ING Bilgi ve İşlem Güvenliği Farkındalığı Bildirimi

ING olarak, tüm işlemlerinizin en yüksek seviyede korunmasını sağlamak için büyük bir çaba sarf ediyoruz. Fakat risklere karşı, işlemlerinizin ve verilerinizin korunması için kişisel farkındalık çok önemli olup aşağıda kişisel olarak alabileceğiniz aksiyonları dikkatinize sunarız.

- **E-Posta Oltalama Dolandırıcılığı**

E-Posta Oltalama dolandırıcılık saldırısı; resmi görünümlü, gönderen adresi, link ve markalar içeren, meşru bankalardan, operatör firmalarından, satıcılardan, kredi kartı şirketlerinden vb. gelmiş gibi görünen e-posta mesajlarının gönderildiği online bir dolandırıcılık tekniğidir. Bu tür e-postalar genel olarak sahte bir web sitesi linki içerir ve hesap sahiplerinin, müşteri isimlerini ve güvenlik bilgilerinin güncellenmesi veya değiştirilmesi gerektiği iletilerek bu bilgilerin girilmesi gerektiği konusunda yanlış bir yönlendirmede bulunabilirler. Ayrıca sahte e-posta ekinde iletilen dosyanın açılması sonrasında zararlı yazılımın bilgisayara buluşmasını sağlayabilirler.

Lütfen bu ve buna benzer, sizden bilgilerinizi isteyen e-postaları tıklamayın, ekte iletilen dosyaları açmayın. Daha fazla bilgi için aşağıda yer alan ING'nin standart e-posta uygulamalarına bakabilirsiniz.

- **Web Siteleri Oltalama Dolandırıcılığı**

Web Oltalama dolandırıcılığı; Sosyal Medya üzerinden kampanya içerikli sahte uzantılara veya arama motoru üzerinden sahte web sitelerine giriş yapılarak açılan sayfada mobil/internet bankacılığı erişim unsurlarını paylaşılması sonucunda gerçekleştirilen dolandırıcılık yöntemidir. Bu tip vakalara maruz kalmamak için işlem yapılacak web sitesinin doğruluğundan emin olunmalıdır. Web adresinde bulunan yanlış bir harf veya rakam sahte bir sitede hesaplara erişim için gerekli olan tüm bilgilerin dolandırıcıların eline geçmesine neden olabilir. Web sitesine arama motoru yerine mümkün olduğunca tarayıcıya web adresi yazılarak ulaşılmalıdır.

Şüphelendiğiniz e-dolandırıcılık saldırıları ile ilgili bildirimde bulunmak için some@ing.com.tr adresine e-posta gönderebilirsiniz.

- **Sosyal Mühendislik Yöntemi**

Kişilerin bankadan ya da resmi kuruluşlardan aradığını iddia eden kişiler tarafından güven sağlanarak, ikna edilerek ya da korkutularak kandırılması ve bu yolla kart şifresi ya da internet/mobil bankacılık erişim unsurlarının ele geçirilmesi veya kişinin bilmediği şahıs veya hesaplara para transferi yapması sonucunda gerçekleşen dolandırıcılık yöntemidir.

- **Kredi Kartı/Banka Kartı Dolandırıcılığı**

Kişisel bilgilerin ele geçirilmesi sonrasında kişinin bilgisi dışında kredi kartı/banka kartı ele geçirilerek fiziki işlemler yapılması ya da kart numarası, son kullanım tarihi ve arka yüzde bulunan güvenlik kodu ele geçirilerek kart sahibinin bilgisi dışında internet üzerinden ya da mail order yoluyla işlem yapılması şeklinde gerçekleşen dolandırıcılık yöntemidir. Kart

verilerinin güvenli olmayan ortamlarda paylaşılmaması, şifrenin dışarıdan herhangi bir şekilde ele geçirilmemesi için elimizle gizleyerek girilmesi, e-ticaret işlemlerinin 3D Secure yöntemi ile yapılmaya özen gösterilmesi ve sanal kart kullanımına yönelmek müşteri olarak alınabilecek en temel önlemlerdir.

• Banka Teminatı Dolandırıcılıkları

Banka teminatı dolandırıcılıkları, ING gibi önde gelen bankalar tarafından düzenlenen banka teminatlarını satın alan bir fona yatırım yapmanız halinde sizi kısa yoldan zengin edebilecek sahte yatırım planlarını kapsar.

Dolandırıcılar sizi yatırım yapmaya davet edebilir ve banka teminatlarının indirimli olarak alınacağını, kısa süre içinde de yüksek bir kârla satılacağını söyleyebilir. Size resmi görünümlü karışık evraklar göstererek bu planların hukuka uygun ve meşru görünmesini sağlamaya çalışacaklardır. Yatırımlarınızın dünya çapındaki büyük bankalarca desteklenen akreditiflerle, banka teminatlarıyla veya diğer teminatlı belgelerle güvence altına alınabileceği konusunda sizi aldatabilirler. Planlarına büyük meblağlar yatırmanız halinde yüksek kârlar elde edeceğinizi iddia edebilirler. Fakat paranızı elden çıkardığınız anda ilgili yatırım şirketiyle birlikte paranız da yok olacaktır.

Bu tür e-postalara lütfen cevap vermeyin. Bunlar dolandırıcılık amacıyla gönderilmektedir ve vaat edilen para size ulaşmayacaktır.

• Sahte İş İlanları

İşe alım dolandırıcıları bazı şirketler adına size iş ilanı ile ilgili e-posta gönderir ve bu iş ilanına başvurmanızı teklif ederler. Aslında bu iş ilanları kara para aklama için kurulan bir tuzaktır. Bu epostalarda sizin isminiz ve diğer kişisel bilgileriniz yer alabilir ve bu da sizin bu e-postaların dolandırıcılar tarafından gönderildiğini anlamanızı zorlaştırabilir. Bu tür iş fırsatları kesinlikle ING ile ilgili değildir.

Lütfen bu tür bir e-postalara kesinlikle cevap vermeyin.

• Ön Ödeme Dolandırıcılığı

Ön ödeme dolandırıcılığında sizlerden mütevazı ücretlerle hukuki ücretleri karşılamanızı, hesap açmanızı veya gümrük harçlarının ödemenizi isteyip karşılığında yüksek meblağda paralar teklif edilebilir. Bazen teklif edilen para aslında hiç almadığınız bir piyango biletinden geliyor gibi gösterilir, bazen de para yurt dışı bir hesapta tutulur fakat hesap sahibi buna erişemez. Yardım edip ücretleri ödemeniz karşılığında bu paranın belirli bir yüzdesini size vereceklerini vaat ederler.
Lütfen bu tür e-postalara cevap vermeyiniz ve her hangi bir ödeme yapmayınız.

Bu tür dolandırıcılık gerçekleştiren suçluların bu tür işlemlerin bir parçası olarak zaman zaman ING'nin veya ING'e bağlı bir kuruluşun ismini kullanmaktadırlar.

• **ING'nin Standart Uygulamaları**

ING olarak müşterilerimizle haberleşme araçlarımızdan birisi e-postadır. Aşağıdaki bilgiler ile bankamız tarafından gönderilen e-postaların gerçekten bankamıza ait olup olmadığını anlayabilirsiniz.

• ING, Bireysel müşterileri olan sizlere tüm e-postalarında isminizle hitap eder.

• ING, sizleri kişisel bilgilerinizi (ad, soyadı, TCKN, anne kızlık soyadı, parola gibi) girmenizi gerektiren sitelere yönlendiren linkleri e-postalarına eklemez.

• ING, e-postalarında sizden asla kişisel bilginizi vererek e-postaya cevap dönmenizi istemez.

• ING, işlemleri güvenlik altına almak için en güncel şifreleme ve kimlik doğrulama mekanizmalarını kullanır.

• ING, kişisel bilgilerinizi e-posta yoluyla doğrulamamanız, teyit etmemeniz veya gerçekliğini ispatlamamanız halinde hesabınızın kapanabileceğini asla iddia etmez.

• ING, sistem güncellemelerinden dolayı e-posta yoluyla önemli bilgilerinizin (ad, soyadı, TCKN, anne kızlık soyadı, parola gibi) doğrulanmasına ihtiyacı olduğunu asla iddia etmez.

• **Web Sitelerinin Doğrulanması**

Müşteriler girdikleri sitenin gerçekten ING'e ait olduğundan ve güvenli bir site olduğundan emin olmalıdır.

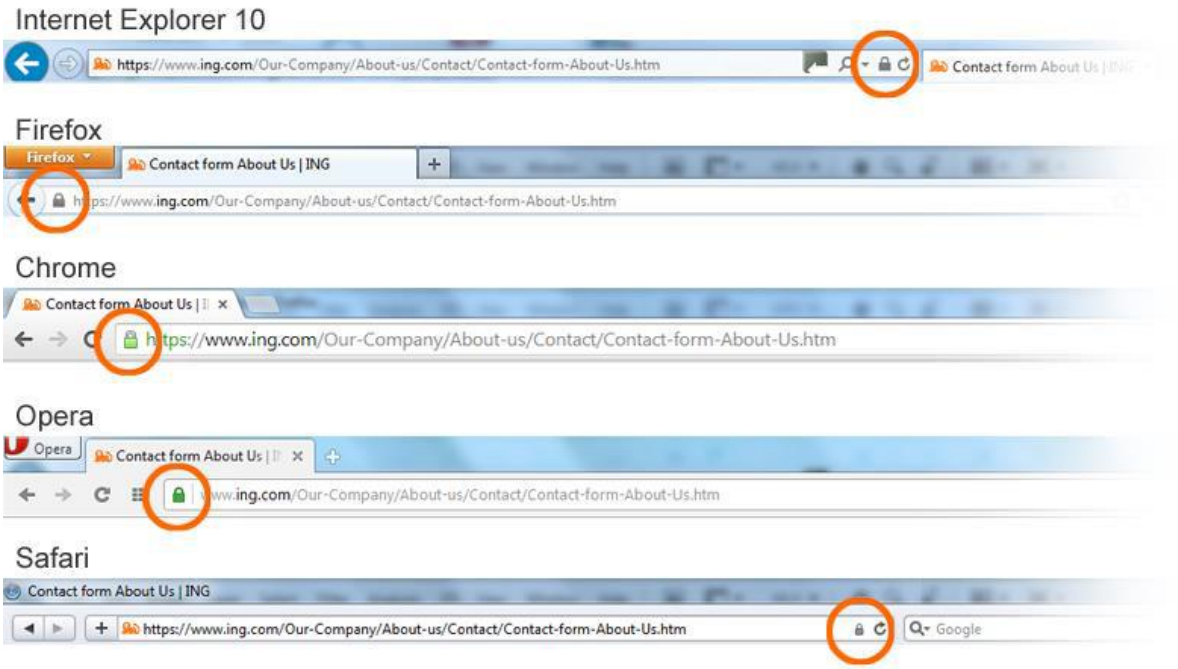
Lütfen web sitenizin güvenli olup olmadığını kontrol edin:

• URL şu şekilde başlamalı: https://

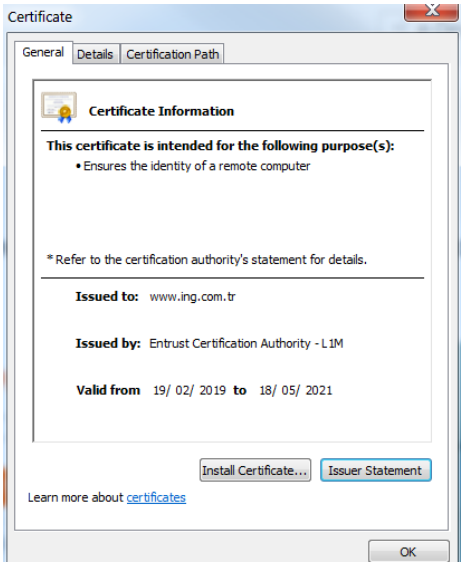
VEYA

• Uygulama penceresinde, SSL (Güvenli Soket Katmanı) Kütüphanesi belirtilmeli.

Eğer https ise, tarayıcıda güvenli kilit ikonu olarak aşağıda gösterildiği şekilde küçük bir kilit ikonu görünecektir.



Kilit ikonuna tıkladığınızda bir güvenlik sertifikası görünmelidir.
Sertifika, web sitesinin kime ait olduğunu gösterir; burada bankanızın adı görünmelidir.
Verilerin ve geçerliliklerinin doğru olduğunu teyit etmelisiniz.
Müşteriler, bir web sitesi hakkında şüphe duymaları halinde bankaları ile iletişime geçmelilerdir.



Akıllı telefonlar için geliştirilen dolandırıcılık amaçlı uygulamalardan nasıl korunabilirsiniz?

Uygulama mağazalarında (App Store, Play Store vb.) yer alan tüm uygulamalar yasal olmayabilir.

Uygulama mağazalarının sahipleri; sürekli olarak sahte anti-virüs programları, İnternet tarayıcıları ve oyunlar gibi dolandırıcılık amaçlı uygulamaları mağazalarından çıkarırlar. Siber dolandırıcılar ING ürünlerini de taklit etmeye çalışabilirler.

Dolandırıcılar sahte bir uygulamayı indirmenizi sağlamak için her türlü yolu deneyeceklerdir. Verilerinizi tehlikeye düşürecek bu uygulamaları telefonunuza yüklemeniz için, ING gibi güvenilir markalardan gönderilmiş gibi gözüken e-posta ve SMS'leri kullanabilirler. Bu sahte uygulamalar bazen güvenlik güncellemeleri şeklinde gelebilir ve gelen linkler üzerine tıklayarak da bilgilerinizin çalınmasına neden olabilirsiniz.

Uygulamalarınızı yalnızca resmi kaynaklardan indirin. Herhangi bir uygulama indirmeden önce biraz araştırma yapın. Bir uygulamanın geniş çapta popüler olması iyi bir uygulama olduğunun işaretidir. Uygulamanın kaç kere indirildiğine bakabilir, yorumlarını okuyabilir, geliştiren firmaya bakabilir ve internet üzerinden biraz araştırma yapabilirsiniz.

Eğer beklenmedik bir SMS, aşina olmadığınız uyarı veya bildirim ya da ING veya bildiğiniz diğer markalardan olağandışı talepler alırsanız dikkatli olun. Dolandırıcılar cihazınıza sahte bir uygulama indirmeye çalışıyor olabilir. Bu nedenle, size gelen her türlü bağlantıya tedbirli yaklaşmalı ve her zaman öncelikle mesajı okumalısınız. Mesajda iletilen bağlantıyı kullanmak yerine doğrudan normalde kullandığınız web sitesi veya uygulama mağazasına gitmeli ve normalde yapacağınız gibi hesabınıza giriş yapmalısınız.

Kendinizi Koruyun

• Kişisel bilgilerinize dikkat edin

Hesap numaralarınız, müşteri numaranız, PIN (şifre), önemli tarihler ve müşteri kimlik numaranız hesabınıza erişmeniz için gereken anahtar bilgilerdir. Bunları asla yazıya dökmeyin, başkası ile paylaşmayın ve e-postalarınıza eklemeyin. Kişisel bilgiler içeren dokümanları güvenli şekilde yok edin ve internet üzerindeki sosyal ağlarda kişisel bilgilerinizi paylaşırken çok dikkatli olun. Çünkü dolandırıcılar sahtekârlık yaparken bu bilgilerinizi kullanabilirler. **Unutmayın ki Müşteri Numaranızı, PIN numaranızı, şifrelerinizi ve güvenlik detaylarınızı korumak sizin sorumluluğunuzdadır.**

• Bilgisayarınıza dikkat edin.

• Bilgisayarınızda bilinen her türlü zayıf noktayı kapatabilmek için bilgisayarınıza en güncel yazılımları ve eklentilerini yükleyerek bilgisayarınızı güncel tutun.

• Bilgisayarınıza zarar vermeye yönelik olan her türlü zararlı yazılımdan (virüs, Truva atı vb.) korumak için anti-virüs programı yüklemeli ve programı güncel tutmalısınız.

• Casus yazılımları engelleyen araçlar indirin ve onları güncel tutun.

• Kişisel güvenlik duvarları yükleyin ve onları güncel tutun.

• Yalnızca bilinen, güvenilir sağlayıcıların programlarını kullanın.

• Spam e-postalara dikkat edin.

• Bu mesajları görmenizi engelleyecek spam filtreleri kullanın.

• Spam mesajlara asla yanıt vermeyin; aksi halde e-posta adresiniz aktif spam listelerine

kaydedilecek ve spam'ler artacaktır.

• Bir spam mesajı okumanız halinde şunu hatırlayın: Gerçek olamayacak kadar iyi bir şey gibi görünüyorsa muhtemelen gerçek değildir.