T.C.

BARTIN ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

BİLİŞİM SİSTEMLERİ VE TEKNOLOJİLERİ ANABİLİM DALI

YÜKSEK LİSANS TEZİ

ORTAOKUL ÖĞRENCİLERİNİN BİLGİ GÜVENLİĞİ VE ETİK FARKINDALIĞI

AHMET YILMAZ

DANIŞMAN

DR. ÖĞR. ÜYESİ AHMET BERK ÜSTÜN

BARTIN-2023

T.C.
BARTIN ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
BİLİŞİM SİSTEMLERİ VE TEKNOLOJİLERİ ANABİLİM DALI

ORTAOKUL ÖĞRENCİLERİNİN BİLGİ GÜVENLİĞİ VE ETİK FARKINDALIĞI

YÜKSEK LİSANS TEZİ

AHMET YILMAZ

BARTIN-2023

KABUL VE ONAY

BEYANNAME

Bartın Üniversitesi Lisansüstü Eğitim Enstitüsü tez yazım kılavuzuna göre Dr. Öğr. Üyesi Ahmet Berk ÜSTÜN danışmanlığında hazırlamış olduğum "ORTAOKUL ÖĞRENCİLERİNİN BİLGİ GÜVENLİĞİ VE ETİK FARKINDALIĞI" başlıklı yüksek lisans tezimin bilimsel etik değerlere ve kurallara uygun, özgün bir çalışma olduğunu, aksinin tespit edilmesi halinde her türlü yasal yaptırımı kabul edeceğimi beyan ederim.

15.08.2023

Ahmet YILMAZ

ÖNSÖZ

Manevi desteklerini üzerimde hissettiğim ve çalışmalarım esnasında bana en büyük desteği sağlayan en başta kızıma ve eşime olmak üzere, başarılı olmama inanan aileme teşekkür ederim.

Tez çalışmamın başından sonuna kadar geçen her aşamadaki katkılarından dolayı danışmanım Dr. Öğr. Üyesi Ahmet Berk ÜSTÜN'e teşekkür ederim. Sağladığı önemli katkılarından dolayı Doç. Dr. Fatma Gizem KARAOĞLAN YILMAZ'a ve Doç. Dr. Ramazan YILMAZ hocalarıma teşekkür ederim. Yüksek lisans eğitimi almama imkân sağlayan Bartın Üniversitesi, Bartın Üniversitesi Lisansüstü Eğitim Enstitüsü'ne ve tez çalışmam için gerekli izinleri sağlayan Bartın İl Milli Eğitim Müdürlüğü'ne teşekkürlerimi sunarım. Ayrıca tez çalışmamın uygulama aşamasında gerekli verilerin toplanabilmesi için gönüllü katılım sağlayan öğrencilerin hepsine gönülden teşekkür ederim…

Ahmet YILMAZ

ÖZET

Yüksek Lisans Tezi

ORTAOKUL ÖĞRENCİLERİNİN BİLGİ GÜVENLİĞİ VE ETİK FARKINDALIĞI

Ahmet YILMAZ

Bartın Üniversitesi
Lisansüstü Eğitim Enstitüsü
Bilişim Sistemleri ve Teknolojileri Anabilim Dalı

Tez Danışmanı: Dr. Öğr. Üyesi Ahmet Berk ÜSTÜN

Bartın-2023, sayfa: 65

Ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalığı üzerine yapılan bu araştırmanın amacı ortaokul seviyesinde yer alan öğrencilerin bilgi güvenliği ve etik farkındalıklarının hangi düzeyde olduğunu ortaya çıkarmaktır. Bu amaç doğrultusunda ilk olarak ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalıklarını belirleyebilmek için bir ölçek geliştirilmiştir. İkinci aşamada ise tarama modeli kullanılarak geliştirilen Bilgi Güvenliği ve Etik Farkındalığı Ölçeği (BGEFÖ) kullanılarak ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalık düzeyleri ortaya çıkarılmaya çalışılmıştır.

Bilgi Güvenliği ve Etik Farkındalığı Ölçeği'nin geliştirilmesi için hazırlanan madde havuzu uzman görüşüne sunularak gerekli değerlendirmeler ve düzeltmeler yapılarak uygulama aşamasına geçilmiştir. BGEFÖ, gerekli izinler alındıktan sonra 2022-2023 eğitim-öğretim yılının ikinci döneminde Bartın ilinin Merkez ilçesindeki ortaokullarda okuyan 621 öğrenciye uygulanmıştır. Ölçek geliştirme çalışmasının birinci aşamasında açımlayıcı faktör analizi (AFA) yapılmıştır. Açımlayıcı faktör analizi sonucunda ölçeğin; Kullanıcı Güvenliği, Veri Güvenliği ve Etik olmak üzere üç alt boyut altında ve 17 maddeden oluştuğu belirlenmiştir. Ölçek geliştirme çalışmasının ikinci aşamasında doğrulayıcı faktör analizi (DFA) yapılarak ölçeğin üç faktörlü yapıda olduğu doğrulanmıştır. BGEFÖ için hesaplanan Cronbach Alfa güvenirlik katsayısı .896 olarak bulunmuştur. Bu çalışmanın ölçek geliştirme aşaması sonucunda ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalık düzeylerini

belirlemek için kullanılabilecek geçerli ve güvenilir bir ölçek geliştirilmiştir.
Araştırmanın tarama aşamasında bağımsız değişkenler hakkında bilgi toplayabilmek için araştırmacı tarafından hazırlanan kişisel bilgi formu ve BGEFÖ kullanılmıştır. MEB'den gerekli izinler alınarak, 2022-2023 eğitim öğretim yılının ikinci döneminde Bartın ilinin Merkez ilçesindeki ortaokullarda okuyan 921 öğrenciye kişisel bilgi formu ve ölçek uygulanmıştır. Araştırmada ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalıklarının hangi düzeyde olduğunu belirlemek için ölçeğin faktör puanları ve ölçek toplamına ilişkin betimsel istatistikler hesaplanmıştır. İki grup arasında karşılaştırma yapılırken ilişkisiz örneklemler t-testi, ikiden fazla grubun karşılaştırması yapılırken Tek Yönlü Varyans Analizi (ANOVA) kullanılmıştır.
Ölçek genelinden elde edilen puanlar incelendiğinde ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalıklarının yüksek düzeyde olduğu, kullanıcı güvenliği farkındalığının ve etik farkındalığının yüksek düzeyde olduğu fakat veri güvenliği farkındalığının orta düzeyde olduğu görülmüştür. Ölçeğin tamamından alınan puanlar dikkate alındığında cinsiyete göre anlamlı bir fark ortaya çıkmamıştır. Fakat etik alt boyutu incelendiğinde ise kızların erkeklere oranla farkındalıklarının daha yüksek olduğu sonucuna ulaşılmıştır. Çalışmaya katılan 11, 12, 13 ve 14 yaş grupları kendi aralarında karşılaştırılmış olup farkındalık düzeyi en yüksek 11 yaş grubunda olduğu görülmüştür. Sınıf seviyelerine göre karşılaştırmalar yapıldığında da 5 ve 6. Sınıf öğrencilerinin farkındalıklarının diğer sınıf seviyelerinden daha yüksek olduğu tespit edilmiştir. Anne eğitim düzeyi öğrencilerin kullanıcı güvenliği ve veri güvenliği alt boyutlarını etkilemediği görülmüştür. Anne eğitim düzeyi ile öğrencilerin etik farkındalığı arasında anlamlı bir ilişkinin varlığı tespit edilmiştir. Baba eğitim düzeyi öğrencilerin veri güvenliği alt boyutunu etkilemediği görülmüştür. Baba eğitim düzeyi ile öğrencilerin kullanıcı güvenliği farkındalığı ve etik farkındalığı arasında anlamlı bir ilişkinin varlığı tespit edilmiştir.

Anahtar Kelimeler: Ortaokul, bilgi güvenliği, bilgi güvenliği farkındalığı, etik, etik farkındalığı, ölçek geliştirme.

ABSTRACT

M. Sc. Thesis

MIDDLE SCHOOL STUDENTS' INFORMATION SECURITY AND ETHICAL AWARENESS

Ahmet YILMAZ

Bartın University
Graduate School
Department of Information Systems and Technologies

Thesis Advisor: Asst. Prof. Dr. Ahmet Berk ÜSTÜN
Bartın-2023, pp: 65

The purpose of this research is to reveal the level of middle school students' knowledge security and their ethical awareness. First of all, a scale was developed to determine middle school students' information security and their ethical awareness in line with this purpose. Secondly, the Information Security and Ethical Awareness Scale (ISEAS) was applied to uncover middle school students' information security and their ethical awareness by using a screening model.

The item pool prepared for developing ISEAS was presented to experts for their opinions, and adjustments were made based on expert evaluations before moving on to the implementation phase. After obtaining the permissions, ISEAS was administered to 621 students studying at middle schools in the central district of Bartın province during the second semester of the 2022-2023 academic year.

In the first stage of scale development, exploratory factor analysis (EFA) was conducted. As a result of EFA, the scale was found to consist of three sub-dimensions: User Security, Data Security, and Ethics, comprising a total of 17 items. In the second stage, confirmatory factor analysis (CFA) was performed, confirming that the scale had a three-factor structure. The calculated Cronbach's alpha reliability coefficient for ISEAS was found to be .896. As a result, a valid and reliable scale was developed, and it can be used to determine the level of

information security and ethical awareness among middle school students.

In the screening phase of the research, a personal information form prepared by the researcher and ISEAS were used to gather information about the independent variables. With the permissions obtained from the Ministry of National Education, a personal information form and scale were administered to 921 students studying at middle schools in the central district of Bartın province during the second semester of the 2022-2023 academic year. In the research, descriptive statistics were calculated for the factor scores of the scale and the total scale score to determine the level of middle school students' information security and their ethical awareness. When comparing two groups, independent samples t-test was used, and for the comparison of more than two groups, a One-Way Analysis of Variance (ANOVA) was employed.

When examining the scores obtained from the scale, it was observed that middle school students had a high level of information security and ethical awareness. The scores from sub-dimensions showed middle school students had a high level of user security awareness and ethical awareness but a moderate level of data security awareness. When considering the scores obtained from the entire scale, no significant difference emerged based on gender. However, when the ethical subscale was examined, it was concluded that girls had a higher level of awareness compared to boys. The participating age groups of 11, 12, 13, and 14 years old were compared among themselves, and it was observed that the awareness level was highest in the 11-year-old group. When comparisons were made according to grade levels, it was found that the awareness of 5th and 6th-grade students was higher than students in other grade levels. The mother's education level was observed not to affect the students' user security and data security sub-dimensions. A significant relationship was found between the mother's education level and students' ethical awareness. The father's education level was observed not to affect the students' data security sub-dimension. However, a significant relationship was found between the father's education level and students' user security awareness and ethical awareness.

Keywords: Middle school, information security, information security awareness, ethics, ethical awareness, scale development.

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

Şekil No | **Sayfa No**

TABLOLAR DİZİNİ

Tablo No **Sayfa No**

EKLER DİZİNİ

SİMGELER VE KISALTMALAR DİZİNİ

N	: Örneklem Büyüklüğü
$\overline{X}$	: Toplam Puanların Ortalaması
χ^2	: Ki-kare
df	: Serbestlik derecesi
p	: Anlamlılık
r	: Korelasyon Katsayısı
ss	: Standart Sapma
%	: Yüzde

KISALTMALAR

ANOVA	: Analysis of Variance
AFA	: Açımlayıcı Faktör Analizi
BGEFÖ	: Bilgi Güvenliği ve Etik Farkındalığı Ölçeği
DFA	: Doğrulayıcı Faktör Analizi
MEB	: Milli Eğitim Bakanlığı
NIST	: Ulusal Standartlar ve Teknoloji Enstitüsü
TTKB	: Talim Terbiye Kurulu Başkanlığı
TDK	: Türk Dil Kurumu
SPSS	: Statistical Package For Social Sciences
KG	: Kullanıcı Güvenliği
VG	: Veri Güvenliği
ETK	: Etik

1. GİRİŞ

Bilgi ve iletişim teknolojilerinin gelişimiyle birlikte bilgi birikiminde hızlı bir artış meydana gelmiş ve toplumsal değişime de neden olan bilginin ne kadar önemli olduğunun fark edilmesi zorunluluk olmuştur (Akkoyunlu & Kurbanoğlu, 2003). Bilimsel gelişmelerin hızlı bir biçimde teknolojiye yansıması ve bilgiye erişimin daha kolay olması toplumu oluşturan bireylerin teknoloji ile bilgi arasındaki dengede sağlıklı bir yapı kurmasını gerektirmektedir (Yayla, 2018). Buradan hareketle toplumsal değişim ve gelişimin sağlanabilmesi için bilgiyi oluşturabilen, nasıl paylaşması gerektiğini bilen, yönetimini sağlayabilen ve kullanabilen bireylerin yetiştirilmesi ihtiyacı ortaya çıkmıştır.

Bilginin paylaşımı aşamasında, bize ait olan kişisel ve önemli bilgilerimiz teknolojik aletlerimizde veya bu aletlerde bulunan çeşitli uygulamalar aracılığıyla sanal dünyada kullanıcılar için ayrılmış olan kısmında yer almaktadır (Güldüren, Çetinkaya & Keser, 2016). Gelişen teknoloji ile depolanması kolaylaşan bilgi için güvenlik riskleri de ortaya çıkmıştır (Calder, 2005). Bilginin güvenliğinin sağlanması da üretilmesi ve kullanılması kadar önemli hale gelmektedir. Bu nedenlere bağlı olarak ülkelerin eğitim politikalarını gelişmekte olan çağın ihtiyaçlarına cevap verecek şekilde düzenlemeleri gerekmektedir (Ünal, 2009). Bu durumlar araştırmacıların eğitim süreçlerinde hızlı ve nitelikli öğrenmelerin sağlanabilmesi için yeni yollar bulmaya yönlendirmiştir.

1.1. Bilgi Güvenliği ve Bilgi Güvenliği Farkındalığı

Bilgi güvenliği, bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini korumayı amaç edinen disiplin bütünüdür (Whitman & Mattord, 2016). Bilgi güvenliği bütünlük, erişilebilirlik ve gizlilik olmak üzere üç ana bileşenden meydana gelmektedir. Ayrıca bu bileşenlerden herhangi birinde meydana gelebilecek olumsuzluk güvenlik zafiyetine neden olur (Puhakainen, 2006). Bilgiye izin almadan veya erişim yetkisi olmayanların bilgiye ulaşmasını, değiştirmesini, zarar vermesini, kullanmasını, ifşa etmesini, yok etmesini, kötü niyetli kişilerin eline geçmesini önlemek bilgi güvenliğinin amaçları arasındadır. Bilgi güvenliği; kullanıcıların güçlü şifreler oluşturması, sahte e-postalara karşı dikkatli olması, dosya indirmeleri güvenilir kaynaklardan yapması gibi konularda kullanıcı bilincini arttırmaya yönelik destekleyici önlemler sağlamalıdır (Whitman & Mattord, 2016).

Güldüren (2015)'e göre teknik arızalarla ilgili tehditler veya doğal afetler, insan eliyle

gerçekleşen tehditler, prosedürel eksikliklerle ilgili tehditler ve kötü amaçlı yazılımlarla ilgili tehditler bilgi güvenliğine yönelik tehditler olarak sıralanmaktadır. Wagner ve Brooke (2007) bilgi güvenliğindeki en zayıf halkanın insan faktörü olduğunu ifade etmiştir. Bilgi güvenliği açısından insan faktörü kaynaklı tehditlerin çok önemli bir zafiyet ortaya çıkarması nedeniyle bilgi güvenliğinin sağlanması için bireylere bu yönde eğitimler verilmesi oldukça önemlidir.

Bilgi güvenliği farkındalığı, bireylerin bilgi ve iletişim teknolojileri kullanımında kendilerine ait olan bireysel bilgilerini istenmeyen olumsuz durumlara karşı korumak için gereken güvenlik önlemlerini alma ve tehditler karşısında farkındalık sahibi olma durumudur (Vural & Sağıroğlu, 2008). Bilgi güvenliği farkındalığının yüksek olması, kullanıcıların siber tehditler ve dolandırıcılıklar karşısında daha dikkatli ve bilinçli davranmasına yardımcı olur (Awad & Krishnan, 2006). Aynı zamanda, kurumların da bilgi güvenliği önlemlerini güçlendirmesi ve çalışanlarını bilgi güvenliği konusunda eğitmesi açısından önemlidir.

1.2. Bilgi Güvenliğine Yönelik Tehditler

Günümüzün şekillenmesine ve geleceğin oluşmasına en önemli katkıyı sağlan bilgi faktörünün önemi oldukça büyüktür. Bu kadar büyük önem arz eden bilginin korunması ve doğru şekilde kullanılması da büyük bir sorumluluk ve önem teşkil etmektedir. Hayatımızın eğitim, ticaret, ulaşım, savunma gibi birçok alanındaki var olan bilginin korunması ve doğru yerde ve zamanda kullanılması gerekmektedir. Fakat tüm bunların yanında var olan bilginin de doğru şekilde korunabilmesi yaşanılan önemli problemlerden biridir (Yılmaz, 2015).

Bilgi güvenliğine yönelik tehditler;

- Doğal kaynaklı,
- Prosedür eksikliği kaynaklı,
- İnsan faktörü kaynaklı,
- Zararlı yazılım kaynaklı olabilmektedir (Öztezcan, 2017).

1.2.1 Doğal Kaynaklı Tehditler

Deprem, sel, heyelan, yangın, çığ düşmesi, savaş gibi birçok doğal afetin geçmişte yaşandığı gibi günümüzde de yaşanmaktadır. Bu türden doğal afetler için insanlar ve devletler birtakım

önlemler almaya çalışmakta fakat yine de doğal afetleri durdurmakta yetersiz kalmaktadırlar. Bu nedenle gelecekte de bu türden doğal afetlerin her an gerçekleşebileceği gerçeği unutulmamalıdır.

Doğa kaynaklı afetlerin bilgi kaynaklarına ve depolanma birimlerine zarar verebilme ve çalışmalarına engel olabileceği daima göz önünde bulundurulmalıdır. Doğal afetlerin bilgi güvenliğine tehdit oluşturmasına yönelik risk yönetiminin yapılması elzem bir durumdur. Bilgi ve belgelerin muhafaza edildiği yerlerin riskler açısından değerlendirmelerinin ve analizlerinin gerçekçi senaryolara uygun şekilde yapılması önem arz etmektedir.

1.2.2 Prosedür Eksikliği Kaynaklı Tehditler

Bilginin üretimden depolanmasına ve yeniden kullanılmasına kadar hemen hemen her aşamasında belli yöntem ve teknikler uygulanmaktadır. Bu yöntem ve tekniklerin ne zaman ve hangi şekilde olacağı ise idari ve yönetim kademesi tarafından belirlenmektedir. Bir işin gerçekleştirilmesinde uyulması gereken kurallar ve yöntemler bütününe prosedür denilmektedir.

Prosedür kaynaklı tehditlerle işletmeler genellikle kurumsallaşmayı tam olarak gerçekleştiremediklerinde karşılaşabilmektedirler. Çalışanlarının görev ve yetki tanımlarının tam olmaması ve sınırlarının kesin hatlarla belirlenmemiş olması, görevi kaldıramayacak personele gereğinden fazla sorumluluk ve yetki verilmesi prosedür kaynaklı aksaklıklara neden olabilmektedir. Ayrıca teknik anlamda verilerin uygun şekilde depolanmaması, yedeklenmemesi ve teknolojik alt yapının bakımlarının aksatılması bilgi güvenliğine yönelik tehdit oluşturmaktadır (Vural & Sağıroğlu, 2010).

1.2.3 İnsan Faktörü Kaynaklı Tehditler

İnsan faktörü farklı bir ifadeyle bilgi sistemlerinin kullanıcıları, bilgi güvenliğinin en zayıf halkasını oluşturmaktadır (Maleki, Shahgholian & Lutfi, 2016). Kullanıcıların gereken eğitimi almaması, tedbirli olmaması ve bilgi güvenliğini önemli görmemesi durumunda bilgi güvenliği için zafiyet ve tehditler kaçınılmaz olmaktadır. Bilgi güvenliği ve etik farkındalığı açısından, insan faktörü önemli bir rol oynar. Çünkü teknolojik güvenlik önlemleri ve politikaları ne kadar güçlü olursa olsun, insanlar hala güvenlik açıkları ve siber tehditlerle karşılaşabilirler. Bu nedenle, insanların bilgi güvenliği ve etik konularında bilinçli ve

dikkatli olmaları gerekmektedir (Herath & Rao, 2009). Bilgi güvenliği ve etik konularında insan faktörünün önemi, çalışanların güvenlik politikalarına uygun davranışlar sergilemeleri, gizli bilgileri koruma alışkanlıkları ve siber saldırılara karşı tetikte olmaları açısından büyük bir rol oynar (D'Arcy & Hovav, 2009). Eğitim ve farkındalık programları, insanların bilgi güvenliği ve etik konularında daha bilinçli olmalarını sağlamak için kullanılır. Bu tür programlar, çalışanların siber tehditleri daha iyi anlamalarına ve güvenli davranış alışkanlıkları geliştirmelerine yardımcı olur (Herath & Rao, 2009). Bilişim teknolojilerinde olumlu yöndeki gelişmelerin yanı sıra olumsuz yönde de gelişmeler olduğu söylenebilir. Bu olumsuzlukların temelinde yatan nedenin insanları dolandırmak ve kolay yoldan para kazanmak sebepli olduğu bilinmektedir (Özkan, 2018). Bu nedenle yalan haber yayma, hırsızlık, kredi kartı dolandırıcılığı, fikri mülkiyet hakkının ihlal edilmesi, gizlilik içeren bilgi ve belgelerin sızdırılması gibi suçlar ortaya çıkmıştır (Dedeoğlu, 2009). Doğal afet kaynaklı, teknik alt yapı kaynaklı tehditlere karşı önlemler almak oldukça faydalı olacaktır ancak kullanıcı kaynaklı tehditlerin de göz önünde bulundurulması ve bilgilendirilmesi önem arz etmektedir.

1.2.4 Zararlı Yazılım Kaynaklı Tehditler

Sanal ortam dürüstlükten uzak olan, ahlaki ve etik dışı tutum ve davranışlardan kaçınmayan bireylerinde olduğu bir ortamdır. Kötücül yazılım kaynaklı tehditler kimlik avı, Sazan avlama (phishing), istenmeyen e-posta (spam), arka kapılar (backdoor), sosyal mühendislik, casus yazılımlar (spyware), bilgisayar virüsleri, bilgisayar solucanları (worm), truva atları (trojen horse), kök kullanıcı takımları (rootkit), klavye dinleme sistemleri (keylogger), botnet ağı şeklinde sıralanabilir. Bunların detaylı açıklamalarına bakılacak olunursa:
Kimlik avı, kötü niyetli bireylerin, kullanıcıların kişisel ve finansal bilgilerini ele geçirmek için sahte e-postalar ve mesajlar kullanarak yaptığı bir dolandırıcılık yöntemidir (Anti-Phishing Working Group, 2020). Genellikle dolandırıcılar, gerçek resmi kurumları taklit ederek sahte e-postalarla kullanıcıları kandırmaya çalışır. Bu sahte e-postalarda, kullanıcıların üyelik bilgilerini güncellemeleri veya kişisel bilgilerini doğrulamaları istenebilir (Symantec, 2020). Kimlik avı saldırılarında, dolandırıcılar hedef aldıkları kişilerin e-postalardaki kötü niyetli bağlantılara tıklamasını isterler. Bu bağlantılar, kullanıcıları sahte web sitelerine yönlendirerek kişisel bilgilerini ele geçirmeyi amaçlar (Ferrara vd., 2020). Kimlik avı tehditlerinden korunmak için kullanıcıların, şüpheli e-postaları veya mesajları

dikkatlice incelemeleri ve sadece güvendikleri kaynaklardan gelen mesajları doğrulamaları önemlidir (Cybersecurity and Infrastructure Security Agency, 2020). "Kimlik avı" terimi, çoğu zaman "phishing" terimiyle aynı anlamda kullanılmaktadır. *Sazan Avlama (phishing),* kötü niyetli kişilerin, hedef aldığı kullanıcıların kişisel ve finansal bilgilerini ele geçirmek için sahte e-postalar, mesajlar veya web siteleri kullanarak yaptığı bir dolandırıcılık metodudur (Sheng vd., 2010). Sazan avlama saldırılarında, dolandırıcılar sahte web siteleri yardımıyla hedef kullanıcıların kişisel bilgilerini vermeleri için yönlendirir (Kumaraguru vd., 2008). Gerçek siteleri taklit eden sahte web siteleri, kullanıcıların güvenini kazanmaya çalışır (Dhamija vd., 2006). Bu tür saldırılardan korunmak için, kullanıcıların sahte e-postaları ve mesajları dikkatlice incelemeleri ve sadece güvenilir kaynaklardan gelen istekleri dikkate almaları önemlidir (Anti-Phishing Working Group, 2015). Kullanıcıların, kırılması zor şifreler kullanması, güvenlik yazılımlarını güncellemesi ve güvenli internet bağlantıları kullanması bu tür saldırılardan korunma yöntemlerindendir (National Cyber Security Centre, 2019).

İstenmeyen e-posta (spam), bu sorun, mesajların veya reklamların toplu olarak gönderilmesiyle gerçekleşen bir sorundur (Feng vd., 2004). Spam göndericileri, genellikle kişisel bilgileri toplamak, dolandırıcılık yapmak veya virüs yaymak gibi kötü niyetli amaçlar güderler (Krombholz vd., 2015). Bu istenmeyen iletiler, kullanıcıların e-posta kutularını doldurabilir, zamanlarını boşa harcayabilir ve güvenlik riskleri oluşturabilir (McAfee, 2020). Ayrıca, spam göndericileri, e-posta adreslerini toplamak için çeşitli teknikler kullanabilirler, örneğin, web sitelerinden veya internet üzerindeki forumlardan adresleri çalabilirler (Benevenuto vd., 2010). Spam'a karşı korunmak için, kullanıcılar güçlü spam filtreleri kullanabilir, e-posta adreslerini dikkatli bir şekilde paylaşabilir ve şüpheli e-postaları açmamak veya yanıtlamamak gibi önlemler alabilirler (Federal Trade Commission, 2021).

Arka kapı (Backdoor), bir sistemde veya yazılımda, yetkisiz erişim için gizlice yerleştirilen bir güvenlik açığı veya arka kapıdır (Kaufman vd., 2002). Bir backdoor genellikle kötü niyetli kişilerin sisteme yetkisiz olarak erişim sağlamasını veya kontrolü ele geçirmesini sağlar (Biryukov vd., 2013). Bu arka kapılar, bilgisayar korsanlarına veya casusluk faaliyetlerinde bulunan kişilere bilgisayarlara sızma fırsatı sunabilir (Kissel vd., 2016). Backdoor'lar, çeşitli yöntemlerle sistemlere yerleştirilebilir. Örneğin, yazılımın kaynak kodunda veya ürünün tasarımında gizlice yerleştirilebilirler (Landau vd., 2014). Ayrıca, güvenlik açıklarını hedefleyen kötü niyetli yazılımların bir parçası olarak da kullanılabilirler (Symantec, 2021). Bu nedenle, güvenlik açıklarının tespiti ve düzeltilmesi önemlidir.

Güvenlik önlemlerinin sürekli olarak güncellenmesi ve denetlenmesi, backdoor saldırılarının önlenmesine yardımcı olabilir.

Sosyal mühendislik, insanların doğal eğilimlerini ve sosyal ilişkilerini kullanarak bilgi elde etmek, manipüle etmek veya yetkisiz erişim sağlamak amacıyla psikolojik ve sosyal yöntemlerin kullanıldığı bir saldırı taktiğidir (Hadnagy, 2011). Sosyal mühendislik saldırılarında, saldırganlar genellikle kurbanlarıyla etkileşime geçer ve güven ilişkisi kurmaya çalışır (Mitnick & Simon, 2002). Sosyal mühendislik yöntemleri arasında sahte kimlikler kullanmak, manipülatif taktikler uygulamak ve duygusal bağlantı kurmaya çalışmak yer alabilir (Renaud & De Angeli, 2009). Bilinmeyen veya güvenilir olmayan kişilerin taleplerine şüpheyle yaklaşmak, kişisel bilgilerin paylaşımını sınırlamak ve güvenlik farkındalığı eğitimlerine katılmak, saldırılardan korunmaya yardımcı olabilir (Gupta vd., 2018).

Casus yazılımlar (Spyware), bir bilgisayar veya mobil cihazın kullanıcısının haberi olmadan kişisel bilgilerini toplayan veya izinsiz olarak kullanıcı etkinliklerini takip eden kötü niyetli yazılımlardır (Christodorescu vd., 2005). Spyware, genellikle kullanıcının bilgisi veya izni olmadan bilgisayarlarına veya cihazlarına sızar ve çeşitli amaçlarla kullanılır (Cai vd., 2018). Bu amaçlar arasında reklam gösterimi, kişisel verilerin çalınması, kullanıcı davranışlarının izlenmesi ve hatta kimlik hırsızlığı bulunabilir (Lederer vd., 2016). Spyware, çeşitli yöntemlerle yayılabilir. Örneğin, zararlı web siteleri veya e-posta eklentileri aracılığıyla bilgisayarlara bulaşabilir (Bhatia vd., 2017). Spyware'den korunmak için, güvenlik yazılımları kullanmak, güvenilir kaynaklardan uygulama indirmek ve e-posta, web tarama gibi alışkanlıklara dikkat etmek önemlidir (Gupta vd., 2018). Ayrıca, bilgisayar ve cihazların düzenli güncellemeleri yapılması ve güvenlik ayarlarının doğru şekilde yapılandırılması da önemli önlemlerdir (Bhatia vd., 2017).

Bilgisayar virüsleri, kötü niyetli yazılımların bir alt kategorisidir ve bilgisayar sistemlerine zarar verebilen veya işlevlerini bozan programlardır (Cohen, 1987). Bilgisayar virüsleri, genellikle kullanıcının bilgisi veya izni olmadan yayılır ve bulaştıkları sistemlerde çeşitli zararlı etkiler yaratırlar (Aycock, 2006). Bu etkiler arasında veri kaybı, sistem çökmesi, hızın yavaşlaması ve hatta kişisel bilgilerin çalınması bulunabilir (Schneider, 2019). Virüsler, çeşitli yollarla yayılabilirler. Örneğin, e-posta eklentileri, USB bellekler veya bulaşmış yazılımlar aracılığıyla diğer sistemlere bulaşabilirler. Virüslerden korunmak için, güvenlik yazılımlarının kullanılması, güncellemelerin düzenli olarak yapılması ve bilinmeyen kaynaklardan yazılım indirilmemesi önemlidir (Szor, 2005). Ayrıca, e-posta eklerinin

dikkatli bir şekilde açılması ve güvenilir olmayan web sitelerine erişimin sınırlanması da önemli önlemlerdir (Schneider, 2019).

Bilgisayar solucanları, kendini kopyalayabilen ve ağ üzerinde otomatik olarak yayılan kötü niyetli yazılımlardır (Spafford, 1989). Bilgisayar solucanları, genellikle ağ trafiğini kullanarak yayılır ve diğer bilgisayarlara bulaşır (Moore vd., 2003). Kendi kendini kopyalayabilme özellikleri sayesinde hızla yayılabilirler ve ağ üzerinde geniş çaplı etkiler yaratabilirler (Worm, 1988). Solucanlar, genellikle sistem kaynaklarını tüketir, ağ performansını düşürür ve hatta sistem çökmesine neden olabilir (Staniford vd., 2002). Ayrıca, solucanlar, bilgisayar kullanıcılarının yetkisi olmaksızın bilgileri toplayabilir veya zararlı eylemler gerçekleştirebilir (Zou vd., 2005). Solucanlardan korunmak için, güncel güvenlik yamalarının ve güvenlik yazılımlarının kullanılması önemlidir (Moore vd., 2003). Ayrıca, ağ trafiğinin izlenmesi, güvenilir olmayan kaynaklardan gelen dosyaların dikkatlice incelenmesi ve kullanıcıların güvenlik bilincinin artırılması da etkili önlemlerdir (Spafford, 1989).

Truva atı (Trojan horse), kullanıcının zararlı bir yazılımı güvenilir bir program veya dosya olarak algıladığı bir tür kötü niyetli yazılımdır (Janczewski & Colarik, 2004). Trojan atları, genellikle kullanıcının izniyle veya bilgisi olmadan bir sisteme bulaşır ve çeşitli zararlı etkiler yaratır (Dhamija & Dusseault, 2008). Bu etkiler arasında veri çalma, kullanıcı aktivitelerini izleme, arka kapılar açma ve bilgisayar sistemini ele geçirme gibi kötü niyetli eylemler bulunabilir (Sabottke vd., 2015). Kullanıcıların dikkatli olması, güvenilir olmayan kaynaklardan yazılım indirmemeleri ve e-posta eklerini dikkatlice kontrol etmeleri önemlidir (Lederer & Kemmerer, 2006). Trojan atlarından korunmak için, güncel güvenlik yazılımları kullanmak, güvenilir kaynaklardan yazılım indirmek ve güvenlik güncellemelerini düzenli olarak yapmak önemlidir (Sabottke vd., 2015). Ayrıca, kullanıcıların bilinmeyen veya şüpheli kaynaklardan gelen dosyalara ve linklere dikkatli olmaları ve sistemlerini düzenli olarak taratmaları gerekmektedir (Janczewski & Colarik, 2004).

Kök kullanıcı takımları (Rootkit), bir bilgisayarın işletim sistemine veya diğer yazılım bileşenlerine gizlenen kötü niyetli bir yazılımdır ve yetkisiz erişim sağlayarak sistemi kontrol etme yeteneğine sahiptir (Gregg, 2011). Rootkitler, bilgisayar korsanları tarafından kullanılan yaygın bir araçtır ve genellikle kullanıcının farkında olmadan faaliyet gösterirler (Anwar vd., 2019). Bu kötü amaçlı yazılımlar, kullanıcının iznini almadan sistemde değişiklikler yapabilir, kullanıcı etkinliklerini izleyebilir ve yetkisiz erişim sağlayarak

gizlice çalışabilir (Fogh, 2006). Rootkitlere karşı mücadele etmek için, güncel güvenlik yazılımlarının kullanılması, güvenlik yamalarının düzenli olarak uygulanması ve güvenilir kaynaklardan yazılım indirilmesi önemlidir (Anwar vd., 2019). Ayrıca, sistemin düzenli olarak taranması, güvenilir olmayan kaynaklardan uzak durulması ve kullanıcıların güvenlik bilincinin artırılması da önemli önlemlerdir (Fogh, 2006).

Klavye dinleme sistemleri (Keylogger), bir bilgisayarda veya mobil cihazda kullanıcının tuş vuruşlarını kaydeden bir kötü niyetli yazılımdır (Patel, Hsu, & Hughes, 2019). Keyloggerlar genellikle kullanıcının haberi olmadan çalışır ve tuş vuruşlarını kaydeder. Bu sayede, kullanıcı tarafından girilen tüm metinler, şifreler, kredi kartı bilgileri ve diğer hassas veriler ele geçirilebilir (Filiol, 2011). Keyloggerlardan korunmanın önemli yollarından biri güvenilir ve güncel bir güvenlik yazılımı kullanmaktır. Ayrıca, güvenilir olmayan kaynaklardan yazılım indirilmemeli, bilinmeyen ekler açılmamalı ve güçlü şifreler kullanılmalıdır (Conti, 2010).

Botnetler, bilgisayar korsanları tarafından kullanılan etkili bir saldırı aracıdır. Bir botnet, zombi bilgisayarları veya cihazları enfekte ederek, bu kaynakları birleştirir ve merkezi bir kontrol noktası altında koordine eder (Stone-Gross vd., 2011). Bu şekilde, saldırganlar büyük miktarda bilgiyi çalabilir, spam e-postaları yayabilir, dağıtılmış hizmet reddi saldırıları (DDoS) gerçekleştirebilir veya diğer zararlı faaliyetlerde bulunabilir (Gupta vd., 2013). Botnetler, genellikle zayıf güvenlik önlemleri veya güncelleme eksiklikleri olan bilgisayarlara sızar. Kötü niyetli yazılımlar, e-posta ekleri, sahte indirme bağlantıları veya web tarayıcı açıklarını kullanarak yayılabilir (Khattak vd., 2017). Botnet saldırılarından korunmanın bir yolu, ağ trafiğini izlemek, anormal aktiviteleri tespit etmek ve zararlı botların tespiti için güvenlik önlemleri almaktır (Stone Gross vd., 2011). Ayrıca, bilinmeyen e-postalara veya şüpheli dosyalara karşı dikkatli olunmalı ve ağ güvenlik ayarları doğru şekilde yapılandırılmalıdır (Khattak vd., 2017).

1.3. Etik ve Etik Farkındalığı

Etik, bireylerin ve toplumun doğru ve yanlış arasında ahlaki değerlendirmeler yaparak davranışlarını düzenlemesini sağlayan bir disiplindir (Rosenstand, 2011). Etik, insanların eylemlerini değerlendirme ve ahlaki standartlara uygun kararlar alma sürecini içerir. Etik, çeşitli felsefi yaklaşımlar ve teorilerle incelenir. Ahlaki kavramlar, değerler, normlar ve ahlaki ilkeler etik çalışmalarında önemli bir rol oynar (Beauchamp & Childress, 2013).

Etik farkındalığı, bilişim ve bilgisayar teknolojilerini etkin olarak kullanan bireylerin ve kurumların ahlaki yükümlülüklerine ve etik değerlerine karşı hassas olması demektir (Reynolds, 2006). Etik farkındalığı sayesinde insanların etik çerçevede kararlar alıp bunları davranışlarına uyarlamalarına yönelik teşvik eder (Schwartz, 2017). Etik farkındalıkları sayesinde bireylerin yanlış olan davranışlardan kaçınmalarına ek olarak doğru olduğu kabul gören davranışları yapmaları beklenmektedir. Etik farkındalığı, günlük karar almalarımızda ve davranışlarımızda bizlere uyumu yakalamayı sağlamamızda yardımcı olur. Etik farkındalıklarının artırılması sonucunda etik açıdan doğru olmayan davranışların ise azalması gerçekleştiği için etik değerler ve ahlaki değerler daha çok ön plana çıkmış olacaktır (Schwartz, 2017). Etik farkındalıkları arttırılmış olan bireyler sayesinde ilerleyen zamanlarda etik farkındalıkları artırılmış toplumlar meydana geleceği unutulmamalıdır. Buradan hareketle, etik çerçevede yetiştirilmiş olan bireylerin sağlıklı toplum yapısının olmazsa olmaz yapı taşı olacağı aşikardır. Etik çerçevede olmayan davranışların yaptırımla cezalandırılacağından ziyade etik unsurlar taşıyan ve toplum tarafından kabul gören olumlu davranışların eğitim yoluyla bireylere aktarılması önem arz etmektedir.

1.4. Bilişim Etiği

Hızlı gelişen ve değişen teknoloji dünyasında güncelliğini koruyan bir alan olan bilişim etiği teknoloji ve etik arasında dengenin sağlanması için araştırma ve tartışmaların sürekli devam ettiği bir konudur. Bilişim etiğini, bilişim sistemlerini ve bilgisayar teknolojilerinin kullanımından kaynaklı meydana gelebilecek olan ahlaki ve etik sorunlar olarak ifade etmek mümkündür (Johnson, 2011). Bilgi ve iletişim teknolojilerini kullanırken uyulması gereken kurallar bütününe bilişim etiği denir (Tıngöy, 2009). Bir diğer deyişle bilişim etiği; teknoloji geliştiricilerinin ve bilişim sistemi kullanıcılarının karşı karşıya kaldıkları etik problemleri temel alır. Bilgiyi oluşturan ve devamlılığını sağlayan bilgi teknolojilerinin ve bilişim sistemlerinin insan haklarına özgürlüklerine ve sosyal adalet kavramlarına ters düşmeden uygun bir şekilde kullanılması önem teşkil etmektedir (Floridi, 2013). Özel hayatın gizliliği, veri güvenliği, siber güvenlik, yapay zeka etiği, kullanıcı güvenliği, internet ve diğer platformlardaki sansür gibi konular bilişim etiğinin önemli konularındandır (Johnson, 2011). Alanyazında bilişim teknolojilerinde etik sorunlar genel olarak (Mason, 1986; Uysal & Odabaşı, 2006; Dedeoğlu, 2007; Himma & Tavani, 2008; Reynolds, 2009; Johnson, 2009; Duymaz, 2013); (i) mahremiyet, (ii) fikri mülkiyet, telif hakları, lisans anlaşması, patent, (iii) güvenlik ve kalite (iv) doğruluk, (v) ifade özgürlüğü, (vi) sayısal uçurum, (vii) siber

zorbalık şeklindedir.

Mahremiyet, bireylerin kendilerine ait olan kişisel bilgilerinin gizliliğini koruma hakkı olarak ifade edilebilir ve ayrıca bu hakkın ihlal edilmesi etik yönden sorun olarak değerlendirilmektedir (Moor, 2008). Mahremiyet sorunu, bireylerin ve kurumların kullanıcı verilerinin izinsiz ve haksız yollarla toplanması ve kullanılması durumlarıyla ilgilidir. Bu türden etik yönden kusurlu olan uygulama ve davranışlar güveni zedeler ve kullanıcıların bilgi teknolojilerine olan güvenini azaltır (Moor, 2008). Mahremiyetin korunabilmesi için bilişim ve bilgisayar sistemlerinde yüksek düzeyde güvenlik önlemlerinin alınması ve kullanıcı verilerinin gizliliğinin sağlanması amacıyla etik yönergelerin uygulanması gereklidir (Floridi, 2013). Birçok firma ve kuruluş kullanıcı verilerine ulaşıp ticari olarak gelirlerini arttırma gayesinde olmakla birlikte bazı çevreler kötü niyetleriyle bu tip çaba içerisinde bulunmaktadırlar. Bu türden durumlara karşı, etik olarak kabul edilebilir veri toplama ve işleme metodlarına ilişkin bilinçli ve duyarlı bir yaklaşımın benimsenmesi mahremiyetin korunması için atılan kritik olarak nitelendirilebilecek bir adım sayılmaktadır (Tavani, 2007).

Siber zorbalık, etik sorunların en önemlilerinden bir tanesidir. Siber zorbalık, bilişim teknolojileri ve internet kullanımı yardımıyla gerçekleştirilen, kişi ya da toplulukları hedef alan zarar verici saldırgan davranışlardır (Wang, Niiya & Mark, 2019). Bu saldırılar sosyal medya, mesajlaşma uygulamaları ve diğer dijital kanallar vasıtasıyla tehdit, iftira, hakaret, ifşa şeklinde gerçekleştirilebilir (Kowalski & Limber, 2012). Siber zorbalığın psikolojik ve duygusal zararlarının yanında mağdur olan kişilerin güvenlik ve mahremiyet yönünden de sıkıntı çekmesine neden olmaktadır. Sosyal etkileşimi temele almasından solayı genler arasında daha sıklıkla karşılaşılan bir etik sorundur (Wang, Niiya & Mark, 2019). Siber zorbalığın önüne geçilebilmesi ve bireylerin mağdur konumuna düşmemesi için eğitim, farkındalık çalışmaları ve etik davranışları konu edinen çalışmaların yaygınlaştırılması çok büyük önem taşımaktadır (Kowalski & Limber, 2012).

Fikri mülkiyet, telif hakları, lisans anlaşmaları ve patentler, kaynaklı etik sorunlar bilişim teknolojileri ve dijital içerik üreticilerin en büyük problemleri arasındadır (McKeon, 2011). İçeriklerin izinsiz şekilde kopyalanması ve çoğaltılması, izinsiz paylaşım, fikri mülkiyet ihlali gibi sorunlar etik açıdan sorun oluşturan davranışlardır. Fikri mülkiyet, inovatif ve özgün şekilde oluşturulan eserlerin veya çalışmaların korunması için tasarlanan hukuki bir kavramdır (WIPO, 2017). Telif hakları, oluşturucusu tarafından ortaya konulan yazılı veya görsel eserlerin sahiplerine tanınan yasal hakları ifade eder (WIPO, 2017). Lisans

anlaşmaları, eser sahibi ile diğer kullanıcılar arasındaki anlaşmadır, eserin kullanım amaç ve kullanım sınırlarını belirler (Lessig, 2001). Patentler ise eser sahibinin eserlerinin belli bir süre boyunca yasal olarak koruma altına alan bir fikri mülkiyet hakkıdır (WIPO, 2019). Patentler sayesinde yeni yeni fikir ve ürünlerin geliştirilmesi teşvik edilebilmektedir.

Güvenlik ve kalite etik sorunların önlenmesi açısından birbirleri ile yakından ilişkilidir. Güvenlik, dijital verilerin korunması, bilişim sistemlerinin çalışmasını aksatacak durumlara ve yetkisiz erişimlere karşı önlem alınması olarak ifade edilebilir (Johnson, 2011). Kalite, bilişim sistemlerinin, verilerin ve yetkisiz erişimleri önlemek amaçlı kullanıcıların beklentilerini karşılaması ve düzgün şekilde işlevini yerine getirmesi anlamına gelmektedir (McNurlin & Sprague, 2006). Bazı yazılım ve veri ihlalleri neticesinde kullanıcılar zarara uğratılabilir, bu gibi güvenlik ihlalleri kalite standartlarını olumsuz yönde etkileyebilir. Kullanıcılar için veri güvenliğinin sağlanması etik bir sorumluluk olmakla birlikte bu hizmetin sağlanmasındaki kalite de etik bir yaklaşımı temsil etmektedir (Johnson, 2011).

Doğruluk, etik açıdan karşılaşılan en büyük problemlerden biridir ve bir durumun, bilginin veya olayın doğruluğu büyük önem taşımaktadır (Floridi, 2013). Doğruluk, bilgi teknolojileri vasıtasıyla aktarılan bilgilerin gerçek, güvenilir ve doğru olduğu anlamına gelmektedir (Johnson, 2011). Doğruluğu sağlıklı olmayan bilginin yani yanlış ve yanıltıcı olması kullanıcıların aldatılması anlamına gelmektedir. Sahte haberler, yanıltıcı ve çerpıtılmış içerikler, manipüle edilmiş veriler bilginin doğruluğunu bozan durumlardır (Floridi, 2013). Günümüz sosyal medyasında ve internet ortamında bu türden problemlerle sıklıkla karşılaşmak mümkündür. Başkalarının özel hayatlarına karşı saygı çerçevesinde olabilmek için doğruluğu sınanmamış olan bilgilerin diğer insanların iletişimine açılmaması gerekmektedir.

İfade özgürlüğü, bireylerin düşüncelerini, görüşlerini ve fikirlerini kısıtlama olmadan özgürce ifade etme hakkıdır (Johnson, 2011). Bilişim teknolojileri ve internetin yaygın kullanımı, ifade özgürlüğü için çok önemli bir ortamdır. Fakat diğer yandan ifade özgürlüğü bazı etik sorunların da temelini oluşturmaktadır. Nefret ve hakaret söylemleri ile yanıltıcı ve doğruluğu sağlam olmayan bilgilerin yayılmasına da sebep olabilmektedir (Johnson, 2011). İfade özgürlüğü birileri için özgürlük olma niteliği taşırken birileri için de mağduriyet oluşturuyorsa bu gibi durumlarda yasal düzenlemeler ve toplumsal normlar ile ifade özgürlüğünün etik sınırlara ihtiyaç var demektir. Etik çerçevede bilişim teknolojilerinin, ifade özgürlüğünü sağlamak, doğruluğu kanıtlanmış bilgilerin dolaşımda bulunmasına müsaade etmek gibi güvence altına almış olduğu eylemler sayesinde kullanıcıların

kendilerini güvende hissetmeleri sağlanmış olur (Lessig, 2006).

Sayısal uçurum, bilgi ve iletişim teknolojilerindeki hızlı gelişmelere bağlı olarak toplumda bazı kesimlerinin diğerlerine göre bilgi ve iletişim teknolojilerini kullanma, erişim ve beceri açısından geride kalmasına sebep olabilir (Selwyn, 2003). Bu durumun en temel sebeplerinden biri sosyo-ekonomik düzeydir. Gelişmekte olan ülkelerde, dezavantajlı bölgelerinde sayısal uçurumun daha belirgin olduğu, toplumun diğer bölümlerinde ise teknoloji ve diğer imkanlara erişim açısından farklılıkların ortaya çıktığı gözlenmektedir (Norris & Pernia, 2019).bilişim teknolojilerinin sağladığı imkanlardan toplumun eşit şekilde faydalanabilmesi ancak sayısal uçurumun azaltılmasıyla mümkün olabilmektedir. Bu da altyapının geliştirilmesi, uygun politikaların seçimi ve dijital becerilerin yaygınlaştırılması ile mümkündür (Selwyn, 2003).

1.5. Araştırmanın Amacı

Ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalığı çalışmamızın birincil amacı; ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalığı düzeylerini ölçebilecek bir ölçme aracı geliştirmektir. Geliştirilmek istenen ölçek sayesinde ortaokul düzeyindeki öğrencilere yönelik ileriki araştırmalarda kullanılabilecek bir ölçme aracı ortaya konulması bu alandaki literatüre katkı sağlamış olacaktır.

Çalışmanın ikincil amacı ise; geliştirilecek olan ölçek yardımıyla öğrencilerin bilgi güvenliği ve etik farkındalık düzeylerinin sınıf düzeyi, cinsiyet, anne-baba eğitim düzeyi durumları açısından farklılık gösterip göstermediği incelenmesidir.

1.6. Araştırmanın Önemi

Gelişen bilgi teknolojileri ve bunlara entegre uygulamalar bilgi güvenliği ve bilgi güvenliği farkındalığının önemini artırmaktadır (Çetinkaya, Güldüren & Keser, 2017). Bilgiyi oluşturup muhafaza eden sistemler bir zincir olarak düşünüldüğünde buradaki en zayıf halkanın insan faktörü olmasından kaynaklı olarak kullanıcı farkındalığı kritik bir öneme sahiptir (Güldüren, 2015). Bilgisayar ve mobil teknolojilerinin kullanım miktarları ve oranları gün geçtikçe artmakta ve bu teknolojilere sahip olup kullanan kullanıcıların yaşı da giderek aşağılara inmektedir.

Bilgi güvenliği farkındalığı ile ilgili literatür incelendiğinde yapılan çalışmaların iş hayatı içerisinde aktif olarak yer alan bireyler, akademisyenler, öğretmenler, lisans öğrencileri, orta

okul öğrencilerinin ebeveynlerine ve lise öğrencilerine yönelik çalışmaların var olduğu görülmektedir (Mart, 2012; Tekerek & Tekerek, 2013; Karaoğlan Yılmaz ve diğerleri, 2014; Akgün & Topal, 2015; Güldüren, Çetinkaya & Keser, 2016; Kapanoğlu, 2016; Mete, 2016; Tekin & Polat, 2016 ve Karaoğlan Yılmaz & Çavuş Ezin, 2017; Hacımustafaoğlu, 2019; Vilander, 2021; Talan & Aktürk, 2021; Van De Mortel, 2021; Zhen, Dong, Xie & Chen, 2022; Akıncan, 2022). Bu çalışmamızın hedef kitlesini oluşturan ortaokul öğrencilerine yönelik ise var olan çalışmaların (Derin & Gençoğlu, 2020; Özen Serter, 2021; Gökçearslan, Günbatar & Sarıtepeci, 2021) sınırlı sayıda olduğu görülmüştür. Ortaokul öğrencileriyle yapılmış olan çalışmalarda yetişkinler için hazırlanmış olan bilgi güvenliği farkındalığı ölçeklerin ve anketlerin kullanıldığı görülmüştür.

Derin ve Gençoğlu (2020), ortaokul öğrencilerine yönelik bilgi güvenliği farkındalığı üzerine 30 maddelik anket çalışması gerçekleştirmiştir. Özen Serter (2021), bilgi güvenliği farkındalığı üzerine Güldüren, Çetinkaya ve Keser (2016) tarafından lise öğrencileri için geliştirilen ölçeği ortaokul öğrencilerine uyarlayarak tarama çalışması gerçekleştirmiştir.

Etik farkındalığı ile ilgili literatür incelendiğinde öğrencilerin etik olmayan davranışlarına yönelik yapılmış olan çalışmalar (Ghazali, 2003; Haines & Leonard, 2007; Namlu & Odabaşı, 2007; Uysal & Odabaşı, 2007; Kuzu, 2009; Aksal, 2011; Beyhan & Tunç, 2012; Duymaz, 2013; Genç, Kazez & Fidan, 2013; Gökçearslan, Günbatar & Berikan, 2015; Çelik & Gündoğdu, 2019; Salman, 2019; Biber & Biber, 2020) yer almasına rağmen, etik bilincinin temellerinin oluşturulmaya başlandığı ortaokul kademesinde öğretim programlarında bu kavramın sınırlı bir şekilde incelendiği görülmüştür (Fidan, 2016).

Gökçearslan, Günbatar ve Berikan (2015), ortaokul öğrencilerine yönelik çalışmalarında bilişim etiği üzerine Yoon (2011) tarafından geliştirilip Arıkan ve Duymaz (2014) tarafından Türkçeye uyarlanan ölçeği kullanmıştır. Salman (2019), yapmış olduğu çalışmada "İnternet Etik İhlali Algı Ölçeği"ni ortaokul öğrencilerine yönelik geliştirmiştir. Biber ve Biber (2020), yapmış olduğu çalışmada Arıkan ve Duymaz (2014) tarafından Türkçeye uyarlanan ölçeği kullanmıştır.

Öğrencilerin teknolojiyi ne kadar uyarladıkları, teknolojiyi kullanırken karşılaştıkları tehditler karşısındaki farkındalık seviyeleri ve etik farkındalığı hakkında kazanması gereken bilgi ve becerilerin niteliği ön plana çıkmaktadır. Seferoğlu ve diğerleri (2018)'ne göre de "Bilişim Teknolojileri ve Yazılım" dersi öğretim programlarının yapılandırılması sürecinde öğrencilerin karşılaştıkları tehlikeler ve bilgi güvenliği hakkındaki bilgi eksiklikleri göz önünde bulundurulması gerekmektedir. Bu çalışma ile ortaokul öğrencilerinin bilgi

güvenliği ve etik farkındalığı konusundaki eksiklikleri ve karşılaşabilecekleri tehlikeler ölçülmeye çalışılarak gerekli önlemlerin alınması açısından, öğretim programlarına katkı sağlaması açısından program geliştirmecilere ve ilgili alanyazına katkı sağlaması açısından önem arz etmektedir. Ortaokul öğrencilerine yönelik yapılan bu çalışma alanyazında yer alan diğer çalışmalardan ayıran bilgi güvenliği farkındalığının yanında etik farkındalığını da ölçen bir ölçek geliştirme çalışması olmasıdır.

1.7. Araştırmanın Problemi

Bu araştırmada "Bilgi ve iletişim teknolojilerini kullanan ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalık durumları nedir?" sorusuna çeşitli boyutlarda cevaplar aranacaktır. Araştırmanın alt problemleri;

1. Öğrencilerin bilgi güvenliği ve etik farkındalık düzeyleri nasıldır?
2. Öğrencilerin bilgi güvenliği ve etik farkındalık düzeyleri yaş, cinsiyet, sınıf düzeylerine göre değişim göstermekte midir?
3. Öğrencilerin bilgi güvenliği ve etik farkındalık düzeyleri anne-baba eğitim düzeylerine göre anlamlı farklılıklar göstermekte midir?

1.8. Sınırlıklar

Araştırmanın sınırlılıkları şunlardır:

1. Araştırma, bilgi güvenliği ve etik farkındalığı konularıyla sınırlıdır.
2. Araştırmanın örnekleminin 2022-2023 Eğitim-Öğretim yılının ikinci döneminde merkez ilçeye bağlı ortaokullarda okuyan 5, 6, 7 ve 8. Sınıf öğrencileri ile sınırlıdır.
3. Ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalıklarının belirlenebilmesini amaçlayan bu çalışmanın verileri geliştirilip kullanılan ölçme aracından elde edilen verilerle sınırlıdır.

2. LİTERATÜR ÖZETİ

Yurt içinde ve yurt dışında yapılmış olan araştırmalarla ilgili literatür taranmıştır. Bu bölümde bilgi güvenliği farkındalığı ve etik farkındalığı üzerine yapılmış olan çalışmalar hakkında bilgiler verilmiştir.

2.1. Bilgi Güvenliği Farkındalığı İle İlgili Araştırmalar

Mart (2012)'ın "Bilişim Kültüründe Bilgi Güvenliği Farkındalığı" isimli yüksek lisans çalışmasında farklı meslek gruplarından 501 bireye geliştirdiği bilgi güvenliği farkındalığı anketini uygulamıştır. Araştırmadan elde edilen sonuçlara göre katılımcıların bilgi güvenliği farkındalıkları ile bilişim kültürleri arasında anlamlı yönde bir ilişki olduğu görülmüştür.

Tekerek ve Tekerek'in 2013 yılında yaptıkları "İlköğretim ve Ortaöğretim Düzeyindeki Öğrencilerinin Bilgi Güvenliği Farkındalık Düzeyleri" konulu çalışmalarında araştırmacılar tarafından geliştirilen bilgi ve bilgisayar güvenliği farkındalık ölçeği Kahramanmaraş İlindeki 2449 öğrenciye uygulanmıştır. Verilerden elde edilen sonuçlara göre öğrencilerin bilgisayar ve bilgi güvenliği farkındalık düzeylerinin yeterli seviyede olduğu saptanmıştır. Bunlara ek olarak öğrencilerin bilgi gerektiren konular ve kurallar konusunda farkındalıklarının düşük olduğu tespit edilmiştir.

Karaoğlan Yılmaz ve arkadaşları (2014)'nın "Üniversite Öğrencilerinin Güvenli Bilgi ve İletişim Teknolojisi Kullanım Davranışları ve Bilgi Güvenliği Eğitimine Genel Bir Bakış" isimli araştırmasında aket uygulaması gerçekleştirilmiştir. Bu anket 214 üniversite öğrencisine uygulanmıştır. Araştırmanın sonuçlarına göre üniversite öğrencilerinin bilgi güvenliği farkındalık düzeylerinin düşük olduğu görülmüştür. Üniversite öğrencilerinin bilgi güvenliği önlemlerinden olan yedekleme, erişim ve paylaşım güvenliği, şifre güvenliği, e-posta güvenliği, internet güvenliği, sosyal mühendislik ve zararlı yazılımları önleyici güvenlik unsurlarından sadece birkaçına yönelik önlem aldığı fakat büyük bir kısmı için herhangi bir önlem almadığı ortaya konulmuştur.

Akgün ve Topal (2015) yapmış oldukları çalışmada, üniversite öğrencilerinin bilgi güvenliği farkındalıklarını ortaya çıkarmışlardır. Araştırma kapsamında Sakarya Üniversitesi Eğitim fakültesi dördüncü sınıfta olan 217 öğrenciye yönelik "Bilişim güvenliği anketi" uygulanmıştır. Araştırma sonuçlarına göre üniversite öğrencilerinin genel anlamda bilişim güvenliği hakkında farkındalıklarının yeterli düzeyde olduğu tespit edilmiştir.

Güldüren, Çetinkaya ve Keser (2016) lise seviyesindeki öğrencilerle bilgi güvenliği

farkındalığı üzerine bir çalışma gerçekleştirmiştir. Çalışma kapsamında öğrencilerin bilgi güvenliği farkındalıklarını tespit edebilmek amacıyla bir ölçek geliştirilmiştir. 607 öğrencinin katılımıyla gerçekleştirilen çalışma sonucunda lise öğrencilerine yönelik bilgi güvenliği farkındalık ölçeği geliştirilmiştir. Hazırlanan ölçek kullanılarak lise öğrencilerinin farkındalıklarını tespit edebilmek için tarama modeli kullanılmış olup öğrencilerin bilgi güvenliği farkındalıkları araştırılmıştır. Araştırma sonucunda lise öğrencilerinin cinsiyetleri ile bilgi güvenliği farkındalıkları arasında anlamlı bir farklılık olduğu tespit edilmiştir.

Kapanoğlu (2016)'nun yapmış olduğu çalışmada öğretmenlerin güvenli internet kullanım durumları ve öğretmenlerin bilgi güvenliği farkındalık düzeylerinin nasıl olduğu ortaya konulmaya çalışılmıştır. Araştırma kapsamında geliştirilen ve öğretmenlere yönelik hazırlanan bilgi güvenliği anketi kullanılmıştır. Araştırmaya katılım sağlayan 1355 öğretmenden elde edilen verilere göre; öğretmenlerin orta düzeyde bilgi güvenliği farkındalıklarının mevcut olduğu tespit edilmiştir.

Mete (2016)'nin çalışmasında üniversite öğrencilerinin bilgi güvenliği farkındalığına etki eden faktörlerin neler olduğu araştırılmıştır. Araştırma kapsamında yüksek öğrenim almakta olan 420 öğrenciye hazırlanmış olan anket uygulanmıştır. Uygulanan anketten elde edilen verilere göre bilgi güvenliğini en çok etkileyen faktörlerin neler olduğu ortaya çıkarılmıştır. Bu araştırmaya göre mobil internet kullanma, şifre oluşturma, e-posta kullanımı, sosyal ağ ve internetin kullanımı gibi faktörlerin bilgi güvenliğini sağlamaya etki eden faktörler olduğu görülmüştür.

Tekin ve Polat (2016) yapmış olduğu çalışmayı velilere yönelik gerçekleştirmiştir. Bu amaçla ortaokul öğrencilerinin velilerinin bilgi güvenliği farkındalıklarının hangi düzeyde olduğunu ortaya çıkarmaya çalışmıştır. Geliştirmiş oldukları güvenli internet kullanımı ve veli farkındalık anketi Elazığ'da bir ortaokuldaki 115 öğrenci velisine uygulanmıştır. Araştırmanın sonuçlarına göre veliler çocuklarının güvenli internet kullanımı konusunda yeterince bilinçli oldukları tespit edilmiştir.

Erdoğmuş (2017)'un yapmış olduğu yüksek lisans tezinde öğrencilerin bilgi güvenliğine yönelik kazanımlarının, bilgi güvenliği farkındalıkları üzerine etkilerini incelemiştir. Elde edilen bulgulara göre bilgi güvenliği farkındalıklarının internet ortamına olan güvene, sınıf seviyesine, yaş ve bölüme göre anlamlı farklılıklar gösterdiği sonucuna ulaşılmıştır.

Karaoğlan Yılmaz ve Çavuş Ezin (2017)'in araştırması ebeveynlerin bilgi güvenliği farkındalıkları üzerinedir. Bu amaç doğrultusunda ortaokul 5 ve 6. Sınıf öğrencilerinin velilerine yönelik anket uygulanmıştır. Araştırmaya 91 ebeveyn katılmıştır. Araştırmadan

elde edilen verilere göre ebeveynlerin farkındalıklarının belli bir düzeyde olduğu görülmüştür. Fakat verilerin yedeklenmesi ve sıklığı konusundaki farkındalıklarının düşük düzeyde olduğu tespit edilmiştir. Diğer bir sonuca göre ise ebeveynlerin çocuklarını bilgi güvenliği hususunda yalnızca sözlü olarak uyarıda bulunduğunu fakat bu konularda bilgilendirici davranışlarda bulunmadığı görülmüştür.

Dönmez (2019)'in lise öğrencilerine yönelik olarak gerçekleştirdiği araştırmada dijital okuryazarlık ile bilgi güvenliği farkındalığı arasındaki olan ilişkiyi incelenmiştir. Bilgi güvenliği farkındalığının "saldırı ve tehditler" alt boyutunun erkekler lehinde farklılaştığı sonucuna ulaşılmıştır. İnternet kullanım süresi, sosyal medya kullanım süresi ile çevrim içi araçları kullanabilme özyeterliği ile bilgi güvenliği farkındalığı arasında pozitif korelasyon olduğu ortaya çıkarılmıştır.

Hacımustafaoğlu (2019)'nun çalışmasında; lise öğrencilerinin bilgi güvenliği farkındalık seviyelerinin siber mağdur olma durumlarına etkisini incelemiştir. Araştırma sonuçlarına göre bu iki değişken arasında anlamlı bir ilişkinin varlığından söz edilememiştir. Lise düzeyindeki öğrencilerin bilgi güvenliğini etkileyen faktörler; cinsiyet, sınıf seviyesi, günlük internet kullanımı, anne-baba eğitim durumu olarak belirlenmiştir.

Derin ve Gençoğlu (2020) "Ortaokul Öğrencilerinin Bilgi Güvenliği Farkındalığı" isimli çalışmalarında, 400 öğrenciye 30 sorudan oluşan anket uygulamışlardır. Araştırmanın sonucuna göre, öğrencilerin bilgi güvenliği farkındalıkları; sınıf, yaş, cinsiyet, internette geçirilen zaman ve internet kullanma amacı değişkenlerine göre anlamlı düzeyde farklılık olduğu görülmüştür.

Talan ve Aktürk (2021)'ün çalışmasında lise öğrencileri arasında erkeklerin kız öğrencilere göre bilgi güvenliği farkındalıklarının yüksek olduğu ortaya çıkmıştır. Öğrencilerin yaşadıkları şehirlere göre karşılaştırması yapıldığında anlamlı farklılıkların görülmediği tespit edilmiştir. İnternet kullanım süresinin günlük 7 saatten fazla olan lise öğrencilerinin bilgi güvenliği farkındalıklarının daha yüksek olduğu tespit edilmiştir. Buna ek olarak sosyal medyada geçirilen zamanın bilgi güvenliği farkındalığına yönelik etkisinin olmadığı ortaya konulmuştur.

Gökçearslan, Günbatar ve Sarıtepeci (2021)'nin çalışmasında kişisel bilgisayar ve akıllı telefon sahibi olunması, okullarda alınan bilişim teknolojileri dersinin bilgi güvenliği farkındalığına olan etkisi araştırılmıştır. Kişisel bilgisayar ve akıllı telefon sahibi olunması ve Bilişim Teknolojileri dersinin alınmış olması bilgi güvenliği farkındalığına yönelik olarak pozitif katkılar sağladığı görülmüştür.

Vilander (2021) yaptığı çalışmada, 18 yaş üzeri bireylerle bilgi güvenliği farkındalığı çalışmıştır. Elde edilen bulgulara göre; bilgi güvenliği farkındalığının yaş ile doğru orantılı olarak arttığı sonucuna ulaşmıştır. Deneyim kazanmamın bilgi güvenliği farkındalığında önemli bir etken olduğuna ve alınan örgün eğitimin belirleyici bir unsur olmadığı sonucuna ulaşılmıştır.

Yıldırım ve Demirer (2021)'in yapmış olduğu çalışmada; 2009 ve 2019 yılları arasında eğitim alanında yapılan 60 adet bilgi güvenliği üzerine yapılan çalışmalar incelenmiştir. Elde edilen bulgulara göre bilgi güvenliği farkındalığının düşük seviyelerde olduğu görülmüştür. Bilgi güvenliği alanında yapılan çalışmaların yıllar geçtikçe artmış olmasına rağmen, okul öncesi, ilkokul ve ortaokul seviyesinde yapılan çalışmaların çok az olduğu dikkat çekmiştir.

Van De Mortel (2021)'in yapmış olduğu çalışmada; bireylerin eğitim düzeyleriyle bilgi güvenliği farkındalıkları arasında anlamlı bir ilişkinin olmadığı sonucuna ulaşılmıştır. Eğitim düzeyinin yüksek olması ya da düşük olması bilgi güvenliği farkındalığını etkileyen bir unsur olarak görülmemiştir.

Özen Serter (2021)'in yapmış olduğu tez çalışmasında; ortaokul öğrencilerinin bilgi güvenliği farkındalıklarının belirlenmesi amaçlanmıştır. Bilgi güvenliği farkındalıklarının belirlenmesi amacıyla ortaokul öğrencilerine Güldüren, Çetinkaya ve Keser (2016) tarafından geliştirilen ölçek uygulanarak veriler toplanılmıştır. Araştırma sonuçlarına göre kızların bilgi güvenliği farkındalığı düzeyinin erkeklere göre daha yüksek olduğu ortaya çıkmıştır. Anne eğitim seviyesi arttıkça öğrencilerin bilgi güvenliği farkındalık seviyelerinde belirgin şekilde artış olduğu tespit edilmiştir.

Akıncan (2022) yapmış olduğu tez çalışmasında ortaokul öğretmenlerinin bilgi güvenliği farkındalık, dijital bağımlılık ve dijital okuryazarlık düzeylerini incelemiştir. Elde edilen bulgulara göre öğretmenlerin dijital okuryazarlığı ile bilgi güvenliği farkındalığı arasında pozitif yönlü olmak üzere anlamlı bir ilişkinin var olduğu tespit edilmiştir.

Zhen, Dong, Xie ve Chen (2022) yapmış oldukları çalışmada; uzaktan çalışma ortamında bilgi güvenliği farkındalığını etkileyen faktörleri incelemişlerdir. Bilgi, davranış ve öğrenme ataleti ile bilgi güvenliği farkındalıkları arasında anlamlı düzeyde ilişki olduğu sonucu ortaya konulmuştur.

Slusky ve Partow (2012) yapmış olduğu çalışmada Amerika'da üniversite öğrencilerinin bilgi güvenliği farkındalık düzeylerini ölçmüştür. Araştırma sonuçlarına göre, öğrenciler tarafından kullanılan uygulamaların özelliklerini, karşılarına çıkabilecek riskler ve bunlara yönelik önlemler hakkında bilgi yönünden eksikliklerinin olmadığını, farkındalıklarının

yüksek olduğu fakat bunu gerçek hayatın içerisinde kullanmadıkları görülmüştür.

Kim (2013), güvenlik zincirinin en zayıf halkasının kullanıcılar olmasından hareketle yapmış olduğu çalışmada; öğrencilerin bilgi güvenliği düzeylerini incelemiştir. Amacı bilgi güvenliği düzeylerinin nasıl olduğunu ortaya çıkararak öğrencilerin bilgi güvenliği düzeylerini geliştirmektir. Üniversite öğrencileriyle yapılan çalışmanın anket sonuçlarına göre, öğrencilerin Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) Özel Raporu çerçevesinde sunulan bilgi güvenliği konularını bilişsel olarak kavradıklarını görmüştür. Çalışma sonuçlarında, bilgi güvenliği eğitimlerinin artırılması ve öğrencilerin teşvik edilmesinin önemi vurgulanmıştır.

2.2. Etik Farkındalığı İle İlgili Araştırmalar

Aksal (2011), öğretmen adaylarına yönelik olarak "Bilgisayar Teknolojilerinin Kullanımında Etik ve Karşılaşılan Sorunlar" isimli araştırmayı gerçekleştirmiştir. Araştırma kapsamında öğretim teknolojileri ve materyal tasarımı dersini gören öğretmen adaylarının bilgisayar teknolojileri alanındaki etik ve sorunlarla ilgili deneyim ve düşüncelerini ortaya çıkararak bu konuda farkındalık kazandırmak amaçlanmıştır. Araştırma sonuçlarına göre öğretmen adaylarının sosyal ağ, sanal iletişim, internet ve haberleşme ile ilgili konularda sorunlar yaşadığı ortaya çıkarılmıştır. Teknolojinin günümüzde eğitimin önemli bir parçası olmasından dolayı teknoloji eğitimi ve etik konusunda uygulanan eğitim programlarının daha fazla zengin hale getirilmesinin gerekli olduğu belirtilmiştir.

Gökçearslan, Günbatar ve Berikan (2015) ortaokul öğrencilerine yönelik araştırma gerçekleştirmiştir. Araştırma kapsamında ortaokul öğrencilerinin bilişim etiği seviyesinin demografik özelliklere göre ve bilişim teknolojileri ve yazılım dersini görme durumlarına göre değişiklik gösterip göstermeme durumu incelenmiştir. Araştırmadan elde edilen sonuçlara göre ortaokul öğrencilerinin bilişim etiği düzeylerinin iyi seviyede olduğu bulunmuştur. Ayrıca bilişim etik düzeyleri cinsiyete ve sınıf seviyelerine göre anlamlı olacak şekilde farklılık göstermiştir. Anne-baba eğitim durumları açısından ve bilişim teknolojileri ve yazılım dersi görme sürelerine göre anlamlı bir farkın olmadığı tespit edilmiştir.

Özdemir (2017), yapmış olduğu çalışmada BÖTE ve Yönetim Bilişim
Sistemlerinde eğitim görmekte olan lisans ve lisansüstü öğrencileriyle çalışmıştır. Öğrencilerin internet teknolojilerinde etik kullanım düzeylerini incelemiştir. Araştırmada 6 alt boyuttan (Sağlıklı İnternet Kullanımı, Temel İlkeler, Güvenlik, Telif Hakkı, Dürüstlük, Çevrimiçi Nezaket) ve 38 maddeden oluşan internet etik kullanım ölçeği geliştirmiştir.

Araştırmadan sonuçlarına göre kızların erkeklere oranla internet etik kullanım düzeylerinin daha yüksek olduğu görülmüştür. Öğrencilerin okudukları sınıf seviyeleri arttıkça internet etik kullanım düzeyinin arttığı görülmüştür. Öğrencilerin ailelelerinin maddi geliriyle internet etik kullanım düzeyleri arasında ters ilişkinin olduğu ve internet kullanım sürelerinin arttıkça internet etik kullanım düzeylerinin de arttığı gözlemlenmiştir. Kişisel bilgisayar sahibi olunması ile internet etik kullanım düzeyleri arasında anlamlı bir ilişkinin bulunmadığı da görülmüştür.

Çelik ve Gündoğdu (2019)'nun "Bilişim Etiği Değerlerine Yönelik Tutum Ölçeğinin Geliştirilmesi" ismindeki çalışması lise öğrencileriyle gerçekleştirilmiştir. Çalışmada lise öğrencilerinin bilişim teknolojileri alanında yer alan değerler hakkındaki tutumlarını nasıl olduğunu belirlemeye yönelik ölçek geliştirmek amaçlanmıştır. 8 alt boyuttan oluşan ölçekle, gizliliğin ihlali, sanal yardımseverlik, sanal zorbalık, telif haklarına saygı güvenlik, sanal ortam iş birliği, sanal ahlak ve paylaşma alt boyutları çerçevesinde öğrencilerin tutumları tespit edilmeye çalışılmıştır. Hazırlanan ölçek hakkındaki bulgular ölçeğin güvenilir ve geçerli olduğu yönündedir.

Salman (2019), ''Ortaokulda Öğrencilerin İnternetteki Etik İhlallerine Yönelik Algılarının İncelenmesi'' adlı çalışmasını ortaokul öğrencileriyle gerçekleştirmiştir. Araştırma kapsamında "İnternet Etik İhlali Algı Ölçeği" geliştirilerek güvenilir ve geçerlik yönünden uygulanabilirliği sınanmıştır. Araştırma sonucunda öğrencilerin internet ortamında etik ihlallere yönelik algılarının yüksek olduğu görülmüştür. Kız öğrencilerin erkeklere göre internet etik ihlallerine yönelik algılarının daha yüksek olduğu tespit edilmiştir. Sınıf düzeyinin arttıkça öğrencilerin internet etik ihlallerine yönelik algılarının azaldığı sonucuna ulaşılmıştır.

Biber ve Biber (2020)'in yaptığı "Ortaokul Öğrencileri İle Meslek Lisesi Öğrencilerinde Bilişim Etiği" isimli çalışmayı meslek lisesinde okuyan ve ortaokulda okuyan öğrencilerle gerçekleştirmiştir. Öğrencilerin bilişim etiği düzeylerini incelemeyi amaçlamışlarıdır. Cinsiyet ve sınıf seviyesine göre öğrencilerin bilişim etik düzeylerinde nasıl değişim olduğu araştırılmıştır. Araştırmada Arıkan ve Duymaz (2014)'ın Türkçe'ye uyarladığı ölçek kullanılmıştır. Araştırmaya ortaokul düzeyinde 101 öğrenci ve meslek lisesi düzeyinde 179 öğrenci katılım sağlamıştır. Araştırma sonucunda ortaokul ve meslek lisesi öğrencilerinin arasında bilişim etiği düzeylerinin anlamlı farklılıklar göstermediği görülmüştür. Ayrıca, cinsiyet faktörü kaynaklı olarak öğrencilerin bilişim etiği düzeylerinin anlamlı şekilde farklılaştığı (erkekler lehine) görülmüştür. Öğrencilere verilen bilişim teknolojileri

derslerinin öğrencilerin bilişim etiği düzeylerine etkisinin olmadığı görülmüştür.

Aydoğdu (2022) yapmış olduğu "Bilişim Etiği Konusunda Geliştirilen Bilgisayar Destekli Öğretim Materyalinin Ortaöğretim Öğrencilerinin Etik Olmayan Bilgisayar Kullanım Düzeylerine Etkisinin İncelenmesi" isimli çalışmasında bilişim etiği konusunda yapılmış olan çalışmaları incelemiştir. 2002-2020 yılları arasında ülkemizde ulusal düzeyde yapılan çalışmaların %18'i ortaokul öğrencileriyle gerçekleştirilmiştir. 1978-2020 yılları arasında bilişim etiği konusunda yapılmış olan uluslararası düzeyde yapılan çalışmaların %7,8'lik kısmını ortaokul düzeyindeki öğrencilerle yapıldığı görülmüştür.

Soldatova, Rasskazova, Zotova, Lebesheva, Geer ve Roggendorf (2014)'un çalışmasında, Avrupa Çevrim İçi Çocukları Projesini kısmını EU Kids Online II çalışmasından elde edilen sonuçlarla karşılaştırmasını yapmışlardır. Araştırmaya göre Rusya'daki çocukların %53'lük kısmı çevrim içi ortamlarda kendilerine uygun olmayan içeriklerin var olduğunu ve %26'lık kısmının ise çevrim içi ortamlarda kendilerine zarar verebilecek içeriklerle karşı karşıya kaldıklarını ifade etmişlerdir. Araştırmanın diğer bir sonucu ise Rusya'daki gençlerin Avrupa'daki yaşıtlarına göre daha fazla cinsel içeriklerle karşılaştıklarını ortaya koymuştur. Rusya'daki çocukların %8 oranında, Avrupa'daki çocukların ise %3 oranında siber zorbalık yaptığı görülmüştür.

Sari, Rejekiningsih ve Muchtarom (2020)'un çalışmasında, Endonezya'da lise öğrencilerinin dijital etik profilleri tarama yöntemi kullanılarak araştırılmıştır. Dijital etik başlığı altında internet kullanımı, pornografik içerik erişimi için siber zorbalık, kişisel veriler, nefret söylemleri gibi durumlar incelenmiştir. Öğrencilerin dijital etik seviyelerinin %35,2'si yüksek düzeyde, %32,8'i yeterli düzeyde, %32'si de iyi düzeyde olduğu tespit edilmiştir.

3. MATERYAL VE METOT

Ortaokul Öğrencilerinin Bilgi Güvenliği ve Etik Farkındalığı araştırmasının bu bölümünde; araştırmanın modeli, evren ve örneklem, veri toplama aracı ve uygulama süreci ve araştırma verilerinin istatistiksel analizi hakkında açıklamalara yer verilmiştir.

3.1. Araştırmanın Modeli

Araştırmaya dair soruların cevaplanmasına odaklanan ya da araştırma hipotezlerinin test edilmesine güvence sağlayan, elde edilen verilerin araştırmanın amacına uygun olacak şekilde toplanmasını ve analizinin sağlayan koşulların düzenlenmesine araştırmanın modeli veya deseni denilmektedir (Balcı, 2009). Ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalığı ile ilgili olan bu çalışma iki aşamadan oluşmaktadır. Birinci aşama ortaokul öğrencilerine yönelik bilgi güvenliği ve etik farkındalık ölçeğinin geliştirilmesi aşamasıdır. İkinci aşamada ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalık düzeylerinin bazı değişkenler (yaş, cinsiyet, sınıf düzeyi vb.) açısından farklılık gösterip göstermediğinin belirlenebilmesi için tarama modeli kullanılmıştır.

Sayıca çok fazla katılımcının bulunduğu evren hakkında genel bir yargı oluşturabilmek için evrenden alınan daha küçük bir gruba yönelik yapılan çalışmaya tarama modeli çalışması denilmektedir (Karasar, 2005). Tarama modelinde amaç; insan topluluklarının, kuruluşların, nesnelerin, olayların doğasını ve özelliklerini betimleyerek açık ve net bir şekilde ortaya konulmasını sağlamaktır (Mc Millian & Schumacher, 2001; Büyüköztürk, Kılıç Çakmak, Akgün, Karadeniz & Demirel, 2012; Özdemir, 2014).

3.2. Araştırmanın Evren ve Örneklemi

Araştırmanın örneklemini 2022-2023 Eğitim-Öğretim yılında Bartın İli Merkez İlçede yer alan ortaokul (5, 6, 7 ve 8. sınıf) öğrencileri oluşturmaktadır. Türkiye'deki tüm ortaokul öğrencileri ise araştırmanın evrenini oluşturmaktadır. Araştırmanın birinci aşaması ölçek geliştirme olduğu için hazırlanan ölçeğin pilot uygulamasının yapılması önem arz etmektedir. Bu husus doğrultusunda hazırlanan ölçeğin uygulanmasına yönelik olarak alanyazın incelendiğinde, ulaşılması gereken örneklem büyüklüğü ile ilgili farklı ölçütler ve görüşlerin bulunduğu görülmüştür. Örneklem büyüklüğü belirlenirken, madde ya da faktör

sayısına bağlı olarak belirlenmeye çalışılmaktadır. Genel kabul gören görüşe göre örneklem büyüklüğünün ölçekte yeralan madde sayısının 5 ila10 katı kadar olması gerekmektedir (Kass & Tinsley, 1979; Kline, 1994; Tavşancıl, 2005). Guilford (1954) ve Kline (1994) 200 katılımcıdan oluşan örneklemin mutlak ölçüt olarak yeterli olacağını söylemiştir. Fakat daha büyük katılımcı sayısına sahip örneklemlerin ölçek geliştirme çalışmaları için daha uygun nitelikler sağlayacağının önemine vurgu yapmışlardır. Çokluk, Şekercioğlu ve Büyüköztürk (2010) ise ölçek geliştirme çalışmalarında faktör analizi yapabilmek için gerekli olan örneklem sayısının en az 300 olması gerektiğini ifade etmişlerdir. Ölçek geliştirme çalışmalarında örneklem büyüklükleri ile ilgili farklı görüşler mevcuttur. Bu görüşler çerçevesinde en kabul gören kural, ölçekteki maddelerin her biri için minimum 10 katılımcı analizinin gerekliliği yönündedir (Kline, 1994; Field, 2009). Ölçeğin geliştirilmesi aşamasında gerçekleştirilecek olan analizlerin duyarlılığının yüksek olabilmesi katılımcı sayısının fazla olmasıyla mümkündür.

Bilgi Güvenliği ve Etik Farkındalığı Ölçeği (BGEFÖ)'nde 37 madde yer almakta olup ölçeğin 621 öğrenci üzerinde uygulanması gerçekleştirilmiştir. Yapılan bu çalışmada örneklem büyüklüğü belirlenirken, örneklem büyüklüğünün belirlenmesi hususundaki görüşler göz önünde bulundurularak, ölçekte yer alan her bir maddeye 10'dan fazla öğrencinin çalışma grubuna katılımının sağlanması gerçekleştirilmiştir. Çalışmaya katılan öğrencilere ilişkin betimsel veriler Tablo 3.1'de verilmiştir.

Tablo 3.1: Pilot uygulamaya katılanların cinsiyetlerine göre dağılımları.

	Sınıf Düzeyi									
	5		**6**		**7**		**8**		**Toplam**	
Cinsiyet	**n**	**%**	**n**	**%**	**n**	**%**	**n**	**%**	**n**	**%**
Kız	89	14,3	92	14,8	55	8,8	72	11,6	308	49,6
Erkek	107	17,2	76	12,2	67	10,8	63	10,2	313	50,4
Toplam	196	31,6	168	27,1	122	19,6	135	21,7	621	100

Tablo 3.1'e bakıldığında; ölçek geliştirme sürecine katılan öğrencilerin %49,6'sı (308 öğrenci) kız, %50,4'ünün (313 öğrenci) erkek öğrencilerden oluştuğu görülmektedir. Öğrencilerin sınıf düzeylerine göre dağılımları incelendiğinde %31,6'sının (196 öğrenci) 5.sınıf, %27,1'inin (168 öğrenci) 6.sınıf, %19,6'sının (122 öğrenci) 7.sınıf ve %21,7'sinin

(135 öğrenci) 8.sınıf öğrencilerinden oluştuğu görülmektedir.

3.3. Bilgi Güvenliği ve Etik Farkındalığı Ölçeğinin Geliştirilmesi Süreci

Bireylerin bilgi güvenliğine ve etik konularındaki farkındalıkları günümüzde çok önem kazanmıştır. Bu nedenle de bu konulardaki farkındalıkların daha küçük yaşlarda hangi düzeyde olup olmadığına yönelik olarak çalışmamız ortaokul seviyesindeki öğrencilerle gerçekleştirilmiştir. Ortaokul öğrencilerinin Bilgi Güvenliği ve Etik Farkındalığı Ölçeği (BGEFÖ), ortaokul seviyesindeki öğrencilerin bilgi güvenliği ve etik farkındalıklarını ölçmek amacıyla geliştirilmiştir.

Ölçek geliştirme amaçlı olan çalışmalar, deneysel ya da kuramsal süreçlerle gerçekleştirilir (Yurdagül, 2005). Deneysel süreçte ölçek geliştirme için alanyazın ya da uzman görüşü yaklaşımları sayesinde aday ölçek formu elde edilir. Hedef kitle olarak belirlenen gruba benzer özelliklerde olan bir örneklem grubu üzerinde pilot çalışması yapılarak ölçek maddeleri hakkında psikometrik özellikler tespit edilerek uygun görülen maddelerle ölçek oluşturulur. Bu nicel süreç büyük örneklem grupları ve faktör analizinin yapılmasını gerektirmektedir. Bu araştırmada ölçme aracının geliştirilmesi için Karasar (2004) ve Balcı (2009) tarafından tavsiye edilen yol haritası izlenmiştir. Buna göre; madde havuzu oluşturma aşaması, oluşturulan madde havuzunun uzman görüşüne sunulması, uzman görüşleri sonrasında elde edilen formun ön denemsinin yapılması, elde edilen verilerle faktör analizinin yapılması ve güvenirlik hesaplamalarının yapılması gerçekleştirilmiştir. Ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalığı ölçeği (BGEFÖ), maddeleri yazılırken birincil olarak bilgi güvenliği ve etik farkındalığına yönelik olarak alanyazın incelemesi yapılmıştır. Bilgi güvenliği ve etik farkındalığına yönelik kategoriler ve maddeler oluşturulurken alan yazında var olan ölçekler ve yapılan çalışmalar incelenmiştir. MEB Talim ve Terbiye Kurulu Başkanlığı'nın 28/05/2013 tarihli ve 22 sayılı kararına göre (TTKB, 2013); ortaokul kademesinde 5 ve 6. sınıf öğrencileri Bilişim Teknolojileri ve Yazılım Dersini görmektedirler. Bu nedenle de Bilişim Teknolojileri ve Yazılım ders içerikleri göz önünde bulundurularak; Kişisel Verilerin Korunumu Kanununda bireysel kullanıcılar için üzerinde hassasiyetle durulan noktalar ölçek maddeleri yazılırken özellikle dikkate alınmıştır.

Alanyazın taraması ve ders içerikleri incelenip ortaokul öğrencilerinin bilgi güvenliği ve etik konularında yaygın olarak öğrencilerden yapması beklenen davranışlardan oluşan 37

maddenin yeraldığı madde havuzu oluşturulmuştur. Bu oluşturulan madde havuzundaki her bir madde hakkında Bilgisayar ve Öğretim Teknolojileri alnında uzman olan 5 akademisyenin görüşleri alınmıştır. Her bir maddenin amaca uygunluğu ve dil yönünden açık ve anlaşılır olup olmadığı incelenmiş olup maddelerde gerekli düzenlemeler gerçekleştirilmiştir. Bilgi Güvenliği ve Etik Farkındalığı Ölçeği (BGEFÖ), öğrencilerin ölçekte yeralan maddelere katılma düzeylerini belirlemek için "Kesinlikle Katılmıyorum (1)", "Katılmıyorum (2)", "Kararsızım (3)", "Katılıyorum (4)" ve "Kesinlikle Katılıyorum (5)" şeklinde beşli likert tipi derecelendirme ölçeği formatında hazırlanmıştır. Karasar (2005)'a göre bir ölçek için en önemli geçerlik ölçütleri kapsam geçerliği, uygulama geçerliği ve yapı geçerliğidir.

3.3.1 Verilerin Faktör Analizine Uygunluğunun Belirlenmesi

Ölçek geliştirme çalışmalarında uygulama sonucunda elde edilen verilerden yola çıkarak faktör analizi yapılarak ölçeğe son hali verilmeye çalışılır. Fakat ölçeğin uygulamasından elde edilen verilerin faktör analizi yapılması için uygun olup olmadığı hakkında bilgi sahibi olabilmek için Kaiser-Meyer-Olkin (KMO) Testi ve Barlett Küresellik Testi yapılması gerekmektedir. Kaiser-Meyer-Olkin (KMO) katsayısı ulaşılan örneklem büyüklüğünün uygunluk ölçüsüdür. KMO katsayısı, uygulama sonucunda elde edilen verilerin örneklem büyüklüğünün yeterince büyük ve uygun olup olmadığının tespit edilmesinde bir ölçüt olarak kullanılmaktadır. KMO katsayısı 0-1 aralığında bir değer alabilir. KMO değerinin yüksek olması, ölçekte yer alan her bir değişkenin diğer değişkenler tarafından çok iyi bir şekilde yordanabileceği anlamına gelmektedir (Field, 2009).

Hesaplanan KMO değeri Hutcheson ve Sofroniou, (1999)'ya göre; 0,5-0,7 arasında olanları vasat, 0,7-0,8 arasında olanları iyi, 0,8-0,9 arasında olanları çok iyi ve 0,9 üzerinde olanları süper olarak nitelendirmiştir. Huck (2012), KMO değerinin 0,6 ve üzerinde olması gerekliliğini vurgulamıştır. Karasar (2010) KMO değerinin 0,5 üzerinde olması gerektiğini söylemektedir. Tabachnick ve Fidell (2015) gerçekleştirilmek istenen faktör analizi için KMO katsayısının 0,6'nın üstünde olması gerektiğini söylemektedir. Kaiser (1974), KMO değerinin 0,5-0,7 arasında olduğunda orta, 0,7-0,8 arasında olduğunda iyi, 0,8-0,9 arasında olduğunda çok iyi ve 0,9 üzerinde olduğunda mükemmel şeklinde sınıflandırılmaktadır. 0,5 değeri KMO için kabul edilebilir sınır olarak belirtilmektedir. Ayrıca bu değerin altında bir sonuç ile karşılaşıldığında faktör analizine devam edebilmek için örneklem büyüklüğünün

artırılması ya da değişkenlerin azaltılması gerekmektedir (Kaiser, 1974).

Barlett Küresellik Testi, ölçeği oluşturan değişkenler arasında ilişki bulunup bulunmadığını kısmi korelasyonlar temeline dayanarak inceler (Büyüköztürk, 2015). Ölçekten elde edilen veriler için hesaplanan ki-kare istatistiğinin anlamlı çıkıyor olması ve Barlett Testinin sonucunun anlamlı çıkıyor olması veri matrisinin faktör analizi için uygun ve normalliğin sağlanmış olmasına kanıt olarak gösterilebilir. Bilgi Güvenliği ve Etik Farkındalığı Ölçeği (BGEFÖ)'nin açımlayıcı faktör analizine uygunluğunun saptanabilmesi amacıyla Kaiser-Meyer-Olkin (KMO) Testi katsayı hesaplaması ve Barlett Küresellik Testi yapılmıştır. Hesaplanan KMO ve Barlett Küresellik testi sonuçları Tablo 3.2'de verilmiştir.

Tablo 3.2. KMO ve Barlett Küresellik Testleri Sonuçları

Kaiser-Meyer-Olkin Örneklem Yeterliği Testi		.932
Barlett Küresellik Testi	Ki-Kare (x^2)	3792.329
	df	136
	Sig.	.000

Tablo 3.2 incelendiğinde; BGEFÖ'nün hesaplanan KMO katsayısı değeri .932 olduğu görülmektedir. Kaiser (1974), Tavşancıl (2005) ve Çokluk ve arkadaşları (2010)'na göre; hesaplanan KMO Testi katsayısının .50'den küçük olması durumu kabul edilebilir bir sonuç olmamakla birlikte .90 ve üzeri hesaplanan KMO değeri için mükemmel nitelikte bir değerdir. Barlett Küresellik testi analizi sonucu .01 düzeyinde anlamlı bulunmuştur [χ^2=3792.329; df=136; p=.000]. Hesaplanan KMO değeri ve Barlett Küresellik testi sonuçlarına göre faktör analizi yapılabilmesi için uygun koşulların sağlandığı sonucuna varılmıştır. Buradan hareketle faktör analizinin diğer bir aşaması olan Açımlayıcı Faktör Analizi (AFA) aşamasına geçilmiştir.

3.3.2 Açımlayıcı Faktör Analizinin Yapılması

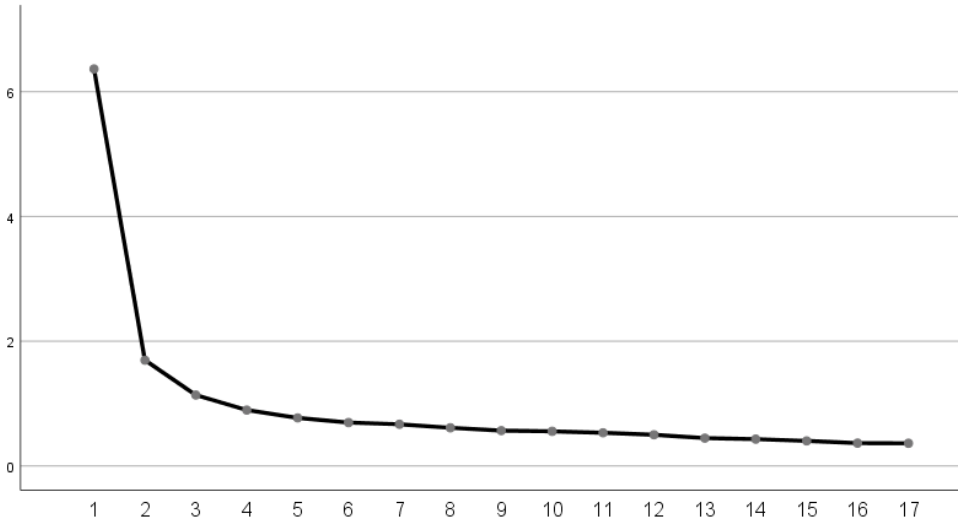
Açımlayıcı faktör analizi bilimsel araştırmalarda ve sosyal bilimlerde sıklıkla kullanılan bir yöntemdir ölçek geliştirme çalışması yürüten araştırmacılar, ölçeklerin yapısını anlamak, ölçeği oluşturacak olan faktörlerin kendi aralarındaki ilişkileri keşfetmek ve ölçme aracını geliştirebilmek için bu analiz yöntemini kullanırlar (Fabrigar, Wegener & MacCallum, 1999). Açımlayıcı faktör analizi, ölçekte bulunan değişkenlerden korelasyon veya kovaryans

matrisi ile birleştirerek birbiriyle ilişkisi bulunanları birleştirerek sayıca daha az olan ve birbirinden bağımsız gizil değişkenlerle oluşturmaktadır (Özdamar, 2013; Fidell, 2015). Açımlayıcı faktör analizi yardımıyla ölçeğin alt boyutlarının ve hangi maddelerin hangi alt boyuta dahil olduğu hakkında bilgi edinilebilir (Tavşancıl, 2014). AFA ile ölçme aracında yer alan faktör yükleri, faktör varyansı ve toplam varyansın ne kadar açıklandığı ortaya çıkarılır (Field, 2013). Faktör yükleri, değişkenlerin ortaya çıkarılan belirli faktörlerle olan ilişkisini gösterirken, faktörlerin varyansı ise veri setindeki değişkenliğin hangi miktarda açıklandığını gösterir (Costello & Osborne, 2005). Ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalıklarını tespit edebilmek amacıyla hazırlanan BGEFÖ'ye ait faktör yapısını ortaya çıkarılabilmek ve ölçekteki maddelerin bu faktörler altında uygunluğunun tespit edilebilmesi için açımlayıcı faktör analizi yapılmıştır.

Ölçek geliştirme çalışmalarının en önemli aşamalarından biri olan madde havuzu oluşturma aşamasında birçok madde aynı ölçeğin içerisinde yazılmaktadır. Bu ölçek maddelerinin aynı davranış ya da durumu ölçmeye yönelik olup olmadığı veya birbiriyle çelişen maddeler madde havuzunda yer alabiliriler. Bu gibi durumların önüne geçilebilmesi için açımlayıcı faktör analizi sayesinde maddelerin ölçekten atımı söz konusu hale gelmektedir. Ölçekten madde ya da maddelerin atılması, istatistiksel yöntemler ve teorik dayanaklara göre gerçekleştirilmektedir. Madde faktör yüklerine, ölçeğin yapısına ve teorik temellere bakılarak ölçekten madde atım işlemi gerçekleştirilir (Field, 2013). Maddelerin düşük faktör yüküne sahip olması ve istenilen faktörle ilişkisinin olmaması durumunda bu maddeler ölçekten çıkarılabilir (Costello & Osborne, 2005). Anlamsız ve düşük faktör yüküne sahip maddelerin ölçekten çıkarılmasıyla ölçek yapısı daha tutarlı ve daha iyi bir kavramsal temele sahip hale gelmektedir (Fabrigar, Wegener & MacCallum, 1999). Bu şekilde ölçeğin güvenirliği ve geçerliği artırılmış olunur.

Ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalığına yönelik hazırlanan ölçeğe ait faktör yapısının ortaya çıkarılması ve ölçekteki her maddenin ortaya çıkan faktörler altındaki uygunluğunun tespit edilebilmesi amacıyla yapılan AFA'da, maddelerin ölçekte kalıp kalmamasına yönelik karar verilmesinde faktör yük değerinin alt sınırı .30 değeri ölçüt olarak belirlenmiştir. Faktör yük değerleri hakkında alan yazında farklı ölçütler yer almaktadır. Kline (1994)'a göre madde yük değeri işarete bakılmaksızın .30 ile .60 arasında olmalı, Tabachnick ve Fidell (2007)'e göre .32 üzerinde olmalı, Stevens (2002)'a göre .30 üzerinde olmalıdır. BGEFÖ'nün faktör sayısının belirlenmesinde dikkate alınan en önemli ölçütlerden biri de öz değer (eigen value)'dir. Öz değer, bir faktörle ilişkili maddelerin faktör

yüklerinin kareleri toplamıdır (Can, 2014). Öz değer her bir faktörün açıklanan toplam varyansın hesaplanmasında kullanılan bir katsayıdır. Öz değer hesaplamasına göre 1 veya 1'den büyük değerlere sahip olan faktörlerin hazırlanan ölçek için önem arz ettiği ve ölçekte yer alması gereken temel faktörlerden olduğu dikkate alınması gerekmektedir (Kaiser, 1960). Buradan hareketle faktör sayısına karar verilirken öz değerlerinin 1'den büyük olmasına dikkat edilmelidir (Thompson, 2008; Güriş & Astar, 2015). Geliştirilmek istenen ölçeğin açımlayıcı faktör analizi sonuçlarına göre tespit edilen faktörlerin açıklanan varyans oranının %60 üzerinde (Alpar, 2013) olması beklenirken bazı kaynaklara göre de %90 üzerinde olması gerekmektedir (Karasar, 2010). Tabacknick ve Fidell (1996)'e göre açıklanan varyansın tek faktörlü desenlerde %30 olması yeterlidir. Çok faktörlü desenlerde ise açıklanan varyans oranının daha yüksek olması beklenir (Büyüköztürk, 2015). Güriş ve Astar (2015)'a göre açıklanan varyans oranının %50 olması kabul edilebilir olarak görülmektedir. Açımlayıcı faktör analizi kapsamında faktör öz değerlerine ait çizgi grafiği Şekil 3.1'de verilmiştir.



Şekil 3.1. Faktör Öz Değerlerine İlişkin Çizgi Grafiği.

Şekil 3.1'de görüldüğü üzere BGEFÖ ait maddelerin 3 ana faktör altında olduğu ve bu faktörlerin öz değerlerinin 1'den büyük oldukları görülmektedir. Bu üç faktörün ölçeğe ilişkin olarak açıkladığı varyansın %54,10 olduğu tespit edilmiştir.

Araştırma kapsamında gerçekleştirilen AFA sonucunda maddelerin yer aldıkları faktörlerdeki yük değerleri incelenmiştir. Düşük yük değerine sahip olan maddeler ile birden fazla faktörde birbirine yakın faktör yük değerlerine sahip olan maddelerin ölçekten

çıkarılmasına karar verilmiştir. Maddeler ölçekten çıkarılırken 0,30 yük değerinden düşük olması kriteri göz önünde bulundurulmasının yanı sıra maddenin kuramsal olarak faktörle olan uygunluğu da göz önünde bulundurulmuştur. AFA öncesinde belirlenmiş olan ölçütler doğrultusunda gerçekleştirilen açımlayıcı faktör analizi neticesinde 20 maddenin BGEFÖ'den çıkarılmasına karar verilmiş olup ölçekte geri kalan 17 maddenin 3 faktör altında toplandığı bir yapının varlığı tespit edilmiştir. Tablo 3.3'te Bilgi Güvenliği ve Etik Farkındalığı Ölçeği'ne ait açımlayıcı faktör analizi sonucunda elde edilen faktör yapısı, her bir faktöre ilişkin özdeğeri (eigen value), her faktörün ölçeğe dair açıklayabildiği varyans oranları ve faktörlerde yer alan maddelerin varimax dik döndürme yöntemine göre ortaya çıkarılan faktör yük değerleri verilmiştir.

Tablo 3.3. Bilgi Güvenliği ve Etik Farkındalığı Ölçeği Faktör Yükleri Matrisi.

		Faktör Yük Değerleri		
Faktörler	**Maddeler**	**1**	**2**	**3**
Etik	M31	0,794		
	M32	0,738		
	M33	0,729		
	M28	0,724		
	M35	0,721		
	M34	0,704		
	M36	0,674		
	M30	0,670		
	M29	0,667		
Veri Güvenliği	M27		0,721	
	M25		0,689	
	M19		0,681	
	M15		0,636	
	M20		0,422	
Kullanıcı Güvenliği	M4			0,834
	M17			0,630
	M5			0,611
Öz Değer		6,365	1,696	1,137
Açıklanan Varyans		28,614	14,525	10,961
Açıklanan Toplam Varyans (%): 54,100				

(0,30'dan düşük yük değerleri tabloda gösterilmemiştir.)

Tablo 3.3 incelendiğinde ölçeğin faktörlerinde yer alan maddelerin faktör yük değerlerinin .422 ile .834 aralığında yer aldıkları görülmektedir. Tablo 3.3'te faktörlerdeki maddelerin faktör yük değerleri verilirken .30 değerinin altında kalan değerler Tablo 3.3'te verilmemiştir. Faktör yük değerleri ve dağılımlarına bakıldığında BGEFÖ'nin birinci alt boyutunu oluşturan faktörde faktör yük değerleri .667 ile .794 aralığında bulunan 9 madde yer almaktadır. İkinci alt boyutunu oluşturan faktörde faktör yük değerleri .422 ile .721 aralığında bulunan 5 madde yer almaktadır. Üçüncü alt boyutunu oluşturan faktörde faktör yük değerleri .611 ile .834 aralığında bulunan 3 madde yer almaktadır. Faktörlere dair hesaplanan öz değerler incelendiğinde ise birinci faktörde 6,365, ikinci faktörde 1,696 ve üçüncü faktörde ise 1,137 olduğu görülmektedir.

Tüm faktörler açıklanan toplam varyansın %54,100'lük kısmını açıkladıkları görülmektedir. Birinci faktör, açıklanan toplam varyansın %26,614'ünü açıklamaktadır. İkinci faktör, açıklanan toplam varyansın %14,525'ini açıklamaktadır. Üçüncü varyans, açıklanan toplam varyansın %10,961'ini açıklamaktadır. Alan yazın, uzman görüşleri ve madde içerikleri dikkate alınarak birinci faktöre "Etik", ikinci faktöre "Veri Güvenliği" ve üçüncü faktöre ise "Kullanıcı Güvenliği" isimlendirmeleri yapılmıştır.

BGEFÖ için yapılan açımlayıcı faktör analizinden sonra ortaya çıkarılmış olan alt boyutlar arasındaki ilişki araştırılmıştır. Alt boyutlar ve ölçeğin tamamı arasındaki korelasyon katsayıları Tablo 3.4'te verilmiştir.

Tablo 3.4. Ölçeğin Alt Boyutları Arasındaki Korelasyon Katsayıları.

	Alt Boyutlar			
	Etik	**Veri Güvenliği**	**Kullanıcı Güvenliği**	**BGEFÖ**
Etik	1	0,464**	0,461**	0,895**
Veri Güvenliği		1	0,460**	0,763**
Kullanıcı Güvenliği			1	0,700**
BGEFÖ				1

(**p<0,01 düzeyinde anlamlıdır.)

Tablo 3.4 incelendiğinde BGEFÖ'nün alt boyutları arasındaki korelasyon katsayılarının 0,460 ile 0,464 arasında değiştiği görülmüştür. BGEFÖ'nün alt boyutları arasındaki ilişkilerin 0,01 düzeyinde anlamlı olduğu ve alt boyutlar arasındaki ilişkilerin pozitif yönlü

olduğu görülmüştür. Alt boyutların kendi aralarındaki ilişkilerin 0,3-0,7 arasında olmasından dolayı ise alt boyutlar arasındaki ilişkilerin orta düzeyde olduklarını görülmektedir. Etik alt boyutu ile BGEFÖ arasındaki korelasyon katsayısı 0,895, veri güvenliği ile BGEFÖ arasındaki korelasyon katsayısı 0,763 ve kullanıcı güvenliği ile BGEFÖ arasındaki korelasyon katsayısının 0,700 olduğu yani korelasyon katsayılarının 0,5 üzeri ve alt boyutların BGEFÖ ile arasında doğrusal ilişkilerin olduğu görülmektedir.

3.3.3 Ölçme Aracının Güvenirliğinin Belirlenmesi

Ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalıklarını ortaya çıkarmak amacıyla hazırlanan BGEFÖ için ve alt boyutları için ayrı ayrı Cronbach Alfa (α) iç tutarlık katsayısı hesaplanmıştır. Tablo 3.5'te ölçeğin bütünü ve her bir alt boyut için hesaplanmış olan iç tutarlık katsayıları verilmiştir.

Tablo 3.5. Ortaokul Öğrencilerinin BGEFÖ Cronbach Alfa İç Tutarlılık Katsayıları.

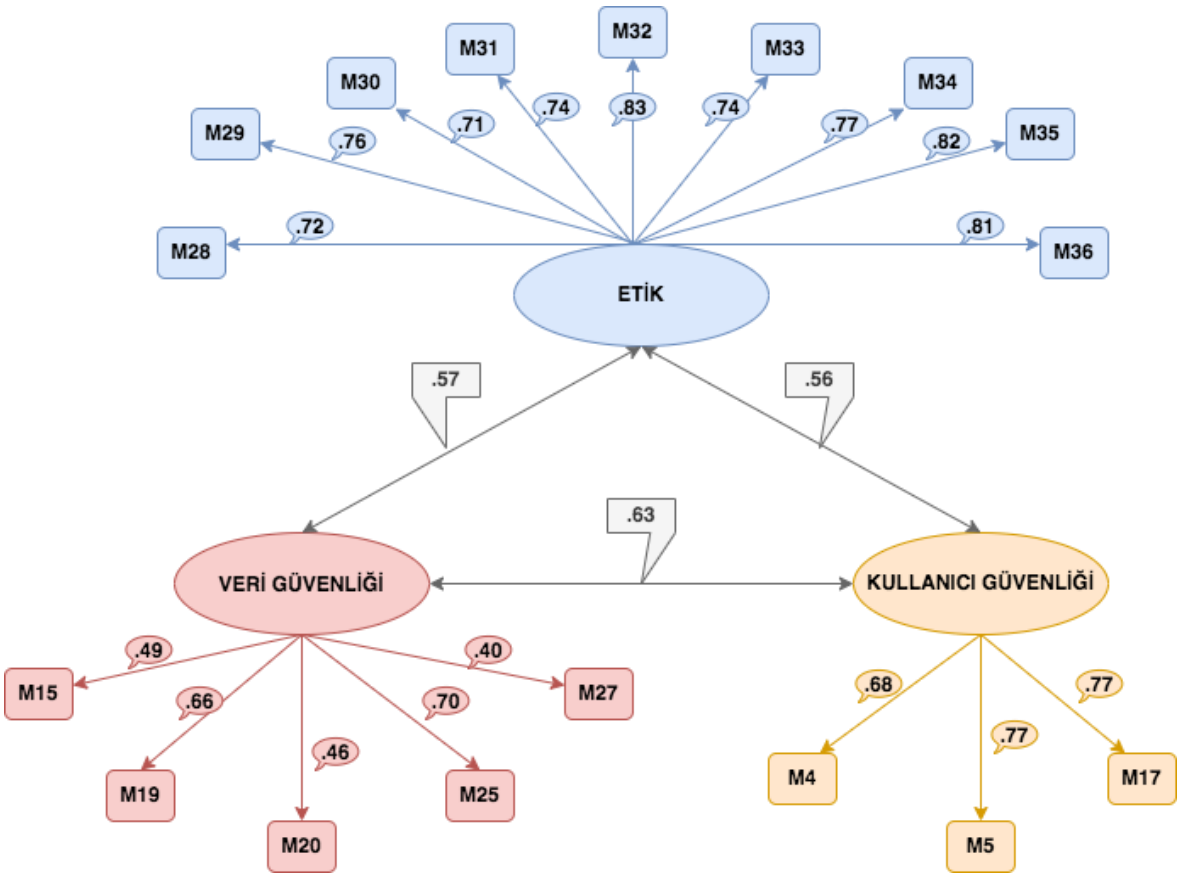
Alt Boyutlar	**Madde Sayısı**	**Cronbach Alfa (α)**
Etik	9	0,912
Veri Güvenliği	5	0,688
Kullanıcı Güvenliği	3	0,687
BGEFÖ	**17**	**0,896**

Tablo 3.5 incelendiğinde ortaokul öğrencilerine yönelik geliştirilen Bilgi güvenliği ve etik farkındalığı ölçeğinin bütününden elde edilen ölçümlerin iç tutarlılığı 0,896 olarak hesaplanmıştır. Güvenirlik hesaplamalarıyla ilgili alan yazın incelendiğinde Nunnally (1978) ve Büyüköztürk (2015) güvenirlik katsayısını 0,70 ve üzerinde olmasını önermektedir. 0,60-0,90 aralığında katsayıysa sahip olan ölçme araçları oldukça güvenilir olarak nitelendirilmektedir (Akt: Tavşancıl, 2006; Özdamar 1999). Geliştirilen ölçeğin veri güvenliği ve kullanıcı güvenliği alt boyutlarının güvenirlik katsayısı bu görüşler doğrultusunda oldukça güvenilir seviyede bulunmuştur. Etik alt boyutunun güvenirlik katsayısı 0,9 üzerinde olduğundan etik alt boyutu yüksek güvenirliğe sahip olduğu görülmektedir. BGEFÖ'nün güvenirlik katsayısına bakıldığında 0,896 olarak tespit edilmiştir. Elde edilen bu katsayı oldukça güvenilir seviyede olmakla birlikte yüksek güvenirlik sınırına çok yakın bir seviyededir.

3.3.4 Doğrulayıcı Faktör Analizinin Yapılması

Ortaokul öğrencilerinin bilgi güvenliği eve etik farkındalıklarının araştırılabilmesi için hazırlanan BGEFÖ, açımlayıcı faktör analizi, alan yazın ve uzman görüşleri dikkate alınarak 3 boyutlu olacak şekilde ortaya konulmuştur. AFA sonrası ortaya çıkan BGEFÖ'ye ait modelin yapı geçerliğini sınamak amacıyla doğrulayıcı faktör analizi yapılmıştır (Kline, 2000). Ulaşılan veriler ile yapılan analizler doğrultusunda oluşturulmuş olan modelin uyum iyiliğinin değerlendirilebilmesi için birçok ölçüm ve kriter dikkate alınmıştır.

Doğrulayıcı faktör analizi aşamasında modelin uyum indeksleri olarak; Ki-Kare ($\chi 2$) iyilik uyumu, İyilik uyum indeksi (GFI), Düzenlenmiş iyilik uyum indeksi (AGFI), Yaklaşık hataların ortalama karekökü (RMSEA), Artık ortalamaların karekökü (RMR), Standardize edilmiş anlık ortalamaların karekökü (SRMR), Karşılaştırmalı uyum indeksi (CFI) ve Normlaştırılmış uyum indeksi (NFI) değerleri incelenmiştir. Üç faktörden oluşan BGEFÖ yapısına ilişkin olarak gerçekleştirilen doğrulayıcı faktör analizi sonucunda elde edilen standart regresyon katsayıları (faktör yükleri) incelendiğinde; her bir madde için elde edilen faktör yüklerinin AFA'da ulaşılan katsayılarla benzer nitelikte olduğu tespit edilmiştir. Hazırlanmış olan model üzerinde herhangi bir modifikasyona gerek duyulmamıştır. Model için elde edilen uyum indeksleri χ^2 / sd=1,902 , NFI=0,914 , RMSEA=0,055, AGFI=0,902 , GFI=0,928 ve CFI=0,957 olarak bulunmuştur. Doğrulayıcı faktör analizi için elde edilmiş olan veriler Şekil 3.2'de sunulmuştur.



Şekil 3.2. BGEFÖ için DFA Sonuçları.

Alan yazında yer alan farklı görüşlere göre modele dair kabul edilebilir ve iyi değerlerin neler olduğu araştırılmıştır. Bu değerler ve geliştirilmiş olan ölçek modeli için elde dilen araştırma modelinin değeri Tablo 3.6'da verilmiştir (Brown, 2006; Jöreskog & Sörbom, 1993; Kline, 2011; Özdamar, 2013; Smith & McMillan, 2001; Sümer, 2000 ve Tabacknick & Fidell, 2015).

Tablo 3.6. BGEFÖ için DFA Uyum İyiliği İndeksleri.

Uyum İndeksleri	Araştırma Modelinin Değeri	Kabul Edilebilir Model Değerleri	İyi Model Değerleri
χ^2 / sd	1,902	≤ 5	≤ 2,5-3
RMSEA	0,055	≤ 0,10	≤ 0,05
AGFI	0,900	< 0,90	< 0,90
GFI	0,928	> 0,90	> 0,95
CFI	0,957	> 0,90	> 0,95
NFI	0,914	≥ 0,90	≥ 0,95
RMR	0,057	≤ 0,08	≤ 0,05

Tablo 3.6'ya bakıldığında; model için DFA sonucu elde edilen χ^2/sd, AGFI ve CFI uyum indekslerinin iyi model değerlerine sahip olduğu; RMSEA, GFI, NFI ve RMR uyum indekslerinin kabul edilebilir değerlere sahip oldukları görülmektedir. BGEFÖ için yapılmış olan DFA sonuçlarına göre model için ulaşılan uyum indekslerinin alanyazında yer alan görüşlere ve kriterlere göre kabul edilebilir düzeyde olduğu söylenebilir. Model için gerçekleştirilen analiz sonucunda ulaşılan ki-kare (χ^2) değeri istatistiksel olarak anlamlı bulunması BGEFÖ'ye ait modelin uygunluğunu gösteren diğer uyum indekslerini desteklemektedir (χ^2=214,901; *p*=0,00).

3.4. Verilerin Toplanması ve Analizi

Ölçek geliştirme sürecinin ikinci aşamasında madde havuzu oluşturulup maddeler hakkında uzman görüşleri alındıktan sonra örnekleme dahil edilen okullarda öğrencilere hazırlanan bu ölçeğin uygulanabilmesi için Bartın Milli Eğitim Müdürlüğü'nden gerekli izinlerin alınabilmesi için başvuru yapılmıştır. Başvuru sonucunda Bartın ili merkez ilçeye bağlı ortaokullar ölçek geliştirme çalışması için gerekli uygulamaların yapılabilmesi için izinler alınmıştır. Öğrencilere 66 maddelik BGEFÖ uygulaması sadece merkez ya da sadece köy okullarında yapılmamıştır. Köy ve merkez okullardan eşit sayıda okulda uygulama gerçekleştirilmiştir. Hazırlanan veri toplama aracı elektronik ortamda öğrencilere sunulmuştur. Öğrencilerin BGEFÖ'ni doldurabilmeleri için bilişim teknolojileri sınıfları kullanılmıştır. Her öğrenci için yeterli zaman verilerek ve tüm maddelere cevaplar alındığından 621 öğrenciye uygulanan formdan elde edilen verilerin tamamı istatistiksel

analize alınmıştır.

Ölçek geliştirme çalışmaları için yapılması gereken Açımlayıcı Faktör Analizi (AFA) ve Doğrulayıcı Faktör Analizi (DFA)'nin farklı örneklem grupları üzerinde gerçekleştirilen uygulamalardan elde edilen verilerle gerçekleştirilmesi gerekmektedir (Çakmak vd., 2014). Faktör analizi tüm veri yapıları için uygunluk sağlamayabilir. Uygulamalardan elde edilen verilerin faktör analizi için uygun olup olmadığı Kaiser-Meyer-Olkin (KMO) katsayısı ve Barlett küresellik (Sphericity) testleri ile incelenmelidir. KMO katsayısının 0,60'tan yüksek çıkması beklenir. Barlett testi, kısmi korelasyon temelinde değişkenler arasında ilişki olup olmadığını inceler. Barlett testinin sonucunun anlamlı çıkması puanların normal dağılımda olduğu bilgisini verir (Büyüköztürk, 2015). Bu şartların sağlanması halinde faktör analizi gerçekleştirilebilmektedir.

Bilgi Güvenliği ve Etik Farkındalık Ölçeği (BGEFÖ)'nin geçerlik ve güvenirlik çalışmalarının yapılabilmesi için gerekli olan örneklem büyüklükleri hakkındaki farklı görüşler göz önünde bulundurularak 621 ortaokul öğrencisine uygulaması gerçekleştirilmiştir. 621 katılımcı, Açımlayıcı Faktör Analizi (AFA) için 421 ve Doğrulayıcı Faktör Analizi (DFA) için 200 kişilik öğrencilerden oluşmak üzere iki alt gruba bölünmüştür. Hazırlanan ölçeğin kapsam geçerliği uzman görüşleri doğrultusunda kontrol edilmiştir. Yapı geçerliğinin değerlendirilmesi amacıyla araştırmaya katılan katılımcılardan elde edilen verilerle geliştirilmek istenen ölçeğin faktör analizi işlemi gerçekleştirilmiştir.

Araştırmanın alt problemlerine yönelik olarak ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalığı düzeylerinin nasıl olduğunu belirlemek amacıyla BGEFÖ faktör puanları ile betimsel istatistiksel hesaplamalar yapılmıştır. Öğrencilerin bilgi güvenliği ve etik farkındalık düzeylerinin demografik özellikler yönünden anlamlı farklılık olup olmadığını incelemek için parametrik testler kullanılmıştır. Buradan hareketle iki grubun karşılaştırılması amacıyla t-testi kullanılırken, ikiden fazla grubun birbirleriyle karşılaştırılmasında ANOVA (Tek yönlü varyans analizi) kullanılmıştır. Elde edilen verilerin analizinde anlamlılık düzeyi p=.05 olarak kabul edilmiştir. Bu araştırmada, ortaokul öğrencileri için hazırlanan ve verileri toplanan ölçme aracımızdan elde edilen verilerin analizinde SPSS (İstatistik paket programı) kullanılmıştır.

4. BULGULAR VE TARTIŞMA

Bilgi Güvenliği ve Etik Farkındalığı Ölçeği'nin geliştirilmesi bu araştırmanın birincil ve asıl amacını oluşturmaktır. İkincil amaç ise oluşturulan BGEFÖ sayesinde ortaokul öğrencilerinden (5, 6, 7 ve 8 sınıf) elde edilen veriler ışığında öğrencilerin bilgi güvenliği ve etik farkındalık düzeylerinin nasıl olduğunun ortaya konulmasıdır. Bu araştırmada "Bilgi ve iletişim teknolojilerini kullanan ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalık durumları nedir?" sorusuna çeşitli boyutlarda cevaplar aranmıştır. Bu amaç doğrultusunda ölçeğe son hali verildikten sonra tarama amaçlı 921 ortaokul öğrencisine BGEFÖ uygulanmıştır. Bu bölümde araştırmanın alt problemlerine yönelik istatistiksel verilerin analizi yapılarak açıklanmıştır.

Araştırmanın alt problemleri:

1. Öğrencilerin bilgi güvenliği ve etik farkındalık düzeyleri nasıldır?
2. Öğrencilerin bilgi güvenliği ve etik farkındalık düzeyleri yaş, cinsiyet, sınıf düzeylerine göre değişim göstermekte midir?
3. Öğrencilerin bilgi güvenliği ve etik farkındalık düzeyleri anne-baba eğitim düzeylerine göre anlamlı farklılıklar göstermekte midir?

4.1. Birinci Alt Probleme İlişkin Bulgular ve Yorum

Araştırmanın birinci alt problemi olan "Öğrencilerin bilgi güvenliği ve etik farkındalık düzeyleri nasıldır?" sorusuna yönelik olarak ortaokul öğrencilerinin BGEFÖ'den aldıkları puanların betimsel istatistikleri hesaplanmıştır. Çalışmaya katılan öğrencilerin BGEFÖ'den elde ettikleri puanlar Tablo 4.1'de verilmiştir.

Tablo 4.1. Ortaokul Öğrencilerinin BGEFÖ Puanları Betimsel İstatistikleri.

Faktör	**N**	**Min**	**Max**	$\bar{X}$	$\bar{X}$ / **Madde**	**ss**
Kullanıcı Güvenliği (3 Madde)	921	3	15	12,28	4,09	2,67
Veri Güvenliği (5 Madde)	921	5	25	17,38	3,48	3,89
Etik (9 Madde)	921	9	45	38,43	4,27	6,52
BGEFÖ (17 Madde)	921	17	85	68,09	4,01	10,67

Tablo 4.1'e bakıldığında araştırmaya katılan ortaokul öğrencilerinin Bilgi Güvenliği ve Etik

Farkındalığı Ölçeği'nden aldıkları puanların ortalamalarının madde sayısına bölümüyle elde edilen ortalamalar incelendiğinde; veri güvenliği faktörüne ait ortalamanın (3,48) en düşük, etik faktörüne ait ortalamanın (4,27) olduğu görülmüştür. Ölçek genelinden elde edilen ortalamanın 4,01 olduğu görülmüştür. Buradan hareketle, ortaokul öğrencilerinin veri güvenliği alt boyutuna yönelik farkındalıklarının daha düşük, etik alt boyutuna yönelik farkındalıklarının daha yüksek olduğu sonucuna varılabilir.

BGEFÖ'den elde edilen puanlar incelendiğinde ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalıklarının yüksek düzeyde, fakat veri güvenliği faktörü özelinde incelendiğinde orta düzeyde olduğu görülmüştür. Araştırmada elde edilen bu sonuç, Tekerek ve Tekerek (2013)'in yaptığı çalışmayla benzer sonuçlar göstermektedir. Ortaokul seviyesinde Beder ve Ergün (2015), Özen Serter (2021)'in yapmış oldukları çalışmalarda bilgi güvenliği farkındalıklarının orta ve düşük seviyede olduğu görülmüştür. Lise, lisans seviyesi ve diğer yetişkin seviyelerinde yapılan çalışmalar (Hacımustafaoğlu, 2019; Slusky & Partow, 2012; Karaoğlan Yılmaz vd., 2017; Dönmez, 2019) incelendiğinde bilgi güvenliği kapsamına giren alt boyutlarda yüksek, etik farkındalığı alt boyutuna girebilecek olan alt boyutlarda orta ve düşük düzeyde kaldıkları görülmektedir.

4.2. İkinci Alt Probleme İlişkin Bulgular ve Yorum

Araştırmanın ikinci alt problemi olan "Öğrencilerin bilgi güvenliği ve etik farkındalık düzeyleri yaş, cinsiyet, sınıf düzeylerine göre değişim göstermekte midir?" sorusuna yönelik olarak ortaokul öğrencilerinin BGEFÖ'den aldıkları puanların cinsiyetlerine göre anlamlı bir farklılık gösterip göstermediğini belirlemek için ilişkisiz örneklemler t-testi yapılmıştır. Tablo 4.2'de ortaokul öğrencilerinin BGEFÖ'den elde edilen puanlarının cinsiyetlere göre t-testi sonuçları verilmiştir.

Tablo 4.2. Ortaokul Öğrencilerinin BGEFÖ'den Elde Edilen Puanlarının Cinsiyetlere Göre t-testi Sonuçları.

Faktör	Cinsiyet	N	$\bar{X}$	ss	t	sd	p
Kullanıcı Güvenliği	Kız	503	12,37	2,65	1.116	919	.265
	Erkek	418	12,17	2,68			
Veri Güvenliği	Kız	503	17,19	3,69	-1.556	919	.120
	Erkek	418	17,59	4,10			
Etik	Kız	503	38,83	6,22	2.045	919	.041*
	Erkek	418	37,94	6,83			
BGEFÖ	Kız	503	68,39	9,99	0.958	919	.338
	Erkek	418	67,71	11,43			

(*p≤.05 anlamlılık düzeyi esas alınmıştır.)

Tablo 4.2 incelendiğinde, kız öğrencilerin kullanıcı güvenliği farkındalıkları ortalamasının ($\bar{X}_{\text{kız}} = 12,37$), erkeklerin kullanıcı güvenliği farkındalıkları ortalamasından ($\bar{X}_{\text{erkek}} = 12,17$) daha yüksek olduğu görülmüştür. Ortaokul öğrencilerinin BGEFÖ Kullanıcı Güvenliği faktör puanları ile yapılan ilişkisiz örneklemler t-testi sonuçlarına göre cinsiyete göre anlamlı farklılık göstermemektedir [$t_{(919)} = 1.116$, $p > .05$]. Kullanıcı güvenliği ile ilgili elde edilen bu sonuç, Tekerek ve Tekerek'in 2013 yılında yapmış olduğu çalışmayla benzer niteliktedir.

Tablo 4.2'ye göre, kız öğrencilerin veri güvenliği farkındalıkları ortalamasının ($\bar{X}_{\text{kız}} = 17,19$), erkeklerin kullanıcı güvenliği farkındalıkları ortalamasından ($\bar{X}_{\text{erkek}} = 17,59$) daha düşük olduğu görülmüştür. Ortaokul öğrencilerinin BGEFÖ Veri Güvenliği faktör puanları ile yapılan ilişkisiz örneklemler t-testi sonuçlarına göre cinsiyete göre anlamlı farklılık göstermemektedir [$t_{(919)} = -1.556$, $p > .05$].

Tablo 4.2'ye bakıldığında, kız öğrencilerin etik farkındalıkları ortalamasının ($\bar{X}_{\text{kız}} = 38,83$), erkeklerin etik farkındalıkları ortalamasından ($\bar{X}_{\text{erkek}} = 37,94$) daha yüksek olduğu görülmüştür. Ortaokul öğrencilerinin BGEFÖ Etik faktör puanları ile yapılan ilişkisiz örneklemler t-testi sonuçlarına göre cinsiyete göre anlamlı farklılık göstermektedir [$t_{(919)} = -2.045$, $p < .05$]. Ulaşılan bu sonuç yapılan diğer çalışmalarla (Salman, 2019; Özdemir, 2012; Gökçearslan, Günbatar & Berikan, 2015; Özen Serter, 2021) benzerlik gösterir niteliktedir.

Güldüren, Çetinkaya ve Keser (2016) ile Talan ve Aktürk (2021), erkeklerin bilgi güvenliği farkındalıklarının kızlara oranla daha yüksek olduğu sonucunu bulmuşlardır.

Tablo 4.2'ye bakıldığında, kız öğrencilerin BGEFÖ ortalamasının ($\overline{X}_{\text{kız}} = 68{,}39$), erkeklerin BGEFÖ ortalamasından ($\overline{X}_{\text{erkek}} = 67{,}71$) daha yüksek olduğu görülmüştür. Ortaokul öğrencilerinin BGEFÖ puanları ile yapılan ilişkisiz örneklemler t-testi sonuçlarına göre cinsiyete göre anlamlı farklılık göstermektedir [$t_{(919)} = .958$, $p < .05$].

Yapılan t-testi sonuçlarına göre kullanıcı güvenliği, veri güvenliği faktörleri cinsiyete göre anlamlı bir farklılık göstermemektedir. Etik faktörü ise cinsiyete göre anlamlı bir farklılık göstermekte olup BGEFÖ'nün tamamı cinsiyet yönünden anlamlı bir farklılık göstermemektedir. Bu bulgular tarama amaçlı olarak elde edilen verilerden yola çıkılarak ulaşılan sonuçları temsil etmektedir. Farklı araştırmalarda uygulama öncesi ve sonrası yani ön test – son test şeklinde yapılan tarama sonuçlarının farklılık gösterebilir.

Ortaokul öğrencilerinin BGEFÖ'den aldıkları puanların yaşlarına göre anlamlı bir farklılık gösterip göstermediğini belirlemek için ANOVA yapılmıştır. Tablo 4.3'te ortaokul öğrencilerinin BGEFÖ'den elde edilen puanlarının yaşlarına göre ANOVA sonuçları verilmiştir.

Tablo 4.3. Ortaokul Öğrencilerinin BGEFÖ'den Elde Edilen Puanlarının Yaşlarına Göre ANOVA Sonuçları.

Faktör	Yaş	N	$\bar{X}$	ss	F	p	Anlamlılık
Kullanıcı Güvenliği	11	340	12,50	2,77	1,41	.238	-
	12	254	12,17	2,55			
	13	201	12,22	2,46			
	14	126	11,99	2,88			
Veri Güvenliği	11	340	18,16	3,98	8,46	.000*	11>12 11>13 11>14
	12	254	17,18	3,56			
	13	201	16,57	4,02			
	14	126	16,92	3,71			
Etik	11	340	39,65	5,86	10,02	.000*	11>13 11>14 12>14
	12	254	38,56	6,09			
	13	201	37,50	7,04			
	14	126	36,32	7,41			
BGEFÖ	11	340	70,31	10,38	10,09	.000*	11>12 11>13 11>14
	12	254	67,92	9,50			
	13	201	66,30	10,89			
	14	126	65,23	12,08			

(*p≤.05 anlamlılık düzeyi esas alınmıştır.)

Tablo 4.3 incelendiğinde elde edilen verilerin analizi sonucunda ortaokul öğrencilerinin Kullanıcı Güvenliği faktöründen aldıkları puanların yaş düzeylerine göre anlamlı bir farklılık göstermediği görülmüştür ($F_{(3, 917)} = 1,41$; $p \geq .05$).

Ortaokul öğrencilerin Veri Güvenliği faktöründen aldıkları puanların yaşlara göre anlamlı bir farklılık gösterdiği görülmüştür ($F_{(3, 917)} = 8,46$; $p \leq .05$). Öğrencilerin hangi yaş grupları arasında anlamlı farklılık olduğunu bulmak amacıyla yapılan Scheffe testinin sonuçlarına göre veri güvenliği faktöründen elde edilen puanların 11 yaş grubu ortalamasının ($\bar{X}_{11yaş}$ = 18,16), 12 yaş grubu ortalamasından ($\bar{X}_{12yaş}$ = 17,18), 13 yaş grubu ortalamasından ($\bar{X}_{13yaş}$ = 16,57) ve 14 yaş grubu ortalamasından ($\bar{X}_{14yaş}$ = 16,92) daha yüksektir.

Ortaokul öğrencilerin Etik faktöründen aldıkları puanların yaşlara göre anlamlı bir farklılık gösterdiği görülmüştür ($F_{(3, 917)} = 10,02$; $p \leq .05$). Öğrencilerin hangi yaş grupları arasında anlamlı farklılık olduğunu bulmak amacıyla yapılan Scheffe testinin sonuçlarına göre; veri güvenliği faktöründen elde edilen puanların 11 yaş grubu ortalamasının ($\bar{X}_{11yaş}$ = 39,65), 13 yaş grubu ortalamasından ($\bar{X}_{13yaş}$ = 37,50) büyük olduğu görülmüştür. 11 yaş grubu

ortalamasının ($\overline{X}_{11yaş}$ = 39,65), 14 yaş grubu ortalamasından ($\overline{X}_{14yaş}$ = 36,32) büyük olduğu görülmüştür. 12 yaş grubu ortalamasının ($\overline{X}_{12yaş}$ = 38,56), 14 yaş grubu ortalamasından ($\overline{X}_{14yaş}$ = 36,32) büyük olduğu görülmüştür.

Ortaokul öğrencilerin BGEFÖ'den aldıkları puanların yaşlara göre anlamlı bir farklılık gösterdiği görülmüştür ($F_{(3, 917)}$ = 10,09; $p \leq .05$). yapılan Scheffe testi ile hangi yaş grupları arasında anlamlı bir farklılık olduğu tespit edilmeye çalışılmıştır. 11 yaş grubu ortalamasının ($\overline{X}_{11yaş}$ = 70,31), 12 yaş grubu ortalamasından ($\overline{X}_{12yaş}$ = 67,92) büyük olduğu görülmüştür. 11 yaş grubu ortalamasının ($\overline{X}_{11yaş}$ = 70,31), 13 yaş grubu ortalamasından ($\overline{X}_{13yaş}$ = 66,30) büyük olduğu görülmüştür. 11 yaş grubu ortalamasının ($\overline{X}_{11yaş}$ = 70,31), 14 yaş grubu ortalamasından ($\overline{X}_{14yaş}$ = 65,23) büyük olduğu görülmüştür. Toplanan veriler sayesinde yapılan analizlere göre kullanıcı güvenliği puanları yaşlara göre anlamlı bir farklılık göstermezken, veri güvenliği, etik ve BGEFÖ puanları yaşlara göre anlamlı farklar göstermektedir.

Veri güvenliği farkındalığında, 11 yaş grubu ile diğer yaş grupları arasında anlamlı düzeyde farklar mevcut olup 11 yaş grubunun veri güvenliği farkındalığı diğer yaş gruplarından daha yüksek düzeydedir. Etik farkındalığı için, 11 yaş grubunun farkındalık düzeyleri 13 ve 14 yaş grubundan daha yüksek, 12 yaş grubunun farkındalık düzeyleri ise 14 yaş grubundan daha yüksek çıkmıştır. BGEFÖ için yine 11 yaş grubunun farkındalık düzeyi 12, 13 ve 14 yaş grubundan daha yüksek olduğu ortaya çıkarılmıştır. Bu durum Vilander (2021)'in; bilgi güvenliği yaş ile doğru orantılıdır sonucuyla örtüşmediği görülmektedir.

Ortaokul öğrencilerinin BGEFÖ'den aldıkları puanların sınıf seviyelerine göre anlamlı bir farklılık gösterip göstermediğini belirlemek için ANOVA yapılmıştır. Tablo 4.4'te ortaokul öğrencilerinin BGEFÖ'den elde edilen puanlarının sınıf seviyelerine göre ANOVA sonuçları verilmiştir.

Tablo 4.4. Ortaokul Öğrencilerinin BGEFÖ'den Elde Edilen Puanlarının Sınıf Seviyelerine Göre ANOVA Sonuçları.

Faktör	Sınıf	N	$\bar{X}$	ss	F	p	Anlamlılık
Kullanıcı Güvenliği	5	244	12,79	2,66	5,189	.001*	5>6 5>7
	6	261	12,01	2,62			
	7	190	11,91	2,63			
	8	226	12,34	2,68			
Veri Güvenliği	5	244	18,72	3,93	14,795	.000*	5>6 5>7 5>8
	6	261	17,14	3,46			
	7	190	16,60	3,86			
	8	226	16,82	3,98			
Etik	5	244	40,00	5,73	9,540	.000*	5>7 5>8 5>
	6	261	38,77	5,93			
	7	190	37,25	6,98			
	8	226	37,30	7,15			
BGEFÖ	5	244	71,52	10,37	13,725	.000*	5>6 5>7 5>8
	6	261	67,94	9,15			
	7	190	65,76	10,88			
	8	226	66,48	11,54			

(*p≤.05 anlamlılık düzeyi esas alınmıştır.)

Tablo 4.4 incelendiğinde, ortaokul öğrencilerin Kullanıcı Güvenliği faktöründen aldıkları puanların sınıflara göre anlamlı bir farklılık gösterdiği görülmüştür ($F_{(3, 917)} = 5,189$; $p \leq .05$). Yapılan Scheffe testi ile hangi sınıf grupları arasında anlamlı bir farklılık olduğu tespit edilmeye çalışılmıştır. 5. Sınıf ortalamasının ($\bar{X}_{5sınıf} = 12,79$), 6. Sınıf ortalamasından ($\bar{X}_{6sınıf} = 12,01$) büyük olduğu görülmüştür. 5. Sınıf ortalamasının ($\bar{X}_{5sınıf} = 12,79$), 7. Sınıf ortalamasından ($\bar{X}_{7sınıf} = 11,91$) büyük olduğu görülmüştür.

Tablo 4.4 incelendiğinde, ortaokul öğrencilerin Veri Güvenliği faktöründen aldıkları puanların sınıflara göre anlamlı bir farklılık gösterdiği görülmüştür ($F_{(3, 917)} = 14,795$; $p \leq .05$). Yapılan Scheffe testi ile hangi sınıf grupları arasında anlamlı bir farklılık olduğu tespit edilmeye çalışılmıştır. 5. Sınıf ortalamasının ($\bar{X}_{5sınıf} = 18,72$), 6. Sınıf ortalamasından ($\bar{X}_{6sınıf} = 17,14$) büyük olduğu görülmüştür. 5. Sınıf ortalamasının ($\bar{X}_{5sınıf} = 18,72$), 7. Sınıf ortalamasından ($\bar{X}_{7sınıf} = 16,60$) büyük olduğu görülmüştür. 5. Sınıf ortalamasının ($\bar{X}_{5sınıf} = 18,72$), 8. Sınıf ortalamasından ($\bar{X}_{8sınıf} = 16,82$) büyük olduğu görülmüştür.

Tablo 4.4 incelendiğinde, ortaokul öğrencilerin Etik faktöründen aldıkları puanların sınıflara göre anlamlı bir farklılık gösterdiği görülmüştür ($F_{(3, 917)} = 9{,}540$; $p \leq .05$). Yapılan Scheffe testi ile hangi sınıf grupları arasında anlamlı bir farklılık olduğu tespit edilmeye çalışılmıştır. 5. Sınıf ortalamasının ($\overline{X}_{5\text{sınıf}} = 40{,}00$), 7. Sınıf ortalamasından ($\overline{X}_{7\text{sınıf}} = 37{,}25$) büyük olduğu görülmüştür. 5. Sınıf ortalamasının ($\overline{X}_{5\text{sınıf}} = 40{,}00$), 8. Sınıf ortalamasından ($\overline{X}_{8\text{sınıf}} = 37{,}30$) büyük olduğu görülmüştür.

Tablo 4.4 incelendiğinde, ortaokul öğrencilerin BGEFÖ'den aldıkları puanların sınıflara göre anlamlı bir farklılık gösterdiği görülmüştür ($F_{(3, 917)} = 13{,}725$; $p \leq .05$). Yapılan Scheffe testi ile hangi sınıf grupları arasında anlamlı bir farklılık olduğu tespit edilmeye çalışılmıştır. 5. Sınıf ortalamasının ($\overline{X}_{5\text{sınıf}} = 71{,}52$), 6. Sınıf ortalamasından ($\overline{X}_{6\text{sınıf}} = 67{,}94$) büyük olduğu görülmüştür. 5. Sınıf ortalamasının ($\overline{X}_{5\text{sınıf}} = 71{,}52$), 7. Sınıf ortalamasından ($\overline{X}_{7\text{sınıf}} = 65{,}76$) büyük olduğu görülmüştür. 5. Sınıf ortalamasının ($\overline{X}_{5\text{sınıf}} = 18{,}72$), 8. Sınıf ortalamasından ($\overline{X}_{8\text{sınıf}} = 66{,}48$) büyük olduğu görülmüştür. Toplanan veriler sayesinde yapılan analizlere göre kullanıcı güvenliği, veri güvenliği, etik ve BGEFÖ puanları sınıf seviyelerine göre anlamlı bir farklılık göstermektedir.

5. Sınıf öğrencilerinin kullanıcı güvenliği, veri güvenliği, etik farkındalıkları ile ölçeğin tamamına yönelik olarak da diğer sınıf seviyelerine göre farkındalıklarının daha yüksek olduğu ortaya çıkmıştır. Bu durum; Van De Mortel (2021)'in bireylerin eğitim durumlarının artması (sınıf seviyeleri olarak düşünülecek olursa) bilgi güvenliği farkındalıklarını arttırmaz görüşüyle paralellik sağladığı söylenebilir. Burada 5. ve 6. Sınıfta ortaokullarda okutulan Bilişim Teknolojileri ve Yazılım dersinin var olması bu öğrenci gruplarının diğerlerine göre daha yüksek düzeyde farkındalıklar sergilemesine neden olduğu düşünülebilir.

4.3. Üçüncü Alt Probleme İlişkin Bulgular ve Yorum

Araştırmanın üçüncü alt problemi olan "Öğrencilerin bilgi güvenliği ve etik farkındalık düzeyleri anne-baba eğitim düzeylerine göre anlamlı farklılıklar göstermekte midir?" sorusuna yönelik olarak ortaokul öğrencilerinin BGEFÖ'den aldıkları puanların anne eğitim durumlarına göre anlamlı bir farklılık gösterip göstermediğini belirlemek için ANOVA yapılmıştır. Tablo 4.5'te ortaokul öğrencilerinin BGEFÖ'den elde edilen puanlarının anne eğitim durumlarına göre sonuçları verilmiştir.

Tablo 4.5. Ortaokul Öğrencilerinin BGEFÖ'den Elde Edilen Puanlarının Anne Eğitim Durumlarına Göre Sonuçları.

Faktör	Anne Eğitim Durumu	N	$\bar{X}$	ss	F	p	Anlamlılık
Kullanıcı Güvenliği	İlkokul (A)	264	12,20	2,76	2,336	.072	-
	Ortaokul (B)	310	12,03	2,70			
	Lise (C)	222	12,47	2,60			
	Üniversite (D)	125	12,69	2,41			
Veri Güvenliği	İlkokul (A)	264	17,18	3,76	,902	.140	-
	Ortaokul (B)	310	17,35	4,09			
	Lise (C)	222	17,72	3,70			
	Üniversite (D)	125	17,19	3,97			
Etik	İlkokul (A)	264	37,98	6,78	7,000	.000	C > B D > B
	Ortaokul (B)	310	37,44	6,86			
	Lise (C)	222	39,52	5,86			
	Üniversite (D)	125	39,85	5,64			
BGEFÖ	İlkokul (A)	264	67,37	10,95	4,609	.003	C > B
	Ortaokul (B)	310	66,84	11,58			
	Lise (C)	222	69,72	9,48			
	Üniversite (D)	125	69,74	9,13			

(*p≤.05 anlamlılık düzeyi esas alınmıştır.)

Tablo 4.5 incelendiğinde, elde edilen verilerin ANOVA sonuçları görülmektedir. Ortaokul öğrencilerinin Kullanıcı Güvenliği faktöründen aldıkları puanların anne eğitim durumlarına göre anlamlı bir farklılık göstermediği görülmüştür ($F_{(3, 917)}$ = 2,336; p ≥ .05). Ortaokul öğrencilerinin Veri Güvenliği faktöründen aldıkları puanların anne eğitim durumlarına göre anlamlı bir farklılık göstermediği görülmüştür ($F_{(3, 917)}$ = ,902; p ≥ .05).

Tablo 4.5'e göre, ortaokul öğrencilerin Etik faktöründen aldıkları puanların anne eğitim durumlarına göre anlamlı bir farklılık gösterdiği görülmüştür ($F_{(3, 917)}$ = 7,000; p ≤ .05). Yapılan Scheffe testi ile hangi sınıf grupları arasında anlamlı bir farklılık olduğu tespit edilmeye çalışılmıştır. Anne eğitim durumu lise olanların ortalamasının ($\bar{X}_{\text{lise}}$= 39,52), anne eğitim durumu ortaokul olanların ortalamasından ($\bar{X}_{\text{ortaokul}}$ = 37,44) büyük olduğu görülmüştür. Anne eğitim durumu üniversite olanların ortalamasının ($\bar{X}_{\text{üniversite}}$= 39,85), anne eğitim durumu ortaokul olanların ortalamasından ($\bar{X}_{\text{ortaokul}}$ = 37,44) büyük olduğu görülmüştür.

Tablo 4.5'e bakıldığında, ortaokul öğrencilerin BGEFÖ'den aldıkları puanların anne eğitim

durumlarına göre anlamlı bir farklılık gösterdiği görülmüştür ($F_{(3, 917)} = 4,609$; $p \leq .05$). Yapılan Scheffe testi ile hangi sınıf grupları arasında anlamlı bir farklılık olduğu tespit edilmeye çalışılmıştır. Anne eğitim durumu lise olanların ortalamasının ($\bar{X}_{lise} = 69,72$), anne eğitim durumu ortaokul olanların ortalamasından ($\bar{X}_{ortaokul} = 66,84$) büyük olduğu görülmüştür.

"Öğrencilerin bilgi güvenliği ve etik farkındalık düzeyleri anne-baba eğitim düzeylerine göre anlamlı farklılıklar göstermekte midir?" sorusuna yönelik olarak ortaokul öğrencilerinin BGEFÖ'den aldıkları puanların baba eğitim durumlarına göre anlamlı bir farklılık gösterip göstermediğini belirlemek için ANOVA yapılmıştır. Tablo 4.6'te ortaokul öğrencilerinin BGEFÖ'den elde edilen puanlarının baba eğitim durumlarına göre sonuçları verilmiştir.

Tablo 4.6. Ortaokul Öğrencilerinin BGEFÖ'den Elde Edilen Puanlarının Baba Eğitim Durumlarına Göre Sonuçları.

Faktör	Baba Eğitim Durumu	N	$\bar{X}$	ss	F	p	Anlamlılık
Kullanıcı Güvenliği	İlkokul (A)	190	11,94	2,88	3,598	.013	D > A
	Ortaokul (B)	246	12,03	2,79			
	Lise (C)	299	12,43	2,56			
	Üniversite (D)	186	12,70	2,35			
Veri Güvenliği	İlkokul (A)	190	17,19	3,87	1,161	.323	-
	Ortaokul (B)	246	17,10	3,94			
	Lise (C)	299	17,67	3,76			
	Üniversite (D)	186	17,43	4,02			
Etik	İlkokul (A)	190	38,21	6,15	7,944	.000	C > B D > B
	Ortaokul (B)	246	36,89	7,02			
	Lise (C)	299	39,03	6,49			
	Üniversite (D)	186	39,68	5,82			
BGEFÖ	İlkokul (A)	190	67,35	10,33	6,049	.000	C > B D > B
	Ortaokul (B)	246	66,03	11,44			
	Lise (C)	299	69,15	10,42			
	Üniversite (D)	186	69,82	9,89			

(*p≤.05 anlamlılık düzeyi esas alınmıştır.)

Tablo 4.6'ya göre, ortaokul öğrencilerin Kullanıcı Güvenliği faktöründen aldıkları puanların baba eğitim durumlarına göre anlamlı bir farklılık gösterdiği görülmüştür ($F_{(3, 917)} = 3,598$; $p \leq .05$). Yapılan Scheffe testi ile hangi sınıf grupları arasında anlamlı bir farklılık olduğu tespit edilmeye çalışılmıştır. Baba eğitim durumu üniversite olanların ortalamasının ($\overline{X}_{\text{üniversite}} = 12,70$), baba eğitim durumu ortaokul olanların ortalamasından ($\overline{X}_{\text{ilkokul}} = 11,94$) büyük olduğu görülmüştür.

Tablo 4.6 incelendiğinde, elde edilen verilerin ANOVA sonuçları görülmektedir. Ortaokul öğrencilerinin Veri Güvenliği faktöründen aldıkları puanların baba eğitim durumlarına göre anlamlı bir farklılık göstermediği görülmüştür ($F_{(3, 917)} = 1,161$; $p \geq .05$).

Tablo 4.5'e göre, ortaokul öğrencilerin Etik faktöründen aldıkları puanların baba eğitim durumlarına göre anlamlı bir farklılık gösterdiği görülmüştür ($F_{(3, 917)} = 7,944$; $p \leq .05$). Yapılan Scheffe testi ile hangi sınıf grupları arasında anlamlı bir farklılık olduğu tespit edilmeye çalışılmıştır. Baba eğitim durumu üniversite olanların ortalamasının ($\overline{X}_{\text{üniversite}} = 39,68$), baba eğitim durumu ortaokul olanların ortalamasından ($\overline{X}_{\text{ortaokul}} = 36,89$) büyük olduğu görülmüştür. Baba eğitim durumu lise olanların ortalamasının ($\overline{X}_{\text{lise}} = 39,03$), baba eğitim durumu ortaokul olanların ortalamasından ($\overline{X}_{\text{ortaokul}} = 36,89$) büyük olduğu görülmüştür.

Tablo 4.6'ya göre, ortaokul öğrencilerin BGEFÖ'den aldıkları puanların baba eğitim durumlarına göre anlamlı bir farklılık gösterdiği görülmüştür ($F_{(3, 917)} = 6,049$; $p \leq .05$). Yapılan Scheffe testi ile hangi sınıf grupları arasında anlamlı bir farklılık olduğu tespit edilmeye çalışılmıştır. Baba eğitim durumu üniversite olanların ortalamasının ($\overline{X}_{\text{üniversite}} = 69,82$), baba eğitim durumu ortaokul olanların ortalamasından ($\overline{X}_{\text{ortaokul}} = 66,03$) büyük olduğu görülmüştür. Baba eğitim durumu lise olanların ortalamasının ($\overline{X}_{\text{lise}} = 69,15$), baba eğitim durumu ortaokul olanların ortalamasından ($\overline{X}_{\text{ortaokul}} = 66,03$) büyük olduğu görülmüştür.

5. SONUÇ VE ÖNERİLER

Ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalıklarının hangi düzeyde olduğunun belirlenebilmesi amacıyla BGEFÖ geliştirilmiştir. Araştırmanın bu bölümünde BGEFÖ 'nün istatistiksel analiz sonuçları ve araştırmanın alt problemlerine yönelik sonuçlara yer verilmiştir.

5.1. Sonuç

5.1.1 BGEFÖ'nün Geliştirilmesi Sürecinde Ulaşılan Sonuçlar

Bilişim ve mobil teknolojilerinin kullanımı giderek artmakta ve bu teknolojilere sahip olup kullanan kullanıcıların yaşı da gün geçtikçe aşağılara inmektedir. Bilişim teknolojilerinde meydana gelen hızlı değişimlere bağlı olarak bilgi güvenliği ile bilgi güvenliği farkındalığının önemi artırmaktadır (Çetinkaya, Güldüren & Keser, 2017). Bilgi sistemleri zincirinin en zayıf halkasının insan faktörü olmasından dolayı kullanıcı farkındalığı kritik önem arz etmektedir (Güldüren, 2015).

Bilgi güvenliği farkındalığı ile ilgili alanyazın incelendiğinde yapılan çalışmaların iş ve meslek gruplarında yer alan yetişkinler, akademisyenler, öğretmenler, lisans öğrencileri ve lise öğrencileri oldukları görülmüştür. Bu araştırmanın hedef kitlesini oluşturan ortaokul öğrencilerine yönelik çalışmaların (Derin & Gençoğlu, 2020; Özen Serter, 2021; Gökçearslan, Günbatar & Sarıtepeci, 2021) sınırlı ve genelde var olan hazır ölçekler kullanılarak bilgi güvenliği farkındalıklarını belirlemeye çalıştıkları görülmüştür. Etik farkındalığı ile ilgili alanyazın incelendiğinde yapılan çalışmaların iş ve meslek gruplarında yer alan yetişkinler, lisans ve lise düzeyinde öğrencilere yönelik yoğunlaştığı görülmektedir. Ortaokul öğrencilerine yönelik olarak etik farkındalığı konusunda alanyazında yer alan çalışmaların (Gökçearslan, Günbatar & Berikan, 2015; Özdemir, 2017; Salman, 2019) sınırlı olduğu görülmüştür. Ortaokul öğrencilerine yönelik olarak yapılan bu çalışmayı diğer çalışmalardan ayıran en önemli yanı; bilgi güvenliği farkındalığı ve etik farkındalığının tek bir ölçekle ölçülebilir kılmasıdır. Araştırma kapsamında ortaokul öğrencilerinin (5, 6, 7 ve 8.sınıf) bilgi güvenliği ve etik farkındalıklarının düzeyini belirlemek amacıyla "Bilgi Güvenliği ve Etik Farkındalığı Ölçeği" geliştirilmiştir. Ölçek geliştirme sürecinin ilk

aşamasında 37 maddeden oluşan ve Bilgisayar ve Öğretim Teknolojileri alanında uzman 5 akademisyenin uzman görüşleri alınarak hazırlanan madde havuzu oluşturulmuştur. Hazırlanan 37 maddelik ölçme aracı 621 öğrenciye uygulanmıştır.

Bilgi Güvenliği ve Etik Farkındalığı Ölçeği (BGEFÖ)'nin yapı geçerliğini değerlendirmek amacıyla faktör analizi gerçekleştirilmiştir. 621 öğrenciye uygulanan BGEFÖ'nün faktör analizine uygunluğunu belirlemek amacıyla KMO katsayısı hesaplanmış ve Barlett küresellik testi gerçekleştirilmiştir. BGEFÖ için hesaplanan KMO katsayısının (.932) ve Barlett küresellik testi sonuçlarının (χ^2=3792.329; df=136; p=.000) öğrencilerden alınan verilerin faktör analizi yapmaya uygun olduğunu göstermiştir.

Açımlayıcı faktör analizi varimax dik döndürme yöntemi kullanılarak gerçekleştirilmiş olup düşük yük değerlerine sahip maddeler ölçekten çıkarılmıştır. Ölçekte kalan 17 maddenin faktör yükleri .422 ile .834 aralığındadır. Ölçeğin Kullanıcı Güvenliği (3 madde), Veri Güvenliği (5 madde) ve Etik (9 madde) olmak üzere üç faktörden oluştuğu ve tüm faktörlerin açıklanan toplam varyansın %54.100'lük kısmını açıkladığı görülmüştür. Oluşturulan üç boyutlu BGEFÖ'nün faktör yapısının doğruluğunun test edilmesi için doğrulayıcı faktör analizi gerçekleştirilmiştir. Doğrulayıcı faktör analizi ile elde edilen değerlerin açımlayıcı faktör analizinden elde edilen değerlerle benzer oldukları görülmüştür.

BGEFÖ'nün alt boyutları arasındaki korelasyon katsayılarının 0,460 ile 0,464 arasında değiştiği görülmüştür. Geliştirilen ölçeğin alt boyutları için Cronbach Alfa (α) iç tutarlık katsayısı hesaplanmıştır. Nunnally (1978) ve Büyüköztürk (2015) güvenirlik katsayısını 0,70 ve üzerinde olması gerekliliğini vurgulamaktadır. Özdamar (1999)'a göre güvenirlik katsayısı 0,60-0,90 aralığında oldukça güvenilir olarak nitelendirilmektedir. BGEFÖ'nün güvenirlik katsayısına bakıldığında 0,896 olarak tespit edilmiştir. Elde edilen bu katsayı oldukça güvenilir seviyede olmakla birlikte yüksek güvenirlik sınırına çok yakın bir seviyededir.

BGEFÖ için yapılan analizler ve ulaşılan sonuçlara göre BGEFÖ'nün ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalığını belirlemede geçerli ve güvenilir ölçümler sunacağını söylemek mümkündür. Geçerliği ve güvenirliği kanıtlanan ölçme aracı ile araştırmanın asıl problemi olan "Bilgi ve iletişim teknolojilerini kullanan ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalık durumları nedir?" sorusuna yanıt aramak için 921 ortaokul öğrencisine 17 madde ve 3 faktörden oluşan ölçme aracı uygulanmıştır. Elde edilen veriler ve bu verilerin analizi sayesinde araştırmanın alt problemlerine dair sonuçlara ulaşılmıştır.

5.1.2 Araştırmanın Alt Problemlerine Dair Ulaşılan Sonuçlar

Araştırmanın birinci alt problemi olan "*Öğrencilerin bilgi güvenliği ve etik farkındalık düzeyleri nasıldır?*" sorusuna yönelik olarak ortaokul öğrencilerinden elde edilen verilerin analizi gerçekleştirilmiştir. Araştırmaya katılan ortaokul öğrencilerinin BGEFÖ'den aldıkları puanların ortalamalarının madde sayısına bölümüyle elde edilen ortalamalar incelendiğinde; veri güvenliği faktörüne ait ortalamanın 3,48, kullanıcı güvenliği faktörüne ait ortalamanın 4,09 etik faktörüne ait ortalamanın 4,27 olduğu görülmüştür. Ölçek genelinden elde edilen ortalamanın 4,01 olduğu görülmüştür. Ortaokul öğrencilerinin veri güvenliği faktörüne yönelik farkındalıklarının en düşük olduğu ve etik faktörüne yönelik farkındalıklarının daha yüksek olduğu görülmektedir. Ölçek genelinden elde edilen puanlar incelendiğinde ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalıklarının yüksek düzeyde olduğu fakat veri güvenliği faktörü farkındalığının orta düzeyde olduğu söylenebilir. Elde edilen bu sonucun Tekerek ve Tekerek (2013)'in yaptığı çalışmayla benzer sonuçlar gösterdiği görülmüştür. Ortaokul seviyesinde yapılan çalışmalarda (Beder & Ergün, 2015; Özen Serter, 2021) bilgi güvenliği farkındalıklarının orta ve düşük seviyede olduğu görülmüştür. Lise, lisans seviyesi ve diğer yetişkin seviyelerinde yapılan çalışmalar (Hacımustafaoğlu, 2019; Slusky & Partow, 2012; Karaoğlan Yılmaz vd., 2017; Dönmez, 2019) incelendiğinde bilgi güvenliği kapsamına giren alt boyutlarda yüksek, etik farkındalığı alt boyutuna girebilecek olan alt boyutlarda orta ve düşük düzeyde kaldıkları görülmektedir. Yapılmış olan bu çalışmalarla BGEFÖ'den elde edilen veriler sonucunda ulaşılan sonuçlar arasındaki farkın teknoloji kullanım yaşının hızlı bir şekilde küçük yaşlara inmesi ve pandemi döneminde öğrencilerin uzaktan eğitim sistemi kapsamında bilişim teknolojileri ve diğer mobil araçlar ve iletişim sistemlerini daha sık kullanmış olmasından kaynaklı olduğu düşünülmektedir.

Araştırmanın ikinci alt problemi olan "*Öğrencilerin bilgi güvenliği ve etik farkındalık düzeyleri yaş, cinsiyet, sınıf düzeylerine göre değişim göstermekte midir?*" sorusuna yönelik olarak ortaokul öğrencilerinden elde edilen verilerin analizi gerçekleştirilmiştir. BGEFÖ'nün tamamı, Kullanıcı güvenliği, veri güvenliği faktörleri cinsiyete göre anlamlı bir farklılık göstermemektedir. Etik farkındalığında kızların puanlarının ortalaması erkeklerin puanlarının ortalamasından anlamlı bir fark oluşturacak derecede yüksek olduğu görülmüştür. Ulaşılan bu sonuç yapılan diğer çalışmalarla (Salman, 2019; Özdemir, 2012;

Gökçearslan, Günbatar & Berikan, 2015; Özen Serter, 2021) benzerlik gösterir niteliktedir. Güldüren, Çetinkaya ve Keser (2016) yapmış olduğu çalışmada ise erkeklerin bilgi güvenliği farkındalıklarının kızlara oranla daha yüksek olduğu sonucu bulunurken aynı şekilde Talan ve Aktürk (2021)'de benzer sonuçları elde etmiştir. Bu çalışmalardan elde edilen sonuçlar, ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalığı çalışmasından elde dilen sonuçlarla farklı olduğu görülmektedir. Bilgi güvenliği ve etik farkındalığı yaşlara göre nasıl değişim gösterdiğini ortaya çıkarabilmek amacıyla istatistiksel analizler yapılmıştır. Yapılan bu analizler sonucunda kullanıcı güvenliği farkındalığında yaş grupları arasında anlamlı bir farklılık bulunamamıştır. Veri güvenliği farkındalığında ise 11 yaş grubu ile diğer yaş grupları arasında anlamlı düzeyde farklar mevcut olup 11 yaş grubunun veri güvenliği farkındalığı diğer yaş gruplarından daha yüksek düzeydedir. Etik farkındalığı için ise 11 yaş grubunun farkındalık düzeyleri 13 ve 14 yaş grubundan daha yüksek, 12 yaş grubunun farkındalık düzeyleri ise 14 yaş grubundan daha yüksek çıkmıştır. BGEFÖ için yine 11 yaş grubunun farkındalık düzeyi 12, 13 ve 14 yaş grubundan daha yüksek olduğu ortaya çıkarılmıştır. Bu durum Vilander (2021)'in; bilgi güvenliği yaş ile doğru orantılıdır sonucuyla örtüşmediği görülmektedir. 5. Sınıf öğrencilerinin kullanıcı güvenliği, veri güvenliği, etik farkındalıkları ile ölçeğin tamamına yönelik olarak da diğer sınıf seviyelerine göre farkındalıklarının daha yüksek olduğu ortaya çıkmıştır. Bu durum Van De Mortel (2021)'in bireylerin eğitim durumlarının artması (sınıf seviyeleri olarak düşünülecek olursa) bilgi güvenliği farkındalıklarını arttırmaz görüşüyle paralellik sağladığı söylenebilir. Burada 5. ve 6. Sınıfta ortaokullarda okutulan Bilişim Teknolojileri ve Yazılım dersinin var olması bu öğrenci gruplarının diğerlerine göre daha yüksek düzeyde farkındalıklar sergilemesine neden olduğu düşünülebilir.

Araştırmanın üçüncü alt problemi olan "*Öğrencilerin bilgi güvenliği ve etik farkındalık düzeyleri anne-baba eğitim düzeylerine göre anlamlı farklılıklar göstermekte midir?*" sorusuna yönelik olarak ortaokul öğrencilerinden elde edilen verilerin analizi gerçekleştirilmiştir. Öğrencilerin kullanıcı güvenliği farkındalığı ve veri güvenliği farkındalıklarının anne eğitim durumlarından etkilenmediği sonucuna ulaşılmıştır. Etik farkındalığının ise anne eğitim düzeyi üniversite ve lise olanların anne eğitim düzeyleri ortaokul düzeyinde olanlardan anlamlı derecede farklılık gösterdiği görülmüştür. Ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalıklarının öğrencilerin anne eğitim düzeyleri ile doğru orantılı değişim gösterdiği söylenebilir. Baba eğitim durumlarının ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalıkları incelendiğinde ise veri güvenliği

farkındalığı alt boyutuna öğrencilerin baba eğitim durumlarının anlamlı bir etkisinin olmadığı görülmüştür. Kullanıcı güvenliği alt boyutunda ise baba eğitim durumu üniversite olanın, baba eğitim durumu ilkokul olandan anlamlı derecede farklı olduğu görülmüştür. Etik farkındalığı alt boyutunda; ise baba eğitim durumu lise ve üniversite olanların farkındalık düzeylerinin baba eğitim durumu ortaokul olanlara göre anlamlı düzeyde farklılık gösterdiği görülmüştür. Ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalıklarının öğrencilerin baba eğitim düzeyleri ile doğru orantılı değişim gösterdiği görülmüştür. Benzer sonuçlar Özen Serter (2021)'in çalışmasında da görülmüştür.

5.2. Öneriler

Bireyler bilişim teknolojilerini, bilgisayarları ve mobil cihazları sadece ortaokul, lise ya da üniversite seviyesine geldiğinde kullanmaya başlamıyor. Gün geçtikçe teknoloji kullanım yaşı daha erken yaşlara inmeye devam ediyor. Bu nedenle de bilginin önemini ve bilişim etiği kapsamına nelerin girip girmediğinin bilgisinin ve eğitiminin ilkokul hatta okul öncesi dönemde verilmesinin gerekli olduğu düşünülmektedir. Bilişim teknolojileri ve yazılım dersinin sadece 5 ve 6.sınıfta olmak yerine ilkokul 3 ve 4.sınıfa da koyulması ayrıca 7 ve 8. Sınıfta da devam ettiriliyor olmasının öğrencilerin var olan farkındalık düzeylerinin artıracağı düşünülmekte ve bu şekilde karşılaşılan bazı etik davranışsal problemlerin azalması beklenmektedir.

Hazırlanan BGEFÖ'nün ön test ve son test olarak kullanılacağı öğretim programları hazırlanarak, programın öğrencilerin farkındalıklarına etkisinin araştırıldığı çalışmalar yapılabilir. Hazırlanmış olan BGEFÖ dil ve anlaşılırlık yönünden ilkokul öğrencilerine de hitap edebildiği için BGEFÖ'nün ilkokullarda kullanılabileceği araştırmalar da yapılabilir.

Ortaokul öğrencilerine yönelik hazırlanan BGEFÖ'nün sene başında ve sene sonunda öğrencilere uygulaması gerçekleştirilerek öğrencilerin yıl içindeki bilgi güvenliği ve etik farkındalıklarında nasıl bir değişim olduğu incelenebilir. Buradan hareketle kullanıcı güvenliği, veri güvenliği ya da etik hususlarında bazı ek önlemler alınarak öğrencilerin farkındalıkları yükseltilmeye çalışılabilir.

Ortaokul öğrencileri için boylamsal çalışmalar da gerçekleştirilebilir. Bir öğrenciye 5.sınıfın başından itibaren her sene başında ya da sonunda BGEFÖ uygulanıp elde edilen veriler diğer senelerle karşılaştırılarak öğrenciye yönelik bireysel değişim takip edilerek bireysel önlemler öğrenciye ve ailesine tavsiye edilebilir.

Ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalığı araştırması Bartın İlinin merkez

ilçesine bağlı merkez okulları ve köy okullarında gerçekleştirilmiş bir çalışmadır. Çalışmaya katılan öğrenci sayısı 921'dir. Farklı araştırmalar farklı şehirlerin farklı yerleşim yerlerinde daha fazla sayıda öğrenciye ulaşarak gerçekleştirilebilir.

Ortaokul öğrencilerinin bilgi güvenliği ve etik farkındalığı araştırması kapsamında alt problemlerde farkındalık düzeylerinin yaş, cinsiyet, sınıf seviyesi, anne-baba eğitim durumlarına göre nasıl değiştiği üzerine çalışılmıştır. Bundan sonraki çalışmalarda farklı değişkenler üzerine odaklanılarak yeni çalışmalar gerçekleştirilebilir.

KAYNAKLAR

Akıncan, E. (2022). *Ortaokul Öğrencilerinin Dijital Okuryazarlık, Dijital Bağımlılık ve Bilgi Güvenliği Farkındalık Düzeylerinin İncelenmesi*. Yayımlanmamış Yüksek Lisans Tezi, Amasya Üniversitesi, Fen Bilimleri Enstitüsü, Amasya.

Alpar, R. (2013). *Uygulamalı Çok Değişkenli İstatistiksel Yöntemler.* Ankara: Detay Yayıncılık.

Anti-Phishing Working Group. (2015). *APWG Phishing Activity Trends Report*. Retrieved from.

Anti-Phishing Working Group. (2020). *Phishing Activity Trends Report, 4th Quarter 2020*. Retrieved from.

Anwar, M. S., Hussain, A., Javaid, A., Ali, M., ve Khalid, A. (2019). State-of-the-art rootkit Detection and Removal Techniques: A Systematic Literature Review. *Computers & Electrical Engineering, 74*, 547-566.

Awad, N. F., & Krishnan, M. S. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and The Willingness to Be Profiled Online for Personalization. *MIS Quarterly, 30(1*), 13-28.

Aycock, J. (2006). *Computer Viruses and Malware*. Springer.

Aydoğdu, F. (2022). *Bilişim Etiği Konusunda Geliştirilen Bilgisayar Destekli Öğretim Materyalinin Ortaöğretim Öğrencilerinin Etik Olmayan Bilgisayar Kullanım Düzeylerine Etkisinin İncelenmesi*. Yayımlanmamış Yüksek Lisans Tezi, Fırat Üniversitesi, Eğitim Bilimleri Enstitüsü, Elazığ.

Beauchamp, T. L., & Childress, J. F. (2013). *Principles of Biomedical Ethics*. Oxford University Press.

Benevenuto, F., Rodrigues, T., Almeida, V. A., ve Almeida, J. M. (2010). Detecting spammers on Twitter. *In Proceedings of the Conference on Email and Anti-Spam*, 1-8.

Bhatia, S., Singh, R., ve Bansal, D. (2017). Malware Detection Techniques: A Brief Review and Comparison. *Procedia Computer Science, 122*, 478-485.

Biryukov, A., Pustogarov, I., ve Weinmann, R. P. (2013). Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization. *In International Conference on Financial Cryptography and Data Security*, 125-141.

Brown, T. A. (2006). *Confirmatory Factor Analysis For Applied Research.* The Guilford Press.

Cai, L., Xing, X., Zhang, Y., Xu, X., ve Guan, L. (2018). Detecting android malware through deceptive user interfaces. *IEEE Transactions on Dependable and Secure*

Computing, 15(3), 438-451.

Can, A. (2014). *SPSS ile Bilimsel Araştırma Sürecinde Nicel Veri Analizi*. Pegem, Ankara.

Chen, H., Chien, E., ve Sebring, M. (2011). Anatomy of Drive-by Download Attack. *In Proceedings of the 2011 ACM Symposium on Applied Computing.602-607.*

Christodorescu, M., Jha, S., Seshia, S. A., Song, D., ve Bryant, R. E. (2005). Semantics-Aware Malware Detection. *In Proceedings of the 2005 ACM SIGPLAN Conference on Programming Language Design and Implementation*, 32-44.

Cohen, F. (1987). Computer Viruses: Theory and Experiments. *Computers & Security, 6(1),* 22-35.

Conti, G. (2010). Ten Years of Keylogging. *In Proceedings of the Third International Conference on Network and System Security*, 258-263.

Costello, A. B., ve Osborne, J. W. (2005). Best practices in exploratory factor analysis: Four recommendations for getting the most from your analysis. P*ractical Assessment, Research & Evaluation, 10(7),* 1-9.

Cybersecurity and Infrastructure Security Agency. (2020). *Phishing and Spoofing. https://www.cisa.gov/phishing (02.04.2023)*

Çakmak, E. K., Çebi, A. ve Kan, A. (2014). E-öğrenme Ortamlarına Yönelik "Sosyal Bulunuşluk Ölçeği" Geliştirme Çalışması. *Kuram ve Uygulamada Eğitim Bilimleri, 14(2),* 755-768.

Çokluk, Ö., Şekercioğlu, G., ve Büyüköztürk, Ş. (2014). Sosyal bilimler için çok değişkenli istatistik: *SPSS ve LISREL Uygulamaları*. Pegem, Ankara.

D'Arcy, J., ve Hovav, A. (2009). Does Location-Based Advertising Work? *Results From A Field Study With Real Users. Journal of Advertising Research, 49(4),* 448-455.

Dedeoğlu, G. (2009). *Etik ve Bilişim*. Etki, İzmir.

Dhamija, R., ve Dusseault, L. (2008). The Seven Flaws of Identity Management: Usability and Security Challenges. *IEEE Security & Privacy, 6(2),* 24-29.

Dhamija, R., Tygar, J. D., ve Hearst, M. (2006). Why Phishing Works. *In Proceedings of The SIGCHI Conference on Human Factors in Computing Systems*, 581-590.

Dönmez, G. (2019). *Lise Öğrencilerinin Bilgi Güvenliği Farkındalığı ile Dijital Okuryazarlığı Arasındaki İlişkinin İncelenmesi.* Yüksek Lisans Tezi, Hacettepe Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.

Erdoğmuş, A. (2017). *Üniversite Öğrencilerinin Bilgi Güvenliği Kazanımlarının, Farkındalıkları Üzerindeki Etkilerinin Analizi: Afyon Kocatepe Üniversitesi Örneği.* Yayımlanmamış Yüksek Lisans Tezi, Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü, Afyon.

Fabrigar, L. R., Wegener, D. T., ve MacCallum, R. C. (1999). Evaluating The Use of Exploratory Factor Analysis in Psychological Research. *Psychological Methods, 4(3*), 272-299.

Federal Trade Commission. (2021). How to Recognize and Report Spam Text Messages. *Retrieved from.*

Feng, M., Gehrke, J., ve Srikant, R. (2004). Spam: A Review. *ACM SIGMOD Record, 33(4),* 22-37.

Ferrara, E., Varol, O., Davis, C., Menczer, F., ve Flammini, A. (2020). The Rise of Social Botnets: Attacks and Defenses. *ACM Transactions on Intelligent Systems and Technology (TIST), 11(3),* 1-28.

Field, A. (2009). *Discovering Statistics Using SPSS (3 ed.).* SAGE Publications Ltd., London.

Filiol, E. (2011). Computer Viruses and Malware. *Science & Business Media*.

Floridi, L. (2013). *The Ethics of Information*. Oxford University Press.

Fogh, C. (2006). *Rootkits: Subverting the Windows Kernel*. Addison-Wesley Professional.

Gökçearslan, Ş., Günbatar, M. S. ve Sarıtepeci, M. (2021). Ortaöğretim Öğrencilerinin Bilgi Güvenliği Farkındalığı Düzeylerinin Belirlenmesi. *YYÜ Eğitim Fakültesi Dergisi, 18(1),* 354-373.

Gregg, M. (2011). Rootkits. *In Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground,* 57-61.

Guilford, J. P. (1954). *Psychometric Methods (2. ed.).* McGraw-Hill, New York.

Gupta, A., Kumaraguru, P., ve Castillo, C. (2013). Characterizing the Life-Cycle of Botnets. *In Proceedings of the 22nd International Conference on World Wide Web,* 419-430.

Gupta, S., Kumaraguru, P., ve Cranor, L. F. (2018). Putting The Human in The loop: Privacy and Security Challenges in User-Driven Profiling. *In Proceedings of the ACM Conference on Computer-Supported Cooperative Work and Social Computing,* 1406-1422.

Güriş, S., ve Astar, M. (2015). *Bilimsel Araştırmalarda SPSS ile İstatistik*. Der Yayınları, İstanbul.

Hacımustafaoğlu, R. (2019).*Ortaöğretim Öğrencilerinin Bilgi Güvenliği Farkındalık Düzeylerinin Siber Mağdur Olma Durumlarına Etkisinin İncelenmesi (Üsküdar Örneği).* Yüksek Lisans Tezi, Sakarya Üniversitesi Eğitim Bilimleri Enstitüsü, Sakarya.

Hadnagy, C. (2011). *Social Engineering: The Art of Human Hacking*. John Wiley & Sons.

Herath, T., ve Rao, H. R. (2009). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. *European Journal of Information Systems, 18(2),* 106-125.

Huck, S. W. (2012). Reading Statistics and Research. NY: Pearson, New York.

Hutcheson, G. ve Sofroniou, N. (1999) *The Multivariate Social Scientist: Introductory Statistics Using Generalized Linear Models*. Sage Publication, Thousand Oaks, CA.

Janczewski, L. J., ve Colarik, A. M. (2004). *Cyber Warfare and Cyber Terrorism*. Idea Group Inc (IGI).

Johnson, D. G. (2011). *Computer Ethics*. In Stanford Encyclopedia of Philosophy. *https://plato.stanford.edu/entries/ethics-computer/ (03.04.2023).*

Jöreskog, K.G., ve Sörbom, D. (1993). *LISREL 8: Structural Equation Modeling With The SIMPLIS Command Language*. Lawrence Erlbaum, New Jersey.

Kass, A. (2009). Sosyal Bilimlerde Araştırma Yöntem, Teknik ve İlkeler. Pegem Akademi, Ankara.

Kass, R. A., ve Tinsley, H. E. A. (1979). Factor Analysis. *Journal of Leisure Research, 11,* 120-138.

Kaufman, C., Perlman, R., ve Speciner, M. (2002). *Network Security: Private Communication in a Public World*. Prentice Hall.

Khattak, S. U., Ullah, S., Ullah, Z., Ahmad, J., Loo, J., ve Kumar, N. (2017). Botnets: A survey. *Computers & Electrical Engineering, 63*.

Kissel, R., Maniatis, P., ve Baker, M. (2016). The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption. *Journal of Information Security and Applications, 28,* 65-77.

Kline, P. (1994). An Easy Guide to Factor Analysis. Routledge, New York.

Kline, R. S. (2011). *Principles and Practice of Structural Equation Modeling*. The Guilford Press, NewYork.

Kowalski, R. M., ve Limber, S. P. (2012). Psychological, Physical and Academic Correlates of Cyberbullying and Traditional Bullying. *Journal of Adolescent Health, 53(1),* 13-20.

Krombholz, K., Hobel, H., ve Huber, M. (2015). Advances in Detecting Spam, Bots, and Malware on Twitter. *IEEE Transactions on Dependable and Secure Computing, 12(3),* 337-349.

Kumaraguru, P., Rhee, Y., Sheng, S., ve Cranor, L. F. (2008). Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer. *In Symposium on Usable Privacy and Security*, 44-54.

Landau, S., McDonald, A., ve Halderman, J. A. (2014). Inadvertent Data and Backdoors in Electronic Medical Records. *Journal of Medical Internet Research, 16(11),* 256.

Lederer, S., ve Kemmerer, R. A. (2006). Empirical Analysis of an Email-Based System for Detecting Malicious Insiders. *Transactions on Information and System Security (TISSEC), 9(3),* 226-262.

Lederer, S., Lauf, S., Macek, B., & Weippl, E. R. (2016). Mobile Spyware Detection Through Atomic Aspects. *In Proceedings of the 31st Annual ACM Symposium on Applied Computing*, 35-40.

Lessig, L. (2001). *The Future of İdeas: The Fate of The Commons in A Connected World*. Random House.

Lessig, L. (2006). *Code version 2.0.* Basic books.

Maleki, H. R., Shahgholian, A. ve Lutfi, A. (2016). The Role of Human Factor in Information Security. *Procedia Computer Science, 102*, 602-608.

McAfee. (2020). What Is Spam? *https://www.mcafee.com/support/ (06.04.2023).*

McKeon, N. (2011). Ethical Issues in Intellectual Property. *American Medical Association Journal of Ethics, 13(2),* 132-136.

McNurlin, B., ve Sprague, R. (2006). *Information Systems Management in Practice*. Prentice Hall.

Mitnick, K. D., ve Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. Wiley.

Moor, J. H. (2008). Why We Need Better Ethics for Emerging Technologies. *Ethics and Information Technology, 10(2-3),* 93-104.

Moore, D., Paxson, V., Savage, S., Shannon, C., Staniford, S., ve Weaver, N. (2003). Inside the Slammer Worm. *IEEE Security & Privacy, 1(4),* 33-39.

National Cyber Security Centre. (2019). Cyber Aware: Phishing Attacks. *https://www.ncsc.gov.uk/collection/phishing-scams (07.04.2023).*

Norris, P., ve Pernia, E. M. (2019). Digital Divide and E-Government: Evidence From the European Union. *Policy & Internet, 11(1),* 102-121.

Özdamar, K. (2013). Paket Programlar ile İstatistiksel Veri Analizi-1: SPSS-MINITAB. Nisan Kitapevi, Eskişehir.

Özdemir, A. (2017). *Yönetim Bilişim Sistemleri ve Bilgisayar Ve Öğretim Teknolojileri Eğitimi Bölümü Öğrencilerinin İnternet Teknolojilerinin Etik Kullanım Düzeylerinin İncelenmesi.* Yayımlanmamış Yüksek Lisans Tezi, Aksaray Üniversitesi Sosyal Bilimler Enstitüsü, Aksaray.

Özen Serter, B. (2021). *Ortaokul Öğrencilerinin Bilgi Güvenliği Farkındalık Düzeyinin Belirlenmesi.* Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.

Özkan, E. (2018). Bilişim Teknolojilerinde Güvenlik ve Siber Suçlar. *Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 20(3),* 197-220.

Öztezcan, B.A. (2017). *Bilgi Güvenliği Farkındalığı Üzerine Bir Araştırma: Marmara Üniversitesi Örneği.* Yayınlanmamış Yüksek Lisans Tezi. Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul.

Patel, A., Hsu, C. H., ve Hughes, S. (2019). Keyloggers. *In Security for Software Engineers,* 181-187.

Renaud, K., ve De Angeli, A. (2009). The Role of Social Influence in Security Decisions. *In International Conference on Human Aspects of Information Security, Privacy, and Trust,* 186-195.

Reynolds, S. J. (2006). A Framework for Improving Ethical Decision Making. Marketing Education Review, 16(1), 15-21.

Rosenstand, N. (2011). The Moral of The Story: *An Introduction to Ethics*. McGraw-Hill.

Sabottke, C., Kang, B., Bos, H., Costin, A., Dietrich, C. J., Plate, T. ve Spreitzenbarth, M. (2015). The Underground Economy of Fake Antivirus Software. *In Proceedings of the 24th USENIX Security Symposium*,1003-1018.

Sari, D. I., Rejekiningsih, T., ve Muchtarom, M. (2020). Students' Digital Ethics Profile in The Era of Disruption: An Overview From The Internet Use at Risk in Surakarta City, Indonesia. *International Journal of Interactive Mobile Technologies (iJIM). 14,* 82-94.

Schneider, F. B. (2019). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

Schwartz, M. S. (2017). *Corporate Social Responsibility*. Routledge.

Selwyn, N. (2003). Apart From Technology: Understanding People's Non-Use of Information and Communication Technologies in Everyday Life. *Technology in Society, 25(1),* 99-116.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., ve Downs, J. (2010). Who Falls for Phish?: A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. *In Proceedings of The SIGCHI Conference on Human Factors in Computing Systems,* 373-382.

Soldatova, G., Rasskazova, E., Zotova, E., Lebesheva, M., Geer, M., ve Roggendorf, P. (2014). Russian Kids Online: Key Findings of The EU Kids Online II Survey in Russia. *Foundation for Internet Development, Moscow, Russia*.

Spafford, E. H. (1989). The Internet Worm Program: An Analysis. *Purdue Technical Report CSD-TR*-823.

Staniford, S., Paxson, V., ve Weaver, N. (2002). How to Own The Internet in Your Spare Time. *In Proceedings of The 11th USENIX Security Symposium,* 149-167.

Stone Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R., ve Kruegel, C. (2011). Your Botnet is My Botnet: Analysis of A Botnet Takeover. *In Proceedings of The 16th ACM Conference on Computer and Communications Security*, 635-647.

Sümer, N. (2000). Yapısal Eşitlik Modelleri: Temel Kavramlar ve Örnek uygulamalar. *Türk Psikoloji Yazıları, 3(6)*, 49-74.

Symantec. (2020). Phishing. *https://www.symantec.com/security-center/threat-report (10.04.2023).*

Symantec. (2021). Backdoor. *https://www.symantec.com/security-center/threat-report (11.04.2023).*

Szor, P. (2005). *The Art of Computer Virus Research and Defense*. Addison-Wesley Professional.

Tabachnick, B. G., ve Fidell, L. S. (2015). *Çok Değişkenli İstatistiklerin Kullanımı* (Çev. Ed. M. Baloğlu). Nobel, Ankara.

Talan,T. ve Aktürk, C. (2021). Ortaöğretim Öğrencilerinin Dijital Okuryazarlık ve Bilgi Güvenliği Farkındalığı Seviyelerinin İncelenmesi. *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi, 18(1)*, 158-180.

Talim ve Terbiye Kurulu Başkanlığı (2013). Ortaokul Yeni Ders Programı. *http://mebk12.meb.gov.tr/meb_iys_dosyalar/63/08/745166/dosyalar/2013_05/280508 43_ortaokul_yeni_ders_programi.pdf (12.04.2023).*

Tavani, H. T. (2007). Informational privacy: Concepts, Theories, and Controversies. *Handbook of Information and Computer Ethics*, 310-335.

Teker, E. (2019). *Öğretmenlerin ve Lise Öğrencilerinin Bilgi Güvenliği Farkındalık Düzeylerinin Değerlendirilmesi*. Yayınlanmamış Yüksek Lisans Tezi. Ankara Üniversitesi, Eğitim Bilimleri Enstitüsü, Ankara.

Tekerek, M., ve Tekerek, A. (2013). Öğrencilerin Bilgi Güvenliği Farkındalığı Üzerine Bir Araştırma. *Turkish Journal of Education, 2*(3), 61-70.

Thompson, B. (2008). *Foundations of Behavioral Statistics: An Insight-Based Approa*ch. Guilford Press, New York.

Van De Mortel, K. (2021). *De Invloed Van Opleiding op Information Security Awareness The Influence of Education on Information Security Awareness*. Master's Thesis. Open Universiteit.

Vilander, J. (2021). *Brıdgıng The Knowıng-Doıng Gap: The Role of Attıtude In Informatıon Securıty Awareness.* Master's Thesis. Unıversıty Of Jyväskylä Faculty Of Informatıon Technology.

Vural, Y. ve Sağıroğlu, Ş. (2010). Veritabanı Yönetim Sistemleri Güvenliği: Tehditler ve Korunma Yöntemleri, *Politeknik Dergisi, 13(2),* 71-81.

Wang, J., Niiya, M., ve Mark, G. (2019). Cyberbullying: A Socio-Technological Perspective. *Computers in Human Behavior, 91*, 277-282.

Whitman, M. E., ve Mattord, H. J. (2016). *Principles of Information Security*. Cengage Learning.

WIPO. (2017). Intellectual Property: A Power Tool for Economic Growth. Retrieved from *https://www.wipo.int/edocs/pubdocs/en/intproperty/450/wipo_pub_450.pdf (15.04.2023).*

WIPO. (2019). Patents. *https://www.wipo.int/patents/en/ (15.04.2023).*

Worm, R. (1988). Experiences with the Morris worm. *Communications of the ACM, 31(5),* 484-497.

Yıldırım, M. ve Demirer, V. (2021). Eğitim Alanında Bilgi Güvenliği Üzerine Sistematik Bir Alanyazın İncelemesi: Türkiye Örneği. *Erzincan Üniversitesi Eğitim Fakültesi Dergisi, 23 (3), 835-856.*

Yılmaz, E. (2015). *Öğretmenlerin Dijital Veri Güvenliği Farkındalığı*. Yayınlanmamış Doktora Tezi. Anadolu Üniversitesi, Eğitim Bilimleri Enstitüsü, Eskişehir.

Zhen, J., Dong, K., Xie, Z., ve Chen, L. (2022). Factors Influencing Employees' Information Security Awareness in the Telework Environment. *Research Square, https://doi.org/10.21203/rs.3.rs-1544020/v2 (15.04.2023).*

Zou, C., Gong, W., Towsley, D., ve Zhang, Z. L. (2005). On the performance of internet worm scanning strategies. In Proceedings of the 2005 ACM SIGMETRICS *International Conference on Measurement and Modeling of Computer Systems,* 261-272.

EKLER

EK 1: Sosyal ve Beşeri Bilimler Etik Kurulu Onay Belgesi

T.C.
BARTIN ÜNİVERSİTESİ REKTÖRLÜĞÜ
Sosyal ve Beşeri Bilimler Etik Kurulu

Sayı : E-23688910-050.01.04-2300023177 12.03.2023
Konu : Sosyal ve Beşeri Bilimler Etik Kurulu Onay Belgesi

Protokol No:	2023-SBB-0102
Araştırmanın Başlığı:	Ortaokul Öğrencilerinin Bilgi Güvenliği ve Etik Farkındalığı
Proje Yürütücüsü:	Ahmet YILMAZ
Başvuru Formunun Geliş Tarih:	16.02.2023
Karar Tarihi:	07.03.2023
Toplantı No:	05

Başvuru dosyasında etik sorun oluşturabilecek sorular/maddeler, süreçler ya da unsurlar bulunmadığından 07.03.2023 tarihli ve 05 numaralı toplantıda 2023-SBB-0102 numaralı başvuruya araştırma için ETİK KURUL ONAY belgesinin verilmesine karar verilmiştir.

Doç. Dr. Elif KARAHAN Kurul Başkanı	Doç. Dr. Sedat BALYEMEZ Başkan yardımcısı	Doç. Dr. Melih BAŞKOL Üye
Doç. Dr. Sefer Yetkin IŞIK Üye	Doç. Dr. Vahit CELAL Üye	Dr. Öğr. Üyesi Hasan Basri KANSIZOĞLU Üye

Adres: Ağdacı Mahallesi Fakülte Caddesi No:54 Bartın
Telefon No: (0 378) 2235500
Faks No: (0 378) 2235042
e-Posta:
İnternet Adresi: http://www.bartin.edu.tr/
Kep Adresi: bartinuniversitesi@hs01.kep.tr
Bilgi için : Elif Karahan, Kurul Başkanı
Telefon No: (0 378) 2235372 - 5372

EK 2: Araştırma İzni

BELGE TARIHI: 13.04.2023 BELGE SAYISI: 2300035039

T.C.
BARTIN VALİLİĞİ
İl Millî Eğitim Müdürlüğü

Sayı : E-64441482-605.01-74359920 13.04.2023
Konu : Araştırma Uygulama İzni Talebi
(Ahmet YILMAZ)

BARTIN ÜNİVERSİTESİ REKTÖRLÜĞÜNE
(Öğrenci İşleri Daire Başkanlığı)

İlgi : a) Bakanlığımızın (Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü) 21.01.2020 tarihli ve E.1563890 sayılı yazısı ekindeki 2020/2 No'lu Genelge'si.
b) Bartın Üniversitesi Rektörlüğü'nün (Öğrenci İşleri Daire Başkanlığı) 16.03.2023 tarhli ve E-44030360-605.01-2300026023 (DYS Kayıt No:73941680) sayılı yazısı.
c) Müdürlük Makamının 12.04.2023 tarihli ve E-64441482-605.01-74314910 sayılı Oluru.

İlgi (b) yazı ile; Bartın Üniversitesi Lisansüstü Eğitim Enstitüsü Bilgisayar Teknolojisi ve Bilişim Sistemleri Ana Bilim Dalı tezli yüksek lisans programı öğrencisi Ahmet YILMAZ'ın Dr. Öğr. Üyesi Ahmet Berk ÜSTÜN yürütücülüğünde "Ortaokul Öğrencilerinin Bilgi Güvenliği ve Etik Farkındalığı" başlıklı tez çalışmasına veri sağlamak amacıyla Müdürlüğümüze bağlı resmi/özel ortaokullarda öğrenim gören öğrencilerin katılımıyla anket çalışması yapma izin talebinde bulunduğu bildirilmiş olup, ilgilinin başvuru belgeleri ilgi (a) Genelge doğrultusunda Müdürlüğümüz Araştırma Değerlendirme Komisyonu tarafından incelenmiştir.

Yukarıda açıklanan araştırma uygulama iznine ilişkin onaylı bir örneği Müdürlüğümüzde muhafaza edilen, uygulama sırasında adı geçen araştırmacının **sadece yazımız ekinde gönderilen mühürlü ve imzalı örnekten çoğaltıp uygulayabileceği veri toplama araçlarının**; kurum faaliyetlerini aksatmadan, gönüllülük esasına göre, başta Türkiye Cumhuriyeti Anayasası olmak üzere 6698 sayılı Kişisel Verilerin Korunması Hakkındaki Kanun'a, ilgi (a) Genelge hükümlerine ve Türk Millî Eğitimi'nin amaçlarına uygun şekilde, denetimi il/ilçe millî eğitim müdürlükleri ile okul/kurum idaresinde olmak üzere 2022-2023 Eğitim Öğretim Yılı'nda Müdürlüğümüze bağlı resmi/özel ortaokullarda öğrenim gören öğrencilerin katılımıyla uygulanmasında sakınca olmadığına ilişkin ilgi (c) Makam Oluru ekte gönderilmiş olup **araştırma ile ilgili sonuç raporunun çalışmanın bitiş tarihinden itibaren 30 gün içinde Müdürlüğümüze gönderilmesi** hususunu;

Bilgilerinize arz ederim.

İsa KIRAL
İl Milli Eğitim Müdür V.

Ekler:
1- Makam Onayı (1 Sayfa)
2- Komisyon Oluru ve Mühürlü Evrak (7 Sayfa)

EK 3: Kişisel Bilgiler Formu

ORTAOKUL ÖĞRENCİLERİNİN BİLGİ GÜVENLİĞİ VE ETİK FARKINDALIĞI ÖLÇEĞİ KİŞİSEL BİLGİLER FORMU

Sevgili öğrenciler, Ortaokul Öğrencilerinin Bilgi Güvenliği ve Etik Farkındalığı isimli çalışmamamızda ortaokul seviyesindeki öğrencilerin bilgi güvenliği ve etik konusundaki farkındalık düzeylerini belirlemek amaçlanmaktadır. Bu çalışmaya katılımınız gönüllülük esaslıdır. Bu çalışmaya katılım sağladığınız taktirde bilgi güvenliği ve etik konularında bilgi edinme imkânı bulabileceksiniz. Aşağıda yer alan sorulara cevap vermeniz yaklaşık olarak 6-7 dakikanızı alacaktır. Katılımınız için teşekkür ederim.

Ahmet YILMAZ

Bartın Üniversitesi Lisansüstü Eğitim Enstitüsü

Bilgisayar Teknolojileri ve Bilişim Sistemleri Bölümü

Cinsiyetiniz:

- Kız
- Erkek

Yaşınız:

- 11
- 12
- 13
- 14

Sınıfınız:

- 5. Sınıf
- 6. Sınıf
- 7. Sınıf
- 8. Sınıf

Annenizin eğitim durumu:

- İlkokul
- Ortaokul
- Lise
- Üniversite

Babanızın eğitim durumu:

- İlkokul
- Ortaokul
- Lise
- Üniversite

Eğitim gördüğünüz okulun türü:

- Özel
- Devlet

Eğitim gördüğünüz okulun yerleşimi:

- Merkez
- Köy

Kendinize ait kullandığınız cihazlar:

- Cep telefonu
- Bilgisayar
- Tablet PC

Sahip olduğunuz cihazları (Cep telefonu, Bilgisayar, Tablet PC) günlük kullanma süreniz:

- 1 saat
- 2 saat
- 3 saat ve üzeri

Sahip olduğunuz cihazlarda (Cep telefonu, Bilgisayar, Tablet PC) internet bağlantısı durumu:

- Var
- Yok

Sahip olduğunuz cihazlarda (Cep telefonu, Bilgisayar, Tablet PC) antivirüs programı kullanma durumu:

- Evet
- Hayır

EK 4: Bilgi Güvenliği ve Etik Farkındalığı Ölçeği (BGEFÖ)

BİLGİ GÜVENLİĞİ VE ETİK FARKINDALIĞI ÖLÇEĞİ Aşağıda sizlere yöneltilen ifadelere "Kesinlikle Katılmıyorum", "Katılmıyorum", "Kararsızım", "Katılıyorum" ve "Kesinlikle Katılıyorum" şeklindeki seçeneklerden yalnızca size en yakın olan birini seçiniz.	**Kesinlikle Katılmıyorum**	**Katılmıyorum**	**Kararsızım**	**Katılıyorum**	**Kesinlikle Katılıyorum**
1.Bilgisayar, telefon ve tablet gibi cihazlarımın şifrelerini belirlerken başkalarının tahmin edemeyeceği şifreler belirlerim.					
2.Kendime ait cihazlarımda kullandığım şifrelerimi kimseyle paylaşmam.					
3.Kullanıcı şifrelerimi oluştururken tahmin edilmesi zor olacak şekilde belirlerim.					
4. Verileri düzenli veya otomatik olarak yedeklerim.					
5.USB bellekleri bilgisayarımdan çıkarırken donanımı güvenli kaldır seçeneğini kullanırım.					
6.Okullarda bilgi güvenliği ile ilgili yeterince bilgilendirmeler yapıldığını düşünüyorum.					
7.İndirdiğim dosyaları açmadan önce virüs taraması yaparım.					
8.Kablosuz modem şifremi aralıklarla değiştiririm.					
9.Başkalarının bilgilerini ve fotoğraflarını paylaşırken onlardan izin alırım.					
10.Başkalarının bilgisayarını ve telefonunu izinsizce karıştırmam.					
11.Başkaları hakkında gerçek dışı paylaşımlarda bulunmam.					
12.Sahibinin izni olmadan resim, video vb. içerikleri kullanmam.					
13.Arkadaşlarımın bilgisayar kullanırken yaptıkları işleri onlardan habersiz izlemem.					
14.Diğer insanlar hakkında izinleri olmadan bilgi toplamam.					
15.Başkalarına ait internet bağlantısını izni olmadan kullanmam.					
16.Doğruluğundan emin olmadığım bilgileri internet ortamında paylaşmaktan sakınırım.					
17.Başkalarının şifrelerini ve üyelik bilgilerini kullanmam.					

ÖZGEÇMİŞ