# ÜNİVERSİTE ÖĞRENCİLERİNİN BİLGİ GÜVENLİĞİ KAZANIMLARININ, FARKINDALIKLARI ÜZERİNDEKİ ETKİLERİNİN ANALİZİ: AFYON KOCATEPE ÜNİVERSİTESİ ÖRNEĞİ

YÜKSEK LİSANS TEZİ

Atılgan ERDOĞMUŞ

DANIŞMAN

Doç. Dr. Sinan SARAÇLI

İNTERNET VE BİLİŞİM TEKNOLOJİLERİ YÖNETİMİ

Haziran, 2017

Bu tez çalışması 16.KARIYER.125 numaralı proje ile
Afyon Kocatepe Üniversitesi BAPK tarafından desteklenmiştir.

**AFYON KOCATEPE ÜNİVERSİTESİ**
**FEN BİLİMLERİ ENSTİTÜSÜ**

**YÜKSEK LİSANS TEZİ**

# ÜNİVERSİTE ÖĞRENCİLERİNİN BİLGİ GÜVENLİĞİ KAZANIMLARININ, FARKINDALIKLARI ÜZERİNDEKİ ETKİLERİNİN ANALİZİ: AFYON KOCATEPE ÜNİVERSİTESİ ÖRNEĞİ

**Atılgan ERDOĞMUŞ**

**DANIŞMAN**
**Doç. Dr. Sinan SARAÇLI**

**İNTERNET VE BİLİŞİM TEKNOLOJİLERİ YÖNETİMİ**

**Haziran, 2017**

## TEZ ONAY SAYFASI

Atılgan ERDOĞMUŞ tarafından hazırlanan "Üniversite Öğrencilerinin Bilgi Güvenliği Kazanımlarının, Farkındalıkları Üzerindeki Etkilerinin Analizi: Afyon Kocatepe Üniversitesi Örneği" adlı tez çalışması lisansüstü eğitim ve öğretim yönetmeliğinin ilgili maddeleri uyarınca 16/06/2017 tarihinde aşağıdaki jüri tarafından oy birliği ile Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü **İnternet ve Bilişim Teknolojileri Yönetimi Anabilim Dalı'nda YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

**Danışman** : Doç. Dr. Sinan SARAÇLI

**Başkan** : Doç.Dr. Halit Eray ÇELİK
Van Yüzüncüyıl Üniversitesi Fen-Edebiyat Fakültesi

**Üye** : Doç.Dr. Sinan SARAÇLI
Afyon Kocatepe Üniversitesi Fen-Edebiyat Fakültesi

**Üye** : Yrd.Doç.Dr. Mehmet Eyüp KİRİŞ
Afyon Kocatepe Üniversitesi Fen-Edebiyat Fakültesi

Afyon Kocatepe Üniversitesi
Fen Bilimleri Enstitüsü Yönetim Kurulu'nun
...../...../..... tarih ve
..... sayılı kararıyla onaylanmıştır.

.....
Prof. Dr. Hüseyin ENGİNAR

**BİLİMSEL ETİK BİLDİRİM SAYFASI**
**Afyon Kocatepe Üniversitesi**

**Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında;**

- Tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- Görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- Başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- Atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- Kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- Ve bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

**beyan ederim.**

**16/06/2017**

**İmza**
**Atılgan ERDOĞMUŞ**

**ÖZET**
Yüksek Lisans Tezi

ÜNİVERSİTE ÖĞRENCİLERİNİN BİLGİ GÜVENLİĞİ KAZANIMLARININ, FARKINDALIKLARI ÜZERİNDEKİ ETKİLERİNİN ANALİZİ: AFYON KOCATEPE ÜNİVERSİTESİ ÖRNEĞİ

Atılgan ERDOĞMUŞ
Afyon Kocatepe Üniversitesi
Fen Bilimleri Enstitüsü
İnternet ve Bilişim Teknolojileri Yönetimi Anabilim Dalı
**Danışman:** Doç. Dr. Sinan SARAÇLI

Ham verinin işlenip yorumlanması sonucunda ortaya çıkan meta, şeklinde tanımlanan bilgi, insanlık tarihi boyunca önemli bir yere sahip olmuştur. Gelişen teknoloji ve insanların değişen ihtiyaçları sonucu bilginin miktarında meydana gelen artış, onun dijital sistemlerde depolanarak, bu sistemler aracılığıyla iletilmesi ve paylaşılması sonucunu doğurmuştur. Bu sonuç, kötü niyetli kişilerin iştahını kabartarak, bilgiyi ele geçirmeye yönelik tehdit çeşitliliğinin artmasına neden olmuştur. Bu tehditler, genellikle savunmasız ve bilinçsiz kullanıcıları hedef aldığından, toplumun bilgi güvenliği kazanımları ve farkındalıklarının artırılması, tehditlere karşı alınacak önlemlerin başında gelmektedir.

Bu araştırmada, üniversite öğrencilerinin, bilgi güvenliğine yönelik kazanımları ve farkındalıkları belirlenerek, demografik özelliklerine göre farklılık gösterip göstermediği araştırılmış, genel güvenlik bilgileri ile farkındalıkları arasındaki ilişkiler, yapısal eşitlik modellemesi ile incelenmiştir.

Afyon Kocatepe Üniversitesi öğrencilerine uygulanan bir anket aracılığı ile derlenen verilerin analiz edilmesi sonucunda, öğrencilerin bilgi güvenliği farkındalıkları; internet güvenliği, sosyal medya kullanımı, internet tarayıcısı ile ağ güvenliği, şifre oluşturma ve sosyal medya tuzakları olmak üzere beş alt boyutta ortaya çıkarken, genel güvenlik bilgileri ise; tehditler ve önlemler olmak üzere iki alt boyutta ortaya çıkmıştır. Bilgi

güvenliği kazanımlarının cinsiyet, yaş ve internet kullanım yıllarına göre, bilgi güvenliği farkındalıklarının ise yaş, bölüm, sınıf ve internet ortamını güvenli bulup bulmamalarına göre anlamlı bir farklılık gösterdiği tespit edilmiştir. Diğer taraftan, kurulan modelden elde edilen sonuçlar bilgi güvenliği farkındalığı üzerinde en fazla etkiye sahip olan alt boyutun "İnternet Güvenliği" olduğunu göstermektedir.

**2017, xi + 64 sayfa**

**Anahtar Kelimeler:** Bilgi güvenliği, Bilgi güvenliği farkındalığı, Yapısal eşitlik modellemesi.

**ABSTRACT**

M.Sc Thesis

ANALYZING THE EFFECTS OF INFORMATION SECURITY ACHIEVEMENTS OF UNIVERSITY STUDENTS ON AWARENESS: AFYON KOCATEPE UNIVERSITY SAMPLE

Atılgan ERDOĞMUŞ

Afyon Kocatepe University

Graduate School of Natural and Applied Sciences

Department of Internet and Information Technologies Management

**Supervisor:** Assoc. Prof. Sinan SARAÇLI

Notion of information as the meaning of processing the raw data has been an important for the people until the past. Related with the developing technology and the changed requirements of the people, the increase of the amount of the information is resulted as keeping it in digital systems and transferring and sharing via these systems. This result caused to increase the variety of threats to capture the information by malevolent people heartsomely. Because these threats target the defenseless and unconscious people, increasing the information security achievements and awareness of the society is the most important precaution for the threats.

In this study, its analyzed whether the achievements and awareness differ for the demographic features and relations between these achievements and awareness are modeled via Structural equation modeling by determining the university students' achievements and awareness towards information security.

As the result of analyzing the data, obtained from the students via a questionnaire at Afyon Kocatepe University, the information security awareness of the students is formed in five subdimensions as; internet security, social media usage, internet browser and network security, password generation and social media traps while the general security knowledge is formed in two subdimensions as threats and precautions. Its

determined that the general security knowledge of the students differs for their gender, age and internet using experiences while information security awareness differs for their age, department, class and whether they think that the internet is safe or not. On the other hand, the results of the models indicate that the most effective sub dimension on "internet security awareness" is "internet security".

**2017, xi + 64 pages**

**Key Words:** Information security, Information security awaresness, Structural equation modeling.

# TEŞEKKÜR

Bu araştırmanın konusu, deneysel çalışmaların yönlendirilmesi, sonuçların değerlendirilmesi ve yazımı aşamasında yapmış olduğu büyük katkılarından dolayı tez danışmanım Sayın Doç. Dr. Sinan SARAÇLI'ya, 16.KARIYER.125 numaralı proje ile araştırmayı destekleyen Afyon Kocatepe Üniversitesi BAPK'ne, araştırma boyunca her konuda yardımlarını esirgemeyen müdürüm Sayın Dr. Murat PEDER'e ve manevi desteklerinden dolayı eşim Başak ERDOĞMUŞ kızım Duru ve oğlum Destan'a teşekkürü bir borç bilirim.

Atılgan ERDOĞMUŞ
AFYONKARAHİSAR, 2017

# İÇİNDEKİLER DİZİNİ

**Sayfa**

## SİMGELER ve KISALTMALAR DİZİNİ

| **Kısaltmalar** | |
|---|---|
| AFA | Açıklayıcı Faktör Analizi |
| DFA | Doğrulayıcı Faktör Analizi |
| YEM | Yapısal Eşitlik Modeli |
| BGK | Bilgi Güvenliği Kazanımı |
| BGF | Bilgi Güvenliği Farkındalığı |

## ŞEKİLLER DİZİNİ

**Sayfa**

# ÇİZELGELER DİZİNİ

**Sayfa**

# 1. GİRİŞ

Bilgi, tarih boyunca "güç" kelimesi ile yanyana kullanılmış, bu gücün farkında olup, bilgiyi analiz ederek, doğru çıkarımlara ulaşanlar ise daima rakiplerinin bir adım önünde yer almıştır. Zaman ilerledikçe, bilgiye dayalı rekabetçi avantajı yakalayıp sürdürebilen, bilgi birikimi ile paylaşımını sermaye haline getiren toplumlar ve kurumların başarıya ulaştıkları görülmektedir (Güçlü ve Sotirofski 2006). Yani bilgi, güç ve başarıya ulaşmak için en önemli anahtardır. Bu nedenle, uygun koşullarda saklanması ve doğru bir şekilde korunması gerekmektedir. Ancak zaman içerisinde bilginin yoğunluğunda meydana gelen artış, verinin saklanmasını, erişimini, analizini, paylaşımını ve güvenliğini zorlaştırmıştır. Bu sorunların önüne geçebilmek için yapılan çalışmalar neticesinde elektronik sistemler geliştirilmiştir. Bu sayede, daha çok bilgi daha küçük cihazlar üzerinde saklanabililir, daha hızlı bir şekilde iletilebilir ve paylaşılabilir hale gelmiştir. Bilginin 0 ve 1'lere dönüşerek sanal ortama girmesi, bilişim ve iletişim teknolojilerinin gelişiminde hızlı bir değişim ve dönüşüm yaşanmasına neden olmuştur. Meydana gelen değişimle birlikte önce internet, daha sonra da akıllı cihazlar hayatımıza girmiş, iki teknolojinin beraber kullanılması sonucu da insanların bilgiye erişimi kolaylaşarak, istedikleri zaman ve mekanda yetkileri bulunan veriye erişebilmelerinin yolu açılmıştır (Vural 2007). Bu durum "mobil yaşam" kavramını hayatımızın içerisine yerleştirmiş, gün geçtikçe artan tüketici talepleri ve bu talebi karşılamaya çalışan teknoloji üreticilerinin girdiği büyük rekabet sonucu ise iş ve sosyal yaşamın her noktasına nüfuz ederek, günlük hayatımızın vazgeçilmez bir parçası haline getirmiştir.

Bilişim kültürünün, toplum yaşantısındaki hayatı kolaylaştırması, uzaklıkları kısaltması ve verimi artırması gibi önemli ve azımsanmayacak etkileri vardır. Ancak bu avantajlardan yararlanılabilmesi için bireylerin, hızlı teknolojik gelişmelerle giderek karmaşıklaşan toplum yaşamına ayak uydurup, çağdaş bilgi ve becerilerle kendilerini donatması gerekmektedir (Mart 2012). Yani, artık sadece okuma-yazma becerisi bilgiye erişim noktasında tek başına yeterli olmamakta, akıllı cihazlar ve içerdiği yazılımların etkin kullanımı için gerekli olan teknolojik okur yazarlığa da sahip olunması gerekmektedir.

Günümüzde özellikle gençler günlük aktivitelerinin büyük bir kısmında akıllı teknolojik cihazları sık sık kullanmaktadır (Aslandağ 2010). Bu teknolojiler, bireylerin günlük hayatlarını planlamalarında, birbirleri ile iletişim kurmalarında ve bilgi paylaşımında sanal ortamın sağladığı hız ve kolay erişililebirlik gibi avantajlar sebebiyle tercih edilmektedir. Ancak bilişim teknolojileri, sosyal yaşamda sağladığı kolaylıkların yanında bir takım sorunları da beraberinde getirmektedir. Bu sorunların başında, sanal dünyaya bağımlı hale gelen bireylerin gerçek yaşamdan uzaklaşmaları gelmektedir. Gerçek hayattan uzaklaşan bireyler, antisosyal bir yaşam tarzı benimseyerek, sanal ve gerçeklik kavramları arasında bilinçsel karmaşa yaşayabilmektedir. Bununla beraber, internet ortamında faydalı içerikler gibi, zararlı içeriklere de erişimin kolay olması nedeniyle, bu içeriklere daha fazla maruz kalınması, her yaştaki bireyin kişisel gelişiminin olumsuz yönde etkilenmesine, bir takım kötü alışkanlıklar edinilmesine, kişilik bozukluklarına ve yasal olmayan faaliyetler içerisinde yer almalarına da neden olabilmektedir.

Teknolojik cihaz kullanımının olumsuz yönlerinden bir tanesi de bilgi güvenliğine yönelik risk faktörlerinin genişlemesine olan etkisidir. Gelişen teknoloji ve akıllı cihazların bilinçsiz kullanımı, bilgi güvenliğine yönelik tehdit ve saldırı yöntemlerinin çeşitlenmesine, bunun doğal sonucu olarak ta bu tehditlere karşı alınacak önlemlerin zorlaşmasına neden olmaktadır (Çetin 2014).

Sahip olduğu bilgiyi korumak isteyen bireyler ve kurumlar, sorunun çözümünü sürekli yanlış yerde arayarak, genellikle teknoloji temelli çözümlere yönelmişlerdir. Bu durum, para ve zaman kaybına neden olmuş, ayrıca risklerin tam anlamıyla bertaraf edilmesini de sağlayamamıştır. Oysa bu teknolojileri kullanan ve yöneten insanlardır ve bu bireylerin büyük çoğunluğu, bilgi güvenliğine karşı oluşabilecek risk ve tehditlerin farkında bile değillerdir (Güldüren *et al.* 2016; Keser ve Güldüren 2015). Farkındalıkları gelişmemiş bireyler, kendileri açısından paylaşmalarında sakınca görmedikleri, ancak başkalarınca elde edilmesi halinde farklı amaçlar için kullanılabilecek, kişisel veya bağlı bulundukları kurumlara ait verilerini, çoğu zaman farkında bile olmadan günlük sosyal yaşamlarında etrafındaki kişilerle veya dijital sosyal ortamlarda herkesin görebileceği bir şekilde paylaşmaktadır. Bunun bilincinde

olan kötü niyetli kişiler, sistemin açıklarını aramak yerine, insanların zafiyetlerini kullanarak hem daha kolay hemde daha az riskli bir şekilde istediklerine ulaşabilmektedir. Görüldüğü üzere bilgilerimiz heran risk altındadır ve onu ele geçirmek isteyenler pusuya yatmış bizim hata yapmamızı beklemektedir. Bizim ise, sadece ağzımızı sıkı tutarak veya dijital olmayan ortamlardaki verilerimizin fiziki güvenliğini sağlayarak bilgimizi koruyamayacağımızı, bununla birlikte akıllı cihazlarımıza hükmeden parmaklarımızı kullanırken de daha dikkatli olmamız gerektiğinin bilincinde olmamız ve bu duruma uygun hareket etmemiz gerekmektedir.

Hızla değişen ve gelişen bilişim kültürü içerisinde, günümüzde bu teknolojileri en çok kullanan, olumlu ve olumsuz yönlerine en fazla maruz kalan gençlerin bilgi güvenliği konusunda bilinçlendirilmesi, gelecek nesillere daha güvenli dünya bırakmak açısında önemlidir. Bu gereklilikten hareket edilerek bu çalışma, üniversite öğrencilerinin bilgi güvenliğine yönelik kazanımları ve farkındalıklarının belirlenmesi, demografik özelliklerine göre farklılık gösterip göstermediğinin araştırılması ve bilgi güvenliği konusundaki kazanımlarının farkındalıkları üzerinde ne yönde ve ne derece etkili olduğu tespit edilmesi amacıyla yapılmıştır.

# 2. LİTERATÜR BİLGİLERİ

## 2.1. Literatür Taraması

Rençber ve Mete (2016), yüksekokul öğrencilerinin bilgi güvenlik farkındalığı davranışlarını etkileyen faktörler ve bu faktörlerin etki düzeylerini incelemişlerdir. Çalışmanın sonucunda bilgi güvenlik farkındalığını en çok etkileyen faktörlerin şifre yönetimi, mobil internet kullanımı, e posta ve internet kullanımı ve sosyal ağ sitelerinin kullanım davranışları olduğu sonucuna ulaşmışlardır.

Kapanoğlu (2016), öğretmenlerin interneti güvenli kullanım durumlarını ve bilgi güvenliği farkındalık düzeylerini araştırmıştır. Çalışma sonucunda, öğretmenlerin bilgi güvenliği farkındalık düzeylerinin "orta düzeyde" olduğu sonucuna ulaşmıştır. Ayrıca, bilgi güvenliği farkındalıklarının branşlara, alınan bilgi güvenliği eğitimine, öğrenim durumuna, yaşanılan bölgeye, internet kullanım süresine ve yaşa göre anlamlı farklılıklar gösterdiğini tespit etmiştir.

Mart (2012), bireylerin, gelişen bilgi ve iletişim teknolojileri ile bilişim kültürüne ne kadar adapte olduklarını ve bu kültürün içinde bilgi güvenliği farkındalıklarını araştırmıştır. Çalışmada; katılımcıların teknoloji kullanımları arasında yaşları ile bilgisayar ve internet kullanım sürelerine göre anlamlı bir fark olduğu, cinsiyetlerine, eğitim durumlarına ve mesleklerine göre ise anlamlı bir fark olmadığı belirtilmiştir. Katılımcıların bilgi güvenliği farkındalıkları arasında ise yaşlarına, cinsiyetlerine ve mesleklerine göre anlamlı bir farklılık olduğu görülürken, eğitim durumlarına, mesleklerine, bilgisayar ve internet kullanım sürelerine göre anlamlı bir farklılık olmadığını belirtmiştir. Ayrıca, katılımcıların bilişim kültürleri ile bilgi güvenliği farkındalıkları arasında zayıf düzeyde, pozitif ve anlamlı bir ilişki olduğu sonucuna ulaşmıştır.

Akgün ve Topal (2015), eğitim fakültelerinde öğrenim gören öğrencilerin bilişim güvenliği farkındalıklarını belirlemek amacıyla bir anket uygulamışlardır. Çalışma sonucunda, katılımcıların, bilişim güvenliği konuları ile ilgili farkındalıklarının yeterli

olmadığını belirtmişlerdir. Ayrıca cinsiyete ve ortalama bilgisayar-internet kullanım yılına göre anlamlı farklılıklar olduğu, bilişim güvenliği eğitimi aldığını belirten adaylar ile almayan adaylar arasında ise beklendiği gibi ciddi bir anlamlı farklılık olmadığı sonucuna ulaşmışlardır. Öğretmen adayları için kapsamı iyi belirlenmiş bir bilişim güvenliği eğitimi verilmesi önerisinde bulunmuşlardır.

Çetin (2014), kişisel veri güvenliği ve farkındalıkları üzerine yapmış olduğu çalışmasında, kişilerin bilgi güvenlik algıları, kullandıkları elektronik cihaz türleri ve cihazlardaki bilgi güvenliği adına aldıkları önlemler ile kullandıkları yöntemleri incelemiş ve "Kişisel Veri Güvenliği Farkındalığı" anketi geliştirmiştir. Analiz sonuçlarına göre; katılımcıların bilgi güvenliği noktasında farkındalık düzeylerinin ortalamanın üstünde olduğu belirlenmiş, kişisel veri paylaşımı farkındalık düzeyinin diğer farkındalık düzeylerine göre en yüksek olduğu tespit edilmiştir.

Güldüren vd. (2016), ortaöğretim kurumlarında öğrenim gören öğrencilerin bilgi güvenliği farkındalık düzeylerini belirlemeye yönelik bir ölçek geliştirmişlerdir. Ölçek, 36 madde ve 3 alt boyuttan (saldırı ve tehditler, mahremiyet, kişisel verilerin korunması) oluşmaktadır. Geliştirilen ölçek üzerinde yapılan analizler sonucunda öğrencilerin bilgi güvenliği farkındalıkları ile cinsiyetleri arasında anlamlı bir farklılığın olduğunu belirtmişlerdir.

Karadağ ve Abuhanoğlu (2015), Gülhane Askeri Tıp Fakültesi Eğitim Hastanesinde görevli personelin bilgi güvenliği konusundaki farkındalık düzeylerinin değerlendirilmesi ve bunun sosyo-kültürel özelliklere göre farklılık gösterip göstermediğinin belirlenmesi amacıyla bir ölçek geliştirmişlerdir. Ölçek, bilgi güvenliği farkındalığını; politika güvenliği, sistem güvenliği ve çalışan güvenliği olarak üç alt ayırmıştır. Araştırma sonuçlarına göre; bilgi güvenliği farkındalık düzeyi % 89.7 olduğu, ayrıca yaş ve unvan değişkenlerinin bilgi güvenliği farkındalığı üzerinde anlamlı etkiye sahip olduğu saptanmıştır.

Keser ve Güldüren (2015), yükseköğretim kurumlarında çalışan öğretim elamanlarının bilgi güvenliği farkındalık düzeylerini belirlemeye yönelik bir ölçek geliştirmişlerdir.

Ölçek, 34 madde ve 2 alt boyuttan (“saldırı ve tehditler” ile “kişisel verilerin korunması” ) oluşmaktadır.

Tekerek ve Tekerek (2013), ilköğretim ve lise öğrencilerinin bilgi ve bilgisayar güvenliği farkındalık düzeylerini belirlemek amacıyla bir ölçek uygulamışlardır. Araştırma sonuçlarına göre, öğrencilerin etik konulardaki bilgi güvenliği farkındalık düzeylerinin yeterli seviyede olduğu, ancak kurallar ve bilgi gerektiren konularda farkındalık düzeylerinin düşük olduğunu tespit etmişlerdir.

Yılmaz vd. (2016), öğretmenlerin dijital veri güvenliği farkındalıklarının belirlenmesine yönelik bir ölçek geliştirmiştir. Ölçek 32 madde ve tek faktörden oluşmaktadır. Araştırma sonucuna 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 farklılık gösterdiğini tespit etmiştir.

Bostan ve Akman (2011), bilişim güvenliği farkındalığının belirlenmesine yönelik bir anket çalışması yapmıştır. Anketteki sorular bilgi ve iletişim teknolojileri kullanımı, kişisel bilgisayar kullanımında gerçek hayat uygulamaları, güvenli web kullanımında farkındalık ve davranış alışkanlıkları olmak üzere dört ana başlık altında gruplandırılmıştır. Araştırma sonuçlarına göre yapılan tespitlerde en öne çıkan husus yaş ilerledikçe bilgisayar güvenliği konusunda hassasiyet azalmasına karşılık web güvenliği konusunda farkındalık ve duyarlılığın artmasıdır. Benzer şekilde kadınların bilgisayar güvenliğine erkeklerden daha çok dikkat ettikleri, erkeklerinse web güvenliğinde kadınlardan daha dikkatli davrandıklarını tespit etmişlerdir.

Parsons vd. (2013), organizasyonlarda bilgi güvenlik farkındalığı konusunda çalışanların durum tespitini belirlemek amacıyla bir ölçek geliştirmişlerdir. Ölçek; şifre yönetimi, e-posta kullanımı, internet kullanımı, sosyal ağ kullanımı, hata raporlama, mobil bilgisayar kullanımı ve bilgileri elden geçirme faktörlerinden oluşmaktadır. Tüm faktörler arasında anlamlı ve pozitif bir ilişki tespit etmişlerdir.

## 2.2. Bilgi Kavramı

Bilgi; ezelden beri insanların ve organizasyonların düşüncesini, yaşayışını, davranışını, gelişimini ve stratejilerini belirleyen etmenlerin başında gelmiş olup, önemini yaşamın çeşitli alanlarında, politikada, sanatta, iş yaşamında, eğitimde vs. günümüze kadar artırarak sürdürmüştür (Demirtaş 2013; Odabaş 2005). Bilginin aktarılmasında ilk çağlardan başlayarak hikâyeler, masallar, destanlar aracı olmuş ve 12. yüzyıldan sonra da üniversiteler, medreseler ve kitaplar önemli roller üstlenmişlerdir. Ancak, son dönemde iletişim ve işbirliğini son derece kolaylaştıran bilişim teknolojilerinin hayatımıza girmesi ve hızlı bir şekilde yaygınlaşmasıyla bilginin yönetilmesi, iş verimliliğinin ve akışlarının hızlandırılması, çalışanlar ve diğer kurumlarla daha hızlı iletişim kurulabilmesi sağlanmış, hayatımız kolaylaşmış, üretilen ve tüketilen bilgilerde de artışlar olmuştur. Elektronik ortamlarda bilginin işlenmesi, taşınması ve saklanması kolaylaşarak, bilgiye zamandan ve mekândan bağımsız olarak istenilen ortamlardan ve istenilen zamanlarda erişilmesi sağlanmıştır (Vural 2007).

Bilginin üretilme, depolanma, korunma, kullanılma, paylaşma, yayılma, etkileşme ve artma hızı, teknolojinin getirdiği hızlı bilgi işleme ve iletişim araçları ile baş döndürücü bir hal almıştır. Günümüz insanı, günlük yaşamında bile gerekli, gereksiz çok fazla sayıda bilgiyle muhatap olmaktadır. Bu kafa karıştırıcı durumdan kurtulmak için bilgiye erişimde seçici yöntemler kullanılarak doğrudan ulaşılmak istenilen bilgiye eriştirecek yöntemler geliştirilmelidir. Bir başka önemli konu da bilginin taşıdığı değerdir. Bilginin değerli veya değersiz olduğunu belirlemek veya bilginin taşıdığı değeri ölçmek, en az bilginin kendisi kadar önemlidir. Elde edilen bilgiyi değerlendirirken bilginin kalitesini gösteren özelliklere bakılması gerekir. Doğruluk, güncellik, konuyla ilgili olma, bütünlük ve öz, gereksinimlere uyum gösterme, iyi sunulma, fiziksel ve idrak yolu ile erişim gibi ölçütler bilginin kalitesini belirleyen etmenlerden bazılarıdır (Canbek 2005).

Süreç içerisinde meydana gelen teknolojik değişim ve dönüşümle beraber insanlar ile organizasyonların geleceğe yönelik planları ve stratejilerinde bir takım değişiklikler yapma ihtiyacı doğmuş, bu ihtiyaca karşılık veremeyenlerin ise özel hayatlarında veya bulundukları sektörde rekabetin gerisinde kaldıkları görülmüştür (Odabaş 2005). Bu

nedenle; tarım toplumundan bilgi toplumuna geçişle birlikte ekonomik bir değer ve güç haline gelen bilgi, üretime ve işletmelerin gelişmesine etki eden önemli olgulardan biri olarak, bu değere sahip olanların ellerindekini geliştirip, yeni değerler üretmesi ile birlikte, rakiplerinin bir adım önlerine geçmelerinin en önemli unsuru haline gelmiştir (Atılgan 2009; Demirtaş 2013).

Bilginin zaman içerisindeki yolculuğunda ona verilen önemde meydana gelen artış sonucunda sürekli olarak yeniden tanımlanmak zorunda kalmış ve anlamı günün gerekliliklerine göre belirlenmiştir. Öyle ki, 1950'lerde bilgi organizasyonlar için sadece bürokratik bir zorunluluk iken, 1990'lara gelindiğinde rekabet avantajı sağlayacak stratejik bir kaynak olarak ortaya çıkmıştır. Bu süreçte, organizasyonların en değerli varlığı çalışanların sahip olduğu bilgi haline gelmiş, bu nedenle de yapısal sermayelerinin yanında insan sermayesine de odaklanarak, organizasyon bilgisinin dışında çalışanların bilgisini de geliştirmeye çalışmışlardır (Atılgan 2009).

Bilgi, tüm organizasyonlar ve insanlar için gelişim ile değişimin kaynağı olarak görüldüğünden ve eğitim hayatından, çalışma hayatına, özel hayattan, kamusal hayata kadar her aşamada aktif rol oynadığından doğru anlamı vererek tanımlamak ve kavramak bundan sonraki süreçte ileriye yönelik gelişimimizi şekillendirmenin en önemli anahtarı olacağı değerlendirilmektedir (Canbek ve Sağıroğlu 2006; Durna ve Demirel 2008). Buradan hareketle Çoban (1996) bilgiyi; belli bir formda işlenmiş ve alan için anlamlı olan, hâlihazırdaki ve gelecekteki kararlar için anlam ifade eden, algılanan veya gerçek değeri olan veri şeklinde tanımlamıştır. Kısaca veri, davranışları etkilediği zaman bilgi olmaktadır. Ghaziri and Elias (2004)'a göre ise bilgi, "tecrübe veya çalışma yoluyla kazanılmış anlayıştır. Aynı zamanda, gerçeklerin birikimi veya kuraldır. Bilgi spesifiktir, bir problem alanından diğerine transfer edilemez, belli bir zamanda kullanılır ve daha sonra o bilgiye ihtiyaç duyulmayabilir. Bilgi; değerlere, inançlara ve güvene bağlıdır. Bilgi, başarılı deneyimlerle gelişir ve sonra da bu tecrübe uzmanlığa dönüşür" (Güçlü ve Sotirofski 2006). Bazen bilgi kesin bir anlam ifade etmeyebilir. Bir karar için anlamlı olan bilgi, başka bir değerlendirme için ham veri olabilir. Bu yüzden, kullanılacak olan kişiye bağlı olarak bilgi ve veri birbirinin yerini alacak şekilde kullanılabilir. Herhangi bir uzman için bilgi olan bir değer, kurumun üst

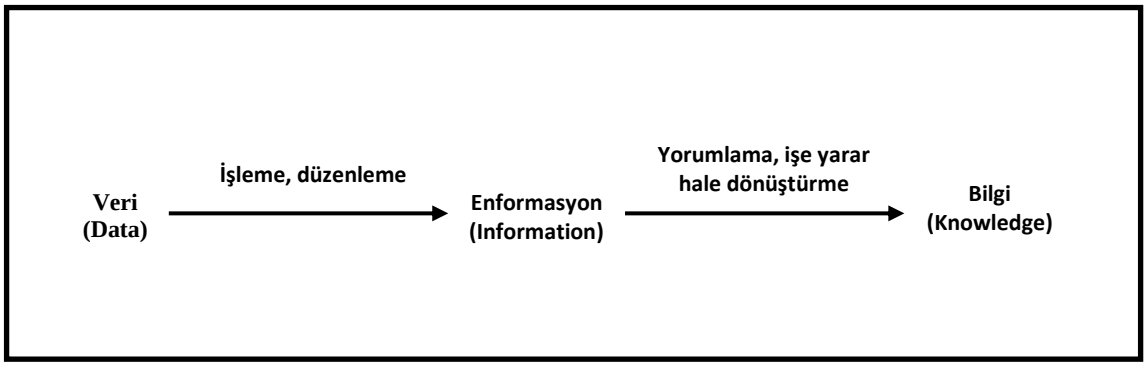
yöneticisi için ham veri anlamına gelebilir (Demirtaş 2013).

Türk Dil Kurumu güncel Türkçe sözlüğünde ise bilgi; insan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, bilim, malumat, öğrenme, araştırma ve gözlem yoluyla elde edilen her türlü gerçek, malumat, vukuf, insan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü, malumat, vukuf. Genel olarak ve ilk sezi durumunda zihnin kavradığı temel düşünceler olarak tanımlanmaktadır (İnt.Kyn.1).

### 2.3. Bilgiyi Oluşturan Temel Unsurlar

Bilginin oluşturulması sürecinde yüklendiği değerler yönüyle aktif rol oynayan bir takım bileşenler vardır ve bu bileşenler birbirleriyle doğrudan ilişkilidir. Bu ilişki sebebiyle de birbirleriyle sık sık karıştırılabilmektedir. Oysaki gerçekte, her bir kavramın anlam ve kullanım amacı bir birinden oldukça farklı olup, bu kavramların kullanım amacı ve yerini tespit etmek bilgiye ve yönetimine daha doğru bir anlam kazandıracaktır. Bu yüzden; karmaşık ilişkileri birbirinden ayırarak, kavramların sahip oldukları kendilerine özgü anlamlarını ve sınırlarını belirlemek, kavramsal kargaşayı ortadan kaldırmak ve doğru kullanımlarını sağlamak adına önemlidir (Durna ve Demirel 2008; Eminağaoğlu ve Gökşen 2009; Odabaş 2005).

Birbirleriyle karıştırılan bu bileşenler, bilginin kendisini ifade etmek için kullanılan veri (data), enformasyon (information) ve bilgi (knowledge) kavramlarıdır. Bilgi toplumu olgusu ile birlikte bu oluşuma büyük oranda zemin hazırlayan ve neden olan bu kavramlar hakkında uzun ve çok boyutlu tartışmalar yapılmıştır. Türkçe literatüre bakıldığında özellikle bilgi ve enformasyon kavramlarının henüz tam anlamıyla sınırlarının belirlenemediği, bu iki terim arasında hala süregelen bir kavram kargaşasının yaşandığı ve çoğu zaman bu iki kavramın birbirlerinin yerine kullanıldığı görülmektedir. İngilizce yazılmış yabancı literatürde bilginin karşılığı olarak knowledge, enformasyonun karşılığı olarak da information sözcüğünün kullanılmaktadır. Ancak Türkçeye çevrilirken çoğu zaman iki sözcükte bilgi olarak çevrilmesi, birtakım karışıklıkların meydana gelmesine sebep olmuştur (Yılmaz 2009).




**Şekil 2.1** Bilginin Oluşum Süreci (Güçlü ve Sotirofski 2006)

Veri, enformasyon ve bilgi kavramlarından birinin ne olduğunu anlayabilmek için öncelikle ilişkili diğer iki kavramın da ne olduğunun bilinmesi önemlidir; çünkü bu kavramlar birbirleriyle doğrudan ilişkilidir ve bir kavramın açıklanması çoğu zaman diğer kavramların açıklanmasını da gerektirmektedir. Bu ilişkiler bağlamında bu kavramlar daha detaylı bir şekilde açıklanmaya çalışılacaktır.

### 2.3.1 Veri

Veri, amaçlar doğrultusunda işlemlerin ham şekliyle kaydedilmesi, üzerinde çalışılmamış ve yorumlanmamış gözlemler, işlenmemiş kayıtlar olarak tanımlanabilir. (Barutçugil 2002). Bilişim teknolojisi açısından veri ise; bir durum hakkında, birbiriyle bağlantısı henüz kurulmamış bilinenler veya kısaca, dijital ortamlarda bulunan ve bu ortamlar aracılığı ile taşınan, sinyaller ve/veya bit dizileridir. (Canbek 2005).

Veri, herhangi bir problemin çözümünde veya bir konuda alınacak kararlarda kilit rol oynar. Fakat verilerden hareketle elde edilecek sonuçları değerlendirerek yorumlamak ve bu sonuçlara belli bir katma değer sağlamak tamamen bireylerin inisiyatifinde olan bir durumdur. Yani veri, enformasyon ve bilginin temelini oluşturan ancak, problemin çözümünde ve kararların alınmasında sebep sonuç ilişkisi kurmamıza tam anlamıyla yardımcı olamayan ham kayıtlardır. Bu nedenle alınacak kararlarda sadece veriler üzerinden hareket etmek, kişileri veya kurumları istenilen doğru sonuca götürmez (Durna ve Demirel 2008).

#### 2.3.1.1 Büyük Veri (Big Data)

Günümüzde internet teknolojileri sayesinde, elimizdeki cep telefonundan, mutfağımızdaki buzdolabına, kolumuzdaki akıllı saatten, salonumuzdaki televizyona kadar internete bağlı pek çok cihaz veri üretebilir hale gelmiştir. Bu durum; gerek bireylerin ve kurumların, gerekse de internet dünyasında saklanan veri büyüklüğünü her geçen gün artmasına neden olmaktadır. Veride meydana gelen artış ve bu verinin analiz edilerek başka amaçlar için kullanılabilirliğinin keşfi, büyük veri (big data) kavramının hayatımıza girmesini sağlamıştır. Kesin bir tanımı olmayan büyük veri kavramı, günümüzde son derece popüler bir hale gelmiş olup, yeni bir devrin başlangıcı olarak kabul edilmektedir. Yeni dönem ile birlikte; kurum, kuruluş ve devletlerin veriye olan bakışı ile veri üzerinden sağladıkları fayda artarak devam etmektedir. (Doğan ve Arslantekin 2016). Buradan da anlaşılacağı üzere, büyük veri sadece fiziksel olarak büyüklüğü ifade etmez. Bunun yanında verinin yüksek hızla, sürekli olarak ve çok farklı çeşitlerde üretilmesi ve üretilen bu verilerin analizinde elde edilen faydaları da kapsar. Bu durumu, Gartner şirketinin "3 V"yi kullanarak yapmış olduğu tarif güzel tanımlamaktadır: Büyük veri; "büyük miktar (volume), büyük hız (velocity) ve/veya büyük çeşitlilik (variety) özelliklerine sahip; karar verme yeteneklerimizi arttıracak, içgörü ve süreç optimizasyonunu geliştirecek yeni bilgi işleme biçimleri gerektiren enformasyon varlıklarıdır" (Gürsakal, 2014).

### 2.3.2. Enformasyon

Enformasyon, düzenlenmiş, organize edilmiş veri olarak da tanımlanabilir ve yalnızca düzenleme işlemini yapan ilgili kişi için bir anlam taşımaktadır (Barutçugil 2002). Enformasyonun amacı herhangi bir konu veya olay hakkında ilgili kişileri ön fikir sahibi yapmaktır. Yani mevcut ve olası duruma ilgililerin dikkatini çekmektir. Belli bir amaçla ilişkilendirilebilmesi için, enformasyonun bir dayanağı ve kaynağı olmak zorundadır. Fakat bu durum, enformasyonun alıcısı belli bir yorum ve ilave yapabiliyorsa gerçekleşebilir aksi takdirde ise ilgisiz anlam kazanır. Örneğin görsel ve işitsel kitle iletişim araçları enformasyona verilebilecek en önemli örneklerdendir. Çünkü bu araçlar bir amaç doğrultusunda, insanlar üzerinde belli etki yaparak onların

algılama ve kavrama özelliklerinde önemli değişikliklere yol açabilir. İletilen mesajın güçlülük ve zayıflık özelliğine bağlı olarak bireyler etkilenir. Enformasyonun zenginliği, oluşturulan içeriğe ve hedef kitleye ulaştırılacak iletişim kanallarına (doğrudan yüz yüze, internet, telefon, faks, TV vb.) bağlı olarak değişir. İçerik yönünden hiçbir anlam ifade etmeyen enformasyonun amaca uygunluğu düşünülemez. İletişim kanalı zayıf veya tutarlı değilse bu durum, enformasyonun niteliğini düşürür (Durna ve Demirel 2008).

Görüldüğü üzere; bilgi, veri ve enformasyon farklı anlamlara sahiptir. Veri ve enformasyon genel olarak olduğu gibi kabul edilebilirken, bilgiyi bu şekilde kabul edemeyiz. Bilgi, içeriğindeki anlam ile zenginleştiğinden, barındırdığı tartışmalara, yorumlara, deneyimlere, algılamalara yer vererek ve onlara ilaveler yaparak ele alınır. Bilgi mutlaka sebep-sonuç ilişkisi temeline dayanır. Bilgi, bazen bireysel kaynağa dayalı olarak ortaya çıkarken bazen de kolektif bir çalışmanın sonucu olarak ortaya çıkabilir (Durna ve Demirel 2008). Genelde veri, işlenmemiş (ham) enformasyon parçacıkları, enformasyon, organize edilmiş bir veri seti, bilgi ise, anlamlı (anlaşılabilir) enformasyonlar olarak tanımlanabilir (A. E. Akgün ve Keskin 2003).

## 2.4 Bilginin Sınıflandırılması

Bilginin ne olduğunu ve neye yaradığını daha iyi anlamak için belirli kriterlere göre sınıflandırılarak tanımlanması ve açıklanması yararlı olacaktır.

### 2.4.1 İçeriğine Göre Bilgi

İçeriğine göre bilgi, bireysel ve kurumsal olmak üzere ikiye ayrılmaktadır.

#### 2.4.1.1 Bireysel Bilgi

Bhatt (2001)'a göre bireysel bilgi, kurumsal bilgi tabanının gelişmesi için gerekli olan kişisel bilgi, beceri ve yetenekler (Odabaş 2005), Barutçugil (2002)'e göre ise, "insanın

geçmişte öğrendikleri ile deneyimlerinin bir toplamı" olarak tanımlamaktadır (Atılgan 2009).

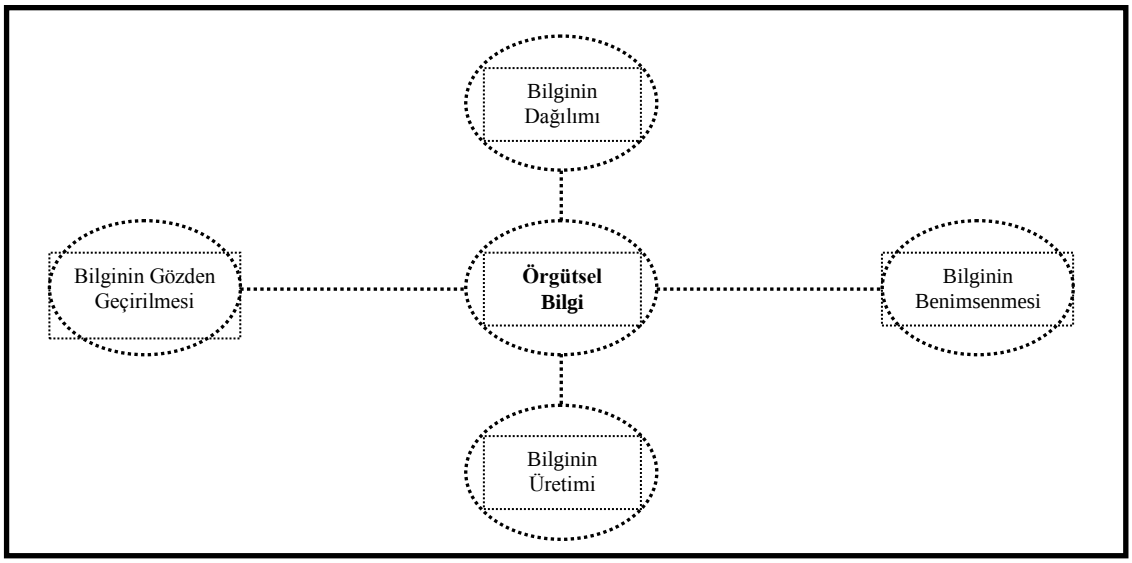
Ipe (2003)'ye göre bireysel bilgi, "organizasyon içinde belli bir bölümde yine belli bir kişiye ait olan bilgidir. Bu bilgi bireylerin bedensel becerileri ve zihinlerine yerleşmiş bilgilerinden oluşur. Bireysel bilgi, problemlerin çözümünde ve özel durumlarda herkesin sahip olduğu ve bireyler tarafından bağımsız olarak kullanılan bilgidir. Bu yönüyle bireysel bilgi kişiye ait özelleştirilmiş değerler bütünüdür" (Durna ve Demirel 2008). Bireysel bilgi, örgüt içinde belli bir bölümde yine belli bir kişiye ait olan bilgidir. Bu bilgi bireylerin bedensel becerileri ve zihinlerine yerleşmiş bilgilerinden oluşur (Durna ve Demirel 2008).

#### 2.4.1.2 Kurumsal Bilgi

Kurumsal bilgi; "kurumun etkinliği, denetimi, yönetimi, geliştirilmesi vb. ile ilgili olarak üretilen, alınan, kullanılan ve bu nedenle özel bir nitelik kazanan her türlü malumat, fikir ve olgulardır" (Özdemirci 2001). Bu olgular, kurumsal etkinliklerin ve gereksinimlerin bir sonucu olarak sistematik çalışma, araştırma ve geliştirme çalışmalarından kaynaklanmaktadır. Bireysel bilginin kurumsal bilgiye, kurumsal bilginin bireysel bilgiye dönüşümü bir döngü olarak varlığını her zaman korumaktadır. Bireylerin bilgi üretmedeki hız ve kapasiteleri kurumsal bilgi düzeyini belirlemede temel faktördür. Bireylerin bilgi üretimine etki eden faktör ise, bilginin etkin kullanımıdır. Kısaca kurumsal bilgi kavramı, paylaşılan ve kullanılan bir değeri ifade etmektedir. Bu paylaşılan değer kuruluşlarda ekonomik, sosyal, kültürel ve tarihsel açıdan bilginin üretilme sürecinde önemli rol oynamaktadır (Özdemirci ve Aydın 2007).

Kurumsal bilgi, bireysel bilgilerin toplamının yanı sıra, diğer organizasyonlar tarafından kolayca taklit edilemeyecek şekilde insan, teknoloji ve yönetim ilkeleri arasında üretilen bilgi kaynaklarını ifade etmektedir. Bu bilgi, organizasyonun paylaşılan normları, kuralları ve iş programları içerisinde bulunabilir. Kurumsal bilgi örgüt içinde mevcutlar arasından ziyade bireyler arasından toplanan ve paylaşılan bilgiden oluşur. Kurumsal bilgi örgüt içi bireylerin bilgilerinin toplanmasının yanı sıra, örgüt içi bireylerin

bilgilerinin örgütsel bilgiye dönüştürülmesinden ortaya çıkan bir değerler bütünüdür. Bu bilgilerin diğer kurumlar tarafından taklit edilmesi zordur çünkü söz konusu üç unsur arasında oluşturulan etkileşim, kurumun kendine özgü tarihini ve kültürünü yansıtmaktadır (Durna ve Demirel 2008; Odabaş 2005).




**Şekil 2.2** Kurumsal Bilginin Gelişim Döngüsü (Bhatt 2000).

Anameriç (2005)'e göre, kurumsal bilgi; müşteriler, ürünler, süreçler, hatalar ve başarılar hakkında sahip olunan enformasyondur. Elde edilen enformasyonun, stratejilere dönüştürülmesi, verimlilik/yenilik/yaratıcılık ve rekabet süreçlerinde kullanılması bilgiyi karşımıza çıkarır. Bu bağlamda kurumsal bilgi;

1. Doğru karar vermede,
2. Geleceğe yönelik tahminlerde bulunmada,
3. Sağlıklı bir iletişimin gerçekleştirilmesinde,
4. Standart bir ürün/hizmet gerçekleştirmede,
5. Var olan problemlerin çözümlenmesinde ve olabilecek problemlere çözüm bulunmasında, kullanılan bir araçtır (Atılgan 2009).

### 2.4.2 Erişilebilir ya da Kayıtlı Olup Olmamasına Göre Bilgi

Literatür çalışmalarında, daha yaygın olarak bilgi, erişilebilir ya da kayıtlı olup olmamasına göre, örtük ve açık bilgi olmak üzere iki gruba ayrılmaktadır.

#### 2.4.2.1 Örtük Bilgi

Örtük bilgi, insanların zihninde bulunan ve herhangi bir yerde kayıtlı olmaması sebebiyle de formüle edilmesi, aktarılması ve iletilmesi kolay olmayan bilgi türüdür. Aynı zamanda kayıtlı olmasına rağmen erişime kapalı olan ve yalnızca ilgililerinin erişimine izin verildiği veri tabanları da örtük bilgi olarak ifade edilebilmektedir (Ağır 2007; Odabaş 2005). Ghaziri and Elias (2004)'a göre örtülü bilgi, tecrübe ile insan zihnine yerleşen bilgidir. Bu bilgi, sezgi, duygu, değer ve inançları içeren bilgi olup, açık bilgiyi oluşturmak içinkullanılır. Bu bilgi kolay fark edilebilir ve ifade edilebilir, kişiseldir, nitelendirilebilirliği ve başkalarıyla paylaşımı zordur, diyalog, senaryo ve metafor kullanımıyla iletilmektedir (Güçlü ve Sotirofski 2006).

Örtük bilgi, bir araya getirilerek ifade edilmez. Bu yüzden onu açığa çıkararak anlamlı bir hale getirmek faydalanma açısından önemlidir. Örneğin bir kişinin yüzündeki tepkiyi okumak ve bunu nasıl yapabildiğimizi ifade etmek örtük bilgiye en güzel örnektir. Ayrıca örtük bilgiyi davranışlardan, hareketlerden ve gözlemlerden de anlayabiliriz. Örneğin herhangi bir konu hakkında kişinin bilgisi varsa onun tavırlarından, düşüncelerinden, hareketlerinden bu durumu anlamak mümkün olabilir. (Durna ve Demirel 2008).

Kurum ve kuruluşlarda, çalışanların sezgi ve tecrübelerinden faydalanmak ve bunları açığa çıkarmak bilginin yönetimine olumlu katkı sağlayacaktır. Modern işletmeler örtük bilginin açığa çıkarılmasında çalışanlara inisiyatif yetkisi vermişlerdir. İnisiyatif yetkisine sahip olan çalışan durum ve şartlar karşısında kendisine ait olan örtük bilgiyi kullanmaktan kaçınmaz. Çünkü onun için başarılı olmak bilgiyi kullanmaktan geçtiğine inanmaktır. Bu nedenle çalışanları yaptıkları işlerle tam yetkili kılarak, onların

bilgilerinden daha çok yararlanmayı bir politika haline getirmek organizasyonların gelişimi açısından da önemlidir (Durna ve Demirel 2008).

#### 2.4.2.2 Açık Bilgi

Açık bilgi, belli bir düzen içerisinde ve belli bir yerde kayıtlı bulunan ve isteyen herkesin erişim sağlayabildiği bilgidir. Aynı şekilde kurumsal açık bilgiler de, herhangi bir organizasyonun faaliyetleri ve deneyimleri sonucunda ortaya çıkan, o organizasyona özgü değerler taşıyan ve çalışanların kolayca erişebildikleri bilgilerdir (Odabaş 2005).

Ghaziri ve Elias (2004)'a göre açık bilgi ise, "kitap, doküman, rapor, kısa not ve eğitim kurslarında düzenlenen bilgidir. Açık bilgi, örtülü bilgiye göre daha hızlı iletilebilir ve düzenlenebilir, çünkü açık bilgi direkt olarak tecrübeden elde edilen bir bilgidir. Bu bilgi, kelime, rakam, sesli veri, bilimsel formül, kayıt veya ürün şeklinde ifade edilebilir; kişilere formal ve sistematik olarak iletilebilir" (Güçlü ve Sotirofski 2006).

Açık bilgi, genel kabul görmüş doğruluğa sahip bir bilgi olarak, bilişim teknolojileri aracılığıyla rahatça paylaşılabilmektedir. Açık bilgi organizasyonlar içerisinde, herkes tarafından rahatça anlaşıldığından, kişiler veya birimler arasındaki iletim süreci daha kolay gerçekleşmektedir. Açık bilginin en önemli özelliklerinden biri de yoruma açık olması ve objektif bir nitelik taşımasıdır. İşletmelerde, müşteriler hakkında oluşturulan veriler, açık bilgi olarak kabul edilebilir. Çünkü bu veri tabanları karar alma sürecinde bilgiye dönüşerek, müşteriler hakkında nerede, ne zaman, nasıl ve kim tarafından hangi tür bir kararın verileceği sorularına rahatça cevap bulunabilir. Bu durumun oluşturulabilmesi için örgüt içindeki bilgi paylaşımının son derece güçlü olması gerekmektedir (Durna ve Demirel 2008).

## 2.5. Bilgi Güvenliği Kavramı

Her türlü örgütsel yapılanmanın, kurumun veya kişisel olarak bireylerin; günlük iş süreçleri içerisinde bilgi ile ilintili işler, parçalar veya unsurlar vazgeçilmez bir biçimde yer almaktadır. Bu bağlamda, kimi zaman kâğıt dokümanlar üzerinde yazılı olarak

bulunabilen bilgi, kimi zamansa bilişim sistemleri aracılığıyla elektronik ortamlarda saklanabilmektedir. Saklanan bu bilgiler, teknolojik cihazlar yoluyla bir yerden bir yere iletilebilmekte ya da kişiler arasında sözlü olarak ifade edilebilmektedir. İşte bu aşamada yani bilginin kayıt edildiği ortamlarda veya iletimi esnasında hangi formatta ve nerede kayıtlı bulunursa bulunsun, başkalarının eline geçmesinin engellenmesi için mutlaka uygun bir şekilde korunması gerekmektedir. Yani, işin niteliği veya sürecin yapısı ne olursa olsun, teknoloji bağlantılı olsun veya olmasın tüm süreçlerin yönetiminde bilgi güvenliğinin de etkin, sürekli ve başarılı bir şekilde sağlanarak yönetilmesi çok önemli bir gereksinim olmaktadır. İşlerin ve süreçlerin sağlıklı yönetimi aynı zamanda ilgili bilgi güvenliği süreçlerinin de sağlıklı yönetimini zorunlu kılmaktadır. Bilgi güvenliği stratejileri ve bunları yönetecek uygun yöntemleri olmayan kurumlar, sadece güvenlik açısından değil, operasyonel ve diğer her türlü iş süreçlerinin yönetimi açısından da ciddi sıkıntılar, maddi ve/veya manevi kayıplarla yüzleşmektedir (Aslandağ 2010; Atılgan 2009; Eminağaoğlu ve Gökşen 2009; Tipton and Krause 2007).

Dünya çapında küresel bir ağın oluşması, internetin hayatımıza girip hızlı bir şekilde yaygınlaşması, sosyal medya ve mobil akıllı cihaz kullanımının artması, bilgiye istenilen yerden ve istenildiği zaman ulaşılabiliyor olması ile birlikte meydana gelen değişiklik üretilen ve kullanılan bilginin türlerini ve şekillerini değiştirdiği gibi oluşabilecek risk türlerini de farklılaştırmıştır. Önceleri kendimizin, evimizin, iş yerimizin, arabamızın güvenliği yani fiziksel güvenlikler ön plandayken, günümüzde artık, kişisel haklar, fikri mülkiyet hakları, ticari sırlar gibi kişisel veya kurumsal verilerimizin başka kişilerin eline geçmesini engellemeye yönelik önlemler daha fazla önem kazanan bir konu haline gelmiştir. Risk algısındaki bu değişiklik ile birlikte artık, "kredi kartı hesabımıza ulaşılır mı? Virüs bilgisayarımı mahveder mi? Mevduat hesabım güvende mi? İşyerimizin bilgisayarı yetkisiz kullanıma kapalı mı? Sosyal medya hesabım başkalarının eline geçti mi?" gibi soruların daha fazla sorulduğu ve cevaplarının arandığı bir döneme girmiş bulunmaktayız (Çetin 2014; Mart 2012).

Bilgi güvenliği konusunun daha iyi anlaşılabilmesi için öncelikle, bilgi güvenliğine olan ihtiyaç neden ortaya çıktı? Bilgimiz kaybolur veya başkalarının eline geçerse ne gibi

risklerle ve sorunlarla karşı karşıya kalırız? Bilgi güvenliği konusunda kurumlar, bireyler ve toplum ne gibi problemler yaşıyor? Zamanında ve doğru bilgi almanın önemi nedir? gibi soruların yanıtlanıp, kişisel ve kurumsal kültür içerisinde üzerinde düşünülerek her bireyin veya organizasyonun kendi sistematiği içerisinde belli başlı bazı stratejiler geliştirmeleri gerekmektedir. Ancak genel itibariyle bu durumun bir türlü gerçekleşmediği, hatta gün geçtikçe bilgilerimizi daha fazla bir şekilde hoyratça ve hatta kendi elimizle dahi paylaştığımız bilinen bir gerçektir. Şunu bilmemiz gerekmektedir ki; bilginin korunması konusuna gereken önemi vermeyip, sürekli bir şekilde ihmal edilmesi neticesinde ciddi iş kayıpları, maddi ve manevi kayıplar ve hatta ölümler olmak üzere çok değişik bilgi güvenliği sorunları meydana gelmektedir (Eminağaoğlu ve Gökşen 2009).

Bilgi en basit benzetme ile para gibi bir metadır. Kişiler, kurumlar ve ülkeler için bilgi, elde edilmesi, aynı zamanda da elde tutulması zor bir metadır (Canbek 2005). Çünkü bilginin, sadece güvenli bir şekilde saklanması ve depolanması güvenlik kapsamında yeterli bir çözüm olmamaktadır. Gelişen ihtiyaçlar çerçevesinde bilginin aynı zamanda bir yerden bir yere nakil edilmesi de kaçınılmaz bir ihtiyaç haline geldiğinden, bu iletim esnasında da güvenlik önlemlerinin alınması gerekmektedir (Aslandağ 2010).

Entelektüel bir mülk olarak bilgi sahibinin korunması da, hayati bir önem arz etmektedir. Bu korunma, hem bilgi kullanımındaki karmaşayı, yozlaşmayı ve kötüye kullanımı önleyeceği gibi; hem de bilgiyi bir çaba göstererek elde eden tüzel veya gerçek kişilerin haklarının korunmasını da sağlayacaktır. İşte bu yüzden patent gibi haklar, entelektüel mülkü korumak amacıyla oluşturulmuştur. Bu bağlamda düşünüldüğünde, bilgi güvenliğinin çok kapsamlı ve farklı iştiraklerin katılımıyla oluşturması gereken bir konu olduğu görülmektedir (Canbek 2005). Bu kadar geniş kapsamlı tedbirler zincirini tek başımıza oluşturmak imkânsız olduğundan, kişisel ve kurumsal verilerin korunması hususunda gerekli kanunları oluşturarak suçluların cezalandırılması hususunda devletlere de fazlasıyla görevler düşmektedir.

Bilgi güvenliği ile ilgili literatürdeki tanımlar dikkate alındığında uzmanların sahip oldukları bilgi birikimi ve özel uzmanlık alanlarına göre bilgi güvenliğine farklı

açılardan bakıldığı görülebilir. Bilgi güvenliğinin temel amacı doğru kişinin kısa zamanda doğruluğundan emin olunan bilgiye ulaşımını garanti altına almaktır. Daha geniş manada ise, "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 süreci bilgi güvenliği olarak tanımlanabilir" (Mart 2012; Vural 2007).

Bilgi güvenliği aynı zamanda, bilginin tehditlere karşı uygun şekillerde korunması ve bir varlık türü olarak izinsiz veya yetkisiz bir biçimde erişimini, kullanımını, değiştirilmesini, ifşa edilmesini, ortadan kaldırılmasını, el değiştirmesini ve hasar verilmesini önlemek olarak tanımlanabilir (Çetin 2014; Puhakainen and Ahonen 2006). Bilgiye yönelik olası saldırılar (tahrip edilmesi, silinmesi, bütünlüğünün ve/veya gizliliğinin zarar görmesi), bilgi altyapısının bozulmasına ve bu da beraberinde işlerin aksamasına neden olmaktadır. Özellikle, farklı kurumlar ve insanlar arasında bilgini paylaşımı arttıkça, üzerindeki çeşitli risklerin oluşması ihtimali de artmaktadır. Tarih boyunca, ülkeler ve askeri komutanlar, ordu rakamları ve hareket yöntemleri gibi bilgilerin korunmasının önemini anlamış bu tür bilgilerin, düşmanın eline geçmesinin sonucunda felaketler oluşabileceğinin farkında olmuşlardır (Aslandağ 2010; Ganbat 2013). Bu nedenle bilgi, geçmiş zamanlarda fiziksel güvenliği sağlanan ortamlarda saklanmaya çalışılmış, bu amaçla da duvarlar örülmüş, kale hendekleri çekilmiş ve giriş çıkışları kontrol eden nöbetçiler görev yapmıştır. Ancak, bilginin güvenliğini sağlamaya yönelik fiziksel önlemler genellikle yeterli olmamış, bilgilerin çalınması veya istenmeyen kişilerin eline geçmesi engellenememiştir (Mart 2012).

Bilgi güvenliği, her organizasyonun sürekliliğinin sağlanmasında büyük önem taşır ve organizasyonun başta elektronik olmak üzere, çeşitli ortamlardaki kritik bilgilerinin ve diğer bilgi varlıklarının korunmasını sağlar. Sadece büyük şirketler, holdingler değil, bunun yanı sıra KOBİ'ler, devlet kurumları, kar amacı gütmeyen herhangi bir organizasyon, okul veya tek başlarına insanlar da bilgi güvenliği sorunları ve risklerini farklı düzeylerde de olsa sürekli yaşamaktadır. Bu risklerin karşılanmasına yönelik yapılacak yatırımlarda en pahalı ve en karmaşık çözüm, her zaman en güvenli çözüm olmamaktadır. Her kişinin veya organizasyonun kendisine en uygun ve en doğru

çözümü seçmesi ve uygulaması gerekmektedir. Basit ve düşük maliyetli bir güvenlik çözümü kimi kurumlar için yetersiz kalırken, aynı çözümün bir başka kurum için yeterli ve etkili olabileceği de unutulmamalıdır. Bununla birlikte, bilgi güvenliği, başlanıp bitirilecek bir çalışma, bir iş de değildir. Bilgi güvenliği yönetimi, kurumlar ve bilgiler var olduğu sürece sürekli yönetilmesi, denetlenmesi gereken bir yaşam döngüsüdür (Eminağaoğlu ve Gökşen 2009).

### 2.5.1 Bilgi Güvenliğinin Temel Unsurları

Bilgi güvenliğinin üç temel unsuru; gizlilik, bütünlük ve erişilebilirlik/kullanılabilirlik olarak ifade edilmektedir (Baykara *et al.* 2013; Tekerek 2008);

#### 2.5.1.1 Gizlilik

Bilgiye sadece yetkilendirilmiş kişilerce ulaşılabilmesi yani yetkisiz erişiminin engellenmesi olarak nitelendirilmektedir. Bilginin gizlilik seviyesi, yasa, kanun, sözleşme gibi resmi zorunluluklara ve kurumun bilgi güvenliği yönetim sistemi uygulama sürecinde yapılmış olan risk analizinin sonucuna dayanarak belirlenmelidir (Ganbat 2013). Temel olarak erişim kontrolünün birçok biçimi, gizliliğin korunması ile ilgilidir. Şifreleme, kilitleme, bilinçlendirme vb. gibi kontroller, varlığın hangi formatta olursa olsun gizliliğinin sağlanmasına örnek olarak verilebilir (Aslandağ 2010).

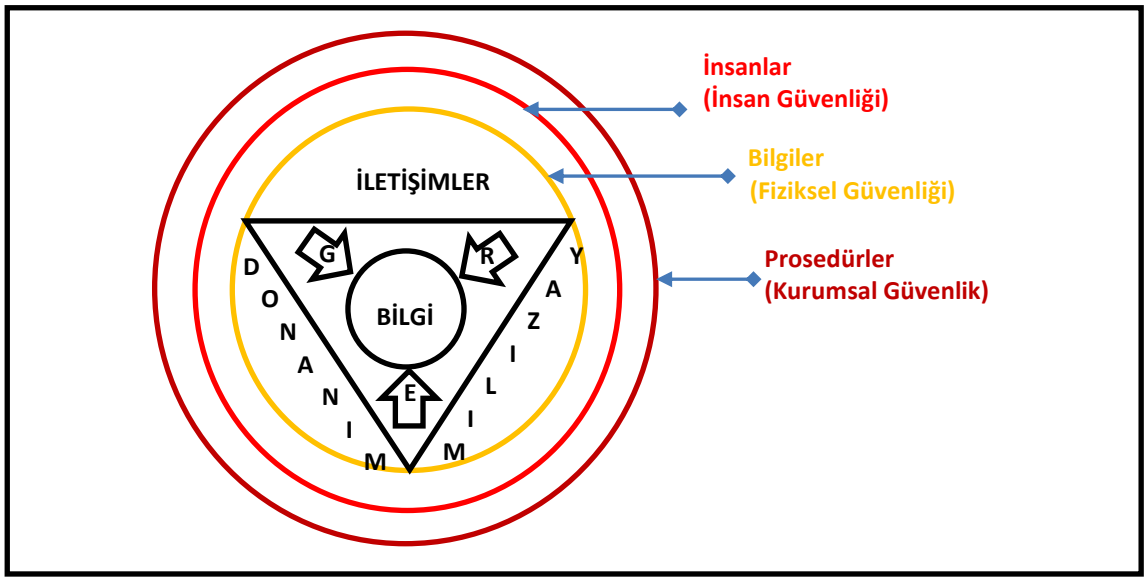
#### 2.5.1.2 Bütünlük

Bilginin yetkisiz kişilerce değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı içeriğinin korunmasıdır (Önel ve Dinçkan 2007). Verinin bozulması kasten yahut kaza ile olabilir ve bu bütünlüğün bozulmuş olduğu gerçeğini değiştirmez (Yıldız 2007). Kurumlarda bilginin bütünlüğünün kaybedilmemesi için bütün bilgi varlıklarına, bu bilgilerden sorumlu kişiler atanmalıdır. Kurumun politikası veya iç düzeninde tanımlanan, bilginin bütünlüğünün korunması ve saklanması için alınan tedbirler için sık sık denetleme yapılmalıdır (Ganbat 2013).

#### 2.5.1.3 Erişilebilirlik/Kullanılabilirlik

Bilginin, yetkisi olan kurumlar ve kişiler tarafından gerekli olduğu zamanlar ulaşılabilir veya kullanılabilir olması anlamına gelir. Matematiksel olarak ifade edilirse, kullanılabilirlik herhangi bir sistemin yapılış amaçlarına göre işlev gördüğü zamanın, işlev gördüğü ve görmediği toplam zamana oranıdır. Herhangi bir sorun ya da problem çıkması durumunda bile bilginin erişilebilir olması gerekmektedir. Bu erişim kullanıcının hakları çerçevesinde olmalıdır. Erişilebilirlik ilkesince her kullanıcı erişim hakkının bulunduğu bilgi kaynağına, yetkili olduğu zaman diliminde mutlaka erişebilmelidir. Bu verilen hizmetin ne kadar güvenilir olduğunun bir ölçütüdür. Kurumlar erişilebilirliğin ne kadar önemli olduğunun ölçümünü yapıp, sistemleri ve verileri bu ihtiyaca göre yedekli hale getirmelidirler (Önel ve Dinçkan 2007; Yıldız 2007).

Bu üç temel güvenlik öğesinden herhangi biri zarar görürse güvenlik zafiyeti oluşur (Güldüren *et al.* 2016). Fussell (2005)'e göre bu unsurlar birbirinden bağımsız olarak düşünülememektedir. Bilginin gizliliğinin sağlanması o bilginin erişilebilirliğini engellememelidir. Aynı zamanda erişilebilen bilginin bütünlüğünün de sağlanması önemlidir. Eğer bir bilgi için sadece gizlilik sağlanıyor ve bilgiye erişim engelleniyor ise kullanılamaz durumda olan bu bilgi bir değer ifade etmeyecektir. Eğer erişimi sağlanıyor ancak bütünlüğü sağlanmıyor ise kurumlar ve kişiler için yanlış veya eksik bilgi söz konusu olacak ve olumsuz sonuçlara neden olabilecektir. Dolayısıyla bilgi güvenliği kavramı temel olarak bu üç unsurun bir arada sağlanması demektir (Mart 2012).




**Şekil 2.3** Gizlilik, Bütünlük, Erişilebilirlik Üçlü Nitelikleri (Ganbat 2013)

## 2.6. Bilişim Sistemleri Güvenliğinin Bilgi Güvenliği İçerisindeki Yeri

Çağımızda bilginin, depolanması, iletilmesi ve ulaşılması aşamalarında dijital ortamların kullanılması sebebiyle bilgi güvenliği denildiğinde, direkt olarak bilişim sistemleri güvenliği akıllara gelmektedir (Akgün ve Topal 2015). Bilişim sistemleri güvenliğini anlamak için de öncelikle bilişim sistemlerini oluşturan öğeleri tanımak ve bilmek gerekmektedir. Bilişim sistemleri denildiğinde önceleri sadece bilgisayar sistemleri ve ağları algılanırken, iletişim ve internet teknolojisinin yaygınlaşması ile birlikte artan mobil cihaz kullanımı, bilişim sistemleri güvenliği kavramının, kapsamının genişlemesine neden olmuştur. Artık, giderek kullanıcı sayısı artan, günlük hayatta elimizden düşürmediğimiz tablet bilgisayar ve akıllı telefonlar, bilgi güvenliği açısından önlem alınması gereken en önemli unsurlar haline gelmiştir (Çetin 2014).

Bu gelişimin yaşanması esnasında kilometre taşı sayılabilecek olay, iletişim ağlarının yaygınlaşmasıyla birlikte merkezileşmiş yapıdan çıkılarak, kullanıcılara ortak kaynakları çok daha kolay paylaşma, merkezi bilgisayarlardan bağımsız işler yapabilme olanağının verilmesidir. Bu durum sosyal hayatı o kadar fazla etkilemiştir ki, bilişim teknolojileri artık sıradan bir bireyin yaşantısının vazgeçilmez bir öğesi haline gelmiştir. (Dedeoğlu 2006; Mart 2012). Bu durum, bilişim sistemlerinin eğitim, sağlık, tarım,

sanayi gibi her alanda kullanılması sonucunu doğurmuş bununla birlikte de ekonomik, sosyal ve kültürel değişim başlamıştır. Çağımızda artık kültürel dönüşümlere etki eden etmenlerin arasına bilişim teknolojilerinde meydana gelen değişim ve dönüşümünde girdiği söylenebilir. Teknoloji ile gelen e-yaşamın gündelik hayatta meydana getirdiği değişiklikler ile artık koltuğumuzdan kalkmadan sinema, tiyatro bileti almak, rezervasyon yaptırmak, faturaları ödemek, para transferi yapmak gibi işlemler saniyelerle ifade edilen hızlarla gerçekleştirilebilmektedir (Mart 2012).

Teknoloji toplum yaşantısında refahı büyük ölçüde arttırmakta, hayatı kolaylaştırmakta, uzaklıkları kısaltmakta, verimi arttırmaktadır. Ancak bu kadar olumlu etkilerinin yanında birtakım olumsuzlukları da beraberinde getirmektedir. Hayatımıza giren her yeni teknoloji, bu teknolojileri benimseyenler ile benimsemeyenler arasındaki uçurumu genişleterek, bireyler ile toplumların yaşamını olumsuz olarak etkilemektedir. Oluşan olumsuzluklardan bir diğeri ise güvenlik sorunudur. Cep telefonu, bilgisayar ve internetin günlük yaşamda etkin bir şekilde kullanılması ile birlikte birçok güvenlik tehdidi ile de karşılaşılmaktadır. Artık her türlü kişisel ve kurumsal veriler elektronik cihazlarda tutulmakta veya bu cihazlar kullanılarak bu bilgilere ulaşılmaktadır. Banka bilgileri, çalışma hayatındaki bilgiler, şifreler hatta günlük ruh hali elektronik cihazlar vasıtası ile anlık olarak depolanmakta ve çevrimiçi uygulamalar vasıtasıyla istenildiği zaman başka kişiler ile paylaşılmaktadır. Teknolojide yaşanan bu hızlı gelişmeler ile gerçek ve sanal yaşantılar birbiriyle iç içe geçmiş, bu durum bilgisayar ağlarını ve teknolojik cihazları, bir saldırı aracı, aynı zamanda kullandığımız sistemleri de açık birer hedef haline getirmiştir. Bu noktada, özellikle ulaşılan bilgi ve bu bilginin güvenliği, yaşantının dengeli bir biçimde devamı için önemli bir unsur olarak karşımıza çıkmaktadır. Özellikle bilginin paylaşımı aşamasında, kişisel bilgilerimiz başta olmak üzere bize ait tüm kritik bilgiler, teknolojik cihazlarımızda veya bu cihazlarda barındırdığımız uygulamalar aracılığı ile sanal dünyanın bize ayrılan bir yerinde saklanmaktadır. Bu noktada da bilgi güvenliği ve bu konudaki güvenlik önlemlerinin sağlanması kişisel ve kurumsal açıdan oldukça önemli hale gelmektedir (Güldüren *et al.* 2016; Karaarslan 2013; Mart 2012; Vural *et al.* 2009).

Bilgi güvenliğini sadece kişisel ve kurumsal açıdan düşünmemek gerekir. Aslından en önemli unsurlardan biriside ülkelerdir. Artık ülkelerin, bilgiyi etkin bir biçimde kullanabilmek için bilişim sistemlerini doğru ve güvenli olarak kullanmak zorunluluğu ortaya çıkmıştır. Bu nedenle de eğitimden sanata, sağlıktan iş yaşamına, e-devlet uygulamalarından diğer birçok alana, bilginin güvenli kullanımı ülkeler açısından önemli bir gereksinim halini almıştır. Güvenliği sağlanamayan ulusal bilgi sistemleri ülkeler açısından ciddi tehditlerin meydana gelmesine neden olmaktadır. Ulusal bilgi sistemlerinin ortak olarak kullanılmaya başlanmasıyla, ülke güvenliği açısından kritik olan bilgilerin güvenliğinin yüksek seviyede sağlanması anayurt güvenliği açısından oldukça önemli bir unsur haline gelmiştir (Vural *et al.* 2009).

Türkiye İstatistik Kurumu ve Bilgi Teknolojileri Kurumunun Ağustos 2016'da yayınlamış olduğu raporlarda Hane Halkı Bilişim Teknolojileri Kullanımında 16-74 yaş arası kişilerde internet kullanımı %55,9'a, Türkiye genelinde İnternet erişim imkânına sahip hanelerin oranı ise 2016 yılı Nisan ayında %76,3 olduğu belirtilmiştir (TUİK 2016).

Türkiye'de yaklaşık %94,6 penetrasyon oranına karşılık gelen toplam 74.457.474 mobil abone olduğu ve taşınabilir cihaz sayısının artışına bağlı olarak çizelge 3.1'de görüldüğü gibi mobil abone sayısına oranla mobil internet kullanımının %66'lara (48.978.066 abone) ulaştığı görülmektedir (BTK 2016; TUİK 2016).

**Çizelge 2.1** Toplam İnternet Abone Sayıları (BTK 2016)

| | 2015-3 | 2016-2 | 2016-3 | Çeyrek Dönem Büyüme Oranı (2016-2…2016-3) | Yıllık Büyüme Oranı (2015-3…2016-3) |
|---|---|---|---|---|---|
| **xDSL** | 6.946.553 | 7.444.432 | 7.549.868 | 1,4% | 8,7% |
| **Mobil Bilgisayardan İnternet** | 1.662.797 | 1.329.239 | 1.287.931 | -3,1% | -22,5% |
| **Mobil Cepten İnternet** | 35.876.797 | 43.992.910 | 47.690.135 | 8,4% | 32,9% |
| **Kablo İnternet** | 596.056 | 664.095 | 688.143 | 3,6% | 15,4% |
| **Eve Kadar Fiber (FTTH)** | 589.321 | 665.086 | 698.861 | 5,1% | 18,6% |
| **Binaya Kadar Fiber (FTTB)** | 1.013.921 | 1.110.507 | 1.123.633 | 1,2% | 10,8% |
| **Fiber (Toplam)** | 1.603.242 | 1.775.593 | 1.822.494 | 2,6% | 13,7% |
| **Diğer** | 92.385 | 99.479 | 117.652 | 18,3% | 27,3% |
| **TOPLAM** | **46.777.134** | **55.305.748** | **59.156.223** | **7,0%** | **26,5%** |

2016 yılı üçüncü çeyrekte 3G abone sayısı 4.5G hizmetinin hayata geçmesi nedeniyle 23.549.215'a düşerken, 4.5G abone sayısı üç aylık dönem içerisinde 45.736.402'e ulaşmıştır. 3G ve 4.5G hizmetiyle birlikte mobil bilgisayardan ve cepten internet hizmeti alan mobil genişbant abone sayısı 48.978.066'ya, sadece 4.5G hizmetiyle birlikte mobil bilgisayardan ve cepten internet hizmeti alan mobil genişbant abone sayısı da 29.301.277'ye yükselmiştir. 2016 yılı üçüncü çeyrekte toplam mobil internet kullanım miktarı 313.447 TByte, 4.5G kullanıcılarının toplam mobil internet kullanım miktarı ise 267.742 TByte olarak gerçekleşmiştir (BTK 2016).

**Çizelge 2.2** 3.5G ve 4.5G Hizmeti Kullanıcı Verileri (BTK 2016)

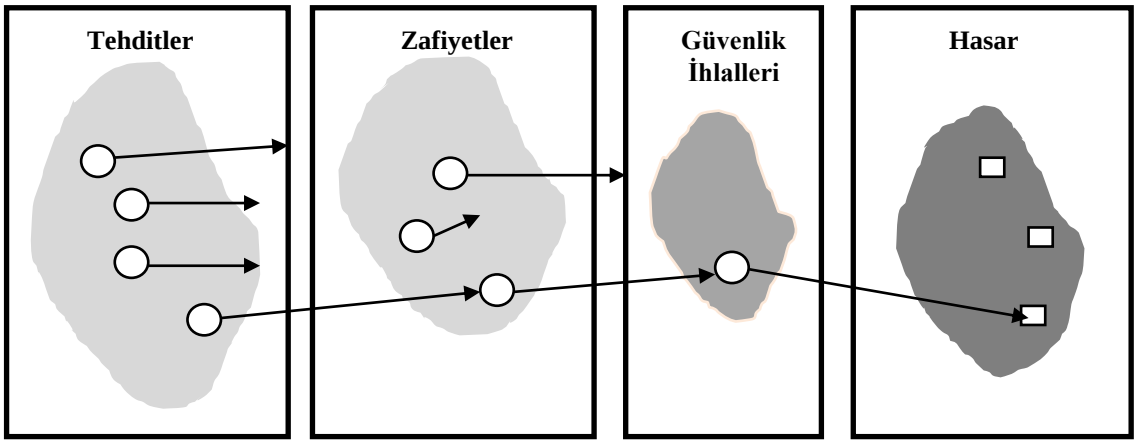
| | 2015-2 | 2015-3 | 2015-4 | 2016-1 | 2016-2 | 2016-3 |
|---|---|---|---|---|---|---|
| **3G Abone Sayısı** | 61.076.640 | 63.066.580 | 64.256.311 | 65.949.652 | 28.599.109 | 23.549.215 |
| **4.5G Abone Sayısı** | - | - | - | - | 38.597.384 | 45.736.402 |
| **Mobil Bilgisayardan İnternet (Toplam)** | 1.646.892 | 1.662.797 | 1.597.606 | 1.465.689 | 1.329.239 | 1.287.931 |
| **Mobil Bilgisayardan İnternet (4.5G)** | - | - | - | - | 398.681 | 459.528 |
| **Mobil Cepten İnternet (Toplam)** | 32.232.558 | 35.876.101 | 37.469.948 | 40.482.100 | 43.992.910 | 47.690.135 |
| **Mobil Cepten İnternet (4.5G)** | - | - | - | - | 24.598.738 | 28.841.749 |
| **Mobil İnternet Kullanım Miktarı TByte (Toplam)** | 126.027 | 156.669 | 165.366 | 194.558 | 255.376 | 313.447 |
| **Mobil İnternet Kullanım Miktarı TByte (4.5G)** | - | - | - | - | 151.262 | 267.742 |

Artan abone ve cihaz sayısı, veri dolaşım hızını ve miktarını artırmıştır. Verilerin dijital ortamda yer almaları kötü niyetli kişileri de bu ortamlara yöneltmiş ve kullanıcılar için tehdit oranını artırmıştır (Çetin 2014). Bu durum günümüzde, bilişim teknolojileri aracılığıyla kayıt altına alınan ve iletilen verilerin korunmasını temel bir ihtiyaç haline getirmiştir.

## 2.7. Bilgi Güvenliğini Tehdit Eden Unsurlar ve Alınacak Önlemler

Tehdit, "bir sistemin veya kurumun zarar görmesine neden olan istenmeyen bir olayın arkasındaki bilinmeyen neden" olarak tanımlanabilir (Can ve Akbaş 2014).

Tehditler, bilgi sistemleri üzerindeki zafiyetleri kullanarak istediklerini elde etmeye çalışırlar. Her tehdidin bir kaynağı ve bu kaynağın yararlandığı sistemdeki bir güvenlik açığı mutlaka vardır. Tehditlerin bilgi varlıklarına etkisi, tehlikenin oluşma olasılığı, bilgi varlığı üzerindeki açık ve varlığın değeri ile doğru orantılıdır. Tehditler uygun ortam şartlarının oluşmasıyla bilgi sistemlerine zarar verecek kusurlar içeren zafiyetlere, zafiyetler saldırganlar tarafından kullanıldığında güvenlik ihlallerine yol açarak bilgi sitemlerine zarar vermektedir (Tekerek 2008; Vural 2007). Tehditlerin bilgi sistemleri üzerinde hasar oluşturmasına kadar izlediği süreç Şekil 3.4'de şematik olarak gösterilmiştir.




**Şekil 2.4.** Tehditlerin Bilgi Sistemlerine Etkisi (Vural 2007)

Durumu sadece bilişim sistemlerine yönelik tehditlere indirgemekte doğru bir yaklaşım değildir. Aslında sanal ortamda karşılaştığımız tehditlerin çoğuna günlük yaşamımızda da sıkça rastladığımızı söyleyebiliriz. Dolayısıyla; kişisel bilgilerin korunması ve bilgi güvenliği alanındaki tüm risk başlıkları gerçek hayatta da yer almaktadır. Yani, bu konulardaki tehditlerle ilgili sadece interneti suçlamak doğru bir yaklaşım değildir. Bu sorunların üstesinden gelebilmek için suçlayıcı tavırlar yerine, toplumu eğitmek ve bilginin ne kadar önemli bir meta olduğu konusunda bilinçlendirmek daha doğru bir yaklaşım olacaktır (Mart 2012).

Bilişim sistemleri üzerinde bilgi güvenliğine yönelik oluşabilecek bu tehditleri, insan kaynaklı, fiziksel ve yazılım kaynaklı tehditler olarak sınıflandırabiliriz (Tekerek 2008; Vural 2007).

### 2.7.1 İnsan Kaynaklı Tehditler

Konu bilgi güvenliği olduğunda çoğunlukla, çeşitli standartlar, yazılımlar (anti virüs yazılımları, güvenlik duvarları, içerik kontrolü yazılımı, veri şifreleme, kimlik doğrulama, yetkilendirme vb.) ve donanımlar geliştirilerek, teknoloji temelli çözümler ortaya konularak, bu teknolojileri kullanan ve işletenlerin insanlar olduğu gerçeği göz ardı edilmiştir. Bu durum kötü niyetli kişilerin güvenliğin en zayıf halkası olarak gördükleri insanların zaafları, dikkatsizlikleri ve bilinçsiz davranışlarından yararlanmaya yönelik bir takım alternatif yöntemler geliştirmelerinin önünü açan en önemli etken olmuştur (Güldüren *et al.* 2016; Keser ve Güldüren 2015; Öztemiz ve Yılmaz 2013; Vural 2007).

Bu durum, bilgi güvenliği sorununun insanlardan bağımsız, yalnızca teknoloji temelli yöntemlerle çözümlenemeyeceğini (Güldüren *et al.* 2016) dolayısıyla da, toplumun bilgi güvenliği konusunda bilinçlendirilerek, farkındalık düzeyleri artırılmasının önemli olduğu sonucunu doğurmaktadır. Bu sayede farkındalıkları oluşan bilinçli bireyler, hem kişisel hem de kurumsal bilgi güvenliğine daha fazla oranda katkı yapacaktır (Çetin 2014).

Önceleri bilişim cihazlarını sadece bu sektörde çalışan profesyoneller kullanıp, işletmekteydi dolayısıyla bilgi güvenliği kavramının, bilişim personeli dışından olan insanlar tarafından zor algılanacağı yönünde bir yargı vardı. Bu yüzden bilişim çalışanlarına, bu durumu teknik olmayan terimlerle diğer insanlara basit bir şekilde anlatmaları gerektiği söylenirdi. Günümüzde insanlar, hepsi birbiri ile iletişim kapasitesine sahip, hızla ilerleyen ve karmaşıklaşan teknolojiler ile kuşatıldığından, bilgi güvenliği eğitimi sadece belli bir gruptaki değil, tüm insanlara verilmesi gerekmektedir. Bu sayede bireyler, kişisel bilgilerinin korunmasında belli bir bilinç seviyesine ulaşarak, çalıştıkları kurumlar ve yaşadıkları ülkelerin de bilgi güvenliği savunma mekanizmasında önemli roller üstleneceklerdir (Aslandağ 2010).

Tipton and Krause (2007), kurumlarda bilgi güvenliği konusunda oluşturulan ilkelere öncelikli uyması gereken grupların, yöneticiler ve bilişimciler olduğunu buna rağmen

tam tersine bu ilkeleri en fazla ihlal eden ve en riskli eylemlerin yaşandığı birimlerinde en değerli ve en gizli bilgileri kullanan, taşıyan ve kaydeden bu iki gruptaki çalışanlar olduğunu belirtmiştir. Bu nedenle kurum içerisinden bilgi güvenliğine zarar veren saldırılar veya kasıtsız eylemler; dışarıdan yapılanlara göre risklerin ve kayıpların çok daha yüksek düzeyde gerçekleşmesine neden olmaktadır (Eminağaoğlu ve Gökşen 2009).

Bu veriler ışığında, insan kaynaklı tehditleri kendi içinde iki alt gruba ayırabiliriz (Tekerek 2008; Vural 2007):

#### 2.7.1.1 Bilinçsiz veya İstem Dışı Davranışlar Sonucu Oluşanlar

Herhangi bir sistem üzerinde yetkiye sahip olan bir kullanıcının, bilgi sistemlerini bilinçsiz veya bilgisizce, yeterli eğitime sahip olmadan kullanması sonucu bilginin gizlilik, bütünlük ve erişilebilirlik ilkelerinin birinin veya birkaçının ihlal edilmesine sebep olan bilmeyerek veya ihmalkârlık sonucu yapılan kullanıcı davranışlarıdır (Vural 2007). En önemli çelişkilerden ve sorunlardan birisi, kurumların en değerli ticari sırlarının USB bellek, DVD, dizüstü bilgisayar veya cep telefonu gibi, yani çok kolay çalınabilecek, kaybolabilecek aygıtlarda koruma önlemleri alınmadan sıkça taşınması ve kullanılmasıdır. Daha da önemlisi, bu gibi aygıtları kullanan insanların neredeyse %70'inin ilgili güvenlik risklerinin ve yüklenmiş oldukları sorumlulukların farkında olmamalarıdır (Eminağaoğlu ve Gökşen 2009).

#### 2.7.1.2 Bilinçli Davranışlar Sonucu Oluşanlar

Bağlı bulunduğu organizasyona kızgın veya küskün olan ve ileriye dönük hiçbir beklentisi olmayan sorunlu personelin görevini ve yetkisini kötüye kullanarak bilinçli olarak yaptığı kötücül davranışlardır. Bu kişiler yerel saldırgan (internal hacker) olarak adlandırılmaktadır (Vural 2007).

Bilinçli veya bilinçsiz olsun, insan kaynaklı tehditler sonucu meydana gelen kayıplar, zararlar, sorunlar devam etmekte ve bilgi güvenliği riskleri kontrol altına

alınamamaktadır. Çünkü temel sorun, bu konuya bireylerin, kurumların ve toplumun bakışı, algılama ve yaklaşım tarzındaki hatalar ve yetersizliklerdir. Konu önemsenmemekte ve her zaman ikinci plana atılmaktadır. Bilgi güvenliğine bireylerin, toplumların ve kurumların bakış açısının öncelikle değişmesi gerekmektedir. Kurumlardaki üst yöneticilere, yazılı ve görsel basınımıza, kanun ve yönetmelikleri düzenleyen yetkililere bu konuda ciddi görevler düşmektedir. Güvenliğin teknolojiden önce insana yatırım yapılmasıyla, bilinçlendirmeyle, kurumların en tepeden başlayarak bu gibi konularda bilgilenmesi, desteklemesi ve önemsemesi ile sağlanacağı ve güvenliğin sürekli yönetilecek bir süreç olduğu unutulmamalıdır (Eminağaoğlu ve Gökşen 2009).

### 2.7.2 Fiziksel Tehditler

Bu tür tehditler genellikle önceden tespit edilemez, doğa olayları veya teknik arızalar olmaları yüzünden de genellikle engellenemezler. Deprem, yangın, su baskını, sel, ani sıcaklık değişimleri, toprak kayması, çığ düşmesi bu tür tehditlere örnek olarak verilebilir. Bu tehditlere karşı tüm tedbirler önceden planlanmalı ve uygulanmalıdır. Fiziksel tehditlerden herhangi birinin meydana gelmesi genellikle tüm bilgi sistemlerinin zarar görmesine veya çalışmamasına sebebiyet vermektedir. Bu tür tehditleri en az indirmek için kurumsal yapıya uygun felaket senaryoları üretilmeli ve felaketten en kısa zamanda nasıl geriye dönülebileceğiyle ilgili iş devamlılığı konusundaki çalışmalar önceden yapılmalıdır (Tekerek 2008; Vural 2007).

### 2.7.3 Yazılım Tehditleri

Yazılım tehditlerinin başlıca amacı sisteme yetkisiz erişim yapılarak, bozulması, hizmetlerin engellenmesi, bilgilerin değiştirilmesi, yok edilmesi, ifşa edilmesi veya çalınması olarak özetlenebilir (Ünver *et al.* 2009). Saldırganlar bu işlemleri, donanım veya yazılım açıklıklarından faydalanarak kendi çıkarları için kullanırlar. Saldırılar çıkar amaçlı olabildiği gibi, kendi ünlerini duyurmak isteyen bireysel saldırganlar veya çeteler tarafından da yapılabilmektedir. Günümüzde saldırıların büyük bir çoğunluğu zararlı yazılımlar (Malicious Programs) olarak adlandırılan programlar aracılığıyla

yapılmaktadır (Vural 2007). Bu tür kötü niyetli yazılımlar genellikle, sistemlerde kullanıcının rutin işlemlerini yaptığı üçüncü parti uygulamaların veya işletim sistemlerinin kullandığı birtakım dosyaların manipüle edilmesiyle oluşturulur. Bunun sonucunda da ilgili yazılım, önceden yaptığı tüm işlemleri sorunsuz yerine getirmenin dışında fazladan kodu yerleştiren kişinin isteklerine de cevap verir duruma geçmektedir. Bu yazılımlar herhangi bir aksaklık yaşatmadığından, fark edilmeleri de oldukça zordur. Bu şekilde hareket eden belli başlı zararlı yazılımlar şunlardır:

- **Virüsler:** Kendilerini çalıştırılabilir programlara veya dosyalara iliştirebilen programlardır. Kendilerini çoğaltabilme özelliğine sahiptirler. Virüslerin etkilerini gösterebilmeleri için öncelikle kullanıcı tarafından çalıştırılmaları gerekmektedir. Çalıştırıldıktan sonra çoğalarak yayılırlar ve sisteme zarar verirler. İleri seviye virüsler kendilerini oluşturan kod parçacığını değiştirebilme yeteneğine sahiptir (Can ve Akbaş 2014).

- **Truva Atı (Trojan):** Aslında yararlı gibi görünen, fakat arka planda kötü niyetli bir şekilde çalışarak sistem içerisindeki kritik bilgileri toplayıp dışarıya çıkaran casus programlardır. Truva atları çalıştırıldığında; bir arka kapı oluşturularak, saldırgana ait sunucu ile bağlantı kurulmaktadır. Saldırgan, şifrelere, e-posta adreslerine, kredi kartı bilgilerine, kişisel belgeler gibi yetkisi olmayan bilgilere erişebilmekte ve bunları kendine yönlendirebilmektedir. Genellikle lisanssız yazılım, mp3, oyun ve cinsel içeriklere ekli olarak gelen dosyalar aracılığıyla bulaşan truva atları, kendilerini virüsler gibi kopyalayamazlar. Truva atının gereken işlevini yerine getirebilmesi için öncelikle çalıştırılması gerekmektedir (Can ve Akbaş 2014; Tipton and Krause 2007).

- **Mantık Bombası (Logic Bomb):** Mantık bombası belirli şartlar oluşana dek etkisiz olarak bekleyen bir program veya program parçasıdır. Bu haliyle gerçek dünyadaki mayına benzetilebilir. 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).

- **Solucanlar (Worms):** Solucanlar, virüslerin bir alt kümesi olarak nitelendirilmektedirler. Virüslerden ayrıldıkları nokta ise yayılmaları ve çalışmaları için kullanıcı tarafından herhangi bir programın çalıştırılmasına gerek olmamasıdır. İnternette sayfalar arasında gezinirken istenmeden otomatik olarak açılan reklamların linklerine tıklanması sonucu solucanlar bilgisayarlara yüklenebilmektedir. Özellikle, ağ üzerinden diğer sistemlere veya bilgisayarlara bulaşabilme durumları solucanları, virüslere kıyasla daha tehlikeli yapmaktadır. Solucanlar, ağ üzerindeki kaynakların yüksek miktarda tüketimine de sebep olmaktadırlar. Fakat virüsler gibi silme işlemi gerçekleştiremezler (Can ve Akbaş 2014).

- **Reklam Destekli Yazılımlar (Adware):** Belirli firmalar tarafından sağlanan reklamları programın içine gömerek kullanıcının bu reklamları tıklamasını sağlayan programların genel adıdır (Tipton and Krause 2007). Bu sayede kullanıcının ilgi alanları hakkında bilgi sahibi olunabilmekte ve ilk etapta zararsızmış gibi görünen bu bilgiler kötü niyetli kişiler tarafından bilgi sahibine yönelik daha büyük manipülasyonlarda kullanılabilmektedir.

- **Casus Yazılımlar (Spyware):** Adware'den farklı olarak, kullanıcının bilgisayarında hem belirli firmaların reklamlarını görüntüleyip hem de bilgisayarınızda ne yaptığınızı belirli bir sunucuya gönderen programlardır (Tipton and Krause 2007). Bu internette hangi sitelere girildiği gibi bilgilerin yanı sıra sosyal medya hesapları, e-mail, kredi kartı ve banka hesap bilgileri ile şifrelerine kadar önemli kişisel bilgileri içerebilir (Atalıç Taş 2010).

## 2.8. Bilgi Güvenliği Farkındalığı

Bilgi güvenliği farkındalığı, bilgi güvenliğini tehdit eden unsurlara karşı alınabilecek önlemlerden ve oluşturulan kişisel veya kurumsal politikalardan haberdar olunması, bu konuda bilinçli davranışlar sergilenmesi şeklinde tanımlanabilir (Siponen 2000). Bilginin yönetimi ve bu bilginin güvenliğinin sağlanması oldukça karmaşık bir süreç olduğundan, bu sürecin süreklilik gerektiren iyi planlamayla yönetilmesi gerekmektedir.

Bu planlama içerisine dâhil edilmesi gereken en önemli unsur olan insan faktörüne bağlı bilgi güvenliği risklerini tamamen ortadan kaldırmak mümkün olmasa da, dikkatli ve iyi eğitimli bireyler ile olası güvenlik ihlallerinin kabul edilebilir bir seviyeye çekilmesi sağlanabilir (Güldüren *et al.* 2016; Keser ve Güldüren 2015; Vural 2007). İnsan ve yönetim hatalarından kaynaklanan güvenlik ihlallerinin sebeplerine bakıldığında son kullanıcılardan ülke yönetimine kadar farklı kademelerde görev yapan kurum veya bireylerin ortak eksikliklerinin eğitim ve bilinçlendirme olduğu görülür (Vural *et al.* 2009). Bu durum, insanların herhangi bir sağlık sorunu yaşamadan önce hastaneye gitmeye gerek duymamaları gibidir. Yani, insanlar veya kurumlar bilgi güvenliğini tehlikeye atan bir tehditle karşılaşmadan önce bilgi güvenliğine ilişkin farkındalık yaratma çabası da göstermemektedir (Öztemiz ve Yılmaz 2013). Bunun sonucu olarak kaybettiğimiz sağlığımız ya da bilgimiz her ne olursa olsun artık geri dönüşü olmayacağının bilinmesi gerekir. Bu bilinçle, toplumun bilgi güvenliği konusunda sosyal ve çalışma hayatlarındaki konumlarına göre farkındalıklarının artırılması için gerekli olan eğitimlerin verilmesi gerekmektedir. Çünkü bilgi güvenliği farkındalığı olmayan bireyler bilgi güvenliği çemberinin çürük halkaları olarak bu sürecin aksamasına neden olacaklardır (Mart 2012).

Örneğin, görevi nedeniyle telefonda hangi bilginin verilip verilmeyeceği konusunda farkındalığı olmayan bir görevliden telefon görüşmeleriyle alınacak bilgiler siber saldırı yapabilmek için gerekli olan saldırıların bir parçasını oluşturabilir. Yüksek seviyede bilgi sistemlerinin güvenliğinin sağlanması için insan faktörü dikkate alınmalı ve bilgi sistemleriyle doğrudan veya dolaylı olarak ilişkide bulunan tüm görevliler bilgi güvenliği konusunda eğitilmelidir (Vural *et al.* 2009).

## 2.9 Genç Yaşta Bilgi Güvenliği Farkındalığı Edinilmesinin Önemi

Eckertova (2013)'ya göre; çocuklar, özellikle de gençler hepsi birbiri ile iletişim kapasitesine sahip, hergün gelişen ve kullanılması için sürekli cazip hale getirilen teknolojiler ile kuşatılmış bulunmaktadır. Bu teknolojilerin belki de en önemli ortak özelliği internete bağlı olmalarıdır. Ancak, iletişim açısından büyük kolaylık olarak görülen bu gelişmeler, aynı zamanda gençleri çeşitli tehlikelere de açık hale

getirmektedir. Yani teknoloji hedeflenen kurbana ulaşmak için oldukça elverişli bir araç da olabilmektedir. Bazen bir tehdit bazen de sosyal ağlarda dikkatsizce yapılan kişisel bilgi paylaşımları, gençleri tehlikeli ve sıkıntılı durumlara sokabilmektedir. İnsanlar internet ortamında gerçek yaşamdakinden farklı davranabilmekte, rahatlıkla bilgi, resim ve video paylaşabilmektedirler. Ancak bu paylaşımlar bazen arkadaşlarla sınırlı kalmayabilmektedir. Sıklıkla bu bilgiler suistimale maruz kalıp, sonrasında tehdit oluşturabilmektedir (Güldüren *et al.* 2016).

Bintziou vd. (1999), bilgi güvenliğine yönelik eğitim için en uygun dönemin ortaöğretim olduğunu ifade etmektedir. Bu yaşlarda insan bilişim cihazları ile ilk defa ciddi anlamda karşılaşır ve korunmaya ihtiyaç duyar. Bu dönemlerde mevcut tehditlerin bilincine varır ve fikir edinir. Fakat gençleri bu tehditlere karşı korumak için çoğu zaman teknik olarak, yapabildiklerine sınırlamalar veya birtakım engellemeler getirilmektedir. Bu tarz önlemler sorunu çözmek yerine büsbütün karmaşıklaştırmakta ve sanal ortamda özgürlük talep eden gençlerin beklentilerini karşılamamaktadır. Bunun yerine, bilgi güvenliği konusunda gençlerin eğitim süreçlerine bizzat dâhil olarak, bilgi düzeylerini artırmaları gerekmektedir. Bu sayede farkındalıkları artıracak ve kendi güvenliklerini sağlama açısından sorumluluk alma yönünde çaba göstereceklerdir.

## 3. MATERYAL ve METOT

Çalışmanın uygulama kısmında analize dahil edilen öğrencilerin demografik özelliklerini ve bilgi güvenliği farkındalıklarını ölçmek için, Öğütçü (2010), Mart (2012) ve Tekerek ve Tekerek (2013)'in çalışmalarında kullanmış oldukları ölçekler değerlendirmeye alınmıştır. Analiz edilen sorulardan derlenen ölçek, 5'li Likert tarzında (1. Hiç katılmıyorum, 5. Tamamen Katılıyorum) hazırlanarak anket formu haline getirilmiştir.

Hazırlanan bu anket formu 1-30 Kasım 2016 tarihleri arasında Afyon Kocatepe Üniversitesi ANS Kampüsünde öğrenim görmekte olan öğrenciler arasından rassal olarak seçilen 550 öğrenciye uygulanmış ve ilgili veriler toplanmıştır. Mevcut anket formları arasından öğrencilerin yanıtlarken yaptıkları hatalar ve verdikleri eksik doldurulmuş anket formları çıkarıldıktan sonra, çözümlemeler geçerli olan 546 anket formu üzerinden gerçekleştirilmiştir. Derlenen verilerin analizinde betimleyici istatistiklerin ve temel istatistiksel analizlerin dışında Açıklayıcı Faktör Analizi (AFA), Doğrulayıcı Faktör Analizi (DFA) ve son yıllarda birçok bilim alanında oldukça yaygın olarak kullanılmakta olan Yapısal Eşitlik Modellemesi (YEM)'nden yararlanılmıştır. Analiz kısmında SPSS ve LISREL paket programlarından yararlanılmıştır.

AFA, birbiriyle ilişkili çok sayıda değişkeni bir araya getirerek az sayıda kavramsal olarak anlamlı yeni değişkenler (faktörler, boyutlar) keşfetmeyi amaçlayan çok değişkenli bir istatistik olarak tanımlanabilir. Daniel (1988)'e göre faktör analizi, bir grup değişkenin kovaryans yapısını incelemek ve bu değişkenler arasındaki ilişkileri, faktör olarak isimlendirilen çok daha az sayıdaki gözlenemeyen gizli değişkenler bakımından açıklamayı sağlamak üzere düzenlenmiş bir tekniktir (Stapleton 1997). Rennie (1997) ise, AFA'ni, maksimum varyansı açıklayan az sayıda açıklayıcı faktöre (kavrama) ulaşmayı amaçlayan ve gözlenen değişkenler arasındaki ilişkileri temel alan bir hesaplama mantığına sahip analitik bir teknik olarak tanımlamaktadır (Büyüköztürk 2002).

AFA genellikle ilişkili olduğu düşünülen j kadar ölçülmüş değişkenin daha az sayıdaki k kadar gözlenemeyen değişken ile açıklanması için kullanılmaktadır (Henson and Roberts 2006). Başka bir şekilde tanımlamak gerekirse, ölçülen j kadar değişkenin kendi ile oluşturduğu jxj korelasyon / kovaryans matrisinin (R-matris) içerisinde yer alan bazı değişkenlerin indirgeme işlemi sonucunda gruplanarak ya da kümelenerek k kadar doğrudan gözlenmeyen değişken veya değişkenler ile ifade edilme sürecidir (Field 2005). Bu süreçte tüm işlemler R-matris üzerinden gerçekleştirilir. Analiz öncesinde elde edilen R-matris işlemlerden sonra yeni bir R matrise dönüşür. AFA'ne bağlı oluşan sonucun kesinliği bu iki matris arasındaki farkın minimum düzeyde olmasına bağlıdır (Field 2005; Tabachnick and Fidell 1989). Dolayısıyla, araştırmacıların bu farkı minimum seviyede tutabilmek için altı önemli unsur olan; örneklem büyüklüğü, değişkenlerin oluşturduğu matrisin yapısı, matrisin faktör analizine uygunluğu, faktör çıkarım yönteminin belirlenmesi, faktör sayısının belirlenmesi ve faktörlerin rotasyonu maddelerini dikkate alması gerekmektedir (Çolakoğlu ve Büyükekşi 2014).

DFA, genel olarak literatüre bakıldığında, daha çok klasik faktör analizi çalışmalarından sonra uygulanan bir yöntem olduğunu görülmektedir. (Bollen and Long 1993; Maruyama 1998). Bu tür çalışmalarda araştırmacılar, AFA çalışmasıyla belirlemiş oldukları faktör yapılarını doğrulayıcı faktör analizine tabi tutmaktadırlar. Dolayısıyla, son derece kabul gören bir uygulama olmasına rağmen, bu tür uygulamalar aslında YEM'nin doğasıyla bir miktar çelişmektedir. Çünkü burada, veri setinin bize söylemiş olduğu faktör yapılarının test edilmesi söz konusudur bir anlamda. Ancak şunu hemen belirtmek gerekir ki, sağlam bir teorik temele sahip olmayan çalışmaların AFA sonuçları çok iyi olsa da, DFA aşamasında hüsran yaşanabilmektedir. Bu durum teorik sorunlardan kaynaklanabilse de Kline (2005) bu noktada DFA'nin AFA'ne oranla çok katı bir istatistiksel test süreci olmasından dolayı bu tür sorunların her zaman olası olduğunu bildirmektedir (İnt.Kyn.2).

YEM özellikle psikoloji, pazarlama vb. bilimlerde değişkenler arasındaki ilişkilerin değerlendirilmesinde ve modellerin testinde kullanılmaktadır (Tüfekçi ve Tüfekçi 2006). YEM, ikinci nesil veri analiz tekniği olarak (Bagozzi and Fornell 1982),

regresyon gibi birinci nesil istatistiksel tekniklere kıyasla, birçok bağımlı ve bağımsız değişkenler arasındaki ilişkilerin modellenmesi ile karmaşık bir araştırma problemini tek bir süreçte, sistematik ve kapsamlı bir şekilde ele almayı sağlamaktadır (Anderson and Gerbing 1988; Dursun ve Kocagöz 2010).

YEM gözlenen ve gözlenmeyen değişkenler arasındaki yapısal ilişkilere ait hipotezlerin test edilmesinde kullanılan kapsamlı bir istatistiksel metottur ve teorik yapıların formüle edilmesi için problemleri çözmedeki başarısı ispatlanmıştır (Reisinger and Turner 1999). Çoklu regresyon, path analizi ve faktör analizi gibi diğer çok değişkenli istatistiksel tekniklere göre daha iyi sonuçlar vermektedir. Diğer istatistiksel teknikler bağımlı ve bağımsız değişkenler arasındaki etkileşimleri dikkate alamamaktadırlar. YEM ayrıca bir model testinde istatistiksel etkinliğini ve açıklayıcılık yeteneğini tek bir kapsamlı metot ile sunabilir (Pang 1996; Yilmaz 2004). YEM değişkenler arasındaki teorik bağlantıya ait doğrusal ilişkileri ortaya koyan tahmin eden ve test eden bir metottur (Rigdon 1998; Çınar ve Saraçlı 2015).

Günümüzde uygulanan, YEM'i destekleyen istatistiksel teoriler 1970'lerin başlarında ortaya çıkmış ve birkaç yıl içerisinde sosyal bilimler araştırmacılarının dikkatini birçok araştırma alanında çekmekte gecikmemiştir. Sosyal ve davranışsal bilimlerde araştırılan soruların tanımlanma ve karmaşıklığındaki artış ve kullanıcı dostu bilgisayar yazılımlarının ortaya çıkması, araştırma hipotezlerinin testinde makul bir yaklaşım olarak YEM'e olan ilginin artmasına sebep olmuştur. YEM'in popülerleşmesinin bir diğer sebebi, araştırmacıların çoklu sayıda gözlenmiş değişkenler ile araştırmalarını aydınlatma gereksinimine daha fazla ihtiyaç duymaları olarak tanımlanabilmektedir. Temel istatistiksel yöntemlerin aksine YEM'de ölçülemeyen kavramların modele yerleştirilebilmesi yöntemin ilgi çekiciliğini artırmıştır (Tezcan 2008).

Teknik olarak YEM doğrusal yapı eşitlik setindeki bilinmeyen parametrelerin tahmin edilmesinde kullanılır. Eşitliklerdeki değişkenler genellikle doğrudan gözlenen değişkenler ile ilişkili gizil değişkenlerdir. YEM gizil değişkenler seti arasında bir nedensellik yapısının var olduğunu ve gizil değişkenlerin gözlenen değişkenler aracılığıyla ölçülebildiğini varsayar (Yılmaz ve Çelik 2005).

# 4. BULGULAR

## 4.1. Öğrencilerin Demografik Özelliklerine Ait Betimleyici İstatistikler

**Çizelge 4.1.** Ankete katılan öğrencilerin demografik özelliklerine ait betimleyici istatistikler

| Değişken | Düzey | Birim sayısı | Oran | Bilgi Güvenliği Farkındalığı | | Genel Güvenlik Bilgisi | |
|---|---|---|---|---|---|---|---|
| | | | | Ort. | S.Sap. | Ort. | S.Sap. |
| Cinsiyet | Kadın | 225 | %41,2 | 3,98 | 0,51 | 3,28 | 0,85 |
| | Erkek | 321 | %58,8 | 3,90 | 0,55 | 3,56 | 0,76 |
| Yaş | 18-19 | 129 | %23,6 | $3,80^{b}$ | ,51 | $3,27^{b}$ | 0,77 |
| | 20-21 | 259 | %47,4 | $3,95^{a}$ | 0,53 | $3,46^{a}$ | 0,81 |
| | 22-23 | 129 | %23,6 | $4,01^{a}$ | 0,56 | $3,55^{a}$ | 0,83 |
| | 24 ve üzeri | 29 | %5,3 | $4,07^{a}$ | 0,46 | $3,55^{a}$ | 0,84 |
| Bölüm | Elektrik-Elektronik Mühendisliği | 112 | %20,5 | $4,01^{a}$ | 0,47 | 3,42 | 0,74 |
| | İktisat | 89 | %16,3 | $3,75^{b}$ | 0,59 | 3,46 | 0,87 |
| | İstatistik | 13 | %2,4 | $3,61^{b}$ | 0,57 | 3,82 | 0,50 |
| | İşletme | 147 | %26,9 | $3,96^{a}$ | 0,50 | 3,36 | 0,83 |
| | Mekatronik Mühendisliği | 56 | %10,3 | $3,88^{ab}$ | 0,57 | 3,51 | 0,72 |
| | Makine Müh. | 33 | %6,0 | $3,98^{a}$ | 0,44 | 3,55 | 0,70 |
| | Maliye | 35 | %6,4 | $4,00^{a}$ | 0,37 | 3,44 | 0,79 |
| | U.T.F | 61 | %11,2 | $4,05^{a}$ | 0,64 | 3,49 | 0,99 |
| Sınıf | Hazırlık | 36 | %6,6 | $3,89^{ab}$ | 0,41 | 3,44 | 0,75 |
| | 1 | 34 | %6,2 | $3,38^{c}$ | 0,70 | 3,24 | 0,89 |
| | 2 | 231 | %42,3 | $3,91^{b}$ | 0,51 | 3,41 | 0,82 |
| | 3 | 198 | %36,3 | $4,03^{a}$ | 0,50 | 3,48 | 0,81 |
| | 4 | 47 | %8,6 | $4,09^{a}$ | 0,52 | 3,64 | 0,72 |
| İnternet Kullanım Yılı | 0-5 | 39 | %7,1 | 3,96 | 0,55 | $3,52^{ab}$ | 0,87 |
| | 5-10 | 328 | %60,1 | 3,94 | 0,50 | $3,35^{b}$ | 0,77 |
| | 10 yıldan fazla | 179 | %32,8 | 3,90 | 0,60 | $3,60^{a}$ | 0,85 |
| İnternet Bağlanma Yeri | Ev | 286 | %52,4 | $3,91^{ab}$ | 0,55 | 3,50 | 0,78 |
| | Okul | 40 | %7,3 | $3,79^{b}$ | 0,65 | 3,47 | 0,81 |
| | Yurt | 219 | %40,1 | $3,99^{a}$ | 0,49 | 3,36 | 0,84 |
| İnternet Kullanım Sıklığı | 0-1 saat | 18 | %3,3 | 3,93 | 0,73 | 3,31 | 0,88 |
| | 1-4 saat | 234 | %42,9 | 3,95 | 0,52 | 3,49 | 0,75 |
| | 4 saatten fazla | 294 | %53,8 | 3,92 | 0,53 | 3,41 | 0,85 |
| İnternet Kullanım Amacı | Araştırma | 50 | %9,2 | 4,06 | 0,53 | 3,56 | 0,85 |
| | İletişim(e-mail) | 73 | %13,4 | 3,94 | 0,51 | 3,53 | 0,78 |
| | Sosyal Medya | 276 | %50,5 | 3,91 | 0,54 | 3,41 | 0,79 |
| | Gündemi Takip | 48 | %8,8 | 3,94 | 0,56 | 3,34 | 0,85 |
| | Eğlence | 99 | %18,1 | 3,91 | 0,52 | 3,45 | 0,86 |
| İnternet Ortamı Güvenli mi? | Evet | 144 | %26,4 | 3,76 | 0,59 | 3,53 | 0,74 |
| | Hayır | 402 | %73,6 | 3,99 | 0,50 | 3,41 | 0,83 |
| Sosyal Ağ Kullanıyor musunuz? | Evet | 502 | %91,9 | 3,94 | 0,53 | 3,45 | 0,80 |
| | Hayır | 44 | %8,1 | 3,92 | 0,54 | 3,42 | 0,88 |
| Şifrenizi Paylaşır mısınız? | Evet | 262 | %48,0 | 3,93 | 0,55 | 3,43 | 0,83 |
| | Hayır | 284 | %52,0 | 3,94 | 0,52 | 3,46 | 0,79 |

Ankete katılan öğrencilerin demografik özelliklerine ait betimleyici istatistikler Çizelge 4.1'de sunulmuştur. Çizelge 4.1 incelendiğinde, katılımcıların %41,2'sinin kadınlardan, %58,8'inin ise erkeklerden oluştuğu görülürken, %23,6'sı 18-19 yaş gurubunda, %47,4'ü 20-21 yaş grubunda, %23,6'sının 22-23 yaş grubunda ve %5,3'ünün ise 24 yaş ve üzeri yaş grubunda bulundukları görülmektedir. Öğrencilerin %20,5'i Elektrik Elektronik Mühendisliği, %16,3'ü İktisat, %2,4'ü İstatistik, %26,9'u İşletme, %10,3'ü Mekatronik Mühendisliği, %6'sı Makine Mühendisliği, %6,4'ü Maliye ve %11,2'si Uluslar Arası Ticaret ve Finansman bölümlerinde okudukları, %6,6'sı hazırlık sınıfı, %6,2'si 1. Sınıf, %42,3'ü 2. Sınıf, %36,3'ü 3. Sınıf ve %8,6'sı 4. Sınıf öğrencisi oldukları belirtilmiştir. Katılımcıların %7,1'i 0-5 yıl, %60,1'i 5-10 yıl ve %32,8'i 10 yıldan fazla süredir internet kullandıklarını belirtirken, %52,4'ü evden, %7,3'ü okuldan ve %40,1'i yurttan internete bağlandıklarını belirtmişlerdir. Öğrencilerin %3,3'ü 1 saat ve daha az, %42,9'u 1-4 saat ve %53,8'i 4 saatten fazla internet kullanım sıklıklarını nitelendirmiş olup, %9,2'si araştırma, %13,4'ü iletişim, %50,5'i sosyal medya, %8,8'i gündemi takip ve %18,1'i ise eğlence (oyun, müzik v.b) amaçlı interneti kullandıklarını belirtmişlerdir. Öğrencilerin %26,4'ü internet ortamının güvenli olduğunu, %73,6'sı internet ortamının güvenli olmadığını, %91,9'u sosyal ağ kullandığını %8,1'i sosyal ağ kullanmadığını ve %48'i şifresini paylaşabileceğini, %52'si ise şifresini paylaşmayacağını belirtmişlerdir.

## 4.2. Öğrencilerin Bilgi Güvenliği Farkındalığı (BGF) ve Bilgi Güvenliği Kazanımlarının (BGK) demografik özelliklerine göre farklılık gösterip göstermediğine ilişkin t testi ve varyans analizi sonuçları

Öğrencilerin BGF ve BGK'nın demografik özelliklerine göre farklılık gösterip göstermediğine ilişkin hipotezler ile istatistiksel olarak anlamlı bulunan t testi ve varyans analizi sonuçları aşağıdaki çizelge (4.2 - 4.7)'de verilmiştir.

Öğrencilerin cinsiyetlerine göre BGK ortalamaları için t testi sonuçları çizelge 4.2'de sunulmuştur.

- **H0:** Öğrencilerin BGK puan ortalamaları cinsiyete göre anlamlı bir farklılık göstermez.
- **H1:** Öğrencilerin BGK puan ortalamaları cinsiyete göre anlamlı bir farklılık gösterir.

**Çizelge 4.2** Cinsiyetlerine göre BGK ortalamaları için t testi sonuçları

| **Değişken** | ***t* istatistiği** | **Serbestlik Derecesi** | ***p*** |
|---|---|---|---|
| BGK | -3,914 | 543 | 0,000* |

Çizelge 4.2'ye göre öğrencilerin BGK'na ait ortalamalarının cinsiyetlere göre anlamlı bir farklılık gösterdiği ($p<0,05$) tespit edilmiş olup, çizelge 4.1'deki ortalamalar incelendiğinde BGK yönünden erkeklerin daha fazla bilgiye sahip oldukları görülmektedir.

Yaşlarına göre BGF ve BGK ortalamaları için varyans analizi sonuçları çizelge 4.3'de sunulmuştur.

- $\mathbf{H_0}$: Öğrencilerin BGF puan ortalamaları yaşlarına göre anlamlı bir farklılık göstermez.
- $\mathbf{H_1}$: Öğrencilerin BGF puan ortalamaları yaşlarına göre anlamlı bir farklılık gösterir.
- $\mathbf{H_0}$: Öğrencilerin BGK puan ortalamaları yaşlarına göre anlamlı bir farklılık göstermez.
- $\mathbf{H_1}$: Öğrencilerin BGK puan ortalamaları yaşlarına göre anlamlı bir farklılık gösterir.

**Çizelge 4.3** Yaşlarına göre BGF ve BGK ortalamaları için varyans analizi sonuçları

| Değişken | Değişim Kaynağı | Kareler Toplamı | Serbestlik Derecesi | Kareler Ortalaması | F | *p* |
|---|---|---|---|---|---|---|
| BGF | Gruplar Arası | 3,529 | 3 | 1,176 | 4,115 | 0,007* |
| | Gruplar içi | 154,947 | 542 | 0,286 | | |
| | Genel | 158,476 | 545 | | | |
| BGK | Gruplar Arası | 5,831 | 3 | 1,944 | 2,958 | 0,032* |
| | Gruplar içi | 356,120 | 542 | 0,657 | | |
| | Genel | 361,950 | 545 | | | |

Çizelge 4.3'e göre öğrencilerin, BGF ve BGK ortalamalarının yaşlarına göre anlamlı bir farklılık gösterdiği tespit edilmiştir (her iki değişken içinde $p<0,05$). Çizelge 4.1'deki ortalamalar incelendiğinde, 18-20 yaş grubunda bulunan öğrencilerin diğer yaş gruplarına göre BGF'nın ve BGK'nın daha düşük olduğu, 24 yaş ve üzeri olanların ise daha yüksek olduğu tespit edilmiştir. Yani yaş arttıkça hem BGK'nın hemde farkındalıklarının arttığı görülmektedir.

Bölümlerine göre BGF ortalamaları için varyans analizi sonuçları çizelge 4.4'te sunulmuştur.

- **$H_0$:** Öğrencilerin BGF puan ortalamaları bölümlerine göre anlamlı bir farklılık göstermez.
- **$H_1$:** Öğrencilerin BGF puan ortalamaları bölümlerine göre anlamlı bir farklılık gösterir.

**Çizelge 4.4** Bölümlerine göre BGF ortalamaları için varyans analizi sonuçları

| Değişken | Değişim Kaynağı | Kareler Toplamı | Serbestlik Derecesi | Kareler Ortalaması | F | *p* |
|---|---|---|---|---|---|---|
| BGF | Gruplar Arası | 6,511 | 7 | 0,930 | 3,293 | 0,002* |
| | Gruplar içi | 151,964 | 538 | 0,282 | | |
| | Genel | 158,476 | 545 | | | |

Çizelge 4.4'e göre öğrencilerin BGF puan ortalamalarının okudukları bölüme göre anlamlı bir farklılık gösterdiği ($p<0,05$) tespit edilmiştir. Çizelge 4.1'deki ortalamalar

incelendiğinde, İktisat ve İstatistik bölümü öğrencilerinin BGF ortalamalarının diğer bölüm öğrencilerine göre daha düşük olduğu, en yüksek puan ortalamasının ise U.T.F bölümü öğrencilerine ait olduğu tespit edilmiştir.

Sınıflarına göre BGF ortalamaları için varyans analizi sonuçları çizelge 4.5'te sunulmuştur.

- **$H_0$**: Öğrencilerin BGF puan ortalamaları sınıflarına göre anlamlı bir farklılık göstermez.
- **$H_1$**: Öğrencilerin BGF puan ortalamaları sınıflarına göre anlamlı bir farklılık gösterir.

**Çizelge 4.5** Sınıflarına göre BGF ortalamaları için varyans analizi sonuçları

| **Değişken** | **Değişim Kaynağı** | **Kareler Toplamı** | **Serbestlik Derecesi** | **Kareler Ortalaması** | **F** | ***p*** |
|---|---|---|---|---|---|---|
| BGF | Gruplar Arası | 13,226 | 4 | 3,306 | 12,315 | 0,000* |
| | Gruplar içi | 145,250 | 541 | 0,268 | | |
| | Genel | 158,476 | 545 | | | |

Çizelge 4.5'e göre öğrencilerin BGF puan ortalamalarının okudukları sınıfa göre anlamlı bir farklılık gösterdiği ($p<0,05$) tespit edilmiştir. Öğrencilerin sınıf düzeylerine bakıldığında BGF'nın 3. ve 4. sınıflarda aynı ve diğer gruplara göre daha yüksek olduğu tespit edilirken 1. Sınıf öğrencilerinin BGF'nın gruplar arasında en düşük seviyede olduğu tespit edilmiştir.

İnternet kullanım yıllarına göre BGK ortalamaları için varyans analizi sonuçları çizelge 4.6'da sunulmuştur.

- **$H_0$:** Öğrencilerin BGK puan ortalamaları internet kullanım yıllarına göre anlamlı bir farklılık göstermez.
- **$H_1$:** Öğrencilerin BGK puan ortalamaları internet kullanım yıllarına göre anlamlı bir farklılık gösterir.

**Çizelge 4.6.** İnternet kullanım yıllarına göre BGK ortalamaları için varyans analizi sonuçları

| Değişken | Değişim Kaynağı | Kareler Toplamı | Serbestlik Derecesi | Kareler Ortalaması | F | *p* |
|---|---|---|---|---|---|---|
| BGK | Gruplar Arası | 7,857 | 2 | 3,928 | 6,024 | 0,003* |
| | Gruplar içi | 354,094 | 543 | 0,652 | | |
| | Genel | 361,950 | 545 | | | |

Çizelge 4.6'ya göre öğrencilerin BGK puan ortalamalarının internet kullanım yıllarına göre anlamlı bir farklılık gösterdiği ($p<0,05$) tespit edilmiştir. Çizelge 4.1'deki ortalamalar incelendiğinde, 10 yıl ve daha fazla süredir internet kullananların BGK'nın daha fazla olduğu, en az farkındalığa sahip grubun ise 5-10 yıldır internet kullananlar olduğu tespit edilmiştir

İnternet ortamının güvenli bulunup, bulunmadığına göre BGF ortalamaları için varyans analizi sonuçları çizelge 4.7'de sunulmuştur.

Çizelge 4.7'ye göre incelendiğinde öğrencilerin internet ortamını güvenli bulup bulmamaları, BGF'na göre anlamlı bir farklılık göstermiştir ($p<0,05$). BGF ortalamaları incelendiğinde internet ortamını güvenli bulmayanların BGF daha yüksek olduğu tespit edilmiştir.

**Çizelge 4.7.** İnternet ortamının güvenliğine göre BGF ortalamaları için t testi sonuçları

| Değişken | *t* istatistiği | Serbestlik Derecesi | *p* |
|---|---|---|---|
| BGF | -4,573 | 544 | 0,000* |

### 4.3. Öğrencilerin BGK ve BGF'na İlişkin AFA Sonuçları

BGK ve BGF ölçeklerinde yer alan sorular (maddelerin / değişkenlerin) için gerçekleştirilen AFA sonuçlarına göre BGK (GGT) Tehditler ve (GGO) Önlemler olmak üzere iki boyut, BGF ise (IG) İnternet Güvenliği, (SMK) Sosyal Medya Kullanımı, (ITA) İnternet tarayıcısı ve Ağ Güvenliği, (SO) Şifre Oluşturma, (SMT) Sosyal Medya Tuzakları olmak üzere beş boyut olarak ortaya çıkmıştır.

BGK'na ilişkin AFA'ne ait bulgular çizelge 4.8'de, BGF'na ilişkin AFA'ne ait bulgular ise çizelge 4.9'da, verilmiştir. AFA'de yer alan BGK'na ilişkin maddelerin geneli için güvenirlilik katsayısı olan Cronbach's Alpha değeri 0.912 olarak, BGF'na ilişkin maddelerin geneli için ise bu değer 0.839 olarak hesaplanmıştır. Bu değerlere göre kullanılan ölçeğin güvenilir olduğu söylenebilir.

**Çizelge 4.8.** BGK değişkenlerine ait AFA Sonuçları ve Cronbach's α değerleri.

| **Faktörler/Maddeler** | **Faktör Yükü** | **Özdeğer** | **Açıklanan Varyans (%)** | **α** |
|---|---|---|---|---|
| **GGT. Tehditler** | | 6.343 | 32.385 | .887 |
| **ISAX1.** Sahte virüs koruma yazılımının ne olduğunu biliyorum. | .812 | | | |
| **ISAX2.** Kimlik hırsızlığına karşı alınması gereken güvenlik tedbirlerini biliyorum. | .795 | | | |
| **ISAX3.** Bilgisayarıma casus yazılım yüklenmesini engelleme yöntemlerini biliyorum. | .764 | | | |
| **ISAX4.** Kötü niyetli yazılımlara (malware) karşı alınması gereken güvenlik tedbirlerini biliyorum. | .722 | | | |
| **ISAX5.** Sosyal mühendislik saldırısına uğramamak için nasıl hareket etmem gerektiğini biliyorum. | .651 | | | |
| **ISAX6.** Bilgisayarımda casus yazılım (spyware) olup olmadığını anlayabilirim. | .630 | | | |
| **ISAX7.** Bilgisayarıma zararlı kod (maliciouscode) bulaşıp bulaşmadığını anlayabilirim. | .612 | | | |
| **GGO. Önlemler** | | 1.259 | 26.092 | .835 |
| **ISAY1.** Bilgi sistemlerinde kullanılan virüs koruma yazılımını nasıl kullanacağımı biliyorum. | .822 | | | |
| **ISAY2.** Taşınabilir cihazlara (portabledevices) yönelik fiziksel güvenliği sağlamak ile ilgili dikkat edilmesi gereken konuları biliyorum. | .786 | | | |
| **ISAY3.** Bilgisayarımdaki virüs koruma yazılımının gerçek zamanlı koruma (realtimeprotection) özelliğini kullanmaktayım. | .725 | | | |
| **ISAY4.** USB sürücülerini kullanırken dikkat edilmesi gereken hususları biliyorum. | .577 | | | |
| **ISAY5.** Taşınabilir cihazlara yönelik veri güvenliği ile ilgili dikkat edilmesi gereken konuları biliyorum. | .582 | | | |
| **ISAY6.** Bilgisayarımdaki virüs koruma yazılımının otomatik güncelleştirme yapmasını sağlayabilirim. | .522 | | | |

**Çizelge 4.9.** BGF değişkenlerine ait AFA Sonuçları ve Cronbach's α değerleri.

| Faktörler/Maddeler | Faktör Yükü | Özdeğer | Açıklanan Varyans (%) | α |
|---|---|---|---|---|
| **IG. İnternet Güvenliği** | | 1.753 | 12.884 | .730 |
| **A1.** Teknolojik cihazıma zararlı yazılımların bulaşması halinde ne gibi belirtilerinin olabileceğinin farkındayım. | .748 | | | |
| **A2.** İnternette gezinirken bilmediğim linkleri tıklamamam gerektiğini, aksi durumda kullandığım teknolojik cihaza zararlı yazılımların bulaşabileceğinin farkındayım. | .719 | | | |
| **A3.** Online alışveriş ve online bankacılık işlemlerimi güvenirliğinden emin olmadığım bir ağ üzerinden gerçekleştirmemem gerektiğinin farkındayım. | .621 | | | |
| **A4.** Online alışveriş ve online bankacılık işlemlerini kesinlikle kendime ait olmayan bir elektronik cihaz üzerinden gerçekleştirmemem gerektiğinin farkındayım. | .602 | | | |
| **A5.** Online kullandığım her hesap ve uygulama için farklı şifreler kullanmam bilgi güvenliğim açısından önemli olduğunun farkındayım. | .518 | | | |
| **SMK. Sosyal Medya Kullanımı** | | 4.894 | 14.011 | .785 |
| **B1.** Sosyal medyada tanımadığım kişilerin arkadaşlık isteklerini kabul ettiğimde, güvenlik açıklığına neden olabileceğimi biliyorum. | .773 | | | |
| **B2.** Sosyal medya sitelerindeki kullanıcı duvarımın herkese açık olmasının, güvenlik sorunu oluşturacağının farkındayım. | .828 | | | |
| **B3.** Sosyal Medya sitelerinde paylaştığım fotoğrafların kötü amaçlı kullanılabileceğinin farkındayım. | .718 | | | |
| **B4.** Sosyal medya sitelerinde konum bilgilerimi paylaşmamın güvenlik sorununa neden olabileceğinin farkındayım. | .694 | | | |
| **ITA. İnternet Tarayıcısı ve Ağ Güvenliği** | | 4.192 | 27.395 | .765 |
| **C1.** Hangi siteye girdiğim ve ne kadar kaldığımın kaydının, çerezler bölümünde tutulduğunun farkındayım. | .698 | | | |
| **C2.** İnternete bağlandığım herhangi bir ağdan bilgilerimin paket dinleyiciler tarafından izlenebileceğinin farkındayım. | .735 | | | |
| **C3.** Tarayıcıma, doğru web adresini yazmama rağmen sahte web sayfasına yönlendirilebileceğimin farkındayım. | .720 | | | |
| **SO. Şifre Oluşturma** | | 1.171 | 10.099 | .569 |
| **D1.** Şifrelerimi ayda bir değiştirmemin ve son beş şifremi tekrar kullanmamam gerektiğinin, bilgi güvenliği açısından önemli olduğunu düşünüyorum. | .654 | | | |
| **D2.** Güçlü bir şifre oluşturmam için şifremin, karmaşık ve uzun olmasının, güvenliğimi artıracağının farkındayım. | .672 | | | |
| **D3.** Şifrelerimi oluştururken kendimle ilgili herhangi bir bilgi bulundurmamaya ve karmaşık şifreler kullanmam gerektiğinin farkındayım. | .701 | | | |

**Çizelge 4.9. (Devam)** BGF değişkenlerine ait AFA Sonuçları ve Cronbach's α değerleri.

| **Faktörler/Maddeler** | Faktör Yükü | Özdeğer | Açıklanan Varyans (%) | α |
|---|---|---|---|---|
| **SMT. Sosyal Medya Tuzakları** | | 1.058 | 9.428 | .631 |
| **E1.** Bazı sosyal ağlara bağlanmam durumunda, konum bilgilerimin görünebilineceğinin farkındayım. | .573 | | | |
| **E2.** Sosyal ağlar üzerinden kullandığım uygulamaların iznim dışında paylaşım yapabileceğinin farkındayım. | .827 | | | |
| **E3.** Uygulama yazılımlarında bulunan kullanıcı bilgilerimin anket, reklam ve pazarlama gibi kurumlara satılabilineceğinin farkındayım. | .705 | | | |

## 4.4. Öğrencilerin BGK ve BGF'na İlişkin DFA Sonuçları

Öğrencilerin BGF ve BGK'nın alt boyutları arasındaki ilişkiyi ortaya koyabilmek için DFA uygulamıştır.

### 4.4.1 Öğrencilerin BGF'na İlişkin DFA Sonuçları

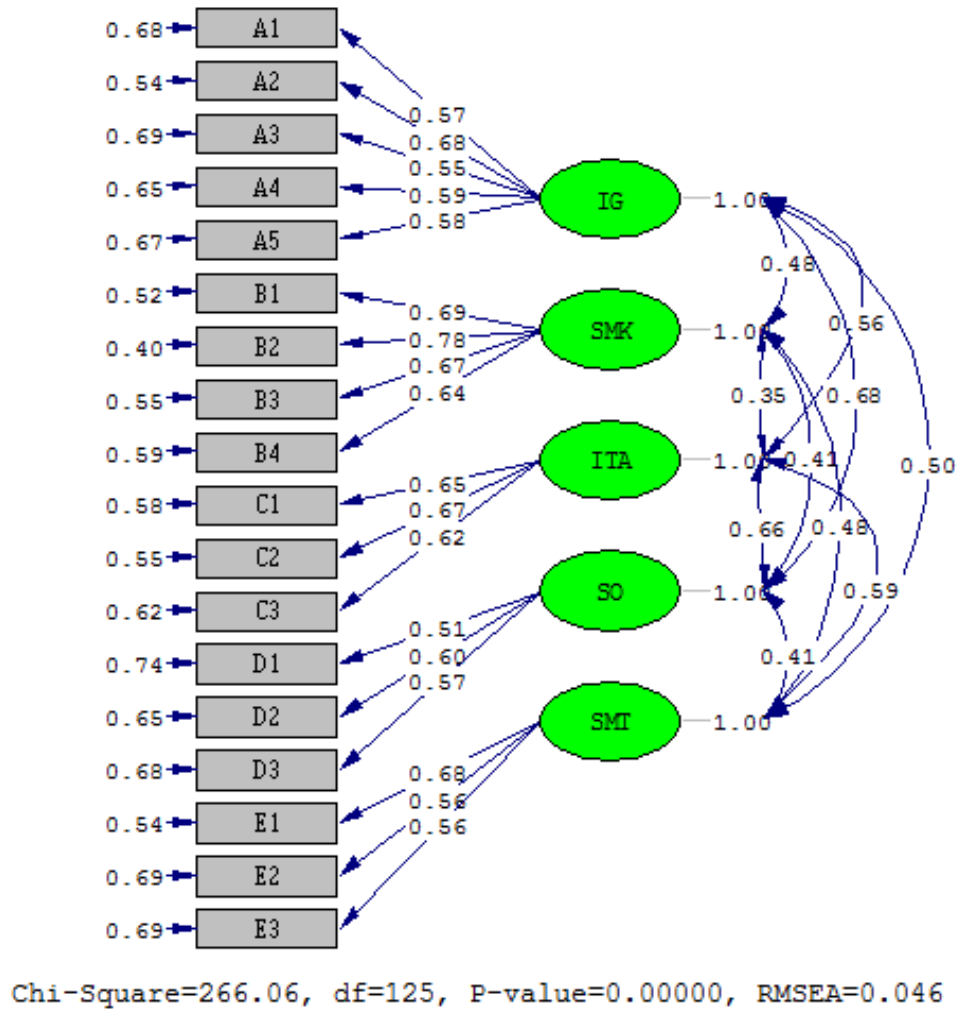
Öğrencilerin BGF'nın alt boyutları olan İnternet Güvenliği, Sosyal Medya Kullanımı, İnternet Tarayıcısı ve Ağ Güvenliği, Şifre Oluşturma ve Sosyal Medya Tuzakları arasındaki ilişkiyi ortaya koyabilmek için uygulanan DFA'ya ilişkin veriler, çizelge 4.10, çizelge 4.11 ve şekil 5.1'de verilmiştir.

BGF'nın DFA modeli için hesaplanan uyum kriterlerine ait değerler çizelge 4.10'da sunulmuştur.

**Çizelge 4.10.** BGF'nın DFA modeli için uyum kriterlerine ait değerler.

| **Uyum Kriterleri** | **Mükemmel Uyum** | **Kabul Edilebilir Uyum** | **IG/SMK/ITA/SO/SMI** |
|---|---|---|---|
| RMSEA | $0 < RMSEA < 0.05$ | $0.05 \leq RMSEA \leq 0.10$ | 0.046 |
| NFI | $0.95 \leq NFI \leq 1$ | $0.90 < NFI \leq 0.95$ | 0.94 |
| NNFI | $0.97 \leq NNFI \leq 1$ | $0.95 \leq NNFI \leq 0.97$ | 0.96 |
| CFI | $0.97 \leq CFI \leq 1$ | $0.95 \leq CFI \leq 0.97$ | 0.97 |
| SRMR | $0 \leq SRMR < 0.05$ | $0.05 \leq SRMR \leq 0.10$ | 0.042 |
| GFI | $0.95 \leq GFI \leq 1$ | $0.90 \leq GFI \leq 0.95$ | 0.95 |
| AGFI | $0.90 \leq AGFI \leq 1$ | $0.85 \leq AGFI \leq 0.90$ | 0.93 |

Şekil 4.1'de kurulan modelin istatistiksel olarak anlamlılığının belirlenmesinde kullanılan ve çizelge 4.10'da verilen değerler incelendiğinde modelin uygun bir model olduğu söylenebilir. Ayrıca $\chi 2$ (125)= 266.06 ; $\chi 2/sd$ =2.128 < 3 değeri de uygun bir model olduğunun bir diğer göstergesidir.




**Şekil 4.1** BGF boyutlarına ilişkin DFA sonuçları

Öğrencilerin BGF alt boyutlarına ilişkin DFA sonuçları ve betimleyici istatistikleri çizelge 4.11'da sunulmuştur.

**Çizelge 4.11** Öğrencilerin BGF altboyutlarına ilişkin DFA sonuçları ve betimleyici istatistikleri

| Gizil Değ./Madde | Std.Yük. | T değeri | Ortalama | Standart Sapma | Cronbach's Alpha |
|---|---|---|---|---|---|
| **IG** | | | | | **0.73** |
| A1 | 0.57 | 12.77 | 3.98 | 1.01 | |
| A2 | 0.68 | 15.75 | 4.15 | 0.99 | |
| A3 | 0.55 | 12.35 | 4.14 | 0.98 | |
| A4 | 0.59 | 13.40 | 4.07 | 1.00 | |
| A5 | 0.58 | 12.99 | 3.99 | 1.09 | |
| **SMK** | | | | | **0.79** |
| B1 | 0.69 | 16.65 | 3.95 | 1.09 | |
| B2 | 0.78 | 19.16 | 4.09 | 1.02 | |
| B3 | 0.67 | 15.89 | 3.95 | 1.04 | |
| B4 | 0.64 | 15.01 | 3.85 | 1.07 | |
| **ITA** | | | | | **0.68** |
| C1 | 0.65 | 14.29 | 3.94 | 1.01 | |
| C2 | 0.67 | 14.77 | 3.65 | 0.99 | |
| C3 | 0.62 | 13.55 | 3.75 | 1.04 | |
| **SO** | | | | | **0.57** |
| D1 | 0.51 | 10.41 | 3.63 | 1.21 | |
| D2 | 0.60 | 12.16 | 3.93 | 1.15 | |
| D3 | 0.57 | 11.56 | 4.05 | 1.02 | |
| **SMT** | | | | | **0.63** |
| E1 | 0.68 | 13.85 | 3.94 | 0.99 | |
| E2 | 0.56 | 11.48 | 3.58 | 1.15 | |
| E3 | 0.56 | 11.43 | 3.63 | 1.05 | |

BGF alt boyutları olan İnternet Güvenliği, Sosyal Medya Kullanımı, İnternet Tarayıcısı ve Ağ Güvenliği, Şifre Oluşturma ve Sosyal Medya Tuzakları için Şekil 4.1.'de verilen DFA sonuçları incelendiğinde, ele alınan öğrencilerin İnternet Güvenliği Farkındalıkları üzerinde en etkili değişkenin 0.68'lık katsayı ile A2 "İnternette gezinirken bilmediğim linkleri tıklamamam gerektiğini, aksi durumda kullandığım teknolojik cihaza zararlı yazılımların bulaşabileceğinin farkındayım" değişkeni, Sosyal Medya Kullanımı Farkındalıkları üzerinde en etkili değişkenin 0.78'lık katsayı ile B2 "Sosyal medya sitelerindeki kullanıcı duvarımın herkese açık olmasının, güvenlik sorunu oluşturacağının farkındayım" değişkeni, İnternet tarayıcısı ve Ağ Güvenliği Farkındalıkları üzerinde en etkili değişkenin 0.67'lık katsayı ile C2 "İnternete bağlandığım herhangi bir ağdan bilgilerimin paket dinleyiciler tarafından izlenebileceğinin farkındayım değişkeni, Şifre Oluşturma Farkındalıkları üzerinde en

etkili değişkenin 0.60'lık katsayı ile D2 "Güçlü bir şifre oluşturmam için şifremin, karmaşık ve uzun olmasının, güvenliğimi artıracağının farkındayım" değişkeni ve Sosyal Medya Tuzakları Farkındalıkları üzerinde en etkili değişkenin 0.68'lık katsayı ile E1 "Bazı sosyal ağlara bağlanmam durumunda, konum bilgilerimin görünebilineceğinin farkındayım" değişkeni olduğu görülmektedir.

Analiz sonuçlarına göre en yüksek ilişkiye sahip iki boyut, 0.68'lik katsayı ile "İnternet Güvenliği Farkındalıkları" ile "Şifre Oluşturma Farkındalıkları" iken, en düşük ilişkiye sahip boyutlar ise 0.35'lik katsayı ile "Sosyal Medya Kullanımı Farkındalıkları" ile "İnternet Tarayıcısı ve Ağ Güvenliği Farkındalıkları" olduğu tespit edilmiştir.

### 4.4.2 Öğrencilerin BGK'na İlişkin DFA Sonuçları

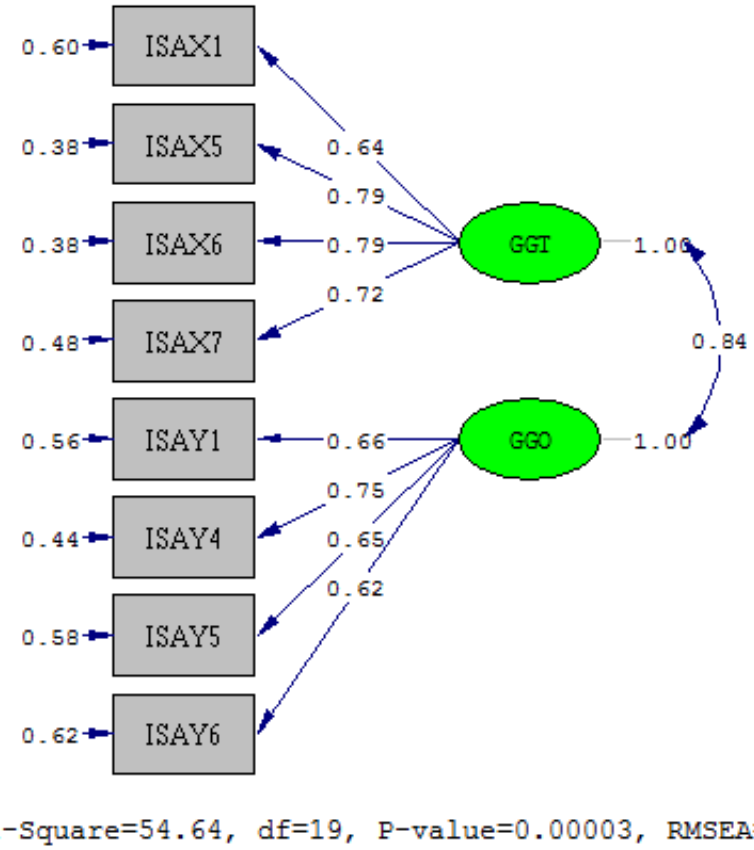
Öğrencilerin BGK'nın alt boyutları olan Tehditler ve Önlemler arasındaki ilişkiyi ortaya koyabilmek için uygulanan DFA'ya ilişkin veriler, çizelge 4.12, çizelge 4.13 ve şekil 4.2'de verilmiştir.

BGK'nın DFA modeli için hesaplanan uyum kriterlerine ait değerler çizelge 4.12'de sunulmuştur.

**Çizelge 4.12** BGK'nın DFA modeli için uyum kriterlerine ait değerler.

| Uyum Kriterleri | Mükemmel Uyum | Kabul Edilebilir Uyum | GGT/GGO |
|---|---|---|---|
| RMSEA | 0 < RMSEA <0.05 | 0.05 ≤ RMSEA ≤ 0.10 | 0.059 |
| NFI | 0.95 ≤ NFI ≤ 1 | 0.90 < NFI ≤ 0.95 | 0.98 |
| NNFI | 0.97 ≤ NNFI ≤ 1 | 0.95 ≤ NNFI ≤ 0.97 | 0.98 |
| CFI | 0.97 ≤ CFI ≤ 1 | 0.95 ≤ CFI ≤ 0.97 | 0.99 |
| SRMR | 0 ≤ SRMR <0.05 | 0.05 ≤ SRMR ≤ 0.10 | 0.029 |
| GFI | 0.95 ≤ GFI ≤ 1 | 0.90 ≤GFI ≤ 0.95 | 0.98 |
| AGFI | 0.90 ≤ AGFI ≤ 1 | 0.85 ≤ AGFI ≤ 0.90 | 0.95 |

Şekil 4.2'de kurulan modelin istatistiksel olarak anlamlılığının belirlenmesinde kullanılan çizelge 4.12'de verilen değerler ile $\chi 2$ (19)= 54.64; $\chi 2/sd$ =2.875 < 3 değeri incelendiğinde modelin uygun bir model söylenebilir.




**Şekil 4.2** BGK boyutlarına ilişkin DFA Sonuçları

Öğrencilerin BGF alt boyutlarına ilişkin DFA sonuçları ve betimleyici istatistikleri çizelge 4.13'de sunulmuştur.

**Çizelge 4.13** Öğrencilerin BGK altboyutlarına ilişkin DFA analizi sonuçları ve betimleyici istatistikleri

| Gizil Değ./Madde | Std.Yük. | *t* değeri | Ortalama | Standart Sapma | Cronbach's Alpha |
|---|---|---|---|---|---|
| **GGT** | | | | | **0.82** |
| ISAX1 | 0.64 | 15.53 | 3.21 | 1.22 | |
| ISAX5 | 0.79 | 20.70 | 3.28 | 1.24 | |
| ISAX6 | 0.79 | 20.74 | 3.33 | 1.26 | |
| ISAX7 | 0.72 | 18.33 | 3.14 | 1.25 | |
| **GGO** | | | | | **0.77** |
| ISAY1 | 0.66 | 15.93 | 3.64 | 1.15 | |
| ISAY4 | 0.75 | 18.68 | 3.55 | 1.16 | |
| ISAY5 | 0.65 | 15.64 | 3.48 | 1.18 | |
| ISAY6 | 0.62 | 14.69 | 3.70 | 1.07 | |

BGK'na ait alt boyutlar olan Tehditler ve Önlemler için şekil 4.2.'de verilen DFA sonuçları incelendiğinde, ele alınan öğrencilerin tehditlere ilişkin bilgileri üzerinde, en etkili değişkenin 0.79'lık eşit katsayı ile ISAX5 "Sosyal mühendislik saldırısına uğramamak için nasıl hareket etmem gerektiğini biliyorum" ve ISAX6 "Bilgisayarımda casus yazılım (spyware) olup olmadığını anlayabilirim" değişkenleri, önlemlere ilişkin bilgileri üzerinde, en etkili değişkenin ise 0.75'lik katsayı ile ISAY4 "USB sürücülerini kullanırken dikkat edilmesi gereken hususları biliyorum." değişkenin, etkili olduğu görülmektedir.

Şekil 4.2'de verilen doğrulayıcı faktör analizi sonuçlarına göre ele alınan öğrencilerin "Tehditler" ile "Önlemler"e ilişkin bilgileri arasında 0.84'lük pozitif bir ilişki olduğu da görülmektedir.

## 4.5 Öğrencilerin BGK ve BGF'na İlişkin YEM Sonuçları

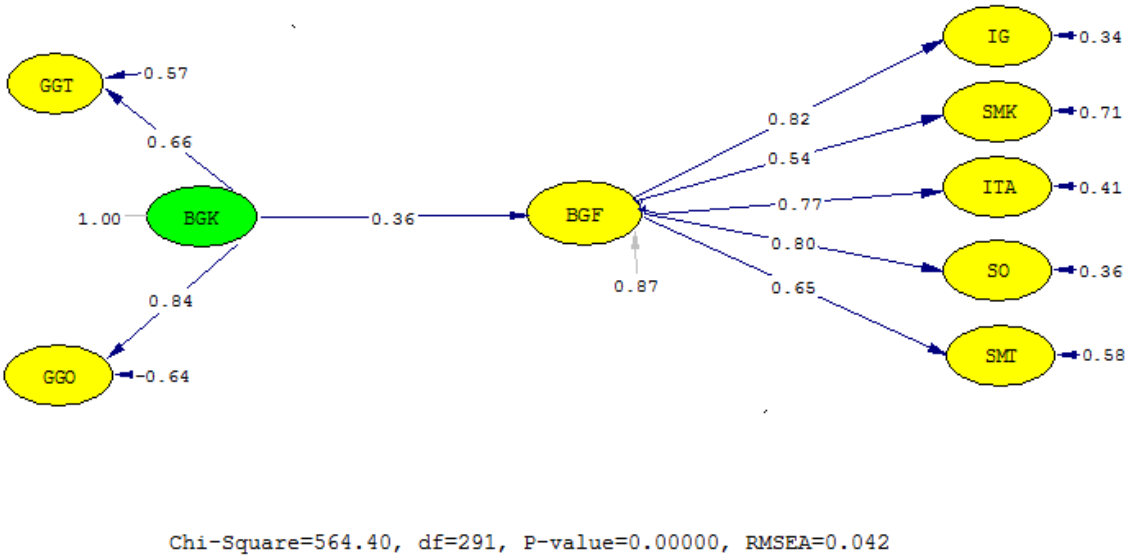
Öğrencilerin BGK ile BGF arasındaki ilişkiyi ortaya koyabilmek için uygulanan YEM'ne ilişkin veriler, çizelge 4.14, çizelge 4.15 ve şekil 4.3'de verilmiştir.

BGK ile BGF arasındaki ilişkinin modellendiği YEM için hesaplanan uyum kriterlerine ait değerler çizelge 4.14'de sunulmuştur.

**Çizelge 4.14** BGK ile BGF arasındaki ilişkiye ait YEM için uyum kriterlerine ilişkin değerler

| Uyum Kriterleri | Mükemmel Uyum | Kabul Edilebilir Uyum | BGK/BGF |
|---|---|---|---|
| RMSEA | 0 < RMSEA <0.05 | 0.05 ≤ RMSEA ≤ 0.10 | 0.042 |
| NFI | 0.95 ≤ NFI ≤ 1 | 0.90 < NFI ≤ 0.95 | 0.94 |
| NNFI | 0.97 ≤ NNFI ≤ 1 | 0.95 ≤ NNFI ≤ 0.97 | 0.96 |
| CFI | 0.97 ≤ CFI ≤ 1 | 0.95 ≤ CFI ≤ 0.97 | 0.97 |
| SRMR | 0 ≤ SRMR <0.05 | 0.05 ≤ SRMR ≤ 0.10 | 0.049 |
| GFI | 0.95 ≤ GFI ≤ 1 | 0.90 ≤GFI ≤ 0.95 | 0.93 |
| AGFI | 0.90 ≤ AGFI ≤ 1 | 0.85 ≤ AGFI ≤ 0.90 | 0.91 |

Şekil 4.3'te kurulan modelin istatistiksel olarak anlamlılığının belirlenmesinde kullanılan çizelge 4.14'de verilen değerler incelendiğinde modelin uygun bir model olduğu söylenebilir. Ayrıca $\chi 2$ (291)= 564.40; $\chi 2/sd$ =1.939 < 3 değeri de uygun bir model olduğunun bir diğer göstergesidir.




**Şekil 4.3** BGK ile BGF alt boyutlarına ilişkin YEM sonuçları

Şekil 4.3 incelendiğinde, öğrencilerin BGK üzerinde, önemler alt boyutunun 0.84, tehditler alt boyutu ise 0.66 katsayılık bir etkiye sahip olduğu, BGK'nın BGF üzerinde 0.36 katsayılık bir etkiye sahip olduğu tespit edilmiştir. BGF alt boyutlarının, BGF üzerindeki etkilerine bakıldığında sırasıyla; 0.82'lik katsayı ile internet güvenliği, 0.80'lik katsayı ile şifre oluşturma, 0.77'lik katsayı ile internet tarayıcısı ve ağ güvenliği, 0.65'lik katsalı ile sosyal medya tuzakları ve 0.54'lük katsayı ile sosyal medya kullanımı olduğu görülmektedir.

Yani BGK'nın önlemler alt boyutu üzerinde yapılacak 1 birimlik gelişimin BGK üzerinde 0.84 birimlik bir etkiye, BGK üzerinde yapılacak 1 birimlik gelişimin BGF üzerinde 0.34 birimlik bir etkiye, internet güvenliği farkındalığı üzerinde yapılacak 1 birimlik gelişimin ise BGF üzerinde 0.82 birimlik bir etkiye sahip olacağı söylenebilir.

Öğrencilerin BGK ile BGF arasında kurulabilecek araştırma hipotezi aşağıdaki gibi yazılabilir.

- **$H_1$:** Öğrencilerin BGK arttıkça BGF da artar.

**Çizelge 4.15** BGK ile BGF'na ilişkin kurulan YEM'ne ait standartlaştırılmış parametre tahmini, *t* istatistiği ve hipotez testi sonucu

| **Hipotezler** | **Yollar** | **Standartlaştırılmış Parametre Tahminleri** | ***t* istatistiği** | **Sonuç** |
|---|---|---|---|---|
| $H_1$ | (GGK)→(BGF) | 0.36 | 5.84 | **Doğrulandı** |

Çizelge 4.15'ten de görüleceği üzere çalışma kapsamında iddia edilen, öğrencilerin BGK arttıkça BGF da artar hipotezi doğrulanmıştır.

## 5. TARTIŞMA ve SONUÇ

Araştırma sonuçları incelendiğinde; kadınların bilgi güvenliği konusundaki kazanımlarının düşük olmasına karşın farkındalıklarının yüksek olması, erkeklerin ise tam tersine kazanımlarının yüksek olmasına karşın farkındalıklarının düşük olarak ortaya çıkması, kadınların bilmedikleri konulara daha temkinli yaklaştıkları şeklinde yorumlanabilir.

Ankete katılan öğrencilerin %48'lik kısmı, şifrelerini başkalarıyla paylaşmalarında herhangi bir sakınca görmemektedirler. Bu durum bilgi güvenliğinin temel unsurlarının başında gelen şifre güvenliği konusunda son derece bilinçsiz olduklarının bir göstergesidir.

Çalışma sonucuna göre; bilgi güvenliği kazanımlarının cinsiyet, yaş ve internet kullanım yıllarına göre, bilgi güvenliği farkındalıklarının ise yaş, bölüm, sınıf ve internet ortamını güvenli bulup bulmamalarına göre anlamlı bir farklılık gösterdiği tespit edilmiştir. Bu sonuca göre; her iki boyutun birden anlamlı farklılık gösterdiği değişkenin yaş kriteri olduğu görülmektedir.

Araştırmada elde edilen sonuçlar incelendiğinde, bireylerin bilgi güvenliğine yönelik farkındalıkları üzerinde en fazla etkiye sahip olan boyutunun, "İnternet Güvenliği Farkındalığı" olduğu görülmektedir. Bu sonucun, alan için de anlamlı olduğu değerlendirilebilir. Çünkü günümüzde, bilgi güvenliğini tehdit eden unsurların başında internet üzerinden çeşitli yollarla gelen saldırılar gelmektedir. Bilinçsiz internet kullanımı, bilgi güvenliğine yönelik tehdit ve saldırı yöntemlerinin çeşitlendirerek, bu tehditlere karşı alınacak önlemlerin zorlaşmasına neden olmaktadır. Bu yüzden, internet güvenliği farkındalığının artırılması, bilgi güvenliğine yönelik potansiyel risk taşıyan faktörlerin, çok yüksek oranda etkisini kaybetmesi sonucunu doğuracağı değerlendirilmektedir.

Çalışmada, tehditler ile önlemler alt boyutlarının BGK üzerindeki etkileri karşılaştırıldığında; önlemler boyutunun katsayı oranlarının daha yüksek olduğu,

dolayısıyla da bilgi güvenliğine yönelik tehlikelere karşı alınacak önlemler konusunda bireylerin bilgi düzeylerinde yapılacak artışın, BGK üzerindeki etkisinin daha yüksek olacağı değerlendirilmektedir. Bu sonuç; önlemler alt boyutunun BGF üzerindeki etkisinin tehditler alt boyutuna oranla daha yüksek olacağı şeklinde de yorumlanabilir.

Çalışmada, tehditler alt boyutu üzerinde en fazla etkiye sahip olan maddenin "Sosyal Mühendislik Saldırıları" olduğu görülmektedir. Bu sonuç, Symantec (2011) tarafından hazırlanan, 2010 yılı "İnternet Güvenlik Tehdileri Raporu"yla benzerlik göstermektedir. Raporda; saldırganların hedefledikleri kurumlarda belirli kişileri araştırdığı, ardından o kişilerin ağ ortamına girebilmek üzere kişiye özel sosyal mühendislik atakları gerçekleştirdikleri bildirilmektedir. Aynı raporda, yapılan bu saldırıların büyük çoğunluğunun da başarıya ulaştığı bilgisi verilmektedir.

Rençber ve Mete (2016)'nin bilgi güvenlik farkındalığı davranışlarını etkileyen faktörler ve bu faktörlerin etki düzeyleri üzerine yapmış oldukları çalışmada, bilgi güvenliğine yönelik tehditlere karşı oluşturulacak farkındalığı en çok etkileyen değişkenler sırasıyla şifre yönetimi, mobil internet kullanımı, e posta ve internet kullanımı ve sosyal ağ sitelerinin kullanımı ile ilgili davranışları olduğu sonucuna ulaşmıştır. Bu sonuç, araştırma sonuçları ile kıyaslandığında birinci sırada internet kullanımına yönelik farkındalık çalışması gelirken bahse konu çalışmada ilk sırada olan şifre yönetimi bizim çalışmamızdaki faktörler arasında ikinci sırada gelmektedir.

Çakır ve Kesler (2012)'in bilgisayar güvenliği üzerine yapmış olduğu çalışmasında, güvenilirliğinden emin olunmayan bağlantıları açarken dikkatli olunması gerektiğinin öneminden bahsedimiştir. Bu değerlendirme, araştırma sonucunda bahsedilen internet güvenliği farkındalığına en çok etki eden maddenin bilinmeyen linklere tıklama konusundaki bilinç olarak ortaya çıkmasını desteklemektedir.

Gökmen ve Akgün (2015) yapmış olduğu çalışmada, günümüzde bilişim sistemlerine yönelik yapılan en önemli saldırılardan birinin de oltalama saldırısı olarak adlandırılan ve kullanıcıların sahte web sitelerine yönlendirilmesi şeklinde gerçekeştirilen sosyal mühendislik saldırıları olduğunu ifade etmişlerdir.

Kapanoğlu (2016), Karadağ ve Abuhanoğlu (2015) Akgün ve Topal (2015) ve Mart (2012) yapmış oldukları çalışmalarında, araştırma sonuçlarını destekleyen şekilde, bilgi güvenliği farkındalıklarının yaşa göre anlamlı farklılıklar gösterdiğini tespit etmişlerdir.

## 6. KAYNAKLAR


Ağır, A. (2007). Bilişim toplumuna geçiş sürecinde bilgi yönetimi yaklaşımı. *İstanbul Üniversitesi İletişim Fakültesi Hakemli Dergisi*, **30**: 5-17.

Akgün, A. E., ve Keskin, H. (2003). Sosyal bir etkileşim süreci olarak bilgi yönetimi ve bilgi yönetimi süreci. *İktisadi ve İdari Bilimler Fakültesi Dergisi*, **5(1):** 1-14.

Akgün, Ö. E., ve Topal, M. (2015). Eğitim fakültesi son sınıf öğrencilerinin bilişim güvenliği farkındalıkları: Sakarya üniversitesi eğitim fakültesi örneği. *Sakarya Üniversitesi Eğitim Bilimleri Dergisi,* **5(2):** 98-121.

Anameriç, H. (2005). Bilgi sistemleri ve yönetimde bilgi sistemlerinin kullanımı. Çizgi Kitabevi, Konya.

Anderson, J. C. and Gerbing D. W. (1988), Structural Equation Modeling in Practice: A Review and Recommended Two-Step Approach. *Psychological Bulletin,* **103**: 411-423.

Anonim, 2016. BTK, 3 aylık pazar veri raporu. Bilgi Teknolojileri ve İletişim Kurumu, Ankara.

Anonim 2016, TUİK, İstatistiklerle Türkiye. Türkiye İstatistik Kurumu, yayın no: 21179, Ankara.

Aslandağ, K. (2010). Bilgi güvenliği kavramı ve bilgi güvenliği yönetim sistemleri ile şirket performansı ilişkisine dair bir uygulama. Yüksek Lisans Tezi, Gebze Yüksek Teknoloji Enstitüsü, Sosyal Bilimler Enstitüsü, Kocaeli.

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

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

Atkinson, S., Furnell, S., and Phippen, A. (2009). Securing the next generation: enhancing e-safety awareness among young people. *Computer Fraud & Security*, **7:** 13-19.

Bagozzi, R. P., and Fornell, C. (1982). Theoretical concepts, measurements, and meaning. *A second generation of multivariate analysis,* **2(2):** 5-23.

Barutçugil, İ. (2002). Bilgi Yönetimi, Kariyer Yayıncılık, İstanbul.

Baykara, M., Daş, R., ve Karadoğan, İ. (2013). Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi. 1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu, Fırat Üniversitesi, Elazığ, 20-21 Mayıs, 231-239.

Bhatt, G. D. (2000). Organizing knowledge in the knowledge development cycle. *Journal of knowledge management,* **4(1):** 15-26.

Bhatt, G. D. (2001). Knowledge management in organizations: examining the interaction between technologies, techniques, and people. *Journal of knowledge management,* **5(1):** 68-75.

Bintziou, A., Alexandris, N., and Chrissikopoulos, V. (1999). Introducing IT-security awareness in schools: the Greek case. IFIP WG 11.8 1st World Conference on Information Security Education WISE1. Citeseer.

Bollen, K.A. and Long, J.S. (1993). Testing structural equation models. A Sage Focus Edition.

Bostan, A., ve Akman, İ. (2011). Bilişim Güvenliği: Kullanıcı Açısından bir Durum Tespiti. IV. Ağ ve Bilgi Güvenliği Sempozyumu, Atılım Üniversitesi, Ankara, 25-26 Kasım, 51-56.

Büyüköztürk, Ş. (2002). Faktör analizi: Temel kavramlar ve ölçek geliştirmede kullanımı. *Eğitim Yönetimi Dergisi,* **32:** 470-483.

Can, Ö., ve Akbaş, M. F. (2014). Kurumsal Ağ ve Sistem Güvenliği Politikalarının Önemi ve Bir Durum Çalışması. *TÜBAV Bilim Dergisi,* **7(2):** 16-31.

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

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

Çakır, S. ve Kesler, M. (2012). Bilgisayar Güvenliğini Tehdit Eden Virüsler ve Antivirüs Yazılımları. XIV. Akademik Bilişim Konferansı, Uşak Üniversitesi, Uşak, 1-3 Şubat, 551-558.

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

Çınar İ. ve Saraçlı S., (2015) Öğretmenlerin Örgütsel Bağlılık ve Motivasyonları Arasındaki İlişkinin İncelenmesi: Çay ilçesi örneği. *International Online Journal of Education Sciences,* **7(4):** 266-281.

Çoban, H. (1996). Bilgi toplumuna planlı geçiş: Bilgi toplumuna geçmek için stratejik planlama ve yönetim bilgi sistemi uygulanması. Devlet Planlama Teşkilatı, Ankara.

Çolakoğlu, Ö. ve Büyükekşi, C. (2014) Açımlayıcı Faktör Analiz Sürecini Etkileyen Unsurların Değerlendirilmesi. *Karaelmas Journal of Educational Sciences,* **2:**58-64.

Dedeoğlu, G. (2006). Bilişim toplumu ve etik sorunları. Alfa Aktüel, Bursa.

Demirtaş, H. (2013). Bilgi güvenliği yönetiminin gerekleri ve başarı dayanakları: Bir uygulama örneği. Yüksek Lisans Tezi, Sakarya Üniversitesi, Sosyal Bilimler Enstitüsü, Sakarya.

Doğan, K. ve Arslantekin, S. (2016). Büyük Veri: Önemi, yapısı ve günümüzdeki durum. *DTCF Dergisi,* **56.1:** 15-36.

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

Dursun Y. ve Kocagöz E. (2010) Yapısal Eşitlik Modellemesi ve Regresyon: Karşılaştırmalı Bir Analiz. *Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,* **35:** 1-17.

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

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.

Field, A. (2005). Discovering statistics using SPSS. Sage Publication, 2nd edition, London, England.

Fossi, M., Egan, G., Haley, K., Johnson, E., Mack, T., Adams, T., Blackbird, J., Low, M., Mazurek, D., McKinney D., and Wood, P. (2011). Symantec internet security threat report trends for 2010. Volume XVI.

Fussell, R. S. (2005). Protecting information security availability via self-adapting intelligent agents. Paper presented at the MILCOM 2005-2005 IEEE Military Communications Conference, 2977-2982.

Ganbat, O. (2013). Bilgi güvenliği yönetim sistemi ISO/IEC 27001 ve bilgi güvenliği risk yönetimi ISO/IEC 27005 standartlarının uygulanması. Yüksek Lisans Tezi, Ege Üniversitesi, Fen Bilimleri Enstitüsü, İzmir.

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

Gökmen, Ö. F. ve Akgün, Ö. E. (2015). Bilgisayar ve öğretim teknolojileri eğitimi öğretmen adaylarının bilişim güvenliği eğitimi verebilmeye yönelik yeterlilik algılarının incelenmesi. *İlköğretim Online* **14(4):** 1208-1221

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

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

Gürsakal, N. (2014). Büyük Veri, Dora Basım Yayın, Bursa.

Henson, R. K., and Roberts, J. K. (2006). Use of Exploratory Factor Analysis in Published Research: Common Errors and Some Commenton Improved Practice. *Educational and Psychological Measurement,* **66:** 393-416.

Ipe, M. (2003). The praxis of knowledge sharing in organizations: A case study. Doctoral dissertation, The University of Minnesota, Minnesota, USA.

Kapanoğlu, G. (2016). Öğretmenlerin bilgi güvenliği farkındalığının incelenmesi. Yüksek Lisans Tezi, Gazi Üniversitesi, Eğitim Bilimleri Enstitüsü, Ankara.

Karaarslan, E. (2013). Siber Güvenlik Deneyleri için Ağ Benzetici ve Ağ Sınama Ortamlarının Kullanımına Dair Ön İnceleme. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri Ve Mühendisliği Dergisi,* **5:** 23-32

Karadağ, M. ve Abuhanoğlu, H. (2015). Sosyo-kültürel özelliklerin bilgi güvenliği farkındalığı üzerine etkisi: Gülhane Askeri Tıp Fakültesi Eğitim Hastanesi'nde bir çalışma. *The Journal of Academic Social Science Studies*, **36:** 379-386.

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

Kline R.B (2005). Principles and Practice of Structural Equation Modeling, Guilford Press, 2nd Edition, New York, USA.

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

Maruyama G.M. (1998) Basics of Structural Equation Modeling, SAGE Publications, 1st Edition, Thousand Oaks, USA.

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

Önel, D. ve Dinçkan, A. (2007). Bilgi güvenliği yönetim sistemi kurulumu. *TÜBİTAK UEKAE (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü) Dergisi*, **1:** 1-16.

Özdemirci, F. (2001). Belge üretimi ve kurumsal bilgi yönetimi. 21. Yüzyıla Girerken Enformasyon Olgusu Sempozyumu, Hatay, 19-20 Nisan, 179-186.

Özdemirci, F. ve Aydın, C. (2007). Kurumsal bilgi kaynakları ve bilgi yönetimi. *Türk Kütüphaneciliği,* **21(2):** 164-185.

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

Pang, N.S.K. (1996). School values and teachers' feelings: A LISREL model. *Journal of Educational Administration,* **34:** 64-83.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., and Jerram, C. (2013). The development of the human aspects of information security questionnaire (HAIS-Q). Paper presented at the 24th Australasian Conference on Information Systems (ACIS), 1-11.

Puhakainen, P. and Ahonen, R. (2006). A Design theory for information security awareness. Oule University Press, Oulu, Finland.

Rençber, Ö.F. ve Mete, S. (2016). Bilgi Güvenlik Farkındalığını Etkileyen Faktörlerin Belirlenmesi:Yüksekokul Öğrencileri Üzerine Bir İnceleme. *Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,* **18(3):**800-823.

Reisinger, Y. and Turner, L. (1999). Structural equation modeling with LISREL: Application in tourism. T*ourism Management,* **20:** 71-88.

Rennie, K.M. (1997). Exploratory And Confirmatory Rotation Strategies in Exploratory Factor Analysis. Paper Presented At The Annual Meeting Of The Southwest Educational Research Association. Austin, January 23-25.

Rigdon, E.E. (1998). Structural equation modeling. In GA Marcoulides (Ed.), Modern methods for business research, New Jersey: Lawrence Erlbaum, 251-294.

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

Stapleton, C.D. (1997). Basic Concepts And Procedures Of Confirmatory Factor Analysis. Paper Presented At The Annual Meeting Of The Southwest Educational Research Association. Austin, January 23-25.

Tabachnick, B. G. and Fidell L. S. (1989). Using Multivariate Statistics. California State University, Northridge, Harper Collins Publishers.

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

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

Tezcan, C. (2008). Yapısal Eşitlik Modelleri. Yüksek Lisans Tezi, Hacettepe Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.

Tipton, H. F. and Krause, M. (2007). Information security management handbook. Auerbach Publicaions, Auerbach, Germany.

Tüfekçi, N. ve Tüfekçİ Ö.K. (2006) Bankacılık Sektöründe Farklı Olma Üstünlüğünün ve Müsteri Sadakatinin Yarattığı Değer: Isparta İlinde bir Uygulama, *Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, **2(4):** 170-183.

Ünver, M., Canbay, C. ve Mirzaoğlu, A. G. (2009). Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler. Bilgi Teknolojileri ve İletişim Kurumu (BTK), Ankara.

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

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

Yıldız, B. (2007). Bilgi güvenliği ve e-devlet kapsamında kamu kurumlarında bilgi güvenliği yönetimi standartlarının uygulanması. Yüksek Lisans Tezi, Gebze Yüksek Teknoloji Enstitüsü, Sosyal Bilimler Enstitüsü, Kocaeli.

Yılmaz, E., Şahin, Y. L., ve Akbulut, Y. (2016). Öğretmenlerin dijital veri güvenliği farkındalığı. *Sakarya University Journal of Education,* **6(2):** 26-45.

Yılmaz, M. (2009). Enformasyon ve bilgi kavramları bağlamında enformasyon yönetimi ve bilgi yönetimi. *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi,* **49(1):** 95-118.

Yılmaz, V. (2004). Consumer behavior of shopping center choice. *Social Behavior and Personality,* **32**: 783-790.

Yılmaz, V. ve Çelik, H.E. (2005). Bankacılık sektöründe müşteri memnuniyeti ve bankaya bağlılık arasındaki ilişkinin yapısal eşitlik modelleriyle araştırılması. VII. Ulusal Ekonometri ve İstatistik Sempozyumu. İstanbul Üniversitesi, İstanbul, 26-27 Mayıs.

## İnternet Kaynakları

**1-** https://www.tdk.gov.tr, 05.03.2017

**2-** http://www.yapisalesitlik.com/yem.php?gln=dogru, 08.03.2017

# ÖZGEÇMİŞ

Adı Soyadı : Atılgan ERDOĞMUŞ
Doğum Yeri ve Tarihi : Mengen / 05.03.1978
Yabancı Dili : İngilizce
İletişim (Telefon/e-posta) : 0506 2420205 / atilgun@gmail.com

Eğitim Durumu (Kurum ve Yıl)

Lise : Yenimahalle Endüstri Meslek Lisesi - Elektrik Bölümü
Lisans : Sakarya Üniversitesi Bilgisayar Mühendisliği
Yüksek Lisans :

Çalıştığı Kurum/Kurumlar ve Yıl: Başbakanlık F-02 2004 - 2017

Yayınları (SCI ve diğer) :

Diğer konular :