SOSYAL AĞLARDA GÜNCEL GÜVENLİK RİSKLERİ VE KORUNMA YÖNTEMLERİ CURRENT SECURITY RISKS AND PREVENTION METHODS IN SOCIAL NETWORKS

Article · January 2015

CITATIONS
0

READS
1,047

3 authors, including:

Eyup Burak Ceyhan
University of Bartın, Turkey
26 PUBLICATIONS **47** CITATIONS

SEE PROFILE

SOSYAL AĞLARDA GÜNCEL GÜVENLİK RİSKLERİ VE KORUNMA YÖNTEMLERİ

Eyüp Burak CEYHAN[1], Ebru DEMİRYÜREK[1], Büşra KANDEMİR[1]
[1]Gazi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Maltepe, Ankara
ebceyhan@gazi.edu.tr, ebru_demiryurek@hotmail.com, busrakandemir06@gmail.com

ÖZET

Günümüzde birçok sosyal ağ ortaya çıkmıştır ve bu sosyal ağlar genellikle birçok kişi tarafından gerçek kimlikleri ile kullanılmaktadır. Ayrıca, sosyal ağlar sohbet, çevrimiçi oyunlar oynama, dosya paylaşımı gibi farklı amaçlar için aktif şekilde kullanılmaktadır. Sosyal ağlarda güvenliğin sağlanması oldukça önemli ve zor bir problemdir. Bu makalede sosyal ağlar açıklanmış, güvenlik problemleri üzerinde durulmuş ve bu problemlere karşı bireysel ve kurumsal olarak alınabilecek olan güvenlik önlemleri sunulmuştur.

Anahtar Kelimeler: Sosyal Ağ, Sosyal Medya, Risk, Tehdit, Güvenlik, Önlemler

CURRENT SECURITY RISKS AND PREVENTION METHODS IN SOCIAL NETWORKS

ABSTRACT

Nowadays, many social networks have appeared and this social networks are being used with real identities by a lot of people. Besides, social networks are also being used actively for different purposes like chatting, playing online games, and document sharings. Ensuring security in social networks is very important and difficult problem. In this article, social networks are described, it has focused what the security problems are and what the security preventions can be taken individually and institutionally.

Keywords: Social Network, Social Media, Risk, Threat, Security, Prevention

I. GİRİŞ (INTRODUCTION)

Milyonlarca kullanıcıları ile sosyal ağlar, günümüz dünyasının vazgeçilmezi haline gelmiş olup çoğu paylaşımlar, görüşmeler, sohbetler, karşılıklı çevrimiçi oyunlar oynama, yarışma gibi sosyal olayların büyük bir çoğunluğu bu sosyal paylaşım sitelerinde gerçekleştirilmeye başlanmıştır.

Barnes'e göre sosyal ağlar birbirleriyle etkileşimde olan ve kişi için psikolojik öneme sahip bireylerden meydana gelmektedir [1]. Bir başka tanıma göre sosyal ağlar; "bireylerin toplum içerisinde kendilerini tanımlayarak, aynı kültürel seviyede rahatlıkla anlaşabilecekleri insanlarla internet iletişim metotları ile iletişime geçmek ve aynı zamanda normal sosyal yaşamda yapılan çeşitli jestleri simgeleyen sembolik hareketleri göstererek insanların oluşturduğu sanal ortamlarda sosyal iletişim kurmaya yarayan araçlar" olarak tanımlanmaktadır [2]. Ayrıca sosyal ağ siteleri, kullanıcının bilgilerinin bir kısmının diğer kullanıcılara açık olduğu, arkadaşlık istekleri gönderip iletişimde bulunduğu ve çeşitli sosyal medya paylaşımlarının olduğu web tabanlı hizmetleri içerisinde barındırmaktadır [3].

Arayüzlerinin ve üyeliğin kolay ve anlaşılır olması, sosyal ağların birçok kullanıcıya hitap etmesini sağlamaktadır. Günümüzde gerçek kimlikleri ile sosyal ağlarda yer alan birçok kullanıcı bulunmaktadır. Bu sayede sosyal ağ kullanıcısı kendi hayatlarında olup bitenleri, güncel olayları, ilgi alanlarını rahat bir şekilde arkadaşı olduğu birçok insanla paylaşabilir, fikirlerini belirtebilir. Ayrıca video, resim gibi sosyal içerik paylaşımlarında bulunabilir, başkalarının paylaştıklarından haberdar olabilir [4].

Yaşamımızda kullanmaktan keyif aldığımız, eski dostlarımızla haberleştiğimiz ve yeni arkadaşlar

edindiğimiz, gruplar oluşturduğumuz, kendimiz ve fikirlerimiz hakkında paylaşımlar yaptığımız ve çeşitli aktivitelerde bulunduğumuz sosyal ağların bu kazandırdıkları yanında davranışlarımızın analiz edilmesine izin verme, düşmanlarımıza fırsat sunma, tehditler alma, kişisel bilgilerimizi paylaşarak güvenliğimizi tehlikeye atma gibi riskleri de beraberinde barındırmaktadır [2].

Bu çalışmada, sosyal paylaşım sitelerinin kullanım alanları, güvenlik gereksinimleri ve ilgi çekiciliği ile dikkatleri üzerine toplayan bu sosyal paylaşım sitelerinin nekadar güvensiz olduğu, var olan tehditler ve kötücül yazılımlar dikkate alınarak açıklanmıştır. Son olarak da sosyal ağlardaki mevcut sorunlar incelenmiş ve özellikle Türkiye'de bu konuda yapılan çalışmalar özetlenmiş ve gelecekte yapılabilecek çalışmalara ışık tutacak bilgiler verilmiştir.

Bu makalenin 2. Bölümün de sosyal ağların kullanım alanları özetlenmiş, 3. Bölümde sosyal ağlarda alınması gereken güvenlik önlemleri belirtilmiş, 4. Bölümde sosyal ağlarda yeralan güncel güvenlik tehditleri çeşitli örneklerle açıklanmış, 5. Bölümde sosyal ağlardaki mevcut sorunlardan korunma yöntemleri irdelenmiş, 6. Bölümde Türkiye'de internetin güvenli kullanılması için yapılan çalışmalar belirtilerek son bölümde sonuç ve değerlendirmeler sunulmuştur.

II. SOSYAL AĞLARIN KULLANIM ALANLARI (USE OF SOCIAL NETWORKS)

İnternet kullanıcı sayısının artmasıyla sosyal paylaşım siteleri hayatımızın her anına dahil olmuştur ve kullanımı her geçen gün yaygınlaşmaktadır [5]. Facebook, Twitter, YouTube, Linked-in, Google+, Instagram, Flickr, Myspace, Blogger ve Skype sık kullanılan sosyal ağlardır. Bu sosyal ağlar, günümüz insanlarının birbirleriyle iletişim kurma biçimini ve bilgi paylaşımını değiştirmiştir. Sosyal ağ kullanıcılarının buralarda harcadığı zaman çok fazladır. Her kullanıcının katılım amacı farklı olsa da günümüzde genellikle kişinin kendi özel yaşamının başka insanlarla paylaşılması, gündem ve siyasetin takip edilmesi ve bu konuda fikirlerin başka insanlara duyurulması amacıyla kullanılan bir araç olmuştur. Çünkü sosyal ağ ortamları bunları sağlamak için yeni bir olanak haline gelmiştir [6].

Blackey ve Chew'e göre sosyal ağların eğitimde kullanılmasının yüksek öğretimdeki öğrenciler, akademisyenler ve kurumlar açısından faydaları vardır. Araştırmacılara göre öğrenme ve öğretim deneyimlerinde sosyal ağlar iletişim becerilerini, sosyal bağlılığı geliştirir ve bu sayede işbirliğine dayalı öğrenmenin gerçekleşmesini sağlar. Çünkü anlaşılır arayüzü ve kullanıcı dostu olması sebebi ile kolay ve ucuz bir şekilde öğrenciler ve akademisyenler tarafından kullanılmaktadır ve eğitimde yaygınlaşması hızlanmaktadır. Çok basit adımlarla bilgi paylaşılacak gruplar oluşturmak, öğretim deneyimlerini zenginleştirmek, öğrencinin öğrenmesini desteklemek, öğretmenin öğretim ve değerlendirme sürecine yardımcı olmak gibi olumlu özellikleri ile fazlasıyla kolaylıklar sağlamaktadır [7].

Günümüzde sosyal ağlar, ergenler ve yetişkinler tarafından daha sık kullanılmaktadır [8]. Yeni yetişen gençler Myspace, Facebook ve Youtube gibi sosyal ağ sitelerini günlük hayatının bir parçası olarak görmektedir. Özel yaşamlarını paylaşma ve tanımadığı diğer kişilere kendini tanıtma amacıyla sosyal ağları kullanmaktadır [9].

Sosyal ağların en çok bilinenlerinden biri olan Facebook, kullanıcılarının oluşturduğu ağlarda farklı izin seviyelerinde, özel veya herkese açık şekildeki paylaşımlarla kullanıcıların birbiri ile bağlanmasını, gruplara katılmasını ve başkaları ile kaynakların paylaşılmasını sağlayan çevrimiçi sosyal ağ yazılımıdır [10]. Diğer çevrimiçi sosyal ağ sitelerine (Friendster, MySpace gibi) benzer bir biçimde, kullanıcılar kendilerini çevrimiçi bir profilde tanıtır, arkadaş edinir, başkalarının profillerine veya sosyal içeriklerine bilgi veya yorum yazabilir [11].

Twitter etkili bir şekilde güncel olayları ve haberleri öğrenmek, web site adreslerini paylaşmak, anlık düşünceleri paylaşmak, bir olay veya kişiyi takip etmek, dil öğrenmek, başkaları ile tartışmak ve işbirliği sağlamak gibi çeşitli amaçlarla kullanılan bir sosyal ağdır [4].

2003 yılında kurulan Myspace, favori müzik gruplarıyla iletişime geçmek isteyenlerin sıklıkla kullandığı sosyal ağ olarak bilinmektedir [12]. Üyelerin profillerinde fotoğraf, video ve müzik paylaşmasına olanak sağlamaktadır.

Youtube sosyal paylaşım sitesi, video paylaşım sistemine sahiptir. Her çeşit video formatında slaytlar, animasyonlar, fragmanlar, amatör çekimlerin site üyelerine veya siteye ulaşabilen her bireyle paylaşılmasına fırsat sunan alt yapıya sahiptir [13]. Paylaşımlara kullanıcılar yorumlar ekleyebilmektedir.

Yurtdışında yapılan çok sayıda araştırmada, internette kişisel bilgilerini kontrolsüzce paylaşan çocukların yüksek bir oranda olduğu gösterilmiştir. Örneğin, eMarketer'in araştırmasına göre (2007), Amerikalı çocukların %75'inin sunulan ürünlere erişim karşılığında kendi kişisel bilgilerini paylaşmaya hazır olduğu belirtilmiştir. Sosyal ağlar konusunda istatistikler sunan *Zoomsphere*'de (2012), sadece Çek Cumhuriyeti'nde Facebook kullanan çocukların 0-19 yaş aralığında olduğu, 13 Şubat 2012'de Çek Cumhuriyeti'nde toplam Facebook kullanıcı sayısı 3,552,080 iken, sosyal ağda kendi kişisel bilgilerini paylaşan çocuk kullanıcıların sayısının yaklaşık 927,000 olduğu aktarılmıştır. Ayrıca Avustralya'da ACMA (Australian Communications and Media

Authority) tarafından yapılan bir araştırmaya göre 2009 yılında 12533 katılımcının olduğu araştırmada, 18 yaş altındakiler hakkında bir örnek gerçekleştirilmiştir. Rapora göre gerçek hayatta %72,97 çocuk takip edilmiştir. Katılanların %60,22'si adı ve soyadını, %63,19'u e-posta adreslerini ve %22,8'i telefon numaralarını paylaşmıştır [14].

Bu kadar ilgi çeken sosyal ağlar günümüz toplumunda birçok farklı amaçlar için kullanılmaktadır. Yeni yetişen gençliği etkilemektedir, bazı alışkanlıklarını değiştirmektedir ve değiştirmeye de devam edecektir [4]. Bahsedilen araştırmalara göre de özellikle ailelerinin kontrol etmediği küçük çocukların bilgilerini düşünmeden tehlikeli insanlarla paylaşmaları, onların sosyal ağlardan kötü etkilenmesine sebep olabilmektedir.

III. SOSYAL AĞIN GÜVENLİK GEREKSİNİMLERİ (SECURITY REQUIREMENTS OF SOCIAL NETWORKS)

Sosyal ağ siteleri, birçok kişi tarafından kullanılmakta olup özellikle de genç insanlar tarafından kullanılmaktadır [15]. İnsanlara yarar sağladığı gibi bazı zararları da olmaktadır. Kullanıcının, bilgilerini kötü amaç için kullanacak kişi ya da kişilerden korunması gerekmektedir. Bu amaçla;

- Bilgiler istenmeyen kişilerden gizlenmelidir. Mahremiyetin internet üzerinden korunması hiç de kolay değildir. Internet'te gezinirken; yapılan tüm alışverişler veya gönderilen tüm e-postalar üçüncü şahıslar tarafından izlenebilmektedir. İnsanlar sosyal ağlarda fotoğraflarını, yediğini içtiğini, hatta özel hayatlarına ilişkin bilgileri de paylaşmaktadır. Kimi zaman bunu farkında olmadan, kimi zamanda kendini başkalarına ne kadar sosyal olduğunu göstermek amacıyla yapmaktadır. Bu bilgiler kötü düşünceli kişilerin eline geçtiğinde, farklı amaçlar için kullanılabilmektedir. Facebook'ta bir sayfayı beğendiğinizde hemen onunla ilgili başka bir sayfa önerilebilmektedir. Hatta yanda çıkan reklamlar bile sizin bilgilerinize bağlantılı olarak seçilip yayınlanmaktadır. Bu durumdan kurtulmak imkânsız gibidir, çünkü bilgilerinizi silseniz hatta hesaplarınızı kapatsanız bile veritabanından verileriniz silinmemektedir. Böyle bir ortamda güvenlik ve mahremiyet ile ilgili çözümler her geçen gün daha da önem kazanmaktadır [16].
- Bilginin kimliği belirsiz kişilerce değiştirilmemesi gerekmektedir. Veriler iletişim sırasında değiştirilmemeli ve üçüncü kişilerce verilerin bütünlüğü bozulmamalıdır [17].
- Bilgilere ulaşmasında olumsuz durumlara neden olmayacak kişilerin, bilgilere erişiminin sağlanması gerekmektedir [17].
- Kullanıcılar arası ilişkilerin, üçüncü şahıslarca erişilememesinin sağlanması gerekmektedir. Sosyal ağlar verdikleri hizmet karşılığı ücret almazlar ama kullanıcıların bilgilerinin gizli tutulmadığı bir gerçektir [18]. Aynı zamanda mahremiyet durumu ortadan kalkmış olur.
- Ağ operatörlerince kullanıcı bilgilerine erişim engellenmiyor olabilir. Kullanıcının gizliliği için IP adresine ve mesajlarına erişilmemesi gerekir.

Örneğin, Facebook'a haberleşme gizliliğini ihlal ederek reklamların daha kişiselleştirilmesi adına kullanıcıların özel mesajlarını izlediği gerekçesiyle dava açılmıştır. Matthew Campbell ve Michael Hurley tarafından Amerika Birleşik Devletleri Yerel Mahkemesi'nde dosyalanan davaya göre Facebook kullanıcı veri ve profili çıkarmak üzere, sistematik olarak mesajlara müdahale etmekte; kullanıcıların haberleri olmadan URL'leri taramakta ve bu bilgileri reklam şirketleri ve pazarlamacılarla paylaşmaktadır. Yani Facebook, kullanıcıların reklamlarla daha çok ilgilenmesi için kullanıcıların özel mesajlarını incelemektedir [19].

IV. SOSYAL AĞLARDA GÜNCEL GÜVENLİK TEHDİTLERİ (RECENT SECURITY THREATS IN SOCIAL NETWORKS)

2013 yılı için Cisco Yıllık Güvenlik Raporu'na [20] göre online siteler arasında güvenlik tehdidi en çok sosyal ağlarda meydana geldiği belirtilmiştir. Sosyal ağların kullanımının artmasıyla riskler de artmıştır.

Sosyal ağlardaki güvenlik açıklıklarının temel nedenleri; bu ağların kuruluş amaçları nedeniyle, mahremiyetin korunmaması ve kullanıcıların kişisel bilgilerini paylaşarak kendilerini bu ortamda hedef haline getirmeleridir [2].

Kullanıcılar sosyal ağ sitelerinde kişisel bilgilerini, eğitim durumlarını, evlilik durumlarını, kişisel resimlerini ve hatta nerede çalıştıklarını da paylaşmaktadırlar [21]. Ayrıca pek çok yerde anne kızlık soyadı da kullanıcının adresinin çalınmasını zorlaştırma olarak görülse de gizlilik bilgisidir ve ileride aile bilgilerinin bulunabileceği anlamına gelmektedir [2]. Bu bilgiler verilirken bu sayfaları kimlerin görebileceğininde düşünülmesi gerekmektedir [22].

Sosyal ağlarda pek çok zararlı uygulama vardır. Sosyal ağlar ücretsiz reklam ortamlarını da kullandıklarından dolayı bu sayfalar pornografik içeriklere yönlendirilebilmektedir [23].

Sosyal ağlardaki güncel güvenlik tehditleri alt başlıklarda sunulmuştur.

1. Kimlik Hırsızlığı (Identity Theft)

Kimlik hırsızlığı, istenmeyen kişilerin bilgilere ulaşması ve bu kişilerin bilgileri kötü amaçları doğrultusunda kullanmasıdır. Kimlik hırsızlığı bugün olduğu gibi geçmişte de vardı. Hırsızlar her zaman

posta kutularından postaları çalma veya çöp kutularını arama gibi yollarla insanların kişisel bilgilerini temin etmenin yollarını aramışlardır. Kullanıcıların sosyal ağlardaki paylaşımları hırsızların işlerini daha da kolaylaştırmaktadır. Bazı saldırganlar da kullanıcıdan izin isteyen uygulamalar ile saldırı yapmaktadır. Kullanıcı, kendi bilgilerine erişilebilmesi izni verdiğinde, saldırgan kullanıcının bilgilerine erişebilmekte ve kötüye kullanabilmektedir. Kimlik hırsızlığında genellikle kullanıcı şifresini ve bireylerin banka hesap bilgilerini çalma hedeflenmektedir. Kimlik hırsızlığında aktif olarak kullanılan yöntemler oltalama ve zararlı yazılımlardır. Oltalama yönteminde dolandırıcılar sahte e-posta göndererek kişileri sahte web sitesine yönlendirir ve kullanıcı bilgilerinin girilmesi durumunda bütün bu bilgiler dolandırıcıların eline geçmiş olur. Bu e-postanın sahte olduğunun anlaşılması da oldukça zordur. Çünkü kuruluşun simgesi ve web sayfasının kopyası kullanılabilmektedir. Diğer bir yöntemde zararlı programların, kullanıcının dikkatini çekmek için isminin değiştirilip bilgisayara indirilmesi sağlanarak yapılmaktadır [24]. Kimlik hırsızlığı ile suçlular daha fazla sayıda insana daha kolay ulaşabildiğinden, sosyal ağlar dolandırıcılar için daha uygun bir hale gelmiştir [25].

2. E-Dolandırıcılık

Başka bir kullanıcının şifresini izinsiz kullanma ve banka hesap bilgilerini çalma gibi teknikler e-dolandırıcılık yöntemleri kapsamındadır. Bu yöntemlerle dolandırıcılar, kullanıcı bilgilerini elde etmek için yasal bir siteden posta gönderiyormuş gibi yaparlar. Kullanıcı ilgili linki tıkladığında bilgilerinin çalınacağı sayfaya yönlendirilmiş olur. Bazı popüler e-dolandırıcılıklar da şunlardır [26].

3. İyi Bilinen Şirketlerin Adlarını Kullanma

Bu yöntemde ünlü firmaların adını kullanan sahte e-posta iletileri veya web siteleri kullanılır. E-posta mesajında, bir yarışmanın kazanıldığı ve oturum açma bilgileri veya parolaya ihtiyaç olduğu söylenir. Bu sahte teknik destek dolandırıcılıkları genelde telefonla yapılır [26].

4. Piyango Dolandırıcılıkları

Sosyal ağ kullanıcısına piyango kazandığına dair bir mail gelir. Aslında böyle bir piyango yoktur ve bu mail siber suçlular tarafından gönderilmiştir. Bu e-postalar, kişiyi kendilerine para göndermeye ikna etmek ve kişiyle iletişim kurmak amacıyla hazırlanmıştır.

Farklı sebeplerle para koparmak için kişiyle iletişime tekrar geçmeye çalışırlar. Kurgusal nitelikteki ödülü almak içinde bazı masraf ücretleri talep edilir. Suçlular bu konularda çok üretkendir. Örneğin, e-posta iletilerine inanılması için şirketin gerçek logoları kullanılır [26]. Şirketin gerçek web adresine veya eposta adresine çok yakın web adresi ve mail adresi de kullanılmaktadır.

5. Sahte Güvenlik Yazılımı Dolandırıcılıkları

"Korkutma amaçlı yazılımlar" olarak da bilinen sahte güvenlik yazılımları, güvenlik açısından yararlı gibi görünse de sınırlı veya sıfır güvenlik sağlayan yazılımlardır. Bu dolandırıcılıklar ile sosyal ağ sitelerinde, reklamlarda, arama motoru sonuçlarında veya bilgisayarda açılan pencereler şeklinde karşılaşılabilir. İşletim sisteminin bir parçası gibi görünebilirler, fakat gerçekte zararlı yazılımlardır [27].

6. Profil Klonlama

Bu saldırı yöntemi sosyal ağ sitelerinde oldukça sık kullanılır çünkü profil klonlamayla ilgili güvenlik önlemi neredeyse hiç yoktur [28]. Bu suç tipinde kullanıcının profil resmi kopyalanır aynı isim ve soyisim ile profil oluşturulur. Oluşturulan bu profil sayfasına pornografik resimler koyma ve cep telefon numarası yazarak cinsel konularda görüşme talebinde bulunma gibi durumlarla karşılaşılmaktadır.

Saldırgan ilgili kişinin profilinin aynısını oluşturur ve genelde profilini çaldığı bu kişinin itibarını zedelemeyi hedefler. Facebook kullanıcılarının resimlerini ve kişisel bilgilerini sınırlandırmaları bu gibi durumlardan korunmalarını sağlayacaktır [29].

7. Üçüncü-Kişi Uygulama Tehlikeleri

Saldırgan, kullanıcı bilgilerine ulaşmak için oyunlar gibi sosyal ağ uygulamalarını kullanır. Bu sayede kullanıcı, sahte uygulamayı kullanarak bilgilerinin saldırgan tarafından ele geçirilebilmesine sebep olmaktadır [30].

8. Sahte Ürün Satışı

Saldırgan, dikkat çeken indirimler ile süslenen çok satan bir ürünün reklamlarını sosyal ağ ortamlarına koyar. Sattığını iddia ettiği ürünün alınabilmesi için kullanıcıdan kullanıcı bilgileri ve banka şifreleri gibi kişisel bilgilerini ister. Eğer kullanıcı ürünü almak için kişisel bilgilerini verirse, saldırgan bu bilgileri elde eder ve amacı doğrultusunda kullanır [30].

9. Kötü Bağlantı İstekleri

Dolandırıcılar, sahte profil oluştururlar ve hedef kullanıcıların onlarla iletişime geçmesi için arkadaşlık istekleri gönderirler. Kullanıcı gelen arkadaşlık isteğini kabul ederse, diğer arkadaşlarıyla paylaştığı bilgileri dolandırıcıların da görmesine neden olur. Bu şekilde dolandırıcılar kullanıcının bilgilerini kötü amaçlı kullanabilirler [31].

10. İstenmeyen Epostalar

İstenmeyen epostalar, kişinin isteği olmadan kişiye gelen reklam içerikli maillerdir. Internet üzerinde aynı mesajın, bu mesajı alma talebinde bulunmamış kişilere toplu olarak gönderilmesi de genelde istenmeyen epostalar olarak adlandırılır.

İstenmeyen epostalar genellikle ticari reklam niteliğinde olup, güvenilmeyen ürünlerden fazla para kazanma amacına yöneliktir. Internet kullanıcıları üzerindeki etkileri incelendiğinde iki tip istenmeyen eposta vardır. E-maille gönderilen istenmeyen eposta bireysel kullanıcıları hedef alır.

Eposta gönderilen kişiler genellikle sosyal ağ sitelerinde aktif olan ve forumlara üye olan kişilerin listelerinin çalınmasıyla oluşturulur. İkinci istenmeyen eposta türü ise ticari amaç dışında gerekmeden bir çok kişiye aynı anda yollanan maillerdir.Bu epostalar belli bir konu üzerinde kamuoyu oluşturmak amacıyla da yollanabilmektedir [32].

11. Düzenbaz Site Kodlamaları

Bu yöntemle kullanıcı webde gezinirken kullanıcının haberi olmadan zararlı yazılım çalıştırılır ve bu sayede kullanıcı bilgileri elde edilmeye çalışılır [33].

V. SOSYAL AĞLARDAKİ MEVCUT SORUNLARDAN KORUNMA YÖNTEMLERİ (DEFENCE MECHANISMS FOR SOCIAL NETWORKS)

Sosyal ağ kullanıcıları her geçen gün artmaktadır ve bu siteler hayatımızda önemli bir yer edinmiştir. Sosyal ağları; hackerlar, siber mühendisler ve spam gönderenler bilgi toplama amacıyla hedef edinmişlerdir [34]. Bu sebeple sosyal ağlarda alınması gereken önlemlerin bilinmesi gerekmektedir. Ayrıca ailelerin, eğitim kurumlarının ve devlet birimlerinin bu sorunlardan korunmak için ortaklaşa çalışması gerekmektedir.

Öncelikle kullanılacak sosyal ağ dikkatlice seçilmelidir. Üye olmadan önce gizlilik politikası, kullanım şartları ve özel şartlar okunmalı, kişisel bilgilerin hangi şartlarla 3. şahıslarla paylaşılacağı bilincine sahip olunmalı ve ona göre karar verilerek üyelik işlemlerine başlanmalıdır [2]. Sitenin insanların yayınladıkları içerikleri izleyip izlemediği öğrenilmelidir. Bu web sitesine kişisel bilgiler verileceğinden, kredi kartı bilgilerinin girildiği bir siteyi seçerken gösterilen hassasiyetin aynısı gösterilmelidir [35].

Çocuk kullanıcılar için en önemli görev ailelerine düşmektedir. İlk olarak aileler çocukları olabildiğince bu ortamlardan uzak tutmalıdır. Bu mümkün olmadığı zamanlarda ise dikkatli olmaları için uyarılarda bulunulmalı, güvenli kullanmaları konusunda eğitilmelidirler. Bunun için ebeveynin çocukla yüz yüze iletişim kurması gerekmektedir. Çocukların bu ağlar hakkındaki deneyimleri öğrenilmeli, çocuğun durumuna göre bilgilendirme yapılmalıdır. Sosyal ağda çocukların gerçek adlarını kullanmadığından, adres, telefon, okul, sınıf ve kimlik bilgileri gibi bilgileri paylaşmadığından emin olunmalıdır. Çocuklar kontrol edilmeli, verilmiş olan önemli bilgiler varsa düzeltilmelidir. Fotoğraflarda detay verilmemesi, fotoğraf etiketlemelerinden kaçınılması, kişisel resimlerin paylaşılmaması ve tanımadıkları kişilerle haberleşmemeleri konusunda kesinlikle uyarılarda bulunulmalıdır [35].

E-posta adresleri kişilerin geçmişleri hakkında bilgiler içermemelidir. Adres belirli bir üniversitenin hangi bölümünde okunduğunu veya hangi şirkette çalışıldığını göstermemelidir. E-posta adresleri; kişinin soyadı ve adı gibi özel bilgiler içermemelidir [34].

Paylaşılması risk içeren bilgi varlıklarından bazıları şunlardır [36].

- E-devlet bilgileri
- İşyeri ve konum bilgileri
- Nüfuz cüzdan bilgileri
- Sağlık güvenlik bilgileri
- Ehliyet, pasaport bilgileri
- İnteraktif banka hesap bilgileri
- Kredi kart bilgileri
- Kurum ve maaş bilgileri
- Her türlü kullanıcı adı ve şifre bilgileri

Bu bilgilere ek olarak anlık konum bilgisi, kullanıcıya ve yakın çevresine ait fotoğraflar, eğitim bilgileri ve özel hayata ilişkin bilgiler de paylaşılmamalıdır.

Bu gibi bilgilerin paylaşılmadığından emin olunmalıdır. Bilgi içeren adresler kullanmaktan kaçınılmalı ve içinde büyük küçük harf, rakam, özel karakterler içeren güçlü şifreler tercih edilmelidir [2]. İnterneti kullanırken kullanıcılar zaman zaman ekran kilitlenmesiyle karşılaşabilirler ve bu yüksek ihtimalle virüs olduğunu gösterir. Herhangi bir mağduriyetin yaşanmaması için kişilerin bilgisayarlarını virüsten kurtarmaları ve her ihtimale karşı bilgisayarlarını yeniden kurmaları önerilir [29].

Sosyal ağlardaki riskleri en aza indiren esas yöntemleri dört maddede toparlayabiliriz.

1. Sadece yayınlanması istenilen bilgiler paylaşılmalıdır [37].

Bir sosyal ağ sitesine koyulan her bilginin kalıcı olacağı varsayılmalıdır. Hesap silinebilse bile arama motorları tarafından taranan bilgilere erişimin olması riski sebebiyle internetteki herhangi biri, fotoğrafları

veya yazıları kolayca bastırabilir veya görüntüleri ve videoları bir bilgisayara kaydedebilir [35]. Bu yüzden sadece genel olduğu düşünülen önemsiz bilgiler paylaşılmalı veya yayımlanmalıdır [2]. Kimlik bilgilerinin detayına hiçbir zaman inilmemeli ve küçük değişiklikler yapılarak paylaşılmalıdır [34].

2. Sadece güvenilen kişiler arkadaş listesine eklenmelidir [37].

Sosyal ağda arkadaş olarak eklenenlerin kim olduklarından emin ve seçici olunmalıdır. Bilgi almak için kimlik hırsızları ve sahtekarlar sahte profiller oluşturabilir. Sosyal ağın kişinin arkadaşlarına ait e-posta adreslerine ulaşması için e-posta adres defterini taramasına izin verilmemelidir [2].

3. Asla tam olarak hiç kimseye güvenilmemelidir. Tanınmayan kişilerden gelen beklenmedik bağlantıları tıklamaktan kaçınılmalıdır [37].

Sosyal ağlarda arkadaşlardan gelen mesajlarda dikkatli olunmalıdır. Mesajlarda bulunan bağlantılar hemen tıklanmamalıdır. Bu sitelerdeki mesajlarda yer alan bağlantılara tıklamada, e-posta mesajlarındaki bağlantılardan nasıl şüphelenip dikkatli olunuyorsa öyle davranılmalıdır [35].

4. Sosyal ağın adı doğrudan tarayıcıya yazılmalı veya kişisel sık kullanılanlar listesi kullanılarak giriş yapılmalıdır. Bu işlem daha güvenilirdir. Tıklanan herhangi bir bağlantının, kişisel bilgileri çalmak için düzenlenen sahte bir link olabileceği ve bunun bir casus veya kötücül yazılımı tetikleyebileceği unutulmamalıdır [35].

Son aylarda ihlal edilen açıklıkların başında gelmektedir. Bunu önlemek veya bu tazağa düşmemek için mutlaka daha dikkatli olunmalı, tıklanacak linklerin bağlantılarına bakılarak gerekli işlem tamamlanmalıdır.

VI. TÜRKİYE'DE İNTERNETİN GÜVENLİ KULLANIMI İLE İLGİLİ YAPILAN ÇALIŞMALAR (STUDIES IN TURKEY TO USE INTERNET SECURELY)

İnternetin yaygın olarak kullanılmaya başlanmasıyla birlikte güvenli internet kullanımıyla ilgili çalışmalar yapılmaya başlanmıştır [38].

Avrupa Birliği Komisyonu internet ortamındaki güvenlik risklerine karşı "Güvenli İnternet Programı" başlatmıştır. Türkiye'de 2013 yılında Güvenli İnternet Günü'nün dördüncüsü gerçekleştirilmiştir. Türkiye'nin Güvenli İnternet Programı'na katılımı henüz gerçekleşmediğinden Türkiye'de şu an bir Güvenli İnternet Merkezi veya Yardım Hattı bulunmamaktadır [39].

İnternet servis sağlayıcıları başka ülkelerden temin edildiği için "hosting" hizmetinin Türkiye'ye getirilmesiyle ilgili Türk Telekom ile çalışmalar yapılmakta olup servis sağlayıcıların ülkemizde de olması sağlanacaktır [40].

İnternet kullanıcılarının çevrimiçi ortamda bilgilerinin korunması amacıyla TÜBİTAK tarafından "Bilgi Güvenliği" ve "Bilgimi Koruyorum" portalları hizmete açılmıştır. Bilgi Güvenliği portalında bilgilendirici rehberler ve bilgi güvenliğini sağlayacak uyarılar yayınlanmaktadır [39].

Türkiye'de internetin bilinçli, güvenli ve etkin kullanımına ilişkin yapılan en önemli çalışmalardan biri Telekomünikasyon İletişim Başkanlığı (TİB) bünyesinde yürütülen çalışmalardır. TİB şimdiye kadar, Türkiye'nin birçok noktasında eğitim semineri vermiştir. TİB bilinçlendirme amaçlı kitapçık, broşür ve benzeri çalışmalar yapmakta ve aynı zamanda internetin güvenli kullanımına özgü yayın yapan ilk internet sitesi "Güvenli Web" ve çocuklar için de "Güvenli Çocuk" web portallarını hizmete açmıştır [39].

ICANN tarafından yapılan düzenlemeyle alan adları yönetimlerinin ülkelere bırakıldığı, 23 olan üst alan adı dışında, başka alan adlarının kullanılmasına da izin verilecektir. Fiber alt yapısının geliştirilmesi için de çalışmalar yapılmaktadır [40].

Çocukların cinsel istismarına sebep olan internet yayınlarının kontrol edilebilmesi amacıyla yurt içi ve yurt dışından kanun uygulayıcı birimlerle sürekli irtibat halinde bulunulmaktadır. Bu çalışmalar sonucunda Bilgi teknolojileri ve İletişim Kurumu Telekomünikasyon İletişim Başkanlığı'nın yoğun çalışmaları ile Türkiye, Uluslararası İnternet Bilgi İhbar Merkezleri Birliği'ne üye olmuştur. İnsanlar internet ortamında işlenen suçları Türkiye'de kurulan İhbar Merkezi'ne web üzerinden şikayet edebilmektedir. Çevrimiçi ortamda kişi hakkının ihlal edildiğini düşünen kullanıcı bireysel başvuru hakkını kullanarak yer sağlayıcıya ulaşabilmekte, ayrıca sonuç alamadığı takdirde Sulh Ceza Mahkemeleri'ne başvuruda bulunabilmektedirler [39].

Ülkemizde çocuk pornografisine ilişkin suçlar TCK'nın Müstehcenlik başlığı altında tanımlanmıştır. Buna rağmen bu konuda bazı eksiklikler bulunmaktadır. Eksikliklerin başında da, çocuk pornografisinin bir tanımının yapılmamış olması gelmektedir. Teknolojinin gelişimiyle de yetişkinlerin çocuk gibi gösterilmesi oldukça basit bir hal almıştır. Ayrıca bu tür görüntüleri bilgisayarda yaymak da kolay olduğundan özel hükümler gerekmektedir ve bu alanda önemli eksiklikler vardır [30].

Ülke özelinde dünyaya örnek bir model olabilecek şekilde düzenlenen "Notice and Takedown" dünyanın uygulamak için aradığı yöntemdir. Bu yöntemde,

5651 sayılı yasa kapsamında suç unsuru taşıyan içeriklerin kaldırılması için ilgili internet siteleriyle irtibata geçilmekte, böylelikle sakıncalı içeriklerin kaldırılması sağlanırken sitelere erişimin tamamen engellenmesinin önüne geçilmektedir [39].

Türkiye'deki çocuk ve gençlerin internet ortamında zararlı içeriklere maruz kalmaması için TİB, internet sağlayıcıları ile yaptıkları çalışmalar sonucunda servis sunucuları tarafından içerik filtreleme servisi sunulmaya başlanmıştır [39].

Türkiye'de sivil insanların yapılan çalışmalarda olmaması ve sorunların ele alınamaması, internetin güvenli kullanılmasına ilişkin etkili videoların bulunmaması önemli eksikliktir. Ülkemizde güvenli internet filmi olmasıyla birlikte, güvenli internet kullanımıyla ilgili seminerlerde verilmektedir [39]. İnternet kullanımında yaşanan olumsuzlukların önüne geçilmesi ve vatandaşların bilgilendirilmesi amacıyla kurulan Güvenli İnternet Çağrı Merkezi uygulaması, Türkiye'de ilk kez Erzincan'da 2011 yılında hayata geçirilmiştir [31].

Siber alan dünyanın herhangi bir yerinden gelebilecek saldırılara açıktır ve bu saldırıları yapanın belli olmaması ve bunu ispat edecek kanıtların olmaması siber güvenliği sağlamayı da zorlaştırmaktadır [41].

Teknolojideki gelişmeler hem heyecan vermekte hem de kaygı vermektedir. Özellikle son yıllarda artış göstermekte olan müstehcenlik, çocukların cinsel istismarı ve fuhuş gibi suçlar nedeniyle Bilgi Teknolojileri ve İletişim Kurumu'na ihbarlar gelmektedir. Bu nedenle internetin çocuklar için güvenle kullanımı için ailelerin önlem alması gerekmektedir. BTK tarafından taslağı hazırlanan güvenli internet paketi; hem bilgisayarda hem de cep telefonlarında kullanıcıların internette olumsuz veya zararlı içerikle karşılaşmalarının önüne geçme amacıyla ücretsiz olarak Kasım 2011'den itibaren kullanılmaya başlanmıştır. Bu hizmeti kullanmak zorunlu olmamakla kullanılmak istendiğinde operatör ile irtibata geçip aile veya çocuk paketi alınabilmektedir [43].

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı siber saldırıları önleme ve müdahale etme konusunda adımlar atmıştır. Bakanlık siber saldırılara karşı alınacak önlem ve altyapı geliştirmelerini içeren Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı yayınlamıştır. Ulusal Siber Güvenlik Stratejisi 2013-2014 Eylem Planı'nda büyük kitlelere sunulan kritik hizmetlerin çoğunun yapısının internete dayalı olması ve siber güvenliğe yönelik çalışma ve soruşturmaların yetersiz olması, kurumların siber güvenlik konusunda nitelikli çalışanlarının olmaması ve ülkenin yerli üretiminin yeterli olmaması Türkiye'nin siber güvenlik politikalarında göz önünde bulundurulması gereken etkenlerdir. Eylem Planı'nda; ulusal siber güvenliğin sağlanması konusunda eksiklikleri giderecek mevzuat oluşturulması ve diğer ilgili mevzuatlarda düzenlemeler yapılması, siber saldırı kaynağının tespiti ve saldırının etkilerinin belirlenebilmesi için güvenilir kayıt mekanizmalarının ve USOM'un koordinasyonunda çalışacak sektörel ve kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) oluşturulması, tüm kurumlardaki bilişim sistemlerinde siber güvenlik altyapısının güçlendirilmesi ve gerekli teknolojinin sağlanması, siber güvenlik alanında insan kaynağının yetiştirilmesi ve bilinçlendirme faaliyetlerinin yapılması, siber güvenlikte yerli teknolojilerin geliştirilmesi ve ulusal güvenlikten sorumlu kurumların siber güvenlik konusunda çalışma ve savunma kapsamlarının genişletilmesi hedeflenmiştir [41].

VII. SONUÇLAR VE DEĞERLENDİRMELER (CONCLUSIONS AND EVALUATIONS)

Bu çalışma ile sosyal ağların kullanım amaçlarına değinilmiş, güvenlik gereksinimleri açıklanmış, sosyal ağlardaki güncel güvenlik riskleri açıklanarak örneklendirilmiş ve mevcut sorunlardan korunma yöntemleri anlatılmıştır. Bu konuda ülkemizde yapılan çalışmalara da yer verilmiştir.

İnternetin her kesime ulaşabiliyor olması kullanıcı sayısını artırmakla birlikte internete olan bağımlılığı da artırmaktadır. İnternetin yaygınlaşması sosyal ağları hayatın bir parçası haline getirmiştir. Günlük yaşama dahil olan sosyal ağlar bir çok amaç için kullanılmaktadır. Sosyal ağların kullanıcılara birçok fayda sağladığı açıktır.

İnternetin kullanım alanlarının artmasıyla sosyal ağların güvenlik sorunları ve tehlikeli yanları ortaya çıkmıştır. Bu yüzden sosyal ortamlar dikkatli seçilmeli ve dikkatle kullanılmalıdır. Doğru kullanılmadıkları takdirde, kişisel bilgilerin çalınmasına, istenmeyen durumlarla karşılaşılmasına, beklenmeyen tehdit ve tehlikelere maruz kalınmasına neden olabileceği unutulmamalıdır.

İnternet aracılığıyla işlenen suçlarla mücadeleye yönelik çalışmalar olsa da yeterli değildir. Kişisel önlemler almak nekadar kolay ve yeterli değilse, hukuki altyapıda da bir o kadar eksikler vardır ve etkin bir mücadele sürdürülmesi için düzenlemeler yapılmalıdır. Çocuk ve gençlerin internet ortamında zararlı içeriklere maruz kalmaması için önlemler alınması gerekmektedir. Çocuklar ebeveynlerin kullanım alışkanlıklarından dolayı çocuk yaşlarda sosyal ağları kullanmakta ve tehlikelerle karşılaşmaktadır. Oyunlara olan bağımlılıkları kişisel verilerinin kolayca elde edilmesine yol açmaktadır. Kimi zaman sosyal ağlarda arkadaşlarına "sosyalim" görüntüsü vermeye çalıştıklarından gittikleri, yedikleri, yaptıkları aktiviteleri paylaşmakta ve istenmeyen kişilerin eline bilgilerin geçmesine neden olunmaktadır.

Tehditlerin önlenmesi oldukça zor olsa da çocukları bilgilendirmek önem arz etmektedir ve ailelerin bu konuda çok dikkatli olması gerekmektedir. Çocuk kullanıcılar için asıl görev ailelerine düşmektedir. Aileler çocuklarının anlayacağı bir üslup ile onlara öğütler vermeli ve yardımcı olmalıdır.

Ülkemizde teknolojik gelişmelerin yeterince gelişmemiş olmasından dolayı bilgisayarların ve işletim sistemlerinin dışarıdan ithal edilmesi ve kullanılan sosyal ağların yabancılar tarafından yapılmış ve veritabanlarının onların elinde bulunması tehdit ve tehlikelerden korunma yöntemlerinin çokta etkili olmayacağını göstermektedir. Bu yüzden sosyal ağlarda karşılaşılabilecek tehdit ve sorunların azaltılması, güvenli bir ortam oluşturulması için kanunlarla korunabilecek çalışmalar yapılmalı ve bu çalışmalar desteklenmelidir. İnternet üzerinden işlenen suçlarla mücadeleye yönelik çalışmalar olsa da yeterli değildir. Hukuki altyapının da, suçlarla etkin mücadele edilebilmesi için düzenlenmesi gerekmektedir.

Günümüzde pek çok sosyal ağ bulunmakta ve kullanılmaktadır. Bu çalışmada da belirtildiği gibi ağ ortamlarında karşılaşılabilecek tehdit ve tehlikelerinin boyutları dikkate alındığında, bunların kullanılmamasını önermenin yerine aşağıdaki önlemlerin ve önerilerin dikkate alınmasının faydalı olacağı düşünülmektedir.

1. Kritik görevlerde bulunan veya bulunma potansiyeli bulunan kişiler sosyal medyayı kullanmamalıdır. Kullanmak zorunda ise dikkatli kullanmalıdırlar.
2. Kullananlar var ise mümkün olduğunca kişisel veri veya bilgileri sosyal ortamlarda paylaşmamalıdır.
3. Sosyal medyada paylaşılan dokümanların/belgelerin veya bilgilerin telif hakkı oluşturabileceği hatırda bulundurularak kullanılmalı veya paylaşım yapılmalıdır.
4. Sosyal medya ortamlarının çok yakın takip edildiği dikkate alınarak mümkün olduğunca az resim, bilgi veya belge paylaşılmalıdır. Bunların yıllar içerisinde biriktirildiği ve burada büyük resimlerin oluşturulabileceği unutulmamalıdır.
5. Çocukların sosyal medya kullanımı belirli bir yaşa kadar yasaklanmalı veya gözetimli olarak kullanmalarına izin verilmelidir. Kontrol veya denetim yoksa açılmasına müsaade edilmemeli veya açılmış ise hesapları kapatılmalıdır.
6. Bu ortamlarda suç unsuru barındıran içerikler paylaşılabilmektedir. Bunların paylaşımının adli sonuçlar doğurabileceği unutulmamalıdır.
7. Bu ortamlarda kişilere hakaret edici yazılar yazılmamalı veya paylaşılmamalıdır. Bunun sonucu olarak adli takip yapıldığı ve ceza alınabileceği unutulmamalıdır.
8. Sosyal ortamlara saldırılar sıkça yapılmaktadır. Erişim şifreleri en önemli hedeflerden birisidir. Şifrelerin çalınmaması ve kolay kırılmasının önüne geçmek için kırılması zor şifreler kullanılmalı ve sıklıkla değiştirilmelidir.
9. Ülkemizde ücretsiz olarak verilen Güvenli İnternet hizmetinden mutlaka faydalanılmalıdır. Telefon operatörleri tarafından ücretsiz verilen bu hizmetin dünyada bu alanda sunulan ilk hizmetlerden birisi olması da önem arz etmekte olup karşılaşılabilecek tehditlerin filtrelenmesi sağlanmakta, kullanıcılarak farklı hizmetler sunabilmektedir.

VIII. TEŞEKKÜR

Makale hazırlanması aşamasında desteğini esirgemeyen ve çok değerli tecrübelerini bizlere aktaran Prof. Dr. Şeref SAĞIROĞLU'na teşekkür ederiz.

IX. KAYNAKLAR

[1]. K. Bilen, O. Ercan, T. Gülmez, "Sosyal Ağların Kullanım Amacı ve Benimsenme Süreci; Kahramanmaraş Sütçü İmam Üniversitesi Örneği", Eğitim ve Öğretim Araştırmaları Dergisi (Journal of Research in Education and Teaching), Şubat 2014, Cilt:3, Sayı:1, Makale No: 11, ISSN: 2146-9199, pp.115-123.

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

[3]. D. M.Boyd, N. B. Ellison, "Social Network Sites: Definition, History and Scholarship", Journal of Computer-Mediated Communication, Vol 13, Issue 1, 2007, article 11, pp.210-230.

[4]. Y. Gülbahar, F. Kalelioğlu, O.Madran, "Sosyal Ağların Eğitim Amaçlı Kullanımı", pp. 1-6, XV. Türkiye'de İnternet Konferansında sunulan bildiri, İstanbul Teknik Üniversitesi, İstanbul, 2010.

[5]. İnternet, "Sosyal Ağ Kullanımı", http://www.campaigntr.com/2011/12/30/1472/sosyal-ag-kullanimi-nereye-gidiyor/, Mart 2015.

[6]. C. Murray, "Schools and Social Networking: Fear or Education?", Synergy Perspectives: Local, Vol. 6, Issue 1,2008, pp. 8-12.

[7]. N. Jones, H. Blackey, K. Fitzgibbon, E. Chew, "Get out of MySpace!", Computers & Education, Vol. 54, 2010, pp. 776–782.

[8]. N. Grant, "On the Usage of Social Networking Software Technologies in Distance Learning Education", In K. McFerrin et al. (Eds.), Proceedings of Society for Information Technology and Teacher Education, International Conference 2008, pp.3755-3759, Chesapeake, VA: AACE.

[9]. F. Özmen, C. Aküzüm, M. Sünkür, N. Baysal, "Sosyal Ağ Sitelerinin Eğitsel Ortamlardaki İşlevselliği (Functionality of Social Networks in Educational Settings)", pp.42-47, 6th

International Advanced Technologies Symposium (IATS'11), 16-18 May 2011, Elazığ, Turkey.

[10]. L. Gonzales, D.Vodicka, "Top Ten Internet Resources for Educators", Leadership, pp. 32-37, 2010.

[11]. J. Peluchette, K.Karl, 'Examining Students' Intended Image on Facebook: "What Were They Thinking?", Journal of Education for Business, Vol. 85, 2010, pp. 30–37.

[12]. İ. Karlı, "Medya Kuruluşları Sosyal Paylaşım Ağlarını Neden Kullanır?", International Conference on New Media and Interactivity, 202-207, İstanbul, 2010.

[13]. İnternet, "Youtube Gizlilik Politikası", https://www.google.com.tr/intl/tr/policies /privacy/, Mart 2015.

[14]. K. Kamil, S. Rene, K. Veronika, "The Risks of Internet Communication 3", International Conference on Education and Educational Psychology (ICEEPSY), pp.1349-1350, 2012.

[15]. J. Palfrey, U. Gasser, "Understanding the first generation of digital natives", Harvard Press, pp.1-5, 2008.

[16]. H. Sayar, M. Dalkılıç, "Internet'te Kişisel Bilgi Güvenliği İçin Anonimleştirici Servisler Üzerine Bir İnceleme", Yüksek Lisans Bitirme Projesi, Ege Üniv., Uluslararası Bilg. Enst. pp.1-10, 2004.

[17]. İnternet, "Sosyal Ağlarda Özel Hayat ve Gizliliğin Korunması", http://prezi.com/ o9tzpjw4c19d/hsa, Mart 2015.

[18]. İnternet, "Sosyal Ağlarda Olmayanlar: Gizlilik ve Güvenlik", http://www.e-siber.com/sosyal-medya/sosyal-aglarda-olmayanlar-gizlilik-ve-guvenlik/, Mart 2015.

[19]. İnternet, "Toplu Dava: Facebook Özel Mesajları Reklamcılar İçin 'Görüntülüyor' mu", http://www.bbc.co.uk/turkce/ekonomi/2014/01/140103_facebook_dava_gizlilik.shtml, Mart 2015.

[20]. İnternet, "2013 Cisco Annual Security Report", http://www.cisco.com/web/offer /gist_ty2_asset/Cisco_2013_ASR.pdf, Mart 2015.

[21]. E. Sezgin, O. Şenkal, "Üniversite Öğrencilerinin Sosyal Ağ Bilgi Güvenlik Farkındalıkları", Akademik Bilişim Konferansı, pp.1-22, 2014, Mersin.

[22]. İnternet, "Facebook'ta Paylaşım ve Başkalarının Sizi Bulması", https://tr-tr.facebook.com/about/privacy/your-info-on-fb, Ağustos 2014.

[23]. N. Yıldırım, A. Varol, "Sosyal Ağlarda Güvenlik: Bitlis Eren ve Fırat Üniversitelerinde Gerçekleştirilen Bir Alan Çalışması", 1-st International Symposium on Digital Forensics and Security, pp.285-292, 2013, Elazığ.

[24]. A. Çubukcu, Ş.Bayzan, "Perception of Digital Citizenship in Turkey and Methods of Increasing this Perception by Using the Internet Conscious, Safe and Effective", Middle Eastern & African Journal of Educational Research, Issue 5, pp.1-27, 2013.

[25]. İnternet, "Kimlik Hırsızlığı", http://www.microsoft.com/tr-tr/security/resources/ identitytheft-whatis.aspx, Mart 2015.

[26]. İnternet, "Microsoft Piyangosu Dolandırıcılığı", http://www.microsoft.com/tr-tr/security/resources/microsoftlottery-whatis.aspx, Mart 2015.

[27]. İnternet, "E-Posta ve Web Dolandırıcılıkları: Kendinizi Korumaya Yardımcı Olma Yöntemleri", http://www.microsoft.com/tr-tr/security/online-privacy/phishing-scams.aspx, Mart 2015.

[28]. A. Kumar, S. Gupta, K. Rai, "Social Networking Sites and Their Security Issues", International Journal of Scientific and Research Publications, 3(4), pp. 1-6, 2013.

[29]. İnternet, "Siber Suçların Kapsamı, Tanımları ve Sınıflandırılması", http://www.batman.pol.tr/ Sayfalar/sibersuclarla.aspx, Mart 2015.

[30]. H. Hekim, O. Başıbüyük, "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", Uluslararası Güvenlik ve Terörizm Dergisi, pp. 1-366, Ağustos 2014.

[31]. İnternet, "Güvenli İnternet Çağrı Merkezi hayata geçirildi", http://www.milligazete.com.tr/ haber/Guvenli_Internet_Cagri_Merkezi_hayata_gecirildi/187353#.VL1aKtKsVqU, Mart 2015.

[32]. İnternet, "Spam", http://web.deu.edu.tr/sss/ spam.html, Mart 2015.

[33]. G. Erdoğan, Ş. Bahtiyar, "Sosyal Ağlarda Güvenlik", Akademik Bilişim Konferansı, pp. 1-6, Mersin, 2014.

[34]. İnternet, "Sosyal Ağ", http://www.hvinsider.com/articles/social-networking-fun-friendly-but-not-always-safe/, Mart 2015.

[35]. İnternet, "Sosyal Ağ Güvenliği İçin 11 İpucu", http://www.microsoft.com/tr-tr/security/online-privacy/social-networking.aspx, Mart 2015.

[36]. İnternet, "SANS (SysAdmin, Denetim, Network, Güvenlik) Critical Security Controls", www.sans.org/critical-security-controls/, Mart 2015.

[37]. D. Sancho, "Security Guide to Social Networks", White-Paper Trend Micro Inc.,pp. 1-10, August 2009.

[38]. İnternet, "Çizgi Kahramanın Arkasından Porno Tuzağı Çıkabilir", http://www.aksiyon.com.tr/toplum/cizgi-kahramanin-arkasindan-porno-tuzagi-cikabilir_529242, Mart 2015.

[39]. Ş. Bayzan, A. Özbilen, "Aplication Examples of Safer Use of The Internetin The World and Investigation of Awareness Activities in Turkey Suggestions for Turkey", cilt 7, no.2, 5th International Computer & Instructional Technologies Symposium, pp. 22-24 September 2011, Fırat University, Elazığ/Türkiye.

[40]. İnternet, "Güvenli İnternet Günü ve BTK Faaliyetleriyle İlgili Basın Toplantısı Yapıldı", http://www.tk.gov.tr/sayfa.php?ID=75, Mart 2015.

[41]. İnternet, "Türkiye'nin Siber Güvenlik Politikası", http://www.ankarastrateji.org/haber/turkiye-nin-siber-guvenlik-politikasi-991/, Mart 2015.

[42]. H. Sayar, M. Dalkılıç, "Internet'te Kişisel Bilgi Güvenliği İçin Anonimleştirici Servisler Üzerine Bir İnceleme", pp.1-10, Akademik Bilişim 2005, Gaziantep Üniversitesi, 2-4 Şubat 2005.

[43]. M. Mert, H. İ. Bülbül, Ş. Sağıroğlu, "Milli Eğitim Bakanlığına Bağlı Okullarda Güvenli İnternet Kullanımı", TÜBAV Bilim Dergisi, 5(4), 2012, pp.1-10.