ENCCLA 2024

Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro

Ação 01/2024: Elaborar diagnóstico das principais vulnerabilidades relacionadas à persecução penal envolvendo ativos virtuais bem como propor Plano de Ações mitigadoras dos riscos, contemplando aspectos relacionados a prevenção, detecção e punição de corrupção e de lavagem de dinheiro

Cartilha Informativa: Principais Golpes com Ativos Virtuais no Brasil

Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro – ENCCLA 2024

Ação 01/2024: Elaborar diagnóstico das principais vulnerabilidades relacionadas à persecução penal envolvendo ativos virtuais bem como propor Plano de Ações mitigadoras dos riscos, contemplando aspectos relacionados a prevenção, detecção e punição de corrupção e de lavagem de dinheiro

Coordenador: MPF

Colaboradores: ABIN, ADPF, AGU, AJUFE, ANM, BB, BCB, CADE, CAIXA, CGE/MG, CGM/SP, CGU, CJF, CNJ, CNMP, COAF, CONACI, CONCPC, CVM, DRCI, FEBRABAN, GNCOC, MPDFT, MPGO, MPMS, MPPR, MPRJ, MPRN, MPS, PCDF, PCRS, PCSP, PF, PGFN, PREVIC, REDE/SECEX-SC, RFB, SAL/MJSP, SENAD/MJSP, SENASP/MJSP.

Cartilha Informativa: Principais Golpes com Ativos Virtuais no Brasil

1. Introdução

Com o aumento da popularidade dos ativos virtuais, mais popularmente conhecidos como "criptoativos" ou "criptomoedas", e de outros ativos digitais, também houve um aumento significativo no número de golpes e fraudes relacionadas a eles.

De acordo com um relatório da CipherTrace, uma empresa de segurança especializada em ativos virtuais, os golpes e as fraudes envolvendo criptoativos resultaram em perdas de aproximadamente US$ 1,9 bilhão em 2020, representando uma ameaça significativa para investidores e usuários de ativos virtuais ao redor do mundo.

Deve ser destacado, adicionalmente, que os golpes e as fraudes envolvem não apenas os ativos virtuais mais conhecidos, caso do Bitcoin, como também projetos de criação de "novos ativos virtuais", com propostas que prometem ganhos fáceis e rápidos, a fim de enganar e lesar os investidores interessados. Um caso emblemático recente foi a criação do "ativo virtual" denominado como OneCoin, um esquema criminoso que arrecadou quase US$ 4,0 bilhões em todo o mundo, segundo site Statista.

No Brasil, a Associação Brasileira de Criptoeconomia (ABCripto) estimou que cerca de 200 mil brasileiros foram vítimas de fraudes com ativos virtuais em 2021, resultando em prejuízos que ultrapassam R$ 1,0 bilhão.

Esses números alarmantes destacam a importância da população de estar informada e preparada para identificar e evitar esses golpes e fraudes. O objetivo desta cartilha é fornecer informações claras e objetivas sobre os tipos mais comuns de golpes com ativos virtuais, como identificá-los, como se proteger e o que fazer ao ser vítima de um golpe ou fraude.

Neste material, você encontrará:

- Definição dos ativos virtuais;
- Descrição detalhada dos principais golpes e fraudes com ativos virtuais;
- Dicas práticas de como se proteger contra esses golpes e fraudes; e
- Orientações sobre o que fazer se você for vítima de um golpe ou fraude

2. O que são Ativos Virtuais?

Ativos virtuais, também conhecidos como "criptoativos" ou "criptomoedas", são representações digitais de valor que podem ser negociados ou transferidos por meios eletrônicos.

Geralmente, as transações envolvendo ativos virtuais ocorrem em redes descentralizadas, baseadas na tecnologia DLT (Distributed Ledger Technology), sendo as mais conhecidas a rede blockchain do Bitcoin, a rede blockchain Ethereum e a rede blockchain Solana. As redes em que são criados e transacionados propiciam registros

realizados de forma distribuída entre os nós participantes, com registros imutáveis, que sinalizam oferecer maior grau de transparência e segurança nas transações.

Os ativos virtuais são armazenados em carteiras digitais, acessíveis por meio de chaves criptográficas privadas, e podem ser usados para diversas finalidades, incluindo pagamentos e investimentos.

Principais Tipos de Ativos Virtuais:

- **Stablecoins:** são projetados para manter um valor estável, geralmente atrelados a um ativo de reserva como o dólar americano. Exemplos incluem o Tether (USDT) e o USD Coin (USDC).
- **Tokens:** podem representar uma ampla gama de ativos, como direitos de propriedade, de obtenção de produtos ou de acesso a serviços. Existem diversos tipos de **tokens**, incluindo:
    - "tokens de utilidade", que fornecem acesso a um produto ou serviço específico
    - "tokens de investimento", que representam uma participação em um ativo subjacente, como ações ou dívidas; e
    - "tokens de governança", que permitem aos seus detentores participar do processo de tomada de decisões de uma rede ou projeto de rede **blockchain**.

Popularidade e Uso:

- Nos últimos anos, a adoção de ativos virtuais tem crescido exponencialmente. Eles são utilizados não apenas por indivíduos como uma forma de investimento ou para a realização de pagamentos, mas também por empresas e instituições financeiras para diversificar suas carteiras e realizar transações de forma mais eficiente.
- Ativos virtuais podem oferecer vantagens como a redução de custos de transação, maior velocidade nas transferências e acessibilidade global. No entanto, também apresentam riscos, como a volatilidade dos preços e a vulnerabilidade a ataques cibernéticos e fraudes.
- As stablecoins se tornaram um ativo virtual de maior preocupação por parte das autoridades internacionais, especialmente pelas possibilidades de uso para evasões de divisas, lavagem de dinheiro e sonegação fiscal, e pela emulação de operações de câmbio sem os devidos registros, o que fere os regramentos estabelecidos[1][2].

[1] Cripto Tether (USDT) é usada na 25 de Março para alimentar contrabando em SP; conheça o esquema (infomoney.com.br)

[2] Relatório CPI de Pirâmides Financeiras: Microsoft Word - RelatÃ³rio CPI 9 out 15 15 v final (camara.leg.br)

- Por outro lado, os ativos virtuais propiciam estudos e avanços por parte das autoridades, considerando os aspectos mais favoráveis desses ativos que permitem pensar em aperfeiçoamentos substanciais nos sistemas financeiros e de pagamentos, em termos de segurança, de custos e de velocidade nas transações.

Por que se Tornaram Instrumentos de Golpes:

- A natureza digital e descentralizada dos ativos virtuais torna difícil a regulação, o monitoramento e a supervisão, criando um ambiente propício para a atuação de golpistas e fraudadores.
- A promessa de altos retornos em um curto período, incluído enriquecimento rápido, atrai investidores inexperientes que podem não estar cientes da veracidade das informações apresentadas ou dos riscos envolvidos.
- A utilização das redes sociais e da internet, por parte de influenciadores mal-intencionados, acaba por ampliar a atração por parte da população, baseada especialmente na credibilidade presumida dos divulgadores, que sugerem retornos substanciais sem se comprometerem com desempenho ou com as regras de prudência adotadas pelas instituições autorizadas atuantes nos mercados tradicionais para a divulgação de ofertas de investimentos.
- A falta de conhecimento técnico por parte de muitos usuários facilita a exploração por criminosos que se aproveitam de fraquezas de segurança e técnicas de engenharia social para enganar as vítimas.

Entender o que são ativos virtuais e como eles funcionam é o primeiro passo para se proteger contra fraudes e golpes. A seguir, estão detalhados os golpes mais comuns, assim como mecanismos que auxiliam na sua identificação.

3. Principais Golpes com Ativos Virtuais

1. **Pirâmide Financeira**

    - **Como Funciona:**
        - Em uma pirâmide financeira, os investidores são atraídos por promessas de altos retornos com pouco ou nenhum risco. Inicialmente, eles recebem os lucros prometidos, que são pagos com o dinheiro de novos investidores.
        - A pirâmide continua a crescer até que não haja novos investidores suficientes para sustentar os pagamentos, e então colapsa, deixando a maioria dos participantes sem o dinheiro investido.
    - **Como Identificar:**

- Promessas de retornos garantidos e muito acima da média de mercado.
- Necessidade de recrutar novos investidores para manter os ganhos.
- Falta de informações claras sobre a empresa ou o produto.
- Pressão para investir rapidamente e não perder a oportunidade.
- Divulgação e disseminação por meio de redes sociais, internet, **"**conhecidos" ou agentes não integrantes ou não familiarizados com o mercado financeiro.

- **História:** João foi atraído por um amigo para investir em uma empresa que prometia duplicar seu dinheiro em poucos meses. Ele precisaria apenas recrutar mais "investidores". João aplicou seus recursos e convidou várias pessoas, mas logo percebeu que a empresa havia sumido com todo o dinheiro.

2. ***Phishing* de Dados**

- **Como Funciona:**
  - Golpistas enviam e-mails ou mensagens[3] que parecem ser de fontes confiáveis, como bancos, outras instituições financeiras ou *exchanges* de ativos virtuais, pedindo que a vítima clique em um link e insira informações pessoais, como login e senha.
  - O link leva a um site falso que captura as informações inseridas pela vítima, permitindo que os golpistas acessem suas contas.
- **Como Identificar:**
  - E-mails ou mensagens com erros gramaticais ou de ortografia.
  - Endereços de e-mail de remetentes que não correspondem ao domínio oficial da empresa.
  - Links que levam a URLs que não correspondem ao site oficial da empresa.
  - Solicitações de informações sensíveis, como senhas ou dados pessoais.
- **História:** Paulo recebeu um e-mail que parecia ser de sua *exchange* de criptoativos, solicitando que ele fizesse login para verificar uma atividade suspeita. Ele clicou no link e inseriu seus dados de login. Pouco depois, percebeu que todos os seus ativos na *exchange* haviam sido transferidos para outra conta sem sua autorização.

3. ***Phishing* de Assinatura**

- **Como Funciona:**

[3] Por meio do Whatsapp, Telegram, SMS, Instagram, Facebook, ou outras redes sociais, por exemplo.

- Golpistas enviam mensagens urgentes pedindo que a vítima assine uma transação para "corrigir um erro" ou para evitar que sua conta seja bloqueada.
- A transação assinada, na verdade, autoriza a transferência de recursos da conta da vítima para a conta dos golpistas.

- **Como Identificar:**
  - Mensagens urgentes e alarmistas pedindo ação imediata.
  - Solicitações para assinar transações sem uma explicação clara e lógica.
- **História:** Carlos recebeu uma mensagem urgente de uma pessoa que se passava por suporte técnico de sua carteira digital (*wallet*), solicitando que ele assinasse uma transação para "corrigir um erro". Ele assinou e perdeu todos os seus ativos virtuais armazenados na carteira.

4. **Investimento em Plataforma Fraudulenta**

- **Como Funciona:**
  - Golpistas criam plataformas de investimento falsas que parecem legítimas e atraem investidores com promessas de altos retornos garantidos.
  - Os investidores depositam dinheiro na plataforma, mas os golpistas desaparecem com os recursos.
- **Como Identificar:**
  - Falta de regulamentação ou registro oficial da empresa.
  - Promessas de retornos fixos e garantidos, independentemente das condições do mercado.
  - Falta de informações claras sobre os responsáveis pela plataforma e sua localização.
  - Testemunhos e avaliações falsas ou inexistentes.
- **História:** Ana investiu suas economias em uma plataforma de investimentos que prometia retornos fixos mensais. A plataforma operou por alguns meses, mas de repente desapareceu, deixando Ana e outros investidores sem nenhum retorno e sem o capital investido.

5. **Golpe Amoroso**

- **Como Funciona:**
  - Golpistas criam perfis falsos em sites de relacionamento e estabelecem um relacionamento com a vítima.
  - Depois de ganhar a confiança da vítima, eles começam a pedir dinheiro para emergências falsas, como problemas médicos ou despesas de viagem.
- **Como Identificar:**

- Solicitações de dinheiro após um breve período de relacionamento.
- Histórias dramáticas e urgentes que requerem assistência financeira.
- Inconsistências nas informações pessoais fornecidas pelo golpista.
- Relutância em se encontrar pessoalmente ou por videochamada.

- **História:** Laura conheceu um homem em um site de relacionamentos que, após algumas semanas, começou a pedir dinheiro para uma emergência médica. Confiando nele, Laura enviou uma grande quantia, apenas para descobrir que o perfil dele era falso e que ela havia sido enganada.

4. Como se Proteger

- **Informe-se:** É fundamental que você se mantenha informado sobre os ativos virtuais e os golpes mais comuns.
- **Verifique as Fontes:** Sempre verifique a legitimidade de empresas e indivíduos antes de investir. Faça uma pesquisa detalhada sobre a reputação e a legalidade da empresa. Eventualmente, consulte o gerente da instituição financeira da qual é cliente para a obtenção de informações mais precisas.
- **Busque verificar a legitimidade de mensagens recebibas:** sempre procure verificar a legitimidade da mensagem entrando em contato diretamente com a empresa, usando números de telefone ou e-mails oficiais.**Use Senhas Fortes e Autenticação de Dois Fatores:** Utilize senhas fortes e únicas para suas contas e habilite a autenticação de dois fatores sempre que possível.
- **Desconfie de Promessas de Lucros Fáceis:** Questione promessas de retornos altos e garantidos. Lembre-se de que investimentos legítimos envolvem riscos proporcionais aos retornos esperados.
- **Desconfie de práticas de vendas agressivas:** Questione práticas de vendas agressivas usadas para pressionar o investidor a tomar decisões apressadas.
- **Reputação e credibilidade:** Não associe a fama ou **o** carisma de influenciadores ou figuras conhecidas popularmente a credibilidade, especialmente em assuntos financeiros. A depender dos resultados da oferta do ativo virtual, o influenciador ou divulgador receberá remuneração certa, independentemente do resultado para os seus “seguidores”.

5. O que Fazer se for uma Vítima

- **Relate o Golpe:** Entre em contato com os órgãos competentes para relatar golpes (ex.: Polícia Civil, Polícia Federal, Ministério Público, Procon, etc.).
- **Preserve Evidências:** Mantenha registros de transações, e-mails, mensagens e outras comunicações que possam servir como evidência.

- **Busque Suporte Jurídico:** Consulte advogados especializados em crimes cibernéticos para obter orientação legal.

6. Conclusão

Mantenha-se vigilante e busque conhecimento necessário para navegar com segurança no mundo dos ativos virtuais, protegendo seu patrimônio, de seus familiares e conhecidos, ajudando a evitar que outros sejam enganados e que ações criminosas desse tipo se perpetuem.

- **Recursos Adicionais:** Utilize os links e contatos fornecidos para mais informações e apoio.

Apêndice

Glossário

- **Blockchain:** Uma tecnologia de registro distribuído que permite a criação de um livro-razão digital seguro e imutável. Utilizada principalmente em criptomoedas.
- **Ativo Virtual (criptoativo ou criptomoeda):** A Lei 14.478 define ativo virtual como "a representação digital de valor que pode ser negociada ou transferida por meios eletrônicos e utilizada para realização de pagamentos ou com propósito de investimento". Exemplos incluem Bitcoin e Ethereum.
- **Distributed Ledger Technology (DLT) ou Tecnologia de Registro Distribuído:** é um sistema de armazenamento de dados distribuído por uma rede de computadores.
- **Prestadoras de Serviços de Ativos Virtuais (também conhecido como *Exchange)*:** pessoa jurídica que executa, em nome de terceiros a compra, a venda e a troca de ativos virtuais (criptoativos) por outros ativos virtuais ou por moedas fiduciárias (Real ou dólar), o que atua na oferta de ativos virtuais.
- **Token:** Representação digital de um ativo ou utilidade que pode ser transferido entre usuários de blockchain.
- **Stablecoin:** Tipo de criptomoeda projetada para manter um valor estável, geralmente atrelado a uma moeda fiduciária como o dólar americano.
- **Phishing:** Forma de engenharia social, onde golpistas tentam obter informações confidenciais se passando por entidades confiáveis através de e-mails, mensagens ou sites falsos.
- **Autenticação de Dois Fatores (2FA):** Método de segurança que requer duas formas de verificação antes de conceder acesso a uma conta ou sistema.

Recursos e Referências

- **CipherTrace:** Website
- **Associação Brasileira de Criptoeconomia (ABCripto):** Website
- **Polícias Civis (Delegacias Especializadas em Crimes Eletrônicos)**
- **Polícia Federal:** Website
- **Procon:** Website
- **Statista:** https://www.statista.com/topics/4495/cryptocurrencies/
- **Investopedia:** Website
- **Chainalysis:** https://www.chainalysis.com/
- **Coinmarketcap:** https://coinmarketcap.com/pt-br/

Fontes:

- CipherTrace. (2020). *Cryptocurrency Crime and Anti-Money Laundering Report*.

- Associação Brasileira de Criptoeconomia (ABCripto). (2021). Relatório de Fraudes com Criptomoedas no Brasil.
- Statista (2022). Os projetos cripto que roubaram seus investidores (*The Crypto Projects Stealing from Their Investors*). Disponível em: https://www.statista.com/chart/27775/biggest-rug-pulls-by-estimated-cryptocurrency-usd-value-stolen/
- Lei nº 14.478, de 22 de dezembro de 2022, que dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais.