ERCİYES ÜNİVERSİTESİ
BİLGİ İŞLEM DAİRE BAŞKANLIĞI

OLTALAMA SALDIRILARI FARKINDALIK EĞİTİMİ

Oltamala (Phishing) saldırılarından korunmanın en etkin yolu kullanıcının bilinçlendirilmesidir.

ÇALIŞTIĞINIZ KURUM ve KURUMLAR SİZE ASLA KİŞİSEL BİLGİLERİNİZ VEYA PAROLANIZI SORAN E-POSTA GÖNDERMEZ.

EĞİTİM İÇERİĞİ

- Oltalama (Phishing) Nedir?
- Oltalama saldırılarıyla nelerin çalınması amaçlanır ?
- E-Posta ile Oltalama
- Oltalama amaçlı gönderilen e-postalar ve sahte web siteleri nasıl tespit edilir?
- Oltalama saldırısına hedef olduysanız neler yapmalısınız ?
- E-posta hesabımın parolası ele geçirildiğinde ne olur?
- Çevrimiçi dolandırıcılıktan korunmanın yolları nelerdir ?
- Kurumsal Oltalama simülasyonu raporlarımız.

OLTALAMA/PHISHING NEDİR ?

Oltamala, dolandırıcıların rastgele kullanıcı hesaplarına e-postalar gönderdikleri bir çevrimiçi saldırı türüdür.

E-postalar, bilinen web sitelerinden veya kullanıcının bankasından, kredi kartı şirketinden, e-posta veya internet hizmeti sağlayıcısından gönderilmiş gibi görünür.

Genellikle hesapları güncelleyebilmek için kredi kartı numarası veya parola gibi kişisel bilgiler sorulur.

Bu e-postalarda kullanıcıları bir başka web sitesine yönlendiren URL (e-posta içerisinde tıklamanız istenilen bir link) bağlantısı yer alır.

Bu site aslında ya sahte ya da değiştirilmiş bir web sitesidir.

Kullanıcılardan da bu siteye gittiklerinde saldırıyı yapan kişiye iletilmek üzere kişisel bilgilerini girmeleri istenir.

OLTALAMA/PHISHING NEDİR ?

Oltalama, genelde bir kişinin parolasını veya kişisel bilgilerini (kredi kartı-banka kartı bilgileri, üye olduğu sitelerin giriş bilgileri vb.) öğrenmek amacıyla kullanılır.

Bir banka veya resmi bir kurumdan geliyormuş gibi hazırlanan e-posta yardımıyla bilgisayar kullanıcıları sahte sitelere yönlendirilir. Bu saldırıları için bankalar, sosyal paylaşım siteleri, e-posta servisleri, online oyunlar vb. sahte web sayfaları hazırlanmaktatır. Burada bilgisayar kullanıcısından kimlik bilgileri, kart numarası, parolası vb. istenir.

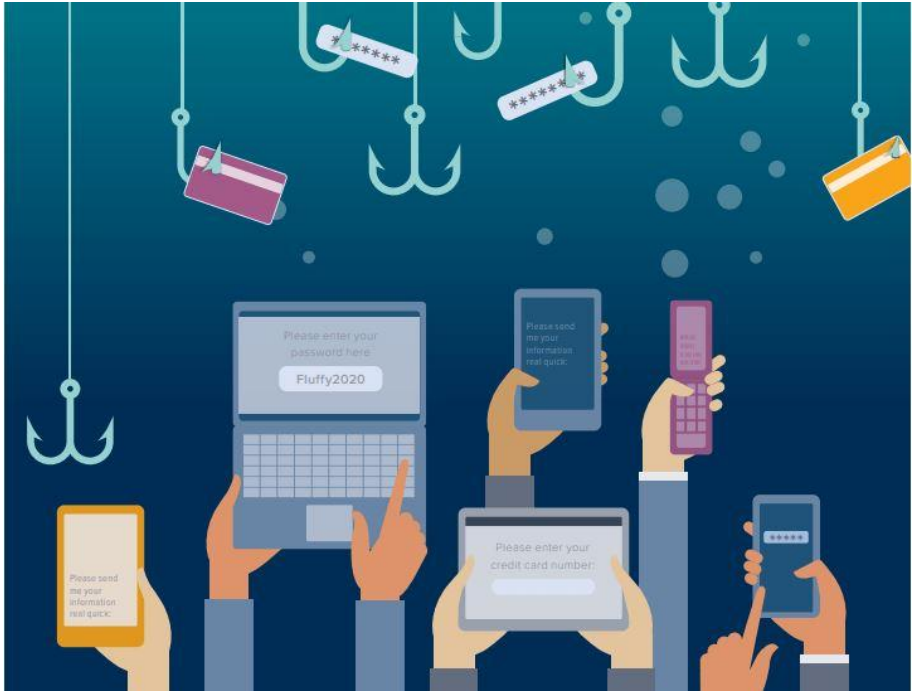
E-posta mesajındaki ve sahte sitedeki talepleri dikkate alan kullanıcıların bilgileri çalınır.

OLTALAMA/PHISHING NEDİR ?

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 eğitimin amacı da zaten bu bilinci yaratarak teknoloji kullanan personel ve öğrencilerimizin zarar görmesini engellemektedir.



Oltalama saldırılarıyla nelerin çalınması amaçlanır ?

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

- Kullanıcı adları hesap numaraları
- Kullanıcı parolaları
- Kredi kartı numaraları
- İnternet bankacılığında kullanılan kullanıcı kodu vb.
- Üye olunan alışveriş sitelerine erişim bilgileri.

E-Posta ile Oltalama

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 gönderilir. Bu e-postalarda kullanıcıya kurumun web sitesine gitmesinin gerektiği, parolasının 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 parolasını girmesini ister. Dolandırıcı bu parolayı kullanarak internet aracılığı ile para transferi, e-ticaret, sizin adınıza bağış toplama, reklam gönderme, çok sayıda spam mesaj gönderme vb. işler yapabilir.

E-Posta ile Oltalama

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.

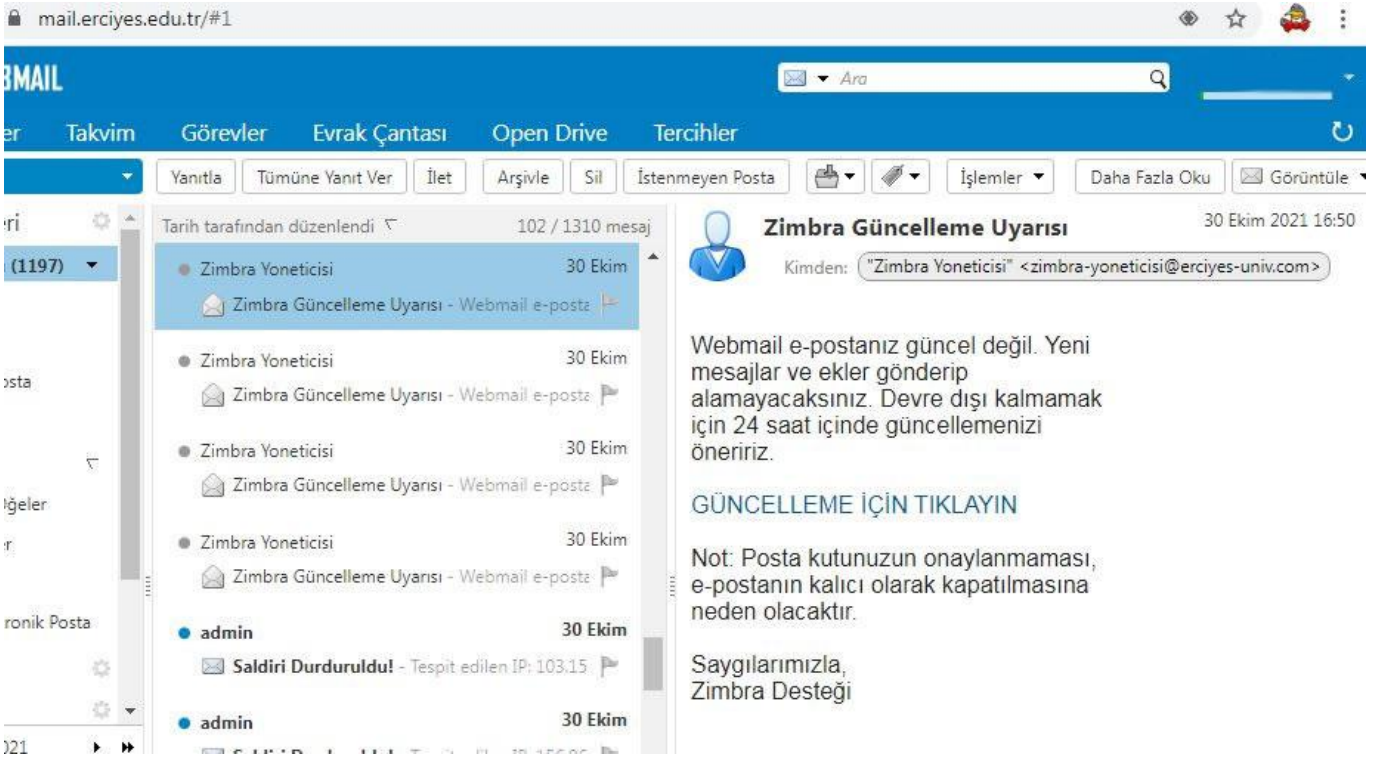
Oltalama amaçlı gönderilen e-postalar ve sahte web siteleri nasıl tespit edilir?

E-posta kullanıcılarının kendilerine şu soruları sormaları gerekmektedir

- E-posta tam olarak kimden geliyor? Görünen ad, gönderen adres, gönderen alan adı kurumsal veya kurumuma mı ait ?
- E-posta tanınmış yasal bir e-ticaret sitesinden, finansal kurumdan, e-posta sağlayıcısından, internet hizmet sağlayıcısından mı geliyor?
- E-postada kişisel bilgilerimi vermem mi isteniyor?
- E-postada ya da web sitesinde yazım veya dil bilgisi hataları var mı?
- E-posta ya da yönlendirildiğim web sitesi, benden yanıt alabilmek için duygusal veya heyecan verici bazı sözler kullanıyor mu?
- Eğer e-postadaki bir bağlantı (link) aracılığıyla bir web sitesine yönlendirilmişsem tarayıcının (browser) üst kısmında yazan URL adresi ile ziyaret ettiğinizi düşündüğünüz yasal şirketin URL adresi birbirine uyuyor mu?

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

Örnek bir oltalama e-postasını inceleyelim, bir güncelleme uyarısı, son derece masum görünmekte, linke tıklayıp linkteki oltalama sitesine bilgilerinizi yazmazsanız, hiçbir zararı olmayan bir e-posta.

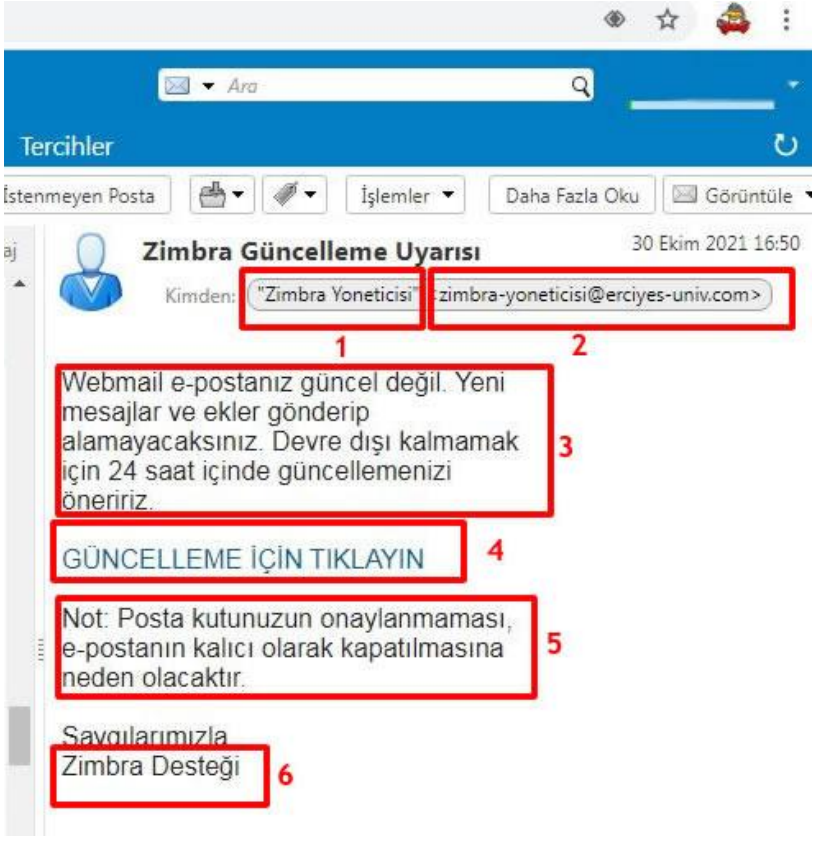


Oltalama amaçlı gönderilen e-postalar ve sahte web siteleri nasıl tespit edilir?

1- Zimbra Yoneticisi görünen ad (Displayed Name) dir ve her e-postada özgür alandır istediğiniz herşeyi yazabilirsiniz, yani kimlik doğrulamak için hiçbir anlamı olmayan bir bilgidir.

2- Adres zimbra-yoneticisi@erciyes-univ.com şeklindedir. Kurumumuzla en ufak bir bağlantısı olmayan bir alan adıdır ve bu alan adları 3-5 dolara satın alınabilir. Alan adımız erciyes.edu.tr dir ve bu alan adından gelmeyen e-postalara kuşku ile bakmalısınız.

3- Oltalama postalarında, ödül ve korku ile panikletip, düşünmeden kişisel bilgileri yönlendirilen sayfaya yazdırma zorlaması mevcuttur. Burada hizmet kesintisi korkusu ile kullanıcıyı panikletme hedeflemiştir.

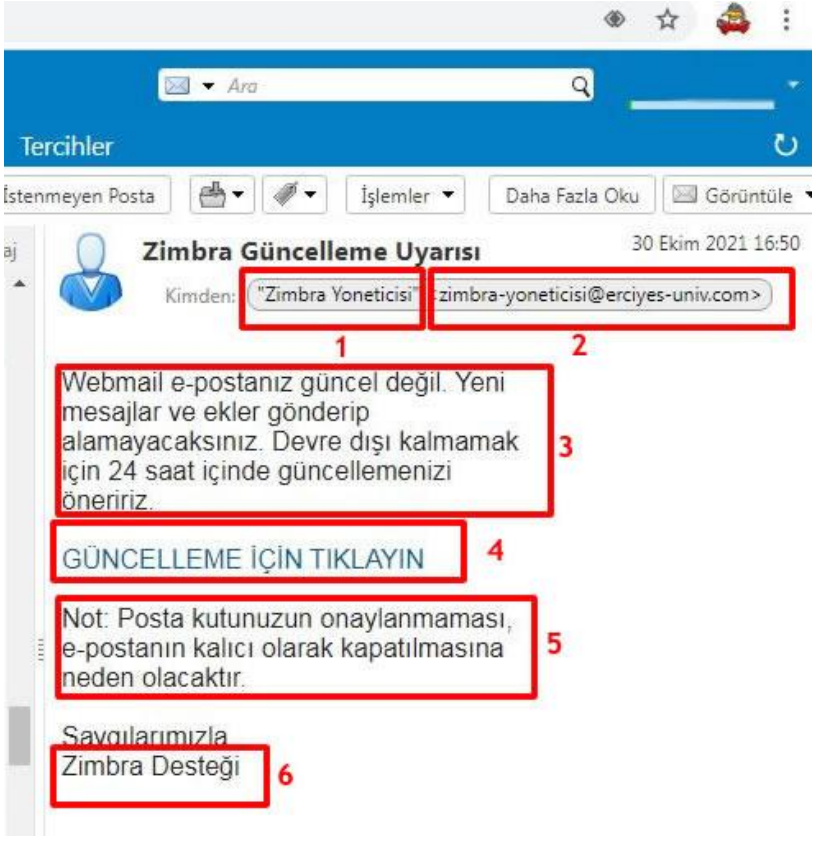


Oltalama amaçlı gönderilen e-postalar ve sahte web siteleri nasıl tespit edilir?

4- Tam bir oltalama postası klasiği olan, bağlantıya tıklatarak bilgileri yazmanızı istedikleri sayfaya sizi çekmektedir. Bazen sizi çektikleri sayfalar kurumsal web sayfalarının birebir kopyasıdır. Bizim örneğimizde de bağlantıya tıkladığınızda karşınıza gelecek olan sayfa tam bir kopyadır. Adres http://www.erciyesmail.xyz/ şeklinde kurumla alakası olmayan bir adrestir. Bu tür adreslere gidilmemelidir.

5- Hizmet kesintisi olacağını, hesabının kapatılacağını tekrar belirterek korkuyu yinelemiştir. Bazen kullanıcıyı bir ödül ile de bağlantıya göndermeye çalışırlar, örneğin kotanız artacak, örneğin çekilişten size ödül çıktı vb.

6- Oltalama e-postasının imzası kurumsal değil. Global kelimeler seçilir çünkü hedef rastgeledir



Oltalama 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.

Eğer e-posta ile size gönderilen bağlantı adresine gitmişseniz, kullanıcı bilgilerinizi bu linkteki sahte sayfaya yazmışsanız, hangi servisin kullanıcı bilgilerini yazmışsanız o servisin bildiğiniz giriş sayfasından hemen parolanızı değiştirmeniz gerekmektedir. Aksi durumda hesabınız ele geçirilir.

Bu tür bir oltalama e-postası aldığınızda kurumunuzun ilgili birimine e-postayı ileterek onları da bilgilendirmeniz, sizden sonra bu oltalama postasının kurumsal kullanıcılara dağılmaması için önlem alınmasında faydalı olacaktır.

E-posta hesabımın parolası 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 saldırgana yönlendirilir ve sizdeki kopyası silinir.
- Hesabınızdaki mesajların tümü silinebilir.
- E-posta hesabınızda kayıtlı bulunan başka sitelerin parolaları ele geçirilir.
- Eposta hesabınızla kayıtlı olduğunuz tüm siteler özellikle alışveriş sitelerinin parolası elde edilir. Alış veriş sitelerinde kayıtlı kredi kartınız var ise bu bilgilere de erişilir.
- E-postanızın parolası ile aynı olan başka hesaplarınızın da parolaları ele geçirilmiş olur.

Çevrimiçi dolandırıcılıktan korunmanın yolları nelerdir ?

- E-posta hesabınız için kullandığınız şifre, diğer hesaplarınızdaki 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.

Çevrimiçi dolandırıcılıktan korunmanın yolları nelerdir ?

- 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 paylaşıp 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 Internet'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.**