Bilgisayar Kullanıcıları için Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

Yeni Tabletinizi Korumak

Giriş

Yeni tabletinizi kutlarız! Bu teknoloji başkalarıyla iletişim kurmak, çevrimiçi alışveriş yapmak, film izlemek, oyun oynamak ve birçok başka aktivite için güçlü ve pratik bir yoldur. Tabletiniz hayatınızın önemli bir parçası olduktan sonra, ki belki bilgisayarınızın yerini almış bile olabilir, tabletinizi ve bilgilerinizi gizli ve güvende tutmak için yapmanız gereken bazı kilit adımlar vardır.

Konuk Yazar

Lori Rosenberg, Bilgi Güvenliği konusunda eğitim materyallerinin hazırlanması, çalışanların ve müşterilerin eğitimi konularında geniş yelpazede bir tecrübeye sahiptir. Ve bu tecrübelerini paylaşmak için yeni ve çekici yöntemler bulma konusunda tutkulu biridir. Onu twitter'da **@InfoSecLori** hesabı ile bulabilirsiniz.

Tabletinizi Korumak

Tabletiniz için en büyük riskin bilgisayar korsanları degil, daha çok sizin olduğunu bilmek sizi şaşırtabilir. Sizin tabletinizi kaybetmeniz, çaldırmanız ya da bir yerde unutmanız, birinin sizin tabletinize izinsiz girmesinden daha olasıdır. Tabletinizi korumak için öncelikle yapmanız gereken ekranın otomatik olarak kapanmasını aktive etmektir. Her ne zaman kullanmak isterseniz, ilk önce yapmanız gereken güçlü bir parola, kaydırma örüntüsü (swiping pattern) ya da parmak izinizle kiliti açmaktır. Bu, tabletiniz çalınır ya da onu kaybederseniz, kişisel bilgilerinizi, mobil uygulamalarınızı ve diğer bilgilerinizi koruyarak kimsenin giriş yapamamasını garanti eder. Otomatik ekran kilitleme aktif hale geldikten sonra, tabletinizi korumak için birkaç ek püf noktası bulunmaktadır:

1. İnternet ile uzaktan tabletinizi takip etmek için yazılım yükleyin ve aktif edin. Bu yolla tabletinizi kaybeder ya da tabletiniz çalınırsa internetten bağlanarak nerede olduğunu bulabilir ya da en kötü durumda üzerindeki tüm bilgileri silebilirsiniz.
2. Cihazınızı güncelleyin ve otomatik güncellemeyi aktif hale getirin ki her zaman son sürüm işletim sistemi ile çalışıyor olsun. Saldırganlar her zaman yazılımda yeni açıklar bulmak için uğraşırlar ve satıcılar da sürekli yeni güncellemeleri ve yamaları piyasaya sürerek bu açıkları kapatmaya çalışır. Her zaman işletim sisteminin ve mobil uygulamaların son sürümünü kullanırsanız, birilerinin tabletinize izinsiz giriş yapmasını zorlaştırmış olursunuz.
3. Tabletinizi ilk defa konfigüre ediyorken dikkatli olun, özellikle güvenlik seçenekleri konusunda. En büyük güvenlik sorunlarından biri başkalarının sizin konumunuzu biliyor ve takip edebiliyor olmasıdır. Herşey için konum takibini devre dışı bırakmanızı ve sadece ihtiyacınız olduğunu düşündüğünüz uygulamak için aktive etmenizi tavsiye ederiz. Harita yazılımları, yerel bir restoran bulma gibi bazı uygulamalar için konumunuzu takip etmek önem taşır ama çoğu uygulama gerçek zamanlı konum bilgisine gerek duymaz.

Yeni Tabletinizi Korumak

4. Birçok tablet ve uygulama bilgilerinizi Bulutta (cloud) depolar. Hal böyle olunca da verilerinizin nerede ve nasıl güvenli olduğu konusunu iyi anladığınızdan emin olun. Örneğin isteyeceğiniz en son şey, internette özel resimlerinizin konumları ile birlikte dünyadaki herkesin göreceği şekilde paylaşmaktır. Buluttaki tüm paylaşımları yetkisiz kılın ve daha sonra özel birşeyleri paylaşmak istediğinizde devreye sokun.
5. Tabletler, sizin uygulamalarınızı cep telefonlarınız ya da laptoplarınız gibi diğer cihazlarla giderek artan bir şekilde senkronize etmektedir. Senkronizasyon mükemmel bir özellik olabilir, ancak hangi uygulamaların ve özelliklerin senkronize edildiğine izin verdiğinize dikkat edin. Eğer senkronizasyon etkinleştirilmiş ise, işteki bilgisayarınızdaki tarayıcınızda daha önce tabletinizin tarayıcısından ziyaret ettiğiniz sitelerin ve sekmeleri gördüğünüzde şaşırmayın.

Tabletinizi korumanın en iyi yolu, ekran kilitlemeyi aktif hale getirmeniz, güvenlik ayarlarını gözden geçirmeniz ve tabletinizi güncel tutmanızdır.

Onu Güvenli Tutmak

Bir kez tabletinizi güvenli hale getirdikten sonra, bu şekilde kaldığı konusunda emin olmalısınız. Uzun vadede tabletinizi güvenli tutmak için aşağıda bazı kilit adımlar verilmiştir.

- Hiçbir zaman tabletinize jailbreak/root yapmayın ya da izinsiz olarak girmeyin. Bu bir çok güvenlik kontrolünü baypas eder ve yararsız bir hale getirir ki bu da tabletinizi saldırılara karşı daha savunmasız kılar.
- Sadece istediğiniz ve kaynağına güvendiğiniz yerlerden uygulama indirin. iPad'ler için sadece iTunes'den uygulama indirin. Bu uygulamalar, kullanıma hazır olmadan önce Apple tarafından taramadan geçirilmektedir. Google için sadece Google Play'den uygulama indirmenizi tavsiye ederiz ve Amazon tabletler için Amazon uygulama mağazasından (Amazon App Store) indirmenizi öneririz. Diğer sitelerden uygulama indirme esnasında bu uygulamalar gözden geçirilmemiş ya da virüslü olabilirler. Son olarak uygulamayı nerden indirdiğiniz dikkate alınmaksızın, eğer indirdiğiniz uygulamayı aktif olarak kullanmıyorsanız ya da artık ihtiyacınız yok ise tabletinizden silmenizi öneririz.
- Yeni bir uygulama yüklüyorken, tabletinizin ilk defa ayarlarını yaptığınız gibi güvenlik seçeneklerini gözden geçirdiğinizden ve ayarlama yaptığınızdan emin olun. Hangi uygulamaların nelere erişeceği konusunda verdiğiniz izinlere dikkat edin. Örneğin, yeni yüklediğiniz bir uygulamanın tüm arkadaşlarınıza ve iletişim bilgilerine erişmesine gerçekten ihtiyacı var mı? Eğer bir uygulamanın izin gereksinimleri konusunda kendinizi rahatsız hissediyorsanız, sizin ihtiyaçlarınızı karşılayacak başka bir uygulama bulun. Ayrıca, düzenli olarak değiştirilmediklerinden emin olmak için izinleri kontrol edin.

Yeni Tabletinizi Korumak

Tabletiniz eğlenmek ve kullanmak istediğiniz güçlü bir araçtır. Bu birkaç basit adımı hatırlamak sizin ve yeni tabletinizin güvenli kalması için çok yararlıdır.

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.

Mustafa Emrah Ünsür, Güvenlik Araştırmacısı olarak araştırmaları, makaleleri ve çevirileri vardır. Beyaz Şapkalı Hacker olarak kendisi tarafından kodlanan ve kodlanmakta olan 'exploit'ler ve 'tool'lar bulunmaktadır. Ayrıca, Sızma Testi Uzmanı olarak özel şirketlere ve devlet kurumlarına Zafiyet ve Sızma Testi yapmış ve yapmaya devam etmektedir.

Kaynaklar

Mobil uygulamaları güvenli bir şekilde kullanmak:	https://www.securingthehuman.org/ouch/2015#january2015
Parolalar:	https://www.securingthehuman.org/ouch/2015#april2015
Bulutu Güvenli Kullanmak:	https://www.securingthehuman.org/ouch/2014#september2014
Mobil Cihazınızı Elden Çıkarmak:	https://www.securingthehuman.org/ouch/2014#june2014
SANS Güvenlik Günü İpucu:	https://www.sans.org/tip_of_the_day.php

Yayın Kurulu : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis