FRAUDES E BURLAS COM CRIPTOATIVOS

MANTENHA-SE ALERTA E PROTEJA-SE

O rápido crescimento dos criptoativos e as suas características específicas – acessibilidade global, velocidade, anonimato e, muitas vezes, irreversibilidade das transações – tornam-no um alvo privilegiado para os cibercriminosos. Os autores de fraudes e burlas utilizam táticas sofisticadas para o enganar, tais como os esquemas de pirâmide financeira, "Esquemas Ponzi", oportunidades de investimento falsas, ofertas gratuitas nas redes sociais e mensagens fraudulentas. Também recorrem a esquemas de burlas românticas ou endereços semelhantes aos verdadeiros para comprometer a sua carteira. Frequentemente, contactam-no através de redes sociais, *e-mail*, chamadas telefónicas inesperadas e aplicações de mensagens que parecem legítimas. Pode enfrentar riscos como perdas financeiras, roubo de identidade e danos emocionais.

Seja cauteloso e siga estas dicas importantes para se manter seguro.

Mantenha-se alerta para possíveis fraudes e burlas com criptoativos:
saiba mais sobre os diferentes tipos de fraudes e burlas (ver páginas 5, 6, 7 e 8).

Identifique sinais de alerta:
aprenda a reconhecer comportamentos, mensagens ou ofertas suspeitas (ver página 2).

Proteja-se e proteja os seus ativos:
proteja os seus dados pessoais (ver página 3).

Saiba o que fazer se for vítima de fraude ou burla
(ver página 4).

Sinais de alerta

Uma promessa que parece demasiado boa para ser verdade.

Uma oferta não solicitada.

Garantia de rápido e elevado retorno.

Urgência na ação (por exemplo, ofertas por tempo limitado que o pressionam a agir de forma imediata).

Um pedido de pagamento através de métodos não rastreáveis (por exemplo, criptoativos, cartões-presente, transferências eletrónicas ou cartões de débito pré-pagos).

Um convite para clicar num *link*, ler um *QR code* ou descarregar uma aplicação.

Um pedido para enviar ou partilhar chaves privadas e frases de recuperação ("seed phrases"), isto é, a lista de palavras para aceder e recuperar a sua carteira de criptoativos.

Um *URL* suspeito ou incorrecto.

Um logótipo com ligeiras distorções, um sítio da internet que replica o aspeto do verdadeiro sítio da internet da empresa, ou que parece profissional, mas que não possui informações de contacto credíveis, dados de registo da empresa, histórico ou presença verificável.

Uma plataforma de negociação desconhecida.

Um anexo suspeito, especialmente .exe, .scr, .zip ou ficheiro Office com uma macro ativada (.docm, .xlsm).

Passos para se proteger:

1 **Pare e pense antes de agir:**

Não se precipite em investir, partilhar informações ou clicar em *links* - os autores de burlas criam deliberadamente um sentimento de urgência. Em caso de dúvida, mesmo que pequena, não avance nem invista, sem antes verificar a fonte de informação.

2 **Verifique cuidadosamente a fonte de informação:**

- Verifique sempre a origem das mensagens, chamadas, *e-mails* e *links*, mesmo que pareçam oficiais, pareçam vir de um amigo ou famíliar, ou mesmo de uma figura pública. Fique atento a erros ortográficos, *URLs* estranhos ou indicadores de segurança em falta, por exemplo, verifique se o *link* do sítio da internet inclui um "s" em "HTTPS" para se certificar que o sítio da internet é seguro e verifique se existem letras adicionadas ou em falta no nome da empresa.
- Não abra *links* de mensagens não solicitadas, instale apenas aplicações oficiais através de lojas de aplicações fiáveis e não leia *QR codes* desconhecidos.
- Mesmo que uma oferta pareça legítima, confirme sempre o sítio da internet da empresa ou verifique se a conta nas redes sociais tem a identidade verificada (por exemplo, com marcas de verificação oficiais).
- Utilize os dados de contacto verificados para contactar diretamente a empresa/pessoa e nunca confie nas informações de contacto fornecidas pelo suspeito de fraude (por exemplo, pesquise o nome da empresa de forma independente ou utilize diretórios de negócios verificados). Os autores de burlas podem alegar estar autorizados ou replicar o sítio da internet de uma empresa autorizada. Pode verificar se o prestador de serviços de criptoativos está autorizado na União Europeia (UE) consultando o registo da ESMA (). Pode também consultar a lista I-SCAN da IOSCO (iosco.org/i-scan/).

3 **Nunca partilhe palavras-passe, chaves privadas ou frases de recuperação (“*seed phrases*”):**

Qualquer pessoa com acesso a estas informações pode assumir o controlo dos seus ativos. As empresas legítimas nunca pedirão as suas palavras-passe ou códigos de segurança por *e-mail*, mensagem ou chamada.

4 **Mantenha os dispositivos e as chaves privadas seguros:**

Utilize palavras-passe fortes e únicas para cada uma das suas contas de criptoativos, mantenha-as em segredo e evite reutilizar as mesmas credenciais em diferentes plataformas. Ative a autenticação multifator sempre que possível. Consulte algumas dicas sobre palavras-passe aqui (). Mantenha o seu *software* e protecção antivírus atualizados e ativados.

5 **Tenha cuidado com ofertas de investimento inesperadas:**

Desconfie de investimentos que prometem elevados retornos. Se parece demasiado bom para ser verdade, provavelmente é uma fraude.

6 **Pense antes de partilhar informações nas redes sociais:**

Os grupos de *chat*, fóruns, publicações nas redes sociais e fotografias podem ser valiosas fontes de conhecimento para os autores de fraudes. Revelar demasiado sobre si ou sobre os seus investimentos pode torná-lo um alvo fácil.

O que fazer se for vítima de fraude ou burla

Pare imediatamente as transações:

Para bloquear quaisquer outras transferências para contas suspeitas e evitar perdas adicionais. Interrompa todos os contactos com os autores da burla – ignore as suas chamadas, *e-mails* e bloqueie o remetente.

Altere as suas palavras-passe em todos os seus dispositivos, aplicações e sítios da internet:

Os autores das fraudes compram palavras-passe divulgadas *online* e experimentam-nas em várias contas. Alterar apenas uma palavra-passe não é suficiente. Certifique-se de que altera todas, para impedir que os autores das fraudes as reutilizem.

Desconecte e cancele os acessos:

Cancele permissões suspeitas nos seus contratos digitais, que são executadas automaticamente na *blockchain*, para impedir que os autores das burlas gastem os seus *tokens* sem consentimento. Muitas carteiras e exploradores de *blockchain* oferecem ferramentas que lhe permitem verificar quais os contratos inteligentes que atualmente têm permissão para gastar os seus *tokens*. Para o fazer, pode:

- Utilizar um "verificador de permissões" de confiança, que confirma se um utilizador ou um endereço de *blockchain* está autorizado a executar uma operação;
- Rever a lista de aprovações, e
- Utilizar o botão "cancelar" diretamente da plataforma.

Transfira os seus fundos:

Se a sua carteira digital for comprometida, transfira imediatamente os restantes ativos para uma nova carteira segura.

Contacte o seu prestador de serviços de criptoativos:

Informe o seu prestador de serviços de criptoativos o mais rapidamente possível, utilizando os canais de contacto oficiais, para explorar opções disponíveis. Mesmo que, na maioria dos casos, não seja possível reverter a transação na *blockchain*, o prestador ainda pode congelar a conta do autor da fraude (se ainda estiver na plataforma dele) e colocar o endereço da carteira na lista negra.

Denuncie e alerte:

Denuncie o incidente à polícia ou à sua autoridade nacional de supervisão financeira e informe a sua rede de contactos (por exemplo, amigos e familiares) para aumentar a consciencialização. Estas ações são a melhor maneira de se proteger a si e aos outros.

Cuidado com a fraude de "recuperação de fundos perdidos":

O autor da fraude pode voltar a contactá-lo como vítima de uma fraude anterior, alegando ser uma autoridade pública (por exemplo, polícia, autoridade fiscal ou financeira, etc.) e oferecendo-se para recuperar o seu dinheiro perdido, mediante o pagamento de uma taxa. Muitas vezes, trata-se de mais uma tentativa para o enganar. Lembre-se: ser enganado uma vez não o impede de ser novamente enganado.

Consulte o aviso conjunto das Autoridades Europeias de Supervisão para saber mais sobre os riscos relacionados com os criptoativos (↖) e a ficha informativa «Uma explicação sobre criptoativos: o que o Regulamento MiCA significa para os consumidores?» (↖).

Autoridade Bancária Europeia, Autoridade Europeia dos Seguros e Pensões Complementares de Reforma, Autoridade Europeia dos Valores Mobiliários e dos Mercados, 2025

Luxemburgo: Serviço das Publicações da União Europeia, 2025

PDF ISBN 978-92-9407-219-1 doi:10.2853/6183955 DZ-01-25-107-PT-N

TIPOS DE FRAUDES COM CRIPTOATIVOS

Esquema "Pump-and-dump" ou "Rug pull"

Vê um anúncio nas redes sociais ou num sítio da internet que promove uma "oportunidade de investimento de tempo limitado" em criptoativos, recomendando o investimento num novo *token* ou projeto de criptoativos. Depois de manifestar o seu interesse, é contactado e redirecionado para uma plataforma de negociação de criptoativos ou para um canal de mensagens (por exemplo, *Telegram*, *Viber* ou *WhatsApp*). Um contacto aparentemente credível promete lucros rápidos ou retornos elevados se investir rapidamente. É incentivado a investir uma pequena quantia e, posteriormente, pressionado a investir mais.

O que pode acontecer:

Descobre que o token em que investiu é inútil e o contacto com o qual interagia deixa de responder. Quando tenta levantar o seu dinheiro, o síto da internet já não existe e a empresa está incontactável. Os autores da burla inflacionaram artificialmente ou exageraram o valor de um criptoativo de baixo valor para aumentar o seu preço ("pump") e, em seguida, venderam os seus ativos ("dump"), provocando uma queda abrupta do seu valor e deixando os investidores com prejuízo. Em alternativa, podem encerrar o projeto e desaparecer com os fundos ("rug pull").

Esquemas de impersonação (falsificação de identidade)

Depois de publicar uma pergunta nas redes sociais ou num sítio da internet sobre um problema com a sua carteira de criptoativos, recebe uma mensagem inesperada ou um *e-mail* de alguém que se faz passar por um contacto de confiança (por exemplo, uma plataforma de negociação de criptoativos, um fornecedor de carteiras, suporte informático ou mesmo um amigo). A pessoa pede-lhe a sua frase de recuperação ("*seed phrases*"), palavras-passe ou chaves privadas (um código criptográfico gerado automaticamente que prova a propriedade dos ativos digitais).

O que pode acontecer:

Depois de partilhar a sua frase de recuperação, palavras-passe ou chaves privadas, o autor da burla usa-as para se apoderar dos seus criptoativos ou outros fundos. Lembre-se que a perda de chaves privadas resulta na perda permanente e irreversível do acesso e da propriedade dos seus criptoativos. Ao contrário das transações bancárias, no caso de transferências de criptoativos, uma vez que os seus fundos desaparecem, a recuperação é quase impossível.

Phishing

Recebe uma mensagem inesperada através de *e-mail*, telefone, *pop-up* ou redes sociais, alegando ser de um conhecido prestador de serviços de criptoativos. A mensagem convida-o a iniciar sessão ou a descarregar uma nova aplicação. Também pode receber um *e-mail* que parece ser da sua aplicação da carteira de criptoativos, sugerindo-lhe que clique num *link* fornecido por uma fonte não oficial ou que atualize a sua aplicação, com o objetivo de resolver um problema de segurança.

O que pode acontecer:

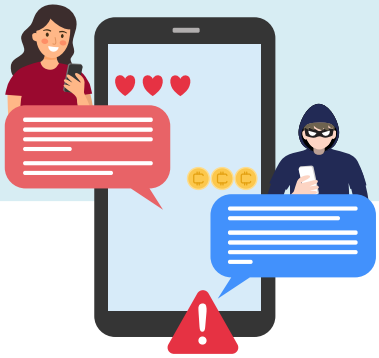
Ao clicar no link, descarregar a aplicação ou ler um QR code, instala um malware que permite ao autor da burla aceder e utilizar as suas informações para roubar os seus criptoativos ou os seus fundos.

Burla através de sorteios ("giveaway")

Depara-se com um anúncio nas redes sociais que alega que as empresas estão a oferecer criptoativos após um pequeno investimento em criptoativos. O anúncio inclui um vídeo ou uma publicação com fotografias de uma celebridade ou de uma marca – geralmente falsas ou obtidas sem autorização – que prometem "duplicar o valor dos seus criptoativos", se enviar primeiro os seus fundos. O logótipo, o *layout*, os depoimentos e a linguagem utilizada parecem profissionais e oficiais, assim como o sítio da internet para o qual é redirecionado.

O que pode acontecer:

Depois de enviar os seus criptoativos, não recebe nada em troca, perdendo todo o dinheiro aplicado. O sorteio era falso e a publicação ou a transmissão ao vivo que personificava celebridades ou empresas foi criada para o enganar.



Burlas românticas

Foi contactado nas redes sociais, aplicações de encontros ou por telefone/mensagem por alguém que não conhece. Essa pessoa procura ter conversas frequentes, pessoais e românticas, criando confiança através de perfis falsos. Gradualmente, direciona a conversa para oportunidades financeiras, alegando lucros elevados com investimentos em criptoativos e incentivando-o a investir com promessas de altos retornos e baixos riscos. Orientam-no para criar uma conta e fazer um pequeno depósito inicial para tornar o esquema credível.

Os autores da burla criam perfis *online* falsos e usam imagens roubadas ou geradas por inteligência artificial para se aproximarem de si.

O que pode acontecer:

O autor da burla retira o máximo de dinheiro possível e depois termina toda a comunicação e desaparece. O sítio da internet ou a aplicação de investimento fraudulento são desativados, deixando-o sem acesso aos supostos investimentos. Em alguns casos, os autores das burlas podem utilizar as informações obtidas durante a burla para visar os seus amigos e familiares e roubar a sua identidade, o que pode trazer-lhe consequências financeiras ou legais (por exemplo, o autor da fraude pode registar carteiras roubadas em seu nome, tornando-o responsável, até prova em contrário, por dívidas ou crimes cometidos em seu nome).

Esquemas de pirâmide financeira "Esquema de Ponzi"

É convidado a participar num projeto que promete retornos elevados e consistentes a partir de investimentos em criptoativos, muitas vezes sustentados por testemunhos ou histórias de sucesso falsas. O esquema pode ser apresentado como uma oportunidade de *marketing* multinível, na qual ganha recompensas não só a partir do seu próprio investimento, mas também por recrutar outras pessoas. Os primeiros investidores aparentam receber pagamentos, incentivando mais pessoas a aderir e a promover o esquema.

Na realidade, não há qualquer negócio genuíno ou lucro a ser gerado. Em vez disso, o dinheiro provém exclusivamente da contribuição de novos investidores, que é utilizada para pagar retornos aos organizadores do esquema e aos primeiros participantes.

O que pode acontecer:

Quando os novos investimentos diminuem, o esquema entra em colapso e, tal como a maioria dos participantes, perde o seu dinheiro. Os organizadores desaparecem, sem que exista qualquer possibilidade de recuperar os fundos. A estrutura multinível ajuda a fraude a aumentar rapidamente, à medida que as vítimas, sem saber, se tornam promotores.

Um endereço semelhante ao verdadeiro que compromete a sua carteira

Após realizar uma transação de criptoativos, repara que aparece um novo endereço no histórico da sua carteira. Este endereço é semelhante a um com o qual interagiu anteriormente. Os autores da burla podem fazer com que apareçam endereços de carteira falsos no seu histórico de transações, através do envio para a sua carteira de uma pequena quantidade de criptoativos de um endereço semelhante. O endereço falso criado pelo autor da burla, acaba por ficar guardado na atividade recente ou nas sugestões automáticas da sua carteira.
Os autores das burlas criam, deliberadamente, endereços parecidos com os legítimos ao alterar apenas alguns caracteres, muitas vezes no meio do endereço, para evitar a sua deteção.

O que pode acontecer:

Quando tenta enviar criptoativos e copia o endereço errado do histórico da sua carteira, envia, sem saber, fundos para a carteira do autor da burla. Como as transações de criptoativos são muitas vezes irreversíveis, os seus fundos perdem-se, na maioria dos casos, de forma permanente. Esta burla baseia-se na ilusão de ótica e no erro humano, explorando o hábito de copiar e colar endereços de carteira sem os verificar cuidadosamente.