///AXUR

EBOOK

As carteiras (*wallets*) como identidades na Web3

Saiba o que são, como funcionam,
e como mantê-las seguras

Sumário

Introdução

Você já deve ter ouvido falar das carteiras digitais usadas para interagir com aplicações da blockchain. Talvez você até já tenha usado uma dessas carteiras para fazer transações, conectar com serviços, marketplaces, etc. Mas você sabe como elas funcionam, e que tipos de carteiras existem? Sabe o que são chaves privadas e frases-semente, e por que é fundamental mantê-las seguras para proteger seus ativos e sua identidade na Web3? Conhece os tipos de golpes mais comuns que afetam usuários de carteiras, e como se proteger desses golpes?

Este artigo responde essas perguntas, com o objetivo de educar usuários sobre um dos aspectos mais importantes da infraestrutura de acesso à Web3, mas que muitas vezes não recebe a devida atenção.

Jônadas Techio
jonadas@axur.com | @Web3Axur
Blockchain Solutions Architect & Web3 Evangelist at Axur

Carteiras ou chaveiros?

No contexto da blockchain e da Web3, uma “carteira” é essencialmente um ***sistema de gerenciamento de chaves criptográficas*** que também serve como ***interface de usuário*** permitindo que você interaja com os aplicativos e serviços da rede, lendo e/ou modificando o estado da blockchain. É nesse sentido, portanto, que usaremos o termo “carteira” daqui por diante.

Embora o uso do termo já esteja difundido, ele é um tanto enganoso, e vale a pena desfazer um mal-entendido comum imediatamente. Ao contrário do que muitas pessoas pensam, quando você faz uma transação na blockchain você ***não está*** “enviando” tokens de sua carteira para a carteira de outra pessoa. Na verdade, você está usando sua chave privada para assinar uma transação e transmiti-la para toda a rede blockchain. Somente após a rede validar sua transação ela será executada, e então essa mudança será refletida nos saldos atualizados do seu endereço e do endereço do destinatário.

Nesse sentido, o termo “carteira” é enganoso justamente

por que as carteiras digitais usadas para interagir com a blockchain ***não armazenam dinheiro*** da mesma forma que as carteiras físicas o fazem. Em vez disso, elas armazenam as chaves privadas que permitem que você assine e faça transações, e as chaves públicas que permitem que você receba ativos. Uma analogia mais adequada seria, portanto, com um ***chaveiro***, com a diferença importante de que, no caso da blockchain, esse "chaveiro" não apenas gerencia as chaves necessárias para interagir com a rede, mas também mostra o registro das transações e os saldos dos endereços associados a essas chaves.

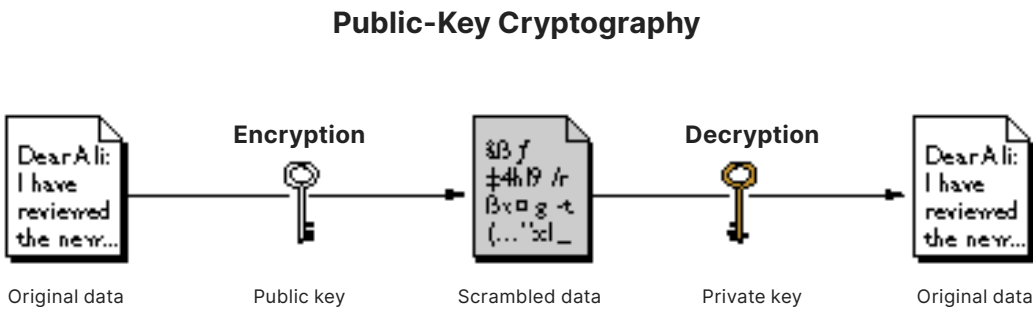
Mas o que são exatamente essas "chaves" que as arteiras gerenciam, e para que elas servem?

Chaves e frases-semente

Uma "chave", no sentido em que o termo é usado em criptografia, é a base de uma transformação, geralmente matemática, de uma mensagem comum em uma mensagem ilegível (criptografada).

Na criptografia de chave pública, que é o padrão usado para a implementação das blockchains, um par de chaves correlacionadas é criado para essa finalidade: a primeira é chamada privada, pois deve ser mantida secreta; a segunda é chamada **pública**, pois pode ser compartilhada com qualquer pessoa que deseje recebê-la. Qualquer participante que tenha acesso à sua chave pública pode criptografar uma mensagem usando essa chave, mas somente você poderá lê-la, usando sua chave privada. Além disso, você pode usar sua chave privada para "assinar digitalmente" uma mensagem, permitindo que outras pessoas verifiquem que você foi o emissor ou emissora; essa verificação também é feita usando sua chave pública.

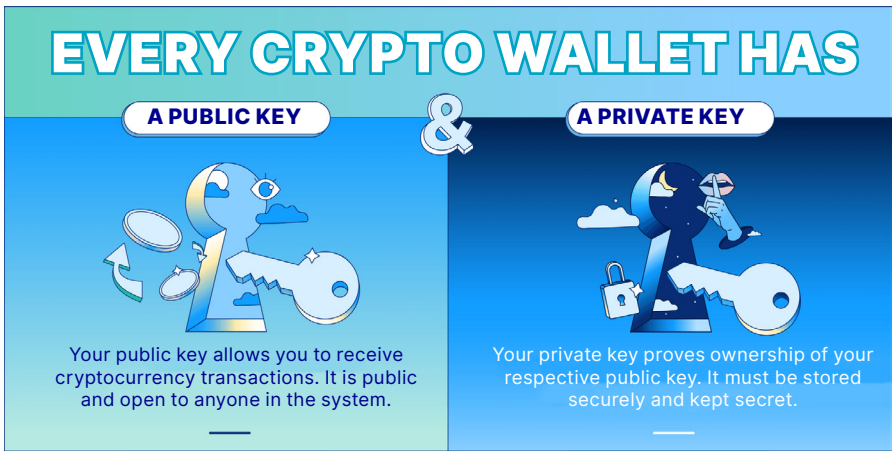
Uma carteira armazena e permite gerenciar esse par de chaves para interagir com uma blockchain.



Fonte: Network Encyclopedia

- Uma **chave pública** remete a um endereço que permite que você envie e receba transações.
- Uma **chave privada** prova que você é proprietário dos bens associados ao seu endereço.

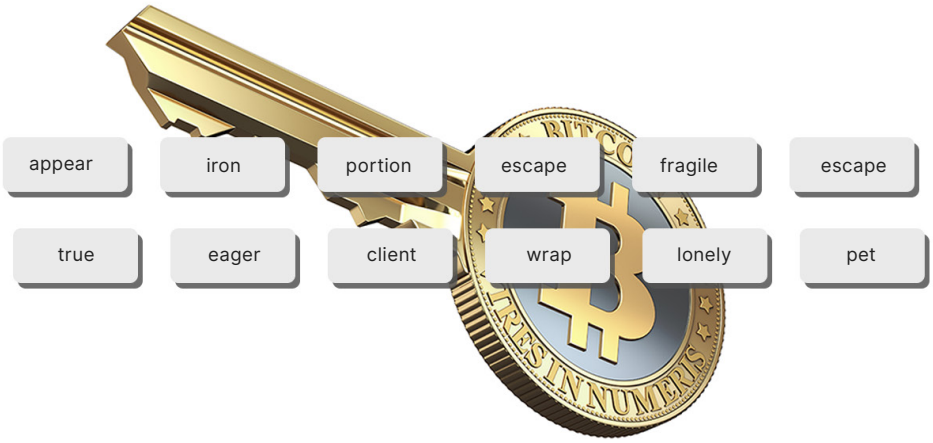
Você pode pensar em sua chave pública como análoga ao número de sua conta bancária, e em sua chave privada como análoga à senha que você usa para acessar sua conta e fazer transações. Assim como no caso do banco, sua chave pública pode ser compartilhada com qualquer pessoa para receber fundos, mas sua chave privada, como sua senha, deve ser mantida em segredo.



Fonte: Crypto.com

A maioria das implementações modernas de carteiras usa uma única chave mestra, também conhecida como frase-semente (*seed-phrase*), para gerar as chaves públicas e privadas. Este sistema de geração de chaves é chamado **determinístico**, porque nele as chaves públicas e privadas estão correlacionadas e sempre podem ser reproduzidas a partir da mesma semente.

As frases-semente são representadas como uma lista de palavras em inglês (geralmente 12, às vezes 24) que você pode escrever e guardar em algum lugar, e pode reutilizar para recuperar sua carteira, caso por alguma razão você perca o acesso à mesma (digamos, por ter um dispositivo roubado ou danificado).



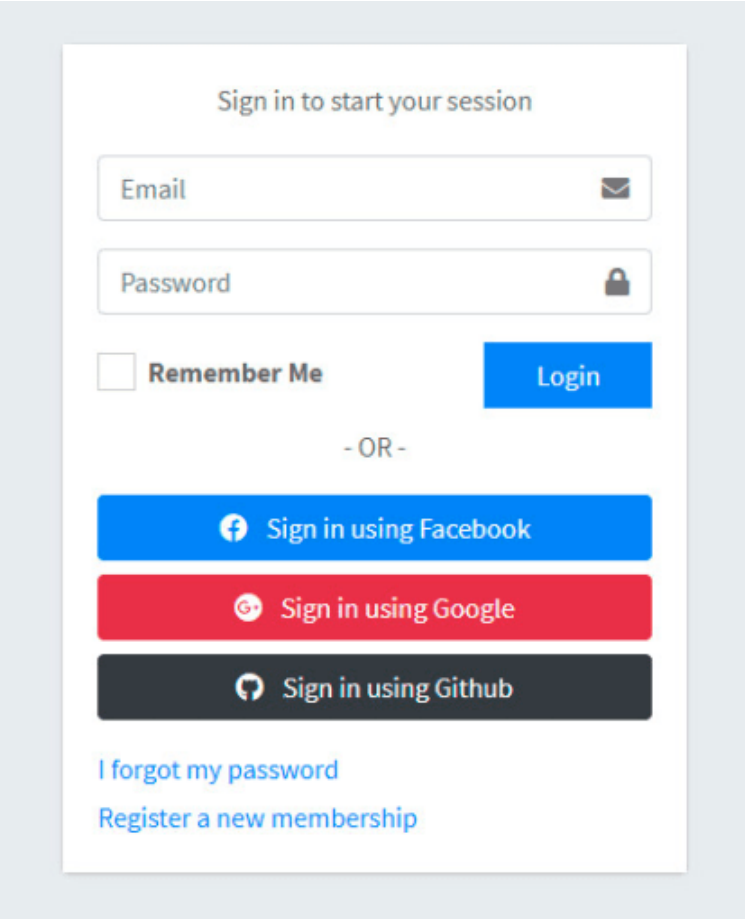
Exemplo de frases-semente - fonte: Realt Academy

Há um conjunto de padrões industriais para implementações de carteiras que garantem a interoperabilidade entre diferentes aplicativos. Graças a estes padrões, você pode facilmente exportar e importar suas chaves entre carteiras de fornecedores diferentes.

Mais que chaveiros - carteiras como identidades na Web3

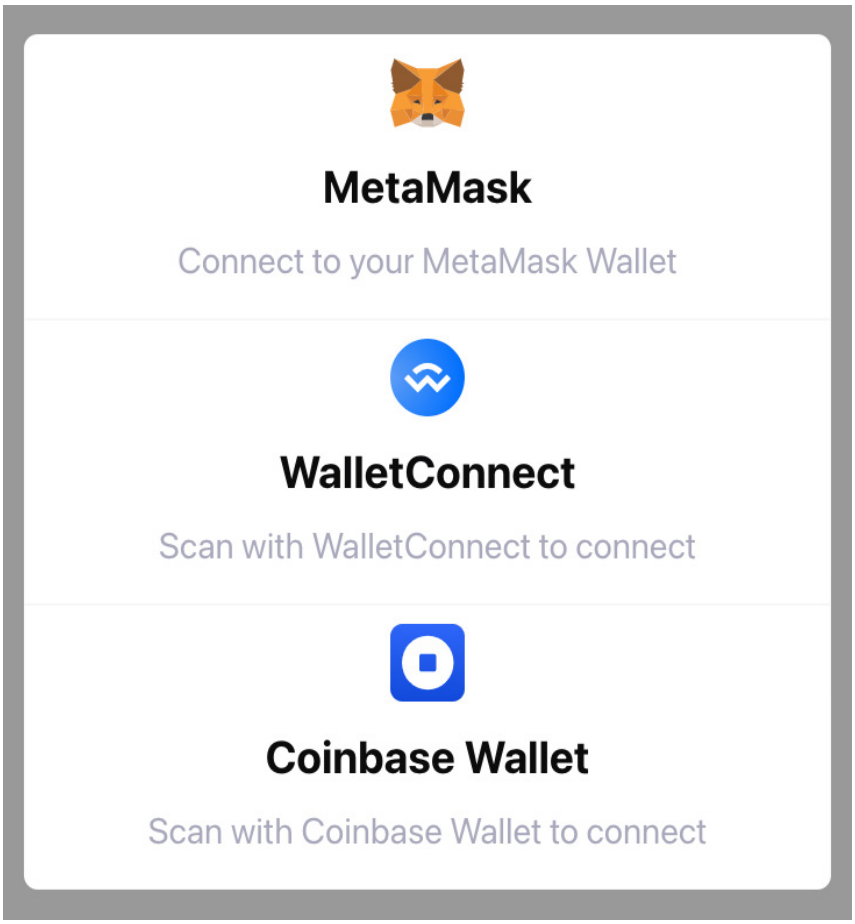
A analogia com os chaveiros ajuda, mas não apanha todas as funções das carteiras. Numa rede blockchain, os nós estão constantemente sincronizando o estado da rede e atualizando o histórico das transações realizadas. Como vimos acima, as carteiras conectam você aos nós da blockchain e permitem que você leia esse histórico e também faça transações, registrando novos dados na rede. Nesse sentido, também podemos dizer que as carteiras funcionam de forma análoga a um navegador da Web tradicional (Web1 / Web2), servindo como porta de entrada para acessar e interagir com essa rede. As carteiras, por sua vez, são sua porta de entrada para a Web3. ***Mas elas vão além, e podem servir também como sua identidade nesse novo ambiente.***

Na Web3, identidade e reputação funcionam de maneira muito diferente do que estamos acostumados hoje. Como regra, na Web2 nossas identidades são vinculadas a algum provedor centralizado, que quase sempre exige que os usuários entreguem informações confidenciais e pessoais. Exemplos dessas identidades são sua conta no Google, Facebook, Twitter, etc.



Login na Web2 - Fonte: Dev.to

Já na Web3, basta vincular sua carteira a um aplicativo descentralizado (dApp) para poder interagir com ele. E, ao contrário do que ocorre com os métodos de autenticação da Web2, os endereços de carteiras são, por padrão, ***pseudônimos***. Se um usuário optar por conectar a mesma carteira com vários dApps, sua identidade (pseudônima) poderá ser facilmente transferível entre eles, o que significa que, com o tempo, o usuário pode construir uma espécie de ***reputação portátil***, mesmo sem precisar revelar informações pessoais.



Login na Web3 - Fonte: Coinbase

À medida que mais e mais aspectos de nossas vidas puderem ser experimentados na Web3 – comunicação, trabalho, educação, entretenimento, finanças, e assim por diante – todos "orquestrados com tokens" (ver definição da Web3 de Dixon e McCormick), nossas próprias identidades se tornarão mais e mais entrelaçadas com o conteúdo de nossas carteiras. Por esta razão, ter uma identidade digital portátil e que preserve a privacidade e forneça segurança se tornará de suma importância neste futuro emergente.

Tipos de carteiras

Tipos de carteiras - Fonte: Odyssey DAO

Uma primeira distinção importante para categorizar carteiras diz respeito a elas estarem ou não conectadas à Internet. As chamadas “carteiras quentes” (*hot wallets*) são conectadas à Internet, enquanto as chamadas “carteiras frias” (*cold wallets*) são mantidas *offline*.

Carteiras quentes (hot wallets)

Nas carteiras quentes, as chaves do usuário são armazenadas e criptografadas no próprio aplicativo, que é mantido *online*. Exemplos de carteiras quentes incluem:

- Carteiras baseadas na web (websites ou extensões do navegador)
- Carteiras para dispositivos móveis (aplicativos para Android ou iOS)
- Carteiras para Desktop (aplicativos instalados em seu sistema operacional)

O uso de uma carteira quente, em suas diferentes formas, é em geral bastante conveniente, mas junto com a conveniência vem também mais risco, já que redes de computadores tendem a ter vulnerabilidades ocultas que podem ser alvo de hackers ou de programas de *malware*, dentre outras formas de invasão do sistema.

As carteiras quentes, por sua vez, podem ser subdivididas em duas outras categorias, de acordo com o modo como as chaves são controladas.

Carteiras quentes custodiadas

São carteiras gerenciadas por uma corretora de criptomoedas (por exemplo, pela Binance, Coinbase, Crypto.com, Mercado Bitcoin, etc.), e exigem que você faça um login com um nome de usuário e senha para acessá-las, da mesma forma como você acessa qualquer aplicativo da Web tradicional.

Com uma carteira custodiada, você não é proprietário de suas chaves e, portanto, não está em pleno controle dos ativos que elas gerenciam. Como diz um ditado popular na comunidade cripto, *"not your keys, not your coins!"* (ou seja, se as chaves não são suas, as moedas também não são!).

Por causa disso, ao usar carteiras custodiadas você deve confiar no prestador de serviços para armazenar com segurança seus ativos e implementar fortes medidas de segurança para impedir o acesso não autorizado. Estas medidas incluem autenticação de dois fatores, confirmação por e-mail e autenticação biométrica. Muitas corretoras não permitirão que você faça transações até que estas medidas de segurança sejam devidamente configuradas pelo usuário.

Carteiras quentes não-custodiadas

Essas carteiras são autogeridas. As chaves e os ativos estão totalmente sob o controle dos usuários. Mas como grande poder implica grande responsabilidade, isso significa que os usuários de carteiras não-custodiadas devem se encarregar de sua própria segurança, tanto no que diz respeito ao armazenamento de chaves quanto de frases-semente. Se alguma delas for perdida, a recuperação pode ser difícil ou impossível, já que normalmente não são armazenadas em nenhum servidor terceirizado.

Carteiras frias (cold wallets)

As carteiras frias estão, por padrão, offline. Isto as torna menos convenientes do que as carteiras quentes, mas, via de regra, também as torna mais seguras.

Exemplos de carteiras frias incluem:

- **Carteiras de papel:** uma carteira de papel é um local físico onde as chaves e frases-semente são escritas ou impressas. Como hackers não têm como acessar estas chaves remotamente, esse método é mais seguro do que manter os fundos em uma carteira quente. Por outro lado, abre-se o risco potencial de que o pedaço de papel seja destruído ou perdido, o que pode resultar em fundos irrecuperáveis.
- **Carteiras de aço inoxidável:** para evitar o risco de destruição de uma carteira de papel em caso de incêndio ou inundação, pode-se também gravar as chaves privadas em uma chapa de aço inoxidável. Alguns fabricantes oferecem inclusive kits prontos para criar esse tipo de carteira.
- **Carteiras de hardware:** uma carteira de hardware é um dispositivo externo (geralmente um dispositivo

USB ou Bluetooth) que armazena suas chaves. Você só pode assinar uma transação apertando um botão físico no dispositivo, que os atores maliciosos não podem controlar.

Carteiras com múltiplas assinaturas (multisig)

Também conhecidas como “multisig”, são carteiras que requerem duas ou mais assinaturas de chaves privadas para autorizar as transações. Esta solução é útil para uma série de casos de uso:

- Um indivíduo que utiliza uma carteira multisig pode evitar a perda de acesso total à carteira em um cenário em que uma chave é perdida, pois nesse caso ainda haverá outras chaves aptas a assinar transações.
- As carteiras multisig podem dificultar o uso indevido de fundos e fraudes, o que as torna uma boa opção para fundos de hedge, bolsas e corporações. Como cada pessoa autorizada terá uma chave e uma transação requer o uso da maioria das chaves, torna-se impossível para qualquer indivíduo realizar unilateralmente transações não autorizadas.

(Todos os tipos de carteira descritos acima tem versões multisig - você pode ter carteiras multisig quentes, frias, de hardware, e assim por diante.)

Como garantir a segurança de sua carteira

Se a chave privada ou a frase semente de sua carteira for perdida ou roubada, você perderá permanentemente o acesso a seus bens. Portanto, é crucial que você aprenda como proteger sua carteira para evitar fraudes.

Veja aqui algumas dicas para garantir a segurança de sua carteira:

1. **Armazene sua chave privada e sua frase-semente em um local seguro.** Considere copiá-las para papel ou aço inoxidável, guardando-os muito bem, ou então, se você preferir ter acesso às chaves online, use um gerenciador de senhas (como o 1Password ou LastPass).

2. **Nunca compartilhe sua chave privada ou frase-semente com ninguém.** Não importa quem perguntar - simplesmente não compartilhe!
3. **Proteja sua senha.** Se sua carteira tem uma senha separada, qualquer um que a obtenha pode obter sua chave privada. Escolha, portanto, uma senha segura, de preferência salvando-a num gerenciador de senhas, e usando 2FA.
4. **Não deixe ativos de grande valor em sua carteira quente usada no dia-a-dia.** Coloque-os em uma carteira fria ou em outra carteira quente separada. Se você tem muitos ativos em sua carteira e compartilha seu endereço publicamente, mais cedo ou mais tarde alguém tentará aplicar algum golpe usando essas informações.
5. **Verifique a URL do site, e-mail, ou perfil em rede social antes de tomar qualquer ação envolvendo sua carteira.** Os golpistas normalmente se fazem passar por uma plataforma confiável para fazer phishing de sua frase-semente ou chave privada.
6. **Desligue as mensagens privadas em aplicativos como Discord e Telegram, e jamais interaja com ativos desconhecidos (como NFTs) que aparecem "do nada" em sua carteira.** Estes são dois vetores de ataque comuns que os golpistas usam.

Além dessas dicas gerais, seguem também sugestões de melhores práticas para o uso de carteiras frias especificamente:

1. **Sua frase-semente é mais importante do que o dispositivo em si.** Se sua carteira fria for danificada, você sempre poderá recuperar seus bens importando sua frase de semente em outra carteira. Portanto, priorize a segurança da frase-semente, conforme indicado acima.
2. **Não use a frase-semente de uma carteira quente na sua carteira fria.** O objetivo da carteira fria é armazenar uma frase-semente offline. Reutilizar uma frase-semente de carteira quente na carteira fria significa traz de volta todos os problemas do armazenamento online.
3. **Fique muito atento a tentativas de phishing de carteira fria.** Compre uma carteira fria somente nos sites oficiais dos fabricantes (como Ledger e Trezor). Não responda a e-mails falsos de suporte ou mensagens privadas pedindo sua frase-semente.

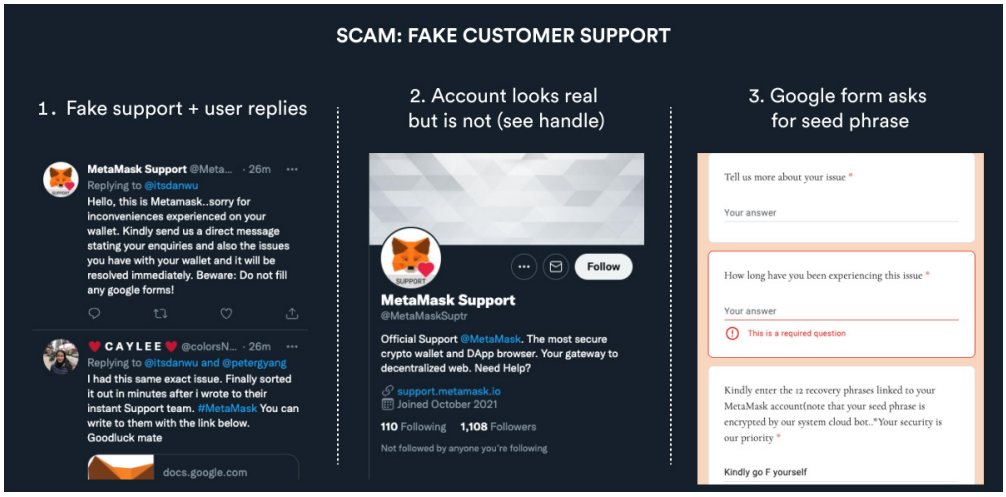
Fraudes comuns envolvendo carteiras, e dicas para evitá-las

Um dos principais objetivos dos golpistas é enganar você para compartilhar sua chave privada ou sua frase-semente. Aqui está uma lista de golpes comuns com essa finalidade, e dicas para evitá-los.

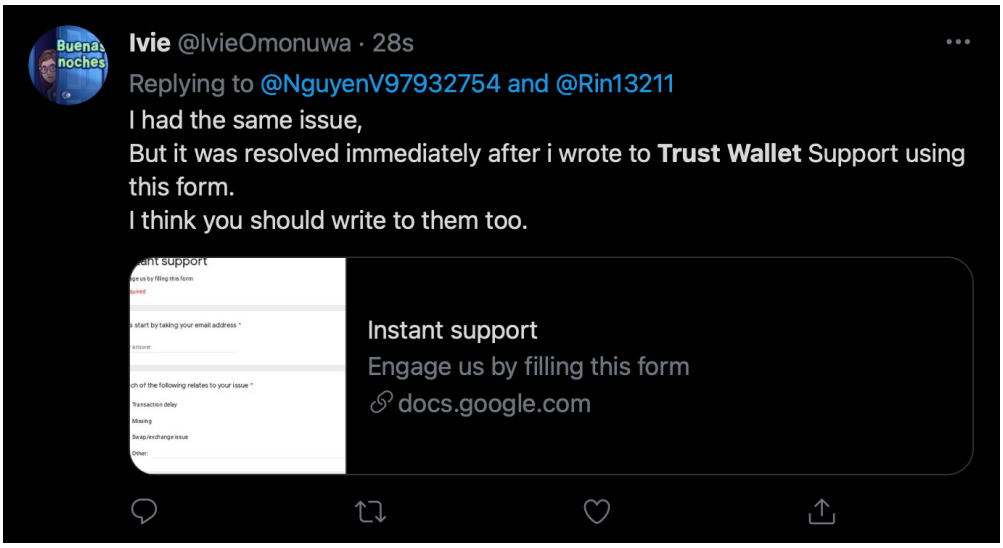
Ataques de *phishing* por contas falsas de suporte ao cliente

Golpistas enviam uma mensagem por email, rede social, SMS, etc., informando que houve algum tipo de problema com sua carteira - por exemplo, “Sua conta Metamask foi invadida”. Os criminosos então tentam convencer você a compartilhar sua chave privada ou sua frase-semente, supostamente para verificar que você é mesmo o dono da conta. Caso isso aconteça:

- Verifique atentamente a URL do site, o endereço de e-mail, o perfil social ou o número de telefone do qual se originou a mensagem.
- Mesmo que a origem pareça confiável, lembre-se: *nenhuma plataforma respeitável solicitará sua chave privada ou frase semente!*



Ataque de suporte falso da MetaMask - Fonte: Odyssey DAO



Ataque de suporte falso Trust Wallet - Fonte: Rainbow

"Airdrops" de tokens e NFTs falsos

Como endereços de carteiras são públicos, literalmente qualquer pessoa pode enviar tokens ou NFTs para esses endereços. Geralmente isso não é um grande problema, porque você pode simplesmente optar por ignorá-los; mas alguns cibercriminosos desenvolveram formas de enviar tokens que podem executar transações em sua conta assim que você interagir com eles. Nesse sentido,

pode-se comparar esses tokens a um trojan que permite que hackers acessem seu computador assim que você interagir com um arquivo malicioso. Uma análise mais detalhada desse tipo de golpe, incluindo um vídeo explicativo, pode ser encontrada aqui.

Como precaução, tome muito cuidado com “brindes” e “presentes”, normalmente ofertados por perfis falsos em redes sociais ou por mensagens instantâneas privadas em servidores do Discord ou em grupos do Telegram. *Jamais interaja com um token de origem desconhecida em sua carteira!*

Assinatura às cegas (*blind-signing*)

Outro tipo de ataque recente e ainda pouco conhecido usado para roubar ativos digitais de carteiras é a assinatura às cegas. Esse ataque se aproveita do fato de que usuários que empregam suas carteiras para interagir com dApps e NFTs muitas vezes não revisam o código dos contratos inteligentes subjacentes a esses aplicativos e, portanto, podem acabar assinando e autorizando transações sem saber exatamente o que estão assinando e autorizando.

Por exemplo, às vezes é necessário conceder a terceiros – digamos, uma corretora de criptomoedas ou um marketplace de NFTs – permissão para realizar transações envolvendo tokens dentro de sua carteira. Uma vez que o acesso de terceiros é aprovado, os usuários do aplicativo podem trocar tokens ou listar NFTs à venda sem pagar taxas adicionais a cada vez. Os invasores descobriram maneiras de enganar as vítimas para que lhes dêem aprovação de terceiros sobre o conteúdo de sua

carteira, que pode ser transferido para outros endereços controlados pelos criminosos.

Carteiras de hardware falsas

Um golpe muito engenhoso envolve o envio de algum tipo de correspondência - pode ser um email ou até mesmo **uma carta física pelo correio**, “assinada” por um CEO de uma fabricante de carteiras de hardware - que tenta convencer o usuário de que sua carteira sofreu algum tipo de ataque e precisa ser substituída. Às vezes um dispositivo novo é inclusive enviado junto com a carta. Mas esses novos dispositivos foram hackeados para fornecer acesso aos golpistas, que então clonam a carteira usando a frase-semente previamente criada para ter acesso aos fundos do usuário.

Caso algo assim aconteça, simplesmente jogue esses dispositivos no lixo e informe o fabricante da tentativa.

Carta falsa assinada pelo “CEO da Ledger” - Fonte: Ledger

Fontes e Leituras Adicionais

- **What is a Crypto Wallet? A Beginner's Guide** (Crypto.com)
- **What is a crypto wallet? | Coinbase**
- **Public Key Cryptography - Network Encyclopedia**
- **Seed Phrase 101** (Realt Academy)
- **How to use a hot wallet?** (Odyssey DAO)
- **The Anatomy of MetaMask. An X-ray of Web3's Beloved Fox | by Julia Wu | Jun, 2022**
- **How to use a cold wallet?** (Odyssey DAO)
- **What is a Hardware Wallet and How Does it Work?** (Crypto.com)
- **How to avoid crypto scams** (Rainbow)
- **How to avoid wallet scams?** (Odyssey DAO)

Fortaleça sua operação de segurança da informação com a gestão de riscos digitais da plataforma Axur

Nossa plataforma é um hub de tecnologia e serviços gerenciados, oferecendo visibilidade de riscos digitais para operações que desejam escalar a prevenção e a resposta a incidentes.

400
empresas

600
marcas

+3.700
grupos fechados em redes sociais

+ de 1.7 bilhão
de sinais analisados

Quase 3 milhões
de mensagens com menções de clientes interceptadas em nossa plataforma

Dados do último ano.

Oferecemos monitoramento, detecção, triagem e reação para os principais grupos de riscos encontrados na internet:

- Fraudes Digitais
- Vazamento de Dados
- Pirataria Online
- Deep & Dark Web

A Plataforma Axur oferece o apoio de especialistas para lidar com ataques de grande impacto, direcionando ações táticas e operacionais de defesa cibernética.

Com os times CTI/ART da Axur, você aumenta a superfície de pesquisa, descoberta e investigação de ameaças da sua estrutura de SI e Threat Intel, revelando padrões de fraudes imperceptíveis para estratégias reativas.

AGENDE UMA DEMO

Desenvolvimento:

Jonadas Techio
Redação

Patrick Santos
Design

Sobre a Axur

Líder em proteção contra riscos digitais na América Latina, a Axur ajuda empresas a preservar a valiosa relação de confiança construída com seus clientes e parceiros por meio de experiências digitais mais seguras.

Contamos com uma equipe de Inteligência Cibernética que, unidos à alta tecnologia de Inteligência Artificial, permitem maior visibilidade e reação rápida aos riscos. Tudo isso integrado à nossa plataforma, que monitora todas as camadas da web 24x7, solicitando takedowns automaticamente.

Nossos times de pesquisa (Axur Research Team) e serviços (CTI Team) em Cyber Threat Intelligence estão prontos para oferecer o apoio necessário à resposta contra ameaças de alto impacto.

Contato para a imprensa

press@axur.com

Endereços

EUA
535 Mission Street – 14th floor
San Francisco, CA 94105

Singapura
109 North Bridge Road
Cityhall District, 179097

Brasil
Rua Mostardeiro, 322 – 15º andar
Porto Alegre, RS 90430-000

axurbr Axur AxurBrasil AxurBrasil AxurBrasil Axur