BAŞKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

E-DÖNÜŞÜM SÜRECİNDE KİŞİSEL BİLİŞİM GÜVENLİĞİ DAVRANIŞI VE FARKINDALIĞININ ANALİZİ

GİZEM ÖĞÜTÇÜ

YÜKSEK LİSANS TEZİ
2010

E-DÖNÜŞÜM SÜRECİNDE KİŞİSEL BİLİŞİM GÜVENLİĞİ DAVRANIŞI VE FARKINDALIĞININ ANALİZİ

ANALYSIS OF PERSONAL INFORMATION SECURITY BEHAVIOR AND AWARENESS IN E-TRANSFORMATION PROCESS

GİZEM ÖĞÜTÇÜ

Başkent Üniversitesi
Lisansüstü Eğitim Öğretim ve Sınav Yönetmeliğinin
İstatistik ve Bilgisayar Bilimleri Anabilim Dalı İçin Öngördüğü
YÜKSEK LİSANS TEZİ
olarak hazırlanmıştır.

2010

Fen Bilimleri Enstitü Müdürlüğü'ne

Bu çalışma, jürimiz tarafından **İSTATİSTİK VE BİLGİSAYAR BİLİMLERİ ANABİLİM DALI 'nda YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Başkan :.....
Prof. Dr. Zehra MULUK

Üye (Danışman) :.....
Doç. Dr. Özlem Müge AYDIN

Üye :.....
Yrd. Doç. Dr. Güvenç ARSLAN

ONAY

Bu tez 13 / 08 / 2010 tarihinde, yukarıdaki jüri üyeleri tarafından kabul edilmiştir.

..... / 0 / 2010
Prof. Dr. Emin AKATA
FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ

TEŞEKKÜR

Sayın Doç. Dr. Özlem Müge AYDIN' a ve Dr. Ali ARİFOĞLU' na tez konusu seçiminden sonuçların yorumlanmasına kadar her süreçte yol gösterici, motive edici ve yardımcı oldukları için,

Aileme eğitim hayatım boyunca verdikleri manevi ve maddi her türlü destek için,

Sayın Bölüm Başkan'ım Prof. Dr. Ali HALICI' ya ve Jüri Başkan'ım Prof. Dr. Zehra MULUK' a tez süresince bilgi ve deneyimlerini paylaştıkları ve verdikleri her türlü destek için,

Türkiye Bilişim Güvenliği Derneği Yönetim Kurulu Başkanı Sayın Faruk KEKEVİ' ye tez sürecinde verdiği destek için,

Yönetim Bilişim Sistemleri Bölümü öğrencisi Derya Yıldız'a anket uygulaması veri girişinde verdiği destek için,

Teşekkürü borç bilirim.

ÖZ

E-DÖNÜŞÜM SÜRECİNDE KİŞİSEL BİLİŞİM GÜVENLİĞİ DAVRANIŞI VE FARKINDALIĞININ ANALİZİ

GİZEM ÖĞÜTÇÜ
Başkent Üniversitesi Fen Bilimleri Enstitüsü
İstatistik ve Bilgisayar Bilimleri Anabilim Dalı

Bu çalışmada e-dönüşüm sürecinde bilgi sistemlerini aktif olarak kullanan grupların bilişim güvenliğine yönelik risk içeren teknolojileri kullanımları, kendilerini risklerden ne şekilde korudukları, herhangi bir bilişim suçuna maruz kalıp kalmadıkları ya da olumsuz bir tecrübe yaşayıp yaşamadıkları ve bazı bilişim teknolojilerini ne derece tehlikeli algıladıkları araştırılmaya çalışılmıştır.

Araştırma kapsamında geliştirilen ölçekler anket formu aracılığıyla Türkiye genelindeki Başkent Üniversitesi kurum ve kuruluşlarında çalışan akademik ve idari personel ile Başkent Üniversitesi öğrencilerine uygulanmıştır.

Anket formu aracılığıyla katılımcılara ilişkin demografik veriler, katılımcıların internet kullanım alışkanlıklarına yönelik veriler, riskli davranış ölçeğine, korumacı davranış ölçeğine, suça maruziyet ölçeğine ve tehlike algısı ölçeğine ilişkin veriler toplanmıştır.

Araştırma sonuçları, geliştirilen ölçekler bazında örneklemler arasında kullanım alışkanlıklarına göre anlamlı farklılıklar olduğunu göstermektedir.

ANAHTAR SÖZCÜKLER: Kişisel Bilişim Güvenliği, Bilişim Güvenliği Farkındalığı, E- Dönüşüm

Danışman: Doç. Dr. Özlem Müge AYDIN, Başkent Üniversitesi, Fen Edebiyat Fakültesi, İstatistik ve Bilgisayar Bilimleri Bölümü

Eş Danışman: Dr. Ali Arifoğlu, Ortadoğu Teknik Üniversitesi, Enformatik Enstitüsü, Bilişim Sistemleri Bölümü

ABSTRACT

ANALYSIS OF PERSONAL INFORMATION SECURITY BEHAVIOR AND AWARENESS IN E-TRANSFORMATION PROCESS

GİZEM ÖĞÜTÇÜ
Başkent University Institute of Science
The Department of Statistics and Computer Science

This study has been carried out in an effort to research, the usage of applications techniques that may contain threats to information security during e-transformation by the active mass users of information systems, how the users protect themselves from these threats, whichever information offence they may be exposed to or whether they had a negative experience or to what extent some information techniques perceive risks.

The scale developed from the content of the survey were applied generally in Turkey to the students and academic and management staff of University of Başkent and its other organizations through a survey form.

The demographic data concerning the participants, the data concerning habits of internet usage of the participants, risk behaviour scale, conservative behaviour scale, exposure to offence scale and the data concerning risk perception scale were collected by the survey forms.

The results of the survey show that on the base of developed scales, there are significant differences within samples and according to their habits of internet usage.

KEY WORDS: Personal Information Security, Information Security Awareness, E-Transformation

Supervisor: Assoc. Prof. Özlem Müge AYDIN, Başkent University, Faculty of Science and Letters, Department of Statistics and Computer Sciences

Co-Advisor: Dr. Ali Arifoğlu, Middle East Technical University, Informatics Institute, Department of Information Systems

İÇİNDEKİLER LİSTESİ **SAYFA**

ÇİZELGELER LİSTESİ **SAYFA**

1. GİRİŞ

Son yıllarda bilgi ve iletişim teknolojilerinde yaşanan hızlı gelişim ve maliyetlerin düşmesi bu teknolojileri çok daha ulaşılabilir ve kullanılabilir bir konuma getirmiştir. 2009 yılı Comscore verilerine göre yaklaşık 6.6 milyar olan dünya nüfusunun 1.07 milyarı, oransal olarak bakıldığında ise dünya nüfusunun %16.2' si internet kullanmaktadır [1]. 2009 yılı Nisan ayı Hane Halkı Bilişim Teknolojileri kullanımı araştırma verilerine göre Türkiye'deki hanelerin %30'u internet erişim imkânına sahiptir [2]. Tüm bu istatistikler birlikte değerlendirildiğinde internetin aynı hızla bireylerin hayatında vazgeçilmez bir konuma geldiği söylenebilmektedir.

İnternet teknolojisinin başlangıcı, 1969 yılında Amerika Savunma Bakanlığı'nın soğuk savaş ya da sıcak çatışma esnasında daha güvenli ve kesintisiz haberleşmeyi sağlamak için oluşturduğu "Arpanet" adında bir projedir. Bu proje, 1983 yılında Arpanet projesinde görevli Dr. Vinton Cerf'in TCP/IP Protokolü üzerindeki çalışmalarını bitirmesinden sonra, sivil platformlara taşınmış ve 80'li yıllardan itibaren de denetimsiz olarak hızla gelişen bir biçimde günlük hayatta yerini almıştır [3]. Günümüzde birçok işlem internet ve çeşitli bilgi teknolojileri aracılığı ile gerçekleştirilmekte ve bu sayede insan hayatı kolaylaştırılmaktadır. İnternetin tasarımı ve kontrolsüz gelişmesi nedeniyle birçok tehdit ile de karşı karşıya kalınmaktadır. Bu tehditler yalnızca internet kullanımı ile ilgili değil, aynı zamanda dijital çağ olarak adlandırılan bu dönemde tüm verilerin dijital ortamlara taşınması ve daha çok verinin daha küçük aygıtlar üzerinde saklanabilir, taşınabilir, çoğaltılabilir hale gelmesi ile de ilgilidir [4].

Geçmişte kâğıt ortamında, mekânsal bağlılık gerektiren işlemler, günümüzde mekândan bağımsız olarak dijital ortamlarda gerçekleştirilebilmektedir. Yeni iletişim teknolojileri, sosyal ağlar ve elektronik uygulamalar birey hayatını da dijital ortama taşımıştır. Dolayısı ile temel olarak veri, korunması gereken bir e-varlık biçimine dönüşmüştür. Birey hayatının dijital ortama taşınması ile kişisel veriler de bu ortamlarda kontrolsüz yığınlar olarak serbestçe dolaşmaya başlamışlardır. Bütün bunlar ile diğer yanda teknolojinin uygunsuz kullanımı ve bireylerin bilgi güvenliği tehditlerine yönelik farkındalık seviyelerinin düşük olması nedeniyle telafisi güç bilgi güvenliği riskleri ve siber suçlar ortaya çıkmaya başlamış, bireyler

dijital hayata karşı kendilerini korumak zorunda kalmışlardır. Aynı zamanda uluslar da tüm bu tehditlere ve bu tehditlerin olası sonuçlarına karşı vatandaşını yasalar önünde koruma altına almak zorunda kalmış, hatta uluslararası işbirliğine gidilmiştir.

E- devlet' e geçilen bu dönemde tüm bu gelişmeler ulusal bilgi güvenliği açısından da tehlike yaratmaktadır. Kasım-Aralık 2004 Türkiye İnternet Güvenliği Araştırması sonuçlarına göre özellikle ülkemizde birçok kurum ve kuruluşun ve her seviyeden bilgisayar kullanıcısının bilgi güvenliğine bakış açısının yeterli seviyede olmadığı tespit edilmiştir [5]. Bu bağlamda bilgi güvenliği sağlamak için bilgi teknolojilerine dayalı olarak gerek yazılımsal gerekse donanımsal birçok koruma yöntemi geliştirilmiştir. Bu sayede bilginin yazılımsal veya donanımsal açıklardan sömürülmesi oldukça zorlaştırılmıştır. Bir takım tehditler, teknik çözümler geliştirilerek ortadan kaldırılmaya çalışılmıştır. Ancak son zamanlarda bu açıkların sömürülmesi yerini bireyin sömürülmesi aracılığıyla bilginin kötüye kullanımına bırakmıştır. Tehditlerden son zamanlarda sıkça duyulan ve örnekleri görülen sosyal mühendislik, güvenliğin en zayıf halkası olan bireyleri hedef almaktadır. Bilgi güvenliğinin sağlanması oldukça zordur ve bu anlamda bilgi güvenliğinin en zayıf halkası tehdide doğrudan veya dolaylı olarak maruz kalan eğitimsiz ya da bilinç eksikliği olan bireylerdir. Temel olarak güvenlik bir ürün değil, bir süreçtir [6]. Dahası, güvenlik bir teknoloji sorunu değildir; bir insan ve yönetim sorunudur [7].

Şahinaslan ve arkadaşları tarafından yapılan araştırma sonucuna göre 2007 yılındaki kurum içinde bilinçli ya da bilinçsiz bir şekilde yapılan güvenlik istismarlarının oranı, farkındalık eğitimleri sonucunda %59'dan %44'e kadar düşürülmüştür [8].

Güvenliği anlayabilmek için önce bilginin bir değeri olduğunu kavramak gerekir. Birey kendisi için değerli olmayan hiçbir unsuru korumak istemez. Bu nedenle güvenlik konusundaki en önemli unsurlardan biri şüphesiz ki farkındalıktır. Bilgi güvenliği riskleri hiçbir zaman tam olarak yok edilemese de geliştirilen yazılımsal ya da donanımsal yöntemlerin dışında bireylerde bilişim güvenliği farkındalığının gelişmesi veya geliştirilmesi ve bu bilincin davranışa dönüşmesi ile kabul edilebilir bir düzeye indirilebilir [8].

Bu çalışmada amaç, bireylerin özellikle internet ve bilgi teknolojilerini kullanımlarına ilişkin davranışlarını belirleyebilmek ile farkındalıklarını ve algılarını ölçmektir. Çalışmanın ikinci bölümünde genel olarak araştırma için önemli olduğu düşünülen kavramlar ve konular açıklanmıştır. Önceki çalışmalar ve literatürdeki boşluklara çalışmanın üçüncü bölümünde değinilmiştir. Çalışmanın dördüncü bölümünde ise, araştırma ile ilgili gerek anket tasarımı gerek örneklem büyüklüklerinin hesaplanması konuları ayrıntılı olarak açıklanmıştır. Pilot çalışma ve sonuçlarına da aynı bölümde yer verilmiştir.

Yapılan araştırma sonucunda elde edilen verilere ilişkin analizler ve bulgular ayrıntılı olarak çalışmanın beşinci bölümünde açıklanmıştır. Ankete katılan cevaplayıcılara ilişkin temel istatistikler, frekans değerleri, çapraz tablolar gibi detaylı analizler aynı bölüm içinde verilmiştir.

Çalışmanın son bölümü olan sonuç ve öneriler kısmında, araştırma sonuçları, öneriler ve ileriye dönük yapılması planlanan çalışmalara değinilmiştir.

2. BİLGİ VE BİLGİNİN ÖZELLİKLERİ

Bilgi kelimesinin kaynağı, Latince'deki herhangi bir şeye şekil vermek anlamına gelen "informare" kelimesinden gelmektedir. Sözlük anlamıyla bilgi; "Öğrenme, araştırma ve gözlem yoluyla elde edilen her türlü gerçek, malumat ve kavrayışın tümü" olarak tanımlanmaktadır [9].

Bilgi; tarih boyunca insanoğlunun düşüncesini, yaşayışını, gelişimini belirleyen faktörlerin başında gelen büyük bir güç olarak yerini korumuştur [9]. Veri ve bilgi kavramsal olarak karıştırılmakta, çoğu kez eş anlamda kullanılmaktadır. Bilgi kavramsal boyutta incelendiğinde veri, enformasyon ve bilgi kavramlarının açıklanması gerekmektedir. Veri; gözlemlenebilen, ölçülebilen veya hesaplanabilen bir davranış ya da tutuma ait değerdir [10].

Bilgiyi daha doğru tanımlayabilmek için benzer kavramların tanımlanması ve aralarındaki farkların irdelenmesi gerekir.

Enformasyon; elde edilebilen, filtrelenen ve işlemden geçirilen verilerdir [10]. Bilgi ise sosyal varlık olan insanlar arasındaki iletişim sırasında paylaşılan, aktarılan ve yeniden şekillendirilen tecrübelerdir. Belirli bir durum, sorun, ilişki, teori veya kurala ait veri ve enformasyonlardan oluşan anlayışlardır. Bilgi bilgisayardan daha çok insan beyninde yer almaktadır [10].

Bilişim; insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla, düzenli ve ussal biçimde işlenmesi bilimidir. Bilgi olgusunu, bilgi saklama, erişim dizgeleri, bilginin işlenmesi, aktarılması ve kullanılması yöntemlerini, toplum ve insanlık yararı gözeterek inceleyen uygulamalı bilim dalıdır [11].

Disiplinler arası özellik taşıyan bir öğretim ve hizmet kesimi olan bilişim, bilgisayar da dâhil olmak üzere bilişim ve bilgi erişim dizgelerinde kullanılan türlü araçların tasarlanması, geliştirilmesi ve üretilmesiyle ilgili konuları da kapsar. Bunun yanı sıra her türlü endüstri üretiminin özdevimli olarak düzenlenmesine ilişkin teknikleri

kapsayan özdevin alanına giren birçok konuda geniş anlamda, bilişimin kapsamı içerisinde yer alır [11].

Bilgi teknolojileri; bilginin toplanması, işlenmesi, saklanması ve gerektiğinde herhangi bir yere iletilmesi ya da herhangi bir yerden bu bilgiye erişilmesini elektronik, optik, bilgisayar yongası gibi tekniklerle kendiliğinden sağlayan, bilgisayar, genel ağ, cep telefonları, banka kartları, akıllı kartlar, telefonla sesli yanıt sistemleri, sayısal yayınlar gibi teknolojiler bütünüdür [11].

Bilgi teknolojileri açısından değerlendirildiğinde sayısal ve mantıksal her bir değerin bir veri olduğu, bilginin ise bu verinin işlenmiş, anlamlı hale gelmiş, açıkça tariflenmiş şekli olduğu kabul edilmektedir [4].

Kişisel veri; kişinin kendisi hakkında bilinmesini ya da bilinebilmesini sağlayan her türlü bilgi ve enformasyon içeren verilerdir [12]. Yani TC kimlik numarası, araç plaka bilgisi, GSM numarası vb. günlük hayatta sıklıkla paylaşmaktan çekinilen birçok bilgi aslında kişisel bilgidir. Bu bilgilerin kanunlar tarafından korunması ise bir kişilik hakkıdır.

Burada önemli bir kavram da veri ya da enformasyon mahremiyetidir. Veri mahremiyeti kişi hakkındaki bilginin toplanması, kullanılması, iletilmesi gibi unsurları bünyesinde barındırır [12].

Bilişim suçları ile mücadelede de bilişim güvenliği farkındalığı ve davranışı kuşkusuz çok önem taşımaktadır.

Bilişim suçu kavramı oldukça karışık terimleri bünyesinde barındıran bir kavramdır. Ülkemizde de bilişim suçu tanımıyla ilgili kavram karmaşası yaşanmaktadır. Bilişim suçu, bilgisayar suçu, sanal suç, internet suçu, bilişim sistemi aracılığıyla işlenen suç vb. isimleri almaktadır [13].

Bilişim suçlarının Avrupa'daki ilk tanımı ise şu şekildedir; AET Uzmanlar Komisyonu'nun 08 Mayıs 1983 tarihindeki Paris Toplantısı'nda yaptığı tanımlamaya göre; "Bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde kanun dışı, ahlakî olmayan ve yetki dışı gerçekleştirilen her

türlü davranıştır.” şeklindedir. Genel anlamda bilişim suçları tanımı ise; her türlü teknoloji kullanılarak, kanuni olmayan yollarla kişisel ya da kurumsal bilgisayarlarda, sistemler üzerinde zarar verici etki bırakmak şeklindedir. Bilişim teknolojilerinde suç meydana gelebilmesi için mutlaka teknoloji kullanılmalıdır. Bu teknoloji bilgisayar, kredi kartı, telefon, pos makinesi, elektronik bir cihaz olarak düşünülebilir [14].

Bilişim suçlarının hukuki tanımı ve TCK’deki yeri; “Bilgileri otomatik bir sisteme tabi olan bilgisayar, bilgisayar programları ile iletişim teknolojilerinin verilerini hukuka aykırı bir biçimde ele geçiren, ele geçirerek değiştiren, yok eden, erişilmez kılan böylece bir başkasının zarara uğratılmasının sağlanması veya kendisine ve başkasına maddi bir çıkar sağlanması bilişim suçunu oluşturmaktadır.” şeklindedir. 5237 sayılı Türk Ceza Kanunu’nda ayrı bir başlık halinde düzenlenen bilişim suçları kanunun 243, 244 ve 245. maddeleri ile tanımlanmaktadır [14].

2.1. Bilginin Bulunduğu Ortamlar

Gelişen bilgi ve iletişim teknolojileri sayesinde bilgi mekândan bağımsız olarak çok kolay erişilebilir, iletilebilir, işlenebilir bir hale gelmiştir. Bilişim güvenliğinin önemli bir parçası bilginin bulunduğu ortamların farkındalığıdır. Genel olarak bilginin yer aldığı ortamlar:

- Fiziksel Ortamlar: Kâğıt, tahta, pano, faks, çöp, kâğıt kutuları, dolaplar, masalar gibi ortamlardır. Kısacası bilgiye temas edilebilen ortamlardır.
- Elektronik ortamlar: Bilgisayarlar, notebooklar, mobil cihazlar, e-postalar, USB, CD, medya kartları vb. manyetik ortamlar.
- Sosyal ortamlar: Telefon görüşmeleri, sohbetler, yemek araları, toplantılar, toplu taşıma araçları vb. bireylerin bilgiye duyarak ya da görerek ulaşabildikleri ortamlardır.
- Tanıtım platformları: İnternet siteleri, broşürler, bültenler, reklamlar, sunular, eğitimler, görseller vb. ortamlardır.

Bilginin bulunduğu ortamlar yalnızca bu gruplandırma ile sınırlı değildir. Bireyin olduğu ve iletişimin gerçekleştiği her ortamda bir bilgi mevcuttur [4].

2.2. Bilgi Güvenliği

Bilgi güvenliği; bilgiye sürekli olarak erişilebilirliğin sağlandığı bir ortamda, bilginin göndericisinden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlüğünün sağlanması ve güvenli bir şekilde iletilmesi süreci bilgi güvenliği olarak tanımlanabilir [15].

Bir diğer ifade ile veri güvenliği, verinin toplanması, son kullanıcıya ulaşması, saklanması ve kullanımı aşamalarında her türlü tehdit ve tehlikelerden korunması; bu amaçla önceden alınacak tedbirler ve saldırı halinde yapılabilecek işlemlerin tümünü kapsayan bir disiplin olarak tanımlanabilir [16].

Bilgi teknolojilerinde yaşanan gelişmeler, daha çok bilginin depolanmasına ve taşınmasına imkân verebilir hale gelmiştir. Çok fonksiyonlu, küçük ama marifeti büyük teknolojik cihazlar sayesinde her geçen gün daha fazla bilgi elektronik ortama aktarılmakta, depolanmakta, işlenmekte, hizmete sunulmakta ve taşınabilmektedir [4].

İnternet kullanımının giderek artması, birçok prosedürün dijital ortamda gerçekleşmesini sağlamış ve e-devlet, e-ticaret, e-bankacılık gibi kavramların oluşmasına neden olmuştur. Bu kavramlar bünyesinde insanların, oturdukları yerden birçok işlerini yapabilmesi, yüksek derecede öneme sahip bilgilerin de internet ortamına aktarılması sonucunu doğurmuştur [17]. Bu bilgi akışında sınırların olmaması bilgi güvenliğini ciddi boyutta tehlikeye sokmuştur [6].

Bilginin elektronik ortamlar ve internet üzerinde yoğun kullanımı ve hareketliliği günümüzde bireyler, kurumlar ve uluslar açısından çeşitli güvenlik risk ve sorunlarını da beraberinde getirmektedir. Bu durum her geçen gün artış göstermekte, teknolojik ilerlemelere paralel olarak; gerek kişisel gerek ulusal bilgi güvenliğinin sağlanması önemli hale gelmektedir. Bilgi, korunması gereken bir unsur halini almıştır. ISO/IEC 17799’ da "...Bilgi, çıktı halinde veya kâğıda yazılı bir halde elektronik ortamda kayıtlı bir halde, posta yoluyla veya elektronik olarak gönderilmiş halde, sinema ve televizyon aracığıyla gösterilerek veya konuşmalar sırasında olduğu gibi herhangi bir yapıda bulunabilir. Hangi yapıda bulunursa

bulunsun veya nasıl kayıt ediliyor veya saklanıyorsa saklansın, bilgi sürekli olarak uygun bir şekilde korunmalıdır." ifadesi yer almaktadır [15].

2.3. Bilgiyi Koruma Unsurları

ISO 270001 standardında bilginin korunması gereken temel unsurları olarak; gizlilik, doğruluk, bütünlük, özgünlük ve erişilebilirlik (kullanılabilirlik) unsurları gösterilmiştir.

Gizlilik; bilginin yetkisiz kişilerin eline geçmesinin engellenmesidir. Hem kalıcı ortamlarda (disk, kaset vb.) saklı bulunan veriler hem de ağ üzerinde bir göndericiden bir alıcıya gönderilen veriler için söz konusudur. Saldırganlar yetkileri olmayan verilere birçok yolla (Parola dosyalarının çalınması, sosyal mühendislik, bilgisayar başında çalışan bir kullanıcının ona fark ettirmeden özel bir bilgisini ele geçirme, parolasını girerken gözetleme gibi) erişebilmektedirler. Bunun yanında trafik analizinin, yani hangi gönderici ile hangi alıcı arası haberleşmenin olduğunun belirlenmesine karşı alınan önlemler de gizlilik hizmeti çerçevesinde değerlendirilir [18].

Veri bütünlüğü, bilginin kendine has özelliklerinin ve doğruluğunun korunmasını ifade eder. Diğer bir ifade ile verinin göndericiden çıktığı haliyle alıcıya ulaşmasıdır. Bu durumda veri, haberleşme sırasında izlediği yollarda değiştirilmemiş, araya yeni veriler eklenmemiş, belli bir kısmı ya da tamamı tekrar edilmemiş ve sırası değiştirilmemiş şekilde alıcısına ulaşır [18].

Erişilebilirlik unsuru ise; veriye erişim yetkisi bulunan kişilerce istenildiğinde ulaşılabilir ve kullanılabilir olma özelliğidir. Diğer bir ifade ile kişilerin erişim yetkileri dâhilinde olan verilere, veri tazeliğini yitirmeden, zamanında ve güvenilir bir şekilde ulaşabilmesidir [4].

Bu temel unsurların yanı sıra ikinci planda değerlendirilebilecek bir takım unsurlar da mevcuttur. Bu kapsamda açıklanabilecek bir unsur olan izlenebilirlik, bilgisayar sistemi ya da ağı üzerinde olan herhangi bir faaliyeti, gerçekleşen olayları daha sonra analiz edilmek üzere kayıt altına almayı ifade etmektedir. Bir

sistemde olabilecek olaylar için kullanıcının parolasını yazarak sisteme girmek, bir web sayfasına bağlanmak, e-posta almak, göndermek ya da MSN ile mesaj yollamak gibi örnekler verilebilir. Toplanan olay kayıtları üzerinde yapılacak analizler sonucunda, bilinen saldırı türlerinin örüntüler olup olmadığına ya da bulanık mantık kullanılarak daha önce rastlanmayan ve saldırı olasılığı yüksek bir aktivite tespit edilip edilmediğine bakılabilir. İzlenebilirlik terimi yerine “emniyet” terimi de kullanılmaktadır [18].

Ağ güvenliği açısından kimlik sınaması; alıcının, göndericinin iddia ettiği kişi olduğundan emin olması şeklinde tanımlanabilir. Bunun yanında, bir bilgisayar programını kullanırken bir parola girmek de kimlik sınaması çerçevesinde değerlendirilebilir. Günümüzde kimlik sınaması, sadece bilgisayar ağları ve sistemleri için değil, fiziksel sistemler için de çok önemli bir hizmet haline gelmiştir. Akıllı karta ya da biyometrik teknolojilere dayalı kimlik sınama sistemleri yaygın olarak kullanmaya başlanmıştır [18].

Bir diğer unsur olarak güvenilirlik, sistemin beklenen davranışı ile elde edilen sonuçlar arasındaki tutarlılık durumu olarak tanımlanabilir. Başka bir deyiş ile güvenilirlik, kullanılan sistemden ne elde edilmek isteniyorsa sistemin kişiye o sonucu eksiksiz ve fazlalıksız olarak her seferinde aynı şekilde verebilmesini ifade eder [18].

Özellikle eş zamanlı olarak gerçekleştirilen sistemlerde kullanılan inkâr edememe unsuru gönderici ve alıcı arasındaki anlaşmazlıkları en aza indirmeyi amaçlamaktadır. Alıcının ya da göndericinin aldığı ya da gönderdiği hiçbir bilgiyi inkâr edememesi temeline dayanır [18].

Belirtilen unsurlar mevcut bilgi ve iletişim teknolojilerine karşı geliştirilmiş olan potansiyel tehditlere karşı bir koruma sağlamayı amaçlamaktadır. Teknolojinin hızlı değişimi ve geliştirilen tehditler farklılaştıkça yeni korunma unsurları da ortaya çıkabilecektir.

Bilişim güvenliğinin sağlanabilmesi için fiziksel güvenliğin, iletişim güvenliğinin, bilgisayar güvenliğinin, veri güvenliğinin ve bilişim güvenliği farkındalığını bir bütün olarak sağlanması gerekir.

2.4. Bilişim Güvenliğine Yönelik Tehditler

Bilişim güvenliğine yönelik tehditlerle ilgili bir sınıflandırma yapmak oldukça güçtür. Doğru kullanılmadığı takdirde her türlü teknoloji bir tehdit haline dönüşebilir. Mevcut ve güncel tehditler alt başlıklarda açıklanmıştır.

2.4.1. Kullanıcı tabanlı tehditler

Kullanıcı tabanlı siber ihlal yöntemleri, bilişim sistemlerine herhangi bir saldırgan yazılım veya sistemdeki güvenlik açıkları gibi teknik unsurlar kullanmadan doğrudan kullanıcıların dikkatsizlik, dalgınlık veya tecrübesizlik gibi zayıf yönlerini dikkate alarak uygulanan erişim tekniklerdir.

2.4.1.1. Şifre ve gizli soru tahmini

Yetkisiz erişim amacıyla en yaygın olarak kullanılan yöntem, şifre veya şifreye erişim için kullanılan gizli soru yanıtının tahmin edilmesidir. Birçok bilişim sistemi, kullanıcıların şifrelerini unutmaları durumunda kullanılmak üzere bir gizli soru ve yanıt ikilisinin tanımlanmasını istemektedir. Günümüzde telefon bankacılığı işlemlerinde banka yetkilileri tarafından sorulan anne kızlık soyadı, gizli soru ve yanıt ilişkisinin en yaygın örneğidir [20].

2.4.1.2. Omuz sörfü

Kullanıcıların bilişim sistemlerine erişim şifrelerini yazarken gözlenmesi, gizlice izlenmesi, ajanda, post-it, not kâğıtları gibi şifre yazılabilecek materyallerin incelenmesi şeklinde uygulanan bir yöntemdir. Bunların dışında sosyal mühendislik kapsamında da sayılabilecek bir diğer tehdit olarak çöp kurcalama (Dumpster Diving) sayılabilmektedir. Bu teknik ile hedef hakkındaki muhasebe kayıtları, fotokopi kâğıtları üzerinden iletişim bilgileri vb. bilgilere ulaşmak amaçlanmaktadır [21].

2.4.2. Yazılım tabanlı tehditler

Yazılım tabanlı tehditler, kötü amaçlı olarak geliştirilen, çoğunlukla veri hırsızlığına yönelik tasarlanan, bilgi sistemine bulaştıktan sonra yazılımı geliştirene bilgi aktaran tehditler olarak düşünülebilir.

2.4.2.1. Virüsler

Bir programa eklenmiş küçük kod parçacığı olarak tanımlanabilir. Virüsler iletişim ağında kendilerini kopyalayarak ya da kendilerini başka programlara ekleyerek kolaylıkla yayılabilmektedirler [16]. Virüslerin çalışmaya kısa süreliğine ara verilmesine neden olan zararsız sayılabilecek etkileri olduğu gibi, sistemlerde ciddi yok edici etkileri de olabilmektedir. Diğer kötücül yazılımlardan en önemli farkları insan etkileşimine ihtiyaç duymalarıdır [19].

Kullanıcılar bir dosyanın açılması, bir e-postanın okunması, bir programın çalıştırılması ile farkına varmadan virüslerin yayılmasına neden olmaktadırlar. Virüs geliştiricilerin çok çeşitli amaçları olabilmektedir. Bunlardan bazıları; zarar verme amacı, belli bir firmanın belli bir ürününe zarar verme amacı, politik mesaj verme amacı, ticari kazanç elde etme amacı ve bilgi çalma amacı olarak düşünülebilir [20].

2.4.2.2. Kurtçuklar

Yapıları virüslere benzemektedir, ancak diğer ismiyle solucanlar yayılmak için virüslerde olduğu gibi insan etkileşimine ihtiyaç duymamaktadırlar. Solucanların aşırı çoğalmaları ancak sistem kaynaklarının aşırı kullanımından dolayı sistemin yavaş çalıştığı fark edildiğinde anlaşılmaktadır [16]. Solucanlar e-posta solucanları, IM (Internet Messaging) solucanları, internet solucanları ve ağ solucanları olarak dört ana grup altında değerlendirilmektedirler [19].

2.4.2.3. Truva atları

Genelde gerekli bir program gibi gözüken ama arka planda yok edici etkisi olan kötücül yazılımlardır. Virüsler veya solucanlar gibi çoğalarak yayılamamaktadırlar

[19]. Çoğu kez kullanıcının ikna edilmesi ile programın bizzat kullanıcının kendi isteği ile çalıştırılması ile sisteme girmektedirler.

2.4.2.4. Servisi engelleyen saldırılar

Bu saldırı türünde (Denial of Service: DoS), sistemdeki programlara virüs bulaşmamaktadır. Ancak sisteme kapasitesinin üstünde yük bindirilerek sistemin kullanılmaz hale gelmesi hedeflemektedir. Örneğin, 10 dakika içinde 100.000 e-posta gelmesi durumunda e-posta hizmeti veren sunucular işlevlerini göremez hale gelebilmekte ve sistem yaygın tabiriyle “çökebilmektedir” [16].

2.4.2.5. Casus yazılımlar

Casus yazılımlar, yerleştikleri sistemlerde kendilerini gizleyerek, trojanlar aracılığı ile arşivlenmiş dosyaları, klavye kaydediciler (keylogger) aracılığı ile klavyeden yapılan tuş vuruşlarını, ekran kaydediciler (screenkogger) aracılığı ile fare ile işlem yapılan ekran görüntülerini kopyalayarak bu bilgileri yazılımı geliştiren kişiye gönderen kötücül yazılımlar olarak tanımlanabilmektedir [19]. Kişisel bilgi güvenliğini en çok tehdit eden saldırı türü olarak değerlendirilmelidirler.

2.4.2.6. Arka kapılar

Truva atları ile karşılaştırılan arka kapılar, bir bilgisayar üzerinde sıradan incelemelerle bulunamayacak şekilde, normal kimlik kanıtlama süreçlerini atlatmayı veya kurulan bu yapıdan haberdar olan kişiye kurulu olduğu sisteme uzaktan erişmeyi sağlayan yöntemler olarak bilinmektedirler [19]. Arka kapılar üreticisinin belirlediği gizli bir geçişe olanak verdikleri için bağlantı onayı (connection authentication) veya elektronik ileti benzeri uygulamalar için de geçerlidir [16].

2.4.2.7. Tarayıcı soyma

URL zerki (URL injection) olarak da adlandırılan tarayıcı soyma (Browser Hijacking), İnternet tarayıcı ayarlarını her zaman veya sadece belirli bölgeler için, kullanıcının belirlediği tarzın dışında davranmasına yol açan yazılımlardır. Bu, en basit olarak, tarayıcı açıldığında gösterilen başlangıç sayfasını, istenilen sitenin adresi ile değiştirilmesi olarak görülebilmektedir. Bunun dışında uygunsuz içerik veya reklâm içeren istemsiz olarak açılan pencereler (pop-up window) gösteren tarayıcı soyma türleri de bulunmaktadır [19].

2.4.2.8. Telefon çeviriciler

Telefon çeviriciler (Dialers), kurbanlarına büyük miktarlarda telefon ücreti ödetmek amacıyla, genellikle milletlerarası uzak mesafe telefon numaralarını, hedef bilgisayar modeminin internet servis sağlayıcısının bağlantı numarası ile değiştirilmesi aracılığıyla gerçekleştirilmektedir. Her zaman yaptığı gibi İnternet'e bağlanan kişi, aslında farklı bir hattı kullandığının geç farkına vardığında, çok büyük miktarlarda telefon faturası ile karşılaşabilmektedir. Bazı telefon çeviriciler ise, tuş basım bilgilerini ve şifre gibi önemli kişisel bilgileri, kullanıcının belli bir süre aktif olmadığı bir aralıkta, telefon hattı kullanarak korsana gönderilmesini sağlayabilmektedirler [19].

Bunlar dışında güncel kötücül yazılımlar arasında, reklâm yazılım (adware), parazit yazılım (parasiteware), hırsız yazılım (thiefware), püsküllü bela yazılım (pestware), tarayıcı yardımcı nesnesi (Browser Helper Object, BHO), uzaktan yönetim aracı (Remote Administration Tool, RAT), ticari RAT (commercial RAT), bot ağı (botnet), ağ taşkını (flooder), saldırgan ActiveX (hostile ActiveX), saldırgan Java (hostile Java), saldırgan betik (hostile script), IRC ele geçirme savaşı (IRC takeover war), nuker, paketleyici (packer), ciltçi (binder), şifre yakalayıcılar (password capture), şifre soyguncular (password hijacker), şifre kırıcılar (password cracker), anahtar üreticiler (key generator), e-posta bombalayıcı (mail bomber), kitle postacısı (mass mailer), e-posta adres hasatçısı (E-mail harvester), web böcekleri (web bugs), aldatmaca (hoax), sazan avlama (phishing), web sahtekârlığı (web scam) ve dolandırıcılığı (fraud), telefon kırma (phreaking, phone breaking), port tarayıcılar (port scanner), sondaj aracı (probe tool), arama motoru

soyguncusu (search hijacker), koklayıcı (sniffer), kandırıcı (spoofer), casus yazılım çerezleri (spyware cookie), iz sürme çerezleri (tracking cookie), turta (PIE), damlatıcı (trickler), savaş telefon çeviricileri (war dialer) ve tavşanları (wabbit) saymak mümkündür [19].

2.5. Sosyal Mühendislik

İnsanlar her işte olduğu gibi güvenlik söz konusu olduğunda da her zaman başrolü oynamaktadır. Bilgisayar ve ağ güvenliği açısından sosyal mühendislik, insan davranışındaki unsurları güvenlik açıkları olarak değerlendirip, bu açıklardan faydalanma yöntemiyle güvenlik süreçlerini aşarak sistem yöneticisi ya da kullanıcıların yetkilerine erişim tekniklerini kapsayan bir terimdir [20].

Tanınmış bir sosyal mühendis olan Kevin Mitnick' e göre araştırmacılar sürekli olarak daha iyi güvenlik teknolojileri geliştirip teknik güvenlik açıklarını sömürmeyi zorlaştırınca, saldırganlar insan unsurunu sömürme yoluna daha çok gideceklerdir [7].

Söz konusu sosyal mühendislik olunca bireysel farkındalığın önemi daha da çok artmaktadır. Kişiler risk içeren bir takım bilgi teknolojilerini kaçınılmaz olarak kullanmak zorundadırlar ve kendilerini korumaları için kilit nokta, riskin farkında olmalarıdır.

2.5.1. Sahte e-posta

Fake mail olarak da adlandırılan sahte e-postaların amacı çoğunlukla insanların dalgınlığından faydalanarak kişinin çok kullandığı iletişim hizmetlerine ilişkin kullanıcı adı ve şifre bilgilerinin ele geçirilmesidir. Özellikle e-postalara ya da MSN Messenger gibi uygulamaların şifrelerini ele geçirmek için kullanılır. Kişiye sanki kendi e-posta hesabından geliyor gibi görünen bir e-posta gönderilir. Kişi e-posta ile gelen linke tıkladıktan sonra e-posta hesabına ilişkin kullanıcı adı ve şifresini soran taklit bir sayfa açılır ve kişinin bu bilgileri girmesi ile girilen bilgiler sahtekârlığı hazırlayan kişinin eline ulaşılır. Bir sosyal mühendislik türüdür ve temeli insanı kandırmaya dayalıdır.

2.5.2. Phishing

Bir internet sitesinin benzer bir web ismi de kullanarak taklit edilmesidir. Kişilerin gizli şifre ve mali bilgilerinin (kredi kartı numaraları vb.) elde edilmesi için sahtekârlarca hazırlanan bir tuzak ve aldatma yolu olarak görülebilmektedir. Elektronik ticaret veya bankacılık uygulamaları için sahte giriş ekranları oluşturularak ziyaretçilerin yanıltılması ve sonucunda kullanıcıya ait önemli bilgilerin ele geçirilmesi mümkün olabilmektedir [16].

2.5.3. Mesaj sağanakları

Mesaj sağanakları (spam, junkmail), belki de kullanıcıların günlük hayatta en sık karşılaştıkları ve sıkıntı çektikleri kötücül yazılımların başında gelmektedir. Spam e-postalar, reklâm, ürün tanıtım ve satma veya diğer kötü amaçlarla kişilerin e-posta hesaplarının istemedikleri türden, onayları alınmadan tanımadıkları kanallardan gelen e-postalarla meşgul edilmesidir [19].

2.5.4. Elektronik dolandırıcılık ve sosyal mühendislik

Günümüzde sosyal mühendislik uygulamaları sistemlere yetkisiz erişim ve kişisel bilgi temini amacıyla olduğu kadar, haksız kazanç elde etmek için de kullanılmaktadır. Cyberfraud olarak da adlandırılan, çeşitli ve sürekli olarak yenilenen senaryolar aracılığıyla yapılan saldırıların en yaygın örnekleri arasında yeşil kart, loto, kara para transferi, sahte ürün tuzakları bulunmaktadır [20].

2.5.5. Sosyal mühendislik ve bilgisayar virüsleri

Bazı bilgisayar virüsleri yayılma hızlarını artırmak için sosyal mühendislik tekniklerini kullanmaktadırlar. İlk örneği Win32/Sober adlı virüs olan söz konusu virüsler yerleştikleri bilgisayar sistemlerindeki belge adlarını inceleyerek bilgisayar kullanıcısının iş veya hobi niteliklerine uygun bir isimle kopyalarını adres defterindeki kişilere göndermektedir [20].

Sober virüsü için Microsoft'un web sitesinde “Bu solucan, kullanıcıları sosyal mühendislik yoluyla e-postadaki ekli bir dosyayı veya yürütülebilir dosyayı açmaya

ikna etmeye çalışır. Alıcı dosyayı ve yürütülebilir dosyayı açarsa, solucan kendisini sistemin adres defterindeki tüm kişilere gönderir.” açıklaması yapılmıştır [20].

2.5.6. E-posta aldatmacaları

Sıklıkla karşılaşılan sosyal mühendislik türlerinden biri olan zincir e-posta diğer adıyla hoaxların amacı, e-posta adresi toplamak ve toplanan e-postaları satmaktır. Gelen e-postada belirtilen sayıda gönderilmesi durumda hediye kazanılacağı, bir karşılık alınacağı gibi insan duygularını sömüren ifadeler bulunur [21].

3. ÖNCEKİ ÇALIŞMALAR

Bilgi ve iletişim teknolojilerindeki hızlı gelişim, güvenlik tehditlerini de beraberinde getirmiştir. Bu teknolojilerin bireyler tarafından kullanımı arttıkça bireylerin tehditlere maruz kalma olasılığı da yükselmektedir. Bu tehditler sonucunda maddi, manevi, ulusal ya da uluslararası birçok zarar oluşmaktadır. Bilişim güvenliğinin başlangıç noktası bireyler olduğu için ulusal güvenliğin sağlanabilmesi amacıyla öncelikle bireysel bilişim güvenliğinin sağlanması gerekmektedir.

Sağıroğlu ve Canbek' in [15] de çalışmalarında ifade ettikleri gibi, literatür incelendiğinde konuyla ilgili bir çok çalışma mevcut olsa da "bilgi ve bilişim sistemleri güvenliğinin" akademik ortamlarda yeterince tartışılmadığı ve konuya gereken önemin verilmediği tespit edilmiştir.

Güvenlik ve farkındalık çok yeni kavramlar olduğundan yapılan akademik çalışma sayısı oldukça sınırlı ve her biri kendi içinde anlamlı farklılıklar göstermektedir.

2005 yılında Furnell [22] ve arkadaşları tarafından, son kullanıcının Microsoft işletim sistemi üzerindeki güvenlik ayarlarıyla bağlantılı olan tehditlere karşı farkındalıklarını tespit etmeye yönelik olarak yapılan anket araştırması sonuçlarına göre, farkındalığın en yüksek olduğu tehdit virüs ve farkındalığın en düşük olduğu tehdit ise phishing saldırılarıdır. Araştırmaya katılanların %80,5'i 17-29 yaş aralığındadır ve yalnızca %30'u bilgisayar açılışında parola kullanmaktadır [22]. Günümüzde en yaygın saldırı türlerinden biri sosyal mühendisliğe dayanan phishing saldırılarıdır.

2006 yılında Hikmet Dijle [23] tarafından hazırlanan yüksek lisans tezi kapsamında yapılan anket araştırması verilerine göre çalışmaya katılan bireylerden %72,5'i lisanssız yazılım kullandığını, %81,3'ü internet üzerinden alışveriş yapmadığını, %86'sı herhangi bir phishing olayı ile karşılaşmadığını ifade etmiştir. Çalışmaya katılanların %51,7'si kullandıkları yazılımın kişisel verilerini internet üzerinden başkalarını iletilebileceğini düşünürken, %15,8'i güvenlik programının kendisini koruduğuna inandığını, %28,6'sı konu hakkında bilgisi olmadığını ifade etmektedir.

Katılımcıların %61'i dolandırıcılık suçunun en tehlikeli bilişim suçu olduğunu düşünmekte ve % 42,2'si hackerlik yapmak istediğini ifade etmektedir [23].

Gerek lisanssız yazılım kullanımı gerek dolandırıcılığın en önemli bilişim suçu olarak kabul edilmesi, bireylerin bilişim güvenliğine yönelik davranışlarında maddi unsurların önemini ortaya koymaktadır. Bu araştırmanın sonuçları değerlendirildiğinde kullanıcılarının konu hakkındaki bilgi düzeylerinin yeterli olmadığı görülmektedir. Aynı zamanda farkındalık ve davranışları arasında bir çelişki olduğu da düşünülmektedir. %75 lisanssız yazılım kullanımı çok büyük bir orandır, öncelikle lisanssız yazılım kullanımı bir bilişim suçudur. Lisanssız kullanılan yazılımlarda gerekli güvenlik güncelleştirmeleri yapılmamaktadır. Yüklü oldukları bilgisayarlar açısından büyük tehdit oluşturmaktadırlar. Bu kullanım oranına rağmen katılımcıların % 51,7'si kullandıkları yazılımların kişisel bilgilerini başkalarına ilettiğini düşünmektedir. Farkındalık ve davranış arasındaki çelişki burada görülmektedir.

2006 yılında Lars Bensmann tarafından yüksek lisans tezi kapsamında Türk kullanıcılarının parola eğilimlerine yönelik bir çalışma yapılmıştır. Parola; bir bilişim sisteminde kimlik sınama kontrolünün temel basamağıdır. Bugün en sık kullanılan erişim denetim yöntemi parola kullanıcı adı eşleşmesidir. Dolayısıyla güvenlik söz konusu olduğunda parola seçimi çok büyük önem taşımaktadır. Yapılan çalışma sonuçlarına göre; Türk kullanıcılara ait parolaların çoğu 7 karakterden az, tümü nümerik ya da tümü alfabetik, nümerik karakterlerle son bulmakta, uzunluğu 7 karakterden fazla olan parolalarda kullanıcı bilgisi, bilinen bir kelime, özel bir isim vb. farklı kullanıcıların da çok kolay tahmin edebileceği içerikte olduğu görülmektedir [24].

Hoonakker' ın [25] 2009 yılında yaptığı çalışmada belirttiği gibi son kullanıcıya dönük olarak yapılan araştırmaların çoğu ticari kaygılar taşımaktadır. Bu alanda yapılan akademik çalışma sayısı oldukça azdır. Günümüzde bilgi ve bilgisayar güvenliği gerek uluslar gerek bireyler açısından çok önemli bir noktada durmaktadır. Ancak ne yazık ki bu konudaki bilgi ve bilinç özellikle birey penceresinden bakıldığında çok düşük düzeydedir. Hoonakker'a göre inançların aksine önemli bir veri istismarı olan kimlik hırsızlığı %91 oranında çevrimdışı

kanallar aracılığı ile gerçekleştirilmektedir. Bunun yanı sıra kimlik hırsızlıklarının yalnızca %5'i virüsler, casus yazılımlar veya hackerlar tarafından, % 3'ü phishing saldırıları aracılığı ile gerçekleştirilmektedir [25].

Hoonakker' ın çalışmasında belirttiği Zhaung, Luo tarafından 2009 yılında yapılan bir araştırma kurumların % 86'sının kimlik tanıma için kullanıcı adı ve parola sistemlerini kullandığını göstermektedir. Bunun nedeni olarak güvenliği sağlamanın en kolay ve ucuz yolunun kullanıcı adı ve parola tanımlamaları olduğu görülmektedir. Ancak bu noktada önemli bir güvenlik zafiyeti ortaya çıkmaktadır. Hoonakker ve arkadaşlarının yaptığı çalışmada 1999 yılında ve 2006 yılında yapılmış olan çalışmaların sonucunda kullanıcıların kolay hatırlanabilir ve tahmin edilebilir şifreler kullandıkları görülmüştür. Aynı çalışmada atıfta bulunulan bir diğer araştırma sonucuna göre bir kurumda çalışanların %20'sinin kurum şifrelerini bir not kâğıdına yazılı olarak bilgisayar ekranlarına yapıştırdıkları görülmüştür. Aynı araştırma bireylerin %66'sı şifrelerini yazılı olarak kâğıtlarda, %58'sinin şifrelerini elektronik kâğıtlara yazarak sakladığı görülmüştür. Schneider güvensiz şifre (yalnızca harflerden oluşan) kullanımının neden olduğu sorunların son yirmi yıldır bilindiğini ancak bu konuda çok az yol alınabildiğini ifade etmektedir. Araştırmaların genelinde de görüldüğü gibi bireysel farkındalığın olmaması en büyük güvenlik zafiyetidir.

2006 yılında Chai ve arkadaşları [26] tarafından yapılmış olan bir araştırma kapsamında dört farklı sınıflandırma yapılmıştır. Birincisi kişilerin internet ve bilişim güvenliği ile ilgili deneyimleri, ikincisi bireylerin kendi bilişim güvenliği davranışlarına karşı olan yargıları, üçüncüsü bilgi güvenliği davranışının algılanan önemi ve son sınıf kullanıcıların kendilerini korumak için geliştirdikleri bilgi güvenliğine yönelik davranışlarıdır. Araştırmanın amacı bu sınıflar arasında anlamlı bir ilişki olup olmadığının tespit edilmesidir. Araştırma sonuçlarına göre kişilerin internet ve bilişim güvenliği ile ilgili deneyimleri ile bilişim güvenliği davranışlarına karşı olan yargıları arasında pozitif yönlü bir ilişki bulunmuştur. Ancak kişilerin internet ve bilişim güvenliği ile ilgili deneyimleri ile kendilerini korumak için geliştirdikleri bilişim güvenliğine yönelik davranışları arasında anlamlı bir ilişki bulunamamıştır [26].

İlkan ve arkadaşları [27] tarafından bir bilgi güvenliği farkındalığına yönelik olarak 2010 yılında yapılan araştırmada akademik personelin bilgi güvenliği farkındalığı ölçülmeye çalışılmıştır. Araştırmada Ryan tarafından 2006 yılında geliştirilen "Information Security Awareness (ISA)" ölçeği kullanılmıştır. Araştırma sonuçlarına göre akademik personelin farkındalık düzeyi yüksek bulunmuştur [27].

Yenisey ve arkadaşları [28] tarafından 2005 yılında Türk üniversite öğrencilerinin çevrimiçi alışveriş davranışlarına yönelik olarak bir araştırma yapılmıştır. Araştırma sonucuna göre çalışmaya katılan bireylerden %50'sinden daha fazlasının online alışveriş yapmama nedeni olarak kredi kartı numaralarının üçüncü şahıslar tarafından ele geçirilme ihtimali olduğu görülmüştür. Aynı çalışmada bireylerin yaş, isim, posta adresi gibi bilgileri paylaşmaktan rahatsızlık duymadıkları, ancak sosyal güvenlik numarası, telefon numarası ve kredi kartı numaralarını vermekten rahatsızlık duydukları tespit edilmiştir [28].

Şahinaslan [8] ve arkadaşlarının çalışmasında görülüyor ki, araştırma yapılan kurumda çalışan bireylerin %80'i farkında olmadan bilgi istismarına yol açmaktadır. En güncel tehditlerin ise, yerine bilgi sızdırma, bilgi hırsızlığı ve istihbarat çalışmalarının olduğu aynı çalışmada ifade edilmektedir [8].

Önceki çalışmalar değerlendirildiğinde görülmektedir ki, yapılan çalışmaların sonuçları çok değerli olmasına rağmen bilişim güvenliğini bir bütün olarak incelememektedirler. Oysa ki bilişim güvenliği, farkındalık ve davranışla bir bütün olarak incelenmelidir. Yalnızca parola güvenliği ya da lisanslı yazılım kullanımı güvenliği sağlamak ya da değerlendirmek için yeterli değildir. Farkındalık bilişim güvenliğini sağlamanın temel unsuru olsa da tek başına bir anlam ifade etmemektedir. Birey bazı güvenlik istismarlarının farkında olabilir, ancak bu bireyin korumacı bir davranış sergileyeceği anlamını taşımamaktadır. Bu nedenle bu araştırmanın tasarımı yapılırken farkındalık, davranış, bilişim suçuna maruziyet ve tehlike algısı bir bütün olarak değerlendirilmiştir.

4. KİŞİSEL BİLİŞİM GÜVENLİĞİ FARKINDALIĞI VE DAVRANIŞI İLE SUÇA MARUZİYETİN İNCELENMESİ

Bilişim güvenliğinin en zayıf halkası olarak görülen, eğitimsiz ya da bilinç eksikliği olan bireylerde, geliştirilen yazılımsal ya da donanımsal korunma yöntemlerin dışında bilişim güvenliği farkındalığının gelişmesi veya geliştirilmesi ve bu bilincin davranışa dönüşümünün sağlanması ile bilişim güvenliği risklerinin tam olarak ortadan kaldırılamasalar bile kabul edilebilir bir düzeye indirilebilecekleri düşünülmektedir.

Araştırma kapsamında öncelikle bireylerin bilişim güvenliğine dair farkındalık düzeyleri hem algısal hem de davranış boyutunda araştırılmıştır. Çalışmanın hedefi; bireylerin bilişim güvenliğine yönelik farkındalıkları ile bilgi ve iletişim teknolojilerini kullanma davranışları arasındaki ilişkinin yönünü, boyutunu tespit etmek ve bu ilişkiyi tanımlayan alt değişkenlerin kritik önemini ortaya koymaktır.

Bu çalışmanın üç temel sorgusu vardır:

- Bireylerin kişisel bilişim güvenliklerine yönelik tehlike algıları ile bilgi ve iletişim teknolojilerini, korumacı ya da riskli olmak üzere, kullanma davranışları arasındaki ilişkinin tutarlı olup olmadığını ve ilişkinin boyutlarını tespit etmektir. Daha açık bir ifade ile bu ilişkinin paralel olup olmadığını belirlemektir.
- Çalışmaya katılacak bireylerin bilişim suçuna maruz kalmaları durumunda ortaya çıkacak bilişim suçuna maruz kalma düzeyinin bireyin bilişim güvenliği farkındalığına ve bilişim teknolojilerini kullanma davranışına ne derece biçimlendirici bir etkisi olup olmadığını tespit etmektir.
- Çalışmaya katılan bireylerin bilişim güvenliği farkındalıkları ve bilgi teknolojilerini kullanma davranışlarının güncel durumunun gerekli oldukları farklı alt değişkenler için tespitini yapmaktır.

Bilişim güvenliği bilincinin genele yayılabilmesi için öncelikle bireylerin bilişim güvenliği farkındalıklarının ölçülmesi gerekmektedir. Ancak bireylerin herhangi bir durumun farkında olup olmamaları, farkındalıklarının gerekliliklerini yerine getirip getirmedikleri anlamını taşımamaktadır. Bu nedenle bireylerin bilişim güvenliğine

doğrudan etkisi olan bilgi ve iletişim teknolojilerini kullanma davranışları da incelenmelidir. Bu ilişkinin yönüne etki edebilecek bir unsur olarak bilişim suçuna maruz kalma düzeyi görülebilir. Ayrıca bilişim güvenliğine yönelik politikaların sağlıklı ve etkili bir şekilde düzenlenebilmesi için alt değişkenler olarak bireylerin konuya ilişkin davranışlarının, değerlerinin ve algılarının da tespit edilmesi ve değerlendirilmesi gerekmektedir. Bu sayede araştırma aracılığı ile yakın geleceği bugün olduğundan çok daha fazla etkileyecek olan; ulusal ve kişisel bilişim güvenliği, kişisel verilerin korunması, bilişim hukuku ve bilişim suçlarıyla mücadele konularına doğru analizler yapılabilmesi için veri sağlanmış olunacaktır.

4.1. Araştırma Tasarımı

Çalışmaya katılan bireylerin bilişim suçuna maruz kalması durumunda ortaya çıkan bilişim suçuna maruz kalma düzeyinin, bireyin bilişim güvenliği farkındalığı ile bilgi ve iletişim teknolojilerini kullanma davranışına ne derece biçimlendirici bir etkisi olup olmadığını tespitini yapmak hedeflenmektedir.

Bireylerin kişisel bilişim güvenliklerine yönelik farkındalıkları ile bilgi ve iletişim teknolojilerini kullanma davranışları arasındaki ilişkinin tutarlı olup olmadığını ve ilişkinin boyutlarını tespit etmek amaçlanmıştır. Daha açık bir ifade ile bu ilişkinin paralel olup olmadığını belirlemektir.

Çalışmaya katılan bireylerin bilişim güvenliği farkındalıkları ve bilgi teknolojilerini kullanma davranışlarının güncel durumunun gerekli oldukları farklı alt değişkenler için tespitini yapmaktır.

4.2. Pilot Çalışma ve Anket Tasarımı

Anket soruları taslak olarak hazırlandıktan sonra, Ocak-Şubat 2010 tarihleri arasında Başkent Üniversitesi İstatistik ve Bilgisayar Bilimleri Bölümü öğretim üyeleri, Türkiye Bilişim Güvenliği Derneği Başkanlığı, Emniyet Genel Müdürlüğü Bilişim Suçları Şube Müdürü ve bilgi güvenliği uzmanları tarafından incelenmiştir. Yapılan öneriler doğrultusunda anket formuna ilişkin gerekli düzenlemeler yapılmış

ve Akademik Bilişim 2010 konferansı öncesi düzenlenen Güvenlik Kursu'nda konusunda uzman 39 katılımcıya ve 23 akademisyene uygulanmıştır.

Yapılan testlerde anketin geçerlilik güvenilirliği incelenmiş ve Cronbach alfa değeri 0,9345 olarak hesaplanmıştır. Buna göre anketin uygulanabileceğine karar verilmiştir.

Anket formu;

- Demografik sorular,
- Katılımcıların bilişim teknolojileri ve bilgisayar güvenliği ile ilgili profillerinin belirlenmesine yönelik sorular,
- Katılımcıların bilişim teknolojilerine yönelik risk içeren davranış profillerinin belirlenmesine yönelik sorular,
- Katılımcıların bilişim güvenliğine ve tehditlere yönelik korumacı davranış düzeylerinin belirlenmesine yönelik sorular,
- Katılımcıların bilişim suçuna maruziyet düzeylerinin belirlenmesine yönelik sorular olmak üzere beş bölümden oluşmaktadır.

4.3. Örneklemin Belirlenmesi

Bireylerin kişisel bilişim güvenliği farkındalıklarına ve bilişim teknolojilerini kullanma davranışlarına yönelik olarak yapılan araştırma konusunun çalışma alanı olarak Türkiye genelinde birçok saygın eğitim ve sağlık kurumu olan Başkent Üniversitesi öğrencileri, akademik ve idari çalışanlarından oluşan bir örneklem seçilmiştir. Çalışma alanı olarak sağlık kurumları olan Ankara Başkent Hastanesi, Alanya Uygulama ve Araştırma Merkezi, Konya Uygulama ve Araştırma Merkezi, İzmir Zübeyde Hanım Uygulama ve Araştırma Merkezi, İstanbul Sağlık, Uygulama ve Araştırma Hastanesi, Ayaş Fizik Tedavi ve Rehabilitasyon Merkezi, Geriatri Psiko-Sosyal Rehberlik Merkezi ve son olarak Başkent Üniversitesi belirlenmiştir. Çalışma alanı seçiminde Başkent Üniversitesi'nin yer alma nedeni, gelecek 10 yıl içinde e-devlet sistemi içinde en aktif olan bireylerin 18-30 yaş arası "dijital yerliler" olduğunun öngörülmesidir. Dijital yerliler genellikle "ağ kuşağı" olarak anılan ve dijital medya ile büyümüş yeni nesli temsil etmektedirler [29]. Çalışma alanı olarak

sağlık kurumlarının seçilme nedeni ise; mevcut sistemde hassas kişisel verilerin en çok bulunduğu ortamların sağlık kurumları olduğunun düşünülmüş olunmasıdır. Bu gibi kurumlarda çalışan bireylerin kişisel veriler konusundaki farkındalıkları çok önem taşımaktadır.

Anket araştırması için öncelikle Başkent Üniversitesi Personel Daire Başkanlığı ve Öğrenci İşleri birimlerinden çalışan akademik ve idari personel ile öğrenci sayıları alınmıştır. Alınan sayılar doğrultusunda örneklem seçimine başlanmıştır. Eğitim kurumu olarak fakülte ve bölümler temel alınarak Başkent Üniversitesi öğrencileri, akademik ve idari personel seçilmiştir. Araştırmada örneklem birimi öğrenci, akademik personel ve idari personel olarak alınmış ve her birim için tabakalı örnekleme yöntemi kullanılarak örneklem büyüklüğü belirlenmeye çalışılmıştır.

Bu konuda benzer bir araştırma olmaması nedeniyle, anket sorularından herhangi birine cevap verme oranı 0.5 olarak alınmış ve heterojen bir dağılım gösterdiği varsayımı altında varyans σ^2=0.25 olarak alınmıştır. Anketteki bir sorudan tahmin edilecek bir oran tahmini ile gerçek oran değeri arasındaki farkı ortaya çıkarmada (d)0.05'lik bir hata hoş görüldüğünde, %95 güven olasılığı ile yapılan parametre tahminleri için başlangıç örneklem büyüklüğü aşağıdaki gibi;

$$\mathrm{n}_0 = \frac{\mathrm{z}^2_{\alpha/2}\mathrm{PQ}}{\mathrm{d}^2} = \frac{(1.96)^2(0.5)(0.5)}{(0.05)^2} = 384.16 \qquad (4.1)$$

olarak hesaplanmıştır.

Çalışmanın yapılacağı birimler akademik personel, idari personel ve öğrenciler olduğuna göre, her birime ilişkin örneklem hacimleri, kendi kitle popülasyonlarına göre ayrıca hesaplanmıştır.

Anketin uygulanacağı akademik personel sayısının belirlenmesinde N_A=1371 olduğu için, akademik personel örneklem hacmi;

$$n = \frac{n_0}{1+\frac{n_0}{N}} = \frac{384.16}{1+\frac{384.16}{11371}} = 300{,}0771 \qquad (4.2)$$

olarak hesaplanmıştır.

Cevaplayıcılara ulaşılamaması veya anketin cevaplanmaması olasılıkları da dikkate alınarak örneklem hacmi %10 oranında artırılmıştır. Buna göre n_A=(0.10).(300.0771) ≈ 330 değeri akademik personel için örneklem hacmi olarak kabul edilmiştir.

330 akademik personel, Başkent Üniversitesi, Ankara Başkent Hastanesi, Alanya Uygulama ve Araştırma Merkezi, Konya Uygulama ve Araştırma Merkezi, İzmir Zübeyde Hanım Uygulama ve Araştırma Merkezi, İstanbul Sağlık, Uygulama ve Araştırma Hastanesi, Ayaş Fizik Tedavi ve Rehabilitasyon Merkezi, Kolej Ayşe Abla' da görev yapan akademik personel sayılarına göre tabakalandırılmış ve sonuçlar Çizelge 4.1'de gösterilmiştir.

Çizelge 4.1 Uygulamanın Yapılacağı 330 Akademik Personelin Tabakalara (Çalıştıkları Kurumlara Göre) Dağılımları:

Kurum (Tabaka)	**Toplam Akademik Personel Sayısı**	**Örnekleme Alınan Akademik Personel Sayısı**
Başkent Üniversitesi	1125	271
Alanya Uyg. ve Araş. Merk.	27	7
Konya Uyg. ve Araş. Merk.	49	12
İzmir Zübeyde Hanım Uyg. ve Araş. Merk.	11	3
İstanbul Sağlık Uyg. Ve Araş. Merk.	54	13
Ayaş Fizik Ted. ve Reh. Merk.	2	2
Kolej Ayşe Abla	103	25
Toplam ≈	**1371**	**333**

Uygulamada yer alacak idari personel sayısı da akademik personel sayısına benzer şekilde; N_i=3684 olduğundan, n_i=348 ve bu sayı %10 artırılarak yaklaşık 380 olarak hesaplanmıştır. İdari personelin de çalıştıkları kurumlar tabakalar olarak alınıp, tabakalı örnekleme yapılmıştır. Bu doğrultuda elde edilen sonuçlar Çizelge 4.2' de verilmiştir.

Çizelge 4.2 Uygulamanın Yapılacağı 380 İdari Personelin Tabakalara (Çalıştıkları Kurumlara Göre) Dağılımları:

Kurum (Tabaka)	**Toplam Akademik Personel Sayısı**	**Örnekleme Alınan Akademik Personel Sayısı**
Başkent Üniversitesi	1982	205
Alanya Uyg. ve Araş. Merk.	406	42
Konya Uyg. ve Araş. Merk.	563	58
İzmir Zübeyde Hanım Uyg. ve Araş. Merk.	121	12
İstanbul Sağlık Uyg. Ve Araş. Merk.	424	44
Ayaş Fizik Ted. ve Reh. Merk.	90	9
Kolej Ayşe Abla	53	5
Geriatri Merk.	45	5
Toplam ≈	**3684**	**380**

Uygulamada yer alacak öğrenci sayısı da akademik ve idari personel sayısına benzer şekilde; $N_{ö}$=7557 olduğundan, $n_{ö}$=365.57 ve bu sayı %10 artırılarak yaklaşık 400 olarak hesaplanmıştır. Öğrencilerin okudukları fakülteler tabakalar olarak alınıp, tabakalı örnekleme yapılmıştır. Bu doğrultuda elde edilen sonuçlar Çizelge 4.3' de verilmiştir.

Çizelge 4.3 Uygulamanın Yapılacağı 400 Öğrencinin Tabakalara (Okudukları Fakültelere Göre) Dağılımları:

Fakülte (Tabaka)	**Toplam Öğrenci Sayısı**	**Örnekleme Alınan Öğrenci Sayısı**
Devlet Konservatuarı	73	4
Diş Hekimliği	114	6
Eğitim Fakültesi	1287	69
Fen-Edebiyat Fakültesi	311	17
Güzel Sanatlar Fakültesi	311	17
Hukuk Fakültesi	706	38
İktisadi ve İdari Bilimler Fakültesi	1005	54
İletişim Fakültesi	458	25
Mühendislik Fakültesi	1019	54
Sağlık Bilimler Fakültesi	1016	54
Ticari Bilimler Fakültesi	957	52
Tıp Fakültesi	300	10
Toplam ≈	**7557**	**400**

5. BULGULAR

Anket tasarımında farklı ölçekler geliştirilmiştir. Her bireye ilişkin her bir ölçekten elde edilen puanlar hesaplanmıştır. Birey puanlarının hesaplanmasında, beşli Likert tipi sorulara verilen cevaplar, soru kökünün olumlu ya da olumsuz olmasına göre derecelendirilerek puana çevrilmiştir.

Bilişim teknolojilerine yönelik risk içeren davranış profillerinin ölçülmesi için geliştirilen ölçeğe ait soruların tamamında ilgili bilişim teknolojilerinin kullanılması durumunda, kullanıcı için risk oluşturması durumu göz önünde tutulmuştur. Riskli davranış ölçeğini oluşturan sorular ekte bulanan anket formundaki 1,2, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 28, 29, 30, 32, 33 ve 36 numaralı sorulardır. Bu ölçek kapsamındaki sorularda “Her zaman” seçeneğinin puanı 5, “Sık sık” seçeneğinin puanı 4, “Bazen” seçeneğinin puanı 3, “Nadiren” seçeneğinin puanı 2 ve “Hiçbir zaman” seçeneğinin puanı 1 olarak alınarak bireylerin toplam puanları hesaplanmıştır. Bu durumda riskli davranış ölçeğinde bir cevaplayıcının alabileceği maksimum puan 100 ve minimum puan 20’dir. Puanlar maksimuma yaklaştıkça cevaplayıcının riske daha yüksek derecede açık olduğu ve minimuma yaklaştıkça ise riske daha düşük derecede açık olduğu anlaşılmaktadır.

Bilişim teknolojilerini kullanarak bireylerin kendilerini ilgili tehditlerden ne derece koruduğunu ölçmek amacıyla korumacı davranış ölçeği geliştirilmiştir. Korumacı davranış ölçeğini oluşturan sorular ekte bulunan anket formundaki 3, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 34, 35, 37, 38, 39, 40 ve 41 numaralı sorulardır. Soru sayısı ve seçenekler riskli davranış ölçeği ile aynı şekilde düzenlendiğinden puanlama da aynı şekilde yapılmıştır.

Bireylerin bilişim suçuna maruz kalıp kalmadığını ve yaşadıkları olumsuz tecrübeleri ölçmek üzere 15 sorudan oluşan suça maruziyet ölçeği geliştirilmiştir. Ölçek soruları ekte sunulan anket formundaki 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55 ve 56 numaralı sorulardır. Seçenekler diğer ölçeklerle aynı olduğundan puanlama da aynı şekilde yapılmıştır. Bu durumda suça maruziyet ölçeğinde bir cevaplayıcının alabileceği maksimum puan 75 ve minimum puan 15’ dir. Puanlar maksimuma yaklaştıkça cevaplayıcının suça ya da olumsuz tecrübeye

daha yüksek derecede maruz kaldığı ve minimuma yaklaştıkça ise suça daha düşük derecede maruz kaldığı anlaşılmaktadır.

Son olarak tehlike algısı ölçeği ile kendi içlerinde tehlike içeren ve yaygın olarak kullanılan bazı teknolojileri cevaplayıcıların ne derece tehlikeli bulduğunu ölçmek için geliştirilmiştir. Tehlike algısı ölçeğini oluşturan sorular ekte bulanan anket formundaki 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85 ve 86 numaraları sorulardır. Bu ölçek kapsamındaki sorular "Çok Tehlikeli" seçeneğinin puanı 5, "Tehlikeli" seçeneğinin puanı 4, "Az Tehlikeli" seçeneğinin puanı 3, "Tehlikesiz" seçeneğinin puanı 2 ve "Fikrim Yok" seçeneğinin puanı 1 olarak alınarak bireylerin toplam puanları hesaplanmıştır. Bu durumda tehlike algısı ölçeğinde bir cevaplayıcının alabileceği maksimum puan 125 ve minimum puan 25'dir. Puanlar maksimuma yaklaştıkça cevaplayıcının ilgili teknolojileri daha yüksek derecede tehlikeli bulduğu ve minimuma yaklaştıkça ise daha düşük derecede tehlikeli bulduğu anlaşılmaktadır.

Frekans dağılımları öncelikle demografik verilere göre daha sonra geliştirilen ölçeklere göre verilmiştir. Araştırmaya katılan bireylerin cinsiyete göre dağılımları Çizelge 5.1'de verilmiştir. Çizelge 5.1'e göre araştırmaya katılan 881 cevaplayıcının; 530 kişi ile % 60.2'si kadın ve 351 kişi ile %39.8'i erkektir.

Çizelge 5.1 Katılımcıların Cinsiyete Göre Dağılımları

CİNSİYET	**Sayı**	**Yüzde**
Kadın	530	60,2
Erkek	351	39,8
TOPLAM	**881**	**100,0**

Araştırmaya katılan Başkent Üniversitesi akademik personelinin yaş ortalaması 37.75, idari personelinin 30.60 ve öğrencilerinin 22.06 olarak hesaplanmıştır. Genel yaş ortalaması 28.14, en küçük yaş 18 ve en büyük yaş 77 olarak bulunmuştur. Cevaplayıcıların diğer yaş istatistikleri Çizelge 5.2'de verilmiştir.

Çizelge 5.2 Katılımcıların Yaş İstatistikleri

KİTLE	SAYI	ORTALAMA	STD. SAPMA	EN YÜKSEK	EN DÜŞÜK
Akademik	169	37,75	11,262	77	20
İdari	317	30,60	5,881	58	19
Öğrenci	395	22,06	2,197	36	18
TOPLAM	**881**	**28,14**	**8,677**	**77**	**18**

Cevaplayıcıların eğitim düzeylerine ilişkin sayı ve toplam içindeki yüzde değerleri Çizelge 5.3'te sunulmaktadır. Buna göre 881 cevaplayıcının %19.2'si akademik personel, %36'sı idari personel ve % 44,8'i öğrencidir. Araştırmaya katılan cevaplayıcıların %70.4'ü önlisans/lisans eğitim düzeyindedir.

Çizelge 5.3 Katılımcıların Eğitim Düzeylerine Göre Dağılımları

		ÖRNEKLEM GRUBU			
		Akademik	**İdari**	**Öğrenci**	**TOPLAM**
İlköğretim	**Sayı**	0	10	0	10
	Yüzde	***%0,0***	***%1,1***	***%0,0***	***%1,1***
Lise	**Sayı**	0	88	0	88
	Yüzde	***%0,0***	***10,0***	***%0,0***	***%10,0***
Önlisans/lisans	**Sayı**	21	204	395	620
	Yüzde	***%2,4***	***%23,2***	***%44,8***	***%70,4***
Yüksek lisans	**Sayı**	49	17	0	66
	Yüzde	***%5,6***	***%1,9***	***%0,0***	***%7,5***
Doktora	**Sayı**	93	4	0	97
	Yüzde	***%10,6***	***%0,5***	***%0,0***	***%11,0***
TOPLAM	**Sayı**	169	317	395	881
	Yüzde	***%19,2***	***%36,0***	***%44,8***	***%100,0***

Araştırmaya katılan bireylerin %22.36'sı güvenlik eğitimi aldığını, % 77.64'ü güvenlik eğitimi almadığını ifade etmiştir. Güvenlik eğitimi alanların %52.79'unu 104 kişi ile idari personeller oluşturmaktadır. Çizelge 5.4'te bilişim güvenliği eğitimi alma durumuna göre cevaplayıcı sayıları ve yüzde değerleri ayrıntılı olarak sunulmuştur.

Çizelge 5.4 Katılımcıların Bilişim Güvenliği Eğitimi Alma Durumuna Göre Dağılımları

		ÖRNEKLEM GRUBU			
		Akademik	**İdari**	**Öğrenci**	**TOPLAM**
Evet	**Sayı**	33	104	60	197
	Güvenlik eğitimi içindeki yüzde	***16,75***	***52,79***	***30,46***	***100,00***
	Görev içindeki yüzde	***20,25***	***32,20***	***15,19***	***22,36***
	Toplam içindeki yüzde	***3,75***	***11,80***	***6,81***	***22,36***
Hayır	**Sayı**	130	219	335	684
	Güvenlik eğitimi içindeki yüzde	***19,01***	***32,02***	***48,98***	***100,00***
	Görev içindeki yüzde	***79,75***	***67,80***	***84,81***	***77,64***
	Toplam içindeki yüzde	***14,76***	***24,86***	***38,02***	***77,64***
TOPLAM	**Sayı**	163	323	395	881
	Güvenlik eğitimi içindeki yüzde	***18,50***	***36,66***	***44,84***	***100,00***
	Görev içindeki yüzde	***100,00***	***100,00***	***100,00***	***100,00***
	Toplam içindeki yüzde	***18,50***	***36,66***	***44,84***	***100,00***

Araştırmaya katılan bireylerin %47.67'si karşılaştıkları bilişim suçlarını ilgili makamlara hiçbir zaman iletmediklerini ifade etmiştir. Çizelge 5.5'te sunulduğu üzere karşılaştıkları bilişim suçunu ilgili makamlara her zaman ilettiklerini ifade edenlerin %55.17'sini idari personeller oluşturmaktadır. Sonuçlar incelendiğinde karşılaşılan bir bilişim suçunu ilgili makamlara iletme oranının düşük olduğu görülmektedir. Bu doğrultuda kişilerin karşılaştıkları bir bilişim suçunu nereye ileteceklerini bilip bilmedikleri incelenmiştir. Bu sonuçlara göre katılımcıların %40.4'ünün bilişim suçunu nereye ileteceklerini bilmedikleri sonucuna ulaşılmıştır. Tüm cevaplayıcılar incelendiğinde ise öğrencilerin %43.3 oranı ile suçu nereye ileteceklerini bilmeyenler içinde en büyük yüzdeye sahip oldukları görülmektedir. Karşılaştığı bilişim suçunu nereye ileteceğini bildiği halde iletmeyen katılımcı oranı yalnızca %8.4'tür. Bu bulgular birlikte değerlendirildiğinde konu hakkındaki farkındalığın düşük olduğu görülmektedir.

Çizelge 5.5 Katılımcıların Karşılaştıkları Bilişim Suçlarını İlgili Makamlara İletme Durumlarına Göre Dağılımları

		ÖRNEKLEM GRUBU			
		Akademik	**İdari**	**Öğrenci**	**TOPLAM**
Hiçbir zaman	**Sayı**	88	148	184	420
	Suçu iletme içindeki yüzde	***20,95***	***35,24***	***43,81***	***100,00***
	Görev içindeki yüzde	***53,99***	***45,82***	***46,58***	***47,67***
	Toplam içindeki yüzde	***9,99***	***16,80***	***20,89***	***47,67***
Nadiren	**Sayı**	39	52	96	187
	Suçu iletme içindeki yüzde	***20,86***	***27,81***	***51,34***	***100,00***
	Görev içindeki yüzde	***23,93***	***16,10***	***24,30***	***21,23***
	Toplam içindeki yüzde	***4,43***	***5,90***	***10,90***	***21,23***
Bazen	**Sayı**	16	45	68	129
	Suçu iletme içindeki yüzde	***12,40***	***34,88***	***52,71***	***100,00***
	Görev içindeki yüzde	***9,82***	***13,93***	***17,22***	***14,64***
	Toplam içindeki yüzde	***1,82***	***5,11***	***7,72***	***14,64***
Sık sık	**Sayı**	5	30	23	58
	Suçu iletme içindeki yüzde	***8,62***	***51,72***	***39,66***	***100,00***
	Görev içindeki yüzde	***3,07***	***9,29***	***5,82***	***6,58***
	Toplam içindeki yüzde	***0,57***	***3,41***	***2,61***	***6,58***
Her zaman	**Sayı**	15	48	24	87
	Suçu iletme içindeki yüzde	***17,24***	***55,17***	***27,59***	***100,00***
	Görev içindeki yüzde	***9,20***	***14,86***	***6,08***	***9,88***
	Toplam içindeki yüzde	***1,70***	***5,45***	***2,72***	***9,88***
TOPLAM	**Sayı**	163	323	395	881
	Suçu iletme içindeki yüzde	***18,50***	***36,66***	***44,84***	***100,00***
	Görev içindeki yüzde	***100,00***	***100,00***	***100,00***	***100,00***
	Toplam içindeki yüzde	***18,50***	***36,66***	***44,84***	***100,00***

Araştırma kapsamında katılımcıların bilinçli kullanılmadığı takdirde her biri kendi içinde risk oluşturabilecek bilgi teknolojilerini kullanım düzeyleri incelenerek riskli davranış ölçeği içerisinde değerlendirilmiştir. Sonuçlar Çizelge 5.6'da ayrıntılı olarak sunulmuştur.

Çizelge 5.6 Riskli Davranış Ölçeğine İlişkin Soruların Frekans Dağılımları

SORULAR	Hiçbir zaman	Nadiren	Bazen	Sık sık	Her zaman
MSN Messenger, GTalk, Skype ve benzeri sohbet programlarını kullanırım.	111 ***%12.6***	126 ***%14.3***	194 ***%22.0***	170 ***%19.3***	280 ***%31.8***
Bir iletişim aracı olarak elektronik posta (e-mail) kullanırım.	39 ***%4.4***	52 ***%5.9***	120 ***%13.6***	223 ***%25.3***	447 ***%50.7***
Kurumsal e-posta adresimi günlük işlerde de kullanırım.	367 ***%41.7***	154 ***%17.5***	139 ***%13.8***	82 ***%9.3***	139 ***%15.8***
İnternette e-posta gruplarına üye olurum.	339 ***%38.5***	240 ***%27.2***	163 ***%18.7***	64 ***%7.3***	73 ***%8.3***
Facebook, Twitter ve benzeri sosyal ağ sitelerini kullanırım.	181 ***%20.5***	95 ***%10.8***	142 ***%16.1***	192 ***%21.8***	271 ***%30.8***
Sosyal ağlarda gönderilen uygulama davetlerini kabul ederim.	327 ***%37.1***	235 ***%26.7***	220 ***%25.0***	45 ***%5.1***	54 ***%6.1***
İnternet bankacılığı kullanırım.	330 ***%37.5***	126 ***%14.3***	141 ***%16.0***	94 ***%10.7***	190 ***%21.6***
İnternet üzerinden alışveriş yaparım.	345 ***%39.2***	171 ***%19.4***	193 ***%21.9***	85 ***%9.6***	87 ***%9.9***
E-Vatandaşlık hizmetleri veren web sayfalarını (TC kimlik no sorgulama, sosyal güvenlik primi sorgulama vb.) kullanırım.	129 ***%14.6***	146 ***%16.6***	265 ***%30.1***	163 ***%18.5***	176 ***%20.2***
İnternet üzerinden oyun oynarım	217 ***%24.6***	166 ***%18.8***	230 ***%26.1***	141 ***%16.0***	127 ***%14.4***
İnternet üzerinden müzik, film, program ve dosya indiririm/kaydederim.	115 ***%13.1***	142 ***%16.1***	179 ***%20.3***	199 ***%22.6***	246 ***%27.9***
İnternet üzerinden video/film izlerim.	155 ***%17.6***	133 ***%15.1***	197 ***%22.4***	199 ***%22.6***	197 ***%22.4***
İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM No, e-posta, Adres) paylaşırım.	313 ***%35.5***	252 ***%28.6***	191 ***%21.7***	61 ***%6.9***	64 ***%7.3***
İnternet ortamında gerektiği durumlarda özlük bilgilerimi paylaşırım. (Ad, Soyad, Doğum Tarihi vb…)	246 ***%27.9***	274 ***%31.1***	221 ***%25.1***	71 ***%8.1***	69 ***%7.8***
Sohbet (chat) yaparken dosya transferi yaparım.	296 ***%33.6***	155 ***%17.6***	218 ***%24.7***	127 ***%14.4***	85 ***%9.6***
Bilgisayarımdaki dosyaları paylaşıma açarım.	500 ***%56.8***	184 ***%20.9***	131 ***%14.9***	36 ***%4.1***	30 ***%3.4***
Halka açık internet erişimi olan yerlerde internet bankacılığı kullanırım.	661 ***%75.0***	111 ***%12.6***	63 ***%7.2***	22 ***%2.5***	24 ***%2.7***
Parolalarımı başkalarıyla paylaşırım.	588 ***%66.7***	163 ***%18.5***	81 ***%9.2***	28 ***%3.2***	21 ***%2.4***
Parolalarımı yazılı olarak kolay ulaşabileceğim yerlerde saklarım.	508 ***%57.7***	138 ***%15.7***	101 ***%11.5***	52 ***%5.9***	82 ***%9.3***
Tanımadığım kişilerden gelen e postaları açarım, gelen ekleri indiririm.	578 ***%65.6***	133 ***%15.1***	91 ***%10.3***	42 ***%4.8***	37 ***%4.2***

Buna göre araştırmaya katılan bireylerden % 31.8'i MSN Messenger, Gtalk vb. sohbet programlarını her zaman kullandıklarını, %12.6'sı ise hiçbir zaman kullanmadıklarını; %50.7'si her zaman bir iletişim aracı olarak e-mail kullandıklarını ve % 30.8'i her zaman sosyal ağ sitelerini kullandıklarını ifade etmiştir. Bu

sonuçlara göre internet ortamında iletişim kanallarının kullanımının yaygın olduğu görülmektedir. Phishing, hoax, spam gibi sosyal mühendislik saldırılarında e-posta kanalları kullanılmaktadır. Araştırma sonuçlarına göre bir iletişim aracı olarak e-mail kullanımı oldukça yaygındır. Bu durumda kişiler bu tür saldırılara karşı riske açık konumdadırlar.

Kötücül ve casus yazılımların yayılma kanallarından biri de sohbet programlarıdır. Sohbet programlarının kullanımının araştırma sonucuna göre yaygın olduğu görülmektedir. Ayrıca katılımcıların % 66.4'ü en az bir kez, sohbet esnasında dosya transferi yaptığını ifade etmiştir.

Özellikle sosyal ağlar günümüzde kişisel verilerin istismarı konusunda oldukça tartışılmaktadır. Buna rağmen araştırma geneline göre; katılımcıların %79.5'i en az bir kez sosyal ağ sitelerine üye olmuştur. (Sosyal ağ siteleri üyelik esasına göre çalışır, bir kez kullanabilmek için önce üye olmak gerekir.) Üye olduktan sonra kullanım oranları değişmektedir; ancak ilgili web sayfalarına üye olabilmek için birçok bilgi üye olurken başlangıçta kayıt edilmektedir. Ayrıca katılımcıların %62.9'u sosyal ağ sitelerinde gönderilen uygulama davetlerini kabul ettiklerini ifade etmiştir. Katılımcılardan % 35.5'i internet ortamında gerektiği durumlarda iletişim bilgilerimi paylaşırım ifadesine hiçbir zaman, %27.9'u internet ortamında gerektiği durumlarda özlük bilgilerimi paylaşırım ifadesine hiçbir zaman yanıtını vermiştir. Bu yanıtlar kişilerin iletişim bilgilerini, özlük bilgilerinden daha mahrem gördükleri kanısı uyandırmaktadır.

İnternet üzerinden dosya paylaşımı ve transferi de risk taşımakta ve çoğunlukla suç oluşturmaktadır. Özellikle herhangi bir bedel ödemeden yapılan dosya paylaşımı çoğu zaman beraberinde kötücül yazılımları da ilgili ortama taşımaktadır. Araştırma sonuçlarına göre katılımcıların %27.9'u her zaman, %22.6'sı sık sık, %20.3'ü de bazen internet üzerinden film, müzik, program ya da dosya transferi yaptığını, %56.8'i ise kendi bilgisayarlarındaki dosyaları hiçbir zaman paylaşıma açmadığını ifade etmiştir.

İnternet bankacılığı son yıllarda daha yaygın kullanılmaya başlanmış ve birçok güvenlik önlemi geliştirilmiştir. Araştırma sonuçlara da katılımcıların %62.5'inin en

az bir kez internet bankacılığı kullandığını, %25'inin ise halka açık internet erişimi olan yerlerde en az bir kez internet bankacılığını kullandığını göstermektedir.

Önceki çalışmalar kişilerin parolalarını yazılı olarak kolay erişebilecekleri yerlerde sakladıklarını ve başkaları ile paylaşmaktan çekinmediklerini göstermektedir. Ancak araştırma sonuçlarına göre katılımcıların % 66.7'si parolalarını hiçbir zaman başkaları ile paylaşmadığını ve % 57.7'si hiçbir zaman parolalarını yazılı olarak kolay erişebilecekleri yerlerde saklamadıklarını ifade etmiştir. Halen en yaygın erişim güvenlik metodunun kullanıcı adı-parola eşleşmesi olduğu düşünülürse kişilerin bu konudaki farkındalıklarının arttığı görülmektedir.

İnternet üzerinden alışveriş son yıllarda oldukça popüler bir alışveriş yöntemi halini almıştır. Katılımcıların % 60.8'i en az bir kez internet üzerinden alışveriş yaptığını, % 39.2'si ise hiçbir zaman internet üzerinden alışveriş yapmadığını ifade etmiştir.

Elektronik devlete geçiş sürecinde birçok vatandaşlık işlemi artık devlet portalları aracılığı ile yapılabilmektedir. Araştırma sonuçları değerlendirildiğinde katılımcıların %85.4'ünün en az bir kez bu portalları kullandığını görülmektedir.

Son yıllarda bilişim suçlarında hızlı bir artış yaşanmaktadır. Özellikle elektronik dolandırıcılık suçu internet kullanan ve kendini korumayan bireyleri tehdit etmektedir. Bu gibi bilişim suçlarından ve kötü tecrübelerden bireylerin kendilerini ne şekilde korudukları ve konu hakkındaki farkındalıkları önemli bir husustur. Bilişim teknolojileri doğru kullanılmadıkları ve gerekli önlemler alınmadığı takdirde risk içermektedir. Ancak günümüz koşullarında bu teknolojilerin kullanılmaması neredeyse imkânsız hale gelmiştir. Bu nedenle bireylerin korumaya yönelik davranışları korumacı davranış ölçeği ile ölçülmeye çalışılmış ve hesaplanan frekans değerleri Çizelge 5.7' de sunulmuştur.

Çizelge 5.7 Korumacı Davranış Ölçeğine İlişkin Soruların Frekans Dağılımları

SORULAR	Hiçbir zaman	Nadiren	Bazen	Sık sık	Her zaman
Birden fazla elektronik posta adresi kullanırım.	262 ***%29.7***	132 ***%15.0***	119 ***%13.5***	102 ***%11.6***	266 ***%30.2***
Bilgisayarımda orijinal (lisanslı) yazılım kullanmaya dikkat ederim.	83 ***%9.4***	113 ***%12.8***	170 ***%19.3***	246 ***%27.9***	269 ***%30.5***
Virüs temizleme, casus yazılım önleme vb. programları kullanırım.	61 ***%6.9***	62 ***%7.0***	80 ***%9.1***	215 ***%24.4***	463 ***%52.6***
Güvenlik duvarı, reklam önleyici vb. programlar kullanırım.	86 ***%9.8***	101 ***%11.5***	129 ***%14.6***	217 ***%24.6***	348 ***%39.5***
İçerik filtreleme programları kullanırım	160 ***%18.2***	120 ***%13.6***	192 ***%21.8***	172 ***%19.5***	237 ***%26.9***
E-posta filtreleme yazılımları kullanırım.	180 ***%20.4***	133 ***%15.1***	183 ***%20.8***	168 ***%19.1***	217 ***%24.6***
İzleme yazılımları kullanarak internet üzerinde yapılan etkinlikler hakkında bilgi sahibi olurum.	256 ***%29.1***	188 ***%21.3***	230 ***%26.1***	116 ***%13.2***	91 ***%10.3***
Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim.	214 ***%24.3***	234 ***%26.6***	215 ***%24.4***	114 ***%12.9***	104 ***%11.8***
Herkesin kullanımına açık bir bilgisayardan ayrılmadan önce geçici internet dosyalarını ve Web gezinti geçmişlerini silerim.	145 ***%16.5***	138 ***%15.7***	154 ***%17.5***	136 ***%15.4***	308 ***%35.0***
Dosyalarımı şifrelerim.	199 ***%22.6***	201 ***%22.8***	206 ***%23.4***	101 ***%11.5***	174 ***%19.8***
İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım.	143 ***%16.2***	107 ***%12.1***	174 ***%19.8***	155 ***%17.6***	302 ***%34.3***
Elektronik/ Mobil imza kullanırım.	508 ***%57.7***	121 ***%13.7***	121 ***%13.7***	71 ***%8.1***	60 ***%6.8***
İnternet sitelerine girerken genellikle sık kullanılanlar listesini kullanırım.	161 ***%18.3***	172 ***%19.5***	222 ***%25.3***	163 ***%18.5***	163 ***%18.5***
Bilgisayarım şifre ile açılır.	241 ***%27.4***	76 ***%8.6***	81 ***%9.2***	68 ***%7.7***	415 ***%47.1***
Bilgisayarımda otomatik kullan özelliğini kapatırım.	200 ***%22.7***	134 ***%15.2***	189 ***%21.5***	116 ***%13.2***	242 ***%27.5***
Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat ederim.	372 ***%42.2***	178 ***%20.2***	168 ***%19.2***	88 ***%10.0***	75 ***%8.5***
Parolalarımı sık sık değiştiririm.	237 ***%26.9***	280 ***%31.8***	194 ***%22.0***	82 ***%9.3***	88 ***%10.0***
Kablosuz modem şifremi değiştiririm.	368 ***%41.8***	223 ***%25.3***	147 ***%16.7***	75 ***%8.5***	68 ***%7.7***
Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım.	300 ***%34.1***	177 ***%20.1***	181 ***%20.5***	100 ***%11.4***	123 ***%14.0***
Kullandığım programların güncellemelerini düzenli olarak yaparım.	123 ***%14.0***	143 ***%16.2***	209 ***%23.2***	203 ***%23.0***	203 ***%23.0***

Buna göre katılımcıların %52.6'sı her zaman virüs programı kullandığını, %39.5'i her zaman güvenlik duvarı kullandığını, %26.9'u içerik filtreleme yazılımı kullandığını, %24.6'sı e-posta filtreleme yazılımı kullandığını ifade etmiştir. Bu sonuçlara göre; güvenlik yazılımları arasında en yaygın olarak kullanılan koruma yazılımı virüs koruma programlarıdır.

Katılımcılardan %11.8'i her zaman web gezinti geçmişlerini ve geçici internet dosyalarını sildiğini ifade etmektedir. Ortak kullanıma açık bir bilgisayar kullanımı söz konusu olduğunda ise bu oran %35'e çıkmaktadır.

Araştırmanın çarpıcı sonuçlarından biri ise; elektronik/mobil imza kullanım oranlarının son derece düşük olmasıdır. Çalışmaya katılanlardan yalnızca %6.8'i elektronik/mobil imzayı her zaman kullandığını ifade etmektedir. Oysaki elektronik bankacılık kullanımın son derece artış gösterdiği araştırma sonuçlarına göre de sabitken, bugün için bilinen en güvenli koruma metodolojisi olan elektronik/mobil imzanın kullanımının bu kadar düşük olması ilgi çekicidir.

Web sayfalarının güvenliği ile ilgili olan SSL Sertifikası, tüm bilgilerin şifrelenerek saklanmasını ve iletilmesini sağlar. Birçok e-ticaret sayfasında bulunmaktadır. Hemen hemen tüm bankaların web sayfaları SSL sertifikalıdır. Cevaplayıcılardan yalnızca %8.5'i girdiği web sayfasının SSL sertifikası olup olmadığına her zaman dikkat ettiğini belirtmiştir. Konu hakkındaki farkındalığın düşük olduğu görülmektedir.

Katılımcılardan %23'ü bilgisayarlarında bulunan programların güncellemelerini her zaman yaptıklarını % 14'ü ise hiçbir zaman yapmadığını ifade etmiştir. Yapılan güncellemeler çoğunlukla güvenlik açıkları ya da sürüm yükseltme ile olduğundan program güncellemeleri en önemli güvenlik gereksinimlerinden biridir. Ülkemizde genelde Windows işletim sistemi kullanılmaktadır. İşletim sistemi ve bilgisayara yüklü bulunan diğer programların özellikle anti virüs programlarının güncellemelerini yapmak güvenliği sağlamak bakımından çok önemlidir.

Kötücül yazılımlar aracılığıyla ya da çeşitli sosyal mühendislik yöntemleri ile parolaları ele geçirmek mümkün olabilmektedir. Parola güvenliğini sağlarken, parolaları kimse ile paylaşmamak ve yazılı olarak saklamamak alınabilecek önlemlerden bazılarıdır. Ancak parolaları belli aralıklarla değiştirmek de en az diğerleri kadar önemli bir koruma şeklidir. Araştırma sonuçlarına göre katılımcılardan %10'u parolalarını her zaman değiştirdiğini %26.9'u ise hiçbir zaman değiştirmediğini ifade etmiştir.

Kablosuz modemler de kullanıcıları için büyük tehlikelere yol açabilmektedirler. Her modem fabrika çıkış şifresi ile gelir ve bu şifre yalnızca marka ve modele göre değişir. Yani istenilen bir modemin fabrika çıkış şifresini bulmak çok kolay ve mümkündür. Dolayısı ile modem şifresinin değiştirilmesi önemli bir husustur. Katılımcılardan %7.7'si modem şifresini her zaman değiştirdiğini %41.8'i ise hiçbir zaman değiştirmediğini ifade etmiştir. Sonuçlara göre konu hakkındaki farkındalığın düşük olduğu görülmektedir.

Katılımcıların bilişim suçuna maruz kalmaları ya da kötü tecrübe yaşama durumları suça maruziyet ölçeği ile incelenmiş ve hesaplanan frekans değerleri Çizelge 5.8'de verilmiştir.

Çizelge 5.8 Suça Maruziyet Ölçeğine İlişkin Soruların Frekans Dağılımları

SORULAR	**Hiçbir zaman**	**Nadiren**	**Bazen**	**Sık sık**	**Her zaman**
Bilgisayar virüsleri nedeniyle sorun yaşadım.	138 ***%15.7***	158 ***%17.9***	312 ***%35.4***	166 ***%18.8***	107 ***%12.1***
Online alışverişten dolayı maddi zarara uğradım.	727 ***%82.5***	67 ***%7.6***	50 ***%5.7***	25 ***%2.8***	12 ***%1.4***
Kredi kartım kopyalandı.	790 ***%89.7***	29 ***%3.3***	31 ***%3.5***	21 ***%2.4***	10 ***%1.1***
Kişisel bilgilerimi internette paylaştığım için sıkıntı yaşadım.	725 ***%82.3***	73 ***%8.3***	49 ***%5.6***	24 ***%2.7***	10 ***%1.1***
Elektronik bankacılık kullandığım için maddi zarara uğradım.	783 ***%88.9***	33 ***%3.7***	32 ***%3.6***	27 ***%3.1***	6 ***%0.7***
Kişisel bilgilerim iznim olmadan üçüncü şahıslarla paylaşıldı/ internette yayınlandı.	757 ***%85.9***	39 ***%4.4***	51 ***%5.8***	24 ***%2.7***	10 ***%1.1***
İnternet üzerindeki hesaplarıma ait kullanıcı adım ve şifrem ele geçirildi.	725 ***%82.3***	76 ***%8.6***	45 ***%5.1***	21 ***%2.4***	14 ***%1.6***
İnternette kimliği belirsiz kişiler tarafından şahsıma yönelik hakaret, tehdit, ahlaksız teklif aldım.	703 ***%79.8***	77 ***%8.7***	61 ***%6.9***	20 ***%2.3***	20 ***%2.3***
Kumar içerikli siteler nedeniyle zarara uğradım.	780 ***%88.5***	24 ***%2.7***	38 ***%4.3***	26 ***%3.0***	13 ***%1.5***
Sosyal ağ siteleri nedeniyle zarara uğradım.	760 ***%86.3***	49 ***%5.6***	42 ***%4.8***	21 ***%2.4***	9 ***%1.0***
Arkadaşlık siteleri nedeniyle zarara uğradım.	745 ***%84.6***	55 ***%6.2***	52 ***%5.9***	19 ***%2.2***	10 ***%1.1***

Çizelge 5.8 Suça Maruziyet Ölçeğine İlişkin Soruların Frekans Dağılımları (Devam)

SORULAR	Hiçbir zaman	Nadiren	Bazen	Sık sık	Her zaman
İnternette gezerken isteğim dışında şiddet ya da pornografik içerikli yayınlarla karşılaştım.	391 ***%44.4***	185 ***%21.0***	155 ***%17.6***	91 ***%10.3***	%6.7 ***%6.7***
Bilgisayarımdaki dosyalarım çalındı/silindi.	739 ***%83.9***	55 ***%6.2***	53 ***%6.0***	20 ***%2.3***	14 ***%1.6***
Adıma sahte hesaplar açıldı.	749 ***%85.0***	48 ***%5.4***	47 ***%5.3***	22 ***%2.5***	15 ***%1.7***
İnternet üzerinden yaptığım yazışmalar isteğim ve bilgim dışında başkaları tarafından izlendi, kaydedildi.	733 ***%83.2***	59 ***%6.7***	49 ***%5.6***	24 ***%2.7***	16 ***%1.8***

Çizelge 5.8'e göre; en çok karşılaşılan olumsuzluğun kişinin isteği dışında şiddet ya da pornografik yayına maruz kalması olduğu (%6.7, her zaman) görülmektedir. Bunun dışında katılımcılardan %84.3'ü en az bir kez virüsler nedeniyle sorun yaşadığını, %20.2'si en az bir kez kimliği belirsiz şahıslar tarafından şahsına yönelik hakaret, tehdit ya da ahlaksız teklif aldığını ifade etmiştir.

Çalışmanın dikkat çekici sonuçlarından biri ise katılımcıların % 85.9'unun kişisel bilgilerinin hiçbir zaman üçüncü şahıslarla paylaşılmadığını ifade etmesidir. Yapılan farklı analizlerle elde edilen sonuçlara göre sosyal ağlara üye olan katılımcılardan %86.3'ü sosyal ağlara üye olduklarından dolayı hiçbir zaman zarara uğramadığını, benzer şekilde sosyal ağlara üye olanların % 62.9'u sosyal ağlardan gelen uygulama davetlerini en az bir kez kabul ettiğini ifade etmiştir. Oysaki sosyal ağlardan gelen uygulama davetleri çoğunlukla kişisel bilgilere erişim sağlamak için geliştirilmektedir ve bu uygulamalar aracılığı ile elde edilen bilgiler çeşitli kuruluşlara maddi çıkar sağlamak amacı ile satılmaktadır. Sosyal ağ sitelerinde bulunan bilgilerin neredeyse tamamı kişisel bilgilerdir. Yalnızca sosyal ağ sitelerine üye olurken, çoğunlukla okunmadan kabul edilen, sözleşmelerin içeriğinde, ilgili verilerin sözleşmeyi kabul ettikten sonra sosyal ağ sitesine ait olduğu ve istenildiği gibi paylaşılabileceğine dair ifadeler bulunmaktadır. Tüm analizler ve durumlar birlikte değerlendirildiğinde sosyal ağlara ilişkin risklerin farkındalığının katılımcılar için düşük olduğu gözlemlenmektedir.

Katılımcıların hangi bilişim teknolojisini ya da davranışı ne düzeyde tehlikeli bulduğunu ölçmek üzere geliştirilmiş olan ölçek sonuçlarına ilişkin frekans değerleri Çizelge 5.9'da ayrıntılı olarak sunulmuştur.

Çizelge 5.9 Tehlike Algısı Ölçeğine İlişkin Soruların Frekans Dağılımları

SORULAR	**Fikrim yok**	**Tehlikesiz**	**Az tehlikeli**	**Tehlikeli**	**Çok tehlikeli**
Virüs yazılımları	133	187	88	167	306
	%15.1	***%21.2***	***%10.0***	***%19.0***	***%34.7***
Casus programlar (Keylogger, Screenlogger,Trojan vb.)	211	61	72	225	312
	%24.0	***%6.9***	***%8.2***	***%25.5***	***%35.4***
Dosya paylaşım programları (Ares, Limewire vb.)	154	124	264	250	89
	%17.5	***%14.1***	***%30.0***	***%28.4***	***%10.1***
ActiveX, Javascript vb. mobil kodlar.	308	225	189	118	41
	%35.0	***%25.5***	***%21.5***	***%13.4***	***%4.7***
Web tarayıcıları (Internet Explorer, Mozilla Firefox, Google Chrome vb.)	129	415	230	80	27
	%14.6	***%47.1***	***%26.1***	***%9.1***	***%3.1***
Sohbet programları (Messenger, ICQ vb..)	92	210	348	162	69
	%10.4	***%23.8***	***%39.5***	***%18.4***	***%7.8***
İstenmeyen/ Spam / Junk e-postalar	172	74	165	292	178
	%19.5	***%8.4***	***%18.7***	***%33.1***	***%20.2***
Online oyunlar	129	153	292	241	66
	%14.6	***%17.4***	***%33.1***	***%27.4***	***%7.5***
USB/Harici bellekler	131	228	278	173	71
	%14.9	***%25.9***	***%31.6***	***%19.6***	***%8.1***
MS Office uygulamaları (Word,Excel vb.)	96	615	104	50	16
	%10.9	***%69.8***	***%11.8***	***%5.7***	***%1.8***
Klavye kullanımı	93	579	101	72	36
	%10.6	***%65.7***	***%11.5***	***%8.2***	***%4.1***
Kopya/ Kırık/ Korsan program kullanımı	109	99	205	286	182
	%12.4	***%11.2***	***%23.3***	***%32.5***	***%20.7***
Müzik/ Resim/ Film gibi materyallerin herhangi bir bedel ödemeden indirilmesi	83	149	211	301	137
	%9.4	***%16.9***	***%24.0***	***%32.2***	***%15.6***
Reklam içerikli e-postaların açılması	104	92	249	296	140
	%11.8	***%10.4***	***%28.3***	***%33.6***	***%15.9***
Elektronik bankacılık kullanımı	91	176	296	228	96
	%10.3	***%20.0***	***%32.9***	***%25.9***	***%10.9***

Çizelge 5.9 Tehlike Algısı Ölçeğine İlişkin Soruların Frekans Dağılımları (Devam)

SORULAR	Fikrim yok	Tehlikesiz	Az tehlikeli	Tehlikeli	Çok tehlikeli
İnternet ortamında yabancılarla sohbet / bilgi paylaşımı	82	69	193	320	217
	%9.3	***%7.8***	***%21.9***	***%36.3***	***%24.6***
İnternetten alışveriş yapılması	72	101	316	275	117
	%8.2	***%11.5***	***%35.9***	***%31.2***	***%13.3***
Pornografik içerikli web sitelerine girilmesi	94	50	88	258	391
	%10.7	***%5.7***	***%10.0***	***%29.3***	***%44.4***
Kumar, bahis sitelerine girilmesi	89	65	98	229	400
	%10.1	***%7.4***	***%11.1***	***%26.0***	***%45.4***
Sosyal ağlara üye olunması (Facebook, Twitter vb.)	87	271	319	149	55
	%9.9	***%30.8***	***%36.2***	***%16.9***	***%6.2***
Bluetooth kullanımı	123	344	262	119	33
	%14.0	***%39.0***	***%29.7***	***%13.5***	***%3.7***
Kablosuz modem kullanımı	104	371	270	102	34
	%11.8	***%42.1***	***%30.6***	***%11.6***	***%3.9***
İnternetten kontör yüklenmesi	175	226	233	169	78
	%19.9	***%25.7***	***%26.4***	***%19.2***	***%8.9***
Kırık veya ücretsiz güvenlik programı kullanımı	161	99	218	245	158
	%18.3	***%11.2***	***%24.7***	***%27.8***	***%17.9***
Bina girişlerinde güvenlik birimine nüfus cüzdanı veya sürücü belgesinin teslim edilmesi	94	145	230	265	147
	%10.7	***%16.5***	***%26.1***	***%30.1***	***%16.7***
Kargo, GSM operatörü vs. gibi kuruluşlara nüfus cüzdanı bilgilerinin verilmesi	83	135	260	241	162
	%9.4	***%15.3***	***%29.5***	***%27.4***	***%18.4***
Vatandaşlık numarasının başka şahıslar tarafından bilinmesi	71	65	123	281	341
	%8.1	***%7.4***	***%14.0***	***%31.9***	***%38.7***

Çizelge 5.9'a göre; katılımcıların % 45.4'ü kumar ve bahis sitelerine girmeyi, % 44.4'ü pornografik sitelere girmeyi, % 35.4'ü casus programları ve % 34.7'si virüs programlarını çok tehlikeli bulduklarını ifade etmiştir.

Katılımcılardan %69.8'i MS Office uygulamalarını, %47.1' i web tarayıcılarını, % 42.1'i ise kablosuz modem kullanımını tehlikesiz bulmaktadır. Ayrıca; katılımcıların %11.8'inin kablosuz modemlerin, %35.0'inin ActiveX vb. mobil kodların ve %24.0'ünün casus programların tehlikeli olup olamadığına dair fikri olmadığı görülmektedir. E-postalar aracılığıyla yayılan ve içeriğinde kötücül kodlar

bulunduran birçok MS Office dosyası bulunmaktadır. Buna rağmen birçok kişi bu uygulamaları tehlikesiz bulmaktadır.

Katılımcılar arasında kablosuz modem kullananların %44'ü kablosuz modem kullanımını tehlikesiz bulmakta ve %6.7' si konu hakkında fikri olmadığını ifade etmektedir. Kablosuz modem kullanımı ile ilgili veriler ve yapılan diğer analizlerden elde edilen sonuçlar birlikte değerlendirildiğinde, kablosuz modem kullanıcılarının konu hakkında çok bilinçli olmadığı düşünülmektedir. Oysaki kablosuz modemler gerekli güvenlik önlemleri alınmadığı takdirde birçok tehlikeyi beraberinde getirmektedir. Konu hakkındaki farkındalığın düşük olduğu görülmektedir.

Sosyal ağlara üye olmayı tehlikesiz bulan katılımcı sayısı %30.8 oranı ile 271 kişi ve konu hakkında fikri olmadığını ifade eden katılımcı sayısı %9.9 oranı ile 81 kişidir. Sosyal ağlarla ilgili diğer ölçeklerden toplanan veriler ve tehlike algısı ölçeğinde toplanan veriler sonucu yapılan analizlerin tamamı kullanıcıların bu konuda yeterince bilinçli olmadıklarını düşündürmektedir.

Web tarayıcıları da benzer şekilde ilgili güncellemeler yapılmadığı ve güvenlik önlemleri alınmadığı takdirde birçok tehlikeyi beraberlerinde getirmektedirler. Buna rağmen katılımcıların %47.1'i web tarayıcılarını tehlikesiz bulduğunu ve %14.6'sı da konu hakkında fikri olmadığını ifade etmektedir. Konuya ilişkin farkındalığın yeterli düzeyde olmadığı düşünülmektedir.

Kişisel verilerin korunması söz konusu olduğu takdirde kişisel verilerin bulunduğu ortamların farkındalığı da önem taşımaktadır. Son günlerde en çok tartışılan ve birçok uygulamada kullanıcı kimliği olarak kullanılan TC kimlik numarası da korunması gereken kişisel bir bilgidir. Bu bağlamda ölçeğin son üç sorusu konu hakkındaki farkındalığı ölçmek amacı ile sorulmuştur. Sonuçlar incelendiğinde; araştırmaya katılan bireylerden %38.7'si TC kimlik numarasının başkaları tarafından bilinmesini çok tehlikeli bulduğunu ifade ederken, katılımcıların %16.7' si bina girişlerinde güvenlik birimine nüfus cüzdanı ya da sürücü belgesinin teslim edilmesini benzer şekilde çok tehlikeli bulduğunu ifade etmektedir. Ancak TC kimlik numarasının kimlik belgeleri üzerinde yazılı olduğu düşünüldüğünde verilen

oranlar bilginin bulunduğu ortamlara ilişkin farkındalığın düşük olduğunu göstermektedir. Ölçekle ilgili diğer frekanslar Çizelge 5.9'da sunulmuştur.

Çizelge 5.10'da verildiği gibi, 163 akademik personele ilişkin RDP ortalaması 46.61 ±10.907; KDP ortalaması 58.25 ±14.576; SMP ortalaması 19.09 ± 4.602 ve TAP ortalaması 79.17 ± 15.308 olarak hesaplanmıştır. İdari personel ve öğrenciler de benzer şekilde incelendiğinde Çizelge 5.10'daki sonuçlara ulaşılmıştır. Akademik personel, idari personel ve öğrencilere ilişkin hesaplanmış olan en düşük ve en yüksek değerleri de Çizelge 5.10'daki son iki sütunda verilmiştir.

Çizelge 5.10 Puan Türlerinin Tanımlayıcı İstatistikleri

Puan Türü	Örneklem Grubu	N	Ortalama	Std. Sapma	En Düşük	En Yüksek
Riskli Davranış Puanı (RDP)	**Akademik**	163	46,61	10,907	20	85
	İdari	323	46,42	13,240	20	100
	Öğrenci	395	55,39	11,138	27	91
	TOPLAM	***881***	***50,48***	***12,697***	***20***	***100***
Korumacı Davranış Puanı (KDP)	**Akademik**	163	58,25	14,576	20	94
	İdari	323	59,11	16,864	20	100
	Öğrenci	395	60,21	12,593	23	96
	TOPLAM	***881***	***59,44***	***14,654***	***20***	***100***
Suça Maruziyet Puanı (SMP)	**Akademik**	163	19,09	4,602	15	54
	İdari	323	21,36	9,400	15	75
	Öğrenci	395	23,59	9,745	15	63
	TOPLAM	**881**	**21,94**	**9,033**	**15**	**75**
Tehlike Algısı Puanı (TAP)	**Akademik**	163	79,17	15,308	25	119
	İdari	323	69,51	20,265	25	125
	Öğrenci	395	76,88	13,195	25	125
	TOPLAM	***881***	***74,60***	***16,943***	***25***	***125***

Çizelge 5.10 incelendiğinde, öğrencilerin RDP ortalaması 55.39 iken akademik ve idari personelin RDP ortalamaları sırasıyla 46.64 ve 46.42' dir. RDP için alınabilecek en düşük değerin 20 ve en yüksek değerin 100 olduğu bilindiğine göre her grubun RDP puanlarının bu aralıktaki ortalama değer olan 60 değerinin altında olduğunu görülmektedir. Öğrencilerin RDP puanı ortalaması diğer gruplardan yüksektir. Bu durumunda öğrencilerin diğer gruplara oranla risk içeren bilgi teknolojilerini daha fazla kullandıkları söylenebilir.

Likert tipi anket sonuçları, puanlara çevrilmiştir. Buna dayanarak, puanların ortalama ve benzeri merkezi eğilim ölçüleri hesaplanabilmektedir. Puan ortalamalarının akademik personel, idari personel ve öğrenciler arasında farklı olup olmadıkları bağımsız K-örneklem testleri ile incelenebilmektedir. Ortalamalar arasındaki farklılıkların incelenmesinde, gözlemler üzerinde normal dağılım ve grup varyanslarının homojen olduğu (kabul edildiği) durumlarda ANOVA (Analysis of Variance Analysis / Varyans Analizi) yöntemi kullanılabilmektedir.

Bu çalışmada Korumacı Davranış Puanı (KDP) ile Tehlike Algısı Puanı (TAP) puanlarının normal dağıldığı, ancak Riskli Davranış Puanı (RDP) ile Suça Maruziyet Puanı (SMP) puanlarının normal dağılmadığı görülmüştür. Her iki puan türünde de, tüm gruplardaki örneklem genişliklerinin normal dağılım varsayımı yapılabilecek kadar geniş olması nedeniyle ANOVA kullanılmıştır.

RDP, KDP, SMP ve TAP puanları akademik personel, idari personel ve öğrenciler için incelendiğinde, μ_A ilgili puan türünün akademik puan ortalamasını, $\mu_İ$ ilgili puan türünün idari puan ortalamasını ve $\mu_Ö$ ilgili puan türünün öğrenci puan ortalamasını göstermek üzere;

H_0: $\mu_{A=} \mu_{İ=} \mu_Ö$

H_1: En az bir ortalama diğerlerinden farklıdır.

hipotezi α= 0.05 düzeyinde test edilmiştir. Elde edilen sonuçlar Çizelge 5.11'de verilen ANOVA tablolarında belirtilmiştir.

Çizelge 5.11 Puan Türlerinin ANOVA Tabloları

		Kareler Toplamı	sd	Kareler Ortalaması	F	P değeri
Riskli Davranış Puanı (RDP)	**Gruplar Arası**	17272,360	2	8636,180	60,858	,000
	Grup içi	124593,501	878	141,906		
	TOPLAM	***141865,862***	***880***			
Korumacı Davranış Puanı (KDP)	**Gruplar Arası**	500,688	2	250,344	1,166	,312
	Grup içi	188482,668	878	214,673		
	TOPLAM	***188983,355***	***880***			
Suça Maruziyet Puanı (SMP)	**Gruplar Arası**	2506,292	2	1253,146	15,877	,000
	Grup içi	69299,520	878	78,929		
	TOPLAM	***71805,812***	***880***			
Tehlike Algısı Puanı (TAP)	**Gruplar Arası**	13832,202	2	6916,101	25,429	,000
	Grup içi	238796,545	878	271,978		
	TOPLAM	***252628,747***	***880***			

Çizelge 5.11'e göre; α=0.05 düzeyinde RDP, SMP ve TAP puanlarında H_0 hipotezi reddedilmiştir ($P_{RDP}= P_{SMP}=P_{TAP}$=0.000<α=0.05). Bu bulguya göre, bu üç puan türünün akademik personel, idari personel ve öğrenci gruplarında kitle ortalamalarının aynı olmadığı sonuçlarına varılmıştır. Gruplar arasında farklılık yaratan grupların belirlenmesi amacıyla Tukey testi uygulanmıştır. Test sonuçlarına göre RDP' da akademik personel ve öğrenciler ile idari personel ve öğrenciler arasında 0.05 düzeyinde anlamlı farklılık bulunmuştur (p=0.00<0.05).

Çizelge 5.10 ve Çizelge 5.11 birlikte incelendiğinde KDP için, akademik personel, idari personel ve öğrenci grupları arasında 0.05 düzeyinde ortalama puanların farklı olmadığı sonucuna varılmıştır (p=0.312). Bu durumda korumacı davranış puan türünde gruplar arası farklılık oluşmadığı görülmektedir.

SMP incelendiğinde gruplar arasında 0.05 düzeyinde ortalama puanların aynı olmadığı olduğu sonucuna varılmıştır. Benzer şekilde farklılık yaratan grupların tespiti için uygulanan Tukey testi sonuçlarına göre akademik personel ve öğrenciler ile idari personel ve öğrenciler arasında anlamlı farklılık oluştuğu gözlemlenmiştir (p=0.00<0.05). Çizelge 5.10'da verildiği üzere akademik personele ilişkin SMP ortalaması 19.09±4.602, idari personel ve öğrenciler için ortalama değerleri sırasıyla 21.36±9.40 ve 23.59±9.745'dir. Suça ve olumsuz tecrübeye en çok maruz kalan grubun öğrenciler olduğu görülmektedir.

Benzer şekilde TAP incelendiğinde gruplar arasında 0.05 düzeyinde ortalama puanların aynı olmadığı olduğu sonucuna varılmıştır (p=0.00<0.05). Benzer şekilde farklılık yaratan grupların tespiti için uygulanan Tukey HSD testi sonuçlarına göre; akademik personel ve idari personel ile idari personel ve öğrenciler arasında anlamlı farklılık oluştuğu gözlemlenmiştir. Çizelge 5.10'da verildiği üzere akademik personele ilişkin TAP ortalaması 79.17±15.308, idari personel ve öğrenciler için ortalama değerleri sırasıyla 69.51±20.26 ve 76.88±13.195'dir. Sonuçlar değerlendirildiğinde, bazı bilgi teknolojilerinin kullanımına ilişkin tehlike algısı puan ortalaması en yüksek olan grup akademik personel ve en düşük olan grup ise idari personeldir.

Dört ölçek arasındaki ilişkiler Çizelge 5.12'de verildiği üzere Pearson Korelasyon Katsayısı (r) ile incelenmiştir.

Çizelge 5.12 Puan Türlerine İlişkin Korelasyon Değerleri

		RDP	KDP	SMP	TAP
Riskli Davranış Puanı (RDP)	***r***	1	0,450	0,463	0,224
	P		0,000	0,000	0,000
	N	881	881	881	881
Korumacı Davranış Puanı (KDP)	***r***	0,450	1	0,200	0,404
	P	0,000		0,000	0,000
	N	881	881	881	881
Suça Maruziyet Puanı (SMP)	***r***	0,463	0,200	1	0,150
	P	0,000	0,000		0,000
	N	881	881	881	881
Tehlike Algısı Puanı (TAP)	***r***	0,224	0,404	0,150	1
	P	0,000	0,000	0,000	
	N	881	881	881	881

Katılımcıların RDP ile KDP değerleri arasındaki ilişkiyi gösteren korelasyon katsayısı değeri 0.45 ve p=0.000 olarak bulunmuştur. Buna göre KDP ve RDP arasında %45'lik pozitif yönlü anlamlı bir ilişki tespit edilmiştir. Katılımcıların RDP değerleri artarken KDP değerlerinin de arttığı söylenebilir.

Araştırmanın önemli bulgularından biri ise RDP ile SMP arasında bulunan anlamlı ilişkidir (p=0.000). Çizelge 5.12'de de gösterildiği gibi RDP ve SMP için korelasyon

katsayısı 0.46 olarak hesaplanmıştır. Diğer bir ifade ile iki puan türü arasında %46.3'lük pozitif yönlü bir ilişki vardır. Buna göre katılımcıların risk içeren teknolojileri kullanımları arttıkça suça maruz kalma düzeyleri de artmaktadır.

TAP ile KDP puanı arasındaki ilişki değeri 0.40 olmak üzere anlamlı bir ilişki tespit edilmiştir (p=0.000). Buna göre tehlike algısı puanı arttıkça korumacı davranış puanının da arttığı görülmektedir.

SMP ile KDP arasında %20'lik pozitif yönlü anlamlı bir ilişki tespit edilmiştir (p=0.000).

Cevaplayıcılar günlük yaklaşık internet kullanım saatlerine göre dört farklı gruba ayrılmıştır. Buna göre; günlük yaklaşık 0-2 saat arasında internet kullananlar 1. Grup, 3-5 saat arasında internet kullananlar 2. Grup, 6-8 saat arasında internet kullananlar 3. Grup ve 9 saat ve üzeri internet kullananlar 4. Grubu oluşturmaktadır. 457 kişiden oluşan 1. Grubun RDP ortalaması 46.69±12.871; KDP ortalaması 56.34±15.239; SMP ortalaması 21.53±8.986 ve TAP ortalaması 70.88±18.32 olarak hesaplanmıştır. Diğer gruplar da benzer şekilde incelendiğinde Çizelge 5.13'deki sonuçlara ulaşılmıştır. Tüm gruplara ilişkin hesaplanmış olan puanların en düşük ve en yüksek değerleri de aynı tabloda son iki sütunda verilmiştir.

Çizelge 5.13 İnternet Kullanım Sürelerine Göre Puan Türlerinin Tanımlayıcı İstatistikleri

	Grup	Sayı	Ortalama	Std. Sapma	En düşük	En Yüksek
Riskli Davranış Puanı (RDP)	**0-2 Saat**	457	46,69	12,87	20	100
	3-5 Saat	287	53,85	10,76	25	91
	6-8 Saat	84	55,40	10,75	27	81
	9 Saat ve +	53	57,06	13,51	36	90
	TOPLAM	***881***	***50,48***	***12,70***	***20***	***100***
Korumacı Davranış Puanı (KDP)	**0-2 Saat**	457	56,34	15,24	20	100
	3-5 Saat	287	61,22	12,95	22	95
	6-8 Saat	84	63,43	12,46	38	93
	9 Saat ve +	53	70,26	13,43	33	96
	TOPLAM	***881***	***59,44***	***14,65***	***20***	***100***
Suca Maruziyet Puanı (SMP)	**0-2 Saat**	457	21,53	8,99	15	75
	3-5 Saat	287	22,59	9,28	15	63
	6-8 Saat	84	21,27	7,59	15	53
	9 Saat ve +	53	23,04	10,08	15	54
	TOPLAM	***881***	***21,94***	***9,03***	***15***	***75***
Tehlike Algısı Puanı (TAP)	**0-2 Saat**	457	70,88	18,32	25	125
	3-5 Saat	287	76,70	14,01	29	125
	6-8 Saat	84	80,04	13,05	25	103
	9 Saat ve +	53	86,74	14,85	47	124
	TOPLAM	***881***	***74,60***	***16,94***	***25***	***125***

RDP, KDP, SMP ve TAP puanları internet kullanım saatine göre dört grup için incelendiğinde, μ_1 ilgili puan türünün 1. Grup puan ortalamasını, μ_2 ilgili puan türünün 2. Grup puan ortalamasını, μ_3 ilgili puan türünün 3. Grup puan ortalamasını ve μ_4 ilgili puan türünün 4. Grup puan ortalamasını göstermek üzere;

H_0: $\mu_{1=}\ \mu_{2=}\ \mu_{3=}\ \mu_4$

H_1: En az bir ortalama diğerlerinden farklıdır.

hipotezi α= 0.05 düzeyinde test edilmiştir. Elde edilen sonuçlar Çizelge 5.14' de verilen ANOVA tablolarında belirtilmiştir.

Çizelge 5.14 İnternet Kullanım Sürelerine Göre ANOVA Tabloları

		Kareler Toplamı	sd	Kareler Ortalaması	F	P
Riskli Davranış Puanı (RDP)	**Gruplar Arası**	14155,44	3	4718,48	32,40	0,00
	Grup İçi	127710,4	877	145,62		
	TOPLAM	***141865,9***	***880***			
Korumacı Davranış Puanı (KDP)	**Gruplar Arası**	12848,88	3	4282,96	21,33	0,00
	Grup İçi	176134,5	877	200,84		
	TOPLAM	***188983,4***	***880***			
Suça Maruziyet Puanı (SMP)	**Gruplar Arası**	299,7923	3	99,93	1,23	0,30
	Grup İçi	71506,02	877	81,53		
	TOPLAM	***71805,81***	***880***			
Tehlike Algısı Puanı (TAP)	**Gruplar Arası**	17871,7	3	5957,23	22,25	0,00
	Grup İçi	234757	877	267,68		
	TOPLAM	***252628,7***	***880***			

Çizelge 5.14'e göre; α=0.05 düzeyinde RDP, KDP ve TAP puanlarında H_0 hipotezi reddedilmiştir ($P_{RDP}= P_{KDP}=P_{TAP}=0.000<\alpha=0.05$). Bu bulguya göre, bu üç puan türünün internet kullanım saatine göre dört grubun kitle ortalamalarının aynı olmadığı sonuçlarına varılmıştır. Gruplar arasında farklılık yaratan grupların belirlenmesi amacıyla Tukey testi uygulanmıştır. Test sonuçlarına göre; RDP için 1. grup ile diğer tüm gruplar arasında fark olduğu tespit edilmiştir. Birinci grubun RDP ortalaması 46.69±12.87 iken diğer grupların ortalamaları sırasıyla; 53.85±10.76, 55.40±10.75 ve 57.06±13.51'dir. KDP benzer şekilde incelendiğinde; birinci grup ile tüm gruplar arasında ve 2. Grup ile 4. Grup arasında fark olduğu tespit edilmiştir. Çizelge 5.13'e göre 1. Grup KDP ortalaması 56.34±15.24 ve diğer grupların ortalamaları sırası ile 61.22±12.95, 63.43±12.46 ve 70.26±13.43'dür.

Bulgular değerlendirildiğinde günlük ortalama internet kullanım süresine göre gruplar arasında anlamlı farklılıklar olduğu görülmektedir. İlişkilerin yönlerini tespit etmek için Çizelge 5.15'te verildiği gibi Pearson Korelasyon Katsayıları incelenmiştir.

Çizelge 5.15 İnternet Kullanım Süresi ile Ölçek Puanlarının Korelasyon Katsayıları

		RDP	KDP	SMP	TAP
İnternet Kullanım Süresi	***r***	0,291	0,257	0,036	0,264
	P	**0,000**	**0,000**	**0,288**	**0,000**
	N	881	881	881	881

Katılımcıların internet kullanım süreleri ile RDP arasında %29.1'lik pozitif yönlü bir ilişki tespit edilmiştir. Buna göre katılımcıların internet kullanım süreleri arttıkça risk içeren bilgi teknolojilerini kullanım ortalamaları da artmaktadır. Benzer şekilde, internet kullanım süresi ile KDP arasında %25.7'lik pozitif yönlü bir ilişki vardır. Bu sonuca göre katılımcılar internette daha çok vakit geçirdikçe kendilerini daha çok koruma eğilimi göstermektedirler. TAP ile internet kullanım süresi arasında da benzer şekilde %26.4'lük pozitif yönlü bir ilişki vardır. Önemli bir ilişki olması beklenen internet kullanım süresi ile SMP arasında anlamlı bir ilişki bulunamamıştır.

Çizelge 5.16 Güvenlik Eğitimi Alma Durumuna Göre Grupların Tanımlayıcı İstatistikleri

GÜVENLİK EĞİTİMİ ALMA DURUMU		**Sayı**	**Ortalama**	**Std. Sapma**	**En düşük**	**En Yüksek**
Riskli Davranış Puanı (RDP)	**Evet**	197	51,959	12,849	20	100
	Hayır	684	50,052	12,629	20	91
	TOPLAM	***881***	***50,479***	***12,696***	***20***	***100***
Korumacı Davranış Puanı (KDP)	**Evet**	197	67,025	14,252	20	100
	Hayır	684	57,258	14,037	20	95
	TOPLAM	***881***	***59,442***	***14,654***	***20***	***100***
Suça Maruziyet Puanı (SMP)	**Evet**	197	23,106	10,732	15	75
	Hayır	684	21,603	8,460	15	63
	TOPLAM	***881***	***21,939***	***9,033***	***15***	***75***
Tehlike Algısı Puanı (TAP)	**Evet**	197	78,989	16,513	25	125
	Hayır	684	73,340	16,866	25	125
	TOPLAM	***881***	***74,603859***	***16,94338***	***25***	***125***

Cevaplayıcılar güvenlik eğitimi alanlar ve almayanlar olmak üzere iki grupta incelenmiştir. Buna göre güvenlik eğitim alan 197 cevaplayıcının RDP puan ortalaması 51.95±12.84; KDP puan ortalaması 67.02±14.25, SMP puan ortalaması 23.10±10.73 ve TAP puan ortalaması 78.98±16.51 olarak hesaplanmıştır.

Güvenlik eğitimi almayan grup için de aynı hesaplamalar yapılmış, her ortalama için en yüksek ve en düşük değerler de tablonun son iki sütununda verilmiştir.
RDP, KDP, SMP ve TAP puanları güvenlik eğitimi almış olma durumuna göre incelendiğinde μ_E ilgili puan türünün güvenlik eğitimi alan grubun puan ortalamasını, μ_H ilgili puan türünün güvenlik eğitimi almayan grubunun puan ortalamasını göstermek üzere;

H_0: $\mu_{E=} \mu_H$

H_1: $\mu_E \neq \mu_H$

hipotezi α= 0.05 düzeyinde test edilmiştir. Güvenlik eğitimi alanlar ile almayanlar arasında RDP ve SMP ortalamalarının 0.05 düzeyinde anlamlı olmadığı (p=0.063 ve p=0.071) görülürken, KDP ve TAP ortalamaları arasında anlamlı fark bulunmuştur (p=0.000 ve p=0.000).

6. SONUÇ VE ÖNERİLER

Bilişim güvenliğine yönelik tehditler için yazılımsal ve donanımsal olarak birçok koruma yöntemi mevcuttur, bunların birçoğu doğru ve geçerlidir. Ancak bir noktadan sonra ne yazık ki tüm önlemler geçerliliğini yitirmektedir. Yapılan araştırmalar en büyük tehdidin bireyin bizzat kendisi olduğunu göstermektedir. Bu noktada en zayıf halka bireydir. Ne yazık ki bilişim güvenliği yalnızca bireyi ilgilendiren bir konu değildir. Bilgi teknolojilerinin hızlı gelişimi birçok yeni kavramı da beraberinde getirmiştir. Mevcut hukuki düzenlemeler bu hızlı değişime aynı hızda yanıt verememektedir. Özellikle Türkiye siber tehditlere çok açık bir konumda bulunmaktadır. İnternet ve bilişim güvenliği toplum için yeni bir olgudur. Diğer ülkelerde bilişim güvenliği konusuna özel önem verilmiş, toplumsal stratejiler ve politikalar oluşturulmuştur. Türkiye' de de bilişim güvenliğine yönelik çalışmalar yapılmış ancak sonuçlandırılamamıştır. E- Dönüşüm Eylem Planı'nın 17. Maddesi olan "Bilişim Güvenliği Konusunda Farkındalık Çalışması", ne yazık ki halen "Henüz Başlamamış Eylemler" kategorisinde bekletilmektedir.

Medyada bilişim ile ilgili yapılan yayınlar incelendiğinde, 2000-2006 yılları arasında internet bankacılığı kullanımını teşvik edici ve tanıtıcı çok sayıda kampanya düzenlendiği görülmektedir. Ancak ne yazık ki buna paralel olarak, internet bankacılığı kullanan çok sayıda banka müşterisinin hesaplarının boşaltıldığı da görülmektedir. Hesabı boşaltılanlar arasında gerçek kişiler, ticari kuruluşlar ve hatta kamu kuruluşları bulunmaktadır. Toplum internet kullanmaya teşvik edilmiş ancak riskleri ve korunma yolları konusunda uyarılmamış ve eğitilmemiştir. Dönemin medya haberleri incelendiğinde, sorumlu kamu yöneticilerinin "güvenlikten bahsederek halkı korkutmayalım" beyanlarına rastlanmaktadır. Buna karşın emsal ülkelerde güvenlik konusunda yoğun farkındalık ve eğitim kampanyaları düzenlendiği gözlemlenmektedir. Türkiye'de ise benzer çalışmaların halen başlamadığı açık bir gerçektir. Bilişim suçlarında her geçen gün artış yaşanmakta birçok güvenlik açığı istismar edilmeye devam edilmektedir.

Bireysel farkındalığın yanı sıra kamusal farkındalığında yeterince gelişmediği ve devletin vatandaşa ait kişisel verileri tam anlamıyla korumadığı görülmektedir. Bunun bir örneği, geçtiğimiz yıllarda bir kamu kurumu tarafından KEY

ödemelerine ilişkin yaklaşık bir milyon vatandaşa ait TC kimlik numarası ve bir takım kişisel bilgilerin internet ortamında yayınlanmış olmasıdır. Tüm uyarılara rağmen aynı bilgiler tekrar aynı şekilde yayınlanmıştır. Gazetelerde bugünlerde rastlanan bir habere göre [30], yetmiş milyon Türk vatandaşına ait TC kimlik numarası, adres, iletişim bilgileri gibi çok sayıda kişisel veriyi bir arada elinde bulunduran ve bu CD'leri isteyene satan, hatta reklamını yapan bir şebeke emniyet güçleri tarafından çökertilmiştir. Bu bilgilerin nereden, ne şekilde sızdırıldığına ve şebeke elemanlarına ne tür bir yaptırım uygulandığına dair bir açıklama yapılmamıştır.

Bütün bunlar göz önünde bulundurulduğunda kişisel verilerin korunmasının ne kadar önemli bir husus olduğu açıkça görülmektedir. Öncelikle toplum bilgi güvenliği risklerine karşı bilinçlendirilmelidir. Ulusal bilgi güvenliği politikasının bireyden genele yayılması gerekmektedir. Bilişim hukukuna ilişkin birçok çalışma yapılmıştır. Ancak mevcut yasal düzenlemeler, uygulama güçlüğü ve yorumlamaya dair sıkıntılar nedeniyle birçok bilişimci tarafından kabul görmemektedir. Bu anlamda hızla hukuki düzenlemeler tamamlanmalı, mevcut düzenlemeler revize edilmelidir. Henüz tasarı halinde bekleyen Kişisel Verilerin Korunması Kanunu'nun bir an önce yasalaştırılması gerekmektedir. Nasıl ki tüketici haklarını korumak için Tüketici Mahkemeleri oluşturulmuşsa benzer şekilde konu hakkında eğitim almış adli kadrolardan oluşan özel bilişim mahkemeleri de kurulmalıdır.

Bu çalışmanın çıkış noktası, bu ürkütücü tablo içerisinde bireylerin ne düşündükleri ve ne yaptıklarını, genel olarak bu konular hakkındaki farkındalıkları, davranışları ve kısmen de olsa bilgi düzeylerinin tespit edilmesidir. Farkındalık düzeyini tespit edebilmek oldukça önemlidir, farkındalık olmadan davranış oluşmaz. Ancak bazı durumlarda farkındalık düzeyi yüksek olduğu halde davranış gelişmeyebilir. Çalışmada kullanılan dört ölçeğe göre oluşan puan ortalamaları değerlendirildiğinde gruplar arasında RDP, KDP ve TAP ortalamaları bakımından anlamlı farklılıklar olduğu ancak SMP ortalamasında farklılık olmadığı görülmektedir. Bu sonuca göre akademik personel, idari personel ve öğrenciler arasında riskli davranış puanı, korumacı davranış puanı ve tehlike algısı puanı türlerinde anlamlı farklılıklar bulunmuştur. Öğrencilerin risk içeren bilgi teknolojileri

kullanım oranları diğer gruplardan daha fazladır. Bu sonuç öğrencilerin riske daha açık bir konumda olduğunu göstermektedir. Bununla birlikte öğrencilerin suça maruziyet puanları da benzer şekilde diğer gruplardan daha yüksektir. Korumacı davranış puanlarında ise anlamlı farklılık bulunamamıştır. Tehlike algısı puan türünde ise en düşük ortalamaya sahip grup idari personeldir.

Araştırmanın temel amacı olan puan türleri arasındaki ilişkinin yönünün ve boyutunun belirlenmesi ile ilgili analiz sonuçlarına göre; katılımcıların tehlike algıları arttıkça kendilerini koruma davranışları da artmaktadır. KDP ve TAP arasına pozitif yönlü bir ilişki bulunmuştur. Riskli davranış puanı ile suça maruziyet puanı arasında da benzer şekilde pozitif yönlü bir ilişki bulunmakta, katılımcıların risk içeren teknolojileri kullanımları arttıkça suça maruz kalma ya da olumsuz tecrübe yaşama oranları da aynı şekilde artmaktadır.

Katılımcıların riskli davranış puanları ile tehlike algıları arasında da pozitif yönlü bir ilişki bulunmuştur. Teknoloji kullanımı arttıkça suça maruziyet artmakta ve bununla birlikte tehlike algısı da artmaktadır.

İnternet kullanım süresi araştırma sonuçlarına göre puan türlerinin değerlendirilmesinde önemli bir etken olmuştur. Buna göre internet kullanım süresi arttıkça kişilerin riskli davranış puanları da artmakta, buna karşılık suça maruziyet puanlarında aynı şekilde artış yaşanmamaktadır. Benzer şekilde internet kullanım süresi arttıkça kişilerin tehlike algısı puanları da artmaktadır.

Güvenlik eğitimi alan gruba ait riskli davranış puanı ile güvenlik eğitimi almayan gruba ait puanlar arasında anlamlı bir farklılık bulunmazken, güvenlik eğitimi alan grubun korumacı davranış puanı güvenlik eğitim almayan gruptan daha yüksektir. Bu sonuç açıkça eğitimin bireylerde farkındalığı arttırdığını göstermektedir.

Anket formundan elde edilen verilerin analizi sonucu ulaşılan diğer önemli bir bilgi ise katılımcıların başlarına gelen ya da karşılaştıkları bir bilişim suçunu hiçbir makama iletmediği, bunun nedeninin de nereye bildireceklerini bilmemeleri olduğudur. Katılımcıların konu ile ilgili güncel hukuki gelişmelerin takip etme

oranları da düşük bulunmuştur (%7.7). Bu konudaki farkındalığın da düşük olduğu gözlemlenmektedir.

Çalışma sonucuna göre kişiler iletişim bilgilerini paylaşmayı özlük bilgilerini paylaşmaktan daha mahrem bulmaktadır. Benzer bir sonuç Şahinaslan ve arkadaşları [7] tarafından da bulunmuştur. TC kimlik numarasının korunmasına dair farkındalığın geliştiği gözlemlenirken, TC kimlik numarasının bulunduğu yerlere yönelik farkındalığın düşük olduğu gözlemlenmiştir. Bununla beraber katılımcıların % 83.8'i kişisel bilgilerinin başkaları tarafından kötü niyetle kullanılabileceğinin farkında olduğunu ifade etmektedir. Buna rağmen araştırmaya katılan katılımcılardan %45.4'ü hacker olmak istediğini ifade etmiştir. Benzer bir çalışma sonucuna göre [22], bu oran %42.2 olarak bulunmuştur.

2005 yılında Furnell [21] ve arkadaşları tarafından yapılan araştırma sonucuna göre katılımcıların %30' u bilgisayar açılışında şifre kullandıklarını ifade etmiştir. Tarafımızdan yapılan araştırma sonuçlarına göre bu oran %47.1 olarak bulunmuştur. Sonuçlar değerlendirildiğinde geçen beş yıl zarfında kullanıcıların bu konudaki farkındalıklarının arttığı görülmektedir.

Araştırma sonuçlarına göre bilgisayarlarında lisanslı yazılım kullanmaya her zaman dikkat edenlerin oranı %30.5, sık sık dikkat edenlerin oranı %27.9 ve hiçbir zaman dikkat etmeyenlerin oranı ise %9.4 olarak bulunmuştur. 2006 yılında Hikmet Dijle tarafından hazırlanan yüksek lisans tezi [23] kapsamında yapılan araştırma sonuçlarına göre katılımcılardan %72.5'i lisanssız yazılım kullandığını ifade etmiştir. Sonuçlar karşılaştırıldığında oranlar arasında anlamlı farklılık olduğu ve bu konuya yönelik farkındalığın arttığı gözlemlenmektedir. Aynı araştırma kapsamında katılımcıların %81.3'ü internet üzerinden alışveriş yapmadığını ifade etmiştir. Tarafımızdan yapılan araştırma sonuçlarına göre ise, katılımcıların %39.2'si internet üzerinden alışveriş yapmadığını ifade etmiştir. Sonuçlar karşılaştırıldığında geçen dört yılda internet üzerinden daha çok alışveriş yapıldığı görülmektedir.

Araştırma kapsamında katılımcıların parolalarını yazılı olarak kolay erişebilecekleri bir yerde saklayıp saklamadıkları da incelenmiştir. Araştırma sonuçlarına göre

katılımcıların %42.30’ u parolalarını yazılı olarak kolay erişebilecekleri yerlerde sakladıklarını ifade etmişlerdir. Yapılan benzer bir çalışmanın [24] sonuçlarına göre ise bu oran %66 olarak bulunmuştur. Buna göre katılımcıların konuya ilişkin farkındalıklarının arttığı gözlemlenmektedir.

Sonuç olarak katılımcıların farkındalık oranlarının çok yüksek olmadığı, bireysel bazda korumacı davranışların henüz tam olarak gelişmediği görülmektedir. Bununla birlikte suça maruziyet oranlarının düşük olduğu gözlemlenmiştir. Konu hakkında eğitim alan bireylerin eğitim almayanlara oranla farkındalıklarının yüksek olduğu ve daha korumacı davrandıkları görülmektedir. Günümüzde doğru ve bilinçli kullanılmadıkları takdirde risk içeren bazı bilişim teknolojilerinin kullanımı kaçınılmaz bir hale gelmiştir. Bu noktada önemli olan bireyin kişisel bilişim güvenliği farkındalığını yükseltmek ve korumacı davranışlar geliştirmesini sağlamaktır. Özellikle e-devlete geçişin sağlandığı bu günlerde gerek kullanıcıları gerekse sistemi korumak için bireysel farkındalığın arttırılması, riskleri en aza indirmek için şarttır. Bu konuda çeşitli eğitimler düzenlenmeli, toplumsal farkındalığı arttırıcı kampanyalar yapılmalıdır. Bunların dışında halen yasa tasarısı olarak bekleyen Kişisel Verilerin Korunması Kanunu bir an önce yasalaştırılmalıdır. Mevcut hukuki düzenlemeler revize edilmeli, adli kadrolar konu hakkında eğitilmelidir. Bilişim Savcılığı ve Bilişim Mahkemeleri kurulmalıdır. Bilgi teknolojilerine dair güvenlik eğitimleri 7’den 70’e tüm topluma verilmeli, TC vatandaşı olan herkesin konu hakkındaki farkındalığının artırılması bir devlet politikası olmalıdır.

KAYNAKLAR LİSTESİ

[1] http://www.comscore.com/Press_Events/Press_Releases/2009/11/93_Percent_of_Internet_Users_in_Turkey_Visited_Google_Sites_in_September_2009,20 Temmuz 2010

[2] http://www.tuik.gov.tr/PreTablo.do?tb_id=60&ust_id=2, 10 Mart 2010

[3] http://www.bilgiportal.com/v1/idx/18/234/internetBiliim-Szl/makale/internet-Tarihi.html, 17 Temmuz 2010.

[4] Şahinaslan, E., Kandemir, R. ve Şahinaslan O. Bilgi Güvenliği Farkındalık Eğitim Örneği. Akademik Bilişim'09 - XI. Akademik Bilişim Konferansı Bildirileri, Harran Üniversitesi, Şanlıurfa-Türkiye, s. 189-194, 2009.

[5] Canbek, G. ve Sağıroğlu, Ş. Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. *Politeknik, 9* (3), 165-174, 2006.

[6] Sağsan, M. Bilgi teknolojileri güvenliği: Ulusal bilginin korunmasına pragmatik bir yaklaşım ve Türkiye perspektifi. Stratejik Analiz, vol.2,no.22,s74-81 2002.

[7] Mitnick D. Kevin, Aldatma Sanatı, ODTU Yayıncılık, Ankara, 2009.

[8] Şahinaslan E., Kantürk A., vd. Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri, Akademik Bilişim'09 - XI. Akademik Bilişim Konferansı Bildirileri, Harran Üniversitesi, Şanlıurfa-Türkiye, s. 597-602, 2009

[9] Vural, Y., Bayındır, M. ve Tamer O. Anayurt Güvenliğinin Sağlanmasında Bilgi Sistemleri Güvenliğinin Önemi. Akademik Bilişim'09 - XI. Akademik Bilişim Konferansı Bildirileri, Harran Üniversitesi, Şanlıurfa-Türkiye, s. 607-612, 2009.

[10] Aktan C. Coşkun, Vural Y. İstiklal, Bilgi Çağı Bilgi Yönetimi ve Bilgi Sistemleri, Çizgi Yayınevi, Konya, 2005.

[11] Köksal, A. Bilişim Terimleri Sözlüğü, Türk Dil Kurumu Yayınları, Ankara,1981. http://tdkterim.gov.tr/?kelime=bili%FEim&kategori=terim&hng=md, (10 Mayıs 2010).

[12] Ketizmen, M. ve Ülküderner, Ç. E-devlet uygulamalarında kişisel verilerin korunma(ma)sı. XII. "Türkiye'de İnternet" Konferansı, Ankara-Türkiye, s.189-194, 2007.

[13] Dülger, M. Volkan, Bilişim Suçları, Seçkin Yayınevi, Ankara, 2006.

[14] http://bulentozer.av.tr/hukuk/bilisim-hukuku/bilisim-suclarinin-tanimi.html, 13 Temmuz 2010.

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

[16] TBD, Bilişim Sistemleri Güvenliği El Kitabı, Kamu Bilişim Platformu Raporları. No.1, TBD Ankara, 54s, 2006.

[17] Uzunay, Y. Dijital saldırılar, emniyet güçleri açısından önemi ve korunma yolları. Polis Bilimleri Dergisi, 5(2), s. 131-146, 2003.

[18] http://www.pro-g.com.tr/whitepapers/bilisim-guvenligi-v1.pdf, 17 Temmuz 2010.

[19] Canbek, G. Ve Sağıroğlu, Ş. Kötücül ve casus yazılımlar. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi,* 22 (1), 121-136, 2007.

[20] İlbaş Ç., Bilişim Suçlarının Sosyo-Kültürel Seviyelere Göre Algı Analizi, Başkent Üniversitesi, Fen Bilimleri Enstitüsü, 87s, 2009.

[21] Burlu K., Bilişimin Karanlık Yüzü, Nirvana Yayıncılık, Ankara, 2010.

[22] Furnell, S. M., Jusoh A. , and Katsabas D. The challenges of understanding and using security : A survey of end-users. Computers & Security,vol.25,no.5, s.27 - 35, 2005.

[23] Dijle, H. Türkiye'de eğitimli insanların bilişim suçlarına yaklaşımı. Yayınlanmamış yüksek lisans tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, 75s, 2006.

[24] Bensmann I., Intelligent Search Strategies on Human Chosen Passwords, Technische Universtat, Fakultat für Informatik, Dortmond, 96s,2009.

[25] Hoonakker, P., Bornoe, N. & Carayon, P. Password authentication from a human factors perspective: Results of a survey among end-users. Proceedings of the Human Factors and Ergonomics Society 53rd Annual Meeting, 2009.

[26] Chai, & Bagchi S., Morrell C., at all, Role of percieved importance of information security: an exploratory study of middle scholl children's information security behavior, Issues in Informing Science and Information Technology, vol.3, s.127-135, 2006.

[27] İlkan M, Iscioglu E., Egelioğlu F. , Doğanalp A., Information Security Awareness of Academic Staff Members: An example of Eastern Mediterranean University of Computing and Technology, *Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı,* Ankara-Türkiye,s. 247-251, 2010.

[28] Yenisey, M. M.,Ozok A.A., and Salvendy G. Perceived security determinants in e-commerce among Turkish university students. Proceedings Of World Academy Of Science, Engineering and Technology, vol.24, no.4,s.259 - 274, 2008.

[29] Tonta Y., Dijital Yerliler, Sosyal Ağlar ve Kütüphanelerin Geleceği, Türk Kütüphaneciliği Dergisi, 23(4), s.742-768, 2009.

[30] http://www.hurriyet.com.tr/gundem/15485772p.asp, 15 Temmuz 2010.

EK 1. Akademik ve İdari Personele Uygulanan Anket Formu

Bu anket çalışması, Başkent Üniversitesi İstatistik ve Bilgisayar Bilimleri Anabilim Dalı'nda yürütülen bir Yüksek Lisans Tezi kapsamında kişisel bilişim güvenliği farkındalığını ölçmeyi amaçlamaktadır. Anketi cevaplama süresi ortalama 10 dakikadır. Anket cevapları herhangi bir kişisel bilgi ile ilişkilendirilmeyecek ve üçüncü şahıslarla paylaşılmayacaktır. İstatistiksel sonuçlar, kamu yararına olmak üzere yayınlanacak, Bilgi Toplumu ve E-Devlet Projeleri yapılandırmasına ışık tutması amacıyla kullanılacaktır. Anket sonuçlarını talep eden cevaplayıcıların ogutcu@baskent.edu.tr
adresine "ANKET" konulu boş bir e-posta göndermeleri yeterlidir.

Katkılarınız ve ayırdığınız zaman için teşekkür eder, saygılar sunarız.

Arş. Gör. Gizem Öğütçü
Başkent Üniversitesi Başkent Üniversitesi, Ticari Bilimler Fakültesi,
Yönetim Bilişim Sistemleri Bölümü, Bağlıca Kampüsü, 06810, Ankara, TÜRKİYE

Yaşınız:……
Cinsiyetiniz: Kadın [ ] Erkek [ ]
Yaşadığınız Şehir: ……..
Eğitim Düzeyiniz: İlköğretim mezunu [ ]
Lise mezunu [ ]
Önlisans / Lisans mezunu [ ]
Y.Lisans mezunu [ ]
Doktora mezunu [ ]

Çalıştığınız kurumdaki göreviniz: Akademik Personel [ ] İdari Personel [ ]

Ünvanınız : …….

Çalıştığınız Birim/Bölüm: ……

İşyeriniz dışındaki internet erişim şekliniz nedir? (Birden fazla şık işaretleyebilirsiniz.)
Kablolu modem ile bağlantı [ ]
Kablosuz modem ile bağlantı [ ]
Cep telefonu aracılığı ile bağlantı [ ]
İnternet kafeden bağlantı [ ]
Erişimim yok [ ]

Bilgisayar güvenliği / internet güvenliğine yönelik eğitim aldınız mı veya iş deneyiminiz oldu mu?
Evet [ ] Hayır [ ]

Ortalama kaç yıldır internet kullanıyorsunuz? .....yıl

Ortalama internet kullanım sıklığınız:
Günde ..... Saat
Haftada …….. Gün
Diğer …….

Yönerge: Aşağıdaki ifadeleri, kullanma sıklığınıza göre cevaplayınız. Yanıtınız yalnızca evet ise her zaman, yalnızca hayır ise hiçbir zaman ifadelerinden birini işaretleyebilirsiniz.

	Her Zaman	Sık Sık	Bazen	Nadiren	Hiçbir Zaman
1.Msn Messenger, GTalk, Skype ve benzeri sohbet programlarını kullanırım.					
2.Bir iletişim aracı olarak elektronik posta (e-mail) kullanırım.					
3.Birden fazla elektronik posta adresi kullanırım.					
4.Kurumsal e-posta adresimi günlük işlerde de kullanırım					
5.İnternette e-posta gruplarına üye olurum.					
6.Facebook, Twitter ve benzeri sosyal ağ sitelerini kullanırım.					
7.Sosyal ağlarda gönderilen uygulama davetlerini kabul ederim.					
8.İnternet bankacılığı kullanırım.					
9.İnternet üzerinden alışveriş yaparım.					
10.E-Vatandaşlık hizmetleri veren web sayfalarını (TC kimlik no sorgulama, sosyal güvenlik primi sorgulama vb.) kullanırım.					
11.İnternet üzerinden oyun oynarım					
12.İnternet üzerinden müzik, film, program ve dosya indiririm/kaydederim.					
13.İnternet üzerinden video/film izlerim.					
14.İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM No, e-posta, Adres) paylaşırım.					
15.İnternet ortamında gerektiği durumlarda özlük bilgilerimi paylaşırım. (Ad, Soyad, Doğum Tarihi vb…)					
16.Bilgisayarımda orijinal (lisanslı) yazılım kullanmaya dikkat ederim.					
17.Virüs temizleme, casus yazılım önleme vb. programları kullanırım.					
18.Güvenlik duvarı, reklam önleyici vb. programlar kullanırım.					
19.İçerik filtreleme programları kullanırım					
20.E-posta filtreleme yazılımları kullanırım.					
21.İzleme yazılımları kullanarak internet üzerinde yapılan etkinlikler hakkında bilgi sahibi olurum.					
22.Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim.					
23.Herkesin kullanımına açık bir bilgisayardan ayrılmadan önce geçici internet dosyalarını ve Web gezinti geçmişlerini silerim.					
24.Dosyalarımı şifrelerim.					
25.İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım.					
26.Elektronik/ Mobil imza kullanırım.					
27.İnternet sitelerine girerken genellikle sık kullanılanlar listesini kullanırım.					
28.Sohbet (chat) yaparken dosya transferi yaparım.					
29.Bilgisayarımdaki dosyaları paylaşıma açarım.					
30.Halka açık internet erişimi olan yerlerde internet bankacılığı kullanırım.					
31.İnternette karşılaştığım bilişim suçlarını ilgili makamlara iletirim.					
32.Parolalarımı başkalarıyla paylaşırım.					

	Her Zaman	Sık Sık	Bazen	Nadiren	Hiçbir Zaman
33.Parolalarımı yazılı olarak kolay ulaşabileceğim yerlerde saklarım.					
34.Bilgisayarım şifre ile açılır.					
35.Bilgisayarımda otomatik kullan özelliğini kapatırım.					
36.Tanımadığım kişilerden gelen e postaları açarım, gelen ekleri indiririm.					
37.Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat ederim.					
38.Parolalarımı sık sık değiştiririm.					
39.Kablosuz modem şifremi değiştiririm.					
40.Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım.					
41.Kullandığım programların güncellemelerini düzenli olarak yaparım.					
42.Bilgisayar virüsleri nedeniyle sorun yaşadım.					
43.Online alışverişten dolayı maddi zarara uğradım.					
44.Kredi kartım kopyalandı.					
45.Kişisel bilgilerimi internette paylaştığım için sıkıntı yaşadım.					
46.Elektronik bankacılık kullandığım için maddi zarara uğradım.					
47.Kişisel bilgilerim iznim olmadan üçüncü şahıslarla paylaşıldı/ internette yayınlandı.					
48.İnternet üzerindeki hesaplarıma ait kullanıcı adım ve şifrem ele geçirildi.					
49.İnternette kimliği belirsiz kişiler tarafından şahsıma yönelik hakaret, tehdit, ahlaksız teklif aldım.					
50.Kumar içerikli siteler nedeniyle zarara uğradım.					
51.Sosyal ağ siteleri nedeniyle zarara uğradım.					
52.Arkadaşlık siteleri nedeniyle zarara uğradım.					
53.İnternette gezerken isteğim dışında şiddet ya da pornografik içerikli yayınlarla karşılaştım.					
54.Bilgisayarımdaki dosyalarım çalındı/silindi.					
55.Adıma sahte hesaplar açıldı.					
56.İnternet üzerinden yaptığım yazışmalar isteğim ve bilgim dışında başkaları tarafından izlendi, kaydedildi.					
57.Bilgisayar ve internet güvenliği ile ilgili hukuki gelişmeleri takip ediyorum.					
58.Başıma gelen/ karşılaştığım bir bilişim suçunu nereye bildireceğimi biliyorum.					
59.Kişisel bilgilerimin başkaları tarafından kötü amaçlarla kullanılabileceğini biliyorum.					
60.Kredi kartı kullanarak alışveriş yaptığımda kredi kartı bilgilerimin karşı tarafça saklanması benim için önemli değildir.					
61.Hacker olmak isterdim.					

Yönerge: Aşağıdaki davranışları ve teknolojilerin kullanımını ne derecede tehlikeli bulduğunuzu işaretleyiniz.	**Çok Tehlikeli**	**Tehlikeli**	**Az Tehlikeli**	**Tehlikesiz**	**Fikrim Yok**
62.Virüs yazılımları					
63.Virüs koruma programları					
64.Casus programlar (Keylogger, Screenlogger,Trojan vb..)					
65.Dosya paylaşım programları (Ares, Limewire vb...)					
66.ActiveX, Javascript vb. mobil kodlar.					
67.Web tarayıcıları (Internet Explorer, Mozilla Firefox, Google Chrome vb.)					
68.Sohbet programları (Messenger, ICQ vb..)					
69.İstenmeyen/ Spam / Junk e-postalar					
70.Online oyunlar					
71.USB/Harici bellekler					
72.MS Office uygulamaları (Word,Excel vb.)					
73.Klavye kullanımı					
74.Kopya/ Kırık/ Korsan program kullanımı					
75.Müzik/ Resim/ Film gibi materyallerin herhangi bir bedel ödemeden indirilmesi					
76.Reklam içerikli e-postaların açılması					
77.Elektronik bankacılık kullanımı					
78.İnternet ortamında yabancılarla sohbet / bilgi paylaşımı					
79.İnternetten alışveriş yapılması					
80.Pornografik içerikli web sitelerine girilmesi					
81.Kumar, bahis sitelerine girilmesi					
82.Sosyal ağlara üye olunması (Facebook,Twitter vb.)					
83.Bluetooth kullanımı					
84.Kablosuz modem kullanımı					
85.İnternetten kontör yüklenmesi					
86.Kırık veya ücretsiz güvenlik programı kullanımı					
87.Bina girişlerinde güvenlik birimine nüfus cüzdanı veya sürücü belgesinin teslim edilmesi					
88.Kargo, GSM operatörü vs. gibi kuruluşlara nüfus cüzdanı bilgilerinin verilmesi					
89.Vatandaşlık numarasının başka şahıslar tarafından bilinmesi					

Anket tamamlanmıştır. Anket formuna ilişkin (varsa) görüş, eleştiri ve önerilerinizi lütfen belirtiniz:

İletişim Bilgilerim:

Arş. Gör. Gizem Öğütçü

Tel: 0090 312 234 10 10 / 1757
Faks: 0090 312 234 11 79 e-mail: ogutcu@baskent.edu.tr

EK 2. Öğrencilere Uygulanan Anket Formu

Bu anket çalışması, Başkent Üniversitesi İstatistik ve Bilgisayar Bilimleri Anabilim Dalı'nda yürütülen bir Yüksek Lisans Tezi kapsamında kişisel bilişim güvenliği farkındalığını ölçmeyi amaçlamaktadır. Anketi cevaplama süresi ortalama 10 dakikadır. Anket cevapları herhangi bir kişisel bilgi ile ilişkilendirilmeyecek ve üçüncü şahıslarla paylaşılmayacaktır. İstatistiksel sonuçlar, kamu yararına olmak üzere yayınlanacak, Bilgi Toplumu ve E-Devlet Projeleri yapılandırmasına ışık tutması amacıyla kullanılacaktır. Anket sonuçlarını talep eden cevaplayıcıların ogutcu@baskent.edu.tr
adresine "ANKET" konulu boş bir e-posta göndermeleri yeterlidir.

Katkılarınız ve ayırdığınız zaman için teşekkür eder, saygılar sunarız.

Arş. Gör. Gizem Öğütçü
Başkent Üniversitesi Başkent Üniversitesi, Ticari Bilimler Fakültesi,
Yönetim Bilişim Sistemleri Bölümü, Bağlıca Kampüsü, 06810, Ankara, TÜRKİYE

Yaşınız:……
Cinsiyetiniz: Kadın [ ] Erkek [ ]
Yaşadığınız Şehir: ……
Okuduğunuz Bölüm: ……
Sınıfınız: Hazırlık [ ]
1 [ ]
2 [ ]
3 [ ]
4 [ ]

Okulunuz dışındaki internet erişim şekliniz nedir? (Birden fazla şık işaretleyebilirsiniz.)
Kablolu modem ile bağlantı [ ]
Kablosuz modem ile bağlantı [ ]
Cep telefonu aracılığı ile bağlantı [ ]
İnternet kafeden bağlantı [ ]
Erişimim yok [ ]

Bilgisayar güvenliği / internet güvenliğine yönelik eğitim aldınız mı veya iş deneyiminiz oldu mu?
Evet [ ] Hayır [ ]

Ortalama kaç yıldır internet kullanıyorsunuz?.....yıl

Ortalama internet kullanım sıklığınız:
Günde ..... Saat
Haftada …….. Gün
Diğer …….

Yönerge: Aşağıdaki ifadeleri, kullanma sıklığınıza göre cevaplayınız. Yanıtınız yalnızca evet ise her zaman, yalnızca hayır ise hiçbir zaman ifadelerinden birini işaretleyebilirsiniz.

	Her Zaman	Sık Sık	Bazen	Nadiren	Hiçbir Zaman
1.Msn Messenger, GTalk, Skype ve benzeri sohbet programlarını kullanırım.					
2.Bir iletişim aracı olarak elektronik posta (e-mail) kullanırım.					
3.Birden fazla elektronik posta adresi kullanırm.					
4.Kurumsal e-posta adresimi günlük işlerde de kullanırım					
5.İnternette e-posta gruplarına üye olurum.					
6.Facebook, Twitter ve benzeri sosyal ağ sitelerini kullanırım.					
7.Sosyal ağlarda gönderilen uygulama davetlerini kabul ederim.					
8.İnternet bankacılığı kullanırım.					
9.İnternet üzerinden alışveriş yaparım.					
10.E-Vatandaşlık hizmetleri veren web sayfalarını (TC kimlik no sorgulama, sosyal güvenlik primi sorgulama vb.) kullanırım.					
11.İnternet üzerinden oyun oynarım					
12.İnternet üzerinden müzik, film, program ve dosya indiririm/kaydederim.					
13.İnternet üzerinden video/film izlerim.					
14.İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (Gsm No, e-posta, Adres) paylaşırım.					
15.İnternet ortamında gerektiği durumlarda özlük bilgilerimi paylaşırım. (Ad, Soyad, Doğum Tarihi vb…)					
16.Bilgisayarımda orijinal (lisanslı) yazılım kullanmaya dikkat ederim.					
17.Virüs temizleme, casus yazılım önleme vb. programları kullanırım.					
18.Güvenlik duvarı, reklam önleyici vb. programlar kullanırım.					
19.İçerik filtreleme programları kullanırım					
20.E-posta filtreleme yazılımları kullanırım.					
21.İzleme yazılımları kullanarak internet üzerinde yapılan etkinlikler hakkında bilgi sahibi olurum.					
22.Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim.					
23.Herkesin kullanımına açık bir bilgisayardan ayrılmadan önce geçici internet dosyalarını ve Web gezinti geçmişlerini silerim.					
24.Dosyalarımı şifrelerim.					
25.İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım.					
26.Elektronik/ Mobil imza kullanırım.					
27.İnternet sitelerine girerken genellikle sık kullanılanlar listesini kullanırım.					
28.Sohbet (chat) yaparken dosya transferi yaparım.					
29.Bilgisayarımdaki dosyaları paylaşıma açarım.					
30.Halka açık internet erişimi olan yerlerde internet bankacılığı kullanırım.					
31.İnternette karşılaştığım bilişim suçlarını ilgili makamlara iletirim.					
32.Parolalarımı başkalarıyla paylaşırım.					

	Her Zaman	Sık Sık	Bazen	Nadiren	Hiçbir Zaman
33.Parolalarımı yazılı olarak kolay ulaşabileceğim yerlerde saklarım.					
34.Bilgisayarım şifre ile açılır.					
35.Bilgisayarımda otomatik kullan özelliğini kapatırım.					
36.Tanımadığım kişilerden gelen e postaları açarım, gelen ekleri indiririm.					
37.Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat ederim.					
38.Parolalarımı sık sık değiştiririm.					
39.Kablosuz modem şifremi değiştiririm.					
40.Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım.					
41.Kullandığım programların güncellemelerini düzenli olarak yaparım.					
42.Bilgisayar virüsleri nedeniyle sorun yaşadım.					
43.Online alışverişten dolayı maddi zarara uğradım.					
44.Kredi kartım kopyalandı.					
45.Kişisel bilgilerimi internette paylaştığım için sıkıntı yaşadım.					
46.Elektronik bankacılık kullandığım için maddi zarara uğradım.					
47.Kişisel bilgilerim iznim olmadan üçüncü şahıslarla paylaşıldı/ internette yayınlandı.					
48.İnternet üzerindeki hesaplarıma ait kullanıcı adım ve şifrem ele geçirildi.					
49.İnternette kimliği belirsiz kişiler tarafından şahsıma yönelik hakaret, tehdit, ahlaksız teklif aldım.					
50.Kumar içerikli siteler nedeniyle zarara uğradım.					
51.Sosyal ağ siteleri nedeniyle zarara uğradım.					
52.Arkadaşlık siteleri nedeniyle zarara uğradım.					
53.İnternette gezerken isteğim dışında şiddet ya da pornografik içerikli yayınlarla karşılaştım.					
54.Bilgisayarımdaki dosyalarım çalındı/silindi.					
55.Adıma sahte hesaplar açıldı.					
56.İnternet üzerinden yaptığım yazışmalar isteğim ve bilgim dışında başkaları tarafından izlendi, kaydedildi.					
57.Bilgisayar ve internet güvenliği ile ilgili hukuki gelişmeleri takip ediyorum.					
58.Başıma gelen/ karşılaştığım bir bilişim suçunu nereye bildireceğimi biliyorum.					
59.Kişisel bilgilerimin başkaları tarafından kötü amaçlarla kullanılabileceğini biliyorum.					
60.Kredi kartı kullanarak alışveriş yaptığımda kredi kartı bilgilerimin karşı tarafça saklanması benim için önemli değildir.					
61.Hacker olmak isterdim.					

Yönerge: Aşağıdaki davranışları ve teknolojilerin kullanımını ne derecede tehlikeli bulduğunuzu işaretleyiniz.	**Çok Tehlikeli**	**Tehlikeli**	**Az Tehlikeli**	**Tehlikesiz**	**Fikrim Yok**
62.Virüs yazılımları					
63.Virüs koruma programları					
64.Casus programlar (Keylogger, Screenlogger,Trojan vb..)					
65.Dosya paylaşım programları (Ares, Limewire vb...)					
66.ActiveX, Javascript vb. mobil kodlar.					
67.Web tarayıcıları (Internet Explorer, Mozilla Firefox, Google Chrome vb.)					
68.Sohbet programları (Messenger, ICQ vb..)					
69.İstenmeyen/ Spam / Junk e-postalar					
70.Online oyunlar					
71.USB/Harici bellekler					
72.MS Office uygulamaları (Word,Excel vb.)					
73.Klavye kullanımı					
74.Kopya/ Kırık/ Korsan program kullanımı					
75.Müzik/ Resim/ Film gibi materyallerin herhangi bir bedel ödemeden indirilmesi					
76.Reklam içerikli e-postaların açılması					
77.Elektronik bankacılık kullanımı					
78.İnternet ortamında yabancılarla sohbet / bilgi paylaşımı					
79.İnternetten alışveriş yapılması					
80.Pornografik içerikli web sitelerine girilmesi					
81.Kumar, bahis sitelerine girilmesi					
82.Sosyal ağlara üye olunması (Facebook,Twitter vb.)					
83.Bluetooth kullanımı					
84.Kablosuz modem kullanımı					
85.İnternetten kontör yüklenmesi					
86.Kırık veya ücretsiz güvenlik programı kullanımı					
87.Bina girişlerinde güvenlik birimine nüfus cüzdanı veya sürücü belgesinin teslim edilmesi					
88.Kargo, GSM operatörü vs. gibi kuruluşlara nüfus cüzdanı bilgilerinin verilmesi					
89.Vatandaşlık numarasının başka şahıslar tarafından bilinmesi					

Anket tamamlanmıştır. Anket formuna ilişkin (varsa) görüş, eleştiri ve önerilerinizi lütfen belirtiniz:

İletişim Bilgilerim:

Arş. Gör. Gizem Öğütçü

Tel: 0090 312 234 10 10 / 1757
Faks: 0090 312 234 11 79 e-mail: ogutcu@baskent.edu.tr