Como evitar golpes e roubo de sua criptomoeda?

Guides O mercado de criptomoedas está crescendo e, com ele, surgem novos esquemas para roubar moedas e dados do usuário. Criptografar carteiras, trocas falsas, vírus, e-mails de phishing e muito mais aconteceram na comunidade de criptografia mais de uma vez. Não apenas as bolsas mundialmente famosas e os grandes detentores de criptomoedas sofrem, mas também os usuários comuns.

Neste artigo, daremos uma olhada nos tipos mais comuns de golpes de criptomoeda e daremos algumas dicas sobre como proteger suas moedas.

Tipos Comuns de Golpes

- Phishing
- Blackmail
- Falsos sorteios
- Falsas Exchanges
- Apps falsos
- Pirâmide
- Tokens falsos
- Malware

1. Phishing

Phishing é um golpe para obter informações de identificação do usuário, como frases mnemônicas, chaves privadas e credenciais de login da conta. Tanto usuários comuns quanto grandes empresas se tornaram repetidamente vítimas de phishing.

O fraudador se faz passar por uma pessoa ou empresa conhecida na comunidade de criptografia, envia e-mails, cria sites falsos ou contas de mídia social.

Por exemplo, no final de 2020, os usuários da carteira Ledger receberam cartas informando que os servidores estavam infectados com malware e que havia risco de roubo de criptomoeda. Para evitar isso, sugeriu-se seguir o link e baixar a atualização de segurança. Usuários desatentos baixaram a atualização de uma versão falsa do site do Ledger e os golpistas receberam seus fundos.

Cuidado com mensagens e e-mails suspeitos que podem conter links ou anexos perigosos. Verifique se há erros ortográficos ou caracteres extras em seus URLs. Em caso de dúvida sobre o remetente da carta, entre em contato com a empresa diretamente através dos dados de contato fornecidos em fonte confiável.

Mesmo que o e-mail tenha sido enviado de um endereço real, ele ainda pode ser fraudulento. Certifique-se de verificar o URL antes de inserir seus nomes de usuário e senhas.

Não siga links recebidos de remetentes desconhecidos.

Para evitar ser vítima de phishing nas redes sociais, verifique se a pessoa é quem diz ser. Algumas redes sociais possuem indicadores de autenticidade.

Proteja suas informações confidenciais, não dê a ninguém suas chaves privadas, logins e senhas.

1. Blackmail

Talvez este seja um dos métodos mais comuns de extorsão de criptomoeda. O fraudador ameaça a vítima divulgando informações confidenciais sobre ela que teoricamente poderiam ser verdadeiras. Por exemplo, um invasor afirma ter evidências de trapaça ou visualização de conteúdo proibido. A propósito, os golpistas nem sempre possuem informações importantes sobre suas vítimas. Eles costumam fingir.

Entre os golpistas, existem indivíduos especialmente criativos. Então, em 2018, vários internautas receberam cartas de advertência. O atacante alegou que alguém as mandou para o assassino, mas se os usuários enviarem moedas BTC para o endereço especificado, a ordem para o assassino será cancelada.

Se você receber esse e-mail, a melhor solução em tal situação é ignorá-lo e não enviar a criptomoeda para o golpista. Os invasores enviam um grande número de cartas todos os dias e, provavelmente, eles não têm informações sobre você, e seu e-mail está simplesmente na lista de correspondência deles.

Se você sentir uma ameaça real do remetente da carta, entre em contato com a polícia local. Você não deve entrar em diálogo e muito menos enviar moedas para o extorsionário. Essas ações podem levar a consequências negativas.

1. Falsos sorteios

Fraudadores, usando nomes famosos na comunidade de criptomoeda para maior persuasão, criam contas em redes sociais e em muitos sites, compram canais do YouTube, oferecendo uma pechincha "me mande moedas e eu vou devolver você 10 vezes mais". O usuário envia suas moedas, mas não recebe nada em troca.

Não participe da distribuição de criptomoeda se, de acordo com seus termos, for necessário enviar moedas para o endereço do organizador. Os organizadores de brindes de feiras não exigem o envio de fundos.

1. Falsas Exchanges

Esses serviços atraem clientes com comissões muito baixas, distribuição gratuita de moedas ou presentes. Freqüentemente, eles atraem com uma taxa muito favorável, oferecendo arbitragem entre as trocas. Os usuários usam um serviço falso, mas quando tentam sacar uma quantia significativa, enfrentam um bloqueio por motivos inexistentes. Essas trocas podem existir por muito tempo e não chamar a atenção, imitando a realidade de uma troca real.

Tenha cuidado com suas credenciais e os sites que você visita. Forneça informações sobre você com cuidado.

Use endereços de e-mail e senhas diferentes ao se registrar. É extremamente perigoso usar o mesmo endereço e a mesma senha, pois se uma conta for hackeada, os invasores poderão obter acesso às suas outras contas.

Marque a URL da troca real ou trocador que você está usando. Sempre verifique o link antes de entrar.

1. Apps falsos

Também houve casos em que os invasores criaram cópias de aplicativos existentes ou aplicativos falsos para plataformas que não tinham versões para celular ou desktop. Por exemplo, em 2017, o aplicativo de troca Poloniex apareceu. Os usuários o instalaram fornecendo seus dados pessoais a golpistas.

Antes de baixar o aplicativo, verifique as informações sobre o desenvolvedor, a quantidade de downloads, leia as análises e comentários.

1. Pirâmide

O esquema clássico de pirâmide tem um esquema muito simples. Por exemplo, o serviço promete retorno de 10% do investimento até o final do mês. Você investiu $100 no projeto. Nesse período, o investidor busca um novo cliente que também investe $100. Depois de receber dinheiro de um novo investidor, o organizador pode pagar a você $110 no final do mês. Para pagar o segundo investidor, o organizador encontra novos clientes. Os investidores obtêm lucro apenas se novas pessoas vierem ao projeto e investirem dinheiro.

As pirâmides apresentam uma série de características em comum: garantem uma alta renda sem risco, solicitam persistentemente a captação de novos clientes, o site não possui informações de contato e evidências documentais de investimentos. Se o projeto tiver esses recursos, provavelmente é fraudulento.

Antes de investir em um projeto desconhecido, tente encontrar o máximo de informações possível sobre ele. Não tenha pressa e não se deixe levar pelas crenças sobre lucro fácil, estude as avaliações de usuários reais.

1. Tokens falsos

Recentemente, finanças descentralizadas (DeFi) se tornaram muito populares. Isso atraiu muitos golpistas. Os invasores criam tokens DeFi falsos e os adicionam a sites descentralizados. Os tokens falsos têm os mesmos nomes e códigos dos tokens originais.

Como resultado, uma bolsa pode ter uma criptomoeda real e suas cópias. Se você comprar um token falso, os fundos irão para golpistas e você ficará com uma moeda, cujo preço provavelmente é igual a zero.

Procure o token não pelo nome, mas pelo endereço do contrato inteligente. Você pode encontrar o endereço original no site do projeto ou por meio de agregadores de criptomoedas. Por exemplo, Coinmarketcap e Coingecko.

Analise as informações do contrato inteligente de token no etherscan, bscscan e polygonscan. Preste atenção à liquidez e ao número de transações.

1. Malware

O vírus copy-and-paste permite que fraudadores interceptem dados da área de transferência. Se você tiver esse tipo de vírus em seu dispositivo, quando você copiar e colar o endereço da área de transferência, ele será automaticamente substituído pelo endereço do fraudador.

Também existem vírus ransomware que podem bloquear o acesso a dados importantes no dispositivo, ameaçando excluí-lo. Para desbloquear, a vítima deve enviar criptomoeda.

Certifique-se de verificar o endereço do destinatário antes de enviar moedas. Caso contrário, se o seu dispositivo tiver o vírus copy-and-paste, você poderá perder seus fundos.

Configure backups regulares. Se você encontrar um vírus ransomware, ele o ajudará a recuperar seus arquivos.

Se você suspeitar que há um vírus em seu dispositivo, faça uma varredura com um antivírus.

Cobrimos os tipos mais populares de golpes que usuários iniciantes e experientes de criptomoeda podem enfrentar. Esperamos que o conhecimento desses métodos o ajude a proteger seus fundos contra perdas.