Sosyal Ağlarda Güvenlik Farkındalığının Arttırılması

Ebru Yeniman Yıldırım

Özet: ***Bilişim teknolojilerindeki gelişmeler, bilişim teknolojilerinin kullanımıyla hizmetlerin daha hızlı sunulması, yaygınlaştırılması, doğru ve yeterli bilgiye hızla ulaşma, iş ve zaman verimliliği gibi pek çok kolaylığı sunarken sanal ortamlarda güven sorununu da beraberinde getirmiştir. Son yıllarda sosyal ağlarda yaşanan olumsuzluklar, bu ortamları kullanmanın sosyalleşmeyi kolaylaştırdığı kadar, yeni tehdit ve tehlikeleri de beraberinde getirmiştir.***

Bu çalışmada, sosyal ağ ortamlarında oluşabilecek riskler ve tehditler vurgulanarak, bilgi güvenliğinin özel hayatın gizliliği hakkına göre alınması gereken önlemler ve dikkat edilmesi gereken hususlar açıklanmaktadır. Bu kapsamda Bursa ilinde yaşayan rastgele seçilen 234 katılımcıya sosyal ağlarda güvenlik konusunda anket uygulaması yapılmıştır. Sosyal ağlarda güvenlikle ilgili elde edilen sonuçlar değerlendirilerek, önerilerde bulunulmuştur.

Anahtar Kelimeler: Sosyal Ağlar, Bilgi Güvenliği, Tehditler, Açıklar, Güvenlik Farkındalığı

Abstract: Evolutions in communication technology give rise to security problems in virtual media along with itself as well as providing many facilities, such as job opportunities, generalizing them, attaining the proper and sufficient information fast, work and time efficiency. The problems people have experienced lately show that using this social media may lead to some new threats and risks along with itself as well as making it easy to be socialized.

The required measures and points to take into account are explained in this study according to the right of privacy in the field of information security by emphasizing the potential risks and threats. In this context, 234 random participants, who were living in Bursa, were chosen for the survey regarding security in social networks. Based on the assessment of the outcomes of the survey on security in social networks, recommendations were provided.

Key words: Social Networks, Information Security, Threats, Shortfalls, Security Awareness

I. GİRİŞ

Sosyal ağlar son yıllarda ülkemizde yoğun bir şekilde kullanılmaktadır. Türkiye İstatistik Kurumu'nun (TÜİK) 2014 Ocak-Mart ayları arasında yaptığı araştırmaya göre internete erişim sağlayabilen 41.2 milyon kişinin %78'i Sosyal ağlara bağlanmıştır. 2015 yılının ilk üç ayında internet kullanan bireylerin %80,9'u sosyal medya üzerinde profil oluşturma, mesaj gönderme veya fotoğraf vb. içerik paylaşmıştır [1].

Sosyal ağlar, ister web ortamında, isterse mobil platformlarda olsun genelde aynı hizmetleri sunmalarına rağmen her bir erişim platformunda kullanıcılar açısından farklı güvenlik ve gizlilik tehlikeleri doğurmaktadır. Özellikle bu ortamları kullanan kişilerin bilgi güvenliği farkındalığının düşük olması, etik kullanım konusunda bilinç seviyesinin yetersizliği; bilinçsiz kullanmanın getireceği olumsuzluklarla karşılaşılabilecek tehlikelerin farkında olunmaması bu konuya önem verilmesi gerektiğini göstermektedir.

Bu kapsamda Bursa ilinde yaşayan rastgele seçilen 234 katılımcıya Sosyal ağlarda güvenlik konusunda uygulanan ankette çarpıcı sonuçlar elde edilmiştir. Anketten elde edilen sonuçlara göre, toplumda ciddi anlamda kullanılan sosyal ağlar konusunda bilgi güvenliği farkındalığının yetersiz olduğu ve önlemler alınması gerektiği vurgulanmıştır.

II. SOSYAL AĞLAR

Sosyal ağlar, kullanıcıların birbirleriyle tanışması, gruplar oluşturması, birbirleriyle irtibata geçmesi, tartışma ortamı oluşturularak, içerik paylaşımında bulunulması ve ortak ilgi alanlarındaki kişilerin bir araya gelebileceği internet siteleri olarak tanımlanmaktadır [2].

Dünyada kullanılan Sosyal ağlar; Facebook, Whatsapp, Twitter, LinkedIn, Instagram, Pinterest, Foursquare, Google+, Skype, Flickr. vb. olarak farklı alanlarda hizmet vermektedir. Bu tür siteler genellikle kullanıcı profilleri, kişisel bilgiler, yerleşim yeri, çalışma yeri, aile bilgileri, üyelikleri, alışkanlıkları ve hobileri gibi pek çok detay bilginin profilden takip edilebildiği veri paylaşım siteleridir. Bu kadar geniş kapsamlı paylaşımlar, son yıllarda saldırganların kaçırmayacağı, güvenliğin tehlikeye girdiği bir sosyal mühendislik alanı haline gelmiştir.

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 [3].

III. SOSYAL AĞLARDA GÜVENLİK RİSKLERİ

Sosyal ağlar, bilinmeyen veya çokta farkında olunmayan pek çok yeni tehlikeleri üzerinde barındıran paylaşım siteleridir. Bu yüzden sosyal ağlarda güvenlik önlemlerinin alınması önem arz etmektedir.

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 [4].

eBizMBA Eylül 2015 verilerine göre en sık kullanılan sosyal ağ sitelerine ve aylık ziyaret sayılarına bakıldığında Facebook'un 900 milyon aylık tekil kullanıcı sayısı ile

birinci sırada olduğu, Twitter'ın 310 milyon ile ikinci, LinkedIn'in 255 milyon aylık tekil kullanıcı sayısı ile üçüncü sırada olduğu görülmektedir [5]. Bu yüzden kullanıcıların sosyal ağları günlük internet kullanımında vazgeçilmez bir alışkanlık haline getirmesi, onları çok yönlü tehlike ve tehditlere maruz bırakmıştır.

Sosyal ağlarda kullanıcıların adına sahte hesaplar açılmakta, kimlik taklidi yapılarak; hesapları ele geçirilen kişilerin tüm bilgilerine erişilebilmektedir. Kimlik hırsızlığı, bir kişinin kimlik bilgilerine erişmek ve bu bilgileri sosyal ağda kendi menfaati için kullanmak demektir [5].

Spam, bir liste veya grup e-posta adresine gönderilen genelde reklam içerikli, istenmeyen e-posta anlamına gelir. Aynı şekilde bir saldırgan bu e-postaları bir sosyal ağ aracılığıyla kullanıcılara gönderip, gönderdiği kişinin kullanıcı bilgilerini elde etmeye çalışabilir [6].

Yeni bir sosyal ağa üye olunduğunda; bu ağdaki diğer kişileri bulmak üzere e-posta hesap ve parola bilgilerini girmeniz istenebilir. Bu sayede elde edilebilecek olan e-posta adresleri, gerçek kişileri beyan eden reklam firmalarına satılabilir. Üye olunan sosyal ağ sitesinin tüm e-posta haberleşmenizi tarayabileceği de unutulmamalıdır [7].

Sosyal ağ sitelerinde kullanıcılar evlilik durumlarını, eğitimlerini, adreslerini, kişisel bilgilerini, kişisel resimler gibi önemli bilgilerini paylaşmakta, hatta nerede çalıştıklarını, önceki tüm eğitimlerini, politik görüşlerini ve ilgi alanlarını da paylaşmaktadırlar [8]. Anne kızlık soyadı da pek çok alanda kullanılan gizlilik bilgisidir ancak, bu ortamlara kullanıcının anne ve dayısının dahi katılması bu bilgilerin biliniyor olmasına neden olacaktır [4].

IV. SOSYAL AĞLARDA ALINMASI GEREKEN GÜVENLİK ÖNLEMLERİ

Sosyal ağların kullanımının hayatımızda her geçen gün giderek artması, güvenlik konusunda ciddi önlemler alınmasını gerektirmektedir. Sosyal ağların tamamında kullanım koşullarının teyit edilerek, gizlilik ayarlarının yapılması ve gerekli güvenlik önlemlerinin alınması gerekir.

Sosyal paylaşım ağları bilgi ve bilgisayar güvenliği açısından değerlendirildiğinde; kullanılırken sorumluluk isteyen, konuyla ilgili bilgi birikimi gerektiren, belirli bir kullanıcı bilincine ve disiplinine sahip kişiler tarafından kullanılması gereken, iletişim ve paylaşım ortamlarıdır. Doğru kullanılmadıkları takdirde, kişisel bilgilerin çalınması, istenilmeyen durumlarla karşılaşılması, beklenilmeyen tehdit ve tehlikelere maruz kalınması ve en önemlisi kişisel bilgilerin mahremiyetine zarar verebilecek pek çok olumsuzlukları içinde barındıran ortamlar olabileceği unutulmamalıdır [4].

Cisco'nun 2013 yılı için Yıllık Güvenlik Raporuna göre online siteler arasında en çok güvenlik tehdidi sosyal ağlarda, özellikle de yüksek sayıda kullanıcısı olan sosyal ağlarda meydana gelmiştir [9].

Kimlik taklidine karşı kullanıcıların sosyal ağ şifrelerinin ve sosyal ağlarda vermiş oldukları e-mail şifrelerinin güçlü olması gerekmektedir. Her türlü şifre işlemleri girilirken azami gizlilik sağlanmalıdır. internet kafe, otel ve halka açık erişim yerlerinden üyelik girişi ve şifre işlemi yapılmamalıdır [10].

Sosyal ağ sitelerine üye olunmadan önce gizlilik politikası, kullanım şartları ve özel şartlar okunarak, karşılaşılabilecek tehdit ve tehlikenin farkında olunarak bu ortamlar kullanılmalı, kişisel bilgilerin hangi şartlarla 3. şahıslarla paylaşılacağı bilincine sahip olunmalı ve ona göre karar verilerek üyelik işlemlerine başlanmalıdır [11].

Sosyal ağlara eklenen fotoğraf veya videolar bu hesapları ele geçiren kişiler tarafından, farklı amaçlar için izinsiz kullanılabilmektedir. Bu nedenle sosyal ağlarda fotoğraf ve video paylaşımında da dikkatli olunması gerekmektedir.

Sosyal ağ sitelerini kullanırken, kayıt olmak için şirket alan adı uzantılı e-posta adresi kullanılmamalıdır. Çalışılan kurumun üye olmak istenilen sosyal paylaşım sitesi için kuralları varsa bunlara uyulmalıdır. Profil sayfalarında kurumsal bilgiler paylaşılmamalıdır. Bazı sosyal ağ sitelerinde, bölge, çalışma alanı veya şirket adı gibi gruplaşmalar olmaktadır. Grup içerisine sızmaya çalışan bilişim korsanlarına karşı farkında olunmalıdır [12]

Sosyal ağ sayfalarında veya adres (URL) kısaltması hizmeti veren sitelerde, görünüşte zararlı olmayan, ancak tıklandıktan sonra kötü niyetli olduğu anlaşılabilen adresler yayınlanmaktadır [13]. Sahte sitelere karşı sadece bir e-posta mesajında veya bir web sitesinde yer alan bağlantılar üzerinden tıklanarak ağlara erişmeye çalışılmamalıdır. Mümkünse adres satırına erişmek istediğiniz web sitenin adresi ilgili yere yazılarak veya kopyalanarak web sitesine erişmeye çalışılmalıdır. Bu sayede, sosyal paylaşım sitesi gibi gösterilen tuzak sitelerin farkında olunmalıdır [14].

Verilerin güvenliğini sağlamak, ağ tabanlı saldırıların önüne geçmek ve saldırı anında farkındalık kazanmak için HTTP yerine mutlaka güvenli taşıma protokolü olan HTTPS (Güvenli Zengin Metin Transfer Protokolü) tercih edilmesi gerekmektedir. HTTPS kullanılarak gönderilen bilgiler üç temel koruma katmanı sağlayan taşıma katmanı güvenliği protokolü ile güven altına alınır:

Şifreleme: Alınan ve gönderilen veriler gizlice dinleme yapanlara karşı korumak için şifrelenir. Yani kullanıcı bir web sitesine göz atarken hiç kimse onun iletişimini "dinleyemez", sayfalar arasındaki etkinliklerini takip edemez veya bilgilerini çalamaz.

Veri bütünlüğü: Veriler aktarılırken, fark edilmeden kasıtlı olarak veya başka bir şekilde değiştirilemez ya da bozulamaz.

Kimlik doğrulama: Kullanıcılarınızın kastedilen web sitesiyle iletişim kurduğu doğrulanır. Saldırılarına karşı korur ve kullanıcının güvenini sağlar [15].

Sosyal ağlar konusunda kullanıcıların farkındalıklarının arttırılması ve güvenlik önlemlerinin alınması için;

•Sosyal ağ sitelerine üye olunmadan önce gizlilik politikasından sitenin yayımlanan içeriği izleyip izlemediği öğrenilerek üye olunmalıdır.

•Tehlikelere karşı zaman zaman verilerin yedeklenmesi,

•Kişisel fotoğrafların sosyal ağlara yüklenmemesi ve eğer yüklenildiyse fotoğrafların etiketlenmemesi, kişisel bilgilerin ve iletişim bilgilerinin mümkünse paylaşılmaması,
•Hesabımızda sosyal ağ ayarlarından her türlü gizlilik ayarları yapılarak sınırlamalar getirilmesi ve gizlilik ayarlarının zaman zaman kontrol edilmesi,
•Tanımadığımız kişilerden gelen arkadaşlık tekliflerinin kabul edilmemesi,
•Dahil olduğunuz uygulamaların adımıza reklam ve yayın yapabileceğini düşünerek ayarlardan gerekli sınırlamaların getirilmesi,
•Sosyal ağ hesabımıza zaman zaman kullanıcı adı ile veya farklı bir hesap ile giriş yapılması gerekmektedir.

V. ARAŞTIRMA

A. Araştırmanın Amacı

Bu araştırmanın temel amacı, günümüzde bilgi ve iletişim teknolojilerinin gelişmesiyle ortaya çıkan sosyal ağların kullanımının giderek artması fakat bu konuda toplumun bilgi güvenliği konusunda yeterli farkındalığının olmamasıdır. Bu ortamlarda meydana gelen güvenlik tehditlerinin önemli kişisel ve kurumsal zararlara neden olması dolayısıyla yapılan bu çalışma ile toplumun bilinçlendirilmesi ve farkındalığının arttırılması amaçlanmaktadır.

B. Araştırmanın Yöntemi

Sosyal ağlarda bilgi güvenliği konusunda 33 sorudan oluşan anket formu 234 kişi tarafından cevaplandırılmıştır. Bu anket formu, sosyal ağ sitelerini (Facebook, Twitter, Instagram, Linkedin vb.) kullanım durumlarını, alışkanlıklarını ve sosyal ağlarda güvenlik algısını belirlemeye yönelik genel bir araştırma eğilimi kapsamında hazırlanmıştır. Ayrıca soruların doğruluğunu teyid etmek amacıyla katılımcıların %25'i ile bire bir telefon görüşmesi de yapılmıştır. Ankete ilişkin istatistiksel sonuçlar yorumlanmaya çalışılmıştır.

C. Araştırmada Elde Edilen Bulgular

Kimlik soruları değerlendirildiğinde analiz grubunun% 59'i erkek, % 41'i kadındır. Yaş dağılımı açısından bakıldığında ise % 68'inin 18-25, % 6'sının 26-40 yaş aralığında olduğu ve % 26'sının ise 40 yaş ve üstünde olduğu görülmektedir.

Tablo 1: Cinsiyet Dağılımı

		Frequency	Percent
Valid	Erkek	137	58,5
	Kadın	97	41,5
	Total	234	100,0

Örneklemde eğitim durumuna baktığımızda % 68'i üniversite mezunu yada öğrenci, %20'si yüksek lisans mezunu yada öğrenci, %6'sı doktora mezunu yada öğrenci, %6'sı da lise mezunudur.

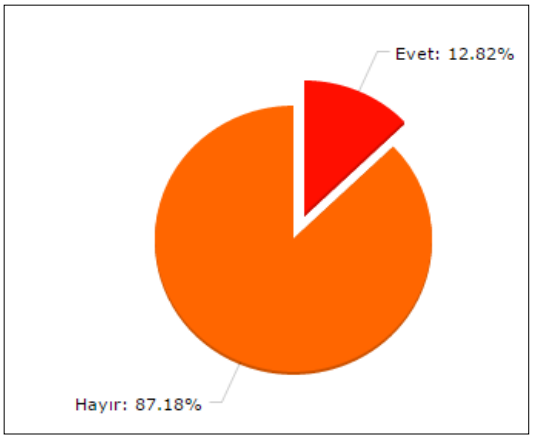
- Sosyal ağ kullanıyor musunuz? Sorusuna 234 katılımcının % 100 gibi oldukça yüksek bir oranının Evet cevabını verdiği görülmektedir. Bu durumda katılımcıların tümünün sosyal ağları kullandığını söyleyebiliriz.
- Sosyal ağları kullanan katılımcıların kullandıkları araçlar sorulduğunda %65'inin akıllı telefon, %51'inin Laptop/Netbook, %27'sinin masaüstü, %18'inin tablet ve %37'sinin hepsini kullandığı belirtilmiştir. Ayrıca katılımcıların sosyal ağ hesaplarını %53 kişisel, %2 kurumsal ve %45 her iki şekilde kullandığı belirtilmiştir.

Tablo 2: Sosyal Ağ Kullanımı

		Frequency	Percent
Valid	Evet	233	99,6
	Hayır	1	0,4
	Total	234	100,0

- Sosyal ağ sitelerine üye olunmadan önce gizlilik politikası, kullanım şartları ve özel şartları okur musunuz? Sorusuna katılımcıların %43'ü Evet, %57'si Hayır demiştir.
- Sosyal ağ hesaplarında kendi isminizi mi kullanırsınız? Sorusuna %96'sı Evet, %4'ü de Hayır demiştir.
- Sosyal ağ hesaplarınızda yazı, resim ve video gibi paylaşımlarınız herkese açık mıdır? Sorusuna %18'i Evet, %82'si de Hayır demiştir.

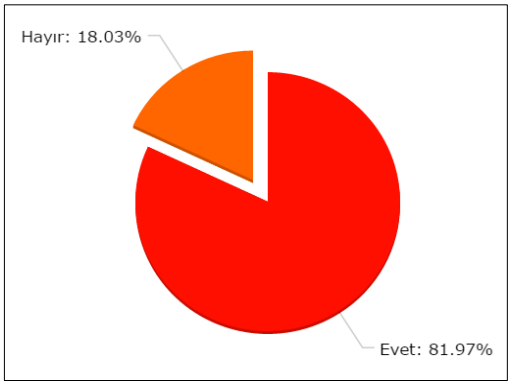
Grafik1. Sosyal Ağların Güvenliği



- Yukarıdaki grafikte görüldüğü gibi, Sosyal ağları güvenli buluyor musunuz? Sorusuna %13'ü Evet, %87'si de Hayır demiştir.

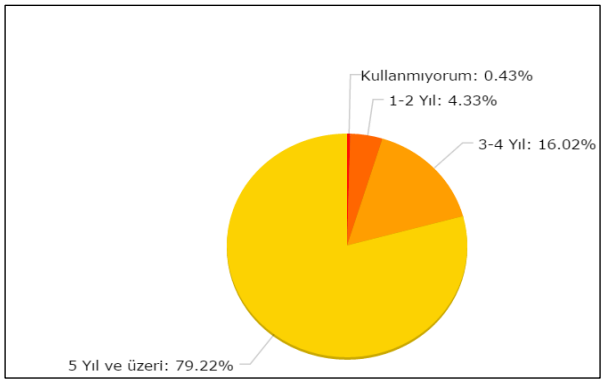
- Sosyal ağı kullandığınız bilgisayarınızda güvenlik programı (antivirüs, antitrojan vb.) bulunuyor mu? Sorusuna %82'si Evet, %18'i Hayır demiştir.

Grafik2. Sosyal Ağ Profilinin Güvenlik Ayarlarını Güncelleme



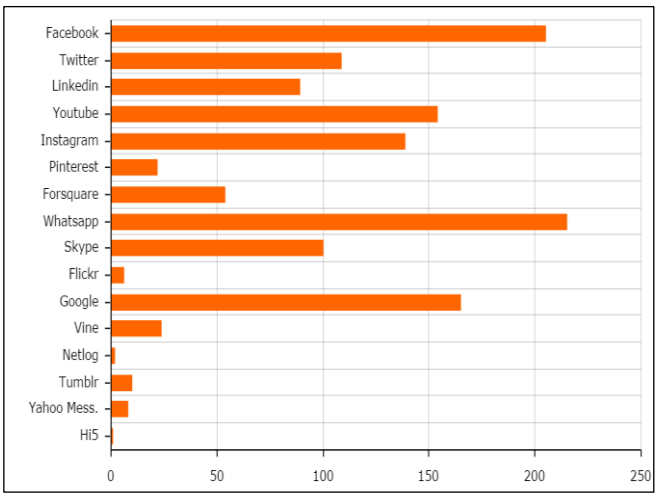
- Yukarıdaki grafikte görüldüğü gibi, Sosyal ağ profilinizin güvenlik ayarlarını güncelliyor musunuz? Sorusuna %82'si Evet, %18'i Hayır demiştir.
- Güncellemenin ise %26'sının her zaman, % 6'sının Kötü niyetli kişilerden zarar gördüğünde, %34'ü yeni güvenlik ayarları öğrenildiğinde, %34'ü sosyal ağ sitesi ayarlarının değiştirilmesi gerektiğine dair uyarı verdiğinde yapıldığı görülmüştür.
- Sosyal ağ kullanırken parolanızın çalınması, bilgisayarınıza virüs bulaşması veya güvenliğinizi tehdit eden herhangi bir olay yaşadınız mı? Sorusuna %27 Evet, %73 Hayır demiştir.
- Sosyal ağ sayfalarında zaman zaman yer alan linklere(URL) tıklar mısınız? Sorusuna % 45 Evet, %55 de Hayır demiştir.
- Sosyal ağ paylaşımları ve ekindeki dosyaları gördüğünüzde ne yaparsınız? Sorusuna %66'sı "Güvenlik nedeniyle seçerek açarım", %32'si "Hiç birisini açmam", %2'si de "Tümünü açarım" cevabını vermiştir.

Grafik3. Sosyal ağların Kullanımı



- Katılımcıların %79'u Sosyal ağları 5 yıl ve üzeri, %16'sının 3-4 yıldır, %4'ünün 1-2 yıldır kullandığını ve %1'inin de kullanmadığını görüyoruz.

Grafik4. En Çok Kullanılan Sosyal ağlar



- Yukarıdaki grafiğe baktığımızda sosyal ağlarda en çok kullanım %93 ile ilk sırada Whatsapp, %89 ile Facebook, %71 Google, %67 Youtube, %60 Instagram, %47 Twitter, %43 Skype, %39 Linkedin, %23 Forsquare ve diğerleri takip etmektedir.
- Gün içerisinde sosyal ağlarda ne kadar zaman geçiriyorsunuz? Sorusuna %40'ı 1 saatten az, %38'i 1-2 saat, %17'si 3-4 saat, %5'i 5 saat ve üzeri zaman geçirdiğini belirtmiştir.
- Sosyal ağlara aşağıdaki araçlardan en çok hangisiyle erişiyorsunuz? Sorusuna %83'ü Akıllı Telefon, %11'i Laptop/Netbook, %4'ü Masaüstü Bilgisayar ve %2'si de Tablet den eriştiğini belirtmiştir.
- Sosyal ağ parolanızı kimlerle paylaşırsınız? Sorusuna %79'u "Hiç kimseyle paylaşmam", %10'u "Diğer (Eşim ve çocuklarımla)", %7'si "Çok güvendiğim arkadaşlarımla", %3'ü "Kız arkadaşımla", %1'i "Babamla ve Annemle"dir.
- Sosyal ağ parolanız çalındığında ne yaparsınız? birden çok seçmeli sorusuna %68'i "Diğer sosyal ağ hesaplarımın şifrelerini hemen değiştiririm", %45'i "Sosyal ağ yöneticisi ile irtibata geçerim", %29'u "Bilgisayarımda casus program taraması yaparım", %8'i "Savcılığa başvururum", %7'si "Polise bildiririm", %5'i de "Bir daha sosyal ağ kullanmam" cevabını vermiştir.
- Sosyal ağ parolanızı hangi sıklıkta değiştiriyorsunuz? Sorusuna katılımcıların %34'ü "Hiç değiştirmem", %30'u "6 ayda bir", %27'si "Yılda bir",
- Hangi amaçla sosyal ağ kullanıyorsunuz? Birden çok seçmeli sorusuna Facebook için cevap veren katılımcıların %80'i "Eski arkadaşlarını bulmak için" kullandığı, %47'si "Duygu ve düşüncelerini paylaşmak", %46'sı "Gruplara üye olarak, sosyalleşmek", %45'i "Çevresindeki insanlar hakkında daha fazla bilgi sahibi olmak", %42'si

"Sohbet etmek", %36'sı "Yeni arkadaşlar edinmek", "Güncel haberleri okumak", %35'i "Yazı paylaşmak", %32 "İlgili konularda bilgi edinmek", %31 "Etkinlik ve duyuruları takip etmek", %29'u "Video izlemek/Paylaşmak", %25'i "Oyun oynamak", %29'u "Mesleği ile ilgili gelişmeleri takip etmek" ve "Arkadaşlarla zaman geçirmek", %25 "Okul duyurularını" ve "Sanatsal Etkinlikleri takip etmek", %21 "Sportif etkinlikleri takip etmek" cevabını vermiştir. Sonuçlara göre, facebook kullananların en çok eski arkadaşlarını bulmak için kullandığı tespit edilmiştir.

VI. SONUÇ VE ÖNERİLER

Bu çalışmada elde ettiğimiz sonuçlara göre;

- Sosyal ağlar konusunda güvenlik farkındalığı arttıkça alacağımız güvenlik önlemleri de artmaktadır. Anket sonuçlarına göre sosyal ağları kullananların yarısının hem kişisel hem de kurumsal hesaplarını sürekli kullandıkları belirlenmiştir. Bu nedenle sosyal ağlarda kişisel ve kurumsal anlamda ilgili kurumlar tarafından eğitimler verilerek toplumda sosyal ağlarda güvenlik farkındalığı arttırılmalıdır.
- Anket katılımcılarının tamamının sosyal ağları kullandığını söyleyebiliriz. Tercih edilen sosyal ağlardan en çok Whatsapp ve Facebook tercih edildiği belirlenmiştir. Sosyal Ağ kullanımında en fazla akıllı telefonlardan bağlanıldığı görülmektedir. Katılımcıların çoğunluğunun, sosyal ağları 5 yıl ve daha fazla yıldır kullandığını da söyleyebiliriz.
- Katılımcıların %53'ünün, sosyal Ağ sitelerine üye olmadan önce gizlilik politikası, kullanım şartları ve özel şartları okumadıkları belirlenmiştir. %47'si ise şartları okuduklarını belirtmişlerdir. Bu kişilerin doğruluğundan emin olmak amacıyla katılımcıların %25 ile birebir telefon görüşmesi yapılarak, doğrulukları teyit edilmiştir. Sanal ortamlarda kullanılan sosyal ağlarda gerekli güvenlik önlemlerinin alınmaması saldırganların bilgilerimize kolayla erişebilmesine olanak sağlayarak, saldırı yapma imkanlarını arttırmaktadır. Bu yüzden de sosyal ağlarda gerekli şartların okunarak, ilgili gizlilik ayarlarının yapılması ve gizlilik ayarlarının sıkça değiştiği göz önüne alınarak takip edilmesi gerekmektedir.
- Katılımcıların çoğunluğu, sosyal ağ hesaplarında yazı, resim ve video gibi paylaşımların herkese açmadıklarını belirtmişlerdir. Katılımcıların %25 ile birebir telefon görüşmesi yapılarak da bu konuda bilgi alınmıştır. Bu sonuca göre katılımcıların bu konuda farkındalıklarının olduğu tespit edilmiştir. Katılımcıların %94'ünün üniversite mezunu veya öğrencisi olduğu dikkate alındığında farkındalığın daha fazla olduğu öngörülebilir.
- Katılımcıların büyük çoğunluğu sosyal ağları güvenli bulmadıklarını belirtmişlerdir. Bu sonuca göre, sosyal ağların katılımcılara güven vermediği söylenebilir.
- Katılımcıların çoğu sosyal ağ kullandığı cihazlarında anti virüs programları kullandıklarını belirtmişlerdir. Kullanılan uygulama yazılımları, işletim sistemi vb. yazılımların zamanında güncellenememesinden dolayı güvenlik zafiyeti oluşmaktadır. Temel güvenlik önlemlerini almak için kullanılan tüm bilgisayar yazılımları güncel tutulmalı, anti-virüs ve güvenlik duvarı yazılımları mutlaka kullanılmalı ve kötücül yazılım ile spam engelleyici filtreler tercih edilmelidir [14]
- Sosyal ağ profilinin güvenlik ayarlarını güncellemenin çoğunlukla yeni güvenlik ayarları öğrenildiğinde ve sosyal ağ sitesi, ayarların değiştirilmesi gerektiğine dair uyarı verdiğinde yapıldığı görülmüştür. Sonuç olarak sosyal ağlarda güvende olmak için her zaman yapılması gereken güncellemelerin katılımcılar tarafından yapılmadığı tespit edilmiştir. Güvenlik için güncellenmelerin düzenli olarak yapılması gerekmektedir.
- Katılımcıların çoğunluğunun sosyal ağ kullanırken parola çalınması, cihazlarına virüs bulaşması veya güvenliklerini tehdit eden herhangi bir olay yaşamadıkları görülmektedir. Arkadaşların e-posta adreslerini vermekten kaçınmak için, sosyal ağ hizmetlerinin e-posta adres defterini taramasına izin vermemek bu uygulamaların dağılmasına engel olacaktır [16].
- Katılımcıların yarısı, sosyal ağ sayfalarında yer alan linklere(URL) tıkladıklarını belirtmişlerdir. Bu sonuca göre katılımcıların güvende olduğunu söyleyemeyiz. Bu linkler çoğunlukla virüs içermekte ve hesabımızı ele geçirmek için saldırganlara fırsat yaratmaktadır. Özellikle bu linkler tıklamamız için reklam içerikli ve cezbedici niteliktedir. Bu yüzden tıklanmamalıdır.
- Katılımcıların büyük çoğunluğu, sosyal ağ paylaşımları ve ekindeki dosyaları güvenlik nedeniyle seçerek açarım demiştir. Normal şartlarda güvenlik dolayısıyla dosyaların tamamının taranarak açılması gerekir.
- Katılımcıların büyük çoğunluğu, sosyal ağ parolalarını hiç kimseyle paylaşmayacağını belirtmiştir. Parolanın tek ve kişiye özel olması ilkesinin benimsenmiş olması güvenlik farkındalığının bir sonucudur. Her bir sosyal ağ hesabında kullanılan parolaların birbirinden farklı olması, art arda gelen

numaralar içermemesi, karakter ve sayı içerecek şekilde kullanılması gerekmektedir.

- Katılımcıların büyük çoğunluğu, sosyal ağ parolaları çalındığında, diğer sosyal ağ hesaplarımın şifrelerini hemen değiştireceğini, katılımcıların yarısı da sosyal ağ yöneticisi ile irtibata geçeceğini belirtmiştir. Katılımcıların güvenli şifreleme konusunda azda olsa farkındalıklarının olduğunu söyleyebiliriz.
- Katılımcıların bir kısmı, sosyal ağ parolasını hiç değiştirmeyeceğini, bir kısmı 6 ayda bir veya yılda bir değiştirebileceğini belirtmiştir. Sonuç olarak, bu konuda farkındalığın olmadığı ve destek verilmesi gerektiği söylenebilir. Sosyal ağlarda güvende olmak için parolaların sıklıkla değiştirilmesi gerekmektedir. Bunun için de parolanın mümkün olduğunca zor ve karmaşık seçilmesi önemlidir. Bilgisayar korsanlarının finansal veya diğer hesaplara girerken sık kullandıkları bir yöntem de hesap giriş sayfasındaki "Parolamı unuttum" bağlantısına tıklatmaktır. Hesabınıza girebilmek için doğum gününüz, oturduğunuz şehir, lisedeki sınıfınız veya annenizin kızlık soyadı gibi güvenlik sorularına verdiğiniz cevaplarınızı ararlar. [16].
- Sonuç olarak, yapılan 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, 2009 yılında ise %30 oranla sosyal ağ sitelerine olduğu görülmektedir [17].
- Bu yüzden ülkemizde son yıllarda önem arz eden sosyal ağlarda güvenlik konusunda sosyal medya, emniyet müdürlükleri (siber suçlar birimi), ilgili kurum ve kuruluşlar ile üniversitelerin, ilgili derneklerin topluma sosyal ağlarda bilgi güvenliği konusunda eğitimler vererek, toplumu bilinçlendirmesi ve farkındalık yaratması gerekmektedir.

KAYNAKLAR

[1] http://www.tuik.gov.tr/ [21 Ağustos 2015 tarihinde erişilmiştir].
[2] KurumsalHaberler, Sosyal Medya Nedir, 2010. Available: http://www.kurumsalhaberler.com/pr/sosyal-medyanedir. aspx . [07 Ağustos 2015 tarihinde erişilmiştir].
[3] D. Hobson, Social networking – not always friendly, Computer Fraud & Security, cilt 2008, no. 2, p. 20, 2008.
[4] 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.
[5] eBizMBA, Top 15 Most Popular Social Networking Sites. Available: http://www.ebizmba.com/articles/social-networkingwebsites [22 Eylül 2015 tarihinde erişilmiştir].
[6] Strighini, G., Kruegel, C., Vigna, G, "Detecting Spammers on Social Networks", ACSAC'10 Austin, Texas, ABD, 6-10, (2010).
[7] Sancho, D., "Security Guide to Social Networks", White- Paper Trend Micro Inc., (2009).
[8] M. Qi ve D. Edgar-Nevill, Social networking searching and privacy issues, Information Security Technical Report, cilt 2011, no. 16, pp. 74-78, 2011.
[9] "Cisco Annual Security Report", (2013). Avaible: http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2013_ASR.pdf [21 Eylül 2015 tarihinde erişilmiştir].
[10] Siber Güvenlik Tehdit Merkezleri Open Web Application Security Project: www.owasp.org / [2012] [19 Ağustos 2015 tarihinde erişilmiştir].
[11] "Facebook Security", Available: http://www.facebook.com/security?v=app_4949752878, 2010 [21 Eylül 2015 tarihinde erişilmiştir].
[12] "A Privacy Paradox: Social Networking in the United States", Available: http://firstmonday.org/ojs/index.php/f%20m/article/view/1394/1312,%20 2010 [20 Eylül 2015 tarihinde erişilmiştir].
[13] Sancho, D., "Security Guide to Social Networks", White-Paper Trend Micro Inc., 2009.
[14] Canbek G., Sağıroğlu Ş., "Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri", ISBN: 975-6355-26-3, Grafiker, Ankara, 2006.
[15] Available: https://support.google.com/webmasters/answer/6073543?hl=t r [22 Eylül 2015 tarihinde erişilmiştir].
[16] Microsoft , Sosyal ağ güvenliği için 11 ipucu, Microsoft, 2015. Available:.http://www.microsoft.com/trtr/security/online-privacy/social-networking.aspx . [21 Ağustos 2015 tarihinde erişilmiştir].
[17]Computer Fraud & Security, Hacking attacks target social networking, ELSEVIER, 2009.