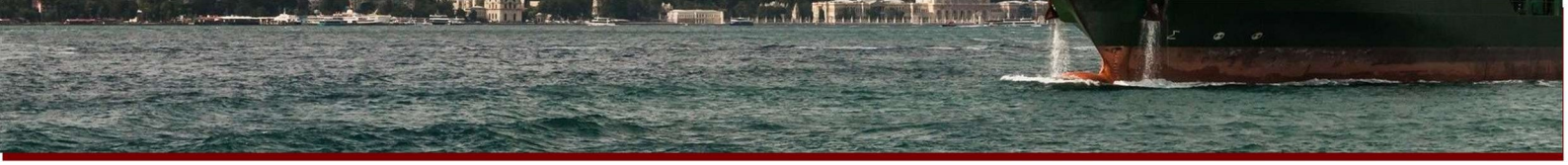


Esenyel | Partners
LAWYERS & CONSULTANTS

Bülten

KONU: Mailleşmeler üzerinden gerçekleştirilen dolandırıcılık fiilleri ve bu suçlara karşı alınabilecek önlemler hakkındadır.

AÇIKLAMALAR:

Malumunuz olduğu üzere e-mail yoluyla gerçekleştirilen dolandırıcılık suçları günümüzde sayıca artmış ve çeşitli şekillerde karşımıza çıkmaya başlamıştır. E-mail üzerinden gerçekleştirilen dolandırıcılık suçunun en etkili olduğu ve mağdurun duyduğu güven neticesiyle fark etmesinin en güç olduğu yöntemlerden biri de müşteri ile iş sahibi arasındaki e-mail silsilesine sızmaktır. Günümüzde sıklıkla, müşteri ile iş sahibi e-mail üzerinden iletişim halinde iken para havalesi aşamasında dolandırıcılar e-mail sistemindeki şifreleri etkisiz hale getirerek devreye girmekte ve mağdura kendi IBAN bilgilerini ileterek suçu tamamlamaktadır.

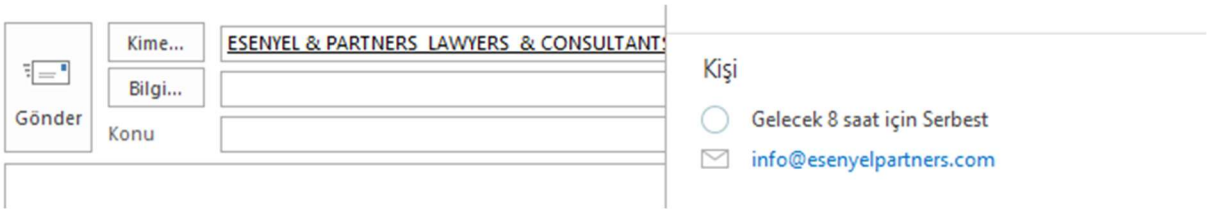
İşbu bilgi notunda da belirtilen dolandırıcılık yöntemleri ve önüne geçmek için alınabilecek önlemler ele alınacaktır.

1. **Klonlama**

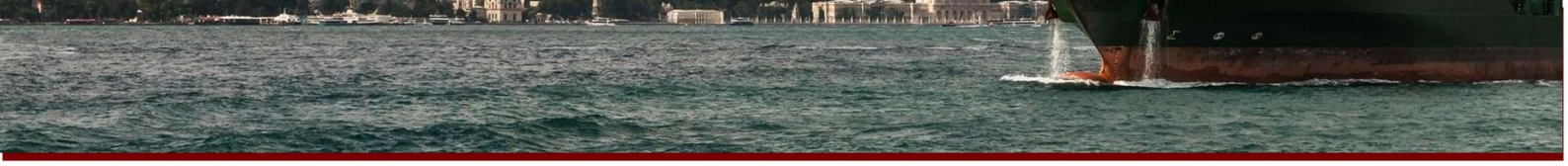
Klonlama yöntemiyle yapılan e-mail saldırıları, daha önceden gönderilmiş bir bağlantıyı veya eki içeren mailleri konu etmektedir. Saldırganlar, resmi e-mailin bir klonunu hazırlayarak güvenli bir bağlantıyı veya dosyayı, zararlı yazılımlı dosyalarla veya eklerle değiştirir. Kullanıcının fark etmesi oldukça zor olan bu tarz maillerde, gönderenin adresini dikkatle incelemek, adresin size ulaşan önceki maillerine bakıp karşılaştırma yapmak oldukça önemlidir.

Halihazırda mailleşme halinde iken sistem yöneticisi/e-mail silsilesi içerisindeki kişi tarafından gönderilmiş gibi görünen bir e-mail gelir; size kişisel bilgilerinizin güncellenmesi gerektiği, bilgilerinizin tekrar girilmesi belirtilir ve sizden bilgilerinizi göndermeniz istenir.

Bu doğrultuda, e-mailin geldiği isim bilgisinin üstüne tıklanmalı ve e-mail adresinin isim ile olan uyumu, önceki mailler aracılığı ile teyit edilmelidir. Örnek görsel aşağıdaki gibidir.



Burada dikkat edilmesi gereken husus e-mailin alışılagelmiş uzantıya sahip bir adresten gönderildiği gibi görünmesine rağmen gönderen kısmına bakıldığında farklı bir hesaptan gelip gelmediğinin teyidinin sağlanmasıdır. Gelen e-mailin kimden geldiğinden emin değilseniz lütfen dikkate almayınız. Bu tür bir durumla karşı karşıya kalırsanız kurumla irtibata geçmeden ve e-mailin doğruluğu



onaylanmadan cevap vermeyiniz. Ayrıca e-mail ekinde dosya varsa, bu dosyayı antivirüs programıyla taramadan açmamalı; PDF, Word dâhil olmak üzere birçok dosyanın zararlı yazılım içerebileceğini dikkate almalısınız.

2. Mızrak Kimlik Avı

Mızrak kimlik avı yöntemi, genelde şirketlere veya belirli bir kişiye yönelik e-mail saldırılarından ibarettir. Hedeflenen kişinin özel bilgileri kullanılarak, atılan sahte e-mailin gerçek gibi görünmesi sağlanır. Bu tarz e-maillerde, saldırganlar genelde kişinin gerçek adını, nerede yaşadığını, meslek arkadaşlarını ve diğer bilgileri içeren detaylarla son derece inandırıcı bir e-mail hazırlayabilir. Bu noktada dikkatli olmak için, hakkınızda bu kadar detaylı bilgiye sahip olan birinin neden e-mail yoluyla size bir talepte bulunduğu sorulmalı; mümkün ise özellikle kişisel veri iletimi ve/veya ödeme yapma aşamalarından önce telefon görüşmeleri ile teyit sağlanmalıdır.

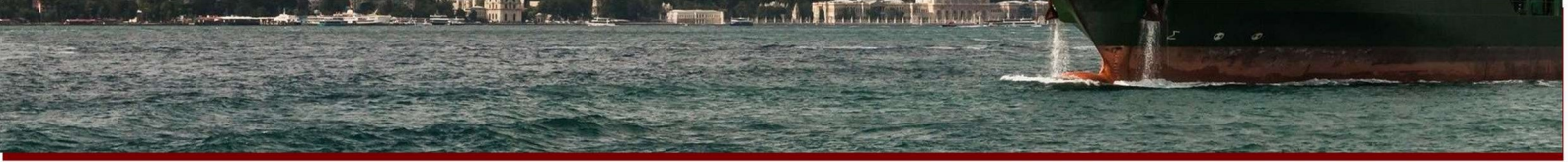
3. Password Fishing

Password Fishing, dolandırıcıların rastgele kullanıcı hesaplarına e-mail gönderdikleri bir çevrimiçi saldırı türüdür. E-mailler, bilinen web sitelerinden veya kullanıcının bankasından, kredi kartı şirketinden, e-mail 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. Kullanıcılar bu siteye girdiklerinde Password Fishing saldırısını yapan kişiye iletilmek üzere kişisel bilgilerini girmeleri istenir.

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

Dolandırıcı, daha önce kurumun web sayfasının bir benzerini oluşturarak size e-mail atar ve e-mail içinde bir link vererek bilgilerinizi güncellemenizi ister. Amaç sizi sahte sayfaya yönlendirip bilgilerinizi çalmaktır. Sayfa içindeki linke tıkladığınızda sizi herhangi bir sosyal medya sayfasına benzer bir adrese yönlendirebilirler; dikkat etmeden bilgilerinizi girerseniz bilgileriniz korsanların eline geçmiş olur.

Bu tür bir durumda yapmanız gereken e-mail içerisinde gelen site bağlantı adreslerine kesinlikle tıklamamaktır. Bu tür bir durumla karşı karşıya kalırsanız karşı tarafla irtibata geçmeden ve e-mailin doğruluğu onaylanmadan lütfen e-maile cevap vermeyiniz.



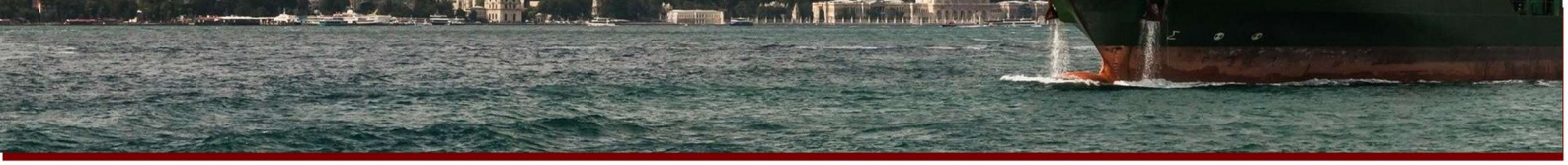
4. Mail Zincirinde Araya Girme

Mail zincirinde araya girme isimli bu yöntemde, saldırganlar öncelikle hedef olarak seçtikleri şirketlerin e-mail hesaplarını ele geçirip yazışmalarını takip ederler. Konuşmaları izler ve ticari yazışmaları dikkatle inceleyerek, yüksek meblağlı bir para transferi tespit ettiklerinde, taraflardan birinin e-mail adresini tek bir harfle taklit ederek yeni bir mail hesabı açarlar. Bu e-mail hesabıyla mail zincirine dâhil olan saldırganlar, araya girerek kendi banka bilgilerini paylaşırlar. Bu doğrultuda, para transferi yapılacak hesap bilgilerinin doğruluğu farklı kanallardan teyit edilmelidir.

Dolandırıcıların kullandığı yöntemleri açıklamamızın akabinde alınabilecek önlemlere dair genel önerilerimiz aşağıdaki gibidir.

- E-mail üzerinden gerçekleştirilen görüşmeler sonucunda ödeme aşamasına geçildiğinde IBAN bilgisi gönderilmeden önce IBAN numarasının doğruluğu için sözlü olarak (telefon vs. ile) teyit sağlandıktan sonra mail üzerinden IBAN bilgisi paylaşılıp ödeme yapılabilir.
- E-mail üzerinden gerçekleştirilen görüşmeler sonucunda ödeme aşamasına geçileceği biliniyor ise, daha önceden haricen telefon görüşmesi yahut farklı bir kanal ile taraflar arasında herhangi bir kod kodu belirlenerek IBAN bildirilecek mailin sonuna ilgili kod eklenebilir.
- Günümüzde QR kod oluşturma hayli kolay bir hal aldığından taraflar arasında haricen paylaşılacak bir QR kod, IBAN bilgilerinin iletildiği e-mail sonuna eklenerek teyit sağlanması mümkündür.

Emniyet Genel Müdürlüğü'ne yapılan başvuru ve incelemeler incelendiğinde sıklıkla mail zincirinde araya girme yönteminin kullanıldığı anlaşılmış olup gelen her maildeki e-mail adresi, e-mail adresinin üstüne tıklanınca çıkan isim ve e-mail imzası bilgilerini teyit etmeniz; şayet mümkün ise yukarıda sıraladığımız önlemleri alarak kendinizi güvence altına almanızı tavsiye ederiz.



Esenyel | Partners
LAWYERS & CONSULTANTS

İlgili Kişiler

Selçuk Sencer ESENYEL

selcuk@esenyelpartners.com

Tel: +90 212 397 1991

Fax: +90 212 397 1992

Mob: +90 506 792 7690

Türker YILDIRIM

turker@esenyelpartners.com

Tel: +90 212 397 1991

Fax: +90 212 397 1992

Mob: +90 505 650 4724

Yasemin TOSUN

yasemin@esenyelpartners.com

Tel: +90 212 397 1991

Fax: +90 212 397 1992

Mob: +90 539 896 47 11