Sosyal Ağlarda Güvenlik: Bitlis Eren ve Fırat Üniversitelerinde Gerçekleştirilen Bir Alan Çalışması

Security On Social Network: A Case Study Done At Bitlis Eren and Fırat Universities

N. Yıldırım[1] ve A. Varol [2]

[1]Bitlis Eren University, Bitlis/Turkey, nilyildirim87@gmail.com
[2]Fırat University, Elazig/Turkey, varol.asaf@gmail.com

Özetçe

Sosyal ağlar 2000'li yıllardan itibaren popüler olmuştur. Popülerliği, günlük tıklanma oranları, milyonları geçen üye sayıları ve bu üyelerin kişisel bilgileri ile sosyal ağlar hackerların, siber mühendislerin, şirketlerin hedefi durumuna gelmiştir. Bu nedenle sosyal ağların güvenlik açısından ne derece yeterli olduğunu ve sosyal ağlarda alınabilecek güvenlik önlemlerinin farkındalığını kullanıcılar açısından anlamak amacıyla bir anket çalışması yapılmıştır. Çalışma Fırat Üniversitesi ve Bitlis Eren Üniversitesi'nde gerçekleştirilmiş ve öğrenciler, öğretim üyeleri ve öğretim elemanları bu anket çalışmasına katılmışlardır. Daha sonra anket sonuçları yorumlanarak kullanıcılar açısından sosyal ağların güvenliği tartışılmıştır.

Anahtar Kelimeler: sosyal ağlar, güvenlik, tehditler, bilgi güvenliği, güvenlik açıkları

Securıty On Socıal Network: A Case Study Done At Bitlis Eren And Fırat Unıversıtıes

Abstract

Social networking has been one of the widely conducted activities in the internet since 2000. With the increasing number of visits per day, and personal information about millions of people, social networking has become one of the tempting targets for hackers, cyber engineers, and companies. Therefore a survey is conducted to evaluate the current security measures in social networking and user awareness of the risks associated with the service. The survey was carried out at Firat and Bitlis Eren Universities' students, faculty members and teaching staff. At the end, the survey results are evaluated and privacy issues of social networking users are discussed.

Keywords: social network, security, threats, information security, vulnerabilities

1. GİRİŞ

SOSYAL ağlar kullanıcıların birbirleriyle tanışması, irtibata geçmesi, tartışma ortamı oluşturması, içerik paylaşımında bulunması ve ortak ilgi alanlarındaki kişilerin bir araya gelebileceği gruplar oluşturulması amacıyla oluşturulan internet siteleri olarak tanımlanmaktadır [1]. eBizMBA Nisan 2013 verilerine göre en sık kullanılan sosyal ağ sitelerine ve aylık ziyaret sayılarına bakıldığında Facebook'un 750 milyon aylık tekil kullanıcı sayısı ile birinci sırada olduğu, Twitter'ın 250 milyon ile ikinci , LinkedIn'in 110 milyon aylık tekil kullanıcı sayısı ile üçüncü sırada olduğu görülmektedir [2].

Tablo1: eBizMBA Nisan 2013 Popüler Sosyal Paylaşım Siteleri

Sıra	Sosyal Paylaşım Sitesi Adı	Aylık tekil kullanıcı sayısı
1	Facebook	750,000,000
2	Twitter	250,000,000
3	LinkedIn	110,000,000
4	Pinterest	85,500,000
5	MySpace	70,500,000
6	Google Plus+	65,000,000

Google Trends verilerine göre Facebook'un günlük ziyaret sayısına bakıldığında bu rakamın 310 milyon olduğu görülmekte ve bu da kullanıcıların yarısının hergün bu siteyi ziyaret ettiği anlamına gelmektedir [3].

Sosyal ağları kullanıcı sayısı açısından ele aldığımızda en fazla nüfusu olan ülkeler kadar üye sayılarının olduğu görülmektedir. Bu nedenle sosyal ağlar siber mühendislerin, hackerların, kullanıcı verisi toplamak amacıyla şirketlerin hedefi durumuna gelmiştir. Spamciler, sosyal ağ sitelerinden bilgi toplamak için uğraşmakta ve fırsat beklemektedirler [4]. Bu durumda kullanıcıların sosyal ağlardaki güvenlikleri konusundaki bilgi düzeyleri araştırma konusu olmaktadır.

2. SOSYAL AĞLARDA GÜVENLİK

Yapılan yeni çalışmalar, web hackleme olaylarının yaklaşık %50'sinin sosyal ağ sitelerinde olduğunu göstermektedir. Breach Security, web hackleme veri tabanları üzerinde çalışmaktadır ve çevrimiçi atakların 2008 yılında %19 oran ile,

2009 yılında ise %30 oranla sosyal ağ sitelerine olduğu görülmektedir [5]. Türkiye'de de son birkaç yıldır bazı gizli videolar ve ses kayıtları izin alınmaksızın sosyal ağlarda paylaşılmaktadır [6].

Şekil 1:Sosyal Ağ Güvenliği [7]

İşyerlerinin en çok sosyal ağ ataklarından korktuğu ve işverenlerin %76 sının sosyal ağ sitelerini engellemek için web filtreleme servislerini kullandıkları görülmektedir [5].

a. Sosyal Ağlarda Güvenlik Problemleri

Sosyal ağlardaki güvenlik açıklıklarının temel nedenleri; bu ağların kuruluş amaçları nedeniyle, mahremiyet ilkelerine uyulmaması, ortamın yönetiminin ve kontrolünün nasıl yapıldığını kullanıcıların tam olarak bilmemesi veya kavramaması ve en önemlisi kullanıcıların kişisel bilgilerini paylaşarak kendilerini bu ortamda hedef haline getirmeleridir [8].

Sosyal ağ sitelerinde kullanıcılar evlilik durumlarını, eğitimlerini, adreslerini, kişisel bilgilerini, kişisel resimler gibi bilgilerini paylaşmakta, hatta nerede çalıştıklarını, önceki tüm eğitimlerini, politik görüşlerini ve ilgi alanlarını da paylaşmaktadırlar [9]. Ancak bir sosyal ağ sayfası oluştururken ve bu bilgiler verilirken bu sayfalara kimlerin bakacağının (patron, komşu, anne-baba, arkadaşların arkadaşları gibi) düşünülmesi gerekmektedir [4].

Şifrelerin sosyal ağlarda paylaşılmış tarihler ile aynı olması önemli güvenlik problemlerindendir [4]. Ayrıca anne kızlık soyadı da pekçok alanda kullanılan gizlilik bilgisidir ancak, bu ortamlara kullanıcının anne ve dayısının dahi katılması bu bilgilerin biliniyor olmasına neden olacaktır [8]. Gizli sorunun cevabını içeren paylaşımlar bazen yapılabilmektedir. Örneğin "Evcil hayvanınızın adı nedir?" sorusunun belirlenmesine karşın "Bu da muhabbet kuşum Boncuk" şeklinde bir paylaşım yapılması, bu gizli sorunun cevabını da ele verecektir. Bu bilgiler doğrultusunda birkaç deneme sonucunda şifre tespiti yapılabilir ve kullanıcı hesabı ele geçirilebilir.

Sosyal ağlarda kimlik taklitleri yapılabilmekte ve kullanıcıların adına sahte hesaplar açılabilmektedir. Ayrıca eklenen fotoğraf veya videolar bu hesaplarda, bazen de farklı amaçlar ile izinsiz kullanılabilmektedir.

Sosyal ağlarda pekçok zararlı uygulamaya, sazan avlama (phishing) saldırılarına, spamlara, sahte link ve bağlantılara da maruz kalınmaktadır. Sosyal ağlar ücretsiz reklam ortamları da kullandıklarından dolayı bu sayfalar pornografik içeriklere yönlendirilebilmektedir [6].

Sosyal ağlarda kullanıcılar sosyal ağlar üzerinde tanıştıkları kötü niyetli kişiler tarafından taciz ve istismar gibi tuzakların kurbanı olabilmektedirler[8]. Kullanıcıların sosyal ağ üzerinden de mesaj içerikleri ile kişisel haklarına müdahale edildiği görülmektedir. Özellikle fotoğraf, ev adresi ve yer bildirimi gibi bilgilerin verilmesi bu tuzaklara yakalanılma riskini artırmaktadır. Ayrıca yer

bildirimi yapılması hırsızlara kapı da açabilmektedir.

b. Mobil Cihazlarda Sosyal Ağ Güvenliği

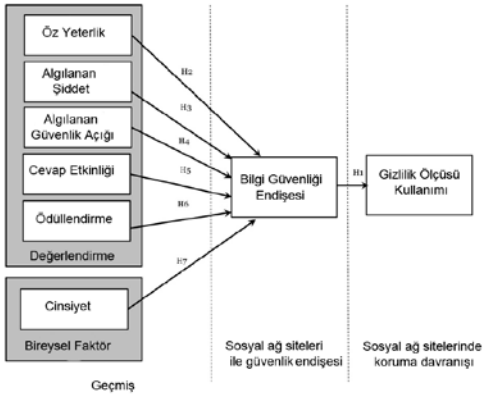
Trend Micro'nun Amerika'da 1000 akıllı telefon ve iPhone kullanıcısı ile yaptığı araştırmada katılımcıların %44'ünün akıllı telefonlar ile internette gezinmenin riskli olduğunu düşünmesine karşın sadece %23'ünün telefonlarında güvenlik yazılımı kullandığı görülmektedir [5]. Oysa ki mobil cihazlara gelen virüs ya da diğer zararlı yazılımlar %80 oranında antivirüs yazılımı kullanılmadığı için sıklıkla etkilerini göstermektedirler. Bu durum akıllı telefonlarda bilgi güvenliğinin büyük bir sorun haline geldiğini göstermektedir.

Akıllı telefon ve tabletlerin güvenlik ayarları incelendiğinde bu aygıtların ayarlarının kullanıcıların kişisel verilerini öncelikli olarak paylaşmaya razı olduğu varsayılarak ayarlandığı görülmektedir [10]. Sosyal ağlarda gezinirken GPS ve WiFi aracılığı ile konum bilgileriniz paylaşılabilmektedir. Ayrıca bazı zararlı uygulamalar da sosyal ağların mobil cihazınızda sürekli açık bulunduğundan, sosyal ağlardaki bilgileri çekmektedir. Bu açıdan mobil cihazlarda sosyal ağ güvenliği önemli bir konu olarak ele alınmalıdır.

c. Sosyal Ağlarda Güvenlik Üzerine Yapılmış Çalışmalar

A. Varol ve Ö.Aydın (2010)'ın 1004 katılımcı ile sosyal ağlar üzerine yaptıkları çalışmada bilgi ve veri paylaşımı güvenliği konusunda kullanıcıların sosyal ağlarda kişisel bilgilerini güvende görmedikleri ancak, çoğunlukla kişisel bilgilerini doğru verdikleri sonucu elde edilmiştir. Yine araştırmada sosyal ağ kullanıcılarının kişisel fotoğraflarını, videolarını ve kişisel bilgilerini bu ağlarda paylaştıkları sonucuna ulaşılmıştır. Ayrıca erkek kullanıcılarla kıyaslandığında kadınların daha fazla bu paylaşımları yaptığı görülmüştür [6].

N. Mohamed ve I.H. Ahmad (2012)'ın Malezya'da 340 kişi ile yaptıkları çalışmada sosyal ağ güvenliği için Şekil 2'deki hipotez model geliştirilmiştir. Kullanıcının öz yeterliği, algıladığı şiddet, algıladığı güvenlik açığı ve cinsiyeti ile bilgi güvenliği arasında pozitif ilgi olduğu tespit edilmiştir. Sonuç olarak bilgi güvenliği ile sosyal ağ sitelerinde gizlilik ölçüsü kullanımı arasında pozitif ilişki olduğu ortaya çıkmıştır [11].



Şekil 2: Sosyal ağ sitelerinde bilgi gizlilik endişeleri, öncülleri ve gizlilik ölçüsü kullanımı hipotez modeli [11]

3. YÖNTEM

Bu çalışmada sosyal ağların güvenlik açısından ne derece yeterli olduğunu, sosyal ağlarda hangi güvenlik problemlerine maruz kalındığını ve sosyal ağlarda alınabilecek güvenlik önlemlerinin farkındalığını kullanıcılar açısından ele almak amacıyla bir kesitsel anket çalışması yapılmıştır. Modeli betimsel tarama olan bu çalışmaya toplamda 306 kullanıcı katılmıştır. Bunlardan 21 'i öğretim üyesi, 51'i öğretim elemanı, 211 'i öğrenci ve 23'ü diğer gurubunda yer almıştır. 60 kişi Fırat Üniversitesinden, 202 kişi Bitlis Eren Üniversitesi'nden ve 42 kişi diğer kurumlardan ankete katılmıştır.

Çalışma kapsamındaki anket, online anket sitesi olan QuestionPro'da hazırlanmıştır ve "sosyalagguvenligi.questionpro.com" adresinden ankete katılım sağlanmıştır.

4. BULGULAR

a. Demografik Bilgiler

Anket çalışması Tablo 2'deki gibi cinsiyete göre %60 oranla erkek, % 40 oranla kadın katılımcılar tarafından tamamlanmıştır.

Tablo 2: Cinsiyete göre betimsel istatistik değerleri

	Frekans	Yüzde	Kümülatif Yüzde	$\bar{X}$	S
Kadın	122	39,9	39,9		
Erkek	184	60,1	100,0	1,601	,4904
Toplam	**306**	**100,0**			

Tablo 3 incelendiğinde yaş aralıklarına göre 18-25 yaş arasında 210 katılımcının ve 26-33 yaş arasında da 76 katılımcının bulunduğu görülmektedir.

Tablo 3: Cinsiyet ve yaş aralıklarına göre dağılım

		Cinsiyetiniz nedir?		
		Kadın	Erkek	Toplam
Yaş aralığınız nedir?	18-25	81	129	210
		%38.57	**%61.43**	**%68.63**
	26-33	38	38	76
		%50	**%50**	**%24.84**
	34-41	3	14	17
		%17.65	**%82.35**	**%5.56**
	42-49	0	2	2
		%0	**%100**	**%0.65**
	50 yaş ve üzeri	0	1	1
		%0	**%100**	**%0.33**
	Toplam	**122**	**184**	**306**
		%39.87	**%60.13**	**%100**

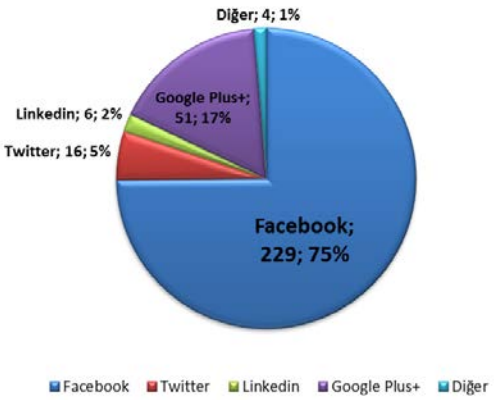
Anket çalışması, Bitlis Eren Üniversitesi, Fırat Üniversitesi ve diğer kurumlardaki öğrencilere, öğretim elemanlarına ve öğretim üyelerine uygulanmıştır. Bitlis Eren Üniversitesi öğrencilerinin 158 kişi ile en fazla katılımı sağladığı görülmektedir. Kuruma ve çalışma durumuna göre yüzde dağılımı Tablo 4'te gösterilmektedir.

Tablo 4: Çalışılan kurum ve çalışma durumuna göre dağılım

		Çalıştığınız kurumu, öğrenci iseniz okuduğunuz üniversiteyi belirtiniz.			
		Bitlis Eren Üniversitesi	Fırat Üniversitesi	Diğer	Toplam
Çalışma durumunuzu belirtiniz.	Öğrenci	158	41	12	211
		%74.88	**%19.43**	**%5.69**	**%68.9**
	Araştırma Görevlisi	14	9	14	37
		%37.84	**%24.32**	**%37.8**	**%12.0**
	Öğretim Görevlisi	9	1	4	14
		%64.29	**%7.14**	**%28.57**	**%4.5**
	Öğretim Üyesi	13	7	1	21
		%61.9	**%33.33**	**%4.76**	**%6.86**
	Diğer	8	2	13	23
		%34.78	**%8.7**	**%56.52**	**%7.52**
	Toplam	**202**	**60**	**44**	**306**
		%66.01	**%19.61**	**%14.3**	**%100**

b. Sosyal Ağ Kullanımı

Şekil 3'te görüldüğü gibi Facebook, Twitter, Google Plus+ , LinkedIn gibi sosyal ağlar içerisinde %75 oranla Facebook en sık kullanılan sosyal ağ durumundadır.



Şekil 3: Katılımcıların en sık kullandığı sosyal ağlar

Çalışma durumları ele alındığında en sık kullanılan sosyal ağ Tablo 5'te görüldüğü gibi öğrenci, öğretim elemanı, öğretim üyeleri için Facebook'tur. Kendi gurupları içerisinde ele alındığında araştırma görevlilerinin %86 oranla en fazla Facebook'u kullandıkları saptanmıştır.

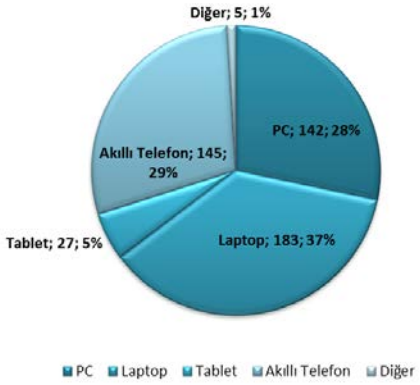
Tablo 5: Çalışma durumuna göre sık kullanılan sosyal ağlar

	Çalışma durumunuzu belirtiniz.					
En sık kullandığınız sosyal ağ hangisidir?	Öğrn.	Araş. Gör.	Öğrt. Gör.	Öğrt. Üyesi	Diğer	Topl.
Facebook	158	32	10	14	15	229
	%74,9	**%86,5**	**%71,4**	**%66,7**	**%65,2**	**%74,8**
Twitter	8	2	2	1	3	16
	%14,3	**%4,8**	**%13,0**	**%5,2**	**%3,8**	**%5,4**
Linkedin	2	1	0	2	1	6
	%,9	**%2,7**	**%,0**	**%9,5**	**%4,3**	**%2,0**
Google Plus+	40	2	2	4	3	51
	%14,3	**%19,0**	**%13,0**	**%16,7**	**%19,0**	**%5,4**
Diğer	3	0	0	0	1	4
	%,0	**%,0**	**%4,3**	**%1,3**	**%1,4**	**%,0**
Toplam	**211** **%69**	**37** **%12.1**	**14** **%4.58**	**21** **%6.86**	**23** **%7.5**	**306** **%10**

Sosyal ağ kullanım sıklıkları ele alındığında Tablo 6'da görüldüğü gibi %44,8 oranla sosyal ağlara günde ortalama 1-5 defa girildiği görülmektedir. Her yaş aralığı için de sıklıkla günde 1-5 kere sosyal ağların ziyaret edildiği görülmektedir.

Tablo 6: Yaş aralıklarına göre sosyal ağ kullanım sıklıkları

	Yaş aralığınız nedir?					
Hangi sıklıkla sosyal ağlara bağlanıyorsunuz?	18-25	26-33	34-41	42-49	50 +	Topl.
Ayda bir kere	14	7	1	0	0	22
	%6,7	**%9,2**	**%5,9**	**%,0**	**%0**	**%7,2**
Haftada bir kere	55	12	5	0	0	72
	%26,2	**%15,8**	**%29,4**	**%,0**	**%0**	**%23,5**
Günde 1-5 kere	96	32	7	2	0	137
	%45,7	**%42,1**	**%41,2**	**%100,0**	**%0**	**%44,8**
Günde 5-10 kere	21	11	2	0	0	34
	%10,0	**%14,5**	**%11,8**	**%,0**	**%0**	**%11,1**
Günde 10 +	24	14	2	0	1	41
	%11,4	**%18,4**	**%11,8**	**%,0**	**%100**	**%13,4**
Toplam	**210** **%68.6**	**76** **%24.8**	**17** **%5.56**	**2** **%0.65**	**1** **%.**	**306** **%100**



Şekil 4: Sosyal ağlara erişmek için kullanılan cihazlar

Sosyal ağlara erişmek için sıklıkla kullanılan cihazlar incelendiğinde Laptop'un %37, Akıllı telefonların %29 ve Masaüstü bilgisayarların %28 oranla kullanıldığı görülmektedir.

c. *Sosyal Ağlarda Kişiye Yönelik Güvenlik Tehditleri*

Sosyal ağ kullanımları ele alındıktan sonra kullanıcıların hayatında bu kadar önemli yer edinmiş olan sosyal ağların kişiler açısından güvenlik tehditlerini incelemek amacıyla, güvenlikle ilgili bulgular incelenmiştir. Kullanıcıların sosyal ağlarda bilgilerini paylaştıkları bilinmektedir. Şekil 5'e göre kadın ve erkeklerin sosyal ağlarda ne tür bilgiler paylaştığına bakıldığında en fazla e-posta adresi, sonrasında kişisel fotoğrafların ve doğum tarihlerinin paylaşıldığı görülmektedir. Kadın kullanıcılardan farklı olarak erkek kullanıcılar telefon numaralarını da paylaşmaktadırlar.

Şekil 5: Sosyal ağlarda paylaşılan bilgilerin cinsiyete göre dağılımı

Sosyal ağlara hangi cihazlar ile güvenle bağlandıkları sorusuyla ilgili olarak Tablo 7 incelendiğinde katılımcıların %43,8 oranla Laptop ile, %35 oranla ise PC ile sosyal ağlara bağlanmanın güvenli olduğunu düşündükleri görülmektedir.

Tablo 7: Sosyal ağlara bağlanmak için güvenli bulunan cihazlar

	Frekans	Yüzde	Kümülatif Yüzde	$\bar{X}$	S
PC	107	35,0	35,0		
Laptop	134	43,8	78,8		
Tablet	3	1,0	79,7		
Akıllı Telefon	51	16,7	96,4	2,1013	1,1592
Diğer	11	3,6	100,0		
Toplam	306	100,0			

Sosyal ağlarda gizlilik/güvenlik ayarlarını kontrol sıklıklarına bakıldığında Tablo 8'e göre %37,9 oranla ayda bir defa, %25,2 oranla da haftada bir defa kontrol edildiği ve ortalama %21'lik kısmın ise yılda bir defa kontrol ettiği veya hiçbir zaman kontrol etmediği görülmektedir.

Tablo 8: Sosyal ağlarda gizlilik/güvenlik ayarları kontrol sıklığı

	Frekans	Yüzde	Kümülatif Yüzde	$\bar{X}$	S
Haftada bir	77	25,2	25,2		
Ayda bir	116	37,9	63,1		
Altı ayda bir	48	15,7	78,8	3,00	1,0834
Yılda bir	25	8,2	86,9		
Kontrol etmiyorum	40	13,1	100,0		
Toplam	306	100,0			

En sık kullanılan sosyal ağ olan Facebook için gizlilik/ güvenlik ayarlarının hangi sıklıkla yapıldığına bakıldığında %38 oranla ayda bir defa kontrol edildiği görülmektedir.

Şekil 6: Facebook'ta gizlilik/güvenlik ayarları kontrolü

Sosyal ağlarda kişisel bilgilerin %76,8 oranla doğru olarak verildiği Tablo 9'da görülmektedir.

Tablo 9: Sosyal ağlarda kişisel bilgilerinizi doğru olarak veriyor musunuz?

	Frekans	Yüzde	Kümülatif Yüzde	$\bar{X}$	S
Evet	235	76,8	76,8	1,2320	,42282
Hayır	71	23,2	100,0		
Toplam	306	100,0			

Kişiler, %83,7 oranla doğru sosyal ağların kişisel bilgilerini korumada yeterli olmadığını düşündükleri Tablo 10'da görülmektedir.

Tablo 10: Sosyal ağların kişisel bilgilerinizi korumada yeterli olduğunu düşünüyor musunuz?

	Frekans	Yüzde	Kümülatif Yüzde	$\bar{X}$	S
Evet	50	16,3	16,3	1,8366	,37033
Hayır	256	83,7	100,0		
Toplam	306	100,0			

Tablo 11'e göre %58,8 oranla sosyal ağlarda kişisel bilgilerin alınıp kurumlar tarafından kullanıldığı düşünülmektedir

Tablo 11: Sosyal ağlarda kişisel bilgilerinizin kurumlar ve şirketler tarafından alınıp kullanıldığını düşünüyor musunuz?

	Frekans	Yüzde	Kümülatif Yüzde	$\bar{X}$	S
Evet	180	58,8	58,8	1,4118	,49296
Hayır	126	41,2	100,0		
Toplam	306	100,0			

Kişiler, Tablo 12'ye göre %66 oranla sosyal ağlarda kişisel bilgilerinin kötüye kullanıldığını düşünmektedir.

Tablo 12: Sosyal ağlarda kişisel bilgilerin kötüye kullanıldığını düşünüyor musunuz?

	Frekans	Yüzde	Kümülatif Yüzde	$\bar{X}$	S
Evet	202	66,0	66,0	1,3399	,47444
Hayır	104	34,0	100,0		
Toplam	306	100,0			

Kişiler Tablo 13'e göre sosyal ağlarda %57,5 oranla spam ya da zararlı uygulamalara maruz kalmaktadırlar.

Tablo 13: Sosyal Ağlarda spamlere ya da zararlı uygulamalara maruz kaldınız mı?

	Frekans	Yüzde	Kümülatif Yüzde	$\bar{X}$	S
Evet	176	57,5	57,5	1,4248	,49513
Hayır	130	42,5	100,0		
Toplam	306	100,0			

Kişiler Tablo 14'e göre arkadaşlarından gelen uygulama tekliflerini güvenliğinden emin olmadan %82,4 oranla kabul etmemektedirler.

Tablo 14: Sosyal ağlarda arkadaşlarınızdan gelen uygulama tekliflerini güvenli olup olmadıklarını bilmeden kabul ediyor musunuz?

	Frekans	Yüzde	Kümülatif Yüzde	$\bar{X}$	S
Evet	54	17,6	17,6		
Hayır	252	82,4	100,0	1,8235	,38184
Toplam	306	100,0			

Sosyal ağlarda açılan bağlantının %74,5 oranla kişileri farklı sayfalara yönlendirmiş olduğu Tablo 15'de görülmektedir.

Tablo 15: Sosyal ağlar üzerinde tıkladığınız bir bağlantı sizi istemediğiniz sayfalara yönlendirdi mi?

	Frekans	Yüzde	Kümülatif Yüzde	$\bar{X}$	S
Evet	228	74,5	74,5		
Hayır	78	25,5	100,0	1,2549	,43652
Toplam	306	100,0			

Sosyal ağlarda kişilerin adına %17,3 oranla sahte hesap açıldığı Tablo 16'da görülmektedir.

Tablo 16: Sosyal ağlarda adınıza sahte üyelik oluşturuldu mu?

	Frekans	Yüzde	Kümülatif Yüzde	$\bar{X}$	S
Evet	53	17,3	17,3		
Hayır	253	82,7	100,0	1,8268	,37904
Toplam	306	100,0			

Sosyal ağlarda kişisel fotoğrafların kullanıcının izni olmaksızın farklı kişiler tarafından %21,9 oranla kullanıldığı Tablo 17'de görülmektedir.

Tablo 17: Sosyal ağlarda fotoğraflarınız izniniz dışında kullanıldı mı?

	Frekans	Yüzde	Kümülatif Yüzde	$\bar{X}$	S
Evet	67	21,9	21,9		
Hayır	239	78,1	100,0	1,7810	,41421
Toplam	306	100,0			

Sosyal ağlarda kişisel hesapların %32,4 oranla başkaları tarafından ele geçirildiği ya da bu çabaya girişildiği Tablo 18'de görülmektedir.

Tablo 18: Sosyal ağlarda hesabınız ele geçirildi mi ya da hesabınızı ele geçirme girişimleri sonucunda hesabınız durduruldu mu?

	Frekans	Yüzde	Kümülatif Yüzde	$\bar{X}$	S
Evet	99	32,4	32,4		
Hayır	207	67,6	100,0	1,6765	,46859
Toplam	306	100,0			

Sosyal ağlarda rahatsızlık verici mesajların %30 oranla alındığı Tablo 19'da görülmektedir.

Tablo 19: Sosyal ağlarda rahatsızlık verici, kişilik haklarınıza müdahale edecek mesajlar alıyor musunuz?

	Frekans	Yüzde	Kümülatif Yüzde	$\bar{X}$	S
Evet	92	30,1	30,1		
Hayır	214	69,9	100,0	1,6993	,45929
Toplam	306	100,0			

Sosyal ağlarda %80 oranla kişilerin tanımadıklarını arkadaş olarak eklemedikleri Tablo 20'de görülmektedir.

Tablo 20: Sosyal ağlarda tanımadığınız kişileri arkadaş olarak ekliyor musunuz?

	Frekans	Yüzde	Kümülatif Yüzde	$\bar{X}$	S
Evet	60	19,6	19,6		
Hayır	246	80,4	100,0	1,8039	,39768

Toplam	306	100,0	100,0

Kişilerin sosyal ağlarda %58,5 oranla bulundukları yeri paylaştıkları Tablo 21'de görülmektedir.

Tablo 21: Sosyal ağlarda bulunduğunuz yeri paylaşıyor musunuz ?

	Frekans	Yüzde	Kümülatif Yüzde	$\bar{X}$	S
Evet	179	58,5	58,5		
Hayır	127	41,5	100,0	1,4150	,49353
Toplam	306	100,0			

"Evcil hayvanınızın adı nedir?" gizli sorusunu belirlemesine karşın "Köpeğim Karabaş'ın fotoğrafları" gibi gizli sorusunun cevabını içeren paylaşımların %82,4 oranla yapılmadığı Tablo 22'de görülmektedir.

Tablo 22: Sosyal ağlarda şifre işlemleri aşamasında belirlediğiniz gizli sorunuzun cevabını içeren paylaşımlar yaptınız mı?

	Frekans	Yüzde	Kümülatif Yüzde	$\bar{X}$	S
Evet	54	17,6	17,6		
Hayır	252	82,4	100,0	1,8235	,38184
Toplam	306	100,0			

Kişilerin %59,82 oranla sosyal ağ güvenliği sağlayan yazılımlar kullanmadığı Tablo 23'de görülmektedir.

Tablo 23: Sosyal ağ güvenliği sağlayan, kişisel bilgilerinizi koruyan internet güvenlik yazılımları kullanıyor musunuz?

	Frekans	Yüzde	Kümülatif Yüzde	$\bar{X}$	S
Evet	125	40,8	40,8		
Hayır	181	59,2	100,0	1,5915	,49236
Toplam	306	100,0			

Kişiler, en sık kullandığı sosyal ağda %74,5 oranla güvenliğin yeterli olmadığını düşündükleri Tablo 24'de görülmektedir.

Tablo 24: En sık kullandığınız sosyal ağda güvenliğin yeterli olduğunu düşünüyor musunuz?

	Frekans	Yüzde	Kümülatif Yüzde	$\bar{X}$	S
Evet	78	25,5	25,5		
Hayır	228	74,5	100,0	1,7451	,43652
Toplam	306	100,0			

d. Kullanıcıların Dilinden Sosyal Ağlardaki Güvenlik Tehditleri

Anket sonunda bulunan "Sosyal ağlardaki güvenlik konusunda yaşadığınız en önemli sorunu birkaç cümle ile belirtiniz" sorusuna verilen bazı yanıtlar aşağıda yer almaktadır.

- Sahte profil oluşturulmasının önüne geçilememesi, taciz içerikli mesajları gönderen kişiyi engellemeden bu mesajların gelmesinin engellenememesi.
- Daha üst düzey güvenlik koruması bulunmasını isterim. Bir kaç sefer şifrem kırıldı.
- Çok fazla yaramaz ileti (spam) ile karşı karşıya kalmak.
- Bence sosyal ağlar artık sadece iletişim ve paylaşım aracı değil. İsmini değiştirip sosyal medya olmuştur. Sosyal medya olarak da şirketler, özellikle hızlı tüketim ürünleri üreten şirketler daha sıklıkla müşteri analizleri yapmak için kullanmaktadırlar. Müşteri analizi yaparken de veri olarak biz kullanıcıların özel bilgilerini bizden habersiz kullanıyorlar. Bunun da etik olmayan bir davranış olduğunu düşünüyorum. Bu açıdan sosyal medya araçlarının bilgi güvenliğini korumadıklarını düşünüyorum.
- Ayarlarını kolay erişilebilecek yerlere özellikle koymuyorlar. Bir girdiğiniz bilgiyi bir daha silemiyorsunuz.

- Sosyal ağın altyapısında kullanıcıya haber verilmeden değişiklik yapılması. Güvenlik açığının artması ve kişisel bilgilerin farklı yerlerle paylaşılması. Örneğin Facebook'un zaman zaman ayarlarını değiştirip kişisel bilgileri yayınlayacağına dair haberlerin çıkması.
- Sosyal ağ hesabı açık olduğunda harici sitelerde istek dışı sayfa beğenmeleri.
- Facebook kredisi aldım kredi kartımla ve kredilerim gelmedi ama kartımdan parası kesildi.
- Sosyal ağ güvenliği sağlayan, kişisel bilgilerinizi koruyan internet güvenlik yazılımları kullanıyor musunuz? Böyle bir yazılımın varlığından haberdar değilim. Eğer kastedilen virüs yazılımları ise evet kullanıyorum. En önemli sorun bu tür ağların benim güvenliğimi hangi sınırlarda koruduğu konusunda bir fikir vermemesidir.
- Bir kaç gün önce arkadaşımın Facebook hesabı ele geçirildi ve paylaşımlar yapıldı arkadaş önerme vs. geri alamadık:(

5. SONUÇ VE ÖNERİLER

Kullanıcıların günde en az 1-5 defa sosyal ağları kontrol ettiği görüldüğünde bu sitelerin hayatımızda ne derece önemli bir yer edindiğini anlamak mümkündür.

Kullanıcılar sosyal ağlara bağlanmak için sırası ile laptop, akılı telefon ve PC'leri kullanmaktadırlar. Ancak laptop ve PC'yi akıllı telefonlara göre daha güvenli buldukları görülmektedir. Kişilerin güvende hissetmediği halde akıllı telefonlar ile sosyal ağlara bağlanmaları akıllı telefon güvenliği hakkında ne yapılacağını bilmiyor olmalarından kaynaklanabilir. Bu durumda iOS tabanlı IPhone ve IPad gibi cihazlarda Safari ayarlarında 'Dolandırıcılık Uyarısı' ve 'Pencereleri Engelle' seçeneklerinin seçili (mavi) olmasına dikkat edilmeli, Android cihazlarda GPS kullanılmadığında devre dışı bırakılmalı ve sosyal ağ uygulamalarının telefon rehberini taramasına izin verilmemelidir [10].

Kullanıcıların sosyal ağ güvenlik ayarlarını ayda bir sıklıkla kontrol ettiği görülmektedir. 10 kişiden 2'si ise sosyal ağ güvenlik ayarlarını yılda bir ya da hiç kontrol etmemektedir. Oysa her paylaşımda dahi belirli listelere izinler vermek için gizlilik ayarları kontrol edilmeli ve sosyal ağ sitelerinin güvenlik ayarlarını sıkça değiştirdiği göz önüne alınarak bu ayarlar takip edilmelidir.

Sosyal ağlarda kullanıcıların büyük çoğunluğunun kişisel bilgilerini doğru olarak verdiği görülmektedir. Oysa ki yine büyük çoğunluk, bu ağların kişisel bilgileri korumada yeterli olmadığını ve 10 kişiden 6'sı bilgilerinin kurumlar tarafından kullanıldığını düşünmektedirler. Sosyal mühendislik saldırılarının sosyal ağlarda yoğun olduğu unutulmamalı ve paylaşılacak bilgiler konusunda dikkatli olunmalıdır.

Kullanıcıların büyük çoğunluğu kişisel bilgilerin kötüye kullanıldığını düşünmektedir. Buna rağmen e-posta adresi, kişisel fotoğraf ve doğum tarihlerinin kullanıcılar tarafından sıklıkla paylaşıldığı sonucuna ulaşılmaktadır. Kullanıcıların yarısından fazlası yer bidirimleri de yapmaktadır. Bu durumda kötü niyetli kişiler paylaşılan mekanlarda kullanıcıları bulabilir ya da dışarda bulunduğunu fırsat bilenler ev soygunu da yapabilirler. Bu güvenlik riskine dikkat çekmek için please rob me (lütfen beni soyun) isminde bir site de açılmıştır [12].

Kullanıcıların yarısından fazlası spam ya da zararlı uygulamalara maruz kalmaktadırlar. Kullanıcıların büyük çoğunluğun uygulamaları emin olmadan açmadığı halde bu zararlı yazılımlara engel olamadıkları sonucuna ulaşılmaktadır. Bu da güvenli sanılan uygulamaların da zararlı uygulama olabileceğini göstermektedir. Arkadaşların e-posta adreslerini vermekten kaçınmak için sosyal ağ hizmetlerinin e-posta adres defterini taramasına izin vermemek bu uygulamaların dağılmasına engel olacaktır [13].

Kullanıcıların 10'undan 2'si adına sahte hesap açıldığı ve kullanıcıların izni dışında fotoğraflarının kullanıldığı görülmektedir. Bunu engellemek için tanınmayan kişilerin sosyal ağlara eklenmemesi ya da güvenli arkadaş listeleri oluşturulup önemli bilgilerin sadece bunlarla paylaşılması önerilebilir. Kimlik hırsızları, kişilerden bilgi alabilmek için sahte profiller oluşturabilmektedirler [13]. Katılımcılara bakıldığında da büyük çoğunluğun tanımadıklarını eklemedikleri görülmektedir ancak sahte üyeliklere de dikkat edilmelidir.

Kullanıcıların 10'undan 3'ünün hesapları başkaları tarafından ele geçirilmekte ya da ele geçirmek amacıyla hesabın zorlandığı görülmektedir. Bunun için şifrenin ve gizli sorunun mümkün olduğunca zor ve karmaşık seçilmesi ve gizli soruyu ele verecek paylaşımların yapılmaması önemlidir. Kullanıcıların büyük çoğunluğunun da buna dikkat ettiği görülmektedir.

Kullanıcıların 10'undan 3'ü sosyal ağlarda rahatsızlık verici mesajlar almaktadırlar. Bu durum gerekli yerelere bildirilmeli ve siber zorbalıkların normal hayatta da karşımıza çıkacağı unutulmamalıdır.

Sosyal ağlarda kullanıcıların büyük çoğunluğu güvenliğin yeterli olmadığını düşündüğü halde kullanıcıların yarısından çoğu sosyal ağlar için antivirüs yazılımları kullanmamaktadırlar. Antivirüs yazılımları zararlı uygulamaları, spam bağlantıları tespit ettiği için bunların kullanılması kullanıcı güvenliğini sağlayacaktır.

KAYNAKLAR

[1] KurumsalHaberler, Sosyal Medya Nedir, 2010. [Çevrimiçi]. Available: http://www.kurumsalhaberler.com/pr/sosyal-medya-nedir.aspx . [20 Ocak 2011 tarihinde erişilmiştir].

[2] eBizMBA, Top 15 Most Popular Social Networking Sites | 4 Nisan 2013. [Çevrimiçi]. Available: http://www.ebizmba.com/articles/social-networking-websites [5 Nisan 2013 tarihinde erişilmiştir].

[3] Pingdom, 29 social networks that have at least one million visitors per day, 25 Mart 2011. [Çevrimiçi]. Available: http://royal.pingdom.com/2011/03/25/social-networks-one-million-visitors-per-day . [07 Nisan 2013 tarihinde erişilmiştir].

[4] D. Hobson, Social networking – not always friendly, *Computer Fraud & Security*, cilt 2008, no. 2, p. 20, 2008.

[5] Computer Fraud & Security, Hacking attacks target social networking, ELSEVIER, 2009.

[6] A. Varol ve O. Aydin, Social Network Analysis: A Case Study in Turkey, *7th International Conference on Intellectual Capital, Knowledge Management and Organisational*, pp. 471-479, 2010.

[7] Socialh.com, Social Media Security, 30 July 2012. [Çevrimiçi]. Available: http://cdn.socialh.com/wp-content/uploads/2012/07/social-media-security.jpg . [05 Nisan 2013 tarihinde erişilmiştir].

[8] U. Yavanoğlu, Ş. Sağıroğlu ve İ. Çolak, Sosyal Ağlarda Bilgi Güvenliği Tehditleri ve Alınması Gereken Önlemler, *Politeknik Dergisi* , cilt 15, no. 1, pp. 15-27, 2012.

[9] M. Qi ve D. Edgar-Nevill, Social networking searching and privacy issues, *Information Security Technical Report*, cilt 2011, no. 16, pp. 74-78, 2011.

[10] Tunca, Sosyal ağlarda güvenlik - 1: Akıllı telefon ve tablet güvenliği,6 Mayıs 2012. [Çevrimiçi]. Available: http://dijitalekoloji.blogspot.com/2012/05/sosyal-aglarda-guvenlik-1-akll-telefon.html . [5 Nisan 2013 tarihinde erişilmiştir].

[11] N. Mohamed ve I. H. Ahmad, Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia» *Computers in Human Behavior*, cilt 28, no. 1, p. 2366–2375, 2012.

[12] PCLabs, Sosyal Ağlarda Güvenlik, Eylülll 2010. [Çevrimiçi]. Available: http://guvenlik.pclabs.com.tr/46/sosyal-aglarda-guvenlik/ . [3 Nisan 2013 tarihinde erişilmiştir].

[13] Microsoft , Sosyal ağ güvenliği için 11 ipucu, Microsoft , 2012. [Çevrimiçi]. Available: http://www.microsoft.com/tr-tr/security/online-privacy/social-networking.aspx . [6Nisan 2013 tarihinde erişilmiştir].