ANADOLU ÜNİVERSİTESİ

Açıköğretim Uygulamaları ve Araştırmaları Dergisi
AUAd

auad.anadolu.edu.tr

Açık ve uzaktan öğrenmede güvenli sosyal ağ kullanımı (editöre mektup)

Doç. Dr. Nilgün TOSUN[a]

[a] Trakya Üniversitesi, Eğitim Fakültesi, Edirne, Türkiye 22030

Özet

Web 2.0 teknolojilerinin gelişimiyle birlikte sosyal ağlar, bireylerin üreten ve aktif rol aldığı platformlara dönüşmüştür. Sosyal ağlar; bireysellik, üretkenlik, iletişim ve etkileşim olanakları çerçevesinde, son yıllarda açık ve uzaktan öğrenme uygulamaları ile de dikkat çekmektedir. Özerklik ve Etkileşimsel Uzaklık, Bağımsız Çalışma, Bağlantıcılık gibi kuramlara dayandırılarak geliştirilen bu uygulamaları başarıya taşıyan önemli etkenlerden biri de güvenli öğrenme ortamları oluşturabilmektir. Bunun için yapılması gereken, bireyleri güvenli sosyal ağ kullanma konusunda bilgilendirmektir. Çok sayıda ve farklı profile sahip bireyin yer aldığı sosyal ağlarda sahte kullanıcılar, hesapların ele geçirilmesi, ortak arkadaşlar özelliği, oltalama, sosyal kötücül yazılımlar, mizanpaj, siber zorbalık ve GPS'ler gibi çok sayıda tehlike ile karşı karşıya kalabilirler. Bu tehlikeli durumlara karşı alınacak önlemlerin bilinmesi, sosyal ağlarda öğrenmeyi daha kolay, keyifli ve başarılı hale getirecektir.

Anahtar Sözcükler: Açık ve uzaktan öğrenme, sosyal ağlar, güvenlik.

Abstract

After the advancement of Web 2.0 technologies, social networks have become platforms where individuals produce and actively participate. In terms of individuality, productivity, communication and interaction possibilities, social networks have also been standing out with open and distance learning applications in the recent years. One of the important factors leading these applications which are developed based on theories such as Autonomy and Transactional Distance, Independent Studying and Connectivism to success is to be able to establish safe learning environments. What needs to be done to achieve this is to inform individuals about safe usage of social networks. In the social networks where there are individuals with many and different accounts, fake users can encounter many dangers such as account hijackings, common friends feature, trolling, social malware software, makeup, cyber bullying and GPSs. Having the knowledge about precautions against these dangers should make learning in social networks easier, more enjoyable and more successful.

Keywords: Open and distance learning, social networks, security.

Kaynak Gösterme

Tosun, N. (2017). Açık ve uzaktan öğrenmede güvenli sosyal ağ kullanımı (editöre mektup). *AUAd, 3*(2), 4-8.

Sayın Editör,

İlk örneklerine 1970'li yılların sonlarında rastlanan sosyal ağlar, internet kullanımının yaygınlaşmasına paralel olarak sayıca artış göstermeye devam etmektedir. Başlangıçta web 1.0 teknolojilerinin desteğiyle sadece içerik okumaya dayalı ve pasif kullanıcıların yer aldığı sosyal ağlar, web 2.0 teknolojilerinin gelişimiyle beraber bambaşka bir yapıya dönüşmüş, kullanıcıların tüketici olmaktan çıkarak üretken ve aktif rol aldığı etkileşimli platformlar halini almıştır.

Günümüzde sosyal ağlar; kullanıcılarına profil oluşturma, içerik üretme, içerikler hakkında beğenide bulunma, yorum yazma, eş zamanlı ya da eş zamansız etkileşimde bulunma, farklı formatlarda yazı, resim, ses, video ve fotoğraf gibi dosyaları paylaşma olanağı sunmaktadır. Kullanıcılara sunulan bu geniş imkanlar, sosyal ağların kullanıcı sayısının artmasına neden olmaktadır. Digital in 2017 Global Overview Ocak 2017 verilerine göre, dünyada aktif sosyal ağ kullanıcı sayısı 2 milyar 789 milyondur. Aynı tarihli verilere göre Türkiye'deki aktif sosyal ağ kullanıcı sayısı 48 milyondur.

Önemli bir kullanıcı kitlesine sahip sosyal ağlar; bireysellik, üretkenlik, iletişim ve etkileşim olanakları çerçevesinde, son yıllarda açık ve uzaktan öğrenme uygulamaları ile de dikkat çekmektedir. Moore'un Özerklik ve Etkileşimsel Uzaklık, Wedemeyer'ın Bağımsız Çalışma, Siemens ve Downes'ın Bağlantıcılık kuramlarına dayandırılarak oluşturulmuş sosyal ağ destekli açık ve uzaktan öğrenme ortamları, başarılı sonuçların elde edilmesinde etkili olmuştur. Açık ve uzaktan öğrenmenin temelini oluşturan öğrenen-öğreten, öğrenen-içerik, öğrenen-öğrenen etkileşiminin ve paylaşımların rahatlıkla yapılabildiği sosyal ağlar, eğitimin her kademesinde, bireysel ve kurumsal her yapıda, hemen her ders için kullanılabilmektedir. Ders içeriklerinin ve ek kaynakların paylaşılması, öğrenen sorularının yanıtlanması, akademik duyurular, canlı dersler gibi çok sayıda etkinlik, sosyal ağlarda yapılabilmektedir.

Açık ve uzaktan öğrenmede başarılı bir sosyal ağ uygulaması; hızlı internet bağlantısı, internet okuryazarlığı, nitelikli içerik, istikrarlı etkileşim ve paylaşımların yanı sıra, güvenli bir ortamı da gerektirir. Çok sayıda ve farklı profile sahip kullanıcının yer aldığı sosyal ağlarda bireysel güvenliği tehdit eden birçok unsura rastlamak mümkündür. Bu tehlike unsurlarından biri sahte kullanıcılardır. Sahte bilgilerle açılmış sosyal ağ hesapları, genellikle dolandırıcılık ve aldatma amaçları güdülerek kullanılmaktadır. Birden çok ve güçlü giriş aktivasyonları kullanılması, sahte hesaplarla öğrenen ya da öğreten olarak sosyal ağa sızmalara karşı alınabilecek önlemlerden biridir. Sosyal ağ hesaplarının ele geçirilmesi ve ele geçirilen hesapların kötü amaçlarla kullanılması ise, bir başka tehlike unsurudur (Ceyhan ve diğ., 2015).

Ele geçirilen bir hesap ile, öğrenen ya da öğreteni yasal ve etik olarak zor durumda bırakacak paylaşım ve etkileşimlerde bulunulabilmektedir. Sosyal ağ kullanıcılarının dikkat etmesi gereken bir diğer güvenlik konusu ise arkadaş listesi mahremiyetidir. Facebook gibi bazı sosyal ağ siteleri, bireylere arkadaş listelerini gizli tutma olanağı sunmaktadır. Herkesin erişimine açık bırakılan arkadaş listeleri, listedeki bir bireyin, kişisel bilgilerini ve paylaşımlarını isteği dışında başkalarının görmesi için zemin oluşturmaktadır. Bu durum, sahte profil oluşturma ve bu yolla aldatma, siber zorbalık gibi olumsuz davranışların ortaya çıkmasına yardımcı olmaktadır. Bu nedenle, sosyal ağ kullanıcılarının arkadaş listelerini herkesin erişimine açık tutmak yerine sadece kendileri görecek şekilde düzenlemeleri uygun olacaktır. Sosyal malware ise, sosyal ağ kullanımının artması ile hayatımıza giren yeni kavramlardan biridir. Sosyal ağ listelerinde yer alan arkadaşlardan gelen uygulama indirme istekleri sonucu bulaşan zararlı yazılımlar olarak bilinir. Bu tür istekleri yerine getirmeden önce bireyler uygulamaya gerçekten ihtiyaç duyup duymadıklarına karar vermeli, bu uygulamanın cihazlarında hangi dosya ve alanlara erişim izni aldığına çok dikkat etmeleri gerekir. Oltalama ya da phishing adı verilen durumda ise sosyal ağ kullanıcıları sahte web sayfalarına yönlendirilmektedir (Pesen, 2016). Bu durumdan korunmanın en iyi yolu ise, rastgele kullanıcı eklememek, kullanıcılardan gelen her bağlantıyı açmamaktır. Kelimelerin bir ya da birden çok harfinin yanlış yazılma özelliği kullanılarak, bireylerin sahte sosyal ağlara yönlendirilmesi olarak bilinen Typosquatting ya da mizanpaj, sıklıkla karşılaşılan tehlike unsurlarından biridir. Örneğin, farkında olmadan Facebook yerine Facevook yazmak, olası bir hatadır. Ya da Twitter yerine Twiteer yazmak (Pesen, 2016). Bu hata, sosyal ağ kullanıcılarının, ustaca taklit edilmiş aslına çok benzer sahte bir sayfaya yönlendirilmesi için yeterlidir. Siber zorbalık ise, sosyal ağ kullanıcıları arasında özellikle bayanların mağdur olduğu bir diğer tehlike unsurudur. Küçük düşürücü ya da hakaret içerikli mesajlar gönderme, tehdit etme, taciz gibi davranışlarla tanımlanabilen siber zorbalık, sahte hesap oluşturmanın engellenemediği sosyal ağlarda sıklıkla rastlanan suçlardan biridir. Bu nedenle, açık ve uzaktan öğrenme amaçlı kullanılan sosyal ağ platformlarında gerçek kimlik belirtmeksizin yer almak isteyen öğrenenlere izin verilmemesi, siber zorbalığın önlenmesinde önemli bir adım olacaktır. Son yıllarda üretilen dijital fotoğraf makinesi ve akıllı telefonların çektiği görüntülerin içine enstantane, diyafram, pozlama, fotoğraf makinesi markası ve modeli gibi teknik bilgiler gömülebilmektedir. Bu resim verisi tanımlama formatı olan EXIF içerisine, GPS'ler sayesinde artık çekimin yapıldığı yerin coğrafi konum bilgisi de eklenmektedir. Sosyal ağlarda paylaşılan fotoğraf ya da videoların, ev ya da iş yeri gibi, adres bilgilerini herkesle paylaşmak istemediğimiz alanları belirgin şekilde içermemesine dikkat edilmelidir.

Sonuç olarak; sosyal ağlar, açık ve uzaktan öğrenmede yararlanılan, sayısı milyonları bulan kullanıcıya sahip önemli etkileşim ve paylaşım platformlarıdır. Bu platformlarda sorunsuz ve başarılı öğrenmenin anahtarlarından biri de güvenliktir. Sosyal ağ kullanıcılarının karşı karşıya kalabilecekleri tehlikeler ve bu tehlikelere karşı alınabilecek belli başlı önlemler, yukarıda kısaca özetlenmeye çalışılmıştır. Sosyal ağ kullanımında güçlü şifreler oluşturmak, bu şifreleri kimseyle paylaşmamak, şifreleri belli periyotlarda değiştirmek, ortak bilgisayarlarda sosyal ağlara girişte parola anımsama önerisine olumsuz yanıt vermek, sosyal ağlardan güvenli çıkış yapmak, iyi bir antivirüs kullanmak, sosyal ağların gerektirdiği güvenlik ve gizlilik ayarlarını araştırıp öğrenmek ve uygulamak, sosyal ağ kullanıcılarını bir çok tehlikeden korumaya yardımcı olacaktır. Açık ve uzaktan öğrenme öğreten ve öğrenenlerini bu konuda bilgilendirmek amacıyla etkinlikler organize etmek ve içerikler paylaşmak da, konuya ilişkin yapılabilecekler arasında sayılabilir.

Kaynakça

Ceyhan, E. B., Demiryürek, E., ve Kandemir, B. (2015). Sosyal ağlarda güncel güvenlik riskleri ve korunma yöntemleri. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 1*(1):1-10.

Digital in 2017 Global Overview (2017). Digital in 2017 Global Overview Report. (https://wearesocial.com/blog/2017/01/digital-in-2017-global-overview) (19.04.2017 tarihinde erişildi.)

Pesen, M. M. (2016). Taklit ve Sahte Domain Adreslerini Tespit Etme Aracı. (http://www.sibergah.com/genel/internet-guvenligi/taklit-ve-sahte-domain-adreslerini-tespit-etme-araci/) (18.04.2016 tarihinde erişildi.)

Yazar Hakkında

Doç. Dr. Nilgün TOSUN

Lisans, yüksek lisans ve doktora eğitimini Trakya Üniversitesi Bilgisayar Mühendisliği Bölümü'nde tamamlamıştır. 2006-2009 yılları arasında, kuruculuğunu yaptığı Trakya Üniversitesi Uzaktan Eğitim Merkezi'nde Müdür Yardımcılığı, 2007-2008 yılları arasında, uzaktan eğitim veren Tunca Meslek Yüksek Okulu Müdür Yardımcılığı ve Teknik Programlar Bölüm Başkanlığı, 2008-2012 yılları arasında ise halen Doç. Dr. olarak ders vermekte olduğu Trakya Üniversitesi Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölüm Başkanlığı görevlerini yürütmüştür. Açık ve uzaktan öğrenme, eğitimde teknoloji entegrasyonu, sosyal ağlar ve sosyal ağlarda güvenlik, döndürülmüş öğrenme konularında çalışmalarını sürdürmektedir.

Posta adresi : Trakya Üniversitesi, Eğitim Fakültesi, Mehmet Akif Ersoy Eğitim Binası, Kosova Yerleşkesi Edirne, Türkiye.
Tel (İş) : +90 284 212 08 08 (1140)
GSM : +90 554 998 56 16
Eposta : nilgunt@trakya.edu.tr