kendi başına böyle bir olay gelmediğini ancak arkadaşının kredi kartı bilgilerinin oyun aracılığıyla çalındığını ifade etmiştir. Devlet okulunda lise düzeyinde okul yöneticiliği yapan DLOY

“dolandırıldım, arkadaşımın hesabı çalınmış, samimi bir arkadaşım…gelen mesajlara evet yanıtını verince hesabımdan para çekilmiş oldu” diyerek soruyu yanıtlamıştır.

Hiç sosyal medya ya da elektronik posta hesaplarınız başkaları tarafından ele geçirildi mi sorusuna tüm öğretmenler hayır cevabını vermiştir.

Sosyal medya kullanımının ve İnternet’in zararlı yönlerine yönelik olarak ne gibi önlemler alınmalı? Siz bu konuda herhangi bir önlem alıyor musunuz sorusuna; özel okulda ortaokul düzeyinde okul yöneticiliği yapan ÖOOY “sosyal medya hesabı kullanmıyorum, çünkü ordaki dosyaların kolay ulaşılabilir olduğunu düşünüyorum ve bir siteye üye olurken istenen bilgilere bakıyorum benden neler isteniyor eğer benden çok özel bilgiler istiyor ise kesinlikle o siteye üyelik filan yapmıyorum…güncelleme yapıyorum, tarama yapıyorum” sözleri ile yanıt vermiştir. Devlet okulunda ortaokul düzeyinde okul yöneticiliği yapan DOOY konu ile ilgili olarak kullanıcıların kullandıkları cihaz veya programa yönelik bilgi sahibi olmaları gerektiğini ve gelebilecek tehditlere karşı her an tetikte olunmasının önemli olduğunu ifade etmiştir. Bununla birlikte toplumsal açıdan alınabilecek önlemler kapsamında kamu spotu yayınlarının artırılmasının faydalı olabileceğini söylemiştir. Özel okulda lise düzeyinde okul yöneticiliği yapan ÖLOY zaman kaybına ve algı yönetimine yönelik daha dikkatli kullanmaya çalıştığını ifade etmiştir. Devlet okulunda lise düzeyinde okul yöneticiliği yapan DLOY antivirüs programlarının gizlilik özelliklerini uyguladığını belirtip, “gün içerisinde gelebilecek telefona, mesajlara karşı uyanık olmak gerek” diyerek düşüncelerini açıklamıştır.

Sosyal medya kullanımının ve İnternet’in zararlı yönlerine yönelik olarak alınması gereken önlemler konusunda öğrencilerinizi yönlendiriyor musunuz sorusuna; özel okulda ortaokul düzeyinde okul yöneticiliği yapan ÖOOY “sosyal medyada konuştuğunuz kişiler gerçekte o kişiler olmayabilir, kendiniz gibi olun ve tanımadığınız kişilerle iletişime geçmeyin” diyerek yönlendirmede bulunduğunu dile getirmiştir. Devlet okulunda ortaokul düzeyinde okul yöneticiliği yapan DOOY okul içerisinde kullanılan internet ağının MEB serverı üzerinden aldıklarını ve okulda cep telefonu kullanımının yasak olduğunu belirtip okul sınırları içinde alınan önlemleri açıklamıştır. Okul dışındaki kullanım konusunda da öğrencilere bilgilendirme seminerleri yapıldığını belirtmiştir. Özel okulda lise düzeyinde okul yöneticiliği yapan ÖLOY “pano çalışmaları yapıyoruz sınıflarda…seminerler düzenliyoruz hatta bu

seminerleri bizzat öğrenciler veriyor…doğru kullanıma yönelik eğitimler veriyoruz" diyerek soruyu cevaplandırmıştır. Devlet okulunda lise düzeyinde okul yöneticiliği yapan DLOY fazla kullanım ve alışkanlıklar konusunda uyardıklarını belirtmiştir.

4.4 Velilerin Bilgi Güvenliği Farkındalığına Yönelik Görüşleri

Araştırma kapsamında yer alan 12 veli ile yarı yapılandırılmış görüşme sorularıyla yüz yüze görüşme gerçekleştirilmiştir. Görüşmede velilere 12 adet soru yöneltilmiştir. Velilerin görüşme esnasında verdikleri cevaplar analiz edilmiştir.

Kaç çocuğunuz var sorusunu; özel okulda ortaokul düzeyinde öğrenim gören çocuğu olan velilerden ÖOV1 bir, ÖOV2 bir, ÖOV3 iki çocuk sahibi oldukları şeklinde cevaplamışlardır. Devlet okulunda ortaokul düzeyinde öğrenim gören çocuğu olan velilerden DOV1 bir, DOV2 iki, DOV3 iki çocuğu olduğunu; özel okulda lise düzeyinde öğrenim gören çocuğu olan velilerden ÖLV1 iki, ÖLV2 iki, ÖLV3 iki çocuğu olduğunu; devlet okulunda lise düzeyinde öğrenim gören çocuğu olan velilerden DLV1 üç, DLV2 iki, DLV3 iki çocuğu olduğunu belirtmiştir.

Evinizde bilgisayar var mı? Varsa, hangi odada/odalarda bulunmaktadır sorusunda; özel okulda ortaokul düzeyinde öğrenim gören çocuğu olan velilerden ÖOV1 3 adet bilgisayar ve 1 adet tabletin yer aldığını ve hepsinin çalışma odasında bulunduğunu, ÖOV2 1 adet bilgisayar olduğunu ve bilgisayarın çocuğunun odasında yer aldığını, ÖOV3 2 adet diz üstü bilgisayar olduğunu ve genellikle salonda olduğunu belirtmiştir. Devlet okulunda ortaokul düzeyinde öğrenim gören çocuğu olan velilerden DOV1 1 adet bilgisayar olduğunu ve bilgisayarın salonda yer aldığını, DOV2 bilgisayarın çocuk odasında bulunduğunu, DOV3 ise evlerinde bilgisayar olmadığını ifade etmiştir. Özel okulda lise düzeyinde öğrenim gören çocuğu olan velilerden ÖLV1 evlerinde bir adet bilgisayar olduğunu ve bu bilgisayarın salonda durduğunu, ÖLV2 bilgisayarın salonda yer aldığını, ÖLV3 bilgisayarın çocukların kendi odasında bulunduğunu söylemiştir. Devlet okulunda lise düzeyinde öğrenim gören çocuğu olan velilerden DLV1 ve DLV2 evlerinde bilgisayar olmadığını, DLV3 ise bilgisayar olduğunu ve çocuk odasında ortak kullanıldığını dile getirmiştir.

Çocuğunuzun/çocuklarınızın kendisine ait tableti, cep telefonu veya bilgisayarı var mı sorusuna; özel okulda ortaokul düzeyinde öğrenim gören çocuğu olan velilerden ÖOV1 "hayır evde olan her bilgisayarın ailemize ait olduğu kavramını ona verdik" diyerek açıklama yaparken, ÖOV2 çocuğuna ait bir tablet olduğunu, bilgisayar

ve cep telefonunu kendisinden alıp kullandığını, ÖOV3 ise şu an için çocuklarının kendisine ait teknolojik cihazları olmadığı yönünde cevap vermişlerdir. Devlet okulunda ortaokul düzeyinde öğrenim gören çocuğu olan velilerden DOV1 çocuğunun cep telefonu, tableti ve bilgisayarı olduğunu, DOV2 kızının diz üstü bilgisayarı ve cep telefonu olduğunu, bunun dışında evde çocuklarına ait 4 adet tablet yer aldığını, DOV3 ise çocuklarının cep telefonları olduğunu ifade etmiştir. Özel okulda lise düzeyinde öğrenim gören çocuğu olan velilerden ÖLV1 çocuklarının kendisine ait tablet ve cep telefonları olduğunu, ÖLV2 çocuklarının bir tablet ve iki cep telefonu olduğunu, ÖLV3 ise çocuklarının bilgisayarı, cep telefonu ve tableti olduğunu söylemiştir. Devlet okulunda lise düzeyinde öğrenim gören çocuğu olan velilerden DLV1 çocuklarının cep telefonu olduğunu, DLV2 sadece büyük çocuğunun cep telefonu olduğunu, DLV3 ise büyük kızının kendisine ait cep telefonu olduğunu dile getirmiştir.

Eğer varsa çocuğunuzun/çocuklarınızın bilgisayarında, cep telefonunda ya da tabletinde yaptıklarını hangi sıklıkta incelersiniz sorusuna; özel okulda ortaokul düzeyinde öğrenim gören çocuğu olan velilerden ÖOV1 "kontrol ediyorum, benim gözetimimde kullanıyor" şeklinde yanıt verirken, ÖOV2 çocuğunun kullandığı cihazları her gün incelediğini, ÖOV3 bazen çocuklarının gelip kendilerinin gösterdiğini bazen de kendisinin yanlarına gidip kontrol ettiğini ifade etmiştir. Devlet okulunda ortaokul düzeyinde öğrenim gören çocuğu olan velilerden DOV1 ortalama haftada bir kez kontrol ettiğini, DOV2 devamlı kontrol ettiğini, DOV3 çocuklarının telefonlarını kendisine göstermediğini belirtmiştir. Özel okulda lise düzeyinde öğrenim gören çocuğu olan velilerden ÖLV1 ara ara kontrol ettiğini, ÖLV2 sıklıkla incelediğini, ÖLV3 haftada bir takip ettiğini dile getirmiştir. Devlet okulunda lise düzeyinde öğrenim gören çocuğu olan velilerden DLV1 bazen baktığını, DLV2 her gün kontrol ettiğini, DLV3 günlük takip ettiğini söylemiştir.

Eğer varsa çocuğunuzun/çocuklarınızın bilgisayarı hangi amaçla kullandığı ve bilgisayarda hangi programları kullandığı hakkında bilgi sahibi misiniz sorusuna; özel okulda ortaokul düzeyinde öğrenim gören çocuğu olan velilerden ÖOV1 ve ÖOV3 bilgi sahibi olduklarını belirtirken, ÖOV2 de "biliyorum ve bu konuda bilgisayar öğretmenlerinden ve babasından destek alıyorum" diyerek yanıt vermiştir. Devlet okulunda ortaokul düzeyinde öğrenim gören çocuğu olan velilerden DOV1 bilgi sahibi olduğunu, DOV2 kızının cep telefonunu zaman zaman kullandığı için kontrol etmiş

olduğunu, diz üstü bilgisayarı ise çocuklarının sadece ödev yapmak için kullandıklarını, DOV3 ise bilgi sahibi olmadığını ifade etmiştir. Özel okulda lise düzeyinde öğrenim gören çocuğu olan veliler ÖLV1, ÖLV2, ÖLV3 ile devlet okulunda lise düzeyinde öğrenim gören çocuğu olan veliler DLV1, DLV2, DLV3 bu konuda bilgi sahibi olduklarını söylemişlerdir.

Bilgi güvenliği kavramını daha önce duydunuz mu? Bu konuda bir bilginiz var mı sorusuna; özel okulda ortaokul düzeyinde öğrenim gören çocuğu olan velilerden ÖOV1 "duydum…ulaşılabilecek her bilginin doğru olup olmadığını kontrol edebilmemiz ya da ben herhangi bir bilgiye ulaşırken doğru kanalları kullanabilmeliyim", ÖOV2 "duydum…interneti doğru kullanmak doğru sitelere girmek" şeklinde yanıt verirken, ÖOV3 duyduğunu ama içeriğini pek bilmediğini belirtmiştir. Devlet okulunda ortaokul düzeyinde öğrenim gören çocuğu olan velilerden DOV1 bu kavramı gerek sosyal medya gerekse okulda öğretmenlerin bilgilendirmesi aracılığıyla duyduğunu belirtmiş ve bu kavramı "size ait olan bilgilerin paylaşılmaması…farkında olmadan bu bilgileri başkasının ele geçirmesi" şeklinde açıklamış, DOV2 duymadığını ve bilgisi olmadığını, DOV3 kavramı daha önce duyduğunu ama ne anlam ifade ettiğini bilmediğini ifade etmiştir. Özel okulda lise düzeyinde öğrenim gören çocuğu olan velilerden ÖLV1 bilgi güvenliği kavramını duyduğunu, ÖLV2 söz konusu kavramı duyduğunu fakat çok detaylı bilgi sahibi olmadığını, ÖLV3 ise bu kavramı daha önce hiç duymadığını dile getirmiştir. Devlet okulunda lise düzeyinde öğrenim gören çocuğu olan velilerden DLV1 ve DLV3 bilgi güvenliği kavramını hiç duymadığını, DLV2 ise duyduğunu ama bilgi sahibi olmadığını söylemiştir.

Eğer varsa evinizde kullandığınız teknolojik cihazlarda antivirüs programı mevcut mu? Antivirüs programlarının gerekliliği hakkında neler düşünüyorsunuz sorusuna; özel okulda ortaokul düzeyinde öğrenim gören çocuğu olan velilerden ÖOV1 "mevcut olması gerektiğini düşünüyorum ama devamlı kontrolünü yapamadığım için şu an için makinalarımda yüklü değil" ve "cihazların bozulmasına, kullanım sıkıntıları yaşamasına neden olabiliyor virüsler" diyerek açıklama yaparken, ÖOV2 teknolojik cihazlarında antivirüs programının mevcut ve güvenlik için gerekli olduğunu, ÖOV3 antivirüs programının yüklü olduğunu, bu programın virüslerden korunmak için gerekli olduğunu ama çok fazla bilgi sahibi olmadığını dile getirmiştir.

Devlet okulunda ortaokul düzeyinde öğrenim gören çocuğu olan velilerden DOV1 bilgisayarda antivirüs programının olmadığını, cep telefonu ve tablette antivirüs programının yüklü olduğunu belirtip, programın gerekli olduğunu fakat yeterli düzeyde koruma sağladığını düşünmediğini açıklamış, DOV2 söz konusu programın yüklü olduğunu ve programın kullanılan cihazdaki virüsleri temizlediğini ifade etmiş, DOV3 ise antivirüs programının olduğunu, programın virüs girmemesi için gerekli olduğunu söylemiştir. Özel okulda lise düzeyinde öğrenim gören çocuğu olan velilerden ÖLV1 söz konusu programın yüklü olduğunu, programın sakıncalı şeylerin teknolojik cihazları çökertmemesi açısından gerekli olduğunu, ÖLV2 antivirüs programının olmadığını ve herhangi bir bilgi sahibi olmadığını, ÖLV3 cihazlarında antivirüs programının yüklü olduğunu, flash belleklerde olan ve bilgisayara gelen virüsleri temizlemek için söz konusu programın gerekli olduğunu düşündüğünü ifade etmiştir. Devlet okulunda lise düzeyinde öğrenim gören çocuğu olan velilerden DLV1 antivirüs programının yüklü olduğunu ama gerekliliği ile ilgili fikri olmadığını, DLV2 cihazlarında antivirüs programının mevcut olup, istemsizce yüklenen olumsuz uygulamaları temizlemek için programın gerekli olduğunu, DLV3 ise programın yüklü olduğunu ancak detaylı bilgisi olmadığını, eşi daha iyi bildiği için eşinin takip ettiğini ifade etmiştir.

Sosyal medya kullanımının ve İnternet'in zararlı yönleri konusunda gündemi takip eder misiniz sorusuna; özel okulda ortaokul düzeyinde öğrenim gören çocuğu olan velilerden ÖOV1 sıklıkla kontrol etmeye çalıştığını, ÖOV2 takip ettiğini, ÖOV3 özellikle takip etmediğini denk gelirse baktığını ifade etmiştir. Devlet okulunda ortaokul düzeyinde öğrenim gören çocuğu olan veliler DOV1, DOV2, DOV3 ile özel okulda lise düzeyinde öğrenim gören çocuğu olan veliler ÖLV1, ÖLV2, ÖLV3 gündemi takip ettiklerini belirtmişlerdir. Devlet okulunda lise düzeyinde öğrenim gören çocuğu olan velilerden DLV1 gündemi takip etmediğini DLV2 ara sıra takip ettiğini, DLV3 ise fırsat buldukça takip ettiğini dile getirmişlerdir.

Sosyal medya kullanımının ve İnternet'in zararlı yönleri konusunda çocuğunuzu/çocuklarınızı bilgilendirir misiniz sorusuna; özel okulda ortaokul düzeyinde öğrenim gören çocuğu olan velilerden ÖOV1 "gündemi takip ettiğim doğrultuda ailemi de bilgilendiririm", ÖOV2 "sürekli konuşup bilgilendiriyorum", ÖOV3 "mümkün olduğunca konu ile ilgili çocuklarımla konuşuyorum" diyerek yanıt

vermişlerdir. Devlet okulunda ortaokul düzeyinde öğrenim gören çocuğu olan velilerden DOV1 ve DOV2 bilgilendirme yaptıklarını, DOV3 ise bilgilendirdiğini ama bir faydası olmadığını düşündüğünü açıklanmıştır. Özel okulda lise düzeyinde öğrenim gören çocuğu olan velilerden ÖLV1 bu konuda sürekli uyardığını ve bilgilendirdiğini, ÖLV2 ve ÖLV3 bilgilendirdiğini ifade etmişlerdir. Devlet okulunda lise düzeyinde öğrenim gören çocuğu olan veliler DLV1, DLV2 ve DLV3 çocuklarına konu ile ilgili bilgilendirme yaptıklarını söylemişlerdir.

Hiç sosyal medya ya da İnternet aracılığıyla dolandırıldınız mı sorusuna velilerin hepsi hayır yanıtını vermiştir.

Hiç sosyal medya ya da elektronik posta hesaplarınız başkaları tarafından ele geçirildi mi sorusunu, velilerin hepsi hayır diyerek cevaplamışlardır.

Sosyal medya ve İnternet kullanımının zararlarından kendinizi ve çocuğunuzu/çocuklarınızı korumak için ne gibi önlemler alıyorsunuz? Bu konuda kullandığınız programlar var mı sorusuna; özel okulda ortaokul düzeyinde öğrenim gören çocuğu olan velilerden ÖOV1 "özellikle tanımadığım kişilerle hiçbir şekilde iletişime geçmiyorum gönderilen mailleri kontrol ediyorum..yada gelen linklerin uzantılarını kontrol etmeye çalışıyorum" ve ÖOV2 "önlem almak için kendi telefonumdan kendisine instagram hesabı açtım..kimlerle görüştüğünü kontrol ediyorum..girdiği siteleri takip ediyorum" diyerek yanıt verirken, ÖOV3 çocuk kilidi gibi bir programı eşinin bilgisayara yüklediğini bu programın çocuklara bir takım sınırlamalar getirdiğini ifade etmiştir. Devlet okulunda ortaokul düzeyinde öğrenim gören çocuğu olan velilerden DOV1 çocuğuna yönelik önlem olarak zaman kısıtlaması yaptığını ve hangi amaçlarla kullandığı takip ettiğini, DOV2 nasıl bir önlem alacağımı bilmediğini sadece kontrol ettiğini ve oğluna zaman kısıtlaması koyduğunu, DOV3 ise herhangi bir önlem almadığını belirtmiştir. Özel okulda lise düzeyinde öğrenim gören çocuğu olan velilerden ÖLV1 kendilerinin ve çocuklarının bu konu hakkında bilinçli olduğunu, ÖLV2 bilmediği sitelere girmediğini, güvenli olmayan sitelerden alışveriş yapmadığını çocuklarının da bilgisayar ve tableti olumsuz yönde kullanmadığını, ÖLV3 çocuklarına sözlü olarak uyarılarda bulunduğu, bilmedikleri, güvenmedikleri sitelere girmemelerini ve bu gibi sitelerde herhangi bir bilgi paylaşımında bulunmamalarını söylediğini, bunun dışında bir önlem almadığını dile getirmiştir. Devlet okulunda lise düzeyinde öğrenim gören çocuğu olan velilerden DLV1 herhangi

bir önlem almadıklarını, DLV2 çocuğuna farklı bir mesaj geldiğini kesinlikle bunları açmaması gerektiğini, virüs taraması yapması gerektiğini söylediklerini kendilerinin bu şekilde bir tutum sergilediklerini, DLV3 çocuklarını uyardıklarını, eşinin telefon ve bilgisayarı kontrol ettiğini, zaman ve kullanılan program açısından devamlı takip ettiklerini söylemişlerdir.

BÖLÜM V
SONUÇ, TARTIŞMA VE ÖNERİLER

Tartışma

Bu bölümde yapılan araştırmada elde edilen bulgular ile literatürde yer alan çalışmalar değerlendirilmiştir.

Araştırmada yer alan öğrencilerin (n=200) BGFÖ puanları incelendiğinde, kişisel verilerin korunması alt boyutu ortalamasının 23,02±5,53, saldırı ve tehditler alt boyutu ortalamasının 52,97±19,40, mahremiyet alt boyutu ortalamasının 39,17±10,37, BGFÖ genel puan ortalamasının 115,15±30,48 olduğu görülmektedir (Tablo 4.10). Bunun yanı sıra öğrencilerin (n=200) okul türüne göre BGFÖ puan ortalamaları değerlendirildiğinde, kişisel verilerin korunması alt boyutu ve mahremiyet alt boyutunda özel okul ve devlet okulunda öğrenim gören öğrenciler arasında (Tablo 4.15), lisede öğrenim gören öğrencilerin (n=100) okul türüne göre BGFÖ puan ortalamaları değerlendirildiğinde, kişisel verilerin korunması alt boyutu ve mahremiyet alt boyutunda özel okul ve devlet okulunda öğrenim gören öğrenciler arasında (Tablo 4.17), öğrencilerin (n=200) okul düzeyine göre BGFÖ puan ortalamaları değerlendirildiğinde, kişisel verilerin korunması alt boyutunda ortaokul ve lisede öğrenim gören öğrenciler arasında, okul düzeyine göre BGFÖ puan ortalamaları değerlendirildiğinde, kişisel verilerin korunması ve mahremiyet alt boyutunda ortaokul ve lisede öğrenim gören öğrenciler arasında (Tablo 4.12) ve devlet okulunda öğrenim gören öğrencilerin (n=100) okul düzeyine göre BGFÖ puan ortalamaları değerlendirildiğinde, kişisel verilerin korunması ve mahremiyet alt boyutunda ortaokul ve lisede öğrenim gören öğrenciler arasında (Tablo 4.14) istatistiksel olarak anlamlı fark olduğu tespit edilmiştir ($p<0,05$). Elde edilen verilere göre okul türüne göre özel okulda, okul düzeyine göre ise ortaokulda öğrenim gören öğrencilerin farkındalık düzeylerinin daha yüksek olduğu görülmüştür.

Nitel verilere bakıldığında görüşme yapılan öğrencilerden (n=12) DOÖ1, ÖLÖ1 ve ÖLÖ2 bilgi güvenliği kavramını duyduklarını söyleyip tanımlama yapmışlardır. Öğrencilerin hepsi teknolojik cihazlarının hepsinde veya bazılarında antivirüs programı kullandıklarını belirtirken, antivirüs programının gerekliliğine yönelik virüslerden bilgisayarı koruma amacı taşıdığını söylemişlerdir. Yalnız devlet okulunda lise düzeyinde öğrenim gören bir öğrenci (DLÖ2) konu ile ilgili hiç bilgi

sahibi olmadığını ifade etmiştir. Lisanssız program kullanımına yönelik olarak hiçbir öğrenci böyle program kullanmadığını dile getirirken, bu programların olumsuz yönlerine dair DOÖ1, DOÖ2, ÖLÖ1, DLÖ2 herhangi bir fikir sahibi olmadıklarını belirtmişlerdir. Sosyal medya kullanımının ve İnternet'in zararlı yönlerine yönelik yapılan açıklamalarda ise öğrenciler (n=12) içerisinde en geniş açıklamayı ÖLÖ3'ün yaptığı görülmüştür. Söz konusu duruma karşı alınabilecek önlemler ile ilgili ise öğrenciler, ağırlıklı olarak güçlü şifre kullanımı ve tanımadıkları kişilerle konuşmama yönünde cevaplar vermişlerdir. Sadece DLÖ1 önleme gerek olmadığını, önlem alınsa bile sorunlarla karşılaşılabileceğini söylemiştir.

Elde edilen bulgulara bakıldığında, nicel verilerden ulaşılan özel okuldaki öğrencilerin farkındalık düzeylerinin daha yüksek olduğu sonucunun nitel verilerle desteklenebileceği görülmüştür. Ortaokul ve lise düzeyinde öğrenim gören öğrenciler arasındaki farkındalık düzeyi farklılığına yönelik ise sonuçların birbirini tam olarak desteklemediği görülmüştür. Görüşmeler rastgele seçilen öğrenciler ile yapılmış olup her öğrencinin bilgisi ve düşünceleri birbirinden farklı olacağı için bu gibi farklılıkların olabileceği düşünülmektedir. Her öğrencinin hem ölçeği doldurması hem de görüşme yapması durumunda veya daha fazla sayıda yapılacak görüşme ile daha net bir sonuca ulaşılabileceği öngörülmektedir.

Çalışmaya katılan öğrencilerin (n=200) cinsiyete göre BGFÖ puan ortalamaları değerlendirildiğinde, saldırı ve tehditler alt boyutunda kadın ve erkek öğrenciler arasında istatistiksel olarak anlamlı fark olduğu tespit edilmiştir ($p<0,05$). Elde edilen verilere göre erkek öğrencilerin farkındalık düzeylerinin daha yüksek olduğu görülmüştür (Tablo 4.11). Cinsiyet değişkenine göre diğer alt boyutlarda anlamlı farklılık görülmemekle birlikte ($p>0,05$), internette günde ne kadar vakit geçirildiği, bilgisayarda günde ve haftada ne kadar vakit geçirildiği ve sosyal ağa üye olma durumlarına göre BGFÖ puanları arasında anlamlı düzeyde farklılık olmadığı görülmüştür ($p>0,05$).

Güldüren ve arkadaşları (2016) tarafından ortaöğretim öğrencilerine yönelik yapılan "Bilgi Güvenliği Farkındalık Ölçeği" sonuçlarına göre erkek öğrencilerin farkındalık düzeylerinin kız öğrencilerin farkındalık düzeylerinden daha yüksek olduğu tespit edilmiştir.

Tekerek ve Tekerek (2013) öğrencilerin bilgi güvenliği farkındalığı üzerine yapmış oldukları araştırma sonucunda, öğrencilerin etik konulardaki bilgi güvenliği farkındalık düzeylerinin yeterli seviyede olduğunu tespit etmiştir. Ancak öğrencilerin kurallar ve bilgi gerektiren konularda farkındalık düzeylerinin düşük olduğu gözlemlenmiştir.

Fogel ve Nehmad (2009) üniversite öğrencileri üzerinde yaptığı çalışmasında ise sosyal ağlarda hesapları olan kişilerin olmayanlara göre daha çok risk alma tutumlarının olduğu ve bunun yanında erkeklerde risk alma tutumunun daha yüksek olduğunu bulmuştur. Bunun sonucu olarak da erkeklerin sosyal ağ hesaplarında daha çok telefon numaralarını ve ev adreslerini paylaşarak bilgi güvenliği açısından riskli davranışlar sergilediği belirlenmiştir (Fogel ve Nehmad, 2009).

Alanyazında yer alan bulguların çalışma sonuçlarını destekler nitelikte olduğu görülmüştür.

Araştırmada yer alan öğretmenlerin (n=120) BGFÖ puan analizinde, genel güvenlik alt boyutu ortalamasının 45,84±9,52, saldırı ve tehditler alt boyutu ortalamasının 40,71±14,89, mobil cihazlar, mahremiyet ve iletişim alt boyutu ortalamasının 57,98±16,74, BGFÖ genel puan ortalamasının 144,53±37,12 olduğu görülmektedir (Tablo 4.22). Bunun yanı sıra öğretmenlerin (n=120) okul düzeyine göre BGFÖ puan ortalamaları değerlendirildiğinde, saldırı ve tehditler alt boyutu, mobil cihazlar, mahremiyet ve iletişim alt boyutu ve ölçek genel puan ortalamalarında ortaokul ve lisede görev yapan öğretmenler arasında istatistiksel olarak anlamlı fark tespit edilmiştir ($p<0,05$) (Tablo 4.25). Özel okulda görev yapan öğretmenlerin (n=60) okul düzeyine göre BGFÖ puan ortalamaları değerlendirildiğinde, saldırı ve tehditler alt boyutu puan ortalamasında ortaokul ve lisede görev yapan öğretmenler arasında istatistiksel olarak anlamlı fark tespit edilmiştir ($p<0,05$) (Tablo 4.26). Devlet okulunda görev yapan öğretmenlerin (n=60) okul düzeyine göre BGFÖ puan ortalamaları değerlendirildiğinde, mobil cihazlar, mahremiyet ve iletişim alt boyutu puan ortalamasında ortaokul ve lisede görev yapan öğretmenler arasında istatistiksel olarak anlamlı fark tespit edilmiştir ($p<0,05$) (Tablo 4.27). Elde edilen verilere göre lisede görev yapan öğretmenlerin farkındalık düzeyinin daha yüksek olduğu görülmüştür.

Nitel verilere bakıldığında görüşme yapılan öğretmenlerden (n=12) ÖLÖT1, ÖLÖT2, ÖLÖT3, DLÖT1 ve DLÖT3 bilgi güvenliği kavramına yönelik sorulan soruda herhangi bir bilgileri olmadığını dile getirmişlerdir. ÖLÖT1 antivirüs programı kullanmadığını belirtmiş olmakla birlikte tüm öğretmenler antivirüs programlarının gerekliliği doğrultusunda açıklama yapmışlardır. Lisanssız program kullanımına yönelik soruya DOÖT1, DOÖT2, DOÖT3, ÖLÖT1, ÖLÖT3, DLÖT1 ve DLÖT2 kullandıkları yönünde yanıt vermişler, ÖOÖT3 ise lisansız program kullanmanın olumsuz yönlerine dair bilgi sahibi olmadığını ifade etmiştir. Çalışmaya katılan tüm öğretmenler sosyal medya kullanımının ve İnternet'in zararlı yönleri konusunda gündemi takip ettiklerini belirtmişlerdir. Mevcut konuyla ilgili öğrencileri bilgilendirme konusunda ise yalnızca ÖLÖT2 "hayır, kendim bile hâkim değilken öğrencilere böyle bir bilgilendirme yapmıyorum" şeklinde olumsuz yönde bir yanıt vermiştir. ÖLÖT2 aynı zamanda sosyal medya kullanımının ve İnternet'in zararlı yönlerine yönelik olarak ne gibi önlemler alınmalı sorusuna "önlem almıyorum, çok uzun zamandır şifremi dahi değiştirmedim" yanıtını vermiştir. Sosyal medya kullanımının ve İnternet'in zararlı yönlerine yönelik olarak alınması gereken önlemler konusunda öğrencilerinizi yönlendiriyor musunuz sorusunda ise DOÖT2 "hayır, hiç olmadı" ve ÖLÖT2 "yapmadım kendim de yapmıyorum" cevabını vermişlerdir. Diğer öğretmenler ise soruları olumlu yönde yanıtlamışlardır.

Öğrencilerin (n=12) öğretmenlerin kendilerini yönlendirmelerine yönelik sorulan soruya verdikleri cevaplara bakıldığında, ÖLÖ3 ise "bu konuda aslında pek bir şey söylemiyorlar sadece internet başında fazla vakit geçirmememizi söylüyorlar" diyerek düşüncesini belirtken, DLÖ3 ise yönlendirmede bulunulmadığını dile getirmiştir. Diğer öğrenciler ise öğretmenlerinin yönlendirmede bulunduğunu ifade etmişlerdir.

Elde edilen bulgulara bakıldığında, nicel verilerden ulaşılan lisede görev yapan öğretmenlerin farkındalık düzeylerinin daha yüksek olduğu sonucunun nitel verilerle tam olarak desteklenmediği görülmüştür. Özellikle bir öğretmenin vermiş olduğu olumsuz yanıtlar lise düzeyinde de farkındalığın her zaman daha yüksek olmayacağını, nicel bulguları genellemenin söz konusu olmayabileceğini göstermiştir. Tek bir kişiden elde edilen verilerle sonuca varmak mümkün olmayacağı gibi daha fazla

öğrenciden ve öğretmenden elde edilecek nicel ve nitel veriler, daha kesin sonuçlara ulaşılmasını sağlayabilecektir.

Araştırmada yer alan öğretmenlerin (n=120) cinsiyetine göre BGFÖ puan ortalamaları değerlendirildiğinde, saldırı ve tehditler alt boyutu puan ortalamasında kadın ve erkek öğretmenler arasında istatistiksel olarak anlamlı fark tespit edilmiştir ($p<0,05$). Erkek öğretmenlerin farkındalık düzeyinin daha yüksek olduğu görülmüştür (Tablo 4.23). Bilgisayarda günde kaç saat vakit geçirdiklerine göre BGFÖ puan ortalamalarına bakıldığında, genel güvenlik alt boyutu ($p<0,05$), mobil cihazlar, mahremiyet ve iletişim alt boyutu ($p<0,05$), saldırı ve tehditler alt boyutu ($p<0,05$) ve ölçek genel ($p<0,05$) puan ortalamalarında gruplar arasında istatistiksel olarak anlamlı fark tespit edilmiştir. Genel güvenlik alt boyutu puan ortalamalarında, günde 0-1 saat internette vakit geçiren grup ile günde 2-4 saat internette vakit geçiren grup arasında anlamlı farklılık yer almaktadır. Farkındalık düzeyi en yüksek olan grubun ise günde 2-4 saat internette vakit geçiren grup olduğu görülmüştür. Mobil cihazlar, mahremiyet ve iletişim alt boyutu ile ölçek genel puan ortalamalarında, günde 0-1 saat internette vakit geçiren grup ile günde 2-4 saat internette vakit geçiren grup arasında ve günde 0-1 saat internette vakit geçiren grup ile günde 5 saatten fazla internette vakit geçiren grup arasında anlamlı farklılık yer almaktadır. Farkındalık düzeyi en yüksek olan grubun ise günde 5 saatten fazla internette vakit geçiren grup olduğu görülmüştür (Tablo 4.33). Bilgisayarda günde kaç saat vakit geçirdiklerine göre BGFÖ puan ortalamaları değerlendirildiğinde, genel güvenlik alt boyutu, mobil cihazlar, mahremiyet ve iletişim alt boyutu ve ölçek genel puan ortalamalarında gruplar arasında istatistiksel olarak anlamlı fark tespit edilmiştir ($p<0,05$). Mobil cihazlar, mahremiyet ve iletişim alt boyutu ile ölçek genel puan ortalamalarında, günde 0-1 saat bilgisayar kullanan grup ile günde 5 saatten fazla bilgisayar kullanan grup arasında anlamlı farklılık yer almaktadır. Farkındalık düzeyi en yüksek olan grubun ise günde 5 saatten fazla bilgisayar kullanan grup olduğu görülmüştür (Tablo 4.31). Bilgisayarda haftada toplam kaç saat vakit geçirdiklerine göre BGFÖ puan ortalamaları değerlendirildiğinde, genel güvenlik alt boyutu ($p<0,05$), mobil cihazlar, mahremiyet ve iletişim alt boyutu ($p<0,05$) ve ölçek genel ($p<0,05$) puan ortalamalarında gruplar arasında istatistiksel olarak anlamlı fark tespit edilmiştir. Genel güvenlik alt boyutunda, haftada toplam 1-2 saat bilgisayar kullanan grup ile haftada toplam 2-4

saat, 5-10 saat ve 10 saatten fazla bilgisayar kullanan gruplar arasında anlamlı farklılık yer almaktadır. Farkındalık düzeyi en yüksek olan grubun ise haftada toplam 10 saatten fazla bilgisayar kullanan grup olduğu görülmüştür. Mobil cihazlar, mahremiyet ve iletişim alt boyutu ile ölçek genel puan ortalamalarında, haftada toplam 1-2 saat bilgisayar kullanan grup ile haftada toplam 10 saatten fazla bilgisayar kullanan gruplar arasında anlamlı farklılık yer almaktadır. Farkındalık düzeyi en yüksek olan grubun ise haftada toplam 10 saatten fazla bilgisayar kullanan grup olduğu görülmüştür (Tablo 4.32). Elde edilen bulgulara bakıldığında genel olarak internette ve bilgisayarda uzun süre vakit geçiren öğretmenlerin farkındalık düzeylerinin daha yüksek olduğu sonucuna ulaşılmıştır. Bu durumun, internet ortamı ve bilgisayar ile daha fazla ilgilenme ve daha fazla bilgi sahibi olma imkânı yarattığı ve bu doğrultuda zaman içerisinde farkındalığın oluştuğu düşünülmektedir.

Yayla (2018) Fatih projesi uygulanan ve uygulanmayan okullardaki öğretmenlerin bilgi güvenliği farkındalığının incelenmesine yönelik yaptığı çalışmada cinsiyete göre erkek öğretmenlerin, okul türüne göre ise ortaokulda görev yapan öğretmenlerin farkındalık düzeylerinin daha yüksek olduğu sonucuna ulaşmıştır.

Yılmaz (2015) öğretmenlerin dijital veri güvenliği farkındalıklarının günlük internet kullanım süresine göre anlamlı farklılık gösterip göstermediğine ilişkin yapılan araştırma sonucunda, günlük internet kullanım süresi daha fazla olan öğretmenlerin dijital veri güvenliği konusunda farkındalıklarının daha fazla olduğunu ortaya koymuştur.

Mart (2012) tarafından bireylerin bilgi güvenliği farkındalıkları ile günlük internet kullanım süreleri arasında anlamlı bir fark olup olmadığını belirlemeye yönelik yapılan araştırma sonucu, bu araştırma bulgularıyla örtüşmemektedir. Mart yapmış olduğu araştırmada, bireylerin bilgi güvenliği farkındalıklarının günlük internet kullanım sürelerine bağlı olarak anlamlı farklılık göstermediğini ortaya koymuştur. Fakat söz konusu araştırma öğretmenler ile değil çeşitli meslek grupları ile gerçekleştirilmiştir. Mevcut farklılığın bu durumdan kaynaklanabileceği düşülmektedir.

Araştırmada yer alan okul yöneticilerinin (n=4) BGFÖ puan ortalamaları değerlendirildiğinde, genel güvenlik alt boyutu ortalamasının 50,75±8,88, saldırı ve tehditler alt boyutu ortalamasının 56,00±17,21, mobil cihazlar, mahremiyet ve iletişim

alt boyutu ortalamasının 64,25±22,63, BGFÖ genel puan ortalamasının 171,00±48,45 olduğu görülmektedir (Tablo 4.35). Araştırmada yer alan okul yöneticilerinin (n=4) BGFÖ puan ortalamaları değerlendirildiğinde, genel güvenlik alt boyutunda özel okulda lise düzeyindeki okul yöneticisinin, saldırı ve tehditler alt boyutunda özel okulda ortaokul düzeyindeki okul yöneticisinin, mobil cihazlar, mahremiyet ve iletişim alt boyutunda özel okulda ortaokul düzeyindeki okul yöneticisinin, ölçek genel puanlarında ise özel okulda ortaokul düzeyindeki okul yöneticisinin en yüksek puanı aldığı ve farkındalık düzeyinin en yüksek olan okul yöneticisi olduğu tespit edilmiştir. Bu bulgulara ve tablo 4.36'da yer alan verilere göre özel okulda görev yapan okul yöneticilerinin devlet okulunda görev yapan okul yöneticilerine göre farkındalık düzeylerinin daha yüksek olduğu görülmektedir.

Nitel verilere bakıldığında görüşme yapılan okul yöneticilerinden (n=4) bilgi güvenliği kavramına yönelik soruya DLOY "duymadım, ama kişisel verilerin korunumu durumunu biliyorum..ama tam olarak bu kavram ile ilgili bilgim yok" diyerek yanıt vermiş diğer okul yöneticileri ise bilgi güvenliği kavramını duyduklarını belirtip kavram ile ilgili açıklama yapmışlardır. Antivirüs programlarının kullanımının değerlendirildiği soruda, okul yöneticilerinin hepsi programı kullandıklarını belirtmiş, DLOY da antivirüs programının bilgisayarında mevcut olduğunu, bu programın bilgisayarı virüslerden korumak için kullandığı ama konu ile ilgili başka bir bilgisi olmadığını ifade etmiştir. Lisanssız program kullanımın sorulduğu soruda DLOY "lisanssız program kullanıp kullanmadığımı bilmiyorum ama genelde kullanmıyorum diye biliyorum" diyerek ve bu programlar ile virüslere karşı bilgisayarın korunmasında problem olabileceğini dile getirip soruyu yanıtladığı, diğer okul yöneticilerinin de lisanssız program kullanmadıkları görülmüştür. Sosyal medya kullanımının ve İnternet'in zararlı yönleri konusunda gündemi takip eder misiniz sorusuna tüm okul yöneticileri gündemi takip ettiklerine dair yanıt vermişler ve öğrencilerini bilgilendirdiklerini dile getirmişlerdir. Sosyal medya kullanımının ve İnternet'in zararlı yönlerine yönelik olarak ne gibi önlemler alınmalı ve alınması gereken önlemler konusunda öğrencilerinizi yönlendiriyor musunuz sorusuna tüm okul yöneticileri çeşitli önlemler aldığını ifade edip, bu doğrultuda öğrencilerini de yönlendirdiklerini belirtmişlerdir.

Elde edilen bulgulara bakıldığında, nicel verilerden ulaşılan özel okulda görev yapan okul yöneticilerinin farkındalık düzeylerinin daha yüksek olduğu sonucunun nitel verilerle desteklendiği görülmüştür. Özel okulda görev yapan okul yöneticilerinin mevcut koşullar dahilinde daha fazla imkana sahip oldukları ve kendilerini geliştirme olanakları daha fazla olabildiği için bu durumun farkındalık düzeylerine de yansıdığı düşünülmektedir.

Görgülü, Küçükali ve Ada (2013), okul yöneticilerinin teknolojik liderlik öz-yeterliliklerinin ne düzeyde olduğunu belirlemek amacıyla yaptıkları çalışmada, okul yöneticilerinin teknolojik liderlik öz yeterliliklerinin yüksek düzeyde olduğunu tespit etmişlerdir.

Sayracı'nın (2018) yapmış olduğu araştırma sonuçlarına göre; okul yöneticilerinin teknolojik liderlik yeterliklerinin yüksek düzeyde olduğu görülmüştür. Okul yöneticilerinin teknolojik liderlik yeterlikleri alt boyutlar açısından incelendiğinde ise; dijital çağ öğrenme kültürünün diğer boyutlara göre en fazla yeterli oldukları boyut olduğu, sistematik gelişimin ise en az yeterli oldukları boyut olduğu görülmektedir. Okul yöneticilerinin teknolojik liderlik ve değişim yönetimi yeterlik alt boyutlarının görev yaptıkları okul türü değişkenine göre anlamlı farklılık görülmemiştir.

Literatürde yer alan çalışmalar incelendiğinde, okul yöneticilerinin bilgi güvenliği farkındalığında yönelik çalışmaların yetersiz olduğu, okul yöneticileri ile ilgili olarak genellikle teknolojik liderlik alanlarında çalışmalar yapıldığı görülmüştür.

Araştırmada yer alan veliler (n=12) ile yapılan görüşmeler sonucunda elde edilen nitel verilere bakıldığında, ÖOV2, DOV2, ÖLV3 ve DLV3 evlerinde bulunan bilgisayarın çocuk odasında bulunduğunu dile getirmiştir. Bilgisayarında çocuk odasında bulunmasının, kullanım esnasında çocukların gözlemlenmesi açısından olumsuz bir durum olabileceği düşünülmektedir. DOV3 çocuklarının kullandığı teknolojik cihazları kontrol etmediğini ve kullandıkları programlara yönelik bilgi sahibi olmadığını belirtmiştir. Bu durum, eğer çocuklar teknolojik cihazları bilinçsizce kullanıyor ise, veli kontrolünün ortadan kalkması ile olumsuz bir şekilde sonuçlanabileceği gibi, alınabilecek olası önlemlerinde önüne geçilmesine neden olmaktadır. Bilgi güvenliği kavramına yönelik soruda ÖOV3, DOV3, ÖLV1, ÖLV2 ve DLV' duyduğunu ama içeriğini pek bilmediğini belirtirken, DOV2, ÖLV3, DLV1

ve DLV3 bu kavramı daha önce hiç duymadıklarını ifade etmişlerdir. Antivirüs programı kullanıyor musunuz ve antivirüs programının gerekliliği hakkında neler düşünüyorsunuz sorusuna; ÖOV1 ve ÖLV2 antivirüs programı kullanmadıkları doğrultusunda cevap vermiş, ÖLV2 ve DLV1 gerekliliği ile ilgili bilgi sahibi olmadığını ifade etmiştir. Sosyal medya kullanımının ve İnternet'in zararlı yönleri konusunda gündemi takip eder misiniz sorusuna tüm veliler takip ettikleri doğrultusunda yanıt verirken DLV1 gündemi takip etmediğini dile getirmiştir. Sosyal medya kullanımının ve İnternet'in zararlı yönleri konusunda çocuğunuzu/çocuklarınızı bilgilendirir misiniz sorusunda tüm veliler bilgilendirme yaptıklarını ifade etmişlerdir. Sosyal medya ve İnternet kullanımının zararlarından kendinizi ve çocuğunuzu/çocuklarınızı korumak için ne gibi önlemler alıyorsunuz sorusuna veliler aldıkları çeşitli önlemleri sayarken, DOV3 ve DLV1 ise herhangi bir önlem almadıklarını belirtmişlerdir. Verilen olumsuz yöndeki cevaplar, velilerin bilgi güvenliği farkındalığı konusunda yetersiz kaldıklarını ortaya koymakta, bu durum hem kendileri hem çocukları için tehlike arz etmektedir.

Öğrencilerin (n=12) velilerinin kendilerine dair evde bilgisayar kullanımına yönelik bir kısıtlama olup olmadığına yönelik sorulan soruya verdikleri cevaplara bakıldığında, ÖOÖ1, ÖOÖ3, DOÖ2, DOÖ3, ÖLÖ1, DLÖ2 ve DLÖ3 herhangi bir kısıtlama olmadığını ifade etmişlerdir. Bu durum velilerin çocuklarını kontrol etmekte yetersiz kaldığını, meydana gelebilecek olumsuzlukları fark etmekte güçlük yaşanabileceğini ve önlemlerin alınamayacağını ortaya koymaktadır.

Yapılan görüşmelerden elde edilen bulgulara bakıldığında, velilerin önemli bir kısmının farkındalık düzeylerinin düşük olduğu, ev ortamında çocukların yeterince gözlemlenmediği, gözlemlense bile neye dikkat edilerek gözlemlenip hangi doğrultuda yönlendireceklerine dair yeterli bilgiye sahip olmadıkları görülmüştür.

Kaşıkçı vd. (2014) yapmış oldukları çalışmada Türkiye ve Avrupa'daki çocukların internet alışkanlıkları ve güvenli internet kullanımını araştırmışlardır. Yapılan çalışma sonucunda Türkiye'deki ebeveynlerin İnternet kullanım oranının oldukça düşük olduğu ve çocuklarını İnternet risklerinden uzak tutmayı sağlayacak yeterli bilgiye sahip olmadıkları görülmüştür.

Karaoğlan Yılmaz ve Çavuş Ezin'in (2017) ebeveynlerin bilgi güvenliği farkındalıklarını inceledikleri çalışmada sonuçlarına bakıldığında, ebeveynlerin bilgi

güvenliği farkındalıklarının belli bir düzeyde bulunduğu fakat verileri yedekleme yerleri ve veri yedekleme sıklığına yönelik farkındalıklarının düşük düzeyde olduğu görülmüştür. Çocukların bilgi güvenliğini sağlamak amacı ile, ebeveynlerin, genellikle çocuklarına sözlü uyarılarda bulunduğu tespit edilmiştir. Ancak somut bir şekilde bilgi güvenliğine yönelik çocuklarına bilgi veremiyor oldukları görülmüştür. Bu doğrultuda ebeveynlerin, çocuklarına, bilgi güvenliği konusunda farkındalık oluşturabilmesi amacıyla kendilerinin de bu konuda yeterli bilgiye sahip olması gerektiği anlaşılmaktadır.

Sonuç

Yapılan araştırma sonucunda aşağıda yer alan sonuçlara ulaşılmıştır;

- Öğrencilerin (n=200) okul türüne göre BGFÖ puan ortalamaları değerlendirildiğinde, özel okulda öğrenim gören öğrencilerin farkındalık düzeylerinin daha yüksek olduğu görülmüştür.
- Lisede öğrenim gören öğrencilerin (n=100) okul türüne göre BGFÖ puan ortalamaları değerlendirildiğinde, özel okulda öğrenim gören öğrencilerin farkındalık düzeylerinin daha yüksek olduğu görülmüştür.
- Öğrencilerin (n=200) okul seviyesine göre BGFÖ puan ortalamaları değerlendirildiğinde, ortaokulda öğrenim gören öğrencilerin farkındalık düzeylerinin daha yüksek olduğu görülmüştür.
- Devlet okulunda öğrenim gören öğrencilerin (n=100) okul seviyesine göre BGFÖ puan ortalamaları değerlendirildiğinde, ortaokulda öğrenim gören öğrencilerin farkındalık düzeylerinin daha yüksek olduğu görülmüştür.
- Nicel verilerden ulaşılan özel okuldaki öğrencilerin farkındalık düzeylerinin daha yüksek olduğu sonucunun nitel verilerle desteklenebileceği görülmüştür. Ortaokul ve lise düzeyinde öğrenim gören öğrenciler arasındaki farkındalık düzeyi farklılığına yönelik ise sonuçların birbirini tam olarak desteklemediği görülmüştür.
- Öğrencilerin (n=200) cinsiyete göre BGFÖ puan ortalamaları değerlendirildiğinde, erkek öğrencilerin farkındalık düzeylerinin daha yüksek olduğu görülmüştür.

- Öğrencilerin (n=200) internette günde ne kadar süre vakit geçirdikleri, bilgisayarda günde ne kadar süre vakit geçirdikleri, bilgisayarda haftada ne kadar süre vakit geçirdikleri ve sosyal ağa üye olma durumlarına göre BGFÖ puanları arasında istatistiksel olarak anlamlı farklılık olmadığı görülmüş, bu değişkenlerin farkındalık düzeyleri üzerinde etkisi olmadığı sonucuna ulaşılmıştır.
- Öğretmenlerin (n=120) okul seviyesine göre BGFÖ puan ortalamaları değerlendirildiğinde, lisede görev yapan öğretmenlerin farkındalık düzeyinin daha yüksek olduğu görülmüştür.
- Özel okulda görev yapan öğretmenlerin (n=60) okul seviyesine göre BGFÖ puan ortalamaları değerlendirildiğinde, lisede görev yapan öğretmenlerin farkındalık düzeyinin daha yüksek olduğu görülmüştür.
- Devlet okulunda görev yapan öğretmenlerin (n=60) okul seviyesine göre BGFÖ puan ortalamaları değerlendirildiğinde, lisede görev yapan öğretmenlerin farkındalık düzeyinin daha yüksek olduğu görülmüştür.
- Nicel verilerden ulaşılan lisede görev yapan öğretmenlerin farkındalık düzeylerinin daha yüksek olduğu sonucunun nitel verilerle tam olarak desteklenmediği görülmüştür.
- Öğretmenlerin (n=120) cinsiyetine göre BGFÖ puan ortalamaları değerlendirildiğinde, erkek öğretmenlerin farkındalık düzeyinin daha yüksek olduğu görülmüştür.
- Öğretmenlerin (n=120) internette günde kaç saat vakit geçirdiklerine göre BGFÖ puan ortalamaları değerlendirildiğinde, genel güvenlik alt boyutunda, günde 0-1 saat internette vakit geçiren grup ile günde 2-4 saat internette vakit geçiren grup arasında anlamlı fark tespit edilmiştir. Farkındalık düzeyi en yüksek olan grubun ise günde 2-4 saat internette vakit geçiren grup olduğu görülmüştür. Mobil cihazlar, mahremiyet ve iletişim alt boyutu ile ölçek genel puan ortalamalarında, günde 0-1 saat internette vakit geçiren grup ile günde 2-4 saat internette vakit geçiren grup arasında ve günde 0-1 saat internette vakit geçiren grup ile günde 5 saatten fazla internette vakit geçiren grup arasında anlamlı fark tespit edilmiştir. Farkındalık düzeyi en

yüksek olan grubun ise günde 5 saatten fazla internette vakit geçiren grup olduğu görülmüştür.

- Öğretmenlerin (n=120) bilgisayarda günde kaç saat vakit geçirdiklerine göre BGFÖ puan ortalamaları değerlendirildiğinde, mobil cihazlar, mahremiyet ve iletişim alt boyutu ile ölçek genel puan ortalamalarında, günde 0-1 saat bilgisayar kullanan grup ile günde 5 saatten fazla bilgisayar kullanan grup arasında anlamlı fark tespit edilmiştir. Farkındalık düzeyi en yüksek olan grubun ise günde 5 saatten fazla bilgisayar kullanan grup olduğu görülmüştür.
- Öğretmenlerin (n=120) bilgisayarda haftada toplam kaç saat vakit geçirdiklerine göre BGFÖ puan ortalamaları değerlendirildiğinde, genel güvenlik alt boyutunda, haftada toplam 1-2 saat bilgisayar kullanan grup ile haftada toplam 2-4 saat, 5-10 saat ve 10 saatten fazla bilgisayar kullanan gruplar arasında anlamlı fark tespit edilmiştir. Farkındalık düzeyi en yüksek olan grubun ise haftada toplam 10 saatten fazla bilgisayar kullanan grup olduğu görülmüştür. Mobil cihazlar, mahremiyet ve iletişim alt boyutu ile ölçek genel puan ortalamalarında, haftada toplam 1-2 saat bilgisayar kullanan grup ile haftada toplam 10 saatten fazla bilgisayar kullanan gruplar arasında anlamlı fark tespit edilmiştir. Farkındalık düzeyi en yüksek olan grubun ise haftada toplam 10 saatten fazla bilgisayar kullanan grup olduğu görülmüştür.
- İnternette ve bilgisayarda daha uzun süre vakit geçiren öğretmenlerin farkındalık düzeylerinin daha yüksek olduğu sonucuna ulaşılmıştır.
- Öğretmenlerin (n=120) sosyal ağa üye olma durumlarına göre BGFÖ puanları arasında istatistiksel olarak anlamlı farklılık olmadığı görülmüş, bu değişkenin farkındalık düzeyi üzerinde etkisi olmadığı sonucuna ulaşılmıştır.
- Okul yöneticilerinin (n=4) BGFÖ puan ortalamaları değerlendirildiğinde, özel okulda görev yapan okul yöneticilerinin devlet okulunda görev yapan okul yöneticilerine göre farkındalık düzeylerinin daha yüksek olduğu görülmüştür.

- Nicel verilerden ulaşılan özel okulda görev yapan okul yöneticilerinin farkındalık düzeylerinin daha yüksek olduğu sonucunun nitel verilerle desteklendiği görülmüştür.
- Veliler ve öğrenciler ile yapılan görüşmeler sonucunda, velilerin önemli bir kısmının farkındalık düzeylerinin düşük olduğu, çocuklarını gözlemleme konusunda ve bilinçli kullanıma dair yönlendirmede yetersiz kaldıkları sonucuna ulaşılmıştır.

Öneriler

Yapılan araştırma sonucunda aşağıda yer alan öneriler sunulmuştur;

- Özel okullarda ve devlet okullarında yer alan öğrenci, veli, öğretmen ve okul yöneticilerinin farkındalık düzeylerinin üst seviyeye çıkarılabilmesi için her bir hedef kitleye özgü seminerler düzenlenebilir, yaşanılabilecek sorunlara yönelik alınması gereken önlemler konusunda bilinçlendirme sağlanabilir.
- Farkındalık sağlanmasına yönelik, belirlenen hedef kitleye uygun bir şekilde çeşitli materyallerin kullanılmasının yanı sıra bilişim alanı ile ilişkili meslek gruplarından uzmanlar çağrılabilir, yaşanmış örnekler ve senaryolar üzerinden bilgilendirme çalışmaları yapılabilir.
- Öğrencilerle daha fazla bir arada olan veli ve öğretmenlerin farkındalıklarının üst seviyeye çekilerek, öğrencileri nasıl yönlendirmeleri konusunda eğitim çalışmaları yapılabilir.
- Öğrencilerin, kendilerine yapılan yönlendirmelere uymaları konusunda ve farkındalıklarının oluşması açısından eğitim çalışmaları yapılabilir.
- Hedef kitleler, bilgi güvenliğinin sağlanmasına yönelik kullanılabilecek programlar konusunda bilgilendirilebilir.
- Söz konusu çalışma alanı ile ilgili olarak deneysel çalışmalar yapılabilir.
- Nitel ve nicel verilerin birbirleri ile ilişkilendirilmesinin daha verimli bir şekilde yapılabilmesi için daha geniş bir örneklem aralığında benzer bir çalışma yapılabilir.

- Farklı bölgelerde yer alan öğrenci, veli, öğretmen ve okul yöneticileri ile benzer araştırmalar yapılarak bölgesel farklılıklar tespit edilebilir ve bu doğrultuda gerekli çalışmalar yapılabilir.

KAYNAKÇA

Altun, R., (2014). Belirli Kısıtlara Göre Bilgi Güvenliği İhlallerinin Tespiti, Yüksek Lisans Tezi, İstanbul Beykent Üniversitesi FBE, İstanbul, 46s (yayınlanmamış).

Aslandağ, K., (2010). Bilgi Güvenliği Kavramı ve Bilgi Güvenliği Yönetim Sistemleri ile Şirket Performansı İlişkisine Dair Bir Uygulama, Yüksek Lisans Tezi, Gebze Yüksek Teknoloji Enstitüsü Sosyal Bilimler Enstitüsü, Kocaeli.

Atılgan, D., (2009). Bilgi yönetimi kavramı ve gelişimi, *Türk Kütüphaneciliği*, 23(1):201-212 s.

Bintziou, A., Alexandris, N. and Chrissikopoulos, V., (1999). Introducing IT-Security Awareness İn Schools: The Greek Case, IFIP WG 11.8 1st World Conference on Information Security Education, WISE Citeseer.

Blanding, F. S., (2004). An Introduction to LAN/WAN Security, Information Security Management Handbook, Fifth Edition, Auerbach Publications, New York.

Burlu, K., (2015). Bilişimin Karanlık Yüzü, 4. Basım, Nirvana Yayınları, Ankara, 114 s.

Büyüköztürk, Ş., Çakmak, E. K., Akgün, Ö. E., Karadeniz, Ş. ve Demirel, F., (2016)., Bilimsel Araştırma Yöntemleri, Pegem Akademi, Ankara, 178s.

Canbek, G. ve Sağıroğlu Ş., (2007). Bilgisayar sistemlerine yapılan saldırılar ve türleri: Bir inceleme, *Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 33(2):1-12 s.

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

Canbek, G., (2005). Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme, Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

Cisco, (2017). Cisco 2017 Annual Cybersecurity Report, USA, 13 s.

Civelek, D. Y., (2011). Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi, Uzmanlık Tezi, Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Bilgi Toplumu Dairesi Başkanlığı, Ankara, 49 s.

Creswell, J. W., (2003). Research design: Qualitative, quantitative, and mixed methods approaches (2nd ed.). Thousand Oaks, CA: Sage.

Creswell, J.W. (2006). "Understanding Mixed Methods Research", http://www.sagepub.com/upm-data/10981_Chapter_1.pdf (Erişim Tarihi: 23 Mayıs 2018)

Çalışkan, E., (2013)., Zararlı Yazılımların Etkisinde Dijital Adli Delillerin Güvenilirliği. Yüksek Lisans Tezi, Bilgi Üniversitesi SBE, İstanbul, 58s (yayınlanmamış).

Çetin, H., (2014). Kişisel veri güvenliği ve kullanıcıların farkındalık düzeylerinin incelenmesi, *Akdeniz Universitesi Iktisadi ve Idari Bilimler Fakultesi Dergisi,* 14(29):86-105 s.

Çetinkaya, L., Güldüren, C. ve Keser, H., (2017). Öğretmenler için bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması, *Journal of Education and Social Sciences,* 46(216): 33-52s.

Çoban, H., (1996). Bilgi toplumuna planlı geçiş: Bilgi toplumuna geçmek için Stratejik Planlama ve Yönetim Bilgi Sistemi Uygulanması, Devlet Planlama Teşkilatı, Ankara.

Davey, L., (2009). The application of case study evaluations, *Elementary Education Online,* 8(2):1-3p.

Davenport, T. ve Prusak, L., (2001)., İş Dünyasında Bilgi Yönetimi, Rota Yayın, İstanbul.

Davies, R. S., (2011). Understanding technology literacy: A framework for evaluating educational technology integration, *TechTrends,* 55(5):45-52p.

Demirtaş, H., (2013). Bilgi Güvenliği Yönetiminin Gerekleri ve Başarı Dayanakları: Bir Uygulama Örneği, Yüksek Lisans Tezi, Sakarya Üniversitesi Sosyal Bilimler Enstitüsü, Sakarya.

Dinçkan, A., (2008). ‘’İş Sürekliliği Yönetim Sistemi Kurulum, TÜBİTAK, UEKAE.’’, https://egitim.sge.gov.tr/ (Erişim tarihi: 7 Nisan 2019), 16 s.

Doğantimur, F., (2009). ISO 27001 Standardı Çerçevesinde Kurumsal Bilgi Güvenliği, Uzmanlık Tezi, Maliye Bakanlığı Strateji Geliştirme Daire Başkanlığı, Ankara, 23 s.

Durna, U. ve Demirel, Y., (2008). Bilgi yönetiminde bilgiyi anlamak, *Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,* 30:129-156 s.

Eckertova, L., Docekal, D. and Pozar, J., (2013). Child Safety on the Internet: Mentor Responsible Parents, 1st Ed., Computer Press, Brno, 54-78 s.

Eminağaoğlu, M. ve Gökşen, Y., (2009). Bilgi güvenliği nedir, ne değildir? Türkiye'de bilgi güvenliği sorunları ve çözüm önerileri, *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* 11(4):1-15 s.

Ercan, M., (2015). Kritik Altyapıların Korunmasına İlişkin Belirlenen Siber Güvenlik Stratejileri, Yüksek Lisans Tezi, Gebze Teknik Üniversitesi SBE, Kocaeli, 19s (yayınlanmamış).

Fogel, J. ve Nehmad, E., (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, *25*(1):153-160 s.

Fussell, R.S., (2005). Protecting Information Security Availability Via Self-adapting Intelligent Agents, Military Communications Conference, IEEE, 17-20 October, USA, 297p.

Gencer, K., (2015). ISO 27001 Kapsamında Kurumsal Bilgi Güvenliğine Dinamik Bir Yaklaşım, Yüksek Lisans Tezi, Afyon Kocatepe Üniversitesi FBE, 1s (yayınlanmamış).

Ghaziri, H. and Elias, A., (2004). Knowledge Management, Prentice Hall Publishing, New Jersey, USA.

Görgülü, D., Küçükali, R. ve Ada, Ş., (2013). Okul yöneticilerinin teknolojik öz yeterlilikleri, *Eğitim Teknolojisi Kuram ve Uygulama,* 3(2):53-71 s.

Güçlü, N. ve Sotirofski, K., (2006). Bilgi yönetimi, *Türk Eğitim Bilimleri Dergisi,* 4(4):351-373 s.

Güldüren, C., Çetinkaya, L. ve Keser, H., (2016). Ortaöğretim öğrencilerine yönelik bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması, *İlköğretim Online,* 15(2):682-695 s.

Gülmüş, M., (2010). Kurumsal Bilgi Güvenliği Yönetim Sistemleri ve Güvenliği, Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi FBE, İstanbul, 125s (yayınlanmamış).

ISO/ IEC 27001, (2013). Information technology — Security techniques — Information security management systems — Requirements, https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en (Erişim Tarihi:1 Eylül 2019).

Johnson, D. G., (2000). Computer Ethics, Prentice Hall, USA, 200p.

Johnson, R. B., & Onwuegbuzie, A. J., (2004). Mixed methods research: A research paradigm whose time has come, *Educational Researcher*, 33(7): 14-26p.

Karaoğlan Yılmaz, F. G. ve Çavuş Ezin, Ç., (2017). Ebeveynlerin bilgi güvenliği farkındalıklarının incelenmesi, *Eğitim Teknolojisi Kuram ve Uygulama,* 7(2):41-57 s.

Kaspersky Resource Center, Adware (Reklam Yazılımı) Nedir?, https://www.kaspersky.com.tr/resource-center/threats/adware (Erişim Tarihi:1 Nisan 2019).

Kaşıkçı, D. N., Çağıltay, K., Karakuş, T., Kurşun, E. ve Ogan, C., (2014). Türkiye'deki ve Avrupa'daki çocukların internet alışkanlıkları ve güvenli internet kullanımı, *Education and Science,* 39(171):230-243 s.

Keser, H. ve Güldüren, C., (2015). Bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme, *Kastamonu Üniversitesi Eğitim Dergisi,* 23(3):1167-1184 s.

Kınay, H., (2012). Lise Öğrencilerinin Siber Zorbalik Duyarlılığının Riskli Davraniş, Korumacı Davranış,Suça Maruziyet ve Tehlike Algısı İle İlişkisi ve Çeşitli Değişkenler Açısından İncelenmesi, Yüksek Lisans Tezi, Sakarya Üniversitesi EBE, Sakarya, 17s.

Koç, F., (2008), BGYS-Varlık Envanteri Oluşturma ve Sınıflandırma Kılavuzu Sürüm 1.00, TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, Kocaeli, 6s.

Marks, A., (2007). Exploring Universities & Information Systems Security Awareness in a Changing Higher Education Environment: A Comparative Case Study Research.

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

Mitnick, K. D. and Simon W.L., (2016). Aldatma Sanatı, 6. Basım, ODTÜ Yayınları, Ankara, 232s.

Mitnick, K., 2002, The Art of Deception, John Wiley and Sons.

Muharremoğlu G., (2013). Kurumsal Bilgi Güvenliğinde Zafiyet, Saldırı ve Savunma Öğelerinin İncelenmesi, İstanbul, 49s.

Odabaş, H., (2005). Bilgi Yönetimi Sistemi, Bilgi Çağı, Bilgi Yönetimi ve Bilgi Sistemleri, Çizgi Kitabevi, Konya.

Özenç, K., (2007). Bilgi ve İletişim Teknolojilerinde Kişisel ve Kurumsal Bilgi Güvenliğinin Sağlanması, Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, 13-14 Aralık 2007, Ankara, 190s.

Öztemiz, S. ve Yılmaz, B., (2013). Bilgi merkezlerinde bilgi güvenliği farkındalığı: Ankara'daki üniversite kütüphaneleri örneği, *Bilgi Dünyası,* 14(1):87-100 s.

Öztürk, C. Tekerek, M. ve Yılmaz, A. S.. (2016). Bilgi Güvenliği Endüstrisinin Ülkelere Göre Karşılaştırılması, 9.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 25-26 Ekim 2016, Bilgi Güvenliği Derneği, Ankara, 235-243 s.

Say, M. ve Sağıroğlu Ş., (2004). Bilgisayar Veri Güvenliği Üzerine Bir İnceleme: Klavye Dinleme Sistemleri, VI. Akademik Bilişim Konferansı, 11-13 Şubat 2004, KTÜ, Trabzon, 5 s.

Sayracı, N., (2018). Okul Yöneticilerinin Değişimi Yönetme Yeterlilikleri ve Teknolojik Liderliği, Yüksek Lisans Tezi, İstanbul Aydın Üniversitesi SBE, İstanbul (yayınlanmamış).

Schneider F.B., (2008). Network neutrality versus internet trustworthiness, *IEEE Security & Privacy, 6*(4):3-4p.

Sharp, E. D., (2004). Information Security in the Enterprise, Information Security Management Handbook, Fifth Edition, Auerbach Publications, New York.

Siponen, M. T., (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1):31-41 s.

Swaminatha M. and Elden C. R., (2003). Wireless Security and Privacy: Best Practices and Design Techniques, Addison-Wesley.

Şahinaslan, Ö., (2013). Siber Saldırılara Karşı Kurumsal Ağlarda Oluşan Güvenlik Sorunu ve Çözümü Üzerine Bir Çalışma, Doktora Tezi, Trakya Üniversitesi FBE, Edirne 11s (yayınlanmamış).

Şimşek, H. ve Yıldırım, A., (2008). Sosyal Bilimlerde Nitel Araştırma Yöntemleri, Seçkin Yayınevi, Ankara.

Taş, K. A., (2010). Bilişim Suçları ve Adana İlinde 2006-2009 Yılları Arasında Meydana Gelen Bilişim Suçlarının Değerlendirilmesi, Yüksek Lisans Tezi, Çukurova Üniversitesi Sağlık Bilimleri Enstitüsü, 11s (yayınlanmamış).

TDK, (2019). https://www.tdk.gov.tr (Erişim Tarihi: 17 Haziran 2019).

Tekerek, M. ve Tekerek, A., (2013). Öğrencilerin bilgi güvenliği farkındalığı üzerine bir araştırma, *Turkish Journal of Education*, 2(3):61-70 s.

Tekerek, M., (2008). Bilgi güvenliği yönetimi, *Kahramanmaraş Sütçü İmam Üniversitesi Fen ve Mühendislik Dergisi*, 11(1):132 s.

Tipton, H. F. and Krause, M., (2007). Information Security Management Handbook, Auerbach Publicaions, Auerbach, Germany.

Turhan, M., (2010). Siber Güvenliğin Sağlanması, Dünya Uygulamaları ve Ülkemiz için Çözüm Önerileri, Uzmanlık Tezi, Bilgi Teknolojileri ve İletişim Kurumu, Ankara, 41s.

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

Ünver, M. ve Canbay C., (2010). Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik, *Elektrik Mühendisleri Odası Dergisi,* 91, 94-103, 97s.

Vardal, N., (2009). Yükseköğretimde Bilgi Güvenliği: Bilgi Güvenlik Yönetim Sistemi için Bir Model Önerisi ve Uygulaması, Yüksek Lisans Tezi, Gazi Üniversitesi EBE, Ankara, 93s (yayınlanmamış).

Vural, Y. ve Sağıroğlu Ş., (2007). Kurumsal Bilgi Güvenliği: Güncel Gelişmeler, X. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, 20-21 Ekim 2007, Bilgi Güvenliği Derneği, Ankara, 191-199 s.

Vural, Y., (2007). Kurumsal Bilgi Güvenliği ve Sızma (Penetrasyon) Testleri, Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimeri Enstitüsü, Ankara.

Vural, Y., Bayındır, M. ve Tamer, O., (2009). Anayurt Güvenliğinin Sağlanmasında Bilgi Sistemleri Güvenliğinin Önemi. XI. Akademik Bilişim Konferansı, 11-13 Şubat, Harran Üniversitesi, Şanlıurfa, 607-612 s.

Wenger, A., Mauer, V. and Cavelty M. D., (2008). International CIIP Handbook, ETH Zurich, Switzerland.

Wright, M.A. and Kakalık, J., (2007). Information Security: Contemporary Cases, Sudbury Jones and Bartlett 187s.

Yaşar, H., (2014). Kurumsal Siber Güvenliğe Yönelik Tehditler ve Mücadele Yöntemleri: Eylem Planı Örneği, Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü, Ankara, 26s (yayınlanmamış).

Yayla, H. G., (2018). Fatih Projesi Uygulanan ve Uygulanmayan Okullardaki Öğretmenlerin Bilgi Güvenliği Farkındalıklarının İncelenmesi, Yüksek Lisans Tezi, Ankara Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara (yayınlanmamış).

Yıldırım, U. ve Öner, Ş., (2004). Bilgi toplumu sürecinde yerel yönetimlerde eğitim-bilişim teknolojisinden yararlanma: Türkiye'de e-belediye uygulamaları, *The Turkish Online Journal Of Educational Technology–Tojet, January, 3*(1):49-60s.

Yıldız, M., (2014). Siber Suçlar ve Kurum Güvenliği, Uzmanlık Tezi, Ulaştırma Denizcilik ve Haberleşme Bakanlığı Bilgi İşlem Dairesi Başkanlığı, Ankara, 63s.

Yılmaz, E., (2015). Öğretmenlerin Dijital Veri Güvenliği Farkındalığı. Yüksek Lisans Tezi, Anadolu Üniversitesi EBE, Eskişehir (yayınlanmamış).

Yılmaz, S. ve Salcan O., (2008). Siber Uzay'da Güvenlik ve Türkiye, 1. Basım, Milenyum Yayınları, İstanbul, 56-57 s.

EKLER

Ek 1: Öğrencilere Yönelik Geliştirilen Demografik Bilgi Anketi

LÜTFEN BU DÖKÜMANI DİKKATLİCE OKUMAK İÇİN ZAMAN AYIRINIZ

Sizi Prof. Dr. Mustafa Murat İNCEOĞLU tarafından yürütülen "Bilgi Güvenliğine Yönelik Öğrenci, Öğretmen, Veli Ve Okul Yöneticilerinin Farkındalıklarının İncelenmesi" başlıklı **araştırmaya** davet ediyoruz. Bu araştırmaya katılıp katılmama kararını vermeden önce, araştırmanın neden ve nasıl yapılacağını bilmeniz gerekmektedir. Bu nedenle bu formun okunup anlaşılması büyük önem taşımaktadır. Eğer anlayamadığınız ve sizin için açık olmayan şeyler varsa, ya da daha fazla bilgi isterseniz bize sorunuz.

Bu çalışmaya katılmak tamamen **gönüllülük** esasına dayanmaktadır. Çalışmaya **katılmama** veya katıldıktan sonra herhangi bir anda çalışmadan **çıkma** hakkında sahipsiniz. **Çalışmayı yanıtlamanız, araştırmaya katılım için onam verdiğiniz** biçiminde yorumlanacaktır. Size verilen **formlardaki** soruları yanıtlarken kimsenin baskısı veya telkini altında olmayın. Bu formlardan elde edilecek kişisel bilgiler tamamen gizli tutulacak ve yalnızca araştırma amacı ile kullanılacaktır.

DEMOGRAFİK BİLGİ ANKETİ

Değerli öğrenciler,

Bilgi güvenliğine yönelik yapılan bilimsel bir çalışma için hazırlanan bu anket ile teknoloji kullanımına yönelik alışkanlıklarınız incelenecektir. Anket ile verdiğiniz cevaplara yalnızca araştırmacı tarafından erişim sağlanacaktır. Araştırmaya katılımınız için teşekkür ederim.

Prof. Dr. Mustafa Murat İNCEOĞLU, mustafainceoglu@yahoo.com

Cansu ALTUNSABAN, cansu.altunsaban@gmail.com

1) Cinsiyetiniz Nedir?

☐ Kadın ☐ Erkek

2) Sınıf Düzeyiniz Nedir?

☐ 5.Sınıf ☐ 6.Sınıf ☐ 7.Sınıf ☐ 8.Sınıf

☐ 9.Sınıf ☐ 10.Sınıf ☐ 11.Sınıf ☐ 12.Sınıf

3) Kardeş sayınız nedir?

☐ Yok ☐ 1 ☐ 2 ☐ 2'den fazla

4) Kiminle Yaşıyorsunuz?

☐ Anne-Baba ☐ Anne ☐ Baba ☐ Diğer:……

5) Evde kendinize ait bir bilgisayarınız var mı?

☐ Var ☐ Yok

6) Bilgisayarınızın evdeki konumu nedir?

☐ Kendi Odamda ☐ Salonda ☐ Oturma odasında

☐ Bir başka aile bireyinin odasında ☐ Diğer:……..

7) Veliniz İnternet ve bilgisayar kullanımınızla ilgili olarak ne gibi kısıtlamalar getiriyor?

☐ Süre kısıtlaması

☐ Kullanılan programlara yönelik kısıtlama

☐ İnternet'te gezinilen sitelere yönelik kısıtlama

☐ Maddi kısıtlama

☐ Hiçbiri

☐ Diğer:…….

8) Bilgisayar kullanırken yardım için kimlere/nelere başvuruyorsunuz?

☐ Aile üyelerine ☐ Arkadaşlarıma ☐ Kitaplara ☐ İnternet kaynaklarına

☐ Hiçbiri ☐ Diğer:……

9) Aşağıdaki teknolojik cihazlardan en çok hangisi kullanıyorsunuz? (En çok kullandığınızdan en az kullandığınıza doğru 1'den başlayarak 4'e kadar sıralayınız. En çok kullandığınız 1 puan, en az kullandığınız 4 puandır.)

☐ Tablet ☐ Laptop ☐ Cep Telefonu ☐ Masaüstü Bilgisayar

10) Teknolojik cihazları (tablet, laptop, cep telefonu, masaüstü bilgisayar) hangi amaçlarla kullanıyorsunuz?

☐ Haberleşmek

☐ Sosyal medyada gezinmek

☐ Ders Çalışmak

☐ Oyun Oynamak

☐ Diğer:…….

11) Kullandığınız teknolojik cihazları paylaşımlı olarak kullanır mısınız?

☐ Evet ☐ Hayır

12) İnternette günde ne kadar süre vakit geçiyorsunuz?

☐ 0-1 saat ☐ 1-2 saat ☐ 2-4 saat ☐ 5 saatten fazla

13) Bilgisayarda günde ne kadar süre vakit geçiyorsunuz?

☐ 0-1 saat ☐ 1-2 saat ☐ 2-4 saat ☐ 5 saatten fazla

14) Haftada toplam kaç saat bilgisayarda vakit geçiyorsunuz?

☐ 0-1 saat ☐ 1-2 saat ☐ 2-4 saat ☐ 5-10 saat ☐ 10 saatten fazla

15) Herhangi bir sosyal ağa üye misiniz?

☐ Evet ☐ Hayır

16) Üye olduğunuz sosyal ağ hesaplarını işaretleyiniz. (15.soruya cevabınız evet ise soruyu yanıtlayınız.)

☐ Facebook

☐

Twitter

☐ Instagram

☐ Snapchat

☐ Diğer:……

17) E-posta hesabınız var mı?

☐ Evet ☐ Hayır

Ek 2: Öğretmenlere Yönelik Geliştirilen Demografik Bilgi Anketi

LÜTFEN BU DÖKÜMANI DİKKATLİCE OKUMAK İÇİN ZAMAN AYIRINIZ

Sizi Prof. Dr. Mustafa Murat İNCEOĞLU tarafından yürütülen "Bilgi Güvenliğine Yönelik Öğrenci, Öğretmen, Veli Ve Okul Yöneticilerinin Farkındalıklarının İncelenmesi" başlıklı **araştırmaya** davet ediyoruz. Bu araştırmaya katılıp katılmama kararını vermeden önce, araştırmanın neden ve nasıl yapılacağını bilmeniz gerekmektedir. Bu nedenle bu formun okunup anlaşılması büyük önem taşımaktadır. Eğer anlayamadığınız ve sizin için açık olmayan şeyler varsa, ya da daha fazla bilgi isterseniz bize sorunuz.

Bu çalışmaya katılmak tamamen **gönüllülük** esasına dayanmaktadır. Çalışmaya **katılmama** veya katıldıktan sonra herhangi bir anda çalışmadan **çıkma** hakkında sahipsiniz. **Çalışmayı yanıtlamanız, araştırmaya katılım için onam verdiğiniz** biçiminde yorumlanacaktır. Size verilen **formlardaki** soruları yanıtlarken kimsenin baskısı veya telkini altında olmayın. Bu formlardan elde edilecek kişisel bilgiler tamamen gizli tutulacak ve yalnızca araştırma amacı ile kullanılacaktır.

DEMOGRAFİK BİLGİ ANKETİ

Değerli öğretmenler,

Bilgi güvenliğine yönelik yapılan bilimsel bir çalışma için hazırlanan bu anket ile teknoloji kullanımına yönelik alışkanlıklarınız incelenecektir. Anket ile verdiğiniz cevaplara yalnızca araştırmacı tarafından erişim sağlanacaktır. Araştırmaya katılımınız için teşekkür ederim.

Prof. Dr. Mustafa Murat İNCEOĞLU, mustafainceoglu@yahoo.com

Cansu ALTUNSABAN, cansu.altunsaban@gmail.com

1) Cinsiyetiniz Nedir?

☐ Kadın ☐ Erkek

2) Kaç yıldır öğretmenlik mesleğini icra ediyorsunuz?

☐ 1 – 5 Yıl ☐ 5 – 10 Yıl ☐ 10 – 15 Yıl ☐ 15 – 20 Yıl ☐ 20 Yıl ve Üstü

3) Evde kendinize ait bir bilgisayarınız var mı?

☐ Var ☐ Yok

4) Aşağıdakilerden en çok hangisi kullanıyorsunuz? (En çok kullandığınızdan en az kullandığınıza doğru 1'den başlayarak 4'e kadar sıralayınız. En çok kullandığınız 1 puan, en az kullandığınız 4 puandır.)

☐ Tablet ☐ Laptop ☐ Cep Telefonu ☐ Masaüstü Bilgisayar

5) Teknolojik cihazları (tablet, laptop, cep telefonu, masaüstü bilgisayar) hangi amaçlarla kullanıyorsunuz?

- ☐ Haberleşmek
- ☐ Sosyal medyada gezinmek
- ☐ İş ile ilgili çalışmaları yapmak
- ☐ E-mailleri incelemek
- ☐ Bankacılık işlemlerini yapmak
- ☐ Oyun Oynamak
- ☐ E-devlet ile ilgili işlemleri yapmak (hastane randevusu almak, trafik borcu ödemek vb.)
- ☐ Diğer:…….

6) Kullandığınız teknolojik cihazları paylaşımlı olarak kullanır mısınız?

☐ Evet ☐ Hayır

7) İnternette günde ne kadar süre vakit geçiyorsunuz?

☐ 0-1 saat ☐ 1-2 saat ☐ 2-4 saat ☐ 5 saatten fazla

8) Bilgisayarda günde ne kadar süre vakit geçiyorsunuz?

☐ 0-1 saat ☐ 1-2 saat ☐ 2-4 saat ☐ 5 saatten fazla

9) Haftada toplam kaç saat bilgisayarda vakit geçiyorsunuz?

☐ 0-1 saat ☐ 1-2 saat ☐ 2-4 saat ☐ 5-10 saat ☐ 10 saatten fazla

10) Sosyal medya kullanımının ve İnternet'in zararlı yönleri konusunda gündemi takip eder misiniz?

☐ Evet ☐ Hayır

11) Sosyal medya kullanımının ve İnternet'in zararlı yönleri konusunda öğrencinizi bilgilendirir misiniz?

☐ Evet ☐ Hayır

12) Hiç sosyal medya ya da İnternet aracılığıyla dolandırıldınız mı?

☐ Evet ☐ Hayır

13) Hiç sosyal medya ya da elektronik posta hesaplarınız başkaları tarafından ele geçirildi mi?

☐ Evet ☐ Hayır

14) Herhangi bir sosyal ağa üye misiniz?

☐ Evet ☐ Hayır

15) Üye olduğunuz sosyal ağ hesaplarını işaretleyiniz. (14.soruya cevabınız evet ise soruyu yanıtlayınız.)

☐ Facebook

☐ Twitter

☐ Instagram

☐ Snapchat

☐ Diğer:……

16) E-posta hesabınız var mı?

☐ Evet ☐ Hayır

Ek 3: Öğrencilere Yönelik Geliştirilen Yarı Yapılandırılmış Görüşme Soruları

LÜTFEN BU DÖKÜMANI DİKKATLİCE OKUMAK İÇİN ZAMAN AYIRINIZ

Sizi Prof. Dr. Mustafa Murat İNCEOĞLU tarafından yürütülen "Bilgi Güvenliğine Yönelik Öğrenci, Öğretmen, Veli Ve Okul Yöneticilerinin Farkındalıklarının İncelenmesi" başlıklı **araştırmaya** davet ediyoruz. Bu araştırmaya katılıp katılmama kararını vermeden önce, araştırmanın neden ve nasıl yapılacağını bilmeniz gerekmektedir. Bu nedenle bu formun okunup anlaşılması büyük önem taşımaktadır. Eğer anlayamadığınız ve sizin için açık olmayan şeyler varsa, ya da daha fazla bilgi isterseniz bize sorunuz.

Bu çalışmaya katılmak tamamen **gönüllülük** esasına dayanmaktadır. Çalışmaya **katılmama** veya katıldıktan sonra herhangi bir anda çalışmadan **çıkma** hakkında sahipsiniz. **Çalışmayı yanıtlamanız, araştırmaya katılım için onam verdiğiniz** biçiminde yorumlanacaktır. Size verilen **formlardaki** soruları yanıtlarken kimsenin baskısı veya telkini altında olmayın. Bu formlardan elde edilecek kişisel bilgiler tamamen gizli tutulacak ve yalnızca araştırma amacı ile kullanılacaktır.

GÖRÜŞME SORULARI

1) Kendinize ait bilgisayar, cep telefonu veya tabletiniz var mı?
2) (Varsa) Evinizde yer alan bilgisayar hangi odada bulunmaktadır?
3) (Varsa) Teknolojik cihazları (tablet, cep telefonu vb.) hangi amaçlar (haberleşme, oyun, sohbet/chat, ders çalışma vb.) doğrultusunda kullanıyorsunuz?
4) (Varsa) Evde bilgisayar kullanımınıza yönelik bir kısıtlama mevcut mu? Kısıtlama mevcut ise, bu konuda ne düşünüyorsunuz? Sizce, neden veliniz size böyle kısıtlamalar getiriyor?
5) Öğretmenleriniz güvenli bilgisayar ve İnternet kullanımı hakkında size ne gibi yönlendirmede bulunuyor?
6) Arkadaşlarınızdan bilgisayar kullanımı konusunda yardım alıyor musunuz? Cevabınız evet ise, arkadaşlarınız ne gibi yardımda bulunuyor?
7) Bilgi güvenliği kavramını daha önce duydunuz mu? Bu konuda bir bilginiz var mı?
8) (Varsa) Bilgisayarınızda veya kullandığınız diğer teknolojik cihazlarda (tablet/ipad, cep telefonu vb.) antivirüs programı yüklü mü?
9) Antivirüs programlarının gerekliliği ve işlevi hakkında neler düşünüyorsunuz?
10) (Varsa) Bilgisayarınızda şifresi kaldırılmış (cracklenmiş) program kullanıyor musunuz? Bu şekilde lisanssız program kullanmanın zararları hakkındaki yorumunuz nedir?
11) Herhangi bir sosyal medya hesabına üye misiniz?

12) Sosyal medya kullanımının ve İnternet'in zararlı yönleri konusunda bilgi sahibi misiniz? Cevabınız evet ise, bu konudaki düşünceleriniz nelerdir?

13) Sosyal medya kullanımının ve İnternet'in zararlı yönleri doğrultusunda yaşadığınız kötü bir tecrübe (sosyal medya hesabının başkasının eline geçmesi, dolandırıcılık vb.) var mı?

14) Sosyal medya kullanımının ve İnternet'in zararlı yönlerine yönelik olarak ne gibi önlemler alınmalı? Siz bu konuda herhangi bir önlem alıyor musunuz?

Ek 4: Öğretmenlere Yönelik Geliştirilen Yarı Yapılandırılmış Görüşme Soruları

LÜTFEN BU DÖKÜMANI DİKKATLİCE OKUMAK İÇİN ZAMAN AYIRINIZ

Sizi Prof. Dr. Mustafa Murat İNCEOĞLU tarafından yürütülen "Bilgi Güvenliğine Yönelik Öğrenci, Öğretmen, Veli Ve Okul Yöneticilerinin Farkındalıklarının İncelenmesi" başlıklı **araştırmaya** davet ediyoruz. Bu araştırmaya katılıp katılmama kararını vermeden önce, araştırmanın neden ve nasıl yapılacağını bilmeniz gerekmektedir. Bu nedenle bu formun okunup anlaşılması büyük önem taşımaktadır. Eğer anlayamadığınız ve sizin için açık olmayan şeyler varsa, ya da daha fazla bilgi isterseniz bize sorunuz.

Bu çalışmaya katılmak tamamen **gönüllülük** esasına dayanmaktadır. Çalışmaya **katılmama** veya katıldıktan sonra herhangi bir anda çalışmadan **çıkma** hakkında sahipsiniz. **Çalışmayı yanıtlamanız, araştırmaya katılım için onam verdiğiniz** biçiminde yorumlanacaktır. Size verilen **formlardaki** soruları yanıtlarken kimsenin baskısı veya telkini altında olmayın. Bu formlardan elde edilecek kişisel bilgiler tamamen gizli tutulacak ve yalnızca araştırma amacı ile kullanılacaktır.

GÖRÜŞME SORULARI

1) Kaç yıldır öğretmenlik mesleğini icra ediyorsunuz?
2) Kendinize ait bilgisayar, cep telefonu, tablet vb. teknolojik cihazlarınız var mı?
3) (Varsa) Teknolojik cihazları (tablet, cep telefonu vb.) hangi amaçlar (haberleşme, oyun, sohbet/chat, iş, e-devlet vb.) doğrultusunda kullanıyorsunuz?
4) Bilgi güvenliği kavramını daha önce duydunuz mu? Bu konuda bir bilginiz var mı?
5) (Varsa) Evinizde kullandığınız teknolojik cihazlarda antivirüs yazılım mevcut mu? Antivirüs programlarının gerekliliği hakkında neler düşünüyorsunuz?
6) (Varsa) Bilgisayarınızda şifresi kaldırılmış (cracklenmiş) program kullanıyor musunuz? Bu şekilde lisanssız program kullanmanın zararları hakkındaki yorumunuz nedir?
7) Herhangi bir sosyal medya hesabına üye misiniz?
8) Sosyal medya kullanımının ve İnternet'in zararlı yönleri konusunda gündemi takip eder misiniz?
9) Sosyal medya kullanımının ve İnternet'in zararlı yönleri konusunda öğrencilerinizi bilgilendirir misiniz?
10) Hiç sosyal medya ya da İnternet aracılığıyla dolandırıldınız mı?
11) Hiç sosyal medya ya da elektronik posta hesaplarınız başkaları tarafından ele geçirildi mi?
12) Sosyal medya kullanımının ve İnternet'in zararlı yönlerine yönelik olarak ne gibi önlemler alınmalı? Siz bu konuda herhangi bir önlem alıyor musunuz?

13) Sosyal medya kullanımının ve İnternet'in zararlı yönlerine yönelik olarak alınması gereken önlemler konusunda öğrencilerinizi yönlendiriyor musunuz?

Ek 5: Velilere Yönelik Geliştirilen Yarı Yapılandırılmış Görüşme Soruları

LÜTFEN BU DÖKÜMANI DİKKATLİCE OKUMAK İÇİN ZAMAN AYIRINIZ

Sizi Prof. Dr. Mustafa Murat İNCEOĞLU tarafından yürütülen "Bilgi Güvenliğine Yönelik Öğrenci, Öğretmen, Veli Ve Okul Yöneticilerinin Farkındalıklarının İncelenmesi" başlıklı **araştırmaya** davet ediyoruz. Bu araştırmaya katılıp katılmama kararını vermeden önce, araştırmanın neden ve nasıl yapılacağını bilmeniz gerekmektedir. Bu nedenle bu formun okunup anlaşılması büyük önem taşımaktadır. Eğer anlayamadığınız ve sizin için açık olmayan şeyler varsa, ya da daha fazla bilgi isterseniz bize sorunuz.

Bu çalışmaya katılmak tamamen **gönüllülük** esasına dayanmaktadır. Çalışmaya **katılmama** veya katıldıktan sonra herhangi bir anda çalışmadan **çıkma** hakkında sahipsiniz. **Çalışmayı yanıtlamanız, araştırmaya katılım için onam verdiğiniz** biçiminde yorumlanacaktır. Size verilen **formlardaki** soruları yanıtlarken kimsenin baskısı veya telkini altında olmayın. Bu formlardan elde edilecek kişisel bilgiler tamamen gizli tutulacak ve yalnızca araştırma amacı ile kullanılacaktır.

GÖRÜŞME SORULARI

1) Kaç çocuğunuz var?
2) Evinizde bilgisayar var mı? Varsa, hangi odada/odalarda bulunmaktadır?
3) Çocuğunuzun/çocuklarınızın kendisine ait tableti, cep telefonu veya bilgisayarı var mı?
4) (Varsa) Çocuğunuzun/çocuklarınızın bilgisayarında, cep telefonunda ya da tabletinde yaptıklarını hangi sıklıkta incelersiniz?
5) (Varsa) Çocuğunuzun/çocuklarınızın bilgisayarı hangi amaçla kullandığı ve bilgisayarda hangi programları kullandığı hakkında bilgi sahibi misiniz?
6) Bilgi güvenliği kavramını daha önce duydunuz mu? Bu konuda bir bilginiz var mı?
7) (Varsa) Evinizde kullandığınız teknolojik cihazlarda antivirüs programı mevcut mu? Antivirüs programlarının gerekliliği hakkında neler düşünüyorsunuz?
8) Sosyal medya kullanımının ve İnternet'in zararlı yönleri konusunda gündemi takip eder misiniz?
9) Sosyal medya kullanımının ve İnternet'in zararlı yönleri konusunda çocuğunuzu/çocuklarınızı bilgilendirir misiniz?
10) Hiç sosyal medya ya da İnternet aracılığıyla dolandırıldınız mı?
11) Hiç sosyal medya ya da elektronik posta hesaplarınız başkaları tarafından ele geçirildi mi?

12) Sosyal medya ve İnternet kullanımının zararlarından kendinizi ve çocuğunuzu/çocuklarınızı korumak için ne gibi önlemler alıyorsunuz? Bu konuda kullandığınız programlar var mı?

Ek 6: Bilgilendirilmiş Onam Formu

EGE ÜNİVERSİTESİ

BİLİMSEL ARAŞTIRMA ve YAYIN ETİĞİ KURULLARI (EGEBAYEK)

BİLGİLENDİRİLMİŞ ONAM FORMU

LÜTFEN BU DÖKÜMANI DİKKATLİCE OKUMAK İÇİN ZAMAN AYIRINIZ

Sizi Prof. Dr. Mustafa Murat İNCEOĞLU tarafından yürütülen "Bilgi Güvenliğine Yönelik Öğrenci, Öğretmen, Veli Ve Okul Yöneticilerinin Farkındalıklarının İncelenmesi" başlıklı **araştırmaya** davet ediyoruz. Bu araştırmaya katılıp katılmama kararını vermeden önce, araştırmanın neden ve nasıl yapılacağını bilmeniz gerekmektedir. Bu nedenle bu formun okunup anlaşılması büyük önem taşımaktadır. Eğer anlayamadığınız ve sizin için açık olmayan şeyler varsa, ya da daha fazla bilgi isterseniz bize sorunuz.

Bu çalışmaya katılmak tamamen **gönüllülük** esasına dayanmaktadır. Çalışmaya **katılmama** veya katıldıktan sonra herhangi bir anda çalışmadan **çıkma** hakkında sahipsiniz. **Çalışmayı yanıtlamanız, araştırmaya katılım için onam verdiğiniz** biçiminde yorumlanacaktır. Size verilen **formlardaki** soruları yanıtlarken kimsenin baskısı veya telkini altında olmayın. Bu formlardan elde edilecek kişisel bilgiler tamamen gizli tutulacak ve yalnızca araştırma amacı ile kullanılacaktır.

1. **Araştırmayla İlgili Bilgiler:**
   a. Araştırmanın Amacı: Devlet okulları ve özel okullarda öğrenim gören öğrencilerin, öğrenci velilerinin, öğretmenlerin, okul yöneticilerinin bilgi güvenliği konusundaki farkındalıklarını araştırmak ve söz konusu bu paydaşların görüşlerinin devlet okulları ile özel okullar arasında farklılık gösterip göstermediğini incelemektir.
   b. Araştırmanın İçeriği: Araştırma kapsamında devlet okulu ve özel okulda ortaokul ve lise düzeyinde öğrenim gören öğrenci, bu öğrencilerin velileri, söz konusu okullarda görev yapan öğretmen ve okul yöneticilerinin bilgi güvenliği alanındaki farkındalıkları incelenecek olup, belirlenen örneklemin bilgi güvenliği alanındaki görüşleri araştırılıp, devlet okulu ve özel okulda yer alan öğrenci,

veli, öğretmen ve okul yöneticilerinin görüşleri karşılaştırılarak değerlendirilecektir.

c. Araştırmanın Nedeni: ☐ Özgün araştırma ■ Tez çalışması
d. Araştırmanın Öngörülen Süresi (*Araştırma takviminde öngörülen süredir*): 10 ay
e. Araştırmaya Katılması Beklenen Katılımcı/Gönüllü Sayısı: 300
f. Araştırmanın Yapılacağı Yerler: Suphi Koyuncuoğlu Ortaokulu, Süleyman Demirel Çok Programlı Anadolu Lisesi, Özel Yeşeren Ortaokulu ve Özel Yeşeren Anadolu Lisesi

2. Çalışmaya Katılım Onayı:

Yukarıda yer alan ve araştırmadan önce katılımcıya/gönüllüye verilmesi gereken bilgileri okudum ve katılmam istenen çalışmanın kapsamını ve amacını, gönüllü olarak üzerime düşen sorumlulukları tamamen anladım. **Çalışma hakkında yazılı ve sözlü açıklama aşağıda adı belirtilen araştırmacı tarafından yapıldı, soru sorma ve tartışma imkanı buldum ve tatmin edici yanıtlar aldım. Bana, çalışmanın muhtemel riskleri ve faydaları sözlü olarak da anlatıldı.** Bu çalışmayı istediğim zaman ve herhangi bir neden belirtmek zorunda kalmadan bırakabileceğimi ve bıraktığım takdirde herhangi bir olumsuzluk ile karşılaşmayacağımı anladım.

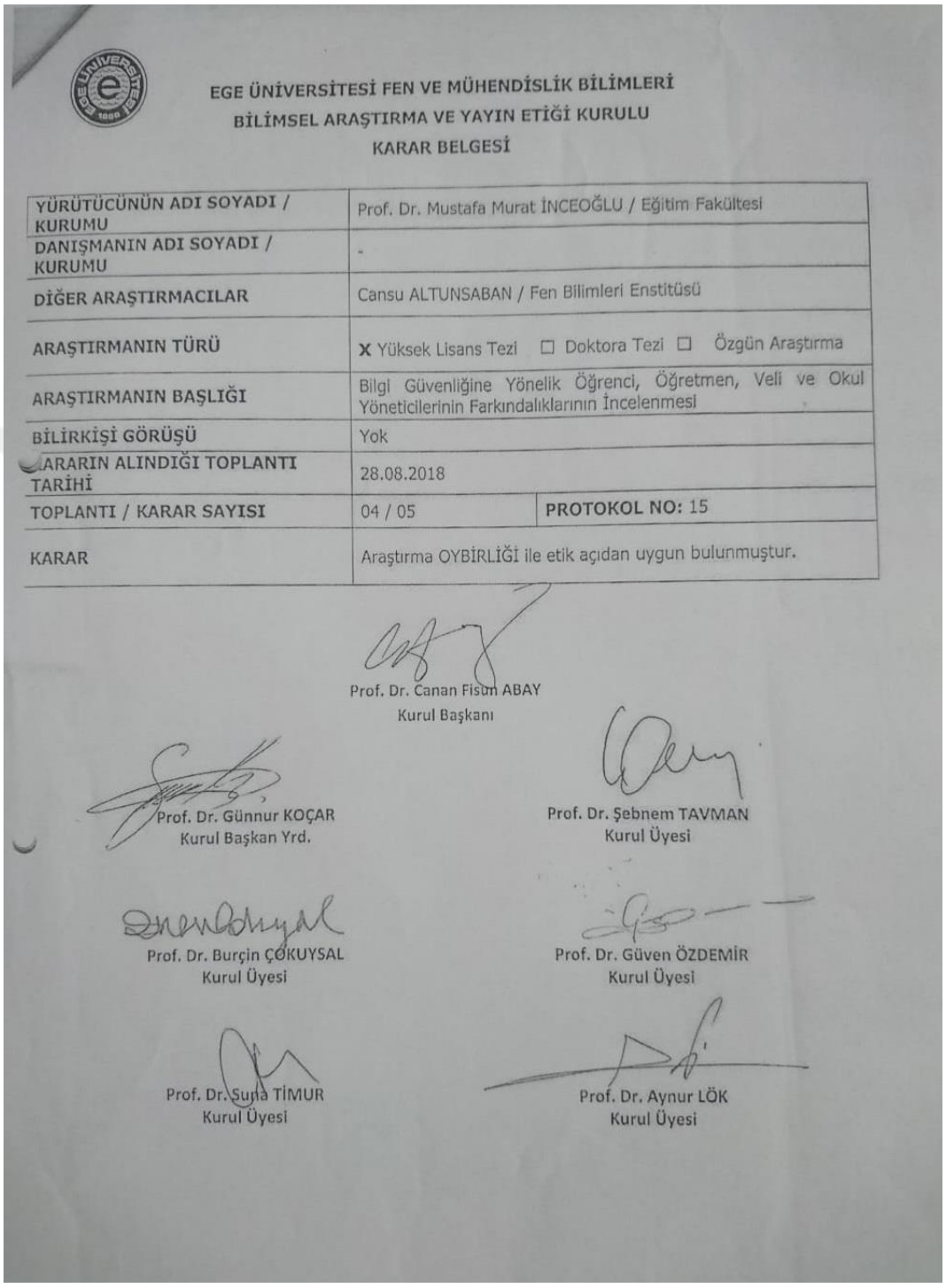
Bu koşullarda söz konusu araştırmaya kendi isteğimle, hiçbir baskı ve zorlama olmaksızın katılmayı kabul ediyorum.

Katılımcının (Kendi el yazısı ile)
Adı-
Soyadı:.....
İmzası:

(Varsa) Velayet veya Vesayet Altında Bulunanlar İçin;
Veli veya Vasisinin (kendi el yazısı ile)
Adı-
Soyadı:.....
İmzası:

Not: *Bu form, iki nüsha halinde düzenlenir. Bu nüshalardan biri imza karşılığında gönüllü kişiye verilir, diğeri araştırmacı tarafından saklanır.*

Ek 7: Etik Kurulu Onay Raporu



EGE ÜNİVERSİTESİ FEN VE MÜHENDİSLİK BİLİMLERİ
BİLİMSEL ARAŞTIRMA VE YAYIN ETİĞİ KURULU
KARAR BELGESİ

YÜRÜTÜCÜNÜN ADI SOYADI / KURUMU	Prof. Dr. Mustafa Murat İNCEOĞLU / Eğitim Fakültesi	
DANIŞMANIN ADI SOYADI / KURUMU	-	
DİĞER ARAŞTIRMACILAR	Cansu ALTUNSABAN / Fen Bilimleri Enstitüsü	
ARAŞTIRMANIN TÜRÜ	X Yüksek Lisans Tezi ☐ Doktora Tezi ☐ Özgün Araştırma	
ARAŞTIRMANIN BAŞLIĞI	Bilgi Güvenliğine Yönelik Öğrenci, Öğretmen, Veli ve Okul Yöneticilerinin Farkındalıklarının İncelenmesi	
BİLİRKİŞİ GÖRÜŞÜ	Yok	
KARARIN ALINDIĞI TOPLANTI TARİHİ	28.08.2018	
TOPLANTI / KARAR SAYISI	04 / 05	PROTOKOL NO: 15
KARAR	Araştırma OYBİRLİĞİ ile etik açıdan uygun bulunmuştur.	

Prof. Dr. Canan Fisun ABAY
Kurul Başkanı

Prof. Dr. Günnur KOÇAR
Kurul Başkan Yrd.

Prof. Dr. Şebnem TAVMAN
Kurul Üyesi

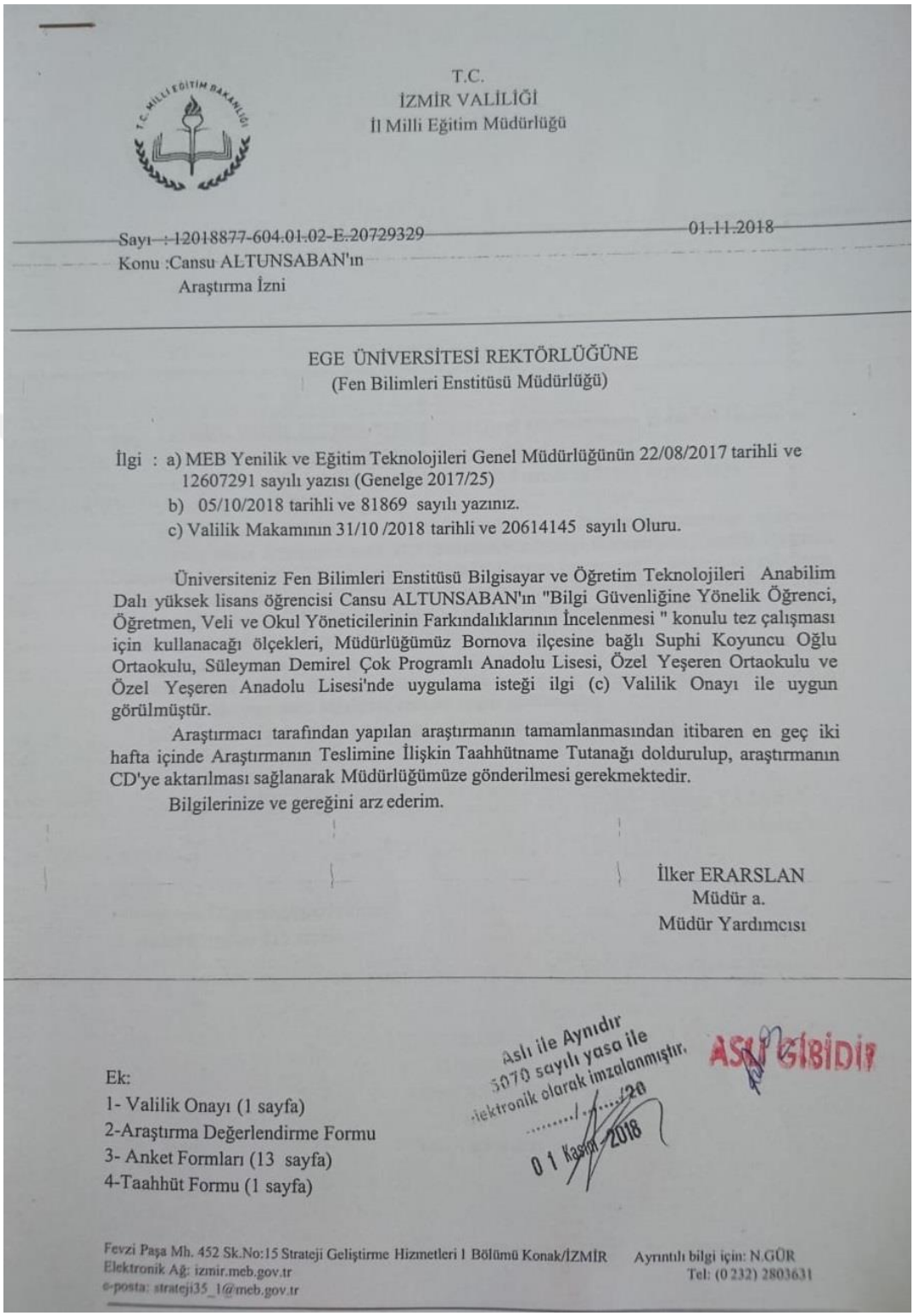
Prof. Dr. Burçin ÇOKUYSAL
Kurul Üyesi

Prof. Dr. Güven ÖZDEMİR
Kurul Üyesi

Prof. Dr. Suna TİMUR
Kurul Üyesi

Prof. Dr. Aynur LÖK
Kurul Üyesi

Ek 8: İl Milli Eğitim Müdürlüğü Araştırma Onayı



T.C.
İZMİR VALİLİĞİ
İl Milli Eğitim Müdürlüğü

Sayı : 12018877-604.01.02-E.20729329 — 01.11.2018
Konu : Cansu ALTUNSABAN'ın
Araştırma İzni

EGE ÜNİVERSİTESİ REKTÖRLÜĞÜNE
(Fen Bilimleri Enstitüsü Müdürlüğü)

İlgi : a) MEB Yenilik ve Eğitim Teknolojileri Genel Müdürlüğünün 22/08/2017 tarihli ve 12607291 sayılı yazısı (Genelge 2017/25)
b) 05/10/2018 tarihli ve 81869 sayılı yazınız.
c) Valilik Makamının 31/10 /2018 tarihli ve 20614145 sayılı Oluru.

Üniversiteniz Fen Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Anabilim Dalı yüksek lisans öğrencisi Cansu ALTUNSABAN'ın "Bilgi Güvenliğine Yönelik Öğrenci, Öğretmen, Veli ve Okul Yöneticilerinin Farkındalıklarının İncelenmesi " konulu tez çalışması için kullanacağı ölçekleri, Müdürlüğümüz Bornova ilçesine bağlı Suphi Koyuncu Oğlu Ortaokulu, Süleyman Demirel Çok Programlı Anadolu Lisesi, Özel Yeşeren Ortaokulu ve Özel Yeşeren Anadolu Lisesi'nde uygulama isteği ilgi (c) Valilik Onayı ile uygun görülmüştür.

Araştırmacı tarafından yapılan araştırmanın tamamlanmasından itibaren en geç iki hafta içinde Araştırmanın Teslimine İlişkin Taahhütname Tutanağı doldurulup, araştırmanın CD'ye aktarılması sağlanarak Müdürlüğümüze gönderilmesi gerekmektedir.

Bilgilerinize ve gereğini arz ederim.

İlker ERARSLAN
Müdür a.
Müdür Yardımcısı

Ek:
1- Valilik Onayı (1 sayfa)
2-Araştırma Değerlendirme Formu
3- Anket Formları (13 sayfa)
4-Taahhüt Formu (1 sayfa)

Aslı ile Aynıdır
5070 sayılı yasa ile
elektronik olarak imzalanmıştır.
...../...../20
01 Kasım 2018

ASLI GİBİDİR

Fevzi Paşa Mh. 452 Sk.No:15 Strateji Geliştirme Hizmetleri I Bölümü Konak/İZMİR
Elektronik Ağ: izmir.meb.gov.tr
e-posta: strateji35_1@meb.gov.tr

Ayrıntılı bilgi için: N.GÜR
Tel: (0 232) 2803631

Ek 9: İl Milli Eğitim Müdürlüğü Araştırma Onayı 2

T.C.
İZMİR VALİLİĞİ
İl Milli Eğitim Müdürlüğü

ARAŞTIRMA DEĞERLENDİRME FORMU

ARAŞTIRMA SAHİBİNİN	
Adı Soyadı	Cansu ALTUNSABAN
Kurumu / Üniversitesi	Ege Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü
Araştırma yapılacak iller	İzmir
Araştırma yapılacak eğitim kurumu ve kademesi	Suphi Koyuncuoğlu Ortaokulu Süleyman Demirel Çok Programlı Anadolu Lisesi Özel Yeşeren Ortaokulu Özel Yeşeren Anadolu Lisesi
Araştırmanın konusu	Bilgi Güvenliğine Yönelik Öğrenci, Öğretmen, Veli ve Okul Yöneticilerinin Farkındalıklarının İncelenmesi
Üniversite / Kurum onayı	---
Araştırma/proje/ödev/tez önerisi	Bilgi Güvenliğine Yönelik Öğrenci, Öğretmen, Veli ve Okul Yöneticilerinin Farkındalıklarının İncelenmesi (Yüksek Lisans Tezi)
Veri toplama araçları	Bilgi Güvenliği Farkındalık Ölçeği(Öğrenci-öğretmen-veli) Demografik Bilgi Anketi (Öğrenci-öğretmen-veli) Görüşme Soruları (Öğrenci-öğretmen-veli)
Görüş istenilecek Birim/Birimler	-----

KOMİSYON GÖRÜŞÜ

İlgi: Milli Eğitim Bakanlığı'nın 22/08/2017 tarihli ve 3558626-10.06-e.12607291 sayılı Araştırma, yarışma ve Sosyal Etkinlik İzinleri Konulu, 2017/25 Sayılı Genelgesi.

Genelge gereğince; araştırma başvurusu olması gereken nitelikler açısından incelenmiş olup, araştırmanın 2018-2019 öğretim yılında eğitim öğretimi aksatmayacak ve eğitim kurumları yöneticilerinin uygun gördüğü şekli ile yapılmasına oybirliği ile karar verilmiştir.

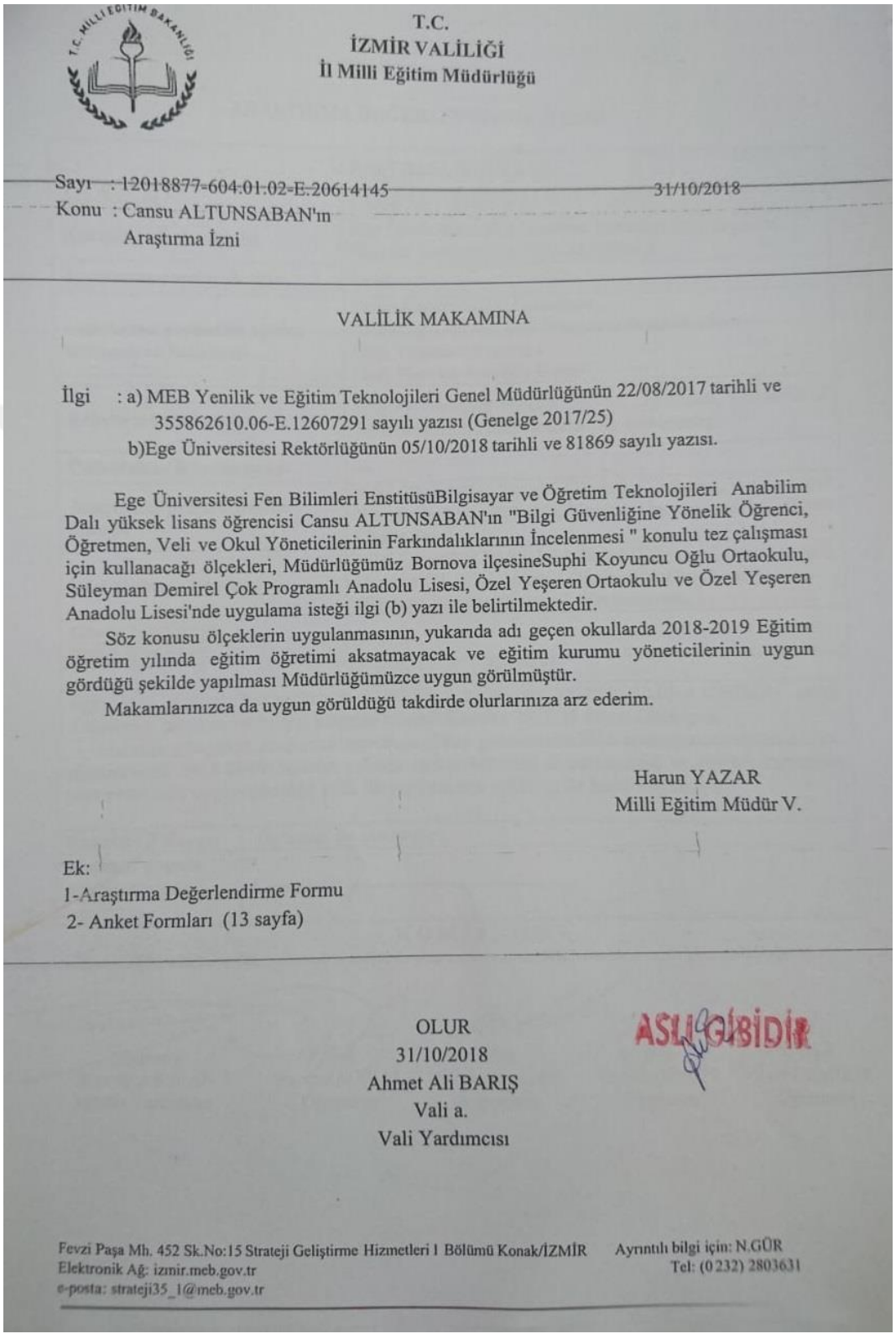
Komisyon Kararı	Oybirliği ile alınmıştır.
Muhalif üyenin Adı ve Soyadı: ----	**Gerekçesi; ----------**

KOMİSYON

26./10/2018

(Başkan)	Üye	Üye	Üye	Üye
İlker ERARSLAN	Nurdan MARAL	Selahattin ANIK	Özlem GÖRÜR	Aslı DEMİREL
Müdür Yardımcısı	Öğretmen	Öğretmen	Öğretmen	Öğretmen

Ek 10: İl Milli Eğitim Müdürlüğü Araştırma Onayı 3



T.C.
İZMİR VALİLİĞİ
İl Milli Eğitim Müdürlüğü

Sayı : 12018877-604.01.02-E.20614145 31/10/2018
Konu : Cansu ALTUNSABAN'ın
Araştırma İzni

VALİLİK MAKAMINA

İlgi : a) MEB Yenilik ve Eğitim Teknolojileri Genel Müdürlüğünün 22/08/2017 tarihli ve 355862610.06-E.12607291 sayılı yazısı (Genelge 2017/25)
b)Ege Üniversitesi Rektörlüğünün 05/10/2018 tarihli ve 81869 sayılı yazısı.

Ege Üniversitesi Fen Bilimleri EnstitüsüBilgisayar ve Öğretim Teknolojileri Anabilim Dalı yüksek lisans öğrencisi Cansu ALTUNSABAN'ın "Bilgi Güvenliğine Yönelik Öğrenci, Öğretmen, Veli ve Okul Yöneticilerinin Farkındalıklarının İncelenmesi " konulu tez çalışması için kullanacağı ölçekleri, Müdürlüğümüz Bornova ilçesineSuphi Koyuncu Oğlu Ortaokulu, Süleyman Demirel Çok Programlı Anadolu Lisesi, Özel Yeşeren Ortaokulu ve Özel Yeşeren Anadolu Lisesi'nde uygulama isteği ilgi (b) yazı ile belirtilmektedir.

Söz konusu ölçeklerin uygulanmasının, yukarıda adı geçen okullarda 2018-2019 Eğitim öğretim yılında eğitim öğretimi aksatmayacak ve eğitim kurumu yöneticilerinin uygun gördüğü şekilde yapılması Müdürlüğümüzce uygun görülmüştür.

Makamlarınızca da uygun görüldüğü takdirde olurlarınıza arz ederim.

Harun YAZAR
Milli Eğitim Müdür V.

Ek:
1-Araştırma Değerlendirme Formu
2- Anket Formları (13 sayfa)

OLUR
31/10/2018
Ahmet Ali BARIŞ
Vali a.
Vali Yardımcısı

ASLI GİBİDİR

Fevzi Paşa Mh. 452 Sk.No:15 Strateji Geliştirme Hizmetleri I Bölümü Konak/İZMİR
Elektronik Ağ: izmir.meb.gov.tr
e-posta: strateji35_1@meb.gov.tr

Ayrıntılı bilgi için: N.GÜR
Tel: (0232) 2803631