**KİMLİK HIRSIZLIĞI, NASIL ÇALIŞIR, KORUNMANIN YOLLARI, KARŞILAŞTIĞINIZDA HAKLARINIZIN VE MAĞDURİYETİNİZİN GİDERİLMESİ NELERDİR?**

Hepimiz dijital dünyanın ve internet çağının fırsatlarından yararlanıyoruz. Aynı şekilde sosyal medya araçları da hayatımızın en önemli parçalarından biri ve biz tüm bunları kullanırken, bizim görmediğimiz birileri de bizim özel ve gizli bilgilerimize ulaşmaya çalışıyor. Peki, kim bunlar? Kimlik Hırsızları.

Kimlik hırsızları, TC numaralarınız, kredi kart bilgileriniz veya sosyal güvenlik numaraları gibi kişisel verilerinizi ele geçirir ve bunları hileli şekilde kullanırlar. Bu hileler ile krediye başvurma, e-ticaret üzerinden satın almalar, adınıza GSM hattı ve telefon alma, ev kiralama, dükkân kiralama, kiralanan yerin doğalgaz, internet, elektrik, su gibi faturalarını sahte kimlik ile adınıza geçirme gibi yaşa dışı işlerde kullanırlar. Sizin bunları fark etmeniz zaman alabilir. İşin farkına vardığınızda, iş işten geçmiş olur ve kimlik hırsızlığı kayıplarınızı büyütür.

Kimlik hırsızları, Sosyal mühendislik teknikleri ile bu bilgileri ele geçirirler. Sosyal ağlarda veya diğer popüler çevrimiçi hizmetlerde ki genel görüntüleriniz onların veri kaynağı olur. Aynı zamanda bilgisayarınıza gönderilen virüs ile sizi tuzağa düşürebilirler. Kişisel bilgileriniz, adres, telefon gibi verileriniz internette bulunuyorsa saldırıya uğrama riskiniz vardır. Eposta adresinizin, internet bankacılığı şifrenizi düzenli değiştirmiyorsanız, çöp kutunuza finansal, kişisel bilgilerinizi içeren fatura veya benzeri belgeleri kişisel bilgileriniz kısmını imha etmeden atıyorsanız, uçak biletinizi sosyal mecrada paylaşıyorsanız, ( üzerinde bulunan kare kod tüm kişisel bilgilerinizi içermektedir.) bilgisayarınızda veya serveranız da koruma programlarınız yoksa açık tehdit durumundasınız.

Mobil çağda internet bağlantısı olan her cihazı kullanırken, kişisel verilerinizi korumanın temel felsefesi, “**HER ŞEYİ MİNİMUMDA TUTUN**. ’dur. Sosyal medyayı tedbirli kullanın, asla kişisel bilgilerinizi paylaşmayın, sosyal mesajlaşma hizmet yolu ile kişisel verinizi paylaşmayın. Doğum tarihinizi paylaşmayın en azından yılınızı. Bir fotoğrafın nerede çekildiğini paylaşmaktan kaçının ve fotoğraflara tam konumu gösteren coğrafi etiketler eklemeyi bırakın. Adresinizi ifşa eden veya evinizde değerli eşyalarınızı nerede sakladığınızı gösteren fotoğrafları yayınlama konusunda dikkatli olun. Adınız, profil fotoğrafınız ve kapak fotoğrafınız her zaman "herkese açıktır" ve değiştirilemez.

Hırsızlar bu herkese açık bilgileri kullanarak benzer Facebook profilleri oluşturabilir ve önemli verileri çalabilecek casus yazılımlarla kullanıcıların cihazlarına virüs bulaştırabilirler. Bilgisayarınızda ve sosyal mecralarınızda güçlü, karmaşık parolalar kullanın. Birden fazla hesap veya hizmet için aynı parolayı hiçbir zaman kullanmayın. En azından birine saldırı olursa, diğerleri savunmasız kalmasın. Mümkünse, parola koruması olmadan herkese açık Wi-Fi'lardan kaçının. Başka seçeneğiniz yoksa tüm iletişiminizi şifreleyecek ve böylece sizi dinleyen suçlulardan koruyacak bir sanal özel ağ (VPN) kullanın. Sosyal medya hesaplarınızı arkadaşınız olmayan kişilerin görüntülemesini engellemek, gizlilik ayarlarınızı değiştirmek, güvenliğinizi bir kademe daha arttıracaktır. İstediğiniz satıcının web sitesine yönlenen bağlantıyı tıklatmak yerine, satıcının URL'sini web tarayıcınızın adres çubuğuna girmeniz daha güvenli olacaktır. URL'yi yazmak daha uzun sürse de bu basit işlem sahte veya kötü amaçlı bir web sitesini ziyaret etmenizi önleyebilir.

Tüm akıllı telefonlarda üç temel güvenlik unsuru vardır. Mobil cihaz kullanıcısı olarak, bu katmanların farkında olup onları cihazlarınızda etkinleştirmektir:

Cihaz Koruması: Cihazınızın kaybolması veya çalınması durumunda verilerin uzaktan "silinmesine" izin verilmesi gerekir.

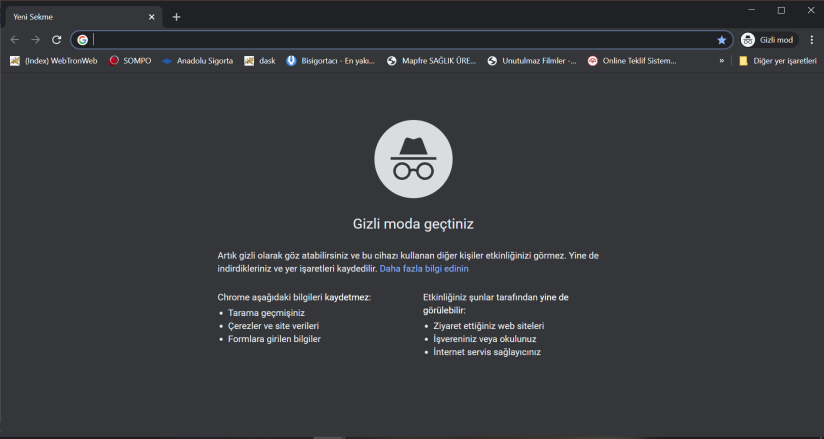
Veri Koruması: Kurumsal verilerin, aynı cihazda veya kişisel ağda çalışan kişisel uygulamalara aktarılmasını engellemek gerekir.

Uygulama Yönetimi Güvenliği: Uygulama içi bilgilerinizi ele geçirilmeye karşı korumanız gerekir.

Temel bir kural olarak, üçüncü taraf uygulama sağlayıcılar yerine yalnızca Apple, Google Play veya Microsoft mağazalarını kullanmanız gerekir. Ancak resmi mağazalardayken bile cihazınıza şüpheli bir şey indirmediğinizden emin olmak için her zaman yorumları okuyun. [Mobil bankacılık saldırılarının %98'inden fazlası Android cihazları hedef alır](https://www.kaspersky.com/blog/android-banking-trojans/9897/). Bu şaşılacak bir durum değildir. Android, dünyadaki en popüler mobil platformdur (küresel akıllı telefon pazarının %80'inden fazlasını oluşturur) ve tüm popüler mobil platformlar arasında yalnızca Android dışarıdan yazılım yüklemeye izin verir. Bu nedenle konum paylaşımını kapatın, bluetooth’u kapatın, gizlilik ve güvenlik ayarlarını kontrol edin, başkalarının hesaplarınıza erişmesini engellemek için extra güvenlik kalkanı kullanın, telefonunuza antivürüs programı yükleyin.

Bu önlemleri almanız yeterli mi? Tabi ki hayır. E-devletten düzenli adınıza açılan hat var mı? Dava var mı? İcra takibi var mı? Çalıştığınız bankalarda kredi kullanımı var mı? Kredi kartınızda tanımadığınız harcama kalemi var mı? Trafik cezaları, HGS ve OGS geçiş ihlalleri ile vergi borçları da var mı? Bunların düzenli kontrolünü sağlanmanız size sonradan fark edilen bu durumlarda tek tek itirazı için fazladan harcayacağınız zaman ve para kaybınızın önüne geçecektir. Bunların yanı sıra BEDAŞ, İGDAŞ ve İSKİ gibi kurumlara gidip abone numaranızı vererek, yeni abonelik açtırmayacağınızı ve adınıza açılan böyle abonelikler olursa, bunlardan doğacak borçlardan sizin değil kurumun sorumlu tutulacağını belirten bir dilekçe verebilirsiniz.

Yine aynı şekilde GSM operatörlerine de mevcut numaranızı bildiren, ıslak imzanız olmadan yeni hat açtırmayacağınızı ve bu konuda sorumluluk kabul etmeyeceğinizi belirten bir dilekçe yollayabilirsiniz. Güveninden emin olmadığınız internet veya mobil araçta GOOGLE CHROME‘u kullanın, Ctrl - Shift - N aynı anda basarak, GOOGLE CHROME gizli moda geçirerek işleminize güvenli devam edebilirsiniz.



Bunca önlemi aldığınız ama kimliğinizi paylaştığınız özel teşebbüs veya kamu kurumuna yapılan siber bir saldırıdan kimlik bilgileriniz çalındı. Savcılığa suç durusunda bulunmanız ve tüm kimliğiniz ile bağlantılı mail, sosyal medya, uygulama şifrelerini değiştireceksiniz. Kredi kartınızı, banka kartlarınızı işleme kapatıp yenisini talep etmeniz gerekli. Savcılıktan alacağınız suç duyurusu belgenizi, GSM operatörünüze, adınıza olan tüm fatura kurumlarına, çalıştığınız bankalara bildirmeniz süreç içinde yaşayabileceğiniz sorunların önüne geçecektir. Çünkü kimliğinizi kopyalayan kişi veya kişilerin savcılık aracılığı ile emniyet birimlerinin hırsızın kimliğini tespit edene kadar tehdit altındasınız.

Jülide ÇİLİNGİR