

Sosyal Ağlarda Güvenlik

Sosyal ağlar, internet üzerinden diğer kullanıcılarla iletişim/etkileşim kurmaya yarayan ağlara verilen genel isim olup en yaygın olarak kullanılan sosyal ağlar günümüzde Facebook, Twitter, Google+, LinkedIn, Foursquare ve Youtube'dur. En çok kullanıcı sayısına sahip Facebook'ta merak ettiğiniz bir konu olduğu zaman Facebook'un kullanıcıları için hazırlamış olduğu Yardım ve Güvenlik Merkez'lerini kullanabilirsiniz:



Sosyal Ağlar; insanların kendileri için internet ortamında bir kimlik oluşturmak suretiyle, internet ortamındaki diğer insanlar ile iletişim/etkileşim kurdukları, farklı birçok bilgiyi paylaştıkları, oyun oynadıkları ve yeni arkadaşlıklar edindikleri web tabanlı uygulamaların ve servislerin genel adıdır.

Günümüzde yaygın olarak kullanılan sosyal ağlara örnek olarak Facebook, Twitter, LinkedIn, Foursquare, Youtube, Google+, Snapchat ve Dailymotion gösterilebilir. "We Are Social ve Hootsuite"nin birlikte yayınladıkları 2018 yılı Dünya sosyal medya kullanım istatistik raporuna göre sosyal ağların kullanımında, ~2.1 milyar kullanıcı ile Facebook birinci sırada karşımıza çıkmaktadır. Facebook'u, ~1.5 milyar kullanıcı ile Youtube ikinci sırada ve ~800 milyon kullanıcı ile Instagram üçüncü sırada takip etmektedir. Aynı raporda Facebook kullanıcılarının ~%34'ününün 18 – 34 yaş grubu arasında olduğu görülmektedir.

Sosyal ağlardaki kullanıcı sayılarının giderek artması, sosyal ağlardaki güvenlik tehditlerinin ve kullanım risklerinin de artmasını beraberinde getirmektedir. Bu

durum ise özellikle sosyal ağlardaki gizliliği ve güvenliği göz ardı etmiş bilinçsiz sosyal ağ kullanıcıları için telafisi mümkün olmayan sorunlara neden olabilmektedir.

Sosyal ağlarda en önemli husus paylaşımlardır. Paylaşmak güzeldir fakat özellikle sosyal ağlarda hangi bilginin kiminle paylaşıldığı çok önemlidir.

Çünkü;

- Paylaşılan her türlü bilgi paylaşan tarafından silinse dahi internet ortamında silinmeden kalabilmektedir.
- Paylaşımlar kolaylıkla gönderilebilir ancak, kolaylıkla geri alınamayabilir.
- Gönderiler masum görünse de, sonradan hayatı olumsuz yönde etkileyebilir.
- Paylaşımlar, günlük hayatı ve ilişkileri olumsuz yönde etkileyebilir.
- “Keşke paylaşmasaydım” denilmesine sebep olabilir.

Özellikle Sosyal ağlarda;

- Doğum tarihi
- Eğitim bilgileri
- Anne kızlık soyadı
- Nüfus cüzdanı bilgileri
- Diğer aile bireylerinin kişisel bilgileri
- Kredi Kartı bilgileri
- Kullanıcı adı ve şifre bilgileri
- Ehliyet bilgileri
- İş yeri bilgileri
- Adres bilgileri
- Tatil yeri ve tarihi
- E-posta adresi
- Kişisel fotoğraf ve videolar

vb. kişisel bilgilerin paylaşılmaması, yaşanması muhtemel mağduriyetlerin önüne geçilebilmesi açısından büyük önem arz etmektedir.

SOSYAL AĞLARDA NE TÜR GÜVENLİK ÖNLEMLERİ ALINMALI

Sosyal ağlarda; Kimlik Hırsızlığı, Dolandırıcılık, Profil Klonlama, İstenmeyen e-postalar, Kötü bağlantı istekleri, sahte ürün satışı vb. güvenlik tehditleri ile karşılaşılabilir.

Unutulmamalıdır ki, İnternet ortamında bilinçsiz kullanıma bağlı olarak en büyük güvenlik tehdidi bizzat kullanıcının kendisi olmaktadır. Bu nedenle özellikle sosyal ağları yoğun bir şekilde kullanan her kullanıcının gerekli güvenlik ve gizlilik tedbirlerini alması gerekmektedir.



FACEBOOK'TA GİZLİLİK VE GÜVENLİK

- Havaalanı, Alışveriş Merkezi vb. kablosuz ağ bağlantısının ortak kullanıldığı ortamlarda bağlantının “https” olarak gerçekleştiğinden ve giriş yapılan adresin doğru olduğundan emin olunmalıdır.
- Facebook hesabının bağlı olduğu e-posta hesabının şifresi belirlenirken güçlü bir şifre politikası (en az 10 karakter, küçük ve büyük harf, rakam ve noktalama işareti içeren) tercih edilmelidir.
- Facebook hesabının bağlı olduğu e-posta hesabının şifresi belli aralıklarla değiştirilmelidir.
- Gerekli kadar profil bilgisi paylaşılmalıdır.
- Giriş uyarı bildirimlerinin alınması ve giriş onaylarının aktif edilmesi için gerekli düzenlemeler yapılmalıdır.
- Paylaşılan içeriklerin kimler tarafından görülebileceği belirlenmelidir.
- Arkadaşlık teklifi ve mesaj gönderebilecek kişiler sınırlandırılmalıdır/belirlenmelidir.
- Paylaşılacak istenen içeriklere göre arkadaşlar gruplandırılmalı, gizlilik ayarları oluşturulan gruplara göre yapılmalıdır.
- Zaman tünelineki paylaşımları görebilecek kişiler sınırlandırılmalıdır/belirlenmelidir.
- Arama motorlarında yapılan sorgulamalara karşı, profil bilgileri kapatılmalıdır.
- Daha detaylı bilgi alabilmek için Facebook'un <https://www.facebook.com/help/> sayfası ziyaret edilebilir.



TWITTER'DA GİZLİLİK VE GÜVENLİK

- Havaalanı, Alışveriş Merkezi vb. kablosuz ağ bağlantısının ortak kullanıldığı ortamlarda bağlantının “https” olarak gerçekleştiğinden ve giriş yapılan adresin doğru olduğundan emin olunmalıdır.
- Güçlü bir şifre politikası (en az 10 karakter, küçük ve büyük harf, rakam ve noktalama işareti içeren) tercih edilmelidir.
- Şifrenin unutulması durumunda, şifre sıfırlamak için kişisel bilgilerin (e-posta ve ya telefon numarası) istenmesi tercih edilmelidir.
- Giriş onaylama denetimi aktif edilmelidir.
- Farklı bir cihazdan hesaba giriş yapılmak istendiğinde e-posta ile bildirimde bulunulması aktif edilmelidir.
- Sürekli tercih edilen tarayıcı (chrome, mozilla, Explorer vb.), mümkün olduğunca en güncel versiyonunda tutulmalıdır.
- Hesap şifresi belli aralıklarla değiştirilmelidir.
- Daha detaylı bilgi alabilmek için Twitter'ın <https://about.twitter.com/tr/safety.html> sayfası ziyaret edilebilir.



LİNKEDİN GİZLİLİK VE GÜVENLİK

Havaalanı, Alışveriş Merkezi vb. kablosuz ağ bağlantısının ortak kullanıldığı ortamlarda bağlantının “https” olarak gerçekleştiğinden ve giriş yapılan adresin doğru olduğundan emin olunmalıdır.

- LinkedIn hesabının bağlı olduğu e-posta hesabının şifresi belirlenirken güçlü bir şifre politikası (en az 10 karakter, küçük ve büyük harf, rakam ve noktalama işareti içeren) tercih edilmelidir.
- LinkedIn hesabının bağlı olduğu e-posta hesabının şifresi belli aralıklarla değiştirilmelidir.
- Gerektiği kadar profil bilgisi paylaşılmalıdır.
- Hesabın bağlı olduğu e-posta adresini kimlerin görebileceği belirlenmelidir.
- Bağlantı kurulan kişilerin başkaları tarafından da görüntülenmesi engellenmelidir.
- Daha detaylı bilgi alabilmek için LinkedIn’in <https://www.linkedin.com/help/linkedin> sayfası ziyaret edilebilir.

KAYNAK: <https://www.guvenliweb.org.tr/dokuman-detay/sosyal-aglarda-guvenlik>