Internet of Me – Çevrimiçi Kimliğinizi Korumak

Çevrimiçi güvenliğinizi korumayla ilgili 10 ipucu

İPUCU 1: Özel bilgileri ÖZEL tutun

Özel bilgiler, kimliğinizi belirleyebilecek hassas bilgilerdir. En sevdiğiniz renk özel bilgi olamaz, çünkü en iyi arkadaşınız da bu rengi seviyor olabilir. Ancak, ev adresiniz kesinlikle özel sayılır ve tanıştığınız herkesle paylaşmamanız gereken bir bilgidir. Özel bilgiler, kimlik bilgilerinizi, biyometrik kayıtlarınızı, pasaport numaranızı, ev veya cep telefon numaranızı, parolalarınızı ve doğum tarihinizi kapsar. Bu bilgiler, doğum yeriniz veya annenizin kızlık soyadı gibi diğer kişisel veya tanımlayıcı bilgilerle birlikte kullanıldığında, kimlik hırsızlığına veya çok daha kötüsüne neden olabilir.

İPUCU 2: HTTPS'yi S'siz kullanmayın

HTTPS'nin sonunda yer alan "S" harfi, İngilizcedeki "secure" yani "güvenli" sözcüğünden gelir. Bu da verilerinizi Internet üzerinden iletirken şifrelemenin kullanıldığı anlamına gelir. (S'siz kullanılan) HTTP'nin aksine, HTTPS, bilgisayarınızın ağ tarayıcısı ile web sitesi arasındaki tüm bilgilerin, parolalarınızı, kredi kartı bilgilerinizi ve özel bilgilerinizi öğrenmek isteyen suçlulardan korunmasını sağlar. Çevrimiçi alışveriş yaptığınızda, bankanızın web sitesini ziyaret ettiğinizde veya herhangi bir özel hesapta oturum açtığınızda, web sitesi adresinin yazdığı URL kutusunun sol üst köşesinde "S"li veya "yeşil kilit"li HTTPS bulunmasına dikkat ederek kötü adamlardan uzak durabilirsiniz.

İPUCU 3: Tıklamadan önce düşünün

En iyi güvenlik yazılımı bile, güvenli olmayan bir bağlantıyı tıklamanız durumunda başınızın derde girmesine karşı sizi korumayacaktır. Güvenli olmayan bağlantılar, komik videoların, şok haberlerin, özel hesapların, harika tekliflerin veya "beğen" düğmelerinin kısa yolları gibi görünebilir. Ancak, bunlar aslında, kişisel bilgilerinizi çalmak veya bilgisayarınızı ele geçirmek amacıyla tasarlanmıştır. Arkadaşlarınız da bilmeden güvenli olmayan bağlantıları e-postayla, Facebook paylaşımlarıyla ve anında iletilerle gönderebilirler. Buna ek olarak, web sitesi reklamlarında ve arama sonuçlarında güvenli olmayan bağlantılara denk gelebilirsiniz. Gelecek sefer yeni bir bağlantıyla karşılaştığınızda, şu tehlike işaretlerine dikkat edin:

- Birisi size bir bağlantı göndermiş ama gönderen kişiyi tanımıyorsunuz.
- Hesabınız devre dışı kalmadan önce bir bağlantıya tıklamanız gerektiğini ileri süren iletiler.
- Üzerine geldiğinizde, görünenden farklı bir URL'si olan bağlantılar.

İPUCU 4: E-postalara dikkat edin

Kötü adamlar her gün gelen kutularımızı istenmeyen postalarla dolduruyorlar! E-postalarını belirlemek biraz zor olabilir, çünkü genellikle bir konuda yardım sağlayan meşru bir kaynaktan gönderilmiş gibi görünüyorlar. Örneğin, "hayatınızın teklifi"ni sunmak, kazandığımız olağanüstü ödülleri duyurmak veya güvendiğimiz bir şirketin acil bir uyarısını iletmek. Aslında, bu sahtekarların sizden gerçekten istediği tek şey, onlara kullanıcı adınızı ve parolanızı veya kredi kartı bilgilerinizi vermeniz veya onlara biraz para transferi yapmanız. Kötü dilbilgisi kullanan,

derhal ilgilenmenizin gerektiğini ileri süren ve acil olduğu konusunda ısrarcı olan e-postalardan ya da parolalarınıza ve/veya diğer kişisel bilgilerinize yönelik isteklerden şüphelenin.

İPUCU 5: Yazılımları düzenli olarak güncelleyin
Bilgisayarınızdaki yazılımları güncellemek, güvenlik sorunlarının "yama" ile düzeltilmesine olanak tanır. Bu da, bilgisayarınızda bulunan tüm bilgilerin bilinen güvenlik açıklarından korunmasını sağlar. Otomatik güncellemeler, güvenlik açıkları bulunur bulunmaz gerekli yamaların uygulanmasını sağlamanın en iyi yoludur. Manuel güncellemeler, hiç güncelleme yapılmamasından daha iyi olsa da, yama kullanıma sunulduğunda bilgisayarınızı otomatik olarak güncellemeyi unutmanız açısından sorun teşkil edebilir.

İPUCU 6: Parolaları düzenli olarak değiştirin
Bir kişinin hesaplarınızdan birinin parolasını öğrenmesi durumunda, söz konusu hesapla ilişkilendirdiğiniz kişisel bilgilerin tümüne erişmesi mümkün olabilir. Örneğin, çevrimiçi banka hesabınızın hesap numarası veya okul hesabınızda bulunan ev adresiniz. Bu nedenle, parolanızı her 6-9 ayda bir değiştirerek saldırganların uzun bir süre boyunca erişimi sürdürmesini engellemelisiniz.

İPUCU 7: Karmaşık parolalar oluşturun
Parolanızın bir bilgisayar korsanı tarafından "ele geçirilmesini" engellemek için karmaşık bir parola oluşturduğunuzdan emin olun. Karmaşık bir parola, büyük ve küçük harf, sayı, simge içerir ve en az 8 karakterden oluşur. Sözlükte bulabileceğiniz türden sözcükleri kullanmaktan sakının. Örneğin, eski parolanız "Ilovecats" ise, cümleyi bozacak şekilde karmaşık bir parola oluşturarak "!_L0V3_ c@t$" ifadesini kullanabilirsiniz. Ancak yine de, bir parola yöneticisi kullanabilirsiniz. Parola yöneticisi, kullanıcının parolaları depolayıp düzenlemesine yardımcı olan bir yazılım uygulamasıdır. Parola yöneticileri genellikle parolaları şifreli olarak depolayarak kullanıcının bir ana parola oluşturmasını gerektirir. Bu ana parola, kullanıcının parola veritabanının tamamına erişmesini sağlayan, çok güçlü olması tercih edilen, tek bir paroladır.

İPUCU 8: Ücretsiz WiFi'ye dikkat edin
Ücretsiz WiFi, ücretsiz kullanımın bilgisayar korsanları dahil herkese açık olması demektir. Suçlu veya bilgisayar korsanı özel bir yazılım kullanarak ziyaret ettiğiniz web sitelerini ve gönderdiğiniz bilgileri görebilir. Bu nedenle, genel kullanıma açık WiFi kullanırken, çevrimiçi bankacılık, okul hesapları, sosyal medya siteleri gibi kişisel verilerinizi saklayan veya bilgisayar korsanlarının erişim sağlamayı isteyeceği web sitelerini ziyaret etmemelisiniz. Özetle, genel kullanıma açık WiFi yalnızca Internet'te gezinmek için kullanılmalıdır.

İPUCU 9: Tüm hesaplarınızda oturumu kapatın
Ortak bir bilgisayar veya size ait olmayan herhangi bir cihaz kullanırken, hesaplarınızda oturumu kapattığınızdan emin olun ve her zaman "parolayı kaydet" kutusunun işaretli olmadığından emin olmak için kontrol edin. Bu, sonraki kullanıcının, güvenli olmayan hesaplarınıza erişmesini engelleyecektir. Oturumu kapatmaya ek olarak, tanımlama bilgilerini ve göz atma geçmişini de silerek sonraki oturumda yanlışlıkla hesabınızın kurtarılmadığından emin olabilirsiniz.

İPUCU 10: Başkalarında farkındalık yaratın
Bu çalıştayda öğrendiğiniz her şey, arkadaşlarınızın ve ailenizin de işine yarayabilir! Tüm bu bilgileri kendinize saklamayın; başkalarında farkındalık yaratın! Okuldaki arkadaşlarınıza daha iyi bir parolayı nasıl oluşturabileceklerini anlatın. Ailenizdekilere, işleri bittikten sonra hesaplarının tamamında oturumu kapatmalarını söyleyin. Herkesi, özel bilgilerini özel tutmaları için teşvik edin. Arkadaşlarınız Starbucks'ta bir fincan kahve içerken, onlara genel kullanıma açık WiFi'de oturum açmanın tehlikelerini anlatın.