ONDOKUZ MAYIS ÜNİVERSİTESİ

EĞİTİM BİLİMLERİ ENSTİTÜSÜ

İLKÖĞRETİM EĞİTİMİ ANABİLİM DALI

Fen Bilgisi Eğitimi Bilim Dalı

ONDOKUZ MAYIS ÜNİVERSİTESİ ÖĞRETMEN ADAYLARININ BİLGİ GÜVENLİĞİ FARKINDALIKLARININ BAZI DEĞİŞKENLER AÇISINDAN İNCELENMESİ

Nurhan KARAYÜCEL EFE

Danışman

Dr. Öğretim Üyesi FERGAN KARAER

YÜKSEK LİSANS TEZİ

Haziran 2019

TELİF HAKKI

2547 Sayılı Yükseköğretim Kanunu Ek Madde 40 hükümleri çerçevesinde (Ek:22/2/2018-7100/10 md.) "*Lisansüstü tezler yetkili kurum ve kuruluşlar tarafından gizlilik kararı alınmadıkça, bilime katkı sağlamak amacıyla Yükseköğretim Kurulu Ulusal Tez Merkezi tarafından elektronik ortamda erişime açılır*."

Araştırmacılar tezlerin tamamı veya bir bölümünü yazarın izni olmadan ticari veya mali kazanç amaçlı kullanamaz, yayınlayamaz, dağıtamaz ve kopyalayamaz. Ulusal Tez Merkezi Web Sayfasını kullanan araştırmacılar, tezlerden bilimsel etik ve atıf kuralları çerçevesinde yararlanırlar.

YAZARIN

Adı : Nurhan

Soyadı : KARAYÜCEL EFE

Bölümü : Fen Bilgisi Eğitimi

İmza :

Teslim Tarihi : …/…/2019

TEZİN

Türkçe Adı : Ondokuz Mayıs Üniversitesi Öğretmen Adaylarının Bilgi Güvenliği Farkındalıklarının Bazı Değişkenler Açısından İncelenmesi

İngilizce Adı : The Investigation of Ondokuz Mayis University Teacher Candidates of Information Security Awareness Levels Regarding in Terms of Some Variables

ETİK İLKELERE UYGUNLUK BEYANI

Tez yazma sürecinde bilimsel ve etik ilkelere uyduğumu, yararlandığım tüm kaynakları kaynak gösterme ilkelerine uygun olarak kaynakçada belirttiğimi ve bu bölümler dışındaki tüm ifadelerin şahsıma ait olduğunu beyan ederim.

Yazar Adı Soyadı: Nurhan KARAYÜCEL EFE

İmza: ……..

KABUL VE ONAY

Nurhan KARAYÜCEL EFE tarafından hazırlanan "**Ondokuz Mayıs Üniversitesi Öğretmen Adaylarının Bilgi Güvenliği Farkındalıklarının Bazı Değişkenler Açısından İncelenmesi**" adlı tez çalışması aşağıdaki jüri tarafından oy birliği ile Ondokuz Mayıs Üniversitesi **İlköğretim Eğitimi** Anabilim Dalı, **Fen Bilgisi Eğitimi Bilim Dalı'**nda Yüksek Lisans tezi olarak kabul edilmiştir.

Danışman: (Unvanı Adı Soyadı) **Dr. Öğretim Üyesi Fergan KARAER**

(Matematik ve Fen Bilimleri Eğitimi, Ondokuz Mayıs Üniversitesi)

Başkan: (Unvanı Adı Soyadı)

(Anabilim Dalı, Üniversite Adı) ……...

Üye: (Unvanı Adı Soyadı)

(Anabilim Dalı, Üniversite Adı) ……...

Üye: (Unvanı Adı Soyadı)

(Anabilim Dalı, Üniversite Adı) ……...

Üye: (Unvanı Adı Soyadı)

(Anabilim Dalı, Üniversite Adı) ……...

Bu tezin **İlköğretim Eğitimi** Anabilim Dalı, **Fen Bilgisi Eğitimi Bilim Dalı**'nda Yüksek Lisans tezi olması için şartları yerine getirdiğini onaylıyorum.

Tarihi: __/__/____

Prof. Dr. Ali ERASLAN

Eğitim Bilimleri Enstitüsü Müdürü

(İmza ve Mühür)

“Her zaman desteği ile yanımda olan

Başta kıymetli **Babam**

Mehmet Zeki KARAYÜCEL

olmak üzere aileme ithaf edilmiştir.”

TEŞEKKÜRLER

Yüksek lisans eğitim hayatım süresince akademik gelişimime büyük katkıları bulunan, tez çalışmalarım boyunca sabır ile özveriyle beni destekleyen değerli hocam ve tez danışmanım Sayın Dr. Öğretim Üyesi Fergan KARAER ’e teşekkürlerimi sunuyorum. Ayrıca tezin her aşamasında beni yönlendiren ve verilerin analizinde yardımlarını esirgemeyen Sayın Dr. Öğretim Üyesi Hatice KARAER ’e ayrıca teşekkür ediyorum. Tez çalışmasında özellikle anketlerin uygulanması sırasında yardımlarını gördüğüm Yüksek lisans öğrenci arkadaşlarım Dilek ÇAVUŞOĞLU ile Kevser ERDOĞAN ’a ve çalışmaya katılarak anketleri dolduran öğretmen adaylarına teşekkür ederim. Hayatımın her anında desteklerini her zaman hissettiğim, başarılarıma benden daha çok sevinen anneme, babama ve kardeşlerime, zor zamanlarda yanımda olup her an destek veren kıymetli eşime, kendisine ait zamandan fedakârlık yapmak zorunda kaldığım biricik kızıma da teşekkür ediyorum.

ONDOKUZ MAYIS ÜNİVERSİTESİ ÖĞRETMEN ADAYLARININ BİLGİ GÜVENLİĞİ FARKINDALIKLARININ BAZI DEĞİŞKENLER AÇISINDAN İNCELENMESİ

Yüksek Lisans Tezi

Nurhan KARAYÜCEL EFE

ONDOKUZ MAYIS ÜNİVERSİTESİ

EĞİTİM BİLİMLERİ ENSTİTÜSÜ

Haziran 2019

ÖZ

Günümüzde öğretmenler, bilgi ve iletişim teknolojileri yardımıyla bilgiyi dijital ortamlarda üretmekte ve saklamaktadır. Eğitim öğretim etkinliklerinde teknolojiyi sıklıkla kullanmaları beklenilen öğretmenlerin sahip oldukları bilgi ve dijital verilerin güvenliğinin farkındalığı son derece önemlidir. Bu bağlamda araştırmanın amacı, OMU Eğitim Fakültesinin yedi farklı bölümde öğrenim gören öğretmen adaylarının bilgi güvenliği farkındalık (BGF) düzeylerini belirlemek ve çeşitli değişkenler açısından incelemektir. Araştırmanın evrenini OMU Eğitim Fakültesinde eğitim-öğrenim gören öğretmen adayları oluştururken, örneklemini 2018-2019 eğitim-öğretim yılında OMU Eğitim Fakültesinin, yedi farklı bölümde 1, 2, 3 ve 4., ve üzeri sınıfta eğitim-öğretim gören 886 kadın 314 erkek olmak üzere toplam 1200 öğretmen adayı oluşturmaktadır. Araştırma, nicel araştırma modellerinden tarama modelinde gerçekleştirilmiştir. Çalışmanın verileri, üç bölümden oluşan anket ile toplanmıştır. Anketin birinci bölümde araştırmacı tarafından geliştirilen öğretmen adaylarının demografik ve coğrafik özelliklerini içeren 12 soru yer almaktadır. İkinci bölümünde, Çetinkaya, Güldüren ve Keser (2017) tarafından geliştirilen BGF ölçeği; üçüncü bölümde, araştırmacı tarafından geliştirilen bilgisayar ve internet kullanımı ile ilgili 13 soru kapalı ve bir açık uçlu soru bulunmaktadır. Araştırma kapsamında OMU Eğitim Fakültesinde eğitim-öğrenim gören 1200 öğretmen adayına üç bölümden oluşan anket uygulanmış ve araştırmada elde edilen nicel veriler SPSS 17 programı ile analiz edilmiştir. Açık uçlu sorudan elde edilen veriler içerik çözümlemesiyle nitel olarak değerlendirilmiştir. Verilerin analizinde kullanılacak istatistik teknikleri belirlemede dağılımların normal dağılım gösterip göstermediği incelenmiş ve araştırmanın pilot çalışması için normal dağılım gösterirken araştırmanın örneklemi için normal dağılım göstermemiştir. Bu nedenle nonparametrik testlerden SPSS 17 paket program ile Kruskal Wallis ve Mann-Whitney U testleri uygulanmış ve anlamlılık düzeyi $p<,01$; $p<,05$ alınmıştır. Elde edilen bulgulara göre, öğretmen adaylarının BGF 'nin olduğunu farkındalık değerlerinin cinsiyet, yaş, sınıf, akademik başarı notu, mezun olduğu lise türü, anne, baba eğitimi, bölüm, bilgisayar sahibi olma süresi, evde internet bağlantısı

olma, internette karşılaşılan zorluklar, internet sitelerine ulaşma yollarına göre farklıdır. Ayrıca internete bağlanma yeri, interneti kullanma süresi, bilgiye ulaşmak için kullanılan kişi ve araç, interneti hafta içinde kaç saat kullandığı ve e-postalarının kontrol süresine göre de farklılıkları anlamlıdır. Ancak yaşadığı yer, anne mesleği ve kardeş sayısı bağlamında farkındalıkların değişmediği gözlemlenmiştir. Buna göre öğretmen adaylarının kurallar ve bilgi gerektiren konularda farkındalık düzeylerinde anlamlı farklılıkların olduğu bulunmuştur. Geleceğin öğretmenlerinin bilgi güvenliği konusunda farkındalık düzeyleri ders ve eğitimler vb. araçlarla artırılırsa öğrencilerin BGF artırılabilir ve bunun sonucunda insan ve internet vb. bilgi güvenliği ile ilgili zararlı etkiler kontrol edilebilir.

Anahtar Kelimeler : Ondokuz Mayıs Üniversitesi, Bilgi Güvenliği, Bilgi Güvenliği Farkındalığı, Öğretmen Adayı, Bilgisayar ve İnternet Kullanma

Sayfa Sayısı : 133

Danışman : Dr. Öğ. Üyesi Fergan KARAER

THE INVESTIGATION OF ONDOKUZ MAYIS UNIVERSITY TEACHER CANDIDATES OF INFORMATION SECURITY AWARENESS LEVELS REGARDING IN TERMS OF SOME VARIABLES

MS Thesis

Nurhan KARAYÜCEL EFE

ONDOKUZ MAYIS UNIVERSITY

GRADUATE SCHOOL OF EDUCATIONAL SCIENCES

June 2019

ABSTRACT

Nowadays, teachers produce and store information in digital environments thanks to emerging information and communication technologies. Since teachers are expected to employ emerging technologies in their instructional practices, the security of their information and awareness of digital data carries at most importance. In this context, the purpose of this study to investigate the information security awareness (ISA) levels of teacher's candidates who are educated in seven different departments that attending Faculty of Education at OMU, and to analyse them in terms of various variables (gender, age, class level, academic achievement grade, graduated high school, mother and father education, department, etc.). As the scope of the study consists of teacher's candidates in different departments that attending Faculty of Education at OMU. The sample of the study consist of 1200 (886 women 314 men) teacher candidates studying in the 1st, 2nd, 3rd and 4th, and above grade of the seven different department at OMU Faculty of Education in 2018-2019 academic year. The study is a screening model, a quantitative research model. The data of the study was collected by a three-part questionnaire. In the first part of the questionnaire, there are 12 questions including the demographic and geographical characteristics of teacher candidates developed by the researcher. In the second part, there is a five-point Likert scale, i.e. "ISA Scale" developed by Çetinkaya, Güldüren and Keser (2017). In the third part, there are 13 closed-ended questions and one open-ended question about computer and internet use developed by the researcher. Within the scope of the research, three-part questionnaire was applied to 1200 teacher candidates studying at OMU Faculty of Education. The data obtained from the scale were evaluated quantitatively using SPSS and the data obtained from the open-ended questions were evaluated qualitatively by content analysis in the research. The researchers tested the data to find that they were whether normally distributed, or not and as a result of the test of normality they resolved to use non-parametric statistical techniques. Thus, Kruskal Wallis and Mann Whitney-U tests

were applied with SPSS 17 package program which is one of the nonparametric tests. Significance level in the test p <, 01; P <, 05 taken. Descriptive statistics indicated that teacher candidate's ISA levels were unsatisfactory. While the awareness levels varied with regard to gender, age, class, academic achievement grade, high school type of graduation, mother, father education, department, time to have computer, having internet connection at home, difficulties encountered in internet, access to internet sites, internet connection place, internet usage time, information person and vehicle used to access the internet, how many hours he used the internet during the week, and the time period for checking his e-mails; it did not change with regard to place of residence, mother's profession and number of siblings. With reference to it was found that there were significant differences in the awareness levels of the teacher candidate about issues requiring rules and knowledge. If these courses' hours can be increased, teacher candidate's ISA can be enhanced and negative effects of related to information security such as people and the internet can be controlled.

Key Words : Ondokuz Mayıs University, Information Security, Information Security Awareness, Teacher Candidate, Using Computer and Internet

Number of Pages : 133

Advisor : Assoc. Prof. Dr. Fergan KARAER

İÇİNDEKİLER

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

SİMGELER VE KISALTMALAR

BG: Bilgi Güvenliği

BGF: Bilgi Güvenliği Farkındalığı

BGFD: Bilgi Güvenliği Farkındalık Düzeyi

BGFÖ: Bilgi Güvenliği Farkındalık Ölçeği

BGYS: Bilgi Güvenliği Yönetim Sistemi

BÖTE: Bilgisayar ve Öğretim Teknolojileri Eğitimi

BT: Bilişim Teknolojileri

DVG: Dijital Veri Güvenliği

MEB: Millî Eğitim Bakanlığı

OMÜ: Ondokuz Mayıs Üniversitesi

PDR: Psikolojik Danışmanlık ve Rehberlik

SSL: Secure Sockets Layer (Güvenli Giriş Katmanı)

TDK: Türk Dil Kurumu

TÜBİTAK: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

TÜİK: Türkiye İstatistik Kurumu

YÖK: Yüksek Öğretim Kurumu

BİRİNCİ BÖLÜM

I. GİRİŞ

Ülkelerin ekonomik gücünün ve gelişmişliğinin ana unsurunu bilgi oluştururken, bilgi toplumunda başarılı olmanın yolu da bilgiyi üretmek, yeni teknolojilere dönüştürmektir. Son yıllarda bilim ve teknolojideki hızlı gelişmeler, bilgi ve teknoloji kavramlarını daha da geliştirip yenilenilerken, bilginin sınırları zaman veya mekân kısıtlanması olmadan hızla yayılarak içinde yaşanılan toplumları küresel olarak etkisi altına almaktadır. Nitekim geçmişte elde edilmesi güç olan günümüzde hızlı şekilde geniş kitlelere ulaşarak hayatımızın hemen hemen her alanını kaplayan cihazlar ile bunlara yüklenen uygulamalarla depolanan, paylaşılan kişisel ve yüksek seviyede önemli bilgiler, sanal dünyanın kullanıcılara ayrılan yerlerinde saklanıp, paylaşılabilir hale gelmiştir (Aslan, 2007; Berberoğlu, 2010; Güldüren, Çetinkaya ve Keser, 2016 Şahin, Çetin ve Yıldırım, 2009).

Böylece toplumdaki tüm bireylerin günlük hayatlarının her alanında yer alan bilginin korunması ile kontrolü tüm toplumu ilgilendiren, gözetilmesi ve korunması gereken bir durum haline gelirken bilgi sistemlerinde, bilgi güvenliğinin (BG) kontrolü ve denetiminde en zor olan kullanıcılar kritik öneme sahiptir (Güldüren, 2015). BG alanındaki çalışmalar, her kurumun BG bakış açısını, güvenlik önlemlerine verdikleri önem ve güvenlik politikaları geliştirmelerini; bunu yapabilmeninin öncelikli yolunun da bilgi güvenliği farkındalıklarının (BGF) artırılmasına yönelik olacağını göstermektedir. BG'nin sağlanmasında kurumların yönerge veya politikalar izlemesi ve bu politikalar uğruna yüksek harcamalar yapması gerekirken kullanıcı faktörü ve BG'nin çok boyutlu yapısı izlenecek politikaların yeniden değerlendirilmesini gerektirmektedir (Güldüren, Çetinkaya ve Keser, 2016).

BG'nin özellikle gelişip yenilenen bilgi toplumunu şekillendirecek olan olan eğitim-öğretim süreçleri ile bağlantılı eğitim sistemlerinin de BG'nin unsurları ve güvenlik kriterleri gözetilerek belirlenmesi gerekmektedir. Nitekim günümüzde internet ve bilişim teknolojilerinden (BT) faydalanılan alanların artması buna bağlı olarak yaygın olarak kullanılmasıyla başta devlet olmak üzere tüm kurumlarda birçok uygulama ve hizmetin elektronik ortama taşınması e-devlet, e-ticaret, e-belediye, e-öğrenme gibi

kavramların hayatımıza girmesini sağlamıştır. Hayatın her alanında yer alan bilginin dijital ortamlarda depolanması, transferi vb. olgularda daha önce olmayan yeni riskleri de beraberinde getirirken BG ile bilişim güvenliği kavramlarının önemini de artırmıştır (Çalık ve Çınar, 2009; Dedeoğlu, 2006; Yavuz ve Ulaş, 2013).

Gizlilik, bütünlük ve süreklilik/ kullanılabilirlik ana unsurlarından oluşan, herkes tarafından erişilen bilginin güvenli bir biçimde gönderen ve alıcı arasında bütünlüğü bozulmadan, belli bir gizlilik içinde iletilmesi BG oluşmaktadır (Vural ve Sağıroğlu, 2008). Dünyada bilgisayar ve internet kullanımı her geçen gün artmaktadır. Nitekim ülkemizde 2016 yılında 16-74 yaş grubunda %61,2; olan bilgisayar ve internet kullanımı 2017'de %66,8'e yükselmiştir (TUİK, 2017). Bilgi ve iletişim teknolojilerinin yaygın hale gelmesinin yanı sıra internet ve çevrimiçi uygulamaların artan kullanımı güvenlik zafiyetlerini meydana getirirken; elde edilmesi ve depolanması güç olan bilgi ile değişen, gelişen teknolojilerin meydana getirdiği risk faktörlerini de göz önünde bulundurularak kurum ve bireylerce korunması gerekmektedir (Baykara, Daş ve Karadoğan, 2013). Bu durumda BG'de ortaya çıkan sorunların büyük kısmının insan kaynaklı olması ile bu konuda her türlü faaliyet insanı ve eğitimini merkeze alarak yürütülmektedir. Böylece BG sağlamak toplumda sadece BG'den sorumlu kişi ve kurumların görevi olmamasının yanı sıra küreselleşen bilgi sistemleri ile doğrudan veya dolaylı yollarla bağlantı kuran, bu sistemleri kullanan tüm birey ve kurumların katkı sağlama zorunluluğu bulunmaktadır (Acılar, 2009; Tsohou, Kokolakis, Karyda ve Kiountouzis, 2008).

BG'de, korunma amaçlı BT kullanmak ya da sahip olmak için bu teknolojilere çok para harcama yerine doğru yer ve zamanda insanların bilinçlendirilmesi gerekmektedir (Gülmüş, 2010; Kruger ve Kearney, 2006; Puhakainen, 2006; Siponen, 2001; Şahinaslan, Kantürk, Şahinaslan ve Borandağ, 2009; Vardal, 2009). Sadece hayatımızı kolaylaştırmakla kalmayan bilgi ve iletişim teknolojileri ile elektronik uygulamalar, yeni BG risklerini, suç türlerini ortaya çıkarırken, dünya ve ülkemizde BG'ye olan ilgi ve ihtiyaca bağlı olarak bu alanda yapılan çalışmalar da artış göstermektedir. BG sorunları ile ilgili araştırmalar genel olarak insan kaynaklı (Kritzinger ve Smith, 2008; Mahabi, 2010; Mathisen, 2004; Penmetsa, 2010; Veiga, 2008) olmakta ve insan dışında teknik (güvenlik duvarı, sanal özel ağ, saldırı tespit/önleme sistemi, anti virüs, içerik kontrolü yazılım, veri şifreleme, kimlik doğrulama, yetkilendirme vb.)

sorunlarla ilgili çalışmalar da bulunmaktadır (Chen, Shaw ve Yang, 2006; Gülmüş, 2010; Kjorvik, 2010; Rezgui ve Marks, 2008).

Bu çalışmalarda BG'nin en zayıf halkası olarak bilgiyi kullanan, bilgiyi yöneten birey görülürken BG seviyesi kullanıcının farkındalığına bağlıdır (Cox, Connolly ve Currall, 2001; Rezgui ve Marks, 2008; Vardal, 2009). Nitekim çoğu birey BT ve iletişim teknolojilerini kullanmaları ile meydana gelecek olan risklerden ve kendilerini maddi olarak zarara uğratabilecek tehditlerden habersiz olurken saldırganın izinsiz olarak ulaştığı bilgilerin silinmesi, değiştirilmesi ile tamiri imkânsız hasarlar meydana gelmektedir (Özenç, 2007).

Toplumlarda BG geçmişte genel olarak yazılı ve basılı ortamlardaki bilgilerin fiziksel olarak güvenliğinin sağlanması olarak düşünülmesine karşılık günümüzde dijital veri güvenliği (DVG) kavramı öne çıkmaktadır. DVG, elektronik ortamlarda bulunan verinin bütünlüğünün bozulmadan, izinsiz erişenlerden korunarak saklanabilmesi ve taşınabilmesi için bilgi işleme platformlarının da güvenli hale getirilmesidir (Canbek ve Sağıroğlu, 2006; Henkoğlu ve Yılmaz, 2013; Yılmaz, Şahin ve Akbulut, 2016). Ancak DVG, doğal afetlerle güç kaynakları, kamera sistemleri ve telefon santrallerinin arızalanması, e-postalara ve bilgisayarlara virüs ile izinsiz erişim sağlanarak zararlı yazılım ile kişisel bilgilerin elde edilmesi, internet bankacılığı ve online yapılan alışverişlerde yaşanan sorunlar oluştururken bunlar arasında başlıca sorun, insanların oluşturduğu tehditlerdir (Wagner ve Brooke, 2007; Yılmaz, Şahin ve Akbulut, 2016).

Yapılan araştırmada Türkiye, Avrupa'da virüs ve istem dışı e-posta saldırılarda beşinci, olta saldırılarında sekizinci sırada yer almaktadır. Artan bu tehditlerle birlikte DVG'e ilişkin araştırmaların önemi her geçen gün daha da artmaktadır. Kişi, kurum ve kuruluşlar BG konusunda genellikle önceden önlem almadıkları, ciddi bir güvenlik sorunu ortaya çıktığında harekete geçtiklerinden özellikle yöneticilerin farkındalık ve BG konusunda dikkatli olmaları gerekmektedir (Kocamustafaoğulları, 2013). Siber saldırıların giderek arttığı günümüzde tehditler, kullanıcıların bilinçsizce ya da yeterli düzeyde eğitim sahibi olmadan teknolojiyi kullanmalarından kaynaklanmaktadır (Symantec, 2013; Tekerek, 2008). Günümüzde yaşamın her safhasında elektronik uygulamaların, iş ve günlük hayatın bir parçası haline gelerek bilişim kültürünün gelişmesini, bu kültürün en değerli varlığı olan bilginin saklanabilmesini, paylaşılabilmesini, iletilebilmesini, ağ üzerinde bulunması ile her noktadan erişilmesi

sonucu çok büyük kolaylıklar sağlarken beraberinde büyük açıklıklar ve tehlikeleri ortaya çıkararak zamanla bireysel ve kurumsal olarak kayıplara neden olmaktadır (Arıtürk, 2015; Gülmüş, 2010; Mart, 2012).

Özellikle internet kullanımının hızla artması ile sınırsız, denetimi olmayan ve yasak olan her türlü bilgi ve bireye kolay ulaşılmasının hem olumlu yanları hem de riskleri bulunmaktadır. İnternette olumsuz birçok siteye kolay erişim sağlanmak, kötü niyetli insanlarla iletişim kurmak ve birçok oyuna bağımlı hale gelmek büyük riskler arasında yer alırken, birçok kişi propaganda amaçlı yasal olmayan yollarla interneti kullanmaktadırlar (Mert, Bülbül ve Seferoğlu, 2012). Bu kullanımlar zamanla bireysel ve kurumsal olarak kayıplar meydana getirdiğinden BG'nin hem birey hem de kurumsal olarak üst seviyelere çıkarılması gerekli görülmektedir (Arıtürk, 2015; Mart, 2012).

1.1 Problem

Bilgi ve yönetilebilen BG'nin sağlanması oldukça karmaşık olup sadece teknik önlemler alınarak, BG'yi sağlamak oldukça güçtür. Özellikle başta insan hataları olmak üzere diğer faktörlerin dikkate alınmaması nedeniyle BG'nin çok iyi planlama yapılarak yönetilmesi gerekmektedir. Bu kapsamda BG'nin sağlanmasında en önemli etkenin teknolojiyi de kendisi icat eden, kullanan insan olduğu gerçeği vurgulanarak farkındalığın kazandırılmasında, risklerin en aza indirgenmesinde oldukça önemlidir (Acılar, 2009; Gülmüş, 2010; Keser ve Güldüren, 2015; Vardal, 2009; Vural, 2007). Böylece BG'nin sağlanmasının en iyi yolu insanların bilinçlenmesi ve ihtiyaç duyulan güvenlik teknolojilerinin doğru yer ve zamanda kullanılmasıyla mümkün olmaktadır (Albrechtsen, 2007; Al-Shehri, 2012; Puhakainen, 2006; Şahinaslan, Kantürk, Şahinaslan ve Borandağ, 2009).

Geliştirilen, hızla ilerleyen ve karmaşıklaşan teknolojilere bağımlı hale gelen günümüz insanı iletişimde neredeyse robotlaşma boyutuna geçerken, bu durum güvenlik sorunlarına da neden olmaktadır. Bu durumda birilerinin kazanma uğruna birilerini oldukça büyük tutarlara sahip olan maddi ve manevi kayıplarına neden olabilmektedir. Bu kapsamda eğitim politikaları ve eğiticilerin BG konusunda yeterliliğe sahip olması gelecek nesillerin bilinçli olmasını sağlarken eğitim öğretimin ana unsuru olan öğretmenlerin yetiştirildiği Eğitim Fakültelerinde BG bilincinin yerleştirilmesi, BG politikalarının en önemli noktasını oluşturmaktadır.

Buna göre çalışmanın problemini Ondokuz Mayıs Üniversitesinde (OMÜ) öğrenim gören Öğretmen adaylarının bazı demografik, coğrafik, psikolojik özellikler ile BGFD anlamlı farklılık gösterip göstermediğinin belirlenmesi oluşturmaktadır. Bu ana problemler çerçevesinde aşağıdaki alt problemler belirlenmiştir.

1- Öğretmen adaylarının demografik özellikler (cinsiyet, yaş, sınıf, akademik not ortalaması, öğrenim gördükleri bölüm, mezun olduğu lise, anne, baba eğitim düzeyleri ve meslekleri, kardeş sayısı, internet ve bilgisayar kullanım süreleri) ve bilgi güvenliği farkındalık düzeyleri (BGFD) arasında anlamlı farklılıklar var mıdır?

2- Öğretmen adaylarının coğrafi özelliklerden yaşadığı yer ile BGFD arasında anlamlı farklılıklar var mıdır?

3- Öğretmen adaylarının psikolojik (davranış ve düşünceler, ilgi alanları, güdüler, hayat tarzları vb.) özelliklerden internet, bilgisayar kullanımları ve bunların BGFD arasında fark var mıdır?

1.2 Amaç ve Önem

Bu çalışmanın temel amacı, OMÜ'de öğrenim gören öğretmen adaylarının BGF farklılıkların demografik (Cinsiyet, yaş, bölüm vb.), coğrafik, psikolojik özellikler arasında anlamlı olup olmadığını ortaya çıkarmaktır. Bununla birlikte öğretmen adaylarının internet ve bilgisayar kullanımlarının BGFD arasında fark var mıdır? Elde edilecek sonuçlar kapsamında BGF ile ilgili gelecekte benzer çalışma yapacaklara öneriler sunmaktır.

Dünyada ve ülkemizde bilgi sistemleri ile doğrudan veya dolaylı olarak temas kuran tüm kullanıcı ve kurumların gerek kişisel gerekse kurumsal bilgilerinin başkalarının eline geçmesi, hizmet, maddi, zaman vb. kayıplara neden olduğundan BG ile ilgili bilgilerinin artırılmasına katkıda bulunmak hem bir görev hem de bir ihtiyaçtır (Vural ve Sağıroğlu, 2011). Gelişen teknolojinin hayatın her alanında yer alması ve bunun kullanımında en önemli etkenin insan olduğu gerçeği dikkate alındığında teknoloji konusunda bilinç ve farkındalığı olmayan bireyler, hem kendilerinin hemde toplumun güvenlik sürecinin zayıflamasına, yok olmasına neden olurken; iyi eğitilmiş bireyler güvenliğin güçlenmesini ve güvenlikle ilgili problemlerin engellenmesini

sağlayabilirler. Bu nedenle, toplumun bilgi ya da DVG konusunda bilinçlendirilmesi ve bu konuda farkındalıkların oluşturulması oldukça önemlidir.

Bir ülkenin en önemli zenginlikleri arasında yer alan bilinçli insanının tek başına yaşaması mümkün olmadığı gibi yaşadığı toplum içinde karşılıklı ilişkiler içerisinde yaşaması ve bilinçlenmesi gerekmektedir. Dünyada/doğada/ekosistemde bulunan dengenin sağlanmasında, toplumun bilinçlenmesinde, gerekli bilginin kazanılmasını kolaylaştıran, gerekli ortamları hazırlayan öğretmenlerin sistemin girdisi ve çıktısı olan insanı ve toplumu en iyi biçimde tanıması gerekmektedir. Bunu yapabilmek için öğretmenin, gelişmeler ve yeniliklere açık, kendini devamlı yenileyen ve en az öğrencileri kadar öğrenme isteği olması beklenmektedir. İnsan eğitiminde yapılacak bir hata, sadece bugünü değil toplumun geleceğini de olumsuz yönde etkileyecektir.

Özellikle günümüz bilgi toplumunda, her alanda meydana gelen baş döndürücü gelişmelerin arttığı teknoloji çağında öğretmenlerin bu gelişmeleri takip ederek, öğretmen olma bilincini, hemen her yerde toplumu bilgilendirme, yeniliklerden haberdar etme, geleceğe hazırlama, insanlara rehber ve önder olma vb. görevlerle genişletmelidir. Bu kapsamda öncelikle gelecek nesilleri yetiştirecek olan öğretmen adaylarının BGF'nın belirlenerek bu doğrultudaki ihtiyaçlarının karşılanması gerekmektedir. Bu durumda bilgi toplumunun gelişmesinde önce kendileri, aileleri, çevreleri ve öğrencilerine katkıda bulunmasında rehberlik edecek olan öğretmen adayları, bilgisayar ile dünyanın her yerindeki bilgilere ulaşarak kendini geliştiren, yetiştiren öğrenci karşısında şimdiden tedbirlerini de alması oldukça önemlidir. Böylece gelecekteki öğrencilerinde BGF oluşturması ile başta sanal dünya olmak üzere öğrencilerini birçok tehlikeden koruyabilecektir.

Bu çalışmada öğretmen adaylarının BGF konusundaki mevcut durumları belirlenerek, öğretmen adaylarının ihtiyaçlarının tespiti ve ilgili kurumlarca gerek eğitim gerekse mesleki yaşamlarındaki ihtiyaçlarının giderilmesi açısından uygulamalar ve planlamalar yapılmasına olanak sağlayabilecektir. Böylece öğretmen adaylarının gelecekteki öğrenci ve velilerinin BG konusunda farkındalık düzeylerini arttırmaya yardımcı eğitim etkinlikleri düzenlenmesine, eğitim ortam ve materyallerini tasarlanmasına katkı sağlayacaktır. Ayrıca program geliştirme uzmanlarına öğretim programı geliştirme, bilinçli kullanıcı yetiştirme, teknolojinin olumsuz kullanım

alanlarına karşı farkındalık kazandırma yönlerinden etkinlikler hazırlama açısından katkı sağlayacağı beklenilmektedir.

1.3 Sayıltılar ile Sınırlılıklar

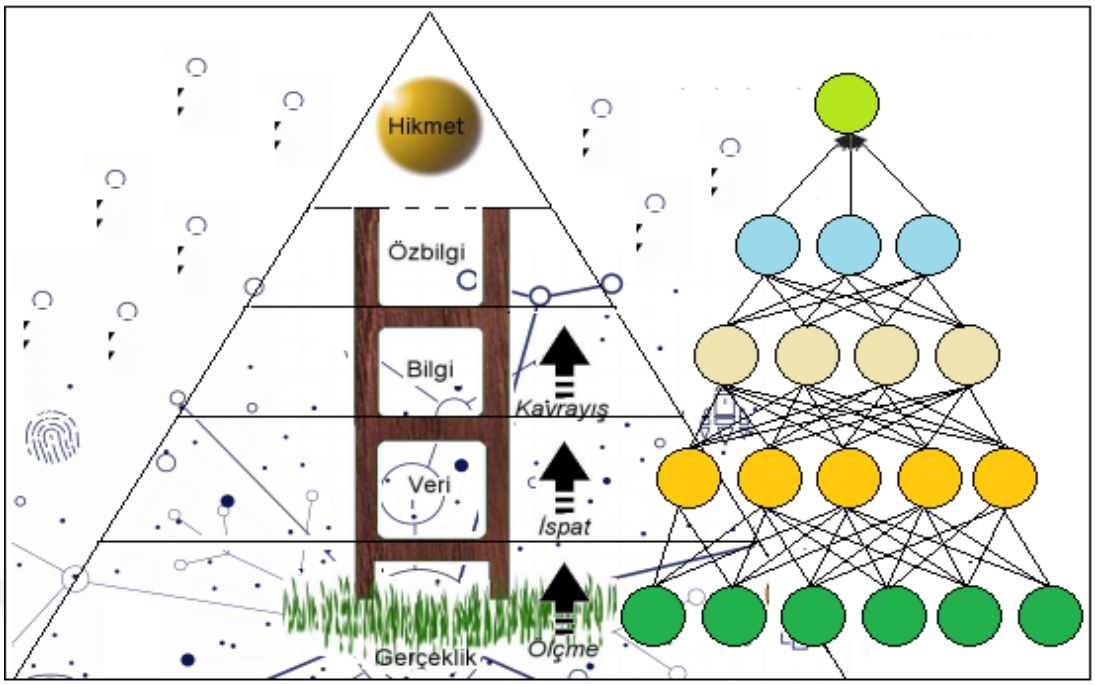
Araştırmada kullanılan anket sorularını, öğretmen adaylarının samimi, doğru cevaplandırdıkları ve anketin öğretmen adaylarınının görüşlerini ortaya koyacak nitelikte olduğu varsayılmaktadır. Araştırmanın konusu öğretmen adaylarının BGFD ile sınırlı tutulurken öğretmen adaylarının, demografik (cinsiyet, yaş, bölüm vb.) coğrafik özellikleri, internet ve bilgisayar kullanımlarının BGFD arasında anlamlı farklılıklar bulunup bulunmadığına ilişkin görüşlerinin ortaya konulması ile sınırlıdır.

Ayrıca araştırma, anketteki sorular ve anketi cevaplayan öğretmen adaylarının verdikleri cevaplar çerçevsinde OMÜ Eğitim Fakültesi'nde 2018-2019 öğretim yılında öğrenim gören öğretmen adayları ile sınırlı olurken Resim, Müzik, Özel Eğitim Öğretmenliği programı (1. ve 4. Sınıf) ile Almanca Öğretmenliği (1. ve 4. Sınıf) öğretmen adayları ankete katılamamışlardır.

1.4 Tanımlar

Yaşadığımız çağa damgasını vuran hayatın altın değerindeki hammaddesi bilgi ile ilgili kavramları tanımlamak, ileriye yönelik gelişmelerimizi şekillendirmede dünün, bugünün ve geleceğin en önemli anahtarı olurken veri, bilgi, özbilgi ve hikmet vb. kavramlar bilginin önemini ve BG ile bilgisayar güvenliğini her zaman öncelikli bir konumda tutmaya yardımcı olacaktır. (Canbek, 2005).

Bilgi çağında ilerlemek, gerçeklik ile hikmet arasında ki veri, bilgi, özbilgi basamaklarını kullanarak bir üst seviyeye çıkarken basamak atlanmadan teker teker geçilmektedir (Şekil 1). Böylece hikmete ulaşmak için her basamak zorlaşır ve daha çok gayret gerektirirken mümkün olan her şeyin miktarı azalmakta ve değeri artmaktadır. Bu kapsamda merdivenin alt basamaklarında verinin ve bilginin paylaşımı daha kolay; hikmete doğru özbilginin paylaşımı oldukça güç ve kişiye özel hale gelmektedir. Özbilgiden hikmete ulaşma, sentezleme gerektirirken, fikirlerin bir araya getirilmesiyle bütün, parçalarının toplamından daha büyük olmaktadır(Canbek, 2005; Canbek ve Sağıroğlu, 2006; Courtney, 2005; Schuler, 2003; Tiwana, 2002).



Şekil 1: Gerçeklikten Hikmete Ulaşmak İçin Aşılması Gereken Bilgi Basamakları (Canbek ve Sağıroğlu, 2006'dan değiştirilerek)

Bu nedenlerle merdivenin alt basamaklarında, bir sorunu çözmek veya belirli bir amaca ulaşmak için gerekli sıralı mantıksal adımlar yani algoritmalar ve programlanabilir bir yapıda olup üst basamaklarda, algoritmik olmayan ve programlanamayan bir yapıdadır. Veri ve bilginin iletiminde BT kullanılırken, özbilgi de buna ek olarak insan etkeni katıldığından bilgi ve özbilgi kavramları veya basamakları birbirleri ile karıştırılmaktadır (Canbek ve Sağıroğlu, 2006; Grover ve Davenport, 2001; Montano, 2004; Sağıroğlu, 2001).

Veri: İngilizce "data", Latince "datum/çoğulu data" "vermeye cesaret etmek" veya "verilen şey" anlamında olurken Türkçe'de de aynı anlamda kullanılmaktadır. BT açısından veri, bir durum hakkında, birbiriyle bağlantısı henüz kurulmamış bilinenler veya sayısal ortamlarda bulunan ve taşınan sinyaller ve/veya bit dizeleri olup verinin işlenmiş hali bilgiyi oluşturan dijital bir kavramdır (Canbek ve Sağıroğlu, 2006).

Bilgi: İnsan aklının alabileceği gerçek, olgu ve ilkelerin tümü ya da bir konu veya iş konusunda öğrenilen, öğretilen şeylerdir (TDK, 2019). Her yerde bulunan bilgi günümüzde yaygın olarak bilişim sistemlerinde; işlenmekte, depolanmakta, iletilmekte, değiştirilmekte, silinmekte veya anonim hale getirilmektedir. Buna göre bilgi, belli bir anlam ifade edecek şekilde verinin düzenlenmiş ya da işlenmiş halidir (Canbek ve Sağıroğlu, 2006).

Özbilgi: Gerçeklerin (tecrübe veya öğrenme ya da iç gözlem şeklinde elde edilen), doğruların veya bilginin, farkında olunması ve anlaşılmasıdır. Verileri bir araya getirilip, işlenmesiyle bilgiyi oluştururken özbilgi, kullanılan bilgilerin toplamından daha üstte bir kavram olup bir güç oluşturabilecek, katma değer sağlayabilecek ya da bir araç haline dönüşmek üzere, daha fazla ve özenli olarak işlenmiş bilgidir. Özbilgi, 5N1K (**Ne**, niçin, nasıl, nerede ve kim) olduğunu bilmek şeklinde beş sınıftan oluşurken **Ne,** gerçeklerin toplamı ve bilgiye en yakın olan sınıftır. **Niçin**, teknolojik gelişmenin altında yatan ilke ve yasaların açıklandığı bilimsel özbilgidir. **Nasıl,** bir şeyi yapabilme becerisi olup **Nerede,** dünya ya da evrendeki bilgilerin olduğunu; **Kim,** neyi ve nasıl yapılacağını bildiğini bilmektir (Canbek ve Sağıroğlu, 2006).

Hikmet: Bilgelik, tasavvur, ileri görüş ve ufkun ötesini görme yetisi ile en ileri seviyede soyutlama ve bir kişinin özel bir iş alanındaki meslek hayatı boyunca elde edilmiş deneyimin özü aynı zamanda güvenilir yargıda bulunmak, karar vermek için özbilginin nasıl kullanılacağını kavramaktır (Awad ve Ghaziri, 2004; Canbek ve Sağıroğlu, 2006; Kirrane, 1999). Hikmetli, insanlara gerçekleri tebliğ etmekte en büyük etken; hikmetsiz, zaman ve mekanı bulmayan; ilimden fayda alamayan, en ileri seviyede yaşama şartından mahrum olmadır (Altıparmak, 2003).

Bilişim: Yapısal bir bilim dalı olarak bilginin elektronik cihazlar aracılığıyla düzenli ve mantıksal bir çerçevede işlenmesidir (Pallı, 2008).

Bilişim teknolojileri (BT): Dijital ortamda bilgiye ulaşma, elde etme, kaydetme, düzenleme, kullanma vb. şekilde toplanan bilginin, muhafazası, ihtiyaç halinde geri çağırılması, verilerin işlenmesi, analiz ve transfer edilmesini sağlayan bir dizi bütününü anlatan kavram (Yurdakul ve Çağlayan, 1997).

Bilgi güvenliği (BG): Teknoloji ile birlikte uyum içinde çalışmanın gerekli olan bir olgudur (Eminağaoğlu ve Gökşen, 2009). Dijital veri veya mevcut bilgilerin, güvenli şekilde muhafazası, taşınması sonucu bütünlüğünün bozulmadan, doğru teknoloji, amaç ve şekilde kullanılmasıyla izinsiz erişimlerin engellenmesi; güvenli bilgi işleme ortamı oluşturma çabalarının tümüdür (Canbek ve Sağıroğlu 2006).

Bilgi güvenliği farkındalığı (BGF): BT kullanan kullanıcıların kişisel bilgilerinin tehlike ve tehditlerden korunması amacıyla gerekli güvenlik analizlerle önlemlerin alınarak tehlikelere karşı farkında olma durumu (Vural ve Sağıroğlu, 2008).

İKİNCİ BÖLÜM

II. KURAMSAL ÇERÇEVE

Bu bölümde, bilgi ve bilişim teknolojileri, BG ve bunu tehdit eden unsurlar, BG'nin sağlanmasındaki süreçler, alınması gereken tedbirler, BGF ve eğitim arasındaki ilişkilere yer verilmiştir.

2.1 Bilgi ve Bilişim Nedir?

Bilgi, anlamlı bir şekilde düzenlenmiş ya da işlenmiş veri olarak tanımlanan; insan aklının alabileceği bütün gerçek, olgu ve ilkelerin tümüdür. Hemen her yerde bulunan günümüzde yaygın olarak bilişim sistemlerinde yer alan bilgi; işlenebildiği, depolanabildiği, iletilebildiği, değiştirilebildiği, silinebildiği veya anonim hale geldiği önemli yer olup dijital olarak işlenmiş veridir. Verilerin bir araya gelmesiyle bilgi oluşturulmaktadır (Canbek ve Sağıroğlu, 2006; Çek, 2017). Teknoloji ve bilgisayarın yaygın olarak kullanılmadığı dönemlerde durağan olan bilgi, günümüzdeki teknolojiler ile hareketli hale gelirken niteliği değişmiş bilgisayara, teknolojiye ve iletişime yakın görülmektedir (İlbaş, 2009).

Bilişim, bilginin elektronik cihazlar ile belli bir mantık çerçevesinde sistemli ve planlı biçimde işlenmesidir (Pallı, 2008). Fransızca "informatiqe" ile aynı kökten gelen bilişim kelimesi, dilimize enformasyon olarak çevrilip daha sonra bilişim ile aynı anlamda kullanılmaktadır (Dülger, 2004). TDK'ya (2019) göre, bilişim, insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makinalar aracılığıyla düzenli ve akla uygun bir biçimde işlenmesidir.

2.2 Bilgi ve Veri Güvenliği Nedir?

Bilgi güvenliği; bilgiye her zaman ulaşılan bir ortamda, bilgiyi gönderen kişiden alıcıya ulaşıncaya kadar bozulmadan, değiştirilmeden ve bir başkasının eline geçmeden güvenli bir şekilde ulaşmasıdır (Schmidt, 2004).

Veri güvenliği; verinin toplanmasından sonra son kullanıcıya ulaşması, saklanması ve kullanım aşamalarında her türlü tehdit ve tehlikeden korumasını amaçlarken aynı zamanda alınacak tedbirler ve saldırı halinde izlenecek aşamaları kapsayan bir disiplindir (Canberk ve Sağıroğlu 2006).

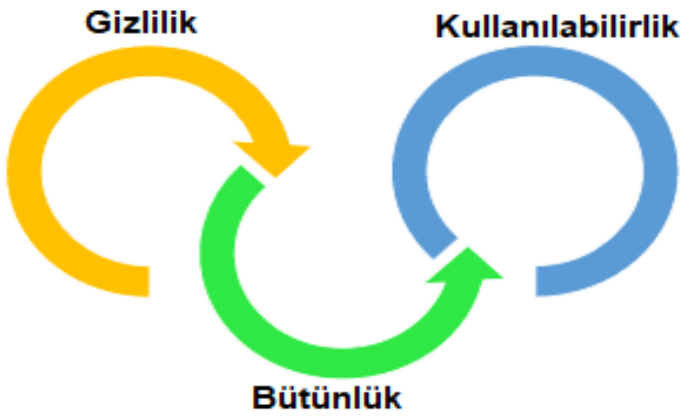
BG, önceleri daha çok yazılı ve basılı ortamlardaki bilgilerin fiziksel olarak güvenliğinin sağlanması olup günümüzde ise bilişim teknolojileri bakımından dijital veri güvenliği kavramı olarak algılanmaktadır (Canberk ve Sağıroğlu 2006).

Dijital veri güvenliği, elektronik ortamlarda bulunan verilerin bütünlüğü bozulmadan ve izin almadan erişilenlerden korunarak saklanabilmesi ve taşınabilmesi için bilgi işleme platformlarının da güvenli hale getirilmesi şeklinde tanımlanmaktadır (Henkoğlu ve Yılmaz, 2016; Yılmaz, Şahin ve Akbulut, 2016).

Geçmişten günümüze kadar her zaman önemini koruyan durağan, hareketli ve kullanılan olarak üç şekilde bulunan bilgi, çok çeşitli ve farklı yerlerde karşımıza çıkarken, sunucular, dizüstü ve kişisel bilgisayarlar, akıllı telefonlar, elektronik posta vb. aracılar ile hızlı bir şekilde elde edilmektedir (Çek, 2017; Gülmüş, 2010). Böylece bilgi teknolojilerinin kullanılmasıyla bilginin devamlı üretimi, geliştirilmesi, depolanması, paylaşılması, taşınması, bölünmesi ve kullanımı daha kolay bir hale gelmektedir. Son yıllarda BT'deki hızlı gelişmeler beraberinde Bilgilerim çalınır mı? Bilgisayarıma virüs bulaşır mı? Mevduat hesabım güvende mi? vb. birçok güvenlik sorunları kullanıcıları meşgul etmektedir (Dedeoğlu, 2006; Vardal, 2009).

2.3 Bilgi Güvenliği Unsurları

Çok farklı şekilde ele alınan BG'de bilginin gizliliği, bütünlüğü, kullanılabilirliği ve sürekliliğinin birlikte sağlanması oldukça önemlidir (Şekil 2). Aynı zamanda temel güvenlik bileşeni olan gizlilik, bütünlük ve erişilebilirliğin de göz önünde bulundurulması gerekmektedir. Kimlik tespiti, güvenirlik ve inkâr edememe bu üç temel güvenlik bileşenin alt bileşenidir (Canberk ve Sağıroğlu, 2006; Güngör, 2015).



Şekil 2: Temel Güvenlik Prensipleri (Güngör, 2015'den değiştirilerek)

2.3.1 Gizlilik (Confidentiality)

Gizlilik, bilginin hangi formda olursa olsun sadece yetkisi olan kişilerce erişiminin sağlanması, yetkisi olmayan kişilerce erişimin sağlanmamasıdır. Bilginin saklanması, iletilmesinde sadece izin verilen kişi veya gruplarca görülmesi istenir. Günümüzde gizliliğin sağlanmasında en önemli etken ise şifreleme teknolojidir (Çek, 2017).

2.3.2 Bütünlük (Integrity)

Bütünlük, bilginin gönderici tarafından hiçbir değişikliğe uğramadan alıcıya ulaşması olup bunun sağlanması için bilgi/verinin değişikliğe uğramaması gerekir. Ayrıca bütünlüğün tam olarak yerine gelmesi için gizliliğin değişmemesi gerekir. Çünkü yetkisi olmayanların bilgiye erişilmesiyle, bilginin değiştirilmesi, silinmesi veya bilgiye hasar verilmesi bütünlüğün de bozulmasına sebep olmaktadır (Yılmaz, 2013).

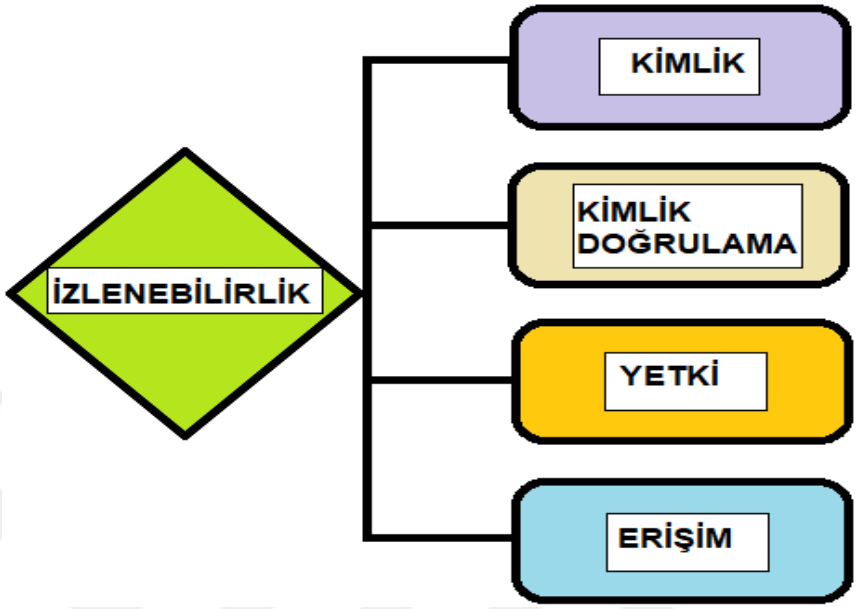
2.3.3 Kullanılabilirlik (Availability)

Kullanılabilirlik, kişilerin ihtiyaç duyduğunda bilgiye ulaşılabilmesi olup gizlilik kavramı içinde kullanılabilmektedir. Kullanılabilirlik aynı zamanda kullanıcıların hakları olan bilgiye sorunlu veya sorunsuz olarak daima ulaşılabilmesidir (Karakuzu, 2015). Birbiri ile bağlantılı olan temel bileşenlerle bilgiye erişim yetkisiz kişilere gizliliği sağlanırken bilgiye erişilebilirlik engellenmemeli, istenmeyen kişilerce bütünlüğü bozulmamalıdır. Bu durumlarda bilgiye erişim sağlanmazsa o bilginin bir anlamı kalmazken erişimi sağlanan bilginin bozulmuş ve değiştirilmişse, bilgide bir bütünlük yoksa bu bilgi sonucunda kişi ya da kurumlar zarar görebilmektedir. Bu temel unsurların bir bütün halinde gerçekleşmesiyle BG sağlanırken bu güvenlik bileşenlerin dışında izlenebilirlik, kimlik doğrulama, güvenirlik ve inkâr edememe alt bileşenleri de bulunmaktadır (Aslan Öztezcan, 2017).

2.3.4 İzlenebilirlik

İzlenebilirlik, basit anlamıyla bilişim sistemlerinde yapılan işlemlerin kayıt altına alınmasıdır. Daha sonra analiz etmek için kullanıcının bilgisayardaki ve internetteki her hareketi kayıt altına alınırken kullanıcının girdiği web sayfaları, kullanıcı ismi ve şifre kayıt altına alınan bilgiler arasındadır (Şekil 3). Ülkemizde 5651 sayılı "İnternet ortamından yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi" hakkındaki yasa ile internette yaşanmış ve yaşanabilecek bütün

olumsuzlukların izlenerek en az seviyeye indirilmesi amaçlanmıştır. Bu amaçla kişi ve kurumların internette gerçekleştirdikleri her işlem kayıt altına alınarak, IP adresiyle bağlantı kurulmaktadır (Aslan Öztezcan, 2017; Gülmüş, 2010).



Şekil 3: Temel Güvenlik Eğitimleri (Andress, 2011'den değiştirilerek)

2.3.5 Kimlik Doğrulama (Authentication)

Kimlik doğrulama sisteme şifreli girilmesi vb. durumlar bilişim sisteminden hizmet alan kişinin gerçek kişi olduğunun anlaşılmasıdır (Pro-G, 2003; Tekerek, 2008). Bu amaçla günümüzde elektronik ortamlarda kimlik doğrulama akıllı ve elektronik imza kartları, tek kullanım şifreler, biyometrik teknolojiler kullanılmaktadır (Gülmüş, 2010).

2.3.6 Güvenilirlik

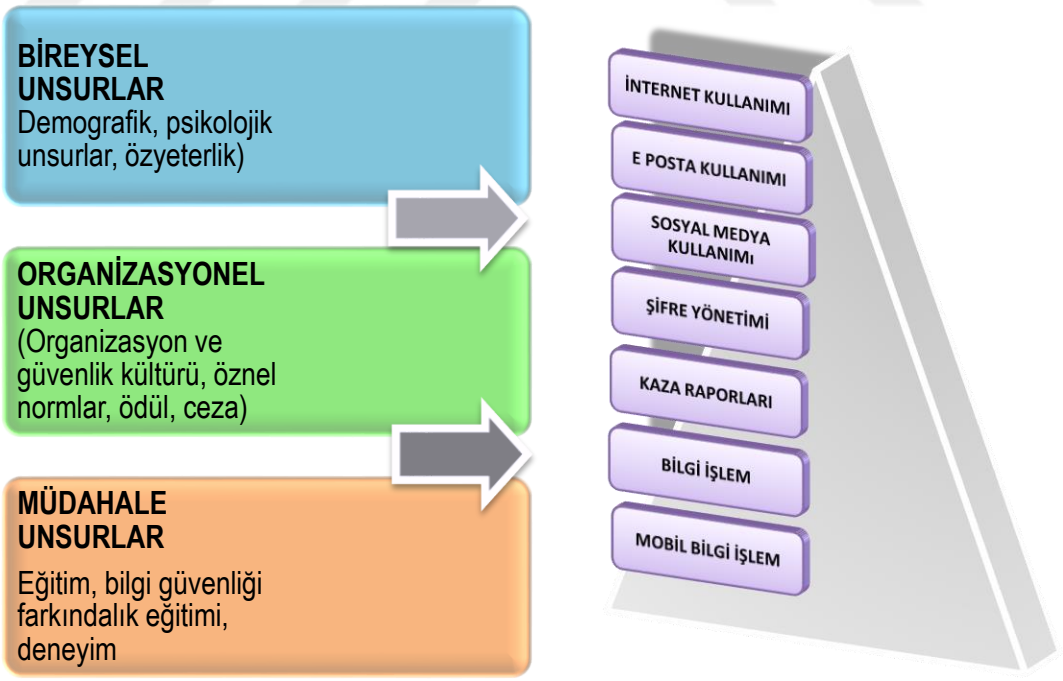
Bilişim sistemlerinde beklenen tutum ile sonuç arasındaki tutarlı olma güvenilirlik, sistemden istenen işlemin ne eksik ne de fazla olmamasıyla sağlanabilmektedir (Gülmüş, 2010).

2.3.7 İnkâr Edilemezlik (Non-Reoudation)

İnkâr edilemezlik, bilgi sistemlerini kullanan gönderici ve alıcının yaptığı işlemlerin neler olduğunu bilerek red edememesi olup bilişim sistemlerinde kullanıcılar tarafından gerçekleştirilen her işlemin kaydı ayrıntılı bir şekilde saklanmaktadır. Bununla birlikte her kişi ve kurum kendisi için önemli olan bilgilerin belli zaman

aralıklarında yedeğini almalı, bilgi güvenilirliğinin artırılması için yedeklemeyi kimin ve hangi tarihte yaptığı bilinmelidir (Güngör, 2015; Yıldız, 2007). Günümüzde e-imza teknolojisinin kurumlar tarafından aktif bir şekilde kullanılmasıyla inkâr edilemezlik ilkesi büyük ölçüde sağlanmıştır (Özler, 2007).

BG güvenliğinin sağlanması; fiziksel korumanın yanında bireylerin BGF kazanması, BG sağlamaya dönük bilgi, tutum ve davranışları sergilemesi ile mümkündür (Maiwald, 2004). Bilginin kavramsallaştırılması politika ve süreç bilgisi ile bu sürece yönelik tutum ve öz-yansıtma davranışları olup bilgi ile mobil bilişim işlemlerinde ve ortamlarında (internet kullanımı, e-posta kullanımı, sosyal ağ sitesi kullanımı, şifre yönetimi, olay bildirimi) gerçekleşmektedir (Şekil 4). Bilgi, tutum ve davranış arasındaki ilişki, bireysel ve (demografik, psikolojik ve özyeterlik; organizasyonel faktörler ve güvenlik kültürü, öznel normlar, ödüller ve cezalar); örgütsel müdahale (eğitim, BGF eğitimi, deneyim) vb. çok sayıda faktörden etkilenmektedir (Parsons, McCormac, Butavicius, Pattinson ve Jerram, 2014). Bu faktörler BG ile ilgili bilgi, tutum ve davranışlar, farklı BG politikaları ve süreçleriyle de etkileşim içindedir (Seferoğlu, Yıldız-Durak, Karaoğlan-Yılmaz ve Yılmaz, 2018).

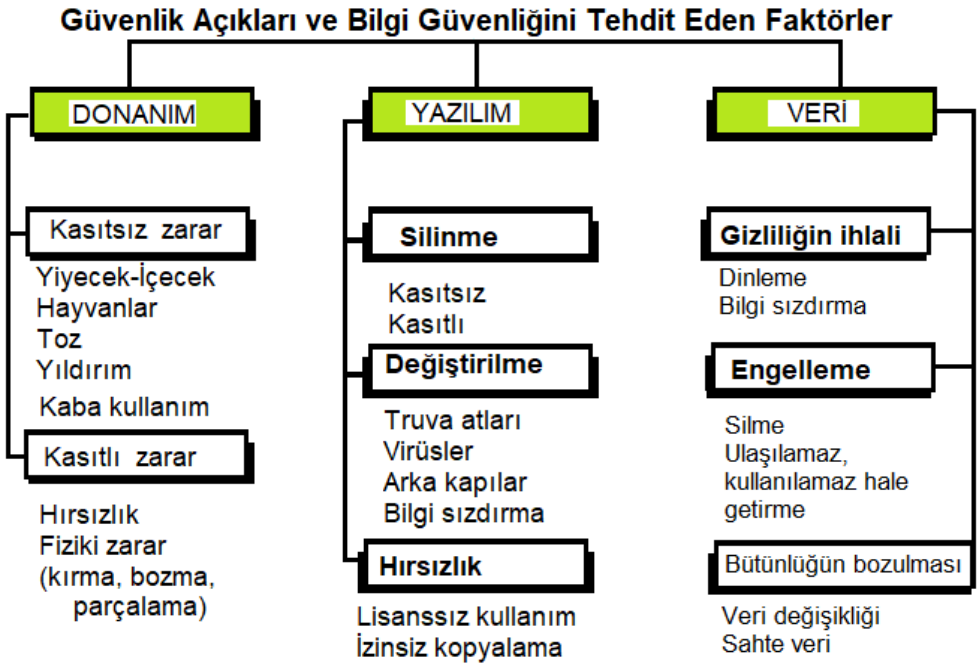


Şekil 4: Bilgi Güvenliğiyle İlgili Unsurlar (Parsons, McCormac, Butavicius, Pattinson ve Jerram, 2014'den değiştirilerek).

2.4 Bilgi Güvenliğini Tehdit Eden Unsurlar

Bilgi teknolojisindeki tehdit ve tehlikeler genel olarak donanım, yazılım ve veri kaynaklarının kullanımı ile ortaya çıkarken bu tehditler hem işletmelere hem de kamu kurum ve kuruluşlarına karşı yapılabilmektedir (Şekil 5). Bu kapsamda BG altyapıları çok sağlam olmayan kamu kurum ve kuruluşlar asıl hedef durumuna gelebildiğinden gün geçtikçe kullanımı artan bilgi ve iletişim teknolojisi saldırıları için alt yapı oluşturulmaktadır. Bu durumda da hedeflerine daha kolay ulaşma çabası içinde ki bilgisayar korsanları bu teknolojileri kullanmaktadırlar (Güngör, 2015).

Dünyada ve ülkemizde kötü niyetli bilgisayar korsanları kişilere ait bilgilerle sanki kendilerine ait gibi işlem yaparken, kişilere ait az sayıda bilgiden yola çıkarak kişinin banka hesabından para çekebilmekte, sahte evrak düzenleyebilmekte ve onlar adına birçok işlemi yapabilmektedir. Bu durum çoğunlukla elektronik sistemlerdeki bilginin çokluğu ve gelişigüzel kullanılması ile birçok suçun oluşmasına ortam hazırlamaktadır. Özellikle 2000'li yıllardan sonra görülmeye başlayan siber saldırılarla internetin sanal boyut güvenliği daha fazla gündeme gelirken, kişilerin BG farkındalıklarının arttırılması önemlidir (Civelek, 2011; Şahinaslan, 2013; Vural ve Sağıroğlu, 2007).



Şekil 5: Günümüzde Yaygın Olarak Ortaya Çıkan Güvenlik Açıkları ve Bilgi Güvenliğini Tehdit Eden Faktörler Faktörler (Öztürk, Yüksek ve Aslan, 2014' den değiştirilerek).

Bilişim kültürleri ile kullanıcıların BGFD' ları arasında anlamlı ve pozitif bir ilişki bulunmasına karşılık teknoloji kullanımının aktif artışı sonucunda kullanıcıların sayısız tehditlerle karşılaşılacağından bu tehditlere karşı önlem alınması gerekmektedir (Mart, 2012). Kurumsal bilgi kaynaklarının korunmasında meydana gelecek tehditler insan ya da doğa kaynaklıdır (Qureshi, 2011). BG 'ye karşı oluşan tehditler kaynaklarına göre kurum içi ve kurum dışı olmak üzere iki gruba ayrılırken, kurum içi tehditler, kullanıcı hataları, lisansız yazılımlar, yetersiz donanım ve yazılıma sahip altyapılar; kurum dışı tehditler istek dışı iletiler, bilgisayar virüsleri, sosyal mühendislik ya da doğal afetlerdir (Al-Awadi ve Renaud, 2008)

Değişen ve ilerleyen teknolojilerle beraber artan saldırı türleri değişmekte, bu saldırılara karşı korunma yöntemleri de gelişerek artmaktadır. Saldırganlar günümüzde kullanıcı zaafları ve kullanıcıları aldatacak sosyal mühendislik yöntemleri ile tehditler oluştururlarken, casus yazılımlar gibi birtakım yöntemler aracılığıyla kullanıcıların port açıklarının tespiti için kullanıcıların internet gezinme geçmişini, işletim sistemi ve kullanılan programın açıklarını, kullanıcıları incelemektedir. Böylece saldırganlar, kullanıcılar için değerli ve önemli olan özel yaşamlarıyla ilgili bilgilere ulaşabilmektedir. Kullanıcıların bilgi ve bilgisayar güvenliğinin sağlanmasında BG sistemlerinin itina ile hazırlanması ve kullanılması gerekmektedir (Canbek ve Sağıroğlu, 2007).

Bilgi sistemlerindeki tehditlerin etkililiği bilgi sistemlerinde bulunan açıkların bulunmasına bağlı olup bilgi sisteminde açıklar ne kadar fazla ve uygun ortama sahipse tehditlerin oluşması da o kadar kolay olmakta ve o denli bilgi sistemlerine zarar vermektedir (Güldüren, 2015). BG'ye ilişkin tehditler sadece elektronik ortamdaki saldırılarla sınırlı olmayıp yangın, sel vb. çeşitli **doğal afetler**, **prosedürel eksiklikler, insan hataları** ve **zararlı yazılımlardan** vb. tehditlerden de kaynaklanır (Güldüren, 2015; Vural, 2007).

2.4.1 Doğal Afetlerden Kaynaklanan Tehditler

Doğal afetler, depremler, su baskınları, seller, yangınlar, toprak kaymaları, fırtınalar ve çığ düşmeleri vb. olup bu tehditler daha önceden bilinmediğinden bunlara karşı önlem almak oldukça zordur. Ancak oluşacak hasarın en az seviye indirilebilmesi adına gerekli tedbirlerin alınması oluşacak zararın en az kayıpla atlatılmasına olanak sağlayacaktır (Vural, 2007). Ayrıca meydana gelen doğal afet sonrasında kurumlarda

mevcut bilgi kaybının yaşanmaması ya da en aza indirilebilmesi için yedeklemelerin düzenli olarak alınması gerekmektedir. Alınan bu yedeklemelerin farklı yerlerde muhafaza edilmesi, bilgi sistemlerinin depreme dayanıklı olan yerlerde kurulması, alternatif iletişim sistemlerinin kullanılması ve planlamanın iyi bir şekilde yapılması yararlı olacaktır (Uslu, 2007).

2.4.2 Prosedürel Eksiklerden Kaynaklanan Tehditler

Prosedürel eksikliklerden kaynaklanan tehditler, kurum ve kuruluşların kurumsallaşma süreçlerini tamamlayamamasından kaynaklanırken teknik ve idari olmak üzere iki grupta toplanılmaktadır (Güldüren, 2015; Vural, 2007).

2.4.2.1 Eksik İdari Prosedürler

a) İşe alınan ve işine son verilen personelin güvenlik prosedürlerinin olmaması, iş süreçlerinin yeterince belgelendirilmemesi,

b) Güvenlikle ilgili eksik görev ve sorumlulukların verilmesi, güvenlik politikalarının ve prosedürlerinin bulunmaması,

c) Çalışan bireylerin güvenlikle ilgili eksik bilgi sahibi olmaları veya bu bilgilerden habersiz olması ve görev paylaşımının olmaması,

d) Acil durumlarda devreye girecek bir bilgi planlarının olmaması,

e) Eğitimle ilgili plan ve uygulamaların eksikliğidir.

2.4.2.2 Eksik Teknik Prosedürler

a) Yedeklemenin olmaması,

b) Yardım masasının olmaması (bilgisayar, kurulumu ve bakımı),

c) Bilgi literatüründe tutulması gereken ve güncelliği sağlayacak prosedürler ile izleme prosedürünün olmaması,

d) Ağ hizmet prosedürlerinin olmaması (e-posta, internet, vb.),

e) Etki alanı hizmet prosedürlerin olmaması (şifre değiştirme, hesap açma, vb.),

f) Sunucu hizmetlerindeki planlama prosedürlerin eksikliği (dns, dhcp, vb.),

g) İletişim hatlarındaki denetim ve yönetime ait prosedürlerin eksik (ses, veri vb.) olmasıdır.

2.4.3 İnsan Faktörlerinden Kaynaklanan Tehditler

BG'nin sağlanmasında, sistemlerde teknik yazılım ve donanım yatırımlarıyla bilginin izinsiz kullanılması önlenmiş olsada insan zaafları sistemlere zarar vermektedir. Günümüzde genel olarak kurum ve kuruluşlar alt yapı ile ilgili önlemler alırken dikkatsiz ve bilinçsiz kullanıcıların sebep olduğu/olacağı açıklardan saldırganlar faydalanmaktadır (Kınay, 2012).

İnsan kaynaklı tehditler, bilinçsiz (istem dışı) ve bilinçli olarak yapılan davranışları olarak ikiye ayrılmaktadır. İstem dışı tehditler arasında en yaygın olanlar, sistem üstünde yetkili olan farklı düzeylerde bilgiye sahip (sistem yöneticileri, yazılım geliştirme uzmanları ve son kullanıcılar gibi) kullanıcının bilgi sistemini bilinçsiz ve bilgisizce yeterli kullanıcı eğitimine erişmeden kullanması, BG ilkelerinden bir veya birkaçının bozulmasına sebep olan, kasıtsız ve ihmalkârca yapılan kullanıcı davranışlarıdır Bu tehditler arasında;

a) Güvenlik politikalarına uyulmaması veya ihlal edilmesi,
b) Gerekli güvenlik tedbirleri alınmadan yazılım geliştirilmesi,
c) Yapılandırma ayarlarının eğitim almamış personel tarafından kurcalanması,
d) Bilişim sistemlerinin kullanım ve yönetiminin yanlış yapılması,
e) Kusurlu veya yanlış yapılandırma,
f) Erişim hak ve yetkilerinin ayarlanamaması, gereksiz servislerin hizmete açılması,
g) Log (sistem) kayıtlarının silinmesi veya tutulmaması,
h) Temizlik ve diğer işlerle uğraşan personelin sunucu fişini çekmesi,
i) Kullanıcının bilgisayar başında olmadığı vakitlerde parola korumalı ekran koruyucunun devreye girmemesi,
j) Sistem yedeklemesinin yapılmaması veya eksik yapılması,

k) Bilgisayar hızını düşüren antivüris programlarının bu mazeretle devre dışı bırakılması,

l) Kullanıcıların tanımadığı kişiler tarafından gönderilen e- posta eklerini açması ve e- postalar ile talep edilen kişisel ve gizli bilgilerini vermesi,

m) Kullanıcıların şifrelerini unutmaları ile şifrelerini mobil cihazlar aracılığıyla değiştirme, şifrelerin kullanılan sistemin ilk ayar durumunda bulunması ya da oluşturulan şifrelerin kâğıda yazılarak masa üstü gibi yerlerde bulundurulması sayılabilir (Canbek ve Sağıroğlu, 2006; Vural, 2007).

Bilinçli olarak gerçekleştiren tehditler, bir işyerinde hiçbir beklentisi olmayan kızgın veya kırgın olan personelin yetkisini kötüye kullanarak sistem üzerinde kasıtlı olarak yaptığı kurumları büyük zararlara uğrattığı kötücül davranışlar olup günümüzde yerel saldırganlar olarak tanımlanmaktadır. Bilinçli yapılan davranışlardan kaynaklanan tehditler arasında;

a) Kendi görev ve yetkisinde bulunmayan başka bilgisayar sistemlerine girerek içerisindeki gizli bilgilere ulaşmak,

b) Çalıştığı kurumdaki konumu gereği, kendisine yarar sağlama amaçlı şifreleri sızdırmak,

c) Veri tabanında kayıtlı bulunan verileri değiştirmek, silmek veya yok etmek,

d) Güvenlik sunucularının (güvenlik duvarı, antivirüs vb.) yanlış yapılandırılması veya devre dışı bırakılmasını sağlamak,

e) Güvenlik kayıtlarında iz bırakılmaması için yapılan art niyetli davranışları silmek, bilgisayarlara kötücül programlarının bulaştırılması sağlamaktır.

Sosyal medya uygulamalarının kullanımı günümüzde yaygınlaşmış ve kullanıcıların profilleri veri madenciliği yöntemiyle çok detaylı bir şekilde araştırılarak elde edilmektedir. Kullanıcıların sosyal medyada kişisel ve konum vb. çok sayıda bilgilerini olumsuz sonuçlar getirebileceği değerlendirmeden paylaşmaları saldırganlar için yol gösterici olmaktadır. Saldırganlar saldırıları için insanların davranışlarını, özellikle sosyal mühendislik yöntemlerini, oltalama ve istem dışı elektronik posta unsularını kullanmaktadır (Şahinaslan, 2013).

2.4.3.1 Sosyal mühendislik

Sosyal medya uygulamalarının kullanımı günümüzde yaygınlaşmış ve kullanıcıların profilleri veri madenciliği yöntemiyle çok detaylı bir şekilde araştırılarak elde edilmektedir. Kullanıcıların sosyal medyada kişisel bilgileri, konum bilgileri vb. çok sayıda bilgilerini paylaşmaları olumsuz sonuçlar getirebilmektedir. Nitekim bu paylaşımlar saldırganlar için yol gösterici nitelikte olurken kullanıcıların sosyal medya paylaşımlarını gözlemleyerek onlara zarar vermektedir. Saldırganlar özellikle sosyal mühendislik, oltalama ve istem dışı elektronik posta unsularını kullanmaktadır (Şahinaslan, 2013).

Sosyal mühendislik, kişi ya da kurumların sistemine sızabilmek için onların davranışlarını izleyerek veri toplanmasıdır. Saldırganlar sosyal mühendislik yöntemlerini kullanırken insanların yardımcı olma isteklerinden ve güven duygularından faydalanırken aslında kandırma faktörüne dayanmaktadır. Bu yüzden, saldırganın ikna ve etkileme kabiliyetini iyi kullanması amacına ve hedefine daha kolay ulaşabilmesini sağlamaktadır. Sosyal mühendislik saldırılarından birisi kurumda çalışan bir personelin aranması (Şekil 6) ve kendilerini bilgi işlem personeli olarak tanıtması kurum personellerinin sisteme bağlanırken kullandıkları şifreleri talep ederek ele geçirmesidir (Hekim ve Başıbüyük, 2013).

Şekil 6: Sosyal Mühendislik Yöntemi (Yaşar ve Çakır, 2015)

Günümüzde sıklıkla görülmeye başlanan sosyal mühendislik saldırılarının diğer saldırılara göre doğuracağı sonuçlar daha da tehlikeli olabilmektedir (Munro, 2005). Sosyal mühendislik yöntemini kullanan saldırganlar aldatma sanatçıları olarak

adlandırılırken, saldırılarında tek hedef "insan" olduğundan engellenme noktasında teknolojik yöntemler yetersiz kalmaktadır (Barber, 2001). Genel olarak bilgisayar korsanı; teknik korsan, çökertici, kırıcı, hacker olarak bilinen sanal âlem suçlularına göre BG'nin sağlanmasında insan faktörü en önemli role sahiptir (Mitnick ve Simon, 2016). Günümüzde yaygın olarak kullanılan sosyal mühendislik saldırı türleri arasında;

1. Kullanıcılardan bilgi elde etmek için sahte senaryolar uydurmak,
2. Kullanıcıları ikna etmek için kaynağın güvenliği olduğunu söylemek,
3. Bilgi alacağı kullanıcıyı ikna etmek için kendini başka biriymiş gibi göstermek,
4. Güvenilir bilgi karşılığında hediye, para vb. teklifler önermek,
5. Güven kazanarak kullanıcıdan bilgi elde etmek,
6. Bilgilere erişmek için kullanılmayan eski donanımlarını incelemek,
7. Bilgi elde etmek için kullanıcıların çöp kutularını karıştırma yer almaktadır (Muharremoğlu, 2013).

Sosyal mühendislik tehditlerine karşı kurum yönetimi tarafından belirlenen personellere yönelik olarak aşağıda verilen bazı denetimler gerçekleştirilebilir.

- ✓ Kurumda çalışan belirli personellere sosyal mühendislik teknikleri içeren manipüle edilmiş bir e-posta gönderilmesi ve personele BG'yi tehdit edecek aktiviteler yaptırılması böylece e-posta içeriği farklılaşabilirken e-posta ekinde yer alan linke tıklanması ya da dosyayı çalıştırılması istenilerek kişisel bilgileri veya kurum bilgileri ele geçirebilir.
- ✓ Kurumun sahip olduğu üslup, kurumda çalışan personelin isimlerini, iş süreçlerini ve iş yapış yöntemi bilen kişilerin kurumda çalışan herhangi bir personeli arayarak yetkili biriymiş gibi kendini tanıtması ve bunun sonucunda personele belirli işlemler yaptırılabilir (Muharremoğlu, 2013).

Kişi ve kurumlar BG zafiyetleri konusunda bir dizi önlem almak zorunda olup alınan önlemler teknolojinin sürekli olarak gelişmesi ve saldırı tekniklerinin gün geçtikçe değişmesi ile geçersiz kalabilmektedir. Bundan dolayı hiçbir kuruluş ya da kişi kendini güvende hissetmemeli ve savunma sistemlerini bu teknolojiye paralel olarak güncellemelidir (Canbek ve Sağıroğlu, 2006). Bu durum insan faktörünün BG'nin

sağlanmasında da karşımıza çıkmaktadır. Dikkatsiz bir kullanıcı BG açıklarına neden olabileceğinden sistem ne kadar güvenli olursa olsun sistemi risk altında bırakacaktır. Nitekim 2011 yılında yapılan bir araştırmada, işletmelerin %43'ü sosyal mühendislik saldırılarına maruz kaldığı, %48'inin her bir saldırı sonucunda maddi kaybının 25 bin dolar olduğu sosyal mühendislik saldırıları konusunda eğitimler düzenlemesi gerektiği ortaya konulmuştur (Dimensional Research, 2011).

2.4.3.2 Oltalama

Genellikle sahte web sayfaları kullanılarak kullanıcıların kimlik bilgilerini ele geçirme yöntemi olan oltalamada kendilerine gelen e-postada yer olan bağlantının, alışveriş yaptığı siteden ya da kullandığı bankadan geldiğini düşünebilmektedir. Kullanıcı kendisine gönderilen e-posta da bulunan linke tıklandığında bu link kullanıcıyı sahte web sayfasına yönlendirerek kullanıcının bilgilerini o web sayfasına girmesini sağlayıp tuzağa düşürmektedir (Bayzan ve Çubukçu, 2013).

Kullanıcıların oltalama yöntemi ile kandırılmasını önlemek için eğitim ve bilinçlendirme çalışmalarının yapılması oldukça önemli bir yere sahiptir. Özellikle kimlik numarası, banka hesabı vb. bilgilerin yazıldığı ara yüzlerin güvenliği kontrol edilerek bu sayfaların güvenliğinden emin olunmalı, kurum, kuruluş ya da firmalara şüphe duyulan e-postalar bildirilmelidir. (Vural ve Sağıroğlu, 2008; Yıldız, 2014).

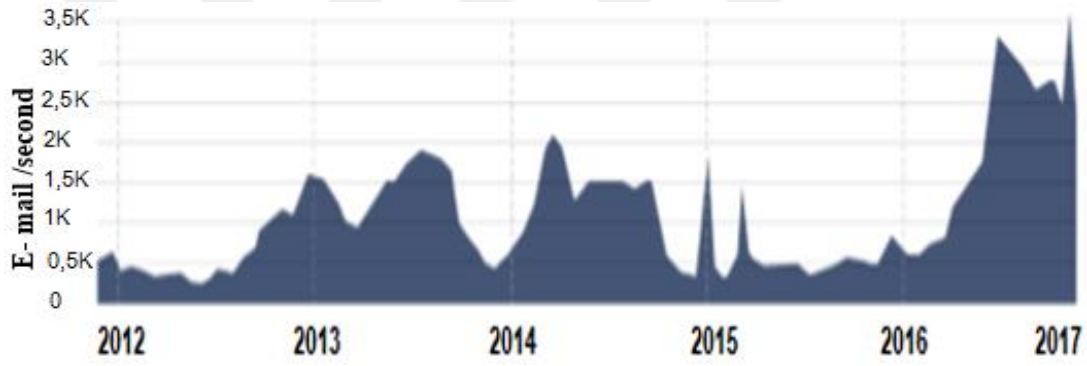
Tahminlere göre önümüzdeki yıllarda teknik bilgiler üzerine kurulu saldırıların yerini, bilgi güvenlik bilincine sahip olmayan kişilerin ortaya çıkartacağı güvenlik açıklarının fazla olacağı, bu açıkların da saldırganlar tarafından ustaca kullanılacağı tahmin edilmektedir (Aslan Öztezcan, 2017). Bu kapsamda devlet tarafından 2009 yılında zorunlu hale getirilen, 2010 yılında uygulanmaya başlanan IBAN numarası ve tek kullanımlık GSM şifre uygulaması dolandırıcılık olayların engellenmesi için hayata geçirilmiş olup suçların önlenmesi ve suçla mücadele adına bu yöntemlerden faydalanılmaktadır. Bu bağlamda sayfa güvenlik kontrol bilincinin kullanıcılara yerleştirilmesi önemli hale gelmektedir.

2.4.3.3 İstem Dışı Elektronik Posta (Spam)

Kolay ve ücretsiz olan bu yöntemde saldırganlar sahte web adresleri aracılığıyla kullanıcıların bilgilerini ele geçirilmeye çalışmaktadır. Bu aldatıcı e-posta içerikleri farklı şekillerde olabilmektedir. Bunlardan bazıları gelen e-postalar yurtdışı kaynaklı olduklarından bozuk bir Türkçe ile ya da farklı bir dilde yazılmaktadır. Bununla

birlikte hesabınız kapatılacak, ceza ödeyeceksiniz vb. kullanıcıları ikna edecek ifadeler içerirken, kullanıcıları tutsak sayfalara yönlendiren bağlantılar bulunmaktadır (Şahinaslan, 2013).

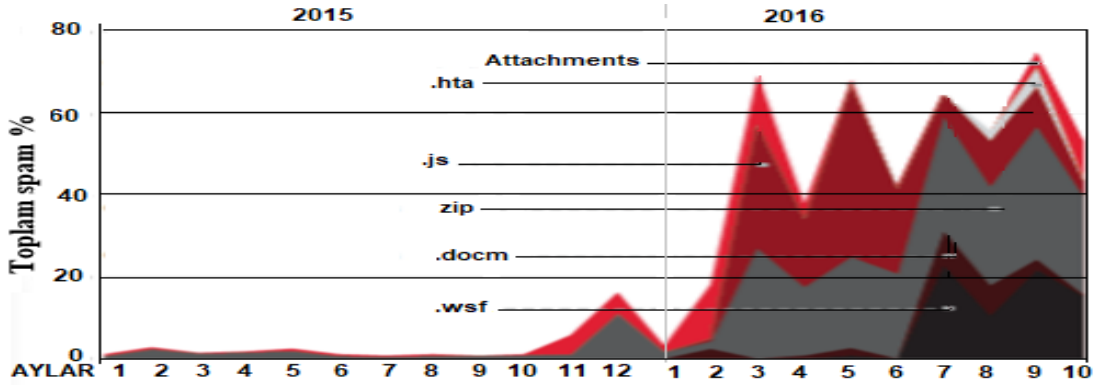
Bilinçli kullanıcılar, bu tarz tuzaklara düşmemekte ve saldırganlarca gönderilen e-postalara cevap vermemekte ancak bilinçsiz kullanıcılar bu e-postalara cevap vererek saldırganların tuzağına düşmektedir (Hekim ve Başıbüyük, 2013). Saldırganlar spam elektronik postalarla hedeflenen kitleden herhangi birinin bu tuzağa düşmesini kendileri için önemli bir başarı olarak görürken bu saldırı yönetimi 2012-2017 yılları arasında en yüksek seviyede ulaşmıştır (Şekil 7). Nitekim elektronik e-postaların %65'ini spamlar oluştururken, bu spamlardan 8 ile 10'u saldırganlar tarafından kötü amaçlı olarak gönderilmektedir (Cisco, 2017).



Şekil 7: 2012-2017 yılları arasında Toplam Spam Hacmi (Cisco, 2017)

E-devlet vb. uygulamalar ile insanlar kamu kurum ve kuruluşlarla hızlı ve kolay bir şekilde haberleşirken gönderilen ve alınan e-postaların güvenliğinin sağlanması ile birey ve kurumların BG'de etkilemektedir. Kurumlar e-posta güvenliğinin sağlanması için yazılım firmalarının ürettiği sertifika ve yazılımlar kullanmasına rağmen tam güvenlik sağlanamamaktadır. Birey ve kurumlar e-posta güvenliğinin sağlanmasında kurum e-posta hizmetini kendi personellerince işletmeli, kaynakları bilinmeyen e-postalar açılmamalı, okunmadan silinmeli, kurum çalışanı personel kurum e-postası kullanmalıdır. Bireyler güvenilir e-posta hizmeti sunan firmaları tercih etmeli, e-posta adresinin üyelik işlemleri sırasında ve sonrasında kullanılan parola farklı olmalıdır. (Öztürk, 2009). Çünkü saldırganlar kötücül yazılım, spam e-postalarda yer alan eklerden yaymaktadırlar. Nitekim Cisco'ya (2017) göre, dünya genelinde Ekim 2015-2016 arasında spam e-postaların yaklaşık %75'i zararlı eklere sahiptir. Spam e-

postaların ekinde ki dosyaların kullanım oranı azalış ve artışları, zararlıların tespit edilme yoğunluğuna göre değişirken yeni saldırılarda, yeni dosya türlerinin kullanım oranının artmıştır (Şekil 8).



Şekil 8: Spam E-Postaların Barındırdığı Zararlı Eklerin Türüne Göre Dağılımı (Cisco, 2017)

2.4.4 Zararlı Yazılımlardan Kaynaklanan Tehditler

Donanım ve yazılımlara ait açıkları kendi çıkarları için kullanan saldırganlar bilgisayar sistemlerine bulaşması ile onlara zarar vermek, bilgi çalmak veya kullanıcıların rahatsız edilmesi için hazırlanan zararlı yazılımlarla istedikleri bilgiye ulaşmaktadır. Kullanıcılar adına tehdit oluşturan saldırılar önceden planlanmış bazı amaçlar doğrultusunda organize olmuş çete veya çıkar maksadı güden örgüt ya da örgütler tarafından gerçekleştirebildiği gibi kendi adını duyurmak isteyen bireysel saldırganlar tarafından da gerçekleştirilebilmektedir (Canbek, 2005; Çalışkan, 2013).

Zararlı yazılımlar hedeflerine sistemde yer alan port ve servis gibi açık olan bir noktanın tespit edilmesi, kullanıcı hataları ve kullanıcıların bilinçsizliğinden faydalanılması sonrasında veya ulaşmak istedikleri bilgisayara yazılımın kullanıcı tarafından yükletilmesi sağlanarak ulaşabilmektedir (Ercan, 2015).

Geçmişte zararlı yazılımlar bireysel eylemler şeklinde gerçekleştiğinde kullanıcıların dosyalarının silinmesine, işletim sisteminin çökmesine ve bilgisayar performansının düşmesine neden olmuştur. Günümüzde daha çok topluma yönelik olup maddi çıkar sağlamak amacıyla kullanıcıların dikkatsizliğinden veya bilgisizliğinden yararlanılmaktadır. Saldırganlar bilgisayarlara yerleştirdikleri zararlı yazılımlar ile internet üzerinden para akışının kontrol edildiği internet bankacılığına ait şifreleri, banka ve kredi kartı vb. önemli bilgilere ulaşabilmektedir (Şahinaslan, 2013).

Günümüzde daha planlı ve organize olarak zararlı yazılım kodları geliştiren saldırganlar, bir araya gelerek güvenlik bilincine sahip olmayan kullanıcılara yönelik saldırılar planlamak ve bu yönde yazılımlar hazırlamaktadır (Gülmüş, 2010).

Kullanıcıların farkındalık düzeylerinin yetersizliği ve saldırganlarca sosyal mühendislik tekniklerinin kullanılmasıyla zararlı yazılımlar kullanıcı bilgisayarlarına erişirken kullanıcı etkileşimi olmadan da teknik önlemlerin yetersizliği nedeniyle bu tip zararlı yazılımlar kullanıcı bilgisayarına bulaşabilmektedir. Bu gibi durumlarda anti-virüs programı yüklemek, güvenlik duvarını etkinleştirmek, anti-malware programları yüklemek ve işletim sistemini güncel tutmak vb. önlemler alınabilmektedir (Çalışkan, 2013). Zararlı yazılımlar ile kişi ve kurumlara ait bilgiler çalınarak başkalarıyla paylaşılırken işletim sistemi ve programların çalışması da etkilenmektedir. Bu durumda mevcut klasör ve dosyalar silinebilir, kopyalanabilir, yeri değiştirebilir ya da yeni dosyalar eklenebilmektedir. Ayrıca fare ve klavye ile yapılan her işlemi kayıt edilirken, açılır pencereler oluşturarak istenmeyen web sayfalarına yönlendirilmekte, bilgisayar diskini biçimlendirmek suretiyle veri kaybına neden olabilmektedir (TÜBİTAK, 2018; 2019)

2.4.4.1 Bilgisayar virüsleri

Biyolojik virüslere benzeyen bilgisayar virüsleri, sistemin içine girerek sistemi içten çökerterek kullanılmayacak hale getirmektedir. Bu virüsler sistem içinde bulunan diğer dosya ve klasörlere kendini kopyalamak suretiyle veri depolama cihazları (CD, DVD, USB Diskler, harici hard diskler vb.) ve veri transferi (sohbet programları, e-posta uygulamaları vb.) yolları ile bulaşmaktadır (Gelişken, 2009).

Bilgisayar virüsleri kullanıcının izni ve bilgisi olmadan cihaz ve işletim sisteminin olanakları ile program ve sistemlere yerleşerek bilgisayardan bilgisayara atlayabilen bilgisayar kodlu parçalar olup bilgisayara, dosyaya ve programlara zarar vermek için sinsice yerleşmektedir (Alaca, 2008; Boğa, 2011; Burlu, 2010). Bu virüsler, araştırma projeleri ile belli başlı firmalara zarar verme, firmaların imajını zedeleme, maddi kazanç sağlama, politik mesaj verme ve bilgi çalma amaçlarıyla oluşturulmaktadır (Burlu, 2010). Kullanıcılar tarafından da en fazla bilinen zararlı yazılım türü olan virüsler, kullanıcıların gelen bir e-postayı açması, internetten *.exe uzantılı bir dosyayı indirmesi ya da taşınabilir bir belleği bilgisayarlara takması sonucunda farkına

varılmadan bulaşmaktadır. Ancak insan etkileşimi ile bulaşan virüslerin aktifleşmesi için kullanıcı tarafından çalıştırılması gerekmektedir (Gülmüş, 2010). Bulaştığı sistem içinde belli amaca hizmet eden virüsler, BG'yi bilginin kaybolması, silinmesi ve bozulması gibi faaliyetler çerçevesinde tehdit ederken programlara eklenerek program yapısını değiştirip, kendi kendilerine çoğalmaktadır (Ünver ve Canbay, 2010).

Virüsler amaçlarına göre, sürücü ya da sıkıştırılmış dosyalara yerleşerek yayılan **dosya;** sabit disk içinde işletim sisteminin çalışması için gerekli dosyaların bulunduğu yere yerleşen **önyükleme (bootsector);** makro özellik barındıran programlara bulaşan **makro,** sürücüler ve yerel ağ üzerinden paylaşılan klasörler aracılığı ile yayılan **ağ** vb. virüsleri olarak gruplandırılmaktadır (Şahinaslan, 2013).

2.4.4.2 Truva Atı (Trojans)

Trojan olarak da adlandırılan Truva atları, başlangıçta faydalı görünen sonradan zararlı olan ikiyüzlü yazılımlardır. Sisteme sanal kapılar açan Truva atları bilişim korsanlarının sisteme sızmasına imkân sağlarken genellikle kullanıcıyı cezbeden programlara konulmaktadır (Gelişken, 2009). E-posta ve farklı internet sayfalarındaki görsel öğeler ile bulaştırılan virüslere benzeyen Truva atları virüsler gibi çoğalmaz, sisteme girdikten sonra belleğe yüklenip, sistemdeki açıkları tespit ederek bilişim korsanına bilgi sağlarken kendilerini gönderen korsanın isteğine göre bilgi değişikliği yapabilmekte veya bu bilgileri silebilmektedir (Boğa, 2011).

2.4.4.3 Bilgisayar Solucanları (Worms)

Solucanlar, bir bilgisayardan başka bir bilgisayara otomatik olarak kendilerini kopyalayan yazılımlardır. Programın çalışmasına gerek duymadan bulaşabilmesi solucanları virüslerden ayıran en önemli özelliktir. Ağ, internet, e-posta ve bilgisayar olmak üzere 4 çeşit olan solucanlar virüslerin alt kümeleri olup sisteme bir kez girdikten sonra kimsenin yönlendirmesine gerek duymadan hızlı ve büyük oranda çoğalarak ilerleyebilmektedir (Canbek ve Sağıroğlu, 2007). Böylece sistemlere yayılarak ağ ve bilgisayarların kullanılmaz hale getirilmesini sağlayan solucanlar, virüsler şeklinde zarar verdiği gibi Truva atı bırakarak da zarar verebilmektedir. Bilgisayarın e-posta listesinde bulunan kişilere bir kopya gönderdikten sonra ulaştığı bilgisayarın da e-posta listesinde bulunan kişilere de bir kopya gönderilerek hızlı bir şekilde çoğalan solucanlar ağların yavaşlamasına, kilitlenmesine ve web sayfaları

görüntülendiği sırada uzun süre beklenmesine neden olabilmektedir (Bilek, 2012; Boğa, 2011; Burlu, 2010).

2.4.4.4 Tuş kaydedici yazılımlar (Keylogger)

Tuş kaydedici yazılımlar, sistemde gizli olarak çalışıp, klavyeye basılan her tuşu okuyarak bunları metin halinde kaydedip bilişim korsanlarına ağ üzerinden bilgi iletmektedir (Burlu, 2010; Gelişken, 2009). Donanım ve yazılım tabanlı şeklinde ikiye ayrılan bu yazılımlardan donanım tabanlı olanlar, yaygın olarak kullanılmamakla birlikte aparatlar ana kart ile klavye arasına yerleştirilmektedir. Yazılım tabanlılar ise daha yaygın olarak bulunmakta çoğu kez kullanıcılar fark etmeden zararlı yazılımlar aracılığı sisteme yerleşir ve kullanıcılar sistemde bir yazılım olup olmadığını anlamazlar, daima gizli halde çalışırlar (Gelişken, 2009).

2.4.4.5 Ekran kaydedici yazılımlar (Screenlogger)

Ekran kaydedici yazılımlar, kullanıcının fareye her tıklamasında bilgileri ya da belli piksel büyüklükte bir grafiği kaydedip belleğe saklayarak, istenildiğinde e- posta yoluyla bilişim korsanlarına göndermektedir (İlbaş, 2009). Ekran kaydedici yazılımlar internet bankacılığı ve e-ticaret sitelerinde keylogger saldırıların önlenmesi için ortaya çıksa da bu yazılımlar sanal klavyenin kullanıldığı sistemlerde, ekrandaki işlemlerin takibini yaparak kullanıcıların bilgilerine ulaşmaktadır (Gökmen, 2014).

2.4.4.6 Casus Yazılımlar (Spyware)

Bilgisayar sistemini ele geçirmek ve gizli bilgilere ulaşmak için kullanıcıların bilgisi olmadan izinsiz olarak sisteme kurulan casus yazılımlar, bilişim korsanlarca amacına uygun olarak geliştirilmekte ve korsanın tanımladığı işlemi yapmaktadır. Buna benzer yazılımlar tarayıcı ayarını değiştirmekte kişisel bilgileri öğrenmekte, verilere ulaşmakta, internette yapılan web sitelerini araştırmakta, kullanıcı adı ile şifreyi çalıp sahte web sitelerine yönlendirmektedir. Bilgisayarda yapılan her değişiklik bilgisayarın açılmasıyla değiştirilirken, casus yazılımlar kendilerini çoğaltmadan arka planda çalışmaktadır. Internet aracılığıyla indirilen bedava ve reklam içerikli bütün yazılımlarda bulunan casus yazılımlardan korunmak için sisteme herhangi bir casus yazılım bulaşmadan anti-spyware programı kurulmalıdır (Gelişken, 2009).

2.4.4.7 Reklam Bedelli Yazılımlar (Adware)

Çoğunlukla reklamcı ve pazarlamacılar tarafından kullanılan özel bir casus yazılımı olan bu yazılımlar yasal bir yazılım bilgisayara kurulduğunda ana kurulumdan bilgisayara yerleşirler. Bu yazılımı kuran çoğu kullanıcı ilk kurulum aşamasındaki şartları okumadığından bu yazılımın kurulduğundan habersiz olmaktadır. Reklam bedelli yazılımların çalışma şekli casus yazılımlar gibi olup bilgisayardaki her işlemi izleyerek reklam firmasına iletirler. Ayrıca sık sık ziyaret edilen sitelere tarayıcı da uygun kişileştirilmiş reklam görüntüler, internette buna benzer yazılımlar kurulur ve indirilirken, casus yazılım bileşeni olanlara hayır denilerek bu yazılımlara karşı önlem alınabilmektedir (Miller, 2003).

2.4.4.8 Çöp Mail

Çöp mail, kullanıcıların e-posta hesaplarına bilgileri olmadan gelen, reklam içerikli metin, resim veya internet sitesiyle ilgili bağıntılardan oluşan, kimin tarafından gönderildiği belli olmayan sahte bilgi dolu e-postalardır. Mesaj içeriği kolay para kazanacağınız e-posta veya ödül kazandınız şeklindeki mesajlar zarar oluşturmazlar ancak içlerinde zararlı scriptler veya solucanlar barındırarak zararlı olabilmektedir. Bu e-postaların içeriğinin sahte oluşları, mesajı gönderen kişi ile mail adreslerinin garip olmasından anlaşılan çöp maillerin zararlarından korunmak için güvenli olmayan kişi veya internet sitelerine e-posta adresleri verilmemeli, filtreleme yazılımlar tercih edilmelidir (Gelişken, 2009).

2.4.4.9 DOS (Denial of Service) ve DDOS (Distributed Denial of Service) Saldırılar

DOS saldırıları, sistemin çökmesine veya sistemi kullanarak kullanıcının sisteme erişiminin engellemesidir. Burada amaç, kullanıcının sisteme izinsiz giriş yapması değil sisteme erişiminin engellenmesidir. DOS saldırılar sonucunda sistem ve servislerin aşırı yüklenmesiyle kullanıcılar hizmet alamazken DOS saldırısını sistemin herhangi bir güvenlik açığı bulunmadığında veya kullanılan yöntemin başarısız olması sonucunda kullanılmaktadır (Yılmaz, 2005; Burlu, 2010). DOS saldırılar tek hedefe doğru bir noktadan gerçekleştirilirken DDOS saldırıları tek hedefe birçok noktadan gerçekleştirilmektedir. Bilişim korsanları bilgisayarlara kötücül yazılımlarla sızarak DDOS saldırılarını gerçekleştirirken bu bilgisayarlar daha sonra kullanılarak hedef kullanıcıların sistemlere erişimi engellenmektedir (Delialioğlu, 2011).

2.4.4.10 Köle Bilgisayar (Zombi)

Bilişim korsanları amaçlarına ulaşmak için DDOS saldırılarında bulundukları birden fazla sistemi ele geçirmesiyle bilgisayarlara zombi adında yazılımlar yerleştirmektedir. Zararlı yazılım yerleştirilen bilgisayarlar tek bir komut ile hedef sisteme yönlendirilerek kontrol altına alındıklarından köle bilgisayar adını alırlar. Bu saldırılar sonucunda köle bilgisayarların sayısı binlere ulaşmakta, bilişim korsanları tarafından birçok yöntem kullanarak bu sistemler köleleştirilmektedir. Bu yöntemler zombi yazılımı direkt yerleştirilme ve Truva atı vb. bir yazılımla bilgisayarlara indirerek yapılmaktadır (Elbahadır, 2010).

2.4.4.11 Mantık Bombaları

Bilişim sistemine yerleştiği zaman hemen sisteme doğrudan zarar vermeyen ancak planlanan saatin gelmesini ya da şartların gerçekleşmesini bekleyen mantık bombaları, saldırganların talimat göndermesiyle göreve başlar, talimat verilinceye kadar kendilerini sistemde etkisiz olarak bulundurarak talimatla birlikte sisteme kalıcı hasar vermektedir (Ercan, 2015; Taş, 2010).

2.4.4.12 SQL Enjeksiyon

Veri tabanlarına ulaştıktan sonra diğer programlama dilleriyle çalışarak yeni kayıt ekleme, silme, listeleme ve güncelleme gibi işlemleri yapan bir yazılım dili olarak bilinmektedir. MySql, MsSql, Oracle vb. birçok veri tabanı SQL diliyle çalışmaktadır. Masaüstü programlar ve web yazılımlar veri tabanı işlemini yaparlarken SQL dilini kullanarak çalışmakta ve SQL komutlarını kullanmaktadır. SQL enjeksiyon saldırısı, SQL komutları ve bazı ortak kullanılan karakterler ile yapılmaktadır (Burlu, 2010; Gündüz, 2013).

2.4.4.13 Arka kapı (back door)

Çok sayıda bulunan arka kapılar, kalıcılığın sağlanması ve istendiği zaman sisteme girmek için sistem yazılımını yapan kişi tarafından gizli olarak yerleştirilen virüs programıdır. Sistem yazılımını yapan kişinin sisteme sızabilmesi için bu programın çalışması gerekmektedir. Truva atları da bu sistemlerden biri olarak iş görmektedir. Genel amaçları kullanıcılara ait özel bilgi ve programlara ulaşmak olurken, sisteme ve kullanıcıya zarar vermemektedirler (Alaca, 2008; Boğa, 2011; Yılmaz, 2005).

2.4.4.14 İzleme ve Gizleme (Sniffing and Spoofing)

Bilişim korsanları (saldırgan) hedeflerine ulaşmak için sosyal mühendislik yöntemlerini kullanarak sistemlere sızarken öncelikle kendilerini gizleyip sistemi izlemektedir. Bilgisayar ağındaki her türlü bilgi ve veriyi izlemeye imkân sağlayan izleme, yöneticiler ve korsanlarca kullanılan önemli bir yöntem olup kullanıcıya ait birçok bilgi bu yöntemle ile ele geçirilebilmektedir (Elbahadır, 2010; Gündüz, 2013). Ağdaki bilgisayarlara, başka bilgisayarmış gibi kendini gösteren ve bu şekilde ulaşılmayan bilgiye ulaşma işlemi olan gizleme, bilişim korsanlarının hedef sisteme sızdıktan sonra güvenlikleri için kimlik bilgilerini gizleyerek ve sistemdeki kayıtlarını silerek arkasında hiçbir iz bırakmadan hareket etmesidir (Elbahadır, 2010; Yılmaz, 2005).

2.4.4.15 Web Sayfa Hırsızlığı ve Web Sayfasının Yönlendirilmesi

IP adresleri bilgisayarların birbirlerini tanıması ve iletişim kurması için veri iletimi sağlayan 32 bitten oluşan veriler olup, 4 haneli 8 bit (xxx.xxx.xxx.xxx) rakamlardan oluşurken web sayfalarının kendilerine özgü IP adresleri bulunmaktadır. DNS, bilgisayarlarda IP adreslerinin tutulduğu ve ağ hizmetlerinin barındığı bir sistem olurken DNS veri tabanı sunucularında alan adları tutulurken, alan adlarının adresleri www.microsoft.com ve www.mynet.com.tr şeklindedir (Alaca, 2008; Elbahadır, 2010). Alan adları tarayıcının adres çubuğuna yazılarak web sitesine ulaşılırken DNS veri tabanında sorgular ve web sayfasının bulunduğu sunucunun IP adresini öğrenir ve IP adresinden de sayfayı tarayıcıya yükler. Uygun bir alan adı almak için kişi veya kurumlar alan adı hizmeti veren servis sağlayıcılara başvurarak bir web sayfası yayınlamaktadır. Alınan alan adı kişiye veya kuruma tescillenerek isim hakkı kişiye ve kuruma ait olurken web sayfası hırsızlığı genel olarak, tescili yapılmış isim hakkı alınmış bir alan adının bilişim korsanlarınca ele geçirilmesi, değiştirilmesi ve üçüncü şahıslara yüksek parayla satılmasıyla meydana gelmektedir (Alaca, 2008). Burada öncelikle gerçek web sitenin (örneğin www.hotmail.com) sahte siteleri (örneğin www.hotmail.c.com ve www.hotmaij.com) yapılıp kullanılmaktadır (Gelişken, 2009). En çok internet bankacılığı ve internet üzerinde yapılan alışverişlerde kullanılan bu yöntemde, saldırganlar sahte web sitesi yaparak kullanıcıların farkına varmayacağı sahte web sayfalarına yönlendirerek, kullanıcıların birçok bilgisi ele geçirilmektedir (Boğa, 2011).

2.4.4.16 Rootkitler

Virüs türevi yazılımlar olan rootkitler, sistem içerisinde sistem yetkilileri ile çalışan hedef dosyalarını ve süreçlerini saklayan ve değiştiren uygulamalardır. Rootkitler sistemi ele geçirdikten sonra uzaktaki kötü niyetli kullanıcılara/korsanlara bilgisayar üzerinde kontrole sahip olma imkânı sağlamaktadır (Burlu, 2010). Rootkitler önceden derlenip hazırlanarak yazılım içine Truva atları yerleştirilmesiyle kuruluma hazır hale getirilmiş programlar olarak da bilinmektedir (Yılmaz, 2005). Kök araçları olarakta bilinen rootkitler sistem araçları içerisinde kullanılan tüm programlara kökler şeklinde sarılarak kendilerini yerleştirmektedir. Genellikle kullanıcının internette gezinirken ya da bir dosya indirirken karanlık bir ekran aracılığıyla evet veya hayır şeklindeki seçeneklerin tıklanması ile sisteme ulaşırlar. Rootkitleri diğer zararlı yazılımlardan ayıran en önemli özellik çok iyi gizlenerek sisteme sızmaları, sistem araçları ile yer değiştirerek hareket etmeleridir (Elbahadır, 2010). Rootkitler sistem yerine tarayıcı ya da çalışan uygulama tarafından gönderilen sorguları cevaplandıracak yeteneğe sahip olduklarından sistem tarafından gelen her sorguyu cevapladıkları için güvenlik yazılımlarından bir sorgu gelmiş olsa dahi bunu cevaplayarak gizliliklerini sürdürebilirler. Rootkitler dosyaları, kayıt defteri kayıtlarını ve çalışan uygulamaların işlemlerini gizler, istenen işlemleri yönlendirir ve arka kapıların açılmasını sağlarlar (Burlu, 2010; Elbahadır, 2010).

2.4.4.17 Botlar

Robot kelimesinden gelen ve sıkça kullanılan botlar, DDOS saldırıları olarak bilinirken aynı anda birden fazla bot ’un bir araya gelerek gerçekleştirdiği saldırılardır (Burlu, 2010). BOTNET olarak da bilinen botlar, toplu saldırılar gerçekleştirilirken kendilerine tanımlanmış komutlar sayesinde bilgisayar kullanıcısı gibi hareket ederler. Botların yayılması; sahte web siteleri, taşınabilir dosyalar ve sahte e-postaların kullanıcılar tarafından temas edilmesi ile gerçekleşmektedir. Botlar sanal kullanıcı gibi internet sitelerinde bulunan virüslü dosya da programları otomatik olarak indirip kurarak bilgisayar korsanlarının sisteme erişimini sağlamaktadır (Gelişken, 2009).

2.4.4.18 Exploit

Geçmişte işletim sistemleri ve kişisel bilgisayarlar DOS gibi tek kullanıcılı iken günümüzdeki çok kullanıcılı sistemler kullanılmaktadır. Sömürmek, istismar etmek, faydalanmak, işletmek ve kötüye kullanmak anlamlarına gelen exploitler program bilgisi yüksek olan kullanıcılar tarafından kullanılmaktadır (Burlu, 2010). Exploit uygulamalar bilişim korsanları tarafından yetkisiz kullanıcı profiline yönetsel yetkiler kazandırarak sistemin zayıflığından yararlanmalarıyla sisteme zarar verirken daha çok çaylak veya "**Script Kiddie**" olarak adlandırılan hack konusuna fazla hakimiyeti olmayan kişilerce kullanılmaktadır. Yazılım konusunda uzman olan kişilerce hazırlanan exploitlerin çaylaklar tarafından ele geçirilmesi ile güvenlik açığı neticesinde mevcut sistemlere saldırılar düzenlenebilmektedir (Elbahadır, 2010; Yılmaz, 2005).

2.4.4.19 Reklam içerikli pencereler (Pop-up Ads)

Bir web sitesi sayfasının yüklendiği sırada kendiliğinden açılan ve reklam içeriği olan tarayıcı pencereler olan Pop up'lar bilişim korsanlarınca bazen basit reklam görüntüsü şeklinde bazen de bir şey vaat ederek kullanıcıları başka sahte sitelere yönlendirebilmektedir. Korsanlar pop-up'lardaki kötü yazılımları kullanıcıların kişisel bilgilerini ele geçirebilmek için kullanmaktadır (Miller, 2003; Ünver ve Mirzaoğlu, 2001).

2.4.4.20 Uzaktan yönetim araçları (RAT: Remote Administration Tools)

Bilişim korsanları bilgisayarlarında yüklü bir program ile kullanıcının internette indirmiş olduğu RAT programları aktif hale getirerek sisteme erişimi sağlanırken bu araçlar Truva atı gibi davranmaktadır (Gelişken, 2009).

2.5 Bilgi Güvenliğinin Sağlanması

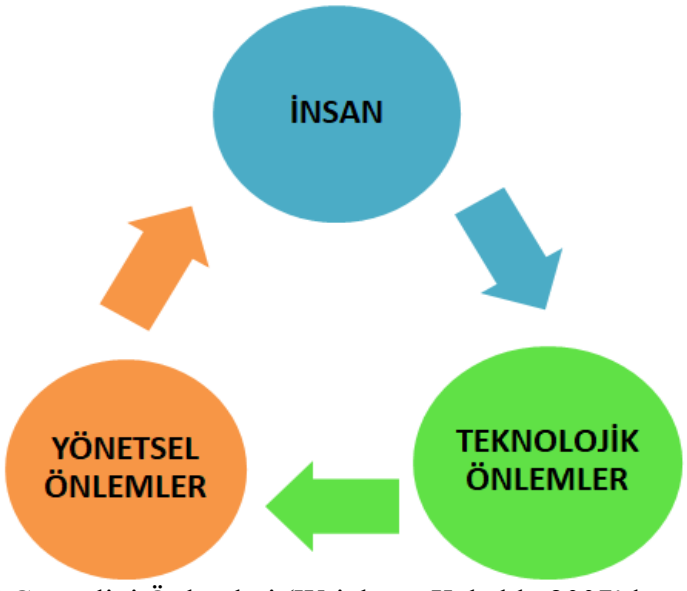
Bilgi doğruluğunun ve bütünlüğünün bozulmadan yetkisi olmayan kişilere geçmesini engellemek için alınan önlem ya da önlemler dizisi olan BG'ye karşı yapılan saldırıları en az seviyeye indirmek için önlem almak gereklidir (Canbek ve Sağıroğlu 2006; Marks, 2007; Vural ve Sağıroğlu, 2007). Kurumsal anlamda, BG, kurumda kullanılan ürün veya hizmetlerin sürekliliğini sağlamak için kurumsal bilginin olası tehlikelere karşı korunmasıdır (Bensghir, 2008). Kurumsal BG'nin sağlanması, kurumun kendi kültür ve yapısına göre önlem almasını gerektirirken güvenlik hedefleri kurumların

yapısına göre farklılık göstermektedir. BG'nin kurumsal olarak hedeflerinin özel firma ve şirketlerde bilgiye yüksek erişilebilirliğin sağlanırken kamu kurumlarında bilgi gizliliği ve korunması oldukça önemlidir (Yıldız, 2007). BG'nin tam olarak sağlanabilmesi birbiriyle bağlantılı olan insan, yönetsel ve teknolojik önlemlerin (Şekil 9) bir bütün olarak gerçekleşmesi ile mümkündür (Öztürk, Tekerek ve Yılmaz, 2016).

2.5.1 Yönetsel Önlemler

BG yönetimi, güvenlik kurallarının belirlenmesi plan, strateji ve politikaların doğru bir şekilde uygulanmasıdır. İş sürecinin bir parçası olarak değerlendirilen bu önlemler yönetim ve kuruma ait bir kültür olarak da bilinmektedir. Kurumlar sahip oldukları BG politikalarını yazılı hale getirerek çalışanlara, paydaşlara ve iş ortaklarına bildirerek, çalışanların politikalardan haberdar olması gereklidir.

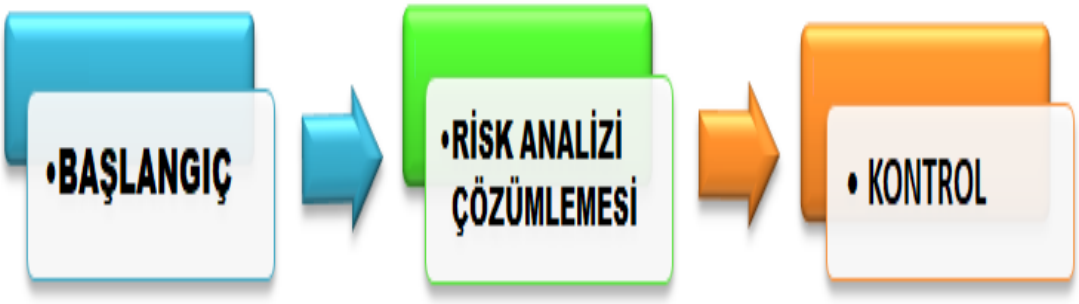
Tek başına alınan güvenlik politikaları yeterli olmayıp bu konuda çalışanların sorumluluklarını bilerek BG bilinciyle ulaştıkları bilgilere sahip olmalıdır. Bunların yanında üst yöneticiler tarafından yayınlanan güvenlik politikaları BG'nin önemini ortaya koyarak uygulama aşamasındaki sorumlulukları tanımlanmalı iş ortaklarını da kapsayacak şekilde güvenlik politikalarını düzenlenmelidir (Doğantimur, 2009). Özellikle risk yönetim politikaları belirlenerek bu güvenlik politikaları kapsamında standartlar yönergeler ve prosedürler hazırlanmalı, süreç sonunda da gerekli güvenlik denetimleri yapılmalıdır (Yıldız, 2014).



Şekil 9: Bilgi Güvenliği Önlemleri (Wright ve Kakalık, 2007'den değiştirilerek)

2.5.1.1 Risk yönetimi

BG'ye yönelik, doğal afetler, prosedürel eksikler, insan ve zararlı yazılımlardan kaynaklanan tehditler tamamen ortadan kaldırılamadığından kurum çalışanları ve yöneticilerin bir risk oluşturma ihtimaline karşı tedbirler alınmalı, risk oluştuğunda anında müdahale için çeşitli politikaların hazırlanarak işlerin aksaması veya kesintiye uğraması engellenebilir (Gülmüş, 2010). Risk yönetiminin ana hedefi, sistemlerin sürekliliğini, erişilebilirliğini, bütünlüğünü, doğruluğunu sağlarken (Şekil 10) bilgi gizliliğini güvence altına almaktır (Ward ve Smith, 2002). Risk yönetim sürecinin son aşaması olan kontrol aşamasında risklerin ya tamamen yok edilmesi ya da en az seviyeye indirilmesi gerekmektedir. Kontrol aşamasında risk planlaması çok iyi bir şekilde yapılmadığı takdirde, kurum işlerinin durmasına ya da aksamasına neden olurken yeni büyük risklerin ortaya çıkmasına neden olabilmektedir (Gülmüş, 2010).



Şekil 10: Risk Yönetimi Sürecinin Aşamaları (Kuyumcuoğlu ve Başoğlu, 2008'den değiştirilerek)

Risk değerlendirilmesi için riskler belirlenip öncelik sırası belirlenmeli oluşacak riskleri bertaraf etmek veya en az seviyeye indirmek için maliyet, yararlılık ve uygulanabilirlik vb. alternatif çözümler göz önünde bulundurularak değerlendirilmeli ve buna göre planlar yapılmalıdır (Yıldız, 2014). Riskleri en alt seviyeye indirmek için esnekliği minimum düzeyde tutmak ve bu durumu güvenlik kültürünün kurum içine yerleştirmek ile mümkün olmaktadır (Koskosas ve Paul, 2004). Risk yönetimi prosedürleri kurum bünyesinde genellikle bilgi işlem bölümleri tarafından yürütülmektedir. Böylece son kullanıcıların risk yönetimi prosedürleri için önlemleri benimsemesi ve uygulaması gerekmektedir (Kuyumcuoğlu ve Başoğlu, 2008).

2.5.1.2 Güvenlik Politikaları

BG'nin sağlanmasında önemli bir yere sahip olan kullanıcıların anlayabileceği şekilde hazırlanan güvenlik politikalarının hem uygulanması hem de yönetimi daha kolaydır (Tekerek, 2008). Kurumların BG politikaları ve uygulamalarını oluşturarak zamanla kritik konuma gelen bilginin tehdit ve tehlikelerden korunması gerekmektedir. Ülkemizde ki kurum ve kuruluşların BG politikaları standartlara uygun olmazken kullanıcılara sözlü ve e-posta yoluyla duyurulup kullanılmasına karşılık kullanıcılara yazılı olarak duyurulması daha uygundur. Çünkü kurumun iş ihtiyacı ve hedefi doğrultusunda yönetimce desteklenip onaylanan güvenlik politikalarını benimseyecek ve iş aşamasında daha kolay uygulayacaktır (Gülmüş, 2010). İyi bir güvenlik politikasının, kullanıcıların işini kolaylaştıran, tepkiye neden olmayan, gerçekçi ve uygulanabilir olmasının yanı sıra güvenlik politikasından sorumlu kişilerin sorumluluk ve yetkilerinin ayrıntılı olması, politikalarda kuşku ve çelişkinin olmaması, yönetim ve birimlere politikaları uygulamaları için idari ve teknik yetki verilmesi gerekmektedir. Denetim ve izleme (e-posta veya dosya içeriği erişimi, kullanıcı hareketlerin kayıt edilmesi vb.) işlemlerinin nasıl yapılacağı ve kişisel hakların korunması için kullanıcı mahremiyet politikaları belirlenmeli, istisnai ve alternatif uygulamalar net bir şekilde belirtilerek kuşku ve şüpheye yer verilmemesi gerekmektedir (Vural ve Sağıroğlu, 2007).

Genel BGF, kullanıcı ya da çalışanların BG ile ilgili temel bilgileri, potansiyel tehditler ve olası etkiler ile ilgili bilgi sahibi olmasıdır. **BG politikası farkındalığı** ise kurum bünyesinde uygulanan ve oluşan tehditlere karşı kullanıcıların ya da çalışanların ne gibi önlemler alacağını kapsayan güvenlik politikalarından haberdar olması ve politikada yer alması gereken hedefleri anlamasıdır. Kullanıcılar mevcut olan politikaları uygularken, kullanıcı hesap şifresinin güvenli olması gerektiğini bilmeli ancak kullanıcı kurumsal şifre belirlerken bu politikalarla ilgili bilgi eksikliği ve bunun nasıl uygulanacağı ile ilgili konularda yeterli değildir (Erol, 2016). Bu nedenlerle kullanıcılar daha fazla bilgilendirilmeli, dikkat edilecek hususlar için alt politikalar geliştirilmelidir. Vural ve Sağıroğlu (2007) 'na göre bazı alt politikalar şunlardır;

a) Kullanıcılara ait hesapların oluşturulması, yeni şifre belirleme, şifre değişikliği ve şifre unutma, e-posta trafiği (gönderim-alım) esnasında

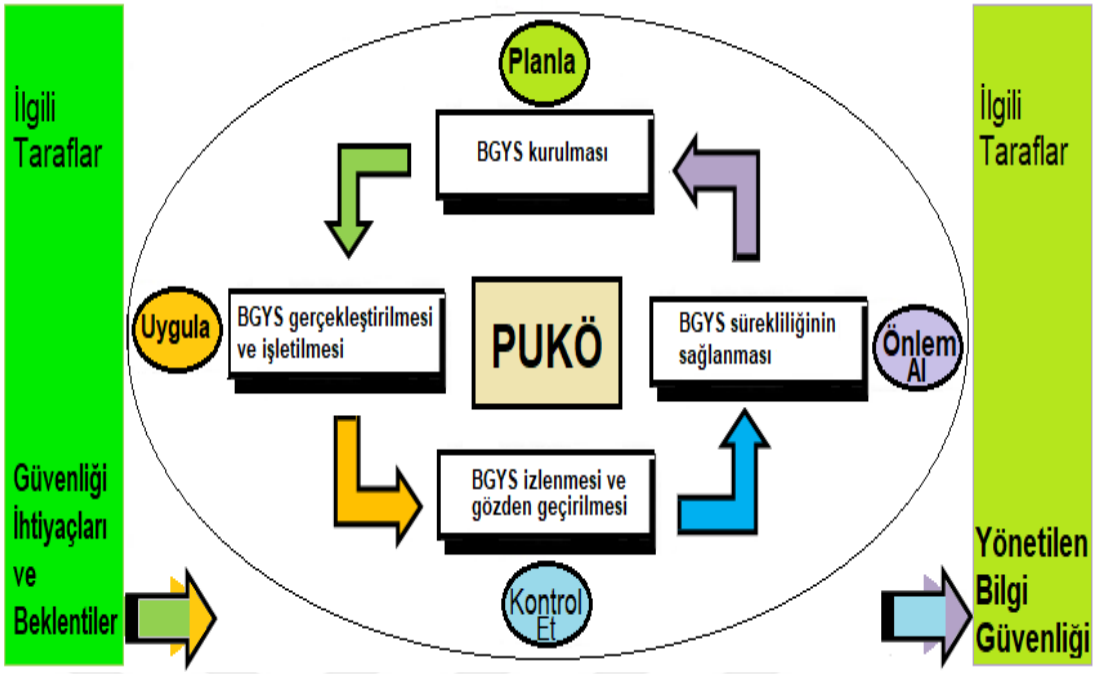
kullanıcılarca yerine getirilmesi gereken kurallar ile üst yönetime ait karar ve haklar,

b) Çalışanların e-posta içeriklerinin gerekli olması durumunda üst yönetim tarafından okunabileceği ifade edilmeli, kullanıcıların bilgisayarlarında uygulanacak olan erişim ve denetim ölçütleri ile sınırlıkları,

c) Sistem güvenlik tedbirlerinin alınabilmesi için yazılım ve donanım kullanımı konusunda açıklamalar yapılmasıdır.

BG'de kurum ve kuruluşlar dünyada kabul görmüş olan standartları esas alarak kullanmalı, bu standartlara göre eksikliklerini gidermelidir. Bu kapsamda Bilgi Güvenliği Yönetim Sistemi (BGYS) kurulmalı üst yöneticiler ve çalışanlarca desteklenerek uygulanmalıdır. Ayrıca iş birliği içinde yer alan kurum ve kuruluşların bu politikalara uyarak taviz vermeden yerine getirmesi gerekmektedir (Özcan, 2009). Kurum ve kuruluşların sadece kendi kurumlarında BG ile ilgili tedbirleri almaları yeterli olmazken aynı zamanda iş yaptıkları firma, şirket, kişilerinde bu konuda tedbirli olmaları için bazı prosedürler hazırlanmalıdır. Bunlar arasında sistemlere nasıl erişimin sağlanacağı, erişim sağlanan bilginin hassasiyet derecesi ve hangi aralıklarla bilgiye erişimin sağlanacağı vb. durumlar bildirilmelidir (Yıldız, 2007).

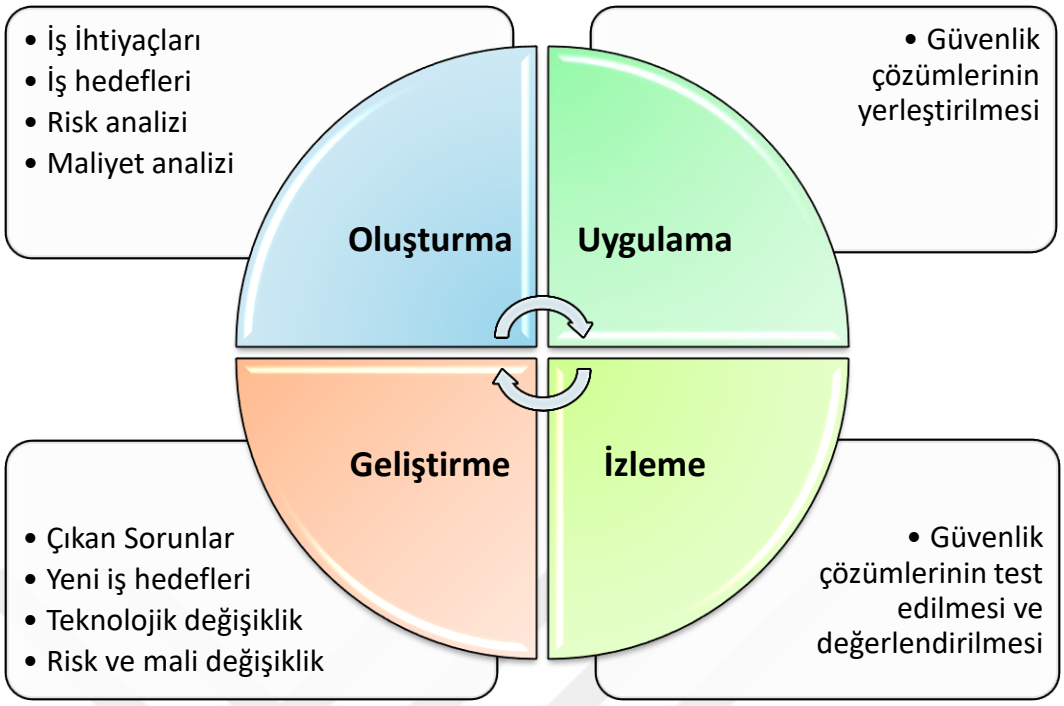
İlk kez 1998'de İngiltere'de yayınlanan BGYS'nin Uluslararası Standartlar Kurumu (ISO) tarafından kabul edilmiş ve en yaygın olarak kullanılan "ISO/IEC27002:2005 standartının Türkçesi Türtk Standartlar Enstitüsü (TSE) tarafından TS ISO/IEC 17799:2005 ve TS ISO/IEC 27001:2005 isimleri ile yayınlanmıştır. Bu standartlar Türkiye'de BGYS konusunda en temel başvuru kaynaklarıdır. Burada BGYS'in kurulumu, gerçekleşmesi, işletilmesi, izlenmesi, gözden geçirilmesi, sürdürülmesi ve tekrar gözden geçirilmesi için Planla–Uygula – Kontrol et – Önlem al (PUKÖ) modeli kullanılmaktadır (Şekil 11). Buna göre BGYS sürekli devam eden gelişim süreci olan PUKÖ gibi döngü içinde sürekli devam etmektedir. PUKÖ BGYS'nin ne yapılacağına karar verilmesi, kararların gerçekleştirilmesi, çalıştığının kontrol edilmesi hedefine uygun çalışmayan kontroller için önlemlerin alınmasını sağlamaktadır (Öztürk, Yüksek ve Aslan, 2014).



Şekil 11: PUKÖ Modeli (Öztürk, Yüksek ve Aslan, 2014'den değiştirilerek)

Kurumdan kuruma farklılık gösteren BG politikalarında temel olarak; BG tanımı, hedefi ve kapsamı, yetkileri ve sorumlulukları, bilgi paylaşımında alınacak güvenliklerin önemi, kurum hedeflerine ulaşmada BG'nin önemi, risk analizinin yapılması ve güvenlik önlemlerinin nasıl alınacağı belirlenmelidir. Ayrıca ek standartların belirlenerek (Şekil 12) doküman haline dönüştürülmesi ve uyulması için her kurum kendi prensiplerini belirlemelidir. Kurumların bilgi sistemlerinde çalışan ve erişimi olan kullanıcıların güvenlik politikalarını uygulamadıkları sürece yaptıkları çalışmalarda başarılı olmaları beklenmezken her kurumda güvenlik politikası yaşam döngüsünün olması gerekmektedir (Yıldız, 2007).

Kullanıcıların güvenlik bilincinin oluşabilmesi için gerekli uygulamalı eğitimler yanında seminer, çalıştay ve hatırlatıcı notlar verilerek kullanıcıların güvenlik bilinci sürekli canlı tutulmalıdır. Güvenlik politikalarının kendilerini kısıtladığını düşünen kullanıcılar güvenlik politikalarını uygulamadıkları durumda, güvenlik politikaları tabana yayılmalı, çalışanların güvenlik politikası ile ilgili kafalarını meşgul eden her soruya cevap verilerek bilgilendirilmeli, kurum çalışanları ve üst yönetim sahiplenmelidir (Yıldız, 2007).



Şekil 12: Güvenlik Politikaları Döngüsü (Tekerek, 2008 'den değiştirilerek)

2.5.1.3 Standartlar, Yönergeler ve Prosedürler

Standartlar, güvenlik politikalarının bir alt basamağı olup kurumdaki işlerin nasıl yapılacağına dair kuralların olduğu dokümanlardır. Burada amaç aynı işi aynı yöntem ve araçla yaparak bütün kurumlardaki işlerin işleyişini bir standarda bağlamaktır. Belirlenen standartların da en az güvenlik politikaları kadar kesin ve bağlayıcı olması gerekmektedir (Yıldız, 2007).

Yönergeler, yol gösterici öneriler içerirken standartların uygulanması sırasında meydana gelen güçlükler karşısında devreye girerken s**tandartlar,** daha kapsamlı ve daha geneldir. Yönergeler, günlük hayatta ve uygulama sırasında meydana gelen problemleri ele alırken standartlarda açık bir şekilde belirtilmeyen, gri alan olarak adlandırılan yerlerin açığa kavuşturulmasında önemli bir yere sahiptir (Pro-G, 2003). Yönergeler, yasalara uygun olarak, kurumun ihtiyaçlarına göre geliştirilip, değiştirilerek, zaman zaman güncellenerek ve uygulanabilir olmasına dikkat edilerek hazırlanmalıdır (Doğantimur, 2009). Kurum güvenliğinde öncellikle güvenlik politikalarının içeriği BG tanımı, kapsamı, amacı, varlıklar, rol ve sorumluluklar, personel güvenliği, paydaşların sistemle olan bağlantısı, erişim ve yetkileri şeklinde ayrıntılı olarak belirlenmelidir (Akay, 2014). Çoğu kurumda BG hizmetlerin aksamadan devam edebilmesi için ayrıntılı iş akış şemaları kurum çalışanlarının elinin

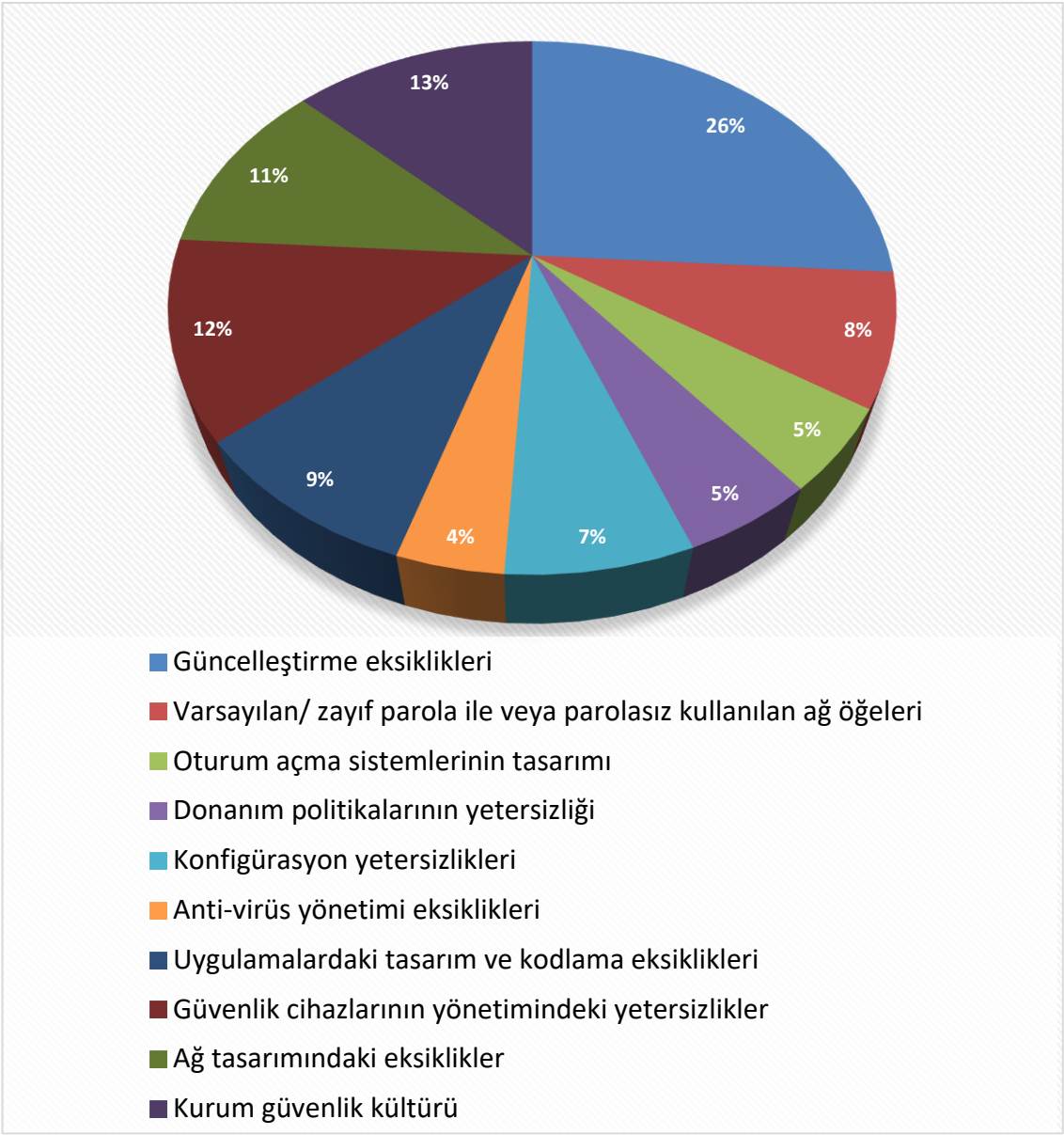
altında bulunmalı güvenlik politikasındaki prosedürler, yönergeler ve standartlar birbirini tamamlar nitelikte olmalıdır. Örneğin kurumsal BG için kurumun standart, yönerge ve politikalarını tüm çalışanların kabul ederek uygulaması, tehdit ve tehlikeler karşısında hangi yollar izleneceğini detaylı bir şekilde bildirilmelidir. Ayrıca kurum çalışanlarının interneti kişisel amaçlarla kullanmaları BG'yi de riske atarken kişisel BG prosedür, yönerge ve standart oluşturmak güçtür (Erol, 2016).

2.5.1.4 Güvenlik Denetimleri

Güvenlik denetimleri, kesintisiz devam eden güvenlik politikalarının belirlenmesi ve bu politikaların korunma sürecinin bir parçası olup bu denetimlerde cevaplanması gereken anahtar sorular arasında;

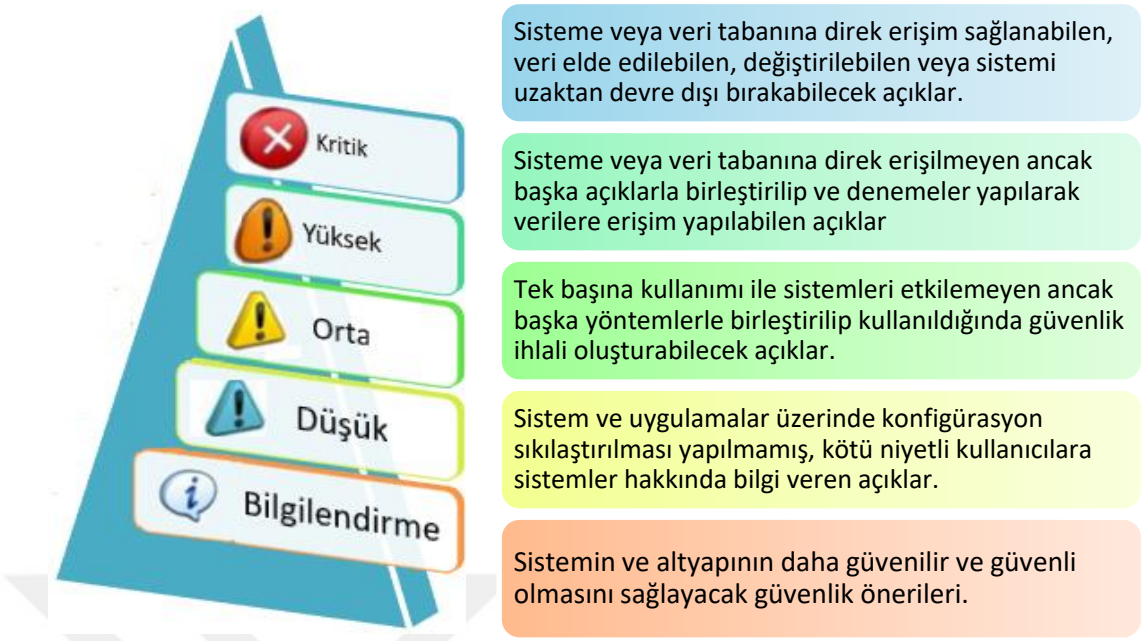
- ✓ Şifreleri kırmak kolay mı, zor mu? Erişim kontrol listeleri mevcut mu? Veriye kimin eriştiği güncel olarak kayıt altına alınıyor mu? Günlük denetim sürekli tekrar kontrol edilip göz gezdiriliyor mu? Güvenlik ayarları işletim sistemleri için uygun kabul edildi mi? Gereksiz uygulamalar ve bilgisayar hizmetleri gözden geçirilerek, gereksiz olanlar eliminasyona tabi tutuldu mu?
- ✓ İşletim sistemleri var olan seviye ile uyuşmakta mıdır? Yedekleme medyaları nasıl saklanıyor, yedeklemelerde gerekli güncellemeler yapılıyor mu, yedeklemelere kimler erişim sağlıyor? yer almaktadır.

Güvenlik denetiminde bu soruların dikkatli, doğru ve dürüstçe cevaplanması ile kurumun BG'nin gerçekçi bir değerlendirmesi yapılabilmektedir. BG, bilgi teknolojilerinin ötesinde insan unsurunu da barındırarak insanların farkında olmadan ve dikkatsiz kullanımları ile güvenlik boşluklarına neden olabilmektedir. Güvenlik denetimi, bilgi teknolojisi alt yapısı ve ekip davranışları içinde sorunlu olan bölümleri su yüzeyine çıkarmayı ve bunlara dikkat çekmeyi hedeflerken yapılan her denetim de olabilecek riskleri belirlemeye yönelik olmalıdır (Doğantimur, 2009). Muharremoğlu (2013), yaptığı araştırmada kurumlarda yapılan güvenlik denetimleri sonucu ortaya çıkan kök nedenlerin dağılımlarında en fazla uygulamalardaki tasarım ve hataların olduğunu belirtmiştir (Şekil 13).



Şekil 13: Güvenlik Denetimlerinde Kök Nedenlerin Dağılımları (Muharremoğlu, 2013)

Buna göre açığın teknik derecesi ve kurum açısından önemi değerlendirilmeye alınmalıdır. Örneğin, çok fazla kullanılmayan bir sistemde meydana gelecek teknik anlamdaki açık seviyesi yüksek olsa bile, önemsiz olarak değerlendirilirken, kritik bir noktada çalışan bir sistemde yer alan küçük bir açık büyük önem taşımaktadır **(**Dinçkan, 2008). Teknik derecelendirmede kullanılan kriterler (Şekil 14) kritik, yüksek, orta, düşük ve bilgilendirme olmak üzere 5 basamakta bulunmaktadır (Muharremoğlu, 2013).



Şekil 14: Açıkların Teknik Olarak Seviyelendirilmesi (Muharremoğlu, 2013'dan değiştirilerek)

Güvenlik standartları ve kılavuzları güvenliğin dinamik bir süreç olduğu bilinciyle hazırlanarak geliştirilirken BG'nin sağlanabilmesi için sistemi kullananların ve teknik personelin kendini güncelleyerek geliştirmesi gereklidir. Teknolojileri kullanan insanların yeterli bilgiye sahip olmadığı durumlarda yalnızca teknoloji değil BG sağlanamadığından teknoloji kullanımı da BG sağlanması aşamasında yetersiz kalacaktır (Vardal, 2009). Genel anlamada virüslerden kurtulma, ağ problemleri çözümleme, yetkisiz erişimleri sınırlandırma vb. yöntemler BG'nin sağlanması için çoğunlukla kullanılan teknolojik çözümler kişisel ve kurumsal BG kavramının içinde yer almaktadır (Civelek, 2011). Teknolojik önlemlerin hem kişisel hem de kurumsal BG için oldukça önemli olurken bu yöntemlerin yanı sıra BG için alınacak teknolojik tedbirler arasında şifreleme teknolojileri, sayısal imza, güvenlik duvarı, yedekleme, anti virüs tedbirleri, yazılım, ağ, internet güvenliği ve kullanıcı hesabı güvenliği yer almaktadır (Özenç, 2007).

2.5.2.1 Şifreleme teknolojileri

Tarih boyunca güvenli bir haberleşmenin sağlanması için değişik yöntem ve teknikler kullanılırken zamanla gelişen iletişim teknolojiyle dijital ortamda bulunan veri güvenliği için çeşitli teknolojiler kullanılmış ve en yaygın olarak günümüzde şifreleme ya da kriptografi tekniği kullanılmaktadır (Keleş ve Güneş, 2013).

Kriptografi, okunur haldeki verinin başkaları tarafından okunmayacak hale getirilmesi ve bu sistemle veri güvenliğine erişilebilirliğinin matematiksel olarak kontrol edilmesidir (Burlu, 2010). Bu sistem ile çeşitli şifreleme yöntemleri kullanılırken veri korunmasının yetersiz kaldığı durumlarda bu sistemin zaman içerisinde çözülmesi yeni teknolojik sistemlerin geliştirilmesini sağlamaktadır (Keleş ve Güneş, 2013). BG'de geçmişte tek anahtarlı şifreleme teknikleri kullanılırken günümüzde çift anahtarlı şifreleme teknolojisi tercih edilmekte şifreleme ve şifrenin çözülmesi için farklı anahtarlar kullanılmaktadır. Burada şifrelemede kullanılan kişiye özel anahtar açık, şifrenin çözülmesi için kişiye özel olan anahtar gizlidir (Öğüt, 2006). Diğer güvenlik durumu steganografi şifreleme teknolojisi bir verinin saklanması nesne içerisine gizlenmesidir (Keleş ve Güneş, 2013). Bu şifreleme teknolojilerinin kullanılması BG'nin sağlanması verilerin ağ üzerinden iletimi için yararlı olmaktadır (Eminağaoğlu ve Gökşen, 2009). Bu kapsamda şifreleme teknolojisini kullanan kurumlar verilerin saklanması aşamasında şifrelenerek gizlenmeli, iletilecek veriler ve oluşturulan şifre anahtarlarının nerede saklanacakları belirlenmelidir. Ayrıca şifreleme uygulamasında kimin yetkisi olduğu bilinmeli, oluşturulan, saklanan ve dağıtılacak olan şifreleme anahtarlarında kim ya da kimler yetkili olduğu belirtilmelidir. Bunlarla birlikte kaybolan şifreleme anahtarlarında kimin inceleme yapacağı kurumda çalışan personeller arasında görev dağılımı görevler ayrılığı prensibine göre olması kişiye bağlı olma durumunun ortadan kaldırması bakımından önemlidir (Yıldız, 2007).

2.5.2.2 Sayısal İmza

El ile atılan imzanın bütün özelliklerinin matematiksel formüllerle dijital ortama aktarılarak, imzalanacak olan yere eklemek için hazırlanırken (Öğüt, 2006), sayısal imzanın kullanılmasının amacı, sahte imzaların önüne geçilerek, veri içeriğinin değiştirilmeden alıcıya aktarılmasıdır (Özler, 2007). Sayısal imzanın veri güvenliğinin sağlanması için özgün, taklit edilemez, tekrarlanamaz, değiştirilmez ve inkâr edilemez vb özelliklere sahip olması gerekmektedir. Burada kullanılan teknik, açık anahtarlı şifreleme teknolojisi olurken bu teknikte açık ve özel anahtarlar mevcuttur. İmzalama işleminde özel anahtar, doğrulama işlemi açık anahtarla yapılırken bu sistemde sabit kalan özel anahtar daima bulunmaktadır (Özçiçek, 2009). Ayrıca BG konusunda sayısal imza, bilgiyi kimin gönderdiğinin teyit edilmesi başkaları tarafından verinin

gönderilme ihtimalini ortadan kaldırması ve veri bütünlüğünü sağlaması, değiştirilme ihtimalini ortadan kaldırması ile önemli avantajları sağlamaktadır (Ermiş, 2006).

2.5.2.3 Güvenlik Duvarı (firewall)

Güvenlik duvarları (firewall) ağ güvenliğinin sağlanmasında en yaygın olarak kullanılan teknolojik önlemlerin başında gelmektedir (Şekil 15). Ateş duvarı binalardan çıkan yangının ve alevlerin diğer odalara yayılmasının engellenmesi için özel duvar (Doğantimur, 2009) olarak bilinirken güvenlik duvarları bilgisayar sisteminin bir parçası olarak bilgisayar ve internet ağına gelen giden veriyi denetleyerek yetkisiz erişimi engellemektedir (Arora, 2012).

Şekil 15: Katmanlı Güvenlik Mimarisi (Ünver, Canbay ve Günaydın, 2010)

Güvenlik duvarlarının sahip olması gereken özellikleri aşağıda verilmiştir (Şahinaslan, 2013).

- ✓ Oluşacak olan tehdit türleri önceden belirlenmeli ve bu tehditlere karşı güncel olarak yeni programlar geliştirilerek koruma özellikleri daima aktif olmalıdır.
- ✓ Kullanıcı ve cihazlar gruplandırılarak güvenlik politikaları doğrultusunda tanımlanan kurallarla daha anlaşılır olmalıdır. Servis ve uygulamaları, ihtiyaç duyacakları network erişim izinleri dikkate alınarak sınıflandırılmalıdır.
- ✓ Port ve IP üzerinden izinler ve yetkilendirmeler düzenlenmeli ve bunlar kimlik doğrulaması ile yapılmalıdır.

- ✓ Kişilerin dijital kurum kimliklerinin merkezi kimlik yönetim sistemi ile doğrulama-yetkilendirme sistemleri üzerinden yapılan uygulama erişimlerinde yetkilendirme ve erişim kontrolü kolaylaşmaktadır.
- ✓ Network üzerinden uzun süre saldırı yaptığı belirlenen ve kuvvetli şüphe oluşturan IP adreslerinin engellenmesi gerekmektedir.

2.5.2.4 Yedekleme

Bilgi sistemindeki bilgilerin geri ulaşılamayacak bir şekilde arıza, hata veya hasar durumunda kaybolmasını engellemek için verilerin kopyasının alınması olup her kurumun yerleşmiş yedekleme politikası bulunması gerekmektedir (Doğantimur, 2009). Bu konuda her kurum, personeline gerekli tebligatı yaparak yedeklemelerin düzenli olarak yapılmasını sağlamalı ve oluşturulan yedeklemelerin çalışıp çalışmadığı da kontrol etmelidir. Yedeklemeler detaylı olarak etiketlenmeli, güvenli bir yerde muhafazası sağlanmalı ve fiziksel erişime kısıtlanmalıdır (Yıldız, 2007).

2.5.2.5 Antivirüs

Virüslerden en etkili bir şekilde korunmayı sağlayan yazılım programları olan antivirüslerin düzenli olarak güncellenmesinin yapılması en önemli tedbirler arasında görülmektedir (Burlu, 2010; Vardal, 2009).

2.5.2.6 Yazılım Güvenliği

Günümüzde kurumlar birçok işlemi internet ortamında yaptıklarından ağ ortamında çalışan yazılımların güvenliğinin sağlanması oldukça önemlidir. Erişim sağlanan uygulama yazılımlardaki güvenlik açıkları, BG'yi tehdit ederken zamanla yazılımlara esneklik ve kullanım kolaylığı sağlanması için birçok eklenti yapılmakta ve yapılan bu eklentiler internet ortamındaki yazılımlar açısından büyük risk taşımaktadır (Vural ve Sağıroğlu, 2007). Yazılımların güvenli olmaması nedeniyle oluşan açık ve zayıf noktalar bazı kişilerce bilinçli ya da istenilmeden kötüye kullanılabilmektedir. Bu tür açıklardan kullanıcılar rahatsız olurken bu yazılımları kullanmak istemediklerinden güvenlik unsurunun mutlaka dikkate alınmalıdır (Beydağlı, Kara, Bahşi ve Alparslan, 2009).

Şekil 16: Yazılım Yaşam Döngüsü (Alparslan, 2016).

2.5.2.7 Ağ Güvenliği

Kablolu veya kablosuz iki veya daha fazla bilgisayarın birbiriyle iletişim halinde çalışması olan ağ, iki ayrı kıtada veya yan yana bulunan iki bilgisayar veya cihaz da olabilmektedir. Paylaşılan bu ağlar üzerinde yetkisiz erişim sağlanıp, sistem ve servisler kullanılamaz hale getirilirken bu durumların yaşanması ile güvenlik ihlalleri de artış göstermiştirr (Gülmüş, 2010). Son zamanlarda kablosuz ağların kullanımı ile ağlardaki güvenlik konusu önemli hale gelirken kablosuz ağ güvenliğini sağlamak için oluşturulan ağlara şifre konulması, MAC adresi filtrelemesi ve ağa ait SSID nin gizli olarak ayarlanması gerekmektedir (Çontar, 2013).

2.5.2.8 İnternet Güvenliği

Dünyanın her yerinde yaygın olarak kullanılan internet ve elektronik işlemler açık elektronik iletişim ağları üzerinden gerçekleşirken, kağıtla yapılan işlemlerin yerini gün geçtikçe ve hızlı şekilde bu elektronik işlemler almaktadır. Bu durumda kişi ve kurumların haberleşmelerini elektronik iletişim ağları üzerinden yapmaları kadar BG ve güvenirliği de o kadar önemli hale gelmektedir. Hukuki açıdan, sanal ortamda veri

değişimi sırasında dışarıdan gelen saldırılar güvenilirlik sorunun ortaya çıkmasına neden olmaktadır (Öğüt, 2006).

İnternette kullanılan ve bilgi alışverişini sağlayan http ve ftp gibi protokoller gönderilen bilgileri şifrelenmeden karşı tarafa ulaştırken BG sağlanamadığından saldırganlar bu protokoller üzerinden gönderilen bilgileri ele geçirebilmektedir. Bu amaçla SSL sertifikası kullanıldığında gönderilen bilgiler karşı tarafa şifrelenerek gönderildiğinden başkaları tarafından görülmesi ve dinlenmesi engellenmektedir. Örneğin güvenlik sertifikaların bulunduğu web sayfalarına girildiğinde http başlığı **https** olarak değişirken **s (security)** harfi güvenli anlamına gelmektedir. Yapılan bir araştırmada kurumların kullanıcılarının şirket dışında, güvenli internet erişimi için %57 oranında SSL, VPN hizmeti verdiği, %36 oranında vermediği, %8 oranında ise diğer cevaplar verirken kurumların yarıdan fazlasını SSL VPN hizmeti verirken %43 oranında hizmet vermedikleri anlaşılmaktadır (TÜBİTAK, 2018;2019).

2.5.2.9 Kullanıcı Hesabı Güvenliği

Hesap ya da sisteme yetki tanımlanırken, işin yapılabileceği en az yetki verilecek şekilde yapılması güvenliği üst seviyeye çıkarırken yetkinin fazla kişiye yayılması güvenlik problemlerine neden olabilmektedir. Bu kapsamda eğer işin yapılması için dosyanın okunması yeterli ise sadece dosyanın okunması yetkisi ya da dosya güncelleme yetkisi verilmeli, başka herhangi bir yetki verilmesi gerekmektedir (Clarke, 2011).

2.5.3 Eğitim ve Farkındalık

Kurumsal BG, yazılım, donanım, insan ve iletişim sistemi gibi bilgi unsurlarının iç ve dış tehditlere karşı korunması olup hem kurum dışı hem de kurum içinden gelecek tehlikelere karşı önlem almak gerekmektedir (Koç, 2008). Kurum içinde tehlikeyi oluşturan en büyük unsur kurumda çalışan personelin kendisi olup bu personeller bilinçli ve bilinçsiz tehlikeler oluşturmaktadır. Bilinçli tehlikelerin zararlarını düşük seviyeye indirmek için kuruma güvenilir personel alınmalı, alınan güvenilir personellerin bilinçsiz yapmış olduğu tehlikeleri düşük seviyeye indirmek için kurum bünyesinde eğitim ve bilinçlendirme çalışmaları ile farkındalıkların arttırılması sonucu BG yönetimi konusunda başarı olunabilmektedir (Eminağaoğlu ve Gökşen, 2009). İnsan kaynaklı güvenlik ihlaller oldukça önemli olup çalışan personellerin BG'nin teknolojik araçlarla sağlanacağını düşünmeleri eğitim ve bilinçlendirmedeki

eksikliklerin bulunduğunu gösterirken kurumlar kendi bünyesinde uygulamalı farkındalık eğitimleri vermeli güvenliğin teknolojik araçlarla sağlanacağı yanılgısına düşmemelidir (Mitnick ve Simon, 2016; Vural ve Sağıroğlu, 2007).

Üniversitelerde teknik gruba dâhil edilmeyen idari, akademik personeller ile öğrencilere yönelik yapılan bilinçlendirme farkındalık programlarında temel hedef, BG'yi tehdit eden risklerle ilgili bilgilere yer verilerek sürekli güncelleme yapılmasıdır. Kurum bünyesinde açılan bilinçlendirme programlarının temel hedefi, kurumda çalışan her çalışanın kuruma ait bütün bilgi kaynaklarının korunmasıdır. (Vardal, 2009; Mitnick ve Simon, 2016).

BG'nin sağlanabilmesi için birçok konuda olduğu gibi istekli, bilgili ve bilinçli bireylerin olması oldukça önemlidir. BG kurumda bir kültür olarak yer almalı ve bunu hedef olarak seçmelidirler. Çünkü kurum dışı gelecek tehditlere her zaman dikkat edilirken daha büyük bir zararı kurum içinde kötü niyetli, bilinçsiz ve dikkatsiz şekilde davranan personeller vermektedir (Eminağaoğlu ve Gökşen, 2009). BG'nin sağlanması aşamasında gerçekleştirilen insan eğitimlerinde, bilginin 5N1K (Ne, nerede, niçin, nasıl, ne zaman ve kim) ile korunması, bilginin korunmadığı durumlarda BG'nin nasıl etkileneceğinin uygulamalı olarak verilmesi ve meydana gelecek sonuçların açıklanması bilinç ve farkındalık oranını artıracaktır (Wenger, Mauer ve Cavelty, 2008).

BG risklerini engellemek için bireylerin iyi bir eğitimden geçmiş olmaları hem bireyler için hem de toplum için önemli olurken gerek eğitim programları gerekse medya kanallarıyla bireylerin farkındalıkları arttırılırken İngiltere, güvenli internet kullanımı ile ilgili öğretim programlarına zorunlu ders eklemeyi planlamıştır (Ulaşanoğlu, Yılmaz ve Tekin, 2010). Dünyada ve ülkemizde BG yapılacak saldırıların önümüzdeki yıllarda daha karmaşık olacağı ve daha büyük kitleleri tehdit edeceğinden BG'ye yönelik yapılan güncel tehditlerle ilgili olarak çalışmalar daha da önemli hale gelecektir (Vural ve Sağıroğlu, 2007).

Nitekim günümüzde BG'ye en fazla önemi bankacılık, finans sektörü, büyük holdingler, yazılım firmaları ve devlet kurumları verirken BG'nin bütün kişi ve kurumlara yayılarak bir kültür haline getirilmesi BG konusunda toplumların bilinçlendirilmesi ile mümkündür. Çünkü bireyler günlük hayatta internet, mobil

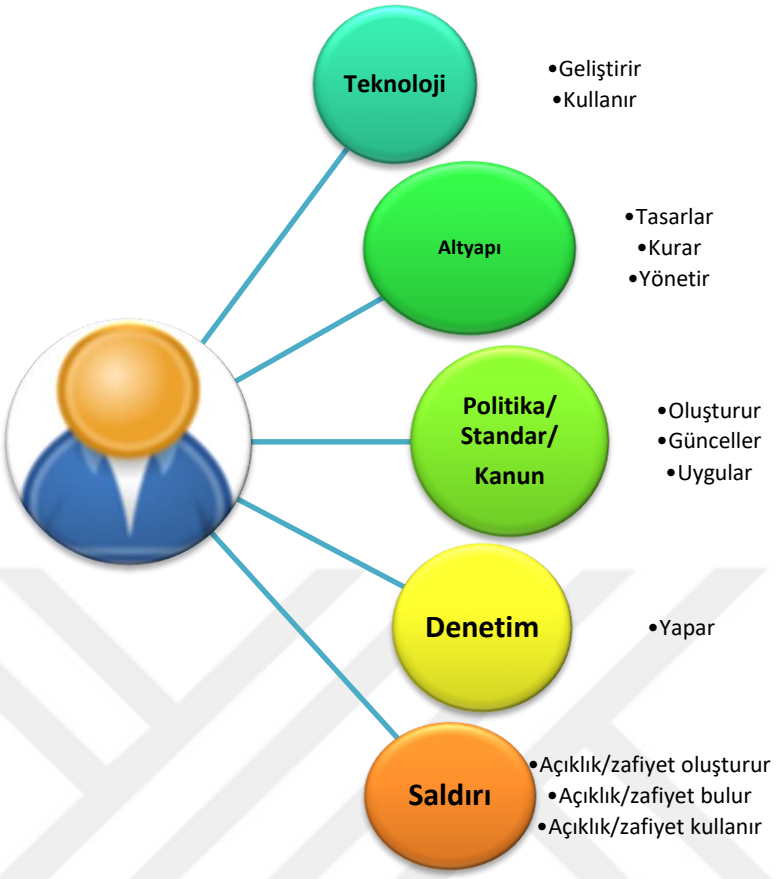
teknolojileri sadece iş ortamlarında değil aynı zamanda kişisel birçok işlemini gerçekleştirirken de kullanmaktadır. Bundan dolayı BG'ye herkes tarafından önem verilmesi gerekmektedir (Swaminatha ve Elden, 2003).

2.5.3.1 Son Kullanıcı Güvenlik Bilinci

Bilgi sisteminde bilgiyi kullanan ya da yönetenlerden biri olarak BG'de sorumluluk öncelikle kullanıcıya bağlı olduğundan kullanıcı farkındalığı son derece önemlidir (Keser ve Güldüren, 2015). Bununla birlikte teknik güvenlik önlemlerinin alınması (güvenlik duvarı, sana özel ağ, anti-virüs, kimlik doğrulama, yetkilendirme vb.) kurumsal ve bireysel BG'de yeterli değildir (Rezgui ve Marks, 2008). Çünkü BG'nin en büyük riski oluşturan insan faktörü üzerinden birçok güvenlik önlemi aşılırken, kurumların bu konuda en ciddi hatalarından biri de insanların karşılaşabileceği riskleri görmezlikten gelmesidir (Şekil 17). Günümüzde teknolojik önlemlerin zamanla artmasıyla güvenlik açıkları en az seviyeye indirilirken saldırganlar insan faktörü üzerinden amaçlarına ulaşmaktadırlar. Gümüş'e (2010) göre, kullanıcıların sosyal mühendislik kavramını bilmedikleri ya da yeterli önemi vermediklerini bu konuyla ilgili hem kurumların hem de çalışanların yeterli düzeyde bilgiye sahip olmadıklarını bildirmiştir. Güvenlik açıklarının diğer nedenleri arasında kendi amaçları doğrusunda personelin kurumsal ağları kullanmasıyla verimliliğin azalması, zararlı yazılımların kullanılması ve kurum itibarını zedeleyecek olan internet sayfalarına girilmesidir (Öztemiz ve Yılmaz, 2013).

BGF ile ilgili kurum bünyesinde yapılan çalışmaların öncelikli hedefi bilgi ve bilgi varlıklarının korunması olduğundan kurumda çalışan herkesin kendi görev ve sorumluluklarını bilmesi ve buna göre davranması gerekmektedir. Ayrıca kurumla iş yapan ortaklarının da BG'nin sağlanmasında sorumlulukları bulunmaktadır. Kurum bünyesinde çalışan personele BGF ile ilgili bilinç aşılanmalı ve bu bilinçle ilgili bilgilerin nasıl korunacağı üzerinde de durulmalıdır (Özcan, 2009).

BFG farkındalığının önemli nedenleri; hatalı kullanılan bilgi varlıklarında farkındalık oluşturarak meydana gelecek riskleri en düşük seviyeye indirmek, karşılaşabileceği sorunları bilip buna göre çözümler bulmak aynı zamanda kuruma ait güvenlik politikasını uygulatıp BG'ye katkıda bulunmasını sağlamaktır (Şahinaslan, Kandemir ve Şahinaslan, 2009).



Şekil 17: Bilgi Güvenliği Unsurları ile İnsan Faktörünün İlişkisi (Erol, 2016)

Özenç (2007)'e göre son kullanıcıların aşağıda ki bazı hususları dikkate alması gerekmektedir. Bunlar;

- ✓ Bilgi sistemlerini kullanan kullanıcılara karşı sorumlu olduklarını bilmeliler,
- ✓ Kullanacakları yazılımların lisanslı olmasına dikkat etmeliler,
- ✓ Kullanacakları anti-virüs yazılımın güncel olmasına dikkat etmeliler
- ✓ Kişisel verilerin internet ortamında nasıl korunması gerektiğini bilmeliler,
- ✓ Şifre korumalı olarak bilgisayar ve e-posta sistemlerini kullanmalı ve ara ara şifreleri değiştirmeliler,
- ✓ Güvenilir olmayan internet sayfalarına girmemeliler,
- ✓ Tanımadıkları şahıslardan gelen e-postaları açmadan silmelidir.

Günümüzde hayatın her alanında yoğun bir şekilde bilgili ve bilgisiz olarak kullanılan bilgi teknolojileri özellikle bilgisiz olarak kullanıldığında birçok tehlikeyi meydana getirmektedir. Örneğin bilgisiz olarak en fazla internette paylaşılan bilgiler, cihaz ve

sistemlerimizi kurarken güvenlik önlemlerinin alınmaması, bazı organizasyonlarca dağıtılan ücretsiz depolama aygıtlarına yüklediğimiz casus yazılımlar ile birçok hata yapılmaktadır (Ercan, 2015). Nitekim Tekerek (2008), e-kavramların hayatımızın bir parçası haline geldiğini, giderek kullanımlarının arttığını ve buna bağlı sistemlerde de hasar oluşturacak kadar tehditlerin arttığını, bu tehditlere karşı hem teknik hem de insan üzerinde farkındalık bilinci oluşturulması gerektiğini belirtmiştir.

2.5.3.2 Son Kullanıcı Bilgi Güvenliği Eğitimleri

Güvenlik politikalarında öncelikle her işin başında yer alan işi yapan ve uygulayan insan olduğundan insan ve davranışlarına oldukça fazla yer verilmektedir. Nitekim Schneier (2000), güvenlik zincirinin en zayıf halkasının insan olduğunu; Poulsen (2000), kurumların güvenlik için çok fazla para harcayarak teknolojik önlemler aldıklarını ancak en önemli unsur olan insanı gözden kaçırdıklarında hata yaptıklarını belirtmişlerdir. Gonzales ve Sawicka'ya (2002) göre, BG'de kurumların hem teknolojik hem de insan unsuruna karşı önlemleri alınması gerekirken ne kadar çok teknolojik önlemler alınırsa alınsın insan faktörünün bu konuda daha çok önemlidir.

BG ile ilgili zafiyetin gelecekte teknik olarak yapılan saldırılarından daha çok bilinçsiz kullanıcıların kandırılması ile olacağı değerlendirilmekte, bilinçlendirme ve farkındalık eğitimleri ile sorunların önlenebileceği düşünülmektedir (Vural, 2007).

BG'ye yönelik kurumda verilen eğitimlerin belirli zaman aralıklarıyla tekrarlanması ve eğitimlerin farklı yöntemler kullanılarak verilmesi gerekmektedir. Kurum bünyesinde bilinçlendirme toplantıları, web tabanlı eğitimler, e-posta bildirimleri, yazı ve duyurular, seminerler, bültenler, poster ve eğitsel oyunlar gibi yöntemler kullanılarak farkındalık eğitimleri verilmelidir (Aslan Öztezcan, 2017).

BG'de insan faktörüne bağlı risklerin tamamen ortadan kaldırılması oldukça güç olurken iyi planlanmış eğitimlerle kabul edilebilir bir seviyeye düşürülebilmesinde çalışanların sorumluluklarını bilerek bilgi ve bilgi kaynaklarının korunması için dikkatli olmaları çok önemlidir (Güldüren, 2015). BG ile ilgili kullanıcıların almış oldukları eğitimler sayesinde kendi üzerlerine düşen görevleri bilinçli ve bilerek uygulamaları korunmada daha etkili olmaktadır (Vural, 2007).

BG'de yapılan hataya göre ortaya çıktığından yapılacak eğitimlerin belirli zaman aralıklarıyla tekrarlanması ve farklı yöntemler kullanılarak uygulamalı olarak

verilmesi bunu yaparken mutlaka alternatif bir planının bulunması gerekmektedir. Nitekim bilinçlendirme toplantıları, web tabanlı eğitimler, e-posta bildirimleri, yazı ve duyurular, seminerler, bültenler, poster ve eğitsel oyunlar vb. yöntemlerle farkındalık eğitimleri verilirken çalışanların sorumluluklarını bilerek bilgi ve bilgi kaynaklarının korunması oldukça önemlidir. BG ile ilgili kullanıcıların almış oldukları eğitimlerle bilinçli ve bilerek uygulamaları sonucunda korunmanın en üst seviyeye çıkması sağlanırken bu durum sadece BG için değil toplumdaki her türlü davranış ve uygulamalar için gereklidir. Örneğin ailede huzur ve başarı isteniyorsa aileyi meydana getiren bireylerin sorumluluklarını bilerek buna göre hareket etmeleri gerekmektedir. Bir okulun veya üniversitenin başarılı olması ve insanın eğitimini yeterli ve çağın gereklerini yerine getirilmesi isteniyorsa okulda ki her bireyin hem kurallara uyması hem de çok çalışması ile mümkün olmaktadır. Benzer şekilde çevrenin temiz ve huzurlu olması isteniyorsa öncelikle birey olarak herkes evinin önünü temizlemeli ve kurallara uymalıdır. Eğer kurallarda bir hata varsa bu parçada değil bütünde giderilmesi ile mümkündür. Böylece kullanıcıların BG'nin oluşturulmasında öncelik BG'ye neden olan sorunların bilinmesi, bunun genele yayılması ve getirilen kurallara herkesin uymasının sağlanması gerekmektedir. Bu şekilde bilgi gizliliğini sağlamak ve kullanıcının belli bir bilince sahip olması sağlanırken kullanıcının bilinçlendirilerek her bilginin önemli olduğunu, bazen önemsiz gibi görünen bilgilerin kurumu savunmasız bırakabileceğini bazen de izinsiz erişime sebep olabileceği bildirilmelidir. Kullanıcılara verilen BGF eğitimleriyle kullanıcılar bilginin kurum için ne derecede önemli olduğunun farkına varacaktır (Özcan, 2009). BG'ye verilecek desteğin ve kalitenin arttırılması için kurumlar BGF eğitimlerin öncellikle gönüllü olan kullanıcılara; akabinde zorunlu olarak herkese vermesi gerekmektedir (Vardal, 2009). Böylece BGF'nin ölçülmesinde şifre koruması ve yönetimi, hassas bilgi yönetimi, sosyal mühendislik, fiziksel koruma, olay tepkisi vb. konularda bilinçlendirme eğitimleri ile BGFD artırılabilir (Veseli, 2011). BG'ye verilecek olan her destek ve kalitenin arttırılmasında eğitim, güven, gönüllülük ve bilinç kavramları oldukça önemli görülürken verilecek olan farkındalık eğitimlerinin öncellikle uygulamalı teoriden uzak olarak verilmesi başarıyı artıracak faktörler başarıyı artıracak faktörler arasında yer almaktadır.

ÜÇÜNCÜ BÖLÜM

III. YÖNTEM

Bu bölümünde, çalışmanın modeli, evreni, örneklemi, veri toplama araç ile elde edilen verilerin analiz aşamaları yer almaktadır.

3.1 Araştırma Modeli

Ondokuz Mayıs Üniversitesi (OMÜ) Eğitim Fakültesi'nin yedi farklı bölümünde öğrenim gören öğretmen adaylarının BGFD'yi etkilediği düşünülen bazı değişkenlerin neler olduğu ve öğretmen adaylarının farkındalık düzeylerinin bu değişkenler açısından farklılık gösterip göstermediğinin belirlenmesi amaçlanan çalışmada tarama modeli kullanılmıştır. Bireylerin bir konu hakkındaki görüşlerine, tutumlarına, davranışlarına yönelik veri toplamak ve bu bireylerin konuya ilişkin genel yapısını ortaya koymak için kullanılan bu model, genel anlamda varolan bir evrenin kendini has özelliklerini anlayabilmek için yapılan çalışmaların tümünü içermektedir (Huck, 2012; Johnson ve Christensen, 2000).

Tarama modelinin amacı, toplumların kurumların, nesnelerin, olayların doğasını ve özelliklerini tanımlarken betimleyici yapıya sahip olup varolan durumun ne olduğunu ortaya konulmasının betimlenmesi olarak ifade edilebilmektedir (Büyüköztürk, Kılıç Çakmak, Akgün, Karadeniz ve Demirel, 2012; Mc Millian ve Schumacher, 2001; Özdemir, 2014).

Bu modelde genelleyici özelliğinden kaynaklı olarak bir örneklemden elde edilen verilerin ışığında örneklemin temsil ettiği evrene yönelik genellemeler de yapılırken veriler farklı özelliklere sahip kesitsel ve boylamsal olarak iki ana alt türde toplanmaktadır. Kesitsel tarama, veri toplama süreci tek seferde gerçekleştirilirken; boylamsal tarama, kesitsel taramanın tersine zaman içinde tekrarlanarak yapılan taramadır (Cohen, Manion ve Morrison, 2007; Fraenkel ve Wallen, 2000). Bu çalışmada var olan durumun ne olduğunun belirlenmesi için en uygun olduğu değerlendirilen tarama modellerinden kesitsel tarama modeli kullanılmıştır.

3.2 Evren ve Örneklem

Evren, araştırma sonuçlarının genellendiği gerçek veya varsayımsal kişi, olay ya da nesnelerin bütünü olup elde edilen verilerin analizi ile ortaya çıkan sonuçların geçerli olacağı, yorumlanacağı gruptur (Balcı, 2015). Genel (hedef) ve ulaşılabilir olarak iki kısma ayrılan evren tanımlanması kolay olmasına karşın ulaşılması genellikle imkânsız grup genel (hedef/ soyut) evren, oluşturuken araştırmacının ulaşabileceği, gerçekçi /somut seçimi olan ulaşılabilir evrendir. Buna göre ulaşılabilen evren araştırmada doğrudan gözlenen veya seçilen bir örnek, kümeye ait yapılan gözlemlerden faydalanarak görüş ortaya konabilen evrendir (Büyüköztürk, Kılıç Çakmak, Akgün, Karadeniz ve Demirel, 2012).

Bu kapsamda araştırmanın genel evreni Türkiye'deki tüm öğretmen adayları oluştururken, ulaşılabilir evrenini OMÜ Eğitim Fakültesindeki öğretmen adayları oluşturmaktadır.

Çalışmanın örneklemini OMÜ Eğitim Fakültesinde 2018-2019 eğitim öğretim yılının bahar döneminde öğrenim gören yedi farklı bölümlerdeki öğretmen adaylarından seçkisiz örnekleme yöntemlerinden basit seçkisiz örnekleme yoluyla belirlenen 1200 öğretmen adayı oluşturmaktadır (Tablo 1,3). Çalışmada basit seçkisiz örnekleme tercih edilmesinin nedeni; diğer örnekleme yöntemlerine göre evreni daha yüksek derecede temsil etme gücüne ve evrenin tüm birimlerinin örnekleme seçilmesi eşit ve bağımsız bir olasılığa sahip olmasıdır (Yıldırım ve Şimşek, 2013).

Tablo 1: Öğretmen Adaylarına Ait Kişisel Bilgilerin (Cinsiyet ve yaş) Frekans ve Yüzde Oranları

Değişken	Grup	f	%
Cinsiyeti	Kadın	886	73,8
	Erkek	314	26,2
	Toplam	1200	100,0
Yaş	18-20	536	44,7
	21-22	465	38,8
	23 ve üzeri	199	16,6
	Toplam	1200	100,0

Çalışmaya katılan öğretmen adaylarının %73,8'i kadın, %26,2'si erkek iken adaylarının yaş ortalaması %44,7'si 18-20, %38,8'i 21-22 yaş aralığında olup 23 ve üzeri olanların oranı %16,6 'dır (Tablo 1).

Tablo 2: Öğretmen Adaylarına Ait Kişisel Bilgilerin (Sınıf, Not Ortalaması, Bölüm, Mezun Olduğu Lise) Frekans ve Yüzde Oranları

Değişken	Grup	f	%
Mezun Olduğu Lise	Anadolu Lisesi	670	55,8
	Anadolu Öğretmen Lisesi	157	13,1
	Düz Lise	183	15,3
	Fen Lisesi	55	4,6
	Meslek Lisesi	135	11,2
	Toplam	1200	100,0
Öğrenim Gördüğü Bölüm	BÖTE	67	5,6
	Eğitim Bilimleri	115	9,6
	Matematik ve Fen Bilimleri	381	31,8
	Özel Eğitim	41	3,4
	Temel Eğitim	262	21,7
	Türkçe ve Sosyal	223	18,6
	Yabancı Diller	111	9,3
	Toplam	1200	100,0
Okuduğu Sınıf	1. Sınıf	339	28,2
	2. Sınıf	307	25,6
	3. Sınıf	303	25,3
	4 ve üzeri	251	20,9
	Toplam	1200	100,0
Akademik Not Ortalaması	2,5 ve altı	217	18,1
	2,6-3,0	450	37,5
	3,1-3,5	461	38,4
	3,6-4,0	72	6,0
	Toplam	1200	100,0

Çalışmaya katılan öğretmen adaylarının %28,2'si 1. sınıf, %25,6'sı 2.sınıf, %25,3'ü 3. sınıf, %20,9'u 4. sınıf ve üzeri sınıfta öğrenim görmektedir. Akademik not ortalaması 2,6-3,0 (%37,5) ve 3,1-3,5 (%38,4) aralığında yoğunluk gösteren öğretmen adaylarının %55,8'i Anadolu Lisesi, en az %4,6 ile Fen Lisesi mezunlarından oluşmaktadır. Araştırmaya katılan öğretmen adaylarının bölümlere dağılımına göre en fazla

Matematik ve Fen Bilimleri eğitimi bölümü (381; %31,8) ve Temel Eğitim (262; %21,7) oluşurken en az katılan Özel Eğitim (41; %3,4) öğretmen adaylarıdır (Tablo 2).

Tablo 3: Öğretmen Adaylarına Ait Kişisel Bilgilerin (Yaşadığı Yer, Anne ve Baba Eğitim Düzeyi, Anne ve Baba Mesleği, Kardeş Sayısı) Frekans ve Yüzde Oranları

Değişken	Grup	f	%
Yaşadığı Yer	Büyükşehir	218	18,2
	Şehir	415	34,6
	İlçe	401	33,4
	Kasaba, Mahalle, Köy	166	13,8
	Toplam	1200	100,0
Anne Eğitim Düzeyi	Üniversite	96	8,0
	Lise	310	25,8
	İlköğretim	696	58,0
	Diğer	98	8,2
	Toplam	1200	100,0
Anne Mesleği	Ev Hanımı	988	82,3
	Diğer	212	17,7
	Toplam	1200	100,0
Baba Eğitim Düzeyi	Üniversite	290	24,2
	Lise	362	30,2
	İlköğretim	497	41,4
	Diğer	51	4,3
	Toplam	1200	100,0
Baba Mesleği	Esnaf	156	13,0
Devlet Çalışanı Memur: Memur, Mühendis, Doktor, Öğretmen, Hukukçu	İşçi	230	19,2
	Devlet Çalışanı Memur	296	24,7
	Serbest, Çiftçi, İşletmeci	306	25,5
	Diğer	212	17,7
	Toplam	1200	100,0
Kardeş Sayısı	1-2	660	55,0
	3 ve üzeri	489	40,8
	Yok	51	4,3
	Toplam	1200	100,0

Öğretmen adaylarının büyük çoğunluğu şehir %34,6 ve ilçede %33,4 yaşarken, anne eğitim düzeyi en fazla %58 ile ilköğretim mezunu, en azı ise %8,2 olarak diğer ve hiç eğitim almamış durumuna sahiptir. Öğretmen adaylarının anne mesleği en fazla %82,3 ev hanımı, %17,7'si diğer meslek (mühendis, doktor, memur, öğretmen ve diğer) gruplarına sahiptir. Anne eğitim düzeyine göre en fazla ilköğretim %58,0 mezunudur. Baba mesleğine göre en fazla %25,5'lik bir oran ile serbest (çiftçi ve işletmeci vb.) iken bunu memur mühendis, doktor, öğretmen, hukukçu %24,7 takip etmektedir. Baba eğitim düzeyinde en fazla ilköğretim mezunu %41,4, en az diğer %4,3 grubundadır. Öğretmen adaylarının kardeş sayısı en fazla %55 1-2 iken kardeşi olmayanların oranı %4,3'dür (Tablo 3).

3.3 Verilerin Toplanması

Çalışmanın verileri, üç bölümden oluşan anket ile toplanmıştır. Anketin birinci bölümde öğretmen adaylarının kişisel bilgilerini içeren 12 soru, ikinci bölümünde Çetinkaya, Güldüren ve Keser (2017) tarafından geliştirilen ve Cronbach Alfa güvenirlik katsayısı 0,980 olan 5 seçenekli likert tipi BGFÖ, üçüncü bölümde bilgisayar ve internet kullanımına yönelik kapalı uçlu 13 ve açık uçlu bir soru bulunmaktadır.

Anketin Birinci Bölümü: Bu bölümdeki kişisel bilgiler kullanılarak çalışmanın bağımsız değişkenlerine ait verileri toplanırken öğretmen adaylarının cinsiyet, yaş, sınıf, akademik not ortalaması, mezun olduklar lise, türü, yaşadığı yer, anne eğitim düzeyi, anne, mesleği, baba eğitim düzeyi, baba mesleği, kardeş sayısı ve öğrenim gördüğü bölüm değişkenleri içermektedir (EK 1).

Anketin İkinci Bölümü: Bu bölümde beşli likert tipi, 2 temel boyut (Bilgi ve Güvenlik) ve 3 alt faktörden (Genel güvenlik, Saldırı ve tehditler, Mobil Cihazlar, Mahremiyet ve İletişim) oluşan BGFÖ 'nin toplam varyansı %61,74, Cronbach Alfa güvenirlik katsayısı 0,980, alt faktörler değerleri 0,967, 0,969 ve 0,926 olup ölçeğin güvenilir olduğu değerlendirilmiştir (Çetinkaya, Güldüren ve Keser, 2017). Bu ölçek Yayla (2018) tarafından öğretmenlere uygulanmış ve Cronbach Alfa güvenirlik katsayısı 0,984 bulunmuştur. Bu özelliklere sahip BGFÖ'nin bu çalışmada kullanılabilmesi için gerekli izinler alınmıştır (EK 2).

BGFÖ'nin öğretmenlere yönelik yapılmasına karşılık öğretmen adaylarına uygun olup olmadığını belirlemek amacıyla BGFÖ 123 öğretmen adayına uygulanmış ve Cronbach Alfa güvenirlik katsayısının 0, 968 olarak bulunmuştur. Bu durumda Cronbach Alfa güvenirlik katsayısı $0.00 \leq \alpha < 0.40$ güvenilir değil, $0.40 \leq \alpha < 0.60$ düşük derecede güvenilir, $0.60 \leq \alpha < 0.90$ oldukça güvenilir ve $0.90 \leq \alpha < 1.00$ yüksek derecede güvenilir olarak değerlendirilmektedir (Özdamar, 1999; Tavşancıl, 2006). Böylece BGFÖ'nin öğretmen adayları için yapılan çalışma içinde güvenilir bir veri toplama aracı olduğu belirlenmiştir.

Anketin Üçüncü Bölümü: Bilgisayar ve internet kullanımına yönelik kapalı uçlu 13 açık uçlu bir soru soru içerenmektedir. Bu bölümde öğretmen adaylarının evde bilgisayara sahip olma durumu, bilgisayarı kendisinden başka kullanmayı bilen olma durumu, evde internet bağlantısı olma durumu, araştırma yapılan yer, internette karşılaştıkları zorluklar, internet sitelerine ulaşma yolları, internete bağlanma yeri, interneti yıl bazında kullanma süresi, bilgiye ulaşmak için kullanılan araç ve kişi tercihi, interneti hafta bazında kullandığı saat ve e-posta kontrol süresine ait sorular bulunmaktadır.

Anketin Uygulanması Süreci: Ölçme aracının kullanımı için öncelikle OMÜ etik kurulundan gerekli izinler alındıktan (EK-3a,b) sonra 2018-2019 eğitim öğretim yılında örnekleme uygulanmıştır. Veriler toplanmadan önce öğretmen adaylarına çalışmanın amacı, önemi ve yapılacak işlemlerle ilgili açıklamalar verilmiştir. Gerekli açıklamalardan sonra çalışmaya dâhil olmak istediğini belirten gönüllü öğretmen adaylarına yaklaşık 20-30 dakikalık bir çalışma sonunda veri veri seti elde edilmiştir. Veriler toplandıktan sonra eksik veya rastgele doldurulduğu tespit edilen 133 anket geçersiz sayılarak değerlendirmeye alınmamıştır. Böylece 1200 anketten çalışmanın verilerinin toplanması için değerlendirmeye alınmıştır.

3.4. Verilerin Çözümlenmesi ve Yorumlanması

Çalışma da verilerin analizi SPSS 17,0 istatistik paket programı ile yapılmıştır. Analizi yapılan verilere ait betimleyici istatistiklerin (yüzde, frekans gibi) yanında ikiden fazla gruplar için nonparametrik Kruskal Wallis ve ikili gruplar arasındaki farklılıkları belirlemek için Mann Whitrey U- testi uygulanmış, $p<.05$ olarak alınmıştır. Çünkü Kruskal Wallis testinde doğrudan ikiden fazla gruplar arasındaki farkılılkları ortaya koymak için yapılacak herhangi bir test olmadığı için Mann Whitrey U- testi yapılmış

ve ilgili tablolarda anlamlı fark olarak gösterilmiştir. Anket çalışması örnekleme uygulanmadan önce 123 katılımcının yer aldığı pilot uygulama yapılarak dağılımının normal olup olmadığı ve homojenlik ön şartları sağlayıp sağlamadığı kontrol edilmiş ve tablolar halinde verilmiştir (Tablo 4, 5).

Tablo 4: Bilgi Güvenliği Ölçeği Betimsel İstatistikleri

Değerler	Oran / Sayı	Değerler	Oran / Sayı
Katılımcı Sayısı	123	Çarpıklık (Skewness)	,299
,218	2,94	Çarpıklık Standart Hata	
Ortanca Değer	2,90	Basıklık (Kurtosis)	-,210
Standart Sapma	0,65	Basıklık Standart Hata	,433

Tablo 5: Bilgi Güvenliği Farkındalık Ölçeğinin Normallik Testi Sonuçları

Bilgi Güvenliği Farkındalığı	Kolmogorov-Smirnov			Shapiro-Wilk		
	İstatistik	sd	p	İstatistik	sd	p
	,062	123	,200*	,987	123	,292

Tablo 5'e göre veri toplama aracından elde edilen veriler test edildiğinde normal dağılım gösterirken örneklem sayısı 30'dan fazla olması nedeniyle Kolmogorov-Smirnov testi gerekmektedir. Bu test sonuçlarını Tablo 4'deki çarpıklık ve basıklık değerleri de desteklemektedir. Çünkü çarpıklık katsayısını çarpıklığın standart hatasına, basıklığın basıklık katsayısını basıklık standart hatasına bölündüğünde ±1,96 ile ±1,96 arasındaki değerler normal dağılım olarak nitelendirilerek kabul edilmiştir (Can, 2014). Pilot çalışmaya benzer çalışma örneklem için yapılmış ancak dağılımın normal olmadığı belirlenmiştir (Tablo 4, 5).

BG Eğitimi ve BGF İlgili Çalışmalar: BG ile ilgili araştırmaların yapılması, hem kullanıcıların BG farkındalık düzeylerinin belirlenmesi ve hem de sunulacak BG eğitimleri için oldukça önemlidir. BG sağlamaya yönelik araştırmaların çoğunun güvenlik yazılımları ve modelleri oluşturma boyutlarındadır (Seferoğlu, Yıldız-Durak, Karaoğlan-Yılmaz ve Yılmaz, 2018; Besnard ve Arief, 2004; Mahabi, 2010; Vardal, 2009).

İnsan faktöründen kaynaklanan BG hatalarını belirlemeye ve bunları ortadan kaldırmaya yönelik araştırmalar son dönemlerde artarken (Karaoğlan Yılmaz, Yılmaz

ve Sezer, 2014; Yılmaz, Karaoğlan Yılmaz, Öztürk ve Karademir, 2017). Stanton, Stam, Mastrangelo ve Jolton (2005), parola belirleme ile ilgili davranışlar üzerine bir çalışma yapmışlar ve parola belirleme davranışlarının bir örüntü taşıdığını belirtmişlerdir.

Mylonas, Kastania ve Gritzalis (2013), mobil cihazlardan uygulama indiren kullanıcıların genellikle ortamla ve indirecekleri uygulamayla ilgili güvenlik kaygısı gütmediklerini, kullanıcıların uygulamanın yer aldığı ortama güven düzeylerine ilişkin kestirimlerde bulunulabilecek bir model geliştirmişlerdir.

Magklaras, Furnell ve Brooke (2006), bilgi teknolojileri altyapısına kurum içinden yapılan saldırılarla ilgili unsurlar tanımlanmaya çalışılmışlar ve kötü amaçlı kullanımların analiz edilmesi ve tehditlerin önlenmesinde başvurulabilecek bir taksonomi geliştirmişlerdir.

Herath ve Rao (2009), normatif inançlar ve BG politikalarına uyum niyetleri vb. potansiyel BG davranışlarına etki eden değişkenleri incelemiştir. Ünver, Canbay ve Mirzaoğlu (2009), BG zafiyetlerini ve Türkiye'de internet üzerinden işlem yapmak için kullanılan T.C Kimlik numarası ile kullanıcıların tüm kişisel bilgilerine erişilebildiğini, bu durumun da önemli güvenlik sorunlarını beraberinde getirdiğini bildirmişlerdir. Karjalainen (2011), BG davranışları teknoloji kabul modellerinin sunduğu değişkenleri ile BG davranışlarının önemli sınırlılıklar taşıdığı belirtilmiştir.

Vroom ve Von Solms (2004), BGF'da kurumsal düzeyde bilgilendirmenin, politikaların, kişilik özelliklerinin, dahil olunan örgüt kültürü vb. birçok faktörün önemli olduğu açıklamışlardır. Yapılan bir çalışmada saldırıların en fazla; indirilen programlar, zararlı yazılımlar, oltalama, sahte içerikli e-postalar, bilgi sızdırma ve fiziksel zarar şeklinde olduğunu belirtilmiştir (Marinos, 2013).

Karaoğlan Yılmaz, Yılmaz ve Sezer (2014), üniversite öğrencilerin güvenli BİT kullanım davranışları sergilediğini bununla birlikte bu davranış düzeyinin gelişen ve değişen teknolojik koşulların oluşturduğu yeni durumlara karşı yetersiz olduğunu bildirmiştir. Yapılan çalışma sonuçları öğrencilerin, bilgisayara erişim güvenliği, zararlı programlar ve korunma yolları, sosyal mühendislik, parola güvenliği, dosya erişim ve paylaşım güvenliği, internet ve ağ güvenliği, e-posta güvenliği, yedekleme yapma vb. konularda temel düzeyde ve en popüler olarak bilinen güvenlik

önlemlerinden yalnızca bir ya da birkaçını aldığını, diğer güvenlik önlemlerini ise almadıklarını göstermektedir.

Keser ve Güldüren (2015), yükseköğretim kurumlarında (YÖK) çalışan öğretim elamanlarının BGFD'ni belirlemeye yönelik bir ölçek geliştirmiştir. Saldırı ve tehditler ile kişisel verilerin korunması olmak üzere iki alt boyuttan oluşan ölçeğin geçerli ve güvenir olduğunu belirtmişlerdir.

Güldüren, Çetinkaya ve Keser (2016), ortaöğretim kurumlarında öğrenim gören öğrencilerin BGF düzeylerini belirlemeye yönelik geliştirdikleri ölçeğinin alt boyutlarını "saldırı ve tehditler", "mahremiyet" ve "kişisel verilerin korunması" olarak belirlenmişlerdiir. Geçerlilik ve güvenirliğin sağlandığı bu ölçekle elde edilen verilere göre öğrencilerin BGF'ları ile cinsiyetleri arasında anlamlı bir farklılığın olduğu bulunmuştur. Bu bağlamda erkek öğrencilerin bilgi güvenliği farkındalıkları kadınlarınkine göre daha yüksek çıkmıştır

DÖRDÜNCÜ BÖLÜM

IV. BULGULAR

Bu bölümde öğretmen adaylarının; **demografik karakteristikleri**; cinsiyet, yaş, sınıf, akademik not ortalaması, öğrenim gördükleri bölüm, mezun olduğu lise, anne, baba eğitim düzeyleri ve meslekleri, kardeş sayısı, internet ve bilgisayar kullanım süreleri açıklanırken; **coğrafi karakteristiklerden** yaşadığı yer ile **psikolojik karakteristiklerden** (davranış ve düşünceler, ilgi alanları, güdüler, hayat tarzları vb.) internet, bilgisayar kullanım durumları ve BGFD açıklanmaktadır.

4.1 Birinci Alt Probleme İlişkin Bulgular

4.1.1 Öğretmen Adaylarının Cinsiyete Göre Bilgi Güvenliği Farkındalık Durumları

OMÜ öğretmen adaylarının BGF'nin cinsiyete göre farklılıklarının anlamlı olup olmadığını belirlemek için nonparametrik ilişkisiz örneklemler için Mann-Whitney U testi yapılmış ve analiz sonuçları Tablo 6'da verilmiştir.

Tablo 6: Öğretmen Adaylarının Cinsiyetleri ile Bilgi Güvenliği Farkındalıklarına İlişkin Mann-Whitney U Testi Sonuçları

	Grup	N	Sıra Ortalaması	Sıra Toplamı	U	p
Bilgi Güvenliği Farkındalığı	Kadın	886	547,45	485039,50	92098,5	,000
	Erkek	314	750,19	235560,50		

*p<.01

Mann-Whitney U testinin analizi sonuçlarına göre öğretmen adaylarının cinsiyetleri ile BGFD arasında farklılığın anlamlı olduğu belirlenmiştir [U = 92098,5, p<.01]. Sıra ortlamalarına göre erkek öğretmen adaylarının BGF'nın kadın öğretmen adaylarından daha yüksek olduğu bulunmuştur (Tablo 6).

4.1.2 Öğretmen Adaylarının Yaşına Göre Bilgi Güvenliği Farkındalık Durumları

Öğretmen adaylarının BGF'nin yaşlarına göre anlamlı farklılık farklılık gösterip göstermediği belirlemek için ikiden fazla gruplar için nonparametrik Kruskal Wallis testi uygulanmış ve analizi sonuçları Tablo 7'de verilmiştir.

Tablo 7: Öğretmen Adaylarının Yaşları ile Bilgi Güvenliği Farkındalıklarına İlişkin Kruskal Wallis Sonuçları

	Yaş	N	Sıra Ortalaması	sd	χ^2	p
Bilgi Güvenliği	18-20	536	592,70			
Farkındalığı	21-22	465	568,29	2	19,647	,000
	23 ve üzeri	199	696,77			

*p<.01

Analiz sonucunda öğretmen adaylarının yaşlarına göre BGF' nin anlamlı farka sahip olduğu [$\chi^2_{(2)}$=19,647, p<.01] bulunmuştur. Farklılığın hangi yaş grupları arasında olduğunu tespit etmek için Mann-Whitney U testi kullanılmıştır (Tablo 8).

Tablo 8: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıklarının Yaş Değişkenine Göre Mann-Whitney U Testi Sonuçları

Grup Karşılaştırması	N	Sıra Ortalaması	Sıra Toplaması	U	p
18-20 yaş	536	350,23	187722,50	43806,500	,000
23 ve üzeri	199	415,87*	82757,50		
21-22 yaş	465	311,78	144980,00	36635,000	,000
23 ve üzeri yaş	199	380,90*	75800,00		

Tablo 8'e göre öğretmen adaylarının BGF' daki anlamlı farkın yaş değişkenlerine göre 18-20 yaş ile 23 ve üzeri ve 21-22 yaş ile 23 ve üzeri yaş grupları arasında olduğu tespit edilmiştir.

4.1.3 Öğretmen Adaylarının Öğrenim Gördükleri Sınıf Düzeylerine Göre Bilgi Güvenliği Farkındalık Durumları

BGF'nin öğretmen adaylarının öğrenim gördükleri sınıf düzeylerine göre anlamlı olup olmadığını belirlemek için yapılan Kruskal Wallis analizi yapılmıştır. Kruskal Wallis sonucunda elde edilen sonuçlar testi analiz sonuçları Tablo 9'da verilmiştir. Analiz sonuçlarına göre öğretmen adaylarının öğrenim gördükleri sınıf düzeylerine göre BGF'nin anlamlı olduğu [$\chi^2_{(3)}$=11,521, p<.05] belirlenmiştir (Tablo 9).

Tablo 9: Öğretmen Adaylarının Okudukları Sınıflar ile Bilgi Güvenliği Farkındalıklarına İlişkin Kruskal Wallis Sonuçları

	Sınıf	N	Sıra Ortalaması	sd	χ^2	p
Bilgi Güvenliği Farkındalığı	1. Sınıf	339	647,41	3	11,521	,009
	2. Sınıf	307	592,85			
	3. Sınıf	303	555,28			
	4. ve üzeri	251	601,09			

*p<.05

Tüm gruplar için olası ikililerinin kıyaslamasının yapılarak anlamlı farkın hangi gruplar arasında olduğunu belirlemek için Mann-Whitney U testi uygulanmıştır (Tablo 10).

Tablo 10: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıklarının Sınıf Değişkenine Göre Mann-Whitney U Testi Sonuçları

Sınıf Karşılaştırması	N	Sıra Ortalaması	Sıra Toplaması	U	p
1.Sınıf	339	338,43*	114727,50	46975,500	,033
2.Sınıf	307	307,01	94253,50		
1.Sınıf	339	344,01*	116619,50	43727,500	,001
3.Sınıf	303	296,32	89783,50		

Yapılan Mann-Whitney U testi sonuçlarına göre öğretmen adaylarının BGF ‘deki farkın 1. Sınıf ile 2. Sınıf ve 1. Sınıf ile 3. Sınıf arasında olduğu bulunmuştur (Tablo 10).

4.1.4 Öğretmen Adaylarının Akademik Not Ortalamasına Göre Bilgi Güvenliği Farkındalık Durumları

Akademik not ortalamasına göre öğretmen adaylarının BGF’nin anlamlı bir farklılık gösterip göstermediğini belirlemek için yapılan Kruskal Wallis analiz sonuçlarına göre öğretmen adaylarının BGF arasında farkın anlamlı olduğu [$\chi^2_{(3)}$=12,333, p<.05] bulunmuştur (Tablo 11).

Tablo 11: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıkları ile Akademik Not Ortalamasına İlişkin Kruskal Wallis Sonuçları

	Akademik Not Ortalaması	N	Sıra Ortalaması	sd	χ^2	p
Bilgi Güvenliği Farkındalığı	2,5 ve altı	217	619,39	3	12,333	,006
	2,6 – 3,0	450	637,13			
	3,1- 3,5	461	563,06			
	3,5 – 4,0	72	554,34			

*p<.05

Öğretmen adaylarının BGF'daki farkın hangi gruplar arasında olduğunu belirlemek için Mann-Whitney U testi yapılmıştır (Tablo 12).

Tablo 12: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıklarının Akademik Not Ortalamasına Göre Mann-Whitney U Testi Sonuçları

Grup Karşılaştırması	N	Sıra Ortalaması	Sıra Toplaması	U	p
2,6 - 3,0	450	484,53*	218036,50	90888,500	,001
3,1 - 3,5	461	428,16	197379,50		

Mann-Whitney U testine göre BGF ile akademik not ortalamaları arasındaki farkın 2,6-3,0 ile 3,1-3,5 akademik not ortalamasına sahip gruplar arasında olduğu belirlenmiştir (Tablo 12).

4.1.5 Öğretmen Adaylarının Mezun Olduğu Lise Türüne Göre Bilgi Güvenliği Farkındalık Durumları

Öğretmen adaylarının BGF'nın mezun olduğu lise türüne göre farklılık olup olmadığını belirlemek için yapılan Kruskal Wallis analizine göre BGF'nın anlamlı olduğu [$\chi^2_{(4)}$=12,087, p<.05] bulunmuştur (Tablo 13).

Tablo 13: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıkları ile Mezun Olduğu Lise Türüne İlişkin Kruskal Wallis Sonuçları **(L: Lise)**

	Lise (L.) Türü	N	Sıra Ortalaması	sd	χ^2	p
Bilgi Güvenliği Farkındalığı	Anadolu L.	670	590,82	4	12,087	,017
	Anadolu Öğretmen L.	157	555,10			
	Düz L.	183	599,42			
	Fen L.	55	645,20			
	Meslek L.	135	684,60			

*p<.05

Öğretmen adaylarının mezun olduğu lise türüne göre anlamlı farkın hangi değişkenler arasında olduğunun belirlemek için yapılan Mann-Whitney U testi uygulanmıştır(Tablo 14).

Tablo 14: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıklarının Akademik Not Ortalamasına Göre Mann-Whitney U Testi Sonuçları **(L: Lise)**

Lise Karşılaştırması	N	Sıra Ortalaması	Sıra Toplaması	U	p
Anadolu L.	670	392,44	262936,50	38151,500	,004
Meslek L.	135	455,40*	61478,50		
Anadolu Öğretmen L.	157	131,55	20654,00	8251,000	,001
Meslek L.	135	163,88*	22124,00		
Düz L.	183	150,27	27498,50	10662,500	,037
Meslek L.	135	172,02*	23222,50		

Öğretmen adaylarının mezun olduğu lise türüne göre anlamlı farkın hangi değişkenler arasında olduğunun belirlemek için yapılan Mann-Whitney U testi sonuçlarına göre BGF ‘deki farkın Anadolu ile Meslek, Anadolu Öğretmen ile Meslek ve Düz ile Meslek Liseleri arasında olduğu görülmüştür (Tablo 14).

4.1.6 Öğretmen Adaylarının Yaşadığı Yere Göre Bilgi Güvenliği Farkındalık Durumları

Öğretmen adaylarının BGF'nın yaşadıkları yere göre değişip değişmediğini belirlemek için uygulanan Kruskal Wallis testi analiz sonuçlarına (Tablo 15) göre öğretmen adaylarının BGF'nın yaşadıkları yere göre farkın anlamlı olmadığı bulunmuştur [$\chi^2_{(3)}$=6,321, p>.05].

Tablo 15: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıkları ile Yaşadığı Yere İlişkin Kruskal Wallis Sonuçları

	Yaşadığı Yer	N	Sıra Ortalaması	sd	χ^2	p
Bilgi Güvenliği Farkındalığı	Büyükşehir	218	614,45	3	6,321	,097
	Şehir	415	618,12			
	İlçe	401	599,31			
	Kasaba ve Köy	166	541,02			

*p>.05

4.1.7 Öğretmen Adaylarının Anne Eğitim Düzeyine Göre Bilgi Güvenliği Farkındalık Durumları

Anne eğitim düzeylerinin öğretmen adaylarının BGF üzerinde anlamlı etkisinin olup olmadığını belirlemek için Kruskal Wallis testi uygulanmıştır. Elde edilen analiz sonuçlarına göre farkın anlamlı olduğu [$\chi^2_{(3)}$=30,592, p<.01] bulunmuştur (Tablo 16).

Tablo 16: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıkları ile Anne Eğitim Düzeyine İlişkin Kruskal Wallis Sonuçları

	Anne Eğitim Düzeyi	N	Sıra Ortalaması	sd	χ^2	p
Bilgi Güvenliği Farkındalığı	Üniversite	96	624,80	3	30,592	,000
	Lise	310	689,57			
	İlköğretim	696	565,02			
	Diğer ve yok	98	546,91			

*p<.01

Öğretmen adaylarının BGF ‘nin anne eğitim düzeyine göre anlamlı farkın hangi eğitim düzeyleri arasında olduğunun belirlemek için Mann-Whitney U testi ile kıyaslaması yapılmıştır (Tablo 17).

Tablo 17: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıklarının Anne Eğitim Düzeyine Göre Mann-Whitney U Testi Sonuçları

Grup	N	Sıra Ortalaması	Sıra Toplaması	U	p
Lise	310	575,68*	178459,50	85505,500	,000
İlköğretim	696	471,35	328061,50		
Lise	310	215,69*	66863,00	11722,000	,001
Diğer	98	169,11	16573,00		

Mann-Whitney U testi sonuçlarına göre Lise ile İlköğretim ve Lise ile Diğer grupları arasında fark olduğu görülmektedir (Tablo 17).

4.1.8 Öğretmen Adaylarının Anne Mesleğine Göre Bilgi Güvenliği Farkındalık Durumları

Öğretmen adaylarının BGF'nin anne mesleğine göre anlamlı farklılaşıp farklılaşmadığını belirlemek için uygulanan Mann-Whitney U Testi sonuçarına (Tablo 18) göre farkın anlamlı olmadığı sonucuna ulaşılmış [U = 98034,000, p>.05] ve öğretmen adaylarının anne mesleğinin BGF 'ye etkili olmadığı anlaşılmıştır.

Tablo 18: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıklarının Anne Mesleğine Göre Mann-Whitney U Test Sonuçları

	Meslek Grubu	N	Sıra Ortalaması	Sıra Toplamı	U	p
Bilgi Güvenliği Farkındalığı	Ev Hanımı	988	593,72	586600,00	98034,000	,144
	Diğer	212	632,08	134000,00		

*p>.05

4.1.9 Öğretmen Adaylarının Baba Eğitim Düzeyine Göre Bilgi Güvenliği Farkındalık Durumları

Öğretmen adaylarının baba eğitim düzeylerinin BGF'nin üzerinde anlamlı olarak farklılaşıp farklılaşmadığını belirlemek için Kruskal Wallis testi uygulanmış ve analiz sonuçlarına göre farkın anlamlı olduğu [$\chi^2_{(3)}$=19,893, p<.01] bulunmuştur (Tablo 19).

Tablo 19: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıkları ile Baba Eğitim Düzeyine İlişkin Kruskal Wallis Sonuçları

	Baba Eğitim Düzeyi	N	Sıra Ortalama	sd	χ^2	p
Bilgi Güvenliği Farkındalığı	Üniversite	290	644,80	3	19,893	,000
	Lise	362	638,42			
	İlköğretim	497	550,61			
	Diğer	51	565,59			

*p<.01

Anlamlı fark çıkan tüm baba eğitim düzeylerinin olası ikililerinin Mann-Whitney U testi ile karşılaştırılması yapılmıştır (Tablo 20).

Tablo 20: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıklarının Baba Eğitim Düzeyine Göre Mann-Whitney U Testi Sonuçları

Grup Karşılaştırması	N	Sıra Ortalaması	Sıra Toplaması	U	p
Üniversite	290	432,36*	125384,00	60941,000	,000
İlköğretim	497	371,62	184694,00		
Lise	362	467,24*	169142,00	76475,000	,000
İlköğretim	497	402,87	200228,00		

Mann-Whitney U test sonuçlarına göre öğretmen adaylarının baba eğitim durumlarının BGFD üzerinde anlamlı bir etkiye sahip olduğu farkın Üniversite ile İlköğretim gruplar ve Lise ile İlköğretim mezunu gruplar arasında olduğu bulunmuştur (Tablo 20).

4.1.10 Öğretmen Adaylarının Baba Mesleğine Göre Bilgi Güvenliği Farkındalık Durumları

Öğretmen adaylarının baba mesleğine göre BGF 'nin anlamlı bir etkiye sahip olup olmadığını belirlemek için Kruskal Wallis testi uygulanmıştır. Kruskal Wallis analizinde elde edilen analiz sonuçlarına göre farkın anlamlı olduğu [$\chi^2_{(4)}$=11,022, p<.05] bulunmuştur (Tablo 21).

Tablo 21: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıkları ile Baba Mesleğine İlişkin Kruskal Wallis Sonuçları **(Devlet Çalışanı Memur: Memur, Mühendis, Doktor, Öğretmen, Hukukçu)**

	Baba Mesleği	N	Sıra Ortalama	sd	χ^2	p
Bilgi Güvenliği Farkındalığı	Esnaf	156	527,92	4	11,022	,026
	İşçi	230	604,78			
	Devlet Çalışanı Memur	296	636,82			
	Serbest, Çiftçi, İşletmeci	306	587,75			
	Diğer	212	616,95			

*p<.05

Anlamlı farkın hangi gruplar arasında olduğu Kruskal Wallis testi çoklu karşılaştırma içermediğinden tüm grupların olası ikililerinin Mann-Whitney U testi ile kıyaslaması yapılmıştır (Tablo 22).

Tablo 22: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıklarının Baba Mesleğine Göre Mann-Whitney U Testi Sonuçları (**DÇM**= Memur, Mühendis, Doktor, Öğretmen, Hukukçu)

Grup	N	Sıra Ortalaması	Sıra Toplaması	U	p
Esnaf	156	178,25	28707,00	15561,000	,027
İşçi	230	203,84*	46884,00		
Esnaf	156	200,11	31216,50	18970,500	,002
DÇM	296	240,41*	71161,50		
Esnaf	156	168,78	26329,00	14083,000	,015
Diğer	212	196,07*	41567,00		

Mann-Whitney U testi sonuçlarına BGFD farklılıkların Esnaf ile İşçi, Esnaf ile Devlet çalışanı (Memur, Mühendis, Doktor, Öğretmen, Hukuk) ve Esnaf ile Diğer meslek grupları arasında olduğu bulunmuştur.

4.1.11 Öğretmen Adaylarının Kardeş Sayısına Göre Bilgi Güvenliği Farkındalık Durumları

Kruskal Wallis testi sonuçlarına göre öğretmen adaylarının BGF'nin kardeş sayısına göre farkın anlamlı olmadığı bulunmuş [$\chi^2_{(2)}$=4,479, p>.05] ve kardeş sayısı öğretmen

adaylarının BGF konusunda anlamlı bir etkiye sahip olmadığı belirlenmiştir (Tablo 23).

Tablo 23: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıkları ile Sahip Oldukları Kardeş Sayısına İlişkin Kruskal Wallis Sonuçları

	Kardeş Sayısı	N	Sıra Ortalama	sd	χ^2	p
Bilgi Güvenliği	Yok	51	602,65			
Farkındalığı	1-2	660	619,03	2	4,479	,106
	3 ve üzeri	489	575,27			

*p>.05

4.1.12 Öğretmen Adaylarının Öğrenim Gördükleri Bölümlere Göre Bilgi Güvenliği Farkındalık Durumları

Öğretmen adaylarının BGF'nin öğrenim gördüğü bölümlere göre anlamlı bir farklılık olup olmadığı belirlemek için Kruskal Wallis testi yapılmıştır (Tablo 24). Bunun sonucunda öğretmen adaylarının BGF anlamlı bir farklılık bulunmaktadır [$\chi^2_{(6)}$=91,719, p<.01].

Tablo 24: Öğretmen Adaylarının Öğrenim Gördüğü Bölüm ile Bilgi Güvenliği Farkındalıklarına İlişkin Kruskal Wallis Sonuçları **(Bil: Bilimleri)**

	Bölüm	N	Sıra Ortalama	sd	χ^2	p
Bilgi Güvenliği Farkındalığı	BÖTE	67	936,49	6	91,719	,000
	Eğitim Bil.	115	578,90			
	Matematik ve Fen Bil.	381	534,73			
	Özel Eğitim	41	551,22			
	Temel Eğitim	262	554,71			
	Türkçe ve Sosyal	223	652,86			
	Yabancı Diller	111	666,89			

*p<.01

Öğretmen adaylarının öğrenim gördüğü bölümlere göre BGF'de anlamlı farklılığın hangi bölümler arasında olduğunun belirlenmesi için Mann-Whitney U testi uygulanmıştır (Tablo 25).

Tablo 25: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıklarının Öğrenim Gördüğü Bölümlere Göre Mann-Whitney U Testi Sonuçları **(Bil: Bilimleri)**

Bölüm Karşılaştırması	N	Sıra Ortalaması	Sıra Toplaması	U	p
BÖTE	67	346,95*	23245,50	4559,500	,000
Mat. ve Fen Bil.	381	202,97	77330,50		
BÖTE	67	67,57*	4527,50	497,500	,000
Özel Eğitim	41	33,13	1358,50		
BÖTE	67	247,96*	16613,50	3218,500	,000
Temel Eğitim	262	143,78	37671,50		
BÖTE	67	201,86*	13524,50	3694,500	,000
Türkçe ve Sosyal	223	128,57	28670,50		
BÖTE	67	114,67*	7683,00	2032,000	,000
Yabancı Diller	111	74,31	8248,00		
BÖTE	67	127,47*	8540,50	1442,500	,000
Eğitim Bil.	115	70,54	8112,50		
Mat. ve Fen Bil	381	280,57	106899,00	34128,000	,000
Türkçe ve Sosyal	223	339,96*	75811,00		
Mat. ve Fen Bil.	381	234,51	89347,50	16576,500	,001
Yabancı Diller	111	287,66*	31930,50		
Eğitim Bil.	115	154,92	17815,50	11145,500	,049
Türkçe ve Sosyal	223	177,02*	39475,50		
Eğitim Bil.	115	104,86	12059,00	5389,000	,043
Yabancı Diller	111	122,45*	13592,00		
Temel Eğitim	262	224,04*	58699,00	24246,000	,001
Türkçe ve Sosyal	223	265,27	59156,00		
Temel Eğitim	262	176,68	46290,00	11837,000	,005
Yabancı Diller	111	211,36*	23461,00		

Mann-Whitney U testi sonuçlarına göre BÖTE ile Eğitim Bilimleri, Matematik ve Fen Bilimleri, Özel Eğitim, Temel Eğitim, Türkçe ve Sosyal, Yabancı Diller grupları arasında; Matematik ve Fen Bilimleri ile Türkçe ve Sosyal ve Yabancı Diller grupları arasında; Temel Eğitim ile Türkçe ve Sosyal ve Yabancı Diller grupları arasında;

Eğitim Bilimleri ile Türkçe ve Sosyal ve Yabancı Diller grupları arasında fark olduğu görülmüştür (Tablo 25).

4.2.1 Öğretmen Adaylarının Bilgisayar Sahibi Olma Süresine Göre Bilgi Güvenliği Farkındalık Durumları

Elde edilen verilere göre 1200 öğretmen adayından 223 öğretmen adayının evinde bilgisayarı olmadığı, 977 öğretman adayının ise evinde bilgisayarı bulunduğu tespit edilmiştir. Öğretmen adaylarının evde bilgisayar sahibi olma süresine göre BGF düzeyleri arasında anlamlı fark olup olmadığına anlamak için uygulanan Kruskal Wallis analiz sonuçlarına göre (Tablo 26) farklılığın anlamlı olduğu görülmüştür [$\chi^2_{(6)}$=53,149, p<.01].

Tablo 26: Öğretmen Adaylarının Bilgisayar Sahibi Olduğu Yıl ile Bilgi Güvenliği Farkındalıklarına İlişkin Kruskal Wallis Sonuçları

	Bilgisayar Sahibi olma	N	Sıra Ortalaması	sd	χ^2	p
Bilgi Güvenliği Farkındalığı	Yok	223	509,45	6	53,149	,000
	2 yıldan az	125	557,73			
	3-4 yıl	116	594,56			
	5-6 yıl	147	568,36			
	7-8 yıl	152	615,27			
	9-10 yıl	117	548,69			
	10 yıldan fazla	320	709,50			

*p<.01

Anlamlı farkın hangi gruplar arasında olduğunu anlamak için Mann-Whitney U testi uygulanmıştır (Tablo 27).

Tablo 27: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıklarının Bilgisayar Sahibi Olduğu Yıla Göre Mann-Whitney U Testi Sonuçları

Grup Karşılaştırması	N	Sıra Ortalaması	Sıra Toplaması	U	p
2 yıldan az	125	182,81	22851,50	14976,500	,000
10 yıldan fazla	320	238,70*	76383,50		
3-4 yıl	116	186,48	21631,50	14845,500	,001
10 yıldan fazla	320	230,11*	73634,50		
3-4 yıl	116	186,75*	21662,50	10991,500	,023
Yok	223	161,29	35967,50		
5-6 yıl	147	196,80	28929,00	18051,000	,000
10 yıldan fazla	320	251,09*	80349,00		
7-8 yıl	152	210,55	32003,00	20375,000	,004
10 yıldan fazla	320	248,83*	79625,00		
7-8 yıl	152	208,11*	31632,50	13891,500	,003
Yok	223	174,29	38867,50		
9-10 yıl	117	176,52	20653,00	13750,000	,000
10 yıldan fazla	320	234,53*	75050,00		
10 yıldan fazla	320	308,75*	98798,50	23921,500	,000
Yok	223	219,27	48897,50		

Test sonucuna göre anlamlı farkın Yok ile 3-4 yıl, 7-8 yıl grupları arasında ve 10 yıldan fazla ile Yok, 2 yıldan az, 3-4 yıl, 5-6 yıl, 7-8 yıl, 9-10 yıl grupları arasında olduğu belirlenmiştir (Tablo 27).

4.2.2 Öğretmen Adaylarının Evde Bilgisayar Kullanmayı Bilen Başka Birisi Olma Kriterine Göre Bilgi Güvenliği Farkındalık Durumları

Evde bilgisayar kullanmayı bilen başka birisi olmasının öğretmen adaylarının BGF üzerinde anlamlı bir etkisi olup olmadığını belirlemek için Kruskal Wallis analizi yapılmıştır (Tablo 28).

Tablo 28: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıkları ile Evde Bilgisayar Kullanmayı Bilen Başka Biri Olmasına İlişkin Kruskal Wallis Sonuçları

	Bilgisayar Kullanan Başka Biri	N	Sıra Ortalaması	sd	χ^2	p
Bilgi Güvenliği Farkındalığı	Evet	1077	606,40	2	3,346	,188
	Hayır	45	571,46			
	Kısmen	78	535,81			

*p>.05

Analiz sonuçlarına bakıldığında göre evde bilgisayar kullanmayı bilen başka birisinin bulunma durumuna göre öğretmen adaylarının BGF'nin aradaki farkın anlamlı olmadığı bulunmuştur [$\chi^2_{(2)}$=3,346, p>.05].

4.2.3 Öğretmen Adaylarının Evde İnternet Bağlantısı Olma Kriterine Göre Bilgi Güvenliği Farkındalık Durumları

Öğretmen adaylarının BGF'nın evde internet bağlantısı olma kriteri ikili gruplar arasındaki farkı anlamaya yarayan Mann-Whitney U testi tercih edilmiştir. Grupların anlamlı olarak farklılaşıp farklılaşmadığını belirlemek için Mann-Whitney U testi yapılmıştır (Tablo 29).

Tablo 29: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıkları ile Evde İnternet Bağlantısı Olma Kriterine İlişkin Mann-Whitney U Test Sonuçları

	Grup	N	Sıra Ortalaması	Sıra Toplamı	U	p
Bilgi Güvenliği Farkındalığı	Var	920	619,43	569874,50	111385,500	,001
	Yok	280	538,31	150725,50		

*p<.05

Mann-Whitney U testi analiz sonuçlarına göre evde internet bağlantısı bulunması ile BGFD 'nin anlamlı farklılık gösterdiği bulunmuştur [U = 111385,500, p<.05]. Sıra ortlamalarına bakıldığında evde internet bağlantısı olan öğretmen adaylarının BGF'nin evde internet bağlantısı olmayan öğretmen adaylarından daha yüksek olduğu anlaşılmıştır.

4.2.4 Öğretmen Adaylarının Araştırmayı En Fazla Yaptıkları Yer Kriterine Göre Bilgi Güvenliği Farkındalık Durumları

Öğretmen adaylarının BGF'de araştırmayı en fazla yaptıkları yere göre anlamlı olarak farklılaşıp farklılaşmadığını belirlemek için uygulanan Mann-Whitney U testi sonuçlarına göre farkın anlamlı olmadığı sonucuna ulaşılmıştır [U = 318801,000, p>.05].

Tablo 30: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıkları ile Araştırmayı En Fazla Yaptıkları Yere İlişkin Mann-Whitney U Test Sonuçları

Grup	N	Sıra Ortalaması	Sıra Toplamı	U	p
İnternet	1144	600,30	686741,00	318801,000	,927
Diğer, Kütüphane	56	604,63	33859,00		

*p>.05

Buna göre öğretmen adaylarının araştırmayı internetten ya da başka bir platformdan yapmalarının BGF konusunda etkili olmadığı anlaşılmıştır (Tablo 30).

4.2.5 Öğretmen Adaylarının İnternet Kullanımında Karşılaştığı En Önemli Zorluğa Göre Bilgi Güvenliği Farkındalık Durumları

Öğretmen adaylarının BGF'nin internet kullanımında karşılaştığı en önemli zorluğa göre anlamlı olarak farklılaşıp farklılaşmadığını belirlemek için Kruksal Wallis testi uygulanmıştır. Kruskal Wallis analiz sonuçlarına göre farkın anlamlı olduğu [$\chi^2_{(3)}$=8,011, p<.05], Tablo 31'de görülmektedir.

Tablo 31: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıkları ile İnternet Kullanımında Karşılaşılan En Önemli Zorluğa İlişkin Kruskal Wallis Sonuçları

	Karşılaşılan Zorluk	N	Sıra Ortalaması	sd	χ^2	p
Bilgi Güvenliği Farkındalığı	İnternet Erişiminin Çok Yavaş Olması	657	613,24	3	8,011	,046
	İnternet Erişiminin Çok Pahalı Olması	141	632,53			
	Aranılan Bilgiye Ulaşamamak	346	579,39			
	İnternet Kul. Karışıklığı, Bilgisayar Kul. Zorluğu	56	500,80			

*p<.05

Mann-Whitney U testi ile tüm grupların olası ikililerinin karşılaştırmasına bakılarak anlamlı farkın hangi gruplar arasında olduğu öğrenilmiştir (Tablo 32).

Tablo 32: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıklarının İnternet Kullanımında Karşılaştığı En Önemli Zorluğa Göre Mann-Whitney U Test Sonuçları

Grup Karşılaştırması	N	Sıra Ortalaması	Sıra Toplaması	U	p
İnternet Erişimi Çok Yavaş Olması	657	362,30*	238034,00	14911,000	,018
İnternet Kullanım Karışıklığı ve Bilgisayar Kullanım Zorluğu	56	294,77	16507,00		
İnternet Erişimi Çok Pahalı Olması	141	105,01*	14806,00	3101,000	,019
İnternet Kullanım Karışıklığı ve Bilgisayar Kullanım Zorluğu	56	83,88	4697,00		

Mann-Whitney U test sonuçlarına göre öğretmen adaylarının internet kullanımında karşılaştığı en önemli zorluğa göre BGFD üzerinde anlamlı bir etkiye sahip olduğu söylenirken anlamlı farkın; internet erişiminin çok yavaş olması ile internet kulllanım karışıklığı, bilgisayar kulllanım zorluğu grupları arasında ve internet erişiminin çok pahalı olması ile internet kulllanım karışıklığı, bilgisayar kulllanım zorluğu grupları arasında olduğu belirlenmiştir (Tablo 32).

4.2.6 Öğretmen Adaylarının İnternet Sitelerine Ulaşma Yollarına Göre Bilgi Güvenliği Farkındalık Durumları

Öğretmen adaylarının internet sitelerine ulaşma yollarının BGF üzerinde anlamlı bir etkiye sahip olup olmadığını belirleyebilmek için Kruskal Wallis uygulanmıştır. Kruskal Wallis analiz sonuçlara göre farkın anlamlı olduğu [$\chi^2_{(2)}$= 7,759, p<.05] belirlenmiştir (Tablo 33).

Tablo 33: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıkları ile İnternet Sitelerine Ulaşma Yollarına İlişkin Kruskal Wallis Sonuçları

	İnternet Sitelerine Ulaşma Yolu	N	Sıra Ortalaması	sd	χ^2	p
Bilgi Güvenliği Farkındalığı	Web Site Linkleri Takip	202	632,02	2	7,759	,021
	Arama Motorları	907	585,79			
	Diğer, Arkadaş Tavsiyesi, Bilgisayar Dergi Linkleri, Reklamlar	91	677,16			

*p<.05

Anlamlı farkın hangi gruplar arasında olduğu Mann-Whitney U testi ile elde edilmiştir (Tablo 34).

Tablo 34: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıklarının İnternet Sitelerine Ulaşma Yollarına Göre Mann-Whitney U Testi Sonuçları

Grup Karşılaştırması	N	Sıra Ortalaması	Sıra Toplaması	U	p
Arama Motorları	907	492,56	446750,50	34972,500	,016
Diğer, Arkadaş Tavsiyesi, Bilgisayar Dergi Linkleri, Reklamlar	91	568,69*	51750,50		

Mann-Whitney U testi sonuçlarına göre anlamlı farkın arama motorları ile diğer, arkadaş tavsiyesi, bilgisayar dergi linkleri, reklamlar arasında olduğu görülmüştür (Tablo 34).

4.2.7 Öğretmen Adaylarının İnternete Bağlanma Yerine Göre Bilgi Güvenliği Farkındalık Durumları

Öğretmen adaylarının BGF'nın internete bağlanma yeri kriterine göre anlamlı olarak farklılaşıp farklılaşmadığını belirlemek için Mann-Whitney U testi uygulanmıştır (Tablo 35).

Tablo 35: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıkları ile İnternete Bağlanma Yerine İlişkin Mann-Whitney U Test Sonuçları

Grup	N	Sıra Ortalaması	Sıra Toplamı	U	p
Cep Telefonu	772	570,59	440492,50	142114,500	,000
Diğer, İnternet Kafe, Yurt, Ev, Okul	428	654,46	280107,50		

*p<.01

Mann-Whitney U testinin analizi sonucunda öğretmen adaylarının internete bağlanma yerine göre BGFD'nin anlamlı farklılık gösterdiği bulunmuştur [U = 142114,500, p<.01]. Sıra ortlamalarına bakıldığında diğer, internet kafe, yurt, ev ve okuldan internete bağlanan öğretmen adaylarının bilgi güvenliği farkındalığının cep telefonundan internete bağlanan öğretmen adaylarından daha yüksek olduğu anlaşılmıştır.

4.2.8 Öğretmen Adaylarının İnterneti Kullanma Süresine Göre Bilgi Güvenliği Farkındalık Durumları

Öğretmen adaylarının interneti kullanma süresine (yıla) göre BGF'nin anlamlı olarak farklılaşıp farklılaşmadığını belirlemek için Kruskal Wallis analizi yapılmış ve elde edilen sonuçlara göre farkın anlamlı olduğu [$\chi^2_{(3)}$= 23,555, p<.01], bulunmuştur (Tablo 36).

Tablo 36: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıkları ile İnterneti Kullanma Süresine İlişkin Kruskal Wallis Sonuçları

	Kullanım Süresi	N	Sıra Ortalaması	sd	χ^2	p
Bilgi Güvenliği Farkındalığı	4 yıldan az	241	545,34	3	23,555	,000
	5-6 yıl	243	562,67			
	7-8 yıl	267	582,45			
	9 yıldan fazla	449	661,32			

*p<.01

Anlamlı farkın hangi gruplardan kaynaklandığını bulmak için Mann-Whitney U testi yapılmıştır (Tablo 37).

Tablo 37: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıklarının İnterneti Kullanma Süresine Göre Mann-Whitney U Testi Sonuçları

Grup Karşılaştırması	N	Sıra Ortalaması	Sıra Toplaması	U	p
4 yıldan az	241	303,14	73056,00	43895,000	,000
9 yıldan fazla	449	368,24*	165339,00		
5-6 yıl	243	309,44	75195,00	45549,000	,000
9 yıldan fazla	449	366,55*	164583,00		
7-8 yıl	267	328,19	87627,50	51849,500	,002
9 yıldan fazla	449	376,52*	169058,50		

Mann-Whitney U test sonuçlarına göre öğretmen adaylarının interneti kullanma süresinin (yılının) BGFD üzerinde anlamlı bir etkiye sahip olduğu farkın 4 yıldan az ile 9 yıldan fazla gruplar, 5-6 yıl ile 9 yıldan fazla gruplar ve 7-8 yıl ile 9 yıldan fazla olan gruplar arasında olduğu bulunmuştur.

4.2.9 Öğretmen Adaylarının Bilgiye Ulaşmak İçin Kullanılan Kişi ve Araç Kriterine Göre Bilgi Güvenliği Farkındalık Durumları

Öğretmen adaylarının bilgiye ulaşmak için kullanan kişi ve araç kriterine göre BGF'nın anlamlı olarak farklılaşıp farklılaşmadığını tespit etmek için Kruskal Wallis testi yapılmış ve analiz sonuçlarına göre farkın anlamlı olduğu [$\chi^2_{(2)}$=12,138, p<.05] bulunmuştur (Tablo 38).

Tablo 38: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıkları ile Bilgiye Ulaşmak İçin Kullanılan Kişi ve Araç Kriterine İlişkin Kruskal Wallis Sonuçları

	Bilgiye Ulaşma Şekli	N	Sıra Ortalaması	sd	χ^2	p
Bilgi Güvenliği Farkındalığı	İnternet	868	591,31	2	12,138	,002
	İnternet Hariç Diğer (İnsanlar, Gazete, TV, Dergi, Radyo)	109	538,78			
	Hepsi	223	666,42			

*p<.05

Öğretmen adaylarının bilgiye ulaşmak için kullanılan kişi ve araç kriterine göre BGFD üzerinde anlamlı farkın kaynağını belirlemek için Mann-Whitney U testi uygulanmıştır (Tablo 39).

Tablo 39: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıklarının Bilgiye Ulaşmak İçin Kullanılan Kişi ve Araca Göre Mann-Whitney U Testi Sonuçları

Grup Karşılaştırması	N	Sıra Ortalaması	Sıra Toplaması	U	p
İnternet	868	532,14	461898,00	84752,000	,004
Hepsi	223	599,95*	133788,00		
İnternet Hariç	109	142,00	15477,50	9482,500	,001
Hepsi	223	178,48*	39800,50		

Mann-Whitney U testi sonuçlarına göre öğretmen adaylarının bilgiye ulaşmak için kullanılan kişi ve araç kriterine göre BGFD İnternet ile Hepsi grupları ve İnternet Hariç ile Hepsi grupları arasında fark olduğu görülmüştür (Tablo 39).

4.2.10 Öğretmen Adaylarının İnterneti Bir Hafta İçinde Kaç Saat Kullandığına Göre Bilgi Güvenliği Farkındalık Durumları

Çalışmaya katılan öğretmen adaylarının haftalık internet kullanım süresine göre BGF 'ları arasında anlamlı fark olup olmadığına belirlemek için Kruskal Wallis testi uygulanmış ve analiz sonuçlarına göre farkın anlamlı olduğu [$\chi^2_{(6)}$=17,131, p<.05] görülmüştür (Tablo 40).

Tablo 40: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıkları ile İnterneti Bir Hafta İçinde Kaç Saat Kullandığına İlişkin Kruskal Wallis Sonuçları

	Haftalık İnternet Kullanım süresi	N	Sıra Ortalaması	sd	χ^2	p
	0-5	134	590,87			
	6-10	235	583,10			
Bilgi	11-15	195	588,31			
Güvenliği	16-20	159	573,79	6	17,131	,009
Farkındalığı	21-25	193	586,56			
	36-40	121	582,22			
	41 saatten fazla	163	704,21			

*p<.05

Gruplar arasındaki anlamlı farkı belirlemek için Mann-Whitney U testi yapılmıştır (Tablo 41).

Tablo 41: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıklarının İnterneti Bir Hafta İçinde Kaç Saat Kullandığına Göre Mann-Whitney U Testi Sonuçları

Grup Karşılaştırması	N	Sıra Ortalaması	Sıra Toplaması	U	p
0-5 saat	134	133,00	17822,50	8777,500	,004
41 saatten fazla	163	162,15*	26430,50		
6-10 saat	235	182,99	43002,00	15272,000	,001
41 saatten fazla	163	223,31*	36399,00		
11-15 saat	195	164,54	32085,00	12975,000	,003
41 saatten fazla	163	197,40*	32176,00		
16-20 saat	159	143,55	22824,50	10104,500	,001
41 saatten fazla	163	179,01*	29178,50		
21-25 saat	193	162,28	31319,50	12598,500	,001
41 saatten fazla	163	197,71*	32226,50		
36-40 saat	121	126,14	15263,50	7882,500	,004
41 saatten fazla	163	154,64*	25206,50		

Mann-Whitney U testi sonuçlarına göre haftada 41 saatten fazla interneti kullanan öğretmen adayları ile interneti 0-5 saat, 6-10 saat, 11-15 saat, 16-20 saat, 21-25 saat, 36-40 saat kullananlar arasında fark olduğu bulunmuştur (Tablo 41).

4.2.11 Öğretmen Adaylarının E-Postalarının Kontrol Süresine Göre Bilgi Güvenliği Farkındalık Durumları

Öğretmen adaylarının BGF'nnin e-postalarını kontrol süresine göre anlamlı farklılık gösterip göstermediği belirlemek için Kruskal Wallis analizi yapılmıştır. Analiz sonuçlarına göre anlamlı fark olduğu [$\chi^2_{(6)}$=65,605, p<.05], bulunmuştur (Tablo 42).

Tablo 42: Öğretmen Adaylarının E-Postalarının Kontrol Süresi ile Bilgi Güvenliği Farkındalıklarına İlişkin Kruskal Wallis Sonuçları

	E-posta Kontrol Süresi	N	Sıra Ortalaması	sd	χ^2	p
Bilgi Güvenliği Farkındalığı	Ayda bir kez	282	540,08	6	65,605	,000
	Haftada bir kez	283	601,96			
	Günde bir kez	161	740,95			
	Ayda birkaç kez	161	522,67			
	Haftada birkaç kez	196	580,64			
	Günde birkaç kez	88	758,66			
	E-posta kullanmıyor	29	480,36			

*p<.01

Mann-Whitney U testi ile anlamlı farkın hangi gruplar arasında olduğu belirlemiştir. Mann-Whitney U testi sonuçlarına göre e-postasını ayda bir kez ile haftada bir kez, günde bir kez, günde birkaç kez kullananlar arasında; haftada bir kez ile günde bir kez, günde birkaç kez kullananlar arasında anlamlı fark olduğu bulunmuştur. Ayrıca ayda birkaç kez ile haftada bir kez, günde bir kez, günde birkaç kez kulllananlar arasında; haftada birkaç kez ile günde bir kez, günde birkaç kez ve E-posta kullanmayanlar ile günde bir kez, günde birkaç kez grupları arasında farklılıklar olduğu bulunmuştur (Tablo 43).

Tablo 43: Öğretmen Adaylarının Bilgi Güvenliği Farkındalıklarının E-Postalarının Kontrol Süresine Göre Mann-Whitney U Testi Sonuçları

Grup Karşılaştırması	N	Sıra Ortalaması	Sıra Toplaması	U	p
Ayda bir kez	282	268,02	75583,00	35680,000	,029
Haftada bir kez	283	297,92*	84312,00		
Ayda bir kez	282	195,27	55067,50	15164,500	,000
Günde bir kez	161	268,81*	43278,50		
Ayda bir kez	282	169,96	47928,50	8025,500	,000
Günde birkaç kez	88	235,30*	20706,50		
Haftada bir kez	283	203,23	57513,50	17327,500	,000
Günde bir kez	161	256,38*	41276,50		
Haftada bir kez	283	233,64*	66121,00	19628,000	,015
Ayda birkaç kez	161	202,91	32669,00		
Haftada bir kez	283	174,00	49241,50	9055,500	,000
Günde Birkaç Kez	88	224,60*	19764,50		
Günde bir kez	161	190,97*	30745,50	8216,500	,000
Ayda birkaç kez	161	132,03	21257,50		
Günde bir kez	161	205,12*	33025,00	11572,000	,000
Haftada birkaç kez	196	157,54	30878,00		
Günde bir kez	161	101,77*	16385,50	1324,500	,000
E-posta kullanmıyor	29	60,67	1759,50		
Ayda birkaç kez	161	108,02	17391,00	4350,000	,000
Günde birkaç kez	88	156,07*	13734,00		
Haftada birkaç kez	196	129,71	25422,50	6116,500	,000
Günde birkaç kez	88	170,99*	15047,50		
Günde birkaç kez	88	65,36*	5752,00	716,000	,000
E-posta kullanmıyor	29	39,69	1151,00		

4.2.12 Öğretmen Adaylarının Hayatlarında İnternet ve Bilgisayar Olmamasına İlişkin Görüşleri

Öğretmen adaylarının "Hayatınızda/yaşamınızda internet ve bilgisayar olmasaydı neler değişirdi?" açık uçlu soruya verdikleri cevaplar içerik analizi ile olumlu ve

olumsuz görüşler olarak iki gruba ayrılmıştır. Öğretmen adaylarının yaşamlarında internet ve bilgisayar olmamasının sebep olacağı eksiklik ve aksaklıkları olumsuz görüşler başlığı altında toplanmıştır (Tablo 44). Öğretmen adaylarının birçok olumsuz görüşü bulunmasına rağmen olumlu görüşlerinin daha fazla olduğu görülmüştür (Tablo 45). Çalışmaya katılan 1200 öğretmen adayından 582'si internet ve bilgisayarın hayatlarında olmama durumuna göre görüş bildirmiştir. Bildirilen 895 görüşten 492'sinin olumlu, 403'ünün olumsuz olduğu görülmüştür.

Tablo 44: Öğretmen Adaylarının İnternet ve Bilgisayar Olmamasına İlişkin Olumlu Görüşleri

Olumlu Görüş	Frekans
Bilgiye ulaşmanın zor olabileceği	194
Bilgiye ulaşmanın zaman alabileceği	85
İletişimin azalabileceği ve iletişim kurmanın güçleşebileceği	53
Hayatın sıkıcı olabileceği ve insanların çok sıkılabileceği	21
Haberleşmenin güçleşebileceği	20
Hayatın daha zor olabileceği	15
Araştırma yapmanın güçleşebileceği	13
Eğitim-Öğretim hayatının eksik kalabileceği, eğitimin zorlaşabileceği	10
Sosyal medyadan haber sahibi olunamayacağı ve alışılamayabileceği	7
Bilgilere ulaşılamayabileceği, çok fazla bilgi edinilemeyeceği	7
Güncel gelişmelerin zamanında takip edilemeyebileceği	5
Hızlı ve görüntülü iletişim sağlanamayabileceği	5
Normatif değerlere takınılabileceği	5
Meşguliyet alanlarının değişip, birçok aktivitenin yapılamayabileceği	5
Bakış açısının değişmeyebileceği	5
Boş zamanların iyi değerlendirilemeyeceği	4
Günlük hayattaki işlerin zaman alabileceği ve sorun yaşanabileceği	4
Birçok alanda geri kalınabileceği	4
Kişisel gelişimin güçleşebileceği	3
Bilgisayar ve İnternet olmasaydı eksiklik hissedilebileceği	3
Hayatın olumsuz etkilenebileceği	3
Her işlemin yavaş olabileceği	3

Zekâ gelişimi bu kadar fazla olmayabileceği	3
Çevirim içi alışveriş kolaylığının olmayabileceği	2
Kütüphanelerde saatlerce kalınabileceği	2
Sunum ve etkinlik hazırlanamayabileceği	2
Daha az bilgiye sahip olunma ve Yazılı kaynaklara bakmak zorunluluğu	2
Toplam	492

Öğretmen adaylarının olumlu görüşlerine göre bilgiye ulaşmanın zor (194), zaman alabileceği (85) iletişimin azalabileceği ve iletişim kurmanın güçleşebileceği(53), hayatın sıkıcı ve insanların çok sıkılabileceği (21), haberleşmenin güçleşebileceği (20), hayatın daha zor olabileceği(15), araştırma yapmanın güçleşebileceği (13) ve eğitim-öğretim hayatının eksik kalabileceği, zorlaşabileceği (10), görüşlerinde daha fazla birlik bulunmaktadır. Bunların yanında bilgiye ulaşmak için daha fazla gözlem yapılabileceği, eğlence amaçlı kullanılamayabileceği, bankacılık işlemlerinin uzun sürebileceği, insanların kendi halinde bir hayata sahip olabileceği, bilginin öğretmenlerden elde edilebileceği, içine kapanıklığı artırabileceği ve kültürel iletişim daha yavaş olabileceği (1) ile ilgili görüşlerde bulunmaktadır (Tablo 44). Öğretmen adaylarının internet ve bilgisayar olmamasına ilişkin olumsuz görüşleri Tablo 45'de verilmiştir.

Tablo 45: Öğretmen Adaylarının İnternet ve Bilgisayar Olmamasına İlişkin Olumsuz Görüşleri

Olumsuz Görüş	Frekans
Aile, akraba, arkadaşlarla daha çok vakit geçirilebileceği	105
Sosyal ilişkiler ve iletişimin artabileceği	106
Zamanın daha iyi değerlendirilip, günler daha dolu geçebileceği	33
Kitap, gazete, dergi vb. yazılı materyallerin daha çok okunabileceği ve okuma alışkanlığı kazanılabileceği	27
Kütüphanelere talebin ve kütüphanelerin sayısının artabileceği	22
Psikolojik ve fiziksel olarak daha sağlıklı bir yaşam olabileceği	13
İnternete ve sosyal medyaya bağımlılığı olmayan bilinçli nesillerin yetişebileceği	13
Kitaplar daha değerli olabileceği	9

Her şeyin daha güzel olabileceği	8
Tembelliğin olmayıp ve çalışkan nesillerin yetişebileceği	7
Araştırmaların daha fazla yapılabileceği ve bu yönde gelişmelerin yaşanabileceği	7
Kişisel gelişimlerini arttırabileceği	7
Hazır bilgi yerine uğraşarak bilgilere sahip olunabileceği	6
Siber suçların olmayacağı	6
İnsanlar farklı görünmeyip kendileri gibi yaşamaya başlayabileceği	5
İnsanların daha güvenli olabileceği	5
Bilgiye ulaşmak için kitaplara başvurulabileceği	4
Gerekli ve doğru bilgiye ulaşmada kolaylık olabileceği	4
Zararlı bilgilere ulaşmanın kolay olmayabileceği	3
Bilgi kirliliği olmayabileceği	3
İnsanlar birbirini aldatmayabileceği	2
Daha çok ders çalışılabileceği	2
Derslerde daha başarılı olunabileceği	2
Toplam	403

Olumsuz görüşlerde ise aile, akraba, arkadaşlarla daha çok vakit geçirilebileceği (105), sosyal ilişkiler ve iletişimin artabileceği (106), zamanın daha iyi değerlendirilip, günler daha dolu geçebileceği (33) düşünülmektedir. Ayrıca, kitap, gazete, dergi vb. yazılı materyallerin daha çok okunabileceği ve okuma alışkanlığı kazanılabileceği (27) ve kütüphanelere talebin ve kütüphanelerin sayısının artabileceği (22) görüşlerinde daha fazla birlik olduğu görülmüştür. Bu görüşler dışında yapılan araştırma ve öğrenmelerin daha kalıcı olabileceği, kelime dağarcığının daha fazla gelişebileceği, hayatın daha eğlenceli olabileceği ve çocukların kötü alışkanlıklara karşı tutumunun olumlu olabileceği görüşler (1) yer almaktadır (Tablo 45). Bir kez (1) görüş bildirenlerin görüşleri Tablo 44 ve 45 ‘de verilmemiştir.

BEŞİNCİ BÖLÜM

V. SONUÇ, TARTIŞMA ve ÖNERİLER

Bu bölümde öğretmen adaylarının; **demografik** (cinsiyet, yaş, sınıf, akademik not ortalaması, öğrenim gördükleri bölüm, mezun olduğu lise, anne, baba eğitim düzeyleri ve meslekleri, kardeş sayısı, internet ve bilgisayar kullanım süreleri açıklanırken) ile **coğrafi** (yaşadığı yer) ve **psikolojik**(davranış ve düşünceler, ilgi alanları, güdüler, hayat tarzları vb) özellikler (internet, bilgisayar kullanım durumları ve BGFD) ile elde edilen bulgular diğer çalışmalarla birlikte değerlendirilmiş, sonuçlar, karşılaşılan problemler ve öneriler başlıklar altında açıklanmaktadır.

5.1 Sonuç ve Tartışma

Bu çalışmada, öğretmen adaylarının BGF belirlenmesi kapsamında alan yazında belirtildiği gibi günümüzde gerçekleştirilen BT kullanımlarında BG sağlanmasında asıl hedef haline gelen insan faktörünün, kişisel, kurumsal, ulusal ve uluslararası bilgi varlıklarını koruyabilmesi için BGF'nin geliştirilmesine katkı sağlamak amacıyla geleceğin öğretmenlerinin BGF'larının nelere göre değiştiğinin ve ne düzeyde olduğunun belirlenmesi oldukça önemlidir.

Öncelikle **demografik** ile **coğrafi** ve **psikolojik özellikler**le ilgili veriler sistematik bir şekilde değerlendirilmiştir. İnsan faktörünün BGF'de öneminin giderek artmasından dolayı, gelecek nesilleri yetiştirecek öğretmen adaylarının farkındalığın arttırılarak geleceğin BG'nin sağlanmasına da katkı sağlayacaktır. Alan yazı çalışmalarında kişilerin BGF seviyeleri ile davranışları arasında her zaman tutarlı bir ilişki olmadığı, BGF yüksek olan bir kişinin bunu davranışa dönüştürmediğinde BGF eksiklikler olduğu görülmüştür. Çalışma ile BGF'nin davranışa dönüşmesi sürecinde önemli olan demografik, coğrafik özellikler belirlenmeye çalışılmıştır.

Araştırmanın sınırlılıkları çerçevesinde; alanyazın taraması sonucu elde edilen veriler ışığında günümüzde eğitim alanında BT kullanımı da oldukça yaygın hale gelirken ana hedefi öğrenmeyi zaman mekân sınırlaması içine sokmadan kalıcılığı sürekliliği ülkemizde ve tüm dünyada her geçen gün hızlı şekilde gelişmekte ve yayılmaktadır. BT öğrenme öğretme sürecinde faydalarının yanı sıra güvenlik problemlerini de beraberinde getirirken gelecek nesilleri yetiştirecek olan öğretmen adaylarına

gelecekteki öğrencilerinin BT bilinçli ve güvenli bir biçimde kullanabilmesinde büyük görevler düşmektedir.

Nitekim genel olarak yapılan çalışmalarda öğrencilerin BG yönelik bilgilerinin düşük düzeyde olurken (NCSA, 2011), ülkemizde interneti güvenli kullanma, bilişim güvenliğini sağlama, güvenlik tehditlerine karşı önlem alma konularında da bilgi düzeyleri düşüktür (Dijle, 2006; Dijle ve Doğan, 2011; Karaoğlan, Yılmaz vd., 2014; Kaşıkçı, Çağıltay, Karakuş, Kurşun ve Ogan, 2014; Mert vd., 2012; Tekerek ve Mart, 2010; Tekerek ve Tekerek, 2013).

OMÜ Eğitim Fakültesi öğretmen adaylarının bazı değişkenler açısından BGF'nı ortaya koymayı amaçlayan bu çalışmada kadın ve erkek öğretmen adayları arasında BGFD'nin anlamlı olarak farklılık gösterirken erkek öğretmen adaylarının BGF'nin kadınlara göre daha yüksek olduğu görülmüştür (Tablo 6). Bu durum benzer çalışmalarla çoğunlukla paralellik göstermektedir. Yayla (2018) erkek öğretmenlerin BGF'nın kadın öğretmenlerden yüksek olduğu sonucuna varmıştır. Yılmaz, Şahin ve Akbulut (2016), erkek öğretmenlerin kadın öğretmenlere göre DVG daha yüksek olduklarını bulmuşlardır. Gökmen ve Akgün (2015)'de BÖTE öğretmen adaylarının BG bilgilerinin cinsiyet ve öğrenim görülen üniversiteye göre değişkenlik gösterdiğini, BÖTE erkek öğretmen adaylarının kadın öğretmen adaylara göre BG bilgilerinin daha yüksek olduğunu belirtmişlerdir. Güldüren. Çetinkaya ve Keser (2016), orta öğretim erkek öğrencilerin BGF düzeylerinin kız öğrencilerinden; Mart (2012), BGF 'de erkek öğretmen adaylarının kadın öğretmen adaylarından; daha yüksek olduğu bulmuşlardır. Bu farklılıkların kadınların teknolojiye ve teknoloji kullanımına (bilgisayar ve internette geçirdikleri zamanın) olan ilgisinin az olmasından kaynaklandığı düşünülmektedir. Buna karşılık Mart (2012), BGF konusunda tehlikelerden daha fazla haberdar olma durumunda kadınların erkeklere oranla daha fazla olduğunu belirtirken genel BGF'da mühendis, avukat, sağlık personeli vb. farklı meslek gruplarındaki kadınların, erkeklerden daha yüksek olduğunu; Tekerek ve Tekerek (2013), ilköğretim ve lise kız öğrencilerin, erkek öğrencilere göre olumlu görüşe sahip olduklarını belirtmiştir. Arıtürk (2015), mühendislik fakültesindeki kadınların erkeklere göre BG ve BGF konusunda geliştirdikleri tutumlarının daha yüksek olduğunu ortaya koymuştur. Bu farklılıkların BT kullanma durumuna kadınların teknolojiye ve teknoloji kullanımına (bilgisayar ve

internette geçirdikleri zamanın) olan ilgisinin mesleklere göre değişebileceğini, ilköğretim ve lisede kız öğrencilerin erkeklere göre erken olgunlaşmasından (Genç, 1989) kaynaklanmış olabileceğini düşündürmektedir.

Bu çalışmada öğretmen adaylarının BGF, 23 ve üzerindeki yaş grubu ile 18-20 ve 21-22 yaş grubundaki öğretmen adayları arasında anlamlı fark bulunurken, 23 ve üzerindeki yaş grubunun farkındalıklarının daha yüksek olduğu bulunmuştur (Tablo 8). Alanda yapılan araştırmalardan Tekerek ve Tekerek (2013) yaş farkına bağlı olarak lise öğrencilerinin BGF'nın ilköğretimde eğitim gören öğrencilerden daha yüksek olduğunu belirtmişlerdir. Yayla (2018), öğretmenlerin yaş gruplarına göre BGF 'de özellikle 30 yaşın altındaki öğretmenlerin farkındalıkların yüksek olduğu, yaş grupları artıkça bilgi güvenliği farkındalıklarının düşük olduğu ve en düşük farkındalığın ise 50 ve üzeri yaşlı öğretmenlerde olduğunu belirtmiştir. Tekerek ve Mart (2010), yaptıkları araştırmada 8 ile 14 yaş grubunda ki çocukların internette çok fazla risk ve tehditle karşı karşıya kaldıklarını ve bu tehditler için yeterli düzeyde farkında olmadıklarını bulmuşlardır. Durak ve Seferoğlu (2017), öğretmenlerin yaş artışı ile bilişim teknolojileri konusundaki yeterlilik durumlarının ters orantılı olduğu ve en ileri teknoloji yeterlikleri ortalamasına hizmet süresi en az olan öğretmen gruplarının sahip olduğunu ifade etmiştir. Yapılan bu çalışmalar değerlendirildiğinde orta yaş grubundakilerin yaşı fazla ve aşağıda olanlara göre BGF fazla olduğu ifade edilebilir.

Yapılan çalışmada 1. sınıftaki öğretmen adayları ile 2. ve 3.sınıftaki öğretmen adayları arasında anlamlı fark olduğu bulunmuş, 1. sınıftaki öğretmen adaylarının BGF 2. ve 3.sınıftaki öğretmen adaylarından daha yüksektir (Tablo 10). Karacı, Akyüz ve Bilgici (2016), üniversite öğrencilerinin siber güvenlik davranışlarının fark edilecek şekilde farklılık göstermediğini; Tekerek ve Tekerek (2013), lise öğrencilerinin ilköğretim öğrencilerine göre farkındalıkların anlamlı bir şekilde yüksek olduğu belirtmişlerdir. Bu durumlarda lise ve üniversite 1 sınıf öğrencilerinin zamanı kullanma ve dikkati bir yöne toplama yanında ilgi alanının genişliğinin artışından; yaş artıkça başarı ve öğretmen olma sorumluluklarının artışına bağlı olarak ilgi alanı daralmasından kaynaklanmış olabileceği düşünülmektedir.

Akademik not ortalaması 2,6-3,0 olan öğretmen adaylarının not ortalaması 3,1-3,5 olan öğretmen adaylarına göre BGF'nin daha yüksek olduğu ve anlamlı düzeyde farklılık gösterdiği belirlenmiştir (Tablo 11, 12). Bu durumun akademik not ortalaması

yüksek olan öğretmen adaylarının okul derslerine daha fazla yoğunlaşıp internet ve bilgisayar kullanım süresinin azalttığı veya yeterince kullanmadığından kaynaklandığı söylenebilir.

Çalışmada öğretmen adaylarının BGF mezun oldukları lise türleri bakımından incelendiğinde; meslek lisesinden mezun olan adaylarının BGF, anadolu lisesi, anadolu öğretmen lisesi ve düz liseden mezun olan adaylara göre daha yüksek düzeydedir (Tablo 14). Karacı, Akyüz ve Bilgici (2016), bilgisayar kullanırken iz bırakmama konusunda meslek lisesinden mezun öğrencilerin düz/genel liselere göre daha olumlu olduğunu belirtmiştir. Meslek lisesinden mezun olan öğretmen adaylarının BGF bilgisayar, internet ve internet teknolojisiyle ilgili aldıkları ders sayılarının fazla olmasından ve bilgisayar ve interneti kullanma süreleri artışından kaynaklanabileceği düşünülmektedir.

Çalışmada öğretmen adaylarının yaşadığı yer bakımından (büyükşehir, şehir, ilçe, kasaba ve köy) anlamlı bir fark bulunmazken (Tablo 15). Tekerek ve Tekerek (2013), ilçe merkezinde eğitim gören öğrencilerin BGF daha yüksek düzeyde olduğu belirtmesine karşılık bilgisayar ve internetin zaman mekan sınırlaması tanımaksızın global boyuta taşınması yaşanılan yerin BGF ‘de önemli etkiye sahip olmadığı gerçeğini akıllara getirmektedir.

Çalışmada öğretmen adaylarının BGF’nin anne ve baba eğitim düzeyleri ile ilişkisinde; annesi lise mezunu olanların, annesi ilköğretim mezunu ve diğer ya da hiç eğitim görmemiş olanlardan yüksek olurken (Tablo 17), babası üniversite ve lise düzeyinde eğitime sahip öğretmen adaylarının, babası ilköğretim mezunu olanlardan yüksek olduğu belirlenmiştir (Tablo 20). Genel olarak eğitim seviyesinin artması ile teknoljiyi daha profesyonel olarak kullanmanın BGF artış gösterebileceği düşünülmektedir. Nitekim alan yazında anne baba eğitim düzeyinin BGF etkisi ile ilgili çalışmaya rastlanılmamasına karşılık Öztezcan (2017), BG ‘de kişisel verilerin korunması konusunda eğitim seviyesi doktora olan akademik personellerin eğitim seviyesi lise olan idari personellere göre daha fazla farkında olduklarını ifade etmiştir. Oktay ve Çakır (2012), ön lisans mezunu öğretmenlerin BT karşı tutumlarının, lisans ve yüksek lisans düzeyinde eğitimi olan öğretmenlerden daha düşük olduğunu bulmuşlardır. Bunlara karşılık, Yılmaz, Şahin ve Akbulut (2016), öğretmenlerin

DVGF öğrenim durumlarına göre değişmediğini, Mart (2012) da eğitim düzeyinin BGF anlamlı nitelendirilebilecek bir etkisinin olmadığını belirtmişlerdir.

Öğretmen adaylarının BGF, anne ve baba mesleğine göre ilişkisinde anne mesleği ile anlamlı olarak farklılık görülmezken; baba mesleği devlet çalışanı memur (memur, mühendis, doktor, öğretmen, hukuk), işçi ve diğer meslek gruplarında olan öğretmen adaylarının BGF, babası esnaf olan öğretmen adaylarından yüksek olduğu ve anlamlı düzeyde farklılaştığı bulunmuştur (Tablo 21, 22). Bu durum BT olan kullanım, ihtiyaçların fazlalığından kaynaklanabilir.

Öğretmen adaylarının BGF düzeyleri ile sahip olduğu kardeş sayısı arasında farkın anlamlı ve etkili olmadığı gözlemlenirken (Tablo 23) öğrenim gördüğü bölümlere göre farklılık bulunmaktadır. Nitekim BÖTE öğretmen adaylarının BGF, diğer altı bölümdeki (Eğitim Bilimleri, Matematik ve Fen Bilimleri, Özel Eğitim, Temel Eğitim, Türkçe ve Sosyal, Yabancı Diller) öğretmen adaylarından daha yüksek olduğu bulunmuştur. Bunun yanı sıra Türkçe ve Sosyal ve Yabancı Diller bölümlerindeki öğretmen adaylarının BGF, Matematik ve Fen Bilimleri, Eğitim bilimleri ve Temel Eğitim bölümlerindeki öğretmen adaylarından daha yüksek olduğu bulunmuştur (Tablo 25). Yılmaz, Şahin ve Akbulut (2016), branş öğretmenleri ile sınıf öğretmenleri arasında DVGF konusunda anlamlı bir fark olmadığını, Çelik ve Bindak (2005), öğretmenlerin bilgisayara yönelik tutumlarının branşa; Oktay ve Çakır (2012) teknolojiye göre tutumlarının değişmediğini; Yayla (2018) ise BT öğretmenlerinin BGF ‘nin diğer branşlara göre yüksek olduğunu belirtmiştir. BÖTE öğretmen adaylarının BGF diğer bölüm öğretmen adaylarından yüksek olmasının nedeni olarak BÖTE bölümü öğretmen adaylarının lisans eğitimlerinde bilgisayar, internet vb. teknoloji konularında alan dersleri ile ilgili eğitim almış olmalarıdan ve bu bölüme kayıt yaptıran öğrencilerin meslek lisesinden mezun olmalarından kaynaklanabileceği düşünülmektedir.

Çalışmada öğretmen adaylarından evde bilgisayarı 10 yıldan fazla süredir olan öğretmen adaylarının BGF, evde bilgisayarı olmayan, 2 yıldan az, 3-4 yıl, 5-6 yıl, 7-8 yıl ve 9-10 yıldır bilgisayara sahip olanlardan yüksek olduğu görülürken; 3-4 yıl ve 7-8 yıldır bilgisayarı olan öğretmen adaylarının BGF bilgisayarı olmayan adaylardan daha yüksek olduğu bulunmuştur (Tablo 27). Çelik ve Bindak (2005) bilgisayarı olan öğretmenlerin bilgisayara yönelik tutumlarının, olmayanlara göre daha yüksek

olduğunu belirtmiştir. Bu durumun bilgisayar ve donanımlarına uzun süre sahip olmanın bilgi ve BT doğru, etkin ve verimli şekilde kullanmayı sağlayabileceği bununda BGF arttıracağı düşünülmektedir.

Bu çalışmada, evde kendisinden başka bilgisayar kullanmayı bilenlerin de olduğu öğretmen adaylarının BGF düzeylerinin bilgisayar kullanmayı bilmeyen ya da kısmen bilenlerin arasında anlamlı bir fark olmadığı görülmüştür (Tablo 28). Gökmen ve Akgün (2015), BÖTE öğretmen adaylarının bilişim güvenliği bilgilerinin bilgisayarı gün içinde kullandığı süre ve ne kadar süre ile bilgisayara sahip olması gibi deneyimlere göre değişmediğini belirtmişlerdir.

Bu araştırmada, evde internet bağlantısı olan öğretmen adaylarının BGF düzeylerinin evde internet bağlantısı olmayanlara göre daha yüksektir (Tablo 29). Bu durumun internet kullanıcısının hemen her zaman interneti aktif kullanıcı rolünde olmasından kaynaklandığı ön görülürken öğretmen adaylarının araştırmayı en çok yaptıkları yere göre bakıldığında anlamlı bir farka sahip olmadığı ve BGF arttırmadığı görülmüştür (Tablo 30). Tekerek ve Tekerek (2013), öğrencilerin interneti ders çalışmak için kullandığını benzer şekilde ABD ulusal BG raporuna göre öğrencilerin % 94'ünün interneti araştırma ve ders yapmak amacıyla kullandığını belirtmişlerdir.

Bu çalışmada öğretmen adaylarının internette karşılaştığı zorluklara ve internet sitelerine ulaşma yollarına göre BGF düzeyleri arasında anlamlı fark bulunmakla birlikte internet kullanım karışıklığı ve bilgisayar kullanımın zor olmasının BGF internetin yavaş ve pahalı olmasından daha düşüktür (Tablo 32). Bu durum günümüzde eğitim başta olmak üzere hayatın birçok alanında bilgisayar kullanımının artması ile kullanım zorluğu ve karışıklığının ortadan kalkmasından kaynaklanabileceği öngörülmektedir. Öğretmen adaylarının internet sitelerine ulaşma yollarına göre arkadaş tavsiyesi, bilgisayar dergi linkleri, reklamlar ve diğer yollar ile ulaşanların BGF'nin internet sitelerine arama motorları ile ulaşanlaradan daha yüksek olduğu bulunmuştur (Tablo 34). Ayrıca öğretmen adaylarının internet sitelerine bağlanma yerine göre BGF düzeyleri arasında anlamlı farklılık olduğu (Tablo 35), evde internete bağlanan öğretmen adaylarının cep telefonları ile bağlananlara göre BGF yüksek olduğu görülmüştür. Bu durumda internete mobil cihazlar üzerinden bağlanmanın kullanım kolaylığı sağladığı, bağlantı süresini kısıtladığı düşünülebilir.

Bu çalışmada interneti 9 yıldan fazla süre kullanan öğretmen adaylarının BGF, interneti 9 yıldan az kullananlara ve (Tablo 36, 37); haftada 41 saat ve daha fazla kullananların da interneti haftada 41 saat ve daha az kullananlardan daha yüksek olduğu belirlenmiştir (Tablo 40,41). Mart (2012), genel olarak BGF internet kullanım sürelerine ve Gökmen ve Akgün (2015), BÖTE öğretmen adaylarının bilişim güvenliği bilgilerinin günlük internet kullanım süresine göre değişmediğini belirtmişlerdir

Bu araştırma ile kişi ve araçların bilgi güvenliğini etkilemesinde hepsini (televizyon, dergi, insan, internet, gazete, radyo) tercih eden öğretmen adaylarının BGF düzeyi, internet ve internet haricindeki kanalları tercih edenlerden daha yüksek olduğu görülmüştür (Tablo 38, 39). Ayrıca e-postasını günde bir kez kontrol eden öğretmen adaylarının BGF düzeyleri e-postasını ayda bir kez, haftada bir kez, ayda birkaç kez, haftada birkaç kez kontrol edenler ve e-postası olmayan öğretmen adaylarına göre daha yüksek olduğu, e-postasını günde birkaç kez kontrol eden öğretmen adaylarının BGF ayda bir kez, haftada bir kez, ayda birkaç kez, haftada birkaç kez kontrol edenler ile e-postası olmayanlardan daha yüksek olduğu, e-postasını haftada bir kez kontrol eden öğretmen adaylarının BGF e-postasını ayda bir kez ve ayda birkaç kez kontrol edenlerden yüksek olduğu bulunmuştur (Tablo 42, 43). Bu durumlarda internete sahip olma ve süresi ile kullanım ve süresi arttıkça BGF artacağı öngörülmektedir.

Öğretmen adaylarının "***Hayatınızda/yaşamınızda internet ve bilgisayar olmasaydı neler değişirdi***?" açık uçlu soruya verdikleri cevaplar incelendiğinde; öğretmen adaylarının çoğunluğunun (492) özellikle bilgiye ulaşma konusunda güçlük çekecekleri, bilgiye ulaşma hızlarında düşüş olacağı, çok sıkılacaklarını, iletişim ve haberleşmenin güçleşeceğini, eğitim-öğretimin zorlaşacağı vb. bilgisayar ve internet kullanımının olumlu yönleri ile ilgili görüş bildirirken, öğretmen adaylarının bir kısmı (403) da aile, akraba, arkadaşlarla daha çok vakit geçirilebileceği, sosyal ilişkiler ve iletişimin artabileceği, zamanın daha iyi değerlendirilip, günlerin daha dolu geçebileceği, kitap, gazete, dergi vb. yazılı materyallerin daha çok okunabileceği ve okuma alışkanlığı kazanılabileceği, kütüphanelere talebin ve kütüphanelerin sayısının artabileceği, psikolojik ve fiziksel olarak daha sağlıklı bir yaşam olabileceği vb. bilgisayar ve internet kullanımının olumsuzlukları ile ilgili olumlu ve olumsuz görüşler bulunmaktadır. Bu görüşlerden de yola çıkarak bilgisayar ve internet

kullanımının hayatımızda olumlu ve olumsuz etkileri olduğu değerlendirilebilir (Tablo 44,45).

Öğretmen adaylarının BGF bazı değişkenler açısından incelenmesi amacıyla yapılan çalışmanın bulgularının, örneklemi oluşturan öğretmen adaylarının kişisel görüş ve tercihleri doğrultusunda oluştuğu gerçeği çalışmanın en temel sınırlılığını oluşturmaktadır. Bu kapsamda her bir üniversitenin kendine özgü akademik ve sosyal dokusu olduğu dikkate alınarak bundan sonraki çalışmaların farklı üniversitelerdeki öğretmen adayları ile gerçekleştirilmesi ve sonuçların bu kapsamda değerlendirilmesi gereklidir. Ayrıca gelecekte yapılacak çalışmalarda öğretmen adaylarının BGF düzeyleri üzerinde etkili olabileceği düşünülen bilgi ve davranış faktörlerini ortaya çıkaracak farklı değişken ve ölçekler eklenerek yeni bir boyut kazandırılabilir. Öğretmen adaylarının BGF gelecek nesilleri etkileyeceğinden BG konusundaki algılarının değişimini belirlemek için bu çalışma gelişimsel olarak tekrarlanabilir. Yapılacak böyle bir çalışmayla öğretmen adaylarının BGF gelişimi dikkate alınarak öğretmen eğitimi programları düzenlenebilir.

Genel olarak araştırma sonuçları dikkate alındığında öğretmen adaylarının BGF arasında çeşitli değişkenlere göre fark bulunmuştur. Yapılan çalışmalarda çok az öğretmenin temel BG konularını öğrettikleri (Pruitt-Mentle ve Pusey, 2010) ya da öğrencilerin temel BG sağlama konularında farkındalıklarının çok düşük olduğu (Tekerek ve Tekerek, 2013) sonuçlarının bulunması okullarda öğrencilere BG konusunda eğitim verilmediği veya öğretmenlerin bu konuda yeterli bilgiye sahip olmadıkları düşünülmektedir. Nitekim NCSA (2011) verilerine göre, öğrencilerin BG bilgilerinin düşüklüğü ve ülkemizde bu alanda yapılan çalışmalarda da benzer sonuçlara ulaşılması (Dijle, 2006; Dijle ve Doğan 2011; KaraoğlanYılmaz vd., 2014; Kaşıkçı, Çağıltay, Karakuş, Kurşun ve Ogan, 2014; Mert vd., 2012; Tekerek ve Mart, 2010; Tekerek ve Tekerek, 2013) bu düşünceyi doğrular niteliktedir.

Bu durumlara göre öğretmen adaylarına BG ve tehditlerine karşı kendilerini nasıl koruyacaklarının öğretilmesi ve bunun yaygınlaştırılması oldukça önemli olurken öğretmen adaylarının BG yönelik yeterli düzeyde bilgilerinin bulunmadıkları ve ders olarak almadıkları düşünülmektedir.

Bu çalışmada karşılaşılan problemlerden birisi BGF ile ilgili olarak ayrı ayrı kişisel, kurumsal ve ulusal seviyede ölçülmesine imkân sağlayacak ölçek, bir model

ve derecelendirme için belirgin standart özelliklerin (kriteri) olmamasıdır. Bu çalışmada BGF belirlenmesi alan yazında yer alan çalışmalarla karşılaştırmalarla yapılmaya çalışılmış ve bu çalışmalarla sınırlı kalınmıştır. Bu durumda BGF belirlenmesinde ilkeler ile bütünleştirilerek değerlendirilmeli, değerlendirmeler kişisel, kurumsal ve ulusal olmak üzere tüm seviyelerde ayrı ayrı belirlenmelidir. **Diğer problem soru tabanlı** BGFD belirleme yaklaşımlarda soruyu hazırlayan uzmanın bilgi birikimi, ilgi alanı, tercihleri vb. gibi parametrelere bağlı olarak ölçümlerde ortaya çıkabilecek subjektif sonuçlar ve hatalı tespitler bulunabilmektedir. Bu sonuçlardan hareketle aşağıdaki öneriler sunulmuştur.

5.2 Öneriler

Eğitim Fakülteleri öğretmen adayları için BG stratejik planlamalar yapılmalı, BGF yeterlilik seviyesi sertifikasyonu ve bunun sınavlarla yapılması gerekli görülmektedir.

BG ve BGF düzeylerinin belirlenmesi çok disiplinli bir yaklaşım gerektirirken bu alanda önemli olan izleme, tespit, öğrenme, uygulama, değerlendirme sürekli gündemde tutularak gün içerisinde kişisel düzeyde uygulamalarla BGF farkındalığın arttırılmasında katkı sağlanabilir.

Farkında olma, davranışlarda değişiklik yapıldığında BG konusunda fayda sağlamaktadır. Davranış değişikliği de ancak sistematik bir yaklaşımla sağlanabilmektedir. Bu durumda BGF eksikliklerin etkin bir şekilde giderilmesine rehberlik etme konularında kazanımlar sağlanmasında ve BGF düzeyleri ölçümüne rehberlik yapacak çalışmaların sayısı artırılmalıdır. Çünkü yetenekler (psikolojik özellik) zamana bağlı olarak, bağımsız ve daha uzun süre geçerliliğini koruyacak yapıya sahip olduğundan yetenekleri temel alan kişisel yeteneklerin değerlendirilmesinde yetenek tabanlı testler, bilgi testleri, görüşmeler vb. farklı yöntemlerle BG etkileyen ön yargı, bilgi ve davranış boyutları ölçülebilir.

Eğitim Fakültelerinde öğretmen yetiştirme programlarında BG konularına ya da derslere yer verilmesinin yararlı olacağı düşünülürken, BÖTE bölümü için zorunlu, diğer öğretmen yetiştirme programları için seçmeli olarak yer almasının BG kullanımı, eğitim verme ve rehberlik yapma yönünden katkı sağlayacağı düşünülmektedir. BG yönelik verilecek eğitimlerin hedeflerinin, içeriğinin, yönteminin belirlenmesinde tüm konu ile ilgili tarafların görüşlerinin alınması ve MEB (2018) BG yönergesinin etkin kullanımı ile verimlilikleri artırılabilir.

Çalışmada kullanılan anketin var olan durumun daha iyi anlaşılması için hedef kitlesi farklı başka çalışmalarda da kullanılması ile elde edilecek farklı örneklemlerin görüşleri ile birleştirilerek öğretmen adaylarının ortak BGF belirlenebilir.

BG ile yapılacak çalışmalarla BG yeterliliği ile siber zorbalık ve siber suçlara maruz kalma, siber dünyanın sosyo-psikolojik özellikler üzerindeki olumlu ve olumsuz etkileri gibi konulara odaklanılmasının güvenli bilgi teknolojisi kullanımının önemine ve nasıl olması gerektiğine yönelik konularda katkı sağlayabileceği düşünülmektedir. Bununla birlikte çağın gerisinde kalmamak teknolojinin nimetlerinden en üst düzeyde faydalanabilmek için başta Eğitim Fakülteleri olmak üzere tüm eğitim ve öğretim kurumlarında gerekli alt yapı ve desteğin sağlanmasının faydalı olacağı değerlendirilmektedir.

KAYNAKÇA

Acılar, A. (2009). İşletmelerde bilgi güvenliği ve örgüt kültürü. *Organizasyon ve Yönetim Bilimleri Dergisi, I* (1), 25-33.

Akay, İ. G. (2014). *Bilgi güvenliği yönetim sistemleri bilgi güvenliği uygulama mülakatları,* Yüksek Lisans Tezi. Bilecik Şeyh Edebali Üniversitesi Sosyal Bilimler Enstitüsü, Bilecik.

Alaca, B. (2008). *Ülkemizde bilişim suçları ve internetin suça etkisi (antropolojik ve hukuk boyutları ile),* Yayınlanmamış Yüksek Lisans Tezi. Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Al-Awadi, M. ve Renaud, K. (2008). *Success factors in information security implementation in organizations.* Paper presented at the IADIS International Conference e-Society, Lisbon, Portugal.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security,* 26(4), 276-289.

Alparslan, E. (2009). *Güvenli Yazılım Geliştirme Modelleri*. Erişim adresi: http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/guvenli-yazilim-gelistirme-modelleri.html

Al-Shehri, Y. (2012). Information security awaraness and culture. *British Journal of Arts and Social Science, 6*(1), 61-69. ISSN:2046-9578.

Altıparmak, Ö. F. (2003). Hikmet ve felsefe ilişkisi. *Harran Üniversitesi İlahiyat Fakültesi Dergisi*, *5*(1), 86-118.

Andress, J. (2011). *The Basic of Information Security.* United State:Elsevier.

Arıtürk, M. (2015). Bilgi güvenliği farkındalığı ve bilgi güvenliğinin karşılaştırılması. *XVII. Akademik Bilişim Konferansı*, Anadolu Üniversitesi, Eskişehir. Erişim adresi: https://ab.org.tr/ab15/ozet/74.html

Arora, M. (2012). E-security ıssues. *International Journal of Computers & Technology*, *3*(2), 301-308.

Aslan Öztezcan, B. (2017). *Bilgi güvenliği farkındalığı üzerine araştırma, Marmara Üniversitesi örneği,* Yayınlanmamış Yüksek Lisans Tezi. Marmara Üniversitesi Sosyal Bilimler Enstitüsü Gazetecilik Anabilim Dalı Bilişim Bilim Dalı, İstanbul.

Aslan, Ö. (2007). *Bilgi toplumunda teknolojinin ve teknoloji politikalarının yeri,* Yayınlanmamış Doktora Tezi. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Awad, E. M. ve Ghaziri, H. M. (2004). *Knowledge Management*. Upper Saddle River, New Jersey: Pearson Education Inernational. 40-41.

Balcı, A. (2015). *Sosyal bilimlerde araştırma yöntem teknik ve ilkeler* (11. Baskı). Ankara: Pegem Akademi Yayınları.

Barber, R. (2001). Social engineering: a people problem? *Network Security*.*7*, 9-11.

Baykara, M., Das, R. ve Karadoğan, İ. (2013). *Bilgi güvenliği sistemlerinde kullanılan araçların incelenmesi*. 1 st International symposium on Digital Forensics and

security, Elâzığ. Erişim adresi: http://perweb.firat. edu.tr/ personel/ yayınları/ fau_721/721_ 80043.pdf

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

Bensghir, T. K. (2008). Kurumsal Bilgi Güvenliği Süreci. Erişim tarihi: 12.02.2019 Erişim adresi: www.erzincan.edu.tr/userfiles/file/stratejidb/guvenlik.ppt

Berberoğlu, B. (2010). Bilgi toplumu ve bilgi ekonomisi yolunda Türkiye ve Avrupa birliği. *Marmara Üniversitesi İ.İ.B.F Dergisi 29*(2), 111-131.

Besnard, D. ve Arief, B. (2004). Computer security impaired by legimate users. *Computers & Security 23*, 253-264.

Beydağlı, E., Kara, M., Bahşi, H. ve Alparslan E. (2009). *Güvenli yazılım geliştirme modelleri ve ortak kriterler standardı.* IV. Ulusal Yazılım Mühendisliği Sempozyumu, İstanbul, 11-17.

Bilek, B. T. (2012). *Bilişim suçları ve üniversite lisans öğrencilerin bilişim suçlarına yönelik görüşleri,* Yayınlanmamış Yüksek Lisans Tezi. Gazi Üniversitesi, Bilişim Enstitüsü, Ankara.

Boğa, U. (2011). *Bilişim suçları ile mücadele yöntemleri*, Yayınlanmamış Uzmanlık Tezi. Radyo Televizyon Üst Kurulu. Ankara.

Burlu, K. (2010). *Bilişimin karanlık yüzü*. Ankara: Nirvana Yayınları.

Büyüköztürk, Ş., Kılıç Çakmak, E., Akgün, Ö. E., Karadeniz, Ş. ve Demirel, F. (2012). *Bilimsel Araştırma Yöntemleri* (13. Baskı). Ankara: Pegem Akademi.

Can, A. (2014). *Spss ile bilimsel araştırma sürecinde nicel veri analizi* (3. Baskı). Ankara: Pegem Akademi.

Canbek, G. (2005). *Klavye dinleme ve önleme sistemleri analiz, tasarım ve geliştirme,* Yayınlanmamış Yüksek Lisans tezi. Gazi Üniversitesi, Ankara.

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

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

Canbek, G. ve Sağıroğlu, Ş. (2007a). Kötücül casus yazılımlar kapsamlı bir araştırma. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, *22*(1), 121-136.

Chen, C. C., Shaw, R, ve Yang, S. C. (2006). Mitigating information security risks by increasing user security awareness: A case study aft an information security awareness' system information technology, *Learning and Performance Journal*, *24*(1), 1-4.

Cisco. (2017). *Cisco 2017 Annual Cyber security Report*.USA. Erişim tarihi: 23.03.2019, Erişim adresi: http://www. cisco. com/c/m/enau/products/security/offers/annual-cyber security-report-2017. html

Civelek, D. Y. (2011). *Kişisel verilerin korunması ve bir kurumsal yapılanma önerisi*, Yayınlanmamış Uzmanlık Tezi. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Bilgi Toplumu Dairesi Başkanlığı, Ankara.

Clarke, G. E. (2011). *Comptia security+ certification study guide* (exam sy0-301). New York: McGraw Hill Professional.

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

Courtney, J. F., Haynes, H. D. ve Paradice, P. B. (2005*). Inquiring organizations: Moving from knowledge management to wisdom,*.Idea Group Inc (IGI), Londra, İngiltere, 91-92.

Cox, A., Connolly, S. ve Currall, J. (2011). Raising information security awareness in the academic setting, *VINE, 31* (2), 11-16.

Çalık, D. ve Çınar, Ö. P. (2009). *Geçmişten günümüze bilgi yaklaşımları bilgi toplumu ve internet*. 14. Türkiye'de İnternet Konferansı Bildirileri, 12-13 Aralık, İstanbul.

Çalışkan, E. (2013). *Zararlı yazılımların etkisinde dijital adli delillerin güvenirliği,* Yayınlanmamış Yüksek Lisans Tezi. İstanbul: Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Çek, E. (2017). *Kurumsal bilgi güvenliği yönetişimi ve bilgi güvenliği için insan faktörünün önemi*, Yayınlanmamış Yüksek Lisans Tezi. İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

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

Çetinkaya, L., Güldüren, C. ve Keser, H. (2017). Öğretmenler için Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması. *Milli Eğitim Dergisi, 216*, 33-52.

Çontar, F. (2013). *Ağ ve yazılım güvenliği*. (6. Basım). İstanbul: Kodlab.

Dedeoğlu, G. (2006). *Bilişim toplum ve etik sorunlar*. Bursa: Alfa Aktüel Yayınları.

Delialioğlu, Ö. (2011). *Bilişim sistemleri güvenliği ve ilgili etik kavramlar*. A. Şentürk (Ed.), Temel Bilgi Teknolojileri ve Bilgisayar Kullanımı. Bursa: Ekin Yayınevi.

Dijle, H. (2006). *Türkiye'de eğitimli insanların bilişim suçlarına yaklaşımı,* Yüksek Lisans Tezi. Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

Dijle, H. ve Doğan, N. (2011). Türkiye'de bilişim suçlarına eğitimli insanların bakışı. *Bilişim Teknolojileri Dergisi, 4*(2). 43-53.

Dimensional Research. (2011). *The risk of social engineering on information security: A Survey of It Professionals*.

Dinçkan, A. (2008). *İş sürekliliği yönetim sistemi kurulumu*. TÜBİTAK, UEKAE. Erişim tarihi: 23.03.2019, Erişim adresi: www.bilgiguvenligi.gov.tr

Doğantimur, F. (2009). *ISO 27001 standardı çerçevesinde kurumsal bilgi güvenliği,* Yayınlanmamış Uzmanlık Tezi. Maliye Bakanlığı Strateji Geliştirme Daire Başkanlığı, Ankara.

Durak, H. ve Seferoğlu, S. S. (2017). *Öğretmenlerin teknoloji kullanım yeterliklerinde etkili olan faktörlerle ilgili bir inceleme.* H. F. Odabaşı, B. Akkoyunlu ve A.

İşman (Ed). Eğitim Teknolojileri Okumaları 2017. (29. Bölüm, ss.537-556). TOJET ve Sakarya Üniversitesi, Adapazarı.

Dülger, M. V. (2004). *Türk ceza hukukunda bilişim suçları*, Yayınlanmamış Yüksek Lisans Tezi. İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul.

Elbahadır, H. (2010). *Hacking interface*. İstanbul: Kodlab,

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.

Ercan, M. (2015). *Kritik altyapıların korunmasına ilişkin belirlenen siber güvenlik stratejileri,* Yayınlanmamış Yüksek Lisans Tezi. Gebze Teknik Üniversitesi SBE, Kocaeli.

Ermiş, K. (2006). Sayısal imza ve elektronik belge yönetimi. *Bilgi Dünyası Dergisi*, *7* (1), 121-146.

Erol, S. E. (2016). *Siber güvenlik farkındalığı için yetenek tabanlı dinamik model,* Yüksek Lisans Tezi. Gazi Üniversitesi. Ankara.

Fraenkel, J. R. ve Wallen, N. E. (2000). *How to design and evaluate research in education.* New York: McGraw-Hill.

Gelişken, U. (2009). *10 adımda bilgisayar güvenliği*. İstanbul: Kodlab yayıncılık.

Gencer, K. (2015). *ISO 27001 kapsamında kurumsal bilgi güvenliğine dinamik bir yaklaşım,* Yayınlanmamış Yüksek Lisans Tezi. Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü. Afyon

Gonzales, J. J. ve Sawicka A. (2002). *A framework for human factors in information security*. WSEAS Int. Conf. on Information Security, 1871-1877, Rio de Janeiro.

Gökmen, Ö. F. (2014). *Bilgisayar ve öğretim teknolojileri eğitimi öğretmen adaylarının bilişim güvenliği eğitimi verebilme yeterliklerinin incelenmesi,* Yayınlanmamış Yüksek Lisans Tezi. Sakarya Üniversitesi Eğitim Bilimleri Enstitüsü, Sakarya.

Gökmen, Ö. F. ve Akgün, Ö. E. (2015). Bilgisayar ve öğretim teknolojileri eğitimi öğretmen adaylarının bilişim güvenliği bilgilerinin çeşitli değişkenlere göre incelenmesi. *Çukurova Üniversitesi Eğitim Fakültesi Dergisi*, *44*(1) 61-84.

Grover, V. ve Davenport, T. H. (2001) General Perspectives on Knowledge Management: Fostering a Research Agenda. *Journal of Management Information Systems, 18* (1), 5-21.

Güldüren, C. (2015). *Yükseköğretim kurumlarındaki öğretim elemanlarının bilgi güvenliği farkındalık düzeylerinin değerlendirilmesi,* Yayınlanmamış Doktora tezi. Ankara Üniversitesi Eğitim Bilimleri Enstitüsü. Ankara.

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

Gülmüş, M. (2010). *Kurumsal bilgi güvenliği yönetim sistemleri ve güvenliği,* Yayınlanmamış Yüksek Lisans Tezi. Yıldız Teknik Üniversitesi Elektrik Mühendisliği Anabilim Dalı, İstanbul

Gündüz, M. Z. (2013). *Bilişim suçların yönelik IP tabanlı delil tespiti,* Yayınlanmamış Yüksek lisans tezi. Fırat Üniversitesi Fen Bilimleri Enstitüsü, Elâzığ.

Güngör, M. (2015). *Ulusal bilgi güvenliği: strateji ve kurumsal yapılanma*, Yayınlanmamış Uzmanlık Tezi. Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı, Ankara.

Hekim, H. ve Başıbüyük O. (2013). Siber suçlar ve Türkiye'nin siber güvenlik politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi, 4* (2), 135-158.

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

Herath, T. ve Rao, H. G. (2009). Protection motivation and deterrence: Aframework for security policy compliance in organisations, *Europan Journal of Information Systems, 18*(2), 106-125.

Huck, S. W. (2012). *Reading statistics and research* (6. Baskı). Boston: Pearson.

İlbaş, Ç. (2009). *Bilişim suçlarının sosyo-kültürel seviyelere göre algı analizi,* Yayınlanmamış Yüksek lisans tezi. Başkent Üniversitesi Fen Bilimler Enstitüsü, Ankara.

Johnson, B. ve Christensen, L. (2000). *Educational Research Quantitative and Qualitative Approaches*. Boston: Allyn and Bacon.

Karacı A., Akyüz H. İ. ve Bilgici G., (2016). Üniversite öğrencilerinin siber güvenlik davranışlarının incelenmesi. *Kastamonu Eğitim Dergisi, 25*(6): 2079-2094.

Karakuzu, Ö. (2015). *Bilgi toplumu dönüşüm sürecinde e-devlet kavramının siber ülke güvenliği açısından değerlendirilmesi,* Yayınlanmamış Yüksek Lisans Tezi. İnönü Üniversitesi Sosyal Bilimler Enstitüsü, Malatya.

Karaoğlan Yılmaz, G., Yılmaz, R. ve Sezer, B. (2014). Üniversite öğrencilerinin güvenli bilgi ve iletişim teknoloji kullanım davranışları ve bilgi güvenliği eğitimine genel bir bakış. *Bartın Üniversitesi Eğitim Fakültesi Dergisi*, *3*(1), 176-199.

Karjalainen, S. (2011). Costumer preferences for feedback on housahold electiricity consumption. *Energy Build, 43,* 67-458.

Kaşıkçı, D. N., Çağıltay, K., Karakuş, T., Kurşun, A. ve Ogan, C. (2014). Türkiye ve Avrupa'daki çocukların internet alışkanlıkları ve güvenli internet kullanımı. *Eğitim ve Bilim, 39*(171), 230-243.

Keleş, M. K. ve A. Güneş, A. (2013). *24 bit renkli dokümanların farklı biyometri teknoloji kullanılarak güvenliğinin sağlanması*. 6.Uluslarası Bilgi Güvenliği ve Kriptoloji Konferansı, 20-21 Eylül 2013, 116-119. Ankara.

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

Kınay, H. (2012). *Lise öğrencilerinin siber zorbalık duyarlılığının riskli davranış, korumacı davranış, suça masumiyet ve tehlike algısı ile ilişkisi ve çeşitli değişkenler açısından incelenmesi*, Yayınlanmamış Yüksek Lisans Tezi. Sakarya Üniversitesi, Sakarya.

Kirrane, D. E. (1999) Getting Wise to Knowledge Management. *Association Management, 51* (8), 31-38.

Kjorvik, H. (2010). *Implementing and improving awareness in information security,* (Yüksek Lisans Tezi, University of Agder, Faculty of Engineering and Science, Grimstad). Erişim adresi: http://brage.bibsys.no/

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

Koç, F. (2008). *BGYS-Varlık Envanteri Oluşturma ve Sınıflandırma Kılavuzu Sürüm1.00.* Kocaeli: TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü.

Koskosas, I. V. ve Paul, R. J. (2004). *The interrelationship and effect of culture and risk communication in setting internet banking security goals*. ICEC '04 6th International Conference on Electronic Commerce, ACM New York, 341-350.

Kritzinger, E. ve Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computer and Security*, 27, 224-231

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

Kuyumcuoğlu, M. ve Başoğlu A. N. (2008). Bilişim sistemlerinde risk yönetimi benimseme modeli. *İstanbul Üniversitesi İşletme Fakültesi İşletme İktisadı Enstitüsü Dergisi*, *19*(61), 143-164.

Mahabi, V. (2010). *Information security awareness: System administrators and end-user perspectives at Florida State University*, Doctoral dissertation. The Florida State University, College of Communication and Information, Florida.

Magklaras, G. ve Furnell, S. (2006). Towards an insider threat prediction specification language. *Information Management & Computer Security, 14*(4), 361-381.

Maiwald, E. (2004). *Fundamentals of network security*. McGraw Hill: Burr Ridge, IL.

Marks, A. (2007). *Exploring Universitesi information systems security awaraness in changing higher education enviroment: a compartive case story research,* PhD Thesis. University of Salford.

Mart, İ. (2012). *Bilişim kültüründe bilgi güvenliği farkındalığı*, Yayınlanmamış Yüksek Lisans Tezi. Kahramanmaraş Sütçü İmam Üniversitesi, FBE, Kahramanmaraş.

Mathisen, J. (2004). *Measuring information security awareness - A survey showing the Norwegian way to do it*, Unpublish Master's thesis. Gjovik University, College Institutionen for Data- och System vetenskap, Hogskolen.

Mc Millian, J. H. ve Schumacher, S. (2001). *Research in education: a conceptual introduction* (5th ed.) New York: Addison Wesley Longman.

Mert, M., Bülbül. H.İ. ve Sağıroğlu. Ş. (2012). Milli Eğitim Bakanlığına bağlı okullarda güvenli internet kullanımı. *TUBAV Bilim Dergisi*, *5*(4), 1-12.

Miller, M. (2003). *Herkes için PC güvenliği ve bilgisayar virüsleri*. (Çev. B. Erol). Alfa Yayınları. İstanbul.

Mitnick, K. D., ve Simon W. L. (2016). *Aldatma Sanatı*. (6. Basım). Ankara: ODTÜ Yayınları.

Montano, B. (2004). *Innovations of Knowledge Management.* Idea Group Inc (IGI), Londra, İngiltere, 302-303.

Muharremoğlu, G. (2013). *Kurumsal bilgi güvenliğinde zafiyet, saldırı ve savunma ögelerinin incelenmesi*, Yayınlanmamış Yüksek Lisans Tezi. İstanbul Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Munro, K. (2005). Social engineering. *Infosecurity Today*, *2*(3), 44.

Mylonas, A., Kastania, A. ve Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, 34, 47-66.

N.C.S.A., (2011) National Cyber Security Alliance State of U.S. Cyber Education, Erişim adresi: http://staysafeonline.org/sites/default/files/resource_documents/Cyber%205.3.11%20PDF. Pdf,

Newby, G. (2002). *Information Security for Libraries*, IGI Global, Pennysylvania. Erişim adresi: http://www.petascale.org/papers/library-security

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

Öğüt, P. (2006). *Küreselleşen dünyada bilgi güvenliğine yönelik politikalar: sayısal imza teknolojisi ve Türkiye,* Yayınlanmamış Yüksek Lisans Tezi. Ankara Üniversitesi, Ankara.

Özcan, B. (2009). *Kurumsal bilgi güvenliği ve COBIT*, Yayınlanmamış Yüksek lisans tezi. Haliç Üniversitesi, Yönetim Bilişim Sistemleri, İstanbul.

Özçiçek, E. Ç. (2009). *İleri-güvenlikli sayısal imza düzeninin uygulanması,* Yayınlanmamış Yüksek Lisans Tezi. Hacettepe Üniversitesi FBE. Ankara.

Özdamar, K. (1999). *Paket programlar ile istatistiksel veri analizi*. Eskişehir: Kaan Kitabevi.

Özdemir, E. (2014). *Kuramdan Uygulamaya Eğitimde Araştırma Yöntemleri*. Ankara: PEGEM Akademi Yayınları.

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

Özler, İ. (2007). *Bilgi güvenliği ve elektronik imza kavramları, ekonomik boyutlarının incelenmesi ve elektronik imza uygulamaları,* Yayınlanmamış Yüksek Lisans Tezi. Dicle Üniversitesi, Diyarbakır.

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

Öztürk, C., Tekerek, M. ve Yılmaz, A. S. (2016). *Bilgi güvenliği endüstrisinin ülkelere göre karşılaştırılması*. 9.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı. Ankara: Bilgi Güvenliği Derneği, 235-243.

Öztürk, H., Yüksek, C. ve Aslan, M. (2014). Bilgi güvenliği politikaları kılavuzu. Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü, Ankara.

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

Pallı, H. (2008). *Türk hukukunda ve mukayeseli hukukta bilişim suçları*, Yayınlanmamış Yüksek Lisans Tezi. Erciyes Üniversitesi Sosyal Bilimler Enstitüsü, Kayseri.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., ve Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAISQ). *Computers & security, 42*, 165-176.

Penmetsa, M. K. (2010). *A methodology for measuring information security maturity in Norwegian and Indian MSME's with special focus on people factor*, Un publish Master's thesis. Gjovik University, College Department of Computer Science and Media Technology, Hogskolen.

Poulsen, K. (2000). Mitnick to lawmakers: People, phones and weakest links. Erişim adresi: http://www.politechbot.com/p-00969.html

Pro-G. (2003). *Bilişim güvenliği. Sürüm 1.1*. Proje Bilişim Güvenliği ve Araştırma San. ve Tic. Ltd. Şti. Erişim adresi: https//:www.pro-g.com.tr/whitepapers/bilişim-guvenligi-v1.pdf

Pruitt-Mentle, D. ve Pusey, P. (2010). *State of k12 cyberethics, safety and security curriculum in US : 2010 Educator opinion.* Educational technology policy, Research and Outreach.

Puhakainen, P. (2006). *A Design theory for information security awareness*. (Un publish Master's thesis), Acta University of Oulu, Faculty of Science Department of Information Processing Science. Erişim adresi: http://jultika.oulu.fi/files/isbn9514281144.pdf

Qureshi, M. S. (2011). *Measuring efficiency of information security policies: a case study of UAE based*, Unpublish Master Thesis. Stockholm University, Swedish.

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

Sağıroğlu, Ş. (2001). *Herkes için etkili bilişim.* Kayseri: Ufuk Kitabevi.

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

Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World*. New York : John Wiley & Sons.

Schuler, A. J. (2003) How to build wisdom and prosper in an "Information age", What's up, Doc? *E-Newsletter, 3*(6): 5-7 (June).

Seferoğlu, S. S., Yıldız-Durak, H., Karaoğlan-Yılmaz, G. ve Yılmaz, R. (2018). *Bilgi güvenliği farkındalığı ve bilgi güvenliği politikalarıyla ilgili bir inceleme*. B.

Akkoyunlu, A. İşman ve H. F. Odabaşı (Ed). Eğitim teknolojileri okumaları 2018, (3. Bölüm, ss. 29-43). TOJET ve Sakarya Üniversitesi, Adapazarı.

Sipahi, B., Yurtkoru, E. S. ve Çinko, M. (2008). *Sosyal Bilimlerde SPSS'le Veri Analizi*. İstanbul: Beta Yayınları.

Siponen, M. T. (2001). Five dimensions of information security awareness. *Computer and Society,* 24-29.

Stanton, J. M., Stam, K. R., Mastrangelo, P. ve Jolton, J. (2005). Analysis of End User Security Behaviors. *Computers and Security, 24*(2), 124-133.

Swaminata, T. M. ve Elden, C. R. (2003). *Wireless Security and Privacy: Best Procties and Design Tecniques*. Boston: Addison-Wesley.

Symantec, (2013). *Internet security threat report*. Erişim adresi: http://www.symantec.com/content/ en/us/ enterprise/other resources/b-ist remain report v18 2012 21231018.en-us.pdf

Şahin, L., Çetin, B. I. ve Yıldırım, K. (2009). Bilişim teknolojilerindeki gelişmelerin işletmelerin strateji ve maliyet üzerine etkileri. *Sosyal Siyaset Konferansları Dergisi*, *56*(1), 547-573.

Şahinaslan, E., Kandemir R. ve Şahinaslan, Ö. (2009). *Bilgi güvenliği farkındalık eğitim örneği*. IV. Akademik Bilişim Konferansı Şubat 2009, Şanlıurfa: Harran Üniversitesi, 1-6.

Şahinaslan, E., Kantürk, A., Şahinaslan, Ö. ve Borandağ, E. (2009). *Kurumlarda bilgi güvenliği farkındalığı, önemi ve oluşturma yöntemleri*. Akademik Bilişim ‹09-XI. Akademik Bilişim Konferansı Bildirileri, 597-602, Şanlıurfa.

Şahinaslan, Ö. (2013). *Siber saldırılara karşı kurumsal ağlarda oluşan güvenlik sorunu ve çözümü üzerine bir çalışma*, Yayınlanmamış Doktora Tezi. Trakya Üniversitesi, Edirne.

T.C. Milli Eğitim Bakanlığı, Bilgi İşlem Dairesi Başkanlığı. (2018) *Milli Eğitim Bakanlığı ve Sistem Güvenliği Yönergesi*. Erişim adresi: http://bidb.meb.gov.tr/meb_iys_dosyalar/2018_06/27173547_Bilgi_ve_Sistem_Guvenligi_Yonergesi_2018.pdf

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

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

Tekerek, M. (2008). Bilgi güvenliği yönetimi. *Kahramanmaraş Sütçü İmam Üniversitesi Fen ve Mühendislik Dergisi, 11*(1), 132-137.

Tekerek, M. ve Mart, İ. (2010). *K8 düzeyi için davranışsal bilgisayar ve internet güvenliği farkındalığı*. 4. Uluslararası bilgi güvenliği ve kriptoloji konferansı bildirileri. 6-8 Mayıs 2010, Orta Doğu Teknik Üniversitesi. Ankara.

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

Tiwana, A. (2002). *Knowledge Management Toolkit: The Orchestrating IT, Strategy, and Knowledge Platforms*, (2nd Edition). New York: Prentice Hall, Upper Saddle River.

Tsohou, A., Kokolakis, S., Karyda, M. ve Kiountouzis, E. (2008). Investigating information security awareness: Research and practice gaps. *Information Security Journal: A Global Perspective*, 207-227.

Türk Dil Kurumu [TDK], (2019). Erişim tarihi: 05.01.2019, Erişim adresi: sozluk.gov.tr

Türkiye Bilimsel ve Teknolojik Araştırma Kurumu [TÜBİTAK], (2018). *Güvenli yazılım geliştirme kılavuzu*, Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi Ankara.

Türkiye Bilimsel ve Teknolojik Araştırma Kurumu [TÜBİTAK], (2019). *Zararlı program ne demektir?* Erişim tarihi: 19.02.2019, Erişim adresi: http://www.bilgimi koruyorum. org.tr/?b311 zararli_program_ne_demektir

Türkiye İstatistik Kurumu [TÜİK] (2017). Türkiye'nin internet kullanım alışkanlıkları. Erişim tarihi: 26.11.2018, Erişim adresi: http://www.tuik.gov.tr/HbPrint.do?it=24862

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

Uslu, T. (2007). *İnternet güvenliği ve risk yönetimi,* Yayınlanmamış Yüksek Lisans Tezi. Kültür Üniversitesi FBE, İstanbul.

Ünver, M. ve Canbay C. (2010). Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik. *Elektrik Mühendisliği Dergisi, 438*, 94-103.

Ünver, M. ve Mirzaoğlu, A.G. (2011). *Yemleme (phishing)*. Bilgi Teknolojileri ve İletişim Kurumu. Ankara

Ünver, M., Canbay C. ve Günaydın Y. (2010). *Köle bilgisayar ve köle bilgisayar ağları (Zombi ve Botnetler)*. BTK Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı, Ankara.

Vardal, N. (2009). *Yükseköğretimde bilgi güvenliği: Bilgi güvenlik yönetim sistemi için bir model önerisi ve uygulaması,* Yayınlanmamış Doktora Tezi). Gazi Üniversitesi, Eğitim Bilimleri Ana Bilim Dalı, Ankara.

Veiga, A. D. (2008). *Cultivating and assessing information security culture*, Doctoral dissertation, University of Pretoria, Faculty of Engineering, Built Environment and Information Technology, Pretoria). Erişim adresi: http://upetd.up.ac.za/ thesis/ available/ etd04242009-165716/

Veseli, I. (2011). *Measuring the effectiveness of information security awareness program*, Unpublish Master Thesis. Gjøvik University College Department of Computer Science and Media Technology, Sweden

Vrooml, C. ve Von Solms, R. (2004). Towards information security behavioural compliance. *Computers and Security, 23*(3), 191-198.

Vural, Y. (2007). *Kurumsal bilgi güvenliği ve sızma (penetrasyon) testleri*, Yayınlanmamış Yüksek Lisans Tezi. Gazi Üniversitesi, Ankara.

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

Vural, Y. ve Sağıroğlu, Ş. (2011). Kurumsal bilgi güvenliğinde güvenlik testleri ve öneriler. *Mühendislik Mimarlık Fakültesi Dergisi, 26*(1), 89-103.

Vural, Y. ve Sağıroğlu Ş. (2007, Ekim). *Kurumsal bilgi güvenliği: güncel gelişmeler*. X. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, 191-199. Ankara.

Wagner A. ve Brooke, C. (2007). Wasting time: The mission impossible with respect to technology-oriented security approaches electronic. *Journal of Business Research Methods, 5*(2), 117-124.

Ward, P. ve L.C. Smith (2002). The development of access control policies for information technology systems. *Computers & Security*, *21*(4), 356–371

Wenger, A., Mauer, V. ve Cavelty M. D. (2008). *The International Handbook on Risk Analysis and Management.* Center for Security Studies, Switzerland: ETH Zürich.

Wright, M. A. ve Kakalık, J. (2007). *Information security: Contemporary cases*. Sudbury Jones and Barlett.

Yaşar, H. ve Çakır, H. (2015). Kurumsal siber güvenliğe yönelik tehditler ve önlemleri. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, *4*(2015), 488-507.

Yavuz, H. ve Ulaş, M. (2013). *Adli bilişime konu olan bilişim suçları ve bilgi güvenliği farkındalık tespiti.* 1. International Symposium on Digital Forensics and Security Proceding Book. Fırat Üniversitesi, Elâzığ.

Yayla, H. G. (2018). *Fatih projesi uygulanan ve uygulanmayan okullardaki öğretmenlerin bilgi güvenliği farkındalığının incelenmesi,* Yüksek Lisans Tezi. Ankara Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.

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

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

Yıldız, M. (2014). *Siber suçlar ve kurum güvenliği*, Yayınlanmamış Uzmanlık Tezi. Ulaştırma Denizcilik ve Haberleşme Bakanlığı Bilgi İşlem Dairesi Başkanlığı, Ankara.

Yılmaz, B. (2013). *E-dönüşüm sistemlerinin bilgi güvenliği açısından incelenmesi e-devlet kullanıcıları üzerine bir araştırma*, Yayınlanmamış Yüksek Lisans Tezi. Marmara Üniversitesi SBE, İstanbul.

Yılmaz, D. (2005). *Hacking: Bilişim Korsanlığı ve Korunma Yöntemleri.* (3. Baskı). İstanbul: Hayat Yayıncılık.

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

Yılmaz, R., Karaoğlan Yılmaz, F. G., Öztürk, H. T. ve Karademir, T. (2017). Lise öğrencilerinin güvenli bilgisayar ve internet kullanımın farkındalıklarının incelenmesi: Bartın ili örneği. *Online Submission, 7(*1), 83-114.

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

EKLER

Ek-1: Kişisel Bilgi Formu ve Öğretmen Adaylarına Yönelik BGF ölçeği

Geleceğin Değerli Öğretmenleri,

"Ondokuz Mayıs Üniversitesi Öğretmen Adaylarının Bilgi Güvenliği Farkındalıklarının Bazı Değişkenler Açısından İncelenmesi'' adlı araştırma kapsamında sizlerin görüş, bilgi ve önerilerinize ihtiyaç bulunmaktadır.

Bilgi güvenliğinize yönelik toplanacak bu bilgiler, bilimsel amaçla kullanılacak ve kesinlikle gizli tutulacaktır. Araştırmanın amacına ulaşmasında en büyük katkıyı siz sağlayacağınızdan aşağıdaki soruları tarafsız, eksiksiz tam ve içtenlikle doldurmanız, araştırmanın sağlıklı ve güvenilir sonuçlara ulaşması açısından son derece önem taşımaktadır.

Lütfen durumunuza uygun olan seçeneği işaretleyiniz ve hiçbir soruyu BOŞ bırakmayınız. Anket soruları dışında araştırmaya yönelik görüş ve önerileriniz varsa anketin sonunda ayrılan bölüme yazmanız bizi son derece memnun edecektir.

Araştırmaya katkılarınız, sabrınız, anlayışınız için teşekkür eder, derslerinizde ve çalışmalarınızda başarılar dilerim. LÜTFEN İSİM YAZMAYINIZ

Nurhan KARAYÜCEL EFE

Cinsiyetiniz	❒Bayan	❒Bay				
Yaşınız	❒18-20	❒21–22	❒ 23–25	❒ 26–28	❒ 29 ve yukarı	
Sınıfınız	❒1	❒2	❒ 3	❒ 4	❒ 5 ve yukarı	
Akademik Not Ort.	❒1,5-2,0	❒2,1 -2,5	❒ 2,6–3,0	❒ 3,1–3,5	❒ 3,6–4,0	
Mezun olduğu Lise	❒Fen Lisesi	❒ Düz (genel)	❒ Anadolu	❒ Meslek	❒ Anadolu Öğretmen	
Yaşadığınız Yer	❒Şehir	❒ İlçe	❒ Kasaba	❒ Köy	❒ Büyük Şehir	
Anne Eğitimi	❒Lise	❒Üniversite	❒ İlköğretim	❒ Yok	❒ Diğer (Lütfen yazınız)	
Anne Mesleği	❒Ev Hanım	❒ Mühendis	❒ Doktor	❒ Memur	❒ Öğretmen	❒ Diğer
Baba Eğitim	❒Üniversite	❒ Lise	❒ İlköğretim	❒ Yok	❒ Diğer (Lütfen yazınız)	
Baba Mesleği	❒ Hukuk	❒ Doktor	❒ Mühendis	❒ Memur	❒ Esnaf	❒Öğretmen
	❒ Çiftçi	❒ İşçi	❒ **İşletmeci**	❒ Serbest	❒ Diğer (Lütfen yazınız)	
Kardeş Sayısı	❒ Yok	❒ 1–2	❒ 3–4	❒ 5–6	❒ 7 ve üzeri	
Öğretmenlik Bölüm	❒ Almanca	❒ Türkçe	❒Matematik	❒ Resim	❒Fen Bilgisi	
	❒ Müzik	❒ Fransızca	❒Bilgisayar	❒ Sınıf	❒ PDR (Rehberlik ve Psikolojik Danışmanlık)	
	❒ Biyoloji	❒ İngilizce	❒ Okul Öncesi	❒ Sosyal	❒ Özel Eğitim	

***Lütfen durumunuza uygun olan seçeneği işaretleyiniz ve hiçbir soruyu BOŞ bırakmayınız. Anket soruları dışında çalışmamıza yönelik görüş ve önerileriniz varsa anketin sonunda ayrılan bölüme yazmanız bizi son derece memnun edecektir.		Kesinlikle katılıyorum (5)	Katılıyorum(4)	Kısmen katılıyorum(3)	Katılmıyorum (2)	Kesinlikle katılmıyorum(1)
1	Bilgi güvenliğinin ne anlama geldiğini biliyorum.	5	4	3	2	1
2	Bilgi güvenliği ile ilgili sorumluluklarımın ne olduğunu biliyorum.	5	4	3	2	1
3	Bilgi güvenliği için şifreleri düzenli değiştirmenin gerekli olduğunu düşünüyorum.	5	4	3	2	1
4	Politika değişimi, yazılım güncellemeleri veya ilave şifreler gibi beni etkileyecek olan bilgi güvenliği değişiklikleri hakkında zamanında bilgilendiriliyorum.	5	4	3	2	1
5	Kullandığım bilgi sistemlerinde tanımlanmış olan kuralları nasıl uygulayacağımı biliyorum.	5	4	3	2	1
6	Yönetim (Okul) tarafından bilgi güvenliği gereksinimleri ile ilgili yeterince bilgilendirildiğimi düşünüyorum.	5	4	3	2	1
7	Güvenlik duvarının (firewall) ne işe yaradığını biliyorum.	5	4	3	2	1
8	Güvenlik duvarı kullanmanın korunmak için kesinlikle yeterli olduğunu düşünüyorum.	5	4	3	2	1
9	Çocukların bilgisayarı güvenli kullanmaları için yapılması gerekenleri biliyorum.	5	4	3	2	1
10	Kişisel verilerimi nasıl korumam gerektiğini biliyorum	5	4	3	2	1
11	İş ile ilgili verilerimi nasıl korumam gerektiğini biliyorum.	5	4	3	2	1
12	Kötü niyetli yazılımın (malware) ne olduğunu biliyorum.	5	4	3	2	1
13	Kötü niyetli yazılımlara karşı alınması gereken güvenlik tedbirlerini biliyorum.	5	4	3	2	1
14	Aldatmaca (hoax) nedir biliyorum.	5	4	3	2	1
15	Zincir e-postalara (chain e-mail) karşı nasıl hareket etmem gerektiğini biliyorum.	5	4	3	2	1
16	Casus yazılım (spyware) nedir biliyorum.	5	4	3	2	1
17	Bilgisayarımda casus yazılım olup olmadığını anlayabilirim.	5	4	3	2	1
18	Bilgisayarıma casus yazılım yüklenmesinin engelleme yöntemlerini biliyorum.	5	4	3	2	1
19.	Kimlik hırsızlığına karşı alınması gereken güvenlik tedbirlerini biliyorum.	5	4	3	2	1
20	Sahte virüs koruma yazılımının ne olduğunu biliyorum.	5	4	3	2	1
21	Hizmet aksatma (Denial of Service- DOS) saldırısı nedir biliyorum.	5	4	3	2	1
22	Kimlik avı (phishing) saldırısı nedir biliyorum.	5	4	3	2	1
23	Sosyal mühendislik saldırısı nedir biliyorum.	5	4	3	2	1

24	Sosyal mühendislik saldırısına uğramamak için nasıl hareket etmem gerektiğini biliyorum.	5	4	3	2	1
25	Siber zorbalık (cyber bullying) nedir biliyorum.	5	4	3	2	1
26	Siber zorbalığa karşı kendimi nasıl koruyacağımı biliyorum.	5	4	3	2	1
27	Siber zorbalığa karşı çocukları nasıl koruyacağımı biliyorum.	5	4	3	2	1
28	Kişisel dijital yardımcıların maruz kalabileceği saldırılara karşı alınması gereken güvenlik tedbirlerini biliyorum.	5	4	3	2	1
29	Web sayfalarında kullanılan aktif içeriğin ne işe yaradığını biliyorum.	5	4	3	2	1
30	Web sayfalarında kullanılan çerezlerin (cookies) ne işe yaradığını biliyorum.	5	4	3	2	1
31	Dijital imza (digital signature) nedir biliyorum.	5	4	3	2	1
32	Şüpheli veya bilinmeyen kaynaklardan gelen özellikle eklentisi olan e-postaları açmanın taşıdığı riski biliyorum.	5	4	3	2	1
33	E-posta gönderirken "Gizli" (BCC) alanının sağladığı avantajları biliyorum.	5	4	3	2	1
34	İstenmeyen elektronik posta (spam) nedir biliyorum.	5	4	3	2	1
35	İstenmeyen elektronik posta miktarını azaltmak için gerekli bilgiye sahibim.	5	4	3	2	1
36	Sosyal ağ sitelerini güvenli olarak nasıl kullanacağımı biliyorum.	5	4	3	2	1
37	USB sürücülerini kullanırken dikkat edilmesi gereken hususları biliyorum.	5	4	3	2	1
38	Taşınabilir cihazlara yönelik fiziksel güvenliği sağlamak ile ilgili dikkat edilmesi gereken konuları biliyorum.	5	4	3	2	1
39	Taşınabilir cihazlara yönelik veri güvenliği ile ilgili dikkat edilmesi gereken konuları biliyorum.	5	4	3	2	1
40	Cep telefonlarının maruz kalabileceği saldırılara karşı alınması gereken güvenlik tedbirlerini biliyorum.	5	4	3	2	1
41	Kablosuz ağların güvenliği ile ilgili alınması gereken tedbirleri biliyorum.	5	4	3	2	1
42	İnternete bağlanabilen cihazlarla seyahat ederken dikkat edilmesi gereken konuları biliyorum.	5	4	3	2	1
43	Kişisel mahremiyet nedir biliyorum.	5	4	3	2	1
44	Bilgi güvenliği konusunda yasal sorumluluklarımı biliyorum.	5	4	3	2	1
45	Bilgi güvenliği konusunda sorun yaşadığımda kime ve nereye başvuracağımı biliyorum.	5	4	3	2	1
46	İnternette gezinirken mahremiyetimi korumak için alınması gereken tedbirleri biliyorum.	5	4	3	2	1
47	Çevrimiçi güvenli alışveriş yapmak için gerekli olan güvenlik tedbirlerini biliyorum.	5	4	3	2	1

48	Mavi diş (Bluetooth) teknolojisi ile veri aktarımı konusunda bilgi sahibiyim.	5	4	3	2	1				

Evde bilgisayarınız var mı?	☐ Yok	☐ Varsa kaç yıldır	☐ 1 yıldan az	☐ 1-2Yıl	☐ 3-4 Yıl	☐5-6 Yıl	☐7-8 Yıl	☐9-10 Yıl	☐10'dan fazla yıl
Evde senin dışında bilgisayar kullanmayı bilen var mı?					☐Evet	☐Hayır	☐ Kısmen		
Evde İnternet bağlantınız var mı?					☐Var	☐Yok			
Araştırmayı en fazla nerede yaparsınız			☐İnternette		☐ Kütüphane		☐ Diğer (Lütfen yazınız)		
İnternet kullanım ile karşılaştığınız en önemli zorluklar	☐İnternet erişiminin çok yavaş olması		☐İnternet erişiminin pahalı olması		☐Aranılan bilgiye ulaşamamak		☐İnternet kullanımı karışık ☐Bilgisayar kullanım zorluğu		
İnternet sitelerine nasıl ulaşırsınız?	☐Arkadaş tavsiyesi		☐Web site linkleri takip ederek		☐Arama motorları ☐Reklamlar		☐Bilgisayar dergi linkleri ☐ Diğer (Lütfen yazınız)		
İnternete bağlanma yeriniz	☐Cep telefonu		☐İnternet kafe		☐Yurt	☐Ev	☐ Okul	☐ Diğer (Lütfen yazınız)	
İnterneti kullanma süresi	☐1 yıldan az		☐1-2 yıl		☐3-4	☐5-6	☐7-8	☐ 9 yıldan fazla	
Bilgiye ulaşmak için en çok kullanan kişi ve araçlar	☐İnsanlar ☐TV		☐İnternet ☐ Dergi		☐Gazete ☐ Radyo		☐ Hepsi ☐ Diğer (Lütfen yazınız)		
İnterneti bir hafta içinde kaç saat kullanırsınız?	☐0-5 saat		☐6-10 saat		☐ 11-15 saat	☐ 16-20 saat	☐ 21-25 saat	☐ 36- 40 saat	☐ 41 fazla
E-postalarınızı kontrol süreniz	☐Ayda bir ☐Ayda birkaç kez		☐Haftada bir ☐Haftada birkaç kez		☐Günde bir ☐Günde birkaç kez		☐E-posta kullanmıyorum		
İnterneti kullanma amacınız	☐Eğitim / araştırma ☐Oyun/Eğlence		☐Sosyal /arkadaş ☐Çevrimiçi eğitim		☐Alışveriş ☐Bankacılık		☐İletişim ☐Diğer	☐Haber alma	
İnternetin sizin için en büyük problemi nedir?	☐Yayın hakları ☐İnternet suçlar		☐Bilgi doğruluğu ☐Uygunsuz yayınlar		☐Gizlilik ☐Hız		☐Herkese eşit erişim hakk ☐Diğer(Lütfen yazınız)		

Hayatınızda/yaşamınızda İnternet ve bilgisayar olmasaydı neler değişirdi. Görüşlerinizi Buraya Yazabilirsiniz

1-

2-

3-

4-

5-

Ek-2: BGFÖ İzin Talebi ve Onay Yazısı (Elektronik Posta)

> E-MAİL fkaraer@omu.edu.tr
>
> fergankaraer@hotmail.com
>
> Adres:
>
> Ondokuz Mayıs Üniv. Matematik ve Fen Bilimleri Bölümü Fen Bilgisi
> ABD
>
> Kurupelit Samsun

> 0362 3121919/5909

-Sayın Dr. Fergan Karaer,

Geliştirmiş olduğumuz "Öğretmenler İçin Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ)"ni yüksek lisans öğrenciniz tez çalışmasında kullanabilirsiniz. Ölçeği ve gerekli bilgileri Dr. Öğretim Üyesi Can Güldüren size mail aracılığıyla gönderecektir.
Çalışmanızla ilgili ihtiyaç duyduğunuz konularda destek sağlayabiliriz. Böylesine önemli bir konuyu sizin de çalışma alanınızın içine katmanız beni ayrıca memnun etti. Araştırma tamamlanınca sonucundan haberdar ederseniz sevinirim.
İyi çalışmalar dilerim.

Prof. Dr. Hafize KESER
Ankara Üniversitesi, Eğitim Bilimleri Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü
Cebeci Kampüsü,06590, Cebeci/ANKARA/Türkiye
Tel.: 0(312)3633350/3216, Faks: 0(312)3636145

Kolay gelsin.
İyi çalışmalar....

****

Can GÜLDÜREN
Dr.Öğr.Üyesi
Bilgisayar Teknolojileri Bölümü
Ofis : +90 312 586 7488
Ufuk Üniversitesi, İncek, Ankara, Türkiye

---- Forwarded Message ----
From: Can GÜLDÜREN <canguldoren@yahoo.com>
To: fkaraer@omu.edu.tr <fkaraer@omu.edu.tr>
Cc: Prof. Dr. Hafize KEŞER <hafize.keser@ankara.edu.tr>; Prof. Dr. Hafize KEŞER <hafizekeser@yahoo.com.tr>
Sent: Monday, November 19, 2018, 12:55:52 PM GMT+3
Subject: Ölçek Kullanım İzni

Sayın Dr. Fergan Karaer,
istemiş olduğunuz ölçek içeriğini ekte sizinle paylaşıyorum.

Ölçek Açıklamaları

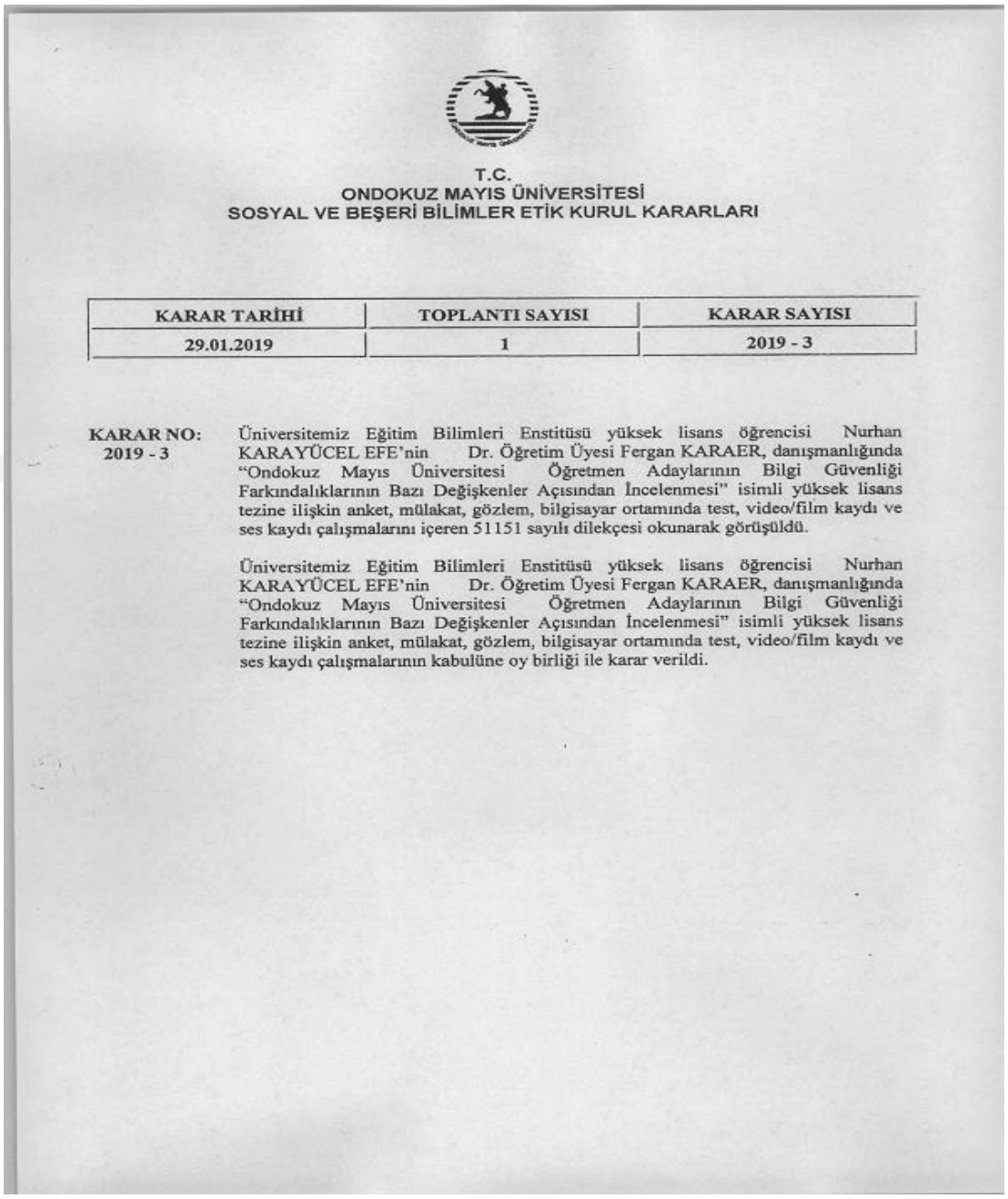
Ölçek öğretmenler üzerinde geliştirilmiştir. Ölçekte ters kodlanmış madde yoktur. Ölçek toplam puanı ve alt faktörlere ilişkin puanlar artıkça, katılımcıların Bilgi Güvenliği Farkındalığı artmaktadır.

Bilgi Güvenliği Ölçek Faktör Yapısı: Genel Güvenlik: 1-13, Saldırı ve Tehditler: 14- 30, Mobil Cihazlar, Mahremiyet ve İletişim: 31-48

İletişim:
Prof. Dr. Hafize KESER, keser@ankara.edu.tr,
Yrd. Doç. Dr. Can GÜLDÜREN, canguldoren@yahoo.com
Dr. Levent ÇETİNKAYA, cetinkayalevent@gmail.com

Kaynakça:
Çetinkaya, L., Güldüren, C., & Keser, H. (2017). Öğretmenler İçin Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması [Development of Information Security Awareness Scale (Isas) for Teachers]. *Millî Eğitim dergisi [National Education Sciences], 216*, 33-52. https://dhgm.meb.gov.tr/yayimlar/dergiler/Milli_Egitim_Dergisi/216.pdf

Ek-3a: Ondokuz Mayıs Üniversitesinin İzin Yazıları



T.C.
ONDOKUZ MAYIS ÜNİVERSİTESİ
SOSYAL VE BEŞERİ BİLİMLER ETİK KURUL KARARLARI

KARAR TARİHİ	TOPLANTI SAYISI	KARAR SAYISI
29.01.2019	1	2019 - 3

KARAR NO: 2019 - 3

Üniversitemiz Eğitim Bilimleri Enstitüsü yüksek lisans öğrencisi Nurhan KARAYÜCEL EFE'nin Dr. Öğretim Üyesi Fergan KARAER, danışmanlığında "Ondokuz Mayıs Üniversitesi Öğretmen Adaylarının Bilgi Güvenliği Farkındalıklarının Bazı Değişkenler Açısından İncelenmesi" isimli yüksek lisans tezine ilişkin anket, mülakat, gözlem, bilgisayar ortamında test, video/film kaydı ve ses kaydı çalışmalarını içeren 51151 sayılı dilekçesi okunarak görüşüldü.

Üniversitemiz Eğitim Bilimleri Enstitüsü yüksek lisans öğrencisi Nurhan KARAYÜCEL EFE'nin Dr. Öğretim Üyesi Fergan KARAER, danışmanlığında "Ondokuz Mayıs Üniversitesi Öğretmen Adaylarının Bilgi Güvenliği Farkındalıklarının Bazı Değişkenler Açısından İncelenmesi" isimli yüksek lisans tezine ilişkin anket, mülakat, gözlem, bilgisayar ortamında test, video/film kaydı ve ses kaydı çalışmalarının kabulüne oy birliği ile karar verildi.

Ek-3b: Ondokuz Mayıs Üniversitesinin İzin Yazıları

T.C.
ONDOKUZ MAYIS ÜNİVERSİTESİ
Eğitim Fakültesi Dekanlığı

Sayı : 98725097-100-E.31368 12/03/2019
Konu : Nurhan KARAYÜCEL EFE'nin Tez Uygulama Çalışması Hk.

EĞİTİM BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

İlgi : 11/03/2019 tarihli ve 42301062-100-E.30466 sayılı yazınız.

Enstitünüz Matematik ve Fen Bilimleri Eğitimi Anabilim Dalı Fen Bilgisi Eğitimi Bilim Dalı yüksek lisans öğrencisi Nurhan KARAYÜCEL EFE'nin, "Öğretmen Adaylarının Bilgi Güvenliği Farkındalıklarının Bazı Değişkenler Açısından İncelenmesi" konulu tez çalışmasını Fakültemiz lisans programında öğrenim gören öğrencilerimize uygulama talebi Dekanlığımız tarafından uygun görülmüştür.
Bilgilerinize rica ederim.

e-imzalıdır
Prof. Dr. Seher BALCI ÇELİK
Dekan V.

Adres: Eğitim Fakültesi Dekanlığı Kurupelit/Samsun
Telefon: 0362 312 19 19 Faks: 0362 457 60 78
Elektronik Ağ: http://www.omu.edu.tr/
Arzu TOPUZ

ÖZGEÇMİŞ

Adı ve Soyadı: Nurhan KARAYÜCEL EFE

Doğum Tarihi: 06.07.1986

İletişim Bilgileri: 0505 038 94 61

E-posta Adresi: n.karayucel@gmail.com

Öğrenim Durumu:

Derece	Bölüm/Program	Üniversite	Yıl
Lisans	Eğitim Fakültesi Fen Bilgisi Öğretmenliği	OMÜ	2009
Yüksek Lisans	Eğitim Bilimleri Enstitüsü	OMÜ	2009-