

Phishing (Oltalama) nedir?

Phishing, dolandırıcıların rastgele kullanıcı hesaplarına e-mail gönderdikleri bir çevrimiçi saldırı türüdür. E-postalar, bilinen web sitelerinden veya kullanıcının bankasından, kredi kartı şirketinden, e-posta veya internet hizmeti sağlayıcısından gönderilmiş gibi gözükür. Genellikle hesapları güncelleyebilmek için kredi kartı numarası veya şifre gibi kişisel bilgiler sorulur. Bu e-postalarda kullanıcıları bir başka web sitesine yönlendiren URL bağlantısı yer alır. Bu site aslında ya sahte ya da değiştirilmiş bir web sitesidir. Kullanıcılardan da bu siteye gittiklerinde phishing saldırısını yapan kişiye iletmek üzere kişisel bilgilerini girmeleri istenir.

Phishing, genelde bir kişinin şifresini veya kredi kartı bilgilerini öğrenmek amacıyla kullanılır. Bir banka veya resmi bir kurumdan geliyormuş gibi hazırlanan e-posta yardımıyla bilgisayar kullanıcıları sahte sitelere yönlendirilir. Phishing saldırıları için bankalar, sosyal paylaşım siteleri, e-posta servisleri, online oyunlar vb. sahte web sayfaları hazırlanmaktadır. Burada bilgisayar kullanıcısından kimlik bilgileri, kart numarası, şifresi vb. istenir. E-posta mesajındaki ve sahte sitedeki talepleri dikkate alan kullanıcıların bilgileri çalınır.

Tam bir aldatmacadır. Saldıran kişi bir “yem” hazırlar ve bu yeme “balıkların” takılmasını bekler. Büyük kayıplar yaşanmaması için bu tür sahtekarlıklara karşı bilinçli olmak gerekmektedir.

Bu yazının amacı da zaten bu bilinci yaratarak teknoloji kullanan insanların zarar görmesini engellemektedir.

Phishing saldırılarıyla nelerin çalınması amaçlanıyor ?

Phishing yöntemi kullanarak bilgisayar kullanıcılarını kandıran saldırganlar genellikle aşağıdaki bilgilere erişmeyi hedeflemektedirler.

- Kullanıcı hesap numaraları
- Kullanıcı şifreleri ve parolaları
- Kredi kartı numaraları
- İnternet bankacılığında kullanılan kullanıcı kodu ve şifreleri vb.

E-Posta ile Phishing

E-posta yöntemini kullanan dolandırıcılar burada da kullanıcıları farklı şekillerde aldatma yoluna giderler.

a) E-postanıza devamlı temas halinde olduğunuz kuruluşlardan gönderiliyormuş izlenimi verilen sahte bir e-posta gönderiliyor. Bu e-postalarda kullanıcıya kurumun web sitesine gitmesinin gerektiği, şifresinin süresinin dolduğu söylenir ve altta o sayfaya yönlendirileceği bir link (bağlantı) verilir. Dolandırıcı daha önceden hazırladığı ve kuruluşun sitesinin aynısı veya benzeri olan bu siteye kullanıcıyı getirdikten sonra, ondan şifreyi girmesini ister. Dolandırıcı bu şifreyi kullanarak internet aracılığı ile para transferi, e-ticaret, sizin adınıza bağış toplama, reklam gönderme, çok sayıda spam mesaj gönderme vb. işler yapabilir.

b) Bazı e-postalarda ise; bir yarışma düzenlendiği ve bu yarışmaya katılması teklif edilen kullanıcılara ödül olarak bir ürün kazandıkları ancak gerekli kişisel bilgileri vermeleri gerektiği söylenir. Bu gibi durumlarda bilgilerini veren kullanıcının tüm bilgileri dolandırıcının eline geçer.

c) Bir başka kullanılan teknikte ise; gelen e-postada müşteriye kişisel bilgilerini güncellemesi gerektiği, tüm bilgileri tekrar girmesi bunun kendileri açısından daha iyi hizmet verebilmeleri için gerekli olduğu söylenir.

d) Bir başka teknikte ise; gelen e-postada kullanıcının e-posta kotasının dolduğu, eğer bilgilerini güncellemezse hesabının kapatılacağı söylenir.

e) Son zamanlarda bazı bankaların başlatmış oldukları ve cep telefonları ile para transferine imkân veren sistem kullanılarak banka müşterilerine sanki kendi hesaplarına para gönderilmiş veya alınmış gibi gösterilip sahte banka sitesi linki (bağlantı yolu) verilerek bu paranın tahsil edilebilmesi için bilgi güncelleştirmesi istendiği bilinmektedir.

Phishing amaçlı gönderilen e-postalar ve sahte web siteleri nasıl tespit edilir?

- E-posta tanınmış yasal bir e-ticaret sitesinden, finansal kurumdan, e-posta sağlayıcısından, internet hizmet sağlayıcısından mı geliyor?
- Kişisel bilgilerinizi vermeniz mi isteniyor?
- E-postada ya da web sitesinde yazım veya dilbilgisi hataları var mı?
- E-posta ya da yönlendirildiğiniz web sitesi, sizden yanıt alabilmek için duygusal veya heyecan verici bazı sözler kullanıyor mu?
- Eğer e-postadaki bir bağlantı (link) aracılığıyla bir web sitesine yönlendirilmişseniz, tarayıcının (browser) üst kısmında yazan URL ile ziyaret ettiğinizi düşündüğünüz yasal şirketin URL adresi birbirine uyuyor mu?

Phishing saldırısına hedef olduysanız neler yapmalısınız ?

Eğer saldırı yasal bir şirketle ilişkiliyse (yani phishing saldırısında gönderilen e-posta tanınmış bir e-ticaret sitesinden, finansal kurumdan, e-mail sağlayıcısından, internet hizmet sağlayıcısından geliyorsa) bu saldırıyı ilgili şirkete bildirin. Böylece, ilgili kuruma sahte web sitesini kapatma ve saldırganın izini sürmesini sağlamak için yardımcı olabilirsiniz.

E-posta hesabımın şifresi ele geçirildiğinde ne olur?

- Gönderilecek mesajın görünen ismi, sizin isminiz yerine genellikle başka bir isimle değiştirilir.
- Mesajın sonuna eklenecek olan imza metni değiştirilir.
- Hesabınızda bulunan veya size sonradan gelecek olan mesajlar saldırganı yönlendirilir ve sizdeki kopyası silinir.
- Hesabınızdaki mesajların tümü silinebilir.

Çevrimiçi dolandırıcılıktan korunmanın yolları

E-posta hesabınız için kullandığınız şifre, diğer hesaplarındaki şifrelerden farklı olmalıdır.

Kişisel bilgilerinizi isteyen e-postalara yanıt vermeyin.

Gelen e-postanın kimden geldiğinden emin değilseniz dikkate almayınız. Unutmayın hiç bir kurum veya kuruluş e-posta yoluyla sizden kişisel bilgilerinizi istemez.

ÇALIŞTIĞINIZ KURUM SİZE ASLA KİŞİSEL BİLGİLERİNİZ VEYA ŞİFRENİZİ SORAN E-POSTA GÖNDERMEZ.

Şüpheli gördüğünüz e-postalardaki URL linklerini tıklamayın.

E-posta mesajlarındaki kısaltılmış URL linklerine (bit.ly,ow.ly, tinyurl.com, is.gd, goo.gl, tiny.cc, cli.gs vb.) kesinlikle tıklamayın.

Şüpheli veya bilmediğiniz web sitelerine kişisel bilgilerinizi vermeyin.

Kişisel bilgilerinizi girmek için banka, kredi kartı ve servis sağlayıcılarının web sitelerini ziyaret ettiğinizde, web sitesinin URL'sini internet tarayıcınıza doğrudan yazın.

Güvenli olan sitelerde bile çevrimiçi olarak bir formu doldurmadan önce, sitenin üçüncü kişilerle bu bilgileri paylaşp paylaşmadığını belirten gizlilik anlaşmasının olup olmadığını kontrol edin.

Antispyware ve antivirüs programları kullanın.

Yasal olmayan veya kaynağı belirsiz yazılımları yüklemeyin ve çalıştırmayın.

Kredi kartı numaraları, kişisel bilgiler, e-posta dahil her türlü şifre hiç bir zaman e-posta ile açıkça yollanmamalıdır. Bir e-posta teknik olarak gideceği yere varana kadar birçok noktadan geçmektedir. Bu noktalarda e-postaların içeriğinin "dinlenmesi" her zaman mümkündür.

Özellikle Kablosuz İnternet'in kullanıldığı alanlarda mecbur kalınmadıkça banka gibi yerlere girilmemeli, kredi kartı, şifre vs. ile ilgili işlemler yapılmamalıdır. Havadaki sinyaller üçüncü şahıslar tarafından dinlenebilir. Sinyaller şifreli dahi olsa unutulmamalıdır ki tüm şifreleme yöntemleri sadece kırılıncaya kadar güvenlidir.

Bu tip saldırılara karşı korunmanın en etkili yolu, **bu konuda bilinçli ve bilgili olmaktır.**