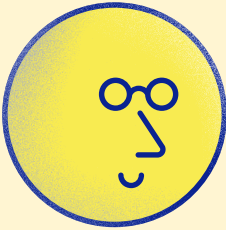


Dolandırıcılık nasıl tespit edilir ve önlenir



Kendinizi dolandırıcılıktan
koruma rehberi



Australian Government



National
Anti-Scam
Centre



ScamWatch
Stop. Better safe than scammed.

Ülkenin tanınması

Avustralya Rekabet ve Tüketici Komisyonu (ACCC), Avustralya genelinde Toprakların geleneksel sahipleri ve koruyucularını kabul eder ve onların kara, deniz ve toplumla devam eden bağlarını tanır. Onlara ve kültürlerine; ve geçmişteki, şimdiki ve gelecekteki Büyüklerine saygılarımızı sunarız.

Australian Competition and Consumer Commission

Ngunawal

23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

© Avustralya Federal Devleti 2023

Bu çalışmanın telif hakları saklıdır. *Telif Hakkı Yasası 1968* kapsamında izin verilen her türlü kullanıma ek olarak, bu çalışmada yer alan tüm materyal Creative Commons Attribution 4.0 Avustralya lisansı altındadır. Bu kapsam dışında olanlar aşağıdaki gibidir:

- Federal Devlet Arması
- Avustralya Rekabet ve Tüketici Komisyonu (ACCC) ve Avustralya Enerji Düzenleme Kurulu (AER) logoları
- Avustralya Rekabet ve Tüketici Komisyonunun telif hakkı sahibi olmadığı ancak bu yayının bir parçası olabilecek ya da bu yayının içeriğinde olabilecek herhangi bir resim, şema, fotoğraf veya grafik.

Lisans şartlarının detaylarına ve CC BY 4.0 AU lisansı yasal koduna Creative Commons internet sitesinde erişilebilir.

Yeniden basılması ve haklar konusunda soru ve isteklerinizi aşağıdaki adrese gönderiniz. Director, Corporate Communications, ACCC, GPO Box 3131, Canberra ACT 2601.

Önemli duyuru

Bu yayındaki bilgiler sadece genel yol gösterici niteliğindedir. Yasal veya profesyonel tavsiye niteliğinde değildir ve herhangi bir yargı alanında yasa metninin ifadesi niteliğini taşımaz. Çünkü, sadece genel yol gösterici olarak amaçlanmıştır, genellemeler içerebilir. Herhangi bir kaygınız varsa bir uzman görüşü alınır.

Avustralya Rekabet ve Tüketici Komisyonu (ACCC) güncel ve doğru bilgiyi vermek için tüm akılcı adımları atmakta ancak bu bilginin doğruluğu, güncelliği ya da eksikleri olup olmadığı konusunda herhangi bir garanti vermemektedir.

Bu yayındaki bilgiyi yeniden yayınlamak veya başka şekilde kullanmak isteyen taraflar, yayınlamadan önce bu bilginin güncelliği ve doğruluğunu araştırmalıdır. Bu araştırmanın, Avustralya Rekabet ve Tüketici Komisyonu'nun (ACCC) rehber ve ilgili geçiş mevzuatı sık sık değiştiğinden, her baskı yayınlamadan önce yapılması gerekir. Tarafların, sorularını aşağıdaki adrese göndermeleri gerekmektedir: Director, Corporate Communications, ACCC, GPO Box 3131, Canberra ACT 2601.

ACCC 05/24_24-13

www.accc.gov.au

İçindekiler

Yardım alabilirsiniz	1
Dolandırıcılık nedir	3
Dolandırıcılığı tespit etmek ve korunmak için basit adımlar	4
Mesaj yoluyla dolandırıcılık	7
Elektronik posta dolandırıcılığı	11
Telefon dolandırıcılığı	15
İnternet sitesi üzerinden dolandırıcılık	19
Sosyal medya, uygulama veya internette mesaj yoluyla dolandırıcılık	23
Bilmeniz gereken en yaygın dolandırıcılıklar	27
Dolandırıcılığı nereye bildirmelisiniz?	31
Daha fazla yardım ve destek	33



Bu rehber Ulusal Dolandırıcılıkla Mücadele Merkezi tarafından, dolandırıcılığı tespit etmenize ve kendinizi dolandırıcılığın yaratacağı zarardan korumanıza yardımcı olmak amacıyla yazılmıştır.

Dolandırıcılık suçtur ve dolandırıcılık yapan kişi suçludur. Avustralya'da pek çok kişi dolandırılmakta ve bazen hayat boyu biriktirmiş oldukları parayı kaybetmektedir. Dolandırıcılık insanların hayatını karartır.

Dolandırıcılığı tespit etmek giderek zorlaşıyor. O nedenle dolandırıcıları durdurmak için birlikte hareket etmemiz gerekir.

Ulusal Dolandırıcılıkla Mücadele Merkezi, Avustralyalıları dolandırıcılıktan korumak için çalışmaktadır.

Biz, dolandırıcıların, Avustralyalıların kişisel bilgilerini ve paralarını çalmaması için yeni yöntemler bulmak üzere hükümet ve özel sektöre birlikte çalışıyoruz. Bunu başarmak için bulduğumuz yöntemlerden bazılarını burada bulabilirsiniz.

Dolandırıcılığı tespit etmeleri ve ondan korunmaları için insanlara yardım ediyoruz

Scamwatch yoluyla dolandırıcılıkla ilgili güncel bilgileri ve kendinizi dolandırıcılıktan koruyabileceğiniz yöntemleri paylaşıyoruz.

Biz, dolandırıcılığa engel oluyoruz

Hükümet ve endüstri ile topladığımız ve paylaştığımız bilgiler yoluyla dolandırıcıların suç işlemeye devam etmelerini zorlaştırıyor ve insanların dolandırıcılığı bildirmelerini kolaylaştırıyoruz.



Yardıma alabilirsiniz

Bunu okuyorsanız, siz ya da tanıdığınız birisinin dolandırılmış olma ihtimali vardır. Ne yazık ki yalnız değilsiniz. Dolandırıcılıklar giderek daha karmaşık hale geldiğinden herkesin dolandırılma ihtimali var.

Dolandırıcılık mağduruysanız, hemen harekete geçmeniz önemlidir.

Dolandırıcıya para kaptırdıysanız, bankanız ya da kartınızı veren kuruluşla iletişime geçin.

1800 595 160 Numaralı telefondan veya www.idcare.org adresinden IDCARE ile iletişim kurun.

Dolandırıcılıklar gerçekmiş gibi göründüklerinden sonuca ulaşıyor. Dolandırıcılar, kaçırılmayacak bir şey gibi görünen ya da güvendiğiniz bir kişiden geldiğini zannettiğiniz bir şey için acele ettiğinizde, uyarıları farketmeyeceğiniz durumdan yararlanır.

Aşağıdaki 3 adımı takip ederek kendinizi dolandırıcılıktan koruyun.

Dur



Emin değilseniz, kimseye kişisel bilgi ya da para vermeyin.

Dolandırıcılar size yardım teklif eder ya da sizden kim olduğunuzu teyit etmenizi ister. Hizmet kuruluşları, polis, banka ya da devlet kurumları gibi bildiğiniz ve güvendiğiniz bir kuruluştan arıyormuş gibi davranırlar.

Kontrol Et



Kendinize sorun - bu mesaj veya arama sahte olabilir mi?

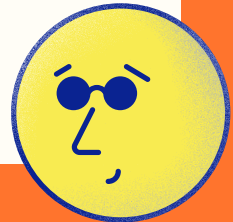
Mesajdaki bağlantıyı asla açmayın. Sadece resmi internet sitesi veya uygulamalarında iletişim bilgileri olan işletme ya da devlet kurumlarıyla iletişim kurun. Emin değilseniz, 'hayır' diyerek telefonu kapatın ya da mesajı silin.

Bildir



Bir şey yanlış görünüyorsa, hemen harekete geçin.

Bir dolandırıcı paranızı veya bilgilerinizi aldıysa veya olağan dışı bir işlem farkederseniz bankanızı arayın. Yardım isteyin ve ReportCyber ve Scamwatch'a bildirin. Dolandırıcılıkları bildirdiğiniz zaman, dolandırıcılığa karşı savunmamızı güçlendirerek tüm Avustralyalılara yardım etmiş olursunuz.



Dolandırıcılık nedir

Dolandırıcılık, birisinin paranızı veya kişisel bilgilerinizi çalmak için sizi kandırmasıdır.

Dolandırıcılıklar ekonomiyle ilgili suçlardır ve bu suçu işleyenler genellikle çok organize ve tecrübelidir.

Dolandırıcılık:

-  suçlular tarafından
-  gerçekleştirilir
-  gerçek gibi görünür
-  inandırıcı senaryolarla yapılır
acele etmeniz için size baskı yapar

Neler dolandırıcılık DEĞİLDİR:

-  Bilgisayar korsanlığı
-  Adil olmayan sözleşme şartları
-  Rahatsız edici pazarlama yaklaşımları

Her olumsuz deneyimin dolandırıcılık olmadığını unutmamak önemlidir. Parasını ödediğiniz bir ürün elinize geçmemiş ya da satın aldığınız bir şeyin kalitesinin düşük olduğunu görmüş olabilirsiniz. Bu hayal kırıklığına uğratır ama bunlara muhakkak dolandırıcılık diyemeyiz. Avustralya Tüketici Yasası, bu gibi sorunlar karşısında Avustralyalı tüketicileri korumaktadır.

Daha fazla bilgi için www.accc.gov.au/consumers internet adresini ziyaret edin.

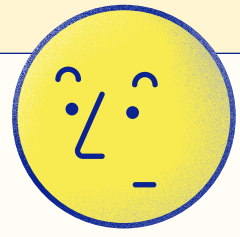
Dolandırıcılığı tespit etmek ve korunmak için basit adımlar

Dolandırıcılık hepimizin başına gelebilir. Dolandırıcılar paranızı çalmak ve kişisel bilgilerinizi almak için inandırıcı senaryolar yaratır ve bu şekilde dolandırıcılık gerçekleşir.

Dolandırıcılar gittikçe daha kurnaz hareket ediyor ve dolandırıcılıklarının gerçek olduğuna sizi inandırmak için yeni teknoloji, ürün, hizmet ve büyük olayları kötüye kullanıyorlar.

Dolandırıcılığı tespit etmek çok zor olabilir. Dikkat edilmesi gereken bazı durumlar şunlardır: Dolandırıcılar bazen bu taktiklerin birkaçını bir arada kullanır.

- 1. Para kazanmak veya daha az para harcamak için fırsatlar:** Dolandırıcılar sizi hiç kaçırılmayacak bir fırsat yakaladığınıza inandırır. Fırsatı kaçırmayın diye acele etmenizi sağlamak üzere baskı yaparlar. Unutmayın, gerçek olamayacak kadar iyi görünen teklifler genellikle gerçek değildir.
- 2. Acıklı hikayeler ve yardım çağrıları:** Dolandırıcı, iyi niyetinizi size karşı kullanmaya uğraşır ve kullanır. Üzüntü verici hikaye ve trajik olayları sizinle paylaşarak yardımınıza ve paranıza neden ihtiyaçları olduğunu açıklarlar.
- 3. Bağlantı ve ekler:** Dolandırıcılar, size, bilgilerinizi ve paranızı çalmak için tasarlanmış dolandırıcılık sitelerine yönlendirmek için bağlantı gönderir. Dolandırıcılar, sizden ekteklere açmanızı isteyebilir. Bunlar, cihazınıza, bilgilerinizi çalan virüsler yerleştirebilir.



4. **Acele hareket ettirmek için baskı:** Dolandırıcılar, sizin yavaş hareket etmenizi ve düşünmeye fırsat bulmanızı istemez. Size acele hareket etmeniz için baskı yapmak isterler. Eğer acele hareket etmezseniz başınıza kötü bir şey geleceğine dair tehdit de edebilirler.
5. **Ödemenizi olağan dışı ya da kendi istedikleri şekilde yapmanızı isterler.** Dolandırıcılar sıklıkla az rastlanan yöntemlerle ödeme yapmanızı isterler. Örneğin, ön ödemeli banka kartı, iTunes kartı veya Bitcoin gibi sanal parayla. Parayı harcadığınız anda artık geri alamazsınız.
6. **Yeni hesaplar açmanızı ya da yeni PayID oluşturmanızı isterler.** Dolandırıcılar, onlara ödeme yapmanız (ya da onların size ödeme yapması) için yeni bir banka hesabı açmanızı veya PayID oluşturmanızı isterler. Bankanızmış gibi rol yaparak, paranızı emniyete almak için yeni hesaplara aktarmanızı isteyebilirler.

Eğer dolandırıcılar paranızı almayı başarırsa, daha fazla almaya çalışacaklardır. Ne yazık ki, üç dolandırıcılık mağdurundan birisi parasını birden çok kez kaptırmıştır. Eğer dolandırıcıya para kaptırdıysanız, paranızı geri almanıza yardım edeceğini söyleyen diğer dolandırıcılara karşı uyanık olun. Bu, dolandırıcılığın ardından yapılan başka bir dolandırıcılık türüdür.



Mesaj yoluyla dolandırıcılık

Dolandırıcılar size, devlet dairesinden, emniyetten, güvenilir ticari işletmelerden, hatta arkadaş veya aile bireylerinden geliyormuş gibi mesaj gönderirler.

Bu mesajlar hep acilmiş gibi görünür ve sizin de acele hareket etmenizi ister. Genellikle, bu mesajlarda dolandırıcılık sitesine yönlendiren bir bağlantı vardır. Dolandırıcılar, bu sitelere girdiğiniz kişisel bilgilerinizi, paranızı çalmak ya da adınızı kullanarak sahtekarlık yapmak için kullanabilirler.

Bu mesajların gerçek gibi görünmesi için, dolandırıcılar, telefon numaralarını, tanıdığınız kişilerin veya yasal ticari işletmelerin arama kimliği ve telefon numaralarını kopyalayarak ya da o numaraların arkasına gizleyerek yanıtlırlar.

Dolandırıcılık mesajları, kurumlardan gelen gerçek mesaj zinciri arasında bile belirebilir. Bu da tespit edilmelerini zorlaştırır.

Bir mesajın dolandırıcılık olduğunu ayırt edebilmek için ipuçları

Bu mesaj:



Hemen harekete geçmenizi, ödeme yapmanızı ya da para aktarmanızı ister.



İçeriğindeki bir bağlantıyı tıklamanızı veya oradaki telefon numarasını aramanızı ister.



Çevrimiçi bir hesaba, kullanıcı adınız ve parolanızla giriş yapmanızı veya diğer kişisel bilgilerinizi vermenizi ister.



Bir aile bireyinden ya da arkadaşınızdan gelir ve iletişim bilgilerinin değiştiğini belirtir.



Hizmeti durduracağını ya da harekete geçmezseniz para cezası uygulanacağını belirtir.



Sizin ya da hesaplarınızın ele geçirildiğini ya da dolandırıcılıkla ilgili kullanıldığını söyler.



Ödemeleriniz veya paket teslimiyle ilgili bir problem olduğunu belirtir.

Kendinizi dolandırıcılık mesajlarından korumak için hangi adımları atmalısınız?

1. Eğer tanıdığınız birisi, telefon numarasının değiştiğini söyleyen bir mesaj gönderirse;



- a. o kişiyi sizde bulunan telefon numarasından arayın
- b. yeni numaralarına sadece onların cevap verebileceği bir soru soran mesaj gönderin. Böylece o kişinin söyledikleri kişi olup olmadığını kontrol edin.



2. Mesajlardaki bağlantılara asla tıklamayın.



3. Bir mesajda, internet sitesine bağlantı varsa, bağlantıyı tıklamayın. Onu yapmak yerine, kendiniz internetten siteyi araştırın veya resmi uygulamayı kullanın.



4. Yazılı mesajdaki telefon numarasını kullanarak cevap vermeyin.



5. Kendiniz, kurumun internet sitesinden bulduğunuz telefon numarasından kurum ya da kişiyi arayın.



Elektronik posta dolandırıcılığı

Dolandırıcılar size, devlet dairesi, emniyet ve ticari işletmeden gönderilmiş gibi görünen elektronik posta gönderirler. Acil durum varmış gösterip acele harekete geçmenizi isterler.

Kurumun gerçek logosunu ve aslına benzeyen elektronik bir posta adresi kullanırlar. Elektronik posta daha da gerçek görünsün diye kurum veya ticari işletmenin elektronik posta adresini kopyalar veya kendi elektronik posta adreslerini onların arkasına gizlerler.

Bir elektronik postanın dolandırıcılık olduğuna dair ipuçları

Bu elektronik posta;



Son yaptığınız ödemeden sonra hesap detaylarının değiştiğini söyler ve yeni hesaba ödeme yapmanızı ister.



Çevrimiçi bir hesaba, kullanıcı adınız ve parolanızla giriş yapmanızı veya diğer kişisel bilgilerinizi vermenizi ister.



Beklemediğiniz bir elektronik postadır ve sizi ekteki belgeyi açmaya yönlendirir.



Beklemediğiniz bir parayı alabilmeniz veya paranın size geri ödenebilmesi için banka detaylarınızı teyit etmenizi ister.



Sizinle ilgili bilgisi veya fotoğraflarınıza sahip olduğunu söyler ve onları yayınlamakla tehdit ederler.



Kimlik hırsızlığı veya bilgi ihlali nedeniyle tazminat almanız veya paranızı kurtarmanız için yardım teklif ederler.

Elektronik posta dolandırıcılığından kendinizi korumanın yolları

1. Elektronik postanın gerçek olup olmadığını;



- a. kurumun internet sitesinden bulduğunuz iletişim detaylarıyla doğrudan kişi veya kurumu arayarak, veya
- b. resmi uygulamadan o kuruma giriş yaparak (bunu bağlantı kanalıyla yapmamalısınız).



2. Derhal sizi tehdit eden ya da gözünüzü korkutan kişilerle iletişimi kesin.



3. Size aşağıdaki teklifleri yapan herhangi bir kişiye kesinlikle kişisel bilgilerinizi vermeyin veya ödeme yapmayın:

- a. tazminat veya daha önce mağdur olduğunuz dolandırıcılık veya bilgi ihlali için yardım teklifi
- b. kazanç, ödül ya da miras konusunda teklif



4. Mümkün olduğunca Çok Faktörlü Kimlik Doğrulama (Multi Factor Authentication) kullanın. Bu ekstra bir koruma sağlar ve dolandırıcının elektronik posta parolanızı ve elektronik posta adresinize girebilmeniz için telefonunuza gönderilen pin kodunu bilmesini engeller.



Telefon dolandırıcılığı

Dolandırıcılar, sizi, tanınmış kurumlardan olduklarını söyleyerek ararlar. Bu kurumlar arasında, hükümet organları, emniyet, yatırım ve hukuk firmaları, bankalar ve haberleşme hizmeti veren kuruluşlar vardır.

Hemen hareket etmenizi istediklerinden, acil bir durum varmış gibi gösterirler. Kişisel veya banka hesap bilgilerinizi vermeye veya bilgisayarınıza giriş izni için sizi ikna etmeye uğraşabilirler.

Arayan kişi, görüşmenin gerçek görünmesi için hali hazırda isminizi ve adresinizi biliyor olabilir.

Bir aramanın telefonla dolandırıcılık girişimi olduğuna dair ipuçları

Arayan kişi:



Ödeme yapmanızı ya da yeni bir hesaba para aktarmanızı ister.



Parolanızı, şifrenizi, tek seferlik kodunuzu veya başka bir güvenlik bilginizi ister.



Kredi kartı ya da banka hesabınızla ilgili finansal bilgilerinizi ister.



Cep telefonunuzda veya bilgisayarınızda, yazılım kurmanız ya da güvenli bir çevrimiçi hesaba girmenizi ister.



Emniyet mensubu olduğunu söyler ve sizi hemen tutuklamakla ya da sınır dışı etmekle tehdit eder.



Banka ya da çevrimiçi hesaplarınızın ele geçirildiğini ya da dolandırıcılığa karıştığını söyler.

Telefon dolandırıcılığında kendinizi korumanın yolları

1. Aramanın gerçek olup olmadığını aşağıdaki yöntemlerle kontrol edin;



- a. kurumun internet sitesinden bulduğunuz iletişim detaylarıyla doğrudan kişi veya kurumu arayarak, veya
- b. resmi uygulamadan o kuruma giriş yaparak (bunu bağlantı kanalıyla yapmamalısınız).



2. Arayan kişinin kim olduğunu bilmiyorsanız ya da sizi tehdit ediyor veya korkutuyorsa, hemen telefonu kapatın.



3. Bilgisayar veya cihazınıza herhangi bir kişinin girişine izin veren yazılım kurmayın.



4. Tanımadığınız numaralardan gelen aramaları açmayın ya da sesli mesaja yönlendirin.



Bilmekte fayda var!

Numaranız gizli veya reklam amaçlı aramalara kapalı olarak kayıtlı (Do Not Call) bile olsa dolandırıcılar sizi arayabilir.



İnternet sitesi üzerinden dolandırıcılık

Dolandırıcılar, internette, devlet görevlisi, gerçek bir ticari işletme, ünlü bir kişi, arkadaş ya da aile bireyi gibi davranabilirler.

Tanınmış markaların internet sitelerine benzeyen sahte siteler oluşturabilirler. Tanınmış kişilerin taklidini yaparak ürün ya da hizmetleri onaylıyor gibi görünebilirler. Onlara güvenmenizi sağlamak için bu internet sitelerine sahte değerlendirmeler yerleştirirler.

İnternette dolaşırken, sahte uyarılar ve hata mesajları içeren sahte reklam logoları ve bildirim pencereleri görebilirsiniz.

İnternet sitesinin sahte olabileceğini gösteren ipuçları

Sahte internet sitesi:



Normalden ya da diğer sitelere nazaran çok düşük fiyata satılan ürünler teklif eder.



Az risk ya da çabayla hızlı ve kolay para kazanma yollarından bahseder.



Bir bağlantıyı tıklamanızı isteyen acil bir uyarı veya hata mesajı içerir.



Bitcoin gibi kripto para veya hediye kartı gibi olağan dışı ve belirli yöntemlerle ödeme yapmanızı ister.



Sadece olumlu değerlendirmelere yer verir.

İnternet sitesi üzerinden dolandırıcılığa uğramamak için atılacak adımlar



1. Fiyatları karşılaştırın. Bir teklif gerçek olamayacak kadar iyi görünüyorsa, muhtemelen gerçek değildir.



2. Paranızı ya da kimlik bilgilerinizi karşınızdaki kişiye vermeden önce, o kişi ya da kurumu araştırın.



3. İnternet sitesinde yazılı değerlendirmelere güvenmeyin. 'Scam' ve 'reviews' kelimelerini internet sitesinin ya da işletmenin adıyla birlikte araştırın.



4. Eğer ekranınızda uyarı veya hata mesajı belirirse üzerine tıklamayın, öyle yapmak yerine, gerçek olup olmadığını kontrol etmek için doğrudan gösterdiği uygulamaya bakın.



5. İnternet üzerinden alışveriş yapmak için kullandığınız cihazı, işletme sistemi ve uygulamalar için otomatik güncellemeyi (automatic updates) etkinleştirerek güncel tutun.



Bilmekte fayda var!

İnternette kendinizi korumak için pratik yöntemleri www.cyber.gov.au adresinde bulabilirsiniz.



Sosyal medya, uygulama veya internetten mesaj yoluyla dolandırıcılık

Eğer tanımadığınız bir kişi sizinle sosyal medya, WhatsApp veya WeChat ya da bir uygulama üzerinden iletişim kuruyorsa, bu dolandırıcılık olabilir.

Dolandırıcılar, başka biri gibi davranmaya çalışırken, o kişinin gerçek fotoğrafını ya da kurumun resmi logosunu kullanırlar. Bu da dolandırıcılığın tespitini zorlaştırır.

Sosyal medyadaki dolandırıcılar, sahte profiller açarak kendilerini devlet kurumundan, gerçek bir ticari kuruluştan veya yatırım şirketinden biri, bir işveren, hatta bir arkadaşınız, aile bireyiniz ya da size ilgi duyan bir kişi gibi gösterirler.

Ünlü kişilerin taklidini yaparak, kendilerini ürün ve hizmet tanıtımı yapıyormuş gibi gösterirler.

Dolandırıcılar, sosyal medya hesaplarınızda paylaştığınız ayrıntılardan sizinle ilgili pek çok şey öğrenirler. Bu bilgileri, hesap şifrelerinizi tahmin etmek için kullanır ya da başka dolandırıcılıklar için hedef haline getirirler.

Sosyal medya ya da uygulamalar üzerinden dolandırıcılığı anlamak için ipuçları

Sosyal medya profili veya uygulama;



Az risk ya da çabayla hızlı ve kolay para kazanma yollarından bahseder.



Sizi, bir yarışmaya veya zaman sınırlı kampanyaya katılmaya davet eder.



Görüşmeyi, uygulamadan, örneğin arkadaşlık uygulamasından özel sohbet veya elektronik postanıza taşımanızı ister.



Ünlü bir kişinin, bir ürün veya hizmeti onayladığını ya da desteklediğini söyler.



Birisinin, satışa koyduğunuz bir ürünü görmeden ve yüksek fiyata alacağını söyler.



Ona para ödemediğiniz takdirde özel bir fotoğrafınızı paylaşmakla tehdit eder.



Size bir iş teklifinde bulunmak için sizinle iletişime geçer.



Bilmekte fayda var!

Farklı sosyal medya platformlarında güvende olmak için gerekli bilgileri www.esafety.gov.au adresinde bulabilirsiniz.

Sosyal medya ve uygulama üzerinden dolandırıcılıklardan korunmanın yolları



1. Profilin sahte olup olmadığını kontrol edin Hesap aktif mi? Kaç tane arkadaş/takipçisi var ve çevrimiçi ne kadar paylaşım yapıyor?



2. 'Scam' (dolandırıcılık) kelimesiyle birlikte profil ismini internette araştırın.



3. Deneyiminiz, uygunluğunuz ve referanslarınızla ilgili görüşmeden ya da mülakatsız iş tekliflerini kabul etmeyin. Teklifi yapan işe alım uzmanını ve işi veren ticari kuruluşu ya da kişiyi araştırın. İş bulma acentasıyla, kendiniz internette aratıp bulduğunuz telefon numarasını arayarak iletişime geçin. İş garantilemek için peşin para ödemeyin.



4. Yatırım tavsiyesini sadece Avustralya Finans Hizmetlerinden yetkili bir kişiden alın ve şirket ya da internet sitesinin Uluslararası Menkul Kıymet Komisyonları Örgütü'nün (IOSCO) yatırımcıya uyarılar portalında listelenmemiş olmasına dikkat edin.



5. Sadece internette tanıştığınız bir kişiye asla para vermeyin. Dolandırıcılar sıklıkla başka ülkede yaşadıklarını ve sizinle şahsen buluşamayacaklarını söyler.



6. Sadece internette tanıştığınız bir kişiye asla özel resimlerinizi göndermeyin.

Dolandırıcıların sizinle şahsen ve elektronik posta yoluyla iletişim kurabileceği diğer yöntemleri de içeren dolandırıcılıkla ilgili bilgileri [Scamwatch](#) internet sitesinde bulabilirsiniz.



Bilmeniz gereken en yaygın dolandırıcılıklar

Dikkat etmeniz gereken en yaygın dolandırıcılık türlerini aşağıda görebilirsiniz. Scamwatch internet sitesinde uyarıcı işaretler, kendinizi nasıl koruyabileceğinizle ilgili bilgi de dahil olmak üzere bu tür dolandırıcılıkların her türü ile ilgili daha fazla bilgi bulabilirsiniz.

Taklit ederek dolandırıcılık

Dolandırıcılar, polis, hükümet dairesi, banka ve tanınmış işletmeler gibi güvenilir kurumlardan arıyormuş gibi davranarak sizi kandırırlar. Arkadaşınız veya bir aile bireyiniz gibi görünmeye bile çalışabilirler. Dolandırıcılar, sahte elektronik posta veya mesajlar göndererek sizinle ilgili bilgi araştırırlar. Bunlar bilgilerinizi çalmak üzere tasarlanmıştır. Resmi bir kurum ya da güvendiğiniz bir kişi gibi görünerek sizi, kişisel bilgilerinizi vermeye ikna etmek için uğraşırlar.

Dolandırıcılar, arama ya da mesajlarını meşru bir telefon numarasından geliyormuş gibi gösteren teknolojiler kullanırlar. Yazılı mesajlarının, bir kuruluştan gelen gerçek mesaj dizininde belirmesini sağlarlar.

Yatırım dolandırıcılığı

Dolandırıcılar, yatırım tekliflerini kaçırılmayacak fırsat gibi göstermek için ikna edici pazarlama tekniği ve yeni teknoloji kullanırlar. Size riski çok az olan ya da hiç riski olmayan büyük kar payı sözü verirler. Paranızı çalabilmek için, size, çabuk harekete geçmenizi sağlayacak baskı taktikleri uygularlar.

İş ve istihdam dolandırıcılığı

Dolandırıcılar, çok az çalışarak yüksek maaş alacağınız iş teklifi yapar. Tanınmış şirket ve çevrimiçi alışveriş platformları adına sizi işe alıyormuş gibi davranırlar. Hatta bazen, size söyledikleri iş gerçekte olmayan bir iştir. Dolandırıcılar, ayrıca tanınmış işe alım agentelerini taklit ederler. Amaçları paranızı ve kimlik bilgilerinizi çalmaktır. İşe girebilmeniz için peşin ödeme yapmanızı isteyebilirler.

Ürün ve hizmet dolandırıcılığı

Dolandırıcılar, paranızı çalmak için alıcı ya da satıcı rolü yaparlar. Sahte internet siteleri kurarak veya meşru perakendecilerin sitelerinde sahte profil açarak gerçek olamayacak kadar düşük fiyatlarda ürün ve hizmet sunarlar. Sahte reklam ve değerlendirme yayınlarlar. Çalıntı logo, .com.au alan adı ve çalıntı Avustralya Ticari İşletme Numarası (ABN) kullanabilirler. Bu tür dolandırıcılıkların tespiti zordur.

Dolandırıcılar ayrıca, bildiğiniz ve güvendiğiniz işletmeler gibi davranıp size sahte faturalar gönderirler. Hatta, yasal faturalar üzerinde değişiklik yaparak sonunda müşterinin size değil de dolandırıcıya para ödemesine neden olurlar.

Romantizm üzerinden dolandırıcılık

Dolandırıcılar, paranızı çalmak için, aşk, randevu ya da arkadaşlık tekliflerinde bulunurlar. Sizi bu ilişkinin gerçek olduğuna inandırmak ve onlara para vermeye ikna etmek için büyük çaba sarf ederler.

Dolandırıcılar sizi sosyal medya, arkadaşlık ya da oyun uygulamaları ve internet sitelerinden bulurlar. Size kısa mesaj veya elektronik posta da gönderebilirler. Sahte profil ve kimliklerin, bazen ünlü kişilerin profillerinin arkasına gizlenirler. Onlara inandığınız anda, hemen 'acil' durum yaratır ve yardımınızı isterler. İstekleri genellikle para ya da başka ürünlerdir.

Tehdit ve haraç dolandırıcılığı

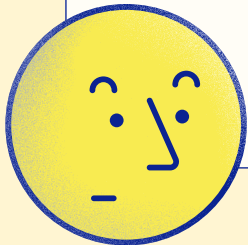
Dolandırıcılar, güvenilir bir kurumun mensubu gibi davranarak, para ödemeniz gerektiğini, aksi takdirde başınıza kötü bir şey geleceğini iddia ederler. Sizi, onlara hemen ödeme yapmadığınız takdirde, tutuklanmak, sınır dışı edilmek hatta fiziksel şiddete uğramakla tehdit ederler.

Para göndermediğiniz takdirde, onlara gönderdiğiniz çıplak resim ve videolarınızı paylaşacaklarına dair şantaj da yapabilirler.

Beklemediğiniz para üzerinden dolandırıcılığı

Dolandırıcılar sizi, alacaklı olduğunuz ya da hakkınız olan, almayı beklemediğiniz para ya da kazandığınız bir ödül olduğuna ikna etmeye uğraşırlar.

Dolandırıcı sizden, para ya da kazandığınız bir şeyi alabilmek için bir ücret ödemenizi ve ya banka hesap ya da kimlik bilgilerinizi vermenizi ister. Maalesef bu gerçek değildir; emeksiz kazanç olmaz.





Dolandırıcılığı nereye bildirmelisiniz?

Biz, Avustralya'yı dolandırıcılar için daha zor bir hedef haline getirmek adına dolandırıcılığın anlaşılması, önlenmesi ve bildirilmesi konusunda herkesi bilinçlendiriyoruz.

Dolandırıcılığı durdurmak ve önlemek için dolandırıcılık raporlarından edindiğimiz bilgileri hükümet, emniyet ve özel sektörle paylaşıyoruz.

Scamwatch'a bildirerek başkalarına yardımcı olun. Scamwatch www.scamwatch.gov.au internet adresindeki bildirim formuyla başınıza gelen dolandırıcılığı bildirin.

Unutmayın, eğer dolandırıcılık mağduruysanız, hemen harekete geçmeniz önemlidir.

- Dolandırıcıya para kaptırdıysanız, bankanız ya da kartınızı veren kuruluşla iletişime geçin.
- 1800 595 160 Numaralı telefondan veya www.idcare.org adresinden IDCARE ile iletişim kurun. 1800 595 160 | idcare.org



Daha fazla yardım ve destek

Dolandırıcılık mağduru olmak son derece üzücüdür. Bunun herkesin başına gelebileceğini ve destek alınabileceğini bilmek önemlidir.

Siz ya da tanıdığınız biri dolandırıldıysa, bunu birisine anlatın. Aile, arkadaş, Aile Doktorunuz ya da aşağıdaki destek hizmetlerinden faydalanabilirsiniz.

Lifeline: 13 11 14 | lifeline.org.au

veya çevrimiçi kriz destek görüşmesi (Günde 24 saat, haftada 7 gün)

Beyond Blue: 1300 22 4636 | beyondblue.org.au

veya çevrimiçi sohbet (Günde 24 saat, haftada 7 gün)

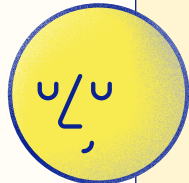
Kids Helpline (Çocuklar için Yardım Hattı): 1800 55 1800 | kidshelpline.com.au

(Günde 24 saat, haftada 7 gün)

Dolandırıcılığın mali durumunuza etkisi çok yıkıcı olabilir.

Mali zorluk yaşıyorsanız, **Ulusal Borç Yardım Hattından** bir danışmanla görüşmek için

1800 007 007 numaralı telefonu, Pazartesi'den Cuma'ya sabah saat 9:30 ile öğleden sonra 4:30 saatleri arasında arayabilir veya Pazartesi'den Cuma'ya sabah saat 9:00 ile akşam 8:00 saatleri arasında Canlı Sohbet yapabilirsiniz.



scamwatch.gov.au