Bilgisayar Kullanıcıları için Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

- Ön Kontrol
- Kaybolan/Çalınan Cihazlar
- Wi-Fi Erişimi
- Ortak Kullanıma Açık Bilgisayarlar

Yolculuğunuz Boyunca Güvenli Kalmak

Giriş

Bu sayıda yolculuk boyunca nasıl güvenli bir şekilde internete bağlanabileceğinizi ve işlerinizi nasıl başarabileceğinizi ele alacağız.

Konuk Yazar

Steve Armstrong, Logically Secure'de CyberCPR'ın teknik yöneticisi, sertifikalı SANS eğitmeni ve SANS kurslarının eski yazarıdır. Twitter'da **@Nebulator** ile aktif olup Google plus'da **+SteveArmstrongSecurity** hesabı ile takip edilebilir.

Ön Kontrol

Ev ya da işyerindeki ağınız güvenli olabilir ancak yolculuk yaparken bağlandığınız herhangi bir ağın güvenilmez olduğunu varsaymak zorundasınız. Kimlerin bu ağda olduğunu ve hangi tehditleri yaratacağını bilemezsiniz. Yolculuk yaparken bilgilerinizi korumak için birkaç basit ön kontrol ölçütü size çok yardımcı olabilir. Yolculuğa çıkmadan bir ya da iki hafta önce:

- 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.
- Uluslararası yolculuklar için, gideceğiniz ülkenin hangi tip elektrik bağlantısı kullandığını öğrenin, cihazlarınızı şarj etmek için adaptör kullanmak zorunda kalabilirsiniz. Dahası, mobil servis sağlayıcınızın size seyahatte iken hangi servisleri sunduğunu kontrol edin. Genel olarak mobil servis sağlayıcıları uluslararası kullanımı daha fazla ücretlendirirler. Hücresel veri kabiliyetinizi kapatmayı ya da uluslararası tarifenizi değiştirmeyi isteyebilirsiniz.
- Cihazınız çalındığında ya da kaybettiğinizde uzaktan cihazınızın nerede olduğunu takip etmek ve hatta uzaktan içindeki bilgileri silmek için bir yazılım yükleyin. Birçok mobil cihaz bu özelliği ile birlikte gelir, yapmanız gereken sadece bunu etkinleştirmenizdir. (Unutmayın, bu programlar çalışmak için internet erişimine ihtiyaç duyar.)

Yolculuğa çıkmadan bir ya da iki gün önce:

- Son versiyonlarını kullandığınızdan emin olmak için cihazlarınızı, uygulamalarınızı ve anti-virüs yazılımlarınızı güncelleyin.
- Cihazınızdaki tüm uygun güvenlik ayarlarını etkinleştirin, güvenlik duvarı gibi.
- Tüm mobil cihazlarınızı güçlü bir şifre ile kilitleyin. Bu yolla, eğer cihazınızı kaybeder ya da çaldırırsanız, insanların

Yolculuğunuz Boyunca Güvenli Kalmak

sizin bilgilerinize ulaşmasını engellersiniz.

- Verilere ulaşılmasını engellemek için tüm cihazlarınızı şifreleyin. iPhone gibi bazı cihazlar, bir şifre tanımladığınızda bunu otomatik olarak yapmaktadır.
- Tüm cihazlarınızı baştan sona yedekleyin. Bu yolla, eğer siz seyahatte iken cihazlarınızın başına herhangi birşey gelse bile güvenli bir yerde duran tüm verilerinize ulaşabilirsiniz.

Yolculuk boyunca güvenli kalmanın anahtarı, cihazlarınızı evden ayrılmadan güvenli hale getirmek, fiziksel olarak emniyette tutmak, daima nerede olduklarını bilmek ve tüm çevrim-içi aktivitelerinizi şifrelemektir.

Kaybolan/Çalınan Cihazlar

Gezinize 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. Bir çözüm, dizüstü bilgisayarınız gibi cihazlarınızı fiziksel olarak kilitlemek için yanınızda kablo götürmenizdir. Eğer suç işlenmesi tamamen bir risk unsuru ise farkına varamayacağınız şey cihazınızı kaybetmenizin çaldırmanızdan daha olası olduğudur. Verizon'un on senelik çalışmasına göre, insanların cihazlarınızı kaybetme olasılıkları, çaldırma olasılıklarından 15 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 çevrim-içi aktivitelerinizin şifreli 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.)

Yolculuğunuz Boyunca Güvenli Kalmak

Ortak Kullanıma Açık Bilgisayarlar

Otel lobilerinde, kütüphanelerinde ya da internet kafelerde kullanılan ortak kullanıma açık bilgisayarları kullanmayın. Sizden önce kimlerin kullandığı hakkında hiçbir bilginiz yoktur ve bu ortak kullanılan bilgisayara isteyerek ya da istemeyerek virus bulaştırmış olabilirler. Mümkün olan her yerde çevrim-içi aktivitelerinizde sadece kontrol edebileceğiniz ve güvendiğiniz bilgisayarları kullanın. Eğer ortak kullanılan bir bilgisayarı kullanmak zorunda iseniz giriş yapılacak ya da şifre girilecek hiçbir servis kullanmayın.

Daha Fazla Bilgi İçin

Aylık OUCH! güvenlik farkındalığı bültenine üye olun, OUCH! arşivlerine erişin ve http://www.securingthehuman.org 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, Türkiye'nin önde gelen kurumsal şirketlerinde ve özellikle bilişim, telekomünikasyon, sanayi, perakendecilik gibi sektörlerde; bilgi güvenliği, iş sürekliliği, risk yönetimi, altyapı hizmetleri, yazılım geliştirme ve proje yönetimi alanlarında yönetici ve danışman olarak 15 yılı aşkın süredir görev yapmaktadır.

Kaynaklar

Şİfreler:	http://www.securingthehuman.org/ouch/2013#may2013
İki Adımlı Doğrulama:	http://www.securingthehuman.org/ouch/2013#august2013
Şifreleme:	http://www.securingthehuman.org/ouch/2014#august2014
Tabletinizi Güvenli Hale Getirmek:	http://www.securingthehuman.org/ouch/2013#december2013
Verizon DBIR 2014:	http://www.verizonenterprise.com/DBIR/2014/

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus