SANS SECURITY AWARENESS

OUCH! | Kasım 2017

Herkes İçin Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

- Sahte Çevrim-içi Mağazalar
- Bilgisayarınız / Mobil Cihazınız
- Kredi Kartınız

Güvenli Bir Şekilde Çevrim-içi Alışveriş

Giriş

Bir çoğumuz için tatil sezonu yaklaşmakta ve pek yakında dünyanın dört bir yanından milyonlarca kişi harika hediyeler alacak. Bir çoğumuz en iyi fiyatların peşinde çevrim-içi alışveriş etmeyi seçeceğiz, uzun kuyruklar ve sabırsız kalabalıklardan kaçınarak. Maalesef, bu aynı zamanda siber suçluların sahte mağaza web siteleri yarattığı, yılın dolandırıcılık ve hırsızlık zamanıdır. Aşağıda çevrim-içi alışverişin rikslerini açıklıyor ve güvenli bir şekilde nasıl en iyi fiyatlarla harika bir alışveriş yapacağınızı anlatıyoruz.

Konuk Yazar

Lenny Zeltser, Minerva Labs'da güvenlik ürünleri geliştirmekte ve kötü amaçlı yazılımlarla mücadele etmek ile ilgili SANS'ta ders vermektedir. Lenny'i Twitter'da **@lennyzeltser** ve güvenlik güncesi **zeltser.com**'dan takip edebilirsiniz.

Sahte Çevrim-içi Mağazalar

Birçok çevrim-içi mağaza meşru iken, bazı sahte web siteleri de siber suçlular tarafından hazırlanmıştır. Suçlular bu sahte web sitelerini, gerçek sitelerin görünüşünü kopyalayarak ya da iyi bilinen mağaza ve markaların isimlerini kullanarak yaparlar. Daha sonra bu düzmece web sitelerini en iyi fiyatları arayan kişileri tuzağa düşümek için kullanıyorlar. Çevrim-içinde sadece düşük fiyatlar için arama yaptığınızda kendinizi bu sahte sitelere yönlendirilmiş olarak bulabilirsiniz. Alışveriş yapmak için bir web sitesini seçerken, diğer web sitelerinden önemli ölçüde ucuz reklam yapılıp yapılmadığına ve ülke çapında tükenmiş ürünler satıp satmadıklarına dikkat edin. Fiyatların çok ucuz ya da mevcut olmasının nedeni sizin teslim alacağınız ürünün meşru olmamasıdır, belki sahte ya da çalınmış olabilir veya bazı durumlarda hiç teslim de edilmeyebilir. Aşağıdakileri gözönünde bulundurarak kendinizi koruyun:

- Fırsat olduğunda daha önceden bildiğiniz, güvendiğiniz ve alışveriş ettiğiniz web sitelerinden alışveriş edin.
- Web sitesinin meşru bir posta adresi olduğunu ve satış ve destek ile ilgili sorular için meşru bir telefon numarasına sahip olduğunu doğrulayın. Eğer site şüpheli görünüyorsa, birini arayıp konuşun. Eğer konuşacak birini bulamıyorsanız, bu sahte bir web sitesinin sahte olduğunun ilk büyük işaretidir.
- İndirimlerin inanılmayacak kadar iyi olması ya da kötü dil bilgisi ve yazım kurallarının oluşu gibi belirgin uyarı işaretleri arayın.
- Daha önceden kullandığınız bir sitenin alan adı biraz farklı ise ve iyi bilinen bir web sitesinin birebir kopyası gibi görünüyorsa büyük bir kuşkuyla davranın. Örneğin, eskiden alan adı https://www.amazon.com olan Amazon'dan online alışveriş yapıyordunuz. Eğer kendinizi http://store-amazoncom.com gibi Amazon'un sitesi gibi duran bir web sitesinde bulursanız, çok şüpheci davranın.

Güvenli Bir Şekilde Çevrim-içi Alışveriş

- Mağazanın adını arama motoru kullanarak arayın ve diğer kişiler bu web sitesi ile ilgili ne söylemişler araştırın. “dolandırıcılık”, “sahtekarlık”, “bir daha asla” or “sahte” gibi ifadeleri arayın. Web sitesine ait herhangi bir inceleme ya da yorumun olmaması, web sitesinin yeni ve belki de güvenilmez olduğuna dair bir işaret olabilir.
- Herhangi bir şey almadan önce web sitesi ile aranızdaki iletişimin şifrelendiğinden emin olun. Birçok tarayıcı şifrelenmiş iletişimi bir kilit ve/veya web sitesinin isminden önce konumlandırılmış yeşil renkli bir HTTPS yazısı ile gösterir.

Web sitesinin profesyonel görünmesi bu sitenin meşru olduğunu göstermez, bunu unutmayın. Eğer web sitesi içinize sinmediyse kullanmayın. Bunu yerine, iyi bilinen, güvenebileceğiniz ya da daha önceden güvenli bir şekilde alışveriş ettiğiniz bir web sitesi bulun. Çok iyi indirimler bulamayabilirsiniz ancak en azından kişisel ve finansal bilgileriniz çalınmadan meşru bir ürün sahibi olursunuz.

Sadece kabul görmüş bir itibarı olan ve güvenilir web sitlerinden alışveriş ederek kendinizi çevrim-içi koruyun.

Bilgisayarınız / Mobil Cihazınız

Meşru sitelerden alışveriş etmenin yanında, bilgisayarınız ve mobil cihazınızın güvenli olduğundan emin olmak isteyebilirsiniz. Siber suçlular, banka ve kredi kartı hesap bilgileriniz ile şifrelerinizi ele geçirmek için cihazlarınıza virus bulaştırmaya çalışacaklardır. Cihazlarınızı güvenli hale getirmek için aşağıdaki adımları atın:

- Eğer evde çocuklarınız var ise, iki ayrı cihaz edinmeyi düşünün, biri çocuklar için biri büyükler için. Çocuklar teknoloji ile etkileşimlidir ve meraklıdır. Bu yüzden kendi cihazlarına virus bulaştırma olasılıkları daha fazladır. Sadece çevrim-içi bankacılık ve alışveriş gibi çevrim-içi işlemler için farklı bir bilgisayar ya da tablet kullanarak cihazlarınıza virus bulaşma olasılığını azaltmış olursunuz.
- Her zaman en son güncellemeleri yükleyin ve güncel bir antivirus yazılımını kullanın. Bu siber suçluların cihazlarınıza virüs bulaştırmalarını zorlaştıracaktır.

Kredi Kartınız

Özellikle yeni bir web sitesinden çevrim-içi alışveriş yaptıktan sonra şüpheli ödemeleri tespit etmek için düzenli olarak kredi kartı bildiriminizi gözden geçirin. Bazı kredi kartı tedarikçileri, kredi kartınızdan her para çekilişinde ya da çekilen para daha önceden belirlenmiş bir miktarı geçtiğinde sizi e-posta ya da metin mesajı ile uyarır. Bir diğer seçenek ise çevrim-içi harcamalar için sadece bir tane kredi kartı kullanmaktır, bu sayede kredi kartınız ele geçirilirse, diğer ödeme işlemlerinizi

etkilemeden kolaylıkla kartınızı değiştirebilirsiniz. Eğer dolandırıcılık yapıldığına inanıyorsanız, kredi kartı sağlayıcınızı hemen arayın. Bu, çevrim-içi alışverişlerinizde neden kredi kartı kullanmak istediğinizin de göstergesidir, mümkün olduğunca vadeli hesap kartlarınızı kullanmaktan kaçının. Vadeli hesap kartlarınız parayı direkt banka hesabınızdan alır, eğer bir dolandırıcılık yapılmışsa, paranızı geri almanız çok daha zor olacaktır. Son olarak, her çevrim-içi alışveriş için benzersiz ve tek bir kart numarası üreten kredi kartlarını, sanal kartlar, hediye kartlarını ya da kredi kartı bilgilerinizi alışveriş yaptığınız mağaza ile paylaşmadığınız PayPal gibi iyi bilinen ödeme servislerini kullanmayı düşünebilirsiniz.

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, 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 yaptıktan sonra, Truth ISC (www.truth-isc.uk) adıyla kurduğu Türkiye ve İngiltere'de faaliyet gösteren danışmanlık şirketinde hizmet vermeye devam etmektedir.

Kaynaklar

Sosyal Mühendislik:	https://securingthehuman.sans.org/ouch/2017#january2017
Güvenli Kalmak için 4 Adım:	https://securingthehuman.sans.org/ouch/2016#october2016
Ev Ağınızı Güvenli Hale Getirmek:	https://securingthehuman.sans.org/ouch/2016#february2016
SANS Güvenlik Günün İpucu:	https://www.sans.org/tip_of_the_day.php