

## Sosyal Ağlar ve Mobil Ağlar

### SOSYAL AĞLAR

Arkadaşlık, fotoğraf, video, mikroblog gibi sadece bir servislik hizmetlerden oluşan veya çevrimiçi sosyalleşme için birçok servisi birlikte sunan sosyal ağ platformları internette ortamında sosyalleşme adına günümüzde yoğun bir şekilde kullanılmaktadır.

Sosyal ağlar, web tabanlı, mobil uygulama veya mobil tarayıcı üzerinden ayrıca web sitelerine kendileriyle entegrasyonu sağlayacak bir takım eklentiler yoluyla faaliyet göstermektedir.

İnternet kullanıcılarının sosyal ağları ve sosyal ağların sunduğu hizmetleri günlük hayatları ile özdeşleştirmelerinden dolayı, ister web tabanlı isterse de mobil platformlarda olsun genel olarak aynı hizmetleri sunan sosyal ağlar, kullanıcılar için her platformda farklı güvenlik ve gizlilik tehlikeleri oluşturmaktadır.

### Sosyal Ağlarda İzin Verilen 3. Parti Uygulamalar

Kullanıcılar sosyal ağlarda, sanal kimlik oluşturarak içerik paylaşımı, mesajlaşma, yorum yazma, oyun oynama, üçüncü parti uygulamalar aracılığı ile çeşitli aktiviteler yapabilmektedir. Fotoğraf, video, yer ve konum bilgisi ve her türden kişisel verinin paylaşılabilirdiği sosyal ağ hesaplarında güvenlik ve gizlilik ayarlarını yeterince bilmeyen ve bazı uygulamalara izin veren kullanıcılar farkında olmadan özel bilgilerini ve şifrelerini üçüncü kişilerle paylaşarak sanal ortamda çok yönlü risklerle karşı karşıya kalmaktadır.

Son yıllarda sosyal ağlarda hızlı bir şekilde yayılmaya devam eden, sayısız güvenlik açığı içeren 3. Parti uygulamaların kullanılmasına izin verilmesi kişisel bilgilerin kötü niyetli kişilerin eline geçmesine neden olabilmektedir. Gerek sosyal ağlardaki uygulamaların gerekse kaynağı belli olmayan internet ortamından indirilen uygulamaların gereğinden fazla kişisel veri talep ettiği bilinmekte, bu uygulamalara karşı da dikkatli olunması gerekmektedir.

İndirilen veya sosyal ağlardaki 3. Parti uygulamalara onay veren kullanıcılar onay verilen uygulamaların arkadaş listelerine ve açık profil bilgilerine erişmesine, kullanıcı adına paylaşım veya beğenide bulunmasına, akıllı cihazlarında bulunan kamera, mikrofon ve diğer bilgilerine erişime de izin vermekte, mesajlarının okunması konuşmalarının dinlenmesi gibi istenmeyen durumlara maruz kalabilmektedir. Özellikle sosyal ağ platformlarında sıkça karşılaşılan "Hangi Irktansın?", "Doğum tarihine göre sana en uygun meslek nedir?", "Hangi ünlüye benziyorsun?", "xx yaşında kime benzeyeceksin?" veya "Profilime en son kim baktı?" şeklindeki veri toplayan uygulamalara izin veren kullanıcılar arka planda özel bilgilerini üçüncü kişilerle paylaşarak, veri güvenliğini riske atmaktadır.

### Asla Paylaşılması Gereken Bilgiler

Sosyal ağlarda çoğu kullanıcı özel bilgilerini bilinçsiz veya bilinçli paylaşarak internet ortamında çok yönlü risklerle karşı karşıya kalmaktadır. Sosyal medyada veya uygulamalarda açıkça paylaşılan özel hayata ait kişisel bilgiler, birileri veya bazı kuruluşlarca veri toplama programları ile toplanıp bir araya getirilerek her amaç için kullanılabilir.

Paylaşıldığında kişileri zor durumda bırakabilecek;

- Kişisel veriler,
- Konum ve yer bilgisi

- Aile ve arkadaşlara ait özel bilgiler(şifre, yaşanan problemler, zaafılar, tatil vb. gibi planlar, Günlük, haftalık ya da aylık aktiviteler, fiziksel özellikler, yetenekler...)

gibi bilgileri sosyal ağlarda ve bilgi talep eden 3. Parti uygulamalarda paylaşıldığında ileride muhtemel sorunlara davetiye çıkarılmaktadır. Kısacası sosyal ağlarda kişiyi ele veren ileride sıkıntıya sebep olabilecek hiçbir bilgi asla paylaşılmamalıdır. Sosyal ağların kullanıcılara hizmetlerini ücretsiz vermeleri kişisel bilgilerin gizliliğinin tehlikede olabileceği anlamına gelmektedir.

### **Sosyal Ağlarda Dikkat Edilmesi Gereken Hususlar**

İnternet kullanıcılarının, kişisel verilerini korumak için kullandıkları sosyal ağ platformlarında aşağıdaki hususlara azami dikkat ve özen göstermesi gerekmektedir.

- Kullandığınız sosyal ağ platformlarının kullanım politikası ve gizlilik sözleşmelerini okuyarak, sosyal ağlardaki gizlilik ve güvenlik ayarlarınızı tekrar gözden geçirin, güvenlik ve gizlilik ayarlarının düzgün yapıldığından emin olun,
- Sosyal ağlardaki hesaplarınıza olan erişimi tanıdığınız ve güvendiğiniz kişilerle sınırlayın,
- Özel ve kişisel bilgilerinizi asla paylaşmayın(gerçek doğum tarihi, dayı ve teyze gibi anne kızlık soyadının ortaya çıkabileceği bilgiler)
- Doğum tarihiniz, doğduğunuz yer, telefon numaranız gibi kişisel bilgilerinizden oluşan kolay tahmin edilebilir şifreler yerine en az 8 karakterden oluşan hem küçük hem büyük karakterler içeren tahmin edilmesi zor güçlü şifreler belirleyin.
- Sosyal medya platformlarına akıllı telefonunuzdan erişiyorsanız, telefonunuzun ayarlar bölümünden uygulamalarınıza verdiğiniz erişim izinlerini kontrol edin ve gereksiz veya riskli olduğunu düşündüğünüz izinleri kaldırın.
- Sosyal medya platformları üzerinden yaptığınız paylaşımların, milyonlarca kişiye erişebileceğini unutmayın ve paylaşımlarınızı buna göre yapın.
- İnternete erişim hakkınızı kullanırken başkalarının haklarını gözetme sorumluluğunuzu unutmayın.
- Kullanılan 3. Parti uygulamaların güvenlik, erişilebilirlik ve gizlilik politikalarını sürekli gözden geçirerek verilen izinleri sorgulayın.
- Sosyal ağlar ve web servislerin 3. parti uygulamalarını engelleyin(Kullanılmayan ağ oyunları ile 3. Parti uygulamalarının yetkileri tamamen kaldırılmalı)
- Sosyal ağlara herhangi bir oyun ya da uygulama kurulmak istendiğinde bunun hangi bilgilere erişmek istediği iyice kontrol edilmelidir.
- Kişisel olmayan bir bilgisayarda asla bir sosyal ağ hesabına giriş yapılmamalı.
- Sosyal ağlara bağlanılacak bilgisayarlarda mutlaka anti-virüs, anti-malware ve anti-spyware türü internet güvenlik yazılımları kullanılmalı, Toplu kullanıma açık kablosuz ağlarda, internet kafelerde sosyal ağ hesaplarına giriş yapılmamalıdır.

### **MOBİL AĞLAR**

Mobil ağlar, akıllı telefonlar ve 3G/4,5G Teknolojileri, internet kullanımını çok ayrı bir boyuta taşımış ve internete her an her yerden ulaşılabilir olma fırsat ve avantajlarını kullanıcılara sunmaya başlamıştır. Bu durum aynı zamanda gençlerin internette yeni bir gizli hayatlarının oluşmasına da sebep vermiştir. Bir anti-virüs firması tarafından yapılan bir araştırmada gençlerin %69'u sosyal paylaşım sitelerinde anlık durumlarını paylaşırken lokaysan bilgilerinin de paylaştıkları, %28'inin gerçek hayatta tanımadığı kişilerle sohbet ettiği ve yaşları 13 ile 17 arasında olan bu gençlerin mobil internet kullanımının son 1 sene içerisinde %256 oranında artış olduğu gözlemlenmiştir. Ayrıca bir genç aylık ortalama 3417

SMS veya mobil internet tabanlı uygulamalardan mesaj göndermektedir. Amerika'da Federal Ticaret Komisyonu tarafından yapılan yakın zamanlı bir arařtırmada ise; Mobil aęlar, akıllı telefonlar ve 3G/4,5G Teknolojileri, internet kullanımını çok ayrı bir boyuta tařımıř ve internete her an her yerden ulařılabilir olma fırsat ve avantajlarını kullanıcılara sunmaya bařlamıřtır. Bu durum aynı zamanda gençlerin internette yeni bir gizli hayatlarının oluřmasına da sebep vermiřtir. Bir anti-virüs firması tarafından yapılan bir arařtırmada gençlerin %69'u sosyal paylařım sitelerinde anlık durumlarını paylařırken lokaysan bilgilerinin de paylařtıkları, %28'inin gerçek hayatta tanımadığı kiřilerle sohbet ettiğı ve yařları 13 ile 17 arasında olan bu gençlerin mobil internet kullanımının son 1 sene içerisinde %256 oranında artış olduğı gözlemlenmiřtir. Ayrıca bir genç aylık ortalama 3417 SMS veya mobil internet tabanlı uygulamalardan mesaj göndermektedir. Amerika'da Federal Ticaret Komisyonu tarafından yapılan yakın zamanlı bir arařtırmada ise;

1. Ailelerin, mobil uygulamaların ne gibi bilgiler topladıklarından, o bilgileri kimin, nasıl kullanacağından haberdar olmadıkları;
2. Mobil uygulamaların sadece %20'si kullanıcılarını güvenlik politikaları hakkında uyardığı;
3. Çoęu uygulamanın (ortalama %60 civarı) kiřisel verileri kullanılan cihazdan alıp bařka yerlere verdiğı (reklam aęlarına, analisttik řirketlere ya da 3. mercilere ulařtırılıyorlar);
4. mercilerin bilgilerin çok büyük bir kısmına mobil uygulamalardan edindikleri bilgilerden ulařtığı ve bu sayede çocukların davranıřsal yüklemelerinden yola çıkarak profil oluřturup bunu ticari çıkarları için kullandığı; sonuçlarına ulařılmıřtır. Bu da demek oluyor ki, mobil platform veri üreticileri hem çok rahatlıkla kullanıcı bilgilerine ulařılabilmekte hem de kullanıcılar bir bilinç dâhilinde hareket etmedikleri için birçok riskle karşı karşıya kalabilmektedir.

### **Mobil Aęlarda nelere dikkat edilmeli?**

- Mobil aęlarda da muhakkak bir anti-virüs yazılımı kullanılmalı. Kullandığınız anti-virüs yazılımının mobil platformlardaki uygulamaların sertifikaları ve güvenilirlikleri hususunda da sizi uyarabildiğinden emin olunuz.
- Mobil telefonunuz için Güvenli İnternet Hizmeti'ni kullanınız. Detaylı bilgi için: [guvenlinet.org.tr](http://guvenlinet.org.tr)
- Mobil marketlerden indirdiğiniz uygulamaları indirmeden önce kullanıcı yorumlarına göz gezdirin. İndirme ařamasında sizden hangi bilgileri ne amaçla topladığı hususunda bilgi sahibi olmaya çalışınız.
- Ortak wi-fi alanlarında mobil aęlarınızı kullanmamanızı öneririz. Mobil aęlarınızdan iřlem yaparken ya özel ve řifreli wi-fi aęlarını ya da 3G/4,5G'yi kullanmanızı öneririz.
- Mobil telefonunuza muhakkak bir tuř kilidi koyun. Tuř kilidi harici artık her bir mobil uygulamaya girerken veya baęlanırken bile řifreleme tekniklerin geliřtirildiğinden haberdar olun ve bu konuda iřletim sistemi operatörünüzden ve kullandığınız mobil marketten bilgi alınız.