GÜVENLİ GÜNLER BÜLTENİ

Bilgisayar kullanıcılarına yönelik hazırlanır. Her ayın 15'i çıkar. Diğer sayılara erişmek ve sonraki mesajların direk posta kutunuza gelmesi için guvenligunler.com adresini ziyaret ediniz.

MAYIS 2019

Oltalama (Phishing)

BİLGİSAYARLAR, akıllı telefonlar ve çeşitli sektörlerde kullanılan elektronik cihazlar bir yandan sağladıkları kolaylıklar sayesinde gündelik hayatımızın ayrılmaz parçası olurken, bir yandan da kötü niyetli kişilerin yararlanabileceği uygulama alanları olabilmektedir.

Bu yazıda, en yaygın bilgisayar saldırı yöntemlerinden biri olan "Phishing" (Oltalama-Kimlik avı) yöntemini inceleyerek alınacak temel önlemlerden söz edeceğiz.

Phishing

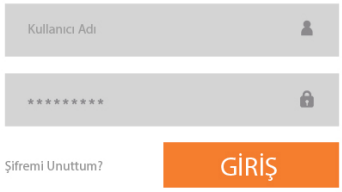
İngilizce fishing (balık tutma) kelimesinden türetilmiş bir terim olan Phishing, kullanıcıların sosyal mühendislik yöntemleriyle aldatılması yoluyla kimlik bilgilerinin edinilmesini amaçlayan bir tür internet sahtekârlığının adıdır.Genel olarak parola, kredi kartı numaraları, banka hesap bilgileri ve diğer gizli bilgileri ele geçirme yöntemi olarak karşımıza çıkmaktadır.

Tarihte ilk kez 1996 yılında, Amerika'daki AOHell adlı bir haber kanalı kullanıcılarının sisteme giriş ad ve şifrelerinin çalınmasıyla başlamış, ardından da 2000'li yıllarda Paypal benzeri elektronik ödeme kanallarının artmasıyla bu uygulamaların hesap bilgilerinin çalınması

şeklinde yaygınlaşmıştır. Phishing saldırı yöntemi temelde kullanıcıların kandırılmasına dayanmaktadır ama çok sayıda çeşidi vardır. Biz sık rastlanılan yöntemlerden söz edeceğiz.

Elektronik Posta Phishing Yöntemi:

Bu alanda genellikle kullanıcıya **"sürpriz ödül"** kazandığı bildirilip ödülü alabilmesi için kişisel bilgilerini girmesi talep edilir ya da sahip olduğu bir hesap link'i bir sahte web sayfasına yönlendirilerek "user name" ve şifre bilgisiyle girmesi istenilir.



Bir yöntemde, **"acil"** mesajıyla kullanıcı korkutularak, ya elektronik postada yer alan link'e gidip kullanıcı bilgilerini girmesi ya da kendisine ait **bilgileri güncellemesi** istenerek gerekli bilgiler ele geçirilir. Bu yönteme benzer bir başka sahtekârlıkta ise, kullanıcıya ait olmayan bir siparişin alındığı hakkında bilgi verilerek kullanıcının paniğe kapılması sağlanır ve gönderilen elektronik postada ürün iptali ile ilgili aşamaları yerine getirmesi istenerek sahtekârlık yapılır.

Diğer bir yöntemde de "elektronik postayla gelen eklentiye (jpeg ya da pdf uzantılı dosya görünümlü) tıklanılması sağlanarak kullanıcı bilgisayarına zararlı yazılım yüklenir. Böylece kullanıcı, elektronik posta üzerinde yer alan link'e tıklayarak işlem yapmak istediğinde, banka benzeri bir sitenin sahte kopyasına yönlendirilir ve bilgilerini o siteye girer.

Arama Motoru Üzerinden Phishing:

Arama motoru üzerinden aradığınız bir ürünün hiç duymadığınız (dolayısıyla sahtekârlarca oluşturulmuş olabilecek) bir sitede çok uygun fiyata satıldığını görüp sipariş vermek için kredi kartı bilgilerinizi girdiğinizde, kredi kartı bilgileriniz korsanlar tarafından çalınmış olur.

Sesli (Voice) Phishing ve Smishing (SMS Phishing):

Elektronik posta phishing yöntemleri olan korkutma, ödül kazanıldığının bildirilmesi ya da veri güncellemesi ve yanlış sipariş düzeltilmesi gibi kandırmacaların telefon ve sms yoluyla gerçekleştirilmesidir.

ALINACAK ÖNLEMLER

» Öncelikle hiçbir koşulda elektronik postayla gelen link'e tıklayarak, yönlendirildiğiniz siteye kullanıcı bilgilerinizi ve şifrenizi girmeyin.

» Bankalar ve firmalar hiçbir zaman elektronik posta üzerinden **güncelleme** bilgisi istemezler; bu tür bilgileri girmeyin ya da telefonla arayan kişilere bu bilgileri vermeyin.

» Size gelen elektronik postaların gerçekten **özel olarak size** yazıldığı konusunda emin olmadan gelen eklentileri, resim dosyası bile olsa açmayın ve bilgisayarınıza indirmeyin. Ayrıca size gelen elektronik postanın **gönderim saatine** de dikkat edin, örneğin hiçbir kuruluş gece saat 3.00 civarında size elektronik posta yollamaz.

» Özelikle **acil** kelimesi içeren elektronik postalarınıza karşı ihtiyatlı olun.

» Antivirüs ve güvenlik duvarı bulunmayan bilgisayarlardan hiçbir şekilde uygulama hesaplarınıza girmeyin.

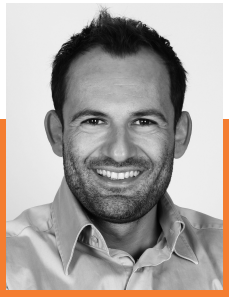
» Yararlandığınız internet arama motorunun güncel versiyonunu kullanın.

» Kullandığı internet arama motorunun güncel versiyonunu kullanınız.

» Kişisel bilgilerinizin talep edilmesi durumunda karşı tarafa bilgi vermeyin. Örneğin, arayanın bankadan aradığını söylemesi durumunda, telefonu kapatıp kendiniz bankayı arayarak konu hakkında bilgi edinin; ayrıca elektronik alışverişlerinizi mümkünse sanal kredi kartı kullanarak ve düşük bir limit belirleyerek yapın.

REFERANSLAR

1. www.phishing.org
2. https://www.guvenliweb.org.tr/haber-detay/turkiyenin-internet-kullanim-aliskanliklari-tuik-2018



YAZAR HAKKINDA

FAZLI YILDIRIM 1999 yılında İstanbul Üniversitesi Bilgisayar Mühendisliği Bölümü'nden mezun olmuştur. Yeditepe Üniversitesi bünyesinde İşletme Yüksek Lisans (MBA) derecesine sahip olup, 2008 yılında Işık Üniversitesi'nde Çağdaş İşletme Doktora Programı'nı başarı ile bitirip Doktor ünvanını almıştır. 2017 yılında Yönetim Bilişim Sistemleri alanında Doçentlik ünvanını elde etmiştir.

Siber Güvenlik, Elektronik Ticaret, Dijital Pazarlama, Müşteri İlişkileri Yönetimi, E-Devlet, Mobil Uygulamaları alanlarında çok sayıda yayınlanmış makalesi olup Müşteri İlişkileri Yönetimi konusunda yayımlanmış bir kitabı bulunmaktadır. Halen Yeditepe Üniversitesi bünyesinde Elektronik Ticaret ve Teknoloji Yönetimi bölümünde görev yapmaktadır.

YASAL UYARI

Bu dokümanın tüm hakları Lostar Bilgi Güvenliği A.Ş.'ye aittir ve Creative Commons BY-NC-ND 4.0 (Attribution-NonCommercial-NoDerivatives 4.0 International - (CC BY-NC-ND 4.0) lisansı altında dağıtılır. Herhangi bir değişiklik yapmadan kaynak gösterilerek dağıtılabilir. Ticari olarak kullanılamaz.