GÜVENLİ GÜNLER BÜLTENİ

Bilgisayar kullanıcılarına yönelik hazırlanır. Her ayın 15'i çıkar. Bültenlerin her ay size ulaşması için üye olunuz: http://eepurl.com/bP-tWn

TEMMUZ 2016

Sosyal Medya Güvenliği

SON BEŞ YILDA HAYATIMIZDA ÇOK GENİŞ YER EDİNEN SOSYAL MEDYA MECRALARININ BU KADAR BÜYÜMESİNDE BİR TEMEL İNSANİ İHTİYACIN KATKISI BÜYÜKTÜR. İnsan psikolojinde önemli yeri olan "beğenilme isteği", kişilerin günlük hayatlarındaki güzel veya duygu yoğunluğu yaşadıkları çeşitli anları paylaşma isteği yaratmaktadır.

İnsanlığın öteden beri var olan bu ihtiyacı nedeniyle, farkında olarak veya olmayarak, sosyal medya ortamlarını beğeni toplama amacıyla hayatımızdan kesitler paylaştığımız eşsiz bir pencere haline getirdik.

Bu paylaşımları yapabilmek için başkalarına, ilgili uygulamalar üzerinde kendi belirlediğimiz düzeyde olanak tanıyarak, hayatımızı gözlemleme izni veriyoruz. Beğeni aldığımız durumlarda mutlu oluyoruz. Ancak. bizim için son derece hassas olabilen bu paylaşımları yaparken gerçekten olması gereken dikkati gösteriyor muyuz?

Sosyal medya mecrasının yaygınlaşmasının bir başka nedeni de toplumsal olaylardan anında haberdar olabilme kolaylığıdır. Bu mecralar aynı okuldan mezun olan öğrenciler, aynı sitede oturan site sakinleri veya aynı derneğe üye kişilerin birbirleriyle haberleşmelerini sağlayan ideal ortamlar haline gelmiştir.

Ne var ki, temelinde çok masum ve bir o kadar da yararlı olan bu iletişim ortamlarını kullanırken bazı temel güvenlik kuralları ile kendimizi ve sevdiklerimizi kötü niyetli kişilerden korumamız gerekir. Prensip edineceğimiz bu kurallar şöyle sıralanabilir:

1. FARKINDALIK

Listemizde bulunan profillerin gerçek sahiplerine ait olduğundan emin miyiz?

Sosyal medya sitelerinde sahte profil üretmek hâlâ çok kolaydır.

2. KONTROL

Gelen arkadaşlık davetlerini kolayca kabul ediyor muyuz?

Sadece yazdığımız bir iletiyi "like" etti diye hiç tanımadığımız bir kişiyi arkadaş listemize eklememeli, onun hakkında daha fazla bilgi sahibi olmalıyız. Tanıdığımız bir kişiye ait gibi görünen ancak kayıtlı profili dışındaki ikinci bir profilden mesaj gelmesi durumunda, ilgili kişiye telefonla ulaşıp bu ikinci profilin doğruluğunu sorgulamamız, hem bizim hem de tanıdığımızın yararına olacaktır.

3. PROFİL

Bir sosyal ağ sitesinde profil oluştururken bilgilerimizi ne ayrıntıda yazıyoruz?

Profil oluşturma formlarında sorulan her alanı doldururken, özel bilgilerimizin istemediğimiz kişilerin veya dolandırıcıların eline geçme riski olduğunu unutmamalıyız.

4. CHECK-IN

Gerçek hayatta bulunduğumuz yerleri sosyal medya ortamlarında sıklıkla işaretliyor muyuz?

Eğer cevabımız "evet" ise, geçmişte hangi zaman aralığında nerelerde bulunduğumuz ve muhtemelen benzer zaman aralıklarında nerelerde olabileceğimiz başkaları tarafından tahmin edilebilir.

5. TEMİZLİK

Güncelliğini yitirmiş mesaj ve fotoğraflarımızı profilimizden siliyor muyuz?

Profilimize kaydettiğimiz tüm mesaj ve fotoğrafları, sonsuza kadar orada kalacakmış gibi değerlendirelim ve gönderelim. Güncelliğini yitirmiş olanları silmeyi ihmal etmeyelim.

6. E-MAIL

Kişisel e-mail adresimizi herkese açık şekilde yayınlıyor muyuz?

Kişisel e-mail adresimiz ile profil kaydı yapmamız durumunda bu adresin istemediğimiz kişilerin eline geçme ve daha çok istenmeyen e-mail alma ihtimalini artırmış oluruz. Sadece bu işlemler için bir e-mail adresi açmamız daha güvenli olacaktır.

7. FOTOĞRAFLAR

Kişisel fotoğraflarımızı yayınlarken aynı zamanda karşı tarafa ne tarz bilgiler verdiğimizi de biliyor muyuz?

Arabamız, mücevherleriniz gibi kişisel varlığımızın da herkese açık bir ortamda rahatça görünmesi, kötü niyetli kişilerin bizler hakkında daha çok bilgi sahibi olmasını sağlar.

8. SAHTE LİNKLER

Arkadaşlarımızdan gelen her linki çekinmeden açıyor muyuz?

Sosyal ağlarda oldukça fazla sayıda sahte link dolaşmaktadır. Bu linkler kullanılarak kişisel bilgilerimizi elde etmeye yönelik sahte adreslere yönlendirilebiliriz.

Facebook

Facebook sayfasında, en sağ-üst koşede bulunan küçük aşağı ok menüsünün içindeki "Ayarlar" (Settings) sayfasında yer alan "Güvenlik" (Security) adımında oldukça detaylandırılmış ve zamanla yeni özellikler eklenmiş seçenekler sunulmaktadır. Buradaki her adım tek tek incelenmeli ve güvenlik bilinci ile seçim yapılmalıdır.

Hemen "Güvenlik" (Security)'nin altında yer alan "Gizlilik Ayar ve Araçları" sekmesinde ise, aşağıdaki üç soruya cevaben geçerli olan konfigürasyon kontrol edilmelidir.

» Paylaştıklarımı kimler görebilir?
» Benimle kimler iletişim kurabilir?
» Aramada beni kimler bulabilir?

"Zaman Tüneli ve Etiketleme Ayarları" sekmesi için aşağıdaki soruların cevabı kontrol edilmelidir.

» Zaman tünelime kimler bir şey ekleyebilir?
» Zaman tünelimdeki şeyleri kimler görebilir?
» İnsanların eklediği etiketleri ve etiketleme önerilerini nasıl yönetebilirim?

Whatsapp

Kullandığınız uygulamanın Mayıs 2016 sonrasına ait bir versiyon olduğundan emin olun. Bu sayede iletişiminiz uçtan uca şifreli olacak ve araya girecek başkaları tarafından takip edilemeyecektir. Settings-> Account -> Privacy bölümünde "Everyone" olarak görünen parametreleri "My Contacts" olarak değiştirmeniz listenizde olmayan kişilerin sizi izlemesini güçleştirecektir.

Twitter

"Profil ve ayarlar" bölümünden "Güvenlik ve gizlilik" sekmesi ayrıntılı seçenekler sunmaktadır. Güvenlik alanındaki "Giriş doğrulaması", "Şifre sıfırlama" ve "Kodla giriş yap" her üç seçeneğinin de aktif hale getirilmesi gerekir.

Instagram

"Profil ve ayarlar" bölümünden "Photos are private" bölümünü "ON" durumuna getirin.

Güvenli bir sosyal medya kullanıcısı olmanız dileğiyle...

YAZAR HAKKINDA

Kayıhan Altınöz yaklaşık 20 yıllık sektör tecrübesine sahip olup, telekom, finans, telekom ve üretim şirketlerinde bilgi güvenliği ekiplerinde çeşitli pozisyonlarda çalışmıştır.