ÖĞRETMENLERİN
DİJİTAL VERİ GÜVENLİĞİ FARKINDALIĞI

Eray YILMAZ

(Doktora Tezi)

Nisan 2015

ÖĞRETMENLERİN DİJİTAL VERİ GÜVENLİĞİ FARKINDALIĞI

Eray YILMAZ

DOKTORA TEZİ

Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı

1. Danışman: Yard. Doç. Dr. Yusuf Levent ŞAHİN

2. Danışman: Doç. Dr. Yavuz AKBULUT

Eskişehir

Anadolu Üniversitesi Eğitim Bilimleri Enstitüsü

Nisan 2015

JÜRİ VE ENSTİTÜ ONAYI

Eray YILMAZ'ın "Öğretmenlerin Dijital Veri Güvenliği Farkındalığı" başlıklı tezi 21.04.2015 tarihinde, aşağıda belirtilen jüri üyeleri tarafından Anadolu Üniversitesi Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliğinin ilgili maddeleri uyarınca Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı Bilgisayar ve Öğretim Teknolojileri Öğretmenliği Programında, Doktora tezi olarak değerlendirilerek kabul edilmiştir.

	Adı-Soyadı	**İmza**
Üye (Tez Danışmanı)	: Yard.Doç.Dr. Yusuf Levent ŞAHİN	.....
Üye	: Doç.Dr. Abdullah KUZU	.....
Üye	: Doç.Dr. Suzan Duygu ERİŞTİ	.....
Üye	: Doç.Dr. Ahmet Naci ÇOKLAR	.....
Üye	: Yard.Doç.Dr.Tayfun TANYERİ	.....

Prof.Dr.Esra CEYHAN
Anadolu Üniversitesi
Eğitim Bilimleri Enstitüsü Müdürü

ÖZET

ÖĞRETMENLERİN DİJİTAL VERİ GÜVENLİĞİ FARKINDALIĞI

Eray YILMAZ
Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı
Anadolu Üniversitesi Eğitim Bilimleri Enstitüsü
Nisan 2015

1. Danışman: Yard. Doç. Dr. Yusuf Levent ŞAHİN
2. Danışman: Doç. Dr. Yavuz AKBULUT

Yaşamın her alanında sıklıkla kullanılan bilgi iletişim teknolojileri sayesinde, geçmişte basılı materyallerle çalışan öğretmenler, günümüzde bilgiyi dijital ortamlarda üretmekte ve yine dijital ortamlarda saklamaktadır. Eğitim öğretim faaliyetlerinde teknolojiyi sıkça kullanan öğretmenlerin sahip oldukları dijital verilerin güvenliği son derece önemlidir. Veri güvenliğinin öneminden yola çıkan bu araştırmanın amacı, Milli Eğitim Bakanlığı'na bağlı okullarda görev yapan öğretmenlerin dijital veri güvenliği farkındalıklarını belirlemeye yönelik bir ölçek geliştirmek ve ilgili ölçeği kullanarak var olan durumu ortaya koymaktır.

Ölçek geliştirme sürecinde alanyazın taraması ve kritik paydaşlarla yapılan odak grup görüşmeleri sonucunda 93 maddeden oluşan madde havuzu ortaya konmuştur. 12 alan uzmanının görüşü alındıktan sonra taslak ölçek formunun ön deneme uygulaması ilkokul, ortaokul ve lise düzeyinde birer okuldan 79 öğretmen ile gerçekleştirilmiştir. Uygulama sonunda katılımcılar tarafından anlaşılamayan maddeler çıkarılmıştır. Ölçeğin yapı geçerliği için 529 öğretmenden toplanan veriler ile açımlayıcı faktör analizi (AFA) yapılmıştır. AFA'dan önce 56 maddeden oluşan taslak ölçek, analiz sonrasında öğretmenlerin dijital veri güvenliği farkındalığını belirlemeye yönelik tek faktörlü 32 maddelik yapıya kavuşmuştur. Beşli Likert tipindeki ölçeğin Cronbach Alfa (α) iç tutarlık katsayısı .945'tir ve toplam açıklanan varyans % 36.053 olarak hesaplanmıştır.

AFA sonucunda ortaya konan faktör yapısını doğrulamak için 335 farklı katılımcı ile doğrulayıcı faktör analizi (DFA) gerçekleştirilmiştir. Modifikasyon indeksleri yardımı ile ideal değerlere ulaşan tek faktörlü yapı, dijital veri güvenliği farkındalık ölçeğinin (DVGFÖ) geçerli ve güvenilir olduğunu, ileride yapılacak araştırmalarda kullanılabileceğini göstermiştir.

Balıkesir ilindeki öğretmenlerin dijital veri güvenliği farkındalıklarını belirlemek için 29 farklı okulda görevli 1446 öğretmenden DVGFÖ kullanılarak veri toplanmıştır. Bulgular, öğretmenlerin dijital veri güvenliği farkındalıklarının 4.16 ortalama ile oldukça yüksek olduğunu göstermiştir. Öğretmenler; parola oluştururken harf, sayı ve özel karakter kullanmanın önemi, e-posta ile gelen kimlik bilgilerini doğrulama mesajlarına (parola, kredi kartı vb.) itibar edilmemesi ve parola hatırlatmak için kullanılan güvenlik sorularına başkalarının tahmin edemeyeceği yanıtlar verilmesi konularında daha yüksek farkındalığa sahiptir. Güvenlik duvarı yazılımları, İnternet sitelerinde kullanılan güvenlik sertifikaları ve verilerin çeşitli uygulamalar (Dropbox, Google Drive vb.) kullanılarak İnternet ortamında saklanabileceği konularındaki farkındalıkları ise daha düşüktür.

Bu araştırmada, bazı demografik değişkenlere ilişkin tanımlayıcı istatistiklerin yanında bu değişkenler ile dijital veri güvenliği farkındalığı arasındaki ilişkiler de incelenmiş ve sonuçlar yorumlanmıştır. Buna göre; cinsiyet, günlük bilgisayar kullanım süresi, günlük İnternet kullanım süresi, kişisel bilgisayar, tablet bilgisayar ve akıllı telefon sahibi olma durumlarına göre öğretmenlerin dijital veri güvenliği farkındalıklarının değiştiği sonucuna ulaşılmıştır.

Araştırmada, MEB tarafından hayata geçirilen projelerde dijital veri güvenliğinin yeterince yer bulmaması ve öğretmenlerin eğitim öğretim etkinliklerinde bilişim teknolojilerini kullanırken dijital veri kaybı yaşamamaları için yapılması gerekenler vurgulanmıştır. Bu araştırmadan elde edilen sonuçların; öğretmenlerde dijital veri güvenliği farkındalığı oluşturulmasına katkı sağlayacağı, MEB'in gerçekleştireceği hizmet içi eğitim faaliyetlerinin planlanmasında içerik belirleme çalışmalarına yön vereceği ve ileriki araştırmalara ışık tutacağı düşünülmektedir.

Anahtar Sözcükler: Öğretmen, Dijital Veri, Veri Güvenliği, Veri Güvenliği Farkındalığı, Ölçek Geliştirme, Açımlayıcı Faktör Analizi, Doğrulayıcı Faktör Analizi

ABSTRACT

DIGITAL DATA SECURITY AWARENESS OF TEACHERS

Eray YILMAZ
Department of Computer Education and Instructional Technology
The Graduate School of Educational Sciences
April 2015

Advisor-1: Asst. Prof. Dr. Yusuf Levent ŞAHİN
Advisor-2: Assoc. Prof. Dr. Yavuz AKBULUT

Teachers who used to work with printed materials produce and keep the information in digital environment today thanks to information and communication technologies which are frequently used in all areas of our lives. The purpose of this study which has derived from the importance of sustaining digital data security of teachers, who use technology in educational activities, is to develop a scale in order to identify the digital data awareness of teachers who work in the schools of Ministry of Education, and to present the existing condition by means of the developed scale.

The literature review and focus group interviews with critical partners led to an item pool of 93 statements. After the reviews of 12 field experts, piloting of the draft form was conducted with 79 teachers who were from different elementary, secondary and high schools. After the application process, incoherent items were taken out by the participants. An exploratory factor analysis was performed for the construct validity of the scale through the data collected from 529 teachers. The draft scale which consisted 56 items before the exploratory factor analysis turned into a single factor structure with 32 items. The internal consistency coefficient (Cronbach's Alpha=α) of the scale was .945 and the total variance was calculated as 36.053 %.

A confirmatory factor analysis was carried out with 335 different participants in order to confirm the factor structure revealed in the exploratory factor analysis. The single factor structure which reached to ideal values by means of modification indexes

proved the reliability and validity of digital data security awareness scale and its applicability for further studies.

In order to identify the digital data security awareness of teachers, the data were collected through the developed scale from 1446 teachers in 29 different schools in Balıkesir province. Findings revealed that digital data security awareness of teachers were quite high with an average of 4.16. Teachers had more awareness regarding the importance of using letters, numbers and special characters when creating password, not considering the e-mails for identity confirmation (password, credit card, etc.) and providing unpredictable responses to the security questions for password reminder. On the other hand, the awareness was lower with regard to the issues of firewall software, security certificate of websites and the storage of data in Internet environment via several applications (Dropbox, Google drive, etc.)

In this research, descriptive statistics with regard to some demographic variables and the relationship between these descriptive statistics and digital data security awareness were investigated and the results were interpreted. It was found that digital data security awareness of teachers varies with regard to gender, duration of daily computer use, duration of daily Internet use, having personal computer, tablet computer and smart phone.

In the study, inadequate consideration on digital data security of the projects developed by the Ministry of Education and the things to be done in order to prevent data loss while using information technologies in educational activities were emphasized. The study can make a contribution to raise the awareness of teachers on digital data security, to direct studies to determine the contents of relevant in service training activities of the Ministry of Education, and can shed light on further research.

Key Words: Teacher, Digital Data, Data Security, Data Security Awareness, Scale Development, Exploratory Factor Analysis, Confirmatory Factor Analysis

ÖNSÖZ

Balıkesir Eskişehir arasında uzun ve yorucu yolculuklarla geçen, bir o kadar da yaşantıma ve bilime olan bakışıma değer katan bir süreç oldu doktora eğitimi. Bu sürecin son aşaması olan doktora tezim ise, akademik duruşumun şekillendiği yolculuğun bir ürünü. Yaklaşık iki yıllık emeğin sonucunda ortaya çıkan bu tezde, Milli Eğitim Bakanlığı'na bağlı resmi ve özel okullardaki öğretmenlerin dijital veri güvenliği farkındalıklarına yönelik bir ölçme aracı ortaya konmuş ve Balıkesir ilindeki öğretmenlerin bu konudaki farkındalıkları incelenmiştir.

Uzun soluklu bir süreçte ortaya koyduğum bu tezin oluşmasında doğrudan veya dolaylı olarak pek çok değerli insan katkı sağladı. Bu nedenle süreçte emeği olan herkesi anmak gerektiğine inanıyorum.

Bu tez çalışmasının başlangıcından tamamlanmasına kadar yardımlarını esirgemeyen, beni sürekli cesaretlendiren, yönlendiren, yol gösteren, bilgi ve deneyimlerini paylaşan, akademik gelişimime büyük katkıları olan değerli danışmanlarım Yard. Doç. Dr. Yusuf Levent ŞAHİN'e ve Doç. Dr. Yavuz AKBULUT'a ne kadar teşekkür etsem azdır.

Tez izleme komitesinde yer alan, değerli görüş ve önerileriyle tezime katkı sağlayan Doç. Dr. Abdullah KUZU'ya ve Doç. Dr. Duygu Erişti'ye, tez savunma jürimde yer alarak yapıcı önerileriyle tezime katkıda bulunan Doç. Dr. Ahmet Naci ÇOKLAR'a ve Yard. Doç. Dr. Tayfun TANYERİ'ye çok teşekkür ederim.

Bilgi ve tecrübeleri ile akademik bakışıma yön veren ders hocalarım Prof. Dr. Hatice Ferhan ODABAŞI'ya, Doç. Dr. Adile Aşkım KURT'a, Doç. Dr. Işıl KABAKÇI'ya ve Yard. Doç. Dr. Sema ÜNLÜER'e teşekkürlerimi sunarım.

Yeterlik sınavının stresli dakikalarını birlikte paylaştığım, tez çalışmalarımızı paralel götürerek sıklıkla bilgi alışverişinde bulunduğum değerli arkadaşlarım Osman EROL'un ve Halil İbrahim HASESKİ'nin de bu sürece katkıları benim için değerlidir.

Doktora sürecinin başından sonuna kadar, özellikle de ölçek geliştirme sürecinde hep yanımda olan dostum Erkan DURAN'a, varlığı sayesinde en yorulduğum ve bunaldığım zamanlarda bile beni yüreklendiren dostum Ozan ŞEREFHANOĞLU'na, verilerin toplanmasında ve araştırma izin onaylarında desteklerinden dolayı Balıkesir İl

Milli Eğitim Müdürlüğü AR-GE birimi çalışanlarına ve özellikle de arkadaşlığımızın uzun bir geçmişe dayandığı Erkan KAMERTAY'a teşekkürü bir borç bilirim.

Bu günlere gelmemde bana her türlü desteği sunan sevgili annem Şahide YILMAZ'a, sevgili babam Sadullah YILMAZ'a ve kardeşim Elif KOBAK'a sonsuz teşekkürler.

Doktora sürecinin başından sonuna en büyük manevi desteği hissettiren meslektaşım ve sevgili eşim Selvin YILMAZ'a, birlikte oyunlar oynayabileceğimiz eğlenceli zamanlarından vazgeçip çalışmama fırsat veren ancak bilgisayarın başına geçtiğimde bu tez ne zaman bitecek diyerek sabırla bekleyen güzel kızım Cansın'a kucak dolusu teşekkürler. İyi ki varsınız…

Eray YILMAZ
Eskişehir, 2015

ÖZGEÇMİŞ

Eray YILMAZ
Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı
Doktora

Eğitim

Yüksek Lisans	2004	Balıkesir Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı
Lisans	2002	Balıkesir Üniversitesi, Necatibey Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü
Lise	1998	Balıkesir Anadolu Teknik Lisesi, Bilgisayar Bölümü

İş

2013-	T.C. Ziraat Bankası Balıkesir Fen Lisesi, Bilişim Teknolojileri Öğretmeni
2011-2013	Balıkesir İl Milli Eğitim Müdürlüğü, AR-GE ve Strateji Geliştirme Birimi
2002-2011	23 Nisan İlköğretim Okulu, Bilişim Teknolojileri Öğretmeni

Seçilmiş Yayınlar

Yılmaz, E. (2014). Why do gamers use Facebook? A study on social network game members in Turkey. *European Journal of Educational Technology*, *2*(1), 17-29.

Yılmaz, E., Şahin, Y. L., Haseski, H. İ. ve Erol, O. (2014). Lise öğrencilerinin İnternet bağımlılık düzeylerinin çeşitli değişkenlere göre incelenmesi: Balıkesir ili örneği. *Eğitim Bilimleri Araştırmaları Dergisi, 4*(1), 133-144.

Haseski, H., Şahin, Y. L., Yılmaz, E. ve Erol, O. (2014). The investigation of the relationship between lifelong learning tendencies and aims of using Facebook. *Journal of Theory and Practice in Education, 10*(2), 331-351.

Kişisel Bilgiler

Doğum Yeri ve Yılı: Afyon – 1980 Cinsiyeti: Erkek Yabancı Dili: İngilizce

İÇİNDEKİLER

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR LİSTESİ

AB : Avrupa Birliği

AFA : Açımlayıcı Faktör Analizi (EFA- Exploratory Factor Analysis)

BİT : Bilgi ve İletişim Teknolojileri

CFI : Comparative Fit Index

DFA : Doğrulayıcı Faktör Analizi (CFA- Confirmatory Factor Analysis)

DVGFÖ : Dijital Veri Güvenliği Farkındalık Ölçeği

EBA : Eğitim Bilişim Ağı

FATİH : Fırsatları Arttırma ve Teknolojiyi İyileştirme Hareketi

GFI : Goodness of Fit Index

GİS : Görevli İşlemleri Sistemi

İLSİS : İl ve İlçe Milli Eğitim Müdürlükleri Yönetim Bilgi Sistemi

MEB : Milli Eğitim Bakanlığı

MEBBİS : Milli Eğitim Bakanlığı Bilişim Sistemleri

MEGP : Milli Eğitimi Geliştirme Projesi

MLO : Müfredat Laboratuvar Okulu

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

RMSEA : Root Mean Square Error of Approximation

TAIS : Teacher Awareness of Internet Safety (İnternet Güvenliğinde Öğretmen Farkındalığı)

TÜİK : Türkiye İstatistik Kurumu

BİRİNCİ BÖLÜM
GİRİŞ

Yeni teknolojilerin ortaya çıkması ve topluma yayılması, yaşam alışkanlıklarının değişmesine, sosyal kavramların da biçimlenmesine neden olmuştur. Bilgi toplumu olma yolundaki hızlı değişim sürecinde etkin rol oynayan bilgi ve iletişim teknolojileri; iletişim, elektronik bankacılık, elektronik imza, uzaktan eğitim, kamu hizmetleri ve e-devlet uygulamaları gibi pek çok alanda yer alarak günlük yaşamı bütünüyle değiştirmeye başlamıştır.

Bilişim teknolojilerindeki gelişmeler sayesinde dünya küçük bir köy haline gelmekte, toplumda e-yaşamın kapıları aralanmaktadır. E-yaşam, zamanla toplumun daha karmaşık bir yapıya bürünmesine neden olmuş, üretim, iletişim, ulaşım, eğitim, ticaret tarzlarını değiştirmiştir (Karakaş, 2002). Ülkemizde de bilgisayar ve mobil iletişim cihazları her geçen gün artarak kullanılmaktadır. Buna paralel olarak da her alanda üretilen bilgi miktarı hızla artmaktadır.

Bilgi toplumuna dönüşüm sürecinde ekonomik ve sosyal yaşamdaki pek çok işlemin kolaylaşmasının yanı sıra bilgi güvenliğine karşı çeşitli boyutlarda risk ve tehditler de ortaya çıkmaktadır. Bu teknolojileri kullanan kişilerin büyük çoğunluğu bilgi güvenliğine karşı oluşabilecek risk ve tehditlerin farkında değildir. Oluşan bu risk ve tehditler, kişilerin çoğunlukla maddi kayba uğramalarına ya da bilgilerinin değiştirilmesi, silinmesi ya da bilgilerine izinsiz olarak erişilmesi gibi istenmeyen bazı durumlara neden olabilmektedir.

Bilgiye sürekli olarak erişilebilen bir ortamda, bilginin göndericisinden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkalarının eline geçmeden bütünlüğünün sağlanması ve güvenli bir şekilde iletilmesi süreci bilgi güvenliği olarak tanımlanabilir (Schmidt, 2004). Bilgi güvenliğinin temel unsurları; gizlilik, bütünlük ve erişilebilirliktir (Fussell, 2005; McCumber, 2005; Schlienger ve Teufel, 2001). Buna göre:

- Gizlilik (Confidentiality): Bilgiye yetkisiz kişilerce erişilememesidir.
- Bütünlük (Integrity): Bilginin doğruluğunun ve tamlığının sağlanmasıdır. Bilginin içeriğinin değiştirilmemiş ve hiçbir bölümünün silinmemiş ya da yok edilmemiş olmasıdır.
- Erişilebilirlik (Availability): Bilginin bilgiye erişim yetkisi olanlar tarafından istenildiği anda ulaşılabilir ve kullanılabilir olmasıdır.

Bu üç temel unsur, bilgi güvenliğinin birbirinden bağımsız düşünülemeyeceği bileşenleridir. Gizliliğinin sağlanması o bilginin erişilebilirliğini engellememelidir. Aynı zamanda erişilebilirliği sağlanan bilginin bütünlüğünün sağlanması da önemlidir. Eğer bir bilgi için yalnızca gizlilik sağlanıyor, ancak bilgiye erişim engelleniyor ise kullanılamaz durumdaki bu bilginin bir değeri olmayacaktır. Eğer erişimi sağlanıyor ancak bütünlüğü sağlanamıyor ise bu kez de yanlış veya eksik bilgi söz konusu olacak ve olumsuz sonuçlara neden olabilecektir. Dolayısıyla bilgi güvenliği kavramı temel olarak bu üç unsurun bir arada sağlanmasıdır (Fussell, 2005).

Bilgi güvenliği kavramı, 1990'lı yıllara kadar olan süreçte yazılı basılı ortamlardaki bilgilerin daha çok fiziksel anlamda güvenliğinin sağlanması olarak ifade edilmiştir. Cep telefonu, bilgisayar ve İnternetin günlük yaşamda etkin bir şekilde kullanılması sonrasındaki büyük dönüşüm ve bilgi transferindeki artış, bilgi güvenliğinin tanımının da değişmesine neden olmuştur. Günümüzde bilgi güvenliği kavramına bilişim teknolojileri açısından bakıldığında dijital veri güvenliği kavramı ön plana çıkmaktadır.

Dijital Veri Güvenliği

Bilgisayarların ve iletişim ağlarının günümüzde yoğun bir şekilde kullanılması ile teknolojik güvenlik ve dijital ortamlardaki verilerin güvenliği konuları önem kazanmıştır. Bilginin elektronik ortamlarda üretilmesi ve sunulması, sağladığı avantajlar yanında çeşitli güvenlik sorunlarını da beraberinde getirmiştir.

Elektrik kesintisi ile oluşan veri kayıpları, dosyalara dışarıdan erişimin engellenmesine yönelik bilgisayarların korunması ve şifrelenmesi, gizlilik ve telif hakları vb. gerekçelerle elektronik ortamdaki dijital verilerin güvenliği önem

kazanmıştır. Bu noktadan hareketle bilgi güvenliği konusunda yapılan çalışmalar dijital veri güvenliği kapsamında değerlendirilmiştir.

Canbek ve Sağıroğlu (2006:168) dijital veri güvenliğini, "elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması sırasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür" biçiminde tanımlamıştır.

Kişiler ve kurumlar, bilişim teknolojilerini kullanırken kendilerini bekleyen tehdit ve tehlikeleri daha önceden analiz ederek gerekli önlemleri aldıklarında dijital veri güvenliğini sağlamış olacaktır (Vural ve Sağıroğlu, 2008).

Keleş ve Güneş'e göre (2013) bilişim teknolojilerindeki gelişmeler sonucunda kurum ve kuruluşlar dokümanlarını saklamak için bilgilerini dijital ortama taşımış ancak bu dokümanların çalınması, yetkisiz kullanıcılar tarafından erişilmesi ile telafisi çok güç sonuçlar ortaya çıkmasına neden olmuştur.

Yaşanabilecek tüm olumsuzlukların önüne geçebilmek adına bilgi ve kişisel verilerin güvenliğinin korunmasına ilişkin acil önlemlerin alınması gerekir. Bu doğrultuda bilgi güvenliği ve kişisel verilerin korunmasına ilişkin standartlar ve yöntemler belirlenmelidir (Ketizmen ve Ülküderner, 2007).

Dijital veri güvenliğinin sağlanmasında etkili olabilecek pek çok önlemden söz edilebilir. Bilgi Güvenliği Derneği tarafından düzenlenen Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Sonuç Bildirgesi'nde (2012); daha güvenli politikaların uygulanması % 58, kişisel ve kurumsal gayretler % 20, daha ileri teknoloji kullanımı % 18, kanun ve yönetmeliklerdeki iyileştirilmeler ise % 7 oranında güvenliğin sağlanmasına katkı sağlar şeklinde raporlanmıştır.

Kişisel verilerin güvenliğini sağlamada kullanılan yaklaşımlardan biri de, veriyi bir nesnenin içerisine gizli biçimde yerleştirmeyi esas alan steganografi (veri gizleme bilimi) tekniğidir. Yalman ve Ertürk (2009) çalışmalarında bu bilimin sayısal ortamdaki kullanım alanı olarak metin, sayısal ses, sayısal resim ve sayısal görüntünün esas alındığı farklı örnekler vermiştir. Çalışma sonunda steganografinin, önümüzdeki yıllarda bilgisayar ağlarındaki ve sayısal ortamlardaki dijital veri güvenliğini sağlamada çok önemli bir yer tutacağı öngörülmektedir.

Kurum ve kuruluşlar genellikle önceden önlem almak yerine, bilgi güvenliği konusunda bir olay baş gösterdiğinde harekete geçme eğilimindedirler. Bu bakımdan bilgi güvenliği konusunda farkındalığın arttırılmasına ihtiyaç vardır. Özellikle yönetim seviyesindeki kişilerin farkındalık ve anlayışı, bilgi güvenliği kültürü oluşturulması açısından önemlidir (Kocamustafaoğulları, 2013).

Ülkemizde dijital ortamda yaşanan problemlerin çözümüne yönelik olarak iç ve dış güvenliğimizi sağlayan birimlerin bünyesinde çeşitli çalışmalar yapılmaktadır. Çiçek ve Okatan (2008) bu birimlere örnek olarak Emniyet Genel Müdürlüğü bünyesindeki Bilişim Suçları ve Sistemleri Şube Müdürlükleri'ni ve Jandarma Genel Komutanlığı bünyesindeki Kriminal Daire Başkanlığı'na bağlı Bilişim Teknolojileri İnceleme Şube Müdürlüğü'nü göstermektedir. Bu birimin aktif görevleri arasında; cep telefonu, sabit disk, SIM kart, multimedya kart ve çeşitli veri kartlarını incelemek yer almaktadır.

MEB Bilgi İşlem Dairesi Başkanlığı tarafından (2012) yayımlanan Bilgi ve Sistem Güvenliği Yönergesi de ilgili bakanlığın kurum olarak konuyu önemsediğinin bir göstergesidir. Yönergenin amacı, Bakanlık merkez ve taşra teşkilatındaki tüm personel ile kendilerine herhangi bir nedenle Bakanlık bilişim kaynaklarını kullanma yetkisi verilen konukların, Millî Eğitim Bakanlığı bünyesinde bulunan bilişim kaynaklarının kullanımına yönelik usul ve esasları belirlemektir.

5018 Sayılı Kamu Mali Yönetimi ve Kontrol Kanunu olarak adlandırılan ve kamu kaynaklarının etkili, ekonomik, verimli ve kurumun amaçlarına uygun biçimde kullanılması, kurum varlıklarının korunması, yolsuzluk ve usulsüzlüklerin önlenmesi amacı ile uygulamaya konulan iç kontrol sisteminin eylem planındaki beş bileşenden en önemlisi Bilgi ve İletişim'dir. Buna göre kurumların sahip olduğu gelen ve giden her türlü evrak dâhil iş ve işlemlerin kaydedildiği, sınıflandırıldığı ve dosyalandığı kapsamlı ve güncel sistemde kayıt ve dosyalar, kişisel verilerin güvenliğini ve korunmasını sağlamalıdır (Tümer, 2010). Devletin yasama organı tarafından çıkarılan bu kanun da devlet kurumlarında dijital veri güvenliğine verilen önemi işaret etmektedir.

Dijital Veri Güvenliğini Tehdit Eden Unsurlar

Bilişim teknolojisindeki gelişmelerin en önemli ürünlerinden olan bilgisayarların ve İnternetin yoğun olarak kullanılması etkinlik ve verimliliği önemli ölçüde arttırmıştır. Ancak bu teknolojiler sağladığı yararlar yanında pek çok dijital veri güvenliği sorununu

da beraberinde getirmiştir. Bu sorunlardan bazıları; bilgisayar virüsleri, teknik problemler, bilgisayar hileleri, bilgi hırsızlığı, yetkili erişimleri kasıtlı veya kasıtsız olarak kötüye kullanma olarak sıralanabilir.

Tehditlerin bilgi sistemlerinde etkili olabilmek için sistem üzerindeki açıkları kullandığını vurgulayan Vural (2007) tehditlerin bilgi varlıklarına etkilerinin; tehlikenin gerçekleşme olasılığı, sistemdeki açık miktarı ve bilginin değeri ile doğru orantılı olduğunu belirtmiştir. Böylece bilgi sistemlerinde tehditler, uygun şartların oluşmasıyla zarar verilebilecek zafiyetlere, zafiyetler de saldırganlar tarafından kullanıldığında güvenlik ihlallerine yol açarak bilgi sitemlerine zarar vermektedir.

Say ve Sağıroğlu (2004) veri girişinde sıkça kullandığımız klavyelerin güvenlik noktasındaki önemine dikkat çekerek, tuşlarına basılan her karakterin başkalarının eline kolaylıkla geçebileceğini, toplanan bu bilgilerin depolanarak uygun bir zamanda istenen adreslere e-posta yoluyla kolaylıkla iletilebileceğini vurgulamıştır.

Dijital veri güvenliğini tehdit eden ana unsurlar arasında; doğal afetler nedeniyle güç kaynaklarının, kamera sistemlerinin ve telefon santrallerinin arızalanması, e-posta, İnternet bankacılığı, çevrimiçi alışveriş ve donanım kaynaklı sorunlar ile yazılım tehditleri sayılabilir. Başlıca yazılım tehditleri şunlardır:

- *Hizmetin Engellenmesi Saldırıları (DDoS-Distributed Denial of Service):* Bilgi ve iletişim sistemlerinin aşırı biçimde yüklenmesi ile devre dışı bırakılması için yapılan saldırılardır (Krause ve Tipton, 2007).
- *Truva Atı (Trojan):* Genellikle lisanssız yazılım, mp3, oyun ve cinsel içeriklere ekli olarak gelen dosyalar aracılığıyla bulaşan ve bilişim sistemlerine zarar veren programlardır (Krause ve Tipton, 2007). Microsoft Güvenlik İstihbarat Raporu (2014) verilerine göre dünya genelinde yapılan araştırmada Türkiye % 25.9 ile "trojen" bulaşan bilgisayar oranında birinci sıradadır.
- *Mantık Bombası (Logic Bomb):* İlgili sisteme girdikten sonra sistem tarihini kontrol ederek harekete geçen ve önceden planlanan saatte sisteme zarar veren ya da programcısından gelen mesaja göre devreye giren zararlı yazılımlardır (Atalıç Taş, 2010).
- *Arka Kapı (Back Door):* Bilgisayar üzerinde sıradan taramalarla bulunamayacak şekilde, kimlik doğrulama süreçlerini atlamayı veya kurulan

bu yapıdan haberdar olan kişiye o bilgisayara uzaktan erişmeyi sağlayan yöntemlerdir (Canbek ve Sağıroğlu, 2007a).

- *Solucanlar (Worms):* Çoğalan, bağımsız şekilde çalışabilen ve ağ bağlantıları üzerinde hareket edebilen programlardır. Virüs ve solucanlar arasındaki temel fark solucanların virüslerin aksine taşıyıcı bir dosyaya gereksinim duymamalarıdır. Tarihte bilinen ilk solucan, 1988 yılında ortaya çıkan Morris'tir ve dünya üzerinde yaklaşık 6000 bilgisayarı etkilemiştir (Nickolov, 2008).
- *Virüsler (Virus):* Bilgisayarın çalışmasını engelleyecek, verileri bozacak, silecek ya da kendilerini İnternet üzerinden diğer bilgisayarlara yayarak bilgisayarın yavaşlaması gibi sorunlara neden olacak şekilde tasarlanmış kötü amaçlı yazılımlardır (Microsoft, 2005).
- *Reklam Destekli Yazılımlar (Adware):* Belirli firmalar tarafından sağlanan reklamları programın içine gömerek kullanıcının bu reklamları tıklamasını sağlayan programlardır (Krause ve Tipton, 2007).
- *Casus Yazılımlar (Spyware):* Adware'den farklı olarak, kullanıcının bilgisayarında hem belirli firmaların reklamlarını görüntüleyip hem de bilgisayarınızda ne yaptığınızı belirli bir sunucuya gönderen programlardır (Krause ve Tipton, 2007).
- *Sazan Avlama-Oltalama (Phishing):* Kimlik hırsızlığında en sık kullanılan yöntemlerden biri olan oltalamada genellikle sahte web sayfaları kullanılmaktadır. Bir banka ya da alışveriş sitesinden e-posta geldiğini düşünen kullanıcı, kredi kartı ya da bankacılık bilgilerini sahte web sayfasına girerek ya da e-postayı yanıtlayarak tuzağa düşmektedir (Çubukçu ve Bayzan, 2013). Bu gibi dolandırıcılık olaylarının engellenebilmesi amacıyla, İnternet bankacılığında kullanılması gerekli olan kullanıcı adı ve şifre bilgilerine ek olarak, 2009 yılında BDDK tarafından zorunlu hale getirilen ve 2010 yılından itibaren uygulanmasına başlanan IBAN numarası ve GSM şebekeleri üzerinden tek kullanımlık şifre düzenlemeleri hayata geçirilmiştir (Turhan, 2010).
- *Zincir E-posta ve İnternet Aldatmacası (Hoax):* Birçok kişinin birbirine gönderdiği ve insanların çok fazla ilgisini çekebilecek sömürü içerikli e-

postaları alıcının listesindeki diğer kişilerle paylaşmasını isteyen iletilerdir. İnternet aldatmacası ise bir kurum, kuruluş ya da tanınmış bir kişi hakkında uydurma hikâye ve haberler üreterek zarara uğratmak, kişisel ya da ulusal güvenliği tehdit edecek durum olduğu havası oluşturarak panik havası estirmek şeklinde ortaya çıkmaktadır. Bu tür e-postalar bilinen ve güvenilir olan bir kaynaktan geliyormuş gibi gönderilmekte ve alıcının bu mesajı, listesindeki tüm kişilerle paylaşması istenmektedir. Zincir e-postalar ve İnternet aldatmacalarının temel amacı; mesajların mümkün olduğu kadar çok kişiye ulaşmasını sağlayarak e-posta adreslerinin toplanmasını sağlamaktır. Bu şekilde ele geçirilen e-posta adresleri üçüncü kişilere bir ücret karşılığında satılmakta ya da istem dışı e-posta göndermede kullanılmaktadır (Schryen, 2007).

- *İstem Dışı Elektronik Postalar (Spam):* Birden çok kopya göndererek ticari olarak reklam yapmayı amaçlayan e-postalardır (Öztürk, 2009).

Güvenliği tehdit edebilecek diğer zararlı yazılımlar arasında; püsküllü bela yazılımları, web böcekleri, uzaktan yönetim araçları, saldırgan ActiveX kontrolleri, saldırgan Java, saldırgan betik, anahtar üreticiler, şifre yakalayıcılar ve kırıcılar ile iz sürme çerezleri sayılabilir (Canbek, 2005).

Günümüzde kötü niyetli kişiler tarafından istismar edilen bir diğer kullanım alanı ise İnternet kullanıcılarının yaklaşık % 80'inin artık olmazsa olmazlarından olan e-posta, İnternet bankacılığı ve çevrimiçi alışveriştir (Arifoğlu, Kömes, Yazıcı, Akgül ve Ayvalı, 2002). E-posta kullanımının yaygınlaşmasını ve çoğu zaman zorunlu olarak kullanımını fırsat bilen kullanıcılar, istem dışı e-posta yolu ile dolandırıcılık, sahtecilik ve kötü niyetli yazılımların yayılmasına neden olmaktadır. İstem dışı e-postalar zarar verme amacıyla kullanılmasa bile, bunların kontrol edilmesi ve ayıklanması diğer kullanıcılar için zaman kaybına neden olmaktadır.

Dijital veri güvenliğini tehdit eden belki de en önemli unsur ise insan kaynaklı tehditlerdir. Tekerek'e göre (2008) bu tehditler kullanıcının bilinçsizce ve bilgisizce, yeterli eğitime sahip olmadan teknoloji kullanması sonucu veya sisteme zarar verme amaçlı yapılan davranışlar sonucu ortaya çıkar. Canbek ve Sağıroğlu (2007b) bilinçli olarak sisteme zarar verme noktasında ortaya çıkan ve son yıllarda sıklıkla kullanılan

toplum mühendisliği kavramını, bir bilgisayar korsanının ilgilendiği bilgisayar sistemini kullanan veya yöneten meşru kullanıcılar üzerinde psikolojik ve sosyal numaralar kullanarak, sisteme erişmek için gerekli bilgiyi elde etme teknikleri olarak tanımlamaktadır.

Dijital dünyada yaşanan olumsuzluklar ile birlikte anılan "hacker" sözcüğü ise dilimize bilgisayar korsanı olarak çevrilmiştir. Türk Dil Kurumu'nun İnternet üzerindeki sözlüğüne göre, bilgisayar ve haberleşme teknolojileri konusundaki bilgisini gizli verilere ulaşmak, ağlar üzerinde yasal olmayan zarar verici işler yapmak için kullanan kimsedir (Türk Dil Kurumu, 2015).

Bireylerin insan kaynaklı tehditlerle karşı karşıya kaldıkları ortamlardan biri de İnternet'tir. Öztürk (2009) İnternet kullanan bireylerin; sanal sosyal ortamlarda cinsel istismar, müstehcen, zararlı içerik, rahatsız edilme, fiziksel rahatsızlıklar, kişilik bozuklukları, bağımlılık, kötü alışkanlıklar edinme, olumsuz etkilenme, kişisel bilgileri paylaşma ve özel hayata dair görüntülerin yayınlanması gibi önemli sorunlarla karşılaştıklarını belirtmektedir.

Kullanıcılar gibi bilişim cihazları da İnternet'teki tehditler nedeniyle zarar görebilir. Şahinaslan, Şahinaslan, Borandağ ve Şahinaslan (2013) İnternet erişimi olan kişisel bir bilgisayarın siber tehditlere karşı risk altında olduğu durumları; sistemin normalden yavaş çalışması, tarayıcı açık olmadığı halde sürekli ağ hareketliliği, yazılımların beklenmedik tepkiler vermesi, disk üzerindeki dosya artışı, istem dışı yüklenen yeni programlar şeklinde özetlemiştir.

Sahip olduğumuz pek çok önemli verinin İnternet üzerinde depolandığını ve paylaşıldığı düşünürsek, İnternet ortamındaki yenilikler de tehdit oluşturabilir. Bu konuda Çakır (2011) henüz taslak halde bulunan HTML5 standardına dikkat çekmiş, düzgün yorumlanmaması ve/veya uygulanmaması halinde İnternet kullanıcılarının güvenliğini tehlikeye sokacağını belirtmiştir.

Symantec (2013) tarafından yayınlanan 18. İnternet Güvenlik Tehdit Raporu (ISTR) verilerine göre 2012'de gerçekleşen siber saldırılar, bir önceki yıla göre % 42 artmıştır. Raporda öne çıkan bulgulara göre; 2012 yılında web tabanlı saldırıların % 30, zararlı mobil yazılımların % 58, sosyal ağ üzerinden kimlik hırsızlığı yapmayı amaçlayan olta saldırılarının % 125 oranında arttığı gözlemlenmiştir. İlgili raporda mobil telefonlara ve mobil ağlara yapılan saldırıların % 32'sinin kullanıcı bilgilerini

çalma amaçlı gerçekleştirildiği ve Android işletim sisteminin siber suçlular için önemli bir platform haline geldiği belirtilmiştir. Avrupa ülkeleri arasında Türkiye; istem dışı e-posta saldırılarında 5., olta saldırılarında 8., virüs saldırılarında ise 5. sırada yer almaktadır.

Bu bağlamda artan siber güvenlik sorunlarına eğilmek üzere 2008 yılının Ekim ayında Bulgaristan'ın başkenti Sofya'da Uluslararası Telekomünikasyon Birliği (ITU) tarafından "Bölgesel Siber Güvenlik Forumu" düzenlenmiştir ve forumda 25 ülkeden 130 katılımcı yer almıştır. Organizasyon sonrasında yayınlanan raporda (International Telecommunications Union, 2008); siber güvenlik kültürünün teşvik edilmesi, çeşitli aktörlerin rolü, örnek uygulamalar, siber geliştirme faaliyetleri hakkında bilgi paylaşımı, Avrupa ve Bağımsız Devletler Topluluğu ülkeleri tarafından karşılaşılan başlıca siber güvenlik sorunları ele alınmıştır. Ayrıca bölgesel ve uluslararası düzeyde farklı paydaşlar arasında işbirliğinin ve koordinasyonun artırılmasına dikkat çekilmiştir.

Dijital veri güvenliğine yönelik riskler bazen maddi zararlara bazen de hayati tehlikelere yol açabilmektedir. Bazı basit önlemler ile sanal dünyanın gerçek tehlikelerinden korunmak mümkündür. Bu önlemler bireysel olabildiği gibi devlet eliyle yasalar yoluyla da olabilmektedir. Bu konuda yapılmış çalışmalar ve var olan çözümler incelendiğinde önlemler şu şekilde özetlenebilir (Karakoç, 2011; Yavanoğlu, Sağıroğlu ve Çolak, 2012):

- Web sayfalarında istemsiz açılan pencerelerin kapatılması,
- Web sayfalarının güvenlik sertifikalarının kontrol edilmesi,
- Bilgisayarda güncel güvenlik yazılımı bulundurulması,
- Lisanslı yazılımların kullanılması,
- Kullanılan şifrelerin birbirinden bağımsız olması, farklı simge, karakter ve rakam içermesi,
- Şifre hatırlatma için kullanılan gizli soruların ve yanıtlarının zor olması,
- Güvenli olmayan e-postaların açılmadan silinmesi,
- E-postalarla gelen bilinmeyen web sayfalarına giriş işlemi yapılmaması,
- Kablosuz ağ modemlerinin şifresiz kullanılmaması,
- Sosyal paylaşım ağlarında şahsi bilgilerin paylaşılmaması,
- Sosyal paylaşım ağlarında ya da sohbet sitelerinde yabancı kişiler ile görüntülü, sesli ve hatta gerçek hayatta yüz yüze iletişime geçilmemesi,

- Bankacılık ve çevrimiçi alışveriş işlemlerinin gerekmedikçe kişisel bilgisayarlar dışında kullanılmaması,
- Çevrimiçi alışveriş işlemlerinde sanal kart ve limit kullanılması,
- İnternet üzerinden tehdit, şantaj ya da cinsel istismara maruz kalma durumlarında yasal yollara başvurulması.

Bilgi güvenliği konusunda yaşanabilecek sorunların hukuki boyutu incelenecek olursa, Yeni Türk Ceza Kanunu'nun 525. maddesinin (b/1) bendi; elektronik verilerin silinmesi, tahrip edilmesi ve değiştirilmesi, sistemlerin yanlış biçimde işlemesine neden olmak ya da işlemesine tamamen engel olmak konularına yaptırımlar getirmektedir (Dülger, 2004).

525. maddesinin (d) bendinde ise kişisel bilgilerin korunması hakkında gerekli bilgiler verilmiş olup bilgisayarda bulunan özel bilgilerin başkaları tarafından kopyalanması, silinmesi veya bozulması durumunda bu işlemi yapan kişi veya kişilere cezai işlemlerin uygulanacağı belirtilmiştir. Ayrıca 5846 sayılı Fikir ve Sanat Eserleri Kanunu (FSEK), Türk Ceza Kanunu (TCK), Türk Ticaret Kanunu (TTK) ve Markaların Korunması Hakkındaki Kanun Hükmünde Kararname hükümleri gereğince; "korsan yazılım kullanılması, kopyalanması veya satışa sunulması suçtur, bilerek veya bilmeyerek korsan yazılım kullandığı tespit edilen şirketler ve kurumlar hakkında cezai işlem yapılır." (Balaman, 2013).

Karakoç (2011) ise bilişim suçları ile ilgili kanuna değinmiştir. Buna göre Türk Ceza Kanunu'nun 10. bölümünde "Bilişim Alanında Suçlar" başlığı altında yer alan 243. madde "Bilişim Sistemine Girme", 244. madde "Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme", 245. madde ise "Banka veya Kredi Kartlarının Kötüye Kullanılması" ile ilgilidir ve bu suçlara ilişkin cezalar öngörülmüştür.

Bilişim suçları üzerine yapılan bir araştırmada, Atalıç Taş (2010) Adana İl Emniyet Müdürlüğü kayıtlarına yansıyan 648 olayı ve 1872 şüpheliyi incelemiştir. Buna göre İnternet üzerinden işlenen suçların ilk sırasında dolandırıcılık olduğu, suç işlemede en çok zararlı yazılım yönteminin kullanıldığı, şüphelilerin % 89'unun erkek ve 21-30 yaş aralığında olduğu saptanmıştır.

İnsan hayatını kolaylaştıran teknolojik gelişmeler, bireylerin bu teknolojileri uygunsuz kullanması, doğabilecek risklerin tahmin edilememesi, tehditlerden habersiz olma, kötü amaçlı kullanım ve dijital veri güvenliği risklerini de beraberinde getirmiştir. Riskleri gidermenin ya da en düşük düzeyde tutmanın yolu bireyler üzerinde farkındalık oluşturmaktan geçmektedir. Bu bağlamda farkındalık kavramını incelemek yerinde olacaktır.

Farkındalık

Farkındalık, günlük yaşamda sıkça kullanılan bir kavramdır. Acar (2004:56) farkındalığı, "bireyin tüm duyu organlarıyla, başka birey veya çevresiyle temasa geçerken neyi, nasıl yaşadığının ayırdında olması" olarak tanımlamıştır.

Geçmiş, bireyler için geride kalmıştır. Gelecek ise belirsizdir. Bireylerin etraflarında olup bitene müdahale edebildikleri zaman dilimi ise sadece yaşanılan an yani şimdidir. Kısacası farkındalık, geçmişe ait hatırlananlar ya da geleceğe yönelik tahminler değil, şimdi olanlara ilişkindir.

Dökmen (2000) yaşamın akışı içinde farkında olmayı gerektiren pek çok alan olduğunu belirtmiş ve farkındalık türlerini dört başlık altında toplamıştır. Buna göre birey;

1. Dış dünyanın (nesnelerin, olayların, canlıların),
2. Kendi iç dünyasının (fizyolojik tepkilerinin, duygularının, düşüncelerinin, isteklerinin),
3. Diğer insanların (ötekilerin) iç dünyalarının,
4. Evrendeki bütünlüğün farkına varabilir.

Alanyazın incelendiğinde farkındalık konusunda yapılan çalışmalar arasında ölçek geliştirme çalışmaları göze çarpmaktadır. Bunlardan bazıları daha önceden yabancı alanyazında ortaya konmuş ölçeklerin Türkçeye uyarlanmasıdır. Bilinçli farkındalık ölçeğini Özyeşil, Arslan, Kesici ve Deniz (2011), duygusal farkındalık düzeyi ölçeğini Kuzucu (2008), çatışma ve şiddete ilişkin farkındalık ölçeğini ise Sargın (2010) Türkçeye uyarlamıştır. Güven ve Aydoğdu ise (2012) çevre sorunlarına yönelik bir farkındalık ölçeği geliştirmiştir.

Alanyazına göre bireylerin çeşitli alanlardaki farkındalıklarının belirlenmesine yönelik ölçme araçlarına ihtiyaç olduğu ve bu ihtiyacı gidermeye yönelik çalışmalar yapıldığı söylenebilir. Bilgi ve iletişim teknolojilerindeki gelişmeler ve bu teknolojilerin yoğun kullanımı dikkate alındığında, bireylerin dijital veri güvenliği konusundaki farkındalıkları da bir başka çalışma alanını oluşturmuştur.

Dijital Veri Güvenliği Farkındalığı

Dikkatli ve iyi eğitilmiş bireyler oluşabilecek güvenlik ihlallerini engelleyebilir. Bu nedenle, toplumun dijital veri güvenliği konusunda bilinçlendirilmesi, bu konuda farkındalık yaratılması ve eğitimlerin düzenlenmesi gereklidir. Bunun için medya kanalları kullanılarak, okullarda seminerler düzenlenerek gereksinimler doğrultusunda eğitim programlarının hazırlanması ve bireyler üzerinde farkındalık oluşturulması gerekmektedir. Örneğin güvenlik sorununun eğitimle çözülmesi gerektiğini düşünen İngiltere'de, ilköğretim çağındaki öğrencilere uygulanan öğretim programında 2011 yılından itibaren İnternet'in güvenli kullanımı ile ilgili zorunlu bir ders yer alması planlanmıştır (Ulaşanoğlu, Yılmaz ve Tekin, 2010).

Dijital veri güvenliğinin sağlanabilmesi için bir takım teknik önlemler de alınabilir. Ancak teknoloji kullanımında insan faktörü göz ardı edilirse alınan önlemler sonuç vermeyecektir. Çünkü bu konuda bilinci ve farkındalığı olmayan insanlar güvenlik sürecinin işlemesinde farklı aşamalarda aksaklıklara neden olacaktır. Şöyle ki bilginin paylaşıldığı bireylerin yapabilecekleri çok küçük hatalar, dikkatsizlikler, bilinçli ya da bilinçsiz yapılabilecek her türlü suiistimaller teknik anlamda alınan tüm güvenlik önlemlerini boşa çıkaracaktır (Şahinaslan, Kantürk, Şahinaslan ve Borandağ, 2009). Bireylerin iş dışındaki günlük yaşamlarında da kablosuz ADSL, İnternet, cep telefonu vb. kullanımları göz önüne alınırsa, yalnızca iş amaçlı değil, bireysel kullanımda da bilgi güvenliği çözümlerinin hızla yaygınlaştırılması gerekmektedir (Swaminatha ve Elden, 2003).

Dijital veri güvenliği konusu genel olarak değerlendirildiğinde alınabilecek önlemlerin başında insan faktörü gelmektedir. Seminerler ve kampanyalar düzenlenmesi, güvenlikle ilgili gelişmeler, zararlı yazılımlar ve kişisel verilerin korunması gibi konularda bilgilendirme yapılması bireylerde farkındalık oluşturulmasına katkı sağlayacaktır.

Eğitim Öğretim Faaliyetlerinde Dijital Veri Güvenliğinin Önemi

Tüm dünya ile birlikte ülkemizde de kamu ve özel kuruluşlar, İnternet teknolojisinin sunduğu olanakları kullanarak, verdikleri hizmetlerin daha hızlı, zamandan ve mekândan bağımsız, çağdaş ve kaliteli hale getirilmesi için yeni arayışlara girmişlerdir. Baykal (2005) bu çalışmaların sonucu olarak gelişen elektronik devlet (e-devlet) kavramını, devletin tüm bürokratik, ekonomik ve hukuksal işlemlerini bilgisayar aracılığıyla iletişim ağları üzerinden doğrudan yapabilmesini sağlayan, vatandaşların devlete karşı görevlerini güvenle yürütebildikleri ve istedikleri hizmetlerden yararlandıkları, zaman ve yer kavramlarını ortadan kaldıran elektronik yapı olarak tanımlamaktadır.

2001 yılında dünya genelinde e-devlet uygulamalarının kullanımının en yüksek olduğu ülkeler Norveç, Danimarka, Kanada ve Finlandiya'dır. Bu ülkelerde e-devlet kullanımı % 50'ye ulaşmakta ve İnternet üzerinden geniş bir hizmet verilmektedir. Türkiye'de ise bu oran % 3'tür ve Estonya, Letonya, Çek Cumhuriyeti ve Slovakya gibi devletlerin gerisindedir (Kızılyel, 2007). Türkiye İstatistik Kurumu (TÜİK, 2014) verilerine göre bireylerin e-devlet kullanım oranı 2013 yılında % 41.3'e yükselmiştir.

MEB ise e-devlet uygulamaları kapsamında merkez ve taşra örgütleri ile tüm eğitim kurumlarını bir dizi bilgi iletişim sistemi aracılığıyla birbirine bağlayan bir çatı projesi olan MEBBİS (Milli Eğitim Bakanlığı Bilişim Sistemleri) projesini hayata geçirmiştir. MEBBİS kapsamında geliştirilen ve halen uygulamada olan eğitim ve öğretim kurumları arasındaki iş, bilgi akışı ve personel işlemlerini bilgisayar ortamlarında yürütmek üzere geliştirilmiş birçok alt sistem bulunmaktadır. Öğrenci bilgilerinin pek çoğunun yer aldığı e-Okul ile İl İlçe Milli Eğitim Müdürlükleri Yönetim Bilgi Sistemi olan İLSİS bu alt sistemlerden bazılarıdır.

1987 yılında MEBBİS programının bir alt sistemi olarak tasarlanan İLSİS Projesinin pilot uygulaması 1994 yılında başlamıştır. İLSİS uygulama yazılımları ile personelin kimlik bilgileri, kadro ve terfi işlemleri, öğrenim ve sicil bilgileri, izin işlemleri ile kuruma ait personel ve norm bilgileri, okutulan kitaplar gibi bilgiler takip edilmektedir (İnci, 2002). Bu modül 2009 yılında kapatılarak MEBBİS'e aktarılmıştır.

Bir başka alt sistem olan web tabanlı okul yönetimi yazılımı e-Okul sayesinde okul yöneticileri; öğrenci işlemlerini (kayıt, nakil, devam takibi, karne, veli bilgilendirme vb.), ders ve sınav işlemlerini (ders programı, sınav takvimi, not girişi

vb.) ve personel işlemlerini İnternet aracılığıyla rahat ve güvenli bir şekilde yapabilmektedir (MEB, 2009).

Öğretmenler; özlükle ilgili işlemlerin yürütüldüğü MEBBİS ile eğitim sisteminin tamamına ait verilerin yer aldığı e-Okul sisteminin kullanımından sınav sorusu hazırlamaya, ders içeriklerinin dijital ortama aktarılmasına kadar eğitim ve öğretim hizmetlerinde bilgisayarı ve İnterneti yoğun olarak kullanmaktadır. Hem karşılaşabilecekleri zararları, hem de yaşanabilecek sorunların hukuki boyutlarını bilmeleri ancak öğretmenlerde dijital veri güvenliği farkındalığını oluşturacak eğitimler ile mümkündür.

Bu bağlamda MEB tarafından eğitim ortamlarının geliştirilmesine ve eğitimde kalitenin arttırılmasına yönelik projelerin, öğretmen eğitimi bileşeninin ve hizmet içi eğitim faaliyetlerinin incelenmesi yerinde olacaktır.

Öğretmenler İçin Dijital Veri Güvenliği

MEB'in büyük ölçekli projelerinden olan Milli Eğitimi Geliştirme Projesi (MEGP), Ekonomik İş Birliği ve Kalkınma Örgütü'ne (OECD) üye ülkelerin birçoğu ile birlikte, Milli Eğitimin hedeflerine ulaşmasında belirleyici olan yeniden yapılanma ve reform çalışmaları kapsamında 10 Temmuz 1990 tarih ve 20570 sayılı resmi gazetede yayınlanarak yürürlüğe girmiştir. Bu proje kapsamında 208 Müfredat Laboratuvar Okulu (MLO); bilgisayar, yazıcı, tarayıcı, TV, video kamera, tepegöz gibi eğitim materyalleri ile donatılmıştır. Müzik ve resim odaları, bilgisayar ve fen laboratuvarları, kütüphaneler, öğretmen çalışma odaları kurulmuştur (MEB, 2002).

MLO'lar, geliştirilen öğretim programlarının, yeni eğitim, öğretim ve yönetim yaklaşımlarının sistem geneline yaygınlaştırılmadan önce deneneceği ve teknolojik gelişmelerin eğitime yansıtılacağı okullardır. Pilot uygulama çalışmalarından elde edecekleri deneyimler ile sistem genelindeki diğer okullara liderlik yapacaklardır (Sönmez, 2005).

MEB'in eğitimde teknoloji entegrasyonu üzerine geliştirdiği bir başka proje ise halen yürütülmekte olan Fırsatları Arttırma ve Teknolojiyi İyileştirme Hareketi (FATİH) projesidir. Eğitimde FATİH Projesinin amacı; eğitim ve öğretimde fırsat eşitliğini sağlamak ve okullardaki teknolojiyi iyileştirmek amacıyla bilişim teknolojileri araçlarının öğrenme-öğretme sürecinde daha fazla duyu organına hitap edilecek şekilde,

derslerde etkin kullanımını sağlamaktır. Eğitimde FATİH projesi beş ana bileşenden oluşmaktadır (FATİH Projesi, 2012).

FATİH projesinin "bilinçli, güvenli, yönetilebilir ve ölçülebilir BT kullanımının sağlanması" bileşeni kapsamında projenin uygulandığı okullardan başlanmak suretiyle eğitim yöneticileri ve öğretmenler "Bilişim Teknolojilerinin ve İnternetin Bilinçli, Güvenli Kullanımı Seminerleri"ne katılmaktadır. FATİH Projesi, dijital veri üzerine kurgulanmıştır ve bu proje için dijital veri güvenliği son derece önemlidir.

Öğretmen Yetiştirme ve Geliştirme Genel Müdürlüğünce (2013a) planlanan ilgili hizmet içi eğitim etkinlik programının amaçları arasında "İnterneti bilinçli ve güvenli kullanır", "İnternet üzerinde yayımlanan, ders etkinliklerinde kullanabileceği materyalleri arar, bulur ve telif haklarına uygun olarak seçer" ifadeleri yer almaktadır.

Öğretmen Yetiştirme ve Geliştirme Genel Müdürlüğü tarafından geliştirilen ve güncellenen standart ölçütlere uygun olarak hazırlanan örnek hizmet içi eğitim programları incelendiğinde 2. seviye modül programlar arasında yer alan "Eğitimde Bilişim Teknolojilerinin Kullanımı Kursu" üniteleri aşağıdaki gibidir (Öğretmen Yetiştirme ve Geliştirme Genel Müdürlüğü, 2013b):

- Bilgi teknolojisi bileşenleri,
- İnterneti etkin kullanma,
- Etkili sunum teknikleri,
- Bilişim teknolojilerini kullanarak ders işleme.

MEB tarafından son yıllarda uygulamaya konulan büyük ölçekli projelerdeki öğretmen eğitimleri ve yürütülen hizmet içi eğitim faaliyetleri incelendiğinde dijital veri güvenliği konusuna yer verilmediği görülmektedir.

İlgili Araştırmalar

Tarihsel gelişimi içinde bilgi sistemlerinin güvenliği ve sonrasında bilgi güvenliği konusunda çok sayıda akademik araştırma yapılmış, makaleler yayınlanmış ve ticari ürünler ortaya çıkartılmıştır (Çetinkaya, 2008). Alanyazın taraması sonucunda ulaşılan dijital veri güvenliği kapsamındaki yerli ve yabancı araştırma örnekleri aşağıda verilmiştir.

Yurt Dışında Yapılan Araştırmalar

Dijital veri güvenliği ile ilgili olarak yabancı ülkelerde yapılan araştırmalar incelendiğinde; bazıları öğretmen ve öğrenci görüşlerine dayanarak veri güvenliği konusundaki farkındalıklarını incelerken, bazıları da şirketleri konu edinmiştir. Öğrenci ve öğretmenlerle gerçekleştirilen araştırmalar ilkokuldan üniversite düzeyine göre sıralanmış, ardından şirketlere yönelik araştırmalar verilmiştir.

Araştırmalar arasında en dikkat çekici olanı 2000-2009 yılları arasındaki 10 yıllık süreçte Tayvan'daki ilkokul ve ortaokul öğretmenlerine yönelik olarak geliştirilen İnternet Güvenliğinde Öğretmen Farkındalığı (Teacher Awareness of Internet Safety-TAIS) projesidir. Projenin araştırmacıları İnternet güvenliğini, öğretmenlerin aşina oldukları dört çekirdek alanda tanımlamıştır. Bu alanlar; iletişim güvenliği, bilgi anlayışı ve uygunluk, çevrimiçi kişilerarası güvenlik, bilgisayar ve İnternet kullanımı güvenliğidir. TAIS projesi birinci etapta yalnızca bilgisayar öğretmenlerini kapsarken ikinci etapta tüm ilkokul ve ortaokul öğretmenlerini içine almıştır. Ancak projenin üçüncü etabında veliler, lise öğrencileri ve öğretmenleri ile öğretmen adayları projeye dâhil edilememiştir. Projede; eğitim seminerleri, atölye çalışmaları, konferanslar gibi çok çeşitli etkinlikler yer almıştır. Ayrıca 7/24 hizmet veren e-Öğretmen web sitesi sayesinde; çevrimiçi öğretmen-öğrenme toplulukları kurulmasına yardımcı olunmuş, öğretim programına uygun güvenli içerikler ve öğretmenlerin sınıflarında kullanabileceği üniteler sunulmuştur (Chou ve Peng, 2011). TAIS projesi İnternet güvenliğine yönelik devlet idaresinde gerçekleştirilen büyük ölçekli ilk projedir. Pek çok ülkede olduğu gibi Türkiye'de de bilişim teknolojilerinin eğitimde kullanılmasına yönelik projeler hayata geçirilmiştir. Ancak TAIS projesi güvenliğe odaklanması nedeniyle bir fark ortaya koymuştur.

Almanya'daki okullarda araştırma yapan Beyer ve Westendorf (2009) ise İnternet güvenliği konusunda verilen eğitimi, sorunları ve açık alanları incelemiştir. Araştırmacılar, okullarda İnternet güvenliğinin sağlanabilmesi için öneriler getirmiştir. Buna göre; öğretmenlere riskler ve bunların sonuçları hakkında eğitim verilmesinde, okullarda öğrenciler için İnternet güvenliğine dikkat çekecek ortamlar sunulmasında, alınacak önlemleri ve projeleri planlayabilmek için okulların, öğrencilerin hangi web sitelerini ne sıklıkta kullanacaklarının belirlenmesinde yarar vardır.

Amerika'da 2001 yılında "Çocuklar İçin İnternet Koruma Kanunu" (CIPA) yürürlüğe girmiştir. Bu kanuna göre 17 yaşından küçükleri İnternet'in olumsuz etkilerinden korumak için okullarda filtre kullanılmaktadır. Yan (2009) bu kanunun lise öğrencilerine yararını incelemiştir. 407 öğrencinin katıldığı çalışmada, ilgili kanun kısıtlamasına tabi lise öğrencileri ile kısıtlamaya tabi olmayan üniversite öğrencilerinin İnternet güvenliği koruma stratejileri konusundaki temel bilgileri ve eğitim algıları karşılaştırılmıştır. Bulgular, ilgili kanunun lise öğrencilerinin okuldaki İnternet kullanımlarında azalma yarattığını düşündürse de, İnternet güvenliğine yönelik temel bilgilerinde veya eğitim fırsatlarında olumlu etkiye sahip olmadığını göstermiştir. Bunun nedeni olarak da lise öğrencilerinin evlerinde İnternet kullanımında herhangi bir kısıtlama olmaması gösterilmiştir.

Üniversite öğrencilerinin bilgi güvenliği farkındalıklarına yönelik ölçme aracı geliştirme çalışmasında Kruger, Drevin ve Steyn (2010), farkındalık programlarında yer alabilecek uygun alanların veya konuların belirlenmesine yardımcı olmak için "bilgi güvenliği sözcük testi" geliştirmiştir. Çalışmada sözcük testini sınamak ve uygulanabilirliğini göstermek için iki bölümden oluşan bir anket kullanılmıştır. İlk bölümde sözcük testi yer alırken, ikinci bölümde katılımcıların davranışları değerlendirilmiştir. Katılımcılar iki farklı sınıfta öğrenim gören üniversite öğrencileridir. Araştırma bulguları, bilgi güvenliği farkındalığını değerlendirmek için sözcük testi kullanımının yararlı olacağını göstermiştir. Aynı zamanda sözcük bilgisi ile davranışlar arasında anlamlı bir ilişki gözlenmiştir.

Dijital veri güvenliği konusunda yapılan, hedef kitlesi öğrenci ve öğretmen olan yurt dışındaki çalışmaların 2000'li yılların başından bu yana sürdüğü görülmektedir. Birleşik Arap Emirlikleri'nde bilgi sistemleri yöneticileri de dâhil olmak üzere üniversite personeli ile çalışan Rezgui ve Marks ise (2008), katılımcıların bilgi güvenliği farkındalıklarını etkileyen faktörleri araştırmıştır. "Sorumluluk", "kültürel varsayımlar ve inançlar" ile "toplumsal koşullar" gibi faktörlerin, üniversite personelinin işlerine karşı davranışlarını ve tutumlarını genel olarak etkilediği, bilgi güvenliği farkındalıklarını ise kısmen etkilediği ortaya konmuştur.

Eğitim araştırmalarının yanında şirket çalışanlarının veri güvenliği farkındalıklarını konu alan araştırmalar da bulunmaktadır. Uluslararası bilgi güvenliği farkındalığı ölçeği geliştiren Kruger ve Kearney (2006) taslak formu bir madencilik

şirketinin Avustralya bölge ofisinde çalışanlara uygulamıştır. Bilgi, tutum ve davranış ölçen sorulardan oluşan 35 soruluk taslak, açık uçlu ve çoktan seçmeli sorularla zenginleştirilmiştir. Ölçeğin son hali şirket çalışanlarına uygulanmıştır. Yönetimin farkındalık performansına yönelik görüşleri doğrultusunda 80-100 puan arası "iyi", 60-79 puan arası "orta", 59 puan ve aşağısı "zayıf" farkındalık düzeyi olarak belirlenmiştir. Katılımcıların genel bilgi güvenliği farkındalığı % 65 iken, bilgi için % 77, tutum için % 76 ve davranış için % 54 olarak bulunmuştur.

Personelin güvenlik önlemlerine bakış açılarını ortaya koymak isteyen Albrechtsen (2007) çalışmasında bilişim teknolojileri şirketlerini ve Norveç'teki bankaları incelemiştir. Güvenliği sağlayan yöneticiler ile personel arasındaki boşluğa dikkat çekmiş ve güvenlik sorunlarının, çalışanların yetersiz bilgi birikimi ve farkındalık eksikliğinden kaynaklandığını görmüştür.

Elektronik ortamda işlenen suçların dağılımını ve maddi zararı araştıran Bilgisayar Güvenliği Enstitüsü (2009) 443 kuruluşun ortalama kaybını 234,244 $ olarak belirlemiştir. Suçların dağılımı incelendiğinde; dolandırıcılık % 29, kötü amaçlı yazılımlardan etkilenme % 64.3, sistem durdurma saldırılarına maruz kalma % 29.2, şifre çalma % 17.3 ve web sitelerinin devre dışı bırakılması % 13.5'tir.

Şirketlerde veri güvenliğine yönelik çalışmalar incelendiğinde, yaşanılan güvenlik sorunlarının genellikle personelin bilgi eksikliğinden kaynaklandığı ve bu konuda farkındalık oluşturulmasına ihtiyaç duyulduğu söylenebilir.

Yurt İçinde Yapılan Araştırmalar

Yabancı ülkelerde gerçekleştirilen ve dijital veri güvenliğinin farklı boyutlarını ortaya koymayı amaçlayan araştırmaların yanında ülkemizde de alana katkı sağlamış önemli araştırmalar yer almaktadır.

Dijital veri güvenliğinin farkındalık boyutunu inceleyen araştırmalar genellikle katılımcı görüşüne dayalı olup veri toplama aracı olarak anket veya ölçek kullanılmıştır. Anket kullanılarak veri toplanan ve "Bilgi Güvenliği Farkındalığı" başlığı taşıyan çalışmalardan birinde Mart (2012) geliştirdiği anketi, farklı meslek gruplarından 157'si öğretmen 501 katılımcıya uygulamıştır. Öğretmenlerin farkındalık düzeylerinin diğer meslek gruplarından farklı olmadığı sonucuna ulaşmıştır. Benzer bir çalışmada MEB Bilgi İşlem Dairesi Başkanlığı (2012) tarafından 7484 katılımcıya yine anket

uygulanmış ve MEB personelinin bilgi güvenliği farkındalık düzeyleri ölçülmüştür. Katılımcılara; MEB Bilgi ve Sistem Güvenliği Yönergesi, parolalar, sosyal ağlar ve e-posta konularında sorular yöneltilmiştir. Bazı konularda farkındalığın yüksek olduğu, bazı konularda ise yeterli bilinç düzeyinin oluşmadığı görülmüştür. Araştırma sonuçlarının; yapılacak etkinlikler ile verilecek eğitimlerin planlanması ve MEB'in bilgi güvenliği politikalarının geliştirilmesi çalışmalarına kaynak oluşturması amaçlanmıştır.

Buraya kadar anlatılan çalışmalarda katılımcıları yetişkinlerden oluşan pek çok ölçme aracı geliştirildiği, ancak doğrudan öğretmenlerin dijital veri güvenliği farkındalıklarına yönelik bir ölçme aracının bulunmadığı görülmektedir.

Alanyazında, ölçek kullanılarak veri toplanan ve farklı öğrenim düzeylerindeki öğrencilerin dijital veri güvenliği farkındalıklarını ortaya koymayı amaçlayan araştırmalar da bulunmaktadır. Tekerek ve Tekerek (2013) Kahramanmaraş ilindeki 2449 ilköğretim ve lise öğrencisine, bilgi ve bilgisayar güvenliği farkındalık düzeylerini ortaya koyabilmek için geliştirdikleri ölçeği uygulamıştır. Araştırma sonunda, öğrencilerin etik konulardaki farkındalık düzeylerinin yeterli, kurallar ve bilgi gerektiren konularda ise farkındalık düzeylerinin düşük olduğu gözlenmiştir. Bunun nedeni olarak bilgi ve bilgisayar güvenliği farkındalık eğitim ve etkinliklerinin yetersiz olduğu gösterilmiş ve bu konudaki derslerin sayısının arttırılması önerilmiştir.

İstanbul ilindeki özel bir üniversitede okuyan 326 öğrenci ile gerçekleştirilen çalışmada ise Kınay, Sözcü, Taşkın ve İpek (2014) tarafından "Bilgi Güvenliği Farkındalığı Ölçeği" geliştirilmiştir. Ölçekte bilgi, eğilim ve davranış düzeylerinde olmak üzere 32 madde bulunmaktadır. Ölçekten elde edilen toplam puanlar; 60 ve aşağısı "düşük", 60-79 arası "orta", 80 ve üzeri ise "yüksek" farkındalık düzeyi olarak isimlendirilmiştir. Her farkındalık seviyesi için alınması gereken kararlar tartışılmıştır. Benzer çoğu araştırmada katılımcıların yalnızca farklı değişkenlere göre betimsel istatistikleri verilirken bu araştırmada puan aralıklarına göre farkındalık düzeyleri belirlenmiştir.

Dijital veri güvenliği başlığı altında incelenebilecek bir başka çalışma alanı da İnternet güvenliğidir. Bu konuda yapılmış çalışmalardan birinde Dönmez, Odabaşı, Kabakçı Yurdakul, Kuzu ve Girgin (2014) tarafından "Öğretmen Adayları İçin Çocukların Karşılaştığı İnternet Risklerine Yönelik Algı Ölçeği" geliştirilmiştir. Çocukların İnternet risklerine karşı korunmasında en önemli rolü üstlenenlerin sınıf

öğretmenleri olabileceği düşünülerek ölçeğin tüm güvenirlik ve geçerlik çalışmaları sınıf öğretmeni adaylarıyla gerçekleştirilmiştir. 5 farklı üniversiteden 392 öğrenci ile AFA ve 272 öğrenci ile de DFA yapılmıştır. Analizler sonucunda 20 maddelik ve 6 faktörlü bir yapıya ulaşılmıştır. Faktörler; cinsellik, zararlı içerikler, İnternet hesaplarının korunması, siber zorbalık, kişisel bilgilerin korunması ve zararlı iletişimler olarak isimlendirilmiştir. Bu araştırmadaki katılımcıların yalnız sınıf öğretmeni olmaları bir sınırlılık gibi görünse de hem alana bir ölçme aracı kazandırılmıştır, hem de öğretmenlik mesleğine adım atmış bireylerin İnternet'teki risklere yönelik algılarının ölçülmesi mümkün olmuştur.

İnternet kullanımında önemli güvenlik tehditlerinden olan sosyal ağların kullanımında da güvenliğin sağlanmasına yönelik bireylerin farkındalıklarının bulunması gerekmektedir. Günümüzde yoğun olarak kullanılan sosyal ağlardan olan Facebook'un gizlilik ayarlarını altı kategoride inceleyen Sel (2013) çalışmasında, 60 ortaokul öğrencisi ile 15 gün arayla bireysel görüşmeler yapmıştır. Başlangıçta öğrencilerin yaklaşık % 70'inin gizlilik ayarlarını bilmediği ortaya çıkmıştır. Öğrencilere gizlilik ayarlarına dikkat etmedikleri durumlarda karşılaşabilecekleri sorunlar ve ayarların nasıl yapılacağı anlatılarak gerçekleştirilen bilinçlendirme ve bilgilendirme çalışmaları sonunda öğrenciler üzerinde farkındalık oluştuğu görülmüştür. Bu araştırmanın sonuçlarına göre gerçekleştirilen eğitimler sayesinde farkındalık düzeyinin arttırılabileceği söylenebilir.

Alanyazın incelendiğinde, yukarıda bahsedilen ve katılımcı görüşlerine dayanan dijital veri güvenliği konulu araştırmaların yanında güvenlik yazılımları, ağ güvenliği, şifreleme gibi teknik konulara odaklanmış çalışmalar da yer almaktadır.

Say ve Sağıroğlu'nun (2004) gerçekleştirdiği çalışmada kişisel veri güvenliğini sağlamada önemli olan klavye dinleme sistem yazılımları ve alınacak önlemler gözden geçirilmiştir. Araştırmacılar tarafından geliştirilen bir anti-casus program ile casus programı bulan ve otomatik olarak kaldıran uygulamalar yapılmıştır. Klavye dinleyen sistemlerin fark edilmesinin oldukça zor ve zaman alıcı olduğu belirtilmiştir.

İnternet'ten gelebilecek tehditlere karşı güvenliğin sağlanması için kullanılan araçlara ve tekniklere değinen Şahin (2005) saldırı sezme sistemlerini incelemiştir. Ardından bir ilköğretim okulunun 20 bilgisayarlı laboratuvarındaki ağ ortamında "Real Secure" adlı saldırı sezme sistemi yazılımının başarısını denemiştir. Etkinlik, hata

toleransı, performans ve hatasızlık değerlendirmelerinden geçirilen yazılımın, uygulandığı ağa güvenlik anlamında büyük yararlar sağladığı görülmüştür.

Bilgisayar ağlarına yönelik bir başka çalışmada Gök, Yazıcı, Duru ve Becerikli (2007) Kocaeli Üniversitesi Bilgisayar Mühendisliği Bölümü ve Mühendislik Fakültesi için güvenli bir kablosuz yerel alan ağı oluşturulmuştur. Bunun için kablosuz yerel alan ağ standartları, açıklar ve saldırı türleri, bu saldırı ve açıkları engellemek için gerekli uygulamalar araştırılmış ve omni anten, köprü, erişim noktaları ve istasyonlar kullanılmıştır.

Şifrelemeye yönelik çalışmalar incelendiğinde, Sağıroğlu ve Özkaya'nın (2007) elektronik ortamlarda veri güvenliği için yapay sinir ağlarına (YSA) dayalı yeni bir yaklaşım sunan çalışması dikkat çekicidir. Şifreleme ve şifreleri çözme için iki YSA modeli kullanılan çalışmada, karakter tabanlı bir eğitim ve test işlemini otomatik gerçekleştirmek için Delphi programlama dilinde bir yazılım geliştirilmiştir. Sonuç olarak ilgili yazılım sayesinde kolay, etkili ve güvenli bir şekilde veri güvenliği için nörol çözüm sağlanmıştır.

Dijital veri güvenliğinin arttırılması noktasında farklı arayışlara giren araştırmacılar biyometrik yöntemlere de başvurmuştur. Bir dijital dokümanın biyometrik yöntemlerle güvenliğinin nasıl sağlanabileceği üzerinde duran Keleş ve Güneş'in (2013) çalışmasında ise, avuç damar izi okuyucular ile biyometrik veri oluşturulup steganografi sayesinde 24 renkli dijital bir doküman avuç damar izi teknolojisi kullanılarak şifrelenmiştir. Başarı oranı ve işlem süresi parmak izi teknolojisi ile karşılaştırılmıştır. Sonuç olarak şifreleme yapılan resimde gözle görünür bir bozulma olmadığı görülmüştür. Ancak avuç damar izi yöntemi ile şifrelenen verilerin parmak izi yöntemi ile şifrelenen verilere göre dört kat daha fazla kapasiteye sahip olduğu, şifreleme ve çözme sürelerinin ise üç kat daha uzun olduğu ortaya konmuştur.

Alanyazındaki dijital veri güvenliğine yönelik bir başka çalışma alanı da bilgi güvenliği standartlarını da kapsayan yazılımların ve araçların geliştirilmesidir. Yüksek lisans tezinde Haklı (2012) bilgi güvenliği standartlarını incelemiş ve kamu kurumlarına yönelik bu standartları uygulayabilecekleri bir model tasarlamıştır. İlgili model önerisi için kamu kurumları ve şirketlere ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'nin uygulanmasında yol gösterici bir yazılım geliştirilmiştir.

Bir başka yüksek lisans tez çalışmasında Kocamustafaoğulları (2013) tarafından organizasyonların bilgi güvenliği farkındalık ve uygulama seviyelerine yönelik kendi öz değerlendirilmelerini yapabilecekleri, ISO/IEC 27001 ve ISO/IEC 27002 bilgi güvenliği standartlarını temel alan, web tabanlı, açık ve anlaşılır, kolay kullanımlı Türkçe bir araç ortaya konmuştur.

Güvenliğin sağlanması noktasında gerek donanım, gerekse yazılım destekli tedbirler alınmaya çalışılsa da güvenliğin zayıf halkası insan faktörüdür. Geliştirilen bu donanım ve yazılımları, veri güvenliğinin farkında olan bireyler bilinçli bir şekilde kullandığında çoğu veri kaybı önlenebilir.

Yaşamı kolaylaştıran e-kavramlar (e-ticaret, e-öğrenme, e-rezervasyon, e-sınav, e-okul, e-banka, e-devlet vb.) üzerinde duran Tekerek (2008) çalışmasında bu sistemlerde bulunan tehditlere dikkat çekmiştir. Bunlara karşı teknik önlemlerin yanında kurallar, cezalar gibi idari önlemler ile insan faktörünün de göz önüne alınması gerektiğini vurgulamıştır.

Dünyadan ve Türkiye'den güncel verilerle mevcut durumu ortaya koyarak bilgi güvenliği konusunda yapılan en yaygın yanlışlıklara dikkat çeken Eminağaoğlu ve Gökşen (2009) ise, toplum geneline ve kurumlara uygulanabilecek etkin çözüm önerileri üretmiştir. Çalışmada genel olarak bilgi güvenliğinde başarı sağlamada en kritik faktörün istekli, bilinçli ve bilgili insanlar olduğuna vurgu yapılmıştır.

Bilinçli bireyler yetiştirmek kadar kullanılan sistemlerdeki güvenlik açıklarının giderilmesi de önemlidir. Ketizmen ve Ülküderner (2007) çalışmalarında, Türkiye Sigortalar Birliği, Sosyal Güvenlik Kurumu, İç İşleri Bakanlığı Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü, Yüksek Seçim Kurulu ve Sağlık Bakanlığı gibi kamu ve özel kurumların İnternet hizmetleri aracılığıyla erişilebilecek kişisel verilere ilişkin örnekler vermiştir. İlgili web uygulamaları üzerinden kolaylıkla başkalarının kişisel verilerine erişilebildiğini ve Türk Ceza Kanunun 135. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak yayma suçunun oluştuğunu ortaya koymuştur.

Alanyazında özellikle AB'nin dijital veri güvenliğine bakışını ortaya koyan ve bu konudaki çalışmalara odaklanmış araştırmalar da yer almaktadır. Özenç (2007), bilgi ve iletişim teknolojilerindeki bilgi güvenliğinin ekonomik boyutu ile AB'nin hukuki yaklaşımı üzerinde durmuş ve uluslararası arenada bilgi güvenliğine ilişkin bazı saldırı örneklerine yer vermiştir. Ülkemizde de "Bilgi Güvenliği Ulusal Koordinasyon Kurulu"

kurularak tüm taraflar arasında bilgi, tecrübe ve doküman paylaşımının yapılmasını önermiştir.

AB'nin kişisel verilerin korunması ve fikri mülkiyet ile ilgili yasal çerçevelerini inceleyen Toğuz (2010) da yüksek lisans tezinde, gelişmiş ülkelerde dijital hak yönetimi sistemlerinin mahremiyetin korunması konusunda yarattığı sıkıntıları ortaya koymayı amaçlamıştır. Türkiye'de kullanılan dijital hak yönetimi sistemlerinin fikri mülkiyet mevzuatının kapsamını aştığını, kişisel veri güvenliği politikası bulunmadığını ve kişilerin kendilerine özel alan bırakmayacak şekilde izlenmelerinin mümkün olduğunu ortaya koymuştur.

Doküman analizi yöntemini uygulayan Henkoğlu ve Yılmaz (2013) ise çalışmalarında; AB bilgi güvenliği politikalarını şekillendiren unsurların, politikaların amaçlarının, nasıl uygulandığının ve etkilerinin değerlendirilmesini amaçlamıştır. Bu kapsamda yayımlanmış AB direktifleri, komisyon tarafından hazırlanan sözleşmeler ve bilgi güvenliği politikaları çok yönlü ve kapsamlı bir kuramsal bilgi güvenliği modeli olan McCumber bilgi güvenliği modeli üzerinde irdelenmiştir. Sonuç olarak; AB bilgi güvenliği politikalarının, ekonomi ve bilgi toplumu politikalarının önemli bir parçası olarak görüldüğü ve bu politikaların günün gereksinimlerine yanıt verebilecek nitelikte olduğu belirlenmiştir.

Yurt içinde ve yurt dışında yapılan çalışmalar incelendiğinde, dijital veri güvenliğinin sağlanmasına yönelik teknik tedbirler ile bireylerin bu konudaki farkındalık düzeylerini ortaya koymayı amaçlayan çalışmaların yer aldığı görülmektedir. Veri kaybının bireyler ve kurumlar için önemi, ekonomik ve hukuki boyutları dikkate alındığında dijital veri güvenliği konusunda gereken hassasiyetin gösterilmesi ve insan faktörü açısından farkındalık oluşturulması gerekmektedir. Özellikle de ülkemizdeki eğitim öğretim faaliyetlerinde teknoloji kullanımının yaygınlaşması, devlet politikaları gereğince BİT'in eğitim öğretim ortamlarına entegrasyonu kapsamında geliştirilen projeler ve ayrılan bütçeler dikkate alındığında, öğretmenlerin dijital veri güvenliğine yönelik farkındalıklarının belirlenmesi gerekmektedir. Alanyazın incelendiğinde, pek çok ölçme aracı bulunmasına rağmen doğrudan öğretmenlerin dijital veri güvenliği farkındalıklarına yönelik bir ölçme aracının bulunmadığı ve bu konuda bir ihtiyaç olduğu görülmektedir.

Amaç

Araştırmada, öğretmenlerin dijital veri güvenliği konusundaki farkındalıklarının belirlenmesi hedeflenmektedir. Bu amaç doğrultusunda aşağıdaki sorulara yanıt aranmıştır.

1. Öğretmenlerin dijital veri güvenliği konusundaki görüşleri nelerdir?
2. Öğretmenlerin dijital veri güvenliği farkındalıklarının belirlenmesinde kullanılabilecek ölçeğin yapısı nasıl olmalıdır?
3. Öğretmenlerin dijital veri güvenliğine yönelik farkındalıkları ne düzeydedir?
4. Öğretmenlerin dijital veri güvenliğine yönelik farkındalıkları;
   a) Cinsiyete,
   b) Branşa,
   c) Görev yapılan öğrenim kademesine,
   d) Mesleki deneyime,
   e) Öğrenim durumuna,
   f) Günlük bilgisayar kullanım süresine,
   g) Günlük İnternet kullanım süresine,
   h) Kişisel bilgisayar, tablet bilgisayar ve akıllı telefon sahibi olma durumuna göre anlamlı farklılık göstermekte midir?

Önem

E-devlet uygulamalarının yaygınlaşması ve kurumların bu teknolojileri benimsemeleri üzerine farklı projeler hayata geçirilmiştir. MEB'in uygulamaya koyduğu MEBBİS ile personel ve öğrenci işlemleri İnternet üzerinden yürütülmeye başlamıştır. Web tabanlı bu sistemleri etkin olarak kullanan öğretmenler için dijital veri güvenliği önem kazanmıştır.

Bir başka nokta ise eğitim öğretim ortamlarında bilişim teknolojilerinin etkin kullanımı amacıyla MEB tarafından hayata geçirilmiş büyük ölçekli projelerdir. MEB tarafından uygulamaya konulan iki büyük projeden MEGP ve FATİH projesi kapsamında açılan kurslar ile yürütülen hizmet içi eğitim etkinlikleri incelendiğinde, öğretmenlerin dijital veri güvenliğine yönelik farkındalıkları ile ilgili bir eğitim başlığına rastlanmamaktadır. Öğretmenlerin bu konudaki farkındalıklarının ortaya konmasına yönelik bir ölçme aracının geliştirilmesi araştırmayı önemli kılmaktadır.

Erkuş'un da (2014) belirttiği gibi psikolojik bir değişkenin ölçülmesi bir gereksinimden kaynaklanmaktadır. Bu araştırmada öğretmenlerin dijital veri güvenliğine yönelik farkındalıklarının belirlenmesi amacıyla bir ölçek geliştirilmiştir. Böylece öğretmenlerin eğitim öğretim etkinliklerinde bilişim teknolojilerini kullanırken dikkat edilmesi gereken noktalardan biri olan dijital veri güvenliğine yönelik farkındalıklarını ortaya çıkaracak önemli bir veri toplama aracı alanyazına kazandırılmıştır.

Araştırma sonunda, okullarda görev yapan öğretmenlerin mevcut dijital veri güvenliğine yönelik farkındalıkları belirlenerek; cinsiyet, branş, görev yapılan öğrenim kademesi, mesleki deneyim, öğrenim durumu, günlük bilgisayar ve günlük İnternet kullanım süresi, bilgisayar, tablet bilgisayar, akıllı telefon sahibi olma durumu değişkenleri açısından farklılık taşıyıp taşımadığının incelenmesi hedeflenmiştir. Bu hedeflere ilişkin ortaya konan çıkarımların; politika yapıcılara, yöneticilere ve eğitimcilere dijital veri güvenliğine ilişkin adımlar atmada yardımcı olması beklenmektedir.

Ayrıca söz konusu araştırma; öğretmenlerin eğitim öğretim etkinliklerinde bilişim teknolojilerini kullanırken veri güvenliğinin arttırılmasını sağlayacak, gerçekleştirilecek hizmet içi eğitim faaliyetlerinin planlanmasında içerik belirleme çalışmalarına yön verecek ve ileriki araştırmalara ışık tutacaktır.

Sınırlılıklar

1. Araştırma, geliştirilen veri toplama araçlarıyla elde edilen veriler ile sınırlıdır.
2. Araştırma, 2013-2015 yılları arasındaki zaman dilimiyle sınırlıdır.
3. Araştırma, Balıkesir ilinde görev yapan öğretmenler ile sınırlıdır.

Tanımlar

Dijital Veri: Bir durum hakkında, sayısal ortamlarda bulunan ve taşınan sinyaller ve/veya bit dizelerinin belli bir anlam ifade edecek şekilde 0 ve 1 haline dönüştürülmüş her türlü veri, ses, görüntü ve video içeriğini ifade etmektedir (Yurdakul ve Çağlayan, 1997; Vural, 2007).

Dijital Veri Güvenliği: Bilgiye sürekli olarak erişilebilirliğin sağlandığı bir ortamda, bilginin göndericisinden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlüğünün sağlanması ve güvenli bir şekilde iletilmesi sürecidir (Schmidt, 2004).

Farkındalık: Bireyin tüm duyu organlarıyla, başka birey veya çevresiyle temasa geçerken neyi, nasıl yaşadığının ayırdında olmasıdır (Acar, 2004).

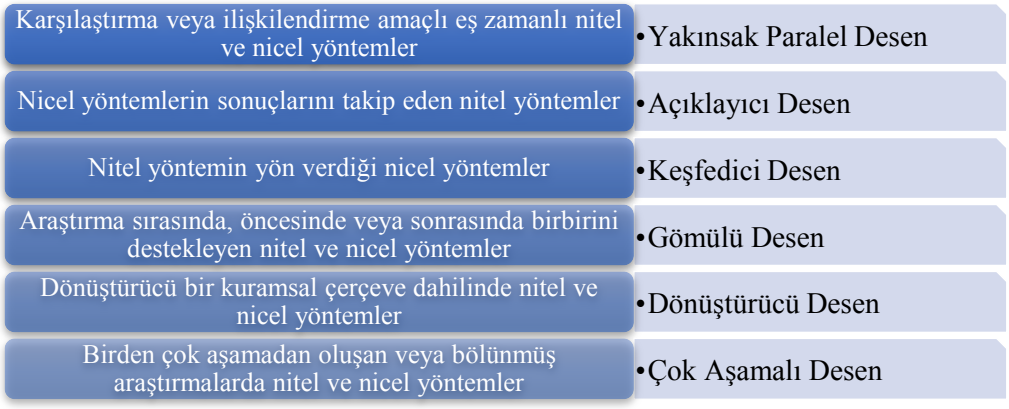
Dijital Veri Güvenliği Farkındalığı: Bireylerin bilişim teknolojilerini kullanırken kişisel bilgilerinin istenmeyen tehdit ve tehlikelerden korunması amacıyla gerekli güvenlik analizlerinin yapılması, önlemlerin alınması ve tehlikelere karşı farkında olunması durumudur (Vural ve Sağıroğlu, 2008).

İKİNCİ BÖLÜM
YÖNTEM

Bu bölümde araştırmanın yöntemi ele alınmıştır. Araştırmada kullanılan model, evren ve örneklem, verilerin toplanması ile ilgili yapılan çalışmalar, verilerin analizi ve araştırmada kullanılan istatistiksel teknikler açıklanmıştır.

Araştırmanın Modeli

Araştırma, nitel ve nicel yaklaşımların birlikte kullanıldığı karma yöntem ile desenlenmiştir. Bu bütünleşik yöntem; tek ya da pek çok aşamalı nitel ve nicel verinin toplanmasını, analiz edilmesini ve birleştirilmesini içerir (Nagy ve Biber, 2010). Alanyazında karma yöntemle ilgili farklı sınıflandırmalar yer almaktadır. Creswell (2011) karma yöntem araştırmalarını; yakınsak paralel, açıklayıcı, keşfedici, gömülü, dönüştürücü ve çok aşamalı desen olmak üzere altı başlık altında sınıflandırmıştır. Bu sınıflandırma ve özellikleri Şekil 1'de özetlenmiştir.



Şekil 1: Karma Yöntem Araştırmalarının Sınıflandırılması (Creswell, 2011, s.541)

Araştırmada, öncelikle nitel veriler toplanmıştır. Nitel verilerin analizinden elde edilen bulgulara göre dijital veri güvenliği farkındalığını ölçmeye yönelik bir ölçek geliştirilmiştir. İlgili ölçek ile nicel veriler toplanarak öğretmenlerin dijital veri güvenliğine yönelik farkındalıkları ortaya konmuştur. Nitel veriler toplandıktan sonraki bulgular, nicel veri toplanmasına yön verdiğinden araştırmada karma yöntemlerden keşfedici desen kullanılmıştır.

Araştırmanın Nitel Boyutu

Araştırmanın nitel boyutunda, öğretmenlerin ve kritik paydaşlardan olan eğitim fakültesinde görevli öğretim üyelerinin dijital veri güvenliği konusundaki görüşlerinin ortaya konması hedeflenmiştir. Bunun için, nitel araştırma desenlerinden olgubilime dayalı olarak görüşme tekniği kullanılmıştır. Yıldırım ve Şimşek'e göre (2013) olgubilim deseni, farkında olduğumuz ancak ayrıntılı bir anlayışa sahip olmadığımız olguların araştırılmasına uygun bir zemin oluşturmakta, odak grup görüşmesi tekniği ise grup dinamikleri sayesinde yanıtların derinliğini ve veri setinin zenginliğini arttırmaktadır.

Çalışma Grubu

Araştırmada amaçlı örnekleme yöntemlerinden maksimum çeşitlilik örnekleme yöntemi kullanılmıştır. Maksimum çeşitliliğe dayalı örneklem oluşturmada amaç, çeşitlilik gösteren durumlar arasındaki ortak ya da ayrılan yönlerin varlığını bulmaya çalışmak ve bu çeşitliliğe göre problemi daha geniş bir çerçevede betimlemektir (Büyüköztürk, Kılıç Çakmak, Akgün, Karadeniz ve Demirel, 2013; Yıldırım ve Şimşek, 2013).

18 katılımcıdan oluşan çalışma grubunun çeşitliliğini maksimum düzeye çıkarabilmek için; cinsiyet, mesleki deneyim, öğrenim kademesi ve görev türü değişkenleri dikkate alınmıştır. Katılımcıların tümü araştırmaya katılmayı gönüllü olarak kabul etmiştir. 12'si Balıkesir ilinin farklı ilçelerinde görev yapmakta olan öğretmenler iken diğerleri ise Anadolu Üniversitesi'nde görev yapmakta olan beş araştırma görevlisi ve bir öğretim üyesidir. Katılımcılara ait bilgiler Tablo 1'de verilmiştir.

Tablo 1

Odak Grup Katılımcılarına Ait Bilgiler

No	Cinsiyet	Mesleki Deneyim	Öğrenim Kademesi	Görevi
K1	Erkek	25 yıl	Lise	Okul Müdürü
K2	Erkek	20 yıl	Ortaokul	Okul Müdürü
K3	Erkek	22 yıl	Lise	Coğrafya Öğretmeni
K4	Erkek	20 yıl	Lise	Biyoloji Öğretmeni
K5	Kadın	13 yıl	İlkokul	Sınıf Öğretmeni

Tablo 1, Devamı

No	Cinsiyet	Mesleki Deneyim	Öğrenim Kademesi	Görevi
K6	Kadın	10 yıl	İlkokul	Sınıf Öğretmeni
K7	Erkek	-	Üniversite	Öğretim Üyesi
K8	Erkek	-	Üniversite	Araştırma Görevlisi
K9	Erkek	-	Üniversite	Araştırma Görevlisi
K10	Erkek	-	Üniversite	Araştırma Görevlisi
K11	Erkek	-	Üniversite	Araştırma Görevlisi
K12	Kadın	-	Üniversite	Araştırma Görevlisi
K13	Erkek	22 yıl	Lise	Okul Müdür Yardımcısı
K14	Erkek	19 yıl	Lise	Matematik Öğretmeni
K15	Erkek	12 yıl	Ortaokul	Türkçe Öğretmeni
K16	Erkek	14 yıl	Ortaokul	Beden Eğitimi Öğretmeni
K17	Kadın	17 yıl	İlkokul	Sınıf Öğretmeni
K18	Erkek	12 yıl	İlkokul	Sınıf Öğretmeni

Katılımcıların 4'ü kadın ve 14'ü erkektir. Mesleki deneyimleri 10 ile 25 yıl arasında değişmektedir. Görevleri; ilkokul, ortaokul, lise veya üniversite düzeyinde öğretmen, okul müdürü, müdür yardımcısı, araştırma görevlisi veya öğretim üyesidir.

Veri Toplama Araç ve Teknikleri

Nitel veri toplama aracı olarak görüşme formu kullanılmıştır. Görüşme sorularının hazırlanmasında dijital veri güvenliğine yönelik alanyazın taraması yapılmıştır. İki alan uzmanı ve bir nitel araştırma uzmanının görüşleri alınarak dokuz açık uçlu sorudan oluşan odak grup görüşme formu (Ek-A) hazırlanmıştır. Görüşmelerde katılımcılara şu sorular sorulmuştur:

1. Sahip olduğunuz kişisel bilgisayar, tablet bilgisayar, akıllı telefon gibi cihazlarda verilerinizin güvenliğini sağlamak için nelere dikkat ediyorsunuz?
2. Verilerinizin güvenliği noktasında şifreler hakkında neler söyleyebilirsiniz?
3. Verilerinizin saklanması ve taşınması için ne tür güvenlik tedbirleri alıyorsunuz?
4. Evde ve okulda bilgisayar ağlarının ve modemlerin güvenliğinin sağlanması için neler yapılmalıdır?

5. e-Okul, MEBBİS, EBA, Görevli İşlemleri Sistemi (GİS) gibi e-devlet uygulamalarının kullanımında veri güvenliği konusunu nasıl değerlendiriyorsunuz?
6. Kişisel bilgilerinizi başkalarıyla paylaşma noktasında nelere dikkat ediyorsunuz?
7. Elektronik posta (e-posta) kullanımında karşılaştığınız güvenlik sorunları nelerdir?
8. İnternet bankacılığı kullanımını ve çevrimiçi alışverişi veri güvenliği bakımından nasıl değerlendiriyorsunuz?
9. Veri güvenliğinin hukuki boyutu hakkındaki düşünceleriniz nelerdir?

Veri Toplama Süreci

Nitel verilerin toplanması sürecinde öncelikle uygulama için Balıkesir İl Milli Eğitim Müdürlüğü Araştırma Değerlendirme Komisyonu'ndan gerekli izinler alınmıştır (Ek-B). Farklı zamanlarda altışar kişilik gruplarla üç odak grup oturumu gerçekleştirilmiştir.

Öğretmenlerden oluşan iki odak grup oturumu için katılımcılar, araştırmacının görevli olduğu okula davet edilmiş ve kendilerini rahat hissedecekleri bir ortamda görüşmeler yapılmıştır. Üniversitede görevli katılımcılar ile yapılan odak grup oturumu ise görevli oldukları üniversitede uygun bir ortamda gerçekleştirilmiştir. Görüşmeler öncesinde katılımcılara sunulan görüşme onay formu (Ek-C) ile izinleri alınmıştır. Görüşmelerden ilki 54 dakika, ikincisi 84 dakika ve son görüşme 48 dakika sürmüştür.

Verilerin Analizi

Odak grup görüşmelerinden elde edilen nitel verilere içerik analizi uygulanmıştır. Yıldırım ve Şimşek'e göre (2013) bu analizde temel amaç, verileri açıklayabilecek kavramlara ve ilişkilere ulaşmak için, birbirine benzer olan verileri bir araya getirerek yorumlamaktır. Buna göre, katılımcıların görüşlerini ifade ederken kullandıkları cümleler analiz birimi olarak seçilmiştir. Cümleler analiz edildikten sonra katılımcı görüşleri bir araya getirilerek üç alan uzmanı ile birlikte temalar belirlenmiştir. Dijital veri güvenliği farkındalığı ile ilgili olduğu düşünülen birçok ifade farkındalık maddesi olarak düzenlenmiş ve 10 farklı tema altında 74 ölçek maddesi ortaya konmuştur.

Nitel verilerin geçerliğinin sağlanabilmesi için araştırmanın örneklemi çeşitlendirilmiş ve katılımcı özellikleri detaylı bir şekilde verilmiştir. Görüşme soruları

alanyazına dayalı olarak yazılmıştır. Görüşmeler veri kaybını önlemek için ses kayıt cihazı ile kaydedilerek elektonik ortama aktarılmıştır. Görüşme kayıtları ve bulgular her gruptan bir katılımcıya sunularak teyit edilmiştir. Bulgular katılımcılardan doğrudan alıntılarla desteklenmiştir. Nitel verilerin güvenirliği noktasında, yapılan görüşmelere yönelik süreç detaylı bir biçimde verilmiştir. Görüşme kayıtları gerektiğinde incelenebilmesi için saklanmıştır.

Araştırmanın Nicel Boyutu

Araştırmanın nicel boyutunda, nitel verilerin analizi sonrasında elde edilen dijital veri güvenliği farkındalığına yönelik maddelerden yola çıkılarak bir ölçek geliştirilmiştir. İlgili ölçek ile nicel veriler toplanarak öğretmenlerin dijital veri güvenliğine yönelik farkındalıkları ortaya konmuştur.

Ölçek Geliştirme Süreci

Daha önceden geliştirilmiş bir ölçek ile bireyin tepkilerine göre ilgili psikolojik özelliğin ne derece var olduğu ortaya konmaya çalışılırken; ölçek geliştirmede ise amaç, o psikolojik özelliğin ne olduğunu belirleyecek maddelerin yapılandırılmasıdır (Erkuş, 2014). Bu nedenle öğretmenlerin dijital veri güvenliği konusundaki farkındalıklarını ölçmeye yönelik olarak hazırlanan ölçeğin hazırlık aşamasında ilk olarak madde havuzu oluşturulmuştur.

Madde Havuzunun Oluşturulması

Araştırmanın nitel boyutunda gerçekleştirilen odak grup oturumları sonrasında madde havuzunun 74 maddesi ortaya çıkmıştır. Bununla birlikte ilgili alanyazında yer alan İnternet'te, sosyal ağlarda ve e-devlet uygulamalarında güvenlik, bilgi güvenliği ve bilişim suçları konulu çalışmalardan yararlanılarak 16 madde daha yazılmıştır (Karakoç, 2011; Ketizmen ve Ülküderner, 2007; Mart, 2012; Öztürk, 2012; Tekerek ve Tekerek, 2013; Yavanoğlu, Sağıroğlu ve Çolak, 2012). Tüm maddeler dikkatle incelendikten sonra ölçekte yer alması gerektiği düşünülen 3 madde de araştırmacı tarafından eklenmiştir. Böylece ölçeğin hedef kitlesinden seçilen kritik paydaşların görüşleri ve alanyazında dijital veri güvenliği kapsamında yapılmış çalışmalar dikkate alınarak 93 maddeden oluşan madde havuzu ortaya konulmuştur.

Kapsam ve Görünüş Geçerliği İçin Uzman Görüşlerinin Alınması

Maddelerin, ölçülmek istenen davranışı (özelliği) ölçmede nicelik ve nitelik olarak yeterli olup olmadığının göstergesi kapsam geçerliğidir (Büyüköztürk, 2009). Madde havuzunda yer alan maddelerin dijital veri güvenliği farkındalığını ölçmedeki yeterliliğini ve kapsama uygunluğunu belirlemek amacıyla 12 alan uzmanından, madde görüş formu kullanılarak uzman görüşü alınmıştır. Madde görüş formu oluşturulurken öncelikle ölçeğin kapsamına ilişkin açıklamaları ve uzmanlardan beklenilenleri yansıtan bir yönerge sunulmuştur. Maddelerin kapsama uygun olup olmadığına ilişkin uzman görüşleri, üçlü derecelendirme ölçeği kullanılarak elde edilmiştir ("Uygun değil" için 1 puan, "Kısmen uygun" için 2 puan, "Tamamen uygun" için 3 puan) (Ek-D). Maddelerin kapsama uygunluğuna karar verirken, her maddenin ortalama puanı hesaplanarak orta derecede uygun seçeneğinin gerçek üst sınırı olan 2.5 puan ile karşılaştırılmıştır (Kılıç Çakmak, Güneş, Çiftci ve Üstündağ, 2011). Erkuş'a göre (2014) görgül ve istatistiksel madde inceleme yönteminde uzmanların uyuşmaya vardığı maddeler kalır, bazıları gözden geçirilir, bazıları ise atılır. Buna göre madde ortalama puanı 2.5'tan küçük olan 32 madde çıkarılmış, 24 maddede düzenleme yapılmış ve 1 öneri maddesi eklenerek 62 madde elde edilmiştir. Maddeler veri toplama aracı üzerinde rastgele sıralanmıştır.

Yazılan tüm maddeler, alanında doktora derecesine sahip, lisede görevli bir edebiyat öğretmeni ile lisans mezunu, ortaokulda görevli bir Türkçe öğretmeni tarafından Türkçe dil uygunluğunun değerlendirilmesi amacıyla incelenmiştir. Uzmanlar tarafından maddeler üzerinde imla, noktalama, dil, anlam ve anlatıma ilişkin gerekli düzenlemeler yapılmıştır.

Taslak ölçek için amaca ilişkin açıklamaları ve katılımcılardan beklenenleri yansıtan bir yönerge hazırlanmıştır. Farkındalık ifadeleri beşli Likert dereceleme ile ölçeklendirilmiştir. Likert tipindeki derecelemeler; "Kesinlikle Katılıyorum", "Katılıyorum", "Kararsızım", "Katılmıyorum", "Kesinlikle Katılmıyorum" biçimindedir. Tamamı olumlu ifadeler içeren maddeler için "Kesinlikle Katılıyorum" derecesinin karşılığı 5 puan, "Kesinlikle Katılmıyorum" derecesinin karşılığı ise 1 puandır. Ölçekten elde edilen toplam puan arttıkça dijital veri güvenliği farkındalığı da artmaktadır. Tüm maddeler olumlu ifadeler içermektedir.

Son olarak ön denemeye hazır hale getirilen taslak ölçek, ölçek geliştirme konusunda deneyimli doktora derecesine sahip iki öğretim üyesi tarafından değerlendirilmiştir. Tüm bu süreçte uzman görüşleri doğrultusunda maddeler; farkındalık ifadesi olup olmadığı, maddelerin ifade ediliş biçimi, çalışmanın amacına uygunluğu ve kapsam geçerliği açısından değerlendirilmiştir.

Ön Deneme Uygulamasının Gerçekleştirilmesi

Ölçek geliştirme sürecindeki deneme uygulamasında örneklem, yalnızca ölçülen özelliğin kapsamını temsil etmeli, heterojen olmalı ve kesinlikle gönüllü katılımcılardan oluşmalıdır (Erkuş, 2014). Buna göre ön denemeye hazır hale getirilen taslak ölçek ile (Ek-E) ilkokul, ortaokul ve lise düzeyinde olmak üzere birer okulda gönüllü öğretmenlerle uygulama yapılmıştır. Karasar (1995), bir ölçeğin geliştirilmesi aşamasında yapılacak ön deneme için katılımcı sayısının 50'den az olmaması gerektiğini belirtmektedir. Buna göre, Balıkesir İli Karesi İlçesindeki 23 Nisan İlkokulu'nda görevli 23 sınıf öğretmeni, Karahallılar Ortaokulu'nda görevli 22 branş öğretmeni ve T.C. Ziraat Bankası Balıkesir Fen Lisesi'nde görevli 34 branş öğretmeni olmak üzere toplam 79 katılımcı ile ölçeğin ön deneme uygulaması gerçekleştirilmiştir. Ölçeğin ortalama yanıtlama süresi 10 dakika olarak belirlenmiştir. Uygulama sonunda bazı maddelerin anlaşılmadığı ya da boş bırakıldığı belirlenmiştir. Boş bırakılma oranı % 10'un üzerinde olan 11 maddenin frekansları ve yüzde oranları Tablo 2'de verilmiştir.

Tablo 2

Ön Deneme Sonrası Anlaşılamayan ve Boş Bırakılan Maddeler

No	Madde	f	Yüzde (%)
2	Ağ trafiğini izleyen yazılımları kullanarak, ağ güvenliğinin kontrol altına alınabileceğini bilirim.	27	34.18
5	Kırma işlemi (crack) uygulanan yazılımların güvenlik açığı oluşturabileceğinin farkındayım.	18	22.78
33*	Verilerin, çeşitli uygulamalar (dropbox, google drive vb.) kullanılarak İnternet ortamında saklanabileceğini bilirim.	18	22.78
59	Kablosuz modemin varsayılan arayüz parolasını değiştirmenin önemini bilirim.	18	22.78

Tablo 2, Devamı

No	Madde	f	Yüzde (%)
50	Kablosuz modemin arayüzünden, modeme bağlı cihazları kontrol etmek gerektiğinin farkındayım.	15	18.99
18*	Güvenlik duvarı yazılımları konusunda bilgi sahibiyim.	12	15.19
52*	Her İnternet alışverişinden sonra sanal kredi kartımın limitini sıfırlamaya dikkat ederim.	11	13.92
54	Programlar ile kurulan eklentilerin güvenliği olumsuz etkileyebileceğini bilirim.	10	12.66
40*	İnternetten alışveriş yaparken sanal kredi kartı kullanmanın önemini bilirim.	8	10.13
43	Parola kurtarma seçeneklerinden ikincil e-posta ve/veya telefon numarasını tercih etmenin önemini bilirim.	8	10.13
60*	İnternet sitelerinde kullanılan güvenlik sertifikaları hakkında bilgi sahibiyim.	8	10.13

*Ölçekte yer almasına karar verilen maddeler

Tablo 2'ye göre, 11 maddenin bilişim teknolojileri alanına özgü kavramlar ve teknik ifadeler içermesi nedeniyle öğretmenler tarafından anlaşılamadığı görülmüştür. Bu kavram ve ifadeler; ağ trafiği, kırma işlemi (crack), modem arayüzü, program eklentileri ve parola kurtarma seçenekleridir.

18, 33, 40, 52 ve 60. maddelerde katılımcıların güvenlik duvarı yazılımları, güvenlik sertifikaları ve bulut bilişim sistemleri konularındaki farkındalıkları sorulmuştur. Bu maddeleri boş bırakmaları, farkındalıklarının olmadığı anlamına gelebilir. Bu durumda "Kesinlikle Katılmıyorum" seçeneğini işaretlemeleri beklendiğinden bu beş maddenin ölçekte yer almasına karar verilmiştir. Boş bırakılan ve anlaşılamayan diğer altı madde ise formdan çıkartılmıştır. Yapı geçerliğini test etmek için örnekleme uygulanacak taslak ölçeğin son halinde 56 madde bulunmaktadır (Ek-F).

Yapı Geçerliğinin İncelenmesi

Ölçeğin yapı geçerliğini incelemek için açımlayıcı faktör analizi yapılmıştır. Tavşancıl'a göre (2006) faktör analizi, her bir madde ile yanıtlayıcıların verdiği tepkiler

arasındaki düzeni ortaya koymada ve psikolojik boyutların içeriğini tanımlamada kullanılan çok değişkenli analiz tekniklerinden biridir.

56 maddelik taslak ölçeğin (Ek-F) uygulanması için Balıkesir İl Milli Eğitim Müdürlüğü'nden gerekli izinler alınarak (Ek-G) farklı türden 18 okul maksimum çeşitlilik örnekleme yöntemine göre belirlenmiştir. Çeşitliliği maksimum düzeye çıkarabilmek için; okulun bulunduğu yerleşim yeri, öğrenim kademesi, okul türü ve resmi/özel okul olma durumları dikkate alınmıştır. Araştırmacı tarafından okulların eğitim yöneticilerine bırakılan veri toplama araçları 10 günlük süreden sonra geri toplanmıştır. Örneklemde yer alan 844 öğretmenden dönen veri toplama aracı sayısı 541'dir (% 64). Bunlardan 12 tanesi (% 2) uygun biçimde doldurulmadığından değerlendirmeye alınmamıştır. Analiz 529 veri toplama aracı ile gerçekleştirilmiştir.

Tablo 3

Veri Toplama Araçlarının Okullardan Dönüş Oranları (AFA)

Okul Adı	Gönderilen	Geri Dönen	Dönüş Oranı (%)
Balıkesir Karesi Ortaokulu	41	38	93
Özel Balıkesir Fırat Ortaokulu	39	30	77
Hacer Özer İlkokulu	21	18	86
Özel Balıkesir Fırat İlkokulu	26	10	38
Cumhuriyet İlkokulu	15	12	80
Sırrı Yırcalı Anadolu Lisesi	62	32	52
Kız Teknik Ve Meslek Lisesi	72	63	88
Burhan Erdayı İlkokulu	41	32	78
Zağnospaşa Ortaokulu	72	54	75
Sevinç Kurşun İlkokulu	58	38	66
Ayvalık Anadolu Lisesi	33	16	48
Ali Hikmet Paşa İlkokulu	46	36	78
Balıkesir Anadolu İmam Hatip Lisesi	66	20	30
Mehmetçik Ortaokulu	110	41	37
Özel Balıkesir Fırat Anadolu Lisesi	25	17	68
Şehit Mehmet Gönenç Anadolu Lisesi	45	33	73
Özel Balıkesir Fırat Fen Lisesi	21	14	67
Edremit Körfez Anadolu Lisesi	51	37	73
Toplam	**844**	**541**	**64**

Açımlayıcı faktör analizi sonucunda ortaya konan faktör yapısını doğrulamak için LISREL 8.7 programı kullanılarak doğrulayıcı faktör analizi (DFA) yapılmıştır. Çokluk, Şekercioğlu ve Büyüköztürk'e göre (2012) bu analiz sayesinde daha önceden tanımlanmış ve sınırlandırılmış bir yapının, bir model olarak doğrulanıp doğrulanmadığı test edilir.

32 maddelik ölçeğin DFA uygulaması için Balıkesir İl Milli Eğitim Müdürlüğü'nden gerekli izinler alınarak (Ek-H) farklı türden 13 okul maksimum çeşitlilik örnekleme yöntemine göre belirlenmiştir. Çeşitliliği maksimum düzeye çıkarabilmek için; okulun bulunduğu yerleşim yeri, öğrenim kademesi, okul türü ve resmi/özel okul olma durumları dikkate alınmıştır. Araştırmacı tarafından okulların eğitim yöneticilerine bırakılan veri toplama araçları bir haftalık süreden sonra geri toplanmıştır. Örneklemde yer alan 519 öğretmenden dönen veri toplama aracı sayısı 335'tir (% 65). Bunlardan 8 tanesi (% 2) uygun biçimde doldurulmadığından değerlendirmeye alınmamıştır. Analiz 327 veri toplama aracı ile gerçekleştirilmiştir.

Tablo 4

Veri Toplama Araçlarının Okullardan Dönüş Oranları (DFA)

Okul Adı	Gönderilen	Geri Dönen	Dönüş Oranı (%)
Mehmet Akif Ersoy İlkokulu	39	38	97
Gaziosmanpaşa İlkokulu	30	23	77
Yıldız Mahallesi 75.Yıl Ortaokulu	43	20	47
Mehmet Vehbi Bolak Ticaret Meslek Lisesi	43	31	72
Gaziosmanpaşa Anadolu Lisesi	36	36	100
Kadriye Kemal Gürel Güzel Sanatlar Lisesi	35	29	83
Bahçelievler Anadolu Lisesi	46	27	59
Şehit Kaymakam Rahmi Bey İlkokulu	25	19	76
Öğretmen Işıl İpek Ortaokulu	30	16	53
Alişuuri İlkokulu	42	18	43
Çiğdem Batubey Ortaokulu	68	34	50
Fatma-Emin Kutvar Anadolu Lisesi	31	19	61
Mehmetçik Ortaokulu	51	25	49
Toplam	**519**	**335**	**65**

Öğretmenlerin Dijital Veri Güvenliği Farkındalıklarının Belirlenmesi

Bu bölümde araştırmacı tarafından geliştirilen DVGFÖ kullanılarak, öğretmenlerin dijital veri güvenliği farkındalıklarını ortaya koymada izlenen yöntem anlatılmıştır.

Araştırmanın Modeli

Araştırmanın bu bölümünde öğretmenlerin dijital veri güvenliği konusundaki farkındalıklarını ortaya koyabilmek için tarama modeli kullanılmıştır. Tarama modeli, geniş gruplarda yer alan bireylerin bir konu hakkındaki fikirleri, tutumları, davranışları hakkında veri toplamak ve grubun konuya ilişkin yapısını ortaya koymak için kullanılan bir araştırma desenidir (Huck, 2012). Ayrıca araştırmada, öğretmenlerin dijital veri güvenliği farkındalıkları çeşitli değişkenlere göre incelenmiştir.

Evren ve Örneklem

Evren, araştırma sonuçlarının genellenmek istendiği elemanlar bütünü, bir çalışmayla ilgili verilerin veya ölçme sonuçlarının tümünün oluşturduğu küme ifadesiyle tanımlanabilir (Karasar, 1995). Araştırmanın evreni 2014-2015 öğretim yılında Balıkesir ilinde Milli Eğitim Bakanlığı'na bağlı resmi ve özel okullarda görev yapan 12760 öğretmendir.

Araştırmanın örneklemi olasılık temelli örnekleme yöntemlerinden tabakalı örneklemeye göre seçilmiştir. Yıldırım ve Şimşek (2013) tabakalı örnekleme yönteminin, sınırları belirlenmiş bir evrende alt tabakaların veya alt birim gruplarının var olduğu durumlarda kullanıldığını belirtmiştir. Buna göre, ilkokul, ortaokul ve lise düzeyinde farklı okul türlerinde görev yapan öğretmenler arasından tabakalı örnekleme yöntemi ile belirlenmiş 1446 öğretmen araştırmanın örneklemini oluşturmaktadır.

Veri Toplama Araç ve Teknikleri

Araştırmada veri toplama aracı olarak (Ek-I), kişisel bilgi formu ile birlikte araştırmacı tarafından geliştirilen DVGFÖ kullanılmıştır.

Kişisel Bilgi Formu: Veri toplama aracının ilk bölümünde yer alan kişisel bilgi formunda öğretmenlerin cinsiyet, branş, görev yapılan öğrenim kademesi, mesleki deneyim, öğrenim durumu, günlük bilgisayar kullanım süresi, günlük İnternet kullanım

süresi, bilgisayar, tablet bilgisayar veya akıllı telefon sahibi olma durumu bilgilerini belirlemek amacıyla sorulmuş toplam 10 madde yer almaktadır.

Dijital Veri Güvenliği Farkındalık Ölçeği: Veri toplama aracının ikinci bölümündeki DVGFÖ, bu araştırma kapsamında araştırmacı tarafından geliştirilmiştir. Tamamı olumlu ifadeler içeren 32 maddeden oluşan ölçek, dijital veri güvenliği konusundaki farkındalığı ölçmeyi amaçlamaktadır. Ölçekteki ifadeler beşli Likert tipinde "Kesinlikle Katılıyorum", "Katılıyorum", "Kararsızım", "Katılmıyorum", "Kesinlikle Katılmıyorum" biçimindedir. "Kesinlikle Katılmıyorum" seçeneğinden başlamak üzere 1'den 5'e artan şekilde puanlanmıştır.

Tek faktörlü yapıya sahip ölçekteki maddelerin faktör yükleri .506 ile .689 arasında değişmektedir. Cronbach Alfa (α) iç tutarlılık katsayısı .945'dir. Açıklanan toplam varyans % 36.053'tür.

Veri Toplama Süreci

Kişisel bilgi formu ve DVGFÖ'den oluşan veri toplama aracının uygulanabilmesi için Balıkesir İl Milli Eğitim Müdürlüğü Araştırma Değerlendirme Komisyonu'ndan izin alınmıştır (Ek-J). Çoğaltılan veri toplama aracı araştırma kapsamındaki 29 okula dağıtılarak 1446 öğretmene ulaştırılmıştır. Geri dönen veri toplama aracı sayısı 870, geri dönüş oranı % 60'tır.

Tablo 5

Veri Toplama Araçlarının Okullardan Dönüş Oranları (Son Uygulama)

Okul Adı	Gönderilen	Geri Dönen	Dönüş Oranı (%)
100. Yıl Teknik ve Endüstri Meslek Lisesi	133	79	59
17 Eylül İlkokulu	37	18	49
Adnan Menderes Anadolu Lisesi	42	13	31
Ali Hikmet Paşa Ortaokulu	51	39	76
Atatürk Anadolu Sağlık Meslek Lisesi	70	46	66
Atatürk İlkokulu	55	20	36
Balıkesir Cumhuriyet Anadolu Lisesi	55	39	71
İMKB Teknik ve Endüstri Meslek Lisesi	65	43	66
Balıkesir Lisesi	61	31	51
Balıkesir Muharrem Hasbi Anadolu Lisesi	45	35	78

Tablo 5, Devamı

Okul Adı	Gönderilen	Geri Dönen	Dönüş Oranı (%)
Balıkesir Teknik ve Endüstri Meslek Lisesi	112	46	41
Beşeylül İlkokulu	26	14	54
Cumhuriyet İlkokulu	49	25	51
Fatih İlkokulu	22	10	45
Fatih Ortaokulu	27	19	70
Fevzi Çakmak İlkokulu	23	18	78
Hacıilbey Ticaret Meslek Lisesi	40	31	78
Hasan Atlı Ortaokulu	37	19	51
Hatice Fahriye Eğinlioğlu İlkokulu	54	37	69
İstanbulluoğlu Sosyal Bilimler Lisesi	40	39	98
İstiklal İlkokulu	28	16	57
Marmara İlkokulu	29	15	52
Mehmet Akif Ersoy Ortaokulu	46	22	48
Mehmet Azman Çavuş Ortaokulu	85	56	66
Mehmet Şeref Eğinlioğlu Ortaokulu	63	35	56
Merkez Ticaret Meslek Lisesi	47	37	79
Plevne Ortaokulu	48	32	67
Şehit Süleymanbey İlkokulu	27	14	52
Şehit Süleymanbey Ortaokulu	29	22	76
Toplam	**1446**	**870**	**60**

Dönen veri toplama araçlarından 33 tanesi (% 3.8) uygun biçimde doldurulmadığından değerlendirmeye alınmamıştır. Analizler 837 öğretmene ait veri toplama aracı ile gerçekleştirilmiştir.

Verilerin Analizi

Öğretmenlerin dijital veri güvenliğine yönelik farkındalıkları belirlenerek; cinsiyet, branş, görev yapılan öğrenim kademesi, mesleki deneyim, öğrenim durumu, günlük bilgisayar kullanım süresi, günlük İnternet kullanım süresi, bilgisayar, tablet bilgisayar veya akıllı telefon sahibi olma durumu değişkenleri bakımından incelenmiştir.

Veri analizine başlamadan önce veri seti gözden geçirilmiş ve kayıp değerler olduğu görülmüştür. Ölçekte yer alan maddelerin her birinde kayıp değerler % 5'ten az olduğu için boş hücreler aritmetik ortalama ile doldurulmuştur (Little ve Rubin, 2002).

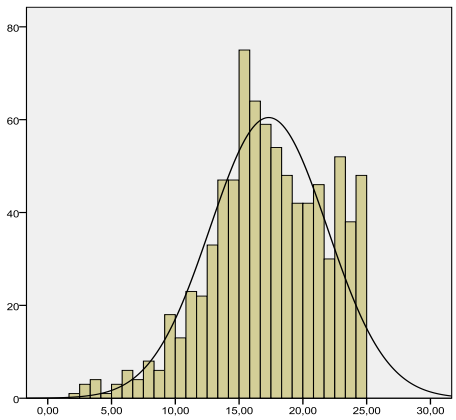
Verilerin dağılımına bakılarak parametrik veya parametrik olmayan istatistiksel yöntemler tercih edilmiştir. Yapılan analizlerde verilerin sola çarpık dağılım gösterdiği belirlenmiş ve ortalama puanların kareleri alınarak dönüşüm uygulanmıştır. Bu dönüşümden sonra normal dağılım gösteren verilerin analizinde parametrik testler kullanılmıştır.

Ölçekten elde edilen ortalama puanlara ait frekans ve yüzde dağılımları hesaplanmıştır. Ayrıca aritmetik ortalama, ortanca ve tepedeğer gibi tanımlayıcı istatistiklerden de yararlanılmıştır. Verilerin hafif bir biçimde sola çarpık dağılım göstermesi nedeniyle yapılan kare alma dönüşümü sonrasında elde edilen ortalama puana ait merkezi eğilim ve merkezi dağılım ölçüleri Tablo 6'da, Histogram grafiği ise Şekil 2'de verilmiştir.

Tablo 6

Ortalama Puana Ait Merkezi Eğilim ve Merkezi Dağılım Ölçüleri

	DVGFÖ (Puan Aralığı 1-5)
Aritmetik Ortalama	4.16
Ortanca	4.16
Tepedeğer	4.00
Standart Sapma	2.15
Çarpıklık	-.396
Basıklık	-.061



Şekil 2: Ortalama Puana Ait Histogram Grafiği

Büyüköztürk'e göre (2011) puanların dağılımında aritmetik ortalama, ortanca ve tepe değer birbirine yakınsa ve çarpıklık (Skewness) - basıklık (Kurtosis) değerleri -1 ile +1 değerleri arasında ise puanların normal dağılım gösterdiği söylenebilir ve parametrik testler kullanılabilir. Buna göre Tablo 6 ve Şekil 2 incelendiğinde ölçekten elde edilen verilerin normal dağıldığı söylenebilir ve analizlerde parametrik testler uygulanabilir.

Büyüköztürk'e göre (2009) bağımsız örneklem t-testi, iki ilişkisiz grup ortalamaları arasındaki farkın anlamlı olup olmadığını test etmek için kullanılır. Araştırmada ortalama puanlar arasındaki farkların anlamlılığı test edilirken, değişkenin iki alt grubu olduğu durumlarda bağımsız örneklem t-testi kullanılmıştır.

Tekyönlü varyans analizi (One way ANOVA) ise, ilişkisiz iki ya da daha çok örneklem ortalaması arasındaki farkın anlamlı bir şekilde farklı olup olmadığını test etmek üzere uygulanır (Büyüköztürk, 2009). Araştırmada bağımsız değişkenin alt grubu ikiden fazla olduğunda ANOVA, farklılığa neden olan grupların tespitinde ise Post Hoc izleme testlerinden Scheffe ve Dunnett C kullanılmıştır. Kalaycı'ya göre (2009) Post Hoc testleri, varyans analizi sonucunda eğer gruplar arasında bir fark bulunmuşsa, farklılığın hangi gruplardan kaynaklandığını görebilmemiz için oldukça önemlidir. Varyansların homojenliği ise Levene Statistic değerlerine bakılarak tespit edilmiştir.

Farklılıkları araştırırken; cinsiyet ve branş ile bilgisayar, tablet bilgisayar veya akıllı telefon sahibi olma durumu için bağımsız örneklem t-testi; görev yapılan öğrenim kademesi, mesleki deneyim, öğrenim durumu, günlük bilgisayar kullanım süresi ve günlük İnternet kullanım süresi için ANOVA kullanılmıştır. Uygulanan fark testlerinin tümünde, APA (2010) yazım rehberinin altıncı basımında raporlama gereği kesinlik kazanan etki büyüklükleri de hesaplanmış ve eta-kare (η^2) değeri verilmiştir. Yapılan tüm analizlerde anlamlılık düzeyi .05 olarak alınmıştır. Verilerin çözümlenmesi ve değerlendirilmesinde SPSS 18.0 yazılımı kullanılmıştır.

ÜÇÜNCÜ BÖLÜM
BULGULAR VE YORUMLAR

Bu bölümde, odak grup oturumları ile toplanan nitel verilerin analizine ait bulgu ve yorumlara, geliştirilen ölçeğin geçerlik ve güvenirlik analizlerine ait bulgu ve yorumlara, demografik değişkenlere ait frekans ve yüzde dağılımlarına, demografik değişkenler ile dijital veri güvenliği farkındalığı arasındaki ilişkilere ait bulgu ve yorumlara yer verilmiştir.

Odak Grup Görüşmelerine Ait Bulgular ve Yorumlar

Katılımcıların görüşme formunda yer alan sorulara verdikleri yanıtlar özetlenmiş, alıntılar yapılarak desteklenen bulgular aşağıda verilmiştir.

Görüşme formunda ilk soru, öğretmenlerin sahip oldukları kişisel bilgisayar, tablet bilgisayar, akıllı telefon gibi bilişim cihazlarında verilerinin güvenliğini sağlamak için nelere dikkat ettiklerini ortaya çıkarmayı amaçlamaktadır. Buna göre katılımcıların öncelikli olarak üzerinde durdukları nokta, bu cihazlarda virüslere ve casus yazılımlara karşı güncel güvenlik programları kullanılmasıdır. Katılımcılardan bazıları cep telefonlarında antivirüs programı kullanırken bazıları da akıllı telefonların güvensiz olduğunu düşünmektedir. Bir başka nokta ise İnternet ortamındaki veri güvenliğidir. Buna göre katılımcılar İnternet sitelerinin SSL sertifikası olup olmadığına, adres çubuğundaki yanlış yönlendirmelere ve dosya indirirken virüslere dikkat ettiklerini, belirli aralıklarla tarayıcı geçmişini sildiklerini belirtmişlerdir. Cihazlarındaki dijital verilerin başkalarının eline geçmesine engel olmak için cihazlarına parola koyduklarını, şifreli giriş yaparken sanal klavye kullandıklarını, ortak kullanılan cihazlara kişisel verilerin kaydedilmesi konusunda dikkat ettiklerini, beni hatırla seçeneğini kullanmadıklarını ve taşınabilir belleklerini her bilgisayara takmadıklarını söylemişlerdir. Ayrıca işletim sisteminin güvenlikle ilgili uyarılarını titizlikle inceleyen, işletim sistemini ve İnternet tarayıcılarını otomatik güncelleyen katılımcılar bulunmaktadır.

"Sahip olduğum kişisel bilgisayarımda, tabletimde mümkün olduğunca virüs programı zaten kullanıyorum." (K2)
"Telefonumun işletim sistemini sürekli güncelliyorum. Telefonumda ayrıca güncel antivirüs programı kullanıyorum." (K4)
"Telefonuma ya da bilgisayarıma benden izinsiz birileri girmesin diye başlangıç şifresi oluşturdum." (K7)
"Şifreli giriş yaparken sanal klavye kullanmaya dikkat ediyorum." (K12)
"Farklı bilgisayarlardan giriş yaparken şifremi tarayıcıya kaydetmemeye özen gösteriyorum." (K4)
"Genelde bilgisayarda çok fazla geçmiş kaydının ve parolaların kaydolmamasına özen gösteriyorum." (K12)
"Mail adresine girerken, Facebook'a, başka sosyal paylaşım ağlarına girerken bu şifrelerin hatırlanması seçenekleri oluyor. Onları kullanmamaya çalışıyorum." (K7)
"Ortak kullanılan cihazlara kişisel bilgi kaydetme konusunda dikkat etmeye çalışıyorum." (K10)
"Ziyaret ettiğim sayfaların adreslerini mutlaka gözümün önünde durur, mutlaka bakarım. İşte yanlış bir yönlendirme var mı diye." (K9)
"Güvenmediğim sitelere girmemeye dikkat ediyorum sanal ortam üzerinde." (K7)
"İşletim sisteminin karşıma çıkardığı mesaj kutularını titizlikle inceliyorum." (K9)
"Özellikle işletim sistemimin ve web tarayıcılarımın güncellemelerine titizlik gösteririm." (K9)

Araştırma kapsamındaki bir diğer soru ise verilerin güvenliği noktasında parolalar ile ilgilidir. Katılımcılar, parolaların güvende olabilmesi için harf, sayı ve özel karakterlerden oluşan güçlü parolalar kullanılması gerektiği konusunda farkındalığa sahiptir. Ancak günlük yaşantılarında çok sayıda parola kullanılması gerektiğinden kısa, kolay ve hatırlayabilecekleri parolalar kullandıklarını belirtmişlerdir. Bununla birlikte çoğu katılımcı her türlü parolanın kırılabileceğini, cep telefonlarına gelen tek kullanımlık parolaların ise daha güvenli olduğunu düşünmektedir. Parolalarını saklamak için kâğıda yazmak, akıllı telefona kaydetmek veya Dropbox hesabında tutmak gibi yöntemler kullanmaktadırlar. Parolalarını belirli aralıklarla değiştirdiğini söyleyen katılımcılar, giriş yaptıkları yerin önem derecesine göre farklı karmaşıklık seviyelerinde parolalara sahiptir.

"O kadar çok yerde o kadar çok şifre kullanıyorsunuz ki, diyorsunuz ki, artık basit ve devamlı hatırlayacağım bir şifre kullanayım." (K1)
"Ben oluştururken sayının yanında harf de koyuyorum. Bunun daha güvenli olduğunu düşünüyorum." (K5)

"Bazen ortak şifreler kullandığımız oluyor." (K2)
"Farklı işler için çok çeşitli şifre kullanırsak daha güvenli olur diye düşünüyorum." (K17)
"Ne kadar da karmaşık olsa herhalde insanlar bunun bir yolunu yöntemini buluyorlar gibi geliyor." (K3)
"Kendi evimizde bile şifremi kaydetmemeye özen gösteriyorum." (K4)
"Kullandığım yerin önem derecesine farklı seviyelerde şifrelerim var." (K8)
"Telefona gelen tek kullanımlık şifreler güvenli olabilir." (K13)
"Şifrelerimi kâğıda yazıp yanımda taşıyorum." (K17)
"Parolalarımı Dropbox hesabımda tutuyorum." (K11)

Odak grup görüşmelerinde öğretmenlere yöneltilen üçüncü soru ise verilerinin saklanması ve taşınması için ne tür güvenlik önlemleri aldıklarıdır. Buna göre katılımcılar dijital verilerini; kişisel bilgisayarlarında, taşınabilir belleklerinde, e-posta hesaplarında, bulut bilişim sistemlerinde (Gmail, Dropbox, Google Drive vb.), DVD veya CD'lerde saklamaktadır. Bununla birlikte katılımcılar, boyutu az olan dosyaları e-posta ve sosyal ağ hesaplarında, büyük boyuttaki dosyaları ise bulut bilişim sistemlerinde saklamanın verilerin taşınması noktasında taşınabilir belleklere göre daha güvenli olduğunu düşünmektedir. Ayrıca taşınabilir bellekleri sınıflandırdıklarını, verileri saklamak yerine taşıma amaçlı kullandıklarını ve güvenli olmadığını düşündükleri cihazlarda kullanmamaya çalıştıklarını belirtmişlerdir. Çok önemli dosyaların şifrelenmesi ve üzerinde çalışılan dosyanın tarihine göre isimlendirip farklı ortamlarda yedeklenmesi de katılımcıların aldıkları önlemler arasındadır.

"Kaybettiğimde veya zarar geldiğinde üzüleceğim bilgileri hard diskimde evde muhafaza etmeye çalışıyorum." (K2)
"Bazı bilgilerimi, belgelerimi de mailime atıyorum. Hem istediğim yerden erişebiliyorum hem Flash diskte saklamaktan daha güvenli geliyor." (K3)
"Bazen CD'ye basıyoruz daha kalıcı olması için." (K4)
"Yazılı soruları veya kişisel verilerin bulunduğu Flash bellekleri sadece evimdeki ya da okulda kendi belirlediğim güvendiğim bir bilgisayarda kullanıyorum." (K6)
"Bulut bilişimin sağladığı Google Drive, Dropbox gibi sistemler üzerinden de gerekli gördüğüm dosyaları saklayabiliyorum." (K7)
"Küçük boyutlu olarak, belge olarak benim için önemli olanları e-mail yoluyla saklıyorum." (K17)
"Bu Flash disklere hiç güvenmediğim için sadece taşıma amaçlı kullanıyorum." (K8)

Öğretmenlere yöneltilen dördüncü soru, evde ve okulda bilgisayar ağlarının ve modemlerin güvenliğini sağlamak için neler yapılması gerektiği ile ilgilidir. Buna göre katılımcılar; kablosuz modemlere karmaşık yapıda parola konması, belirli aralıklarla bu parolaların değiştirilmesi ve hiç kimseyle paylaşılmaması gerektiğini belirtmişlerdir. Ayrıca bazı katılımcılar; kablosuz modemlerde MAC filtreleme yapılabileceğinin, görünebilirliğin kapatılabileceğinin, ara yüzden bağlı cihazların takip edilebileceğinin, ağ trafiğini izleyen yazılımlar ile ağ güvenliğinin kontrol altına alınabileceğinin farkındadır. Okullardaki ağ yapısını değerlendiren öğretmenler, MEB hattı kullanıldığı için okuldaki İnternette güvenlik sorunu yaşanmayacağını düşünmektedir ve öğrenciler nedeniyle okuldaki bilgisayar ağında dosya paylaşımını güvenlik açısından sakıncalı bulmaktadır.

"Modemlere şifre koyarak başkalarının kullanmasını engellemek amacıyla güvenlik şifresi koyuyoruz." (K18)
"Şifreli kullanıyoruz ve bir iki ayda bir değiştiriyoruz." (K1)
"Modemin ağda görünmemesini sağlıyorum." (K9)
"Zaman zaman modemin ara yüzüne bağlanıp modeme kimlerin bağlı olduğunu görmeliyiz." (K12)
"Ağ trafiğini izleyen, kontrol eden yazılımlar olduğunu biliyorum." (K7)
"MEB hattı olduğu için okuldaki hattımız ondan dolayı güvenlik sorunu yaşamayız diye düşünüyorum." (K1)
"Öğrenciler nedeniyle dosya paylaşımını güvenlik açısından sakıncalı buluyorum." (K3)

Diğer bir soruda, öğretmenlerin e-Okul, MEBBİS, EBA, GİS gibi e-devlet uygulamalarının kullanımında veri güvenliğini değerlendirmeleri istenmiştir. Buna göre katılımcılar, e-devlet uygulamalarına girişte cep telefonuna gelen parolanın güvenliği arttıracağını düşünmektedir. Ayrıca e-devlet uygulamalarında alt yapının güçlendirilmesi, bu uygulamaların güvenli kullanımı konusunda bilgilendirilme yapılması ve güçlü parolalar kullanılması konusunda yaptırım getirilmesi gerektiğini belirtmişlerdir. Katılımcıların bazıları ise e-Okulda yönetici parolasına sahip okul müdürlerinin, öğretmenlerin tüm bilgilerini görebilmesi nedeniyle endişe duymaktadır.

"e-Okul, EBA, GİS gibi sitelere cep telefonu şifresiyle girilmesi güvenliği arttıracaktır." (K1)
"e-devlet uygulamalarında alt yapının güçlendirilmesi gerektiğine inanıyorum." (K7)
"Türkiye'deki kamunun bu dijital veri güvenliği konusunda, siber güvenlik konusunda çok eksiklikleri olduğunu yazıyorlar, çiziyorlar." (K15)

"Bence İLSİS'in kullanımı ile ilgili İLSİS'teki verilerin güvenliğini sağlamaya ve kullanıcıların bilinçlendirilmesine yönelik bir eğitim programı yapılmalı." (K9)
"Güvenli şifre kullanmıyorsunuz şeklinde bilinçlendirmeleri ile bir yaptırıma gidilebilir diye düşünüyorum." (K10)
"Sistemin başındakilerin güvenli olması gerekir." (K17)

Odak grup görüşme formunda yer alan altıncı soru, öğretmenlerin kişisel bilgilerini başkalarıyla paylaşma noktasında nelere dikkat ettiklerini ortaya çıkarmayı amaçlamaktadır. Katılımcılar bu soruyu sosyal ağlar bağlamında değerlendirmiş ve bazıları, en ince ayrıntısına kadar güvenlik ayarları yapıldığında bile paylaşımların güvenli olmadığını belirtmiştir. Katılımcıların çoğu, fotoğraflarını ve kişisel bilgilerini paylaştığını, yer bildiriminde bulunduğunu ifade etmiştir. Buna karşın doğum tarihini, telefon numarasını paylaşmayan ve tanımadığı kişileri sosyal ağına eklemediğini belirten katılımcılar da vardır.

"Sosyal paylaşımlardaki riskin çok büyük olduğunu düşünüyorum." (K1)
"Sosyal ağların güvenliği için yapabileceğim çok bir şey olduğunu zannetmiyorum." (K2)
"Gizlilik ayarları olmasına rağmen yine de çok güvenli olduğunu düşünmüyorum." (K4)
"Tanımadığım kişileri mümkün olduğunca eklemiyorum." (K14)
"Facebook'ta yer bildiriminde bulunuyorum." (K1)
"Doğum tarihi gibi şahsi bilgiler konusunda doğru bilgileri vermiyorum." (K16)
"Sosyal ağlarda kişisel bilgilerimi paylaşmamaya dikkat ediyorum." (K10)

Araştırma kapsamındaki bir diğer soru ise, e-posta kullanımında öğretmenlerin karşılaştığı güvenlik sorunlarını belirlemeye yöneliktir. Buna göre katılımcılar; güvenli olmayan e-postaları açmadan sildiklerini, e-postadaki ekleri önce bilgisayara indirip sonra açtıklarını, istem dışı e-posta filtresi etkili ve virüs taraması yapan e-posta sağlayıcılarını tercih ettiklerini, güvenli bulmadıkları e-postaları istem dışı e-posta olarak işaretlediklerini belirtmişlerdir. Ayrıca katılımcılar; şifresi farklı olan ikinci bir e-posta hesabı veya cep telefonu ile doğrulama yöntemini kullanarak e-posta hesaplarının güvence altına alınabileceğini düşünmektedir.

"Bilmediğimiz kişilerden gelen mailleri açmamaya özen gösteriyorum." (K14)
"Gelen e-postadaki ekleri önce bilgisayarıma indirip sonra açıyorum." (K3)
"e-postaları virüs taramasından geçiren siteleri tercih ediyorum." (K6)
"Sahte e-postaları spam olarak işaretliyorum." (K8)

"Cep telefonu ile doğrulama yöntemini kullanıyorum." (K10)
"Şifresi farklı olan ikinci bir mail adresi ile doğrulama yöntemi kullanılabilir." (K12)

Öğretmenlere yöneltilen sekizinci soruda, İnternet bankacılığı kullanımında ve çevrimiçi alışverişte veri güvenliğini nasıl değerlendirdikleri sorulmuştur. Katılımcıların aldıkları önlemler arasında; sanal klavye ve sanal kart kullanılması, cep telefonuna gelen tek kullanımlık parolalar kullanılması, yalnızca kendilerine ait veya güvenilir cihazlardan giriş yapılması sayılabilir. Ayrıca katılımcılar, güvenli olduğunu düşündükleri sitelerden alışveriş yaptıklarını, İnternet sitelerindeki güvenlik sertifikalarını ve adres çubuğundan başka bir siteye yönlendirme olup olmadığını kontrol ettiklerini ifade etmiştir.

"Sanal klavye kullanılması tercih ediliyor." (K17)
"Bankanın kredi kartının internet ortamında sanal kart yaratıyorum." (K2)
"Bankalarda cep telefonuna mesaj geldiği için onların güvenliğinde çok sıkıntı yok." (K6)
"İnternet bankacılığı ve alışveriş yaparken kendime ait cihazları kullanıyorum." (K7)
"İnternet bankacılığı kullanırken güvenilir bir bilgisayardan girmeye çalışıyorum." (K4)
"Güvenmediğim sitelerden alışveriş yapmıyorum." (K9)
"Çevrimiçi alışveriş yaparken SSL sertifikası var mı diye bakıyorum." (K11)
"Bankacılık vs. gibi güvenlik isteyen bir siteye bağlandığım zaman farklı bir yere yönlendirilmediğimden emin oluyorum." (K8)

Odak grup görüşmelerindeki son soru ise, veri güvenliğinin hukuki boyutu konusunda öğretmenlerin düşüncelerini ortaya koymaya yöneliktir. Katılımcılar, hukuki düzenlemelerin yeterli olmadığını, bununla birlikte Türkiye'de hukuki sürecin çok hızlı işlediğine ve geliştiğine inandıklarını belirtmişlerdir. Ayrıca hukuki boyutun eksikliği nedeniyle sosyal ağlara şüpheyle yaklaştıklarını, İnternet kullanımı ve sosyal medyanın hukuki boyutu konularında bilgilendirme yapılması gerektiğini ifade etmişlerdir. Katılımcıların bu konuyu yönelik olarak önerileri arasında, bilişim suçlarına yönelik ortaokullarda ve liselerde bir saatlik seçmeli ders okutulması ve öğretmenlerden uzman görüşü alınması sayılabilir.

"Türkiye'de hukuki sürecin çok hızlı işlediğine ve geliştiğine inanıyorum." (K2)
"Hukuki boyutun eksikliği nedeniyle sosyal ağlara hep şüpheyle yaklaşıyorum." (K2)

"Hukuki düzenlemelerin yeterli olduğunu düşünmüyorum." (K13)
"Suçlunun bulunması çok zor olduğu için çekiniyoruz." (K3)
"İnternet kullanımı ve sosyal medyanın hukuki boyutu anlamında hepimizin bilgilendirilmesi gerekiyor." (K4)
"Öğretmenlerden uzman görüşü alınabilir." (K6)
"Bilişim suçları ile ilgili ortaokulda ve lisede bir saatlik ders olabilir." (K6)

Katılımcılar, veri güvenliğinin hukuki boyutu kapsamında lisanslı yazılım kullanma ve telif haklarına da değinmişlerdir. Buna göre katılımcılar, sanal ortamdaki telif hakları konusunda içeriğin asıl sahibini bulmanın zor olduğunu düşünmekte ve hangi durumların suç olup olmadığını bilmediklerini ifade etmektedir. Lisansları olmayan yazılımların bilgisayarlara zarar verebileceğinin farkında oldukları halde maliyetleri nedeniyle yalnızca okullarında lisanslı yazılım kullandıklarını, evlerinde ise lisanssız veya çoklu kullanıcıya izin veren lisanslı yazılımları kullandıklarını belirtmişlerdir.

"Sanal ortamda telif hakları konusunda içeriğin asıl sahibini bulmak zor." (K8)
"Lisansları olmayan yazılımlar bilgisayara zarar verebiliyor." (K13)
"Evde lisanslı yazılım kullanmıyoruz." (K3)
"Okulda kullandığımız programlar lisanslı." (K3)
"Maliyetleri bildiğim kadarıyla çok yüksek. Dolayısıyla bunlar evden yerine daha çok kurumlarda kullanılıyor." (K4)
"Bazı virüs yazılımlarında alıyorsunuz, 3-4 bilgisayarda kullanabiliyorsunuz." (K6)

Yapılan odak grup görüşmeleri sonrasında 18 katılımcı, kendilerine yöneltilen sorulara ilişkin 10 farklı tema altında 477 adet görüş bildirmiştir. Temalar altında toplanan katılımcı görüşlerinin, görüşmelere göre dağılımı Tablo 7'de verilmiştir.

Tablo 7

Katılımcı Görüşlerinin Görüşmelere Göre Dağılımı

Tema Adı	**Görüşme (1) 54 dakika**	**Görüşme (2) 84 dakika**	**Görüşme (3) 48 dakika**	**Görüş Sayısı**
1.Bilişim cihazlarında veri güvenliği	18	34	18	70
2.Parola güvenliği	28	24	17	69
3.Verilerin saklanması, yedeklenmesi ve taşınması	15	20	17	52
4.Bilgisayar ağlarında ve modemlerde veri güvenliği	17	15	13	45
5.e-devlet uygulamalarında veri güvenliği	6	6	10	22
6.Sosyal paylaşım ağlarında veri güvenliği	29	14	16	59
7.e-posta kullanımında veri güvenliği	16	8	6	30
8.İnternet bankacılığı ve çevrimiçi alışverişte veri güvenliği	18	16	21	55
9.Veri güvenliğinde hukuki boyut	24	7	10	41
10.Lisanslı yazılımlar ve telif hakları	26	4	4	34
Toplam	**197**	**148**	**132**	**477**

Tablo 7'ye göre en fazla görüş (197) ilk odak grup oturumunda elde edilmiştir. Bu gruptaki öğretmenlerin kendilerini daha rahat hissettikleri ve çok sayıda farklı yanıt verdikleri görülmüştür. İkinci görüşme, üniversitede görevli araştırma görevlileri ve öğretim üyesi ile gerçekleştirilmiş olup ilk görüşmeye göre daha uzun sürmüştür. Ancak konu başlıkları derinlemesine irdelendiğinden ve daha çok teknik kavramlar üzerinde durulduğundan daha az sayıda (148) görüş ortaya konmuştur. Üçüncü ve son odak grup oturumunda ise katılımcılardan ikisi çekingen davranışlar sergilemiş ve daha az söz almıştır. Dolayısıyla en az maddenin ortaya konduğu görüşme (132) üçüncü görüşme olmuştur.

Ulaşılan 10 temadan en çok görüş bildirilenler "bilişim cihazlarında veri güvenliği" (70) ve "parola güvenliği" (69) olurken, "e-devlet uygulamalarında veri güvenliği" temasında yalnızca 22 görüş kaydedilmiştir. Her katılımcının bildirdiği görüş sayısının temalara göre dağılımı ise Tablo 8'de verilmiştir.

Tablo 8

Katılımcı Görüşlerinin Temalara Göre Dağılımı

Tema	**Katımcıların Belirttiği Görüş Sayısı**																	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**
1.Bilişim cihazlarında veri güvenliği	6	2	1	5	2	2	6	4	10	3	3	8	4	3	4	2	2	3
2.Parola güvenliği	7	4	7	5	2	3	5	6	2	5	5	1	5	3	2	2	3	2
3.Verilerin saklanması, yedeklenmesi ve taşınması	2	3	4	2	1	3	7	4	4	3	2	-	3	1	1	6	4	2
4.Bilgisayar ağlarında ve modemlerde veri güvenliği	7	-	5	1	-	4	3	3	3	-	3	3	1	5	1	1	3	2
5.e-devlet uygulamalarında veri güvenliği	2	2	-	-	-	2	2	-	2	2	-	-	2	1	2	-	2	3
6.Sosyal paylaşım ağlarında veri güvenliği	5	3	6	4	8	3	3	-	4	2	-	5	3	3	1	8	-	1
7.e-posta kullanımında veri güvenliği	3	-	5	1	1	6	-	2	2	3	-	1	-	2	1	1	-	2
8.İnternet bankacılığı ve çevrimiçi alışverişte veri güvenliği	2	4	3	6	2	1	2	2	2	3	2	5	3	1	8	-	6	3
9.Veri güvenliğinde hukuki boyut	2	6	4	2	2	8	-	-	2	-	-	5	2	-	2	-	1	5
10.Lisanslı yazılımlar ve telif hakları	8	1	10	2	3	2	-	1	-	-	1	2	1	1	-	2	-	-
Toplam	**44**	**25**	**45**	**28**	**21**	**34**	**28**	**22**	**31**	**21**	**16**	**30**	**24**	**20**	**22**	**22**	**21**	**23**

Tablo 8'e göre görüşmelerde en çok görüş bildiren katılımcılar 1 ve 3 numaralı katılımcılardır. Her ikisi de okul müdürü olup görüşmelerde kendilerini öğretmenlere göre daha rahat hissetmiş ve sık sık söz alarak görüş bildirmişlerdir. Yapılan üç odak grup oturumunda en az 11 numaralı katılımcı görüş bildirmiştir. Az sayıda söz almış ve kısa ifadeler kullanarak sözlerini tamamlamıştır.

Katılımcılar tarafından belirtilen görüşlere dayanılarak elde edilen 477 ifade, benzer olmalarına ve dijital veri güvenliği ile ilgili olma durumlarına göre düzenlenmiştir. Geliştirilen ölçeğe alt yapı oluşturan bu maddelerin temalara göre dağılımı Tablo 9'da verilmiştir.

Tablo 9

Maddelerin Temalara Göre Dağılımı

Tema	**Madde Sayısı**
Bilişim cihazlarında veri güvenliği	18
Parola güvenliği	12
Verilerin saklanması, yedeklenmesi ve taşınması	6
Bilgisayar ağlarında ve modemlerde veri güvenliği	7
e-devlet uygulamalarında veri güvenliği	4
Sosyal paylaşım ağlarında veri güvenliği	5
e-posta kullanımında veri güvenliği	5
İnternet bankacılığı ve çevrimiçi alışverişte veri güvenliği	9
Veri güvenliğinde hukuki boyut	3
Lisanslı yazılımlar ve telif hakları	5
Toplam	**74**

Tablo 9'a göre, öğretmenlerin dijital veri güvenliği farkındalıklarını belirlemeye yönelik geliştirilen ölçeğe alt yapı oluşturan 74 maddenin 10 tema altında toplandığı görülmektedir.

Ölçeğin Geçerlik ve Güvenirlik Analizlerine Ait Bulgular ve Yorumlar

Faktör analizi öncesinde 56 maddelik taslak ölçek üzerinde madde istatistikleri yapılmıştır. Buna göre 1. ve 8. maddelerin madde toplam korelasyonlarının .40'tan küçük olduğu görülmüştür. Aynı zamanda çıkarıldıklarında Cronbach Alfa (α) değeri de yükselmektedir. Beklenen sınırlarda yer almayan bu iki madde analizden çıkartılmıştır.

Açımlayıcı faktör analizi 529 katılımcıya ait veri toplama aracı ile gerçekleştirilmiştir. Örneklem büyüklüğü konusunda Comrey ve Lee (1992), 100 katılımcının yetersiz, 200'ün ortalama, 300'ün iyi, 500'ün çok iyi ve 1000 katılımcının ise mükemmel olduğunu belirtmektedir (akt. Akbulut, 2010). Toplanan verilerin faktör analizine uygunluğu Kaiser-Meyer-Olkin (KMO) ve Barlett Küresellik testi ile sınanmıştır. Analiz sonuçları Tablo 10'da verilmiştir.

Tablo 10

KMO ve Barlett Küresellik Testi Sonuçları-1

Kaiser-Meyer-Olkin Örneklem Uyum Ölçüsü		.951
Barlett Küresellik Testi	X^2	15113.267
	sd	1431
	p	<.001

Tablo 10'da görüldüğü gibi örneklem büyüklüğünün uygunluğu KMO ve Barlett istatistiği ile onaylanmıştır (KMO=.951, X^2=15113.267, p<.001). KMO değerinin eşik değer olan .600'den büyük olması ve Barlett-Küresellik testi için bulunan X^2 değerinin anlamlı olması nedeniyle örneklemin faktör analizine uygun olduğu söylenebilir (Cohen, Manion ve Morrison, 2007).

Faktör yapısını ortaya koyabilmek için SPSS 18.0 ile açımlayıcı faktör analizi yapılmıştır. Açımlayıcı faktör analizinde Maximum Likelihood yöntemi kullanılmıştır. Bu yöntem Stevens'a göre (1996) ölçek geliştirme çalışmalarında faktörler altında gerçekten işe yarayan ortak varyansı dikkate alır ve düşük varyansa karşın daha sağlam bir yapı sunar.

54 maddeden oluşan veri seti üzerinde döndürme (rotation) yapılmamış Maximum Likelihood analizinde, özdeğeri 1'den büyük olan dokuz boyut ile toplam varyansın % 50.167'sinin açıklandığı görülmüştür. Analiz sonuçları Tablo 11'de verilmiştir.

Tablo 11

Toplam Açıklanan Varyans (54 Madde)

Bileşen	Başlangıç Özdeğerleri			Yük Değerleri		
	Toplam	Varyans (%)	Birikimli (%)	Toplam	Varyans (%)	Birikimli (%)
1	18.790	34.796	34.796	18.283	33.858	33.858
2	2.858	5.293	40.088	2.372	4.393	38.251
3	2.290	4.242	44.330	1.775	3.287	41.538
4	1.776	3.289	47.619	1.263	2.339	43.877
5	1.292	2.392	50.011	.790	1.463	45.340
6	1.243	2.303	52.313	.792	1.467	46.807
7	1.126	2.085	54.399	.671	1.243	48.050

Tablo 11, Devamı

Bileşen	Başlangıç Özdeğerleri			Yük Değerleri		
	Toplam	Varyans (%)	Birikimli (%)	Toplam	Varyans (%)	Birikimli (%)
8	1.069	1.979	56.378	.611	1.132	49.182
9	1.009	1.868	58.246	.532	.985	50.167
10	.989	1.831	60.077			
11	.973	1.802	61.879			
12	.932	1.726	63.605			
13	.855	1.584	65.188			
14	.848	1.571	66.759			
15	.776	1.436	68.195			

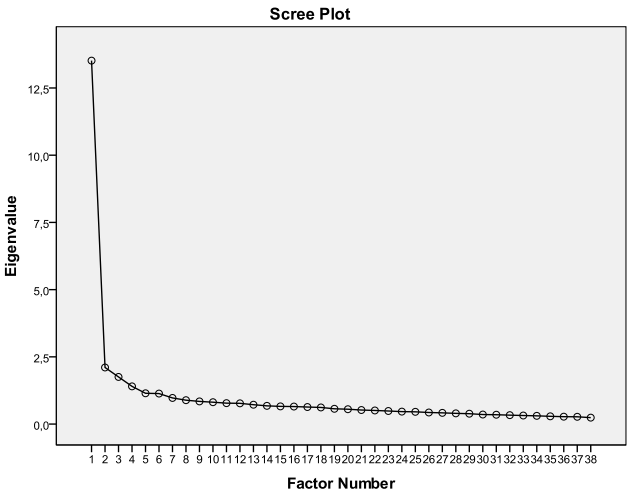
Tablo 11'e göre özdeğeri 1'den büyük dokuz faktör görünse de, ideal faktör yapısının belirlenebilmesi için döndürme yapılmıştır. Döndürme işlemlerinde "varimax" yöntemi tercih edilmiştir. Tavşancıl (2006), varimax yönteminde basit yapıya ve anlamlı faktörlere ulaşmada faktör yükleri matrisinin sütunlarına öncelik verildiğini ve daha az değişkenle faktör varyanslarının en yüksek olması sağlanacak şekilde döndürme yapıldığını belirtmektedir. Farklı denemelerden sonra madde istatistikleri incelenmiş ve beklenen sınırlarda yer alamayan 17 madde çıkartılarak açımlayıcı faktör analizi yeniden yapılmıştır.

Analiz başlangıcında 39 madde olmasına karşın 1. maddenin madde toplam korelasyonu .40'tan küçük ve ortak faktör varyansı da .30'dan küçüktür. Atıldığında Cronbach Alfa (α) değeri yükselmektedir. Dolayısıyla 1. madde çıkarılarak 38 madde ile AFA yapılmıştır. Analiz sonucunda elde edilen değerler ve yamaç birikinti grafiği aşağıda verilmiştir.

Tablo 12

Toplam Açıklanan Varyans (38 madde)

Bileşen	Başlangıç Özdeğerleri			Yük Değerleri		
	Toplam	Varyans (%)	Birikimli (%)	Toplam	Varyans (%)	Birikimli (%)
1	13.517	35.571	35.571	12.988	34.179	34.179
2	2.105	5.539	41.110	1.578	4.153	38.332
3	1.753	4.613	45.723	1.219	3.208	41.540
4	1.403	3.691	49.414	.925	2.434	43.974
5	1.145	3.014	52.428	.664	1.747	45.721
6	1.134	2.985	55.414	.642	1.691	47.411
7	,972	2,558	57,971			
8	,888	2,338	60,309			
9	,843	2,218	62,527			
10	,813	2,140	64,667			
11	,778	2,047	66,715			
12	,771	2,030	68,745			
13	,720	1,895	70,640			
14	,678	1,783	72,423			
15	,658	1,731	74,154			



Şekil 3: Yamaç-Birikinti Grafiği

Tablo 12'de özdeğeri 1'den büyük altı faktör görünse de birinci faktöre ait özdeğer, ikinci faktöre ait özdeğerin yaklaşık sekiz katıdır. Aynı zamanda Şekil 3 incelendiğinde, birinci faktöre ait özdeğerden sonra hızlı bir düşüş görülmektedir ve ikinci faktörden itibaren toplam varyansa katkı azalmaktadır. Çokluk, Şekercioğlu ve

Büyüköztürk (2012) bu tür durumlarda faktör sayısının 1 olarak belirlenmesine karar verilebileceğini belirtmiştir.

Büyüköztürk'e göre (2009) faktör yük değerlerinin .45 ya da daha yüksek olması seçim için iyi bir ölçüdür. Bu bağlamda pek çok araştırmada bu değer .50 olarak kabul edilmiştir (Demir ve Akengin, 2010; Ursavaş, Şahin ve McIlroy, 2014). Bu araştırmada da madde faktör yük değerlerinin alt kesme noktası .50 olarak belirlenmiştir. Tek faktöre göre yapılan analizde faktör yük değerleri .50'nin altında olan altı madde ölçekten çıkartılmıştır. Oluşan yeni veri setinin faktör analizine uygunluğu Kaiser-Meyer-Olkin (KMO) ve Barlett Küresellik testi ile sınanmıştır. Analiz sonuçları Tablo 13'te verilmiştir.

Tablo 13

KMO ve Barlett Küresellik Testi Sonuçları-2

Kaiser-Meyer-Olkin Örneklem Uyum Ölçüsü		.949
Barlett Küresellik Testi	X^2	8010.484
	sd	496
	p	<.001

Tablo 13'te görüldüğü gibi örneklem büyüklüğünün uygunluğu KMO ve Barlett istatistiği ile onaylanmıştır (KMO=.949, X^2=8010.484, p<.001). Açımlayıcı faktör analizi sonucunda elde edilen değerler Tablo 14'te verilmiştir.

Tablo 14

Toplam Açıklanan Varyans (32 madde)

Bileşen	Başlangıç Özdeğerleri			Yük Değerleri		
	Toplam	Varyans (%)	Birikimli (%)	Toplam	Varyans (%)	Birikimli (%)
1	12.168	38.026	38.026	11.537	36.053	36.053
2	1.879	5.872	43.898			
3	1.493	4.664	48.562			
4	1.240	3.875	52.437			
5	1.086	3.394	55.831			
6	.965	3.014	58.845			
7	.833	2.605	61.450			
8	.805	2.516	63.966			
9	.790	2.470	66.436			
10	.749	2.340	68.776			
11	.692	2.163	70.939			
12	.667	2.084	73.022			
13	.648	2.026	75.049			
14	.626	1.957	77.006			
15	.599	1.871	78.877			

Tablo 14'e göre, 32 maddeden oluşan tek faktörlü DVGFÖ'nün toplam açıklanan varyans oranı % 36.053 olarak bulunmuştur. Büyüköztürk (2009) tek faktörlü desenlerde açıklanan varyansın % 30 ve üzerinde olmasının yeterli görülebileceğini ifade etmiştir. Buna göre ortaya konulan tek faktörün, açıklanan varyansa katkısının yeterli olduğu söylenebilir. Ölçeğin tek faktörlü yapısına ilişkin yük değerleri Tablo 15'te verilmiştir.

Tablo 15

Maddelerin Faktör Yük Değerleri

Madde	Faktör 1
M37	.689
M49	.688
M41	.677
M52	.664
M43	.663
M50	.662
M24	.642
M26	.640
M42	.637
M31	.633
M45	.627
M25	.625
M56	.621
M53	.600
M51	.597
M19	.592
M35	.591
M54	.588
M32	.587
M22	.583
M27	.571
M11	.568
M10	.566
M18	.565
M16	.560
M28	.557
M40	.554
M29	.536
M39	.531
M6	.512
M9	.510
M30	.506

Tablo 15'e göre, maddelerin faktör yükleri .506 - .689 arasında değişmektedir ve Cronbach Alfa (α) iç tutarlılık katsayısı .945'tir. Bu değer Kalaycı'nın (2009) önerdiği yüksek güvenilirlik sınırı olan .80'in üzerindedir. Buna göre ölçüm sonuçlarının yüksek derecede güvenilir olduğu söylenebilir. Benzer çalışmalarda Cronbach Alfa (α) katsayıları; Dönmez ve diğerlerinin (2014) geliştirdiği Öğretmen Adaylarının Algılanan İnternet Riskleri Ölçeği'nde.856, Tekerek ve Tekerek (2013) tarafından geliştirilen Bilgi Güvenliği Farkındalığı Ölçeği'nde .720 ve Mart'ın (2012) geliştirdiği Bilgi Güvenliği Farkındalığı Belirleme Anketi'nde .638 olarak hesaplanmıştır.

Tablo 16

Madde Ayırt Edicilik Değerleri

Madde	Korelasyon Katsayısı	Madde	Korelasyon Katsayısı	Madde	Korelasyon Katsayısı
M6	.512	M27	.552	M42	.623
M9	.488	M28	.533	M43	.639
M10	.553	M29	.515	M45	.603
M11	.558	M30	.483	M49	.668
M16	.560	M31	.620	M50	.643
M18	.557	M32	.563	M51	.568
M19	.583	M35	.561	M52	.644
M22	.564	M37	.671	M53	.575
M24	.624	M39	.511	M54	.582
M25	.605	M40	.535	M56	.604
M26	.628	M41	.664		

Tablo 16'daki madde ayırt edicilik değerleri incelendiğinde .483 ile .671 arasında değiştiği gözlenmektedir. Büyüköztürk'e göre (2009) madde-toplam korelasyonu katsayısının .40'tan büyük olması çok iyi derecede bir madde olduğunun göstergesidir. Buradan hareketle ölçek maddelerinin ayırt edici, güvenirliği yüksek ve benzer davranışı ölçmeye yönelik olduğu söylenebilir.

Açımlayıcı faktör analizinde, değişkenler arasındaki ilişkilerden hareketle faktör bulmaya, kuram üretmeye yönelik bir işlem; doğrulayıcı faktör analizinde ise değişkenler arasındaki ilişkiye dair daha önce belirlenen bir hipotezin test edilmesi söz konusudur (Stevens, 1996; Tabachnick ve Fidell, 2001).

Açımlayıcı faktör analizi sonucu elde edilen modelin uygunluğu LISREL 8.7 paket programı kullanılarak doğrulayıcı faktör analizi (Confirmatory Factor Analysis) ile incelenmiştir. Alanyazın bu analiz sonucunda uygun modelin belirleyicisi olarak χ^2, RMSEA, CFI ve GFI ölçütlerini işaret etmektedir (Brown, 2006; Tabachnick ve Fidell, 2001). Buna göre elde edilen modelin uygunluğu; Ortalama Hataların Karekökü (Root Mean Square Error of Approximation; RMSEA), Karşılaştırmalı Uygunluk İndeksi (Comparative Fit Index; CFI) ve Uygunluk İndeksi (Goodness of Fit Index; GFI) ölçütleri ile sınanmıştır. Analiz sonuçları Tablo 17'de verilmiştir.

Tablo 17

Doğrulayıcı Faktör Analizinin Değerlendirilmesi

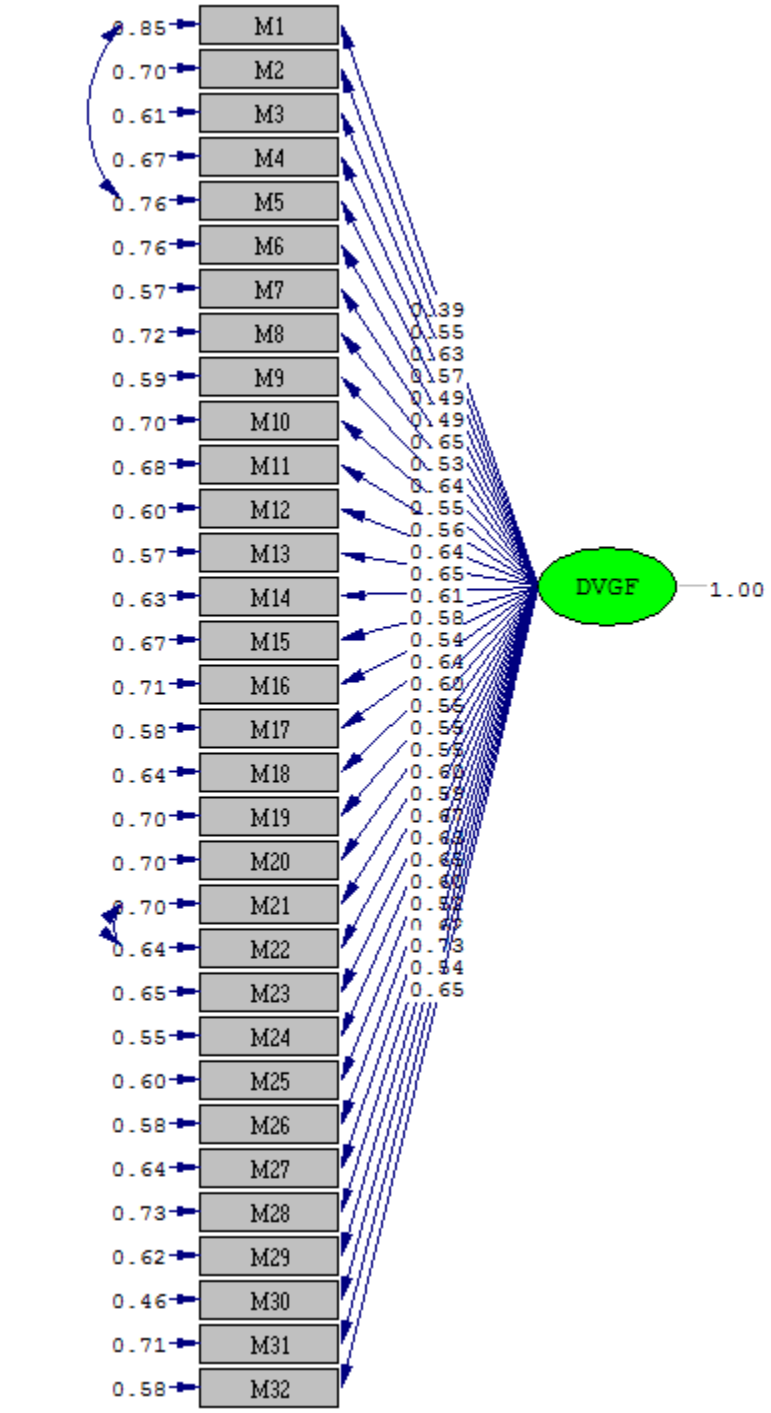
Uyum İndeksi	Değer	Ölçüt	Değerlendirme	Dayanak
χ^2	$0 \leq \chi^2 < 924$	$0 \leq \chi^2 \leq 2sd$	-	Yılmaz ve Çelik (2009)
p	.000	$.05 \leq p \leq 1.00$	-	-
χ^2/sd	3.90	$0 \leq \chi^2/sd \leq 5$	Orta düzeyde uyum	(Sümer, 2000)
RMSEA	.09	$0 \leq RMSEA \leq .10$	Zayıf uyum	(Kelloway, 1998; Tabachnick, Fidell, 2001)
SRMR	.07	$0 \leq SRMR \leq .08$	İyi uyum	(Brown, 2006; Hu ve Bentler,1999)
NFI	.93	$.90 \leq NFI \leq 1.00$	İyi uyum	(Kelloway, 1998; Schumacher, Lomax, 1996; Sümer, 2000; Tabachnick, Fidell, 2001; Thompson, 2004)
NNFI	.95	$.90 \leq NNFI \leq 1.00$	İyi uyum	(Kelloway, 1998; Schumacher, Lomax, 1996; Sümer, 2000; Tabachnick, Fidell, 2001; Thompson, 2004)
CFI	.95	$.90 \leq CFI \leq 1.00$	İyi uyum	(Hu ve Bentler,1999; Sümer, 2000; Tabachnick, Fidell, 2001)
GFI	.74	$.90 \leq GFI \leq 1.00$	İyi uyuma yakın	(Schumacher, Lomax, 1996; Hooper, Coughlan ve Mullen, 2008; Kelloway, 1998; Sümer, 2000)
AGFI	.71	$.90 \leq AGFI \leq 1.00$	İyi uyuma yakın	(Schumacher, Lomax, 1996; Hooper, Coughlan ve Mullen, 2008; Kelloway, 1998; Sümer, 2000)

$\chi^{2=1801.58;\ sd=462}$

Tablo 17'deki uyum indekslerine göre beklenen ve gözlenen kovaryans matrisleri arasındaki fark anlamlıdır (χ^2(462):1801.58; p<.01). p değerinin kritik değer bağlamında >.05 olması beklenmektedir, ancak birçok doğrulayıcı faktör analizi çalışmasında bu değer örneklem büyüklüğüne bağlı olarak anlamlı çıkmaktadır (Çokluk, Şekercioğlu ve Büyüköztürk, 2012). χ^2/sd değeri 3.90 olarak hesaplanmıştır. Bu değer Sümer'e göre (2000) orta düzeyde uyum anlamına gelmektedir.

Modelin uygunluğuna ilişkin RMSEA değerinin sıfıra yaklaşması uygun modelin habercisi olarak kabul edilmektedir (Steiger, 2007). Araştırmada bu değer .09 olarak bulunmuştur ve zayıf uyuma işaret etmektedir (Kelloway, 1999; Tabachnick, Fidell, 2001). SRMR değerinin .07 olması ise iyi uyum anlamına gelmektedir (Brown, 2006; Hu ve Bentler,1999). NFI değeri .93, benzer şekilde NNFI değeri de .95'tir ve bu değerlerin iyi uyuma işaret ettiği görülmektedir (Kelloway, 1989; Schumacher, Lomax, 1996; Sümer, 2000; Tabachnick, Fidell, 2001; Thompson, 2004). Bir diğer ölçüt olan CFI değeri .95 olarak hesaplanmıştır ve farklı kaynaklara göre iyi uyumun göstergesidir (Hu ve Bentler, 1999; Sümer, 2000; Tabachnick, Fidell, 2001). GFI değeri .74 ve AGFI değeri de .71 hesaplanmıştır. AGFI ve GFI değerlerinin .90'a yaklaşması nedeniyle bu iki değerin iyi uyuma yakın olduğu söylenebilir.

Tüm göstergeler, modelin iyi uyuma sahip olduğunu ve ölçeğin tek boyutta iyi düzeyde açıklanabildiğini ortaya koymuştur. Modelin uyumunu arttırmak için hata kovaryansları eklenerek M1-M5 ve M21-M22 maddeleri ilişkilendirilmiştir. Modele ilişkin diyagram (path diagram) Şekil 4'te verilmiştir.



Şekil 4: Yapısal Eşitlik Modeline İlişkin Diyagram

Şekil 4'te her bir maddenin hata varyansı ve korelasyon katsayıları verilmiştir. Maddelere ilişkin korelasyon katsayılarının .39 ile .73 arasında değiştiği görülmektedir. Bununla birlikte ölçekte yer alan tüm maddelerin t değerleri $p<.01$ düzeyinde anlamlıdır ($t>2.56$).

Öğretmenlerin Dijital Veri Güvenliği Farkındalıklarının Belirlenmesine Yönelik Bulgular ve Yorumlar

Veri toplama aracının ilk bölümünü oluşturan kişisel bilgi formundan elde edilen katılımcı özelliklerine ait bulgular Tablo 18'de verilmiştir.

Tablo 18

Bağımsız Değişkenlere İlişkin Frekans ve Yüzde Dağılımları

		f	%
Cinsiyet	Kadın	431	51.5
	Erkek	394	47.1
	Kayıp Veri	12	1.4
Branş	Sınıf Öğretmeni	152	18.2
	Branş Öğretmeni	669	79.9
	Kayıp Veri	16	1.9
Görev yapılan öğrenim kademesi	İlkokul	207	24.7
	Ortaokul	213	25.4
	Lise	417	49.8
Mesleki deneyim	0-4 yıl	21	2.5
	5-9 yıl	96	11.5
	10-14 yıl	141	16.8
	15-19 yıl	212	25.3
	20 yıl ve üzeri	339	40.5
	Kayıp Veri	28	3.3
Öğrenim durumu	Ön Lisans	64	7.6
	Lisans	690	82.4
	Yüksek Lisans	56	6.7
	Doktora	4	.5
	Kayıp Veri	23	2.7
Günlük bilgisayar kullanım süresi	Hiç Kullanmıyorum	31	3.7
	1-2 saat	528	63.1
	3-4 saat	166	19.8
	4 saatten fazla	89	10.6
	Kayıp Veri	23	2.7

Tablo 18, Devamı

		f	%
Günlük İnternet kullanım süresi	Hiç Kullanmıyorum	30	3.6
	1-2 saat	561	67.0
	3-4 saat	131	15.7
	4 saatten fazla	78	9.3
	Kayıp Veri	37	4.4
Kendime ait bilgisayarım var	Evet	719	85.9
	Hayır	96	11.5
	Kayıp Veri	22	2.6
Tablet bilgisayarım var	Evet	399	47.7
	Hayır	400	47.8
	Kayıp Veri	38	4.5
Akıllı telefonum var	Evet	536	64.0
	Hayır	268	32.0
	Kayıp Veri	33	3.9
	Toplam	837	100.0

Tablo 18'e göre örneklemi oluşturan öğretmenlerin 431'i (% 51.5) kadın, 394'ü (% 47.1) erkektir. Öğretmenlerin cinsiyete göre dağılımı incelendiğinde, frekanslar birbirine yakın olmakla birlikte kadınların çoğunlukta olduğu görülmektedir.

Araştırmaya katılan öğretmenlerin 152'si (% 18.2) sınıf öğretmeni, 669'u (% 79.9) branş öğretmenidir. Katılımcıların büyük çoğunluğu branş öğretmenidir. Görev yaptıkları öğrenim kademesi incelendiğinde, 207'si (% 24.7) ilkokulda, 213'ü (% 25.4) ortaokulda ve 417'si de (% 49.8) lisede görev yapmaktadır. Bu üç öğrenim kademesinden yalnızca ilkokullarda sınıf öğretmeni bulunduğundan branş öğretmenlerine göre sayıları daha azdır.

Katılımcıların 21'i (% 2.5) 0-4 yıl, 96'sı (% 11.5) 5-9 yıl, 141'i (% 16.8) 10-14 yıl, 212'si (% 25.3) 15-19 yıl ve 339'u (% 40.5) 20 yıl ve üzeri süredir öğretmenlik mesleğini yürütmektedir. Hizmet puanına göre yer değiştirme isteğinde bulunabildiklerinden Türkiye'nin en batısındaki illerden biri olan Balıkesir'deki öğretmenlerin hizmet puanına bağlı olarak mesleki deneyimleri de yıl olarak fazladır.

Öğretmenlerin 64'ü (% 7.6) ön lisans, 690'ı (% 82.4) lisans, 56'sı (% 6.7) yüksek lisans ve yalnızca 4'ü (% .5) doktora düzeyinde öğrenim görmüştür. Genellikle eğitim fakültelerinden mezun olup mesleğe başlayan öğretmenlerin büyük çoğunluğunun öğrenim durumu lisans düzeyinde iken çok azının lisansüstü öğrenime yöneldiği söylenebilir.

Günlük bilgisayar kullanım süreleri incelendiğinde, öğretmenlerin 31'i (% 3.7) bir günlük süre içinde hiç bilgisayar kullanmadığını belirtirken, 528'i (% 63.1) 1-2 saat, 166'sı (% 19.8) 3-4 saat ve 89'u (% 10.6) 4 saatten fazla bilgisayar kullanmaktadır. Günlük İnternet kullanım süreleri incelendiğinde, öğretmenlerin 30'u (% 3.6) bir günlük süre içinde hiç İnternet kullanmadığını belirtirken, 561'i (% 67) 1-2 saat, 131'i (% 15.7) 3-4 saat ve 78'i (% 9.3) 4 saatten fazla İnternet kullanmaktadır. Haftalık 15-30 saat arasında derse giren öğretmenlerin ders planlamaya, yazılı sınavları ve performans ödevlerini değerlendirmeye ayırdıkları süreler dikkate alındığında günlük bilgisayar ve İnternet kullanımına çoğunlukla 4 saatten az zaman ayırdıkları söylenebilir.

Araştırmaya katılan öğretmenlerin 719'u (% 85.9) kişisel bilgisayara, 399'u (% 47.8) tablet bilgisayara ve 536'sı da (% 64) akıllı telefona sahiptir. FATİH projesi kapsamındaki okullarda görev yapan öğretmenlere MEB tarafından ücretsiz tablet bilgisayar verilmesi bu oranları etkilemiştir. Bununla birlikte günümüzde mobil cihaz kullanımının hızla artmasının sonucu olarak öğretmenlerin de çoğunlukla akıllı telefona sahip olduğu görülmektedir. Veri toplama aracının ikinci bölümünü oluşturan DVGFÖ maddelerine ilişkin tanımlayıcı istatistikler Tablo 19'da verilmiştir.

Tablo 19

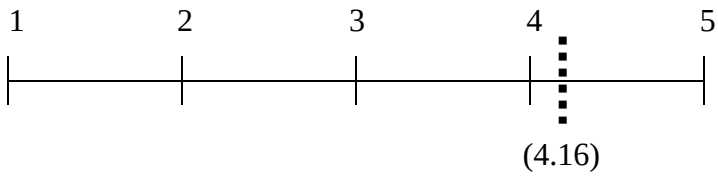
DVGFÖ Maddelerine İlişkin Tanımlayıcı İstatistikler

	$\bar{X}$	*SS*
2.Parola oluştururken harf, sayı ve özel karakter kullanmanın önemini bilirim.	4.44	.84
13.Parola hatırlatmak için kullanılan güvenlik sorularına başkalarının tahmin edemeyeceği cevaplar verilmesi gerektiğini bilirim.	4.41	.78
8.E-posta ile gelen kimlik bilgilerini doğrulama mesajlarına (parola, kredi kartı vb.) itibar edilmemesi gerektiğini bilirim.	4.41	.83
14.Parola oluştururken karakter sayısının fazla olmasının önemini bilirim.	4.38	.78
12.Antivirüs yazılımı kullanmanın önemini bilirim.	4.35	.82
28.Cep telefonuna gelen tek kullanımlık parola ile yapılan giriş işlemlerinin, güvenliği arttırdığını bilirim.	4.35	.86

Tablo 19, Devamı

	$\bar{X}$	*SS*
10.Güvenli olmadığını düşündüğüm e-postaları açmadan silmeye dikkat ederim.	4.34	.86
15.Parolaların herhangi bir ortamda saklanmasının güvenlik riski oluşturacağının farkındayım.	4.32	.81
18.Başkalarının tahmin edemeyeceği parolalar oluşturmaya dikkat ederim.	4.32	.84
30.İnternet sitelerinde kullanıcı oturumunu kapatırken "güvenli çıkış" bağlantısını kullanmanın önemini bilirim.	4.31	.92
3.Farklı işlemler için farklı parola kullanmanın önemini bilirim.	4.29	.86
25.Kendime ait olmayan cihazlarda, parola gerektiren işlemler yapmamaya dikkat ederim.	4.27	.81
24.İzinsiz kullanılmaması için cihazlara (akıllı telefon, tablet, bilgisayar vb.) parola konulabileceğinin farkındayım.	4.27	.86
9.Taşınabilir depolama birimlerini (Flash bellek, taşınabilir sabit disk) kullanmadan önce virüs taraması yapılması gerektiğini bilirim.	4.25	.87
17.Üzerinde çalışma yapılan dosyaların birden fazla ortamda yedeklenmesi gerektiğini bilirim.	4.21	.88
26.İşletim sisteminin (Windows, Android vb.) güvenlikle ilgili uyarılarını dikkate alırım.	4.19	.85
27.Elektrik kesintisine karşı dizüstü bilgisayarları bataryası ile kullanmanın önemini bilirim.	4.17	.90
11.Programların, üreticinin kendi sitesinden indirilmesinin önemini bilirim.	4.13	.90
4.İzinsiz kullanılmaması için dosyalara parola konulabileceğinin farkındayım.	4.12	.92
6.Flash bellekleri, veri saklamak yerine sadece veri taşımak için kullanmanın farkını bilirim.	4.12	.97
32.Lisanslı olmayan yazılımların güvenlik açıkları oluşturabileceğinin farkındayım.	4.06	.96
20.Taşınabilir depolama birimlerini (Flash bellek, taşınabilir sabit disk) "Donanımı Güvenle Kaldır" seçeneğini kullanarak çıkartmaya dikkat ederim.	4.05	1.03
22.Parolaların belirli aralıklarla değiştirilmesi gerektiğinin farkındayım.	4.01	.97
29.Sanal klavye kullanmanın önemini bilirim.	3.94	1.06
7.İşletim sisteminin (Windows, Android vb.) güncel olmasına dikkat ederim.	3.93	1.00
1.Zararlı yazılımlar (virüs, solucan, truva atı vb.) konusunda bilgi sahibiyim.	3.91	1.11
23.Almak istemediğim çöp e-postaları "spam/gereksiz/önemsiz" olarak işaretlemeye dikkat ederim.	3.90	1.04
19.İnternet adres çubuğunda yanlış yönlendirme olup olmadığına dikkat ederim.	3.87	1.03
21.Karmaşık yapıdaki parolaların kırılabileceğini bilirim.	3.80	1.09
16.Verilerin, çeşitli uygulamalar (Dropbox, Google Drive vb.) kullanılarak İnternet ortamında saklanabileceğini bilirim.	3.69	1.13
31.İnternet sitelerinde kullanılan güvenlik sertifikaları hakkında bilgi sahibiyim.	3.64	1.11
5.Güvenlik duvarı yazılımları konusunda bilgi sahibiyim.	3.36	1.23
Ölçeğin Geneli	4.16	2.15

Tablo 19'a göre ölçekten alınan ortalama puan 4.16'dır. Bu da öğretmenlerin dijital veri güvenliği konusundaki farkındalıklarını "Katılıyorum" düzeyine çok yakın ifade ettiklerini göstermektedir.



Şekil 5: Ölçekten Alınan Ortalama Puan

Ölçekte yer alan maddeler incelendiğinde, ortalama puanlar 3.36 ile 4.44 arasında değişmektedir. Maddelerin ortalama puanları birbirine yakın olmakla birlikte, öğretmenlerin dijital veri güvenliği farkındalığı ile ilgili ifadelere verdikleri yanıtlar değişkenlik göstermektedir.

Ölçekteki maddelerin ortalama puanları dikkate alındığında 2. madde en yüksek ortalamaya ($\overline{X}$=4.44, SS=.84) sahiptir. Buna göre öğretmenler parola oluştururken harf, sayı ve özel karakter kullanmanın önemi konusunda yüksek farkındalığa sahiptir. Yüksek ortalamaya sahip diğer iki madde ise; 8. madde ($\overline{X}$=4.41, SS=.83) ve 13. maddedir ($\overline{X}$=4.41, SS=.78). Buna göre öğretmenler, e-posta ile gelen kimlik bilgilerini doğrulama mesajlarına (parola, kredi kartı vb.) itibar edilmemesi gerektiğinin ve parola hatırlatmak için kullanılan güvenlik sorularına başkalarının tahmin edemeyeceği yanıtlar verilmesi gerektiğinin farkındadır denilebilir.

Ölçekteki en düşük ortalama puana ($\overline{X}$=3.36, SS=1.23) sahip 5. maddeye göre öğretmenlerin güvenlik duvarı yazılımları konusundaki farkındalıkları diğer maddelere göre en azdır. Düşük ortalamaya sahip diğer iki madde ise; 31. madde ($\overline{X}$=3.64, SS=1.11) ve 16. maddedir ($\overline{X}$=3.69, SS=1.13). Buna göre öğretmenlerin, İnternet sitelerinde kullanılan güvenlik sertifikaları ve verilerin çeşitli uygulamalar (Dropbox, Google Drive vb.) kullanılarak İnternet ortamında saklanabileceği konularındaki farkındalıkları daha düşüktür.

Öğretmenlerin dijital veri güvenliği farkındalıklarının cinsiyete göre anlamlı farklılık gösterip göstermediğine ilişkin yapılan t-testi sonuçları Tablo 20'de verilmiştir.

Tablo 20

Dijital Veri Güvenliği Farkındalığının Cinsiyete Göre Karşılaştırılması

Cinsiyet	*N*	$\bar{X}$	*SS*	*sd*	*t*	*p*
Kadın	431	4.10	2.15	823	-3.393	.001*
Erkek	394	4.23	2.13			

*p<.05

Tablo 20'de kadınların ve erkeklerin ölçekten aldıkları ortalama puanlar arasında cinsiyete göre istatistiksel olarak anlamlı bir fark olduğu görülmektedir [$t_{(823)}$=-3.393, p<.05, η^2=.014]. Erkeklerin dijital veri güvenliği farkındalıklarının kadınlara göre daha fazla olduğu söylenebilir.

Öğretmenlerin dijital veri güvenliği farkındalıklarının branşa göre anlamlı farklılık gösterip göstermediğine ilişkin yapılan t-testi sonuçları Tablo 21'de verilmiştir.

Tablo 21

Dijital Veri Güvenliği Farkındalığının Branşa Göre Karşılaştırılması

Branş	*N*	$\bar{X}$	*SS*	*sd*	*t*	*p*
Sınıf Öğretmeni	152	4.14	2.18	819	-.583	.560
Branş Öğretmeni	669	4.17	2.14			

Tablo 21'de öğretmenlerin ölçekten aldıkları ortalama puanlar arasında branşa göre istatistiksel olarak anlamlı bir fark olmadığı görülmektedir [$t_{(819)}$=-.583, p>.05]. Bu durum, MEB tarafından öğretmenlere sunulan, öğretim faaliyetlerinde teknoloji kullanımına yönelik hizmet içi eğitim seminerlerinin branş ayrımı yapılmaksızın tümüne zorunlu olarak uygulanması ile açıklanabilir.

Öğretmenlerin dijital veri güvenliği farkındalıklarının görev yaptıkları öğrenim kademesine göre anlamlı farklılık gösterip göstermediğine ilişkin yapılan ANOVA sonuçları Tablo 22'de verilmiştir.

Tablo 22

Dijital Veri Güvenliği Farkındalığının Görev Yapılan Öğrenim Kademesine Göre Karşılaştırılması

Varyansın Kaynağı	Kareler Toplamı	*sd*	Kareler Ortalaması	*F*	*p*	Anlamlı Fark
Gruplar arası	57.021	2	28.510	1.347	.261	-
Gruplar içi	17648.871	834	21.162			
Toplam	17705.892	836				

Tablo 22'de öğretmenlerin ölçekten aldıkları ortalama puanlar incelendiğinde [$F_{(2\text{-}834)}$=1.347, p>.05] görev yapılan öğrenim kademesine göre istatistiksel olarak anlamlı farklılık olmadığı görülmektedir. FATİH projesi liselerden başlanarak ortaokullara, daha sonra da ilkokullara uygulanacağından ilgili proje Balıkesir ilinde bugüne kadar yalnızca liselerde hayata geçirilmiş ve bu kapsamda lise öğretmenleri "Güvenli İnternet Kullanımı" kursuna katılmıştır. Buna rağmen araştırmaya katılan lise öğretmenlerinde dijital veri güvenliği farkındalığı konusunda bir fark oluşmadığı söylenebilir.

Öğretmenlerin dijital veri güvenliği farkındalıklarının mesleki deneyimlerine göre anlamlı farklılık gösterip göstermediğine ilişkin yapılan ANOVA sonuçları Tablo 23'te verilmiştir.

Tablo 23

Dijital Veri Güvenliği Farkındalığının Mesleki Deneyime Göre Karşılaştırılması

Varyansın Kaynağı	Kareler Toplamı	*sd*	Kareler Ortalaması	*F*	*p*	Anlamlı Fark
Gruplar arası	71.212	4	17.803	.839	.500	-
Gruplar içi	17057.611	804	21.216			
Toplam	17128.823	808				

Tablo 23'te öğretmenlerin ölçekten aldıkları ortalama puanlar incelendiğinde, [$F_{(4\text{-}804)}$=.839, p>.05] mesleki deneyime göre istatistiksel olarak anlamlı farklılık olmadığı görülmektedir. Teknolojinin son yıllardaki hızlı değişimi ile eğitim öğretim ortamlarında bilişim teknolojilerinin kullanımı hızla artarken bu teknolojileri genç

neslin daha etkili kullandığı düşünülse de dijital veri güvenliği farkındalığının öğretmenlik mesleğinde geçirilen yıla göre değişmediği söylenebilir.

Öğretmenlerin dijital veri güvenliği farkındalıklarının öğrenim durumuna göre anlamlı farklılık gösterip göstermediğine ilişkin yapılan ANOVA sonuçları Tablo 24'te verilmiştir.

Tablo 24

Dijital Veri Güvenliği Farkındalığının Öğrenim Durumuna Göre Karşılaştırılması

Varyansın Kaynağı	Kareler Toplamı	*sd*	Kareler Ortalaması	*F*	*p*	Anlamlı Fark
Gruplar arası	11.794	3	3.931	.183	.908	-
Gruplar içi	17409.992	810	21.494			
Toplam	17421.786	813				

Tablo 24'te öğretmenlerin ölçekten aldıkları ortalama puanlar incelendiğinde [$F_{(3\text{-}810)}$=.183, p>.05] öğrenim durumuna göre istatistiksel olarak anlamlı farklılık olmadığı görülmektedir. Daha önceleri ön lisans mezunu olarak mesleğe başlayan ve halen sürdüren öğretmenler olsa da, günümüzde en az lisans mezunu olan öğretmenlerin çok azı lisansüstü öğrenime yönelmektedir. Bununla birlikte öğrenim durumunun öğretmenlerin dijital veri güvenliği farkındalıkları arasında bir fark oluşturmadığı söylenebilir.

Öğretmenlerin dijital veri güvenliği farkındalıklarının günlük bilgisayar kullanım süresine göre anlamlı farklılık gösterip göstermediğine ilişkin yapılan ANOVA sonuçları Tablo 25'te verilmiştir.

Tablo 25

Dijital Veri Güvenliği Farkındalığının Günlük Bilgisayar Kullanım Süresine Göre Karşılaştırılması

Varyansın Kaynağı	Kareler Toplamı	*sd*	Kareler Ortalaması	*F*	*p*	Anlamlı Fark
Gruplar arası	1073.851	3	357.950	17.758	.000*	3,4>2>1
Gruplar içi	16327.723	810	20.158			
Toplam	17401.574	813				

*p<.05 (1.Hiç kullanmıyorum, 2.1-2 saat, 3.3-4 saat, 4.4 saatten fazla)

Tablo 25'te öğretmenlerin ölçekten aldıkları ortalama puanlar incelendiğinde, [$F_{(3\text{-}810)}$=17.758, p<.05, η^2=.062] günlük bilgisayar kullanım süresine göre istatistiksel olarak anlamlı farklılık olduğu görülmektedir. Gruplar arasındaki farklılığı ortaya koyabilmek için yapılan Scheffe testi sonucunda; hem günde 4 saatten fazla, hem de günde 3-4 saat bilgisayar kullananların, günde 1-2 saat bilgisayar kullananlardan, günde 1-2 saat bilgisayar kullananların da hiç kullanmayanlardan dijital veri güvenliği konusunda daha fazla farkında oldukları görülmektedir. Buna göre günlük bilgisayar kullanım süresi arttıkça dijital veri güvenliği farkındalığının da arttığı söylenebilir.

Öğretmenlerin dijital veri güvenliği farkındalıklarının günlük İnternet kullanım süresine göre anlamlı farklılık gösterip göstermediğine ilişkin yapılan ANOVA sonuçları Tablo 26'da verilmiştir.

Tablo 26

Dijital Veri Güvenliği Farkındalığının Günlük İnternet Kullanım Süresine Göre Karşılaştırılması

Varyansın Kaynağı	Kareler Toplamı	*sd*	Kareler Ortalaması	*F*	*p*	Anlamlı Fark
Gruplar arası	1168.129	3	389.376	19.453	.000*	3,4>1,2
Gruplar içi	15932.576	796	20.016			
Toplam	17100.705	799				

*p<.05 (1.Hiç kullanmıyorum, 2.1-2 saat, 3.3-4 saat, 4.4 saatten fazla)

Tablo 26'da öğretmenlerin ölçekten aldıkları ortalama puanlar incelendiğinde, [$F_{(3\text{-}796)}$=19.453, p<.05, η^2=.068] günlük İnternet kullanım süresine göre istatistiksel olarak anlamlı farklılık olduğu görülmektedir. Gruplar arasındaki farklılığı ortaya koyabilmek için, varyans eşteşliği şartı sağlanmadığından Dunnett C yapılmıştır. Test sonucunda; hem günde 4 saatten fazla, hem de günde 3-4 saat İnternet kullananların; hem günde 1-2 saat bilgisayar kullananlardan, hem de hiç kullanmayanlardan dijital veri güvenliği konusunda daha fazla farkında oldukları görülmektedir. Buna göre günlük İnternet kullanım süresi günde 3 saatin üzerine çıktığında dijital veri güvenliği farkındalığının da arttığı söylenebilir.

Öğretmenlerin dijital veri güvenliği farkındalıklarının kişisel bilgisayar sahibi olma durumlarına göre anlamlı farklılık gösterip göstermediğine ilişkin yapılan t-testi sonuçları Tablo 27'de verilmiştir.

Tablo 27

Dijital Veri Güvenliği Farkındalığının Kişisel Bilgisayar Sahibi Olma Durumuna Göre Karşılaştırılması

Kişisel bilgisayarım var	*N*	$\bar{X}$	*SS*	*sd*	*t*	*p*
Evet	719	4.19	2.13	813	4.562	.000*
Hayır	96	3.91	2.20			

*p<.05

Tablo 27'de öğretmenlerin ölçekten aldıkları ortalama puanlar arasında kişisel bilgisayar sahibi olma durumlarına göre istatistiksel olarak anlamlı bir fark olduğu görülmektedir [$t_{(813)}$=4.562, p<.05, η^2=.025]. Kişisel bilgisayarı olan öğretmenlerin dijital veri güvenliği farkındalıklarının kişisel bilgisayarı olmayanlara göre daha fazla olduğu söylenebilir. Bu durum kendine ait bir bilgisayar sayesinde öğretmenlerin daha fazla dijital veri üretmeleri, bilgisayarlarında kişiye özel veri saklamaları ve bunların güvenliğini sağlayabilmek adına farkındalıklarının yüksek olması ile açıklanabilir.

Öğretmenlerin dijital veri güvenliği farkındalıklarının tablet bilgisayar sahibi olma durumlarına göre anlamlı farklılık gösterip göstermediğine ilişkin yapılan t-testi sonuçları Tablo 28'de verilmiştir.

Tablo 28

Dijital Veri Güvenliği Farkındalığının Tablet Bilgisayar Sahibi Olma Durumuna Göre Karşılaştırılması

Tablet bilgisayarım var	*N*	$\bar{X}$	*SS*	*sd*	*t*	*p*
Evet	399	4.23	2.14	797	3.930	.000*
Hayır	400	4.08	2.15			

*p<.05

Tablo 28'de öğretmenlerin ölçekten aldıkları ortalama puanlar arasında tablet bilgisayar sahibi olma durumlarına göre istatistiksel olarak anlamlı bir fark olduğu görülmektedir [$t_{(797)}$=3.930, p<.05, η^2=.019]. Tablet bilgisayarı olan öğretmenlerin dijital veri güvenliği farkındalıklarının tablet bilgisayarı olmayanlara göre daha fazla olduğu söylenebilir.

Öğretmenlerin dijital veri güvenliği farkındalıklarının akıllı telefon sahibi olma durumlarına göre anlamlı farklılık gösterip göstermediğine ilişkin yapılan t-testi sonuçları Tablo 29'da verilmiştir.

Tablo 29

Dijital Veri Güvenliği Farkındalığının Akıllı Telefon Sahibi Olma Durumuna Göre Karşılaştırılması

Akıllı telefonum var	*N*	$\bar{X}$	*SS*	*sd*	*t*	*p*
Evet	535	4.19	2.14	801	2.561	.011*
Hayır	268	4.09	2.18			

*p<.05

Tablo 29'da öğretmenlerin ölçekten aldıkları ortalama puanlar arasında akıllı telefon sahibi olma durumlarına göre istatistiksel olarak anlamlı bir fark olduğu görülmektedir [$t_{(801)}$=2.561, p<.05, η^2=.008]. Akıllı telefonu olan öğretmenlerin dijital veri güvenliği farkındalıklarının akıllı telefonu olmayanlara göre daha fazla olduğu söylenebilir.

Çoğunlukla Android işletim sistemine sahip tablet bilgisayarların ve akıllı telefonların, Windows işletim sistemine sahip kişisel bilgisayarlardan farklı olması nedeniyle kullanıcıların bu yeniliği öğrenme ve alışma sürecinde veri güvenliği noktasında daha dikkatli oldukları düşünülmektedir. Özellikle İnternet bağlantısı olan mobil cihazlar veri güvenliği noktasında bir tehdit oluşturmaktadır ve bireyler mobil cihazlarındaki kayıtlı parolalar, fotoğraflar ve dokümanlar konusunda endişe duymaktadır. Bu nedenlerle tablet bilgisayarı veya akıllı telefonu olan öğretmenlerin dijital veri güvenliği farkındalıkları, bu teknolojilere sahip olmayan öğretmenlere göre daha yüksektir.

DÖRDÜNCÜ BÖLÜM
SONUÇ VE ÖNERİLER

Bu bölümde araştırma bulgularına dayalı olarak ulaşılan sonuçlar ve öneriler yer almaktadır. Öncelikle araştırmanın nitel boyutunda gerçekleştirilen odak grup görüşmelerinden elde edilen sonuçlar, ardından araştırmanın nicel boyutundaki ölçek geliştirme sürecinde ulaşılan sonuçlar, son olarak geliştirilen ölçek kullanılarak belirlenen öğretmenlerin dijital veri güvenliği farkındalıkları ile farkındalıklarının farklı değişkenlere göre sonuçları verilmiştir. Araştırma sonuçları doğrultusunda uygulamaya ve ileride yapılacak araştırmalara yönelik öneriler getirilmiştir.

Sonuç

Öğretmenlerin dijital veri güvenliği farkındalıklarını ortaya koymak üzere geliştirilen ölçeğin madde havuzu oluşturulması aşamasında öğretmenlerin ve kritik paydaşlar olan bilişim teknolojileri alanında görev yapan öğretim üyelerinin ve araştırma görevlilerinin görüşleri alınmıştır. Gerçekleştirilen odak grup görüşmeleri ile şu sonuçlara ulaşılmıştır:

- Katılımcılar, sahip oldukları bilişim cihazlarında veri güvenliğini sağlamak için virüslere ve casus yazılımlara karşı güncel güvenlik yazılımları kullanmakta, cihazlarına parola koymaktadır.
- Parola güvenliği konusunda harf, sayı ve özel karakterlerden oluşan güçlü parolalar kullanılması gerektiğinin farkında olmalarına rağmen katılımcılar, günlük yaşantılarında çok sayıda parola kullanılması gerektiğinden kısa, kolay ve hatırlayabilecekleri parolalar kullanmaktadır.
- Katılımcılar dijital verilerini saklamak için; kişisel bilgisayar, taşınabilir bellek, e-posta hesabı, bulut bilişim sistemleri (Gmail, Dropbox, Google Drive vb.), DVD veya CD kullanmaktadır.
- Katılımcılar kablosuz ağ güvenliğini saklamak için; modemlerine karmaşık yapıda parola koymakta, belirli aralıklarla bu parolaları değiştirmekte ve hiç kimseyle paylaşmamaktadır.
- e-devlet uygulamalarına girişte cep telefonuna gelen parolanın güvenliği arttıracağını düşünen katılımcılar; alt yapının güçlendirilmesi, uygulamaların

güvenli kullanımı konusunda bilgilendirilme yapılması ve güçlü parolalar kullanılması konusunda yaptırım getirilmesi gerektiğini belirtmiştir.

- Güvenlik ayarları yapılsa da sosyal ağlardaki paylaşımların güvenli olmadığını düşünen katılımcılar, buna rağmen fotoğraflarını ve kişisel bilgilerini paylaştıklarını, yer bildiriminde bulunduklarını ifade etmiştir.
- Katılımcılar, güvenli olmayan e-postaları açmadan silmekte ve güvenli bulmadıkları e-postaları istem dışı e-posta olarak işaretlemektedir.
- İnternet bankacılığı ve çevrimiçi alışverişte sanal klavye, sanal kart ve cep telefonuna gelen tek kullanımlık parola kullanmayı tercih eden katılımcılar, yalnızca kendilerine ait veya güvenilir cihazlardan giriş yapmakta ve güvenli olduğunu düşündükleri sitelerden alışveriş yapmaktadır.
- Katılımcılar, hukuki düzenlemelerin yeterli olmadığını, bununla birlikte Türkiye'de hukuki sürecin çok hızlı işlediğine ve geliştiğine inandıklarını belirtmiştir.

Odak grup görüşmeleri sonunda ölçek geliştirme sürecinde madde havuzuna katkı sağlayan 74 maddeye ulaşılmış ve bu maddeler aşağıda verilen 10 tema altında toplanmıştır.

- Bilişim cihazlarında veri güvenliği
- Parola güvenliği
- Verilerin saklanması, yedeklenmesi ve taşınması
- Bilgisayar ağlarında ve modemlerde veri güvenliği
- e-devlet uygulamalarında veri güvenliği
- Sosyal paylaşım ağlarında veri güvenliği
- e-posta kullanımında veri güvenliği
- İnternet bankacılığı ve çevrimiçi alışverişte veri güvenliği
- Veri güvenliğinde hukuki boyut
- Lisanslı yazılımlar ve telif hakları.

Madde havuzunun uzman görüşüne sunulmasından sonra elde edilen taslak ölçek formunun ön deneme uygulaması gerçekleştirilmiş ve yapı geçerliği için açımlayıcı faktör analizi yapılmıştır. Açımlayıcı faktör analizine ilişkin modelin

uygunluğunu test etmek için doğrulayıcı faktör analizi gerçekleştirilmiştir. Tüm göstergeler, modifikasyon indeksleri yardımıyla ideal değerlere ulaşan tek faktörlü yapıdaki dijital veri güvenliği farkındalık ölçeğinin geçerli ve güvenilir olduğunu, ileride yapılacak çalışmalarda kullanılabileceğini göstermiştir.

Geliştirilen ölçek kullanılarak, Balıkesir ilindeki öğretmenlerin dijital veri güvenliği farkındalıklarını belirlemek için öğretmenlerden toplanan veriler analiz edilmiştir. Araştırmada, bazı demografik değişkenlere ilişkin tanımlayıcı istatistiklerin yanında bu değişkenler ile dijital veri güvenliği farkındalığı arasındaki ilişkiler de incelenmiş ve şu sonuçlara ulaşılmıştır:

Öğretmenlerin dijital veri güvenliği farkındalıkları 4.16 ortalama ile oldukça yüksektir. En yüksek ortalama puan ile öne çıkan maddeler 2., 8. ve 13. maddelerdir. Buna göre öğretmenler; parola oluştururken harf, sayı ve özel karakter kullanmanın önemi, e-posta ile gelen kimlik bilgilerini doğrulama mesajlarına (parola, kredi kartı vb.) itibar edilmemesi ve parola hatırlatmak için kullanılan güvenlik sorularına başkalarının tahmin edemeyeceği yanıtlar verilmesi konularında daha yüksek farkındalığa sahiptir. Kruger ve diğerleri (2010) ise araştırmalarına katılan üniversite öğrencilerinin % 48'inin "güçlü parola" kavramının ne anlama geldiğini bilmediğini belirlemiştir.

Ölçekteki en düşük ortalamaya sahip maddeler ise 5, 31 ve 16. maddelerdir. Buna göre öğretmenlerin; güvenlik duvarı yazılımları, İnternet sitelerinde kullanılan güvenlik sertifikaları ve verilerin çeşitli uygulamalar (Dropbox, Google Drive vb.) kullanılarak İnternet ortamında saklanabileceği konularındaki farkındalıkları daha düşüktür. Tekerek ve Tekerek (2013) çalışmasında öğrencilerle çalışarak benzer sonuca ulaşmıştır. Buna göre öğrencilerin; kötücül yazılım denetlemesi, belge koruma, kişisel bilgisayar güvenliği, güvenlik duvarı ve filtreleme yazılımları kullanımı konularında farkındalık düzeylerinin çok düşük olduğu belirlenmiştir.

Ortalama puanı 3.36 ile en düşük olan ölçek maddesine göre öğretmenlerin farkındalıklarının en düşük olduğu konu güvenlik duvarı yazılımlarıdır. Şahinaslan ve diğerleri (2013) güvenlik duvarının önemine dikkat çekerek; İnternet üzerinden gelebilecek yetkisiz kaynak erişimlerini engellediğini, son kullanıcı ve sistemleri korumada bir süzgeç görevi gördüğünü, ağ trafiği üzerinde güvenlik riskine karşı ilk savunma hattı olduğunu belirtmiştir.

Cinsiyete göre öğretmenlerin dijital veri güvenliği farkındalığı incelenmiş olup, erkeklerin kadınlara göre farkındalıkları daha yüksek bulunmuştur. Çukurbaşı ve İşman da (2014) çalışmalarında 472 öğretmen adayının dijital yerli özelliklerini incelemiş ve istatistiksel olarak bulunan anlamlı farkın erkeklerin lehine olduğunu ortaya koymuştur. Alanyazında farklı sonuçlara ulaşan araştırmalar da bulunmaktadır. Mart (2012) farklı meslek gruplarından oluşan 501 katılımcı ile gerçekleştirdiği çalışmasında, bilgi güvenliği farkındalıkları arasında cinsiyete göre anlamlı bir fark bulmuş ancak kadınların erkeklere kıyasla karşılaşabilecekleri tehlikelerden daha fazla haberdar oldukları sonucuna ulaşmıştır. Buna göre öğretmenlik mesleğinde bilgi güvenliği farkındalığı söz konusu olduğunda, erkeklerin farkındalığı daha fazla iken sağlık personeli, mühendis, avukat gibi farklı meslek gruplarında kadınların farkındalıklarının daha fazla olduğu görülmektedir. Cinsiyete göre farklılığın araştırıldığı bir başka çalışmada Tekerek ve Tekerek (2013) ilköğretim ve lise öğrencilerinin bilgi güvenliği farkındalıklarını incelemiş ve kız öğrencilerin, erkek öğrencilere göre anlamlı şekilde daha olumlu görüşe sahip olduklarını ortaya koymuştur. Mühendislik fakültesi öğrencilerinden oluşan 218 katılımcı ile çalışan Arıtürk (2015) bilgi güvenliği ve bilgi farkındalığı durumlarını incelemiştir. Buna göre kadınların % 7'sinin hem bilgi güvenliği hem de bilgi farkındalığı yüksektir ve % 93'ünün de bilgi güvenliği ve bilgi farkındalığı tutumundan yalnızca biri yüksektir. Erkeklerin ise % 3'ünün bilgi güvenliği ve farkındalığı tutumu düşük, % 12'sinin her ikisi için yüksek ve % 85'inin de iki kavramdan yalnızca birinin tutumu yüksektir. Kadınların erkeklere göre bilgi güvenliği ve bilgi farkındalığı konusundaki tutumlarının daha yüksek olduğu söylenebilir. Oktay ve Çakır (2012) gönüllü 222 öğretmen ile gerçekleştirdikleri çalışmada, kadın öğretmenlerin teknolojiye yönelik tutumlarının erkek öğretmenlerden yüksek olduğu sonucuna ulaşmıştır. Çelik ve Bindak ise (2005) Siirt ilinde görev yapan 261 öğretmen ile gerçekleştirdiği araştırmada kadın ve erkek öğretmenlerin bilgisayara yönelik tutumları arasında fark olmadığını bulmuştur.

Araştırma sonunda ulaşılan bir başka sonuç da, sınıf öğretmenleri ile branş öğretmenleri arasında dijital veri güvenliği farkındalığı konusunda istatistiksel olarak anlamlı bir fark bulunmadığıdır. Benzer araştırmalarda Oktay ve Çakır (2012) öğretmenlerin teknolojiye yönelik tutumlarının, Çelik ve Bindak ise (2005) öğretmenlerin bilgisayara yönelik tutumlarının branşa göre değişmediğini belirlemiştir.

Öğretmenlerin dijital veri güvenliği farkındalıkları, görev yapılan öğrenim kademesine göre de değişmemektedir. Bir başka deyişle ilkokul, ortaokul ve lise öğretmenlerinin dijital veri güvenliği farkındalıkları arasında istatistiksel olarak anlamlı fark yoktur. İlköğretim ve lise öğrencileri örnekleminde çalışan Tekerek ve Tekerek (2013) ise öğrenim kademesine göre bilgi güvenliği farkındalığını incelediğinde, lisede öğrenim gören öğrencilerin ilköğretim öğrencilerine göre anlamlı şekilde daha yüksek farkındalığa sahip olduğunu belirlemiştir.

Araştırma sonuçlarına göre öğretmenlerin dijital veri güvenliği farkındalıklarının farklılık göstermediği diğer bağımsız değişken ise mesleki deneyimdir. Bir başka deyişle öğretmenlerin meslekte geçirdiği yılların az ya da çok olması farkındalıklarında anlamlı fark oluşturmamaktadır. Alanyazında farklı sonuçlara ulaşan çalışmalar da bulunmaktadır. Mart (2012) yaş değişkenini incelemiş ve 25-34 yaş arasındaki öğretmenlerin bilgi güvenliği konusunda yetersiz kaldıklarını ve bunun için farkındalık eğitimlerine gereksinim duyduklarını belirtmiştir. Oktay ve Çakır da (2012) ilköğretim öğretmenlerinden 0-9 yıl arasında mesleki deneyime sahip olanların teknolojiye karşı tutumlarının diğerlerinden daha yüksek olduğu sonucuna ulaşmıştır.

Öğrenim durumu dikkate alındığında da durum aynıdır. Öğretmenlerin dijital veri güvenliği farkındalıkları öğrenim durumlarına göre değişmemektedir. Bu sonucu destekleyen Mart'ın (2012) çalışmasında da katılımcıların eğitim durumlarının bilgi güvenliği farkındalıkları üzerinde anlamlı bir etkisi olmadığı bulunmuştur. Oktay ve Çakır (2012) ise bu sonuçlardan farklı olarak ön lisans mezunu öğretmenlerin teknolojiye karşı tutumlarının, hem lisans hem de yüksek lisans mezunu öğretmenlerden daha düşük olduğunu bulmuştur.

Araştırmada günlük bilgisayar kullanım süreleri incelendiğinde; günde 3 saatten fazla bilgisayar kullanan öğretmenlerin 1-2 saat bilgisayar kullananlardan, günde 1-2 saat bilgisayar kullananların da hiç kullanmayanlardan dijital veri güvenliği konusunda daha fazla farkında oldukları belirlenmiştir. Bir başka deyişle günlük bilgisayar kullanım süresi arttıkça dijital veri güvenliği farkındalığı da artmaktadır. Benzer çalışmada Çelik ve Bindak (2005) bilgisayarı daha sık kullanan öğretmenlerin, bilgisayara yönelik tutumlarının hiç kullanmayan veya nadiren kullananlara göre daha olumlu olduğunu bulmuştur. Alanyazında farklı sonuçlara ulaşan araştırmalar da yer almaktadır. Buna göre Mart (2012) katılımcıların bilgi güvenliği farkındalıklarının

bilgisayar kullanım sürelerine bağlı olarak anlamlı bir şekilde değişmediği sonucuna ulaşmıştır. Oktay ve Çakır da (2012) ilköğretim öğretmenlerinin teknolojiye karşı tutumlarının bilgisayar başında geçirdikleri süreye göre değişmediğini belirtmiştir.

Günlük İnternet kullanım süreleri incelendiğinde ise, günde 3 saatten fazla İnternet kullanan öğretmenlerin hem günde 1-2 saat İnternet kullananlardan, hem de hiç kullanmayanlardan dijital veri güvenliği konusunda daha fazla farkında oldukları sonucuna ulaşılmıştır. Mart'ın (2012) çalışmasında ise bu araştırmanın sonucundan farklı olarak katılımcıların bilgi güvenliği farkındalıklarının İnternet kullanım sürelerine bağlı olarak anlamlı bir şekilde değişmediği ortaya konmuştur.

Araştırmada son olarak katılımcıların sahip oldukları bilişim cihazlarına göre dijital veri güvenliği farkındalıkları incelenmiştir. Buna göre; kişisel bilgisayarı, tablet bilgisayarı veya akıllı telefonu olan öğretmenlerin bu cihazlara sahip olmayanlara göre farkındalıklarının daha fazla olduğu görülmüştür. Alanyazındaki çalışmalar bu sonucu desteklemektedir. Çelik ve Bindak'ın (2005) araştırmasında bilgisayarı olan öğretmenlerin bilgisayara yönelik olumlu tutumları, olmayanlara göre daha yüksek bulunmuştur. Cüre ve Özdener de (2008) 163 öğretmen ile gerçekleştirdikleri araştırmada, öğretmenlerin bilgi ve iletişim teknolojileri (BİT) uygulama başarı puanları ile BİT'e yönelik tutum puanları arasında yüksek düzeyde, pozitif ve anlamlı bir ilişki olduğu sonucuna ulaşmıştır. Uzun ve Sadioğlu (2013) ise derslerde tablet bilgisayar kullanılmasını destekleyen öğretmenlerin, desteklemeyen veya bu konuda fikri olmayanlara göre bilgisayara yönelik tutumlarının ve kullanım sıklıklarının daha yüksek olduğunu tespit etmiştir. Özkale ve Koç (2014) çalışmalarında bilgiye kolay ve hızlı ulaşma, öğretimi kolaylaştırma, zaman ve mekan sınırlılıklarını giderme, kitap taşıma zahmetini ortadan kaldırma, öğrenci başarısını artırma ve derslere görsellik katarak ilgi çekici hale getirme gibi avantajları nedeniyle eğitimde tablet kullanılmasına yönelik öğretmen, öğrenci ve velilerin genellikle pozitif tutum sergilediklerini belirtmiştir.

Öğretmenlerin dijital veri güvenliği farkındalıklarını etkileyen değişkenler genel olarak incelendiğinde; branş, görev yapılan öğrenim kademesi, mesleki deneyim ve öğrenim durumu değişkenlerinin anlamlı bir fark oluşturmadığı bulunmuştur. Buna karşın cinsiyet, günlük bilgisayar kullanım süresi, günlük İnternet kullanım süresi ile kişisel bilgisayar, tablet bilgisayar veya akıllı telefon gibi bilişim cihazlarına sahip olmanın dijital veri güvenliği farkındalığını olumlu etkilediği sonucuna ulaşılmıştır.

Araştırma sonuçları göstermektedir ki, öğretmenlerin dijital veri güvenliği farkındalıklarını etkileyen değişkenler; meslekleri ile ilgili özellikleri değil, bilişim cihazlarına sahip olma durumları ve bu teknolojileri kullanma süreleridir.

Öneriler

Araştırmadan elde edilen bulgular doğrultusunda, uygulamaya ve ileride yapılacak araştırmalara yönelik sunulan öneriler aşağıda verilmiştir.

Uygulamaya Yönelik Öneriler

Dijital veri güvenliğine yönelik tehditlerin ortadan kaldırılmasında en kritik etken insandır. Bu konuda yaşanan sorunların tamamen ortadan kaldırılabilmesi ya da en aza indirilebilmesi için özellikle okullarda ve toplum genelinde dijital veri güvenliği farkındalık eğitimleri verilmeli, bilinçlendirme çalışmaları yapılmalı ve farkındalığı arttıracak projeler yapılandırılmalıdır. Bu konuda, devlete ve özel sektöre, sivil toplum kuruluşlarına, yazılı ve görsel basına, üniversitelere ve okullara büyük sorumluluklar düşmektedir.

Bireylerde dijital veri güvenliği farkındalığı yaratabilmek için küçük yaşlardan itibaren eğitim verilmeli, ortaokul ve liselerde zorunlu bir ders olarak yer almalıdır. Bilişim Teknolojileri dersi öğretim programına ve ders kitaplarına konu ile ilgili içerik eklenmelidir. Öğretmenlerde ve eğitim yöneticilerinde hizmet içi eğitim seminerleri ile farkındalık bilinci oluşturulmalıdır. Bu seminerlerde özellikle veri güvenliği ile ilgili bilişim teknolojileri alanına özgü kavramlara ve teknik konulara ağırlık verilmelidir. Bu sayede toplumun geleceğinin şekillenmesinde önemli bir role sahip olan öğretmenler; hem öğrencilerine yol gösterebilecek, hem de kendilerine ait dijital verilerin güvenliğini sağlayabilecektir.

Toplumun geneli için gerçekleştirilebilecek başlıca bilinçlendirme faaliyetleri; İnternet siteleri oluşturulması, dijital veri güvenliğine ilişkin kampanyalar düzenlenmesi, bilgisayar ve İnternet kullanıcılarına güvenlikle ilgili gelişmeler, kötücül yazılımlar ve korunma yolları, kişisel verilerin korunması ile ilgili kanun ve yönetmelikler hakkında bilgilendirme yapılması olarak sayılabilir.

Sonuç olarak dijital veri güvenliği, bilişim teknolojilerini kullanan her bireyin bilmesi ve dikkat etmesi zorunlu bir konudur. Kötü niyetli kişiler tarafından verilerin kolaylıkla ele geçirilip kullanılabileceği dikkate alınırsa, ülkemizdeki kişi, kurum ve kuruluşların bu konuda gereken hassasiyeti göstermeleri, gerekli önlemleri almaları, yeni yaklaşımları yakından takip ediyor olmaları gerekmektedir. Yapılacak yasal düzenlemelerin de pek çok dijital veri güvenliği sorununun önüne geçeceği düşünülmektedir.

Yapılacak Araştırmalara Yönelik Öneriler

Bu araştırmanın sonucunda alanyazın taraması ile birlikte öğretmenlerin ve kritik paydaşların da görüşleri alınarak geçerli ve güvenilir dijital veri güvenliği farkındalık ölçeği geliştirilmiştir. Süreç içerisinde bireylerin bilişim teknolojilerini kullanım alışkanlıklarının, tutum ve davranışlarının değişebileceği düşünüldüğünde geliştirilen tüm ölçekler gibi bu ölçeğin de uzun vadede geçerli ve güvenilir bir yapı sergileyemeyeceği göz önünde bulundurulmalıdır.

Bu araştırmanın örneklemi öğretmenlerden oluşturulmuş ve ortaya konulan Dijital Veri Güvenliği Farkındalık Ölçeği bu meslek grubuna yönelik geliştirilmiştir. Diğer meslek gruplarına yönelik örneklemler oluşturulabileceği gibi öğrenciler için de ilgili ölçeğin yeniden yapı geçerliği ve güvenirlik çalışmalarının yapılması önerilmektedir.

Bu araştırma öğretmenlerin dijital veri güvenliği farkındalıkları; cinsiyet, branş, görev yapılan öğrenim kademesi, mesleki deneyim, öğrenim durumu, günlük bilgisayar kullanım süresi, günlük İnternet kullanım süresi, bilgisayar, tablet bilgisayar veya akıllı telefon sahibi olma değişkenlerine göre incelenmiştir. İleriki araştırmalarda dijital veri güvenliği farkındalığına etkisi olabilecek farklı değişkenler kullanılabilir. Gelecekte yapılacak araştırmalarda farklı örneklemlerden elde edilecek sonuçlar bu araştırmanın sonuçları ile karşılaştırılabilir.

EKLER

EK A - ODAK GRUP GÖRÜŞME FORMU

Öğretmenlerin Dijital Veri Güvenliği Farkındalığının Belirlenmesi

Görüşme Başlama Saati :
Görüşme Bitiş Saati :
Görüşme Tarihi :
Görüşme Yapılan Yer :

Giriş

Merhaba, yazılı izin mektubumda belirttiğim üzere, yürütmekte olduğum doktora tez çalışması kapsamında sizlerle öğretmenlerin dijital veri güvenliği farkındalığının belirlenmesi hakkında konuşmak istiyorum. Belirtmek istediğiniz bir düşünce ya da sormak istediğiniz bir şey var mı?

Görüşme sorularına geçmeden önce adınız, soyadınız, branşınız, göreviniz ve mesleki deneyiminizi bizimle paylaşarak kendinizi tanıtır mısınız?

Görüşmemizin yaklaşık 60 dakika süreceğini tahmin ediyorum. İzin verirseniz başlayabilir miyim?

Görüşme Soruları

1. Sahip olduğunuz kişisel bilgisayar, tablet bilgisayar, akıllı telefon gibi cihazlarda verilerinizin güvenliğini sağlamak için nelere dikkat ediyorsunuz?
2. Verilerinizin güvenliği noktasında şifreler hakkında neler söyleyebilirsiniz?
3. Verilerinizin saklanması ve taşınması için ne tür güvenlik tedbirleri alıyorsunuz?
4. Evde ve okulda bilgisayar ağlarının ve modemlerin güvenliğinin sağlanması için neler yapılmalıdır?
5. e-Okul, MEBBİS, EBA, Görevli İşlemleri Sistemi (GİS) gibi e-devlet uygulamalarının kullanımında veri güvenliği konusunu nasıl değerlendiriyorsunuz?
6. Kişisel bilgilerinizi başkalarıyla paylaşma noktasında nelere dikkat ediyorsunuz?
   - Sahip olduğunuz cihazlarda dosyaları paylaşıma açma,
   - Sosyal ağlarda paylaşımda bulunma.
7. Elektronik posta (e-posta) kullanımında karşılaştığınız güvenlik sorunları nelerdir?
8. İnternet bankacılığı kullanımını ve çevrimiçi alışverişi veri güvenliği bakımından nasıl değerlendiriyorsunuz?
9. Veri güvenliğinin hukuki boyutu hakkındaki düşünceleriniz nelerdir?

Teşekkür ederim.

EK B - ODAK GRUP GÖRÜŞME İÇİN İL MİLLİ EĞİTİM MÜDÜRLÜĞÜ İZNİ

T.C.
BALIKESİR VALİLİĞİ
İl Milli Eğitim Müdürlüğü

Sayı: 99191664/605.01/116912 09/01/2014
Konu: Araştırma İzni

VALİLİK MAKAMINA
BALIKESİR

İlgi : a) Milli Eğitim Bakanlığı Yenilik ve Eğitim Teknolojileri Genel Müdürlüğünün 07.03.2012 tarih ve 2012/13 sayılı genelgesi
b) Eray YILMAZ' a ait 08.01.2014 tarih ve 88119 sayılı dilekçe

Başvuru Sahibinin Adı Soyadı	Eray YILMAZ		
Danışmanı	Yard. Doç. Dr. Yusuf Levent ŞAHİN , Doç. Dr. Yavuz AKBULUT		
Kurumu/Üniversite/Görev Yeri	Anadolu Üniversitesi		
Alan/Bölüm	Eğitim Bilimleri Enstitüsü		
Tez,Araştırma veya Anketin Konusu	Öğretmenlerin Dijital Veri Güvenliği Farkındalığının Belirlenmesi		
Başvuru Tarihi	08.01.2014	**Başvuru Sayısı**	88119
Çalışma Başlama Tarihi	10.02.2014		
Çalışma Bitiş Tarihi	30.05.2014		
Veri Toplama Araçları	Odak Grup Görüşme Formu		
Araştırma Türü	Doktora Tezi		

ÇALIŞMA YAPLACAK EĞİTİM KURUMLARININ LİSTESİ			
S.No	**Okulun Adı**	**S.No**	**Okulun Adı**
1	Balıkesir İlindeki Tüm Resmi ve Özel Okullar		

Bakanlığımıza bağlı okul ve kurumlarda yapılacak Araştırma, Yarışma ve Sosyal Etkinlik izinleri ilgi (a) genelge gereğince yukarıdaki bilgileri belirtilen çalışmanın, eğitim kurumlarında, okul/kurum müdürlüklerinin denetiminde yapılması Müdürlüğümüzce uygun görülmektedir.

Makamlarınızca da uygun görüldüğü taktirde olurlarınıza arz ederim.

Yakup YILDIZ
Müdür a.
Müdür Yardımcısı

OLUR
09/01/2014
Sabri CANER
Vali a.
İl Milli Eğitim Müdürü

Eki : Dilekçe ve Ekleri (5 Sayfa)

Bu belge, 5070 sayılı Elektronik İmza Kanununun 5 inci maddesi gereğince güvenli elektronik imza ile imzalanmıştır

EK C - GÖRÜŞME ONAY FORMU

Sayın ……,

Öncelikle yürütmekte olduğum doktora tezi kapsamında yapacağım araştırmaya verdiğiniz katkılardan dolayı size teşekkür etmek istiyorum. Bu form, araştırmanın amacını ve sizin katılımcı olarak haklarınızı tanımlamayı amaçlamaktadır.

Bu araştırmanın amacı, öğretmenlerin dijital veri güvenliği konusundaki farkındalıklarına ilişkin görüşlerinin belirlenmesidir.

Bu konudaki görüş ve önerilerinizin gönüllülük ilkesine dayanarak araştırmama ışık tutacağına inanıyorum. Bu çalışmayı gerçekleştirirken araştırma verilerimin geçerliliği, güvenilirliği ve görüşme sırasında olabilecek kesintileri önleyebilmek amacıyla ses kaydı yapmak istiyorum. Ses kayıtlarındaki görüş ve önerileriniz araştırmamda yalnızca bilimsel veri olarak kullanılabilecektir.

Çalışmanın doğasında ve kullandığım tekniklere yönelik her türlü soruyu, dilediğiniz zaman aşağıda belirttiğim telefonlara ulaşarak sorabilirsiniz.

İsminiz ve/veya görüşmemiz sırasında geçen diğer isimler istemediğiniz takdirde kullanılmayacak, takma isimler kullanılacaktır. Eğer ses kaydı için izin verirseniz kayıtlar, bu çalışma dışında hiçbir amaçla kullanılmayacaktır. İstediğiniz takdirde ses kayıtları, veriler raporlaştırıldıktan sonra silinebilecek ya da size teslim edilebilecektir.

Bu çalışma gönüllülük ilkesine dayandığından istediğiniz anda görüşmeyi kesebilir, çalışmadan ayrılabilirsiniz. Bu durumda toplanan bilgi ve tüm kayıtlar ile yazılan raporları size teslim edeceğim. Çalışma raporunun bir örneğini de sizinle paylaşabileceğimi bilmenizi isterim. Bu sözleşmeyi okuduğunuz ve çalışmama gönüllü olarak katıldığınız için teşekkür ederim.

İsminizin kullanılmasını kabul ediyor musunuz?

Evet_____ Hayır_____

Cep telefonu aracılığıyla ses kaydı yapılmasına izin veriyor musunuz?

Evet_____ Hayır_____

Görüşmemiz sırasındaki sözlerinizin doğrudan alıntı yapılmasını onaylıyor musunuz?

Evet_____ Hayır_____

Bu koşulları kabul ediyorum. .../.../...	Bu koşulları kabul ediyorum. .../.../...
…… İmza:	Araştırmacı Eray YILMAZ İmza:

İletişim:
Eray YILMAZ
(505) 698 39 79
T.C. Ziraat Bankası Balıkesir Fen Lisesi

EK D - KAPSAM GEÇERLİLİĞİ UZMAN GÖRÜŞÜ FORMU

Değerli katılımcı, dijital veri güvenliği farkındalığına yönelik geliştirilmekte olan ölçek için alanyazın taraması yapılmış ve kritik paydaşlarla gerçekleştirilen odak grup görüşmeleri sonucunda aşağıdaki madde havuzu ortaya konulmuştur. Maddelerin ölçekte yer almasına ilişkin uzman görüşünüze başvurulmuştur. Lütfen maddeleri dikkatle okuyarak sizce en uygun olan seçeneği (X) ile işaretleyiniz. Maddenin düzenlenmesi gerektiğini düşünüyorsanız ilgili sütuna yazınız. Eklemek istediğiniz madde varsa formun sonuna ekleyiniz.

Dijital Veri Güvenliği Farkındalığı	**Tamamen Uygun**	**Kısmen Uygun**	**Uygun Değil**	**Madde şu şekilde düzenlenmeli:**
İzinsiz kullanımı engellemek için dosyalarıma parola koyarım.				
İzinsiz kullanımı engellemek için cihazlarıma parola koyarım.				
İzinsiz kullanımı engellemek için mümkün olan cihazlarda biyometrik yöntemleri (parmak izi, avuç içi vb.) kullanırım.				
Kendime ait olmayan cihazlara kişisel verilerimi kaydetmem.				
Taşınabilir depolama birimlerimi (Flash disk, CD vb.) kullanmadan önce virüs taraması yaparım.				
İnternetten/e-posta hesabımdan dosya indirdiğimde virüs taraması yaparım.				
Anti virüs yazılımı kullanırım.				
Antivirüs yazılımları kullanmanın veri güvenliğini arttırdığını düşünürüm.				
Zararlı yazılımlar (virüs, solucan, truva atı vb.) konusunda bilgi sahibiyim.				
Kullandığım yazılımların güncel olmasını sağlarım.				
Taşınabilir depolama birimlerimi “Donanımı Güvenle Kaldır” seçeneğini kullanarak çıkartırım.				
Elektrik kesintisi ile oluşacak veri kayıplarına karşı kesintisiz güç kaynağı kullanırım.				
Elektrik kesintisi ile oluşacak veri kayıplarına karşı dizüstü bilgisayarımı bataryası ile birlikte kullanırım.				
İşletim sisteminin güvenlikle ilgili uyarılarını dikkate alırım.				
Mobil cihazlardaki (tablet, akıllı telefon vb.) verilerin güvende olduğunu düşünürüm.				
Mobil cihazlar için sunulan uygulamaların güvenli olduğunu düşünürüm.				
Kullanmadığım zamanlarda İnternet erişimini kapatırım.				
İnternet adres çubuğunda yanlış yönlendirme olup olmadığını kontrol ederim.				
Ulaşmak istediğim İnternet sitesinin adresini doğrudan adres çubuğuna yazarım.				
İnternette kişisel bilgilerimi girdiğim işlemlerde diğer web sayfalarını kapatırım.				
Bir İnternet sitesinin güvenli olduğunu anlayabilirim.				

Bir İnternet sitesinin güvenli olup olmadığına değil aradığım içeriğe sahip olmasına bakarım.				
Güvenlik uyarısı ile karşılaştığım İnternet sitelerine girmem.				
İnternet erişimi olan cihazlarda verilerimin güvende olmadığını düşünürüm.				
İnternette yapılan yazışmalara başkaları tarafından ulaşılabileceğini bilirim.				
Programları üretici firmaların kendi sitesinden indiririm.				
Programların beraberinde eklenti kurup kurmadığına dikkat ederim.				
Farklı işlemler için aynı parolayı kullanırım.				
Kullandığım yerin önem derecesine göre farklı zorluk seviyelerinde parolalar kullanırım.				
Parola oluştururken harf, sayı ve özel karakter içermesine dikkat ederim.				
Daha güvenli parola oluşturmak için karakter sayısını arttırırım.				
Başkalarının tahmin edemeyeceği parolalar oluşturmaya dikkat ederim.				
Parola hatırlatma için kullanılan gizli soru ve cevaplara başkalarının tahmin edemeyeceği cevaplar veririm.				
Parola kurtarma seçenekleri (ikinci e-posta, güvenlik sorusu vb.) ile parola güvenliğimi arttırırım.				
Kendime ait olmayan cihazlarda parola gerektiren işlemler yapmam.				
Karmaşık yapıdaki parolaların da kırılabileceğini düşünürüm.				
Parolalarımın kaydedilmemesi için "Beni hatırla" seçeneğini kullanmam.				
Parolalarımı belirli aralıklarla değiştiririm.				
Parolaların herhangi bir ortamda saklanmasının güvenlik riski oluşturduğunu düşünürüm.				
Verilerimin güvenliği için taşınabilir disk yerine CD veya DVD kullanırım.				
Üzerinde çalıştığım dosyaları birden fazla ortamda yedeklerim.				
Taşınabilir depolama birimlerimi sadece antivirüs yazılımı olan bilgisayarlarda kullanırım.				
Flash disklerimi veri saklamak yerine sadece veri taşıma amaçlı kullanırım.				
Verilerimi saklamak için bulut bilişim sistemlerini (dropbox, google drive vb.) kullanırım.				
Verilerim silindiğinde geri getirilemeyeceğini düşünürüm.				
Dosya paylaşımının veri güvenliği bakımından risk oluşturduğunu düşünürüm.				
Ağ trafiğini izleyen yazılımlar kullanarak ağ güvenliğimi kontrol altına alırım.				
Güvenlik duvarı yazılımları kullanırım.				
Kablosuz modemimin arayüzündeki varsayılan giriş parolasını değiştiririm.				
Kablosuz modemimin arayüzünden bağlı olan cihazları kontrol ederim.				
Kablosuz modemimin diğer cihazlar tarafından görünebilirliğini kapatırım.				
Kablosuz modemime sadece izin verdiğim cihazların bağlanmasını sağlarım.				

e-devlet sitelerinin güvenli kullanımı konusunda bilgi sahibiyim.				
e-devlet sitelerindeki kişisel verilerimin güvende olmadığını düşünürüm.				
e-devlet sitelerinde güçlü parola kullanımının zorunlu olması gerektiğini düşünürüm.				
e-devlet sitelerine cep telefonuna gelen parola ile girilmesi gerektiğini düşünürüm.				
e-devlet sitelerini kapatırken "güvenli çıkış" bağlantısını kullanırım.				
Sosyal ağlarda kişiye özel bilgilerimi paylaşmam.				
Sosyal ağlarda tanımadığım kişilerden gelen arkadaşlık isteklerini kabul etmem.				
Sosyal ağlarda arkadaşlık isteğinde bulunan kişilerin öncelikle profil bilgilerini incelerim.				
Sosyal ağlarda sahte profiller ile sosyal mühendislik ataklarına maruz kalabilirim.				
Sosyal ağlarda sadece görmesini istediğim kişilerle paylaşımda bulunurum.				
Sosyal ağlardaki gizlilik ve güvenlik ayarlarını yaparım.				
Güvenli olmadığını düşündüğüm e-postaları açmam.				
Almak istemediğim çöp e-postaları "spam/gereksiz/önemsiz" olarak işaretlerim.				
E-posta ile gelen kimlik bilgilerini doğrulama mesajlarına (parola, kredi kartı vb.) itibar etmem.				
Gelen e-postadaki ekleri önce indirip sonra açarım.				
Önemli olmayan işlerimde beni yansıtmayan farklı bir e-posta hesabı kullanırım.				
E-posta hesabımı kurtarabilmek için gelen e-postalarımın içeriklerini bilirim.				
İnternetten alışveriş yapmanın güvenli olmadığını düşünürüm.				
Ortak kullanıma açık yerlerde (İnternet cafe, okul vb.) İnternetten alışveriş yaparım.				
Güvenli olduğunu düşündüğüm İnternet sitelerinden alışveriş yaparım.				
İnternetten alışverişte kredi kartımı kullanırım.				
İnternetten alışverişte sanal kredi kartı kullanırım.				
Her İnternet alışverişi sonrası sanal kartımın limitini sıfırlarım.				
Her İnternet alışverişi sonrası kredi kartımı internet alışverişine kapatırım.				
Ortak kullanıma açık yerlerde (İnternet cafe, okul vb.) İnternet bankacılığını kullanırım.				
İnternet bankacılığını cep telefonuma gelen parola sayesinde güvenli bulurum.				
İnternet bankacılığında banka hesaplarımı düzenli olarak kontrol ederim.				
İnternet bankacılığında sanal klavye kullanırım.				
Sanal ortamda suçluların tespit edilebileceğini düşünürüm.				
Sanal ortamda karşılaştığım hukuka aykırı durumları ilgililere bildiririm.				
Sanal ortamla ilgili yasal düzenlemelerin yetersiz olduğunu düşünürüm.				
Veri güvenliğinin hukuki boyutu konusunda bilgi sahibiyim.				
Kişisel verilerin korunmasına dair kanun hakkında				

bilgi sahibiyim.				
Lisanslı olmayan yazılımların güvenlik açıkları olduğunu düşünürüm.				
Lisans ücreti ödememek için ücretsiz yazılımları tercih ederim.				
Kullanım süresi dolan programları silerim veya satın alırım.				
Programların kullanım süresi dolduğunda ücretsiz kullanmaya devam edebilmek için bir şeyler yaparım.				
Sanal ortamdaki içeriklerin telif haklarına uygun davranırım.				
Telif hakkı karşılanmayan içeriklerin güvenli olmadığını düşünürüm.				
Telif hakları konusunda bilgi sahibiyim.				
Başkasına ait verileri sahibinin izni olmadan dağıtırım.				
Önerilen yeni madde:				
Önerilen yeni madde:				
Önerilen yeni madde:				
Maddelere ilişkin genel düşünceleriniz varsa lütfen belirtiniz.				

EK E - ÖN DENEMEDE KULLANILAN TASLAK ÖLÇEK FORMU

Değerli Meslektaşım,

Bu veri toplama aracı, öğretmenlerin dijital veri güvenliği farkındalıklarını ortaya koymak amacıyla hazırlanmıştır. Elde edilen veriler yalnızca bilimsel çalışmalar için kullanılacak, bireysel değerlendirme yapılmayacaktır. Bu nedenle isminizi yazmanıza gerek yoktur. Ölçekte 62 madde yer almaktadır ve yanıtlama süresi yaklaşık 20 dakikadır. Lütfen maddeleri dikkatle okuyarak size en uygun olan seçeneği (X) ile işaretleyiniz.

Katılımınız için teşekkür ederim.

Eray YILMAZ
T.C. Ziraat Bankası Balıkesir Fen Lisesi
Bilişim Teknolojileri Öğretmeni

No	Dijital Veri Güvenliği Farkındalığı	Kesinlikle Katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle Katılmıyorum
1	Parolaların kaydedilmemesi için "Beni Hatırla" seçeneğini kullanmamaya dikkat ederim.	□	□	□	□	□
2	Ağ trafiğini izleyen yazılımları kullanarak, ağ güvenliğinin kontrol altına alınabileceğini bilirim.	□	□	□	□	□
3	Ulaşmak istediğim İnternet sitesinin adresini doğrudan adres çubuğuna yazmak gerektiğini bilirim.	□	□	□	□	□
4	Kullanılan yazılımların güncel olması gerektiğinin farkındayım.	□	□	□	□	□
5	Kırma işlemi (crack) uygulanan yazılımların güvenlik açığı oluşturabileceğinin farkındayım.	□	□	□	□	□
6	Sosyal ağlarda kişisel bilgileri (doğum tarihi, fotoğraf, konum vb.) paylaşmanın veri güvenliği bakımından risk oluşturduğunun farkındayım.	□	□	□	□	□
7	Taşınabilir depolama birimlerini (Flash disk, taşınabilir sabit disk) sadece antivirüs yazılımı olan bilgisayarlarda kullanmaya dikkat ederim.	□	□	□	□	□
8	Zararlı yazılımlar (virüs, solucan, truva atı vb.) konusunda bilgi sahibiyim.	□	□	□	□	□
9	Yapılan işlemin önemine göre farklı zorluk seviyelerinde parola kullanmanın önemini bilirim.	□	□	□	□	□
10	Sadece güvenli olduğunu düşündüğüm İnternet sitelerinden alışveriş yapmaya dikkat ederim.	□	□	□	□	□
11	Parola oluştururken harf, sayı ve özel karakter kullanmanın önemini bilirim.	□	□	□	□	□
12	Farklı işlemler için farklı parola kullanmanın önemini bilirim.	□	□	□	□	□
13	İzinsiz kullanılmaması için dosyalara parola konulabileceğinin farkındayım.	□	□	□	□	□
14	İnternetten indirilen dosyalarda virüs taraması yapılması gerektiğini bilirim.	□	□	□	□	□
15	İnternetin ortak kullanıma açık olduğu yerlerde (İnternet cafe, okul vb.) internetten alışveriş yapmamaya dikkat ederim.	□	□	□	□	□
16	Kendime ait olmayan cihazlara kişisel verilerimi kaydetmemeye dikkat ederim.	□	□	□	□	□
17	İnternette yapılan yazışmalara başkaları tarafından ulaşılabileceğini bilirim.	□	□	□	□	□
18	Güvenlik duvarı yazılımları konusunda bilgi sahibiyim.	□	□	□	□	□
19	Kablosuz modemin diğer cihazlar tarafından görünebilirliğinin kapatılabileceğini bilirim.	□	□	□	□	□
20	Flash diskleri veri saklamak yerine sadece veri taşımak için kullanmanın farkını bilirim.	□	□	□	□	□

21	İşletim sisteminin (Windows, Android vb.) güncel olmasına dikkat ederim.	□	□	□	□	□
22	Kablosuz modeme sadece izin verilen cihazların bağlanabileceğini bilirim.	□	□	□	□	□
23	Sosyal ağlardaki gizlilik/güvenlik ayarlarının yapılması gerektiğinin farkındayım.	□	□	□	□	□
24	E-posta ile gelen kimlik bilgilerini doğrulama mesajlarına (parola, kredi kartı vb.) itibar edilmemesi gerektiğini bilirim.	□	□	□	□	□
25	İnternetin ortak kullanıma açık olduğu yerlerde (İnternet cafe, okul vb.) internet bankacılığı işlemleri yapmamaya dikkat ederim.	□	□	□	□	□
26	Taşınabilir depolama birimlerini (Flash disk, taşınabilir sabit disk) kullanmadan önce virüs taraması yapılması gerektiğini bilirim.	□	□	□	□	□
27	Güvenli olmadığını düşündüğüm e-postaları açmadan silmeye dikkat ederim.	□	□	□	□	□
28	Programların, üreticinin kendi sitesinden indirilmesinin önemini bilirim.	□	□	□	□	□
29	Antivirüs yazılımı kullanmanın önemini bilirim.	□	□	□	□	□
30	Parola hatırlatmak için kullanılan güvenlik sorularına başkalarının tahmin edemeyeceği cevaplar verilmesi gerektiğini bilirim.	□	□	□	□	□
31	Parola oluştururken karakter sayısının fazla olmasının önemini bilirim.	□	□	□	□	□
32	Parolaların herhangi bir ortamda saklanmasının güvenlik riski oluşturacağının farkındayım.	□	□	□	□	□
33	Verilerin, çeşitli uygulamalar (dropbox, google drive vb.) kullanılarak İnternet ortamında saklanabileceğini bilirim.	□	□	□	□	□
34	Üzerinde çalışma yapılan dosyaların birden fazla ortamda yedeklenmesi gerektiğini bilirim.	□	□	□	□	□
35	Güvenlik uyarısı ile karşılaşılan İnternet sitelerine girmemeye dikkat ederim.	□	□	□	□	□
36	İnternet bankacılığında hesapların düzenli olarak kontrol edilmesi gerektiğinin farkındayım.	□	□	□	□	□
37	Başkalarının tahmin edemeyeceği parolalar oluşturmaya dikkat ederim.	□	□	□	□	□
38	Sosyal ağlarda tanımadığım kişilerden gelen arkadaşlık isteklerini kabul etmemeye dikkat ederim.	□	□	□	□	□
39	İnternet adres çubuğunda yanlış yönlendirme olup olmadığına dikkat ederim.	□	□	□	□	□
40	İnternetten alışveriş yaparken sanal kredi kartı kullanmanın önemini bilirim.	□	□	□	□	□
41	Taşınabilir depolama birimlerini (Flash disk, taşınabilir sabit disk) "Donanımı Güvenle Kaldır" seçeneğini kullanarak çıkartmaya dikkat ederim.	□	□	□	□	□
42	Karmaşık yapıdaki parolaların kırılabileceğini bilirim.	□	□	□	□	□
43	Parola kurtarma seçeneklerinden ikincil e-posta ve/veya telefon numarasını tercih etmenin önemini bilirim.	□	□	□	□	□
44	Parolaların belirli aralıklarla değiştirilmesi gerektiğinin farkındayım.	□	□	□	□	□
45	Almak istemediğim çöp e-postaları "spam/gereksiz/önemsiz" olarak işaretlemeye dikkat ederim.	□	□	□	□	□
46	İzinsiz kullanılmaması için cihazlara (akıllı telefon, tablet, bilgisayar vb.) parola konulabileceğinin farkındayım.	□	□	□	□	□
47	Her İnternet alışverişinden sonra kredi kartının İnternet alışverişine kapatılabileceğini bilirim.	□	□	□	□	□
48	Kendime ait olmayan cihazlarda, parola gerektiren işlemler yapmamaya dikkat ederim.	□	□	□	□	□
49	Ağda dosya paylaşımının veri güvenliği bakımından risk oluşturabileceğinin farkındayım.	□	□	□	□	□
50	Kablosuz modemin arayüzünden, modeme bağlı cihazları kontrol etmek gerektiğinin farkındayım.	□	□	□	□	□
51	Sosyal ağlarda paylaşımda bulunurken yalnızca görmesini istediğim	□	□	□	□	□

	kişilere izin vermeye dikkat ederim.					
52	Her İnternet alışverişinden sonra sanal kredi kartımın limitini sıfırlamaya dikkat ederim.	□	□	□	□	□
53	İşletim sisteminin (Windows, Android vb.) güvenlikle ilgili uyarılarını dikkate alırım.	□	□	□	□	□
54	Programlar ile kurulan eklentilerin güvenliği olumsuz etkileyebileceğini bilirim.	□	□	□	□	□
55	Elektrik kesintisine karşı dizüstü bilgisayarları bataryası ile kullanmanın önemini bilirim.	□	□	□	□	□
56	Cep telefonuna gelen tek kullanımlık parola ile yapılan giriş işlemlerinin, güvenliği arttırdığını bilirim.	□	□	□	□	□
57	İnternet bankacılığında sanal klavye kullanmanın önemini bilirim.	□	□	□	□	□
58	İnternet sitelerinde kullanıcı oturumunu kapatırken "güvenli çıkış" bağlantısını kullanmanın önemini bilirim.	□	□	□	□	□
59	Kablosuz modemin varsayılan arayüz parolasını değiştirmenin önemini bilirim.	□	□	□	□	□
60	İnternet sitelerinde kullanılan güvenlik sertifikaları hakkında bilgi sahibiyim.	□	□	□	□	□
61	Sosyal ağlarda arkadaşlık isteğinde bulunan kişilerin öncelikle profil bilgilerini incelemeye dikkat ederim.	□	□	□	□	□
62	Lisanslı olmayan yazılımların güvenlik açıkları oluşturabileceğinin farkındayım.	□	□	□	□	□

EK F - YAPI GEÇERLİĞİ İNCELENEN TASLAK ÖLÇEK FORMU

Değerli Meslektaşım,

Bu veri toplama aracı, öğretmenlerin dijital veri güvenliği farkındalıklarını ortaya koymak amacıyla hazırlanmıştır. Elde edilen veriler yalnızca bilimsel çalışmalar için kullanılacak, bireysel değerlendirme yapılmayacaktır. Bu nedenle isminizi yazmanıza gerek yoktur. Ölçekte 56 madde yer almaktadır ve yanıtlama süresi yaklaşık 10 dakikadır. Lütfen maddeleri dikkatle okuyarak size en uygun olan seçeneği (X) ile işaretleyiniz.

Katılımınız için teşekkür ederim.

Eray YILMAZ
T.C. Ziraat Bankası Balıkesir Fen Lisesi
Bilişim Teknolojileri Öğretmeni

No	Dijital Veri Güvenliği Farkındalığı	Kesinlikle Katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle Katılmıyorum
1	Parolaların kaydedilmemesi için "Beni Hatırla" seçeneğini kullanmamaya dikkat ederim.	□	□	□	□	□
2	Ulaşmak istediğim İnternet sitesinin adresini doğrudan adres çubuğuna yazmak gerektiğini bilirim.	□	□	□	□	□
3	Kullanılan yazılımların güncel olması gerektiğinin farkındayım.	□	□	□	□	□
4	Sosyal ağlarda kişisel bilgileri (doğum tarihi, fotoğraf, konum vb.) paylaşmanın veri güvenliği bakımından risk oluşturduğunun farkındayım.	□	□	□	□	□
5	Taşınabilir depolama birimlerini (Flash bellek, taşınabilir sabit disk) sadece antivirüs yazılımı olan bilgisayarlarda kullanmaya dikkat ederim.	□	□	□	□	□
6	Zararlı yazılımlar (virüs, solucan, truva atı vb.) konusunda bilgi sahibiyim.	□	□	□	□	□
7	Yapılan işlemin önemine göre farklı zorluk seviyelerinde parola kullanmanın önemini bilirim.	□	□	□	□	□
8	Sadece güvenli olduğunu düşündüğüm İnternet sitelerinden alışveriş yapmaya dikkat ederim.	□	□	□	□	□
9	Parola oluştururken harf, sayı ve özel karakter kullanmanın önemini bilirim.	□	□	□	□	□
10	Farklı işlemler için farklı parola kullanmanın önemini bilirim.	□	□	□	□	□
11	İzinsiz kullanılmaması için dosyalara parola konulabileceğinin farkındayım.	□	□	□	□	□
12	İnternetten indirilen dosyalarda virüs taraması yapılması gerektiğini bilirim.	□	□	□	□	□
13	İnternetin ortak kullanıma açık olduğu yerlerde (İnternet cafe, okul vb.) internetten alışveriş yapmamaya dikkat ederim.	□	□	□	□	□
14	Kendime ait olmayan cihazlara kişisel verilerimi kaydetmemeye dikkat ederim.	□	□	□	□	□
15	İnternette yapılan yazışmalara başkaları tarafından ulaşılabileceğini bilirim.	□	□	□	□	□
16	Güvenlik duvarı yazılımları konusunda bilgi sahibiyim.	□	□	□	□	□
17	Kablosuz modemin diğer cihazlar tarafından görünebilirliğinin kapatılabileceğini bilirim.	□	□	□	□	□
18	Flash bellekleri, veri saklamak yerine sadece veri taşımak için kullanmanın farkını bilirim.	□	□	□	□	□
19	İşletim sisteminin (Windows, Android vb.) güncel olmasına dikkat ederim.	□	□	□	□	□
20	Kablosuz modeme sadece izin verilen cihazların bağlanabileceğini bilirim.	□	□	□	□	□
21	Sosyal ağlardaki gizlilik/güvenlik ayarlarının yapılması gerektiğinin farkındayım.	□	□	□	□	□
22	E-posta ile gelen kimlik bilgilerini doğrulama mesajlarına (parola, kredi kartı vb.) itibar edilmemesi gerektiğini bilirim.	□	□	□	□	□
23	İnternetin ortak kullanıma açık olduğu yerlerde (İnternet cafe, okul vb.) internet bankacılığı işlemleri yapmamaya dikkat ederim.	□	□	□	□	□

24	Taşınabilir depolama birimlerini (Flash bellek, taşınabilir sabit disk) kullanmadan önce virüs taraması yapılması gerektiğini bilirim.	□	□	□	□	□
25	Güvenli olmadığını düşündüğüm e-postaları açmadan silmeye dikkat ederim.	□	□	□	□	□
26	Programların, üreticinin kendi sitesinden indirilmesinin önemini bilirim.	□	□	□	□	□
27	Antivirüs yazılımı kullanmanın önemini bilirim.	□	□	□	□	□
28	Parola hatırlatmak için kullanılan güvenlik sorularına başkalarının tahmin edemeyeceği cevaplar verilmesi gerektiğini bilirim.	□	□	□	□	□
29	Parola oluştururken karakter sayısının fazla olmasının önemini bilirim.	□	□	□	□	□
30	Parolaların herhangi bir ortamda saklanmasının güvenlik riski oluşturacağının farkındayım.	□	□	□	□	□
31	Verilerin, çeşitli uygulamalar (dropbox, google drive vb.) kullanılarak İnternet ortamında saklanabileceğini bilirim.	□	□	□	□	□
32	Üzerinde çalışma yapılan dosyaların birden fazla ortamda yedeklenmesi gerektiğini bilirim.	□	□	□	□	□
33	Güvenlik uyarısı ile karşılaşılan İnternet sitelerine girmemeye dikkat ederim.	□	□	□	□	□
34	İnternet bankacılığında hesapların düzenli olarak kontrol edilmesi gerektiğinin farkındayım.	□	□	□	□	□
35	Başkalarının tahmin edemeyeceği parolalar oluşturmaya dikkat ederim.	□	□	□	□	□
36	Sosyal ağlarda tanımadığım kişilerden gelen arkadaşlık isteklerini kabul etmemeye dikkat ederim.	□	□	□	□	□
37	İnternet adres çubuğunda yanlış yönlendirme olup olmadığına dikkat ederim.	□	□	□	□	□
38	İnternetten alışveriş yaparken sanal kredi kartı kullanmanın önemini bilirim.	□	□	□	□	□
39	Taşınabilir depolama birimlerini (Flash bellek, taşınabilir sabit disk) "Donanımı Güvenle Kaldır" seçeneğini kullanarak çıkartmaya dikkat ederim.	□	□	□	□	□
40	Karmaşık yapıdaki parolaların kırılabileceğini bilirim.	□	□	□	□	□
41	Parolaların belirli aralıklarla değiştirilmesi gerektiğinin farkındayım.	□	□	□	□	□
42	Almak istemediğim çöp e-postaları "spam/gereksiz/önemsiz" olarak işaretlemeye dikkat ederim.	□	□	□	□	□
43	İzinsiz kullanılmaması için cihazlara (akıllı telefon, tablet, bilgisayar vb.) parola konulabileceğinin farkındayım.	□	□	□	□	□
44	Her İnternet alışverişinden sonra kredi kartının İnternet alışverişine kapatılabileceğini bilirim.	□	□	□	□	□
45	Kendime ait olmayan cihazlarda, parola gerektiren işlemler yapmamaya dikkat ederim.	□	□	□	□	□
46	Ağda dosya paylaşımının veri güvenliği bakımından risk oluşturabileceğinin farkındayım.	□	□	□	□	□
47	Sosyal ağlarda paylaşımda bulunurken yalnızca görmesini istediğim kişilere izin vermeye dikkat ederim.	□	□	□	□	□
48	Her İnternet alışverişinden sonra sanal kredi kartımın limitini sıfırlamaya dikkat ederim.	□	□	□	□	□
49	İşletim sisteminin (Windows, Android vb.) güvenlikle ilgili uyarılarını dikkate alırım.	□	□	□	□	□
50	Elektrik kesintisine karşı dizüstü bilgisayarları bataryası ile kullanmanın önemini bilirim.	□	□	□	□	□
51	Cep telefonuna gelen tek kullanımlık parola ile yapılan giriş işlemlerinin, güvenliği arttırdığını bilirim.	□	□	□	□	□
52	İnternet bankacılığında sanal klavye kullanmanın önemini bilirim.	□	□	□	□	□
53	İnternet sitelerinde kullanıcı oturumunu kapatırken "güvenli çıkış" bağlantısını kullanmanın önemini bilirim.	□	□	□	□	□
54	İnternet sitelerinde kullanılan güvenlik sertifikaları hakkında bilgi sahibiyim.	□	□	□	□	□
55	Sosyal ağlarda arkadaşlık isteğinde bulunan kişilerin öncelikle profil bilgilerini incelemeye dikkat ederim.	□	□	□	□	□
56	Lisanslı olmayan yazılımların güvenlik açıkları oluşturabileceğinin farkındayım.	□	□	□	□	□

EK G - AÇIMLAYICI FAKTÖR ANALİZİ İÇİN İL MİLLİ EĞİTİM MÜDÜRLÜĞÜ İZNİ

T.C.
BALIKESİR VALİLİĞİ
İl Milli Eğitim Müdürlüğü

Sayı: 99191664/605.01/3989989 17/09/2014
Konu : Araştırma İzni

VALİLİK MAKAMINA
BALIKESİR

İlgi : a) Milli Eğitim Bakanlığı Yenilik ve Eğitim Teknolojileri Genel Müdürlüğünün 07.03.2012 tarih ve 2012/13 sayılı genelgesi
b) Eray YILMAZ' a ait 16.09.2014 tarih ve 3965795 sayılı dilekçe

Başvuru Sahibinin Adı Soyadı	Eray YILMAZ		
Danışmanı	-		
Kurumu/Üniversite/Görev Yeri	Eskişehir Anadolu Üniversitesi		
Alan/Bölüm	Eğitim Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı		
Tez,Araştırma veya Anketin Konusu	Öğretmenlerin Dijital Veri Güvenliği Farkındalığının Belirlenmesi		
Başvuru Tarihi	16.09.2014	**Başvuru Sayısı**	3965795
Çalışma Başlama Tarihi	17 Eylül 2014		
Çalışma Bitiş Tarihi	31 Aralık 2014		
Veri Toplama Araçları	Anket Formu		
Araştırma Türü	Doktora Tezi		

ÇALIŞMA YAPLACAK EĞİTİM KURUMLARININ LİSTESİ			
S.No	**Okulun Adı**	**S.No**	**Okulun Adı**
1	Ekli Listede Belirtilen Okullar		

Bakanlığımıza bağlı okul ve kurumlarda yapılacak Araştırma, Yarışma ve Sosyal Etkinlik izinleri ilgi (a) genelge gereğince yukarıdaki bilgileri belirtilen çalışmanın, eğitim kurumlarında, okul/kurum müdürlüklerinin denetiminde yapılması Müdürlüğümüzce uygun görülmektedir.
Makamlarınızca da uygun görüldüğü taktirde olurlarınıza arz ederim.

Hüseyin AŞIK
Müdür a.
Müdür Yardımcısı

OLUR
17/09/2014
Yusuf CENGİZ
Vali a.
İl Milli Eğitim Müdürü

Ekler :
1-İlgi (b) Dilekçe ve Ekleri (6 Sayfa)
2-Araştırma Değerlendirme Formu (1 Sayfa)

Bu evrak güvenli elektronik imza ile imzalanmıştır. http://evraksorgu.meb.gov.tr adresinden ba15-1291-3744-b9f6-2422kodu ile teyit edilebilir.

EK H - DOĞRULAYICI FAKTÖR ANALİZİ İÇİN İL MİLLİ EĞİTİM MÜDÜRLÜĞÜ İZNİ

T.C.
BALIKESİR VALİLİĞİ
İl Milli Eğitim Müdürlüğü

Sayı: 99191664/605.01/5739645 26/11/2014
Konu: Araştırma İzni

VALİLİK MAKAMINA
BALIKESİR

İlgi : **a)** Milli Eğitim Bakanlığı Yenilik ve Eğitim Teknolojileri Genel Müdürlüğünün 07.03.2012 tarih ve 2012/13 sayılı genelgesi
b) Eray YILMAZ'a ait 26.11.2014 tarihli ve 5730127 sayılı dilekçe

Başvuru Sahibinin Adı Soyadı	Eray YILMAZ		
Danışmanı	Yrd. Doç. Dr. Yusuf Levent ŞAHİN Doç. Dr. Yusuf AKBULUT		
Kurumu/Üniversite/Görev Yeri	Eskişehir Anadolu Üniversitesi		
Alan/Bölüm	Eğitim Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Eğitimi Anadilim Dalı		
Tez,Araştırma veya Anketin Konusu	Öğretmenlerin Dijital Veri Güvenliği Farkındalığının Belirlenmesi		
Başvuru Tarihi	26.11.2014	**Başvuru Sayısı**	5730127
Çalışma Başlama Tarihi	26.11.2014		
Çalışma Bitiş Tarihi	30.05.2015		
Veri Toplama Araçları	Öğretmenlerin Dijital Veri Güvenliği Farkındalığı Ölçeği		
Araştırma Türü	Doktora tezi		

ÇALIŞMA YAPLACAK EĞİTİM KURUMLARININ LİSTESİ			
S.No	**Okulun Adı**	**S.No**	**Okulun Adı**
1	Balıkesir İlindeki ekli listede belirtilen ilkokul, ortaokul ve liseler.	----------	----------

Bakanlığımıza bağlı okul ve kurumlarda yapılacak Araştırma, Yarışma ve Sosyal Etkinlik izinleri ilgi (a) genelge gereğince yukarıdaki bilgileri belirtilen çalışmanın, eğitim kurumlarında, okul/kurum müdürlüklerinin denetiminde yapılması Müdürlüğümüzce uygun görülmektedir.

Makamlarınızca da uygun görüldüğü taktirde olurlarınıza arz ederim.

Hüseyin AŞIK
Müdür a.
Müdür Yardımcısı

26 Kasım 2014

Şeyma SALIK
Memur

Güvenli Elektronik İmzalı
Aslı ile Aynıdır.

OLUR
26/11/2014
Yusuf CENGİZ
Vali a.
İl Milli Eğitim Müdürü

Eki :
Dilekçe ve Ekleri (7 Sayfa)

Bu evrak güvenli elektronik imza ile imzalanmıştır. http://evraksorgu.meb.gov.tr adresinden d7d0-1880-3947-9a09-d225 kodu ile teyit edilebilir.

EK I - DİJİTAL VERİ GÜVENLİĞİ FARKINDALIĞI VERİ TOPLAMA ARACI

Değerli Meslektaşım,

Bu veri toplama aracı, öğretmenlerin dijital veri güvenliği farkındalıklarını ortaya koymak amacıyla hazırlanmıştır. Elde edilen veriler yalnızca bilimsel çalışmalar için kullanılacak, bireysel değerlendirme yapılmayacaktır. Bu nedenle isminizi yazmanıza gerek yoktur. Ölçekte 32 madde yer almaktadır ve yanıtlama süresi yaklaşık 10 dakikadır. Lütfen maddeleri dikkatle okuyarak size en uygun olan seçeneği (X) ile işaretleyiniz. Katılımınız için teşekkür ederim.

Eray YILMAZ
T.C. Ziraat Bankası Balıkesir Fen Lisesi
Bilişim Teknolojileri Öğretmeni

A) Kişisel Bilgiler

Cinsiyet: □Kadın □Erkek

Branş: □Sınıf öğretmeni □Branş Öğretmeni

Görev yapılan öğrenim kademesi: □İlkokul □Ortaokul □Lise

Mesleki deneyim: □1-5 yıl □6-10 yıl □11-15 yıl □16-20 yıl □21 yıl ve üzeri

Öğrenim durumu: □Ön Lisans □Lisans □Yüksek Lisans □Doktora

Günlük bilgisayar kullanım süresi: □1 saatten az □1-3 saat □4-6 saat □7 saat ve üzeri

Günlük İnternet kullanım süresi: □1 saatten az □1-3 saat □4-6 saat □7 saat ve üzeri

□Kendime ait bilgisayarım var. □Tablet bilgisayarım var. □Akıllı telefonum var.

EK I - DEVAMI

B) Dijital Veri Güvenliği Farkındalık Ölçeği

No	Dijital Veri Güvenliği Farkındalığı	Kesinlikle Katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle Katılmıyorum
1	Zararlı yazılımlar (virüs, solucan, truva atı vb.) konusunda bilgi sahibiyim.	□	□	□	□	□
2	Parola oluştururken harf, sayı ve özel karakter kullanmanın önemini bilirim.	□	□	□	□	□
3	Farklı işlemler için farklı parola kullanmanın önemini bilirim.	□	□	□	□	□
4	İzinsiz kullanılmaması için dosyalara parola konulabileceğinin farkındayım.	□	□	□	□	□
5	Güvenlik duvarı yazılımları konusunda bilgi sahibiyim.	□	□	□	□	□
6	Flash bellekleri, veri saklamak yerine sadece veri taşımak için kullanmanın farkını bilirim.	□	□	□	□	□
7	İşletim sisteminin (Windows, Android vb.) güncel olmasına dikkat ederim.	□	□	□	□	□
8	E-posta ile gelen kimlik bilgilerini doğrulama mesajlarına (parola, kredi kartı vb.) itibar edilmemesi gerektiğini bilirim.	□	□	□	□	□
9	Taşınabilir depolama birimlerini (Flash bellek, taşınabilir sabit disk) kullanmadan önce virüs taraması yapılması gerektiğini bilirim.	□	□	□	□	□
10	Güvenli olmadığını düşündüğüm e-postaları açmadan silmeye dikkat ederim.	□	□	□	□	□
11	Programların, üreticinin kendi sitesinden indirilmesinin önemini bilirim.	□	□	□	□	□
12	Antivirüs yazılımı kullanmanın önemini bilirim.	□	□	□	□	□
13	Parola hatırlatmak için kullanılan güvenlik sorularına başkalarının tahmin edemeyeceği cevaplar verilmesi gerektiğini bilirim.	□	□	□	□	□
14	Parola oluştururken karakter sayısının fazla olmasının önemini bilirim.	□	□	□	□	□
15	Parolaların herhangi bir ortamda saklanmasının güvenlik riski oluşturacağının farkındayım.	□	□	□	□	□
16	Verilerin, çeşitli uygulamalar (dropbox, google drive vb.) kullanılarak İnternet ortamında saklanabileceğini bilirim.	□	□	□	□	□
17	Üzerinde çalışma yapılan dosyaların birden fazla ortamda yedeklenmesi gerektiğini bilirim.	□	□	□	□	□
18	Başkalarının tahmin edemeyeceği parolalar oluşturmaya dikkat ederim.	□	□	□	□	□
19	İnternet adres çubuğunda yanlış yönlendirme olup olmadığına dikkat ederim.	□	□	□	□	□
20	Taşınabilir depolama birimlerini (Flash bellek, taşınabilir sabit disk) "Donanımı Güvenle Kaldır" seçeneğini kullanarak çıkartmaya dikkat ederim.	□	□	□	□	□
21	Karmaşık yapıdaki parolaların kırılabileceğini bilirim.	□	□	□	□	□
22	Parolaların belirli aralıklarla değiştirilmesi gerektiğinin farkındayım.	□	□	□	□	□
23	Almak istemediğim çöp e-postaları "spam/gereksiz/önemsiz" olarak işaretlemeye dikkat ederim.	□	□	□	□	□
24	İzinsiz kullanılmaması için cihazlara (akıllı telefon, tablet, bilgisayar vb.) parola konulabileceğinin farkındayım.	□	□	□	□	□
25	Kendime ait olmayan cihazlarda, parola gerektiren işlemler yapmamaya dikkat ederim.	□	□	□	□	□
26	İşletim sisteminin (Windows, Android vb.) güvenlikle ilgili uyarılarını dikkate alırım.	□	□	□	□	□
27	Elektrik kesintisine karşı dizüstü bilgisayarları bataryası ile kullanmanın önemini bilirim.	□	□	□	□	□
28	Cep telefonuna gelen tek kullanımlık parola ile yapılan giriş işlemlerinin, güvenliği arttırdığını bilirim.	□	□	□	□	□
29	Sanal klavye kullanmanın önemini bilirim.	□	□	□	□	□
30	İnternet sitelerinde kullanıcı oturumunu kapatırken "güvenli çıkış" bağlantısını kullanmanın önemini bilirim.	□	□	□	□	□
31	İnternet sitelerinde kullanılan güvenlik sertifikaları hakkında bilgi sahibiyim.	□	□	□	□	□
32	Lisanslı olmayan yazılımların güvenlik açıkları oluşturabileceğinin farkındayım.	□	□	□	□	□

EK J - SON UYGULAMA İÇİN İL MİLLİ EĞİTİM MÜDÜRLÜĞÜ İZNİ

T.C.
BALIKESİR VALİLİĞİ
İl Milli Eğitim Müdürlüğü

Sayı: 99191664/605.01/118260 07/01/2015
Konu: Araştırma İzni

VALİLİK MAKAMINA
BALIKESİR

İlgi : **a)** Milli Eğitim Bakanlığı Yenilik ve Eğitim Teknolojileri Genel Müdürlüğünün 07.03.2012 tarih ve 2012/13 sayılı genelgesi
b) Eray YILMAZ'a ait 05.01.2015 tarihli ve 7948 sayılı dilekçe

Başvuru Sahibinin Adı Soyadı	Eray YILMAZ		
Danışmanı	Yrd. Doç. Dr. Yusuf Levent ŞAHİN Doç. Dr. Yusuf AKBULUT		
Kurumu/Üniversite/Görev Yeri	Eskişehir Anadolu Üniversitesi		
Alan/Bölüm	Eğitim Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı		
Tez,Araştırma veya Anketin Konusu	Öğretmenlerin Dijital Veri Güvenliği Farkındalığı		
Başvuru Tarihi	05.01.2015	**Başvuru Sayısı**	7948
Çalışma Başlama Tarihi	06.01.2015		
Çalışma Bitiş Tarihi	30.05.2015		
Veri Toplama Araçları	Öğretmenlerin Dijital Veri Güvenliği Farkındalığı Ölçeği		
Araştırma Türü	Doktora Tezi		

ÇALIŞMA YAPLACAK EĞİTİM KURUMLARININ LİSTESİ			
S.No	**Okulun Adı**	**S.No**	**Okulun Adı**
1	Balıkesir ilindeki ekli listede belirtilen ilkokul, ortaokul ve liseler	2	----------

Bakanlığımıza bağlı okul ve kurumlarda yapılacak Araştırma, Yarışma ve Sosyal Etkinlik izinleri ilgi (a) genelge gereğince yukarıdaki bilgileri belirtilen çalışmanın, eğitim kurumlarında, okul/kurum müdürlüklerinin denetiminde yapılması Müdürlüğümüzce uygun görülmektedir.

Makamlarınızca da uygun görüldüğü taktirde olurlarınıza arz ederim.

Hüseyin AŞIK
Müdür a.
Müdür Yardımcısı

OLUR
07/01/2015
Yusuf CENGİZ
Vali a.
İl Milli Eğitim Müdürü

Eki :
Dilekçe ve Ekleri (6 Sayfa)

Bu evrak güvenli elektronik imza ile imzalanmıştır. http://evraksorgu.meb.gov.tr adresinden e9b0-5e3f-3fd8-bb5f-b016 kodu ile teyit edilebilir.

EK K - MADDE-MADDE KORELASYON DEĞERLERİ

Madde		M6	M9	M10	M11	M16	M18	M19	M22	M24	M25	M26	M27	M28	M29	M30	M31
M6	Pearson Correlation	1	.215**	.333**	.358**	.573**	.384**	.319**	.302**	.299**	.306**	.411**	.359**	.258**	.161**	.171**	.292**
	p (p<.01)		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M9	Pearson Correlation	.215**	1	.522**	.331**	.150**	.276**	.264**	.393**	.441**	.390**	.282**	.290**	.387**	.348**	.309**	.272**
	p (p<.01)	.000		.000	.000	.001	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M10	Pearson Correlation	.333**	.522**	1	.489**	.347**	.446**	.248**	.396**	.383**	.403**	.387**	.225**	.289**	.289**	.282**	.272**
	p (p<.01)	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M11	Pearson Correlation	.358**	.331**	.489**	1	.422**	.363**	.432**	.354**	.327**	.383**	.364**	.312**	.348**	.278**	.278**	.387**
	p (p<.01)	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M16	Pearson Correlation	.573**	.150**	.347**	.422**	1	.463**	.446**	.291**	.322**	.309**	.399**	.309**	.205**	.226**	.142**	.416**
	p (p<.01)	.000	.001	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.001	.000
M18	Pearson Correlation	.384**	.276**	.446**	.363**	.463**	1	.432**	.333**	.399**	.381**	.373**	.248**	.261**	.324**	.289**	.381**
	p (p<.01)	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M19	Pearson Correlation	.319**	.264**	.248**	.432**	.446**	.432**	1	.307**	.425**	.347**	.422**	.320**	.294**	.392**	.311**	.424**
	p (p<.01)	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000
M22	Pearson Correlation	.302**	.393**	.396**	.354**	.291**	.333**	.307**	1	.508**	.481**	.401**	.406**	.438**	.364**	.369**	.310**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000
M24	Pearson Correlation	.299**	.441**	.383**	.327**	.322**	.399**	.425**	.508**	1	.564**	.487**	.423**	.396**	.368**	.312**	.428**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000
M25	Pearson Correlation	.306**	.390**	.403**	.383**	.309**	.381**	.347**	.481**	.564**	1	.513**	.445**	.398**	.300**	.357**	.351**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000
M26	Pearson Correlation	.411**	.282**	.387**	.364**	.399**	.373**	.422**	.401**	.487**	.513**	1	.585**	.424**	.348**	.316**	.397**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000
M27	Pearson Correlation	.359**	.290**	.225**	.312**	.309**	.248**	.320**	.406**	.423**	.445**	.585**	1	.499**	.345**	.315**	.355**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000
M28	Pearson Correlation	.258**	.387**	.289**	.348**	.205**	.261**	.294**	.438**	.396**	.398**	.424**	.499**	1	.389**	.425**	.317**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000
M29	Pearson Correlation	.161**	.348**	.289**	.278**	.226**	.324**	.392**	.364**	.368**	.300**	.348**	.345**	.389**	1	.453**	.377**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000
M30	Pearson Correlation	.171**	.309**	.282**	.278**	.142**	.289**	.311**	.369**	.312**	.357**	.316**	.315**	.425**	.453**	1	.330**
	p (p<.01)	.000	.000	.000	.000	.001	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000
M31	Pearson Correlation	.292**	.272**	.272**	.387**	.416**	.381**	.424**	.310**	.428**	.351**	.397**	.355**	.317**	.377**	.330**	1
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	
M32	Pearson Correlation	.233**	.295**	.240**	.279**	.231**	.265**	.305**	.308**	.442**	.383**	.411**	.410**	.351**	.343**	.366**	.477**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M35	Pearson Correlation	.195**	.420**	.346**	.301**	.174**	.237**	.296**	.387**	.374**	.412**	.351**	.385**	.468**	.447**	.354**	.321**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M37	Pearson Correlation	.350**	.259**	.391**	.379**	.406**	.408**	.416**	.346**	.435**	.405**	.413**	.338**	.344**	.347**	.334**	.466**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M39	Pearson Correlation	.232**	.234**	.275**	.274**	.277**	.247**	.316**	.256**	.338**	.301**	.282**	.228**	.222**	.254**	.250**	.278**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M40	Pearson Correlation	.241**	.241**	.267**	.221**	.302**	.262**	.290**	.332**	.330**	.325**	.312**	.248**	.234**	.267**	.253**	.472**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M41	Pearson Correlation	.343**	.319**	.423**	.328**	.440**	.434**	.361**	.317**	.356**	.357**	.391**	.301**	.301**	.370**	.313**	.436**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M42	Pearson Correlation	.391**	.263**	.314**	.311**	.416**	.361**	.350**	.346**	.482**	.356**	.359**	.303**	.321**	.292**	.253**	.433**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M43	Pearson Correlation	.293**	.319**	.331**	.370**	.332**	.342**	.363**	.340**	.404**	.345**	.337**	.321**	.349**	.331**	.355**	.404**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M45	Pearson Correlation	.258**	.337**	.327**	.369**	.267**	.379**	.345**	.377**	.304**	.389**	.293**	.287**	.327**	.354**	.318**	.385**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M49	Pearson Correlation	.324**	.326**	.398**	.428**	.390**	.377**	.381**	.364**	.337**	.389**	.372**	.352**	.320**	.254**	.287**	.464**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M50	Pearson Correlation	.312**	.272**	.387**	.388**	.405**	.350**	.375**	.372**	.397**	.355**	.372**	.290**	.314**	.252**	.256**	.411**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M51	Pearson Correlation	.204**	.332**	.242**	.278**	.228**	.210**	.385**	.369**	.373**	.371**	.386**	.388**	.375**	.369**	.351**	.398**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M52	Pearson Correlation	.361**	.293**	.327**	.325**	.375**	.321**	.363**	.334**	.324**	.338**	.401**	.410**	.364**	.352**	.301**	.403**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M53	Pearson Correlation	.241**	.359**	.301**	.285**	.235**	.306**	.317**	.343**	.346**	.363**	.316**	.375**	.350**	.338**	.375**	.303**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M54	Pearson Correlation	.471**	.173**	.335**	.329**	.525**	.357**	.405**	.216**	.321**	.345**	.424**	.293**	.212**	.208**	.183**	.457**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M56	Pearson Correlation	.361**	.301**	.398**	.323**	.337**	.305**	.383**	.304**	.357**	.332**	.440**	.317**	.311**	.358**	.326**	.297**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000

EK K - DEVAMI

Madde		M32	M35	M37	M39	M40	M41	M42	M43	M45	M49	M50	M51	M52	M53	M54	M56
M6	Pearson Correlation	.233**	.195**	.350**	.232**	.241**	.343**	.391**	.293**	.258**	.324**	.312**	.204**	.361**	.241**	.471**	.361**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M9	Pearson Correlation	.295**	.420**	.259**	.234**	.241**	.319**	.263**	.319**	.337**	.326**	.272**	.332**	.293**	.359**	.173**	.301**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M10	Pearson Correlation	.240**	.346**	.391**	.275**	.267**	.423**	.314**	.331**	.327**	.398**	.387**	.242**	.327**	.301**	.335**	.398**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M11	Pearson Correlation	.279**	.301**	.379**	.274**	.221**	.328**	.311**	.370**	.369**	.428**	.388**	.278**	.325**	.285**	.329**	.323**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M16	Pearson Correlation	.231**	.174**	.406**	.277**	.302**	.440**	.416**	.332**	.267**	.390**	.405**	.228**	.375**	.235**	.525**	.337**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M18	Pearson Correlation	.265**	.237**	.408**	.247**	.262**	.434**	.361**	.342**	.379**	.377**	.350**	.210**	.321**	.306**	.357**	.305**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M19	Pearson Correlation	.305**	.296**	.416**	.316**	.290**	.361**	.350**	.363**	.345**	.381**	.375**	.385**	.363**	.317**	.405**	.383**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M22	Pearson Correlation	.308**	.387**	.346**	.256**	.332**	.317**	.346**	.340**	.377**	.364**	.372**	.369**	.334**	.343**	.216**	.304**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M24	Pearson Correlation	.442**	.374**	.435**	.338**	.330**	.356**	.482**	.404**	.304**	.337**	.397**	.373**	.324**	.346**	.321**	.357**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M25	Pearson Correlation	.383**	.412**	.405**	.301**	.325**	.357**	.356**	.345**	.389**	.389**	.355**	.371**	.338**	.363**	.345**	.332**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M26	Pearson Correlation	.411**	.351**	.413**	.282**	.312**	.391**	.359**	.337**	.293**	.372**	.372**	.386**	.401**	.316**	.424**	.440**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M27	Pearson Correlation	.410**	.385**	.338**	.228**	.248**	.301**	.303**	.321**	.287**	.352**	.290**	.388**	.410**	.375**	.293**	.317**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M28	Pearson Correlation	.351**	.468**	.344**	.222**	.234**	.301**	.321**	.349**	.327**	.320**	.314**	.375**	.364**	.350**	.212**	.311**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M29	Pearson Correlation	.343**	.447**	.347**	.254**	.267**	.370**	.292**	.331**	.354**	.254**	.252**	.369**	.352**	.338**	.208**	.358**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M30	Pearson Correlation	.366**	.354**	.334**	.250**	.253**	.313**	.253**	.355**	.318**	.287**	.256**	.351**	.301**	.375**	.183**	.326**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M31	Pearson Correlation	.477**	.321**	.466**	.278**	.472**	.436**	.433**	.404**	.385**	.464**	.411**	.398**	.403**	.303**	.457**	.297**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M32	Pearson Correlation	1	.435**	.379**	.304**	.342**	.426**	.356**	.399**	.347**	.371**	.318**	.445**	.349**	.395**	.315**	.360**
	p (p<.01)		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M35	Pearson Correlation	.435**	1	.463**	.304**	.302**	.362**	.333**	.434**	.415**	.376**	.311**	.445**	.415**	.417**	.214**	.316**
	p (p<.01)	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M37	Pearson Correlation	.379**	.463**	1	.404**	.396**	.492**	.527**	.451**	.425**	.501**	.456**	.381**	.477**	.379**	.450**	.428**
	p (p<.01)	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M39	Pearson Correlation	.304**	.304**	.404**	1	.404**	.424**	.363**	.399**	.405**	.430**	.419**	.278**	.306**	.360**	.288**	.394**
	p (p<.01)	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M40	Pearson Correlation	.342**	.302**	.396**	.404**	1	.534**	.410**	.415**	.443**	.445**	.419**	.259**	.311**	.243**	.336**	.280**
	p (p<.01)	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M41	Pearson Correlation	.426**	.362**	.492**	.424**	.534**	1	.485**	.536**	.471**	.542**	.435**	.313**	.435**	.352**	.430**	.443**
	p (p<.01)	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
M42	Pearson Correlation	.356**	.333**	.527**	.363**	.410**	.485**	1	.491**	.331**	.408**	.430**	.359**	.464**	.368**	.449**	.373**
	p (p<.01)	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000
M43	Pearson Correlation	.399**	.434**	.451**	.399**	.415**	.536**	.491**	1	.525**	.494**	.510**	.422**	.431**	.409**	.336**	.383**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000
M45	Pearson Correlation	.347**	.415**	.425**	.405**	.443**	.471**	.331**	.525**	1	.503**	.483**	.385**	.447**	.390**	.292**	.376**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000
M49	Pearson Correlation	.371**	.376**	.501**	.430**	.445**	.542**	.408**	.494**	.503**	1	.607**	.329**	.456**	.466**	.433**	.460**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000
M50	Pearson Correlation	.318**	.311**	.456**	.419**	.419**	.435**	.430**	.510**	.483**	.607**	1	.480**	.454**	.391**	.423**	.466**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000
M51	Pearson Correlation	.445**	.445**	.381**	.278**	.259**	.313**	.359**	.422**	.385**	.329**	.480**	1	.573**	.446**	.299**	.358**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000
M52	Pearson Correlation	.349**	.415**	.477**	.306**	.311**	.435**	.464**	.431**	.447**	.456**	.454**	.573**	1	.541**	.474**	.515**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000
M53	Pearson Correlation	.395**	.417**	.379**	.360**	.243**	.352**	.368**	.409**	.390**	.466**	.391**	.446**	.541**	1	.366**	.440**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000
M54	Pearson Correlation	.315**	.214**	.450**	.288**	.336**	.430**	.449**	.336**	.292**	.433**	.423**	.299**	.474**	.366**	1	.436**
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000
M56	Pearson Correlation	.360**	.316**	.428**	.394**	.280**	.443**	.373**	.383**	.376**	.460**	.466**	.358**	.515**	.440**	.436**	1
	p (p<.01)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	

KAYNAKÇA

Acar, N. V. (2004). *Ne kadar farkındayım: Gestalt terapi (2. Baskı).* Ankara: Babil Yayınevi.

Akbulut, Y. (2010). *Sosyal bilimlerde SPSS uygulamaları: Sık kullanılan istatistiksel analizler ve açıklamalı SPSS çözümleri.* İstanbul: İdeal Kültür ve Yayıncılık.

American Psychological Association. (2010). *Publication manual of the American Psychological Association (6. Baskı).* Washington DC: Author.

Atalıç Taş, K. (2010). *Bilişim suçları ve Adana ilinde 2006-2009 yılları arasında meydana gelen bilişim suçlarının değerlendirilmesi.* Yayımlanmamış Yüksek Lisans Tezi, Çukurova Üniversitesi, Sağlık Bilimleri Enstitüsü, Adana.

Albrechtsen, A. (2007). A qualitative study of users' view on information security. *Computer and Security*, *26*(7), 276-289.

Arıtürk, M. (2015). Bilgi farkındalığı ve bilgi güvenliğinin karşılaştırılması. *XVII. Akademik Bilişim Konferansı*, 4-6 Şubat 2015, Anadolu Üniversitesi, Eskişehir.

Arifoğlu, A., Kömes, A., Yazıcı, A., Akgül, M. K. ve Ayvalı, A. (2002). *E-devlet yolunda Türkiye*. Ankara: Türkiye Bilişim Derneği Yayınları.

Balaman, Y. (2013). *Ortaöğretim bilgi ve iletişim teknolojisi ders kitabı*. Ankara: Fırat Yayıncılık.

Baykal, N. (2005). Bilgi teknolojisinin, ulusal güvenlik ve ulusal güvenlik stratejisi ile ilgili boyutu. *Hava Harp Akademileri Sempozyumu*, 12, İstanbul.

Beyer, A. ve Westendorf, C. (2009). How to establish security awareness in schools. Pohlmarm, N., Reimer, H. ve Schneider, W. (Ed.), *Securing Electronic Business Processes*. (177-186). Kranzberg: Vieweg.

Bilgi Güvenliği Derneği. (2012). *Uluslararası bilgi güvenliği ve kriptoloji konferansı (ISCTurkey 2012) sonuç bildirgesi.* http://www.bilgiguvenligi.org.tr/index_files/pdf/ISCTURKEY2012_pdf/54.pdf adresinden 14 Aralık 2013 tarihinde edinilmiştir.

Brown, T. A. (2006). *Confirmatory factor analysis for applied research.* New York: Guilford Press.

Büyüköztürk, Ş. (2009). *Sosyal bilimler için veri analizi el kitabı (9. Baskı).* Ankara: Pegem Akademi.

Büyüköztürk, Ş. (2011). *Sosyal bilimler için veri analizi el kitabi (14. Baskı).* Ankara: Pegem Akademi.

Büyüköztürk, Ş., Kılıç Çakmak, E., Akgün, Ö. E., Karadeniz, Ş. ve Demirel, F. (2013). *Bilimsel araştırma yöntemleri*. Ankara: Pegem Akademi.

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

Canbek, G. ve Sağıroğlu, Ş. (2007a). Kötücül ve casus yazılımlara karşı elektronik imzanın sağlamış olduğu korunma düzeyi. *Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı*, Ankara, 263-269.

Canbek, G. ve Sağıroğlu, Ş. (2007b). Bilgisayar sistemlerine yapılan saldırılar ve türleri: Bir inceleme. *Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 23*(1-2), 1-12.

Canbek, G. (2005). *Klavye dinleme ve önleme sistemleri: Analiz, tasarım ve geliştirme.* Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.

Chou, C. ve Peng, H. (2011). Promoting awareness of Internet safety in Taiwan in-service teacher education: A ten-year experience. *Internet and Higher Education, 14,* 44-53.

Cohen, L., Manion, L. ve Morrison, K. (2007). *Research methods in education (6th ed).* London: Routledge.

Computer Security Institute. (2009). *14th Annual computer crime and security survey*. http://www.mediabistro.com/portfolios/samples_files/1041692_KZwy61VoDrY91T_6Zsy4FCwSQ.pdf adresinden 12 Mart 2015 tarihinde edinilmiştir.

Comrey, A. L. ve Lee, H. B. (1992). *A first course in factor analysis (2nd ed).* Hillsdale, NJ: Erlbaum.

Cresswell, J. W. (2011). *Planning, conducting and evaluating quantitative and qualitative research (4th Ed.).* Boston: Pearson Education.

Cüre, F. ve Özdener, N. (2008). Öğretmenlerin bilgi ve iletişim teknolojileri (BİT) uygulama başarıları ve BİT'e yönelik tutumları. *Hacettepe Üniversitesi, Eğitim Fakültesi Dergisi, 34*, 41-53.

Çakır, E. (2011). HTML5 güvenliği: Yeni nesil web tehditleri. *IV. Ağ ve Bilgi Güvenliği Sempozyumu*, 25-26 Kasım 2011, Ankara.

Çelik, H. C. ve Bindak, R. (2005). İlköğretim okullarında görev yapan öğretmenlerin bilgisayara yönelik tutumlarının çeşitli değişkenlere göre incelenmesi. *İnönü Üniversitesi, Eğitim Fakültesi Dergisi, 6*(10), 27-38.

Çetinkaya, M. (2008). *Bilgi güvenliği yönetim sistemi altyapısının değerlendirilmesi için bir test aracı geliştirilmesi.* Yayımlanmamış Yüksek Lisans Tezi, İstanbul Kültür Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

Çiçek, İ. ve Okatan, A. (2008).Ülkemizde adli bilişim laboratuarı kurulumu ve bilişim suçlarıyla mücadeleye katkıları. *II. Ağ ve Bilgi Güvenliği Sempozyumu,* 16-18 Mayıs 2008, Girne, KKTC.

Çokluk, Ö., Şekercioğlu, G. ve Büyüköztürk, Ş. (2012). *Sosyal bilimler için çok değişkenli istatistik: SPSS ve LISREL uygulamaları (2. Baskı).* Ankara: Pegem Akademi.

Çubukcu, A. ve Bayzan, Ş. (2013). Türkiye'de dijital vatandaşlık algısı ve bu algıyı İnternet'in bilinçli, güvenli ve etkin kullanımı ile artırma yöntemleri. *Middle Eastern & African Journal of Educational Research, 5,* 148-174.

Çukurbaşı, B. ve İşman, A. (2014). Öğretmen adaylarının dijital yerli özelliklerinin incelenmesi (Bartın Üniversitesi örneği). *Bartın Üniversitesi, Eğitim Fakültesi Dergisi, 3*(1), 28-54.

Demir, S. B. ve Akengin, H. (2010). Sosyal bilgiler dersine yönelik bir tutum ölçeğinin geliştirilmesi: Geçerlik ve güvenirlik çalışması. *e-Uluslararası Eğitim Araştırmaları Dergisi, 1*(1), 26-40.

Dökmen, Ü. (2000). *Yarına kim kalacak? Evrenle uyumlaşma sürecinde varolmak gelişmek uzlaşmak.* İstanbul: Sistem Yayıncılık.

Dönmez, O., Odabaşı, H. F., Kabakçı Yurdakul, I., Kuzu, A. ve Girgin, Ü. (2014). Öğretmen adayları için hazırlanan algılanan İnternet riskleri ölçeğinin güvenirlik ve geçerlik çalışmaları. *8. Uluslararası Bilgisayar ve Öğretim Teknolojileri Sempozyumu,* 18-20 Eylül 2014, Trakya Üniversitesi, Edirne.

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

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

Erkuş, A. (2014). *Psikolojide ölçme ve ölçek geliştirme I: Temel kavramlar ve işlemler (2.Baskı).* Ankara: Pegem Akademi.

FATİH Projesi. (2012). *Proje hakkında.* http://fatihprojesi.meb.gov.tr/tr/icerikincele.php?id=6 adresinden 17.12.2013 tarihinde edinilmiştir.

Fussell, R. S. (2005). Protecting information security availability via self-adapting intelligent agents. *Military Communications Conference*, IEEE, 297.

Gök, O., Yazıcı, S., Duru, N. ve Becerikli, Y. (2007). Kablosuz yerel alan ağlarda güvenlik uygulaması. *III. İletişim Teknolojileri Ulusal Sempozyumu*, 18-19 Ekim 2007, Adana.

Güven, E. ve Aydoğdu, M. (2012). Çevre sorunlarına yönelik farkındalık ölçeğinin geliştirilmesi ve öğretmen adaylarının farkındalık düzeylerinin belirlenmesi. *Öğretmen Eğitimi ve Eğitimcileri Dergisi, 1*(2), 185-202.

Haklı, T. (2012). *Bilgi güvenliği standartları ve kamu kurumları bilgi güvenliği için bir model önerisi*. Yayımlanmamış Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi, Fen Bilimleri Enstitüsü, Isparta.

Henkoğlu, T. ve Yılmaz, B. (2013). Avrupa Birliği (AB) bilgi güvenliği politikaları. *Türk Kütüphaneciliği, 27*(3), 451-471.

Hooper, D., Coughlan, J. ve Mullen, M. (2008). Structural equation modeling: Guidelines for determining model fit. *The Electronic Journal of Business Research Methods, 6*(1), 53-60.

Hu, L. T. ve Bentler, P. M. (1999). Cutoff criteria for fit ındexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling, 6*(1), 1-55.

Huck, S. W. (2012). *Reading statictics and research (6th. Ed.).* Boston: Pearson.

International Telecommunications Union. (2008). *Regional cyber security forum meeting report.* http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/sofia-cybersecurity-forumreport-oct-08.pdf adresinden 16.03.2014 tarihinde edinilmiştir.

İnci, Ş. (2002). *Türk Milli Eğitiminde eğitim teknolojisi politikaları ve uygulamaları*. Yayınlanmış Yüksek Lisans Tezi, Yüzüncü Yıl Üniversitesi, Sosyal Bilimler Enstitüsü, Van.

Kalaycı, Ş. (2009). *SPSS uygulamalı çok değişkenli istatistik teknikleri.* Ankara: Asil Yayınevi.

Karakaş, Z. (2002). *Teknoloji yönetimi.* Yayımlanmamış Yüksek Lisans Tezi, Sakarya Üniversitesi Sosyal Bilimler Enstitüsü, Sakarya.

Karakoç, M. (2011). Bilişim suçlarına genel bakış, bilişim suçlarını önleme çalışmaları ve güvenli internet kullanımı. *Suç ve Önleme Sempozyumu,* Bursa.

Karasar, N. (1995). *Bilimsel araştırma yöntemi: Kavramlar, ilkeler ve teknikler*. Ankara: 3A Araştırma Eğitim Danışmanlık Ltd. Şti.

Keleş, M. K. ve Güneş, A. (2013). 24 bit renkli dokümanların farklı biyometri teknoloji kullanılarak güvenliğinin sağlanması. *6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı,* 20-21 Eylül 2013, Ankara.

Kelloway, K. E. (1998). *Using Lisel for structural equation modeling: A researcher' s guide.* London: Sage.

Ketizmen, M. ve Ülküderner, Ç. (2007). E-devlet uygulamalarında kişisel verilerin korun(ma)ması. *XII. Türkiye'de İnternet Konferansı*, 8-10 Kasım 2007, Ankara.

Kılıç Çakmak, E., Güneş, E., Çiftci, S. ve Üstündağ, M. T. (2011). Web sitesi kullanılabilirlik ölçeğinin geliştirilmesi: Geçerlik, güvenirlik analizi ve uygulama sonuçları. *Pegem Eğitim ve Öğretim Dergisi, 1*(2), 31-40.

Kınay, H., Sözcü, Ö. F., Taşkın, E. ve İpek, İ. (2014). Bilgi güvenliği farkındalığı ölçeğinin ilk bulguları. *8. Uluslararası Bilgisayar ve Öğretim Teknolojileri Sempozyumu*, 18-20 Eylül 2014, Trakya Üniversitesi, Edirne.

Kızılyel, S. (2007). E-devlet güvenliğinin sağlanmasında idari sorumluluk ve yetki paylaşımı. *Türk İdare Dergisi, 456*, 55-79.

Kocamustafaoğulları, M. (2013). *Bilgi güvenliği farkındalığı ve uygulama seviyesi değerlendirmek için bilgi güvenliği prototip uygulaması.* Yayımlanmamış Yüksek Lisans Tezi, Çankaya Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.

Krause, M. ve Tipton, H. (2007). *Information security management handbook.* Londra: CRC Press, ISDN: 0849319978.

Kruger, H., Drevin, L. ve Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security,18*(5), 316-327.

Kruger, H. A. ve Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*, 289-296.

Kuzucu, Y. (2008). Duygusal farkındalık düzeyi ölçeğinin uyarlanması: Geçerlik ve güvenirlik çalışmaları. *Türk Psikolojik Danışma ve Rehberlik Dergisi, 3*(29), 51-64.

Little, R. J. A. ve Rubin, D. R. (2002). *Statistical analysis with missing data (Second Edition).* New York: Wiley.

Mart, İ. (2012). *Bilişim kültüründe bilgi güvenliği farkındalığı.* Yayımlanmamış Yüksek Lisans Tezi, Kahramanmaraş Sütçü İmam Üniversitesi, Fen Bilimleri Enstitüsü, Kahramanmaraş.

McCumber, J. (2005). *Assessing and managing security risk in IT systems*. Washington: CRC Press.

MEB. (2002). *MLO modeli (Düzeltilmiş 3. Baskı).* Ankara: EARGED Yayınları.

MEB. (2009). *e-Okul kullanım kılavuzu*. http://e-okul.meb.gov.tr adresinden 15.12.2013 tarihinde edinilmiştir.

MEB Bilgi İşlem Dairesi Başkanlığı. (2012). *Bilgi ve sistem güvenliği yönergesi*. http://bigb.meb.gov.tr/meb_iys_dosyalar/2012_06/18113300_yonerge.pdf adresinden 17 Mart 2014 tarihinde edinilmiştir.

Microsoft. (2005). *Bilgisayar virüsü nedir?* http://www.microsoft.com/turkiye/athome/security/viruses/intro_viruses_what.mspx adresinden 24.12.2013 tarihinde edinilmiştir.

Microsoft. (2014). *Security intelligence report, Volume 17.* http://www.microsoft.com/en-us/download/confirmation.aspx?id=44937 adresinden 17.03.2015 tarihinde edinilmiştir.

Nagy, S. ve Biber, H. (2010). *Mixed methods research.* Newyork: The Guilford Press.

Nickolov, E. (2008). *Modern trends in the cyber attacks against the critical information infrastructure.* Regional Cybersecurity Forum, 7-9 Ekim, 2008, Sofya, Bulgaristan. http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/sofiacybersecurity-forum-report-oct-08.pdf adresinden 22.12.2013 tarihinde edinilmiştir.

Oktay, S. ve Çakır, R. (2012). İlköğretim öğretmelerinin teknoloji kullanımları ve teknolojiye yönelik tutumları arasındaki ilişkinin incelenmesi. *X. Ulusal Fen Bilimleri ve Matematik Eğitimi Kongresi*, 27-30 Haziran 2012, Niğde.

Öğretmen Yetiştirme ve Geliştirme Genel Müdürlüğü. (2013a). *Hizmet içi eğitim etkinlik programı*. http://hedb.meb.gov.tr/net/_Duyuru_dosyalar/fatih/EK-1.pdf adresinden 17.12.2013 tarihinde edinilmiştir.

Öğretmen Yetiştirme ve Geliştirme Genel Müdürlüğü. (2013b). *Geliştirilen ve güncellenen standart kriterlere uygun olarak hazırlanan örnek hizmet içi eğitim programları*. http://hedb.meb.gov.tr/net/_standart_program/ adresinden 17.12.2013 tarihinde edinilmiştir.

Özenç, K. (2007). Bilgi ve iletişim teknolojilerinde kişisel ve kurumsal bilgi güvenliğinin sağlanması. *Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı*, 13-14 Aralık 2007, Ankara.

Özkale, A. ve Koç, M. (2014). Tablet computers and their usage in educational settings: A literature review. *SDU International Journal of Educational Studies, 1*(1), 24-35.

Öztürk, Ö. (2009). *E-postalarda spam sorunu ve çözüm önerileri*. Uzmanlık Tezi, Bilgi Teknolojileri ve İletişim Kurumu, Ankara.

Özyeşil, Z., Arslan, C., Kesici, Ş. ve Deniz, M. E. (2011). Bilinçli farkındalık ölçeğini Türkçeye uyarlama çalışması. *Eğitim ve Bilim, 36*(160), 224-235.

Rezgui, Y. ve Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security, 27*, 241-253.

Sağıroğlu, Ş. ve Özkaya, N. (2007). Bilgi güvenliği için nörol çözümler. *Politeknik Dergisi, 10*(1), 21-25.

Sargın, N. (2010). Öğretmen adaylarının çatışma ve şiddete ilişkin farkındalık düzeylerinin çeşitli değişkenlere göre incelenmesi. *Kuram ve Uygulamada Eğitim Yönetimi, 16*(4), 601-616.

Say, M. ve Sağıroğlu, Ş. (2004). Bilgisayar veri güvenliği üzerine bir inceleme: Klavye dinleme sistemleri. *Akademik Bilişim Konferansı'04*, 11-13 Şubat 2004, Karadeniz Teknik Üniversitesi, Trabzon.

Schlienger, T. ve Teufel, S. (2001). *Analyzing information security culture: Increased trust by an appropriate information security culture.* University of Fribourg, Fribourg.

Schmidt, A. H. (2004). *Building a mosaic of security for a better world, security matters*. USA: Aspatore Books.

Schryen, G. (2007). *Anti-spam measures: Analysis and design. springer science*. Germany: Business Media, ISDN:9783540717485.

Schumacher, R. E. ve Lomax, R. G. (1996). *A beginner's guide to structural equation modeling.* New Jersey: Lawrence Erlbaum Associates Publishers.

Sel, H. (2013). Erişim, güvenlik ve gizlilik boyutunda ortaokul öğrencilerinin Facebook kullanımı. *XV. Akademik Bilişim Konferansı,* 23-25 Ocak 2013, Akdeniz Üniversitesi, Antalya.

Sönmez, S. (2005). *İşbirliğine dayalı öğrenme yöntemi, birleştirme tekniği ile bilgisayar okur-yazarlığı öğretiminin akademik başarıya ve kalıcılığa etkisi*. Yayımlanmamış Yüksek Lisans Tezi, Çukurova Üniversitesi, Sosyal Bilimler Enstitüsü, Adana.

Steiger, J. H. (2007). Understanding the limitations of global fit assessment in structural equation modeling. *Personality and Individual differences, 42,* 893-898.

Stevens, J. (1996). *Applied multivariate statistics for the social sciences (3rd Ed.).* Mahwah, New Jersey: Lawrence Erlbaum.

Sümer, N. (2000). Yapısal eşitlik modelleri. *Türk Psikoloji Yazıları, 3*(6), 49-74.

Swaminatha, M. ve Elden, C. R. (2003). *Wireless security and privacy: Best practices and design techniques*. London: Addison-Wesley.

Symantec, (2013). *İnternet security threat report*. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf adresinden 22.12.2013 tarihinde edinilmiştir.

Şahin, Y. L. (2005). *İnternet'te güvenlik ve saldırı sezme sistemleri.* Yayımlanmamış Yüksek Lisans Tezi, Anadolu Üniversitesi, Fen Bilimleri Enstitüsü, Eskişehir.

Şahinaslan, E., Kantürk, A., Şahinaslan, Ö. ve Borandağ, E. (2009). Kurumlarda bilgi güvenliği farkındalığı, önemi ve oluşturma yöntemleri. *XI. Akademik Bilişim Konferansı*, 11-13 Şubat 2009, Harran Üniversitesi, Şanlıurfa.

Şahinaslan, Ö., Şahinaslan, E., Borandağ, E. ve Şahinaslan, A. M. (2013). Güvenli bir toplum için son kullanıcı siber güvenliği. *XV. Akademik Bilişim Konferansı,* 23-25 Ocak 2013, Akdeniz Üniversitesi, Antalya.

Tabachnick, G. B. ve Fidell, L. S. (2001). *Using multivariate statistics (4th Ed.).* USA: Allyon and Bacon Press.

Tavşancıl, E. (2006). *Tutumların ölçülmesi ve SPSS ile veri analizi.* Ankara: Nobel Yayın Dağıtım.

Tekerek, M. (2008). Bilgi güvenliği yönetimi. *KSÜ Fen ve Mühendislik Dergisi, 11*(1), 132.

Tekerek, M. ve Tekerek, A. (2013). A research on students' information security awareness. *Turkish Journal of Education, 2*(3), 61-70.

Thompson, B. (2004). *Exploratory and confirmatory factor analysis: Understanding concepts and applications.* Washington, DC: American Psychological Association.

Toğuz, Ö. (2010). *Avrupa Birliği ve Türkiye'de kişisel verilerin korunması ve fikri mülkiyet.* Yayımlanmamış Yüksek Lisans Tezi, Ortadoğu Teknik Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara.

Turhan, M. (2010). *Siber güvenliğin sağlanması, dünya uygulamaları ve ülkemiz için çözüm önerileri*. Uzmanlık Tezi, Bilgi Teknolojileri ve İletişim Kurumu, Ankara.

Tümer, S. (2010). *Kamuda iç kontrol sistemi ve uygulama aşamaları*. Ankara: Güncel Mevzuatı Araştırma Derneği Yayınları.

Türk Dil Kurumu, TDK. (2015). *Güncel Türkçe sözlük.* http://www.tdk.gov.tr/ adresinden 30.01.2015 tarihinde edinilmiştir.

Türkiye İstatistik Kurumu (2014). *Sürdürülebilir kalkınma göstergeleri, 2012-2013.* http://www.tuik.gov.tr/HbPrint.do?id=16124 adresinden 22.02.2015 tarihinde edinilmiştir.

Ulaşanoğlu, M. E., Yılmaz, R. ve Tekin, M. A. (2010). *Bilgi güvenliği: Riskler ve öneriler.* Bilgi Teknolojileri ve İletişim Kurumu, Ankara.

Ursavaş, Ö. F., Şahin, S. ve McIlroy, D. (2014). Öğretmenler için teknoloji kabul ölçeği: Ö-TKÖ. *Eğitimde Kuram ve Uygulama, 10*(4), 885-917.

Uzun, A. ve Sadioğlu, Ö. (2013). Sınıf öğretmenlerinin Fatih projesi ve proje kapsamında dağıtılacak tablet bilgisayarlara ilişkin görüşleri. *VII. Uluslararası Bilgisayar ve Öğretim Teknolojileri Sempozyumu*, 6-8 Haziran 2013, Erzurum.

Vural, Y. (2007). *Kurumsal bilgi güvenliği ve sızma (Penetrasyon) testleri.* Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.

Vural, Y. ve Sağıroğlu, Ş. (2008). Kurumsal bilgi güvenliği ve standartları üzerine bir inceleme. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 23*(2), 507-522.

Yalman, Y. ve Ertürk, İ. (2009). Kişisel bilgi güvenliğinin sağlanmasında steganografi biliminin kullanımı. *Bilgi Çağında Varoluş: "Fırsatlar ve Tehditler" Sempozyumu,* 1-2 Ekim 2009, Yeditepe Üniversitesi, İstanbul.

Yan, Z. (2009). Differences in high school and college students' basic knowledge and perceived education of Internet safety: Do high school students really benefit from the children's Internet protection act? *Journal of Applied Developmental Psychology, 3,* 209-217.

Yavanoğlu, U., Sağıroğlu. Ş. ve Çolak. İ. (2012). Sosyal ağlarda bilgi güvenliği tehditleri ve alınması gereken önlemler. *Politeknik Dergisi, 15*(1), 15-27.

Yıldırım, A. ve Şimşek, H. (2013). *Sosyal bilimlerde nitel araştırma yöntemleri (9. Baskı).* Ankara: Seçkin Yayıncılık.

Yılmaz, V. ve Çelik, H. E. (2009). *Lisrel ile yapısal eşitlik modellemesi-I.* Ankara: Pegem Akademi.

Yurdakul, C. ve Çağlayan, M. U. (1997). *Bilgi teknolojileri Türkiye için nasıl bir gelecek hazırlamakta?* Ankara: Türkiye İş Bankası Kültür Yayınları.