



Sosyal Medya Güvenli Sular mı?



Dikkat edin son dönemlerde siber suçlarla ilgili haberlerde yine bir artış var. Malum internet trendlerini en az 2-3 yıl geriden takip etmek gibi bir huyumuz vardır. Siber suçlarda da durum böyle aslında. Çoğu abartılı, teknik bilgi yoksunu kişiler tarafından yazılan bu haberleri gelin yine de hafife almayın! Aksi takdirde, sosyal medya faaliyetleriniz nedeniyle işinizi ve çevrenizi bile kaybedebileceğinizin farkında mısınız?

Internet üzerinden erişim ve etkileşim arttıkça bu durumun yanında bazı riskler getirmesi de kaçınılmaz olmaktadır. Ama merak etmeyin durum bilgisayarınızı kapatıp, modemini ADSL bağlantısını sağlayan kabloyu çekmenizi gerektirecek kadar vahim değil. Birkaç basit kurala uyararak sosyal medyanın güvenli sularına açılabilirsiniz.

Önce Wikipedia'dan noktasına virgüline dokunmadan sosyal medyanın ne olduğuna dair tanımı aktaralım:

“Zaman ve mekan sınırlaması olmadan (mobil tabanlı), paylaşımın, tartışmanın esas olduğu bir insan-iletişim şeklidir. Sosyal medya platformlarında insanlarla buluşur ve iletişimde bulunursunuz. İnsanlara yardım eder, yardım alır sorularına cevap verir ve kendi sorularınızı sorarsınız. Bu bakımdan sosyal medya informal eğitim yollarından da birtanesidir.”

Keşke kullanım ve uygulama gerçekten bu kadar iyi niyetli ve masumane olsa...

İnternet iletişimi yıllardır takma isimler üzerinden yürürken, Facebook bu konudaki anlayışı temelden sarstı. Bugün Facebook'ta takma isim kullanmak, sistemden uzaklaştırılma sebebi.

Bugün Facebook'ta takma isim kullanmak, sistemden uzaklaştırılma sebebi.

Hem bu platformda gerçek adınızı kullanmamak; arkadaşlarınızın sizi bulamaması ve bütün o muhabbetten, paylaşımından uzak kalmanız anlamına da gelebilir.

Önde gelen IT güvenlik şirketlerinden Sophos tarafından yapılan bir araştırmaya göre; Facebook kullanıcılarının %41'i kendilerine gelen arkadaşlık tekliflerini kimden geldiğine bakmadan kabul ediyor. Güvenlik ayarlamaları ile ek önlemler almadığınız sürece, bu durum evinizin kapısını bir yabancıya açmanız ile eşdeğer.

Paylaşılan her doğum tarihi, e-mail adresi, lokasyon, adres, telefon numarası ve IM takma adları; “scammer”ler (mesela Afrika'da herhangi bir bankada çalıştığını iddia eden, bir sebepten dolayı bir çeki bozdurmak ya da para transferi yapmak için yardımınıza ihtiyacı olduğunu söyleyen kişi bir “scammer”dir) ya da “social engineer”ler (hassas bilgileri ele geçirmek için insanları faka bastırmaya çalışan kişiler olarak tanımlayalım) için bulunmaz nimettir.

Daha 10 yıl önce bu tür bilgilere ulaşabilmek için o

kişiyi gece gündüz takip etmeniz gerekirdi. Şimdi ise bu tür bilgiler sadece bir tık uzağınızda.

Facebook ya da diğer sosyal medya ortamlarında, arkadaşlarınızı ince eleyip sık dokuyun. Gerçek hayatta 1500 arkadaşınız yokken Facebook'da nasıl olabilir ki?

En iyisi, her dahil olduğunuz sosyal ağda güvenlik ayarlarını en üst düzeyde tutun. Her şeyi kapalı ve gizli tutun. Sisteme alıştıkça ve yakın arkadaş çevreniz oluştuğunda kişiye özel hakları gevşeterek yolunuzu devam edersiniz.

Sosyal medyada paylaştığınız resimlere, videolara ve yazdığınız mesajlara dikkat edin.

Mesela vur patlasın çal oynasın yaptığınız ve sarhoş olup masanın üstünde dans ettiğiniz geceye ait fotoğraflar bilgisayarınızın sabit sürücüsünde kalsın. Siz her baktığınızda gülümsüyor olabilirsiniz ama patronunuz görmese daha iyi olabilir.

Kendinize şöyle basit bir kural koyun: “annenizin görmekten sıkıntı, utanç duyacağı şeyleri internette

paylaşmayın.” Eski moda gibi görünebilir ama işe yarayacağına emin olabilirsiniz. Ya da herkese açık ortamlarda

gittiğiniz bir iş görüşmesini anlatmayın. Yine şu anki patronunuzun hoşuna gitmeyebilir.

ABD'de şirketlerin %8'i, en az bir elemanını sosyal medyada yazdığı yorumlar ya da uygunsuz davranışlar yüzünden işten çıkarmış durumda. Burada bahsettiğimiz, belden aşağı konularda faaliyet gösteren siteleri gezmek değil. Mesela şirketi Twitter'da kötülemek bu kapsama giriyor.

Görülebileceği gibi, sosyal medyada güvenlik demek kendini sadece dolandırıcılara karşı korumaya çalışmak değildir!

Yine mesajlarınızda kişisel ve hassas bilgiler paylaşmayın. Telefon numaranız, o an nerede olduğunuz ya da tatile gideceğiniz gibi bilgiler sizde saklı kalsın.

Takma ad kullanabileceğiniz platformlarda takma ad kullanın.

Mesela iş yerinize ait telefon numarasını, adresini

İNTERNET DÜNYASI

paylaşmayın. Yazışmalar için iş değil, özel e-mail adresinizi kullanın.

Hadi sahtekarlardan vazgeçtik; sosyal medyada tanışıp, bir gece çıkıp pek beğenmediğiniz bir hanımefendi ya da beyefendinin öbür gün iş yerinizin kapısına dayanmasını istemezsiniz.

Yine aynı şekilde iş yerinizi tanımlarken kullandığınız ifadelere dikkat edin. Şirketinize ait sırları ve "aile" için de kalması gereken olayları ulu orta ifşa etmeyin.

Yine benim de ağırlıklı olarak dikkat ettiğim bir konu iş ve özel arkadaşlarınızı birbirinden ayrı tutmak. İş yaptığım insanlar XING ya da LinkedIn'de listemde bulunurken, Facebook hesabımda sadece gerçekten tatil resimlerimle ilgilenebilecek olan kişiler bulunmakta.

Sosyal medyalarda yayılan Koobface gibi solucanlara, zararlı yazılımlara karşı da uyanık olmanızda fayda var; çünkü verdikleri zarar genelde geri dönmeyecek düzeyde olabiliyor.

Bu tür solucan ve virüsler Facebook ya da Twitter gibi platformlarda sizi mesela çok komik olduğunu iddia ettikleri bir videoyu izlemeniz üzere bir linke tıklamaya davet ederler. Gerisi mahvolmuş bir bilgisayar, kaybolup gitmiş değerli bilgiler, resimler, yazılar oluyor. Arada ele geçmesi muhtemel gizli bilgiler saymıyorum bile.

Kullanımı çok yaygın olan URL kısaltma servisleri de potansiyel birer tehlike kaynağı. Yine aynı şekilde bilhassa Twitter ile bağlantılı hizmet sağlayan üçüncü partilerin ciddiyet ve güvenliğinin gözden geçirilmesinde büyük fayda var.



Sosyal medyada güvenlik demek, kendini sadece dolandırıcılara karşı korumaya çalışmak değildir!

Mesela yukarıda tarif geçen vur patlasın çal oynasın gecesinin resimleri sizin için ne kadar sıkıntı verici ise yan masanızda oturan iş arkadaşınız için de o kadar sıkıntılı olabilir. Nede olsa masa üzerinde sarhoş dans eden tek kişi siz değildiniz!

Koca koca IKEA dolaplarını, kılavuzunu okumadan birleştirmede ya da en son model ses sistemimizi kullanım kitapçığının kapağını bile açmadan kurmada üzerimize yoktur. Ama siz yine de kullandığınız sosyal medya aracının gizlilik ve kullanıcı sözleşmelerini okumadan geçmeyin.

Bankaların bazı güvenlik aşamalarını cep telefonunuz ile birleştirmiş olması akıllıca görünebilir ama cep telefonu diz üstü bilgisayardan daha kolay unutulmuş ya da çalınan bir alet. Cep telefonunuzu gözünüzün önünden ayırmayın. Gözünüzün önünden ne kadar ayırmasanız da o cep telefonuna şifrelerinizi kayıt etmeyin. Ne olur ne olmaz!

Telefonunuza ait güvenlik ayarlarını da kurcalamaktan geri durmayın; en üst seviyede tutmaya bakın.

Yine son dönemin lokasyon bazlı servislerine dikkat etmesi gereken tek kişiler çapkın erkekler değil. Siz siz olun yine bu tür şeyleri çok fazla kullanmayın.

Peki bu kadar tehlide karşı çok dikkatli olmak dışında ne yapabilirim? Öncelikle internet tarayıcınızı ayarlarını tekrar gözden geçirerek işe başlayabilirsiniz. Şifrelerinizin hepsini hatırlamaya uğraşmaktan üşenen kişilerdenseniz ve her yerde aynı şifreyi kullanıyorsanız, size herhangi bir Password Manager programı kullanmanızı tavsiye ederim.

Bazılarının yukarıda yazılanlara gülüp geçtiğini: "hadi canım bu kadar da dikkatsiz olunur mu" ya da "abartılıyor canım" dediğini duyar gibiyim. Fakat şöyle bir araştırın bakalım; ofisinizde kaç kişinin bilgisayar şifresi doğum günü ya da eşinin / çocuklarının adı? Sandığınızdan çok değil mi?

Halen güvenli sularda olduğunuzu mu düşünüyorsunuz?