

Bilişim Güvenliği : Kullanıcı Açısından Bir Durum Tespiti

Atıla BOSTAN

Atılım Üniversitesi
Bilgisayar Mühendisliği Bölümü
abostan@atilim.edu.tr

İbrahim AKMAN

Atılım Üniversitesi
Bilgisayar Mühendisliği Bölümü
akman@atilim.edu.tr

Bilişim teknolojisinde güvenliği sağlama konusunda, kullanıcı farkındalığı ve kazanılmış davranış alışkanlıkları, en zayıf noktalar olarak kabul edilmenin yanında, vazgeçilmez bileşenleri oluşturmaktadır. Bilgisayar ve iletişim güvenliğini yüksek seviyede sağlamak amacıyla mevcut teknolojilerin kullanımı için yoğun bir uğraş verilmektedir, yeterli güvenlik seviyesine erişmede kullanıcılar ve onların gerçek hayat uygulamaları önemli rol oynamaktadır. Bu çalışmada, güvenlik farkındalığı ve uygulamaları konusunda 466 katılımcı üzerinde yaptığımız anket çalışması sonuçlarına dayalı olarak, kullanıcıların bilgisayar ve web güvenliği konusundaki hassasiyet ve farkındalıkları ile yaş, cinsiyet, bilgi ve iletişim teknolojileri kullanım deneyimi ve eğitim seviyesi ilişkisini belirlemeye çalıştık.

Otomatik veri işleme tekniklerinden faydalanarak iş süreçlerinin geliştirilmesi ve modernizasyonu, bilgisayar ağlarını kullanmayı neredeyse alternatifsiz bir teknoloji haline getirmiştir. Günümüzde orta ve büyük ölçekli firmalar hem kendi iş süreçlerinin idaresi ve takibi için hem de müşterilerine verdiği hizmeti ve tanıtımı yaygınlaştırabilmek için bilgisayar ağlarından faydalanmaktadır. Her ne kadar sadece firma/kurum içi bilgisayar ağı kullanımı mümkün olsa da firma dışı sistemler ile entegrasyon, İnternet gibi çok yaygın bir ağı sağladığı ortam ve hizmetlere ulaşma ihtiyacı (firma/kurum fonksiyonlarını etkin olarak yerine getirebilmek için), İnternet ağına çevrim-içi erişmeyi gerektirmektedir. İnternet gibi genele açık ve kontrolü zor bir ortama bağlantı kurmak şüphesiz beraberinde bir çok güvenlik ihtiyacını da gündeme getirmektedir. İş süreçlerinde gizliliği ve kişiselliği sağlamak için bilginin emniyetli ve güvenli metotlarla işlenmesi gereklidir. Bu özellikler genellikle ağ ve bilgi güvenliği olarak adlandırılmaktadır. Sayısal ortamlarda güven ifadesi aktörlerin kimliğinin onaylanmasını içerirken, gizlilik ifadesi ise yetkisiz erişimin/dinlemenin, içerik değiştirmenin ve hizmet kesintisinin engellenmesi konularını kapsamaktadır.

Bilgi sistemleri güvenliğinin başarısı büyük oranda son kullanıcı davranışları ve farkındalığına bağlıdır [1]. Güvenlik mekanizmaları insanlar tarafından tasarlandığı, uygulandığı, işletildiği ve aynı zamanda yine insanlar tarafından ihlal edildiği için, bu sistemlerin tasarımında insani faktörleri göz önüne alınmalıdır [2]. Bilgisayar ve iletişim güvenliği-

ni en yüksek seviyede sağlamak için mevcut teknolojilerin kullanımı konusunda yoğun bir uğraş verilmektedir, son yapılan araştırmalar güvenlik ihlallerinin yıllar bazında artış gösterdiğini ortaya koymaktadır. Computer Security Institute'un 2008 [3] ve 2009 [4] raporları, kötü amaçlı yazılım bulaşması, e-posta yemlemesi ve web aldatma yöntemlerini en çok izlenen ihlaller olarak belirtmektedir. Güvenlik ihlallerinin çoğunda temel unsur olarak, kullanıcı davranışlarındaki farkındalık eksikliği belirtilmektedir. Buna rağmen gerçek güvenlik uygulamalarında, kullanıcı farkındalığı eğitimlerinin en az önem verilen konu olduğu tespit edilmiştir [1]. Hatta, kullanıcılar güvenli kullanımı temin edecek tedbirlerin teknik olarak farkında olsalar bile, yanlış/hatalı davranışta bulunabilmektedirler. Güvenli kullanımı temin etmede teknik farkındalığın yeterli olmadığını ve kullanıcıların her zaman bilgileri/inançları doğrultusunda davranmadıklarına işaret eden araştırmalar mevcuttur [5,6]. Uygulamalarda güvenli kullanım yöntemlerinin, kullanıcılar tarafından, kazanılması, içselleştirilmesi ve alışkanlık haline getirilmesine ihtiyaç vardır [6]. Bilgi güvenliği mekanizmalarını geliştirirken, kullanıcı davranışları ve güdülerine odaklanılmasının gerekli olduğu konusunda araştırmacılar çoğunlukla hemfikirdir [7,8,9]. Diğer taraftan, güvenlik mekanizmalarının etkinliğini değerlendirebilmek için, deneysel laboratuvar ortamlarından ziyade, gerçek hayat uygulamaları incelenmelidir [8].

Sunulan bu çalışmada, kullanıcıların sayısal ortam güvenliği konusunda farkındalık seviyelerinin yanında, gerçek hayat güvenlik uygulamalarını incelemeyi esas aldık. 466 katılımcı ile 12 sorudan oluşan bir bilgi güvenliği farkındalığı anketi gerçekleştirdik. Anketi, iş süreçleri ve bilgi paylaşımında en çok kullanılan araçlar olmaları sebebi ile, kişisel bilgisayar güvenliği ve bu konudaki davranış şekilleri/kalıpları, ve güvenli web konuları ile sınırlı tuttuk. Bunun paralelinde, katılımcıların demografik bilgilerini aldığımız dört sorunun haricinde anketteki sorular bilgi ve iletişim teknolojileri kullanımı, kişisel bilgisayar kullanımında gerçek hayat uygulamaları, güvenli web kullanımında farkındalık ve davranış alışkanlıkları olmak üzere iki ana başlık altında gruplandırıldı.

Metodoloji

Ulusal ve uluslararası literatüre incelendiğinde bilişim üzerine yapılan çalışmalarda yaş, cinsiyet, eğitim ve dene-

yimin önemli demografik faktörler arasında yer aldığı görülmektedir. Örneğin, eserlerinde Rahim, Rahaman, Seyal [10], Lau, [11] yaş, cinsiyet, eğitim ve deneyimin bilişim etiği konusunda bireylerin davranışları konusunda anlamlı etkisi olduğunu göstermişlerdir. Benzer şekilde Levy [12] ve, Lian ve Lin [13] yapmış oldukları çalışmada cinsiyet, eğitim, yaş gibi demografik faktörlerin bilişim teknolojilerinin sağladığı fırsatlardan yararlanma üzerinde önemli etkileri bulunduğunu saptamışlardır. Diğer iki çalışmada ise Colley ve Maltby [14] ve Yang ve Tung [15] İnternet çalışmalarında sosyo-demografik faktörlerin göz önüne alınması gerektiği ve bu türden çalışmaların halen araştırılmaya muhtaç olduğu belirtilmiştir. Nitekim, Zhang [16] ve Jaeger [17] yapmış oldukları çalışmalarda kişilerin bazı demografik özelliklerinin bilişim alanında çeşitli faktörler ve algılamalar üzerinde anlamlı etkileri olduğu sonucuna varmışlardır.

Yukarıda verilen nedenlerle, bu bildiride, seçilmiş sosyo-demografik faktörler ile seçilmiş bilgisayar ve web kullanım güvenliği farkındalığı arasındaki ilişki incelenmektedir. Çalışmada kullanılacak olan sosyo-demografik faktörler bağımsız değişkenler olarak ele alınmak üzere

1. yaş (değişken adı: yaş),
2. Cinsiyet (değişken adı: cins),
3. Eğitim (değişken adı: eğit),
4. Deneyim (değişken adı: dene)

kalemlerinden oluşmaktadır. Bağımlı değişkenler ise bilgisayar ve web güvenliği farkındalığı altında iki temel kategoride ele alınmıştır. Bu kategoriler altında yer alan değişkenler ile bunlara karşılık gelen hipotezler aşağıda verilmektedir.

Bilgisayar Güvenliği: Bu kategoride yer alan değişkenler:

1. Kişinin bilgisayar güvenliği konusunda bilgi düzeyi (Y1),
2. Kişinin kullanılan bilgisayar üzerinde önemli bilgi saklayıp saklamadığı (Y2),
3. Kişinin bilgisayarında bulunan bilgileri yedekleme sıklığı (Y3),
4. Kişinin bilgisayarında güvenlik taraması sıklığı (Y4),
5. Kişinin bilgisayarında lisanslı bir virüs koruma sistemi kullanıp kullanmadığı (Y5)

Bu çerçevede kurulan hipotezler aşağıda verilmektedir (Tablo 1-Tablo 4).

Tablo 1: Yaş ve Bilgisayar güvenliği hipotezleri

Hipotez	Tanım
H1 _{yaş,Y1}	Yaş ile kişinin bilgisayar güvenliği bilgi düzeyi arasında anlamlı bir ilişki vardır.
H1 _{yaş,Y2}	Yaş ile kişinin kullanılan bilgisayar üzerinde önemli bilgi saklayıp saklamadığı arasında anlamlı bir ilişki vardır.
H1 _{yaş,Y3}	Yaş ile kişinin bilgisayarında bulunan bilgileri yedekleme sıklığı arasında anlamlı bir ilişki vardır.
H1 _{yaş,Y4}	Yaş ile kişinin bilgisayarında güvenlik taraması sıklığı arasında anlamlı bir ilişki vardır.
H1 _{yaş,Y5}	Yaş ile kişinin bilgisayarında lisanslı bir virüs koruma sistemi kullanıp kullanmadığı arasında anlamlı bir ilişki vardır.

Tablo 2: Cinsiyet ve Bilgisayar güvenliği hipotezleri

Hipotez	Tanım
H1 _{cins,Y1}	Cinsiyet ile kişinin bilgisayar güvenliği bilgi düzeyi arasında anlamlı bir ilişki vardır.
H1 _{cins,Y2}	Cinsiyet ile kişinin kullanılan bilgisayar üzerinde önemli bilgi saklayıp saklamadığı arasında anlamlı bir ilişki vardır.
H1 _{cins,Y3}	Cinsiyet ile kişinin bilgisayarında bulunan bilgileri yedekleme sıklığı arasında anlamlı bir ilişki vardır.
H1 _{cins,Y4}	Cinsiyet ile kişinin bilgisayarında güvenlik taraması sıklığı arasında anlamlı bir ilişki vardır.
H1 _{cins,Y5}	Cinsiyet ile kişinin bilgisayarında lisanslı bir virüs koruma sistemi kullanıp kullanmadığı arasında anlamlı bir ilişki vardır.

Tablo 3: Eğitim ve Bilgisayar güvenliği hipotezleri

Hipotez	Tanım
H1 _{eğit,Y1}	Eğitim ile kişinin bilgisayar güvenliği bilgi düzeyi arasında anlamlı bir ilişki vardır.
H1 _{eğit,Y2}	Eğitim ile kişinin kullanılan bilgisayar üzerinde önemli bilgi saklayıp saklamadığı arasında anlamlı bir ilişki vardır.

H1 _{eğit,Y3}	Eğitim ile kişinin bilgisayarında bulunan bilgileri yedekleme sıklığı arasında anlamlı bir ilişki vardır.
H1 _{eğit,Y4}	Eğitim ile kişinin bilgisayarında güvenlik taraması sıklığı arasında anlamlı bir ilişki vardır.
H1 _{eğit,Y5}	Eğitim ile kişinin bilgisayarında lisanslı bir virus koruma sistemi kullanıp kullanmadığı arasında anlamlı bir ilişki vardır.

Tablo 4: Deneyim ve Bilgisayar güvenliği hipotezleri

Hipotez	Tanım
H1 _{dene,Y1}	Deneyim ile kişinin bilgisayar güvenliği bilgi düzeyi arasında anlamlı bir ilişki vardır.
H1 _{dene,Y2}	Deneyim ile kişinin kullanılan bilgisayar üzerinde önemli bilgi saklayıp saklamadığı arasında anlamlı bir ilişki vardır.
H1 _{dene,Y3}	Deneyim ile kişinin bilgisayarında bulunan bilgileri yedekleme sıklığı arasında anlamlı bir ilişki vardır.
H1 _{dene,Y4}	Deneyim ile kişinin bilgisayarında güvenlik taraması sıklığı arasında anlamlı bir ilişki vardır.
H1 _{dene,Y5}	Deneyim ile kişinin bilgisayarında lisanslı bir virüs koruma sistemi kullanıp kullanmadığı arasında anlamlı bir ilişki vardır.

Web web güvenliği : Bu kategoride yer alan değişkenler:

6. Kişinin web sayfaları güvenliği konusunda bilgi düzeyi (Y6),
7. Kişinin güvenli web sitelerinin nasıl ayırt edileceği konusundaki bilgisi (Y7),
8. Kişinin web siteleri sertifika hatası kavramı hakkında bilgisinin olması (Y8),

Belirtilen değişkenlere karşılık gelen hipotezler yandaki tablolarda verilmektedir (Tablo 5-Tablo 8).

Tablo 5: Yaş ve web güvenliği hipotezleri

Hipotez	Tanım
H2 _{yaş,Y6}	Yaş ile kişinin web sayfaları güvenliği bilgi düzeyi arasında anlamlı bir ilişki vardır.

H2 _{yaş,Y7}	Yaş ile kişinin güvenli web sitelerinin nasıl ayırt edileceği konusundaki bilgisi arasında anlamlı bir ilişki vardır.
H2 _{yaş,Y8}	Yaş ile kişinin web siteleri sertifika hatası kavramı hakkında bilgisi arasında anlamlı bir ilişki vardır.

Tablo 6: Cinsiyet ve web güvenliği hipotezleri

Hipotez	Tanım
H2 _{cins,Y6}	Cinsiyet ile kişinin web sayfaları güvenliği bilgi düzeyi arasında anlamlı bir ilişki vardır.
H2 _{cins,Y7}	Cinsiyet ile kişinin güvenli web sitelerinin nasıl ayırt edileceği konusundaki bilgisi arasında anlamlı bir ilişki vardır.
H2 _{cins,Y8}	Cinsiyet ile kişinin web siteleri sertifika hatası kavramı hakkında bilgisi arasında anlamlı bir ilişki vardır.

Tablo 7: Eğitim ve web güvenliği hipotezleri

Hipotez	Tanım
H2 _{eğit,Y6}	Eğitim ile kişinin web sayfaları güvenliği bilgi düzeyi arasında anlamlı bir ilişki vardır.
H2 _{eğit,Y7}	Eğitim ile kişinin güvenli web sitelerinin nasıl ayırt edileceği konusundaki bilgisi arasında anlamlı bir ilişki vardır.
H2 _{eğit,Y8}	Eğitim ile kişinin web siteleri sertifika hatası kavramı hakkında bilgisi arasında anlamlı bir ilişki vardır.

Tablo 8: Deneyim ve web güvenliği hipotezleri

Hipotez	Tanım
H2 _{dene,Y6}	Deneyim ile kişinin web sayfaları güvenliği bilgi düzeyi arasında anlamlı bir ilişki vardır.
H2 _{dene,Y7}	Deneyim ile kişinin güvenli web sitelerinin nasıl ayırt edileceği konusundaki bilgisi arasında anlamlı bir ilişki vardır.
H2 _{dene,Y8}	Deneyim ile kişinin web siteleri sertifika hatası kavramı hakkında bilgisi arasında anlamlı bir ilişki vardır.

Araştırma Yöntemi

Önerilen hipotezlerin test edilmesi amacıyla bir taslak anket formu hazırlanmıştır. Bu anket formu uygulanmadan önce bir pilot çalışma gerçekleştirilmiş ve ayrıca konunun uzmanı olan kişilerle görüşülmüştür. Tüm bu çalışmalar sonucunda elde edilen görüş ve öneriler anket formuna olabildiğince yansıtılmaya çalışılarak bu form son haline getirilmiştir. Anket formu Tablo 9'da özetlenmektedir. Bu tablodan da görüleceği gibi, anket formu 12 soru içermektedir. Bu soruların tanımları ve karşılık gelen cevap değerleri ile değişken sembolleri yine Tablo 9'da verilmektedir.

Anket Elektrik Mühendisleri Odası (EMO) tarafından değişik ortamlarda vatandaşlarla yüzyüze görüşmelerle uygulanmış olup sonuçta 466 adet cevaplanmış anket elde edilmiştir. Önceki bölümlerde verilen hipotezlerin (Tablo 1-Tablo 8) analizi için çoklu doğrusal regresyon modeli kullanılmıştır. Bu model aşağıda özetlenmektedir.

$Y_i = a_0 + a_1 \text{ yaş} + a_2 \text{ cins} + a_3 \text{ eğit} + a_4 \text{ dene}$ $i=1,2,...,8$

Gerektiğinde değişkenler arasındaki ikili ilişkileri incelemek amacıyla %5 yeterlilik düzeyinde Ki-kare (χ^2) test yöntemi de kullanılmıştır.

Tablo 9: Anket formu özeti

Soru	Değişken	Tanım	Cevap alternatifleri
1	Yaş	Yaşınız?	<21, 21-30, 31-40, 41-50, 51-60, >60
2	Cinsiyet	Cinsiyetiniz?	erkek/kadın
3	Eğit	Eğitim durumunuz?	doktora/yüksek lisans, lisans, ön lisans, öğrenci (üniversite), Lise ve altı
4	Dene	Bilişim deneyiminiz (yıl)?	yok, 1-5, 6-10, 11-15, 16-20, >21
5	Y_1	Bilgisayar güvenliği bilgi düzeyiniz nedir?	çok fazla, fazla, orta, az, hiç yok (10. soruya geçiniz)

6	Y_2	Kullandığınız bilgisayarda sizin için önemli bilgi bulunduruyor musunuz?	evet/hayır
7	Y_3	Bilgisayarınızda bulunan bilgileri yedekleme sıklığınız nedir?	çok sık (ayda 2 veya daha çok), sık (ayda 1), orta (2-6 ayda 1), az (yılda 1), yedekleme yapmıyorum
8	Y_4	Bilgisayarınızda güvenlik taraması yedekleme sıklığınız nedir?	çok sık (ayda 5 veya daha çok), sık (ayda 3-4), orta (ayda 2), az (ayda 1), güvenlik taraması yapmıyorum
9	Y_5	Bilgisayarınızda lisanslı bir virüs koruma sistemi kullanıyor musunuz?	evet/hayır
10	Y_6	Web sayfaları güvenliği bilgi düzeyiniz nedir?	çok fazla, fazla, orta, az, hiç yok (12. soruya geçiniz)
11	Y_7	Güvenli web sitelerini nasıl ayırt edersiniz?	Ayırt edemem, erişirken aldığım uyarı ile, site içerisinde güvenlik logosunun varlığıyla, web tarayıcısının göstereceği küçük kilit sembol ile
12	Y_8	Web siteleri sertifika hatası kavramı hakkında bilginiz var mı?	evet/hayır

Tanımlayıcı Bulgular

Anket katılımcılarının demografik özellikleri Tablo-10'da sunulmuştur.

Tablo 10: Katılımcı Demografik Özellikleri

Değişken	Miktar	Oran (%)
Yaş		
<21	95	20
21-30	211	45
31-40	94	20
41-50	49	11
51-60	12	3
>61	5	1
Cinsiyet		
Erkek	255	55
Kadın	205	44
Belirtmemiş	6	1
Eğitim Durumu		
Lise	125	27
Öğrenci(Üniversite)	113	24
Ön Lisans	22	5
Lisans	151	32
Doktora/Y.Lis.(Master)	21	5
Diğer	34	7
Bilgi ve İletişim Teknolojileri Kullanım Deneyimi		
Deneyimim yok	52	11
1-5 Yıl	154	33
6-10 Yıl	170	36
11-15 Yıl	78	17
16-20 Yıl	7	2
>= 21 Yıl	5	1

Anket katılımcılarının yaş gruplarına dağılımı incelendiğinde katılımcıların çoğunluğunun 40 yaşından daha genç olduğu görülmektedir. En büyük katılım oranı %45 ile 21-30 yaş grubunda izlenirken, 40 yaş ve daha geç grupların toplamı %85'tir. Katılımcıların cinsiyetlere göre dağılımları incelendiğinde erkeklerin kadınlara nazaran %11 oranında daha fazla temsil edildiği göze çarpmaktadır. Erkek (%50.98) ve kadın (%38.54) katılımcıların büyük çoğunluğu 21-30 yaş grubundan oluşmaktadır. Her iki grupta 40 yaş üzeri katılımcı oranı ise erkekler için %13.33, kadınlar için %14.17 olup benzer dağılım göstermektedir. Ancak, yaş ve cinsiyet dağılımları arasındaki %5 yeterlilik düzeyinde ilişki anlamlı bulunmamıştır ($x^2=10.500$; $sd=5$; $p\text{-değeri}=0.062$).

Lisans seviyesinde eğitim sahibi olanların oranı %32 ile en büyük katılımcı kategorisini oluştururken, bunu %27 ve %24 ile sırasıyla lise ve üniversite öğrencisi kategorileri takip etmektedir. Bu dağılım, katılımcı yaş dağılımı ile paralellik gösterdiği izlenmekte ve aralarındaki ilişkinin tutarlı olduğu gözlenmektedir ($x^2=79.710$; $sd=4$; $p\text{-değeri}=0.000$). Buna karşılık, eğitim ve cinsiyet

değişkenleri arasında ise anlamlı bir ilişki bulunamamıştır ($x^2=2.605$; $sd=1$; $p\text{-değeri}=0.107$).

Katılımcıların Bilgi ve İletişim Teknolojileri Kullanım Deneyimleri konusundaki yanıtları incelendiğinde, 6-10 yıllık deneyim kategorisinin %36 ile en büyük kesimi oluşturduğu, bu kategoriyi %33'lük bir oranla 1-5 yıllık deneyim grubunun izlediği görülmektedir. Anket katılımcıları arasında Bilgi ve iletişim teknolojileri kullanım deneyimi 1-10 yıl arasında olan miktar %69 ile büyük bir kesimi oluşturmaktadır. Bu bulgunun katılımcı yaşları ile beraber yorumlanması neticesinde, genç kuşağın bu teknolojileri daha çok kullandığı yönündeki yaygın kanaatin bu çalışma bulguları ile de desteklendiği görülmektedir. Bu paralelde yaş ve bilişim deneyimi arasında istatistiksel olarak anlamlı bir ilişki bulunmuştur ($x^2=29.60$; $sd=4$; $p\text{-değeri}=0.000$). Diğer taraftan erkek ve kadın katılımcıların büyük çoğunluğunun (erkek=%43; kadın=%41) en az önlisans mezunu olduğu görülmektedir. Eğitim ve bilişim deneyimi için yapılan test sonuçları bu değişkenler arasında beklendiği gibi anlamlı bir ilişki bulunduğunu göstermektedir ($x^2=127.210$; $sd=20$; $p\text{-değeri}=0.000$). Tüm bunlara ek olarak erkek ve kadın katılımcıların büyük çoğunluğunun bilişim deneyimlerinin 1-10 yıl arasında olduğu (erkek=%69; kadın=%71) görülmektedir. Ancak, cinsiyet ve bilişim deneyimi incelendiğinde test sonuçları bu değişkenler aralarındaki ilişkinin anlamlı olmadığını göstermektedir ($x^2=3.304$; $sd=4$; $p\text{-değeri}=0.508$).

Analiz Sonuçları

Yukarıda verilen 32 hipotez (Tablo 1 - Tablo 8) %5 yeterlilik derecesinde incelenmiş ve aşağıda verilen sonuçlara ulaşılmıştır.

Bilgisayar Güvenliği: Yapılan regresyon analiz sonuçları Tablo 11'de verilmektedir.

Tablo 11: Bilgisayar güvenliği farkındalığı regresyon analiz sonuçları

Bağımsız değişken	Bağımlı değişken	Hipotez	Alpha değeri	p-değeri*
Yaş	Y1	H1 _{yaş, Y1}	- 0.379	0.000*
Cins	Y1	H1 _{cins, Y1}	- 0.329	0.000*
Eğit	Y1	H1 _{eğit, Y1}	0.115	0.000*
Deney	Y1	H1 _{dene, Y1}	0.499	0.000*
Yaş	Y2	H1 _{yaş, Y2}	- 0.208	0.000*
Cins	Y2	H1 _{cins, Y2}	- 0.105	0.080

Eğit	Y2	H1 _{eğit, Y2}	0.049	0.039*
Deney	Y2	H1 _{dene,Y2}	0.138	0.000*
Yaş	Y3	H1 _{yaş, Y3}	- 0.306	0.000*
Cins	Y3	H1 _{cins,Y3}	- 0.244	0.022*
Eğit	Y3	H1 _{eğit, Y3}	0.176	0.000*
Deney	Y3	H1 _{dene,Y3}	0.382	0.000*
Yaş	Y4	H1 _{yaş, Y4}	- 0.440	0.000*
Cins	Y4	H1 _{cins,Y4}	- 0.207	0.041*
Eğit	Y4	H1 _{eğit, Y4}	0.144	0.000*
Deney	Y4	H1 _{dene,Y4}	0.391	0.000*
Yaş	Y5	H1 _{yaş, Y5}	- 0.254	0.000*
Cins	Y5	H1 _{cins,Y5}	- 0.103	0.060
Eğit	Y5	H1 _{eğit, Y5}	0.066	0.002*
Deney	Y5	H1 _{dene,Y5}	0.144	0.000*

*İstatistiksel olarak 5% düzeyinde yeterlilik belirtir.

Bu tabloda verilen alpha değerleri ile %5 istatistiksel derecesinde yeterlilik testi için kullanılan p-değerleri incelendiğinde aşağıda verilen hususlar göze çarpmaktadır.

- Cinsiyet ile kişinin çalıştığı bilgisayarda kendisi için önemli bilgiler bulundurma (H1cins,Y2) hususu hariç (p-değeri= 0.080) diğer tüm bağımsız değişkenlerin bilgisayar güvenliği farkındalığı kategorisi altında verilen faktörlerle %5 yeterlilik düzeyinde istatistiksel olarak anlamlı ilişkisi olduğu görülmektedir.
- Yaş ve cinsiyet ile bağımlı değişkenler arasındaki ilişki negatif bulunmuştur. Buna karşılık eğitim düzeyi ve deneyim ile yine bilgisayar güvenliği kategorisi altında verilen faktörler arasındaki ilişki pozitif bulunmuştur. Diğer bir deyişle kadınların ve daha ileri yaşta kişilerin bilgisayar güvenliği hakkındaki hassasiyetleri azalmaktadır. Buna karşılık kişilerin eğitim ve deneyim düzeylerinin artışı ile bu hassasiyetler ve farkındalık daha üst düzeye çıkmaktadır.

Web Güvenliği: Bu grup için regresyon analiz sonuçları Tablo 12’de verilmektedir. Buna göre

Tablo 12: Web güvenliği farkındalığı regresyon analiz sonuçları

Bağımsız değişken	Bağımlı değişken	Hipotez	Alpha değeri	p-değeri*
Yaş	Y6	H2 _{yaş, Y6}	- 0.374	0.000*
Cins	Y6	H2 _{cins,Y6}	- 0.217	0.019*
Eğit	Y6	H2 _{eğit, Y6}	0.153	0.000*
Deney	Y6	H2 _{dene,Y6}	0.437	0.000*
Yaş	Y7	H2 _{yaş, Y7}	- 0.629	0.356
Cins	Y7	H2 _{cins,Y7}	- 2.230	0.106
Eğit	Y7	H2 _{eğit, Y7}	0.792	0.145
Deney	Y7	H2 _{dene,Y7}	1.420	0.032*
Yaş	Y8	H2 _{yaş, Y8}	- 0.223	0.000*
Cins	Y8	H2 _{cins,Y8}	0.002	0.979
Eğit	Y8	H2 _{eğit, Y8}	0.099	0.000*
Deney	Y8	H2 _{dene,Y8}	0.187	0.000*

*İstatistiksel olarak 5% düzeyinde yeterlilik belirtir.

Tablo 12’de verilen alpha değerleri ile %5 istatistiksel derecesinde yeterlilik testi için kullanılan p-değerleri incelendiğinde aşağıda verilen hususlar göze çarpmaktadır.

Kişilerin yaş, cinsiyet, eğitim ile güvenli web sitelerini ayırt edebilmesi (H2yaş,Y7, H2cins,Y7, H2eğit,Y7) hususu (karşılıklı olarak p-değeriyaş,Y7 = 0.356; p-değericins,Y7 = 0.106; p-değerieğit,Y7 = 0.145) arasındaki ilişki anlamlı bulunmamıştır. Benzer şekilde cinsiyet ile web siteleri sertifika hatası kavramı hakkında bilgisinin olup olmaması hususu (H2cins,Y8) arasındaki ilişki de istatistiksel olarak %5 yeterlilik düzeyinde anlamlı değildir (p-değericins,Y8 = 0.979). Bunun dışında kalan diğer tüm bağımsız değişkenlerin web güvenliği kategorisi altında verilen faktörlerle %5 yeterlilik düzeyinde istatistiksel olarak anlamlı ilişkisi olduğu görülmektedir.

- Eğitim ve deneyim ile web güvenliği kategorisinde yer alan tüm bağımlı değişkenler arasındaki ilişki pozitif bulunmuştur. Diğer bir deyişle bilgisayar güvenliği kategorisine benzer şekilde kişilerin eğitim ve deneyim düzeylerinin artışı ile web konusundaki hassasiyetler ve farkındalık daha üst düzeye çıkmaktadır. Benzer şekilde kişinin cinsiyet ve web siteleri sertifika hatası kavramı hakkında bilgisinin olup olmaması arasındaki ilişki de anlamlı olmamakla birlikte pozitif bulunmuştur. Bu ise kadınların erkeklerle oranla web siteleri sertifika hatası hakkında daha hassas olduklarına işaret etmektedir. Buna karşılık yaş, cinsiyet ile web sayfaları güvenliği hakkında bilgi

düzeyi, güvenli web sitelerini ayırt edebilme özelliği arasındaki ilişki negatif bulunmuştur. Bu ise erkeklerin ve daha genç yaştakilerin bu konularda daha yetkin olduklarını göstermektedir. Benzer şekilde yaş ve web siteleri sertifika hatası bilgi düzeyi arasında negatif bir ilişki saptanmıştır. Bu ise erken yaştakilerin web sayfası sertifika hatası bilgi düzeyinin daha fazla olduğunu göstermektedir.

Sonuçlar

Bilişim teknolojilerinin bulunduğumuz çağın yükselen değeri olduğu ve teknolojiye hızlı gelişmeler sonucunda, bilişim teknolojilerinin yaşantının tüm alanlarını etkilediği bilinmektedir. Ancak bilişim teknolojilerinde yaşanan bu gelişmelerin başta güvenlik olmak üzere çeşitli sorunları da beraberinde getirdiği açıktır. Güvenlik sorunları arasında ise ağ ve bilgi güvenliği ilk sırayı almakta olup bilişim teknolojileri kullanıcısının bu konu ile ilişkisi önem kazanmaktadır.

Bu çalışmada bilişim teknolojileri kullanıcılarının demografik özellikleri ile bilgisayar ve web güvenliği konuları arasındaki ilişkiler incelenmiştir. Bu amaçla EMO'nun önemli desteği ve 466 katılımcıyla bir anket çalışması gerçekleştirilmiştir. Elde edilen verilerin analizleri sonucunda;

- Yaşın artması ile bilgisayar güvenliği konusundaki hassasiyetin azaldığı,
- Kadınların erkeklere oranla bilgisayar güvenliği konusunda daha hassas olduğu,
- Eğitim seviyesi yükseldikçe bilgisayar güvenliğinde daha hassas davranıldığı,
- Bilgi ve iletişim sistemleri kullanım deneyiminin artması ile bilgisayar güvenliği konusunda hassasiyet ve farkındalığın da arttığı,
- Yaşın artması ile web güvenlik uygulamaları farkındalığının da arttığı,
- Erkeklerin güvenli web kullanımı konusunda kadınlardan daha yetkin olduğu,
- Eğitim seviyesi yükseldikçe web güvenliği konusunda hassasiyet ve farkındalığın da arttığı
- Bilgi ve iletişim sistemleri kullanım deneyiminin artışı ile güvenli web kullanımında hassasiyetin arttığı

tespit edilmiştir.

Yapılan tespitlerde en öne çıkan husus yaş ilerledikçe bilgisayar güvenliği konusunda hassasiyet azalmasına karşılık web güvenliği konusunda farkındalık ve duyarlılığın artmasıdır. Benzer şekilde kadınlar bilgisayar güvenliğine

erkeklerden daha çok dikkat ederken erkekler de web güvenliğinde kadınlardan daha dikkatli davranmaktadır. Bilgi ve iletişim teknolojileri kullanım deneyimi ve eğitim seviyesi ise hem bilgisayar güvenliği hem de web güvenliği bağımlı değişkenleri ile yondeş ilişkilidir.

Ulaşılan sonuçlar paralelinde, bilgisayar güvenliği ve web güvenliğinde hassasiyet ve farkındalık seviyesini yükseltmek, kullanıcılardan kaynaklanan güvenlik açıklarını en aza indirebilmek amacı ile, kullanıcıların bilgi ve iletişim teknolojisi kullanım deneyimlerinin çeşitlendirilerek artırılmasının ve kullanıcı eğitim seviyesinin yükseltilmesinin olumlu etki yaratacağı sonucuna ulaşılmıştır.

Teşekkür

Elektrik Mühendisleri Odası'na bu çalışmanın veri toplanması ve bu verinin sayısallaştırılması aşamalarında göstermiş oldukları desteklerden ötürü teşekkür ederiz.

Referanslar

- (1) D'Arcy J. and Hovav A. Detering Internal Information Misuse, Communications of the ACM, October 2007, Vol. 50 No.10
- (2) Adams A. and Sase M. A. Users Are Not The Enemy, Communications of the ACM, December 1999, Vol. 42 No.12
- (3) Computer Crime & Security Survey, Computer Security Institute, İnternet adresi <http://www.cse.msstate.edu/~cse6243/readings/CSISurvey2008.pdf>, (son erişim tarihi 11 Haziran 2011).
- (4) 14th Annual CSI Computer Crime & Security Survey, Comprehensive Addition, Computer Security Institute, İnternet adresi http://gocsi.com/sites/default/files/pdf_survey/CSI%20Survey%202009%20Comprehensive%20Edition.pdf, (son erişim tarihi 11 Haziran 2011).
- (5) Palfreyman K. and Rodden T. A Protocol For User Awareness And World Wide Web, Computer Supported Cooperative Work'96, Cambridge MA, USA, 1996 ACM 0-89791-765-0/96/11
- (6) Gross J. B. and Rosson M. B. Looking for Trouble: Understanding End-User Security Management, CHIMIT'07, March 30-31, 2007, Cambridge MA, USA. 2007 ACM 1-59593-635-6/97/0003
- (7) Stanton J. M. and Stam K. R. Mastrangelo Paul, Jolton Jeffrey, Analysis of End User Security Behaviors, Computers & Security, March 2005, sayfa 124-133
- (8) Herzberg A. and Jbara A. Security and Identification Indicators for Browsers against Spoofing and Phishing Attacks, ACM Transactions on Internet Technology, September 2008, Vol. 8, No. 4, Article 16.
- (9) West R. The Psychology of Security, Communications of the ACM, April 2008, Vol. 51 No.4
- (10) Rahim, M. M., M.N. Rahaman and Seyal, A.H. "Software piracy among academics: an empirical study in Brunei Darussalam", Information Management & Computer Security (2000), 8 (1), 14-26.
- (11) Lau, E.K.W. "An empirical study of software piracy", Business Ethics: An European Review, 2003-12 (3), 233-245.
- (12) Levy K. Overcoming the Digital Divide. Panel Discussion (2002): E-Government and Citizen Centered Government Round Table. İnternet adresi <http://www.epa.gov/customerservice/2002conference/levy.pdf>. (son erişim tarihi 25.07.2006)
- (13) Lian J.W. and Lin T.M. Effects of consumer characteristics on their acceptance of online shopping: Comparisons among different product types, Computers in Human Behavior (2008). 24(1): 48-65.
- (14) Colley, A. & Maltby, J.. Impact of the Internet on our lives: male and female personal perspectives. Computers in Human Behavior, 24(2008), 2005-2013.
- (15) Yang, Shu Ching & Tung Chieh-Ju, Comparison of Internet addicts and non-addicts in Taiwanese high school. Computers in Human Behavior (2007), 23, 79-96.
- (16) Zhang, Y. Age, gender, and Internet attitudes among employees in the business world. Computers in Human Behavior, 21(2005), 1-10.
- (17) Jaeger P.T. The endless wire: e-government as global phenomenon. Government Information Quarterly, 2003-20, 323-31.