T.C.
İSTANBUL ÜNİVERSİTESİ CERRAHPAŞA
ADLİ TIP VE ADLİ BİLİMLER ENSTİTÜSÜ

Danışman
Prof. Dr. H. Bülent ÜNER

TÜRKİYE'DE BİLGİ GÜVENLİĞİ ALGISININ İSTATİSTİKSEL ANALİZİ

FEN BİLİMLERİ ANABİLİM DALI
YÜKSEK LİSANS TEZİ

HALİME CEYLAN

İSTANBUL, 2019

İstanbul, 09 Eylül 2019

İSTANBUL ÜNİVERSİTESİ-CERRAHPAŞA
ADLİ TIP ve ADLİ BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ
FEN BİLİMLERİ ANABİLİM DALI BAŞKANLIĞINA

Lisansüstü Öğretim Yönetmeliğinin 36.maddesi uyarınca Enstitünüz Fen Bilimleri Anabilim Dalı'nın yüksek lisans öğrencisi Halime CEYLAN'ın

"Türkiye'de Bilgi Güvenliği Algısının İstatiksel Analizi"

Adlı tezi jürimizce tetkik edilmiş ve kendisine tez savunması yaptırılmıştır.

Yukarıda adı geçen tezin ve tez savunmasının kabul edilmesine oy birliğiyle karar verilmiştir.

Prof. Dr. H. Bülent ÜNER
Jüri Başkanı
Danışman

Prof. Dr. İmdat ELMAS
Üye

Doç. Dr. Hüseyin ÇAKAN
Üye

Dr. Öğr. Üyesi Belma GÖLGE
Üye

Dr. Öğr. Üyesi Selda MERCAN
Üye

ÖNSÖZ

Tez çalışmam süresince bilgi ve tecrübeleriyle beni yönlendiren danışman hocam sayın Prof. Dr. H. Bülent ÜNER'e,

Değerli fikirleri ve yönlendirmeleriyle araştırmamda önemli katkıları olan ve tanımaktan onur duyduğum Doç. Dr. Gökhan ERSOY'a,

Tez sürecinde tüm idari konularda bana her türlü kolaylığı sağlayan öğrenci işlerinde görevli Mehmet SALDIRAN'a,

Ölçek geliştirme aşamasındaki katkılarından dolayı iş arkadaşlarıma,

Hayatım boyunca maddi ve manevi hiçbir desteği esirgemeyen anne ve babama teşekkürlerimi borç bilirim.

İÇİNDEKİLER

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR

AFA	Açımlayıcı Faktör Analizi
BÖTE	Bilgisayar ve Öğretim Teknolojileri Eğitimi
DFA	Doğrulayıcı Faktör Analizi
DoS	Denial of Service
DVGFÖ	Dijital Veri Güvenliği Farkındalık Ölçeği
KMO	Kaiser-Meyer-Olkin
PDA	Personal Digital Assistant (Kişisel Dijital Asistan)
SPSS	Statistical Package for Social Sciences
YEM	Yapısal Eşitlik Modeli

ÖZET

Her gün yeni teknolojik gelişmeler ortaya çıkmakta ve bilgi toplumu olma yolunda hızlı adımlar atılmaktadır. Bunun sonucunda bilgi ve iletişim teknolojileri yaşantımızın vazgeçilmez bir parçası halini almaktadır. Bu teknolojilerin hayatımızda birçok kolaylık sağlamasının yanı sıra birtakım riskleri barındırdığı da bir gerçektir. Bu risklere karşı farkındalık sağlanması ve alınacak birtakım tedbirlerle kontrol altında tutulması önemlidir. Aksi takdirde bilişim sistemleri, bilişim suçları için açık hedef haline gelmektedir. Bunun için de öncelikle kişilerin bilgi güvenliği farkındalık seviyelerinin belirlenmesi, yetersiz bulunan konuların tespiti ve alınacak önlemler açısından önemlidir.

Bu çalışmada bilgi ve bilişim teknolojileriyle sürekli iç içe olan bilişim sektörü çalışanlarının bilgi güvenliği farkındalıklarını ölçmeye yönelik 35 maddeden oluşan ve Cronbach alfa güvenilirlik değeri 0.906 bulunan bir ölçek geliştirilmiştir. Ayrıca bu ölçek vasıtasıyla elde edilen verilerin analizi yapılarak bilgi güvenliği farkındalığının yaş, cinsiyet, eğitim düzeyi ve mesleki tecrübeye göre değişiklik gösterip göstermediği araştırılmıştır. Bunun sonucunda yaş ve mesleki tecrübe arttıkça bilgi güvenliği farkındalığının arttığı görülmüştür. Cinsiyet ve eğitim düzeyinin ise bilgi güvenliği farkındalığı üzerine anlamlı bir etkisi olmadığı sonucuna varılmıştır. Ayrıca bilişim sektörü çalışanlarının farkındalık düzeylerinin düşük olduğu alanlar tespit edilmiş ve bu alanlardan gelebilecek risklere karşı hangi önlemler alınabileceğinden bahsedilmiştir.

Anahtar Kelimeler: Bilgi, Bilgi Güvenliği, Farkındalık, Bilişim Suçları, Ölçek Geliştirme

ABSTRACT

New technological developments are emerging every day and fast steps are being taken towards becoming an information society. As a result, information and communication technologies become an indispensable part of our lives. It is a fact that these technologies have many risks in addition to providing many convenience in our lives. It is important to raise awareness of these risks and to keep them under control with some measures to be taken. Otherwise, information systems are becoming clear targets for information crimes. For this purpose, first of all it is important to determine the information security awareness level of the people, to determine the issues that are found to be insufficient and to take precautions.

In this study, a 35-item scale with a Cronbach alpha reliability value of 0.906 was developed to measure the information security awareness of the information sector employees who are constantly intertwined with information and information technologies. In addition, the data obtained through this scale was analyzed to determine whether information security awareness varies according to age, gender, education level and professional experience. As a result, it was seen that information security awareness increased with increasing age and professional experience. It was concluded that gender and education level had no significant effect on information security awareness. In addition, the areas where the awareness level of the IT sector employees are low have been identified and what measures can be taken against the risks that may arise from these areas have been mentioned.

Keywords: Information, Information Security, Awareness, Cyber Crimes, Scale Development

1.Giriş ve Amaç

Son yıllardaki gelişmelerle birlikte bilgi ve iletişim teknolojileri hayatımızın ayrılmaz bir parçası haline gelmiştir. Günlük işlerimizi kolaylaştırmış, daha az zaman ve emek harcayarak daha çok iş yapabilmemize imkan tanımıştır. Doğru ve yeterli bilgiye kolaylıkla erişebilme imkanı sunmuştur. Bilgi ve iletişim teknolojilerinin günlük hayatımızın her aşamasında yoğun olarak kullanılması, sağladığı avantajların yanı sıra bir takım güvenlik risklerini de beraberinde getirmiştir. Bu risklere karşı önlem alınmaması bilişim suçlarına elverişli bir ortam hazırlamaktadır. Bilişim suçlarına maruz kalmamak için bu risklerin birtakım tedbirlerle kontrol altında tutulması gerekir.

Bilgi teknolojilerine yönelik riskler teknoloji ya da kullanıcı kaynaklı olabilmektedir. Ancak teknik açıdan ne kadar önlem alınırsa alınsın, kullanıcıların bilinçsiz ya da dikkatsiz kullanımı, bütün bu önlemleri geçersiz kılabilmekte ve çok ciddi güvenlik sorunlarıyla karşı karşıya kalınabilmektedir. Bu noktada kullanıcılarda bilgi güvenliği konusunda farkındalık oluşturulması ve bu farkındalığın davranışa dönüşmesi büyük önem taşımaktadır.

Kullanıcılarda farkındalık geliştirilebilmesi için, öncelikle mevcut durumun analiz edilmesi ve hangi konularda eksiklikler olduğu tespit edilmelidir.

Bilgi ve iletişim teknolojileri ile günlük hayatlarında sürekli iç içe olan bilişim sektörü çalışanlarının bilgi güvenliği farkındalıkları büyük önem taşımaktadır. Bu çalışmada bilişim sektörü çalışanlarının bilgi güvenliği farkındalıklarının ölçülmesi hedeflenmiştir.

Tez çalışmasının'Genel bilgiler' kısmında konuyla ilgili genel kavramlar ve bilgi güvenliğine yönelik tehditlerin neler olduğu incelenmiş, bilgi güvenliğine yönelik işlenen bilişim suçlarından bahsedilmiş ve konuyla ilgili daha önceden yapılmış benzer çalışmalar incelenmiştir.

'Gereç ve Yöntem' bölümünde bilişim çalışanlarının bilgi güvenliği farkındalıklarını ölçmeye yönelik 35 madde ve 9 faktörden oluşan geçerli ve güvenli bir 'Bilgi Güvenliği Farkındalığı Ölçeği' geliştirilmiştir. Daha sonra ölçek aracılığıyla elde edilen verilerin istatistiksel analizi yapılarak Türkiye'deki bilişim çalışanlarının bilgi güvenliği farkındalıklarının

-Yaş,

-Cinsiyet,

-Öğrenim derecesi ve

-Bilişim sektöründeki deneyim yılı

değişkenlerine bağlı olarak değişiklik gösterip göstermediği incelenmiştir. Ayrıca bilişim çalışanlarının bilgi güvenliği farkındalık seviyelerinin düşük olduğu konular saptanmıştır.

Çalışmanın 'Bulgular' bölümünde, ölçek aracılığıyla toplanan verilerin istatistiksel analizi ile elde edilen sonuçlar detaylı bir şekilde açıklanmıştır.

'Tartışma' başlığı altında, elde edilen bulgular yorumlanmış ve daha önceki yapılmış olan çalışmalarla kıyaslanarak sonuçlardaki benzerlik ve farklılıklar ortaya konulmuştur.

Tez çalışmasının ‘Sonuç’ bölümünde ise bu çalışmanın ana fikri ve öneminden bahsedilmiş, ileride yapılacak çalışmalar için öneriler sunulmuştur.

2.Genel Bilgiler

2.1. Kavramlar

90'lı yıllara kadar sadece basılı-yazılı ortamlarda bulunan bilgi, önce bilgisayarların keşfi, daha sonra da internetin keşfiyle elektronik ortamlara taşınmıştır. Günümüzde ise, bilgisayar, tablet, akıllı telefon, kişisel dijital asistan (PDA) gibi cihazlar ve bulut bilişim teknolojileri diye tabir edilen sanal ortamlar yardımıyla bilginin üretilmesi, saklanması ve taşınması çok daha kolay hale gelmiştir. Tüm bu teknolojiler sağladıkları birçok avantajın yanında bir takım risk ve tehditleri de beraberinde getirmiştir.

Bu bölümde öncelikle veri, bilgi ve bilgi güvenliği gibi bu çalışma kapsamındaki terimlerin tanımları yapılacak, sonrasında ise yukarıda bahsedilen teknolojilerin getirdiği tehditler kısaca açıklanacaktır.

2.1.1. Genel kavramlar

Veri: Bilişim teknolojileri açısından, bir durum hakkında aralarında bağlantı kurulmamış bilinenlerdir. Diğer bir deyişle, sayısal ortamlardaki bit dizeleri veri olarak adlandırılmaktadır (1).

Bilgi: Verilerin bir anlam ifade edecek şekilde düzenlenmiş şeklidir. İşlenmiş veri olarak da ifade edilebilir. Kısaca, veri üzerinde uygulanan bütün işlemlerin sonucu bilgi olarak tanımlanabilir (1).

Bilişim: İnsanoğlunun iletişimde kullandığı bilginin özellikle elektronik makineler vasıtasıyla düzenli ve akla uygun bir şekilde işlenmesi bilimidir (2).

Bilgi teknolojileri: Bilgilerin toplanması, işlenmesi ve gerektiğinde herhangi bir yere iletilmesi veya bu bilgilere erişilmesini elektronik, optik, bilgisayar yongası gibi araçlarla kendiliğinden sağlayan teknolojiler bütünüdür (3).

Bilgi Güvenliği: Bilginin göndericiden alıcıya ulaşana kadar gizlilik içerisinde, bozulmadan, değişmeden ve başka kişilerce ele geçirilmeden güvenli bir şekilde iletilmesi sürecidir (4).

ISO 270001'e göre, bilgi güvenliği ile korunması gereken bilgilerin özelliklerinden üçü şunlardır:

-**Gizlilik:** Yalnızca yetkili tarafların bilgileri görebilmesini sağlar.

-**Bütünlük**: Bilgilerin doğru olmasını ve yetkisiz kişilerin veya kötü amaçlı yazılımların bu verileri değiştirmemesini sağlar.

-**Kullanılabilirlik**: Verilerin yetkili kullanıcılar tarafından erişilebilir olmasını sağlar (5).

Bilgi güvenliği farkındalığı: Bilgi güvenliğini riske atan davranışlar ve bu davranışlara karşı nasıl önlem alınabileceğini içeren güvenlik politikalarının bilincinde olunması durumuna denir (6).

2.1.2. Bilgi güvenliğine yönelik tehditler

Zararlı Yazılımlar: Bu yazılımlar bulaştığı cihazlardaki donanım ve dosyalara zarar veren, yazılımların ayarlarında değişiklik yapan, bilgisayardaki verileri izinsiz bir şekilde başkalarına gönderen veya bilgisayarı yabancıların erişimine açan kötücül yazılımlardır.

En yaygın zararlı yazılımlar; virüsler, solucanlar (worm), truva atları (trojan horse), arka kapılar (backdoor), mesaj sağanakları (spam), klavye dinleme sistemleri (keylogger), casus yazılımlar (spyware) ve botnet olarak belirtilebilir (7).

En çok rastlanan zararlı yazılımlar aşağıda kısaca açıklanmıştır.

- **Virüs:** Bilgisayarlar, mobil cihazlar, sunucu ve bilgi sistemleri üzerinde çalışan işletim sistemi ve uygulama yazılımlarına kendini kopyalayarak yayılır. İnternet ve taşınabilir kayıt ortamları ile dağılır. Bilgi hırsızlığı, engelleme, bozma ve zarar vermeye yöneliktirler (8).

- **Solucanlar:** Worm türü zararlılar olarak adlandırılırlar ve ağ sistemi üzerinde çok yoğun veri trafiği oluştururlar. Hedefleri diğer bilgisayarlara yayılmak ve işletim sistemi zafiyetlerini kullanmaktır. Yayılmak için kullanıcının dosya açmasına gerek duymazlar (8).

- **Truva Atları:** Kullanıcının haberi olmadan arka planda işleyen bu programlar sistem internete bağlıyken dışarı veri aktarırlar. Truva atları genelde indirilen müzik, dosya ve programlarla cihazlara yüklenmekte ya da e-posta aracılığıyla kullanıcılara ulaşmaktadır (9).Diğer bir şekilde ifade edecek olursak, kullanıcısına faydalı bir

araç, dosya gibi görünen, yüklendiğinde şifreler, kurgulanmış özel kişisel bilgiler toplayan, sistem dosyalarını silebilen zararlı yazılımlardır (8).

- **Arka Kapılar: N**ormalde gerekli olan kimlik kanıtlama süreçlerini atlamayı ya da kurulan bu yapıdan bilgisi olan art niyetli kişilere o bilgisayara uzaktan erişim sağlayan yöntemlere denilmektedir (10).

- **Mesaj Sağanakları (Spam):** İnternet üzerinde aynı mesajın çok sayıdaki kopyasının, bumesajı almak için bir talepte bulunmamış kişilere ısrarla gönderilmesine spam denir. Spam mesajlar genellikle ticari reklam amaçlıdır (9).

- **Tuş kaydediciler (Keylogger):** Keylogger programların içine gizlenerek kullanıcının bilgisayarına kendi bilgisi haricinde yüklenen programlardır. Program kullanıcının bilgisayarında aktifleştiği an itibariyle klavye ile yazılan her şey kaydedilir, raporlanır ve bu rapor bu yazılımı derleyen ya da yazan kötü amaçlı kişilere gönderilir. Böylelikle kullanıcının bilgisayarından yaptığı tüm e-posta, bankacılık ve finans şifreleri ele geçirilebilmektedir (9).

- **Casus yazılım (Spyware):** Kullanıcılara ait önemli bilgilerin ve kullanıcıların yaptığı işlemlerin, kişinin bilgisi olmadan toplanmasını ve bu bilgilerin art niyetli kişilere gönderimini sağlayan yazılımlardır. Casus yazılımları, virüs ve solucanlardan ayıran özelliği, hedef sisteme bir kere bulaştıktan sonra kendini kopyalayarak daha fazla yayılmaya ihtiyaç duymamalarıdır (11).
- **Botnet:** Saldırganların internet kullanıcılarının sistemlerine zararlı yazılımlar yüklemesiyle oluşan bot adında birçok bilgisayarın oluşturduğu ağ sistemine botnet

denir. Art niyetli kişiler oluşturdukları botnet ağı vasıtasıyla tek merkezden dünyanın farklı yerlerindeki bilgisayarları (istenmeyen e-posta göndererek, virüs yayarak, sunucu sistemlere saldırarak v.b.) kendi amaçlarına göre yönetebilmektedirler (12).

Sahte antivirüs yazılımları: Bilgisayarlara zarar vermek niyetiyle yazılan fakat kendilerini birer virüs koruma yazılımı ya da casus yazılımları önleme aracı gibi gösteren yazılımlardır. Çoğunlukla bilgisayarınızda virüs tespit edildiği ve bu virüsleri temizlemek için (bir linke tıklayarak) bir program indirmeniz gerektiği şeklindeki mesajlarla bulaşırlar. Başka bir yöntem de e-posta aracılığıyla sahte antivirüs programının linkini kullanıcıya göndererek kullanıcının bu yazılımı yüklemesi sağlanır (12).

Servisi Engelleyen Saldırılar (Denial of Service: DoS): Bu saldırı çeşidinde sistemdeki programlara virüs bulaşmaz. Fakat sistem kapasitesini aşacak şekilde yüklenerek kullanılamaz duruma getirilir. Örnek olarak, 10 dakika içinde 200.000 e-posta gelmesiyle e-posta hizmeti veren sunucu iş yapamaz duruma gelebilmekte ve sistem bilinen ifadesiyle "çökebilmektedir" (13).

Bilişim korsanlığı (Hacking): Hack, izinsiz olarak sisteme girme, sistemin işleyişini kontrol etme, sistemdekiverilerden bilgi sahibi olma veya sistemin işleyişini durdurmadır (9).

Zincir E-posta ve İnternet Aldatmacası (Hoax):Zincir e-posta birçok kişi tarafından birbirine gönderilen ve kişilerin ilgisini çekebilecek e-postaları alıcının listesindeki başka kişilerle paylaşmasını talep eden iletilerdir. İnternet aldatmacası, bir kurum, kuruluş ile ilgili gerçek dışı haber üreterek zarar vermek amacıyla yapılır. Bu e-postalar güvenilir kaynaktan gelmiş gibi gönderilir ve alıcının bu e-poatayı listesindeki bütün herkesle paylaşması istenir.

Zincir e-postalar ve internet aldatmacalarının asıl amacı; e-postaların mümkün olduğunca fazla kişiye ulaşması ve bu e-posta adreslerini toplamayı sağlamaktır. Bu yöntemle elde edilen e-posta adresleri başka kişilere satılmakta ya da istem dışı (spam) e-posta göndermede kullanılmaktadır(14).

Sosyal Mühendislik: İnsanların zaaflarından yararlanarak, çeşitli yöntemlerle önemli bilgileri ele geçirmeye çalışmaktır. Kişilerin karar verme süreçlerini değiştirmeye yönelik teknikler içerir (15).

Sosyal mühendislikte en fazla kullanılan yöntem oltalama (phishing) yöntemidir.

- **Oltalama (Phishing):** Kişilerin önemli bilgilerini (şifre, kredi kartı numarası vs.)elde etmek amacıyla sahtekarlarca hazırlanan bir yöntemdir. Örneğin, sahte giriş ekranları oluşturularak kişilerin önemli bilgileriyle bu ekrana giriş yapmaları sağlanır. (13).

2.2. Bilgi Güvenliği İhlalinden Doğan Adli Vakalara Örnekler

Bu bölümde Türkiye'de ve dünyada bilgi güvenliği ihlalinden doğan adli vakalara örnekler verilecektir.

2.2.1.Türkiye'den bilgi güvenliğine yönelik işlenen bilişim suçlarına örnekler

İhlas Haber Ajansı'nın 2015 yılında yaptığı bir habere göre 'Ortam Sanal Suç Gerçek' adlı kitabın da yazarı olan bilişim suçları uzmanı İsa Altun'un kredi kartı bilgileri ele geçirilmiş ve hesabından 3 bin 450 TL çekilmiştir. Dolandırıcıların ATM'ye yerleştirdikleri bir düzenek ile İsa Altun'un kredi kart bilgileri ele geçirilmiştir (16). Uzmanlık alanı bilişim suçları olan bir

kişinin bile bu suça maruz kalması dolandırıcıların bu konuda ne derece ilerlemiş olduklarını göstermektedir.

2018 yılında yapılan bir habere göre Ankara'dan Önder Tandoğaç, internetten banka hesabına girildiğini ve 5 bin 499 TL'lik alışveriş yapıldığını belirterek şikâyetçi oldu. Ankara Cumhuriyet Başsavcılığı Bilişim Suçları Bürosu paranın QR kod (dijital barkod) okutularak çekildiği tespit etti ve para çekimi sırasında kullanılan cep telefonu numarası belirlendi. Telefon üzerine kayıtlı olan Meral Yıldırım ifade için getirildi. Yıldırım, telefonu 14 yaşındaki oğlunun kullandığını, parayı çeken kişinin de o olabileceğini söyledi. U.U. savcılıktaki ifadesinde internette bir oyun grubunda Aytaş Selim Nazlıer (20) ve Çağdaş Turhan (20) ile tanıştığını, "Bankaların sahte internet sitelerini oluşturup, Facebook üzerinden insanlara gönderdiklerini, kimlik ve müşteri bilgileriyle hesaptan para transferi yaptıklarını söylediler. Yazılıma meraklı olduğum için kabul ettim. Kendileri bankaların sahte internet sitelerini oluşturacak, ben de parayı çekecektim. Para karşılığında bana 50-100 TL arasında ödüyorlardı." dedi. 14 yaşında olduğu için serbest bırakıldı, izini kaybettirdi (17).

Kayseri Adliyesi Cumhuriyet Savcısı Nezafet Salman, kendilerine intikal eden ve 50'den fazla kişinin mağdur olduğu bir bilişim suçuna dikkat çekti. Lise ikinci sınıf öğrencisi olan suçlunun, 50'den fazla çocuğun bilgisayarına internet aracılığıyla program göndererek bilgisayara takılı haldeki kameraları sensörlü bir talimatla çalıştırdığını, odasında rahatça hareket eden çocuğun fotoğraflarını çektiğini ve bu lise ikinci sınıf öğrencinin en az 10 ayrı bilişim suçu işlediğini tespit ettiklerini belirtti (18).

Yukarıdaki iki haber göstermektedir ki, teknolojiye meraklı olan çocuklar ve gençler bilişim suçlusu olabilmektedir.

Anadolu Ajansı tarafından yapılan bir habere göre, Eski 1. Ordu Komutanı emekli Orgeneral Hurşit Tolon kendisini polis olarak tanıtan kişilerce dolandırıldı. Müşteki Hurşit Tolon kendisini Çankaya İlçe Emniyet Müdürlüğünde terörle mücadele grup amiri Menderes Utku olarak tanıtan kişinin, hesabından terör örgütlerine para yatırıldığını ve bankaya gitmesi gerektiğini söylediğini aktardı. Telefondaki kişinin kendisi ve yakınlarının tüm kimlik ve hesap bilgilerine sahip olduğuna dikkati çeken Tolon, adının Hıssan Al Jesem olduğunu sonradan öğrendiği kişi tarafından 12 bin 620 dolar dolandırıldığı şeklinde beyanda bulundu. Aralarında emekli Orgeneral Hurşit Tolon'un da bulunduğu 8 kişiyi toplam 400 bin lira dolandıran biri Suriye uyruklu 2 zanlı tutuklandı (19).

2.2.2.Dünyadan bilgi güvenliğine yönelik işlenen bilişim suçlarına örnekler

Jonathan James isimli hacker 16 yaşındayken ABD savunma bakanlığındaki bilgisayarlardan birine arka kapı (backdoor) programı yerleştirerek bilgi çalmıştır. Daha sonra ise NASA(Uluslar arası Uzay İstasyonu) bilgisayarlarından yaklaşık 1.7 milyon dolar değerinde yazılım çalmıştır. NASA'nın sızıntıyı araştırmak için üç hafta boyunca tüm sistemi kapatmasına sebebiyet vermiştir. 25 yaşına geldiğinde ise birçok yüksek profilli şirketin bilgilerinin çalınması olaylarında şüpheli olarak gösterilince intihar etmiştir (20).

Gerçek ismi Adrian Lamo olan fakat internet kafe ve kütüphaneleri kullanarak bilişim suçlarını işlemesi nedeniyle "Evsiz hacker" olarak bilinen kişi New York Times, Microsoft, Yahoo! ve Bank of America'nın sistemlerine girerek bilgilerini çalmıştır. Lamo, 2010 yılında Amerika Askeri Yetkililerine Amerikan askeri Bradley Manning'in Wikileaks'e bilgi sızdırdığını ihbar etmiştir. 37 yaşında şüpheli bir şekilde hayatını kaybetmiştir. Ölümünün ardında ABD ordusuyla ilgili öğrendiği gizli bilgilerin olduğu düşünülüyor (21).

Bu iki haber, en yüksek güvenlikli şirketlerin ve kurumların bile bilişim açıkları olabileceği ve bu açıklardan faydalanan kötü niyetli kişilerin saldırıları dolayısıyla çok büyük zararlarla karşılaşabileceğini göstermektedir.

2.3. Türkiye'de Bilişim Suçları İle İlgili Kanunlar

Türk Ceza Kanunu'nun konuyla ilgili maddeleri özetle aşağıdaki şekildedir (22) :

TCK (Bilişim Suçları)

Madde 243- Bilişim sistemlerine yetkisiz erişim suçu

Madde 244 -Sistemi engelleme, bozma, erişilmez kılma, verileri yok etme ya da değiştirme suçu

Madde 245 - Kredi Kartı suçları ve bankaya karşı işlenen suçlar.

TCK (Bilişim Vasıtalı Suçlar)

Madde 124 - Haberleşmenin engellenmesi

Madde 132 - Haberleşmenin gizliliği ihlal edilmesi

Madde 133 - Kişiler arası konuşmaların dinlenmesi ve kayda alınması

Madde 135 - Kişisel verilerin kaydedilmesi

Madde 136 - Verileri hukuka aykırı olarak verme veya ele geçirme

Madde 142 - Nitelikli Hırsızlık

Madde 158 - Nitelikli Dolandırıcılık

2.3.1.Bilişim suçları

Bilişim Sistemlerine Girme Suçu:

Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir (TCK m.243/1).

Bilişim sistemine girme fiili nedeniyle sistemin içerdiği veriler yok olur veya değişirse, 6 aydan 2 yıla kadar hapis cezasına hükmolunur (TCK m.243/3).

Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır (TCK m.243/4) (23).

Sistemi Engelleme, Bozma, Erişilmez Kılma, Verileri Yok Etme Veya Değiştirme Suçu:

Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır (TCK m.244/1).

Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır (TCK m.244/2).

Yukarıdaki fiillerin (TCK m.244/1-2) bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır (TCK m.244/3).

Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki

yıldan altı yıla kadar hapis ve beş bin güne kadar adli para cezasına hükmolunur (TCK m.244/4) (23).

Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu:

Başkasına ait banka veya kredi kartını her ne suretle olursa olsun ele geçiren kimse, kart sahibinin rızası olmadan kendisi kullanarak veya başkasına kullandırtarak menfaat elde eder veya elde edilmesine imkan sağlarsa işlediği bu bilişim suçu nedeniyle 3 yıldan 6 yıla kadar hapis ile birlikte beş bin güne kadar adli para cezası ile cezalandırılır (TCK m. 245/1).

Başkasına ait banka hesaplarıyla ilişkilendirerek sahte banka veya kredi kartı üreten, satan veya satın alan kişi işlediği bilişim suçu nedeniyle 3 yıldan 7 yıla kadar hapis ve 10 bin güne kadar adli para cezası ile cezalandırılır (TCK m. 245/2).

Sahte olarak üretilen veya sahtecilik yapılarak değiştirilen bir banka veya kredi kartını kendisine haksız kazanç elde etmek üzere kullanan kişi işlediği bilişim suçu nedeniyle 4 yıldan 8 yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır (TCK m. 245/3) (23).

2.3.2.Bilişim vasıtalı suçlar

Haberleşmenin Engellenmesi Suçu:

Kişiler arasındaki haberleşmenin hukuka aykırı olarak engellenmesi halinde, altı aydan iki yıla kadar hapis veya adlî para cezasına hükmolunur (TCK m. 124/1).

Kamu kurumları arasındaki haberleşmeyi hukuka aykırı olarak engelleyen kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır(TCK m. 124/2).

Her türlü basın ve yayın organının yayınının hukuka aykırı bir şekilde engellenmesi halinde, ikinci fıkra hükmüne göre cezaya hükmolunur(TCK m. 124/3) (24).

Haberleşmenin Gizliliği İhlali:

Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis veya adlî para cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, verilecek ceza bir kat arttırılır(TCK m. 132/1).

Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır (TCK m. 132/2).

Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın hukuka aykırı olarak alenen ifşa eden kişi, bir yıldan üç yıla kadar hapis veya adlî para cezası ile cezalandırılır(TCK m. 132/3) (24).

Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması:

Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır(TCK m. 133/1).

Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır(TCK m. 133/2).

Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa eden kişi, iki yıldan beş yıla kadar hapis ve dört bin güne kadar adlî para cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur(TCK md. 133/3) (24).

Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme:

Kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçunun cezası 2 yıldan 4 yıla kadar hapis cezasıdır (TCK m. 136) (24).

Nitelikli Hırsızlık:

TCK 142.madde 2.fıkra (e) bendine göre ‘Suçun bilişim sistemlerinin kullanılması suretiyle işlenmesi hâlinde, beş yıldan on yıla kadar hapis cezasına hükmolunur.’(24)

Nitelikli dolandırıcılık:

TCK 158.madde 1.fıkra (f) bendine göre ‘Dolandırıcılık suçunun bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi halinde üç yıldan on yıla kadar hapis ve beş bin güne kadar adli para cezasına hükmolunur.’ (24)

2.4. Bilgi Güvenliği Farkındalığı ile İlgili Ulusal ve Uluslararası Çalışmalar

2.4.1. Bilgi güvenliği farkındalığı ile ilgili ulusal çalışmalar

2010 yılında Gizem Öğütçü tarafından hazırlanan "E-Dönüşüm Sürecinde Kişisel Bilişim Güvenliği Ve Farkındalığının Analizi**"** isimli tez çalışması kapsamında geliştirilen ölçek Başkent üniversitesi akademik ve idari personeli ile öğrencilere uygulanmıştır(25). Analiz sonuçlarına göre, internet kullanım süresi arttıkça riskli davranış gösterme olasılığı artmaktadır. Güvenlikle ilgili bir eğitim almanın farkındalığı artırdığı sonucuna varılmıştır. Kişilerin çoğunluğunun kişisel bilgilerinin başkaları tarafından kötü amaçla kullanılabileceğinin bilincinde olduğu gözlenmiştir. Ayrıca, çalışma sonucunda öğrencilerin, akademik ve idari personele kıyasla riske daha açık oldukları görülmüştür.

Mehmet Tekerek ve Adem Tekerek'in (2013) ilköğretim ve lise öğrencilerinin bilgi güvenliği farkındalığını ölçmek için Kahramanmaraş'ta öğrenim gören 2449 öğrenciye uyguladığı 'Bilgi ve Bilgisayar Güvenliği Farkındalık Ölçeği' analiz sonuçlarına göre, kız öğrencilerin erkeklere göre daha yüksek farkındalık oranına sahip olduğu ortaya çıkmıştır(26).

Çalışmanın sonucunda, öğrencilerin etik konularda farkındalık düzeylerinin yeterli olduğu, ancak, güvenli şifre kullanımı, güvenli sanal iletişim, zararlı yazılımlar, belge koruma, kişisel bilgisayar güvenliği gibi bilgi gerektiren konularda farkındalıklarının düşük olduğu sonucuna ulaşılmıştır.

Merve Arıtürk'ün 2014 yılında yaptığı "bilgi farkındalığı ve bilgi güvenliğinin karşılaştırılması" isimli çalışmada programlama dersi alan mühendislik fakültesi

öğrencilerine uyguladığı anketin analiz sonuçlarına göre, kadınların bilgi güvenliği tutumlarının erkeklere göre daha yüksek olduğu sonucuna varılmıştır(27). Ayrıca ankete katılanların %55'inin internette görülebilecek sorunlara/tehditlere karşı doğru davranış sergilediği, %50'sinin bilgi sorularının çoğunluğunu doğru cevapladığı görülmüştür.

"Üniversite Öğrencilerinin Güvenli Bilgi ve İletişim Teknolojisi Kullanım Davranışları ve Bilgi Güvenliği Eğitimine Genel Bir Bakış" (2014) başlıklı çalışmalarında Gizem Karaoğlan Yılmaz, Ramazan Yılmaz ve Barış Sezer, üniversite 1.sınıf öğrencilerden nitel ve nicel gözlemler yoluyla veri toplamışlardır(28). Bu verilerin analizi sonucunda, öğrencilerden çoğunun antivirüs programı kullandığı ancak antivirüs programlarını düzenli olarak güncellemedikleri bilgisine ulaşılmıştır. Ayrıca öğrenciler arasında korsan yazılım kullanımının yaygın olduğu sonucuna ulaşılmıştır. Öğrencilerin yedekleme ve şifre kullanımı konusunda da farkındalık seviyelerinin düşük olduğu gözlenmiştir. Buna göre, öğrencilerin yaklaşık olarak yarısı kullanıcı adı ve şifre gerektiren ortamlarda aynı kullanıcı adı ve şifreyi kullanmaktadır.

"Kişisel Veri Güvenliği Ve Kullanıcıların Farkındalık Düzeylerinin İncelenmesi" (2014) başlıklı çalışmasında Hakan Çetin, "Kişisel Veri Güvenliği Farkındalığı" anketi geliştirmiş, geliştirdiği bu anketi Antalya ilinde 526 kişiye uygulamıştır(29). Bu anketlerden 501 tanesi değerlendirmeye uygun bulunmuş ve sonuçlar analiz edilmiştir. Buna göre, kadınların farkındalık düzeylerinin erkeklere oranla daha yüksek olduğu görülmüştür. Katılımcıların bilgisayarlarında antivirüs programı kullanma konusuna önem verdikleri ancak tablet ve akıllı telefonlarında antivirüs programı kullanma konusunda aynı özeni göstermedikleri tespit edilmiştir. Ayrıca katılıcıların ancak yarısının güvenlik duvarı kullandığı sonucuna ulaşılmıştır.

Eray Yılmaz (2015), "Öğretmenlerin Dijital Veri Güvenliği Farkındalığı" isimli doktora tezinde, Balıkesir ilinde görevli 1446 öğretmene uyguladığı Dijital Veri Güvenliği Farkındalığı Ölçeği (DVGFÖ) sonuçlarını analiz ettiğinde, erkeklerin kadınlara göre farkındalıklarının daha yüksek olduğu sonucuna ulaşmıştır(30). Günlük bilgisayar kullanma süresi ve günlük internet kullanma süresi arttıkça farkındalığın da arttığını gözlemlemiştir. Branş, mesleki deneyim ve öğrenim durumunun ise farkındalık düzeyi üzerinde bir etkisi olmadığı sonucuna ulaşmıştır. Ayrıca, öğretmenlerin en yüksek farkındalığa sahip oldukları konuların, parola güvenliği ve e-posta yoluyla gelen kimlik doğrulama mesajları olduğu, en düşük farkındalığa sahip oldukları konuların ise güvenlik duvarı yazılımları, internet sitelerinde kullanılan güvenlik sertifikaları ve bulut depolama uygulamaları olduğu sonucuna varmıştır.

"Bilgisayar ve Öğretim Teknolojileri Eğitimi Öğretmen Adaylarının Bilişim Güvenliği Bilgilerinin Çeşitli Değişkenlere Göre İncelenmesi" (2015) isimli çalışmalarında Ömer Faruk Gökmen ve Özcan Erkan Akgün, Sakarya, Amasya, Erzincan ve Siirt üniversitelerinin BÖTE bölümünde okuyan 3. ve 4. Sınıf öğrencilere "Bilişim Güvenliği Bilgisi" anketini uygulamıştır. Elde edilen sonuçlara göre, öğrencilerin bilişim güvenliği bilgilerinin düşük olduğu anlaşılmıştır. Erkek öğrencilerin bilişim güvenliği bilgilerinin kadın öğrencilere göre daha yüksek olduğu sonucuna varmıştır. Ayrıca öğrencilerin bilişim güvenliği bilgilerinin; yaş, sınıf, bilgisayara sahip olma süresi, günlük bilgisayar kullanma süresi, günlük internet kullanma süresi ve bilgi güvenliği ile ilgili bir ders ya da kurs alınıp alınmaması durumuna göre farklılaşmadığı görülmüştür(31).

Can Güldüren tarafından 2015'te hazırlanan "Yükseköğretim Kurumlarındaki Öğretim Elemanlarının Bilgi Güvenliği Farkındalık Düzeylerinin Değerlendirilmesi " isimli tez

çalışmasında yükseköğretim kurumlarında çalışan öğretim elemanlarının bilgi güvenliği farkındalık seviyelerini belirlemek amacıyla bir ölçek geliştirilmiş ve bu kişilere bilgi güvenliği farkındalığı kazandırmak amacıyla bir web sitesi geliştirilmiştir. Bu web sitesi üzerinden 65 katılımcıya 12 hafta süresince bilgi güvenliği farkındalık eğitimi verilmiştir ve bu web sitesinin öğretim elemanlarına bilgi güvenliği farkındalığı kazandırmada etkili olduğu, uygulamadan sonra bilgi güvenliği farkındalığı konusunda bilinçlendikleri görülmüştür(32).

Can Güldüren, Levent Çetinkaya ve Hafize Keser tarafından "Ortaöğretim Öğrencilerine Yönelik Bilgi Güvenliği Farkındalık Ölçeği Geliştirme Çalışması" (2016) başlıklı makalelerinde, geliştirilen ölçekte Keser ve Güldüren tarafından 2015'te geliştirilen ölçekten farklı olarak 2 yerine 3 faktör yapısı oluştuğundan bahsedilmiştir. Önceki geliştirilen ölçekte 'Saldırı ve Tehditler' ve 'Kişisel Verilerin Korunması' faktörleri oluşurken, bu ölçekte bu iki faktöre ek olarak 'Mahremiyet' faktörü de oluşmuştur. Ölçeğin analizi sonucunda, ortaöğretim kurumlarındaki erkek öğrencilerin kız öğrencilere oranla farkındalık oranlarının daha yüksek olduğu görülmüştür(33).

Yrd. Doç. Dr. Zülfiye Bıkmaz tarafından hazırlanan "Sağlık Yönetimi Bölümü Öğrencilerinin Mobil Güvenlik Farkındalığı ve Dijital Veri Güvenliği" (2017)isimli çalışmanın sonucunda, en yüksek farkındalığın cihazlara parola konulması gerektiği konusunda, en düşük farkındalığın ise internet sitelerinde kullanılan güvenlik sertifikaları konusunda olduğu görülmüştür. Yaş, cinsiyet ve bilgi teknolojileri kullanım deneyiminin farkındalık düzeyleri üzerinde anlamlı bir etkisi olmadığı sonucuna varılmıştır(34).

Ayrıca, öğrencilerin %86,8'inin güvenlik yazılımlarının gerekli olduğunu düşündüğü, %61,8"inin akıllı telefonlar için güvenlik yazılımlarından haberdar olduğu ve %42,6"sının akıllı cihazlarında güvenlik için bir yazılım kullandığı sonucuna ulaşılmıştır.

Çalışmada, öğrencilerin %72,1'i uygulama yüklerken kişisel verilere erişim izni isteyip istemediğine dikkat ederken, %69,1'inin kişisel verilerine erişim izni istendiğinde uygulamayı indirmekten vazgeçtiği sonucuna ulaşılmıştır.

Bilgi güvenliği farkındalığı ile ilgili Türkiye'de yapılan çalışmalara bakıldığında daha çok yükseköğretim kurumlarındaki öğrenci, idari personel ve akademik personel ile ortaokul ve lise öğrencileri ve öğretmenlerine yönelik çalışmalar yapıldığı görülmektedir. Bilişim çalışanlarının bilgi güvenliği farkındalığına yönelik bir çalışmaya rastlanmamıştır.

2.4.2. Bilgi güvenliği farkındalığı ile ilgili uluslararası çalışmalar

Chan ve Mubarak (2012), Güney Avustralya'da Yüksek Öğretim Kurumu çalışanlarının bilgi güvenliği farkındalığını ölçmek amacıyla anket çalışması yapmışlardır (35). Bu çalışmanın sonucunda bilgi güvenliği farkındalık seviyesinin oldukça düşük olduğu sonucuna ulaşmışlardır. Özellikle sosyal mühendislik ve oltalama konularında katılımcıların farkındalık seviyesinin çok düşük olduğu görülmüştür. Katılımcıların şifre güvenliği konusunda da farkındalıklarının yeterli seviyede olmadığı, şifrelerini başkalarıyla paylaşmakta sakınca görmedikleri anlaşılmıştır. İstenmeyen e-postalar konusunda ise farkındalık seviyeleri yüksek çıkmıştır.

Aloul (2012), okullarda, üniversitelerde, kamu ve özel sektörde bilgi güvenliği farkındalığının önemini anlatan bir çalışma hazırlamıştır (36). Bu çalışmayı hazırlarken 2010 yılında Birleşik Arap Emirlikleri'nde öğrenciler ve uzmanlar üzerinde yapılan bir araştırmadan yararlanmıştır. Çalışmanın sonunda ise etkili ve başarılı bir bilgi güvenliği farkındalığı programı geliştirmek için gereken önemli faktörlerin üzerinde durmuştur.

Alzamil (2012) Suudi Arabistan'daki bilgi teknolojileri çalışanlarının bilgi güvenliği farkındalığına yönelik bir çalışma yapmıştır (37). Bu çalışmanın sonucunda, katılımcıların bilgi güvenliğinin önemini bildiklerini, ancak, tehditlerin sadece dış kaynaklı olabileceğini düşündükleri ve gerekli önlemleri almadıkları için güvenlik açıkları oluştuğu kanısına varmıştır. Özellikle iş arkadaşlarıyla bilgi alışverişinde bulunurken, kör bir güven ve tedbirli olmama durumlarında güvenlik açıkları ortaya çıkmaktadır. Ayrıca eğitimin bilgi güvenliği üzerindeki etkisini kabul etmelerine rağmen, çoğu kurumun bilgi güvenliği eğitim programlarını öncelikli olarak görmedikleri sonucuna ulaşılmıştır.

Kim (2013) üniversite öğrencilerinin bilgi güvenliği farkındalıklarını ölçmek amacıyla bir çalışma yapmıştır (38). Buna göre, en yüksek farkındalık seviyesi önemli dosyaları şifreleme konusundadır. Bunu sırayla antivirüs programı kullanımı ve şifreleri düzenli olarak değiştirme konuları takip etmektedir. Öğrencilerin e-posta eklerini açma konusunda ise en düşük farkındalık düzeyine sahip oldukları sonucuna varılmıştır.

Farook ve diğerleri, 2015'te üniversite öğrencilerinin bilgi güvenliği farkındalığını analiz etmek amacıyla Finlandiya'da bir yükseköğretim kurumu olan Turku Üniversitesi'nde bir anket çalışması yapmışlardır (39). Bu çalışmadan elde edilen veriler analiz edildiğinde cinsiyet ve bilgi güvenliği ile ilgili eğitim alıp almamanın bilgi güvenliği farkındalığı üzerinde anlamlı bir etkisinin olduğu; yaş, uyruk, eğitim düzeyi gibi faktörlerin ise dikkate değer bir etkisinin olmadığı sonucuna ulaşılmıştır.

Durkovic ve Milosevic (2018) tarafından hazırlanan çalışmada, Sırbistan'daki belediyeçalışanlarının bilgi güvenliği farkındalıkları ölçülmüş ve çalışanlarını farkındalık

düzeylerinin yeterli olduğu sonucuna ulaşılmıştır (40). Ayrıca yaş değişkeninin, farkındalık seviyeleri üzerinde dikkate değer bir etkisi olmadığı anlaşılmıştır.

Yurtdışında yapılan çalışmalar incelendiğinde, yalnızca Alzamil tarafından 2012'de Suudi Arabistan'da bilişim sektörü çalışanlarının bilgi güvenliği farkındalığını ölçmeye yönelik bir çalışma yapılmış olduğu görülmektedir.

Genel durum değerlendirildiğinde, Türkiye'de bilişim sektöründe çalışanların bilgi güvenliğini farkındalığını ölçmeye yönelik olan bu çalışmanın literatürdeki eksikliği gidereceği düşünülmektedir.

3.Gereç ve Yöntem

3.1. Materyal

Bu çalışmada bilişim sektörü çalışanlarının bilgi güvenliği farkındalıklarını ölçmek amacıyla Bilgi Güvenliği Farkındalığı Ölçeği geliştirilmiştir.

3.1.1. Örneklem belirleme

Ölçek oluşturma aşamasında kapsamlı araştırmalar sonucu ve alanında uzman 5 kişinin görüşleri alınarak bir 72 soruluk bir madde havuzu oluşturulmuştur. Daha sonra bu madde havuzundan aynı yargıyı ölçmeye yönelik olduğu düşünülen benzer maddeler atılmıştır. Bu işlemin ardından maddelerin ifadenin netliği ve ölçek yapısına uygunluğu açısından incelenmesi için 2 faklı bilgi güvenliği uzmanının görüşüne başvurulmuştur. Bütün bu incelemelerin sonunda 4 adet demografik verileri ölçme amaçlı soru, 5 adet evet/hayır tipi soru ve 40 maddelik 5'li likert tipi sorulardan oluşan bir ölçek elde edilmiştir. Likert tipi sorularda seçenekler 'Kesinlikle Katılıyorum', 'Katılıyorum', 'Kararsızım', 'Katılmıyorum' ve 'Kesinlikle Katılmıyorum' şeklindedir.

Oluşturulan bu maddeler Google Formlar aracılığıyla bilişim çalışanlarına gönderilmiştir.
Ölçeğe toplam 200 bilişim çalışanı tarafından katılım sağlanmıştır. Katılımcılar bilişim sektörünün farklı alt dallarında çalışmaktadır. Yazılım, donanım, veri bilimci, bilgisayar ve öğretim teknolojileri öğretmenliği bunlardan birkaçıdır. Ayrıca katılımcıların sektördeki unvan ve kıdemleri de teknisyen, uzman, mühendis, analist, proje yöneticisi, müdür, öğretmen, web tasarımcı olmak üzere çeşitlilik göstrmektedir.

3.1.2. Geçerlik ve güvenirlik analizleri

Ölçeğin yapı geçerliliğini belirlemek amacıyla açımlayıcı faktör analizi (AFA) yöntemi uygulanmıştır. Barlett testi yapılmış ve KMO değerine bakılmıştır. Faktör analizi için varimax yöntemi kullanılmıştır. Faktör analizinin sonrasında maddeler toplam açıklanan varyansı %62.76 olan 9 faktör altında toplanmıştır. Ölçekten 5 madde eş yükleme ve faktör yükü 0,4'den düşük olduğu için çıkartılmıştır. Bilgi Güvenliği Farkındalığı Ölçeği'ndeki 35 madde için "Cronbach Alpha" hesaplaması yapılmıştır. Ölçeğin güvenirliği 0.906 bulunmuştur. Bulunan Cronbach alfa değeri ve açıklanan varyans değerine bakıldığında Bilgi Güvenliği Farkındalığı Ölçeği'nin geçerli ve güvenilir olduğu görülmüştür.

Ölçeğin faktör yapısı Tablo I'de verilmiştir.

TabloI. Bilgi Güvenliği Farkındalığı Ölçeği Faktör Yapısı

Boyut	**Faktör Yükü**	**Madde Analizi**
Sosyal Paylaşım Güvenliği (Özdeğer=8,647; Açıklanan Varyans=8,734; Alpha=0,811)		
Tanımadığım kişileri ağıma eklemem	0,891	0,711
Tanımadığın kişilerin ağına eklenmekten çekinirim	0,827	0,661
Sosyal ağ hesaplarının e-posta adres defterini taramasına izin vermem	0,656	0,588
İnternet ortamında iletişim bilgilerimi/kişisel bilgilerimi paylaşmam	0,631	0,593

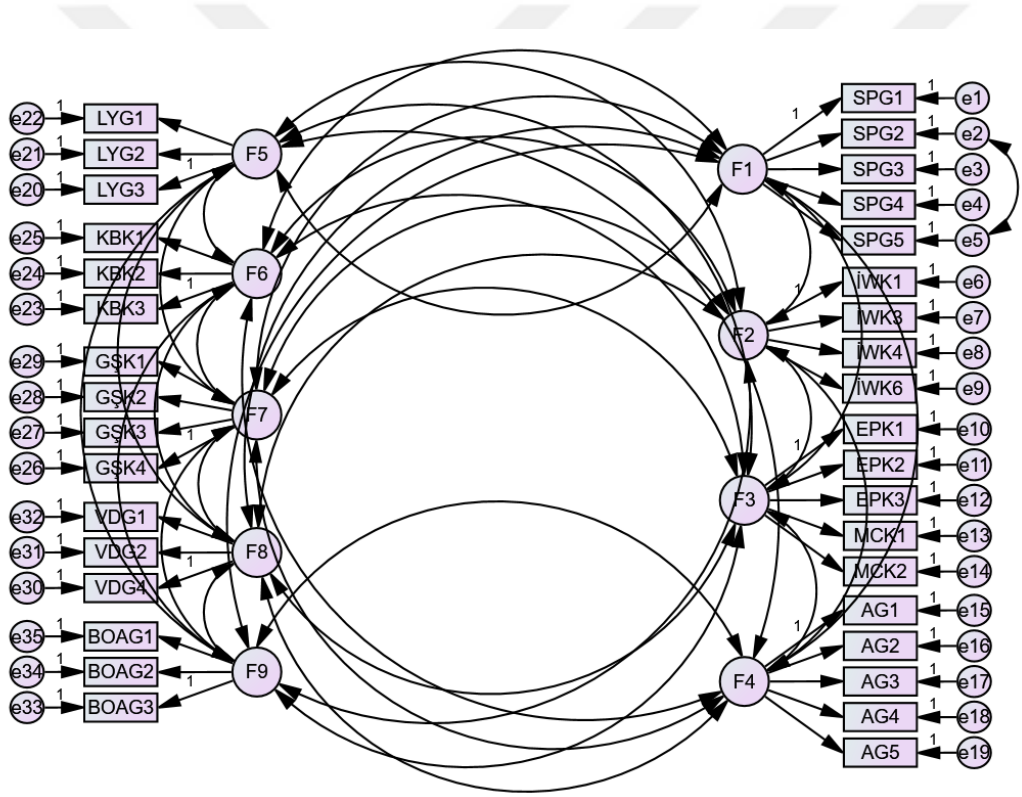
Üyelik gerektiren sitelere (sosyal ağ vs) kaydolmadan önce gizlilik politikası ve kullanım şartlarını okurum	0,514	0,502
İnternet Web Kullanımı Güvenliği (Özdeğer=2,414; Açıklanan Varyans=8,181; Alpha=0,765)		
Web adres çubuğunda farklı yönlendirme olup olmadığını kontrol ederim	0,737	0,512
Ziyaret ettiğim web sitelerinin güvenlik sertifikalarını kontrol ederim	0,690	0,666
İndirdiğim dosyaları virüs taramasından geçiririm	0,597	0,588
Tarayıcı eklentilerini devre dışı bırakırım	0,543	0,516
Mobil Cihaz ve Eposta Kullanım Güvenliği (Özdeğer=2,308; Açıklanan Varyans=7,825; Alpha=0,782)		
E-posta eklerini açmadan önce uzantılarına dikkat ederim	0,733	0,650
Bir banka ya da ticari kuruluştan gelse bile e-postalardaki linklere tıklamam	0,712	0,618
İndireceğim uygulamalar hakkındaki kullanıcı yorumları ve indirme sayısına dikkat ederim	0,690	0,533
E-posta eklerini açmadan önce virüs taraması yaparım	0,528	0,577
Gelen smslerdeki linklere tıklamam	0,419	0,427

Ağ Güvenliği (Özdeğer=1,818; Açıklanan Varyans=7,345; Alpha=0,756)		
Cihazlarımda kablosuz ağlara otomatik bağlanma özelliği kapalıdır	0,832	0,628
Halka açık/şifre istemeyen kablosuz internet erişimine bağlanmam	0,672	0,582
Kablosuz modem şifremi belirli aralıklarla değiştiririm	0,644	0,487
Kablosuz internetimi başkalarının kullanımına açmam	0,479	0,452
Ortak kullanıma açık kablosuz ağlara bağlıyken şifre gerektiren işlemler yapmam	0,428	0,469
Lisanslı Yazılım Güvenliği (Özdeğer=1,585; Açıklanan Varyans=7,152; Alpha=0,785)		
Korsan/crack yazılım kullanmam	0,826	0,644
Ücretsiz film, müzik, yazılım indirmem	0,820	0,705
Kullanıcı sözleşmesini okudum kabul metnini okumadan onaylamam	0,579	0,531
Kişisel Bilgisayar Güvenliği (Özdeğer=1,455; Açıklanan Varyans=6,520; Alpha=0,678)		
Bilgisayarımdaki önemli dosyalara şifre koyarım	0,735	0,554
Bilgisayarda işim bittiği zaman log off/turn off/shut down ile kapatırım	0,627	0,488
Kendime ait bilgisayar dışındaki bilgisayarlardan kullanıcı adı ve şifre gerektiren işlemlerimi yapmam	0,571	0,434

Güvenli Şifre Kullanımı (Özdeğer=1,417; Açıklanan Varyans=5,737; Alpha=0,664)		
Şifre ile giriş yapılan hesaplarda şifreyi otomatik hatırla özelliğini kullanmam (şifremi kaydetmemesine dikkat ederim)	0,678	0,397
Bilgisayarımdan uzaklaşacağımda şifre korumalı ekran koruyucuyu aktifleştiririm	0,517	0,433
Aynı kullanıcı adı ve şifreyi birden fazla hesabımda kullanmam	0,495	0,484
İşim bittiği zaman hesaplarımdan (e-posta, sosyal ağ vs) güvenli çıkış bağlantısı ile çıkış yaparım	0,488	0,484
Veri Depolama Güvenliği (Özdeğer=1,182; Açıklanan Varyans=5,671; Alpha=0,663)		
Usb bellekleri çıkarırken donanımı güvenle kaldır seçeneğini kullanırım	0,779	0,508
Kullandığım programları/yazılımları güncellerim	0,755	0,482
Flash bellekleri veri saklamak için kullanmam	0,613	0,439
Bankacılık İşlemleri ve Online Alışveriş Güvenliği (Özdeğer=1,139; Açıklanan Varyans=5,595; Alpha=0,635)		
Online alışveriş yaparken sanal kart kullanırım ve sanal kartıma limit belirlerim	0,719	0,480
İnternet bankacılığı kullanırken/kredi kart bilgilerimi girerken sanal klavye tercih ederim	0,670	0,466

Online alışverişte 3 boyutlu güvenlik (3d secure) yöntemi kullanırım	0,635	0,394
Toplam Varyans=%62.76; Genel Güvenirlik (Alpha)=0.906		

Açımlayıcı faktör analizi (AFA) ile elde edilen faktör yapısı doğrulayıcı faktör analizi (DFA) ile test edilmiştir. Doğrulayıcı faktör analize ilişkin diyagram Şekil 1'de verilmektedir.



Şekil 1. Bilgi Güvenliği Farkındalığı Ölçeği Doğrulayıcı Faktör Analizine İlişkin Diyagram

Doğrulayıcı faktör analizinin uyum iyiliği değerleri aşağıdadır.

Tablo II. Bilgi Güvenliği Farkındalığı Ölçeği Doğrulayıcı Faktör Analizi İndeks Değerleri

İndeks	**Normal Değer***	**Kabul Edilebilir Değer****	**Bilgi Güvenliği Farkındalığı Ölçeği**
χ2/sd	<2	<5	1.86
GFI	>0.95	>0.90	0.91
AGFI	>0.95	>0.90	0.90
CFI	>0.95	>0.90	0.90
RMSEA	<0.05	<0.08	0.07
RMR	<0.05	<0.08	0.08

*, ** (41,42).

Doğrulayıcı faktör analizi (DFA) ile hesaplanan uyum istatistikleri ile açımlayıcı faktör analizi (AFA) ile belirlenen faktör yapısının uyumlu olduğu sonucuna varılmıştır. Faktör yükleri, t değerleri ve R^2 değerleri Tablo III'de görülmektedir.

Tablo III. Bilgi Güvenliği Farkındalığı Ölçeği Faktör Yükleri ve Maddelere İlişkin Regresyon Katsayıları

Maddeler		**Faktörler**	**β**	**Std. β**	**S.Hata**	**t**	**p**	R^2
SPG1	<---	F1	1	0,594				0,546
SPG2	<---	F1	0,974	0,447	0,177	5,514	p<0,001	0,467
SPG3	<---	F1	1,477	0,908	0,163	9,037	p<0,001	0,465
SPG4	<---	F1	1,358	0,876	0,151	8,969	p<0,001	0,439

SPG5	<---	F1	0,926	0,554	0,140	6,589	p<0,001	0,402
İWK1	<---	F2	1	0,578				0,448
İWK3	<---	F2	1,765	0,758	0,234	7,529	p<0,001	0,548
İWK4	<---	F2	1,426	0,622	0,214	6,676	p<0,001	0,596
İWK6	<---	F2	1,579	0,740	0,212	7,434	p<0,001	0,647
EPK1	<---	F3	1	0,714				0,597
EPK2	<---	F3	0,851	0,754	0,092	9,207	p<0,001	0,581
EPK3	<---	F3	0,874	0,670	0,105	8,332	p<0,001	0,631
MCK1	<---	F3	0,552	0,493	0,088	6,245	p<0,001	0,647
MCK2	<---	F3	0,742	0,623	0,095	7,805	p<0,001	0,702
AG1	<---	F4	1	0,652				0,588
AG2	<---	F4	0,845	0,613	0,121	6,989	p<0,001	0,569
AG3	<---	F4	1,056	0,687	0,139	7,601	p<0,001	0,514
AG4	<---	F4	0,933	0,593	0,137	6,805	p<0,001	0,597
AG5	<---	F4	0,859	0,569	0,130	6,585	p<0,001	0,539
LYG3	<---	F5	1	0,646				0,544
LYG2	<---	F5	1,266	0,767	0,151	8,389	p<0,001	0,567
LYG1	<---	F5	1,365	0,838	0,159	8,561	p<0,001	0,566
KBK3	<---	F6	1	0,577				0,655
KBK2	<---	F6	1,034	0,600	0,170	6,08	p<0,001	0,544
KBK1	<---	F6	1,402	0,762	0,208	6,755	p<0,001	0,569
GŞK4	<---	F7	1	0,585				0,509
GŞK3	<---	F7	1,462	0,721	0,211	6,935	p<0,001	0,548
GŞK2	<---	F7	0,879	0,471	0,168	5,238	p<0,001	0,528

GŞK1	<---	F7	0,753	0,513	0,135	5,586	p<0,001	0,574
VDG4	<---	F8	1	0,669				0,536
VDG2	<---	F8	0,877	0,634	0,146	6,026	p<0,001	0,578
VDG1	<---	F8	0,771	0,586	0,133	5,815	p<0,001	0,768
BOAG3	<---	F9	1	0,682				0,824
BOAG2	<---	F9	0,688	0,523	0,124	5,531	p<0,001	0,596
BOAG1	<---	F9	0,952	0,617	0,155	6,130	p<0,001	0,611

Sonuçlar incelendiğinde faktör yükleri yüksek, standart hata değerleri düşük, **t** değerleri anlamlı bulunmuştur. (p<0,001). Ayrıca $\boldsymbol{R^2}$değerleri de yüksektir. Böylelikle ölçeğin yapı geçerliliği doğrulanmıştır.

3.2. Elde Edilen Verilerin İstatistiksel Analizi

Ölçek aracılığıyla toplanan verilerin SPSS (Statistical Package for Social Sciences) for Windows 18.0 programı ile analizi yapılmıştır. Öncelikle betimsel istatistikler (frekans, yüzde, ortalama, standart sapma) yapılmıştır.

Ölçekteki maddeler 1 ile 5 arasında puanlanmıştır. Dağılım aralığını hesaplamak için, Dağılım aralığı=En büyük değer- En küçük değer/ Derece sayısı formülü kullanılmıştır. Bu aralığın genişliği 4 puandır. Bu aralık 5 eşit parçaya bölünmüştür. 1.00- 1.79 arası “çok düşük”, 1.80-2.59 arası “düşük”, 2.60- 3.39 “arası orta”, 3.40-4.19 arası ” yüksek” , 4.20-5.00 arası “çok yüksek” olarak sınır değerleri belirlenmiş ve bulgular yorumlanmıştır (40).

Daha sonra iki bağımsız gruptaki sürekli verilerin karşılaştırılması amacıyla t-testi yapılmıştır. Sonrasında ise, ikiden fazla bağımsız gruptaki sürekli verilerin karşılaştırılması amacıyla tek

yönlü (one-way) Anova testi yapılmıştır. Anova testi sonrasında farklılıkları belirlemek için ise Scheffe testi yapılmıştır. Araştırmanın sürekli değişkenleri arasında pearson korelasyon analizi uygulanmıştır.

4. Bulgular

Bu kısımda, geliştirilen ölçekler yardımıyla elde edilen verilerin analiz edilmesi sonucu varılan bulgular yer almaktadır.

Tablo IV, ankete katılan kişilerin yaş, cinsiyet, eğitim durumu ve bilişim sektöründe çalışma süresine göre frekans ve yüzde olarak dağılımlarını göstermektedir.

Tablo IV. Tanımlayıcı Özellikler

Gruplar	**Frekans(n)**	**Yüzde (%)**
Yaş		
<26	67	33,5
26-35 Arası	99	49,5
36 Ve Üzeri	34	17,0
Cinsiyet		
Kadın	36	18,0
Erkek	164	82,0
Eğitim Durumu		
Lise	22	11,0
Ön lisans	32	16,0
Lisans	119	59,5
Yüksek Lisans	27	13,5

Bilişim Sektöründe Çalışma Süresi		
5 Yıldan Daha Az	106	53,0
5-10 Yıl Arası	55	27,5
11 Yıl Ve Üzeri	39	19,5

Tablo V, anketteki evet/hayır tipindeki sorulara verilen cevapların frekans ve yüzde değerlerini göstermektedir.

Tablo V. Güvenlik Davranışları

Gruplar	**Frekans(n)**	**Yüzde (%)**
Herhangi Bir Şifreyi Başkasının Bilme Durumu		
Evet	63	31,5
Hayır	137	68,5
Kişisel Bilgisayarın Şifre Korumalı Olma Durumu		
Evet	162	81,0
Hayır	38	19,0
Akıllı Telefonun Şifre Korumalı Olma Durumu		
Evet	171	85,5
Hayır	29	14,5
Kullanılan Cihazlarda Antivirüs Programı Yüklü Olma Durumu		
Evet	130	65,0
Hayır	70	35,0

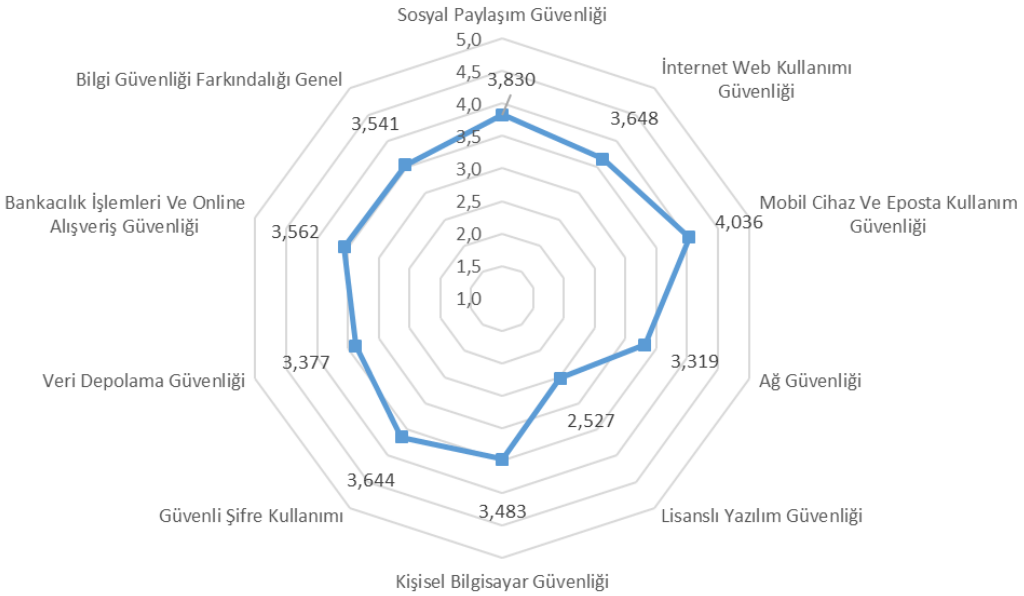
Cihazlarda Güvenlik Duvarının Açık Olma Durumu		
Evet	138	69,0
Hayır	62	31,0

Tablo VI, bilgi güvenliği farkındalığı puan ortalamaları, standart sapma, minimum ve maksimum değerleri göstermektedir.

Tablo VI. Bilgi Güvenliği Farkındalığı Puan Ortalamaları

	N	Ort	Ss	Min.	Max.
Sosyal Paylaşım Güvenliği	200	3,830	0,847	1,000	5,000
İnternet Web Kullanımı Güvenliği	200	3,648	0,920	1,000	5,000
Mobil Cihaz Ve Eposta Kullanım Güvenliği	200	4,036	0,788	1,000	5,000
Ağ Güvenliği	200	3,319	0,942	1,000	5,000
Lisanslı Yazılım Güvenliği	200	2,527	1,077	1,000	5,000
Kişisel Bilgisayar Güvenliği	200	3,483	1,063	1,000	5,000
Güvenli Şifre Kullanımı	200	3,644	0,952	1,250	5,000
Veri Depolama Güvenliği	200	3,377	1,033	1,000	5,000
Bankacılık İşlemleri Ve Online Alışveriş Güvenliği	200	3,562	0,999	1,000	5,000
Bilgi Güvenliği Farkındalığı Genel	200	3,541	0,612	1,060	5,000

Çalışanların “sosyal paylaşım güvenliği” ortalaması yüksek 3,830±0,847 (Min=1; Maks=5), “internet web kullanımı güvenliği” ortalaması yüksek 3,648±0,920 (Min=1; Maks=5), “mobil cihaz ve eposta kullanım güvenliği” ortalaması yüksek 4,036±0,788 (Min=1; Maks=5), “ağ güvenliği” ortalaması orta 3,319±0,942 (Min=1; Maks=5), “lisanslı yazılım güvenliği” ortalaması zayıf 2,527±1,077 (Min=1; Maks=5), “kişisel bilgisayar güvenliği” ortalaması yüksek 3,483±1,063 (Min=1; Maks=5), “güvenli şifre kullanımı” ortalaması yüksek 3,644±0,952 (Min=1.25; Maks=5), “veri depolama güvenliği” ortalaması orta 3,377±1,033 (Min=1; Maks=5), “bankacılık işlemleri ve online alışveriş güvenliği” ortalaması yüksek 3,562±0,999 (Min=1; Maks=5), “bilgi güvenliği farkındalığı genel” ortalaması yüksek 3,541±0,612 (Min=1.06; Maks=5), olarak saptanmıştır.



Şekil 2. Bilgi Güvenliği Farkındalığı Puan Ortalamaları

Araştırmaya katılan çalışanların Sosyal Paylaşım Güvenliği ile ilgili maddelere verdiği yanıtların dağılımları Tablo VII'de gösterilmektedir.

Tablo VII. Çalışanların Sosyal Paylaşım Güvenliği İle İlgili İfadelere Verdikleri Cevapların Dağılımları

	Kesinlikle Katılmıyorum		**Katılmıyorum**		**Kararsızım**		**Katılıyorum**		**Kesinlikle Katılıyorum**			
	f	**%**	**f**	**%**	**f**	**%**	**f**	**%**	**f**	**%**	**Ort**	**Ss**
Tanımadığım Kişileri Ağıma Eklemem	7	3,5	12	6,0	29	14,5	77	38,5	75	37,5	4,010	1,039
Tanımadığın Kişilerin Ağına Eklenmekten Çekinirim	6	3,0	13	6,5	24	12,0	92	46,0	65	32,5	3,980	0,990
Sosyal Ağ Hesaplarının E-posta Adres Defterini Taramasına İzin Vermem	5	2,5	21	10,5	32	16,0	71	35,5	71	35,5	3,910	1,076
İnternet Ortamında İletişim Bilgilerimi/kişisel Bilgilerimi Paylaşmam	5	2,5	19	9,5	32	16,0	70	35,0	74	37,0	3,950	1,067
Üyelik Gerektiren Sitelere (sosyal Ağ Vs) Kaydolmadan Önce Gizlilik Politikası Ve Kullanım Şartlarını Okurum	29	14,5	34	17,0	35	17,5	51	25,5	51	25,5	3,310	1,393

Araştırmaya katılan çalışanların İnternet Web Kullanımı Güvenliği ile ilgili maddelere verdiği yanıtların dağılımları Tablo VIII'de gösterilmektedir.

Tablo VIII. Çalışanların İnternet Web Kullanımı Güvenliği İle İlgili İfadelere Verdikleri Cevapların Dağılımları

	Kesinlikle Katılmıyorum		**Katılmıyorum**		**Kararsızım**		**Katılıyorum**		**Kesinlikle Katılıyorum**			
	f	**%**	**F**	**%**	**f**	**%**	**f**	**%**	**f**	**%**	**Ort**	**Ss**
Web Adres Çubuğunda Farklı Yönlendirme Olup Olmadığını Kontrol Ederim	6	3,0	4	2,0	29	14,5	62	31,0	99	49,5	4,220	0,973
Ziyaret Ettiğim Web Sitelerinin Güvenlik Sertifikalarını Kontrol Ederim	19	9,5	39	19,5	39	19,5	52	26,0	51	25,5	3,380	1,310
İndirdiğim Dosyaları Virüs Taramasından Geçiririm	12	6,0	30	15,0	42	21,0	63	31,5	53	26,5	3,570	1,201
Tarayıcı Eklentilerini Devre Dışı Bırakırım	14	7,0	45	22,5	40	20,0	47	23,5	54	27,0	3,410	1,288

Araştırmaya katılan çalışanların Mobil Cihaz Ve Eposta Kullanım Güvenliği ile ilgili maddelere verdiği yanıtların dağılımları Tablo IX'da gösterilmektedir.

Tablo IX. Çalışanların Mobil Cihaz Ve Eposta Kullanım Güvenliği İle İlgili İfadelere Verdikleri Cevapların Dağılımları

	Kesinlikle Katılmıyorum		**Katılmıyorum**		**Kararsızım**		**Katılıyorum**		**Kesinlikle Katılıyorum**			
	f	**%**	**f**	**%**	**f**	**%**	**f**	**%**	**f**	**%**	**Ort**	**Ss**
E-posta Eklerini Açmadan Önce Uzantılarına Dikkat Ederim	4	2,0	13	6,5	16	8,0	68	34,0	99	49,5	4,220	0,984
Bir Banka Ya Da Ticari Kuruluştan Gelse Bile E-postalardaki Linklere Tıklamam	7	3,5	25	12,5	42	21,0	61	30,5	65	32,5	3,760	1,140
İndireceğim Uygulamalar Hakkındaki Kullanıcı Yorumları Ve İndirme Sayısına Dikkat Ederim	6	3,0	13	6,5	11	5,5	53	26,5	117	58,5	4,310	1,039
E-posta Eklerini Açmadan Önce Virüs Taraması Yaparım	11	5,5	29	14,5	31	15,5	62	31,0	67	33,5	3,730	1,223
Gelen Smslerdeki Linklere Tıklamam	5	2,5	8	4,0	28	14,0	68	34,0	91	45,5	4,160	0,979

Araştırmaya katılan çalışanların Ağ Güvenliği ile ilgili maddelere verdiği yanıtların dağılımları Tablo X'da gösterilmektedir.

Tablo X. Çalışanların Ağ Güvenliği İle İlgili İfadelere Verdikleri Cevapların Dağılımları

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum			
	f	%	f	%	f	%	f	%	f	%	Ort	Ss
Cihazlarımda Kablosuz Ağlara Otomatik Bağlanma Özelliği Kapalıdır	23	11,5	46	23,0	38	19,0	46	23,0	47	23,5	3,240	1,346
Halka Açık/şifre İstemeyen Kablosuz İnternet Erişimine Bağlanmam	25	12,5	38	19,0	45	22,5	43	21,5	49	24,5	3,270	1,351
Kablosuz Modem Şifremi Belirli Aralıklarla Değiştiririm	39	19,5	55	27,5	30	15,0	44	22,0	32	16,0	2,870	1,382
Kablosuz İnternetimi Başkalarının Kullanımına Açmam	17	8,5	34	17,0	33	16,5	51	25,5	65	32,5	3,570	1,325
Ortak Kullanıma Açık Kablosuz Ağlara Bağlıyken Şifre Gerektiren İşlemler Yapmam	12	6,0	29	14,5	34	17,0	67	33,5	58	29,0	3,650	1,210

Araştırmaya katılan çalışanların Lisanslı Yazılım Güvenliği ile ilgili ifadelere verdiği cevapların dağılımları Tablo XI'de gösterilmektedir.

Tablo XI. Çalışanların Lisanslı Yazılım Güvenliği İle İlgili İfadelere Verdikleri Cevapların Dağılımları

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum			
	f	%	f	%	f	%	f	%	f	%	Ort	Ss
Korsan/crack Yazılım Kullanmam	50	25,0	48	24,0	45	22,5	35	17,5	22	11,0	2,660	1,321
Ücretsiz Film, Müzik, Yazılım İndirmem	56	28,0	60	30,0	36	18,0	28	14,0	20	10,0	2,480	1,303
Kullanıcı Sözleşmesini Okudum Kabul Metnini Okumadan Onaylamam	54	27,0	59	29,5	49	24,5	20	10,0	18	9,0	2,440	1,239

Araştırmaya katılan çalışanların Kişisel Bilgisayar Güvenliği ile ilgili maddelere verdiği yanıtların dağılımları Tablo XII'de gösterilmektedir.

Tablo XII. Çalışanların Kişisel Bilgisayar Güvenliği İle İlgili İfadelere Verdikleri Cevapların Dağılımları

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum			
	f	%	f	%	f	%	f	%	f	%	Ort	Ss
Bilgisayarımdaki Önemli Dosyalara Şifre Koyarım	27	13,5	53	26,5	30	15,0	38	19,0	52	26,0	3,180	1,419

Bilgisayarda İşim Bittiği Zaman Log Off/turn Off/shut Down İle Kapatırım	13	6,5	34	17,0	21	10,5	45	22,5	87	43,5	3,790	1,331
Kendime Ait Bilgisayar Dışındaki Bilgisayarlardan Kullanıcı Adı Ve Şifre Gerektiren İşlemlerimi Yapmam	17	8,5	42	21,0	29	14,5	52	26,0	60	30,0	3,480	1,337

Araştırmaya katılan çalışanların Güvenli Şifre Kullanımı ile ilgili maddelere verdiği yanıtların dağılımları Tablo XIII'de gösterilmektedir.

Tablo XIII. Çalışanların Güvenli Şifre Kullanımı İle İlgili İfadelere Verdikleri Cevapların Dağılımları

	Kesinlikle Katılmıyorum		**Katılmıyorum**		**Kararsızım**		**Katılıyorum**		**Kesinlikle Katılıyorum**			
	f	**%**	**f**	**%**	**f**	**%**	**f**	**%**	**f**	**%**	**Ort**	**Ss**
Şifre İle Giriş Yapılan Hesaplarda Şifreyi Otomatik Hatırla Özelliğini Kullanmam (şifremi Kaydetmemesine Dikkat Ederim)	16	8,0	49	24,5	20	10,0	38	19,0	77	38,5	3,550	1,413

Bilgisayarımdan Uzaklaşacağımda Şifre Korumalı Ekran Koruyucuyu Aktifleştiririm	2	1,0	25	12,5	34	17,0	44	22,0	95	47,5	4,020	1,114
Aynı Kullanıcı Adı Ve Şifreyi Birden Fazla Hesabımda Kullanmam	38	19,0	45	22,5	33	16,5	20	10,0	64	32,0	3,130	1,536
İşim Bittiği Zaman Hesaplarımdan (e-posta, sosyal Ağ Vs) Güvenli Çıkış Bağlantısı İle Çıkış Yaparım	12	6,0	29	14,5	24	12,0	45	22,5	90	45,0	3,860	1,296

Araştırmaya katılan çalışanların 'Veri Depolama Güvenliği' ile ilgili maddelere verdiği yanıtların dağılımları Tablo XIV'de gösterilmektedir.

Tablo XIV. Çalışanların Veri Depolama Güvenliği İle İlgili İfadelere Verdikleri Cevapların Dağılımları

	Kesinlikle Katılmıyorum		**Katılmıyorum**		**Kararsızım**		**Katılıyorum**		**Kesinlikle Katılıyorum**			
	f	**%**	**f**	**%**	**f**	**%**	**f**	**%**	**f**	**%**	**Ort**	**Ss**
Usb Bellekleri Çıkarırken Donanımı Güvenle Kaldır Seçeneğini Kullanırım	30	15,0	29	14,5	36	18,0	45	22,5	60	30,0	3,380	1,427

Kullandığım Programları/yazılımları Güncellerim	15	7,5	26	13,0	26	13,0	67	33,5	66	33,0	3,710	1,258
Flash Bellekleri Veri Saklamak İçin Kullanmam	29	14,5	50	25,0	39	19,5	49	24,5	33	16,5	3,030	1,320

Araştırmaya katılan çalışanların Bankacılık İşlemleri Ve Online Alışveriş Güvenliği ile ilgili maddelere verdiği yanıtların dağılımları Tablo XV'de gösterilmektedir.

Tablo XV. Çalışanların Bankacılık İşlemleri Ve Online Alışveriş Güvenliği İle İlgili İfadelere Verdikleri Cevapların Dağılımları

	Kesinlikle Katılmıyorum		**Katılmıyorum**		**Kararsızım**		**Katılıyorum**		**Kesinlikle Katılıyorum**			
	f	**%**	**f**	**%**	**f**	**%**	**f**	**%**	**f**	**%**	**Ort**	**Ss**
Online Alışveriş Yaparken Sanal Kart Kullanırım Ve Sanal Kartıma Limit Belirlerim	22	11,0	37	18,5	24	12,0	49	24,5	68	34,0	3,520	1,403
İnternet Bankacılığı Kullanırken/kredi Kart Bilgilerimi Girerken Sanal Klavye Tercih Ederim	29	14,5	45	22,5	46	23,0	42	21,0	38	19,0	3,070	1,334

Online Alışverişte 3 Boyutlu Güvenlik (3d Secure) Yöntemi Kullanırım	11	5,5	16	8,0	20	10,0	50	25,0	103	51,5	4,090	1,195

Her bir faktörün birbirleriyle aralarındaki korelasyon değerleri Tablo XVI'da verilmiştir.

Tablo XVI. Bilgi Güvenliği Farkındalığı Puanları Arasında Korelasyon Analizi

		Sosyal Paylaşım Güvenliği	İnternet Web Kullanımı Güvenliği	Mobil Cihaz Ve Eposta Kullanım Güvenliği	Ağ Güvenliği	Lisanslı Yazılım Güvenliği	Kişisel Bilgisayar Güvenliği	Güvenli Şifre Kullanımı	Veri Depolama Güvenliği	Bankacılık Ve Online İşlemleri Alışveriş Güvenliği	Bilgi Güvenliği Farkındalığı Genel
Sosyal Paylaşım Güvenliği	r	1,000									
	p	0,000									
İnternet Web Kullanımı Güvenliği	r	0,358**	1,000								
	p	0,000	0,000								
Mobil Cihaz Ve Eposta Kullanım Güvenliği	r	0,373**	0,533**	1,000							
	p	0,000	0,000	0,000							
Ağ Güvenliği	r	0,454**	0,418**	0,429**	1,000						
	p	0,000	0,000	0,000	0,000						
Lisanslı Yazılım Güvenliği	r	0,240**	0,269**	0,153*	0,399**	1,000					
	p	0,001	0,000	0,031	0,000	0,000					
Kişisel Bilgisayar Güvenliği	r	0,330**	0,458**	0,402**	0,383**	0,249**	1,000				
	p	0,000	0,000	0,000	0,000	0,000	0,000				
Güvenli Şifre Kullanımı	r	0,338**	0,521**	0,383**	0,391**	0,298**	0,493**	1,000			
	p	0,000	0,000	0,000	0,000	0,000	0,000	0,000			
Veri Depolama Güvenliği	r	0,176*	0,270**	0,338**	0,311**	0,336**	0,233**	0,281**	1,000		
	p	0,013	0,000	0,000	0,000	0,000	0,001	0,000	0,000		
Bankacılık İşlemleri Ve Online Alışveriş Güvenliği	r	0,282**	0,383**	0,386**	0,337**	0,329**	0,341**	0,329**	0,145*	1,000	
	p	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,041	0,000	
Bilgi Güvenliği Farkındalığı Genel	r	0,637**	0,726**	0,697**	0,739**	0,545**	0,657**	0,695**	0,511**	0,586**	1,000
	p	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000

*<0,05; **<0,01

Bilgi güvenliği farkındalığının yaşa göre farklılaşma durumu Tablo XVII'de verilmiştir.

Tablo XVII. Bilgi Güvenliği Farkındalığı Puanlarının Yaşa Göre Farklılaşma Durumu

	Grup	**N**	**Ort**	**Ss**	**F**	**p**	**Fark**
Sosyal Paylaşım Güvenliği	25 Ve Altı	67	3,690	0,984	1,421	0,244	
	26-35 Arası	99	3,911	0,796			
	36 Ve Üzeri	34	3,871	0,666			
İnternet Web Kullanımı Güvenliği	25 Ve Altı	67	3,623	0,911	0,694	0,501	
	26-35 Arası	99	3,606	0,964			
	36 Ve Üzeri	34	3,816	0,801			
Mobil Cihaz Ve Eposta Kullanım Güvenliği	25 Ve Altı	67	3,818	0,873	5,598	**0,004**	**2>1** **3>1**
	26-35 Arası	99	4,077	0,758			
	36 Ve Üzeri	34	4,347	0,558			
Ağ Güvenliği	25 Ve Altı	67	3,218	0,977	0,623	0,537	
	26-35 Arası	99	3,356	0,916			
	36 Ve Üzeri	34	3,412	0,956			
Lisanslı Yazılım Güvenliği	25 Ve Altı	67	2,229	1,080	4,779	**0,009**	**2>1** **3>1**
	26-35 Arası	99	2,609	1,015			
	36 Ve Üzeri	34	2,873	1,134			
Kişisel Bilgisayar Güvenliği	25 Ve Altı	67	3,493	1,035	0,339	0,713	
	26-35 Arası	99	3,434	1,110			
	36 Ve Üzeri	34	3,608	0,993			

Güvenli Şifre Kullanımı	25 Ve Altı	67	3,619	0,920	1,165	0,314	
	26-35 Arası	99	3,583	0,960			
	36 Ve Üzeri	34	3,868	0,981			
Veri Depolama Güvenliği	25 Ve Altı	67	3,139	1,075	2,704	0,069	
	26-35 Arası	99	3,498	1,011			
	36 Ve Üzeri	34	3,490	0,961			
Bankacılık İşlemleri Ve Online Alışveriş Güvenliği	25 Ve Altı	67	3,383	1,058	3,109	**0,047**	**3>1**
	26-35 Arası	99	3,566	0,981			
	36 Ve Üzeri	34	3,902	0,859			
Bilgi Güvenliği Farkındalığı Genel	25 Ve Altı	67	3,409	0,615	3,297	**0,039**	**3>1**
	26-35 Arası	99	3,566	0,615			
	36 Ve Üzeri	34	3,729	0,556			

Bilgi güvenliği farkındalığının cinsiyete göre farklılaşma durumu Tablo XVIII'de verilmiştir.

TabloXVIII. Bilgi Güvenliği Farkındalığı Puanlarının Cinsiyete Göre Farklılaşma Durumu

	Grup	**N**	**Ort**	**Ss**	**t**	**sd**	**p**
Sosyal Paylaşım Güvenliği	Kadın	36	3,839	0,839	0,069	198	0,945
	Erkek	164	3,828	0,851			
İnternet Web Kullanımı Güvenliği	Kadın	36	3,285	1,037	-2,653	198	**0,009**
	Erkek	164	3,727	0,875			

Mobil Cihaz Ve Eposta Kullanım Güvenliği	Kadın	36	3,728	0,941	-2,631	198	**0,029**
	Erkek	164	4,104	0,736			
Ağ Güvenliği	Kadın	36	3,150	0,971	-1,190	198	0,235
	Erkek	164	3,356	0,934			
Lisanslı Yazılım Güvenliği	Kadın	36	2,759	0,897	1,434	198	0,153
	Erkek	164	2,476	1,109			
Kişisel Bilgisayar Güvenliği	Kadın	36	3,482	1,114	-0,012	198	0,991
	Erkek	164	3,484	1,055			
Güvenli Şifre Kullanımı	Kadın	36	3,542	1,058	-0,710	198	0,479
	Erkek	164	3,666	0,929			
Veri Depolama Güvenliği	Kadın	36	3,389	0,910	0,078	198	0,938
	Erkek	164	3,374	1,061			
Bankacılık İşlemleri Ve Online Alışveriş Güvenliği	Kadın	36	3,157	0,974	-2,724	198	**0,007**
	Erkek	164	3,650	0,985			
Bilgi Güvenliği Farkındalığı Genel	Kadın	36	3,407	0,708	-1,452	198	0,148
	Erkek	164	3,570	0,588			

Bağımsız Gruplar T-Testi

Bilgi güvenliği farkındalığının eğitim durumuna göre farklılaşma durumu Tablo XIX'de verilmiştir.

Tablo XIX. Bilgi Güvenliği Farkındalığı Puanlarının Eğitim Durumuna Göre Farklılaşma Durumu

	Grup	**N**	**Ort**	**Ss**	**F**	**p**
Sosyal Paylaşım Güvenliği	Lise	22	3,773	0,980	2,546	0,057
	Önlisans	32	3,813	0,821		
	Lisans	119	3,933	0,765		
	Yüksek Lisans	27	3,444	1,025		
İnternet Web Kullanımı Güvenliği	Lise	22	3,716	0,940	2,416	0,068
	Önlisans	32	3,898	0,886		
	Lisans	119	3,653	0,822		
	Yüksek Lisans	27	3,269	1,234		
Mobil Cihaz Ve Eposta Kullanım Güvenliği	Lise	22	3,909	0,841	2,331	0,076
	Önlisans	32	3,969	0,774		
	Lisans	119	4,145	0,688		
	Yüksek Lisans	27	3,741	1,074		
Ağ Güvenliği	Lise	22	3,482	0,943	0,406	0,749
	Önlisans	32	3,344	0,940		
	Lisans	119	3,313	0,913		
	Yüksek Lisans	27	3,185	1,091		
Lisanslı Yazılım Güvenliği	Lise	22	2,197	1,176	0,972	0,407
	Önlisans	32	2,688	1,173		
	Lisans	119	2,527	1,007		
	Yüksek Lisans	27	2,605	1,180		

Kişisel Bilgisayar Güvenliği	Lise	22	3,621	1,051	0,579	0,629
	Önlisans	32	3,563	1,096		
	Lisans	119	3,487	1,021		
	Yüksek Lisans	27	3,259	1,231		
Güvenli Şifre Kullanımı	Lise	22	3,750	0,893	0,446	0,720
	Önlisans	32	3,719	0,985		
	Lisans	119	3,643	0,893		
	Yüksek Lisans	27	3,472	1,208		
Veri Depolama Güvenliği	Lise	22	3,091	1,222	0,779	0,507
	Önlisans	32	3,448	0,990		
	Lisans	119	3,378	1,005		
	Yüksek Lisans	27	3,519	1,059		
Bankacılık İşlemleri Ve Online Alışveriş Güvenliği	Lise	22	3,273	0,941	1,207	0,309
	Önlisans	32	3,729	1,096		
	Lisans	119	3,605	0,937		
	Yüksek Lisans	27	3,407	1,171		
Bilgi Güvenliği Farkındalığı Genel	Lise	22	3,492	0,572	1,203	0,310
	Önlisans	32	3,611	0,639		
	Lisans	119	3,575	0,530		
	Yüksek Lisans	27	3,348	0,891		

Tek Yönlü Varyans Analizi

Bilgi güvenliği farkındalığının bilişim sektöründe çalışma süresine göre farklılaşma durumu Tablo XX'de verilmiştir.

Tablo XX. Bilgi Güvenliği Farkındalığı Puanlarının Bilişim Sektöründe Çalışma Süresine Göre Farklılaşma Durumu

	Grup	**N**	**Ort**	**Ss**	**F**	**p**	**Fark**
Sosyal Paylaşım Güvenliği	5 Yıldan Daha Az	106	3,730	0,938	1,929	0,148	
	5-10 Yıl Arası	55	4,004	0,631			
	11 Yıl Ve Üzeri	39	3,856	0,830			
İnternet Web Kullanımı Güvenliği	5 Yıldan Daha Az	106	3,547	0,925	1,356	0,260	
	5-10 Yıl Arası	55	3,750	0,914			
	11 Yıl Ve Üzeri	39	3,776	0,905			
Mobil Cihaz Ve Eposta Kullanım Güvenliği	5 Yıldan Daha Az	106	3,885	0,824	4,313	**0,015**	**2>1** **3>1**
	5-10 Yıl Arası	55	4,222	0,602			
	11 Yıl Ve Üzeri	39	4,185	0,850			
Ağ Güvenliği	5 Yıldan Daha Az	106	3,204	0,929	1,756	0,175	
	5-10 Yıl Arası	55	3,422	0,983			
	11 Yıl Ve Üzeri	39	3,487	0,898			
Lisanslı Yazılım Güvenliği	5 Yıldan Daha Az	106	2,324	1,095	4,825	**0,009**	**3>1**
	5-10 Yıl Arası	55	2,649	0,976			
	11 Yıl Ve Üzeri	39	2,906	1,062			
Kişisel Bilgisayar Güvenliği	5 Yıldan Daha Az	106	3,475	1,068	0,155	0,856	
	5-10 Yıl Arası	55	3,442	1,070			

	11 Yıl Ve Üzeri	39	3,564	1,063			
Güvenli Şifre Kullanımı	5 Yıldan Daha Az	106	3,616	0,896	0,108	0,897	
	5-10 Yıl Arası	55	3,664	1,047			
	11 Yıl Ve Üzeri	39	3,692	0,981			
Veri Depolama Güvenliği	5 Yıldan Daha Az	106	3,280	1,028	1,131	0,325	
	5-10 Yıl Arası	55	3,533	0,924			
	11 Yıl Ve Üzeri	39	3,419	1,182			
Bankacılık İşlemleri Ve Online Alışveriş Güvenliği	5 Yıldan Daha Az	106	3,440	0,999	1,677	0,190	
	5-10 Yıl Arası	55	3,697	1,013			
	11 Yıl Ve Üzeri	39	3,701	0,961			
Bilgi Güvenliği Farkındalığı Genel	5 Yıldan Daha Az	106	3,437	0,589	3,320	**0,038**	**2>1**
	5-10 Yıl Arası	55	3,653	0,550			**3>1**
	11 Yıl Ve Üzeri	39	3,665	0,715			

Tek Yönlü Varyans Analizi

5. Tartışma

Bu araştırma kapsamında bilişim sektöründe çalışan kişilerin bilgi güvenliği farkındalık seviyelerini belirlemek için 'Bilgi Güvenliği Farkındalığı Ölçeği' isimli yeni bir ölçek geliştirilmiştir.

Toplam 43 sorudan oluşan ölçek üç bölümden oluşmaktadır. İlk 4 soru kullanıcılara ait demografik verileri ölçme amaçlı çoktan seçmeli sorulardır. Sonraki 5 soru evet/hayır şeklinde seçmeli olarak, geriye kalan 35 soru ise likert tipte sorulmuştur. Faktör analizine 35 soru dahil edilmiş, evet/hayır tipindeki 5 soru faktör analizine alınmamıştır.

Ölçek 200 kişiye uygulanmıştır. Çalışma grubunun sayısının belirlenmesinde Tavşancıl'ın (2002)faktör analizi konusunda verdiği bilgiler dikkate alınmıştır. Tavşancıl (2002), örneklem büyüklüğünün ölçekteki madde sayısının en az 5 katı olması gerektiğini belirtmiştir (44). Bu durumda 35 maddelik ölçek için örneklem sayısı en az 175 olmalıdır.

Ölçeğin yapı geçerliliğini belirlemek amacıyla açımlayıcı faktör analizi (AFA) yöntemi uygulanmıştır. Barlett testi yapılmış ve p=0.000 bulunmuştur. Büyüköztürk'e göre p değeri < 0,05 ise veri seti faktör analizi için uygundur (45). Barlett testi yapıldıktan sonra KMO değerine bakılmıştır. Field (2000) de Kaiser-Meyer-Olkin testi için alt sınır değerinin 0.50 olması gerektiğini ve KMO≤0.50 için veri kümesinin faktörlenemeyeceğini belirtmiştir (46). KMO değeri .826 olarak bulunmuştur ve bu değer örneklemin büyüklüğünün faktör analizi uygulamak için "iyi" olduğunu göstermektedir (47).

Faktör analizi için varimax yöntemi kullanılmıştır. Faktör analizinin sonrasında maddeler toplam açıklanan varyansı %62.76 olan 9 faktör altında toplanmıştır. Ölçekten 5 madde eş yükleme ve faktör yükü 0,4'den düşük olduğu için çıkartılmıştır.

Bilgi Güvenliği Farkındalığı Ölçeği'ndeki 35 maddenin güvenirliğini hesaplamak amacıyla Cronbach Alpha iç tutarlılık katsayısı hesaplanmıştır. İç tutarlılık katsayılarının hesaplanması güvenirlik çalışmalarında sık kullanılan bir ölçüttür. Maddelerin kendi aralarındaki homojenliğini ve kavramı ölçüp ölçmediğini gösterir (48). Cronbach alfa güvenirlik katsayısı, likert tipi puanlamalarda kullanılması uygun bir iç tutarlılık yöntemi olarak gösterilmektedir (49). Ölçeğin genel güvenirliği 0.906 olarak bulunmuştur. Cronbach alfa katsayısının .60'dan büyük olması ölçeğin oldukça güvenilir olduğunu göstermektedir (50).

Uyumluluk için x2 / sd oranı hesaplanmış ve 1.86 bulunmuştur. Bu değerin 3'ün altında bulunması mükemmel uyumu göstermektedir (47). GFI ve AGFI değerleri sırasıyla .91 ve .90 olarak bulunmuştur. GFI ve AGFI değerlerinin.90 ve yukarısında olması iyi uyumu göstermektedir. Buna göre GFI ve AGFI iyi uyuma sahiptir. CFI indeksinin 0.90 olduğu görülmüştür. İndeksin .90 ve üzeri olması iyi bir uyum iyiliğine sahip olduğunu göstermektedir (47)

RMSEA değeri .07 bulunmuştur. RMSEA değerinin .80'den az çıkması iyi uyuma işaret etmektedir. RMR uyum indeksi .08 olarak bulunmuş ve iyi uyuma karşılık gelmekte olduğu anlaşılmıştır. (47).

Çalışmanın örneklemine bakıldığında, 164 erkek katılımcı ve 36 kadın katılımcıdan oluştuğu görülmektedir. TÜİK verilerine göre Türkiye'de 2017 yılı itibariyle bilişim sektörü

çalışanlarının 76.111'i erkek iken sadece 25.293'ü kadındır (51). Sektörün erkek ağırlıklı olması göz önünde bulundurulduğunda, katılımcıların da çoğunluğunun erkeklerden oluşmasının normal olduğu düşünülmektedir.

Ölçeğe katılımın en çok 26-35 yaş arası çalışanlarda olduğu görülmektedir. Daha sonra ise 25 yaş altı katılımcılar gelmektedir. Sektörde çalışmaya başlama yaşının 18 olduğunu varsayarsak 26-35 yaş aralığının daha geniş olması katılımın da daha çok bu gruptan sağlanmış olmasına neden olmuştur diyebiliriz. 36 yaş üzeri çalışanlarda katılımın düşük olması ise daha genç yaştaki çalışanların araştırmalara ve bilimsel çalışmalara daha açık olduğunu göstermektedir.

Örnekleme bakıldığında en çok katılımın sektörde 5 yıldan daha az zamandır çalışanlardan en çok katılımın sağlandığı görülmekledir. Sektörde çalışma süresi arttıkça ölçeğe katılım oranı da düşmüştür. En az katılım 15 yıl ve üzeri çalışanlardan sağlanmıştır. Bu da yine sektörde daha yeni olan kişilerin araştırmalara daha açık olduğunu göstermektedir.

Katılımcıların büyük çoğunluğunun (%68,5) şifrelerini başkalarıyla paylaşmadığı sonucu elde edilmiştir.

Katılımcıların %81,0'inin bilgisayarlarının şifre korumalı olduğu, %85,5'inin ise akıllı telefonlarının şifre korumalı olduğu sonucuna varılmıştır. Söz konusu bilişim sektörü çalışanları olduğu için bu oranın yüksek çıkması beklenilen yöndedir.

Kullanılan cihazlarda antivirüs programı yüklü olma durumu göre katılımcıların 130'u (%65,0) evet, 70'i (%35,0) hayır cevabı vermiştir. Yine cihazlarda güvenlik duvarının açık olma durumu göre katılımcıların 138'i (%69,0) evet, 62'si (%31,0) hayır cevabı vermiştir.

Antivirüs programı ve güvenlik duvarı kullanımının önemi düşünüldüğünde bu sonucun bilişim çalışanları için beklenenin aksine düşük çıktığı düşünülmektedir.

Çalışanların "sosyal paylaşım güvenliği" ortalaması yüksek 3,830±0,847 (Min=1; Maks=5), "internet web kullanımı güvenliği" ortalaması yüksek 3,648±0,920 (Min=1; Maks=5), "mobil cihaz ve eposta kullanım güvenliği" ortalaması yüksek 4,036±0,788 (Min=1; Maks=5), "ağ güvenliği" ortalaması orta 3,319±0,942 (Min=1; Maks=5), "lisanslı yazılım güvenliği" ortalaması zayıf 2,527±1,077 (Min=1; Maks=5), "kişisel bilgisayar güvenliği" ortalaması yüksek 3,483±1,063 (Min=1; Maks=5), "güvenli şifre kullanımı" ortalaması yüksek 3,644±0,952 (Min=1.25; Maks=5), "veri depolama güvenliği" ortalaması orta 3,377±1,033 (Min=1; Maks=5), "bankacılık işlemleri ve online alışveriş güvenliği" ortalaması yüksek 3,562±0,999 (Min=1; Maks=5), "bilgi güvenliği farkındalığı genel" ortalaması yüksek 3,541±0,612 (Min=1.06; Maks=5), olarak saptanmıştır.

Bu sonuçlara bakıldığında, genel bilgi güvenliği farkındalığının yüksek olması beklenilen bir sonuçtur. Bilişim sektörü çalışanlarının bilgi teknolojileriyle sürekli iç içe olmaları nedeniyle bilgi güvenliği konularında genel bir aşinalık kazanmış olmaları beklenilir. Bu da elde edilen sonucu anlamlı kılmaktadır.

Alt faktörlere göre farkındalık seviyeleri incelendiğinde sadece 'lisanslı yazılım güvenliği' konusunda farkındalığın düşük olduğu görülmektedir. Bu konunun hem etik açıdan hem de bilgi güvenliği açısından olumsuz yönleri konusunda bilişim sektörü çalışanlarına bir eğitim uygulanmasının iyi olacağı düşünülmektedir.

Çalışanların sosyal paylaşım güvenliği, internet web kullanımı güvenliği, ağ güvenliği, kişisel bilgisayar güvenliği, güvenli şifre kullanımı, veri depolama güvenliği puanları yaşa göre

anlamlı farklılık göstermemektedir (p>0.05). Ancak internet bankacılığı ve online alışverişte yaş arttıkça farkındalık seviyesinin de arttığı görülmüştür.

Elde edilen sonuçlar cinsiyete göre incelendiğinde, erkeklerin internet web kullanımı güvenliği puanları ($\bar{x}$=3,727), kadınların internet web kullanımı güvenliği puanlarından ($\bar{x}$=3,285) yüksek bulunmuştur. Yine erkeklerin mobil cihaz ve eposta kullanım güvenliği puanları ($\bar{x}$=4,104), kadınların mobil cihaz ve eposta kullanım güvenliği puanlarından ($\bar{x}$=3,728) yüksek bulunmuştur. Bankacılık işlemleri ve online alışveriş güvenliği konusunda da erkeklerin puanları kadınlara göre daha yüksektir.

Çalışanların sosyal paylaşım güvenliği, ağ güvenliği, lisanslı yazılım güvenliği, kişisel bilgisayar güvenliği, güvenli şifre kullanımı, veri depolama güvenliği, bilgi güvenliği farkındalığı genel puanları cinsiyete göre anlamlı farklılık göstermez (p>0,05).

Eğitim düzeyinin bilişim sektöründe çalışanların bilgi güvenliği farkındalığı üzerinde anlamlı bir etkisi olmadığı tespit edilen sonuçlar arasındadır. Bunun nedeni eğitim programı müfredatlarının bilgi güvenliğine yönelik dersleri içermemesi olabilir.

Çalışanların bilişim sektöründe çalışma süresine göre mobil cihaz ve eposta kullanım güvenliği puanları anlamlı farklılık göstermektedir. Bilişim sektöründe çalışma süresi yüksek olanların mobil cihaz ve eposta kullanım güvenliği puanları, bilişim sektöründe çalışma süresi 5 yıldan daha az olanların mobil cihaz ve eposta kullanım güvenliği puanlarından ($\bar{x}$=3,885) yüksek bulunmuştur.

Çalışanların bilişim sektöründe çalışma süresine göre bakıldığında, lisanslı yazılım güvenliği puanları anlamlı farklılık göstermektedir. Farkın nedeni; bilişim sektöründe çalışma süresi 11 yıl ve üzeri olanların lisanslı yazılım güvenliği puanlarının ($\bar{x}$=2,906), bilişim sektöründe

çalışma süresi 5 yıldan daha az olanların lisanslı yazılım güvenliği puanlarından ($\bar{x}$=2,324) yüksek olmasıdır.

Yine genel bilgi güvenliği farkındalığına göre bilişim sektöründe çalışma süresi yüksek olanların farkındalığı, 5 yıldan daha az tecrübeli olanlara göre daha yüksektir.

Çalışanların sosyal paylaşım güvenliği, internet web kullanımı güvenliği, ağ güvenliği, kişisel bilgisayar güvenliği, güvenli şifre kullanımı, veri depolama güvenliği, bankacılık işlemleri ve online alışveriş güvenliği puanları bilişim sektöründe çalışma süresine göre anlamlı farklılık göstermez ($p>0.05$).

Yılmaz'ın çalışmasına bakıldığında öğretmenlerin meslekteki tecrübe yılının artmasının bilgi güvenliği farkındalığı üzerinde anlamlı bir etkisi olmadığı görülmüştür. Ancak burada dikkat edilmesi gereken husus, bu çalışmanın katılımcılarının bilişim sektörü çalışanlarından oluştuğudur. Kullanıcıların sürekli bilgi ve iletişim teknolojileri ile iç içe olduğu düşünüldüğünde, bu sonucun anlamlı olduğu düşünülmektedir.

Alzamil'in 2012 yılında Suudi Arabistan'da bilgi teknolojileri çalışanları ile yaptığı çalışmada genel olarak bilgi güvenliği farkındalığının çok düşük olduğu sonucu elde edilmiştir. Bu çalışmada ise genel olarak bilgi güvenliği farkındalığının yüksek olduğu sonucunu elde ettik. Bu noktada diyebiliriz ki Türkiye'deki bilişim çalışanlarının bilgi güvenliği farkındalığı Suudi Arabistan'dakilere göre oldukça iyi seviyededir.

6. Sonuç

Bu çalışmada bilişim sektörü çalışanlarının bilgi güvenliği farkındalıklarının yaş, cinsiyet, öğrenim düzeyi ve bilişim sektöründeki tecrübe yılına göre değişimi incelenmiştir. Bu doğrultuda 35 sorudan ve 9 alt faktörden oluşan, geçerliği ve güvenirliği testlerle kanıtlanmış bir ölçek geliştirilmiştir.

Oluşturulan bu Bilgi Güvenliği Farkındalığı Ölçeği'nden elde edilen verilerin analizi sonucu Türkiye'de bilişim sektöründe çalışanların bilgi güvenliği farkındalık seviyelerinin genel olarak yüksek olduğu görülmüştür.

Bu çalışmanın sınırlılığı, veri toplama süresinin sınırlılığından dolayı katılımcı sayısının da sınırlı kalmış olmasıdır. İleride yapılacak olan çalışmalara bir öneri olarak, Bilgi Güvenliği Farkındalığı ölçeğini daha fazla katılımcıya ulaştırarak bir farkındalık analizi çalışması yapılabilir.

KAYNAKLAR

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

(2) "Güncel Türkçe Sözlük", TDK. 2015. http://www.tdk.gov.tr

(3) "Büyük Türkçe Sözlük", TDK. 2012. http://www.tdk.gov.tr

(4) Vural Y. Kurumsal Bilgi Güvenliği ve Sızma Testleri [Yüksek Lisans Tezi]. Ankara: Gazi Üniversitesi 2008.

(5) Ciampra M. Security Awareness: Applying Practical Security in Your World. 3. Baskı USA: 2010.

(6) Şahinaslan E, Kandemir R, Şahinaslan Ö. Bilgi güvenliği farkındalık eğitimi örneği. 11. Akademik Bilişim Konferansı Bildirileri; 2012; Urfa. http://ab.org.tr/ab09/bildiri/117.pdf

(7) Çiftçi H. Her Yönüyle Siber Savaş. Tübitak Popüler Bilim Kitapları. Ankara, 2012.

(8) Şahinaslan Ö. Siber Saldırılara Karşı Kurumsal Ağlarda Oluşan Güvenlik Sorunu Ve Çözümü Üzerine Bir Çalışma [Doktora Tezi]. Edirne: Trakya Üniversitesi, 2013.

(9) Tunçbilek B. Bilişim Suçları Ve Üniversite Lisans Öğrencilerinin Bilişim Suçlarına Yönelik Görüşleri [Yüksek Lisans Tezi]. Ankara: Gazi Üniversitesi, 2012

(10) Canbek G, Sağıroğlu Ş. Bilgisayar Sistemlerine Yapılan Saldırılar Ve Türleri: Bir İnceleme. Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi 2007 Aralık; 23 (1-2) 1

(11) Canbek G, Sağıroğlu Ş. Kötücül Ve Casus Yazılımlar: Kapsamlı Bir Araştırma. Gazi Üniv. Müh. Mim. Fak. Der. 2007; 22(1) : 121-136.

(12) Yaşar H, Çakır H. Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri. Düzce Üniversitesi Bilim ve Teknoloji Dergisi 2015; 3: 488-507.

(13) Bilişim Sistemleri Güvenliği El Kitabı Sürüm 1.0. Türkiye bilişim derneği yayınları. Ankara:2006

(14) http://www.bilgiguvenlik.net/2012/04/zincir-e-posta-ve-internet-aldatmacas.html (03.06.2019)

(15) https://bilgiguvenligi.saglik.gov.tr/files/BGYS_Dokuman_Ornekleri/BG.PR...%20B%C4%B0LG%C4%B0%20G%C3%9CVENL%C4%B0%C4%9E%C4%B0%20%C4%B0HLA L%20OLAYLARI%20PROSED%C3%9CR%C3%9C.pdf (03.06.2019)

(16) https://www.iha.com.tr/haber-bilisim-suclari-uzmani-bile-dolandirildi-501940/ (13.07.2019)

(17) http://www.hurriyet.com.tr/gundem/birakilan-14luk-hacker-araniyor-41022567 (13.07.2019)

(18) http://www.haber7.com/teknoloji/haber/954347-lise-ogrencisinin-bilisim-sucu-sasirtti (13.07.2019)

(19) https://www.aa.com.tr/tr/turkiye/emekli-orgeneral-tolon-kendisini-dolandiranlarla-yuzlesti-/1322613 (13.07.2019)

(20) https://www.nytimes.com/2000/09/23/us/youth-sentenced-in-government-hacking-case.html (14.07.2019)

(21) https://www.theguardian.com/us-news/2018/mar/16/adrian-lamo-dead-chelsea-manning-wikileaks (14.07.2019)

(22) http://bidb.ahievran.edu.tr/dosyalar/BilisimSuclari.pdf (20.07.2019)

(23) https://internet.btk.gov.tr/turkiye-de-bilisim-hukuku (20.07.2019)

(24) https://www.turkhukuksitesi.com (21.07.2019)

(25) Öğütçü G. E-Dönüşüm Sürecinde Kişisel Bilişim Güvenliği Davranışı ve Farkındalığının Analizi [Yüksek Lisans tezi] Ankara: Başkent Üniversitesi, 2010.

(26) Tekerek M, Tekerek A. A Research on Students' Information Security Awareness. Turkish Journal of Education 2013, 2(3) :61-70

(27) Arıtürk M. Bilgi Farkındalığı Ve Bilgi Güvenliğinin Karşılaştırılması. 17. Akademik Bilişim Konferansı; 2015 Şubat 4-6; Eskişehir.

(28) Karaoğlan Yılmaz G, Yılmaz R, Sezer B. Üniversite Öğrencilerinin Güvenli Bilgi ve İletişim Teknolojisi Kullanım Davranışları ve Bilgi Güvenliği Eğitimine Genel Bir Bakış. Bartın Üniversitesi Eğitim Fakültesi Dergisi 2014, 3(1), 176-199.

(29) Çetin H. Kişisel Veri Güvenliği Ve Kullanıcıların Farkındalık Düzeylerinin İncelenmesi. Akdeniz İ.İ.B.F. Dergisi 2014, 86-105

(30) Yılmaz E. Öğretmenlerin Dijital Veri Güvenliği Farkındalığı [PhD tezi], Eskişehir: Anadolu Üniversitesi, 2015.

(31) Gökmen ÖF, Akgün ÖE. Bilgisayar ve Öğretim Teknolojileri Eğitimi Öğretmen Adaylarının Bilişim Güvenliği Bilgilerinin Çeşitli Değişkenlere Göre İncelenmesi. Çukurova Üniversitesi Eğitim Fakültesi Dergisi 2015; 44: 61-84.

(32) Güldüren C. Yükseköğretim kurumlarındaki öğretim elemanlarının Bilgi Güvenliği Farkındalık Düzeylerinin değerlendirilmesi [Doktora Tezi]. Ankara: Ankara Üniversitesi,2015.

(33) Güldüren C, Çetinkaya L, Keser H. Ortaöğretim Öğrencilerine Yönelik Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması. İlköğretim Online 2016; 15(2): 682-695.

(34) Bıkmaz Z. Sağlik Yönetimi Bölümü Öğrencilerinin Mobil Güvenlik Farkındalığı Ve Dijital Veri Güvenliği Farkındalıklarının Belirlenmesi. Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi 2017; 1(1):22-30

(35) Chan H, Mubarak S. Significance of Information Security Awareness in the Higher Education Sector**.** International Journal of Computer Applications 2012 Aralık; 60-10.

(36) Aloul F. The Need For Effective Information Security Awareness. Journal Of Intelligent Computing Research 2010; 1: 176-183

(37) Alzamil Z. Information Security Awareness at Saudi Arabians' Organizations: An Information Technology Employee's Perspective. International Journal of Information Security and Privacy 2012 Eylül; 6(3): 38-55

(38) Kim EB. Information Security Awareness Status of Business College: Undergraduate Students. Information Security Journal: A Global Perspective 2013; 22:171–179

(39) Farooq A, Isoaho J, Virtanen S. Information Security Awareness in Educational Institution: An Analysis of Students' Individual Factors. 14th IEEE Internatıonal Conference on Trust , Security and Privacy in Computing and Communications; 2015; Helsinki.

(40) Durkovic D, Milosevic M. An Analysis of User's Information Security Awareness. 7th International Scientific Conference Technics and Informatics in Education; 2018 Mayıs.

(41) Büyüköztürk, Ş. (2010). Sosyal Bilimler için Veri Analizi El Kitabı, Pegem Akademi Yayıncılık, Ankara.

(42) Şimşek ÖF. Yapısal Eşitlik Modellemesine Giriş, Temel İlkeler ve LİSREL Uygulamaları. (2007) , s.4-22. Ekinoks Yayınevi: Ankara.

(43) Sümer, N. (2000). Yapısal Eşitlik Modelleri. (2000) No.3, S.6, 49-74. Türk Psikoloji Yazıları, Ankara.

(44) Sümbüloğlu, K. Biyoistatistik. (1993), Özdemir Yayıncılık, Ankara.

(45) Tavsancıl, E. ve Keser, H. İnternet Kullanımına Yönelik Likert Tipi Bir Tutum Ölçeğinin Geliştirilmesi. Eğitim Bilimleri Dergisi 2002; 1 (1), 79- 100.

(46) Field, A. (2000). Discovering Statistics Using SPSS for Windows.(2000), Sage Publications, London.

(47) Çokluk, Ö., Şekercioğlu, G. ve Büyüköztürk, Ş. (2012). Sosyal Bilimler İçin Çok Değişkenli İstatistik: SPSS ve Lisrel Uygulamaları. (2012), Pegem Akademi Yayıncılık, Ankara.

(48) Karakoç,F.Y., Dönmez, L. (2014) Ölçek Geliştirme Çalışmalarında Temel İlkeler. Tıp Eğitimi Dünyası, 40: 39-49.

(49) Ercan,İ., Kan,İ. (2014). Ölçeklerde Güvenirlik ve Geçerlik. Uludağ Üniversitesi Tıp Fakültesi Dergisi 2014; 40: 39-49.

(50) Özdamar, K. Paket Programlar İle İstatistiksel Veri Analizi. (2004), Kaan Kitabevi, Eskişehir.

(51) https://biruni.tuik.gov.tr/medas/?kn=124&locale=tr (28.07.2019)

EK - Bilgi Güvenliği Farkındalığı Ölçeği

Bu anket çalışması, İstanbul Üniversitesi Adli Tıp Enstitüsü'nde yürütülen bir yüksek lisans tezi kapsamında, bilişim sektöründe çalışan kişilere uygulanmak üzere hazırlanmıştır.

Elde edilecek bilgiler yalnızca bu bilimsel çalışma kapsamında kullanılacaktır.

BÖLÜM 1

1.Yaşınız?

- 25 ve altı
- 26-35 arası
- 36-45 arası
- 46 ve üzeri

2.Cinsiyetiniz?

- Kadın
- Erkek

3. En son mezun olduğunuz eğitim derecesi?

- Lise
- Ön lisans
- Lisans
- Yüksek Lisans
- Doktora

4. Bilişim sektöründe kaç yıldır çalışıyorsunuz?

- 5 yıldan daha az
- 5-10 yıl arası
- 10-15 yıl arası
- 15 yıldan fazla

BÖLÜM 2

		Evet	**Hayır**
1	Herhangi bir şifrenizi sizden başkası biliyor mu?		
2	Kişisel bilgisayarınız şifre korumalı mı?		
3	Akıllı telefonunuz şifre korumalı mı?		
4	Kullandığınız cihazlarda antivirüs programı yüklü müdür?		
5	Kullandığınız cihazlarda güvenlik duvarı açık mıdır?		

BÖLÜM 3

		Kesinlikle Katılıyorum	**Katılıyorum**	**Kararsızım**	**Katılmıyorum**	**Kesinlikle Katılmıyorum**
1	Bilgisayarımdan uzaklaşacağımda şifre korumalı ekran koruyucuyu aktifleştiririm.					
2	Şifre ile giriş yapılan hesaplarda şifreyi 'Otomatik Hatırla' özelliğini kullanmam. (Şifremi kaydetmemesine dikkat ederim.)					

3	Aynı kullanıcı adı ve şifreyi birden fazla hesabımda kullanmam.					
4	İşim bittiği zaman hesaplarımdan (e-posta, sosyal ağ vs.) güvenli çıkış bağlantısı ile çıkış yaparım.					
5	Bilgisayarımdaki önemli dosyalara şifre koyarım.					
6	Bilgisayarda işim bittiği zaman log off/turn off/shut down ile kapatırım.					
7	Kendime ait bilgisayar dışındaki bilgisayarlardan kullanıcı adı ve şifre gerektiren işlemlerimi yapmam.					
8	E-posta eklerini açmadan önce					

	virüs taraması yaparım.					
9	E-posta eklerini açmadan önce uzantılarına dikkat ederim.					
10	Bir banka ya da ticari kuruluştan gelse bile e-postalardaki linklere tıklamam.					
11	Gelen SMS'lerdeki linklere tıklamam.					
12	İndireceğim uygulamalar hakkındaki kullanıcı yorumları ve indirme sayısına dikkat ederim.					
13	Web adres çubuğunda farklı yönlendirme olup olmadığını kontrol ederim.					
14	Ziyaret ettiğim web sitelerinin güvenlik sertifikalarını					

	kontrol ederim.					
15	Tarayıcı eklentilerini devre dışı bırakırım.					
16	Reklam engelleyici eklentiler kullanırım.					
17	İndirdiğim dosyaları virüs taramasından geçiririm.					
18	Sosyal ağ hesaplarının e-posta adres defterini taramasına izin vermem.					
19	Üyelik gerektiren sitelere (sosyal ağ vs.) kaydolmadan önce gizlilik politikası ve kullanım şartlarını okurum.					
20	Tanımadığım kişileri ağıma eklemem.					
21	Tanımadığım					

	kişilerin ağına eklenmekten çekinirim.					
22	İnternet ortamında iletişim bilgilerimi/kişisel bilgilerimi paylaşmam.					
23	Cihazlarımda kablosuz ağlara otomatik bağlanma özelliği kapalıdır.					
24	Ortak kullanıma açık kablosuz ağlara bağlıyken şifre gerektiren işlemler yapmam.					
25	Halka açık/şifre istemeyen kablosuz internet erişimine bağlanmam.					
26	Kablosuz modem şifremi belirli aralıklarla değiştiririm.					
27	Kablosuz internetimi					

	başkalarının kullanımına açmam.					
28	Online alışveriş yaparken sanal kart kullanırım ve sanal kartıma limit belirlerim.					
29	Online alışverişte 3 boyutlu güvenlik (3D secure) yöntemi kullanırım.					
30	İnternet bankacılığı kullanırken/kredi kart bilgilerimi girerken sanal klavye tercih ederim.					
31	Ücretsiz film, müzik, yazılım indirmem.					
32	Korsan/crack yazılım kullanmam.					
33	'Kullanıcı sözleşmesini okudum.' kabul metnini okumadan onaylamam.					

34	Flash bellekleri veri saklamak için kullanmam.					
35	USB bellekleri çıkarırken ‘Donanımı güvenle kaldır’ seçeneğini kullanırım.					

Özgeçmiş

Bireysel Bilgiler

Adı : Halime

Soyadı : CEYLAN

Doğum yeri ve tarihi : Çankaya – 10.08.1989

Uyruğu : Türkiye Cumhuriyeti

E-posta : halimeceylan89@gmail.com

Eğitim Durumu

2015- - Yıldız Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği (Y.L.)

2014- - İstanbul Üniversitesi, Adli Tıp Enstitüsü, Fen Bilimleri (Y.L.)

2007-2013 Orta Doğu Teknik Üniversitesi, Fen Edebiyat Fakültesi, Matematik

2003-2007 Süleyman Demirel Anadolu Lisesi

Yabancı Diller

İngilizce: Çok iyi

Rusça: Başlangıç seviyesinde

İspanyolca: Başlangıç seviyesinde

Sertifikalar

2017 - İleri Ofis Programları

2017 - Görsel Programlama (C#)

2018- Algoritma ve Programlama