



**ORTAOKUL ÖĞRENCİLERİNİN BİLGİ GÜVENLİĞİ  
FARKINDALIK DÜZEYİNİN BELİRLENMESİ**

**Başak Özen Serter**

**YÜKSEK LİSANS TEZİ**

**EĞİTİM BİLİMLERİ ANABİLİM DALI**

**EĞİTİM TEKNOLOJİSİ BİLİM DALI**

**GAZİ ÜNİVERSİTESİ**

**EĞİTİM BİLİMLERİ ENSTİTÜSÜ**

**AĞUSTOS 2021**

## TELİF HAKKI VE TEZ FOTOKOPİ İZİN FORMU

Bu tezin tüm hakları saklıdır. Kaynak göstermek koşuluyla tezin teslim tarihinden itibaren 12 (on iki) ay sonra tezden fotokopi çekilebilir.

### YAZARIN

Adı : Başak  
Soyadı : ÖZEN SERTER  
Bölümü : Eğitim Teknolojisi Bilim Dalı  
İmza :  
Teslim tarihi :

### TEZİN

Türkçe Adı : Ortaokul Öğrencilerinin Bilgi Güvenliği Farkındalık Düzeyinin Belirlenmesi  
İngilizce Adı : An Analysis of Information Security Awareness Level Among Middle School Students

## **ETİK İLKELERE UYGUNLUK BEYANI**

Tez yazma sürecinde bilimsel ve etik ilkelere uyduđumu, yararlandıđım tüm kaynakları kaynak gösterme ilkelerine uygun olarak kaynakçada belirttiđimi ve bu bölümler dıřındaki tüm ifadelerin řahsıma ait olduđunu beyan ederim.

Yazar Adı Soyadı : Başak ÖZEN SERTER

İmza : .....

## JÜRİ ONAY SAYFASI

Başak ÖZEN SERTER tarafından hazırlanan “Ortaokul Öğrencilerinin Bilgi Güvenliği Farkındalık Düzeyinin Belirlenmesi” adlı tez çalışması aşağıdaki jüri tarafından oy birliği / oy çokluğu ile Gazi Üniversitesi Eğitim Teknolojileri Bilim Dalı’nda Yüksek Lisans tezi olarak kabul edilmiştir.

**Danışman:** Prof. Dr. Şaban ÇETİN

Eğitim Programları ve Öğretim Anabilim Dalı, Gazi Üniversitesi .....

**Başkan:** Doç. Dr. Aslıhan Selcen BİNGÖL

Eğitim Programları ve Öğretim Anabilim Dalı, Gazi Üniversitesi .....

**Üye:** DR. Öğr.Üyesi Cennet GÖLOĞLU DEMİR

Çocuk Gelişimi Anabilim Dalı, Bandırma On Yedi Eylül Üniversitesi .....

Tez Savunma Tarihi: 02/08/2021

Bu tezin Eğitim Teknolojileri ilim Dalı’nda Yüksek Lisans tezi olması için şartları yerine getirdiğini onaylıyorum.

Prof. Dr. Yücel GELİŞLİ

Eğitim Bilimleri Enstitüsü Müdürü

.....



*Varlıklarından güç aldığım canım anneme, canım babama...*

## TEŞEKKÜR

Yüksek lisans çalışmalarım süresince bilgisi, deneyimi ve kıymetli katkıları ile bana rehberlik eden değerli hocam Sayın Prof. Dr. Şaban ÇETİN'e, her durumda olduğu gibi bu çalışmamda da sabır ve ilgisini esirgemeyen, büyük destekleriyle bana güç veren ve çalışmalarımı tamamlayabilmem için gereken ortamı hazırlayan canlarım, annem Zarife ÖZEN ve babam Mustafa ÖZEN'e, uzakta olmasına rağmen motivasyonumu en üst seviyede tutmamı sağlayarak yanımda olduğunu hissettiren canım ablam Burcu ÖZEN GÜVEL'e, varlığı ve sevgisiyle daima yanımda olduğunu hissettiren ve başarılarımı destekleyen canım eşim Hakan SERTER'e ve biricik güzel kızım Zeynep Beren SERTER'e sonsuz teşekkürler. İyi ki varsınız.

# **ORTAOKUL ÖĞRENCİLERİNİN BİLGİ GÜVENLİĞİ FARKINDALIK DÜZEYİNİN BELİRLENMESİ**

**(Yüksek Lisans Tezi)**

**Başak ÖZEN SERTER**

**GAZİ ÜNİVERSİTESİ**

**EĞİTİM BİLİMLERİ ENSTİTÜSÜ**

**Ağustos,2021**

**ÖZ**

Bu çalışma ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeylerinin belirlenmesi, farklı değişkenler açısından incelenmesi amacını taşımaktadır. Araştırma bu yönüyle betimsel araştırma olup tarama modeli altında yer almaktadır. Çalışmada bilgi güvenliği farkındalık düzeyleri cinsiyet, anne - baba eğitim düzeyi ve internet veya internetin kullanıldığı uygulamalara ayırdığı günlük süre bağımsız değişkenlerine göre karşılaştırılmıştır. Araştırmanın evrenini Ankara ili Sincan ilçesi Milli Eğitim Müdürlüğüne bağlı 43 resmi ortaokul, örneklemini ise 2020-2021 eğitim öğretim yılı Ankara ili Sincan ilçesindeki Milli Eğitim Müdürlüğüne bağlı 6 devlet ortaokulunda öğrenim gören 614 öğrenci oluşturmaktadır. Araştırmada ele alınan bağımsız değişkenler hakkında bilgi toplayabilmek amacıyla araştırmacı tarafından geliştirilen “Kişisel Bilgi Formu” kullanılmıştır. Bunun yanında ortaöğretim kurumlarında öğrenim gören öğrencilerin bilgi güvenliği farkındalık düzeylerini belirlemeye yönelik olarak Güldüren, Çetinkaya ve Keser (2016) tarafından geliştirilen 36 madde ve 3 faktörden oluşan “Bilgi Güvenliği Farkındalık” ölçeği kullanılmıştır. Mevcut araştırmada ise “Bilgi Güvenliği Farkındalık Ölçeği” ortaokul öğrencilerine uygulanmıştır. Mevcut araştırmada ölçeğin orijinal halinin uygulandığı örneklemden farklı bir örnekleme uygulanması göz önüne alınarak yeniden geçerlik ve güvenilirlik çalışması yapılmasına karar verilmiştir. Yapılan analizler sonucunda 2 madde analiz dışında bırakılarak 34 madde ve 3 faktörden oluşan

ölçme modeli kullanılmıştır. Araştırma kapsamında ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeylerinin nasıl olduğunu belirlemek için ölçeğin faktör puanları ile ölçek toplamına ilişkin betimsel istatistikler (minimum, maksimum, ortalama, standart sapma) hesaplanmıştır. İki grubun karşılaştırılmasında İlişkisiz Örneklem t-testi kullanılırken, ikiden fazla grubun karşılaştırılmasında Tek Yönlü Varyans Analizi (ANOVA) kullanılmıştır. Varyans analizinin anlamlı olduğu durumlarda hangi gruplar arasında anlamlı farklılığın olduğunu belirlemek için Tukey çoklu karşılaştırma testinden yararlanılmıştır. Bulgular öğrencilerin kişisel verilerin korunmasına daha çok önem verirken, saldırı ve tehditler boyutuna en az önemi verdiklerini göstermektedir. Bilgi güvenliği farkındalık düzeylerinin kızlarda erkeklere göre daha yüksek olduğunu görülmüştür. Kişisel verilerin korunması faktörünün anne eğitim düzeylerine göre anlamlı farklılık gösterdiği, annesi lise mezunu olan öğrencilerin annesi ilköğretim mezunu olan öğrencilere göre bilgi güvenliği farkındalık düzeyinin yüksek olduğu görülmüştür. Ancak internete ayırdıkları günlük süreye ve baba eğitim düzeyine göre anlamlı bir farklılık göstermediği görülmektedir.

Anahtar Kelimeler : Farkındalık, Bilgi Güvenliği, Ortaokul Öğrencileri.

Sayfa Adedi : XVI + 91

Danışman : Prof. Dr. Şaban ÇETİN

# **AN ANALYSIS OF INFORMATION SECURITY AWARENESS LEVEL AMONG MIDDLE SCHOOL STUDENTS**

**(M.S. Thesis)**

**Başak ÖZEN SERTER**

**GAZI UNIVERSITY**

**GRADUATE SCHOOL OF EDUCATIONAL SCIENCES**

**August, 2021**

## **ABSTRACT**

This study aims to determine and assess the information security awareness levels of middle school students in terms of different variables. In this respect, the research is a descriptive research within the scope of survey model. In this study the information security levels are compared according to independent variables such as gender, parental educational level and the amount of time spent online per day or on the applications that require internet usage. 43 middle schools affiliated to the Ministry of Education, in Sincan district of Ankara constitutes as the population and 614 students studying in 6 state schools affiliated to the Ministry of Education, in Sincan district of Ankara during the 2020-2021 academic year constitutes as the sample of this study. To collect data about the different variables discussed, a “Personal Data Form” developed by the researcher was used. Besides the “Information Security Awareness Scale” of 36 items and 3 factors developed by Güldüren, Çetinkaya and Keser (2016) was used to determine the information security awareness levels of the middle schools students. The “Information Security Awareness Scale” was applied in the present study. Considering the difference between the original sample and the sample of the present study, it is decided to redo the validation and reliability study. As a result of the analysis done, the scale model which is consisted of 34

items and 3 factors were used leaving out 2 items. Within the research context, descriptive statistics related to the factor scores and the total score (minimum, maximum, average, standard deviation) were calculated to determine the information security awareness levels of middle school students. While Independent Samples t-test was used to compare two groups, One-Way Analysis of Variance (ANOVA) was used when comparing more than two groups. In the cases where variance analysis was significant, Tukey Multiple Comparison test was used to determine between which groups a significant difference exists. Findings indicate that protection of personal data was more important for students while attacks and threats were the least important factors. It is observed that the information security awareness levels of girls are higher compared to boys. It is also observed that the protection of personal data factor differs depending on the education levels of the mothers. The information security awareness levels of the students whose mothers are highschool graduates are observed higher than those whose mothers are primary school graduates. Yet, no significant difference was found in terms of their daily usage of the internet and parental educational levels.

Key words : Awareness, Information Security, Middle School Students.

Page Number : XVI + 91

Supervisor : Prof. Dr. Şaban ÇETİN



## İÇİNDEKİLER

|                                       |     |
|---------------------------------------|-----|
| İÇİNDEKİLER.....                      | xi  |
| TABLolar LİSTESİ .....                | xiv |
| ŞEKİLLER LİSTESİ .....                | xv  |
| SİMGELER VE KISALTMALAR LİSTESİ ..... | xvi |

### BÖLÜM I

|                                         |   |
|-----------------------------------------|---|
| 1. GİRİŞ.....                           | 1 |
| 1.1. Problem Durumu .....               | 1 |
| 1.2. Araştırmanın Amacı.....            | 4 |
| 1.3. Araştırmanın Önemi .....           | 4 |
| 1.4. Varsayımlar.....                   | 5 |
| 1.5. Sınırlılıklar.....                 | 5 |
| 1.6. Konu ile ilgili Araştırmalar ..... | 5 |

### BÖLÜM II

|                               |    |
|-------------------------------|----|
| 2. KAVRAMSAL ÇERÇEVE .....    | 15 |
| 2.1. Tanımlar .....           | 15 |
| 2.1.1. Dijital Teknoloji..... | 15 |
| 2.1.2. Bilgi.....             | 15 |
| 2.1.3. Güvenlik .....         | 16 |

|                                                                     |    |
|---------------------------------------------------------------------|----|
| 2.1.4. Bilgi Güvenliği .....                                        | 17 |
| 2.1.5. Farkındalık .....                                            | 19 |
| 2.2. Bilgi Güvenliğine Yönelik Tehditler .....                      | 19 |
| 2.2.1. Doğal Tehditler .....                                        | 19 |
| 2.2.2. ProsedürHatalarından Kaynaklanan Tehditler .....             | 20 |
| 2.2.3. İnsan Faktöründen Kaynaklanan Tehditler .....                | 20 |
| 2.2.4. Kötücül Yazılımlardan Kaynaklanan Tehditler .....            | 23 |
| 2.2.4.1. Kimlik Avı.....                                            | 24 |
| 2.2.4.2. Sazan Avlama (Phishing) .....                              | 25 |
| 2.2.4.3. İstenmeyen E-Posta Sağanakları (Spam) .....                | 26 |
| 2.2.4.4. Arka Kapılar (Backdoor) .....                              | 27 |
| 2.2.4.5. Sosyal Mühendislik.....                                    | 27 |
| 2.2.4.6. Casus Yazılımlar (Spyware) .....                           | 28 |
| 2.2.4.7. Bilgisayar Virüsleri.....                                  | 29 |
| 2.2.4.8. Bilgisayar Solucanları (Worm) .....                        | 30 |
| 2.2.4.9. Truva Atları (Trojen Horse) .....                          | 31 |
| 2.2.4.10. Kök Kullanıcı Takımları (Rootkit) .....                   | 32 |
| 2.2.4.11. Klavye Dinleme Sistemleri (Keylogger) .....               | 33 |
| 2.2.4.12. Botnet Ağı.....                                           | 33 |
| 2.3. Bilgi Güvenliğine Yönelik Tedbirler .....                      | 34 |
| 2.2.1. Kişisel Verilerin Korunumuna Dair Yasal Dayanak .....        | 34 |
| 2.2.2. Ebeveyn Denetimi.....                                        | 36 |
| 2.2.3. İnternet Bankacılığı ve Çevrimiçi Alışverişte Güvenlik ..... | 38 |
| 2.2.4. Sosyal Ağlarda Güvenlik .....                                | 41 |

## BÖLÜM III

|                |    |
|----------------|----|
| 3. YÖNTEM..... | 47 |
|----------------|----|

|                                                         |           |
|---------------------------------------------------------|-----------|
| 3.1. Araştırma Modeli .....                             | 47        |
| 3.2. Evren ve Örneklem .....                            | 47        |
| 3.3. Veri Toplama Araçları .....                        | 49        |
| 3.3.1. Kişisel Bilgi Formu.....                         | 49        |
| 3.3.2. Bilgi Güvenliği Farkındalığı Ölçeği (BGFÖ) ..... | 49        |
| 3.3.2.1. BGFÖ Geçerlik ve Güvenirliliği.....            | 50        |
| 3.4. Verilerin Analizi.....                             | 56        |
| <b>BÖLÜM IV</b>                                         |           |
| <b>4.BULGULLAR VE YORUM.....</b>                        | <b>58</b> |
| <b>BÖLÜM V</b>                                          |           |
| <b>5. SONUÇ VE ÖNERİLER.....</b>                        | <b>66</b> |
| 5.1. Sonuç .....                                        | 66        |
| 5.2. Öneriler .....                                     | 69        |
| <b>KAYNAKLAR .....</b>                                  | <b>71</b> |
| <b>EKLER .....</b>                                      | <b>82</b> |
| EK 1. Kişisel Bilgiler Formu .....                      | 83        |
| EK 2. Bilgi Güvenliği Farkındalık Ölçeği.....           | 84        |
| EK 3. Bilgi Güvenliği Farkındalık Ölçeği İzni .....     | 86        |
| EK 4. CV .....                                          | 87        |

## TABLÖLAR LİSTESİ

|                                                                                                                                                                           |    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Tablo 1. Örneklemi Oluşturan Öğrencilerin Demografik Özelliklerine İlişkin Frekans ve Yüzde Değerleri .....                                                               | 48 |
| Tablo 2. Bilgi Güvenliği Farkındalığı Ölçeği (BGFÖ) Uyum İndeksleri ve Uyum İndekslerinin Kabul Sınırları .....                                                           | 53 |
| Tablo 3. Bilgi Güvenliği Farkındalık Ölçeğinin Cronbach $\alpha$ Katsayıları .....                                                                                        | 56 |
| Tablo 4. Çalışmaya Katılan Öğrencilerin “Bilgi Güvenliği Farkındalık Ölçeği” Puanları Betimsel İstatistikleri .....                                                       | 58 |
| Tablo 5. Araştırmaya Katılan Ortaokul Öğrencilerinin Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Puanlarının Cinsiyetlerine Göre İlişkisiz Örneklem t-Testi Sonuçları ..... | 59 |
| Tablo 6. Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Puanlarının Anne Eğitim Düzeyine Göre ANOVA Sonuçları .....                                                            | 61 |
| Tablo 7. Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Puanlarının Baba Eğitim Düzeyine Göre ANOVA Sonuçları .....                                                            | 63 |
| Tablo 8. Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Puanlarının İnternete Ayrılan Günlük Süreye Göre ANOVA Sonuçları .....                                                 | 64 |

## ŞEKİLLER LİSTESİ

|                                                                              |    |
|------------------------------------------------------------------------------|----|
| Şekil 1. Data, İnförmatıon ve Knowledge Arasındaki İlişki Döngüsü .....      | 16 |
| Şekil 2. Güvenlik Unsurları .....                                            | 18 |
| Şekil 3. Bilgi Güvenliğı Unsurları İle İnsan Faktörü Arasındaki İlişki ..... | 22 |
| Şekil 4. Veri Sorumlusuna Başvuru Ve Kurula Şikayet .....                    | 35 |
| Şekil 5. Bilgi Güvenliğı Farkındalık Ölçeğı'ne İlişkin Yol Diyagramı .....   | 54 |

## SİMGELER VE KISALTMALAR LİSTESİ

|         |                                                                 |
|---------|-----------------------------------------------------------------|
| BİLGEM  | Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi |
| BGF     | Bilgi Güvenliği Farkındalığı                                    |
| BGFÖ    | Bilgi Güvenliği Farkındalığı Ölçeği                             |
| KVK     | Kişisel Bilgilerin Korunumu                                     |
| MA      | Mahremiyet                                                      |
| ST      | Saldırı ve Tehditler                                            |
| TSE     | Türk Standartları Enstitüsü                                     |
| TÜBİTAK | Türkiye Bilimsel ve Teknolojik Araştırma Kurumu                 |

# BÖLÜM I

## GİRİŞ

### 1.1. Problem durumu:

Değişimin ve gelişimin hızlı olduğu, teknolojinin her alanda insanı sarmaladığı ve teknolojiden bağımsız düşünmenin imkânsız hale geldiği bir dünyada yaşıyoruz. Bilim ve teknolojideki gelişmeler; yaşadığımız çağı bilgi çağı, bu çağda yaşayan toplumları bilgi toplumu olarak adlandırmamıza sebep olmuştur. Bilgisayar, internet ve diğer bilgi teknolojileri ile çağımızda maddi üretim yerine bilgi üretimi önem kazanmıştır (Karalar ve Sarı, 2007).

Bilgi teknolojilerindeki hızlı gelişmeler, toplumsal yapıların değişmesine ve yeniden şekillenmesine neden olmaktadır. Yaşanan bu hızlı değişim süreci, beraberinde yeni kavramlar ve olgular getirmiştir. Bu yeni kavramlardan biri de, bilgi çağı ya da bilgi toplumdur (Çalık ve Sezgin, 2005).

Bilgi toplumu, bilginin temel güç ve başlıca sermaye kaynağı olduğu toplumdur. Bilgi toplumunda, bilgi amaç değil, araçtır ve toplumsal yaşamın her aşamasını aydınlatan, yönlendiren başlıca güçtür. Bilgi toplumunda, bilgi bir hayat biçimi, düşünme ve yaşam tarzıdır (Fındıkçı, 1998, s.83)

İçinde bulunulan çağ bilgi çağıdır. Böyle bir dönemde, geçerli bilginin üretilmesi ve kullanılması oldukça önemlidir. Bilgi toplumunda bilgi üretim yerleri, üniversiteler ve akademik araştırma merkezleridir. Bilgi toplumunun bir özelliği, öğrenebilen insandır. Bilgi toplumunda birey, bilim dünyasının verilerini anlamak, yorumlamak, kullanmak,

yenilerini ortaya koymak, problem çözme yeteneği kazanmak durumundadır (Çalık ve Sezgin, 2005).

Çağ bilgi çağı ise bilginin kullanılmasıyla üretilen teknolojiler de bu çağın bir parçasıdır. Çağımızın anahtar kelimelerinden bir tanesi olan teknoloji Türk Dil Kurumu'na göre “bir sanayi dalı ile ilgili yapım yöntemlerini, kullanılan araç, gereç ve aletleri ve bunların kullanım biçimlerini kapsayan uygulama bilgisi, uygulayım bilimi” ve “insanın maddi çevresini denetlemek ve değiştirmek amacıyla geliştirdiği araç gereçlerle bunlara ilişkin bilgilerin tümü” şeklinde tanımlanmaktadır (Türk Dil Kurumu [TDK], 2011).

İnternet ise yirminci yüzyılın son yıllarında ortaya çıkmış bir teknolojidir. İnternet ile yazı ve sese dayalı iletişimin yanında, görsel olarak iletişim kurmak da artık mümkün hale gelmiştir. Dahası, dünyanın neredeyse tamamında bulunan mevcut ağlar sayesinde internet ile kişilerarası anlık iletişim sağlanabilmektedir. Gerek internetin yaygınlaşmaya başlaması ve ucuz hale getirilmesi, gerek tablet, akıllı telefon, internete erişimi olan kol saatleri, küçük bilgisayarlar, vb. aletlerin geliştirilmesiyle, internet tüm insanlığın özellikle de genç neslin ilgisini çekmeye başlamıştır (Avşar Arık, 2018).

Günümüz teknolojisinde banka işlemlerini gerçekleştirmek, alışveriş yapmak, araştırma yapmak, fatura ödemek, sosyal çevreyle iletişim kurmak, bir adres bulmak, oyun oynamak, fotoğraf veya video çekmek, okumak – yazmak ve daha birçok şey için teknolojiden ve internetten yararlanıyoruz. Artık bankalar, okullar, mağazalar, kitaplar, gazeteler ve hatta ailemiz ve arkadaşlarımız bile teknoloji ve bize sunduğu hizmetler sayesinde hep elimizin altındalar ve bizlere bir tık kadar yakınlardır.

Dijital teknolojiler sayesinde bireyler dünyanın her yerinden insanlarla kolaylıkla iletişim kurabilmekte, onların yaşayışları ve kültürleri hakkında bilgi edinebilmektedir. Bu sayede de değerli bakış açıları kazanmakta ve yeni fırsatlar elde etmektedir. Bütün bu yenilikleri ve gelişmeleri görmezden gelmek doğru olmadığı gibi, fiziksel ve ruhsal boşluğa sebep olacak şekilde sosyal çevreden soyutlanarak bu teknolojilere bağımlı hale gelmek de doğru değildir. Aksi takdirde insanlarla çevrimiçi iletişimi yüz yüze iletişime tercih eden, gazete, kitap, ansiklopedi sayfalarının kokularını bilmeyen, arkadaşlarıyla sokakta oyun oynamanın güzelliğine varamayan, hareketsiz yaşamı normalleştiren bir nesille karşı karşıya kalmamız kaçınılmaz olur.

Dünya üzerinde internet kullanıcılarının sayısı, geçen yıla oranla 400 milyon artmıştır bu da yıllık %10 luk büyümeyi göstermektedir. Dünyanın dört bir yanındaki internet

kullanıcılarının sayısı 4,5 milyara yaklaşmaktadır (wearesocial.com). We Are Social 2019 verilerine göre dünya nüfusu 7734 milyarken bunun 5155 milyarı (%67'si) cep telefonu kullanıcısı, 4479 milyarı (%58'i) internet kullanıcısı, 3725 milyarı (%48'i) aktif sosyal medya kullanıcısı, 3660 milyarı (%47'si) cep telefonu üzerinden sosyal medya kullanıcısıdır. 2018 yılına göre dünya nüfusu %1'den fazla artış gösterirken; cep telefonu kullananların sayısı %2,4'ten fazla, internet kullanıcılarının sayısı %10'dan fazla, sosyal medya kullanıcılarının sayısı %9,6'dan fazla ve cep telefonu üzerinden sosyal medya kullanıcılarının sayısı ise %15'ten fazla artış göstermiştir.

İstatistiklerden yola çıkıldığında teknolojinin her geçen gün hayatımıza biraz daha fazla girdiğini ve etkisi altına aldığı kitlenin her geçen gün büyüdüğünü görmekteyiz. Bu da insanların teknolojiden vazgeçememesine sebep olmaktadır. Sadece dijital teknolojilerin yer aldığı bir dünyaya doğan ve bu teknolojilerin dilleri ana dilleri olan (Taş, 2014) Z kuşağı değil, sonradan teknolojiyle tanışan nesil de bu hızlı değişime ayak uydurmaktadır.

Bakıldığında bize birçok fayda sunan teknoloji ve beraberinde getirdiği hizmetler, yaşamı kolaylaştırmakta ve ihtiyaçlara daha kolay ve hızlı bir şekilde erişimi sağlamaktadır. Bilgi teknolojileri bize bu hizmetlere kolaylıkla erişimi sağlarken birçok kişisel veriye de ihtiyaç duymaktadır. Web sitelerine üyelikler, bankacılık işlemleri, sosyal medya paylaşımları, hastane sistemleri, akademik çalışmalara erişim vb. işlem için ad, soyad, kimlik numarası, doğum tarihi, fotoğraf gibi birçok kişisel bilgi istenebilmektedir. Bu sebeple de güvenlik tedbirleri almadan bilişim teknolojilerini kullanmamak gerekmektedir. Aynı zamanda bu teknolojinin içinde doğan ve aktif bir şekilde kullanan neslin de teknolojinin faydaları ve zararları konusunda bilinçlendirilmesi önem arz etmektedir.

Bilgi güvenliği; bize ait olan bilgilerin başkalarının eline geçmemesidir. Üç temel güvenlik ögesi vardır: Gizlilik, bütünlük ve erişilebilirlik. Gizlilik, bilginin yetkisiz kişilerin eline geçmesidir. Bütünlük, bilginin yetkisi olmayan kişilerce değiştirilmemesidir. Erişilebilirlik ise bilginin ilgili ve yetkili kişiler tarafından ulaşılabilir ve kullanılabilir olması durumudur. Bu öğelerden herhangi biri zarar görürse güvenlik zaafiyeti oluşur (TÜBİTAK-BİLGEM, 2011).

Oluşan bu güvenlik açığı sebebiyle, internet bankacılığına ait hesap bilgilerimiz bir saldırganın eline geçebilir, bir web sitesi içeriği bir saldırgan tarafından amacı dışında değiştirilebilir, erişim izniniz olduğu halde bir web sitesine erişiminiz engellenebilir, sosyal medya hesabınız saldırganların eline geçebilir ve yakın çevrenizle iletişime geçerek

yakınlarınızı zarar verip onları dolandırabilir, bir suç örgütü kimliğini gizlemek için sizin kişisel bilgilerinizi kullanarak ve hatta kullandığınız bilgisayarları ele geçirerek hedeflediklerini bu yolla yapabilir. Saydığımız bu riskler bilgi teknolojilerini, bilgi güvenliğini göz ardı etmeden kullanmak gerektiğini göstermektedir.

Bilginin paylaşımı aşamasında, kişisel bilgilerimiz başta olmak üzere tüm kritik bilgilerimiz, kullanılan teknolojik cihazlarda ve bu cihazlara indirilen uygulamalar aracılığıyla sanal dünyanın bize ayrılan bölümünde saklanmaktadır. Tam da bu noktada bilgi güvenliği hakkında bilgi sahibi olunması ve öğrenilen bilgilerin uygulanarak güvenlik önlemlerinin sağlanması kişisel ve kurumsal açıdan oldukça önemlidir (Güldüre, Çetinkaya ve Keser, 2016).

## **1.2. Araştırmanın Amacı:**

Bu araştırmanın genel amacı, ortaokul 7. ve 8. sınıf öğrencilerinin bilgi güvenliği farkındalık düzeylerini incelemektir. Bu amaç doğrultusunda aşağıdaki araştırma sorularına cevap aranmıştır.

1. Ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeyleri nasıldır?
2. Ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeyleri cinsiyete göre anlamlı farklılık göstermekte midir?
3. Ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeyleri anne eğitim durumuna göre anlamlı farklılık göstermekte midir?
4. Ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeyleri baba eğitim durumuna göre anlamlı farklılık göstermekte midir?
5. Ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeyleri internet veya internetin kullanıldığı uygulamalara ayırdığı günlük süreye göre anlamlı farklılık göstermekte midir?

## **1.3. Araştırmanın Önemi:**

Günümüz teknolojisinde bilgi ve bilgilendirmenin bu kadar kolay ve hızlı olması bireyin kişiliğini ve sosyal çevresiyle olan etkileşimini değiştirmektedir. Özellikle yeni neslin dijital teknolojilerle iç içe büyümesi benlik algılarını, kişiliklerini, düşünce şekillerini, insanlarla olan diyaloglarını, aile ve toplum içindeki davranışlarını etkilemektedir. Hayatımıza bu kadar dahil olan teknolojinin ve internetin bize sunduğu imkanları

kullanırken zarar görmemek ve başkalarına da zarar vermemek açısından bilgi güvenliği hakkında bilgi sahibi olmak gerekmektedir.

Bu araştırma öğrencilerin bilgi güvenliği farkındalık düzeylerini belirlemek ve bu konudaki eğitim ihtiyacını görmek açısından önemlidir. Aynı zamanda giderek artan kontrolsüz ve bilinçsiz teknoloji kullanımı ile ilgili farkındalık yaratmak istenmektedir. Gereksinimi olan öğrencilere bilişim teknolojileri rehberlik hizmetleri kapsamında gereken eğitimin verilebilmesi açısından da önem teşkil etmektedir.

#### **1.4. Varsayımlar:**

Araştırmaya katılan öğrencilerin uygulanan ölçme araçlarına samimi ve doğru cevaplar verdikleri varsayılmıştır.

#### **1.5. Sınırlılıklar:**

1. Bu araştırma 2020-2021 eğitim-öğretim yılında, Ankara ilinin Sincan ilçesinde öğrenim gören 7. ve 8.sınıf öğrencileri ile sınırlıdır.
2. Öğrencilerin bilgi güvenliği konusundaki farkındalıklarını belirlemek amacıyla kullanılan ölçekten elde edilen veriler ile sınırlıdır.

#### **1.6. Konuyla İlgili Yapılan Araştırmalar**

Güldüren, Çetinkaya ve Keser (2016) “Ortaöğretim öğrencilerine yönelik bilgi güvenliği farkındalık ölçeği geliştirme (BGFÖ) çalışması” adlı çalışmalarının sonucunda öğrencilerin bilgi güvenliği farkındalıklarını belirlemek amacıyla geliştirilen ölçeğin tamamından alınan ortalama puanların cinsiyete göre anlamlı bir farklılık gösterdiği belirlenmiştir. Erkek öğrencilerin farkındalık düzeylerinin kız öğrencilere nazaran daha yüksek olduğu tespit edilmiştir. Ölçeğin “saldırı ve tehditler”, “mahremiyet” ve “kişisel verilerin korunması” alt faktörlerinde de ortalama puanlar incelendiğinde erkek öğrencilerin puanları kız öğrencilerinkinden daha yüksek çıkmıştır. Alt faktörler incelendiğinde “saldırı ve tehditler” faktöründe kız ve erkek öğrencilerin farkındalık düzeyleri arasındaki fark en fazla, “kişisel verilerin korunması” faktöründe kız ve erkek öğrencilerin farkındalık düzeyleri arasındaki fark ise en azdır.

Aksoy ve Sayın (2018) tarafından ortaokul ve lise öğrencilerinin şifre oluşturma ve ilgili duyarlılık seviyesinin ölçülmesi, şifre oluşturma konusundaki bilinç düzeylerinin belirlenmesi amacıyla yapılan çalışmada şu bulgulara rastlanmıştır. Öğrencilerin ortaokul seviyesinde daha kolay ve akılda kalıcı şifreleri daha uzun süreli kullandıkları, lise seviyesindeki öğrencilerin tüm hesapları için genellikle aynı şifreyi belirlediklerini fakat belirledikleri şifreleri daha kısa süreli kullandıkları görülmüştür. Özel karakterli şifrelerin ortaokul öğrencileri tarafından kısmen daha çok tercih edildiği, genellikle öğrencilerin tamamında bu karakterleri kullanma eğilimi olmadığı tespit edilmiştir. Araştırmaya dahil olan öğrencilerin yarısından fazlasının şifre gizliliğine önem verdiği de bulgular arasındadır.

Gökçearslan ve Seferoğlu (2016) tarafından yapılan çalışmada ise ortaokul öğrencilerinin internet kullanım biçimleri (kullanım süreleri, düzeyleri, mekanları), riskli internet davranışları ve bu davranışların çeşitli değişkenler (cinsiyet, anne-baba öğrenim durumu, internet kullanım süresi gibi) açısından incelenmesi amaçlamaktadır. Bulgulara göre öğrencilerin çoğunluğunun günlük birkaç saat internet kullandığı ancak çok uzun süre internet kullanan öğrencilerin de azımsanmayacak oranda olduğu görülmüştür. Öğrencilerden kullanım düzeylerini değerlendirmeleri istenmiş ve bu öz değerlendirme sonucunda çoğunluğun kendini internet kullanımında orta ve ileri düzeyde gördüğü belirlenmiştir. Fakat bu durumun Avrupa Birliği Çevrim İçi Çocuklar Projesi sonuçlarına göre (Haddon ve Livingstone, 2012) gerçeği yansımadığı görülmüştür. Öğrencilerin yarısı Avrupa genelinde olduğu gibi interneti kendi özel alanlarında kullanmaktadır. Aileler en çok kısıtlamayı kullanım süresi ve internette gezinilen siteler konusunda yapmaktadır. Bulgulara göre “fotoğraflarını sosyal paylaşım sitelerinde yayınlama”, “internette tanımadığı kişilere buluşma teklif etme”, “sanal ortamlarda kişisel sayfalara erişimi sağlayan kullanıcı isimleri ve şifrelerini başkalarıyla paylaşma”, “internet’te patlayıcı yapımı ve silahlarla ilgili sitelere girme” gibi riskli internet davranışları sergiledikleri tespit edilmiştir. Riskli internet davranışları cinsiyet ve anne öğrenim durumu ile ilişkili çıkmıştır. Bu sonuçlar dikkate alınarak öğrencilere çevrimiçi riskler konusunda bilgilendirilme yapılmasının faydalı olacağı kanısına varılmıştır.

Beder ve Ergün (2015) tarafından yapılan “Ortaokul öğrencilerinin güvenli internet kullanım durumlarının belirlenmesi” adlı çalışmada öğrencilerin internet kullanırken karşılaşılabilecekleri durumlar senaryo haline getirilmiş ve hazırlanan çizimlerle videolar

oluşturulmuştur. Araştırma sonuçlarına göre öğrencilerin güvenli internet kullanımıyla ilgili bilinç düzeyi genel itibarıyla yüksek çıkmıştır. Cinsiyete göre bakıldığında kız öğrencilerin erkek öğrencilere göre daha bilinçli hareket ettikleri sonucuna varılmıştır. Öğrencilerin “Telif Hakkı İhlali” ve “Sorun Olabilecek Paylaşımlar” ile ilgili bilinç seviyelerinin düşük olduğu, “Yazılımsal Tehditler” ile ilgili kararsız kaldığı durumlar belirlenmiştir. 8. sınıf öğrencilerinin 6. sınıf öğrencilere göre bilinç düzeylerinin daha düşük olduğu görülmüştür. Bu durum 8. sınıf öğrencilerinin daha özgür ve rahat hareket etme isteklerinin bir sonucu olarak ortaya çıktığı düşünülmüştür.

Tekin ve Polat (2016) tarafından yapılan “Ortaokul öğrenci velilerinin güvenli internet kullanımı farkındalığı” isimli araştırmada Güvenli İnternet Kullanım Ölçeği uygulanmış, verilerin analizi sonucunda öğrenci velilerinin güvenli internet kullanımı konusunda farkındalıklarının yüksek olduğu ortaya çıkmıştır. Bu farkındalık üzerinde velilerin cinsiyetinin, akıllı telefona sahip olma durumunun, öğrenim durumunun ve internet kullanım amacının etkisinin olmadığı görülmüştür. Sosyal ağ kullanan ve internet ortamında daha uzun süre geçiren velilerin gizlilik, kişisel veri paylaşımı, uygunsuz içeriklere karşı duyarlı olma ve internet kullanım kuralları ile daha fazla karşılaşması sebebiyle farkındalık düzeylerinin yüksek olduğu sonucuna varılmıştır. Eğitsel veri madenciliği yöntemlerinden biri olan birliktelik kuralı analiz sonuçlarına göre, veliler çocuklarının kişisel bilgilerini paylaşmamaları, internetten alışveriş yapmamaları, internet ortamında herhangi bir tartışma/kavgaya katılmamaları, internette kötü niyetli kişilerin olabileceği konularında daha fazla farkındalık sahibi oldukları görülmüştür.

Yılmaz, Karaoğlu Yılmaz, Öztürk ve Karademir (2017) yaptıkları çalışmada lise öğrencilerinin güvenli bilgisayar ve internet kullanım farkındalık profillerinin ortaya konulmasını amaçlamıştır. Araştırma sonuçları, öğrencilerin büyük çoğunluğunun güvenli bilgisayar ve internet kullanım farkındalıklarının düşük olduğunu ve birçok çevrimiçi risklerle karşı karşıya kalabileceklerini göstermektedir. Öğrencilerin sosyal ağ farkındalığı teması altında verdikleri yanıtlar incelendiğinde; kişisel bilgileri paylaşmama, istenmeyen kişilerden gelen mesajları ve uygulamaları engelleyebilme, profilinin/sayfalarının güvenlik ayarlarını değiştirebilme gibi işlemleri yapan/yapabilen öğrenci sayısının yarıyı geçtiği ve diğer temalara göre bilgi ve farkındalıklarının daha yüksek olduğu görülmektedir. Öğrenciler tehditler ve korunma yolları güvenliği teması altında verdiği cevaplarda; zararlı yazılım ve virüslerin verebileceği zararların, zararlı programlardan korunma yazılımlarının

farkında olma, bu programları kullanma, zararlı yazılımların bilgisayara bulaşıp bulaşmadığını fark edebilme ile ilgili farkındalığı yüksek olan öğrenci sayısının fazla olduğu görülmektedir. Öğrencilerin e-posta kullanma farkındalıklarının, güvenli şifre oluşturma konusundaki farkındalıklarına göre daha yüksek olduğu sonucu ortaya çıkmıştır. Güvenli e-posta kullanımının ön koşulu, güvenli şifre oluşturmada geçer. Bu sebeple öğrencilerin bu açıdan da risk altında olduğu görülmektedir. Öğrencilerin yaklaşık yarısının erişim ve şifre güvenliği ile e-posta güvenliği temalarına yönelik bilgi ve farkındalıklarının diğer temalara oranla biraz daha yüksek olduğu ancak öğrencilerin büyük çoğunluğunun; tehditler, korunma yolları, yazılım yükleme ve güncelleme, internet ve ağ güvenliği, kullanıcı farkındalığı ve sosyal mühendislik temalarına yönelik farkındalıklarının ise düşük olduğu söylenebilir.

Gökmen ve Akgün (2014), Bilgisayar ve Öğretim Teknolojileri Eğitimi (BÖTE) öğretmen adaylarının bilişim güvenliği bilgilerinin seviyesinin tespit edilmesi amacıyla yapmış oldukları çalışmada öğretmen adaylarının bilişim güvenliği bilgi düzeylerinin düşük olduğu, bunun cinsiyete ve öğrenim gördüğü üniversiteye göre farklılık gösterdiği tespit edilmiştir. BÖTE öğretmen adaylarının büyük kısmının e-posta eklerinin ve e-posta eki içerisindeki bağlantıya tıklama güvenliğine yönelik bilgilerinin yeterli düzeyde olmadığı görülmüştür. Öğretmen adaylarının vekil (proxy) sunucusunun işlevleri hakkında eksik bilgiye sahip olduklarını göstermiştir. Bilgi sahibi olmayanların sayısı da oldukça fazladır. Adayların taşınabilir aygıtlarla öğrencilerin kişisel bilgilerinin, ödevlerinin taşınmasının bir suç olduğu konusunda bilgi sahibi olmadıkları saptanmıştır. Bazı adayların güvenlik duvarının görevinin tam olarak ne olduğunu bilmedikleri, katılımcılarının yarısına yakınının bu konuda bilgi sahibi olduğu görülmüştür. Adayların çoğunluğunun güvenli şifre oluşturma konusunda yeterli bilgiye sahip oldukları ortaya çıkmıştır. BÖTE öğretmen adaylarının bilişim güvenliği bilgilerinin yaşa, bilgisayara sahip olma süresine, sınıf düzeyine, günlük bilgisayar kullanım süresine, günlük internet kullanım süresine ve bilişim güvenliğine yönelik bir eğitim alma durumuna göre değişmediği sonucuna ulaşılmıştır.

Gökmen ve Akgün (2016), yaptığı çalışmada bazı öğretmen adaylarının bilişim suçu konusunda bilgi sahibi olmadığı, bilişim suçuna maruz kaldıkları, bilişim suçu işledikleri ve bir bilişim suçuyla karşılaştıklarında ne yapmaları gerektiğini bilmedikleri görülmüştür. Ayrıca öğretmen adaylarının birçoğunun bilişim güvenliğinin tanımı ve kapsamı konusunda yetersiz bilgiye sahip oldukları da tespit edilmiştir. Öğretmen adaylarının

bilişim teknolojilerinin güvenli kullanımı, kişisel bilgilerin korunumu, bilişim güvenliğini tehdit eden unsurlara karşı önlemler alma, güvenlik yazılımları, güvenli çevrimiçi alışveriş ve internet bankacılığı, web sitelerinin güvenliği, sosyal ağların güvenli kullanımı, güvenli şifre oluşturma, virüslerden korunma, güncellemeler, e-posta hesaplarının güvenliği, işletim sisteminin güvenliği gibi konularda eğitime ihtiyaç duydukları belirlenmiştir.

Yılmaz, Şahin ve Akbulut (2016), öğretmenlerin dijital veri güvenliği farkındalıklarının oldukça yüksek olduğu görülmüştür. Erkek öğretmenlerin kadın öğretmenlere göre farkındalık düzeylerinin daha yüksek olduğu sonucuna varılmıştır. Günlük bilgisayar ve internet kullanım süreleri incelendiğinde 3saatten fazla bilgisayar kullanan öğretmenlerin diğerlerine göre farkındalık düzeylerinin yüksek olduğu ortaya çıkmıştır. Öğretmenlerin sahip oldukları bilişim cihazları (bilgisayar, tablet bilgisayar, akıllı telefon) arttıkça dijital veri güvenliği farkındalığının da arttığı görülmüştür. Bunun yanında dijital veri güvenliği farkındalığının branş, öğrenim kademesi, öğrenim durumu ve mesleki deneyim değişkenlerine göre anlamlı bir farklılık göstermediği saptanmıştır.

Karaoğlu Yılmaz ve Çavuş Ezin (2017) nin yaptığı çalışmanın analiz sonuçları incelendiğinde ebeveynlerin farkındalıklarının belirli bir düzeyde olduğu fakat veri yedekleme yerleri ve yedekleme sıklığı konularında beklenen düzeyde olmadığı görülmüştür. Ebeveynlerin, çocuklarının bilgi güvenliğini sağlamak amacıyla onları sıklıkla uyardıkları ama somut olarak onlara yardımcı olmadıkları gözlemlenmiştir. Çocukların bilgi güvenliği farkındalığını artırmanın yolunun ebeveynlerin bu konudaki bilgi ve uygulamalarının artırılmasıyla sağlanacağı düşünülmektedir. Ebeveynlerin en çok zararlı yazılımlar hakkında bilgi sahibi oldukları diğer tehdit unsurları hakkında farkındalıklarının yetersiz olduğu görülmüştür. Aynı zamanda ebeveynlerin parola oluşturmada farklı kombinasyonları önemli ölçüde kullandıkları ve güçlü şifreler oluşturmaya özen gösterdikleri sonucuna da ulaşılmıştır.

Rençber ve Mete (2016), bilgi güvenlik farkındalığını etkileyen faktörlerin belirlenmesi amacıyla yaptıkları çalışmanın sonucunda şifre yönetimi, mobil internet kullanımı, e-posta ve internet kullanımı ve sosyal ağ sitelerinin kullanım davranışları en etkili faktörler olarak belirlemiştir.

Mert, Bülbül ve Sağiroğlu (2012) 8.sınıf öğrencileri güvenli internet kullanımı üzerinde yaptıkları araştırma sonuçlarında öğrencilerin çoğunluğunun güvenli şifre oluşturmada yetersiz olduğu belirlenmiştir. Öğrencilerin en çok doğum tarihlerini, en az ise ev

adreslerini, telefon numaralarını ve aile bireylerine ait bilgilerini paylaştıkları gözlemlenmiştir. Öğrencilerin %65'i şifresini kimseyle paylaşmazken geri kalan kısmı ise sevgilisi, ailesi ve arkadaşlarıyla paylaştığını belirtmiştir. Öğrencilerin %74'ü TC kimlik numarasının internette paylaşılması gereken bir bilgi olduğunu belirtmiştir. Öğrencilerin %76'sı haber sitelerinin güvenliği olduğunu belirtmiştir.

Altınöz, Tosun, Çinkılıç ve Çay (t.y.), “Siber güvenlik ve bilinçli sosyal medya kullanımı dersi pilot uygulamasına ilişkin öğretmen görüşleri” adlı çalışmada öğretmenler, öğrencilerin siber güvenlikle ilgili birçok kavramı öğrenmiş olduklarını ve güvenli internetin ne anlama geldiğini kavradıklarını belirtmiştir. Hangi davranışların siber suçlar kapsamına girdiği konusunda bilinçlendiklerini ifade etmişlerdir. Çocukların ve gençlerin dijital ortamda karşılaşacakları tehlikeler ve yapacakları yanlış davranışların sonuçları hakkında bilgilendirilmelerinin son derece önemli olduğu vurgulanmaktadır. Siber zorbalık, sosyal ağlar kanalıyla yayılan oyunlar (Mavi Balina, Mariam, 48 Hours Challenge vb.), sosyal ağ bağımlılığı, şifre hırsızlığı, siber dolandırıcılık gibi birçok tehlike hakkında bireylerin küçük yaşlardan itibaren bilgilendirilmesi önem arz etmektedir. Bu yönüyle pilot ders uygulamalarının çocuk ve gençler üzerindeki olumlu etkisi ve katkısı sevindiricidir.

Ünal ve Ergen (2018) tarafından yapılan araştırma kapsamında siber uzay ortamında gerçekleştirilen faaliyetler esnasında siber güvenlikle ilgili davranışlar ölçülmüştür. Bulgulara göre kadınların yazılım güncelleme sıklığı erkeklere göre daha yüksektir. Cihaz güvenliği davranış sıklığı ise özel sektör çalışanlarında, kamu çalışanlarına göre daha yüksek olduğu tespit edilmiştir. Bir başka bulgu ise internette geçirilen süre arttıkça siber güvenlik davranışlarının sıklığı gözlemlenmiştir. Siber güvenlik davranışı sıklığı ile gelir ve eğitim düzeyi arasında anlamlı bir farklılaşma görülmemiştir.

Güldüren (2015), yaptığı doktora tezinde yükseköğretim kurumlarındaki öğretim elemanlarının bilgi güvenliği farkındalığı kazandırmak amacıyla çoklu ortam materyalleri içeren web sitesi geliştirerek deneysel bir çalışma yapmıştır. Kazandırılmak istenen içerik çoklu ortam materyalleri ile katılımcılara verildikten sonra son test bilgi güvenliği farkındalık düzeyi toplam puanlarını artırdığı belirlenmiştir. Analiz sonucuna göre, geliştirilen çoklu ortam materyalleri ve web sitesinin bilgi güvenliği farkındalığı konusunda genel bilgilendirme açısından faydalı, detaylı ve önemli noktalara değinilerek

hazırlanan videolar içerdiği görülmüş, oldukça iyi tasarlanmış ve kullanımı kolay olduğu kanısına varılmıştır.

Kapanoğlu (2016) öğretmenlerin bilgi güvenliği farkındalığının incelenmesine yönelik yaptığı yüksek lisans tez çalışmasında verilerin analizi sonucu öğretmenlerin bilgi güvenliği farkındalığı “orta düzeyde yeterli” şeklinde çıkmıştır. Öğretmenler dijital ortamda en fazla resimlerini, isim/soyisimlerini, duygu/düşüncelerini, doğum tarihlerini, ilgi alanlarını, araştırmalarını ve eposta adreslerini paylaşmaktadırlar. Bunun yanında telefon numarası, aile bireylerinin bilgilerini ve kimlik numaralarını paylaşan öğretmenler de bulunmaktadır. Katılımcıların %81,5’i teknolojik cihazlarında anti-virüs yazılımı kullandığı saptanmıştır. Katılımcıların yarıdan fazlasının anti-virüs taramasını bilgisayarlarında yavaşlama olduğunda ya da rutin olarak ayda bir kez yaptığı görülmüştür. Öğretmenlerin %74,9’u e-posta güvenliğinin en önemli bileşeni olan “spam”in istenmeyen posta olduğunu bilmektedir. Öğretmenlerin yarıya yakını kişisel bilgilerin düzenlenmesini gerektiren bankadan gelen e-postaların içinde yer alan linki açmadan banka ile iletişime geçecekleri gözlemlenmiştir. Araştırmaya katılan öğretmenlerin bilgi güvenliği farkındalık düzeylerinin cinsiyet ve internet kullanım süreleri arasında anlamlı bir farklılık olmadığı sonucuna ulaşılmıştır. Ancak bilgi güvenliği farkındalık düzeyleri ile yaşları, öğrenim durumları, bulundukları bölge, görev süresi, bu konuda alınan eğitim durumları ve branşları arasında anlamlı bir farklılık bulunmuştur. Farkındalık düzeylerinin en fazla olduğu branşın bilgisayar öğretmenliği olduğu bunu sırasıyla Türkçe, matematik, fen ve teknoloji, sınıf öğretmenliği ve sosyal bilgiler öğretmenliğinin takip ettiği sonucuna ulaşılmıştır.

Erdoğan (2017), üniversite öğrencilerinin bilgi güvenliği kazanımlarının, farkındalıkları üzerindeki etkilerinin analizi üzerine yaptığı yüksek lisans tezinde öğrencilerin bilgi güvenliği farkındalıkları; internet güvenliği, sosyal medya kullanımı, internet tarayıcısı ile ağ güvenliği, şifre oluşturma ve sosyal medya tuzakları olmak üzere beş alt boyutta ortaya çıkmıştır. Bilgi güvenliği kazanımlarının cinsiyet, yaş ve internet kullanım yıllarına göre, bilgi güvenliği farkındalıklarının ise yaş, bölüm, sınıf ve internet ortamını güvenli bulup bulmamalarına göre anlamlı bir farklılık gösterdiği tespit edilmiştir. Öte yandan, bilgi güvenliği farkındalığını en çok etkileyen alt boyutun “İnternet Güvenliği” olduğu sonucuna ulaşılmıştır.

Dönmez (2019)'in yaptığı yüksek lisans çalışmasında lise öğrencilerinin bilgi güvenliği farkındalığı ile dijital okuryazarlığı arasındaki ilişki incelenmiştir. Öğrencilerin dijital okuryazarlık durumlarının iyi durumda olduğu, cinsiyet değişkeni ile arasında anlamlı bir farklılaşma olmadığı sonucuna ulaşılmıştır. Bunun yanında bilgi güvenliği farkındalığının cinsiyete göre farklılaştığı, bu farklılaşmanın “saldırı ve tehditler” alt boyunda ve erkekler lehine olduğu görülmüştür. Analiz sonuçlarında dijital okuryazarlık ile bilgi güvenliği farkındalığı arasında anlamlı ve pozitif yönde bir ilişki saptanmıştır. Dijital okuryazarlık arttıkça bilgi güvenliğindeki “mahremiyet” alt boyutunun öneminin arttığı sonucuna ulaşılmıştır. Araştırmada günlük internet kullanım süresi, sosyal medya kullanım süresi ve çevrim-içi araçları kullanmadaki özyeterliliği ile bilgi güvenliği farkındalığı arasında anlamlı ve pozitif yönde farklılaşma saptanmıştır.

Hacımustafoğlu (2019) tarafından yapılan çalışmada lise öğrencilerinin bilgi güvenliği farkındalık düzeylerinin siber mağdur olma durumlarına etkisini incelenmiş ve veri analizi sonucunda bu ikisi arasında herhangi bir ilişki bulunmamıştır. Ortaöğretim öğrencilerinin bilgi güvenliği farkındalığı yeterli düzeyde, siber mağduriyet ile karşı karşıya kalma durumları ise düşük düzeyde çıkmıştır. Bilgi güvenliği farkındalığını etkileyen faktörler cinsiyet, sınıf düzeyi, anne eğitim durumu, günlük internet kullanımı iken siber mağduriyete maruz kalma durumunu etkileyen faktörler cinsiyet ve internet kullanım süresi olarak belirlenmiştir.

Vilander (2021) araştırmasında 18 yaş ve üstü bireylerde bilgi güvenliği farkındalığı konusunda çalışmış, bilgi güvenliği farkındalığının yaş ile doğru orantılı bir şekilde arttığı sonucuna ulaşmıştır. Deneyimin bilgi güvenliği farkındalığında önemli bir faktör olduğu ancak alınan örgün eğitimin bu konuda belirleyici olmadığı sonucuna varılmıştır. Bu çalışmada katılımcılar olumsuz bir durumu tespit etme yeterliliğine sahip olmadıklarını sahipse de bunu nasıl bildireceklerini gördüler. Bilgi ile davranış arasında zayıf ya da orta düzeyde bir ilişki olması beklense de korelasyon katsayıları limitlere uysa da hipotez doğrulanmamıştır. Davranış skorları genellikle bilgiden yüksek çıkmıştır. Tutumun ise güvenli davranış oluşturma konusunda bilgiden daha etkin olduğu söylenebilir. Tutum ise güvenli davranışın oluşturulmasında önemli bir faktördür ve bilgi ile davranış arasında uzlaştırıcı bir göreve sahiptir. Bilgi ve davranış arasında oluşan boşluğun tutum ile ilgili olduğu söylenebilir.

Derin ve Gençoğlu (2020), “Ortaokul Öğrencilerinin Bilgi Güvenliği Farkındalığı” adlı çalışmasında kızların erkek öğrencilere göre tehlike oluşturacak durumları bildikleri, 7. ve 8. sınıf öğrencilerinin farkındalık düzeylerinin 5. ve 6. sınıf öğrencilerinkinden yüksek olduğu tespit edilmiştir. İnterneti daha çok kullanan öğrencilerin olası tehlikelerin daha çok farkında oldukları görülmüştür. İnterneti sadece sosyal medya amaçlı kullanan öğrencilerin olası tehlikelerin çok farkında olmadığı da çıkan sonuçlar arasındadır.

Gökçearslan, Günbatar ve Sarıtepeci (2021), çalışmalarında bilgi güvenliği farkındalığını; kişisel bilgisayar ve akıllı telefona sahip olma, bilişim teknolojileri dersi alma ve bundan yararlanma durumu kapsamında incelemişlerdir. Saldırı ve Tehditler ile Mahremiyet alt boyutlarını etkileyen en önemli değişken kişisel bilgisayara sahip olunması iken, Kişisel Verilerin Korunumu alt boyutunda en önemli değişken Bilişim Teknolojileri (BT) dersinden sağlandığı düşünülen faydadır. BT dersi gören ve bu dersin olumlu yönde etkisinin olduğunu düşünen öğrencilerin bilgi güvenliği farkındalık düzeylerinin de yüksek çıktığı sonucuna ulaşılmıştır.

Talan ve Aktürk (2021), lise öğrencileri üzerinde yaptığı araştırmasında erkeklerin kadınlara göre bilgi güvenliği farkındalık düzeylerinin yüksek olduğu, ancak yaşadıkları şehirlere göre farklılık göstermediği sonucuna ulaşmıştır. Bölgesel olarak daha az gelişmiş şehirlerde de teknolojiye ulaşmanın, gelişmiş şehirlerdekinden çok da farklı olmadığı düşünülebilir. Gün içinde 7 saatten fazla internet kullanan öğrencilerin bilgi güvenliği farkındalıklarının yüksek olduğu ancak sosyal medyada geçirilen zamanın BGF’ ni etkilemediği görülmüştür. Araştırmada dijital okuryazarlık ile bilgi güvenliği farkındalığı arasında pozitif yönde ve anlamlı bir ilişki saptanmıştır.

Ulsamer, Schutz, Fertig ve Keller (2021) yaptıkları çalışmada bilgi güvenliği farkındalığı kazandırmada kullanılacak iki yöntemi karşılaştırmıştır. Kullanıcıyı sorunun odağına koyarak öğrenmesini artırmak ve özellikle kullanıcı kaynaklı oluşabilecek tehlikeleri en aza indirmek mümkün olabildiği gösterilmektedir. Sanal gerçeklik kullanılarak sürükleyici hikaye anlatma yönteminin geleneksel elektronik öğrenmelere göre bilginin devamlılığını daha çok sağlayabildiği, kalıcılığı artırdığı ve katılımcıların çoğu tarafından sanal gerçeklik kullanılarak oluşturulan hikayenin takip edilebilirliğinin yüksek olarak değerlendirildiği görülmüştür. Aynı zamanda çıkan sonuçlar sanal gerçeklik deneyiminin katılımcıları olayın bir parçası olarak hissettirdiğini ve role soktuğunu göstermiştir. E-öğrenmelerin

resmi hayal etme noktasında kaldığı katılımcıyı olaya dahil edemediği değerlendirmeler arasındadır.



## BÖLÜM II

### KAVRAMSAL ÇERÇEVE

#### 2.1. Tanımlar

##### 2.1.1. Dijital Teknoloji

Deren (2006)' e göre dijitalleşme; doküman, fotoğraf, video gibi görsel ya da işitsel içeriklerin kodlarla ifade edilerek algılanmasını, işlenmesini ve depolanmasını sağlamaktır.

Buradan hareketle dijital teknoloji için de sayılara dayalı bir teknoloji türüdür denilebilir. Bütün bilgiler sayılarla yaratılmış kodlarla kaydedilir. Dijital olması sebebiyle analog bilgilere kıyasla daha güvenli ve hızlı bir şekilde iletilir. Bilgisayar programları, cep telefonları, internet sayfaları, ses dosyaları vb. dijital teknolojinin kullanıldığı alanlardır.

##### 2.1.2. Bilgi

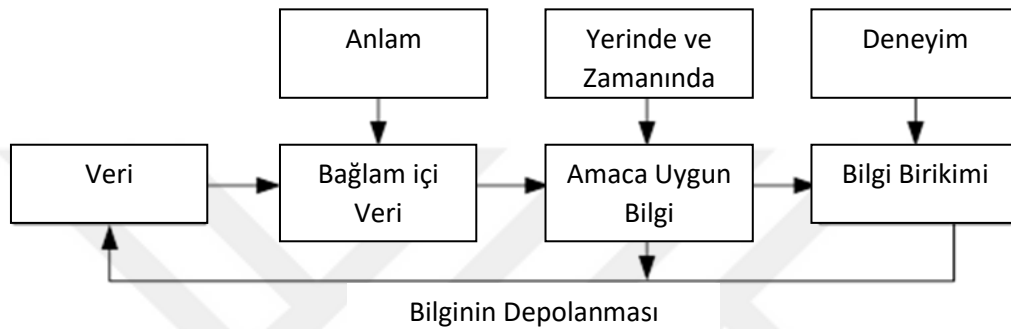
Türk Dil Kurumu bilgiyi “öğrenme, araştırma veya gözlem yolu ile elde edilen gerçek, malumat. İnsan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü” olarak tanımlamaktadır.

Bilgi kavramını açıklarken karşımıza birbiriyle ilişkili ancak birbiri yerine kullanılamayacak ölçüde farklı anlamlara sahip üç kavram çıkmaktadır. Bunlar arasındaki ilişkiyi aynı zamanda farklılıkları ayırt ederek başlamak bilgi teknolojileri ile ilgili yapılacak çalışmalar için faydalı olacaktır (Kelley, 2002).

Veri (data), olay veya durumlarla ilgili soyut ve nesnel gerçeklerden oluşur. Bilginin işlenmemiş, filtrelenmemiş ham halidir. Bilgi haline gelebilmesi için düzenlenmesi şarttır. Analiz sürecinin bir parçası, bir ögesidir.

Bilgi (information); arındırılmış, anlamlandırılmış, açıklanmış verilerdir. Tekrar kullanılabilir şekilde işlenmiş ve birbirleriyle ilişkilendirilmiş verilerden oluşur. Bilgi verilerin konuşma diline, tablo ve grafiklere dönüşmüş halidir. Yani toplanan veriler değerlendirir, çözümlenir ve de düzenlenirse anlamlı ve kullanılabilir bir hal alır.

Bilgi (knowledge): Bilginin deneyim, değer ve içgörü ile buluşmasıdır. Eyleme dönüştürülebilir bilgilerdir.



Şekil 1. Data, Information Ve Knowledge Arasındaki İlişki Döngüsü (Kaynak: Brackett, M. (2013). Data Topics. The Data – Information - Knowledge Cycle. <https://www.dataversity.net/the-data-information-knowledge-cycle/> adresinden erişilmiştir.

Bu döngüde yukarıda da belirtildiği gibi verilerin (data) birbirleriyle ilişkilendirilip anlamlandırılmasıyla konuyla ilgili güncel bilgilerin (information) elde edildiği, buna deneyimin ilave edilmesiyle de bilginin hayat bulması (knowledge), eylem olarak varlığını sürdürmesi şematize edilmiştir. Bilgilerin depolanması süreci döngüsel kılmaktadır.

### 2.1.3. Güvenlik

Güvenlik; toplum yaşamında yasal düzenin aksamadan sürdürülmesi ve bireylerin korkmadan, güven içinde yaşamlarına devam edebilmesidir (TDK, 2011). Kişi, kurum ya da kuruluşlara yönelik yapılan dahili ya da harici tehdit, taciz, sabotaj vb. olaylar karşısında alınabilecek önlemlerin tümüdür (“Güvenlik”, t.y.).

Carnegie Mellon Üniversitesi tarafından ortaya konulan “güvenlik yaşam döngüsü” kavramından da anlaşılacağı üzere güvenlik durağan bir yapı değildir. Birbirini etkileyen ve yenilenen bir sistem olduğu dikkat çekmektedir. Bu döngü bilindik saldırı ve problemlere karşı koruma ve sağlamlaştırma ile başlar, bilinmeyen saldırılara karşı hazırlık

süreci ile devam eder. Ardından bilinmeyen saldırıların tespiti ve tespit edilen saldırılara hızlı bir şekilde müdahale edilmesi ile süreç yenilenir. Geçmişte edinilen bilgiler doğrultusunda sistemde iyileştirme yapılarak güvenliğin sürekliliği sağlanır (aktaran Canbek ve Sağıroğlu, 2007a).

#### **2.1.4. Bilgi Güvenliği**

Bilgi güvenliği, bilginin izinsiz ve yetkisiz bir şekilde erişimini, kullanımını, değiştirilmesini, yayınlanmasını, yok edilmesini ve zarar verilmesini engellemektir. (Puhakainen, 2006).

Canbek ve Sağıroğlu (2007b) yaptıkları çalışmada, bilgi güvenliğini bilginin bir varlık olarak gelebilecek tüm zararlara karşı muhafaza edilmesi, yetki verilmemiş kişilerin eline geçmesinin önlenmesi ve uygunsuz amaçlara yönelik kullanımlarının engellenmesi şeklinde tanımlamıştır. Gelişen ve yaygınlaşan teknoloji ve teknolojinin sunduğu fırsatlar sayesinde günlük rutinlerimiz haline gelen birçok iş ve işlemler elektronik ortamda yapılabilmektedir. Bu da bilgi güvenliğini kaçınılmaz kılmaktadır.

Büyük küçük işletmeler, devlet kurumları, okul ev gibi kar amacı taşımayan her oluşum elektronik ortamlarda önemli bilgi ve belgelere sahiptir. Bu oluşumların güvenli bir şekilde devamlılığının sağlanmasında ve bilgiye dayalı varlıklarını korumasında bilgi güvenliği oldukça önemli rol oynar (Eminağaoğlu ve Gökşen, 2009).

Daha önce de bahsettiğimiz gibi bilgi güvenliğinin 3 temel ögesi vardır. Bunlar gizlilik, bütünlük ve erişilebilirlik.

*Gizlilik:* Bilginin yetkisi olmayan kişilerin eline geçmesidir. Bilgiyi işleme, saklama ve transferi aşamalarında yetkisiz kişilerden korumak, ulaşılabilir olmasını engellemektir.

*Bütünlük:* Bilgiyi olması gerektiği haliyle muhafaza etmektir. Bilginin bir bölümünün veya tamamının değiştirilmesi, yok edilmesi, hasara uğraması veya istenmeyen yeni verilerin ilave edilmesi bütünlük ögesini sarsmaktadır.

*Erişilebilirlik:* Bilginin anlamını yitirmeden, tam ve eksiksiz bir şekilde istenen ve belirlenen süre boyunca ulaşılabilir ve kullanılabilir olmasını sağlamaktır.

Bilgi güvenliğinin 3 temel ögesine ek olarak kimlik kanıtlama ve inkar edememe ögeleri de temel ögeler arasında yer almaktadır. Bu ögeleri tamamlayan ek ögeler ise sorumluluk, erişim denetimi, güvenilirlik ve emniyettir (Canbek ve Sağıroğlu, 2006).

*Kimlik Kanıtlama:* Kullanıcının veya işlemin doğrulanması ile sistemsel kaynaklardan hangilerine ulaşma yetkisi olduğunun belirlenme sürecidir.

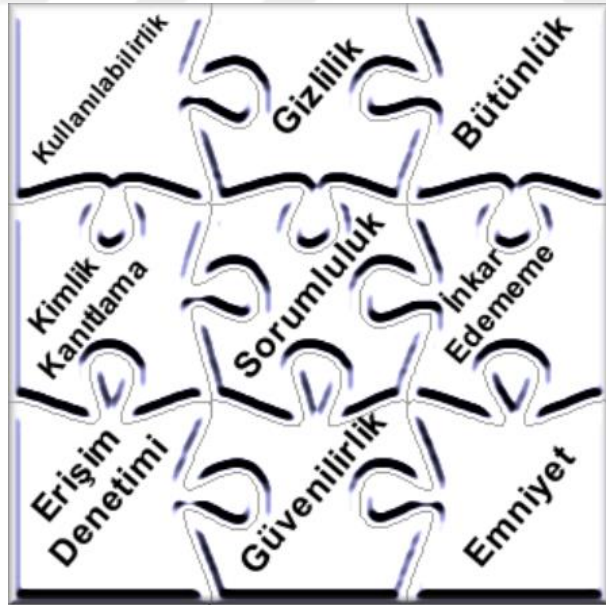
*İnkâr Edememe:* Alınan ya da iletilen bilgilerin, alındığının ya da teslim edildiğinin inkar edilememesidir.

*Sorumluluk:* Yapılan iş veya işlemin sorumlusunu tayin etmektir.

*Erişim Denetimi:* Bir bilgiye ulaşabilmek adına gerekli olan izinlerin alınıp verilmesidir.

*Güvenilirlik:* Bir bilgi ya da bilgisayar sisteminin kesintisiz güvenli bir biçimde tasarım ihtiyaçlarına uygun olarak çalışmasıdır.

*Emniyet:* Bir bilgisayar sistemi veya yazılımının kendisinde veya içinde bulunduğu ortamda tehlike yaratabilecek olası durumları engellemektir.



Şekil 2. Güvenlik Unsurları (Kaynak: Canbek, G. ve Sağıroğlu, Ş. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. Politeknik Dergisi, 9(3), 165-174.)

Yukarıda belirtilen tüm ögeler tek başına düşünülemez, hepsi birbirini tamamlar niteliktedir. Tüm bu ögeler bir arada olursa bilgi güvenliğinden bahsedilebilir. Bu unsurların birbirini tamamlayıcı unsurlar olduğu hiçbir zaman unutulmamalıdır.

Bilgi güvenliği; bir kez sağlanması gereken, tamamlanıp bitirilebilecek bir iş olarak düşünülemez. Bilgi güvenliği teknoloji, bilgi ve teknoloji kullanıcıları var olduğu müddetçe devam eden ve daima yönetilmesi, denetlenmesi gereken bir döngüdür (ISO, 2005).

#### **2.1.5. Farkındalık**

Farkındalık, bir konuda bilinçli olmaktır. Hem konuyla ilgili bilgiye sahip olmak hem de bilgiyi fayda sağlayacak şekilde kullanabilecek durumda olmaktır.

Bostan ve Şengül (2014) farkındalığı, yapılan iş ve işlemlerle alakalı bilgi sahibi olma ve bu iş ve işlemler için gerekli olan ihtiyaçları bilerek, nasıl sonuçlar doğurabileceğine hakim olma hali olarak tanımlamıştır. Farkındalığın temelinde ise eğitim vardır. Yapılan iş, kullanılan materyal hakkında bilgi sahibi olmak, avantaj ve dezavantajlarını yordayabilmeyi sağlar. Karşılaşılabilecek tehditler hakkında fikir sahibi olmak ise bu tehlikelerden kaçınmayı da kolaylaştırır.

### **2.2. Bilgi Güvenliğine Yönelik Tehditler**

#### **2.2.1. Doğal Tehditler**

AFAD (Afet ve Acil Durum Yönetimi Başkanlığı) dünya üzerinde gözlemlenmiş 31 çeşit afetten bahsetmektedir. Deprem, sel, toprak kayması, çığ, yangın, savaş, terror saldırısı gibi farklı kategorilerde birçok doğal afet yaşanmaktadır. Bu doğal afetlerin ortak noktaları ise aniden gelişmesi, insanlar tarafından engellenmesinin mümkün olmaması, birçok can ve mal kaybına sebep olmasıdır.

Bu doğal oluşumların bilgi kaynaklarını zarara uğratma ve çalışmasına engel olma riski de söz konusudur. Bir durum için risk söz konusuysa risk yönetimi şarttır. En az zararla bu durumları atlatabilmek adına olma ihtimali olan tehditler önceden iyi bir şekilde analiz edilmeli ve bu tehditlere uygun planlamalar yapılmalıdır.

### **2.2.2. Prosedür Hatalarından Kaynaklanan Tehditler**

Prosedür; herhangi bir işte izlenecek yollar, uyulması gereken kurallar ve yöntemler bütünüdür. İdari ve teknik anlamda izlenmesi gereken yollara uyulmadığı takdirde yine bilgi tehlikeye girer.

İdareden kaynaklı prosedürel aksaklıklar genel olarak faaliyetlerini sürdürürken şahıslara bağımlı kalan işletmelerin karşı karşıya kaldığı aksaklıklardır. Personelleri arasında iş bölümünün ve görev tanımının net bir şekilde yapmayan, yetkileri bu sorumluluğu kaldıramayacak kişilere veren, iş akışını belirlemeyen, personel alımlarında veya işten çıkarmalarda güvenliğe dikkat etmeyen kısacası kurumsallaşma sürecini tamamlamamış olan işletmelerin bilgi güvenliği tehdit altındadır. Buna ilave olarak teknik anlamda yaşanabilecek aksaklıklar da prosedürel aksaklıklar olarak ifade edilebilir. Verileri uygun depolama yöntemleriyle saklamama, bilgi ve belgelerin yedeklenmesine ve yedekleme koşullarına dikkat etmeme, işletmenin sahip olduğu teknolojik ekipmanların hem donanım olarak hem de yazılım olarak bakımlarını yaptırmama da teknik olarak bilgi güvenliğini tehdit eder (Vural ve Sağıroğlu, 2010).

### **2.2.3. İnsan Faktöründen Kaynaklanan Tehditler**

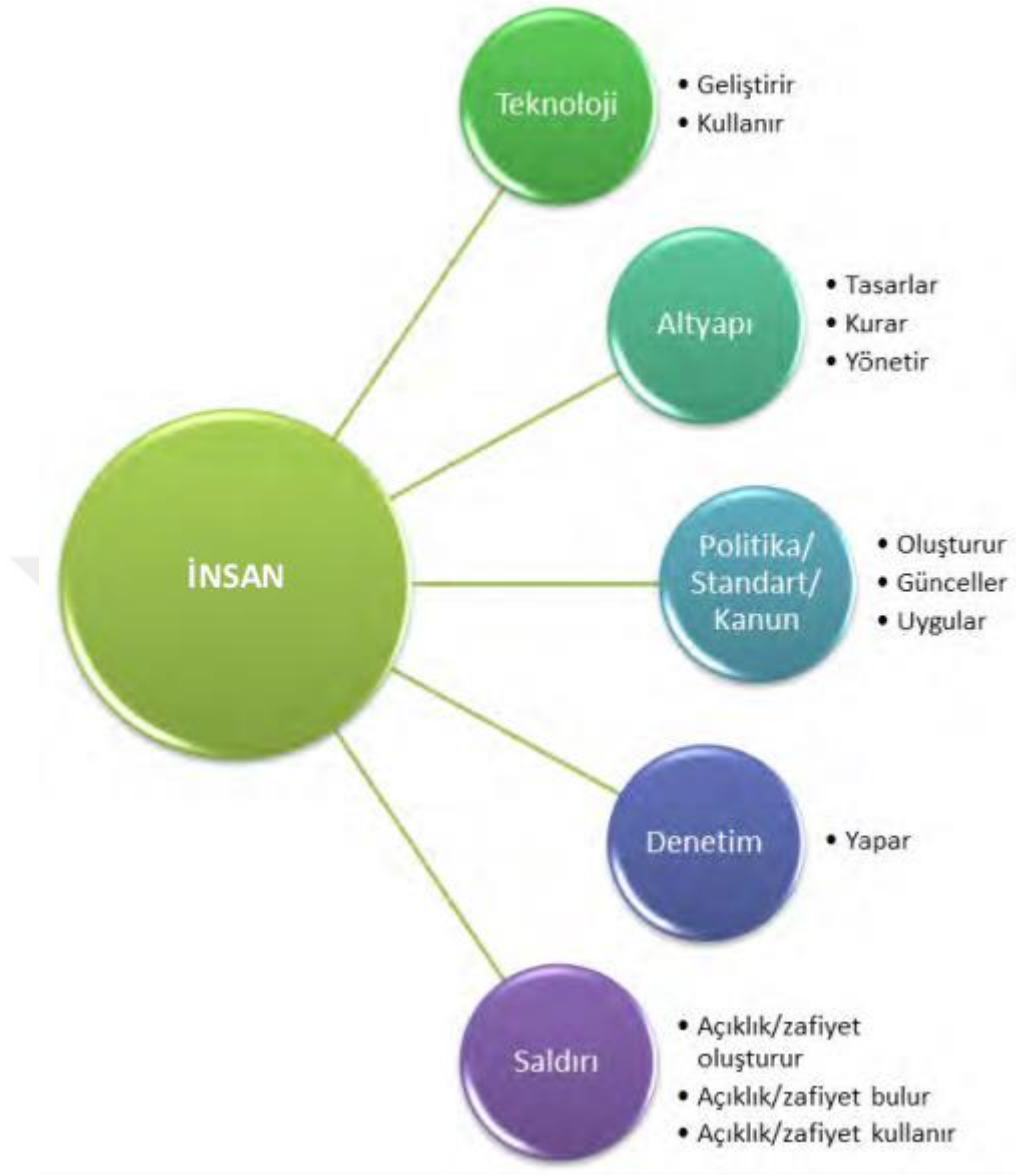
Teknolojiyi kullananlar bireyler ve kurumlardır. Güvenlik açığını yaratan da bu sistemin kullanıcısı aynı zamanda da en zayıf halkasıdır. Kullanıcılar gereken tedbirleri almaz, bu konuda üzerine düşeni yapmazsa en değerli varlığımız olan bilginin güvenliği tehlikeye girer. Yani gelişen teknoloji, bir varlık türü olan bilgi için tehdit oluşturmaya başlar.

Tehdit; yaşama, ortama, bilgiye, etkinliğe veya mülke zarar verebilecek güce sahip olduğunu gösteren kendiliğinden gerçekleşen veya insan yapımı olan oluş ya da eylemdir (Risk Steering Committee, 2010).

Buradan da anlaşılacağı gibi bilişim teknolojilerindeki gelişmelerin sundukları hep olumlu yönde olmamaktadır. Hırsızlık, kredi kartı dolandırıcılığı, kişilere veya kurumlara yönelik yanlış bilgi yayma veya hakaret etme suretiyle zarar verme, eser sahibinin izni olmaksızın fikirlerinin kopyalanıp çoğaltılması, kişilerin özel bilgi ve belgelerinin istenmeyen kişilerle paylaşılması gibi yeni suçlar da ortaya çıkmış ve hak ihlali kolaylaşmıştır (Dedeoğlu, 2006).

Bilginin yönetilmesi, buna baęlı olarak da yönetilen bilginin güvenlięinin saęlanması oldukça komplike bir süreçtir. Sadece teknik olarak güvenlię önlemleri almak yeterli deęildir. Kullanıcıların da bilgilendirilmesi, bilinçlendirilmesi ve dikkatli davranması son derece önemlidir. Kullanıcı faktörünün göz ardı edilmemesi ve doęru planlanmış bir bilgilendirme doęabilecek riskleri sıfırlamasa da bu risklerin en aza düşürülmesinde oldukça etkili olacaktır (Keser ve Güldüren ,2015; Kruger ve Kearney, 2006).

Erol ve Saęiroęlu (2018) yaptıkları çalışmada insanın bilgi güvenlięi sürecinin neresinde yer aldığını gösteren bir şema oluşturmuşlardır. Oluşturulan bu şemada da insanın süreç içerisinde ne kadar önemli bir role sahip olduęu görölmektedir. İnsan teknolojiyi üreten, geliştiren, geliştirdięi teknolojide yeni tasarımlar oluşturup bunları yöneten, kullanım standartları oluşturarak yasalaştıran, denetleyen ve düzenleyendir. Bilgi güvenlięini saęlamada, düzenlemede, denetlemede yer aldığı gibi bilgi güvenlięini tehlikeye sokan tehditler oluşturmada ve saldırılar gerçekleştirmede de etkilidir. Dolayısıyla insanı bilgi güvenlięinin bir parçasıdır diyerek bu süreçteki rolünü azımsamak hiç de doęru bir yaklaşım deęildir.



Şekil 3. Bilgi Güvenliği Unsurları ile İnsan Faktörü Arasındaki İlişki (Kaynak: Erol, S.E. ve Sağıroğlu, S. (2018). Siber Güvenlik Farkındalığı, Farkındalık Ölçüm Yöntem ve Modelleri. Ş. Sağıroğlu ve M. Alkan (Ed.), Siber Güç ve Savunma Farkındalık ve Caydırıcılık (s.105-141). Ankara:Grafiker)

Bilgisayar teknolojileri kullanıcılarının bilgi güvenliği konusundaki tutum, davranış ve algıları doğabilecek zararların seyrini belirleyecektir. İnsanların bu konuda düşük risk görmeleri tedbirsiz davranmalarına, çok yüksek risk görüp çok kaygılanmaları ise bilişim teknolojilerini kullanmaktan kaçınmalarına sebep olacaktır (aktaran Huang, Rau ve Salvendy, 2010).

#### 2.2.4. Kötücül Yazılımlardan Kaynaklanan Tehditler

Sanal ortam, fiziken bir gerçekliği olmayan fakat var olduğu kabul edilen internet ağları sayesinde iletişimde bulunmayı ve her türlü bilgiye ulaşmayı hedefleyen ortamlardır. Birçok yeniliği, kolaylığı sunabilen bu ortamlar gerçek ve tüzel kişilerin bilgi güvenliğini tehlikeye atabilecek tehditleri de içermektedir (Yavanoğlu, Sağıroğlu ve Çolak, 2012).

Bilgi güvenliği söz konusu olduğunda karşı taraf olarak nitelendirilen ve bilgiyi tehlikeye atan şey genellikle kötü niyetli kişiler yani saldırganlar ve onların yaptığı saldırılar olmaktadır. Bilgisayar sistemini veya yazılımları tehlikeye sokan, doğrudan ya da dolaylı olarak zarar verme amacı güden, gidişatı aksatma ve yapılacak eylemleri sekteye uğratmayı hedefleyen her tür girişim saldırı olarak nitelendirilmektedir (Canbek ve Sağıroğlu, 2007a). Sanal ortam dürüst olmayan, ahlaki ve vicdani yönden zayıf olan kişiler için hedefledikleri dolandırıcılık eylemlerini kolayca gerçekleştirebildikleri uygun bir zemin oluşturmaktadır. Bilişim teknolojileri kullanıcıları dilediği bilgi ve belgeleri şahsi bilgisayarlarında, tablet ve telefonlarında saklama ve dilediği platformda paylaşma hakkına sahip elbette ancak bunları kötü niyetli kişilerin olası eylemlerinden ve kötücül yazılımlarından da korumak mecburiyetindedir.

Kötücül yazılım (malware) , İngilizce “malicious software”in kısaltılmış halidir. Kötücül yazılımlar, kullanıcının haberi olmadan veya kullanıcıyı yanıltarak sistemlere yetkisiz bir şekilde bulaşmaktadır (Heiser, 2004). Kötücül yazılımlar dört temel amaca hizmet eder: Bilgi toplama, kazanç sağlama,

Antivirüs programı üreticileri iyi sonuçlar alabilmek adına bireysel inisiyatif kullanarak durumu çözmek amaçlı yeni ürünler tasarlamaktadır. Güncel kötücül yazılımların da takip edilerek incelenmesiyle oluşturulan bu teknolojileri içeren kapsamlı bir güvenlik ürünü kullanmak gereklidir. Elbette bunlar bile korunmak için yeterli olmayacaktır. Kullanıcıların sağduyulu davranması da işin önemli bir boyutudur (“Bilgisayar Virüsleri ve Kötü Amaçlı Yazılımlarla İlgili Bilgiler ve SSS”, t.y.).

Bilgisayar sistemlerinde veya yazılımlarında oluşacak saldırılar ya da kötücül yazılımlar hakkında ne kadar bilgi sahibi olunsu da bunun için ne kadar önlem alınsa da, alınan hiçbir önlemin kişileri, kurumları ya da sistemleri tam anlamıyla koruyamayacağı açıktır. Çünkü saldırılar da saldırı şekilleri de her geçen gün farklılaşmaktadır. Ancak yine de kötücül yazılımlar hakkında bilgi sahibi olmak, ne gibi zararlar verebileceğini bilmek ve buna karşı tedbir alabilmek adına farkındalık kazanmak doğabilecek zararları en aza indirebilmek

açısından oldukça önemlidir. Bilgisayar güvenlik uzmanı Bruce Schneier'in da dediği gibi "Eğer riskleri bilmezseniz, neye mal olacağınızı da anlayamazsınız".

Öncelikle çocuklar olmak üzere, evlerdeki kullanıcıların (anne, baba, çocuk vs.) ve şirket/kurum kullanıcılarının bilinçsiz kullanımları kötü amaçlı zararlı yazılımların sistemlere bulaşmasına sebep olmaktadır (Canbek ve Sağıroğlu, 2008).

Zararlı yazılımların üretilmesinde ve hedef cihazlara yayılmasında genellikle aşağıdaki yollar izlenmektedir (Zhou ve Jiang, ).

Yeniden Paketleme (Repackaging) Yoluyla Saldırı: Saldırganlar sık kullanılan ve çok tercih edilen uygulamaları indirir, parçalara ayırır ve içlerine zararlı yazılımları yerleştirerek yeniden birleştirir. Bu şekilde dışarıdan orijinal uygulama indirdiğini düşünen mağdurlar kullandıkları cihazlara zararlı yazılımları dahil etmiş olur.

Kod Yükleme (Update Attack) Yoluyla Saldırı: Bu yöntemle oluşturulan kötücül yazılımlar zararlı yazılımları tespit eden programlar tarafından da çok fark edilemeyen, kolay tespit edilemeyen türlerdir. Bu yöntemde zararlı yazılım kodları bir bütün olarak değil parçalar halinde saldırgan tarafından belirlenen şekilde cihazlara dahil edilmektedir.

İndirme (Download) Yoluyla Saldırı: Bu saldırı şekli daha geleneksel bir yoldur. Kullanıcının ihtiyaç ve isteklerine yakın linkler, uygulamalar ve içeriklerle karşılaştırmayı amaçlar. Kullanıcıyı ikna ederek sahte sayfalara yönelmesine ve orada işlem yapmasına sebep olur. Bu şekilde de direkt olarak hedeflenen cihazlara yayılır.

Virüs, solucan, Truva atı, e-posta sağanakları, sazan avlama, arka kapılar, kimlik taklit etme, casus yazılım, sosyal mühendislik, klavye izleme yazılımları başlıca kötücül yazılımlardandır.

#### **2.2.4.1. Kimlik Avı:**

1993 yılında Eugene Pauly adında yaşlı bir adam şiddetli mide krampları, bulantı ve kusma şikayeti ile hastaneye kaldırılır. Yapılan araştırmalar Pauly'nin şikayetlerinin beyin hücrelerinin viral ensefalit tarafından geri döndürülemez şekilde zarar görmesinden kaynaklı olduğunu ortaya koyar. Virüs medial temporal lobunu neredeyse tamamen tahrip etmiş, bu da E.P.'nin birkaç dakika önce yaptığı şeyleri dahi anımsayamaz hale gelmesine sebep olmuştur. Ancak Pauly'nin şaşırtıcı bir şekilde rutin yürüyüşlerini yapıp evine geri

dönebilmek gibi alışkanlık haline dönüşen davranışları yerine getirebildiği gözlemlenmiştir (Bayley ve Squire 2002). Beyin düzenli bir şekilde tekrar ettiği davranışları yani alışkanlıkları gerçekleştirirken bunlara rehberlik etmek ya da bu davranış için düşünmek zorunda kalmamaktadır. E.P gibi beyninde ciddi hasar oluşmuş bireyler dahi karmaşık olmasına rağmen sık tekrar edilmesinden kaynaklı alışkanlık haline dönüşen davranışları yerine getirebilmektedir. Yapılan son çalışmaların çoğu sosyal medya davranışının da alışkanlık olduğunu göstermektedir (Wood, Quinn ve Kashy, 2002). İnsanların alışkanlıklarından yararlanan yeni çevrimiçi aldatma biçimleri ortaya çıkmıştır. Bunlardan en önemlisi kimlik avı saldırılarıdır.

Sanal ortamda başka bir kişinin bilgileriyle o kişinin adına hesap oluşturarak onun yerine geçmek veya onu taklit etmektir. Kötü niyetli kişiler kimlik hırsızlığı ile önemli, güvenilir, saygın, sosyal çevresi geniş olan insanların bilgilerini çalmak suretiyle kimliklerini taklit ederek yerine geçmeye çalıştığı kişiye maddi manevi zarar verebilir, ideolojisini yayarak yandaş toplayabilir, çevresini ve bağlantılarını kullanarak dolandırıcılık yapabilirler.

Kimlik avı güvenilir bir web sitesi kılığına girmekle de mümkündür. İyi planlanmış bir saldırıda taklit edilen web sunucusu gerçeğiyle neredeyse aynı görünerek avını tuzağa düşürür. Bu şekilde mağduru bilgilerini açıklamak için ikna etmesi de oldukça kolay hale gelir ve bu sayede saldırganlar kişisel bilgilerin yanı sıra mağdurun parasını çalabilir veya daha tehlikeli tuzaklara düşürecek eylemlerde bulunabilir (Castiglione, Prisco ve Santis, 2009).

#### **2.2.4.2. Sazan Avlama (Phishing):**

Phishing kelimesi İngilizce password (şifre) ve fishing (balık avı) kelimelerinin birleşmesiyle oluşmaktadır. İçerdiği kelimelerden yola çıkarak şifre avı anlamına gelen phishing kavramının Türkçe karşılığı literatürde sazan avlama veya yemleme olarak kullanılmaktadır (“Yemleme”, 2020). Brein Phish 1980 yılında ilk defa psikolojik yöntemlerle banka bilgilerine ulaşarak insanları zarara uğratmıştır. Bu sebeple de “phishing” kelimesiyle efsaneleşen Brein Phish’in soyadına gönderme yapıldığı düşünülmektedir (Canbek, 2005). Sazan avlama gerçek banka veya kurum ismi ve logosu kullanılarak doğru adresten geldiğini düşündüren bildirimlerle gerçekleştirilir. Bu e-postalarda gönderilen kişiyi ilgilendiren konuya dair link bulunmaktadır. Kişiyi sahte web sayfasına yönlendiren bu link ile açılan sahte web sayfasında girilen kişisel bilgiler kötü

niyetli kişilerce kopyalanarak ele geçirilmiş olur (Erdemir, 2018). Görüldüğü üzere phishing de bir tür kimlik avıdır. Yukarıda bahsettiğimiz kimlik avında bir başkasının kimlik bilgilerini kullanarak o kişinin adına hesaplar açmak ve o hesaplarla işlemler yürütmekten söz edilmektedir. Sazan Avlama yönteminde de saldırgan insanların güvenliğini kazanmış olan saygın bankaları, kurumları, şirketleri vb. taklit etmek, onların web adreslerine benzeyen sahte adresler oluşturarak kişisel bilgilere ulaşmayı hedeflemektedir.

Saldırıda kullanılan e-posta içeriğinin gerçekçi olması, kullanılacak sahte web sayfasının asıl web sayfasına ne ölçüde benzediği bu saldırıların amacına ulaşmadaki başarısını artıracaktır (Berghel'den aktaran Şenol ve Karacan, 2012).

Genellikle kullanıcı adını ve şifresini doğrulatmanın gerekliliğini anlatan ve bankalardan geldiğine inandırılan e-posta veya mesajlara sahte linkler yerleştirilerek avın hesap bilgilerine ulaşılır ve avın banka hesabında istenen hareketler yapılarak saldırgan tarafından zarar uğratılır (Emm, 2008).

#### ***2.2.4.3. İstenmeyen E-Posta Sağanakları (Spam):***

Elektronik posta, internetin en eski ve en vazgeçilmez kullanım araçlarından biridir. Spam ise teknolojinin yaygınlaşmasıyla birlikte daha sık duymaya başlanan kelimelerden bir tanesidir. İstenmeyen elektronik posta anlamına gelen spam reklamların uygunsuz şekilde ulaştırılması, kandırma ve aldatma amacı taşımasından ötürü bu kategoride yer alır. Çoğu zaman sistem tarafından fark edilip ayrıştırılarak yok edilir. İstenmeyen e-postalar gönderilen mesajın içeriğinden, sıklıkla aynı kelimelerin kullanımından ve kişinin mailine sıkça gelmesinden anlaşılabilir. Kişilerin hassas verilerine kötü niyetli kişilerin erişmesine sebep olurken gizliliği ve güvenliği tehdit eder.

Kötü niyetli e-postaların konu satırı alıcının ilgisini çekebilecek şekilde düzenlenmektedir. Spamler alıcıyla ilgili içerikleri barındırmakla birlikte kişiye e-postanın önemli olduğu algısını hissettirerek açılmasının gerekli olduğuna inandıracak şekilde hazırlanmaktadır. Bunun asıl amacı ise kişisel bilgilere ulaşmaktır (Sah ve Parmar, 2017). Hatta bu e-postalar ile alıcının bilgisayarına sızdırılan kötü amaçlı uygulamalar bilgisayarının ele geçirilmesine ve kişiyi bir bot ağının içerisine çekmesine sebep olabilir. Alıcıyı bu şekilde örgütlenmiş bir saldırının otomatik üyesi haline getirebilir (Yavanoğlu, Sağiroğlu ve Çolak, 2012).

Tüm bu istenmeyen e-posta sađanaklarından korunabilmek için elektronik posta programları ile spamleri ayırt etmeye yarayan koruma amaçlı oluşturulan yazılımlar entegre biçimde çalışmalıdır. Hatta gelen istenmeyen e-postaların gelmemesi için alıcı listesinden çıkmak için koyulan linklere de tıklarken de dikkatli olunmalıdır. Aksi takdirde kişi, hesabının aktif bir hesap olduğunu doğrulamış olmakta ve mail adresinin daha çok yerle paylaşılmasına ve farklı amaçlarla kullanılmasına sebebiyet vermektedir (Canbek ve Sağırođlu, 2007b).

#### **2.2.4.4. Arka Kapılar (Backdoor):**

Bilgisayar sistemlerinin güvenliđini atlatan, şifrelemesini es geöen ve genellikle gizli bir şekilde geröekleşen bilgisayar sistemine uzaktan izinsiz erişimi sađlayan, hedef sistemden veri aktarmayı veya sistemi çalışmaz hale getirmeyi hedefleyen yazılımlardır. Programlar içine gizlenebileceđi gibi ayrıca bir program da olabilir. Truva atları sisteme arka kapı yüklemek için de kullanılabilir (Canbek ve Sağırođlu, 2007a). Bazen Truva atlarıyla karıştırlanabilir. Ancak Truva atları yararlı yazılımlar gibi görünerek sisteme dahil olurken, arka kapılar sisteme girişı sađlayan gizli yollar açar (Canbek ve Sağırođlu, 2007b). Arka kapı tasarlayan saldırganlar farklı yazılım ya da servislere bu arka kapıları yerleştirerek hedefledikleri sistemleri ele geçirmeye çalışmakta ve bu sistemlerde kod komut çalıştırarak sistemi uzaktan yönetmektedirler. Program yazılımcıları tarafından müşteriye daha iyi hizmet sunabilmek adına yerleştirilebildikleri gibi devlet/istihbarat örgütlerince de hedef hakkında bilgi toplamak gerektiğinde ve hedefi yok etmek amacıyla donanımlara da yerleştirilebilir. Bu sebeple arka kapıların uzaktan tetiklenmesini engellemek için kullanılan uygulamaları sınırlı yetkilerle çalıştırmak ve yönetim birimlerine sadece size ait adreslerden erişim tanımlamak etkili olabilir (bgasecurity.com).

#### **2.2.4.5. Sosyal Mühendislik:**

Sosyal mühendislik insanların davranışlarını istekleriniz doğrultusunda şekillendirme sanatı ve bilimidir. Sosyal mühendislik güvenliđin en önemli parçasını aynı zamanda en zayıf noktasını yani insanı hedef alır. En güvenli bilgisayarın kapalı bilgisayar olduđu söylenirse de bir kişiyi ikna edip o bilgisayarı açtırdığınız anda artık o da güvende değildir. (Harl, 1997)

Sosyal mühendislik, kullanıcıları zararlı yazılım barındıran programları şüphe çekmeden indirmeye ve çalıştırmaya yönlendirerek bilgisayar sisteminin kontrolünü ele geçirme eylemidir. Bazı sosyal mühendislik yazılımları işletim sisteminde görünen hata pencereleri şeklinde ortaya çıkar ve kullanıcıdan bir web sayfasına girebilmek için onay ister ve bu şekilde sistemi ele geçirir. Bazense sistemde ortaya çıkan sahte virüs alarmlarını kaldırmak için sahte anti-virüs programları veya sahte casus yazılım önleyiciler sunarak kullanıcının bunları sistemine indirmesi sağlanır (Barwinski, 2005).

Bir kurumun kendi bünyesindeki kişiler içinde bulundukları sisteme en çok zarar verenler arasında yer almaktadır. Özellikle kurumla ilişkisini kesen ya da ilişkisi kesilen kişilere yönelik güvenlik önlemleri artırılmalıdır. Sıkça görülen sosyal mühendislik eylemleri aşağıdaki gibi ifade edilebilir (Canbek ve Sağıroğlu, 2007a).

- Telefonla yardım masalarını taklit etmek suretiyle insanları kandırarak kişisel bilgilerini elde edilmesi
- Omuz sörfü olarak adlandırılan bilgisayarda yazı yazarken klavye hareketlerinin dışardan geçen kişiler tarafından izlenmesi
- Ofis, iş yeri gibi çalışma ortamlarında çöp kutusu karıştırarak bilgi ve işlemlere erişilmesi
- Şifreleri ele geçirmek amacıyla sahte yazılımların yüklenmesi

Albert Einstein “Yalnızca iki şey sonsuzdur, evren ve insanoğlunun aptallığı; aslında evrenin sonsuzluğundan o kadar da emin değilim.” der. İnternet dünyasının ilk ve en ünlü hackerlarından Amerikalı bilgisayar bilimci Kevin D.Mitnick ise “insanlar aptallarsa ya da daha sık görülen şekliyle, doğru güvenlik uygulamaları konusunda bilgisizlerse, toplum mühendisliği saldırıları başarılı olmaktadır” (Mitnick, 2016) diye ekler. Çünkü istenilen bilgisayar ya da bilgi sisteminde eylemleri gerçekleştirmek veya gizli bilgileri açığa çıkarıp yayınlamak amacıyla insanlar tarafından yapılan psikoloji manipülasyonu bu şekilde amaca ulaşır.

#### **2.2.4.6. Casus Yazılım (Spyware):**

Casus yazılım, kullanıcıdan habersiz ve kullanıcının onayı olmaksızın bilgisayarlarından verileri toplayarak üçüncü şahıslara iletmesi amacıyla tasarlanmış yazılımlardır. Casus

yazılımlarla e-postaların takip edilmesi, parola/şifre/kredi kartı numaraları gibi gizli bilgileri ele geçirilmesi, klavyede tuş vuruşlarının takip edilmesi gibi kötü amaçlı işlemler yapılabilmektedir. Aynı zamanda internet alışverişlerinde satın alma işlemleriyle ve göz atma alışkanlıklarının takip edilmesiyle de gizli bilgiler kötü niyetli kişiler tarafından casus yazılımlarla elde edilebilir (“Casus Yazılım Nedir?-Tanım”, t.y). Bu tür yazılımlar girdikleri sistemde asıl amacının dışına çıkarak kullanıcının gezdiği web sitelerin HTML kodlarının asıllarını kullanıcının haberi olmadan değiştirir ve anlaşmalı olduğu yerlerin reklamlarını dahi yayınlayabilir. Ayrıca sahte açılır pencereler veya sahte sistem mesajları veya bildirimleri de bilgisayarlara casus yazılımların sızdırılması için kullanılan bir diğer yöntemdir. Genellikle kullanıcılar aniden görünen açılır pencereleri kapatma eğilimindedir ve bu riski aza indirir ancak sistemin gönderdiği mesajlara karşı daha duyarlı oldukları aşıkardır. Bu sebeple de sahte sistem mesajlarına kanma ve tıklama sıkça olmakta ve casus yazılımın sisteme sızma riski de artmaktadır (Canbek ve Sağıroğlu, 2008). Çoğu program ve uygulamayı bilgisayarlara veya mobil cihazlara indirme esnasında kurulum öncesinde lisans anlaşmalarının okunup kabul edilmesi şartı vardır. Ülkemiz için önemli sorunlardan biri de bu anlaşma metnlerinin İngilizce olmasıdır. Hem metnin İngilizce olması hem de sözleşmelerin çok ciddi yaptırımları doğurabileceği bilincinin tam oturmaması sebebiyle çoğunlukla kabul edilen metinler kötücül yazılımlar veya zarara uğratacak yaptırımlar içeriyor olabilmektedir (Canbek, 2005).

Sonuç olarak casus yazılımların dört temel işlevi vardır. Saklanmak, bilgileri toplamak, topladığı bilgileri üçüncü şahıslarla paylaşmak ve girdiği sistemde varlığını devam ettirmek. Bu yazılımlar bahsettiğimiz bu dört işlevle ağlarda ve ana bilgisayarlarda risk oluşturur. Casus yazılımlar Truva atı, virüs, solucan vb içerebilmektedir (Barwinski, 2005).

Casus yazılımlardan yüksek oranda koruma sağlayacak yöntemlerin başında işletim sisteminin güncellemelerini zamanında yapmak ve bilinmeyen program ve uygulamaları indirmekten kaçınmak gelmektedir (Canbek ve Sağıroğlu, 2007b).

#### **2.2.4.7. Bilgisayar Virüsleri**

Biyolojik anlamda virüs, sadece diğer organizmaların canlı hücrelerinde çoğalabilen küçük bir enfeksiyona sebep olan ajandır. Bilgisayar virüslerinin isimlendirilmesinde bu biyoloji teriminden esinlenilmiştir. Biyolojik terim olarak virüs nasıl çoğalmak için canlı hücreye

ihtiyaç duyuyorsa, bilgisayar virüsleri de başka programlara ihtiyaç duyar. E-posta yoluyla bulaşabildiği gibi taşınabilir aygıtlarla (usb bellek, cd, dvd, disket..) da bulaşabilmektedir.

Tespit edilen ilk bilgisayar virüsü 1986'da Brain adı verilen virüstü. Bu virüsü ürettikleri yazılımları yasadışı şekilde kopyalamak isteyen hırsızlara karşı geliştirdiklerini savunan Pakistanlı Basit ve Amjad Farooq Alvi adındaki iki kardeş, hırsızların sabit disklerinin önyükleme bölümüne engel olacak şekilde geliştirmişlerdir. Bu sayede hırsızların çaldıkları yazılımları kullanmalarına engel olmak istemişlerdir. Disket kopyalandıkça da virüs yayılımı sağlanmıştır ("Bilgisayar Virüsleri ve Kötü Amaçlı Yazılımlarla İlgili Bilgiler ve SSS", t.y.).

Virüs yazılımları girdikleri sistemde yer alan dosyalarda değişikliklere sebep olarak dosyaları işlevsiz hale getirebilir, veri kaybına sebep olabilir (Samet ve Aslan, 2018)

Virüsler kodlarını ana bilgisayara ekleyerek dosyadan dosyaya yayılmaktadırlar. Kullanıcı virüse ne kadar uzun süre maruz kalırsa bulaştığı makinede o kadar fazla yayılır. Kendiliğinden yayılmaları söz konusu değildir, insan etkileşimine ihtiyaç duyarlar (Emm, 2008).

Bilgisayar virüsleri dosya virüsleri, ön yükleme virüsleri, makro virüsleri ve betik virüsler olarak 4 başlıkta sınıflandırılabilir (Canbek ve Sağıroğlu, 2007b).

#### **2.2.4.8. Bilgisayar Solucanları (Worm):**

Kopyalama konusunda kendi kendine yetebilen bir bilgisayar yazılımıdır, yayılmak için başka dosya, belge ve programlara güvenmezler (Barwinski, 2005). Solucanları virüslerden ayıran en önemli özellik de budur: Yayılma şekilleri. Virüslerin yayılması için insan etkileşimi gerekirken solucanlar kendiliğinden yayılabilmektedir. Yayılmak için internet ağlarını kullanır ve bu şekilde makineden makineye kendini kopyalayarak diğer kullanıcılara da ulaşmış olur (He, Chan ve Guizani, 2015).

Bilgisayar solucanları dört grupta incelenebilir: e-posta solucanları, internet mesajları solucanları, ağ solucanları ve internet solucanları (Canbek ve Sağıroğlu, 2007b). E-posta solucanları yayılmak için e-postaları kullanır ve dikkatsiz veya bilinçsiz kullanıcıları zararlı kodu çalıştırmaya ikna ederek makineye bulaşmış olur (Emm, 2008). Hatta e-posta adresinde kayıtlı olan ve güvenlik sağlayıcılarla doğrudan ilgili olmayan tüm adreslere kendini postalayarak daha da yayılır. İnternet mesajları solucanları ağ bağlantısına ihtiyaç

duyan mesajlaşma uygulamalarını kullanır. Gelen eklentiye açan kullanıcı solucanı sisteme dahil etmiş olur. Artık sisteme giren kötücül yazılım listedeki diğer kullanıcılara kendini göndererek çoğalır, bu şekilde büyük kitlelere yayılmaya devam eder. İnternet solucanları kendilerini güvenlik yönünden açıkları olan savunmasız sistemlere, makinelere kurarak birkaç saat içinde çok geniş kitlelere dünyanın her yerine yayılma imkanı bulur (Canbek ve Sağıroğlu, 2007b).

#### **2.2.4.9. Truva Atları (Trojan Horse):**

Efsaneleşen hikayeye göre Troya kralının oğlu, Sparta kralının karısına aşık olur ve onun da rızasıyla onu Troya şehrine kaçırır. Bunun üzerine Sparta kralı hem karısını hem de Troya şehrini almak için savaş açar. Yaklaşık on yıl süren bu savaşta askerler artık yorgun düşmüştür. Bunun üzerine Akhalıların komutanı Odysseus'un aklına savaşın gidişatını değiştirecek dahice bir fikir gelir. Ahşaptan yapılmış olan devasa at heykelinin içine Odysseus ile birlikte en yiğit askerler saklanır ve diğer askerler tarafından Troya şehrinin kapısına bir asker eşliğinde bırakılır. Bu hareketle savaştan çekildiklerini hissettiren Akhalı askerler pusuya yatarlar. Troya kapısında at heykeliyle bekleyen asker ise Troyalılara bu heykelin tanrıça Athena tarafından gönderildiğini bu hediye kabul ederlerse Athena tarafından ödüllendirileceğini, kabul etmezlerse Athena'nın lanetinin üzerlerine olacağını söyler. Troyalılar savaşı kazandıklarını düşündüren bu hediye kabul ederler ve zafer kutlamaları yaparlar. Troyalılar kutlamalardan yorgun düştüklerinde tahta atın içinden çıkan Akhalı askerler onlara saldırarak Troya şehrini ele geçirerek savaşı kazanırlar (Marganyan, 2019).

İsmi bu efsanedeki Truva atından alan bu kötücül yazılım kullanıcının şüphelenmeyeceği şekilde meşru bir yazılım veya program gibi görünür ve kurban bilgisayarda amaçladığı zararları vermeye başlar. Kendini kopyalama veya kendini çoğaltma gibi bir mekanizmaya sahip değildir. Bu özellikleriyle virüslerden ayrılmaktadırlar. Truva atları sisteme yararlı bir uygulama görünümünde yüklenmek, kasıtlı olarak kurumsal bir ağa tanımlanmak veya e-posta yoluyla belirlenen mağdur listesine gönderilmek suretiyle yayılmaktadır (Emm, 2008).

Genellikle arka kapılar ile karıştırılan Truva atları, arka kapılardan farklı olarak sisteme gizlice sızmak yerine faydalı bir yazılım gibi görünerek sisteme yerleşir (Canbek ve Sağıroğlu, 2007b). Sisteme kullanıcının izni olmadan yüklenmemelerine rağmen

yüklendikten sonra kullanıcının bilgisi ve onayı olmadan işlemler yapabilirler. (“Bilgisayar Virüsleri ve Kötü Amaçlı Yazılımlarla İlgili Bilgiler ve SSS”, t.y.). Truva atları belirlenen bir saatte, belirlenen bir konumda, belli bir zaman aralığında, belli web sitelerinin ziyaret edilmesiyle aktifleşecek şekilde programlanmış da olabilmektedir (Dama, 2014).

Araştırmalar sırasında Truva atının Google Play uygulamasını da manipüle edebileceğine rastlanmıştır. Kötü amaçlı yazılıma sahip uygulamalar Google Play mağazasının güvenlik duvarından geçemedikleri için prensiplere uygun olmayacak şekilde kazanç sağlamak amacıyla mağazanın kullanıcı uygulamasını nasıl manipüle edeceklerini öğrenirler. Son yıllarda Truva atının akıllı telefon kullanıcılarının bilgisi olmadan uygulamaları indirip, değerlendirip bunlar hakkında yorum yaptıkları tespit edilmiştir. Kullanıcıya direkt olarak zarar vermiyor gibi görünse de kullanımdan dolayı ve de ücretli uygulamaları bedava göstermesinden dolayı ödeme yapması gerekebilir (“How Trojans manipulate Google Play”, 2016).

#### **2.2.4.10. Kök Kullanıcı Takımı (Rootkit):**

Çalışan dosyaları, sistemsel bilgileri veya işleyen süreçleri, işletim sisteminden gizleyerek varlığını devam ettiren yazılımlardır. Yönetimsel haklara sahip en kötücül yazılımlardandır (“Rootkits, Part 1 of 3: The Growing Threat”, 2006). Rootkitler üçüncü şahısların sisteme erişimini ve sistemi uzaktan yönetmesini ve kontrolünü sağlar. Bu programlar uzaktan sistemsel sorunları çözebilmek adına faydalı olmasına karşın kötü niyetli kişilerce kişisel bilgilere izinsiz erişim ve sisteme kötücül yazılımlar yüklemek gibi kötü amaçlarla kullanılabilirler (“Bilgisayar Virüsleri ve Kötü Amaçlı Yazılımlarla İlgili Bilgiler ve SSS”, t.y.).

Rootkitleri diğer kötücül yazılımlardan ayıran en önemli özellik, üst seviye yönetimsel haklara sahip olmalarıdır. İşlevinden ötürü faydalı kullanım alanları da vardır. Kopyalamayı engellemede, anakart üreticileri tarafından üretilen yazılımları kontrol sürecinde, güvenlik duvarlarında... Antivirüs programları da bir rootkit gibidir. Sistem yönetiminde söz sahibi olur ve güvenliği yazılımlara direkt müdahalede bulunarak sağlar (Gündoğan, 2020).

#### **2.2.4.11. Klavye Dinleme Sistemleri (Keylogger):**

İki tür klavye dinleme sistemi mevcuttur. Biri donanım diğeri yazılım klavye dinleme sistemidir. Donanım klavye dinleme sistemleri doğrudan klavye içine yerleştirilebildiği gibi klavye kablosunun ucuna takılan küçük bir aparat yardımıyla veya bilgisayar kasasına içine yerleştirilen bir cihaz yardımıyla da olabilmektedir. Yazılım klavye dinleme sistemlerinde herhangi bir parçaya kabloyu gereksinim yoktur. Klavyede basılan tuş bilgilerini kaydeden ve çeşitli ortamlarda depolayarak gerektiğinde kullanan kötücül yazılımlardır. Klavye dinleme sistemleri Truva atı, spam vb. şekillerde veya direkt kurulum yapılarak sisteme dahil edilir. Sistem başlatıldığında anda o da devreye girer. İşletim sisteminde tüm yapılan hareketleri gizlice takip eder. Kullanıcının bilgisi olmadan izlenen ve elde edilen bu bilgiler istenen farklı formatlarda yedeklenir. Yedeklenen bilgilerin e-posta veya FTP (File Transfer Protocol) ile aktarımı sağlanır. Klavye dinleme sistemleri adının ötesinde çok daha fazla işlevi olan bir yazılım türüdür. Klavye tuş vuruşlarını ve fare hareketlerini izleyebilir, ekran görüntüsü alabilir, klavye kullanılarak gönderilen e-posta ve anlık mesajlaşma uygulamalarındaki mesajlara ulaşabilir, internet kullanılarak erişim sağlanan web site adreslerini elde edebilir, sistemde kurulumu yapılan ya da kaldırılan programları izleyebilir veya üzerinde çalışılan dosyalarla ilgili bilgileri elde edebilir. Klavye dinleme sistemlerinin eşlerin birbirini takibinde, okul idaresinin öğrencileri takibinde, kurumların çalışanını takibinde, ebeveynlerin çocuklarını takibinde kullandıklarına rastlanmaktadır (Canbek, 2005).

#### **2.2.4.12. Botnet Ağı:**

Bir saldırgan tarafından güvenlik açıkları olan ve bu sebeple de uzaktan yönetimi kontrol altına alınmış internet erişimine sahip bilgisayar topluluğudur (Barwinski, 2005).

Botnet, “robot” ve “network” kelimelerinin kısaltmalarının birleşiminden oluşan bir kelimedir. Aynı anda birçok ele geçirilmiş makineyi kapsamaktadır. Bu ağı elinde bulunduran kişi spam gönderen veya farklı saldırılar gerçekleştirecek kişilere bu ağı büyük meblağlara satabilir veya kiralayabilir. Bu şekilde saldırgan kazanç sağlarken birçok mağdur oluşur.

### **2.3. Bilgi Güvenliğine Yönelik Tedbirler**

#### **2.3.1. Kişisel Verilerin Korunumuna Dair Yasal Dayanak**

6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun 3.maddesinin 1.fıkrasının (a) bendinde kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi olarak tanımlanmaktadır. Kişisel verilerin işlenmesi ise; tamamen ya da kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak şartıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, korunması, değiştirilmesi, düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi içerir. 6.maddesinin 1.fıkrasında da özel nitelikli kişisel verileri detaylandırmıştır. Bu kapsamda ırk, din, etnik köken, siyasi düşünce, felsefi görüş, mezhep, kılık ve kıyafet, vakıf, dernek ya da sendika üyelikleri, sağlık durumu, cinsel hayat, ceza mahkûmiyeti, güvenlik tedbirleriyle ilgili veriler ve kişinin ölçülebilir biyolojik izleri ile genetik verileri yer almaktadır.

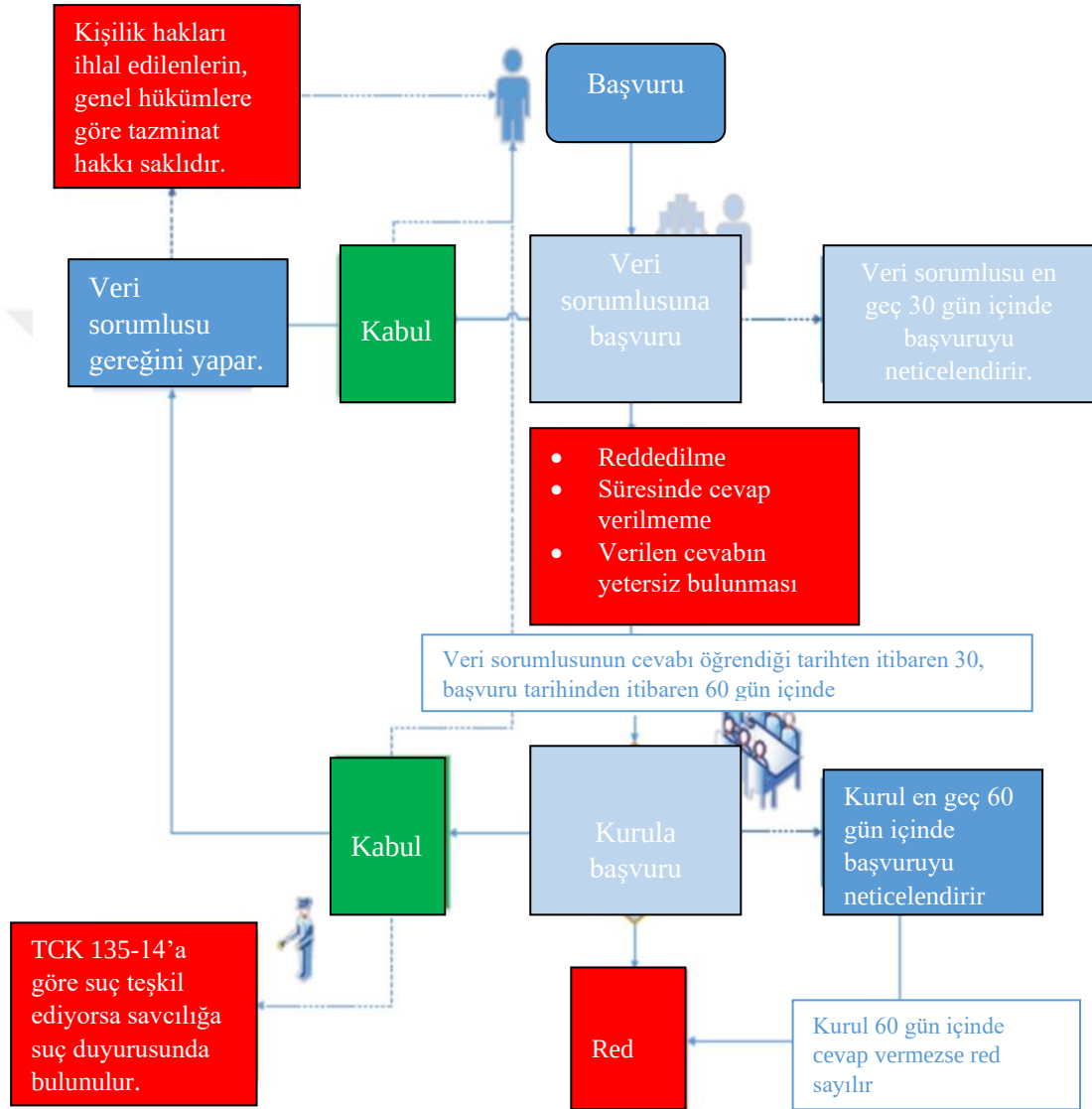
Kanun içeriğinden de anlaşılacağı gibi kişisel veriler arasında ad, soyad, doğum yeri, doğum yılı, kimlik numarası, iletişim bilgileri, ev-iş adresi, anlık konum, banka hesap numaraları, imzalar, çeşitli uygulamalar veya araçlar için kullanılan şifreler, fiziksel özellikler, parmak izi, avuç içi, yüz, iris, retina, ses vb. yer almaktadır.

29677 sayılı Resmi Gazetede de belirtildiği üzere kişisel veriler ve özel nitelikli kişisel veriler kişinin açık rızası olmadan işlenemez.

Türkiye Cumhuriyeti Anayasası'nın 20. maddesine 2010 yılında eklenen hükmü uyarınca: “Herkes kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel verileri hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızası ile işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir”.

Buna aykırı hareket eden gerçek veya tüzel kişiler 5237 sayılı Türk Ceza Kanunu'nun 135 ila 140. Maddeleri kapsamında hapis ve para cezaları ile cezalandırılır. Kişisel verilerin kaydedilmesi, hukuka aykırı olarak verilmesi veya ele geçirilmesi, verilerin yok

edilmemesi durumlarında mağdur ya da suçtan zarar gören şikayet etmese dahi suçu işleyen kişi ceza alır. Diğer durumlarsa şikayete bağlıdır.



Şekil 4. Veri Sorumlusuna Başvuru Ve Kurula Şikayet (Kaynak: Paşaoğlu, C. ve Vural, Y. (2018). Dünyada ve Türkiye’de Kişisel Verilerin Korunması. Ş. Sağiroğlu ve M. Alkan (Ed.), Siber Güç ve Savunma Farkındalık ve Caydırıcılık (s.281-308). Ankara:Grafiker)

Günlük hayatta *daha iyi hizmet verebilmek adına* telefon görüşmeleri; olası suçların önlenmesi veya tespit edilmesi adına görüntüler; kredi kartları sayesinde beğeniler; okul, iş yeri, spor merkezleri, kütüphaneler gibi yerlere giriş ve çıkış izinlerinin ya da saatlerinin

takip edilmesi amacıyla ise biyometrik veriler kayıt altına alınmaktadır (Küzeci, 2010). Güvenlik veya kontrol sebebiyle kaydedilen yukarıda bahsedilen verilere internet bankacılığında, sosyal medya hesaplarında, alışveriş sitelerinde, çevrimiçi forum veya oyun sitelerinde paylaşılan kişisel bilgiler de eklenince kişisel verilerin korunması epey zorlaşmaktadır.

Kişisel verilerin işlenmesinde kişinin açık rızasının gerekliliği anayasada da belirtilmiş olsa da hakkın aranması için ihlal edilmesi söz konusudur. Bu hakkın ihlal edilmesi ise bireyin maddi ve manevi zarar görmüş olması anlamına gelmektedir ki bu da hiç istenmeyecek bir durumdur. Bu sebeple doğabilecek zararları en aza indirmek için öncelikle bireylerde farkındalık yaratmalı, haklarından ve sorumluluklarından haberdar edilmeli aynı zamanda bu konuda bireysel olarak alınabilecek tedbirler konusunda bilgilendirilmelidir.

### **2.3.2. Ebeveyn Denetimi**

Çocuklarımızı güneşin zararlı ışınlarından, çok soğuklardan, trafikte karşılaşılabilecekleri kazalardan, sigara alkol gibi vücut sağlığını bozabilecek alışkanlıklardan ve buna benzer birçok olumsuz durumdan koruma güdüsüyle hareket eden ebeveynler olarak çocuklarımızı sosyal ağların veya internet tabanlı oyunların, içeriklerin zararlarından ne kadar koruyabiliyoruz?

Çocuklarımız ve gençlerimiz internetten değil onların zararlarından korunmalıdır. Onları, gelişen teknolojinin faydalarından yararlanırken doğabilecek zararlarından korumak adına yetkililerin ve ebeveynlerin gerekli tedbirleri alması gerekmektedir. Bunlar yapılırken çocuğun öğrenme ve bilgiye erişme hakkını da ihlal etmemeye özen gösterilmelidir. Yaşadığımız şu dönemde öğrenciler e-kütüphanelerden ve bilimsel yayınlardan yararlanarak ödevler hazırlayabilmekte, yürüttükleri projelerine katkı sağlayabilmekte, merak ettikleri konular hakkında detaylı bilgiye ulaşabilmektedir. Ancak bunları yaparken karşısına uygunsuz siteler de çıkabilir ve merakları farklı alanlara kayabilir. Kumar, pornografi, uyuşturucu, dolandırıcılık, hırsızlık, zararlı madde üretimi-tüketimi, terör eylemleri gibi birçok içerikle karşılaşabilirler. Yaşları itibariyle merak duygularının en yüksek olduğu dönemlerde olmalarının etkisiyle de hem fiziksel hem ruhsal olarak zarara uğrayabilirler. Dolayısıyla öncelikli ilk şart ebeveynlerin rol model olmasıdır. Eğer anne-baba internet kullanım süresine, sıklığına, kullanım amacına, ziyaret ettiği sitelere ve paylaşımlarına dikkat ediyorsa ailenin tüm bireyleri için de uygulanması kolay krallar

haline dönüşebilir. İkinci önemli şart onlarla kuracağımız sağlıklı bir iletişimdir. Çocuklarımızın internetle tanıştıkları ilk andan itibaren onların ne izlediklerini, ne okuduklarını, hangi oyunları oynadıklarını, kimlerle konuştuklarını, neler paylaştıklarını sormalıyız. Bunu baştan itibaren rutin haline getirdiğimizde kısıtlanmışlık hissi yaşamalarına engel olur, aksine ilgilenilen ve önemsenen bireyler olduğunu hissettirmiş oluruz. Ebeveynler ne kadar işin içinde olursa, onları gelebilecek zararlardan koruyabilme potansiyelleri de o derece artar. Rol model olma ve sağlıklı iletişimin yanı sıra teknik olarak bunu kontrol altına almaya destek olan ebeveyn denetim araçları vardır. Ebeveyn denetim araçları çocuğunuzun görebileceği içerikleri belirlemek için kullanılan ayarlardan oluşur. Onların görmelerini veya tecrübe etmelerini istemediğimiz şeylerden korumaya yardımcı olur. Bu araçlar filtreleme yazılımları ve internet kullanımını kontrol etmek için üretilen diğer araçları kapsar. Ebeveynlerin filtreleme araçlarını tercih etmeleri çocukların sağlıklı gelişimi için oldukça önemlidir. Çünkü çevrimiçi yapılan en masum aramalar her zaman masum sonuçlar vermeyebilir.

Bu filtreleme sisteminde aile ve çocuk profilleri yer almaktadır. Çocuk profilleri daha kısıtlıdır. İçerisinde sosyal medya ve sohbet siteleri yer almaz. İçeriği belli olan ve iyi yönetilen forum siteleri ve sohbet alanı bulunmayan uygun oyun siteleri profilin içindedir. Aile profilinde ise sohbet siteleri, forum siteleri ve anlık mesajlaşma içeren oyun siteleri isteğe bağlı olarak ilave edilebilir. Çocukların güvenli internet kullanımı için geliştirilmiş birçok uygulama ve yazılım bulunmaktadır (“Ebeveyn Denetim Araçları”, 2017).

Aynı zamanda ebeveynler bilgisayar ve internetin güvenli şekilde kullanımını sağlamak için çocuklarıyla birlikte uygulanabilir ve anlaşılabilir kurallar listesi hazırlamalı ve bunu çocuğun görebileceği internet kullanım alanlarına asmalıdır. Bu listede aşağıdaki maddeler yer alabilir: (Canbek ve Sağıroğlu, 2007c).

- İletişim bilgilerimizi ve fotoğraflarımızı internette paylaşma
- Seni rahatsız eden herhangi bir durumda anne-babaya haber ver
- Sanal ortamda tanıştığın kimse ile buluşma
- İnternet üzerinden gelen hiçbir kötü içerikli mesaja, e-postaya cevap verme
- Gönderenini tanımadığın hiçbir iletiyi açma
- İnternet kullanım zamanlarını anne-baba ile paylaş

- İnterneti faydalı şekilde kullan

Ebeveynlerin çocukları ile iyi bir iletişim içinde olmaları, onlarla bilinçli ve güvenli internet kullanımı hakkında konuşmaları, çocukları aile güvenliği yazılımlarıyla takip etmeleri ve uygun olmayan içerikler bulunduran siteleri engellemeleri, internet kullanım zamanlarını belirlemeleri, çocukların internet kullanımlarında ebeveyn kontrolünde olmalarını ve rahatsız edici bir durumla karşılaşmaları halinde ebeveynleriyle paylaşımlarını sağlamaları onları tehlike ve tehditlerden büyük ölçüde koruyacaktır.

Aynı zamanda Bilgi Teknolojileri ve İletişim Kurumu tarafından 4/5/2007 Tarihli ve 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanununun 10. Maddesinin 4. Fıkrasının (d) bendi uyarınca Bilgi İhbar Merkezi kurulmuştur. [ihbarweb.org.tr](http://ihbarweb.org.tr) adresi, ilgili kanunun 8. maddesinde yer alan intihara yönlendirme, cinsel istismar, uyuşturucu ve madde kullanımını kolaylaştırma, sağlığa zararlı madde temini, fuhuş, müstehcenlik, kumar oynanması için imkan sağlama, Atatürk aleyhine işlenen suçlar, yasadışı bahis suçlarıyla ilgili içeriklerin web üzerinden ihbar edilebilmesi için 23 Kasım 2007'den bu yana yayındadır ([ihbarweb.org.tr](http://ihbarweb.org.tr)). Bu adresten de, zararlı görülen içerikleri barındıran siteler gerekli önlemlerin alınabilmesi için ihbar edilmeli, böylelikle diğer internet kullanıcılarının da zarar görmeleri engellenmelidir.

### **2.3.3. İnternet Bankacılığı Ve Çevrimiçi Alışverişte Güvenlik**

İnternet bankacılığı; işlem yapacak kişinin para çekme ve para yatırma gibi somut para işlemleri dışında, banka şubelerine gitmeden, sıra beklemeden, mesai saatinde yetişme kaygısı duymadan, internet erişiminin olduğu her an para transfer etme, ödeme yapma gibi birçok bankacılık işlemlerinin yapılabildiği bankacılıktır (Ayvaz Reis, Gülseçen ve Bayrakdar, 2010).

İnternet bankacılığı bankaların müşterilerine 7 gün 24 saat birçok hizmeti uzaktan sağlamasıyla gerçekleşir. Yaşadığımız dönem internet erişimiyle zamandan ve mekandan bağımsız bir şekilde birçok ihtiyacın karşılanabildiği ve birçok bankacılık işleminin bankalara gitmeden kolaylıkla halledilebildiği bir dönemdir. Bunun en önemli sebebi ise internet bankacılığının ve çevrimiçi alışverişin hızlı ve pratik olmasıdır. Bunun yanı sıra dönemsel olarak yaşanan özel durumlar da bu imkanların kullanımını artırmakta hatta

zorunlu hale bile getirebilmektedir. 2019 yılının sonlarında başlayan hala devam eden COVID-19 salgın sürecinde de bu imkanları kullanmanın rahatlığını insanlara göstermektedir. Salgının yayılmasını önlemek ve en az zararla bu süreci atlatabilmek adına tüm ihtiyaçların olabildiğince uzaktan halledilebilme çabası içinde olmak yerinde bir karardır. Kalabalık alışveriş merkezlerine gitmeden ya da evden çıkmadan gıda, giyim, kitap, mobilya, elektronik eşya, ilaç gibi her türlü ihtiyacın karşılanabilmesi büyük bir avantajdır. Bu hizmet kolaylık ve zamandan tasarruf sağlarken, hizmet alan kişiye geniş bir yelpaze sunmakta, birçok seçeneğe ulaşmada kolaylık sağlamaktadır. Hal böyle olunca teknoloji kaynaklı birçok tehditle de karşı karşıya kalınmaktadır.

Bazen sadece bir internet bankacılığında kullanılan şifrenin ele geçirilmesi tüm sürecin ele geçirilmesi anlamına gelebilmektedir. Çünkü internet bankacılığı işlemlerinde bazen sistem otomatik olarak diğer devlet kurumlarına yönlendirebilmekte ve şahsınıza ait daha detaylı bilgiye ulaşmalarını mümkün kılmaktadır. Bunun için kişisel verilerin her birinin korunması oldukça önemlidir.

İzmir Ekonomi Üniversitesi Bilgisayar Mühendisliği Bölümü öğretim üyesi Prof. Dr. Süleyman Kondakçı gazetede yer alan ifadesinde, bazı dolandırıcıların internet üzerinden sahte iş ilanı vererek adaylardan talep ettiği veya yaptığı görüntülü mülakatlar aracılığıyla adayların kendi ağzından kişisel bilgilerini alıp kullanarak banka hesapları açtığını, yine sahte promosyon siteleri ve indirilen güvenilir olmayan uygulamalarla da kişisel verilerin ele geçirilebilmekte olduğunu belirtmiştir (“Online Alışverişte Güvenlik Uyarısı”, 2019).

İnternet bankacılığı kullanmak zamandan kazanç sağlasa da zaman kadar yapılan işlemin, internet bankacılığı kullanıcısının ve bankaların da güvenliğinin önemi unutulmamalıdır. Güvenlik sağlanmadan yapılan iş ve işlemler ciddi kayıplar doğurabilmektedir. Bu sebeple de bankalar sistem güvenliğine dikkat etmeli, hem çalışanlarını hem de müşterilerini korumak adına kişisel bilgileri korumada dikkat edilmesi gereken hususlar konusunda bilgilendirme yapmalı ve müşterilerin hesaplarında normal gidişatına ters düşecek bir hareketlenme fark ettiğinde duruma anında müdahale etmelidir (Ayvaz Reis, Gülseçen ve Bayrakdar, 2010).

Güvenli internet alışverişi ve güvenli internet bankacılığı için bankaların ve uzmanların sunduğu tavsiyelere uymak siber saldırılara maruz kalma riskini oldukça azaltmaktadır. Kullanılması tavsiye edilen güvenlik tedbirleri ise şöyledir:

*Güvenli bağlanın:* Size ait olmayan, ortak kullanıma açık olan ve güvenliğinden emin olmadığınız bilgisayarlardan bankacılık işlemleri veya alışveriş yapamayın. Kullanacağınız bilgisayarda antivirüs programının yüklü olmasına ve kullandığınız uygulamaların güvenilir olmasına dikkat edin.

İnternet bankacılığı kullanırken ve E-ticaret sitelerinde alışveriş yaparken ödeme ekranında <http://> yerine <https://> yazmasına ve alışveriş yapılan sitenin SSL sertifikası olmasına mutlaka dikkat edilmelidir. Bu sertifika, kredi kartı bilgilerinin şifrelenmesini ve başkaları tarafından kopyalanmasını engellemektedir (“İnternet Bankacılığı ve Çevrimiçi Alışveriş”, 2017).

*3D Secure Ödeme Sistemleri Kullanın:* Bu sistemle ödeme işlemi sırasında mağazadan bağımsız banka sunucuları üzerinde bir sayfada güvenlik doğrulaması yapılır. Kart bilgileriniz alışveriş yaptığınız internet mağazası tarafından hiçbir şekilde görüntülenemez. Banka işyerine ödemenin alındığı bilgisini gönderir ve ödeme tamamlanır (“İnternette Güvenli Alışveriş İçin 9 Kural”, 2020)

*Sanal Kart Kullanın:* Sanal kart kredi kartınız içinde oluşturacağınız farklı numaraya ve farklı bilgilere sahip yeni bir karttır. Sanal kartınıza alışveriş yapacağınız zaman limit belirleyerek, alışverişiniz bittiğinde kalan limiti sıfırlayarak olası izinsiz harcamalardan korunabilirsiniz.

*Mesafeli Satış Sözleşmesini Mutlaka Okuyun:* Satış sözleşmesinde, iade koşulları ya da ürünün kullanılmış olmasıyla ilgili özel maddeler yer alabilir. Detaylara hakim olmak kandırılmışlık hissi yaşamadan daha güvenli alışveriş yapmanızı sağlar (“İnternette Güvenli Bir Alışveriş Yapmanın Püf Noktaları Neler?”, 2019). Bu sözleşmeyi sunmayan platformlardan asla alışveriş yapmak güvenilir olmayacaktır. Sözleşme metinleri de dikkatli bir şekilde okunmalı, araya sıkıştırılmış, müşteri güvenliğini tehlikeye atacak veya müşteriyi zarara uğratacak yaptırımların olmadığından emin olunmalıdır.

*Güçlü Şifreler Belirleyin ve Şifrelerinizi Sık Sık Değiştirin:* Sadece internet bankacılığı ve çevrimiçi alışveriş için değil sosyal ağ hesapları, kurum hesapları, e-posta hesapları, bilgisayar tablet telefon gibi teknolojik cihazlara erişim gibi birçok farklı durumda şifreler oluşturulmaktadır (Doğan ve Aşan, 2016). Veri güvenliğini sağlamak için de bu şifrelerin kırılmalarını zorlaştıracak güçlü şifreler oluşturulmalıdır. İçinde büyük küçük harflerin, rakamların, özel karakterlerin bulunduğu, en az sekiz veya on iki karakterden oluşan, bir kelimenin tamamını içermeyen, önceki şifrelerinizden oldukça farklı olan, hatırlanması

kolay ama başkaları tarafından tahmin edilmesi zor şifreler tercih etmek diğerlerine nazaran daha güvenlidir (Microsoft, 2021). Parola oluştururken tüm gerçek kelimelerden, isimlerden, plaka numaralarından kaçının. Unutmayın en iyi parola, uydurulmuş bir dizilimdir (Guttman, Leong & Malkin, 1999 ).

Oluşturduğunuz şifrelerin belirli aralıklarla yenilenmesi; bunun yanında banka, sosyal medya siteleri, oyun siteleri, alışveriş siteleri gibi giriş bilgisi isteyen her bir uygulama için de ayrı şifreler oluşturulması oldukça etkilidir. Aynı zamanda şifrelerin akılda tutulabilmesi için alenen bilgisayar, telefon, cüzdan gibi kolay ulaşılabilir yerlere kaydedilmemesi, gerekirse küçük hatırlatıcılar eklenmesi ve üçüncü şahıslarla paylaşılmaması da güvenlik önlemleri arasında yer alır.

Kullanılan parolalar asla komut dosyalarına ya da oturum açma prosedürlerine kaydedilmemelidir çünkü bunlar sisteme erişimi olan herkes tarafından kullanılabilir (Guttman, Leong ve Malkin, 1999 ).

*Kredi Kartı Ekstrelerini Kontrol Edin:* İnternet bankacılığında kullanılan kredi kartlarının ödeme dökümleri mutlaka düzenli olarak kontrol edilmelidir. Kart sahibi tarafından yapılmayan bir ödeme veya alışveriş fark edildiğinde anında kartın bağlı bulunduğu banka ile iletişime geçilerek yapan saldırganın tespiti ve sıkıntının giderilmesi için işlemler başlatılmalıdır.

#### **2.3.4. Sosyal Ağlarda Güvenlik**

Son yıllarda teknolojinin kullanım amaçlarının çeşitlenmesi ve kullanım alanlarının genişlemesi sebebiyle bilgi teknolojileri ile iletişim teknolojileri kavramları arasındaki fark neredeyse yok olmuştur. Bazen birbiri yerine de kullanılan bu kavramlardan bilgi teknolojileri verileri toplayan, işleyen, düzenleyen ve saklayan donanım ve yazılımı ifade ederken; iletişim teknolojileri ise kişiler arası iletişimi ve etkileşimi sağlayan elektronik yapıları ve sosyal ağları ifade etmektedir (Huang, Guo, Xie ve Wu, 2012).

Açılımı Social Network Site ya da Social Network Sistem olan SNS ifadesi, Sosyal Ağ Servisi veya Sosyal Medya olarak bilinmektedir.

Sosyal ağlar, kişilerin sanal ortamda birer kimlik oluşturmak suretiyle birbirleriyle internet üzerinden iletişim kurmalarına ve etkileşimde bulunmalarına olanak sağlayan servislerdir (Palfrey ve Gasser'den aktaran Edoğın ve Bahtiyar, 2014).

Sosyal ağ siteleri, insanların sınırlı bir sistem içinde tamamen açık veya yarı açık hesaplar oluşturmalarına, bağlantılarını paylaşan diğer üyelere ulaşmalarına ve sistem içindeki diğer kullanıcılar tarafından yapılan paylaşımları izleme ve onların bağlantılarına ulaşabilmeye müsaade eden web tabanlı hizmetler olarak tanımlanmaktadır. (Boyd ve Ellison, 2007).

Geçmişte kullanılan iletişim araçlarına ek olarak, kişilerin kendini ifade etmesine, kendilerini göstermesini, bağlantılarını paylaşmasına ve diğer kullanıcılarla bağlantı kurmasına ve devam ettirebilmesine olanak tanıyan sitelerdir (Ellison, Steinfield ve Lampe, 2007) .

İnternet kullanılarak gerçekleştirilen iletişim ve etkileşim günümüzde genellikle facebook, instagram, twitter, whatsapp vb. üzerinden sağlanmaktadır. Bağımlılık haline dönüşen bu araçlar hiçbir ücret ödemeksizin sosyalleşmeyi sağlarken eski arkadaşları bulmayı, yeni arkadaşlar edinmeyi, kolay ve hızlı bir şekilde veri aktarmayı, kişinin kendi iradesiyle sunduğu kişisel verilerinin kullanılmasına müsaade ederek maddi ve manevi anlamda tehditlere maruz kaldığı, eğlenceli olduğu kadar içinde gizli tehlikeler de barındıran uygulamalardır (Yavanoğlu, Sağıroğlu ve Çolak, 2012). Kişiler bu ağlarda birçok kişisel bilgi paylaşarak, siber zorbalık, gözetlenme ve kimlik hırsızlığının kurbanı olabilirler (Taddicken, 2014). Aynı zamanda banka hesaplarının ele geçirilmesi, teknolojik aygıtlara (bilgisayar, telefon, tablet, harici bellek vb.) virüs bulaştırılması, insanların toplum önünde aşağılanması gibi birçok ciddi tehditle karşı karşıya kalabilirler (Yavanoğlu, Sağıroğlu ve Çolak, 2012).

Bu sitelerde üyelik için istenen ad, soyad, doğum tarihi, telefon, e-mail adresi gibi bilgilerin yanı sıra; kişinin arzusuna göre yaşadığı şehir, kişisel fotoğraf ve videolar, aile bağları, dosyalar, konum bilgisi de paylaşılabilir. Kişinin yakın çevresi ve sevdikleriyle iletişimini ve paylaşımını artırmaya yönelik olan ve oldukça masum görünen bu ağlar dikkat edilmediğinde ve gereken güvenlik tedbirleri alınmadığında dolandırıcılık, çocuk istismarı gibi maddi ve manevi yönden ağır sonuçlar doğurabilecek tehlikelere sebep olabilmektedir. Kişilerin sevimli ve masumca bulduğu çocukları ile ilgili paylaşımlar kötü niyetli kişilerce kötü amaçlarla, izniniz olmadan farklı platformlarda kullanılabilir.

Kullanılan sosyal ağlardan bazıları üyelik sırasında kullanıcının e-posta adresi erişim bilgilerini de talep etmektedir. Bu sayede listede bulunan diğer e-posta adreslerine ulaşabilmesine, özel yazışmalara erişilebilmesine, zararlı içerikli e-postalara sizin adınıza

izin vermek suretiyle bilgilerinizi ele geçirmesine izin vererek çok büyük bir güvenlik açığı oluşturmaktadır (Yavanoğlu, Sağıroğlu ve Çolak, 2012).

Bunun yanında sosyal ağlar hakkında düşünmemiz gereken oldukça derin bir taraf daha bulunmaktadır. Sosyal ağlar özel işletmelerce, üyelere kişisel verileri toplayarak reklamcılara satmak suretiyle kazanç elde etmek amaçlı kurulmaktadır. Dolayısıyla üye olunan her sosyal ağ, kişisel verilerin hiç de farkında olmadan yayılması anlamına gelmektedir. Yani gizlilik ayarları tam koruma sağlamamakta, burada aldığınız güvenlik önlemleri sizi yalnızca diğer üyelere karşı korumaktadır (“Protect Yourself and Your Data When Using Social Networking Sites”, 2013). Bu, sosyal ağ sitelerinin gizlilik politikalarında da açıkça belirtilmektedir.

Web günlükleri, terör amaçlı bir araya gelen grupların siyasi, dini ya da ekonomik ideolojilerini hedef kitlelere duyurabildikleri, gruplaşma ve ayrışmayı hedefleyen bir platform olarak da kullanılmaktadır. Bu kitleler web günlüklerinde arayüzler kodlayarak kişilerin sosyal ağlardaki paylaşım ve mesajlarını taramak suretiyle anlamsal bağlantılar ortaya çıkararak haberleşmeye imkan sağlamakta ve örgütlenmelerini kolaylaştırmaktadır (Yang ve Ng, 2007).

Sosyal ağ sitelerinden bazıları ise kolay ya da çözülebilir şifreleme teknikleri kullanarak üyelik bilgilerinin kötü niyetli kişilerce ulaşılmasını olanak sağlamaktadır.

Bu sitelere üye olurken güvenlik önlemlerinin alındığından emin olunmalıdır. Az kullanılan ve sadece bu tarz üyelikler için kullanmayı tercih ettiğiniz e posta bilgileriyle giriş yapılmalı, hesaplar için güçlü şifreler oluşturulmalı, profiller herkes tarafından değil sadece yakın çevrenin görebileceği şekilde sınırlandırılmalı, aile bireylerinin özellikle de çocukların fotoğraf ve videolarının paylaşımından kaçınılmalı, direkt mesaj bölümünden dahi banka hesap numaraları ve şifreler paylaşılmamalı, konum bilgisi verilmemelidir. Bu platformlarda paylaşılan fotoğraflarda bulunan diğer kişiler etiketlenmemeli veya başkalarının sizi etiketlemesine müsaade edilmemelidir. Bunu yapanlar uyarılmalı, doğurabileceği sıkıntılar anlatılmalıdır. Çünkü çok basit görünmesine karşın bir bankacılık işleminde sorulan anne adı, baba adı, çocuk sayısı, anne kızlık soyadı gibi bilgiler bu sayede belirlenebilmektedir.

Bunun yanı sıra sosyal medya ağlarına üyeliklerde 13 yaş sınırlaması vardır ve buna dikkat edilmesi oldukça önemlidir. Ancak teknoloji içine doğan nesil erken dönemde teknoloji kullanmaya başladıklarından bu durum daha da tehlike arz etmektedir (Office of

Communication [Ofcom], 2008). Sosyal ađın gizlilik politikalarında yer alan yař kısıtına dikkat edilmeli, aileler bu konuda bilinçlendirilmelidir. Buna rađmen yanlış bilgiler girerek kaydolan çocuklar için tehlike daha da büyük olmaktadır. Çocuklar kişisel bilgilerinin güvenliğini sağlamada bilinçli olmadıkları gibi, herkesi kendileri kadar masum görmekte ve kötü niyetli insanların anlattıklarına kolayca inanarak onların söylediklerini de yapma eğilimde olabilmektedirler. Bu sebeptendir ki çocuklar teknoloji kullanırken ebeveynleri tarafından yakından takip edilmeli, yönlendirilmeli ve onlara karşılaşılabilecekleri her türlü olumsuz durumu aileleri ile paylaşımlarının ehemmiyeti anlatılmalıdır. Tüm bunlar dikkate alınarak bilgi paylaşımı gerçekleştirilmeli ve gereken yazılım tedbirleriyle de riskler en aza indirilmeye çalışılmalıdır.

Sosyal ađlarda en çok karşılaşılan güvenlik tehditleri ise şunlardır: Kimlik taklidi, istenmeyen e-postalar, kötü amaçlı sosyal ađ uygulamaları, siteler arası kod çalıştırma ve istek sahteciliđi, phishing, casus yazılımlar, sahte linkler... (Yavanođlu, Sađırođlu ve Çolak, 2012).

Zeydan (2006), internet bađlantısına sahip telefon, tablet bilgisayar vb. araçlarda karşılaşılabilecek tehditlerin sebeplerini řu şekilde ifade etmiştir. İşletim sistemindeki yani donanımları belli amaçlar çerçevesinde programlayabilen yazılımlardaki (“İşletim Sistemi”, 2020) eksiklikler, kullanıcıların sahip olduđu sosyal medya, oyun vs. hesaplarına üyeliklerde veya üyelik sonrası ayarlardaki eksiklikler, bluetooth yazıcı gibi dosya ve cihaz paylaşımı sırasında oluşan açıklar, ađ tarayıcısı açıkları, kötücül ve casus yazılımlar ile güvenilir olmayan yazılımlardır.

Tüm bunlar dikkate alınarak sosyal ađ üyelikleri gerçekleştirilmeli, gizlilik politikalarının yer aldıđı metinler dikkatlice okunup anlaşıldıktan sonra sıkıntı yaratacak bir ifadenin yer almadığından emin olunduđu takdirde üyelikler yapılmalı, mümkün olduđuca kişisel veriler paylaşılmamalı ve kullanılan sosyal ađın gizlilik ayarları da herkes tarafından görülmeyecek şekilde belirlenmelidir (Erdođan ve Bahtiyar, 2014).

Bilgi güvenliğini sağlamak amacıyla alınacak önlemleri řu şekilde derleyebiliriz (Canbek ve Sađırođlu, 2007b; Şenol ve Karacan, 2012).

- Kullanılan cihaz yazılımlarının güncelleştirmeleri zamanında yapılmalıdır.
- Cihazlarda güncel ve güvenilir olan anti-virüs programları kullanılmalıdır.

- Kullanılan uygulamaların her birine farklı ve kolay tahmin edilemeyen şifreler belirlenmelidir.
- Belirlenen şifreler belli aralıklarla yenilenmelidir.
- Gelen e-postaların gönderici adresleri dikkatle incelendikten sonra içeriği dikkate alınmalıdır.
- Bankalardan, alışveriş sitelerinden veya sosyal medya hesaplarından gelen mesajlar ve e-postalar açılırken bunların sahte adreslerden gelmiş olma ihtimalleri göz önünde bulundurulmalı ve kullanıcı adı, şifresi gibi kişisel bilgilerin güncellenmesini talep eden e-postalarda yer alan linkler açmamalıdır.
- Kişisel bilgilerle ilgili güncellemeleri yönlendirme mailleri veya mesajlarıyla değil uygulamanın kendisi açılarak yapılmalıdır.
- Kullanılan bankacılık veya sosyal medya uygulamaları işlemler bittikten sonra “çıkış” yapılarak kapatılmalıdır.
- Çocukların kullanımında onlara güvenli olan ve olmayan alanlar doğru bir şekilde anlatılmalı ve karşılaşılabilecekleri rahatsız edici ve kötü durumları ebeveynleriyle paylaşmaları gerektiği öğretilmelidir.
- Ev kullanıcıları ve çocuklar ile kurum çalışanları karşılaşılabilecekleri riskler hakkında bilgilendirilmelidir.
- Her kurumda bilişim teknolojileri alanında uzman bir personel bulundurulmalı, bilgi ve sistem güvenliği sağlama konusunda bilgi ve tecrübelerinden faydalanılmalıdır.
- Ortaokuldan başlayarak kurumlarda çalışan personellere kadar tüm seviyelerde bilişim teknolojilerini doğru kullanma, bilgi güvenliği farkındalığı, doğabilecek riskler ve bunlara karşı alınabilecek tedbirler hakkında eğitimler verilmelidir.
- Gerçek anlamda güvenliğini sağlanabilmesi, tehditlerin saptayabilmesi ve bu tehditleri gidermeye yönelik teknoloji ve prosedürleri devreye sokabilmesi için kurumlar ve şirketler TS ISO IEC 27001 standardında belirtilen bilgi güvenliği yönetim sistemini kurmalıdır (Türk Standartları Enstitüsü [TSE], t.y.).

- G venlik politikası, bir sitenin teknolojisine ve bilgi varlıklarına erişim izni verilen kullanıcıların uyması gereken kuralların b t n d r. Karar vericiler ve y neticiler tarafından oluřturulan bu g venlik politikasına kullanıcı uymakla y k ml d r. Bu sebeple internete veya bařka bir genel aęa baęlanmadan  nce erişim saęlayıcısı olarak kullanılması planlanan sitenin g venlik politikası dikkatlice okunmalıdır (Guttman, Leong & Malkin, 1999 ).
- Her kullanıcı kendi sistem rutinlerinin farkında olmalıdır. Var olan dosyalarda deęişiklik, kaybolma, erişim sıkıntısı, tuhaf yeni dosyaların ortaya  ıkması gibi alıřılmadık bir durumla karřı karřıya kalındığında g venlik yetkilisiyle iletiřime ge erek yardım istenmelidir (Guttman, Leong & Malkin, 1999 ).



## BÖLÜM III

### YÖNTEM

Bu bölümde araştırma modeli, evren ve örneklem, araştırmada kullanılan veri toplama araçları, verilerin toplanmasında izlenen yol ve verilerin analizinde uygulanan istatistiksel teknikler üzerinde durulmuştur.

#### 3.1. Araştırmanın Modeli

Bu çalışmada ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeylerinin belirlenmesi ve farklı değişkenler açısından incelenmesi amacını taşımaktadır. Araştırma bu yönüyle betimsel bir araştırma olup tarama modeli altında yer almaktadır. Tarama modelleri, geçmişte var olmuş ya da var olan bir durumu mevcut şekliyle betimlemeyi amaçlayan modellerdir. Araştırmaya konu olan olay, birey ya da nesne, kendi koşulları içinde ve olduğu gibi tanımlanmaya çalışılır. Onları, herhangi bir şekilde değiştirme, etkileme çabası gösterilmez. Önemli olan anlaşılacak istenen durumu uygun bir biçimde belirlemektir (Karasar, 2012, s.81).

#### 3.2. Evren ve Örneklem

Araştırmanın evrenini Ankara ili Sincan ilçesi Milli Eğitim Müdürlüğüne bağlı 43 resmi ortaokul oluşturmaktadır.

Araştırmanın örneklemi ise 2020-2021 Eğitim-Öğretim yılı Ankara ili Sincan ilçesindeki Milli Eğitim Müdürlüğüne bağlı 6 devlet ortaokulunda öğrenim gören 614 ortaokul öğrencisi oluşturmaktadır.

İki aşamalı örnekleme yöntemi kullanılmıştır. Birinci aşamada küme örnekleme ile 6 ortaokul seçilmiştir. İkinci aşamada ise uygun örnekleme ile 614 öğrenciye ulaşılmıştır.

Çalışmanın yapılacağı ortaokullar ve öğrenci sayıları belirlenirken Millî Eğitim Bakanlığı 2020-2021 Eğitim-Öğretim dönemi örgün eğitim istatistikleri (MEB, 2021) dikkate alınmıştır. Bu araştırmada veri toplamak için Sincan'da bulunan okulların seçilmesinin temel sebebi örnekleme ulaşılabilirliğinin kolay olmasıdır. Çalışma grubunu oluşturan öğrencilerin demografik özelliklerine ilişkin frekans ve yüzde değerleri Tablo 1'de gösterilmektedir.

Tablo 1.

*Örnekleme Oluşturan Öğrencilerin Demografik Özelliklerine İlişkin Frekans ve Yüzde Değerleri*

| Değişkenler         | Kategoriler       | Frekans (f) | Yüzde (%) |
|---------------------|-------------------|-------------|-----------|
| Sınıf               | 7.Sınıf           | 286         | 46,60     |
|                     | 8.Sınıf           | 328         | 53,40     |
|                     | Toplam            | 614         | 100,00    |
| Cinsiyet            | Kız               | 325         | 52,90     |
|                     | Erkek             | 289         | 47,10     |
|                     | Toplam            | 614         | 100,00    |
| Baba Öğrenim Düzeyi | İlkokul Mezunu    | 169         | 27,50     |
|                     | Ortaokul Mezunu   | 140         | 22,80     |
|                     | Lise Mezunu       | 222         | 36,20     |
|                     | Üniversite Mezunu | 83          | 13,50     |
|                     | Toplam            | 614         | 100,00    |
| Anne Öğrenim Düzeyi | İlkokul Mezunu    | 236         | 38,40     |
|                     | Ortaokul Mezunu   | 176         | 28,70     |
|                     | Lise Mezunu       | 175         | 28,50     |
|                     | Üniversite Mezunu | 27          | 4,40      |
|                     | Toplam            | 614         | 100,00    |
| Günlük Ayrılan Süre | 0-1 saat          | 100         | 16,30     |
|                     | 1-3 saat          | 245         | 39,90     |
|                     | 3-5 saat          | 162         | 26,40     |
|                     | 5 saat ve üstü    | 107         | 17,40     |
|                     | Toplam            | 614         | 100,00    |

Tablo 1 incelendiğinde, çalışma grubunu oluşturan 614 öğrencinin 286'sı (%46,60) 7. sınıf ve 328'i (%53,40) 8. sınıftır. Öğrencilerin 325'i (%52,90) kız ve 289'u (%47,10) ise erkektir. Tablo 1'e göre araştırmaya katılan öğrencilerden 169'nun(%27,50) babası ilkokul mezunu, 140'nın (%22,80) babası ortaokul mezunu, 222'sinin (%36,20) babası lise mezunu ve 83'sünün (%13,50) babası ise üniversite mezunudur. Tablo 1'e göre araştırmaya katılan öğrencilerden 236'sının (%38,40) annesi ilkokul mezunu, 176'sının (%28,70) annesi ortaokul mezunu, 175'nin (%28,50) annesi lise mezunu ve 27'sinin (%4,40) annesi ise üniversite mezunudur. Tablo 1 incelendiğinde, araştırmaya katılan ortaokul öğrencilerinin 100'ü (%16,30) internet veya internetin kullanıldığı uygulamalara günlük 0-1 saat arasında süre ayırdığı, 245'i (%39,90) internet veya internetin kullanıldığı uygulamalara günlük 1-3 saat arasında süre ayırdığı, 162'si (%26,40) internet veya internetin kullanıldığı uygulamalara günlük 3-5 saat arasında süre ayırdığı ve 107'si (%17,40) internet veya internetin kullanıldığı uygulamalara günlük 5 saat ve üstünde süre ayırdığı görülmektedir.

### **3.3. Veri Toplama Araçları**

Araştırmada, Kişisel Bilgi Formu ve Bilgi Güvenliği Farkındalığı Ölçeği ve kullanılmıştır. Aşağıda bu ölçeklere ait bilgiler verilmiştir.

#### **3.3.1. Kişisel Bilgi Formu**

Araştırmada ele alınan bağımsız değişkenler hakkında bilgi toplayabilmek amacıyla araştırma sürecinde araştırmacı tarafından geliştirilen “Kişisel Bilgi Formu” kullanılmıştır. Kişisel Bilgiler Formu'nda cinsiyet, sınıf düzeyi, anne-baba eğitim düzeyi, internet veya internetin kullanıldığı uygulamalara günlük ayrılan toplam süreye ilişkin bilgiler yer almaktadır.

#### **3.3.2. Bilgi Güvenliği Farkındalığı Ölçeği (BGFÖ)**

Ortaöğretim kurumlarında öğrenim gören öğrencilerin bilgi güvenliği farkındalık düzeylerini belirlemeye yönelik olarak Güldüren, Çetinkaya ve Keser (2016) tarafından geliştirilen “Bilgi Güvenliği Farkındalık” ölçeği kullanılmıştır. Güldüren, Çetinkaya ve Keser (2016) tarafından yapılan çalışma ortaöğretim kurumlarında öğrenim gören 607

öğrenciyle gerçekleştirilmiştir. Çalışmanın ilk aşamasında, 407 kişilik katılımcı grubu ile Açıklayıcı Faktör Analizi (AFA) yapılmıştır. AFA sonucunda, ölçeğin 36 madde ve 3 faktörden (“Saldırı ve Tehditler: ST”, “Mahremiyet: MA” ile “Kişisel Verilerin Korunması: KVK”) oluştuğu belirlenmiştir. Çalışmanın ikinci aşamasında, 200 kişilik katılımcı grubu ile gerçekleştirilen Doğrulamalı Faktör Analizi (DFA) sonucunda 3 faktörlü yapı doğrulanmıştır. Ölçeğin tamamı için Cronbach's Alpha güvenirlik katsayısı ,955; her faktör için sırasıyla ST: ,954, MA: ,890 ile KVK: ,808'dir. Elde edilen bu bulgular geliştirilen ölçeğin ortaöğretim kurumlarındaki öğrencilerin bilgi güvenliği farkındalık düzeylerini belirlemek için gerekli psikometrik özelliklere sahip bir ölçme aracı olduğu görülmüştür.

### **3.3.2.1. Bilgi Güvenliği Farkındalık Ölçeği Geçerlik ve Güvenirliği**

Güldüren, Çetinkaya ve Keser (2016) tarafından geliştirilen ölçeğin geçerlik ve güvenirlik çalışması ortaöğretim öğrencileri üzerinden yapılmıştır. Mevcut araştırmada ise “Bilgi Güvenliği Farkındalık Ölçeği” ortaokul öğrencilerine uygulanmıştır. Mevcut araştırmada ölçeğin orijinal halinin uygulandığı örneklemden farklı bir örnekleme uygulanması göz önüne alınarak yeniden geçerlik ve güvenirlik çalışması yapılmasına karar verilmiştir. Geçerlik çalışması için ölçeğin geliştirildiği özgün formundaki model yapısı göz önünde bulundurularak Doğrulamalı Faktör Analizi (DFA) yapılmıştır.

DFA için varsayımların test edilmesi gerekmektedir. Bu varsayımların başında araştırma örnekleminin faktör analizi yapmak için uygun olup olmadığının belirlenmesi gelmektedir. Örneklemin DFA için uygun olup olmadığını belirlemek için Kaiser-Meyer-Olkin (KMO) katsayısı ve Barlett Küresellik testi hesaplanmıştır (Leech, Barrett ve Morgan, 2005). Örnekleme büyüklüğünü faktör analizine uygun olması için ve DFA'ya devam edebilmek için KMO katsayısının ,50'nin üstünde ve Barlett Küresellik testinin anlamlı çıkması gerekmektedir (Tabachnick ve Fidell, 2013; Tavşancıl, 2014; Field, 2009). Elde edilen analiz bulguları sonucunda, KMO değeri ,98 ve Barlett Küresellik testi sonucu anlamlı bulunmuştur ( $\chi^2 = 22551,914$ ;  $p=0,00 < 0,05$ ). KMO katsayısının ,90'dan büyük olması veri yapısının faktör analizi için mükemmel derecede yeterli olduğu yorumu yapılabilir (Leech vd., 2005). Ayrıca Barlett Küresellik testinin anlamlı çıkması verilerin çok değişkenli normal dağılımdan geldiğini ve dolayısıyla DFA' nın bir diğer varsayımının karşılandığını göstermektedir. Bir diğer varsayım olarak çok değişkenli uç değer olup

olmadığını tespit etmek için maddelerin Mahalonobis uzaklıkları hesaplanmış ve çok değişkenli uç değer olmadığı görülmüştür. Son olarak bir diğer varsayım olarak maddeler arasında çoklu bağlantı sorunu olup olmadığı incelenmiştir. Bu varsayım için ölçekteki maddeler arasında pearson korelasyonları hesaplanmıştır. Maddeler arasında hesaplanan korelasyon değerlerinden hiçbirisi ,70'in üzerinde değer bulunmamıştır. Elde edilen bu bulguya göre maddeler arasında çoklu bağlantı sorunu olmadığını göstermektedir.

DFA için varsayımların sağlanmasından sonra analize geçilmiştir. DFA' da model parametrelerinin kestiriminde en çok olabilirlik yöntemi kullanılmıştır. DFA sonucunda elde edilen modelin veri uyumunu değerlendirmek için uyum indeksleri olarak Ki-Kare( $\chi^2$ ) serbestlik derecesine (sd) oranı ( $\chi^2/sd$ ), Yaklaşık Hataların Ortalama Karekökü (RMSEA), Standartlaştırılmış Artık Ortalamaların Karekökü (SRMR), İyi Uyum İndeksi (GFI), Düzenlenmiş İyi Uyum İndeksi (AGFI), Karşılaştırmalı Uyum İndeksi (CFI), Normlaştırılmış Uyum İndeksi (NFI) ve Normlaştırılmamış Uyum İndeksi (NNFI) uyum indeksleri kullanılmıştır. DFA ile elde edilen  $\chi^2/sd$  oranının 5'ten küçük olması, GFI değerinin ,90'dan yüksek olması, SRMR ve RMSEA değerlerinin ise ,05' ten düşük çıkması, model veri uyumu için ölçüt değerler olarak kabul edilmektedir (Jöreskog & Sörbom, 1993; Marsh & Hocevar, 1988). Ancak bu değerlerden GFI ve AGFI' nin ,85'ten büyük çıkması, SRMR ve RMSEA değerlerinin ,10'dan düşük olması model veri uyumu için yeterli düzeyde kabul edilebilir ölçütler olarak değerlendirilmektedir (Anderson ve Gerbing, 1984; Cole, 1987; Marsh, Balla, ve McDonald, 1988). Diğer uyum indeks istatistiklerinden CFI, NFI ve NNFI indekslerinin ise ,95'in üzerinde olması çok iyi bir uyumu göstermektedir. CFI,NFI ve NNFI değerlerinin ,90-0,95 arasında olması ise kabul edilebilir bir uyumu göstermektedir (Sümer, 2000).

Orijinal ölçekteki üç faktörden ve 36 maddeden oluşan model yapısı DFA ile analiz edilmiştir. Analiz sonucunda model veri uyum indeks değerleri, maddelere ilişkin t değerleri, faktör yük değerleri ve hata varyansları elde edilmiştir. DFA sonucunda elde edilen bulguların değerlendirilmesinde ilk kontrol edilmesi gereken maddelere ilişkin t değerlerinin manidarlık düzeyidir. Model veri uyumunun sağlanması için maddelere ilişkin t değerlerinin manidar olması gerekmektedir. Buna göre, eğer maddelere ilişkin t değerleri 1,96'yı aşarsa ,05 düzeyinde ve 2,56'yı aşarsa ,01 düzeyinde manidardır. Manidar olmayan t değerlerine sahip maddeler analiz dışı bırakılması gerekmektedir. Fakat sadece t değerlerine göre maddelerin çıkarılmasına karar vermeden önce maddelere ilişkin hata

varyanslarının kontrol edilmesi gerekmektedir (Çokluk, Şekercioğlu ve Büyüköztürk, 2012, s.304).

İlk yapılan DFA sonucunda, Madde 11 için elde edilen t değeri 1,68 olarak bulunmuş ve Madde 12 için elde edilen t değeri ise 1,26'dır. Her iki madde için de elde edilen t değerleri ,05 anlamlılık düzeyinde 1,96'dan düşük olduğu için her iki maddenin de manidar t değeri vermediği görülmüştür. Manidar olmayan t değerlerinin yanında bu iki madde için hata varyansları ve faktör yükleri de incelenmiştir. Buna göre, Madde 12 için elde edilen hata varyans değeri 1,00, faktör yük değeri ise ,07 olarak bulunmuştur. Madde 11 için elde edilen hata varyans değeri ise ,99 ve faktör yük değeri ise ,09 olarak bulunmuştur. Maddelerin faktör yük değerlerinin ,30'dan yüksek ve hata varyanslarının ise ,90'dan düşük olması maddelerin ölçülmek istenen özelliği ölçebildiklerini göstermektedir (Çokluk, Şekercioğlu ve Büyüköztürk, 2012). Bu nedenle Madde 11 ve Madde 12 için elde edilen faktör yük değerlerinin ,30'dan düşük olması ve hata varyanslarının ise ,90'dan yüksek olması bu maddelerin analiz dışı bırakılmasını gerekli kılmıştır. Bu doğrultuda ilk olarak Madde 12 analiz dışı bırakılmıştır. Madde 12 çıkarıldıktan sonra yeniden yapılan DFA' da Madde 11 için faktör yük değeri ,10 ve hata varyans değerinin ise ,99 olduğu görülmüştür. Bu nedenle Madde 11'de analiz dışı bırakılmıştır. Her iki maddenin de analiz dışı bırakılması ile 34 madde ile yeniden DFA yapılmıştır.

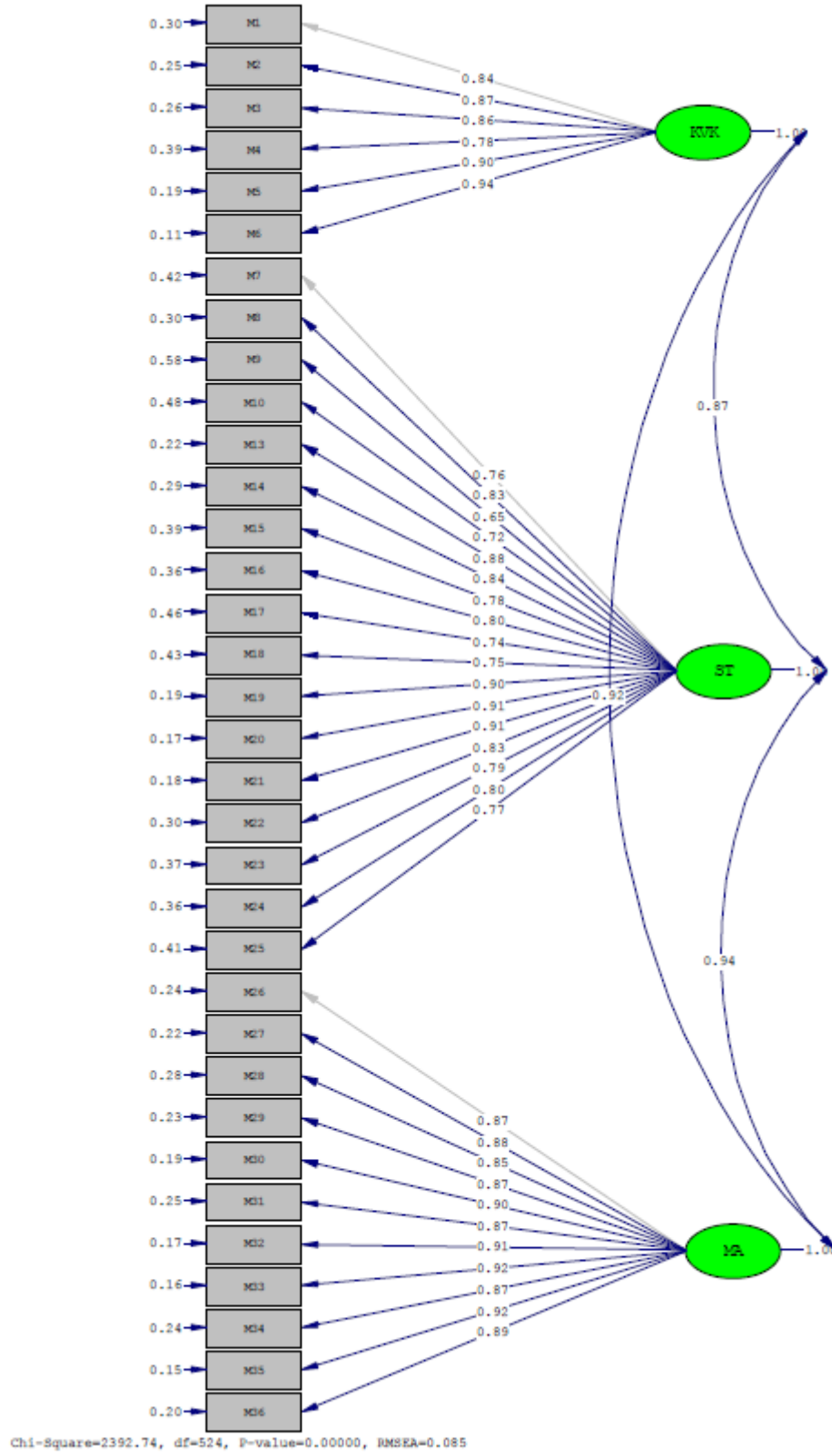
Üç faktörlü 34 maddeden oluşan yeni model için t değerleri, faktör yük değerleri ve hata varyansları incelenmiştir. Her bir madde için elde edilen t değerleri ,01 anlamlılık düzeyinde 2,56'dan büyük bulunmuştur. DFA sonucunda elde edilen model veri uyum indeksleri Tablo 2'de gösterilmektedir.

Tablo 2.

Bilgi Güvenliği Farkındalığı Ölçeği (BGFÖ) Uyum İndeksleri ve Uyum İndekslerinin Kabul Sınırları

| Uyum İndeksleri | BGFÖ | Sınır Değerler                   |
|-----------------|------|----------------------------------|
| $\chi^2/sd$     | 4,56 | $\leq 5$                         |
| RMSEA           | ,08  | $\leq ,05$<br>veya<br>$\leq ,10$ |
| SRMR            | ,05  | $\leq ,10$                       |
| GFI             | 1,00 | $\geq ,85$                       |
| AGFI            | 1,00 | $\geq ,85$                       |
| CFI             | ,99  | $\geq ,90$                       |
| NFI             | ,98  | $\geq ,90$                       |
| NNFI            | ,98  | $\geq ,90$                       |

Tablo 2 incelendiğinde model – veri uyumuna ilişkin elde edilen uyum indeks değerlerinin tamamının, ölçüt değerlerini karşıladıkları görülmüştür. Böylece 34 maddeden ve 3 faktörden oluşan ölçme modeli, veri uyumunun oldukça iyi olduğu söylenebilir. Bilgi Güvenliği Farkındalık Ölçeği’ ndeki maddelere ilişkin elde edilen standart faktör yük değerleri ve yol diyagramı Şekil 1’de gösterilmektedir.



Şekil 5. Bilgi Güvenliği Farkındalık Ölçeği'ne İlişkin Yol Diyagramı

Şekil 1’de iki maddenin çıkarılmasının ardından 34 madde ve üç faktörden oluşan ölçme modeline ilişkin standart faktör yük değerleri ve hata varyansları gösterilmektedir. Öncelikle her bir madde için elde edilen t değerlerinin anlamlı olduğu görülmüştü ( $p < ,01$ ). Uyum indeks değerlerinin de model veri uyumunu sağlaması neticesinde maddelere ilişkin standart faktör yük değerleri hesaplanmıştır. Şekil 1’de görüldüğü üzere ortaokul öğrencilerine yönelik uygulanan Bilgi Güvenliği Farkındalık Ölçeği 34 maddeden oluşmaktadır. Maddelerin faktörlere dağılım şu şekildedir.

1.Faktör (Kişisel Verilerin Korunması) =M1,M2,M3,M4,M5,M6

2.Faktör (Saldırı ve Tehditler) =M7,M8,M9,M10,M13,M14,M15,M16,M17, M18,M19,M20,M21, M22,M23,M24,M25

3.Faktör (Mahremiyet)= M26,M27, M28,M29,M30,M31,M32,M33,M34,M35,M36

Kişisel Verilerin Korunması faktörü altında yer alan maddelerin faktör yük değerleri  $\lambda = ,78$  ile  $\lambda = ,94$  arasında ve hata varyansları da  $\varepsilon = ,11$  ile  $\varepsilon = ,39$  arasında değişmektedir. Saldırı ve Tehditler faktörü altında yer alan maddelerin faktör yük değerleri  $\lambda = ,65$  ile  $\lambda = ,91$  arasında ve hata varyansları da  $\varepsilon = ,17$  ile  $\varepsilon = ,58$  arasında değişmektedir. Mahremiyet faktörü altında yer alan maddelerin faktör yük değerleri  $\lambda = ,85$  ile  $\lambda = ,92$  arasında ve hata varyansları da  $\varepsilon = ,15$  ile  $\varepsilon = ,28$  arasında değişmektedir. Her üç faktör altında yer alan maddelerin faktör yük değerlerinin ,30’dan yüksek ve hata varyanslarının ise ,90’dan düşük olması maddelerin ölçülmek istenen özelliği ölçebildiklerini göstermektedir (Çokluk, Şekercioğlu ve Büyüköztürk, 2012). Model veri uyum indeks değerlerinin kabul edilebilir değerler arasında bulunması ve maddelerin faktör yük değerleri ile hata varyanslarının ölçüt değerleri karşılaması ölçeğin geçerliğinin sağlandığını göstermektedir. Buna göre, ölçeğe ilişkin modelin veriye oldukça iyi düzeyde uyum sağladığını ve modelde yer alan maddelerin ilgili yapıları iyi temsil ettikleri söylenebilir.

Ortaokul öğrencileri için Bilgi Güvenliği Farkındalık Ölçeği’ nin geçerliğinin sağlanmasının ardından güvenilirliğine geçilmiştir. Ölçeğin güvenilirliği için faktörlerin ve ölçek toplam puanının Cronbach  $\alpha$  katsayısı hesaplanmış ve elde edilen sonuçlar Tablo 3’de gösterilmiştir.

Tablo 3.

Bilgi Güvenliği Farkındalık Ölçeğinin Cronbach  $\alpha$  Katsayıları

| <b>Faktör Adı</b>           | <b><math>\alpha</math> Değeri</b> |
|-----------------------------|-----------------------------------|
| Kişisel Verilerin Korunması | ,93                               |
| Saldırı ve Tehditler        | ,95                               |
| Mahremiyet                  | ,97                               |
| Ölçek Toplam                | ,98                               |

Ölçeğin güvenirliğini ortaya çıkarmak amacıyla faktörlere ve ölçek toplam puana ilişkin Cronbach Alfa iç tutarlılık katsayısı hesaplanmıştır. Kline (1999) ,80 güvenirlik katsayısının ölçümlerin güvenirliği için uygun olduğunu belirtmesine rağmen ,70 değerinden yüksek olan değerlerinde güvenirlik için yeterli olduğu görüşünü savunmaktadır. Tablo 3 incelendiğinde Kişisel Verilerin Korunması faktörünün  $\alpha$  değerinin ,93 bulunurken, Kişisel Verilerin Korunması faktörünün  $\alpha$  değerinin ,95 olarak ve Mahremiyet faktörünün  $\alpha$  değerinin ,97 olduğu görülmektedir. Ayrıca ölçeğin bütünü için elde edilen  $\alpha$  değerinin ,98 olduğu görülmektedir. Elde edilen bu değerlere göre ortaokul öğrencilerine yönelik Bilgi Güvenliği Farkındalık Ölçeği' nin faktörlerinin ve toplam puanının güvenirliğinin oldukça yüksek olduğu söylenebilir.

#### 3.4. Verilerin Analizi

Araştırma kapsamında toplanan veriler SPSS programına aktarılmıştır. Daha sonra veri seti incelenerek yanlış girilen veri ya da kayıp veri olup olmadığı kontrol edilmiştir. Yanlış girilen ve kayıp veri olmadığı görülmüştür. Araştırma kapsamında, Güldüren, Çetinkaya ve Keser (2016) tarafından lise öğrencilerinin bilgi güvenliği farkındalıklarını belirlemek amacıyla geliştirilmiş “Bilgi Güvenliği Farkındalık Ölçeği” ortaokul öğrencilerine uygulanmıştır. Ölçeğin uygulandığı örneklemin orijinal formun uygulandığı örneklemden farklı olması sebebi ile ölçek için yeniden geçerlik ve güvenirlik çalışması yapılmıştır. Ölçeğin geçerliği için DFA gerçekleştirilmiş ve güvenirliği için ise Cronbach Alfa iç tutarlılık katsayısı hesaplanmıştır. DFA için varsayımlar test edilmiş ve veri setinde çok değişkenli uç değer olmadığı görülmüştür. Ayrıca veri setinde çok değişkenliği normalliğin sağlandığı, çoklu bağlantı sorunun olmadığı görülmüştür.

Arařtırma kapsamında ortaokul ğrencilerinin bilgi gvenlięi farkındalık dzeylerinin nasıl olduęunu belirlemek iin BGF faktr puanları ile lek toplamına iliřkin betimsel istatistikler (minimum, maksimum, ortalama, standart sapma) hesaplanmıřtır.

Arařtırmada ortaokul ğrencilerinin bilgi gvenlięi farkındalık dzeylerinin demografik deęiřkenlere gre anlamlı farklılık gsterip gstermedięini incelemek iin parametrik testlerden yararlanılmıřtır. Buna gre, iki grubun karřılařtırılmasında İliřkisiz rneklemler t-testi kullanılırken, ikiden fazla grubun karřılařtırılmasında Tek Ynl Varyans Analizi (ANOVA) kullanılmıřtır. Varyans analizinin anlamlı olduęu durumlarda hangi gruplar arasında anlamlı farklılıęın olduęunu belirlemek iin Tukey oklu karřılařtırma testinden yararlanılmıřtır. Verilerin analizinde anlamlılık dzeyi  $p=,05$  olarak alınmıřtır. leęin geerlięinin incelenmesinde LISREL 8.8 paket programı ve leęin gvenirlięi ile dięer analizlerde ise SPSS 21.0 paket programı kullanılmıřtır.

## BÖLÜM IV

### BULGULAR VE YORUM

Bu bölümde, araştırma kapsamında toplanan verilerin analizlerinin sonucunda elde edilen bulgular, araştırma sorularının sırasına uygun olarak tablo ve açıklamalarıyla birlikte verilmiştir.

#### **Birinci araştırma sorusu “Ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeyleri nasıldır?” a ilişkin elde edilen bulgular ve yorumlar**

Çalışmaya katılan ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeylerini incelemek için “Bilgi Güvenliği Farkındalık Ölçeği” nden aldıkları puanların betimsel istatistikleri hesaplanmıştır. Elde edilen sonuçlar Tablo 4’ de gösterilmektedir.

Tablo 4.

#### *Çalışmaya Katılan Öğrencilerin “Bilgi Güvenliği Farkındalık Ölçeği” Puanları Betimsel İstatistikleri*

| Faktörler                             | n   | Min | Max | Ort.   | Ort./Madde sayısı | s.s   |
|---------------------------------------|-----|-----|-----|--------|-------------------|-------|
| Kişisel Verilerin Korunması (6 Madde) | 614 | 6   | 30  | 22,43  | 3,74              | 6,77  |
| Saldırı ve Tehditler (17 Madde)       | 614 | 19  | 84  | 54,05  | 3,18              | 17,86 |
| Mahremiyet (11 Madde)                 | 614 | 11  | 55  | 39,45  | 3,59              | 13,36 |
| Ölçek Toplam (34 Madde)               | 614 | 36  | 167 | 115,93 | 3,41              | 35,96 |

Tablo 4’e göre araştırmaya katılan ortaokul öğrencilerinin Bilgi Güvenliği Farkındalık Ölçeği faktörlerinden aldıkları ortalama puanların madde sayısına bölünmesi ile elde edilen ortalamalar incelendiğinde; öğrencilerin kişisel verilerin korunmasına daha çok önem verirken (3,74) saldırı ve tehditler boyutuna ise en az önemi (3,18) verdikleri görülmektedir.

**İkinci araştırma sorusu olan “Ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeyleri cinsiyete göre anlamlılık farklılık göstermekte midir?” e ilişkin elde edilen bulgular ve yorumlar**

Çalışmaya katılan öğrencilerin “Bilgi Güvenliği Farkındalık Ölçeği” nden aldıkları puanların cinsiyetlerine göre anlamlı bir farklılık gösterip göstermediğini belirlemek için ilişkisiz örneklem t-testi yapılmıştır. Elde edilen sonuçlar Tablo 5’de gösterilmektedir.

Tablo 5.

*Araştırmaya Katılan Ortaokul Öğrencilerinin Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Puanlarının Cinsiyetlerine Göre İlişkisiz Örneklem t-Testi Sonuçları*

| Faktörler                   | Cinsiyet | n   | $\bar{X}$ | s.s   | t    | sd  | p     |
|-----------------------------|----------|-----|-----------|-------|------|-----|-------|
| Kişisel Verilerin Korunması | Kız      | 325 | 23,49     | 5,75  | 4,19 | 612 | ,000* |
|                             | Erkek    | 289 | 21,23     | 7,60  |      |     |       |
| Saldırı ve Tehditler        | Kız      | 325 | 56,47     | 16,28 | 3,60 | 612 | ,000* |
|                             | Erkek    | 289 | 51,31     | 19,14 |      |     |       |
| Mahremiyet                  | Kız      | 325 | 41,45     | 11,58 | 4,00 | 612 | ,000* |
|                             | Erkek    | 289 | 37,19     | 14,81 |      |     |       |
| Ölçek Toplam                | Kız      | 325 | 121,42    | 31,60 | 4,07 | 612 | ,000* |
|                             | Erkek    | 289 | 109,74    | 39,44 |      |     |       |

\*p ≤ ,05

Tablo 5 incelendiğinde, ortaokul öğrencilerinin BGFÖ Kişisel Verilerin Korunması faktör puan ortalamalarının cinsiyetlerine göre anlamlı bir farklılık gösterdiği görülmüştür [t(612)= 4,19; p ≤,05]. Ayrıca, kızların kişisel verilerin korunması farkındalıkları ortalaması ( $\bar{X}$ =23,49), erkeklerin kişisel verilerin korunması farkındalıkları ortalamasından ( $\bar{X}$ =21,23) daha yüksektir. Bu bulgu kişisel verilerin korunmasında kızların erkeklere göre farkındalıklarının daha yüksek olduğunu göstermektedir.

Tablo 5 incelendiğinde, ortaokul öğrencilerinin BGFÖ Saldırı ve Tehditler faktör puan ortalamalarının cinsiyetlerine göre anlamlı bir farklılık gösterdiği görülmüştür [t(612)= 3,60; p ≤,05]. Ayrıca, kızların saldırı ve tehditler faktörü ortalaması ( $\bar{X}$ =56,47), erkeklerin saldırı ve tehditler faktör ortalamasından ( $\bar{X}$ =51,31) daha yüksektir. Bu bulgu kızların saldırı ve tehditler bilgi güvenliği farkındalıklarının erkeklere göre daha yüksek olduğunu göstermektedir.

Tablo 5 incelendiğinde, ortaokul öğrencilerinin BGFÖ Mahremiyet faktör puan ortalamalarının cinsiyetlerine göre anlamlı bir farklılık gösterdiği görülmüştür [ $t(612)=4,00$ ;  $p \leq,05$ ]. Ayrıca, kızların mahremiyet faktörü ortalaması ( $\bar{X}=41,45$ ), erkeklerin mahremiyet faktör ortalamasından ( $\bar{X}=37,19$ ) daha yüksektir. Bu bulgu kızların mahremiyet bilgi güvenliği farkındalıklarının erkeklere göre daha yüksek olduğunu göstermektedir.

Tablo 5 incelendiğinde, ortaokul öğrencilerinin BGFÖ toplam puan ortalamalarının cinsiyetlerine göre anlamlı bir farklılık gösterdiği görülmüştür [ $t(612)=4,07$ ;  $p \leq,05$ ]. Ayrıca, kızların BGFÖ toplam puan ortalaması ( $\bar{X}=121,42$ ), erkeklerin BGFÖ toplam puan ortalamasından ( $\bar{X}=109,74$ ) daha yüksektir. Bu bulgu kızların bilgi güvenliği farkındalıklarının erkeklere göre daha yüksek olduğunu göstermektedir.

**Üçüncü araştırma sorusu olan “Ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeyleri anne eğitim düzeylerine göre anlamlılık farklılık göstermekte midir?” e ilişkin elde edilen bulgular ve yorumlar**

Çalışmaya katılan ortaokul öğrencilerinin Bilgi Güvenliği Farkındalık Ölçeği faktör ve toplam puanlarının anne eğitim düzeylerine göre anlamlı bir farklılık gösterip göstermediğini incelemek için ANOVA yapılmıştır. Elde edilen sonuçlar Tablo 6’da gösterilmektedir.

Tablo 6.

*Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Puanlarının Anne Eğitim Düzeyine Göre ANOVA Sonuçları*

| Faktörler                          | Anne Eğitim Düzeyi    | n   | $\bar{X}$ | s.s   | F    | p     | Anlamlı Farklılık |
|------------------------------------|-----------------------|-----|-----------|-------|------|-------|-------------------|
| <b>Kişisel Verilerin Korunması</b> | (1) İlkokul Mezunu    | 236 | 21,53     | 7,01  | 2,80 | ,039* | 3>1               |
|                                    | (2) Ortaokul Mezunu   | 176 | 22,51     | 6,58  |      |       |                   |
|                                    | (3) Lise Mezunu       | 175 | 23,33     | 6,61  |      |       |                   |
|                                    | (4) Üniversite Mezunu | 27  | 23,77     | 6,17  |      |       |                   |
| <b>Saldırı ve Tehditler</b>        | (1) İlkokul Mezunu    | 236 | 52,36     | 17,80 | 1,40 | ,241  |                   |
|                                    | (2) Ortaokul Mezunu   | 176 | 54,97     | 17,87 |      |       |                   |
|                                    | (3) Lise Mezunu       | 175 | 55,64     | 17,95 |      |       |                   |
|                                    | (4) Üniversite Mezunu | 27  | 52,33     | 17,19 |      |       |                   |
| <b>Mahremiyet</b>                  | (1) İlkokul Mezunu    | 236 | 37,94     | 13,59 | 1,80 | ,146  |                   |
|                                    | (2) Ortaokul Mezunu   | 176 | 39,88     | 13,18 |      |       |                   |
|                                    | (3) Lise Mezunu       | 175 | 40,88     | 13,28 |      |       |                   |
|                                    | (4) Üniversite Mezunu | 27  | 40,55     | 12,45 |      |       |                   |
| <b>Ölçek Toplam</b>                | (1) İlkokul Mezunu    | 236 | 111,84    | 36,25 | 1,81 | ,143  |                   |
|                                    | (2) Ortaokul Mezunu   | 176 | 117,37    | 35,86 |      |       |                   |
|                                    | (3) Lise Mezunu       | 175 | 119,85    | 35,86 |      |       |                   |
|                                    | (4) Üniversite Mezunu | 27  | 116,66    | 32,76 |      |       |                   |

\*p ≤ ,05

Tablo 6'ya göre araştırmaya katılan ortaokul öğrencilerinin Kişisel Verilerin Korunması faktöründen aldıkları puanların anne eğitim düzeyine göre anlamlı bir farklılık gösterdiği görülmüştür ( $F_{(3,613)}=2,80$ ;  $p \leq ,05$ ). Buna göre öğrencilerin kişisel verilerin korunması farkındalıkları üzerinde anne eğitim düzeylerinin etkisi bulunmaktadır. Anlamlı farklılığın hangi gruplar arasında olduğunu belirlemek için yapılan Tukey karşılaştırma testi sonuçlarına göre annesi lise mezunu olan ortaokul öğrencilerinin Kişisel Verilerin Korunması faktör puan ortalaması ( $\bar{X}=23,33$ ), annesi ilkokul mezunu olan ortaokul öğrencilerinin faktör puan ortalamasından ( $\bar{X}=21,53$ ) daha yüksektir.

Tablo 6'ya bakıldığında araştırmaya katılan ortaokul öğrencilerinin Saldırı ve Tehditler faktöründen aldıkları puanların anne eğitim düzeylerine göre anlamlı bir farklılık göstermediği görülmüştür ( $F_{(3,613)}=1,40$ ;  $p>,05$ ). Tablo 6'ya göre, araştırmaya katılan ortaokul öğrencilerinin Mahremiyet faktöründen aldıkları puanların anne eğitim

düzeylerine göre anlamlı bir farklılık göstermediği görülmüştür ( $F_{(3,613)}=1,80$ ;  $p>,05$ ). Benzer şekilde, araştırmaya katılan ortaokul öğrencilerinin BGFÖ toplam puanların anne eğitim düzeylerine göre anlamlı bir farklılık göstermediği görülmüştür ( $F_{(3,613)}=1,81$ ;  $p>,05$ ) Buna göre, ortaokul öğrencilerinin Saldırı ve Tehditler, Mahremiyet faktör puanlarının ve BGFÖ toplam puanlarının annelerinin eğitim düzeylerine göre anlamlı bir şekilde değişmemektedir.

**Dördüncü araştırma sorusu olan “Ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeyleri baba eğitim düzeylerine göre anlamlılık farklılık göstermekte midir?” e ilişkin elde edilen bulgular ve yorumlar**

Çalışmaya katılan ortaokul öğrencilerinin Bilgi Güvenliği Farkındalık Ölçeği faktör ve toplam puanlarının baba eğitim düzeylerine göre anlamlı bir farklılık gösterip göstermediğini incelemek için ANOVA yapılmıştır. Elde edilen sonuçlar Tablo 7’de gösterilmektedir.

Tablo 7.

*Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Puanlarının Baba Eğitim Düzeyine Göre ANOVA Sonuçları*

| Faktörler                          | Baba Eğitim Düzeyi    | n   | $\bar{X}$ | s.s   | F    | p    | Anlamlı Farklılık |
|------------------------------------|-----------------------|-----|-----------|-------|------|------|-------------------|
| <b>Kişisel Verilerin Korunması</b> | (1) İlkokul Mezunu    | 169 | 21,90     | 6,92  | ,602 | ,614 |                   |
|                                    | (2) Ortaokul Mezunu   | 140 | 22,39     | 6,86  |      |      |                   |
|                                    | (3) Lise Mezunu       | 222 | 22,83     | 6,35  |      |      |                   |
|                                    | (4) Üniversite Mezunu | 83  | 22,48     | 7,44  |      |      |                   |
| <b>Saldırı ve Tehditler</b>        | (1) İlkokul Mezunu    | 169 | 52,59     | 17,95 | ,517 | ,671 |                   |
|                                    | (2) Ortaokul Mezunu   | 140 | 54,60     | 17,96 |      |      |                   |
|                                    | (3) Lise Mezunu       | 222 | 54,54     | 17,02 |      |      |                   |
|                                    | (4) Üniversite Mezunu | 83  | 54,72     | 19,75 |      |      |                   |
| <b>Mahremiyet</b>                  | (1) İlkokul Mezunu    | 169 | 38,20     | 13,84 | ,727 | ,536 |                   |
|                                    | (2) Ortaokul Mezunu   | 140 | 39,67     | 13,32 |      |      |                   |
|                                    | (3) Lise Mezunu       | 222 | 40,17     | 12,50 |      |      |                   |
|                                    | (4) Üniversite Mezunu | 83  | 39,68     | 14,69 |      |      |                   |
| <b>Ölçek Toplam</b>                | (1) İlkokul Mezunu    | 169 | 112,69    | 36,66 | ,644 | ,587 |                   |
|                                    | (2) Ortaokul Mezunu   | 140 | 116,67    | 36,10 |      |      |                   |
|                                    | (3) Lise Mezunu       | 222 | 117,55    | 33,72 |      |      |                   |
|                                    | (4) Üniversite Mezunu | 83  | 116,89    | 40,09 |      |      |                   |

Tablo 7'ye göre araştırmaya katılan ortaokul öğrencilerinin Kişisel Verilerin Korunması faktöründen aldıkları puanların baba eğitim düzeyine göre anlamlı bir farklılık göstermediği görülmüştür ( $F_{(3,613)}=,602; p>,05$ ). Tablo 7'ye göre araştırmaya katılan ortaokul öğrencilerinin Saldırı ve Tehditler faktöründen aldıkları puanların baba eğitim düzeyine göre anlamlı bir farklılık göstermediği görülmüştür ( $F_{(3,613)}=,517; p>,05$ ). Tablo 7'ye göre, araştırmaya katılan ortaokul öğrencilerinin Mahremiyet faktöründen aldıkları puanların baba eğitim düzeylerine göre anlamlı bir farklılık göstermediği görülmüştür ( $F_{(3,613)}=,727; p>,05$ ). Benzer şekilde, araştırmaya katılan ortaokul öğrencilerinin BGFÖ toplam puanların baba eğitim düzeylerine göre anlamlı bir farklılık göstermediği görülmüştür ( $F_{(3,613)}=,644; p>,05$ ). Buna göre, ortaokul öğrencilerinin Kişisel Verilerin Korunması, Saldırı ve Tehditler, Mahremiyet faktör puanlarının ve BGFÖ toplam puanlarının babalarının eğitim düzeylerine göre anlamlı bir şekilde değişmemektedir.

**Beşinci araştırma sorusu olan “Ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeyleri internet veya internetin kullanıldığı uygulamalara ayırdığı günlük süreye göre anlamlı farklılık göstermekte midir?” e ilişkin elde edilen bulgular ve yorumlar**

Çalışmaya katılan ortaokul öğrencilerinin Bilgi Güvenliği Farkındalık Ölçeği faktör ve toplam puanlarının baba eğitim düzeylerine göre anlamlı bir farklılık gösterip göstermediğini incelemek için ANOVA yapılmıştır. Elde edilen sonuçlar Tablo 8’de gösterilmektedir.

Tablo 8.

*Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Puanlarının İnternete Ayırılan Günlük Süreye Göre ANOVA Sonuçları*

| Faktörler                          | Günlük Süre        | n   | $\bar{X}$ | s.s   | F     | p    | Anlamlı Farklılık |
|------------------------------------|--------------------|-----|-----------|-------|-------|------|-------------------|
| <b>Kişisel Verilerin Korunması</b> | (1) 0-1 saat       | 100 | 22,88     | 7,60  | ,468  | ,705 |                   |
|                                    | (2) 1-3 saat       | 245 | 22,24     | 6,75  |       |      |                   |
|                                    | (3) 3-5 saat       | 162 | 22,72     | 6,18  |       |      |                   |
|                                    | (4) 5 saat ve üstü | 107 | 21,98     | 6,90  |       |      |                   |
| <b>Saldırı ve Tehditler</b>        | (1) 0-1 saat       | 100 | 56,72     | 19,19 | 1,173 | ,319 |                   |
|                                    | (2) 1-3 saat       | 245 | 53,63     | 17,76 |       |      |                   |
|                                    | (3) 3-5 saat       | 162 | 54,23     | 16,26 |       |      |                   |
|                                    | (4) 5 saat ve üstü | 107 | 52,21     | 19,02 |       |      |                   |
| <b>Mahremiyet</b>                  | (1) 0-1 saat       | 100 | 40,27     | 14,27 | ,643  | ,587 |                   |
|                                    | (2) 1-3 saat       | 245 | 39,16     | 13,18 |       |      |                   |
|                                    | (3) 3-5 saat       | 162 | 40,19     | 12,69 |       |      |                   |
|                                    | (4) 5 saat ve üstü | 107 | 38,19     | 13,94 |       |      |                   |
| <b>Ölçek Toplam</b>                | (1) 0-1 saat       | 100 | 119,87    | 39,51 | ,857  | ,463 |                   |
|                                    | (2) 1-3 saat       | 245 | 115,04    | 35,84 |       |      |                   |
|                                    | (3) 3-5 saat       | 162 | 117,16    | 32,75 |       |      |                   |
|                                    | (4) 5 saat ve üstü | 107 | 112,39    | 37,44 |       |      |                   |

Tablo 8’e göre araştırmaya katılan ortaokul öğrencilerinin Kişisel Verilerin Korunması faktöründen aldıkları puanların internete ayırdıkları günlük süreye göre anlamlı bir farklılık göstermediği görülmüştür ( $F_{(3,613)}=,468$ ;  $p>,05$ ). Tablo 8’e göre araştırmaya katılan ortaokul öğrencilerinin Saldırı ve Tehditler faktöründen aldıkları puanların internete ayırdıkları günlük süreye göre anlamlı bir farklılık göstermediği görülmüştür ( $F_{(3,613)}=1,173$ ;  $p>,05$ ). Tablo 8’e göre, araştırmaya katılan ortaokul öğrencilerinin

Mahremiyet faktöründen aldıkları puanların internete ayırdıkları günlük süreye göre anlamlı bir farklılık göstermediği görülmüştür ( $F_{(3,613)}=,643$ ;  $p>,05$ ). Benzer şekilde, araştırmaya katılan ortaokul öğrencilerinin BGFÖ toplam puanların internete ayırdıkları günlük süreye göre anlamlı bir farklılık göstermediği görülmüştür ( $F_{(3,613)}=,857$ ;  $p>,05$ ). Buna göre, ortaokul öğrencilerinin Kişisel Verilerin Korunması, Saldırı ve Tehditler, Mahremiyet faktör puanlarının ve BGFÖ toplam puanlarının internete ayırdıkları günlük süreye göre anlamlı bir şekilde değişmemektedir.



## BÖLÜM V

### SONUÇ VE ÖNERİLER

#### 5.1. Sonuç

Bilginin dijital ortamlarda sıkça kullanılması, paylaşılması ve saklanması; bilginin değiştirilmesi, üçüncü şahıslarla paylaşılması, erişiminin engellenmesi ya da farklı amaçlar için kullanılması gibi birçok tehlike doğurur.

Bilgi ve bilgisayar güvenliğinde güvenlik süreçlerinin belirlenmesinde olası saldırıların iyi analiz edilmiş olması ve gerçekleşme ihtimali yüksek olan durumlar için önlemler alınması ya da yeni önlemler tasarlanması daha etkili olacaktır. Bilgisayar sistemlerine yapılan saldırılar çoğunlukla direkt olarak güvenlik sistemini yok etmeyi ya da çökertmeyi hedeflemez. Sistem açıklarından faydalanır, korunmasız olduğu alanları araştırarak sistemi zayıf noktasından ele geçirmeyi hedefler. Ulaşmak istediği bilgilere güvenlik sistemine fark ettirmeden yapmak asıl amaçtır (Canbek, 2005). Güvenlik açığı, ilgili alanın (uygulama, program, sistem vs.) güvenliğini tehdit eden ve tehlikeye sokan beklenmedik bir anda gerçekleşerek istenmeyen sonuçlara sebep olan sistemden veya sistem kullanıcısından kaynaklı zayıflıklardır (Guttman, Leong ve Malkin, 1999 ). Shamir'in bu konuda söylediği “güvenliğe saldırılmaz, güvenlik atlatılır” sözü durumu özetlemektedir (Shamir'den aktaran Canbek, 2005). Bu noktada da genellikle kullanıcı faktörünün yarattığı boşluklardan ve oluşturduğu açıklardan yararlanır. Dolayısıyla kullanıcı ne kadar bilinçli olursa aldatılma riski o kadar düşük olacak, bunun doğal sonucu olarak da elinde bulundurduğu bilgi o kadar güvende olacaktır.

Teknolojinin içene doğan ve teknolojiyi hayatlarının odağında yaşamak mecburiyetinde olan çocuklarımız, sahip oldukları en kıymetli varlık olan bilgiyi korumanın gerekliliğini

algılayamazsa ciddi sorunlarla karşılaşacaktır. Çocuklar ve gençler, şimdi ve gelecekte bu konuda önemli role sahiptirler. Onların bilgi güvenliğine önem veren bilinçli kullanıcılar olmaları birçok saldırıyı engellemeyi ve bu bilinci yaymaya yardımcı olmayı sağlayacaktır.

Bu araştırmanın bilgi güvenliği farkındalığı üç alt boyutta incelenmiştir. Bunlar Kişisel Verilerin Korunumu (KVK), Saldırı ve Tehditler (ST), Mahremiyet (MA) tir. Birinci araştırma sorusu “*Ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeyleri nasıldır?*” şeklinde düzenlenmişti. Araştırma verileri doğrultusunda ortaokul öğrencilerinin bilgi güvenliğinde en çok önemi kişisel verilerin korunması faktörüne verdikleri, saldırı ve tehditler faktörüne ise en az önemi verdikleri gözlemlenmiştir. Beder ve Ergün (2015) tarafından yapılan çalışmada “Telif Hakkı İhlali” ve “Sorun Olabilecek Paylaşımlar” ile ilgili bilinç düzeylerinin düşük seviyede olduğu, “Yazılımsal Tehditler” konusunda kararsız kaldıkları sonucuna ulaşılmıştır. Hacımustafaoğlu (2019)’ da yaptığı çalışmada ortaöğretim öğrencilerinin bilgi güvenliği farkındalığının yeterli düzeyde olduğunu görmüştür. Yılmaz, Karaoğlu Yılmaz, Öztürk ve Karademir (2017) liselerde öğrenim gören öğrenciler üzerinde yaptıkları çalışmada öğrencilerin yarısına yakınının erişim ve şifre güvenliği konusunda, yarısından fazlasının ise sosyal ağların güvenliği, e-posta güvenliği ile tehditler ve korunma yolları konusunda farkındalıklarının yüksek olduğu sonucuna varılmış ancak yazılım yükleme, güncelleme ve yedekleme ile kullanıcı farkındalıkları ve sosyal mühendislik farkındalıklarının düşük olduğu görülmüştür.

İkinci araştırma sorusu “*Ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeyleri cinsiyete göre anlamlılık farklılık göstermekte midir?*” şeklindeydi. Burada ise bilgi güvenliği farkındalığının kişisel verilerin korunumu, saldırı ve tehditler ile mahremiyet alt boyutlarının tümünde kız öğrencilerin erkeklere göre farkındalıklarının daha yüksek olduğu sonucuna ulaşılmıştır. Bu doğrultuda Beder ve Ergün (2015) yaptıkları çalışmada kız öğrencilerin erkek öğrencilere göre güvenli internet kullanımı konusunda daha bilinçli hareket ettikleri sonucuna ulaşmıştır. Yine Derin ve Gençoğlu (2021) çalışmasında kızların erkeklere göre bu konuda daha bilinçli olduklarını görmüştür. Buna zıt olarak Güldüren, Çetinkaya ve Keser (2016) ortaöğretim öğrencileri üzerinde yaptıkları çalışmada, bilgi güvenliği farkındalık düzeylerinin üç alt faktörde de toplam puanlar göz önüne alındığında da erkek öğrencilerin kız öğrencilere göre daha yüksek olduğu görülmüştür. Talan ve Aktürk (2021)’ün yaptığı çalışma lise öğrencilerinin bilgi güvenliği farkındalığının cinsiyet

bileşeni açısından Güldüren, Çetinkaya ve Keser' in yaptığı çalışmayla paralellik gösterdiği görülmüştür.

*“Ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeyleri anne eğitim düzeylerine göre anlamlılık farklılık göstermekte midir?”* şeklindeki üçüncü araştırma sorusuna yönelik elde edilen verilere göre araştırmaya katılan ortaokul öğrencilerinin bilgi güvenliği farkındalığının anne eğitim düzeylerine göre anlamlı bir farklılık göstermediği ancak kişisel verilerin korunması farkındalıkları üzerinde anne eğitim düzeylerinin anlamlı bir etkisi olduğu sonucuna varılmıştır. Yapılan çalışmada annesi lise mezunu olan öğrenci ile annesi ilkokul mezunu olan öğrenci arasında farklılaşmanın belirgin olduğu sonucu çıkmıştır. Annesi lise mezunu olan öğrencilerin, ilkokul mezunu olan öğrencilere göre kişisel verilerin korunumu konusunda farkındalıklarının daha yüksek olduğu söylenebilir. Ancak ST ve MA alt boyutlarına bir etkisi olmadığı gözlemlenmiştir. Tekin ve Polat (2016) tarafından yapılan çalışmada velilerin çocuklarının kişisel bilgileri paylaşmaması, internet alışverişi yapmaması, internette tartışma ortamına dahil olmaması ve internette karşılaşabilecekleri kötü niyetli kişilerin varlığından haberdar olması konularında farkındalık düzeylerinin yüksek olduğu ancak velilerin cinsiyetinin güvenli internet kullanımı farkındalığına etkisi olmadığı sonucu çıkmıştır. Buna zıt olarak anne-baba öğrenim durumlarının bireysel güvenli internet kullanımı farkındalığına bir etkisi olmadığı sonucuna ulaşılmıştır. Aynı şekile Vilander (2021) araştırmasında 18 yaş ve üstü bireylerde bilgi güvenliği farkındalığı konusunda çalışmış, bilgi güvenliği farkındalığının yaş ile doğru orantılı bir şekilde arttığı sonucuna ulaşmıştır. Deneyimin bilgi güvenliği farkındalığında önemli bir faktör olduğu ancak alınan örgün eğitimin bu konuda belirleyici olmadığı sonucuna varılmıştır.

*Dördüncü araştırma sorusu “Ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeyleri baba eğitim düzeylerine göre anlamlılık farklılık göstermekte midir?”* şeklinde düzenlenmişti. Baba eğitim düzeylerinin bilgi güvenliği farkındalığına ve 3 alt boyutuna etkisi olmadığı görülmüştür. Karaoğlu Yılmaz ve Çavuş Ezin (2017) çalışmasında velilerin çocuklarının bilgi güvenliği konusunda farkındalıklarını artırmak amaçlı çocuklarını sıkça uyardıkları ancak onlara somut bir fayda sunamadıkları, velilerin en çok zararlı yazılımlar hakkında bilgi sahibi oldukları diller tehditler hakkında yetersiz oldukları sonucuna ulaşmıştır.

Son araştırma sorusu ise “Ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeyleri internet veya internetin kullanıldığı uygulamalara ayırdığı günlük süreye göre anlamlı farklılık göstermekte midir?” şeklindeydi. Elde edilen veriler internet ve internetin kullanıldığı uygulamalara ayırdıkları günlük sürenin ortaokul öğrencilerinin Kişisel Verilerin Korunması (KVK), Saldırı ve Tehditler (ST), Mahremiyet (MA) farkındalıklarını ve genel bilgi güvenliği farkındalığını etkilemediğini göstermiştir. Buna zıt olarak Derin ve Gençoğlu (2021) internet daha çok kullanan öğrencilerin olası tehlikeleri oldukça farkında olduğu, interneti sadece sosyal medya amaçlı kullanan öğrencilerin ise tehlikelerden habersiz olduğu sonucuna ulaşmıştır. Talan ve Aktürk (2021)’in yaptığı çalışma internet kullanım süresi açısından değerlendirildiğinde Derin ve Gençoğlu’nun çalışmasıyla paralellik göstermektedir.

## 5.2. Öneriler

Dünya teknolojiyle evrilirken, okullarda platform oyunu oynama becerisi, oyunlarda matematiksel taktikler geliştirme, e-sportmenlik gibi dersler verilirken çocuklar ve gençler başta olmak üzere toplumu teknolojinin getirebileceği zararlardan korumak adına dijital teknolojiden uzaklaştırmak akılcı bir çözüm olmayacaktır.

Dijital teknolojiler bilginin varlığını sürdürdüğü yeni ortamlar sunmaktadır. O zaman öncelikle bilgi güvenliğini sağlamanın ne derece önemli olduğu ve sahip olunan bilginin güvenliği sağlanmadığında ne gibi olumsuzluklara sebep olacağı fark ettirilmelidir. Bu konuda eğitim verecek uzmanlar yetiştirilmeli, dijital teknolojileri kullanan herkesi bilinçlendirmek hedeflenmelidir. Bu bilincin kazandırılmasında okulların gücünden yararlanılmalıdır. Okullarda dijital vatandaşlık ayrı bir disiplin olarak verilmelidir.

- Her kullanıcının kullanım alanına ve ihtiyacına uygun olarak eğitimler planlanmalıdır. Her bilişim teknolojileri kullanıcılarına genel bilgiler içeren bir eğitim planlaması yapılması genel farkındalık kazandırmayı sağlasa da kullanışlılık açısından yeterli olmayacaktır. Karşılaşılabilecek tehlikelerden korunmak için eğitimlerin özelleştirilmesi önemlidir. Her bilişim teknolojileri kullanıcısının ihtiyaçları farklılık göstermektedir. Farklılıklar göz önünde bulundurularak her kullanıcı grubunun karşılaşılabileceği tehditler analiz edilmeli ve buna yönelik eğitim programları hazırlanmalıdır.

- Biliřim teknolojilerini kullanan herkes bilgi gvenlięi konusunda eęitilmeli ancak bu eęitim sadece bilgi dzeyinde kalmamalı, uygulama kısmında ne derece kazanım saęladıkları gzlemlenmeli ve takip edilmelidir. Bloom'un ęrenme hiyerarřisi de gz nne alınarak kalıcılıęın ve faydanın yksek seviyede olması iin kullanıcıları iřin odaęına yerleřtirerek ęrenme dzeyleri artırılmalıdır.
- Yařanılan bu dnemde teknolojinin ve teknoloji kullanılan tm araların hızlı deęiřimine řahit olunmaktadır. Biliřim teknolojilerinde yenilikler ve deęiřimler olacak ve bundan dolayı oluřabilecek tehdit ve tehlikeler de farklılıklar gsterecektir. Bu sebeple eęitimlerin gncel bilgilerle yinelenmesi olduka nemlidir.



## KAYNAKLAR

- AFAD (t.y.). *Doğal Afetler*. <https://www.afad.gov.tr/afadem/dogal-afetler> sayfasından erişilmiştir.
- Aksoy, B. & Sayın, H. (2018, Ekim). *Ortaokul ve lise öğrencilerinin şifre oluşturma bilincinin belirlenmesi. international conference on data science and applications (ICONDATA)*, 446-453, Yalova.
- Altınöz, M., Tosun, N., Çinkiliç, T. & Çay, E. (t.y.). *Siber güvenlik ve bilinçli sosyal medya kullanımı dersi pilot uygulamasına ilişkin öğretmen görüşleri*. <https://dergipark.org.tr/tr/download/article-file/718889> adresinden erişilmiştir.
- Anderson, J. C., & Gerbing, D.W. (1984). The effect of sampling error on convergence, improper solutions, and goodness-of-fit indices for maximum likelihood confirmatory factor analysis. *Psychometrika*, 49, 155-173.
- Avşar Arık, I. (2018). *Teknoloji bağımlılığı ve sosyal kimlik oluşumu: Y nesli*. Yüksek Lisans Tezi, Hacettepe Üniversitesi Sosyal Bilimleri Enstitüsü, Ankara.
- Ayvaz Reis, Z., Gülseçen, S. ve Bayrakdar, B. (Şubat, 2010). Güvenli internet bankacılığı eğitim sistemi: GIBES. *XII. Akademik Bilişim Konferansı*, 1(1), Muğla, Türkiye, 1-5
- Barwinski, M. A. (2005). *Taxonomy of spyware and empirical study of network drive-by-downloads*. Thesis, Calhoun: Institutional Archive of the Naval Postgraduate School, California.
- Bayley, P. J., & Squire, L. R. (2002). Medial temporal lobe amnesia: gradual acquisition of factual information by nondeclarative memory. *The Journal of Neuroscience*, 22, 5741–5748.
- Beder, A. & Ergün, E. (2015). Ortaokul öğrencilerinin güvenli internet kullanım durumlarının belirlenmesi. *Eğitim Bilimleri ve Uygulama*, 14(27), 23-41.

- Bilgi Teknolojileri ve İletişim Kurumu (2020). İnternet Bilgi İhbar Merkezi.  
<https://www.ihbarweb.org.tr/> tarihinden sayfasından erişilmiştir.
- Bilgisayar Virüsleri ve Kötü Amaçlı Yazılımlarla İlgili Bilgiler ve SSS (t.y.).  
<https://www.kaspersky.com.tr/resource-center/threats/computer-viruses-and-malware-facts-and-faqs> sayfasından erişilmiştir.
- Bostan, A. ve Şengül, G. (2018). Siber Güvenlik Farkındalığı Oluşturma. Ş. Sağıroğlu ve M. Alkan (Ed.), *Siber Güç ve Savunma Farkındalık ve Caydırıcılık* (s.143-161). Ankara:Grafiker.
- Boyd, D.M., Ellison N.B. (2007). Social network sites: definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1), 210–230.  
<https://doi.org/10.1111/j.1083-6101.2007.00393.x>
- Brackett, M. (2013). Data Topics. The Data – Information - Knowledge Cycle.  
<https://www.dataversity.net/the-data-information-knowledge-cycle/> adresinden erişilmiştir.
- Canbek, G. (2005). *Klavye dinleme ve önleme sistemleri analiz tasarım ve geliştirme*. Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.
- Canbek, G. ve Sağıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. *Politeknik Dergisi*, 9(3), 165-174.
- Canbek, G. ve Sağıroğlu, Ş. (2007a). Bilgisayar sistemlerine yapılan saldırılar ve türleri: bir inceleme. *Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 23 (1-2), 1-12.
- Canbek, G. ve Sağıroğlu, Ş. (2007b). Kötücül ve casus yazılımlar: Kapsamlı bir araştırma. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, 22(1), 121-136.
- Canbek, G. ve Sağıroğlu, Ş. (2007c). çocukların ve gençlerin bilgisayar ve internet güvenliği. *Politeknik Dergisi*, 10(1), 33-39
- Canbek, G. ve Sağıroğlu, Ş. (2008). Casus yazılımlar: Bulaşma yöntemleri ve önlemler. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, 23(1), 165-180.
- Casus Yazılım Nedir? (t.y.). <https://www.kaspersky.com.tr/resource-center/threats/spyware> sayfasından erişilmiştir.
- Castiglione, A., De Prisco, R., De Santis, A. (2009). Do you trust your phone?. *Lecture Notes in Computer Science LNCS 5692*, 50–61.

- Cole, D. A. (1987). Utility of confirmatory factor analysis in test validation research. *Journal of Consulting and Clinical Psychology*, 55, 1019-1031.
- Çalık, T. ve Sezgin, F. (2005). Küreselleşme, bilgi toplumu ve eğitim. *Kastamonu Eğitim Dergisi*, 13(1), 55-66.
- Çokluk, Ö., Şekercioğlu, G. ve Büyüköztürk, Ş. (2012). *Sosyal bilimler için çok değişkenli istatistik SPSS ve LISREL uygulamaları*. Ankara: Pegem.
- Dama, M. (2014). *Windows fonksiyonları kullanılarak özgün bir casus yazılım tasarımı ve alınabilecek önlemler*. Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü, Ankara.
- Dedeoğlu, G. (2009). *Etik ve Bilişim*. İzmir (2009): Etki.
- Deren, A. S. (2006). *Sanal ortamda kültürel miras enformasyon sistemlerinin kurulması ve Türkiye için durum analizi*. Yayınlanmamış yüksek lisans tezi. İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.
- Derin, M. A. ve Gençoğlu, M. T. (2020). Ortaokul öğrencilerinin bilgi güvenliği farkındalığı. *Savunma Bilimleri Dergisi* 38, 159-181.
- Doğan, O. ve Aşan, H. (2016). Bireylerin şifre yapılarına yönelik bir araştırma ve şifre öneri sistemi. *Yönetim Bilişim Sistemleri Dergisi*, 1(3), 192-201.
- Dönmez, G. (2019). *Lise öğrencilerinin bilgi güvenliği farkındalığı ile dijital okuryazarlığı arasındaki ilişkinin incelenmesi*. Yüksek Lisans Tezi, Hacettepe Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.
- Ebeveyn Denetim Araçları (2017). <https://www.guvenliweb.org.tr/dokuman-detay/ebeveyn-denetim-araclari> sayfasından erişilmiştir.
- Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook “friends:” Social capital and college students’ use of online social network sites. *Journal of Computer-Mediated Communication*, 12(4).
- 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

- Emm, D. (2008) *Changing threats, changing solutions: A history of viruses and antivirus*.  
<https://securelist.com/changing-threats-changing-solutions-a-history-of-viruses-and-antivirus/36202/> sayfasından alınmıştır.
- Erdemir, A. (2018). Advances impacting reputation. A.Erdemir (Ed.), *Reputation Management Techniques in Public Relations* (s. 368-369). United States of Amerika: IGI Global.
- Erdoğan, G. ve Bahtiyar, Ş. (Şubat, 2014). Sosyal ağlarda güvenlik. *XVI. Akademik Bilişim Konferansı Bildirileri, Mersin Üniversitesi*, 267-272.
- Erdoğan, A. (2017). *Üniversite öğrencilerinin bilgi güvenliği kazanımlarının, farkındalıkları üzerindeki etkilerinin analizi: Afyon Kocatepe Üniversitesi Örneği*. Yüksek Lisans Tezi, Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü, Afyon.
- Erol, S.E. ve Sağiroğlu, S. (2018). Siber güvenlik farkındalığı, farkındalık ölçüm yöntem ve modelleri. Ş. Sağiroğlu ve M. Alkan (Ed.), *Siber Güç ve Savunma Farkındalık ve Caydırıcılık* (s.105-141). Ankara:Grafiker.
- Fındıkçı, İ. (1998). Enformasyon bilgi toplumu dünyası; Bilgi toplumunda eğitim ve öğretmen. *Bilgi ve Toplum Dergisi*. Nisan, 1998.
- Field, A. (2009). *Discovering statistics using SPSS for windows*, Dubai: Sage.
- Gökçe Arslan, Ş. & Seferoğlu, S.S. (2016). Ortaokul öğrencilerinin internet kullanım biçimleri: Riskli davranışlar ve fırsatlar. *Kastamonu Eğitim Dergisi*, 24(1), 383-404.
- Gökçe Arslan, Ş., Günbatar, M. S. ve Sarıtepeci, M. (2021). Ortaöğretim öğrencilerinin bilgi güvenliği farkındalığı düzeylerinin belirlenmesi. *YYÜ Eğitim Fakültesi Dergisi*, 18(1), 354-373.
- Gökmen, Ö.F. & Akgün, Ö.E. (2014). Bilgisayar ve öğretim teknolojileri eğitimi öğretmen adaylarının bilişim güvenliği bilgilerinin çeşitli değişkenlere göre incelenmesi. *Çukurova Üniversitesi Eğitim Fakültesi Dergisi*, 44(1), 61-84.
- Gökmen, Ö.F. & Akgün, Ö.E. (2016). Öğretmen adaylarının bilişim suçlarına yönelik deneyimleri ve bilişim güvenliği ders içeriğine yönelik görüşleri. *Mustafa Kemal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 13(33), 178-193.
- Guttman, E., Leong, L., & Malkin, G. (1999). *Request for comments: 2504, Users' Security Handbook*, ISOC, RFC 2504, 34

- Güldüren, C. (2015). *Yükseköğretim kurumlarındaki öğretim elemanlarının bilgi güvenliği farkındalık düzeylerinin değerlendirilmesi*. Doktora Tezi, Ankara Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.
- Güldüren, C., Çetinkaya, L. & Keser, H. (2016). Ortaöğretim öğrencilerine yönelik bilgi güvenliği farkındalık ölçeği geliştirme (BGFÖ) çalışması. *Elementary Education Online*, 15(2), 682-695.
- Gündoğan, A. (2020). *Rootkit nedir?*. <https://www.technopat.net/2020/07/25/rootkit-nedir/sayfasından-erişilmiştir>.
- Güvenlik (t.y.). <https://www.turkcebilgi.com/g%C3%BCvenlik#post> adresinden erişilmiştir.
- Hacımustafaoğlu, R. (2019). *Ortaöğretim öğrencilerinin bilgi güvenliği farkındalık düzeylerinin siber mağdur olma durumlarına etkisinin incelenmesi (Üsküdar Örneği)*. Yüksek Lisans Tezi, Sakarya Üniversitesi Eğitim Bilimleri Enstitüsü, Sakarya.
- Haddon, L.ve Livingstone, S. (2012). EU kids online: National perspectives. <http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/PerspectivesReport.pdf>.
- Harl, G. (1997). *People hacking: The psychology of social engineering*. Talk at Access All Areas III Conference, Mayıs 1997. <http://www.genocide2600.com/~tattooman/social-engineering/aaatalk.html> sayfasından erişilmiştir.
- He, D., Chan, S. and Guizani, M. (2015). Mobile application security: malware threats and defenses. *IEEE Wireless Communications*, 22(1), 138-144, February 2015. doi: 10.1109/MWC.2015.7054729
- Heiser, J. G. (2004). Understanding Today's Malware. *Information Security Technical Report*, 9(2), 47-64, April-June 2004.
- How Trojans manipulate Google Play (2016). <https://securelist.com/how-trojans-manipulate-google-play/75894/> sayfasından erişilmiştir.

- Huang, I., Guo, R., Xie, H. ve Wu, Z. (2012). *The Convergence of Information and Communication Technologies Gains Momentum*, The Global Information Technology Report 2012, World Economic Forum, INSEAD. Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.357.1969&rep=rep1&type=pdf>
- Huang, D.L., Rau, P.P. ve Salvendy, G. (2010). Perception of information security. *Behaviour & Information Technology*, 29(3), 221-232.
- ISO International Organization for Standardization. (2005). ISO/IEC 27001:2005
- İnternet Bankacılığı ve Çevrimiçi Alışveriş (2017). <https://www.guvenliweb.org.tr/dokuman-detay/internet-bankaciligi-cevrimici-alisveris-sayfasindan-erisilmistir>.
- İnternette Güvenli Bir Alışveriş Yapmanın Püf Noktaları Neler? (2019). <https://www.isbank.com.tr/blog/internette-guvenli-bir-alisveris-yapmanin-puf-noktalari-neler-sayfasindan-erisilmistir>.
- İnternette güvenli alışveriş için 9 kural. (2020, Nisan 3). *Hürriyet*. <https://www.hurriyet.com.tr/ekonomi/internette-guvenli-alisveris-icin-9-kural-41485235-adresinden-erisilmistir>.
- İşletim Sistemi (2020). [https://tr.wikipedia.org/wiki/%C4%B0%C5%9Fletim\\_sistemi](https://tr.wikipedia.org/wiki/%C4%B0%C5%9Fletim_sistemi) adresinden erişilmiştir.
- Jöreskog, K.G., & Sörbom, D. (1993). *LISREL 8: Structural equation modeling with the SIMPLIS command language*. New Jersey: Lawrence Erlbaum.
- Kapanoğlu, G. (2016). *Öğretmenlerin bilgi güvenliği farkındalığının incelenmesi*. Yüksek Lisans Tezi, Gazi Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.
- Karalar, H., & Sarı, Y. (2007, Ocak). *Bilgi teknolojileri eğitiminde BDÖ yazılımı kullanma ve uygulama sonuçlarına yönelik bir çalışma*. Akademik Bilişim 2007 Konferansı'nda sunulan bildiri, Kütahya.
- Karaoğlu Yılmaz, F. G. ve Çavuş Ezin, Ç. (2017). Ebeveynlerin bilgi güvenliği farkındalıklarının incelenmesi. *Eğitim Teknolojisi Kuram ve Uygulama Dergisi*, 7 (2), 41-57.
- Karasar, N. (2012). *Bilimsel Araştırma Yöntemi*. Ankara: Nobel Yayın Dağıtım

- Kelley, J. (2002). *Knowledge nirvana – Achieving The Competitive Advantage Through Enterprise Content Management and Optimizing Team Collaboration*, Xulon Press.
- Keser, H. ve Güldürüen, C. (2015). Bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. *K.Ü. Kastamonu Eğitim Dergisi*, 23(3), 1167-1184.
- Kişisel Verilerin Korunması Kanunu (2016). *T.C. Resmi Gazete*, 29677, 07.04.2016.
- Kline, R. B. (2011). *Principles and practice of structural equation modeling* (3th edition). New York: The Guilford
- Kruger, H. ve Kearney, W.D. (2006). A prototype for assesing information security awareness. *Computer and Security*, 25, 289-296.
- Küzeci, E. (2010). Anayasal bir hak: Kişisel verilerin korunması. *Bilişim Dergisi*, 128, 142-149
- Leech, N.L., Barrett, K.C., & Morgan, G.A. (2005). *SPSS for intermediate statistics: Use and interpretation*. New Jersey: Lawrence Erlbaum Associates.
- Margaryan, P. (2019). *Troya Savaşı Efsanesi*. <https://arkeofili.com/troya-savasi-efsanesi/sayfasından-erişilmiştir>.
- Marsh, H.W., & Hocevar, D. (1988). A new more powerful approach to multitrait multi method analyses: Application of second-order confirmatory factor analysis. *Journal of Applied Psychology*, 73, 107-117. <http://psycnet.apa.org/index.cfm?fa=buy.optionToBuy&id=1989-07244-001.pdf> sayfasından erişilmiştir.
- Marsh, H.W., Balla, J. R., & McDonald, R. P. (1988). Goodness-of-fit indexes in confirmatory factor analysis: The effect of sample size. *Psychological Bulletin*, 103, 391-410.
- MEB (2021). *Millî Eğitim İstatistikleri, Örgün Eğitim 2022-2021*. T.C. Millî Eğitim Bakanlığı Strateji Geliştirme Başkanlığı, Ankara. [Online]: <http://sgb.meb.gov.tr/www/milli-egitim-istatistikleri-orgun-egitim-2020-2021/icerik/95> adresinden erişilmiştir.
- Mert, M., Bülbül, H.İ. & Sağıroğlu, Ş. (2012). Milli Eğitim Bakanlığına bağlı okullarda güvenli internet kullanımı. *TUBAV Bilim Dergisi*, 5(4), 1-12.

- Microsoft (2021). *Create and Use Strong Passwords*. <https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb> sayfasından erişilmiştir.
- Mitnick, K.D. (2016). *Aldatma Sanatı*. (N. E. Tezcan, Çev.). ODTÜ (Orijinal çalışmanın yayın tarihi 2005).
- Office of Communication (Ofcom) (2008). *Social networking: A quantitative and qualitative research report into attitudes, behaviors and use*. London.
- Online Alışverişte Güvenlik Uyarısı (2019). <https://www.hurriyet.com.tr/ekonomi/online-alisveriste-guvenlik-uyarisi-41398329> adresinden erişilmiştir.
- Öztürk, O. (2002). *Ruh sağlığı ve bozuklukları*. Ankara: Nobel Tıp Kitabevleri.
- Palfrey, J. ve Gasser, U. (2008). *Understanding the first generation of digital natives*. Harvard Press.
- Paşaoğlu, C. ve Vural, Y. (2018). Dünyada ve Türkiye’de kişisel verilerin korunması. Ş. Sağiroğlu ve M. Alkan (Ed.), *Siber Güç ve Savunma Farkındalık ve Caydırıcılık* (s.281-308). Ankara:Grafiker.
- Protect Yourself and Your Data When Using Social Networking Sites (2013). <https://securityinabox.org/en/guide/social-networking/> sayfasından erişilmiştir.
- Puhakainen, P. (2006). *A Design theory for information security awareness*. Master’s thesis, Acta University of Oulu, Faculty of Science Department of Information Processing Science, Oulu. [Online]: <http://herkules oulu.fi> adresinden erişilmiştir.
- Rençber, Ö.F. & Mete, S. (2016). Bilgi güvenlik farkındalığını etkileyen faktörlerin belirlenmesi: yüksekokul öğrencileri üzerine bir inceleme. *Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 18(3), 800-823.
- Risk Steering Committee (2010). DHS Risk Lexicon, U.S. Department Of Homeland Security. <https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf> sayfasından erişilmiştir.

- Rootkits, Part 1 of 3: The Growing Threat (2006). [https://web.archive.org/web/20060823090948/http://www.mcafee.com/us/local\\_content/white\\_papers/threat\\_center/wp\\_akapoor\\_rootkits1\\_en.pdf](https://web.archive.org/web/20060823090948/http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_akapoor_rootkits1_en.pdf). sayfasından erişilmiştir.
- Sah, U.K. and Parmar N. (2017). An approach for malicious spam detection in email with comparison of different classifiers. *International Research Journal of Engineering and Technology (IRJET)*, 4(8), 2238-2242.
- Samet, R. ve Aslan, Ö. (2018). kötü amaçlı yazılımlar ve analizi. Ş. Sağıroğlu ve M. Alkan (Ed.), *Siber Güç ve Savunma Farkındalık ve Caydırıcılık* (s.224-257). Ankara:Grafiker.
- Sümer, N. (2000). Yapısal eşitlik modelleri: Temel kavramlar ve örnek uygulamalar. *Türk Psikoloji Yazıları*, 3(6), 49-74.
- Şenol, A. ve Karacan, H. (2012). *Sazan avlama (phishing): Kullanılan teknikler ve bunlardan korunma yöntemleri*. 5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara.
- Tabachnick, B. G. and Fidell, L. S. (2013). *Using multivariate statistics*. Boston: Pearson.
- Taddicken, M. (2014). The “privacy paradox” in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, 19(2), 248–273.
- Talan,T. ve Aktürk, C. (2021). Ortaöğretim öğrencilerinin dijital okuryazarlık ve bilgi güvenliği farkındalığı seviyelerinin incelenmesi. *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi*, 18(1), 158-180. DOI: 10.33437/ksusbd.668255
- Tavşacı, E. (2014). *Tutumların ölçülmesi ve SPSS ile veri analizi*. Ankara: Nobel.
- Tekin, A. & Polat, E. (2016). Ortaokul öğrenci velilerinin güvenli internet kullanımı farkındalığı. *Journal Of Instructional Technologies & Teacher Education*, 5(2), 80-92.
- The Global State Of Digital In October 2019. <https://wearesocial.com/uk/blog/2019/10/the-global-state-of-digital-in-october-2019> adresinden erişilmiştir.

- Türk Standartları Enstitüsü (TSE), (t.y.). *TS ISO/IEC 27001 Bilgi Güvenlik Yönetim Sistemi*. <https://tse.org.tr/IcerikDetay?ID=2311> sayfasından erişilmiştir.
- Türk Ceza Kanunu (2004). *T.C. Resmi Gazete*, 25611, 12.10.2004.
- Türk Dil Kurumu (TDK), (2011). Bilgi ve Teknoloji. <https://sozluk.gov.tr/> adresinden 14.12.2019 tarihinde erişilmiştir.
- Türk Dil Kurumu (TDK), (2011). Güvenlik. <https://sozluk.gov.tr/> adresinden erişilmiştir.
- Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) - Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM), (2011). [http://www.bilgimikoruyorum.org.tr/?b121\\_bilgi-guvenligi-ne-demektir](http://www.bilgimikoruyorum.org.tr/?b121_bilgi-guvenligi-ne-demektir) adresinden 09.01.2020 tarihinde erişilmiştir.
- Türkiye Cumhuriyeti Anayasası (1982). *T.C. Resmi Gazete*, 17863, 09.11.1982.
- Uçar, O. (2016). *Siber dünyada modern arka kapılar: bilgi güvenliği akademisi, Netsec Etkinliği*, İstanbul. <https://www.bgasecurity.com/makale/siber-dunyada-modern-arka-kapilar/> adresinden erişilmiştir.
- Ulsamer, P., Schutz, A. E., Fertig, T. and Keller, L. (2021). *Immersive storytelling for information security awareness training in virtual reality*. Proceedings of the 54th Hawaii International Conference on System Sciences, URI: <https://hdl.handle.net/10125/71482>
- Ünal, A.N. & Ergen, A. (2018). Siber uzayda yeterince güvelli davranıyor muyuz? İstanbul ilinde yürütülen nicel bir araştırma. *MCBÜ Sosyal Bilimler Dergisi*, 16(2), 191-216.
- Vilander, J. (2021). *Bridging the knowing-doing gap: The role of attitude in information security awareness*. University Of Jyväskylä Faculty Of Information Technology
- Vural, Y. ve Sağıroğlu, Ş. (2010). Veritabanı yönetim sistemleri güvenliği: Tehditler ve korunma yöntemleri, *Politeknik Dergisi*, 13(2), 71-81.
- Wood, W., Quinn, J. M., & Kashy, D. A. (2002). Habits in everyday life: Thought, emotion, and action. *Journal of personality and social psychology*, 83, 1281.
- Yang C. C., Ng T. D. (2007). Terrorism and crime related weblog social network: link, content analysis and information visualization. *IEEE International Conference on Intelligence and Security Informatics, ISI* . DOI: 10.1109/ISI.2007.379533

- Yavanoğlu, U., Sağıroğlu, Ş. ve Çolak, İ. (2012). Sosyal ağlarda bilgi güvenliği tehditleri ve alınması gereken önlemler. *Politeknik Dergisi*, 15(1), 15-27.
- Yemleme (2020). <https://tr.wikipedia.org/wiki/Yemleme> adresinden erişilmiştir.
- Yılmaz, R., Karaoğlu Yılmaz F.G., Öztürk, H.T. & Karademir T. (2017). Lise öğrencilerinin güvenli bilgisayar ve internet kullanım farkındalıklarının incelenmesi: Bartın ili örneği. *Pegem Eğitim ve Öğretim Dergisi*, 7(1), 83-114.
- Yılmaz, E., Şahin, Y.L. & Akbulut, Y.(2016). Öğretmenlerin dijital veri güvenliği farkındalığı. *Sakarya University Journal Of Education*, 6(2), 26-45.
- Zeydan, Ö. (2006). *Kişisel bilgisayarlar ve internet güvenliği*. XI. Türkiye'de İnternet Konferansı'nda sunulmuş bildiri, TOBB Ekonomi ve Teknoloji Üniversitesi, Ankara
- Zhou, Y. and Jiang, X. (2012). Dissecting android malware: Characterization and evolution. *Security and Privacy (SP)*, 95-109.

## **EKLER**



## EK.1. Kişisel Bilgiler Formu

### 1. Cinsiyetiniz:

- 1) Kız ( )
- 2) Erkek ( )

### 2. Sınıf Düzeyiniz:

- 1) 7.Sınıf ( )
- 2) 8.Sınıf ( )

### 3. Babanın Öğrenim Durumu:

- 1) Okur – Yazar Değil ( )
- 2) İlkokul Mezunu ( )
- 3) Ortaokul Mezunu ( )
- 4) Lise Mezunu ( )
- 5) Yüksek Okul / Üniversite Mezunu ( )
- 6) Lisans Üstü Eğitim Mezunu (Yüksek Lisans / Doktora) ( )

### 4. Annenin Öğrenim Durumu:

- 1) Okur – Yazar Değil ( )
- 2) İlkokul Mezunu ( )
- 3) Ortaokul Mezunu ( )
- 4) Lise Mezunu ( )
- 5) Yüksek Okul / Üniversite Mezunu ( )
- 6) Lisans Üstü Eğitim Mezunu (Yüksek Lisans / Doktora) ( )

### 5. İnternet veya İnternetin Kullanıldığı Uygulamalara Günlük Ayrılan Süre:

- 1) 0-1 saat
- 2) 1-3 saat
- 3) 3-5 saat
- 4) 5 saat ve üstü

## EK.2. Bilgi Güvenliği Farkındalık Ölçeği

| Aşağıda bilgi güvenliği farkındalığına yönelik görüşlerinizi tanımlayan 36 madde bulunmaktadır. Aşağıdaki ifadelere ne derece katılıp-katılmadığınızı seçeneğin altındaki kutuya (X) işareti koyarak belirtiniz. Lütfen her soruyu dikkatli okuyunuz ve boş madde bırakmayınız. | Kesinlikle katılmıyorum | Katılmıyorum | Kısmen katılmıyorum | Katılıyorum | Kesinlikle katılıyorum |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|--------------|---------------------|-------------|------------------------|
| 1. Bilgi güvenliğinin ne anlama geldiğini biliyorum.                                                                                                                                                                                                                            | 1                       | 2            | 3                   | 4           | 5                      |
| 2. Bilgi güvenliği ile ilgili sorumluluklarımın ne olduğunu biliyorum.                                                                                                                                                                                                          | 1                       | 2            | 3                   | 4           | 5                      |
| 3. Kullandığım bilgi sistemlerinde tanımlanmış olan kuralları nasıl uygulayacağımı biliyorum.                                                                                                                                                                                   | 1                       | 2            | 3                   | 4           | 5                      |
| 4. Yönetim tarafından bilgi güvenliği gereksinimleri ile ilgili yeterince bilgilendirildiğimi düşünüyorum.                                                                                                                                                                      | 1                       | 2            | 3                   | 4           | 5                      |
| 5. Çocukların bilgisayar güvenli kullanmaları için yapılması gerekenleri biliyorum.                                                                                                                                                                                             | 1                       | 2            | 3                   | 4           | 5                      |
| 6. Kişisel verilerimi nasıl korumam gerektiğini biliyorum                                                                                                                                                                                                                       | 1                       | 2            | 3                   | 4           | 5                      |
| 7. Aldatmaca (hoax) nedir biliyorum.                                                                                                                                                                                                                                            | 1                       | 2            | 3                   | 4           | 5                      |
| 8. Zincir e-postalara (chain e-mail) karşı nasıl hareket etmem gerektiğini biliyorum.                                                                                                                                                                                           | 1                       | 2            | 3                   | 4           | 5                      |
| 9. Casus yazılım (spyware) nedir biliyorum.                                                                                                                                                                                                                                     | 1                       | 2            | 3                   | 4           | 5                      |
| 10. Bilgisayarım casus yazılım olup olmadığını anlayabilirim.                                                                                                                                                                                                                   | 1                       | 2            | 3                   | 4           | 5                      |
| 11. Bilgisayarım casus yazılım yüklenmesinin engelleme yöntemlerini biliyorum.                                                                                                                                                                                                  | 1                       | 2            | 3                   | 4           | 5                      |
| 12. Kimlik hırsızlığı (identity theft) nedir biliyorum.                                                                                                                                                                                                                         | 1                       | 2            | 3                   | 4           | 5                      |
| 13. Kimlik hırsızlığına karşı alınması gereken güvenlik tedbirlerini biliyorum.                                                                                                                                                                                                 | 1                       | 2            | 3                   | 4           | 5                      |
| 14. Sahte virüs koruma yazılımının ne olduğunu biliyorum.                                                                                                                                                                                                                       | 1                       | 2            | 3                   | 4           | 5                      |
| 15. Hizmet aksatma (Denial of Service - DoS) saldırısı nedir biliyorum.                                                                                                                                                                                                         | 1                       | 2            | 3                   | 4           | 5                      |
| 16. Kimlik avı (phishing) saldırısı nedir biliyorum.                                                                                                                                                                                                                            | 1                       | 2            | 3                   | 4           | 5                      |
| 17. Sosyal mühendislik (social engineering) saldırısı nedir biliyorum.                                                                                                                                                                                                          | 1                       | 2            | 3                   | 4           | 5                      |
| 18. Sosyal mühendislik saldırısına uğramamak için nasıl hareket etmem gerektiğini biliyorum.                                                                                                                                                                                    | 1                       | 2            | 3                   | 4           | 5                      |
| 19. Siber zorbalık (cyberbullying) nedir biliyorum.                                                                                                                                                                                                                             | 1                       | 2            | 3                   | 4           | 5                      |
| 20. Siber zorbalığa karşı kendimi nasıl koruyacağımı biliyorum.                                                                                                                                                                                                                 | 1                       | 2            | 3                   | 4           | 5                      |
| 21. Siber zorbalığa karşı çocukları nasıl koruyacağımı biliyorum.                                                                                                                                                                                                               | 1                       | 2            | 3                   | 4           | 5                      |
| 22. Dijital imza (digital signature) nedir biliyorum.                                                                                                                                                                                                                           | 1                       | 2            | 3                   | 4           | 5                      |
| 23. Web sayfalarında kullanılan çerezlerin (cookies) ne işe yaradığını biliyorum.                                                                                                                                                                                               | 1                       | 2            | 3                   | 4           | 5                      |
| 24. Web Sitesi sertifikasının (web site certificate) ne işe yaradığını biliyorum.                                                                                                                                                                                               | 1                       | 2            | 3                   | 4           | 5                      |
| 25. Son kullanıcı lisans sözleşmesi (end-user license agreement) nedir biliyorum.                                                                                                                                                                                               | 1                       | 2            | 3                   | 4           | 5                      |
| 26. Şüpheli veya bilinmeyen kaynaklardan gelen özellikle eklentisi olan e-postaları açmanın taşıdığı riski biliyorum.                                                                                                                                                           | 1                       | 2            | 3                   | 4           | 5                      |
| 27. Sosyal ağ sitelerini (social networking sites) güvenli olarak nasıl kullanacağımı                                                                                                                                                                                           | 1                       | 2            | 3                   | 4           | 5                      |

|     |                                                                                                                                     |   |   |   |   |   |
|-----|-------------------------------------------------------------------------------------------------------------------------------------|---|---|---|---|---|
|     | biliyorum.                                                                                                                          |   |   |   |   |   |
| 28. | USB sürücülerini (USB drives) kullanırken dikkat edilmesi gereken hususları biliyorum.                                              | 1 | 2 | 3 | 4 | 5 |
| 29. | Taşınabilir cihazlara (portable devices) yönelik fiziksel güvenliği sağlamak ile ilgili dikkat edilmesi gereken konuları biliyorum. | 1 | 2 | 3 | 4 | 5 |
| 30. | Taşınabilir cihazlara yönelik veri güvenliği ile ilgili dikkat edilmesi gereken konuları biliyorum.                                 | 1 | 2 | 3 | 4 | 5 |
| 31. | Kişisel mahremiyet nedir biliyorum.                                                                                                 | 1 | 2 | 3 | 4 | 5 |
| 32. | Bilgi güvenliği konusunda yasal sorumluluklarımı biliyorum.                                                                         | 1 | 2 | 3 | 4 | 5 |
| 33. | İnternette gezinirken mahremiyetimi korumak için alınması gereken tedbirleri biliyorum.                                             | 1 | 2 | 3 | 4 | 5 |
| 34. | İnternette gezinirken hakkımda toplanan bilgi miktarının nasıl sınırlandırılacağını biliyorum.                                      | 1 | 2 | 3 | 4 | 5 |
| 35. | Şifre kullanımına ilave olarak alınması gereken tedbirlerin neler olduğunu biliyorum.                                               | 1 | 2 | 3 | 4 | 5 |
| 36. | Çevrimiçi güvenli alışveriş yapmak için gerekli olan güvenlik tedbirlerini biliyorum.                                               | 1 | 2 | 3 | 4 | 5 |

### Ek.3. Bilgi Güvenliği Farkındalık Ölçeği Kullanım İzni

Re: Bilgi Güvenliği Farkındalık Ölçeği İzni

Gelen Kutusu x

**Can GÜLDÜREN**  
Alıcı: ben ▾

30 Ara 2019 Pzt 18:44 (12 gün önce) ☆ ↩ ⋮

Başak selam,

**Ölçek Açıklamaları:**  
Ölçek 14-18 yaş arası Lise (K12) öğrencileri üzerinde geliştirilmiştir. Ölçekte ters kodlanmış madde yoktur. Ölçek toplam puanı ve alt faktörlere ilişkin puanlar attıkça, katılımcıların Bilgi Güvenliği Farkındalığı artmaktadır.

**Bilgi Güvenliği Ölçek Faktör Yapısı:** Kişisel Verilerin Korunması: 1-6, Saldırı ve Tehditler: 7- 25, Mahremiyet: 26-36

Kolay gelsin.  
İyi çalışmalar....

\*\*\*\*\*

Can GÜLDÜREN  
Dr.Öğr.Üyesi  
Bilgisayar Teknolojileri Bölümü  
Ofis :  
Ufuk Üniversitesi, İncek, Ankara, Türkiye

On Monday, December 30, 2019, 04:24:24 PM GMT+3, Başak Özen < > wrote:

#### **Ek.4. CV**

#### **KİŞİSEL BİLGİLER**

**Adı Soyadı** : Başak ÖZEN SERTER

#### **EĞİTİM DURUMU:**

**Yüksek Lisans** : Gazi Üniversitesi  
Eğitim Bilimleri Enstitüsü Eğitim Teknolojileri Bilim Dalı Tezli Yüksek Lisans,  
Ağustos 2021

**Lisans** : Gazi Üniversitesi  
Eğitim Fakültesi İlköğretim Matematik Öğretmenliği Bölümü, Haziran 2009  
Mezuniyet Derecesi : 80,4 / 100  
Yan alan: Fen Bilgisi Öğretmenliği

**Lise :** Ayrancı Lisesi ( Y.D.A.L ), Haziran 2005  
Bölümü: Fen Bilimleri  
Mezuniyet Derecesi : 4,90 / 5

**İlköğretim :** Çankaya Hamdullah Suphi İ.Ö.O., Haziran 2001  
Mezuniyet Derecesi : 5,00 / 5

#### **İŞ İLE İLGİLİ BECERİLER:**

#### **KATILDIĞI KONFERANS, EĞİTİM ve SEMİNERLER**

1. SEBİT-EĞİTSEL SENARYO ÜRETİMİ KURSU (5-16 Aralık 2016)

2. **ÖZEL YETENEKLİLERDE DESTEK EĞİTİM ODASI EĞİTİCİ EĞİTİMİ KURSU (11-15 Nisan 2016)**
3. **EĞİTİMDE YARATICI DRAMA KURSU (7-28 Mayıs 2014)**
4. **EĞİTİM REFORMU GİRİŞİMİ Bünyesinde Katıldığı EĞİTİMDE İYİ ÖRNEKLER KONFERANSI 2012’da Aldığı Seminerler:**
  - **Eleştirel Düşünme**
    - İlköğretimde Geometri Öğretiminde Teknoloji Kullanımı ve Geogebra Uygulamaları (6.-8.Sınıflar)
    - Voleybol Problemi:Model Oluşturma Etkinliklerinin Matematik Öğretiminde Kullanılması(6.-8.Sınıflar)
    - Pinpon Toplarıyla Matematik Öğreniyorum (1.-5.Sınıflar)
    - Küçük Adımlar, Büyük Çözümler: Karbon Ayak İzimi Hesaplıyorum - Gezeganimizi Koruyorum(6.-8.Sınıflar)
    - Harriet Tubman, Sokrates, Annem ve Ben (1.-5.Sınıflar)
  - **Kaynaştırma ve Özel Eğitim**
    - Paralimpik Okul Günleri
5. **LİDERLİK OKULU Bünyesinde Katıldığı Seminerler(2011):**
  - **Liderlik ve Takım Çalışması**
  - **Kriz Yönetimi**
  - **Proje Yönetimi**
6. **ODTÜ İŞLETME TOPLULUĞU Tarafından Düzenlenen FİNANS KONGRESİ(2010) Kapsamında Katıldığı Seminerler:**
  - **Sıcak Para Hareketleri, Sabah Gazetesi Ekonomi Yazarı Meliha OKUR**
  - **BDDKnın ve Türk Bankacılık Sektörünün Gelişimi, Uluslararası Finansal Krizin Nedenlerine İlişkin Değerlendirme, BDDK Başkan Yardımcısı İhsan Uğur DELİKANLI**
7. **EĞİTİM REFORMU GİRİŞİMİ Bünyesinde Katıldığı EĞİTİMDE İYİ ÖRNEKLER KONFERANSI 2010’da Aldığı Seminerler:**
  - **Eğitimde Katılımcı İşbirliği**
    - Bileşik Makine Tasarlıyorum
    - İlköğretim Öğrencilerinin Geometri ile İlgili Anlamlarının İncelenmesi
    - Koşarak Öğreniyorum
  - **Ölçme ve Değerlendirme**

- **Portfolyo Ağı**
- **Stajyer Öğretmenlerin Oryantasyonunda Okul Müdürlerinin Sorumluluklarına Yönelik Öğretmen Görüşleri**, Prof.Dr. Ayşen Bakioğlu-Marmara Üniversitesi
- **Öğrenme-Öğretme Etkinlikleri**
  - **Matematik ve Müzik (6.-8. Sınıflar)**
  - **Resim Perspektifinden Matematiğe Bakış (6.-8. Sınıflar)**
  - **Akyaka Doğa Bilim Kampı (6.-8. Sınıflar)**
  - **Akran Eğitim Modeli il Matematiğin Eğlenceli Yüzü (Ortaöğretim)**
  - **23 Periwood, 23 Fırça (Ortaöğretim)**

**8. ODTÜ İŞLETME TOPLULUĞU Tarafından Düzenlenen LEADERS@METU 2010 Kapsamında:**

- **Liderlik Semineri**, Reckitt Benckiser Türkiye Başkanı Caner TUNAMAN
- **Liderlik Eğitimi**, Furla Eğitim, Yönetim Danışmanlığı ve Organizasyon Kurucusu – Başdanışmanı Semen ÖNER

**9. ODTÜ İŞLETME TOPLULUĞU Tarafından Düzenlenen FİNANS KONGRESİ(2009) Kapsamında Katıldığı Seminerler:**

- **Finansal Krizin Olumsuz Etkilerine Türkiye Neden Yeteri Kadar Ekonomi Politikası Tepkisi Veremedi?**, TOBB Üniversitesi Öğretim Üyesi ve Radikal Gazetesi Ekonomi Yazarı Fatih ÖZATAY
- **Kriz Ortamlarında Finansal Yöneticilerinin Değişen Rolü**, Philip MorrisSA A.Ş. Finans, Bilişim Hizmetleri ve İdari İşler Direktörü Taner KERMAN

**SERTİFİKALAR:**

- 9.EĞİTİMDE İYİ ÖRNEKLER KONFERANSI 2012 (31 Mart 2012)
- LİDERLİK OKULU, LİDERLİK VE TAKIM ÇALIŞMASI KATILIM SERTİFİKASI (15 Ocak 2011-15 Şubat 2011)
- LİDERLİK OKULU, KRİZ YÖNETİMİ KATILIM SERTİFİKASI (15 Ocak 2011-15 Şubat 2011)
- LİDERLİK OKULU, PROJE YÖNETİMİ KATILIM SERTİFİKASI (15 Ocak 2011-15 Şubat 2011)
- ODTÜ İŞLETME TOPLULUĞU FİNANS KONGRESİ (15-16-17 Aralık 2010)
- 7.EĞİTİMDE İYİ ÖRNEKLER KONFERANSI 2010 (17-18 Nisan 2010)
- ODTÜ İŞLETME TOPLULUĞU LEADERS@METU 2010 ( 4-5-6 Ocak 2010 )
- ODTÜ İŞLETME TOPLULUĞU FİNANS KONGRESİ ( 16-17-18 Aralık 2009 )

- MEB ONAYLI BILGISAYAR İŞLETMENLİĞİ SERTİFİKASI (60 saat teorik + 100 saat uygulama)

#### **KATILIM BELGELERİ:**

- **ODTÜ İşletme Topluluğu Finans Kongresi Katılım Belgesi 1**  
Sıcak Para Hareketleri, Sabah Gazetesi Ekonomi Yazarı Meliha OKUR
- **ODTÜ İşletme Topluluğu Finans Kongresi Katılım Belgesi 1**  
BDDKnın ve Türk Bankacılık Sektörünün Gelişimi, Uluslararası Finansal Krizin Nedenlerine İlişkin Değerlendirme, BDDK Başkan Yardımcısı İhsan Uğur DELİKANLI
- **ODTÜ İşletme Topluluğu Leaders@METU 2010 Katılım Belgesi 1**  
Liderlik Semineri, Reckitt Benckiser Türkiye Başkanı Caner TUNAMAN
- **ODTÜ İşletme Topluluğu Leaders@METU 2010 Katılım Belgesi 2**  
Liderlik Eğitimi, Furla Eğitim, Yönetim Danışmanlığı ve Organizasyon Kurucusu - Başdanışmanı Semen ÖNER
- **ODTÜ İşletme Topluluğu Finans Kongresi Katılım Belgesi 1**  
Finansal Krizin Olumsuz Etkilerine Türkiye Neden Yeteri Kadar Ekonomi Politikası Tepkisi Veremedi?, TOBB Üniversitesi Öğretim Üyesi ve Radikal Gazetesi Ekonomi Yazarı Fatih ÖZATAY
- **ODTÜ İşletme Topluluğu Finans Kongresi Katılım Belgesi 2**  
Kriz Ortamlarında Finansal Yöneticilerinin Değişen Rolü, Philip Morris A.Ş. Finans, Bilişim Hizmetleri ve İdari İşler Direktörü Taner KERMAN

#### **İŞ DENEYİMLERİ:**

1. **Sincan Yıldırım Beyazıt Ortaokulu / Sincan, ANKARA**  
Ocak 2020 - Halen
2. **Sincan İMKB Ortaokulu / Sincan, ANKARA**  
Ocak 2015 – Ocak 2020
3. **İBB.Abdüleziz Paşa Ortaokulu / Silivri, İSTANBUL**  
Ocak 2014 – Ocak 2015
4. **Gazi İlkokulu / Silivri, İSTANBUL**  
Eylül 2012 – Ocak 2014

**5. İl Genel Meclisi İlköğretim Okulu / Çankaya, ANKARA**

Eylül 2011 – Ocak 2012

**6. Sınav Dergisi Dershanesi/Çukurambar Şubesi**

Mart 2008 – Haziran 2008

**YAYINLAR:**

Özen Serter, B. ve Çetin, Ş. (2021). Ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeyinin incelenmesi. Gazi Üniversitesi Genç Araştırmacılar Kongresi'nde sözlü bildiri, 28-30 Haziran 2021, Ankara.





*GAZİLİ OLMAK AYRICALIKTIR...*