Bitget

BETTER TRADING BETTER LIFE

# AMA de segurança: prevenção de fraudes



Apresentação: Gabriel Melo

# Conteúdo


1 Como você armazena suas criptomoedas?

2 Golpes comuns em criptomoedas e celulares

3 Como garantir a segurança dos ativos da sua conta

4 Como diminuir a chance de cair em um golpe?

5 Como sabemos que a Bitget é segura e confiável?

6 Whitelist de emails oficiais da Bitget

7 Golpes de criptomoedas que aconteceram de verdade

Bitget

# Casos de roubos terríveis

Business

## Ethereum Lending Protocol XCarnival Hit With $3.8M Exploit, Recovers 50%

The DeFi protocol persuaded a hacker to return $1.9 million.

## Harmony Attacker Moves Over $44M Worth of Stolen Ether; Authorities Alerted

Harmony is working with two blockchain tracing and analysis firms and collaborating with the FBI, developers said.

## DragonEx Hack: USD 7 million in Crypto Stolen, Compensations in Sight



1

Como você armazena suas criptomoedas?

# 1. Como você armazena suas criptomoedas?

**Corretora centralizada (CEX)**

**Carteira quente (DEX)**

**Carteira fria**



Bitget



## Corretora centralizada (CEX)

**Prós**

- Boa para traders ambiciosos, fácil de navegar
- Variedade de produtos financeiros e campanhas

**Contra**

- Opções de corretoras demais



## Carteira quente (DEX)

**Prós**

- Fácil acesso a diferentes Dapps
- Descentralizada

**Contra**

- Risco de invasão



## Carteira fria

**Prós**

- O mais alto nível de segurança

**Contras**

- Custo do hardware
- Perder ou esquecer onde guardou



# 2

## Golpes comuns em criptomoedas e celulares

# Golpes comuns em criptomoedas

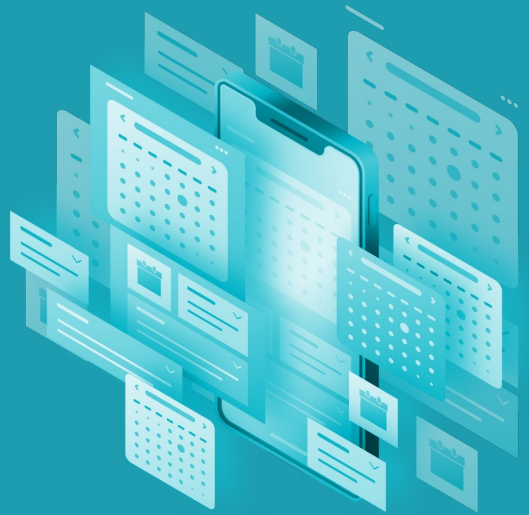
- Promessas de multiplicar seu dinheiro
- Promessas de dinheiro grátis
- Explicações vagas sobre para onde seu dinheiro está indo



# Golpes comuns em criptomoedas

- Grandes esquemas de criptomoedas em redes sociais. Esse tipo de golpe é comumente encontrado nas redes sociais. Os criminosos geralmente se comunicam com você como administradores nas redes sociais, se apresentam como especialistas em criptomoedas e solicitam seu endereço de carteira ou senha da conta.

- Obrigações contratuais que exigem a retenção bloqueada de criptomoedas sem a capacidade de venda.



- Erros ortográficos óbvios e erros tipográficos em emails, posts de redes sociais e outras comunicações.

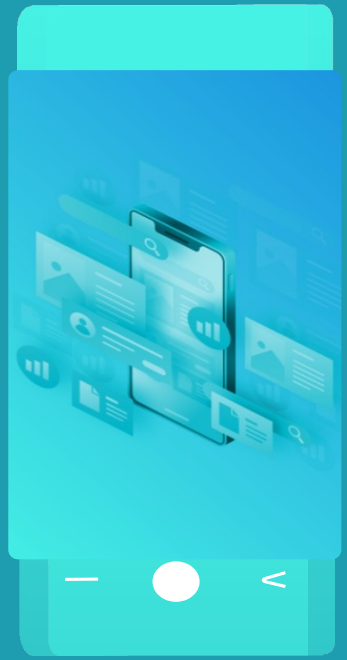
# Golpes comuns em criptomoedas

- Influenciadores falsos ou alegações de ser (ou ter o endosso de) uma celebridade.
- Manipulação psicológica, como extorsão ou chantagem, ameaçando outras pessoas com informações confidenciais em sua posse para obter dinheiro solicitado ilegalmente e forçá-las a pagar em bitcoin ou outras moedas.
- Plataforma de trading falsa para atrair usuários para negociar (por favor, reconheça o site oficial da Bitget em www.bitget.com).



# Golpes comuns em celulares

Um golpe comum no celular são corretoras de criptomoedas falsas. Ao baixar o Bitget exchange, tenha o cuidado de identificar o canal oficial de download (Google Play Store, App Store), e não baixe nada de terceiros ou de links enviados por estranhos na comunidade.





# 3

## Como garantir a segurança dos ativos da sua conta

Bitget

# Para a segurança dos ativos da sua conta

**01**

NUNCA compartilhe sua chave privada com ninguém.

**02**

Atualize regularmente suas senhas fortes.

**03**

Ative a autenticação de dois fatores sempre que possível.

**04**

Anote sua chave particular fisicamente (evite salvá-la online ou tirar foto dela) e guarde-a em um local seguro.

**05**

Evite clicar em links suspeitos (email de phishing).

**06**

Não ligue para nenhum número de telefone de alguém que alega ser um representante do atendimento ao cliente da Bitget.



# 4

## Como diminuir a chance de cair em um golpe?

**Como posso me proteger para diminuir a chance de cair em um golpe?**



## Faça sua própria pesquisa

Um erro comum é correr para um investimento só porque todo mundo está fazendo isso. Mesmo que vários sites sugiram investir em um determinada criptomoeda, é sempre aconselhável fazer sua própria pesquisa completa (mesmo que seja por meio de pesquisas simples no Google), pois os riscos geralmente são altos.

## Não confie em ninguém cegamente



Ao investir em criptomoedas, você encontrará corretoras e projetos oficiais de criptomoedas, bem como contas e sites falsos. Quando se trata de celebridades e influenciadores, é fácil se empolgar e acreditar em DMs (mensagens diretas) que prometem bons retornos de criptomoedas. A regra de ouro é sempre ser cético em relação a tudo. Afinal, é o seu dinheiro suado que estará em jogo se você confiar na pessoa ou empresa errada.

**Como posso me proteger para diminuir a chance de cair em um golpe?**

## Proteja sua carteira de criptomoedas



Como sua carteira é a principal unidade de armazenamento para todos os seus ativos de criptomoedas, é importante proteger sua carteira com autenticação de dois fatores (2FA) e senhas complexas. Também é essencial armazenar suas chaves em segurança – e evitar compartilhá-las com qualquer pessoa.

## Verifique todos os URLs



Ao acessar sites e corretoras de criptomoedas, lembre-se de verificar o URL cuidadosamente – especialmente se você possui fundos nesse site ou planeja movimentar fundos por meio dessa corretora. Mesmo que uma única letra ou número esteja fora do lugar, pare aí mesmo!

# Como posso me proteger para diminuir a chance de cair em um golpe?

## Recuse ofertas com taxas



Se uma oferta de criptomoeda exigir uma taxa inicial, recuse imediatamente – especialmente se a “oferta” envolver uma taxa a ser paga em criptomoeda. Muitas oportunidades de investimento aparentemente empolgantes no espaço cripto são fraudes. Antes de investir em qualquer coisa, verifique o site da empresa para entender como eles protegem seus clientes. Você também pode verificar as avaliações de outros investidores para obter uma direção mais clara.

A adoção cada vez maior de criptomoedas vem com o desafio de evitar golpistas e seus assaltos. Embora existam alguns projetos verdadeiramente promissores no mercado, é mais seguro aderir ao velho ditado: “Se parece bom demais para ser verdade, provavelmente é”.

Se você se deparar com um novo projeto, reserve um tempo para fazer sua própria pesquisa, procurar análises de investidores, verificar atentamente quaisquer incoerências ou detalhes suspeitos – e preste atenção aos avisos de sites respeitáveis e autoridades legais. Você também deve tomar as medidas certas para garantir que sua carteira esteja protegida com autenticação em várias etapas e tenha chaves de segurança fortes que são armazenadas de forma segura. Por fim, nunca compartilhe sua chave privada com terceiros não confiáveis.



# 5

## Como sabemos que a Bitget é segura e confiável?

# Como sabemos que a Bitget é segura e confiável?



A Bitget recebeu licenças regulatórias dos EUA, Canadá e Austrália, certificando que é uma corretora confiável. Com relação à segurança, a corretora também nunca foi hackeada.



A Bitget recebeu 12 classificações A+ do SSL Labs, e a equipe técnica está constantemente monitorando os servidores em busca de possíveis vulnerabilidades e ataques para proteger todas as credenciais de usuário na plataforma da Bitget.



# 6

## Whitelist de emails oficiais da Bitget

# Whitelist de emails oficiais da Bitget

Confirme que você está acessando: **www.bitget.com**



Atendimento ao cliente:
support@bitget.com



Operação quantitativa:
vip@bitget.com

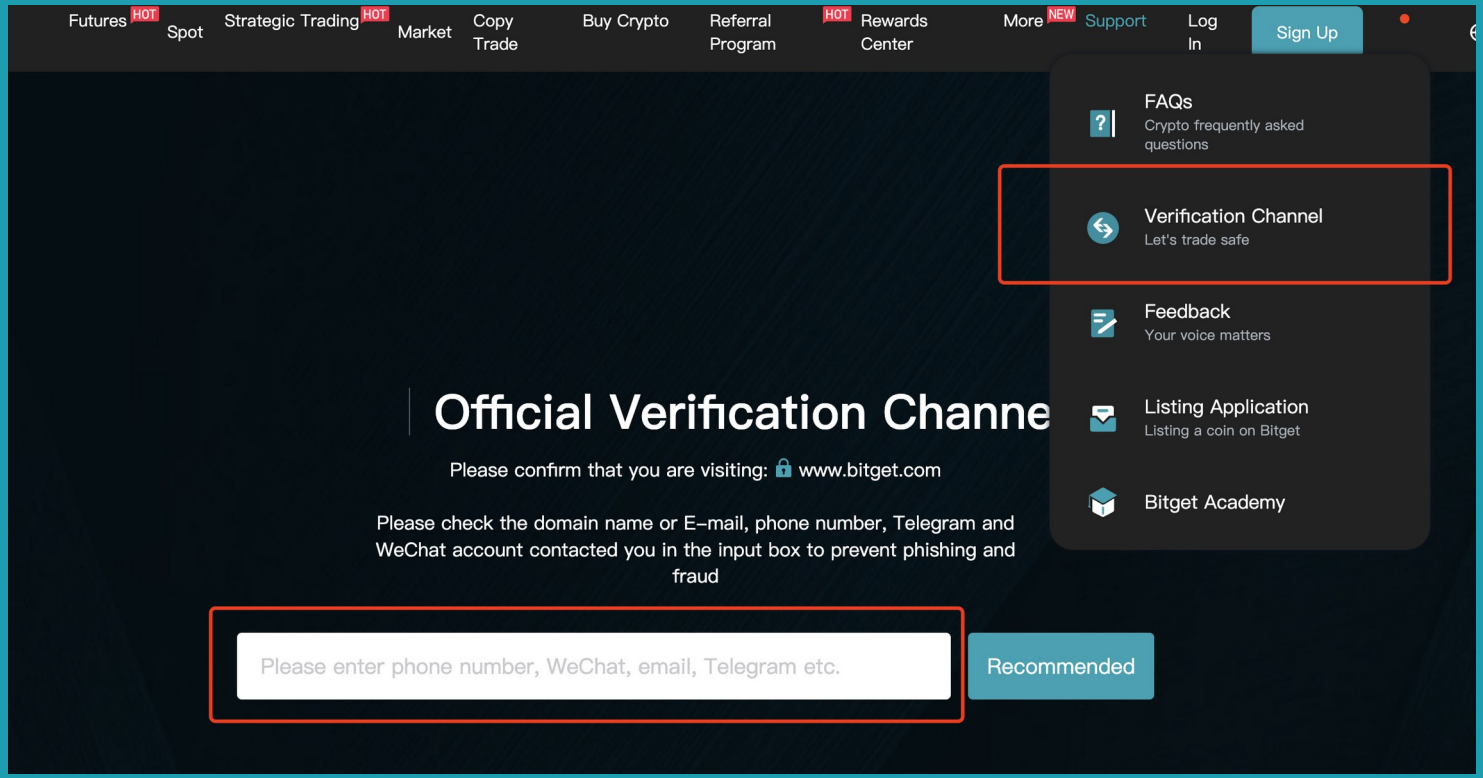


Parcerias:
BD@bitget.com



Email:
notification@noreply.bitget.com

# Canal de verificação oficial





# 7

## Golpes de criptomoedas que aconteceram de verdade

# Golpes de criptomoedas que aconteceram de verdade



Nome: FaZe Clan
Tipo de golpe: Pump and dump
Ano: 2021
Valor perdido: US$30.000

Uma organização de eSports de sucesso com o nome de FaZe Clan mostrou seu apoio online para uma nova criptomoeda chamada “Save the Kids” (KIDS). Membros influentes com uma grande base de seguidores, como RiceGum e Sommer Ray, promoveram o novo 'site de tokens (que não existe mais no momento da redação) em suas contas de redes sociais, alegando que o projeto estava ajudando a construir um mundo melhor para as crianças e prometeu doar uma parte dos rendimentos do token para caridade.

Muitos fãs compraram o token e “bombearam” dinheiro para esse esquema de cripto de caridade, acreditando que seu investimento estava protegido devido aos influenciadores de alto perfil mostrando seu apoio. Infelizmente, todo o dinheiro deles desapareceu quase da noite para o dia.

À medida que as acusações cresciam, o FaZe Clan demitiu e suspendeu vários membros que supostamente estavam envolvidos com o golpe.

# Lição aprendida

- Não importa quem esteja promovendo um novo projeto de criptomoeda, certifique-se de fazer sua própria pesquisa antes de investir.
- Mesmo que pareça por uma boa causa, seja cético em relação a novos projetos quando houver pouca ou nenhuma informação disponível.

# Golpes de criptomoedas que aconteceram de verdade



Nome: OmiseGo
Tipo de golpe: Airdrop
Ano: 2017
Valor perdido: US$56.000

O valor envolvido é relativamente pequeno em comparação com outros golpes. OmiseGo ocorreu antes que as criptomoedas chegassem ao hype de hoje, portanto, foi um golpe relativamente grande, levando em consideração o contexto e o sentimento do mercado na época.

A equipe de gestão da OmiseGo planejava fazer um Airdrop do seu token (OMG) em setembro de 2017, mas adiou por um motivo desconhecido. A notícia, no entanto, já tinha se espalhado, e a campanha de Airdrop já tinha ganhado uma popularidade significativa em plataformas de redes sociais como Twitter e Telegram.

Os golpistas decidiram tirar proveito da popularidade criando contas falsas no Twitter e sites para enganar usuários desavisados, para que entregassem suas chaves privadas.

O golpe foi detectado depois que cerca de 300 tokens ETH foram roubados dos participantes, avaliados na época em torno de US$56.000. No auge do mercado de alta mais recente, isso teria sido igual a US$1,45 milhão e, convertido para o valor de hoje, no momento da redação, seria igual a US$570.000.

# Lição aprendida

- Não importa quanto você esteja empolgado com relação a um projeto, sempre verifique as fontes oficiais para obter mais informações e atualizações.

- Nunca envie suas chaves privadas para contas de redes sociais de ninguém. Nem mesmo para canais oficiais.

# Obrigado!

**www.bitget.com**

