

Deposit to earn rewards



Sign up and deposit to receive up to **17,500 USDT** in bonuses.
Exclusive for new users only.

Get it now

[PDF Database Document] - BTCC Cryptocurrency Exchange

<https://www.btcc.com/tr-TR/academy/crypto-basics/8-types-of-crypto-scams-to-avoid-in-2024-5>

2024'te Kaçınılması Gereken 8 Kripto Dolandırıcılığı Türü



Bir kripto para dolandırıcılığının kurbanı mı oldunuz? Eğer öyleyse, yalnız değilsiniz - kripto kullanıcıları 2023'te dolandırıcılık, halı çekme ve hack'ler nedeniyle \$2 milyara yakın ve 2024'ün ilk yarısında \$1,4 milyardan fazla kaybetti.

Kendinizi korumaya yönelik önemli bir adım, var olan çeşitli kripto para dolandırıcılığı türleri hakkında kapsamlı bir anlayış kazanmaktır. Bunlar, kimlik avı girişimlerinden ayrıntılı Ponzi şemalarına kadar uzanır ve dolandırıcılar, şüphelenmeyen bireyleri sömürmek için sürekli olarak yeni taktikler geliştirir. Tetikte ve bilgili kalarak riskleri önemli ölçüde azaltabilirsiniz. Kapsamlı kılavuzumuz, sekiz yaygın kripto yatırım dolandırıcılığı türünü özetlemektedir. Ayrıntılara

girelim.

- [Kripto Dolandırıcılığı Nedir?](#)
- [En Yaygın Sekiz Kripto Para Dolandırıcılığı Nedir?](#)
- [Kimlik Avı Dolandırıcılığı](#)
- [Romantizm Dolandırıcılığı](#)
- [Kimliğe bürünme ve hediye dolandırıcılığı](#)
- [Kripto Yatırım Dolandırıcılığı](#)
- [Santaj ve Haraç Planları](#)
- [Bulut Madenciliği Şemaları](#)
- [Sahte Kripto Para Borsaları ve Cüzdanları](#)
- [SIM Değiştirme Dolandırıcılığı](#)

Kripto Dolandırıcılığı Nedir?

Özünde, bir kripto para birimi dolandırıcılığı, kripto para birimleri kullanan bir kişiden yasa dışı olarak para, kişisel veri veya dijital varlık elde etmeye yönelik yasa dışı bir girişimdir. Kripto para birimlerinin merkezi olmayan ve genellikle takma adlı doğası, bu tür dolandırıcılık faaliyetlerini kolaylaştırarak çalınan fonların izini sürmeyi ve kurtarmayı zorlaştırır. Ne yazık ki, bir kripto dolandırıcılığında para kaybedildiğinde, onu geri almak genellikle göz korkutucu ve olası olmayan bir iştir.

Dolandırıcılıkların çeşitliliği ve karmaşıklığı kafa karıştırıcı olabilir ve bu da gerçek fırsatları dolandırıcılıklardan ayırt etmeyi zorlaştırabilir. Dolandırıcılar tarafından kullanılan yaygın bir taktik, yatırımcılara minimum riskle veya hiç risk almadan gerçekçi olmayan getiriler vaat etmek ve bireyleri önemli finansal kazançlar beklentisiyle cezbetmektir. Bu dolandırıcılıklar ayrımcılık yapmaz, yalnızca acemileri değil, aynı zamanda deneyimli yatırımcıları ve hatta büyük şirketleri de hedef alır.

En Yaygın Sekiz Kripto Para Dolandırıcılığı Nedir?

Yukarıda belirttiğimiz gibi, kripto kullanıcıları 2023'te dolandırıcılık, halı çekme ve hack'ler nedeniyle \$2 milyara yakın ve 2024'ün ilk yarısında \$1,4 milyardan fazla kaybetti. Dolandırıcılıkların her birini daha derinlemesine inceleyelim, nasıl çalıştıklarını ve bunların kurbanı olmayı nasıl önleyebileceğinizi görelim.

Kimlik Avı Dolandırıcılığı

Kimlik avı dolandırıcılığı, dolandırıcılar tarafından kimliğiniz, şifreleriniz ve kripto para cüzdan anahtarlarınız dahil olmak üzere kişisel bilgilerinizi ifşa etmeniz için sizi kandırmak için sahte web siteleri, sosyal medya profilleri oluşturdukları veya sahte e-postalar gönderdikleri aldatıcı bir taktiktir. Bu dolandırıcılıklar, masum kurbanlara güven aşılama için borsalar gibi meşru kripto para platformlarını kurnazca taklit eder. Aldığınız e-postalar veya mesajlar güvenilir görünebilir ve genellikle özel anahtarınız veya oturum açma kimlik bilgileriniz gibi hassas bilgileriniz için cazip teklifler veya acil talepler içerir.

Bu bilgileri farkında olmadan dolandırıcılara ifşa ettiğinizde, dijital varlıklarınızı çalmak için bu bilgilerden yararlanabilirler. Bu, sağladığınız ayrıntıları kullanarak gerçek platformlardaki kripto para hesaplarınıza erişmeyi ve bunları boşaltmayı içerebilir. Bu nedenle, kişisel veya finansal bilgilerinizi isteyen herhangi bir istenmeyen iletişime karşı dikkatli olmak çok önemlidir, özellikle de gerçek olamayacak kadar iyi anlaşmalar vaat ediyorsa veya bir aciliyet duygusu yaratıyorsa.

Romantizm Dolandırıcılığı

Dikkatli olunması gereken bir başka tehlikeli dolandırıcılık, özellikle kripto romantizm dolandırıcılığı şeklinde duygusal manipölasyonu içerir. Bu şemalarda dolandırıcılar, titizlikle hazırlanmış, genellikle uzun bir ilişki yoluyla güveninizi kazanmak için flört sitelerinde veya popüler sosyal medya platformlarında hayali profiller oluşturur. Haftalar hatta aylar boyunca, sizinle bir bağ kurarlar ve duygusal bağları kendi avantajlarına kullanırlar.

Dolandırıcı güveninizi kazandıktan sonra, bir kripto para birimi planına yatırım yapma fikrini ortaya atacak veya doğrudan bir kripto para birimi transferi talep edecektir. Ancak, vaat edilen yatırım için fonları kullanmak yerine, para derhal kendi ceplerine yönlendirilir. Bu dolandırıcılıklar yoluyla meydana gelen mali kayıplar şaşırtıcı olabilir ve astronomik miktarlara ulaşabilir. AARP'ye göre, Kasım 2023'te ABD Adalet Bakanlığı ve Gizli Servis, 70'ten fazla kurbanı hedef alan dolandırıcılardan 9 milyon dolar değerinde Tether aldı. Büyük bir kısmı romantizm planlarıyla hedef alınmıştı.

Kimliğe bürünme ve hediye dolandırıcılığı

Dolandırıcılar, sahte yatırım fırsatlarını ve sahte eşantyonları teşvik etmek için ünlüleri, etkileyicileri ve saygın şirketleri taklit ederek giderek daha fazla aldatıcı taktikler benimsiyor. İşte bu dolandırıcılıkların nasıl ortaya çıktığına daha yakından bir bakış:

Sahte Ünlü Onayları: Dolandırıcılar sahte sosyal medya profilleri oluşturur veya gerçek, doğrulanmış hesaplara sızar. Sahte kripto para birimi planlarının reklamını yapmak, kazançlı eşantyonlar veya garantili yüksek getiri ile yatırım beklentileri vaat etmek için bu platformlardan yararlanırlar. Kurbanlar, gelecekte önemli bir getiri elde etme bahanesiyle belirli bir adrese kripto para göndermeye ikna edilir.

Sosyal Medya Dolandırıcılıkları: Dolandırıcılar, Facebook ve Instagram gibi platformlarda sahte profiller, sayfalar veya gruplar oluşturur. Daha sonra bu sayfaları sahte yatırım planlarını veya kimlik avı bağlantılarını tanıtmak için kullanacaklar - 2024'te, bazen derin sahte olarak adlandırılan sahte sosyal medya dolandırıcılıkları 25 milyar doları aştı. Dolandırıcılar, kurbanları cezbetmek için sahte referanslar, başarı hikayeleri ve büyük kârların ekran görüntülerini yayınlayarak bunu başarmayı başardılar. Bu gönderilerdeki bağlantılar, kullanıcıları oturum açma kimlik bilgilerini veya özel anahtarları yakalayan bir siteye yönlendirecektir.

Kripto Yatırım Dolandırıcılığı

Dolandırıcılar bazen çok az riskle veya hiç risk almadan yüksek getiri vaat eden cazip kripto yatırım planları tasarlarlar. Genellikle sizi yatırımlarının güvenli ve karlı olduğuna ikna etmenin ayrıntılı yollarını içerirler. En yaygın türler arasında Ponzi şemaları, pompala ve boşalt şemaları ve sahte ICO'lar ve NFT'ler bulunur.

İşte nasıl çalıştıkları:

Ponzi Şemaları

Ponzi şemaları, erken yatırımcılara ödeme yapmak için yeni yatırımcıların fonlarından yararlanarak çalışır ve gelişen bir yatırım fırsatı yanılgısını teşvik eder. Bu strateji, ek yatırımcı akınını cezbeder, ancak yeni yatırımcı havuzu azaldıkça, plan kaçınılmaz olarak patlar ve katılımcıların çoğunluğu için önemli kayıplara neden olur. Bu planlar bugün devam etse de, 2017/2018 kripto para birimi

patlaması sırasında çoğaldı ve öncelikle yüksek getirili yatırım programları (HYIP'ler) olarak kendini gösterdi.

Pompa ve Boşaltma Şemaları

Pompala ve boşalt planları, dolandırıcıların aldatıcı iddialar yoluyla bir kripto para biriminin fiyatını yapay olarak şişirmesini içerir. Önemli miktarda düşük fiyatlı, düşük hacimli bir kripto para birimi biriktirirler ve ardından sosyal medya ve diğer pazarlama kanallarında agresif bir tanıtım kampanyası başlatırlar. Bu strateji, şüphelenmeyen yatırımcıları cezbederek kripto para biriminin değerini daha da artırır. Dalgalanmanın zirvesinde, dolandırıcı varlıklarını tasfiye ederek dramatik bir fiyat çöküşünü tetikler ve diğer yatırımcıları değer kaybetmiş veya değersiz varlıklarla baş başa bırakır.

ICO ve NFT Dolandırıcılığı

İlk Para Teklifleri (ICO'lar) ve Değiştirilemez Token'lar (NFT'ler), projeler için meşru bağış toplama yolları olarak hizmet eder. Bununla birlikte, dolandırıcılar, vaat edilen devrim niteliğindeki teknolojiler veya özel dijital varlıklar gibi hayali girişimler için fon talep ederek bu mekanizmalardan sıklıkla yararlanır. Yatırımcıları sahte promosyon malzemeleriyle cezbederler, ancak yeterli fon biriktirdiklerinde aniden ortadan kaybolurlar ve yatırımcıları boş vaatler ve mali kayıplarla baş başa bırakırlar.

Şantaj ve Haraç Planları

Bu şemaların çalışma şekli, değişim aracı olarak kripto para birimi olmasına rağmen, geleneksel parasal dolandırıcılıkların işleyişini yansıtır. Kripto dolandırıcıları, kurbanları kripto para birimi ödemeleri yapmaya zorlamak için kişisel fotoğraflar, videolar veya finansal kayıtlar gibi hassas bilgilere sahip olduklarından yararlanarak şantaj veya şantaj taktikleri kullanır. Mağdurlar, bu hassas verilerin, genellikle yaklaşan bir son tarih tehdidi altında ifşa edilmesi durumunda ortaya çıkacak sonuçlardan korktukları için boyun eğerler. Böylece dolandırıcılar, korkmuş kurbanlarından kripto para biriminde ödeme almayı başarır.

Bulut Madenciliği Şemaları

Bu dolandırıcılıkların kurbanları, kripto madenciliği müteahhitleri gibi davranan sahte şirketler tarafından kullanılan aldatıcı taktiklerin kurbanı oluyor. Bu sözleşmeler, maliyetli ekipmanlara sahip olmayı gerektirmeden kripto para madenciliğinden elde edilen kar vaatleriyle ikna eder. Ancak gerçek şu ki, bu şirketler, ne madencilik ekipmanına ne de yatırımcılara vaat ettikleri getirileri yerine getirmek için finansal araçlara sahip olmayan dolandırıcılar tarafından kurulan paravanlardır. Bazı durumlarda, bu madencilik dolandırıcılıkları başlangıçta, ilk yatırımcılara yeni yatırımcılardan sağlanan fonlar kullanılarak ödeme yapılan ve dolandırıcılık döngüsünü daha da sürdüren Ponzi şemaları olarak işlev görür.

Sahte Kripto Para Borsaları ve Cüzdanları

Dolandırıcılar, para çalmak için meşru platformları taklit eden sahte kripto para borsaları ve cüzdanları tasarlayarak onları şüphelenmeyen gözle neredeyse ayırt edilemez hale getirir. Bu sahte siteler, düşük ücretler, gelişmiş güvenlik ve özel işlevler dahil olmak üzere çekici tekliflerle kurbanları cezbeder. Ancak, kurbanlar hesap oluşturup paralarını yatırdıktan sonra, dolandırıcılar çalınan parayla hızla kaçır ve kurbanları eli boş bırakır.

Bu yılın Mayıs ayında, İngiltere'de iki adam kurbanlardan yaklaşık 6 milyon sterlin değerinde kripto para çaldı. Kurbanların çevrimiçi cüzdanlarına erişebilmek için Blockchain.com web sitesini kopyaladılar.

SIM Deęiřtirme Dolandırıcılığı

Bu kripto dolandırıcılığı taktikleri son derece karmaşıktır ve kurbanların cep telefonu numaralarını kripto cüzdanları da dahil olmak üzere çevrimiçi hesaplarına bir ağ geçidi olarak kullanır. Dolandırıcılar, doğrulama kodlarını ele geçirmek ve hatta şifreleri sıfırlamak için bu bilgilerden yararlanır ve böylece dijital varlıklara doğrudan erişim elde eder. Sosyal medya profilleri, veri ihlalleri veya kimlik avı e-postaları gibi çeşitli yollarla cep telefonu numaraları alabilirler. Dolandırıcılar genellikle cep telefonu numaranızı sosyal medya, veri ihlalleri veya kimlik avı e-postası yoluyla öğrenebilir. Bu bilgilerle, bir dolandırıcı daha sonra mobil sağlayıcınızla iletişime geçebilir ve mesajlarınızı bu şekilde okuyabilecek ve kripto borsanızda veya cüzdanınızda kurduğunuz iki faktörlü kimlik doğrulamayı atlayabilecekleri bir SIM takası isteyebilir.