Herkes İçin Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

Yolculuğunuz Boyunca Güvenli Olmak

Giriş

Teknolojiden en yüksek oranda yararlanmanızı sağlamaya yardım etmek istiyoruz ve buna seyahatleriniz de dahil. Bu sayıda yolculuğunuzda cihazlarınızla hem internete bağlanıp hem de nasıl güvenle kullanacağınızı paylaşacağız.

Konuk Yazar

Mark Williams BlueCross Blueshield of Tennessee'de Kurumsal Güvenlik Mimarıdır. Aynı zamanda SANS eğitmeni ve ISSA Chattanooga şubesinin başkanıdır. Oldukça yoğun seyahat eder ve sizlerin teknolojik araçlarınızla birlikte yolculuk yaparken karşılaştığınız sorunları bilir.

Ön Kontrol

Ev ya da işyerindeki ağınız güvenli olabilir ancak yolculuk yaparken bağlandığınız ağların güvenilmez olduğunu varsaymak zorundasınız. Kimlerin sizinle aynı ağda olduğunu ve neler yaptığını bilemezsiniz. Yolculuk yaparken bilgilerinizi korumak için aşağıda yer alan birkaç basit adım size çok yardımcı olabilir :

- En güvendeki bilgi, sahip olmadığınız bilgidir. Yanınızda götüreceğiniz cihazlarınızda hangi bilgilere ihtiyacınız olmadığını belirleyin ve gereksiz bilgileri kaldırın. Bu, eğer cihazınızı kaybeder, çaldırır veya cihazınıza sınır görevlisi ya da gümrük tarafından el konulursa önemli ölçüde olumsuz etkiyi azaltmanıza yarayacaktır. Eğer bir iş gezisi ise danışmanlarınıza şirketin yolculukta kullanabileceğiniz olası başka bir cihaz temin edip edemeyeceğini sorun.
- Tüm mobil cihazlarınızı güçlü bir şifre ile kilitleyin. Bu yolla, eğer cihazınızı kaybeder ya da çaldırırsanız, insanların sizin bilgilerinize ulaşmasını engellersiniz. Ek olarak verilere ulaşılmasını engellemek için tüm disk şifreleme ile mobil cihazlarınızı ve dizüstü bilgisayarlarınızı şifreleyin. Birçok mobil cihazda bu özellik, siz ekran kilidi için parola belirlediğinizde aktif hale gelir.
- Cihazınız çalındığında ya da kaybettiğinizde uzaktan cihazınızın nerede olduğunu takip etmek ve hatta uzaktan içindeki bilgileri silmek için bir yazılım yükleyin ya da varsa etkinleştirin.
- Son versiyonlarını kullandığınızdan emin olmak için cihazlarınızı, uygulamalarınızı ve anti-virüs yazılımlarınızı güncelleyin. Birçok saldırı, güncel olmayan yazılımları kullanmaya odaklanır.
- Tüm cihazlarınızı tamamen yedekleyin. Bu yolla, eğer siz seyahatte iken cihazlarınızın başına herhangi birşey gelse bile güvenli bir yerde duran tüm verilerinize ulaşabilirsiniz
- Uluslararası yolculuklarınızda, mobil servis sağlayıcınızın sunduğu servisleri kontrol edin. Genellikle servis

Yolculuğunuz Boyunca Güvenli Olmak

sağlayıcılar uluslararası veri kullanımı için oldukça yüksek tutarlar faturalandırmaktadır ve belki de mobil verinizi kapatmayı ya da yerel bir ön ödemeli kart almayı tercih edebilirsiniz.

Yolculuğunuz boyunca güvenli olmanın anahtarı cihazlarını evden ayrılamadan güvenli hale getirmek, fiziksel olarak emniyette tutmak ve tüm çevrimiçi aktiviteleri şifrelemektir.

Kaybolan/Çalınan Cihazlar

Yolculuğunuza başladığınızda fiziksel olarak cihazlarınızın emniyette olduğundan emin olun. Örneğin, hiçbir zaman cihazlarınızı arabada insanların görebileceği bir yerde bırakmayın çünkü hırsızlar arabanın camını kolayca kırarak değerli olan herşeyi alabilirler. Verizon'un yakınlarda gerçekleştirdiği bir araştırmaya göre insanların cihazlarınızı kaybetme olasılıkları, çaldırma olasılıklarından 100 kat daha fazla. Bu da seyahat sırasında, örneğin havaalanında güvenlikten geçerken, taksi, restoran ya da otel odasından ayrılırken veya uçaktan inerken, cihazınızı iki kez kontrol etmeniz gerek demek oluyor.

Wi-Fi Erişimi

Seyahat ederken internete erişmek çoğu zaman otelde, kafelerde ya da havalanında ortak kullanılan Wi-Fi erişim noktalarını kullanmak demek oluyor. Ortak kullanılan Wi-Fi erişim noktalarının problemi sadece bu ağı kimin kurduğunu bilmemeniz değil, kimin bu ağa bağlandığını bilememeniz. Hal böyle olunca bu noktalar güvenilmez olarak algılanmalı, hatta yolculuğa çıkmadan tüm önlemleri almanızın nedeni bu. Ayrıca, Wi-Fi radio frekanslarını kullanarak sizin cihazınızla iletişime geçer, bu da size fiziksel olarak yakın olan herhangi birinin potansiyel olarak bu iletişime ulaşabileceği ve dinleyebileceği anlamına gelir. İşte bu yüzden ortak kullanılan bir Wi-Fi'ye bağlanıyorsanız, tüm çevrimiçi aktivitelerinizin şifrelenmiş olduğundan emin olun. Örneğin, tarayıcınız ile çevrim-içi işlem yapıyorsanız ziyaret ettiğiniz ağ sitelerinin şifreli iletişimi desteklediğinden emin olun (URL'lerinde 'https://' ve kapalı bir asma kilit simgesi vardır). Bununla birlikte, tüm çevrim-içi aktivitelerinizin şifrelendiği VPN (Sanal Özel Ağ) hesabına sahip olabilirsiniz. Bu size şirketiniz tarafından verilmiş ya da kendi kullanımınız için bu özelliği almış olabilirsiniz. Eğer güvenebileceğiniz hiçbir Wi-Fi erişim noktası yok ise, mobil telefonunuza bağlanmayı düşünebilirsiniz (Uyarı: Daha önceden de belirtildiği gibi, uluslararası seyahat yaparken pahalı olabilir, mobil servis sağlayıcınızdan kontrol edin.)

Ortak Kullanıma Açık Bilgisayarlar

Otel lobilerinde ya da internet kafelerde kullanılan ortak kullanıma açık bilgisayarları hiçbir hesabınıza ya da hassas veriye erişmek için kullanmayın. Sizden önce kimlerin kullandığı hakkında hiçbir bilginiz olmadığı gibi ve bu ortak kullanılan

Yolculuğunuz Boyunca Güvenli Olmak

bilgisayara isteyerek ya da istemeyerek virus bulaştırmış olabilirler. Mümkün olan her yerde çevrim-içi aktivitelerinizde sadece kontrol edebileceğiniz ve güvendiğiniz bilgisayarları kullanın. Ortak bilgisayarlar ancak hava durumu ya da haberler gibi ortak bilgilere erişmek için kullanılmalıdır. Google hesabınız gibi hesaplarınıza erişmek, sizi izleyen siber saldırganlara davetiye çıkarmak anlamına gelebilir.

Daha Fazla Bilgi İçin

Aylık OUCH! güvenlik farkındalığı bültenine üye olun, OUCH! arşivlerine erişin ve securingthehuman.sans.org/ouch/archives adresini ziyaret ederek SANS güvenlik farkındalığı çözümleri hakkında daha fazla bilgi edinin.

Türkçe Çevirisi

Selma Süloğlu, ODTÜ Bilgisayar Mühendisliğinde doktorasını tamamlamış olup SOSoft Bilişim Teknolojilerinde biyometrik güvenlik sistemleri üzerinde çalışmaktadır.

Sema Yüce (https://tr.linkedin.com/in/semayuce), Türkiye'nin önde gelen kurumsal şirketlerinde ve özellikle bilişim, finans, telekomünikasyon, sigortacılık, sanayi, perakendecilik gibi sektörlerde; bilgi güvenliği, uyum, BT yönetişim/strateji, risk yönetimi, iş sürekliliği, hizmet yönetimi, altyapı hizmetleri, yazılım geliştirme ve program/proje yönetimi alanlarında yönetici ve danışman olarak 19 yılı aşkın süre görev yapmış olup, Nisan 2016 itibarıyla Trust ISC (www.trustisc.com) adıyla uzmanlık alanlarında hizmet vermekte olduğu kendi danışmanlık şirketini kurmuştur.

Kaynaklar

Parolalar:	https://securingthehuman.sans.org/ouch/2015#april2015
Yedekleme:	https://securingthehuman.sans.org/ouch/2015#august2015
Kötü Amaçlı Yazılımlar:	https://securingthehuman.sans.org/ouch/2016#march2016
Şifreleme:	https://securingthehuman.sans.org/ouch/2016#june2016
OUCH Arşivi / Çeviriler:	https://securingthehuman.sans.org/ouch/archives