GÜVENLİ GÜNLER BÜLTENİ

Bilgisayar kullanıcılarına yönelik hazırlanır. Her ayın 15'i çıkar. Diğer sayılara erişmek ve sonraki mesajların direk posta kutunuza gelmesi için guvenligunler.com adresini ziyaret ediniz.

EKİM 2017

Güvenliğimizin İlk Cephesi: Parolalarımız

GÜNÜMÜZDE KREDİ KARTI HIRSIZLIĞI, BANKA DOLANDIRICILIĞI, WikiLeaks, telefon dinlemesi, fidye yazılım vs. derken, insanlık tarihinin en büyük ilerlemelerinden biri olarak bildiğimiz interneti kullanmaya korkar olduk.

Peki gerçekten de yapacak bir şey yok mu? Mahalle aralarındaki sokaklarda büyüyen bizler, nasıl şu an çocuklarımızı kapının önüne çıkarmaya korkuyorsak, gün geçtikçe internet de bu hale mi gelecek? Bunu engellemenin, en azından makul bir hale getirmenin bir yolu yok mu gerçekten?

Size bir iyi bir de kötü haberim var. İyi haber: tabii ki alınacak bazı önlemler var, hem oldukça basit ve masrafsız yöntemlerle. Bu yazıda güvenliği sağlamakla ilgili temel ilkelerden söz edecek ve doğrudan uygulayabileceğiniz bazı pratik tavsiyelerde bulunacağım.

1. Güvenliği kişisel hijyeniniz gibi görün

Arka planda ne kadar karmaşık işlemler (internet üzerinden havale, kredi kartı ile alışveriş ya da Netflix'ten film seyretme) yapılırsa yapılsın bu işlemleri güvenli kılmanız için almanız gereken temel önlem hep aynıdır: önce kendinizi (kimliğinizi) sonra kaynağınızı (paranızı/malınızı) korumak. Bunu da tıpkı kişisel hijyeniniz gibi ele almanız gerekir. Nasıl sağlığınızı korumaya özen göstermeyip bulunduğunuz ortamlara, yediğinize içtiğinize

dikkat etmeyince hastalıklardan kaçınamazsanız, güvenliğinize dikkat etmeyince de eninde sonunda hack'lenirsiniz.

Dahası, temizliğine dikkat etmeyen birinin çevresindekiler için de potansiyel bir sağlık tehlikesi oluşturması gibi, siz de bu şekilde istemeden de olsa sevdiklerinize zarar verebilirsiniz.

Eminim bu yazıyı okuyan herkes, Facebook'tan para isteyen bir yakının yarım saat sonra arayıp hesabının hack'lendiğini ya da telefonunun çalındığını söylediğine şahit olmuştur.

O kişi olmayın!

2. Karşınızdakini gerçekten tanıyor musunuz, emin olun

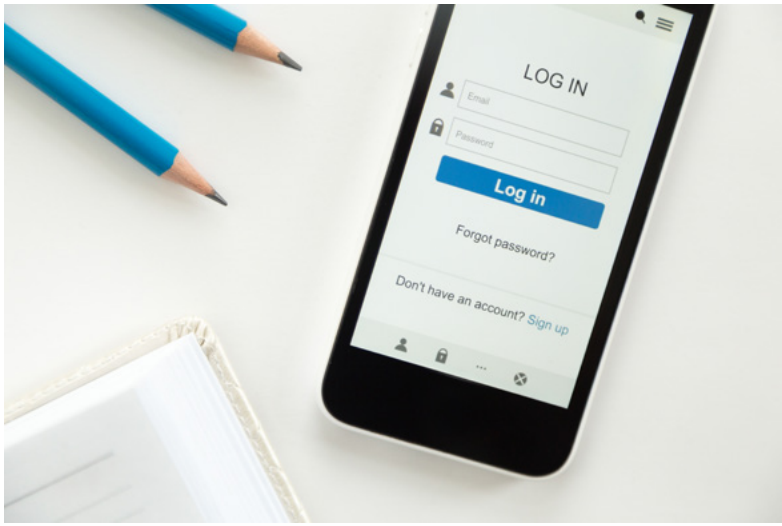
Bazen ayağınıza kadar gelen bir fırsat ('son 5 üyeye tv hediyemiz var, kaçırmayın'), bazense hiç beklemediğiniz bir e-posta ('fatura detaylarınız ektedir') sizi tehlikelerle karşı karşıya bırakabilir. İnternette herkesin herkesle iletişime geçebileceğini ve kimin kim olduğundan emin olamayacağınızı unutmayın. Konu ne kadar kritik görünürse görünsün karşınızdakinin söylediği kişi olduğundan emin olmadan herhangi bir girişimde bulunmayın. Whatsapp'tan borç isteyen arkadaşınızı, en azından sesini duymak için arayın ya da size ekstre yollayan banka e-postasının ayrıntılarına bakmadan pdf'e tıklamayın.

3. Güvenin ama yine de teyit edin

Günümüzün iş dünyası birçok noktada karşılıklı güven üstüne kuruludur. Dolayısıyla "hiç kimseye güvenmeyin" gibi bir ilke ne pratiktir ne de psikolojik açıdan uygulanabilirdir. Karşınıza çıkacak insanların büyük bir kısmı da sizin gibi güvene layık insanlardır kuşkusuz. Ancak bu, kayıtsız şartsız herkese güveneceğiniz ya da en azından o işin yapılıp yapılmadığını kontrol etmeyeceğiniz anlamına gelmez. Bankaya giden komşunuza birkaç yüz liralık aidatınızı emanet edin ama sonra ödenmiş mi ödenmemiş mi bakmayı unutmayın.

4. Hiçbir şeyi, özellikle de e-postanızı tek bir parolaya emanet etmeyin

Parolalar kaybedilebilir, tahmin edilebilir ya da ele geçirilebilir. Bu nedenle mümkün olan her hesabınızda ikinci bir aktif parola kullanın. Bu sayede sizi hack'leyecek kişilere karşı çok önemli bir güvenlik önlemi almış olursunuz.



5. Telefonunuzu, e-postanızı ve bankacılık parolanızı kimseye emanet etmeyin

İnternet üstünden yapılan dolandırıcılıklar her zaman kimlik hırsızlıkları ile bağlantılıdır ve günümüzde kullandığımız bazı araçlar kimliğimizin doğrulanması bakımından diğerlerine göre çok daha ön plandadır.

Bunların en önemlisi tartışmasız akıllı telefonlarımızdır. Siz banka hesabınıza ve e-postanıza çift parola (çift faktörlü yetkilendirme) tanımlarsınız ama bu parolalar ekran kilidi olmayan

telefonunuza gelir ve telefonunuzu çalmış olan kişi... Dolayısıyla e-posta ya da sosyal medya hesaplarınız için ne tür önlemler alırsanız alın, bunların hemen hepsi telefonunuzu kaybettiğiniz anda geçersiz kalır. Eğer güvenlik konusunda tek bir önlem alacaksanız cep telefonunuzu parolasız açılamaz hale getirin ve bu parola da en az altı basamaktan oluşsun. (Hayır, parmak izi parolanın yerini tutmaz, isteyen uyuyan babasının parmak izi ile araba almaya kalkan kızın hikayesini internetten bulup okuyabilir.)

Telefon için aldığınız önlemlerin aynını dizüstü bilgisayarınız ve tabletiniz için de almanız yararlı olacaktır.

Telefon ve bilgisayardan sonra korumanız gereken en önemli şey ise e-postanızdır. İçinde birçok önemli yazışmanın (belki de bazı kimlik belgelerinin şifrelerinin) olması bir yana, e-postanız başka hesaplarınıza ait parolaların reset'lenmesi işleminde kullanıldığı için de kritik öneme sahiptir. E-postanızı korumanın en pratik yolu çift parola kullanmak ve ikinci parolanın sms ya da başka bir yolla telefonunuza gelmesini sağlamaktır. Böylece virüs vs. yoluyla bilgisayarınızı ele geçiren biri bile e-postalarınıza ulaşmak için telefonunuza ihtiyaç duyar.

Hatırlarsanız yazının başında "Bir iyi bir de kötü haberim var" demiştim.

Kötü haber: Bu ilkeleri her an disiplinle, gevşetmeden uygulamanız gerekir. Tıpkı tecrübeli bir şoförün üşengeçlik ya da ihmalkârlık sonucu yaptığı tek bir kritik hatayla geri dönülemez zararlara yol açması gibi, siz de, bu ilkeleri bir kez göz ardı etmeniz, umursamamanız durumunda hem kendinizin hem de çevrenizdekilerin güvenliğini tehlikeye atmış olursunuz.

YAZAR HAKKINDA

Kıvılcım Hindistan
CISA/CISSP/CRISC
ISO 27001 / BS 25999 LA
@kivil