

# Dolandırıcılığa Karşı Korunma

CommBank'te güven ve emniyet bizim için birinci önceliktir. Dolandırıcılar tarafından kendilerine para göndermeleri için baskı yapılan veya kandırılan müşterilerin sayısının giderek arttığını görüyoruz. Bu dolandırıcılık girişimleri oldukça incelikli ve çeşitli şekillerde yapılabiliyor. Gözünüzü dört açmanız ve içinize kurt düşüren bir durum olduğunda bize haber vermeniz önemlidir. Kendinizi dolandırıcılıktan nasıl koruyacağınızı ve dolandırıcılık girişimlerini nasıl bildireceğinizi öğrenmek için lütfen bu adrese bakın: [commbank.com.au/safe](https://commbank.com.au/safe).

## Doğrulama ve Onaylama

- CommBank uygulamasındaki güvenlik kontrolünü tamamlayın.
- Kimliğinizi kanıtlamak için ilave bir kontrol adımı ekleyen çok unsurlu doğrulamayı etkinleştirin.
- Bankadan aradığını iddia eden kişilerin kimliğini doğrulamak için **CallerCheck** (Arayan Kişi Kontrolü) özelliğini kullanın.
- Kendinizi çalışanlarımıza tanıtmak için şubede **CustomerCheck** (Müşteri Kontrolü) özelliğini kullanın.
- İlk kez yapılan ödemelerde hesap bilgileri doğru görünmediğinde, **NameCheck** (İsim Kontrolü) özelliği size uyarı verir.

## Cihaz ve Ödeme Güvenliği

- Antivirüs yazılımını güncellemeyi unutmayın; böylece bilgisayarınızı yaygın tehditlerden koruyabilirsiniz.
- Kartınızı temassız veya temassız olarak okutmak gibi güvenli ödeme yöntemlerini kullanın.
- Dijital cüzdanınıza erişimi olan cihazlarınızı başkalarıyla paylaşmayın.

## Şifre ve Kişisel Bilgiler

- Şifrelerinizi ve PIN numaralarınızı asla paylaşmayın; kişisel bilgilerinizi paylaşırken çok dikkatli olun.
- NetCode'unuzu, CommBank çalışanları da dâhil olmak üzere kimseyle paylaşmayın.
- Şifrenizi NetBank ve CommBank uygulamasından dilediğiniz zaman değiştirebilirsiniz.
- Güçlü şifreler oluşturun ve şifrelerinizi düzenli aralıklarla değiştirin. Şifre oluşturma ipuçlarımızı öğrenmek için [commbank.com.au/password-security](https://commbank.com.au/password-security) adresini ziyaret edin.

## E-posta, SMS ve Çevrim içi

- Şüpheli e-postalar veya SMS'lerdeki bağlantılara tıklamayın.
- Aldığınız bir mesajla ilgili şüpheleriniz varsa, bu mesajı güvendiğiniz biriyle konuşun veya resmî iletişim kanallarından doğrudan ilgili kuruma ulaşın.
- Üçüncü taraflardan aldığınız otomatik, şüphe uyandıran veya tehditkâr aramaları sonlandırın.
- Sosyal medyada ve çevrim içi platformlarda tanımadığınız kişilere karşı dikkatli olun.

## Durun. Kontrol Edin. Reddedin.

**Durun.** Bir anormallik mi fark ettiniz? Emin değilseniz, yapabileceğiniz en iyi şey durmaktır. Bir nefes alın.  
**Kontrol edin.** Güvendiğiniz birine sorun veya resmî iletişim kanallarından doğrudan ilgili kuruma ulaşın.  
**Reddedin.** Görüşmeyi sonlandırın, e-postayı silin, telefon numarasını engelleyin. Şifrelerinizi değiştirin.

Dolandırıcılık mağduru olduğunuzu düşünüyorsanız **13 22 21** numaralı telefondan veya yurt dışındaysanız **+61 2 9999 3283** numaralı telefondan hemen CommBank'e ulaşın.

Ana diliniz İngilizce değilse, devletin sunduğu ücretsiz Sözlü ve Yazılı Çeviri Hizmeti bizimle iletişim kurmanızda yardımcı olabilir. Bu hizmet 150'nin üzerinde dilde verilir. Bu hizmeti bizi aradığınızda veya şubemizi ziyaret ettiğinizde sizin için ayarlayabiliriz.

**Bilmeniz gerekenler:** Size e-posta veya kısa mesaj göndererek NetBank müşteri numaranız, şifreniz veya NetCode'unuz gibi bankacılık bilgilerinizi istemeyiz; e-posta veya kısa mesajdan doğrudan giriş yapmanız için bağlantı göndermeyiz. Bankacılık işlemlerinize güvenle ulaşmak için her zaman tarayıcınıza [commbank.com.au](https://commbank.com.au) adresini yazın veya CommBank uygulamasını kullanın. CommBank'ten aldığınız bir mesaj ya da e-posta şüpheli görünüyorsa, [hoax@cba.com.au](mailto:hoax@cba.com.au) adresine yönlendirin ve silin. Commonwealth Bank of Australia ABN 48 123 123 124 AFSL ve 234945 Avustralya kredi lisansı.



# Sık görülen dolandırıcılık girişimleri hakkında önemli bilgiler



## Yatırım (Kripto dâhil)

Dolandırıcılar, genellikle kripto veya diğer yatırım fırsatlarının aralarında olduğu yüksek getiri vaatleriyle kişileri kandırırlar. Dolandırıcılar size telefonla, e-postayla veya sosyal medya platformlarından ulaşmaya çalışabilir.

### Kendinizi korumanın yolları:

- Gerçek olamayacak kadar iyi görünüyorsa, muhtemelen gerçek değildir.
- Siz istemeden gelen tekliflere ve hızla yatırım yapmanızı veya eyleme geçmenizi gerektiren baskılara karşı temkinli olun.
- Şirketin veya aracının meşruluğunu öncelikle ASIC internet sitesinden doğrulayın.



## Uzaktan Erişim

Dolandırıcıların, güvenilir bir şirket ya da kurumda çalıştıklarını iddia ederek sizi aramaları veya hesap ya da cihazlarınıza erişmeye çalışmaları.

### Kendinizi korumanın yolları:

- Üçüncü tarafların arayarak size baskı yaptıkları veya talepte bulundukları durumlarda asla uzaktan erişim yazılımlarını indirmeyin.
- İlgili kurumu, resmi internet sitesinde bulunan meşru iletişim bilgilerini kullanarak dilediğiniz zaman geri arayabilirsiniz.
- CommBank'te çalıştığını iddia eden biri sizi ararsa, uygulamadaki CallerCheck özelliğiyle aramayı doğrulamamızı bizden her zaman isteyebilirsiniz.

## Ele Geçirilen İş E-posta Adresleri



Dolandırıcılar, ele geçirilen adreslerden veya asistanınız, müşteriniz, avukatınız, müdürünüz ya da tedarikçiniz gibi güvenilir kişilerden gelmiş gibi gösterilen e-posta adreslerinden gelen e-postalarla işletmeleri hedef alabilir.

### Kendinizi korumanın yolları:

- İlk kez ödeme yapmadan veya ödeme bilgilerini değiştirmeden önce, bu bilgileri teyit etmek üzere ilgili kurumu resmî iletişim numarasından arayın.
- Ödeme yaparken, hesap isminin verilen BSB ve hesap numarasıyla eşleşip eşleşmediğini kontrol etmek için NameCheck özelliğini kullanın.
- Çalışanlara, ortalama (phishing) girişimlerini tanımları ve bildirmeleri için eğitim verin.

## E-posta ve Kısa Mesajlarla Ortalama Yöntemiyle Dolandırıcılık



Dolandırıcılar, sizi sahte internet sitelerine yönlendiren veya hassas kişisel bilgilerinizi isteyen bağlantılar içeren aldatıcı kısa mesajlar veya e-postalar kullanır.

### Kendinizi korumanın yolları:

- Şüpheli e-postalar veya SMS'lerdeki bağlantılara tıklamayın.
- Mesajların güvenilirliğini ilgili kuruma resmî iletişim kanallarını kullanarak doğrudan ulaşarak teyit edebilirsiniz.
- CommBank'ten gelen şüpheli mesajları hoax@cba.com.au adresine bildirin.



# Sık görülen dolandırıcılık girişimleri hakkında önemli bilgiler



## İlişkiler

Dolandırıcılar ilişki kurmak üzere sahte profiller oluştururlar ve mağdurlarını para ya da kişisel bilgilerini göndermek üzere yönlendirirler.

### Kendinizi korumanın yolları:

- Güvenmediğiniz kimseye para göndermeyin; bu kimselerle şifrelerinizi, kredi kartı ya da hesap bilgilerinizi asla paylaşmayın.
- İlişki kurmak istediğiniz kişiyi Google veya sosyal medya uygulamalarını kullanarak araştırın. Size gönderilen fotoğrafların sahibinin başka biri olmadığına emin olmak için tersten fotoğraf araması yapın.
- Çevrim içi ilişkinizle ilgili olarak ailenizle ve arkadaşlarınızla konuşun. Onlar size bakış açılarını sunabilir ve sizin fark etmediğiniz tehlike işaretlerini görebilir.

## İstihdam Fırsatları

Yüksek mali getiri karşılığında neredeyse hiç çaba gerektirmeyen veya hızlı para kazandırmayı vaat eden iş teklifleri.

### Kendinizi korumanın yolları:

- Şirketi ve teklifi resmî kanalları kullanarak doğrulayın; şirketin meşru ve halihazırda işlem gören bir şirket olduğundan emin olmak için araştırma yapın.
- Bilmediğiniz şirketler veya tanımadığınız kişilerden sosyal medya, şifreli sohbet, e-posta, telefon veya mektup gibi yollarla gelen iş tekliflerine karşı temkinli olun.
- Meşru şirketler sizden asla avans ödemesi yapmanızı veya şirket fonları ya da işlemleri için kişisel bankacılık bilgilerinizi kullanmanızı istemez.



## Çevrim İçi Alışveriş

Dolandırıcılar, alıcıları sahte veya hiç olmayan ürünleri satın almaları için kandırmak amacıyla çevrim içi mağazalar veya reklamlar oluşturabilir.

### Kendinizi korumanın yolları:

- Yalnızca tanınmış ve güvenli internet sitelerinde alışveriş yapın ve gerçek olamayacak kadar iyi görünen tekliflere karşı temkinli olun.
- Güvenli ödeme yöntemlerini kullanın ve satıcılara doğrudan para transferi yapmaktan kaçının.
- "Sınırlı teklifler" ve satış sonu "geri sayımları"nın baskısı altında kalmayın ve acele etmeyin.

## Tehdit ve Cezalar

Dolandırıcılar, ceza veya dava tehdidinde bulunarak para sızdırmak amacıyla güvenilir kurumlar ve yetkililerin kimliğini takınırlar.

### Kendinizi korumanın yolları:

- Tehdit içeren aramaları sonlandırın ve ilgili kurumla doğrudan iletişime geçin.
- Meşru kurumlar hediye veya mağaza kartları, iTunes kuponları, havale veya Bitcoin gibi alışılmadık yöntemlerle sizden ödeme yapmanızı asla istemezler.
- Güvenliğinizden endişe duyuyorsanız polisin yardım hattını arayın.

