Akdeniz İ.İ.B.F. Dergisi (29) 2014, 86-105

KİŞİSEL VERİ GÜVENLİĞİ VE KULLANICILARIN FARKINDALIK DÜZEYLERİNİN İNCELENMESİ

PERSONAL DATA SECURITY AND DETERMINATION OF ITS USERS' AWARENESS LEVEL

Hakan ÇETİN[1]

ÖZ

Dünya çapında küresel bir ağın oluşması, üretilen ve kullanılan bilginin türlerini ve şekillerini değiştirdiği gibi oluşabilecek risk türlerini de farklılaştırmıştır. Kişisel verilerin başka kişilerin eline geçmesi bu risk türlerinden birisidir. Kişisel verilerin korunması konusunda hem devletlere hem de kişilere düşen görevler bulunmaktadır. Çalışma kişisel veri güvenliği üzerinde gerçekleştirilmiş olup kişilerin bilgi güvenlik algıları, kullandıkları elektronik cihaz türleri ve cihazlardaki bilgi güvenliği adına aldıkları önlemler ve kullandıkları yöntemler incelenmiştir. Kişisel veri güvenliğini ölçmek amacıyla literatür taraması ve kişiler ile yüz yüze görüşmelerden elde edilen sorulardan oluşturulan "Kişisel Veri Güvenliği Farkındalığı" anketi geliştirilmiştir. Geliştirilen anket Antalya ilinde 526 kişiye uygulanmış ve 501 tanesi değerlendirmeye uygun görülmüştür. Katılımcılara ait verilerin analizinde t testi, faktör analizi ve varyans analizi kullanılmıştır. Analiz sonuçlarına göre; katılımcıların bilgi güvenliği noktasında farkındalık düzeylerinin ortalamanın üstünde olduğu belirlenmiş, kişisel veri paylaşımı farkındalık düzeyinin diğer farkındalık düzeylerine göre en yüksek olduğu tespit edilmiştir.

Anahtar Kelimeler: *Kişisel Veri Güvenliği, Veri, Bilgi, Bilgi Güvenliği, Veri Güvenliği Farkındalığı, Teknoloji*

ABSTRACT

The occurrence of a global network all around the world not only changed the types and forms of the produced and used data, but also differentiated the risk types that might occur. Acquisition of the personal data by other people is one of these risks types. There are duties for people as well as state for the protection of personal data. This study which was carried out on the protection of personal data, investigated the people' perception of information security, types of electronic device they use and the precautions taken for information security on devices and methods they used. A questionnaire of "Awareness of Personal Data Protection" was developed with the aim of measuring personal data protection with questions obtained by literature review and face to face interview with people. The questionnaire was applied to 526 people in Antalya and 501 of them has ben considered for the evaluation. T test, factor analysis and

[1] Akdeniz Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Ekonometri Bölümü, Yrd. Doç. Dr.

variance analysis were used in the analysis of data belonging to participants. According to results; awareness level of participants about information security was determined as higher than average and awareness level of personal data sharing was found the highest among other awareness levels.

Key Words: *Personal Data Protection, Data, Information, Information Security, Awareness of Data Protection, Technology*

GİRİŞ

Günümüzde eğitim hayatından, çalışma hayatına kadar her aşamada aktif olarak bilgi ve iletişim teknolojileri kullanılmaktadır. Şartlar itibari ile kişilerin bilgi ve iletişim teknolojilerini doğru tanımlanmaları teknolojiden verimli şekilde yararlanılmasını sağlamaktadır. Buna bağlı olarak bilgi ile ilişkili tüm kavramların, yöntemlerin ve stratejilerin öneminin de aynı oranda anlaşılması ve kavranması gerekmektedir (Canbek ve Sağıroğlu, 2006:69).

İnternetin hayatımızı kuşattığı günümüzde her türlü kişisel veriler elektronik cihazlarda tutulmaktadır. Banka bilgileri, çalışma hayatındaki bilgiler, ödevler hatta günlük ruh hali elektronik cihazlar vasıtası ile anlık olarak depolanmakta ve internet kullanılarak istendiği zaman başka kişiler ile paylaşılmaktadır. İnternetin giderek hayatımızın vaz geçilmez bir parçası olmasıyla birlikte siber saldırı sayısı artmıştır. Buna bağlı olarak da bilgi güvenliğinin sağlanması zorlaşmıştır (Karaarslan, 2013). Kişisel verilerin dijital ortamdan gelen tehditlere ve saldırılara karşı korunması için bilgi güvenliğinin oldukça önemli olduğu yadsınamaz bir gerçekliktir. Kişisel veri güvenliği sadece kişinin kendisini değil çalıştığı kurumu da ilgilendirmektedir. Kurumlar bilgi güvenliğini sağlayabilmek için yüksek miktarda paralar ödeyerek koruma tedbirleri almaktadırlar. Bu üst seviyede alınan önlemler bilgi güvenliğinin yüzde yüz sağlandığı anlamına gelmemektedir (Şahinaslan vd, 2009).

Bilgi güvenliği üzerinde yapılan çalışmalarda teknoloji ve insan faktörünün bilgi güvenliğine etkisinin %50'lerde olduğu görülmektedir (Şahinaslan vd, 2009). Bu orandan da anlaşıldığı gibi kişisel veri güvenliği ve güvenlik farkındalık düzeyinin yüksekliği kişisel olarak kendi dijital güvenliğini sağlarken çalıştığı kurumunda güvenliğini sağladığını göstermektedir.

Kişisel veri güvenliği kavramından sadece bilgisayar güvenliği anlaşılmamalıdır. Giderek kullanıcı sayısı artan tablet pc ve akıllı telefon diye adlandırılan taşınabilir cihazlarda veri güvenliği içerisinde değerlendirilmektedir. Türkiye İstatistik Kurumu ve Bilgi Teknolojileri Kurumunun 2014'ün ikinci çeyreğinde yayınlamış olduğu raporlarda Hane

Halkı Bilişim Teknolojileri Kullanımında 16-74 yaş arası kişilerde internet kullanımı %53,8'e (40 Milyon), hane oranının ise %60'lara ulaştığı belirtilmiştir. Türkiye'de yaklaşık %93,81 penetrasyon oranına karşılık gelen toplam 71.908.742 mobil abone sayısının olduğu ve taşınabilir cihaz sayısının artışına bağlı olarak Tablo 1'de görüldüğü gibi mobil internet kullanımının %37'lere (31.104.046 abone) ulaştığı belirtilmektedir (TUIK, 2014, BTK, 2014). 2014 yılı üçüncü çeyrekte 3G abone sayısı 56.780.787'e ulaşırken, toplam mobil internet kullanım miktarı 89.940 TByte olarak gerçekleşmiştir (BTK, 2014)

Tablo 1. Türkiye'deki Toplam İnternet Abone Sayısı

	2013 3. Çeyrek	**2014 2. Çeyrek**	**2014 3. Çeyrek**	**Çeyrek Büyüme Oranı (2014-2 2014-3)**	**Yıllık Büyüme Oranı (2013-3 2014-3)**
DSL	6.662.999	6.655.076	6.721.902	1,0%	0,88%
Mobil Bilgisayardan İnternet	1.742.995	1.379.300	1.277.070	-7,4%	-26,73%
Mobil Cepten İnternet	21.099.677	27.066.363	29.826.976	10,2%	41,36%
Kablo İnternet	483.046	496.038	514.965	3,8%	6,61%
Fiber	967.309	1.330.922	1.393.614	4,7%	44,07%
Diğer	120.159	105.103	103.165	-1,8%	-14,14%
Toplam	31.076.185	37.032.802	39.837.692	7,6%	29,19%

Kaynak: BTK, 3.Çeyrek Pazar Veri Raporu 2014:38

Artan abone ve cihaz sayısı veri dolaşım hızını ve miktarını artırmıştır. Verilerin dijital ortamda yer almaları kötü niyetli kişileri de bu ortamlara yöneltmiş ve kullanıcılar için tehdit oranı artmıştır. Bu kapsamda çalışma kişisel veri güvenliğinin önemi üzerinde durmuş bilgi ve bilgi güvenliği kavramlarını açıklamıştır. Bilgi Güvenliği farkındalığı üzerinde yapılan çalışmaların yazın taraması gerçekleştirilmiş ve son bölümde ise geliştirilen "Kişisel Veri Güvenliği Farkındalığı" anketinden elde edilen bulgular üzerinde durulmuştur.

1. Bilgi, Bilgi Güvenliği ve Kişisel Verilerin Korunması

"Information" kelimesinin Türkçe karşılığı olarak bazen "enformasyon" bazen "bilgi" kavramları kullanılmaktadır. Çoğu kimse "bilgi" terimini kullandığı zaman "information" ya da "knowledge" ayrımı gözetmemektedir. Knowledge ve Information terimleri aslında kullanılış şekilleri olarak farklılık arz etmektedir. Myers (1996) bu iki terim arasındaki

farkı şu şekilde ifade etmektedir. Information (Enformasyon) işlenmiş ve anlam kazanmış veri, bilgi ise değer kazanmış enformasyondur.

Bilgi ait olduğu alana ve elde ediliş şekillerine göre literatürde teknik bilgi, akademik bilgi, teorik bilgi, tarihi bilgi, dini bilgi, bilimsel bilgi vb. gibi farklı biçimlerde arz edebilmektedir. Bilginin yönetimi açısından literatürde en yaygın olarak kullanılan bilgi türleri örtülü-açık bilgi ve bireysel-sosyal bilgidir (Zaim, 2005:74). Buckland (1991:1) "bilgi" terimini üç ayrı anlamda tanımlamaktadır:

- Süreç olarak bilgi
- Bilgi olarak bilgi
- Nesne olarak bilgi

Süreç Olarak Bilgi, yeni bir şeyler öğrenildiğinde bunu mevcut bilgiler ile değiştirme veya karşılaştırma işlemiyle bu bilgilerin başkalarına aktarılması veya söylenmesi sürecine "süreç olarak bilgi" adı verilmektedir. Kısacası bu sürece bilgilenme süreci de denilmektedir.

Bilgi Olarak Bilgi, süreç içerisinde karşı tarafa aktarılan değere ise "bilgi olarak bilgi" adı verilmektedir.

Nesne Olarak Bilgi, "Bilgi" terimi bilgilendirici, bilgi taşıyıcı nesneler (kitap, dergi, film, belge, vd.) için de kullanılmaktadır. Bu anlamda yapılan bilgilendirme işlemlerine "nesne olarak bilgi" denilmektedir.

"Barnatt'ın ifadesi ile bilgi, işlenmiş, derlenmiş, organize edilmiş, yorumlanmış, karar alabilmede kullanılabilmek için bir işlem sürecinden geçirilerek, anlamlı ve değerli hale dönüştürmüş, kararları ve davranışları etkiyen değerdir" (Tutar, 2010:23).

Bilgi güvenliği kavramı ise bilginin tehditlere karşı uygun şekillerde korunması anlamına gelmektedir. Canbek ve Sağıroğlu (2006:72) bilgi güvenliğini "Bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesi olarak" tanımlamaktadır. Bilginin korunmasında dikkat edilmesi gereken noktalar bulunmaktadır. Bilginin korunmasında gizliliğin gözetilmesi, bütünlüğün sağlanması ve istenildiği zaman ulaşılabilmesi özelliklerinin olması gerekmektedir.

Bilgi gizliliğinin gözetilmesi; Bilginin sadece izin verilen kişi veya kişiler tarafından kullanılabilir olması gizlilik özelliğini tanımlamaktadır. Bilginin sadece yetkili kişiler tarafından erişilebilir durumda olması, (Clarke, 2011) yetkisiz kişilerin erişiminin engellenmesidir.

Bilginin bütünlüğü; Bir bilginin kısmen bozulmuş veya kısmen değiştirilmiş olması bütünlüğünün bozulması anlamına gelmektedir (Dulaney, 2010). Bilgi bütünlüğünün sağlanabilmesi için; İçeriğinin doğru, güncel ve geçerli olması, yetkisiz kişiler tarafından değiştirilmemiş olması gerekmektedir.

Bilginin erişilebilirliği; Gizlilikten farkı, kimlerin bilgiye erişebildiğinden çok, bilginin erişilebilir olup olmaması ile ifade edilmektedir (Dulaney, 2010). Bilginin olması gereken yerde ve gerektiğinde kullanıma hazır olduğunun güvence altında tutulmasıdır.

Bilgi güvenliğinin sağlanması bilgi ve iletişim teknolojilerinin kullanımının artması ile birlikte giderek zorlaşmaktadır. Saldırı sayısı artmakta her gün farklı zararlı yazılım türleri ağda gezinir hale gelmektedir. Riskin bu kadar arttığı ortamda kişisel verilerin korunması temel bir hak olmaktadır (Kalkınma Bakanlığı, 2013:12).

Kişisel verilerin korunmasına yönelik olarak Türkiye Cumhuriyeti ilk çalışmasına 1989 yılında kanun tasarısı hazırlığı ile başlamıştır. Tasarı çalışmaları 2006 yılına kadar sürmüş ve 2008 yılında Türkiye Büyük Millet Meclisine sevk edilmiş fakat yasalaşamadan hükümsüz sayılmıştır. 2012 yılında tasarı tekrar başbakanlığa gönderilmiş ve halen kişisel verilerin korunması kanunun yasalaşması beklenmektedir.

2. Kişisel Veri Güvenliği Tehditleri ve Önlemler

Bilişim teknolojilerinde yaşanan gelişmeler birçok yeniliğin ve güzelliğin yanında bilgisayar ağlarını ve sistemlerini bir saldırı aracı haline getirmiş ve kullanılan sistemler de açık birer hedef haline gelmiştir (Johnson, 2000).

Türkiye'de 2005 yılında Koç.net tarafından yapılan çalışmada internet kullanıcılarının %65'nin güvenlik duvarı kullanmadığı, %30'nun casus yazılımlara karşı korunmadığı, web sunucularının %43'ünün güvenlik zaafı gösterdiği ve Alan adı hizmeti sağlayan sunucuların %22'sinin güvenlik açığı olduğu tespit edilmiştir (Koç.net, 2005:5).

Kişisel Veri Güvenliğini tehdit eden unsurlar; İşletim Sistemi açıkları, Kullanıcı hesap açıkları, Paylaşımlar ve hizmetler, Web tarayıcı açıkları, Virüsler, trojan'lar, truva atları, casus yazılımlar, spam, exploit ve keylogger gibi zararlı yazılımlar ile korsanlar şeklinde ifade edilebilir (Zeydan, 2006).

Kişisel verilerin korunmasında kullanılan yöntemleri Şahinaslan ve arkadaşları (2009) beş temel yapıda Vacca (2009) ise üç ana bölümde özetlemiştir.

Şahinaslan ve arkadaşlarına göre;

Cihaz Sistem Güvenliği: Kullanılan ürün ister sabit bir masaüstü bilgisayar isterse taşınır bir cihaz olsun bu tip sistemlerde güvenliğin sağlanabilmesi için öncelikle sisteme bir giriş şifresi konulmalıdır. Sistem

güncellemeleri sürekli yapılmalı sistem güncel tutulmalıdır. Sistemde paylaşıma açık bir klasör veya dosya olup olmadığı kontrol edilmeli var ise kapatılmalıdır. Güvenilirliğini bilemediğimiz yazılımlar sisteme kurulmamalıdır. Ayrıca sunucu hizmetleri olan ftp ve telnet gibi portallar kapalı tutulmalıdır.

Zararlı Yazılım Güvenliği: Virüs, Trojan, gibi casus yazılımlar ile spam, keylogger gibi zararlı yazılımlardan sistemi koruyabilmek için antivürüs ve anti-spyware tipi programlar kullanılmalı ve sürekli güncelleme yaparak yazılımın yeni tehlikelere karşı diri kalması sağlanmalıdır. Ayrıca işletim sisteminin güvenlik risk düzeyi en üst seviyeye getirilmelidir. İnternet aracılığı ile sisteme gelen zararlı yazılımların bulaşma yöntemleri kullanıcı tarafından iyi bilinmeli ve zararlı yazılım yakalayan yazılımların arka planda sürekli çalışması sağlanmalıdır.

Kişisel Güvenlik Duvarı: Firewall olarak da ifade edilen güvenlik duvarı sistem üzerinden geçen trafiği denetleyerek kural tablosu üzerinde yazılı olan kurallara göre saldırganların yada zararlı yazılımların engellenmesini sağlamaktadır.

Erişim Güvenliği: Sistemden başka noktalara erişim sağlarken gizlilik, güvenilirlik ve kullanılabilirlik kriterleri dikkate alınarak işlem yürütülmelidir. Kullanıcı erişim güvenliğini sağlarken sanal özel ağ olarak ifade edilen VPN programlarını kullanmalıdır. İnternet kullanılarak bağlantı sağlanan web sayfalarında SSL sertifikalı https protokolüne sahip sitelere güvenmelidir. Dosya sistemleri şifrelenerek yetkisiz erişime karşı koruma sağlanmalıdır. Kablosuz iletişimde şifre rutin olarak değiştirilmeli ve WPA2 şifreleme seviyesi kullanılmalıdır. Sistemi eğer bir çocuk kullanıyor ise ebeveyn kontrolünde kullanmalıdır (Şahinaslan vd., 2009).

Sosyal Ağları Kullanım Güvenliği: Sosyal paylaşım sitelerinde kişiler kendileri ile ilgili önemli ve kritik bazı bilgileri paylaşabilmektedirler. Paylaşılan bilgiler gerekli önlemler alınmazsa kötü niyetli şahıslar tarafından kullanılmakta ve kullanıcılar bir anda hedef haline gelebilmektedir. Kullanıcılar sosyal paylaşım sitelerinde kart bilgileri, sigorta bilgileri, nüfus cüzdan bilgileri, kurum bilgileri vb. kritik bilgileri kesinlikle paylaşmamalıdır.

Vacca'ya (2009) göre ise;

Mantıksal Güvenlik: Uygulama ve Altyapı güveliği olmak üzere iki ana yapıdan oluşmaktadır. Sistemi tasarlayan yazılımcıların uygulama geliştirmeden kaynaklanan hatalar ile sistemin kullandığı iletişim ağlarından gelebilecek tehditlerin önlenmesi için alınan güvenlik önlemlerini içermektedir (Tan ve Aktaş, 2011:34).

Fiziksel Güvenlik: Donanımsal kaynakların korunması için gerekli olan önlemlerdir.

Çevre Güvenliği: Donanımın veya iletişim ağının genel güvenliğini içine alan sistemi tehdit edebilecek etkilerden korunmak için alınan genel önlemlerdir.

3. Bilgi Güvenliği Farkındalığının Önemi ve Literatür Taraması

İnternet teknolojisinin gelişmesi ve dünyanın küresel bir köy haline dönüşmesi farklı demografik özelliklere sahip bireylerin yaşamlarını kolaylaştırmıştır. Mesafeler ortadan kalkmış işlem süresi olabildiğince kısalmıştır. Bunca değişimin yaşandığı dünyamızda da hırsızlık, saldırı ve savunma teknikleri de değişime uğramıştır.

Bilişim teknolojileri ile birlikte bilgilerimiz sanal ortama taşınmış ve bütün bilgiler sanal ortamda dolaşır hale gelmiştir. Bu noktada bilgi güvenliği ve iletişim teknolojileri bir bütün olarak düşünülmeye başlanmıştır. Bilişim teknolojilerini uygunsuz kullanma, bireylerdeki risk algısının zafiyeti, bilgi güvenliği tehditlerinden habersizlik bir takım olumsuzlukları ve telafisi güç bilgi güvenliği risklerini de bünyesinde barındırmaktadır. Yapılan araştırmalar bilgi güvenliği risklerini gidermede insan faktörünü göz ardı ederek oluşturulacak sistemlerin çok etkili ve yararlı olmadığını göstermektedir (Mart, 2012).

İnsan faktörünün arka plana atılması bilgi güvenliğini riske atacak ve bilgilerin uygun bir şekilde korunmamasının yolunu açacaktır. Bilgilerin düzgün şekilde korunamaması şu riskleri doğurabilecektir (Sayarı, 2009);

- Kuruma ait gizli ve hassas bilgiler ile kurumun işlerliğini sağlayan bilgi ve süreçler başka rakiplerin eline geçebilecektir.
- Kurumun ismi, güvenilirliği ve itibarı toplum gözünde zarar görebilecektir.
- Ülke çıkarının zarar görmesi söz konusu olabilecektir.
- İş sürekliliğinin aksamasına sebebiyet verebilecektir.
- Müşteri mağduriyeti ve memnuniyetsizliğine sebep olabilecektir.
- Yasal yaptırımlara ve tazminatlara maruz kalmalar olabilecektir.

Bilgi güvenliği politikası çalışmalarına kaynak oluşturulması amacıyla Türkiye Milli Eğitim Bakanlığının 2012 yılında 7484 çalışanı üzerinde yapmış olduğu çalışmada kişilere bilgi güvenliği farkındalık anketi uygulanmıştır. Analizler sonucunda katılımcıların Bilgi ve sistem güvenliğini önemli olarak gördükleri belirtilmiştir. Şifre güvenliği açısından anketi yanıtlayan kişilerin %42,22'si şifre güvenliği için gerekli olan kriterlere uygun şifre belirlemedikleri ve %15,71'inin de unutmamak için tüm şifrelerini tek bir şifre olarak belirledikleri tespit edilmiştir. Bilgisayarlarında kullandıkları

şifrelerin paylaşımında %65,37'lık kesim şifrelerini hiç kimse ile paylaşmadıklarını ifade etmişlerdir. Ayrıca araştırmada şu bulgulara rastlanmıştır; Katılımcıların %67,92'si bilgisayarında antivirüs yazılımı bulundurmadığını, %7,91'nin kaynağı bilinmeyen e-posta ekinde gelen dosyaları kesinlikle açmadığını ve derhal sildiğini ifade etmektedir. (MEB, 2013).

Eurobarometer (2011) tarafından Avrupa Birliği üyesi ülkelerde gerçekleştirilen araştırmada katılımcıların %10'luk kesiminin günlük hayatta kimlik bilgilerini,%50'lik kesiminin sosyal bilgilerini, %90'ıda hassas bilgilerini paylaşmadıklarını ifade etmektedir. Aynı araştırmada % 70'lere varan oranda kişilerin verilerini verirken tedirgin oldukları, verilerinin kullanımı noktasında izin alınması gerektiği ve kullanılmasından endişeli oldukları paylaşılmaktadır. (Avrupa Komisyonu, 2011)

Zeydan'ın (2006) yapmış olduğu çalışmada internete bağlı olan bilgisayarların birçok tehdit ile karşı karşıya olduğunu belirtmiştir. Bu tehditlere karşı antivirüs, güvenlik duvarı, anti casus gibi yazılımların bilgisayarlarda yüklü olmasını ve kullanılan her türlü yazılımın güncel sürümlerinin bulundurulması gerektiği vurgulamıştır.

Ketizmen ve Ülküderner (2012) belirli şartlar altında kamu ve özel sektörün kişisel verileri kaydetmesi gerektiğini belirtmektedirler. Kişisel verilerin kaydedilmesi bunların başkaları tarafından elde edilmesi olasılığını da ortaya çıkardığından dolayı kişisel verilerin güvenliğinin sağlanması devletin gerekli çalışmaları yürütmesi ile sağlanacağı ifade edilmiştir.

Şahinaslan vd. (2009) yaptığı çalışmada kurumlarda bilgi güvenliğinde sadece teknik önemlerin alınmasının yeterli olmayacağı en önemli faktörün insan olduğu ve bilgi güvenliğine yönelik oluşabilecek risklerin önlenmesinin farkındalık düzeyinin artırılması ile mümkün olabileceği belirtilmiştir. Bu kapsamda çalışmada bilgi güvenliği farkındalığı oluşturma yöntemleri ele alınmıştır.

Türkiye'de bilgi güvenliği sorunları ve çözüm önerileri üzerine Eminağaoğlu ve Gökşen'in (2009) yapmış oldukları çalışmada bilgi güvenliğinde yapılan en yaygın hatalar ortaya konulmuş ve hatalara karşı alınabilecek önlemler ile çözüm önerileri üzerinde durulmuştur.

4. Yöntem

4.1. Evren ve Örneklem

Araştırma evrenimizi Antalya il merkezinde yaşayan bireyler oluşturmaktadır. Araştırma kapsamında uygulanacak anketin evren için maliyeti yüksek olacağından örnekleme alma yöntemine gidilmiş ve

örneklem rassal olarak belirlenmiştir. Çalışmanın örneklemini 503 kişi oluşturmakta olup 2 kişinin hiçbir cihaz kullanmadığını ifade etmesinden dolayı 501 kişi üzerinden sürdürülmüştür. Örneklem seçilirken, farklı sosyal ağlar ve e-mailler ile ulaşılan bireylerden araştırmaya katılmaya istekli olmaları dikkate alınmıştır. Araştırma bilgisayar teknolojisini kullanan kişilerle kısıtlanmıştır. Örnekleme ilişkin demografik bilgiler bulgular kısmında yer alan Tablo 4 de gösterilmiştir.

4.2. Veri Toplama Aracı

Bu araştırma Antalya'da yaşayan bireylerin kişisel veri güvenliği farkındalık düzeylerinin tespitine yöneliktir. Bu amaç doğrultusunda gerekli literatür çalışmaları ve konu ile ilgili anketler incelenerek "Kişisel Veri Güvenliği Anketi" hazırlanmıştır. Anketin kapsam geçerliği için uzman görüşünden faydalanılmış, alanda çalışan 2 uzman ile 1 ölçme değerlendirme uzmanı tarafından anket incelenmiştir. İncelemeler sonucunda gerekli düzeltmeler yapılarak ankete son hali verilmiştir. Anket 20 çoktan seçmeli ve 22 tane 5'li likert tipinde dereceleme ölçeği ile hazırlanan (1:Kesinlikle Evet, 2:Evet, 3:Bazen, 4:Hayır, 5:Kesinlikle Hayır) toplam 42 sorudan oluşmaktadır. Geliştirilen anket Antalya ilinde yaşayan farklı yaşlara sahip katılımcılara uygulanmıştır. Katılımcılardan elde edilen cevaplar veri setimizi oluşturmaktadır.

4.3. Yapı geçerliği ve güvenirlik analizi

22 maddeden oluşan veri toplama aracına ilişkin faktör yapısının ortaya çıkarılması için açımlayıcı faktör analizi (AFA) gerçekleştirilmiştir. Faktör analizi yapılırken temel bileşenler analizi tekniği kullanılmıştır. KMO (Kaiser Meyer Olkin) değeri .754 bulunmuş ve Bartlett küresellik testi sonucu istatistiki olarak anlamlı çıkmıştır (χ^2 =1985,86 SD=136 $p<0.01$). Field (2000) KMO için alt sınırın 0,50 olduğu ve faktör analizi için KMO'nun 0,50'nin üzerine olması gerektiğini ifade etmektedir. Elde edilen sonuç veri setinin faktör analizi için uygun olduğunu göstermektedir. Analiz sonucunda yedi faktörün özdeğerinin 1'den yüksek olduğu görülmüştür. Faktör sayısını kontrol etmek için yığılma eğrisi (Scree Plot) incelenmiş, 5 noktadan sonra eğrinin düzleşmeye başladığı ve bu bağlamda 5 faktöre döndürme işleminin yapılması gerektiği ortaya çıkmıştır. Ayrıca faktörlere yüklenen maddelerin faktör yükleri incelendiğinde bazı maddelerin belirlenen ölçütten (.40) daha düşük olduğu ve bazı maddelerin de birbirine çok yakın faktör yükleriyle birden fazla faktöre yüklendiğinden dolayı bu özelliklere sahip 5 maddenin ölçme aracından çıkartılmasına karar verilmiştir. Daha sonra faktör analizi geri kalan maddelerle birlikte 5 faktörlü yapı için Varimax döndürme tekniği kullanılarak yeniden gerçekleştirilmiştir. Bu 5 faktörün toplam varyansı açıklama oranı %57,21'dir. Maddelerin faktör

yükleri ve yüklendikleri faktörler Tablo 2'de yer almaktadır. Faktörler isimlendirilirken o faktöre yüklenen maddelerin ortak özellikleri dikkate alınmıştır.

Tablo 2. Kişisel Veri Güvenliği Faktör Analizi Yük Dağılım Sonuçları

Maddeler	Faktörler ve Faktör Yükleri				
	1	2	3	4	5
Umuma açık yerlerdeki bilgisayarlardan internet bankacılığını kullanmam.	,869				
Umuma açık yerlerdeki bilgisayarlardan internet alışverişi yapmam.	,869				
Kendime ait olmayan bilgisayarlardan şifrelerimden her hangi birisini kullanarak işlem yapmam.	,718				
Özel işlerimi kurumdaki bilgisayarımdan yapmam.	,487				
Sosyal Paylaşım sitelerinden gelen gizli içerikli mesajlara cevap vermem.		,740			
İnternette üyelik gerektiren sitelere güvenlik kriterlerine dikkat etmeden üye olmam.		,555			
Sosyal Paylaşım sitelerinden gelen arkadaşlık tekliflerini kabul etmem.		,539			
Gizli bilgi içeren evrakımı ağ üzerinde paylaşmam.		,535			
Kaynağı bilinmeyen e-posta ekinde gelen dosyaları açmam.		,510			
Dijital bilgilerimi yedeklerim.			,652		
Mail, Sosyal Ağ (Facebook, twitter,…) gibi tüm hesaplarımda farklı şifreler kullanırım.			,641		
Kullandığım şifrelerde büyük küçük harf, noktalama işareti veya özel karakter kullanırım.			,630		
USB veya harici diske gizli/önemli verileri şifreleyerek saklarım.			,602		
Bilgisayarımı işlemlerim bittiğinde mutlaka kapatırım.				,854	
Bilgisayarımı sürekli açık bırakmam.				,843	
İnternetten alışverişte kredi kart numaramı verirken çekinirim.					,863
İnternetten alışverişte TC kimlik numaramı verirken çekinirim.					,833

Maddeler arasındaki iç tutarlılığı gösteren Croncbah's Alpha güvenirlik katsayısı için SPSS yardımıyla güvenirlik analizi gerçekleştirilmiştir ve ölçme aracının tümüne ait iç tutarlılık katsayısı .782'dir. Ölçme aracının alt ölçeklerine ait güvenirlik kat sayıları Tablo 3'de verilmiştir.

Tablo 3. Alt ölçeklere ait aritmetik ortalama, standart sapma ve güvenirlik katsayıları

	Faktörler	Aritmetik Ortalama	Standart Sapma	Cronbach's Alpha
Faktör1	Kendine ait olmayan bilgisayarlardan işlem yapma farkındalığı	2,0758	,89240	.769
Faktör2	Kaynağı belirsiz ileti farkındalığı	1,9143	,62156	.612
Faktör3	Kişisel ve yedekleme ve şifreleme farkındalığı	1,9081	,97444	.750
Faktör4	Bilgisayar güvenliği farkındalığı	2,3960	,78819	.571
Faktör5	Kişisel veri paylaşımı risk farkındalığı	1,8465	,97315	.785

Faktör1: "Kendine ait olmayan bilgisayarlardan işlem yapma farkındalığı" faktörü kişilerin kendilerine ait olmayan bilgisayarlardan internete bağlandıklarında şifre ve kişisel bilgilerini kullanmadıklarını ifade eden maddelerden oluşur. Faktör; "Umuma açık yerlerdeki bilgisayarlardan internet bankacılığını kullanmam", "Umuma açık yerlerdeki bilgisayarlardan internet alışverişi yapmam", "Kendime ait olmayan bilgisayarlardan şifrelerimden her hangi birisini kullanarak işlem yapmam", "Özel işlerimi kurumdaki bilgisayarımdan yapmam" maddelerinden meydana gelmektedir. Bu faktörün Cronbach's Alpha iç tutarlılık katsayısı .769'dur.

Faktör2: "Kaynağı belirsiz ileti farkındalığı" faktörü gerek elektronik posta gerekse sosyal ağlardan gelen internet kaynaklı iletilere karşı nasıl davranıldığını ortaya koyan maddelerden oluşmaktadır. Faktör; "Sosyal Paylaşım sitelerinden gelen gizli içerikli mesajlara cevap vermem", "İnternette üyelik gerektiren sitelere güvenlik kriterlerine dikkat etmeden üye olmam", "Sosyal Paylaşım sitelerinden gelen arkadaşlık tekliflerini kabul etmem", "Gizli bilgi içeren evrağımı ağ üzerinde paylaşmam", "Kaynağı bilinmeyen e-posta ekinde gelen dosyaları açmam" maddelerinden meydana gelmektedir. Bu faktörün Cronbach's Alpha iç tutarlılık katsayısı .612'dir.

Faktör3: "Kişisel ve yedekleme ve şifreleme farkındalığı" faktörü kişisel verilerin yedeklenmesi ve korunmasında ön planda olan şifreleme

işlemi ve şifre belirleme farkındalık düzeyini ortaya koyan maddelerden meydana gelmektedir. Faktör; "Dijital bilgilerimi yedeklerim", "Mail, Sosyal Ağ (Facebook, twitter,…) gibi tüm hesaplarımda farklı şifreler kullanırım", "Kullandığım şifrelerde büyük küçük harf, noktalama işareti veya özel karakter kullanırım", "USB veya harici diske gizli/önemli verileri şifreleyerek saklarım" maddelerinden oluşmaktadır. Bu faktörün Cronbach's Alpha iç tutarlılık katsayısı .750'dir.

Faktör4: "Bilgisayar güvenliği farkındalığı" faktörü güvenlik açıklarından birisi olan kişisel bilgisayarın işi olmadığı halde açık bırakılmasının kontrolünün yapılarak bilgisayar güvenlik farkındalığının ölçülmesini sağlamaktadır. Faktör; "Bilgisayarımı işlemlerim bittiğinde mutlaka kapatırım", "Bilgisayarımı sürekli açık bırakmam" maddelerinden oluşmaktadır. Bu faktörün Cronbach's Alpha iç tutarlılık katsayısı .571'dir.

Faktör5: "Kişisel veri paylaşımı risk farkındalığı" faktörü internet ortamında kişisel verilerini paylaşırken hissettiği risk düzeyini tespit etmektedir. Faktör; "İnternetten alışverişte kredi kart numaramı verirken çekinirim", "İnternetten alışverişte TC kimlik numaramı verirken çekinirim" maddelerinden meydana gelmektedir. Bu faktörün Cronbach's Alpha iç tutarlılık katsayısı .785'dir.

4.3. Verilerin Analizi

Geliştirilen anket 526 katılımcıya uygulanmıştır. Katılımcıların 23 tanesinin anketi tek düze doldurmasından iki kişinin de herhangi bir cihaz kullanmıyorum cevabından dolayı analize dahil edilmemiştir. 501 denekten elde edilen veriler sayısallaştırılarak SPSS 17.0 paket programına yüklenerek istatistiki analizler gerçekleştirilmiştir. İstatistiksel analizlerde verilere frekans analizi, bağımsız iki örneklem T Testi, faktör analizi ile tek yönlü varyans analizi uygulanmış gerekli görülen yerlerde veriler tablolaştırılmış ve yorumlanmıştır.

5. Bulgular

5.1.Kişisel Bilgilere İlişkin Bulgular

Tablo 4'de gösterilen katılımcıların demografik bilgilerine göre; araştırmanın %53,3'ünü (267) erkekler, %46,7'sini (234) ise kadınlar oluşturmaktadır. Eğitim düzeylerine bakıldığında %12,2'sini (61) lise mezunu, %12,8'ini (64) Ön Lisans mezunu, %57,7'sini (289) Lisans mezunu ve %17,4'ünün (87) de Lisansüstü mezunu oluşturmaktadır. Araştırmaya katılanların yaş dağılımına bakıldığında 16-20 yaş arası 157 kişi (%29,3), 21-25 yaş arası 112 kişi (%22,4), 26-30 yaş arası 84 kişi (16,2), 31-35 yaş arası 57

kişi (%11,3), 36-40 yaş arası 48 kişi (%9,6), 41-50 yaş arası 43 kişi (%8,6) ve 51 yaş ve üzeri ise 10 kişiden (%2) oluşmaktadır. Araştırmaya katılanların medeni durumlarına bakıldığında %46,7'sinin (234 kişi) Evli, %53,3'nün (267 kişi) bekar olduğu görülmektedir. Aylık gelir dağılımında 1000 TL ve altı olan kişi sayısı 213 (%42,5), 1001 ve 1500 TL arası olan 54 (%10,7), 1501 ve 2000 TL arası olan 32 (%6,3), 2001 ve 3000 TL arası olan 79 (%15,7), 3001 ve üstü olan ise 123 (%24,5) kişidir. Yarıya yakın bir oranının gelir düzeyinin 1000 TL ve altı çıkmasındaki etken çalışmaya katılanların bir kısmının hala eğitim hayatına devam ediyor olmasından kaynaklanmaktadır.

Tablo 4. Katılımcıların Demografik Verileri

Eğitim Durumu	**Kişi Sayısı**	**Frekans (%)**	**Cinsiyet**	**Kişi Sayısı**	**Frekans (%)**
Lise	61	12,2	Erkek	267	53,3
Ön Lisans	64	12,8	Kadın	234	46,7
Lisans	289	57,7			
Lisansüstü	87	17,4			
Yaş Durumu			**Gelir Dağılımı**		
16-20	157	29,3	1000 TL ve altı	213	42,5
21-25	112	22,4	1001-1500 TL	54	10,7
26-30	84	16,2	1501-2000 TL	32	6,3
31-35	57	11,3	2001-3000TL	79	15,7
36-40	48	9,6	3001 TL ve üzeri	123	24,5
41 ve üstü	104	20,2			
Toplam	501	100	**Toplam**	501	100

Araştırmaya katılan kişiler tarafından verilen bilgilerde elektronik cihaza sahip olma durumları sorusuna sadece 2 kişi hiçbir elektronik cihaz kullanmadığını beyan etmiştir. 501 kişinin elektronik cihaz kullanımı ile ilgili dağılımı ise Tablo 5'de gösterilmiştir.

Tablo 5'e göre akıllı cep telefonuna sahip olan katılımcı sayısı 403 kişi, Standart cep telefonuna sahip olan 106 kişi, bilgisayara sahip olan 380 kişi ve tablete sahip olan ise 120 kişidir. Tekil olarak akıllı cep telefonu kullanıcı sayısı 80 kişidir. Akıllı cep telefonu, Standart cep telefonu, bilgisayar ve tablet cihazlarının tümüne birden sahip olan katılımcı sayısı ise 12'dir.

Tablo 5. Elektronik Cihaz Sahip Olma Durumu

Akıllı Cep Telefonu	Standart Cep Telefonu	Bilgisayar	Tablet	Kişi Sayısı
√				80
	√			25
		√		12
			√	2
İki cihaza sahip olanlar				
√		√		203
√			√	12
	√	√		51
	√		√	2
Üç cihaza sahip olanlar				
√	√	√		10
√		√	√	86
	√	√	√	6
Tüm cihazlara sahip olanlar				
√	√	√	√	12
Toplam: 403	106	380	120	

5.2. Kullanıcıların Cihaz Güvenliği Verileri

"Kullanılan cihazlarda antivirüs programı yüklü müdür?" sorusuna verilen cevaplarda toplam 403 tane Akıllı cep telefonu kullanılmasına rağmen sadece 175 (%44) tanesinde antivürüs programı yüklüdür. Katılımcıların 380 tanesi bilgisayara sahip olduklarını ifade etmektedir. Bilgisayarlardaki antivürüs programının bulunma durumu ise 366 (%96,3) gibi yüksek bir orana sahiptir. Tablet cihazlarında ise 120 kişiden 58 (%48,3) tanesi cihazlarında antivürüs programının yüklü olduğunu belirtmişlerdir. Kullandıkları hiçbir cihazda antivürüs programı olmadığını belirten kişi sayısı ise 67'dir.

Standart cep telefonu kullanan ve antivirüs kullanmayan toplam 92 kişi dışında kalan katılımcıların "cihazlarında kurulu olan antivürüs programlarının kategorilerilerine" bakıldığında %42,1'inin (172 kişi) Ücretsiz tam sürüm ile en önde olduğu, ikinci sırada %31,8 ile (130 kişi) Tam sürüm (Lisanslı) kullandığı tespit edilmiştir. Yasal olmayan şekilde kırılarak kullanılan antivürüs programını ise %13,9'u (57 kişi) kullanmakta, geriye kalan %12,2'si (50 kişi) ise deneme sürümünün yüklü olduğunu beyan etmektedir.

Katılımcı "cihazlarının güvenlik duvarlarının açık olup olmadığı" yönündeki soruya katılımcıların %56,7'si Evet cevabı verirken, %18,4'ü Hayır cevabı vermiştir. %25,2'si ise bilmiyorum seçeneğini işaretlemiştir.

5.3. Bilgi güvenliği düzeyi ve genel bakış

Araştırtmaya katılan katılımcıların "Bilgi Güvenliği benim için önemlidir" genel sorusuna %75,9'luk kısmı "kesinlikle evet" derken, %20,4'lük kısmı ise "evet" yanıtı vererek %96,3'lük gibi büyük bir çoğunluk bilgi güvenliğinin önemli olduğunu ifade etmiştir.

Kullanıcıların tehdit kavramları farkındalığına bakıldığında 446 kişi ile Antivirüs kavramı bilinirlikte en ön sırada yer almaktadır. İkinci sırada 367 kişi ile Spam kavramı gelmektedir. Sırasıyla 275 kişi Truva atı, 193 kişi Firewall, 179 kişi Worm, 127 kişi Veri Sızıntısı, 84 kişi Program Ekme, 65 kişi Oltalama ve 58 kişi Backdoor kavramlarını bildiklerini belirtmişlerdir.

"Cihazlarınızı tehdit eden son tehlikelerden haberdar mısınız" sorusuna verilen cevapta 243 kişi (%48,5) haberdar olduğunu ifade ederken 258 kişi (%51,5) ise haberdar olmadığını ifade etmektedir. Kişisel bilgi güvenliği konusunda eğitim almak isteyenlerin oranı ise %74,3'tür. (372 kişi) Eğitim alınmak istenen ortamlara bakıldığında %41,9 (156 kişi) ile yüzyüze eğitim en ön sırada yer almaktadır. %21'i (78 kişi) tüm belirtilen ortamlardan eğitim almak istediğini ifade ederken, %21,2 (79 kişi) ise sadece İnternet sitelerindeki makalelerden eğitim almak istediklerini ifade etmiştir. %15,9 (59 kişi) oranında ise kişiler uzaktan eğitim ile kişisel veri güvenliği bilgisini alabileceklerini belirtmişlerdir.

"Bilgi güvenliği ihlali olduğunda olayı ilk kime haber veririsiniz" sorusuna araştırmaya katılan katılımcıların %28'i nereye bildireceği ile ilgili bir düşüncesinin olmadığını ifade etmektedirler. Sırasıyla %14'ü İnternet Servis Sağlayıcısına, %13,4'ü Aileme ve Arkadaşlarıma, %12,6'sı hiç kimseye, %11,5'i Polise, %10,5'i Yazılımın tedarik edildiği firmaya ve %9,9'u ise bilgi işlem grup başkanlığına bildireceğini bildirmektedir.

5.4. Şifre Belirleme ve E-Posta Verileri

"Katılımcıların elektronik cihazlarını vermiş olduğu şifreyi nasıl belirlediğine" yönelik sorulan soruda en önemli belirleme davranışlarının %50,1'ile İçinde büyük, küçük harf, rakam ve simge gibi farklı karakterlerden oluşan bir dizilimi tercih ettikleri, %17,2'si Unutmamak için tüm şifrelerimi aynı yapıyorum, %15,8'i Unutmamak için akılda kolay kalan bir şifre belirliyorum, %11,7'si Şifrelerimi en az altı karakterden oluşturuyorum.

"Şifrenizi ne sıklıkla değiştiriyorsunuz" sorusuna katılımcıların %40,9 gibi oranı Şifremin birisinin eline geçtiğinden şüphelenirsem değiştiriyorum demişlerdir. %19,5'lil kısmı ise şifrelerini hiç değiştirmediklerini ifade etmektedir. %17,5'i Şifremi birisine vermek zorunda kalırsam değiştiriyorum. Derken %10,3'ü ise Şifremi altı aydan daha

kısa sürede değiştiriyorum demiştir. %3,5 ile Şifremi çok sık değiştiriyorum en az orana sahip olan değişkendir.

Kendilerine ait olan elektronik cihazların şifresini katılımcılar %57 (278 kişi) oranında hiç kimse ile paylaşmadıklarını ifade ederken, %28,7'si (140 kişi) de aile fertlerinden birisiyle paylaştığını ifade etmektedir. %12,9'u (63 kişi) ise arkadaşı ile şifresini paylaşabileceğini belirtmektedir.

Bankanızdan gönderilmiş bir e-posta mesajında sizden bir bağlantıyı (linki) tıklayarak kişisel bilgilerinizi güncellemeniz istendiğine kullanıcıların vermiş oldukları yanıtlarda %39,9 ile "E-posta mesajını görmezden gelirim" ve %31,9 ile "Bankayı arayıp gönderilen e-posta konusunda bilgi alırım" en önde gelmektedir. %15,2 ile "E-posta mesajındaki bankanın logosu adresi ve diğer bilgileri doğru ise istenilen bilgileri veririm" seçeneği yer almaktadır. Aynı soruya ne yapacağını bilmeyen kişi oranı ise %7,6'dır.

Katılımcıların karşılaştıkları tehdit unsurlarından en dikkat çekicileri; %36,7 ile Spam ve %12,5 ile Solucan (Worm) olmuştur. Aynı soruda hiçbir tehdit ile karşılaşmadım diyen kişilerin oranı ise %44,2'dir.

Tablo 6. Cinsiyet değişkenine göre bağımsız iki örneklem t-testi analiz sonuçları

	Cinsiyet	N	Aritmetik Ortalama	Fark	Standart Sapma	t	*p*
Kendine ait olmayan bilgisayarlardan işlem yapma farkındalığı	Erkek	264	2,101	0,0548	,8471	,681	,496
	Kadın	231	2,046		,9425		
Kaynağı belirsiz ileti farkındalığı	Erkek	264	2,003	0,19***	,6453	3,431	,001
	Kadın	231	1,813		,5781		
Kişisel verileri yedekleme ve şifreleme farkındalığı	Erkek	264	2,054	0,314***	1,0418	3,628	,000
	Kadın	231	1,740		,8633		
Bilgisayar güvenliği farkındalığı	Erkek	264	2,314	-0,174**	,7736	-2,474	,014
	Kadın	231	2,489		,7959		
Kişisel veri paylaşımı risk farkındalığı	Erkek	264	1,960	0,243***	1,0222	2,800	,005
	Kadın	231	1,716		,8985		

* : 0.10 yanılma düzeyinde anlamlı
** : 0.05 yanılma düzeyinde anlamlı
*** : 0.01 yanılma düzeyinde anlamlı

Test sonucunda elde edilen sonuçlar Tablo 6 incelendiğinde Kendine ait olmayan bilgisayarlardan işlem yapma farkındalığı faktöründe

cinsiyet yönünden bir farklılığın olmadığı sonucuna ulaşılmıştır [t(493) = ,681, $p > 0.05$].

Kaynağı belirsiz ileti farkındalığı faktöründe cinsiyete göre yapılan analizde kadınların erkeklere göre internet üzerinden gelen kaynağı belirsiz iletilere karşı daha duyarlı oldukları sonucuna varılmıştır [t(493) = 3,431, $p < 0.05$].

Kişisel verileri yedekleme ve şifreleme farkındalığı faktörüne ilişkin cinsiyet karşılaştırması yapıldığında kadınların kişisel verilerini şifrelemede ve şifrelerini belirlerken göstermiş oldukları farkındalığın erkeklerden daha yüksek olduğu tespit edilmiştir [t(493) = 3,628, $p < 0.05$].

Bilgisayar güvenliği farkındalığı faktörü kişisel bilgisayarların gereksiz yere açık bırakılarak güvenlik riski oluşturulmama farkındalığının cinsiyet değişkenine göre yapılan analiz sonucunda erkeklerin kadınlara göre farkındalık düzeylerinin yüksek olduğu tespit edilmiştir [t(493) = -2,474, $p < 0.05$].

Kişisel veri paylaşımı ve risk farkındalığı faktöründe internetten alışveriş esnasında istenen bilgilerin kişide hissettirdiği risk ölçülmüştür. Analiz sonucunda kadınların erkeklere göre daha çok riski hissettikleri tespit edilmiştir [t(493) = 2,800, $p < 0.05$].

Faktör analizi sonucunda elde edilen alt faktörler üzerinde eğitim durumu açısından fark olup olmadığını anlamak için tek yönlü varyans analizi gerçekleştirilmiştir. Sonuçlar istatistiksel olarak anlamsız bulunduğundan faktörlerde fark gözlemlenmemiştir. Aynı şekilde yaş değişkeni açısından karşılaştırma yapıldığında hiçbir alt faktöre ilişkin istatistiki anlamlı fark gözlemlenmemiştir.

SONUÇ

Araştırma kapsamında katılımcılara uygulanan anket sonucunda katılımcıların cihaz kullanımında en ön sırada akıllı cep telefonu ve bilgisayar cihazı yer almaktadır. İki cihaz birden kullanan kişi sayısı ise 203 tür. Standart cep telefonu kullanan kişi sayısı cihazlar arasında en az kullanılan cihazdır. Bu sonuçlar kişilerin değişen teknolojiye hızlı adapte olduğunu gösteren verilerdendir.

Kullanılan cihazın güvenirliliğinin artırılmasında büyük bir etken olan antivirüs programı kullanımı katılımcı bilgisayarlarının hemen hemen tamamında yüklü iken akıllı cep telefonu ve tabletlerinin yarıya yakınında yüklüdür. Yüklü olan antivirüs programlarının kategorilerinde kullanıcıların yarıya yakını ücretsiz tam sürüm kullanırken üçte bir katılımcı ise lisanslı tam

sürüm kullanmaktadır. Kullanılan cihazların güvenlik duvarı açıklığında katılımcıların yarısı güvenlik duvarını aktif olarak kullanırken yarısı kullanmamaktadır. Katılımcıların kişisel bilgisayarlarında bilgi güvenliği sağlama adına gerçekleştirilen adımlardan bir tanesi olan antivirüs kullanımı oranının yüksek olduğu fakat cep telefonu ve tablet gibi cihazlarda bu önlemin yeterli düzeyde alınmadığı görülmektedir.

Katılımcıların bilgi güvenliği düzeylerine bakıldığında büyük bir çoğunluğunun bilgi güvenliğinin önemli olduğunu belirtirken, yarısının bilgi güvenliği ile ilgili son tehlikelerden haberdar olmadığı belirtilmiştir. Herhangi bir bilgi güvenliği tehlikesi olduğunda ise katılımcıların dörtte birinden fazlası nereye haber vereceğini bilmemektedir. Bu doğrultuda katılımcıların büyük çoğunluğu bilgi güvenliği konusunda eğitim almak istediklerini de beyan etmişlerdir.

Veri güvenliğinin sağlanmasında önemli bir etken olan şifre belirleme işleminde katılımcıların yarısının farkındalığının olduğu ve şifre verme kriterlerine uygun şifre ürettiklerini belirtmektedirler. Kaynağı bilinmeyen bir E-posta aldıklarında ise temkinli yaklaştıklarını ifade etmektedirler.

Kişisel veri güvenliğinde kişilerin kendine ait olmayan cihazlardan işlem yapma farkındalığında katılımcılar arasında her hangi bir fark görülmemiş olup genel ortalama olarak katılımcıların farkındalık düzeyinin ortalamanın üstünde olduğu tespit edilmiştir.

Kaynağı belirsiz ileti farkındalığı, kişisel verileri yedekleme ve şifreleme farkındalığı, kişisel veri paylaşımı risk farkındalığı faktörlerinde katılımcılar arasında farkındalık düzeyinin genel ortalamanın üstünde olduğu ve kadınların farkındalık düzeylerinin erkeklere göre daha yüksek çıktığı tespit edilmiştir. Erkeklerin kadınlara göre farkındalık düzeyinin yüksek çıktığı tek faktör bilgisayar güvenliği farkındalığıdır. Analizler sonucunda kişisel veri paylaşımı risk farkındalığı en yüksek farkındalık düzeyi olarak ortaya çıkmıştır.

KAYNAKÇA

BTK (2014), Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı, Türkiye Elektronik Haberleşme Sektörü, Üç Aylık Pazar Verileri Raporu, http://www.tk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/ucaylik14_3.pdf

BUCKLAND, M. (1991). Information and Information Systems. New York: Green Wood Press.

CANBEK, G. VE SAĞIROĞLU, Ş. (2006) *Bilgi ve Bilgisayar Güvenliği Casus Yazılımlar ve Korunma Yöntemleri*, Ankara.

CLARKE, G., (2011) CompTIA Security+ Certification Study Guide (Exam SY0-301). s.l.:McGraw Hill Professional.

DULANEY, E., (2010) CompTIA Security+Study Guide: Exam SY0-201. Fourth Edition dü. s.l.:John Wiley & Sons.

EMİNAĞAOĞLU, M. VE GÖKŞEN, Y. (2009), Bilgi güvenliği nedir, ne değildir, Türkiye' de bilgi güvenliği sorunları ve çözüm önerileri, Dokuz Eylül Üniversitesi sosyal Bilimler Dergisi, Cilt:11, Sayı:4, 1-15

EUROBAROMETER SPECİAL (2011) Avrupa Komisyonu. 359, Temmuz

FİELD, A. (2000) *Discovering Statistics using SPDD for Windows*, London – Thousand Oaks – New Delhi: Sage publications.

JOHNSON, D. G., (2000) Computer Ethics. Prentice Hall. ISBN:0131112414, USA.200 s.

KALKINMA BAKANLIĞI, (2013) Bilgi Toplumu Stratejisinin Yenilenmesi Projesi, Bilgi Güvenliği, Kişisel Bilgilerin Korunması ve Güvenli İnternet Ekseni Mevcut Durum Raporu, Ankara

KARAARSLAN, E. (2013) Siber Güvenlik Deneyleri için Ağ Benzetici ve Ağ Sınama Ortamlarının Kullanımına Dair Ön İnceleme (A Preliminary Study on Using Network Simulation and Network Testbeds for Cyber Security Experiments).Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, 7(7).

KETİZMEN, M. VE ÜLKÜDERNER, Ç. (2012), E-Devlet Uygulamalarında Kişisel Verilerin Korun(ma)ması, XVII. Türkiye'de İnternet Konferansı, 7-9 Kasım 2012, Anadolu Üniversitesi

KOÇ. NET. (2005). Rizikometre 2005 Türkiye Internet Güvenliği Araştırma Sonuçları. İstanbul: KoçNet A.Ş.

MART İ., (2012) Bilişim Kültüründe Bilgi Güvenliği Farkındalığı, Kahramanmaraş Sütçü İmam Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, Kahramanmaraş

MEB, (2013), Bilgi Güvenliği Farkındalık Anketi Değerlendirme Raporu, http://bigb.meb.gov.tr/meb_iys_dosyalar/2013_01/03030227_anketsonucdegerlendirme.pdf

MYERS, P.S. (1996), Knowledge Management and Organizational Design, Boston:Butterworth-Heinenman.

ŞAHİNASLAN E., KANTÜRK A., ŞAHİNASLAN Ö., BORANDAĞ E. (2009) Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi ve

Oluşturma Yöntemleri, XI. Akademik Bilişim Konferansı, Harran Üniversitesi, Şanlıurfa, 597-602.

TAN H., AKTAŞ A.Z. (2011) Bir Kuruluşun Bilgi Sistemi Güvenliği İçin Bir Yaklaşım, 4. Ağ ve Bilgi Güvenliği Sempozyumu Bildiri Kitabı, 34.

TUIK (2014) Türkiye İstatistik Kurumu, Hanehalkı Bilişim Teknolojileri Kullanım Araştırması, http://www.tuik.gov.tr/PreHaberBultenleri.do?id=16198 erişim tarihi: 12.24.2014.

TUTAR, H. (2010) Yönetim Bilgi Sistemleri, Seçkin Yayıncılık, İkinci Baskı, Ankara.

SAYARI, N. (2009), "Bilgi Güvenliği ve Yönetimi", Türkiye Bilişim Derneği Ankara Şubesi Eğitim Etkinliği, Ankara

VACCA, J. (2009) *Computer and Information Security Handbook*, Morgan Kaufmann,

ZAİM, H. (2005). Bilginin Artan Önemi ve Bilgi Yönetimi, İstanbul: İşaret Yayınları.

ZEYDAN, Ö. (2006) Kişisel Bilgisayarlar ve İnternet Güvenliği, XI. "Türkiye'de İnternet" Konferansı 21- 23 Aralık