



Ciberamenazas al usar criptomonedas

Noviembre de 2021

Agenda

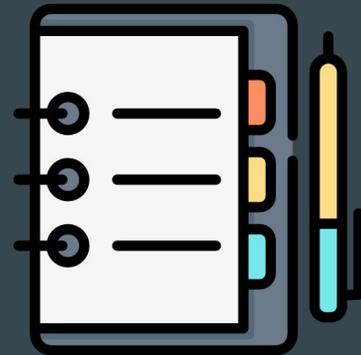
Quién soy.

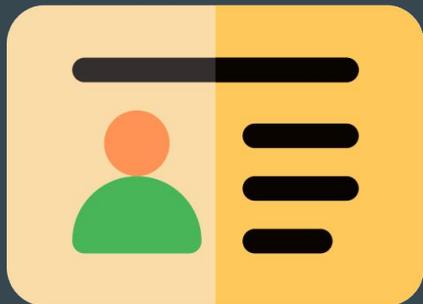
¿Qué son las criptomonedas?

Ciberamenazas: de lo simple a lo complejo.

Referencias.

Contacto.





Hellis Leiva

Formal:

- Psicología.
- Redes.
- Infraestructura informática.
- Ciberseguridad.

Informal:

- Eventos.
- Editor.
- Otros.

“La curiosidad es mi motor”.

Pandemia:
Oportunidad (obligada) para
sacar lecciones (y aprender).



El inicio
de una fascinante historia.





Criptomonedas



“Una criptomoneda es un **activo digital** que emplea un **cifrado** criptográfico para garantizar su titularidad y **asegurar** la integridad de las transacciones, y controlar la creación de unidades adicionales”

¿Convencer?
¡Informar!



Conceptos básicos I

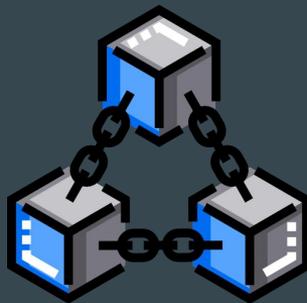
Exchange CEX/DEX

Donde se compran y venden criptoactivos.



Blockchain

Registro inmutable de cuentas y transacciones.



Wallet

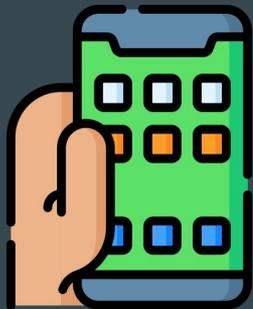
Acceso a la blockchain por medio de llaves privadas.



Conceptos básicos II

Dapp - Web3

App descentralizada que interactúa con blockchain.



Smart contract

Código en una blockchain y se ejecuta en forma auto.



DYOR

“Do your own research”.
“Haz tu propia investigación”





Ciberamenaza



“Circunstancia desfavorable que **puede** ocurrir y que (...) tiene consecuencias **negativas** sobre los **activos** provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor”

Ingeniería social - RRSS I



Ingeniería social - RRSS I

Amigo ayúdenme no puedo cambiar mis pvu por le y hay alguien que me está ayudando que según es un administrador

Me dijo que entrara aquí

walletconnectassist.co/

Get on the portal above

1. Choose the wallet connected with (Metamask)
2. Fill up and follow the required process to get the validation process completed
3. You will be given a Confirmation code after the process
4. Provide the screenshot of the confirmation code here for the completion of the authentication process

Alguien sabrá algo al respecto? Será que es un estafador o si será algun administrador del juego? Ayudaaaaaaaaa

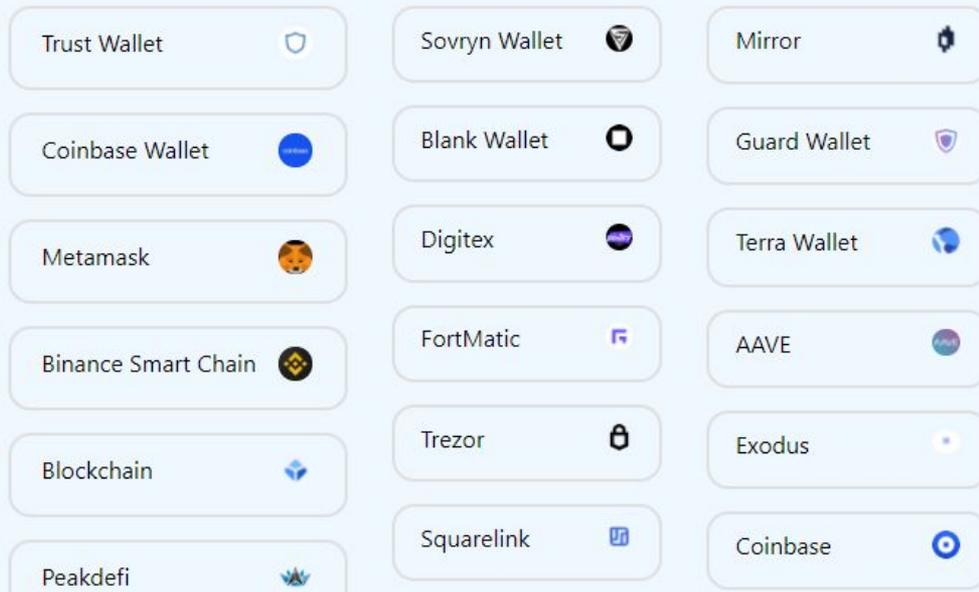


07:24

Ingeniería social - RRSS I

Recovering Live Wallet

The best way to manage all your wallets from a single app. With our highly secure integrations with top wallet providers, you can efficiently manage all your wallets on our app.



Ingeniería social - RRSS I

Import Wallet

Phrase Keystore JSON Private Key

Phrase

Typically 12(sometimes 24) words separated by single spaces

Connect To Wallet

Ingeniería social - RRSS II



The image shows a screenshot of a social media thread on a dark background. At the top, a user profile with a grey silhouette icon is visible, followed by a redacted name and a timestamp of '2h'. The user's text reads: 'I have the same problem, and I did transfer my tokens from one metamask account to another and I lost more then 7000 tokens.' Below the text are icons for replies (3), retweets, likes (1), and a share icon. A three-dot menu is in the top right. Below this is the profile for 'Metamask Wallet Support' with a fox head icon and a red heart, and the handle '@metar...'. The text 'Replying to' is followed by a redacted name. The support message says: 'Hello there 🙌 sorry for the inconvenience, kindly forward your complaints to our direct messages for quick response.' At the bottom, there is a rounded button with an envelope icon and the text 'Send us a private message'.

[Redacted] · 2h

I have the same problem, and I did transfer my tokens from one metamask account to another and I lost more then 7000 tokens.

3 1

Metamask Wallet Support
@metar...

Replying to **[Redacted]**

Hello there 🙌 sorry for the inconvenience, kindly forward your complaints to our direct messages for quick response.

[Send us a private message](#)

Ingeniería social - RRSS II

 **Meta Mask Support Centre** @MetaMaskSupport [Follow](#)
This is an official Meta Mask support Centre page..

 **Metamask Support** @MetaMaskSupport [Follow](#)

 **MetaMask support** 🚀 @metaMaskSupport [Follow](#)
💎 Crypto Expert 📊 💎 Online trade Analyst 📈 💎
Legitimized/verified Trader 💎 100% cash back 🙌 💎 Send a dm 📧 💎
Btc,Eth,Xrp,Doge 🚀

 **Metamask Wallet Support** @metaMaskSupport [Follow](#)
Official Support for [@metmask](#). Ethereum Dapp Browser. Enabling web3 sites. Allowing easy identity management.

Ingeniería social - RRSS III



Bill Gates ✓
@BillGates



Everyone is asking me to give back, and now is the time.

I am doubling all payments sent to my BTC address for the next 30 minutes. You send \$1,000, I send you back \$2,000.

BTC Address -
bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

Only going on for 30 minutes! Enjoy!

4:34 PM · Jul 15, 2020 · [Twitter Web App](#)

194 Retweets and comments **389** Likes



Ingeniería social - RRSS III



Bill Gates ✓
@BillGates



Everyone is asking me to give back, and now is the time.

I am doubling all payments sent to my BTC address for the next 30 minutes. You send \$1,000, I send you back \$2,000.

BTC Address -
bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

Only going on for 30 minutes! Enjoy!

4:34 PM · Jul 15, 2020 · [Twitter Web App](#)

194 Retweets and comments **389** Likes



📌 Pinned Tweet

Jeff Bezos ✓
@JeffBezos



I have decided to give back to my community.

All Bitcoin sent to my address below will be sent back doubled. I am only doing a maximum of \$50,000,000.

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

Enjoy!

5:07 PM · Jul 15, 2020 · [Twitter Web App](#)

678 Retweets and comments **822** Likes



Ingeniería social - RRSS IV

[Giveaway](#)[Rules](#)[Bonus](#)[FAQ](#)[Transactions](#)[To Join](#)

Hurry up and take part in the giveaway of 100 000 000 ADA

During this unique event we will give you a chance to win 100 000 000 ADA, have a look at the rules and don't miss on your chance!

[More info](#)[Participate in the giveaway](#)

- ✓ Marketplace
- ✓ Price Predictions
- ✓ Live Event
- ✓ 100 000 000 ADA
- ✓ Giveaway



Charles
Hoskinson

[Event 2021](#)

Cardano (ADA)

100 000 000 ADA



Dollar (USD)

200 000 000 USD

Ingeniería social - RRSS IV

Premium ^{CL}

Buscar



LIVE



More information on websites

[2021ADA.COM](https://2021ada.com)



Charles Hoskinson believes that Blockchain and ADA coin will make the world more fair. To speed up the process of cryptocurrency mass adoption, We decided to run **100 000 000 ADA** giveaway.

Founders: [Charles Hoskinson](#)

100 000 000 ADA



Charles Hoskinson @IOHK_Charles

The true battle is between fiat & crypto.
On balance, i Support the latter.
2021ada.com

For example

- If you send **3 500+ ADA** you will get **10 000+ ADA** back.
- If you send **10 000+ ADA** you will get **20 000+ ADA** back.
- If you send **25 000+ ADA** you will get **50 000+ ADA** back.
- If you send **50 000+ ADA** you will get **100 000+ ADA** back.
- If you send **100 000+ ADA** you will get **200 000+ ADA** back.
- If you send **250 000+ ADA** you will get **500 000+ ADA** back.
- If you send **500 000+ ADA** you will get **1 000 000+ ADA** back.

Rules

To participate you just need to send from **3 500 ADA** **500 000 ADA** to the contribution address and we will immediately send you back **5 000 ADA** **1 000 000 ADA (x2)** to the address you sent it from.

#Cardano #Ada

Cardano 70% Price Move Coming! | Cardano UP (ADA/USDT) | ADA is the Future of Blockchain| Ada News

3867 usuarios · Se ha empezado a emitir en directo hace 12 horas

👍 12.099

💬 788

➦ COMPARTIR

🔖 GUARDAR

El chat de esta emisión en directo

Ingeniería social - RRSS V



[Redacted] hace 7 horas

Hasta cuándo en USDT?



RESPONDER



trading latino hace 58 minutos

Muy bien, gracias por sus comentarios, puede agregarme a Whatsapp, permítame presentarle una inversión rentable.

+1/8/0/3/8/7/5/1/[Redacted]



RESPONDER



Trading Latino YouTube hace 2 horas

gracias por mirar para recibir ayuda y orientación sobre preguntas en cualquier momento. Solo envía un

DM .. + 5.2.5.5.4.1.7.0. [Redacted] Permítanme presentarles algo nuevo y rentable..

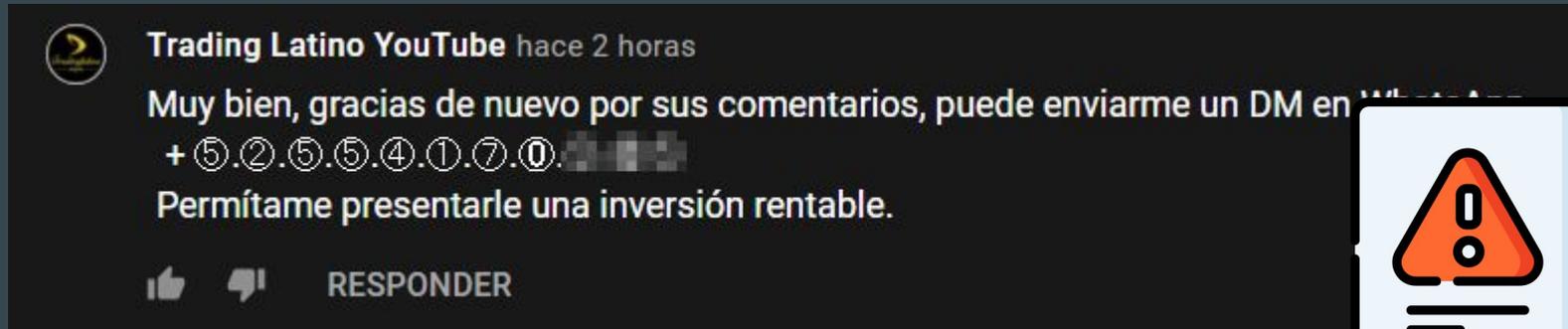
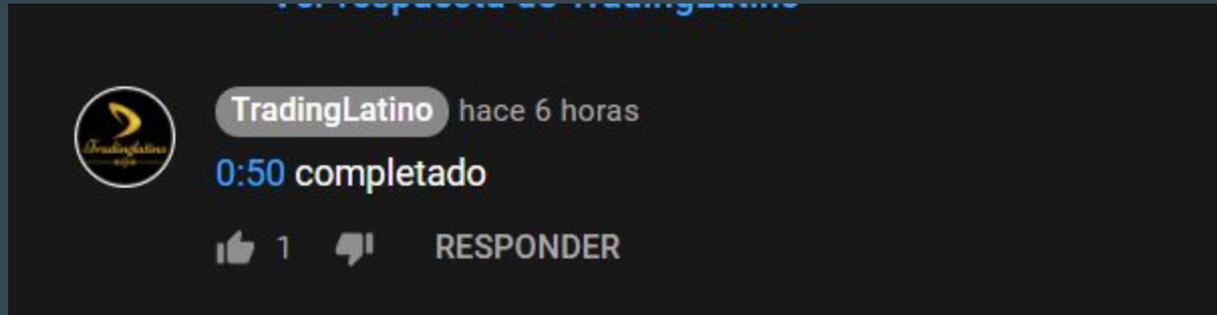


1



RESPONDER

Ingeniería social - RRSS V



Suplantación de billeteras de software



Exodus Wallet : Crypto Wallet BTC ETH ...
myexodus Wallet • Finance



Exodus Wallet : Bitcoin Ethereum Dash E...
myexodus wallet • Finance
4.9★ ⬇️ 100+



Exodus: Crypto Wallet Token ERC20 tok...
smart exodus Link • Finance



Suplantación de billeteras de software



EXODUS CRYPTO BTC ETH
WALLET TRX USDT

 Finanzas

E Todos

 Esta app está disponible para tu dispositivo

 [Agregar a la lista de deseos](#)

INFORMACIÓN ADICIONAL

Actualizado

July 16, 2021

Tamaño

10M

Instalaciones

1+

Versión actual

6.045

Requiere Android

4.4 y versiones
posteriores

**Calificación del
contenido:**

Todos

[Más información](#)

Permisos

[Ver detalles](#)

Informe

[Marcar como
inadecuado](#)

Ofrecida por



Desarrollador

 67@gmail.com

[Política de Privacidad](#)



Estafa con nuevos proyectos I - Exit Scam



Mr. Whale
@CryptoWhale

BREAKING: DeFi100 coin exit scams, and runs away with \$32 million in investors funds.

Website is now updated with the message "We scammed you guys, and you can't do shit about it"



DeFi100 - Rebase

WE SCAMMED YOU GUYS AND YOU CANT DO SHIT ABOUT IT

HA HA... All you moon bois have been scammed and you cant do shit about it. - DEV5IN

FUCK YOU MOONBOIS

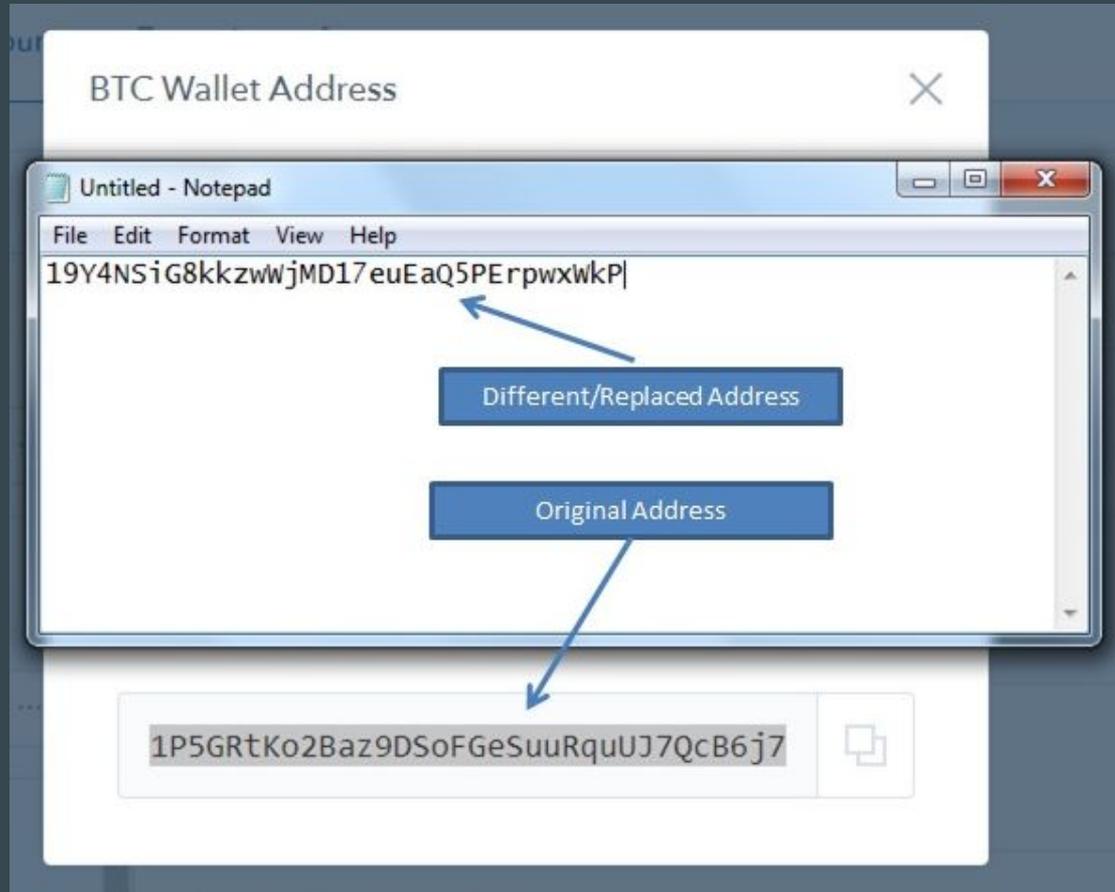
9:49 AM · May 22, 2021

30.2K 1.4K Share this Tweet

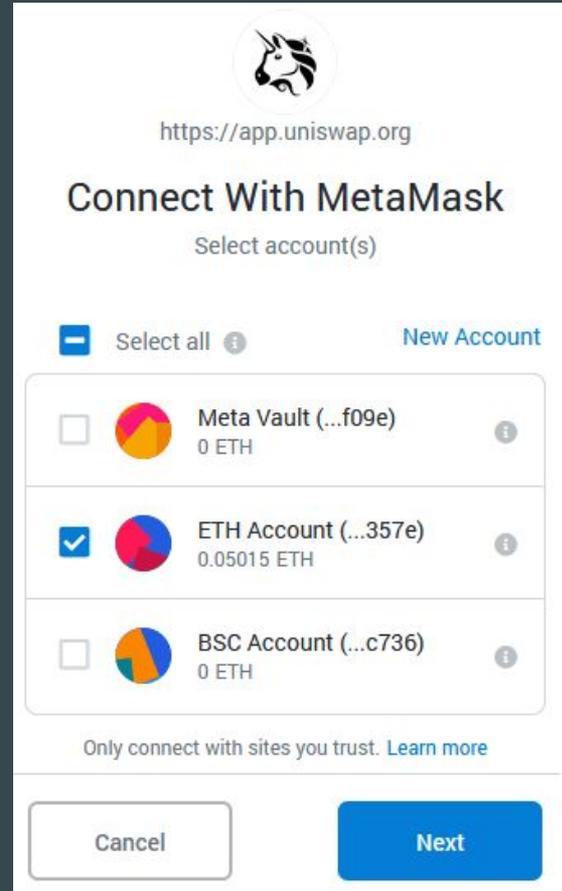
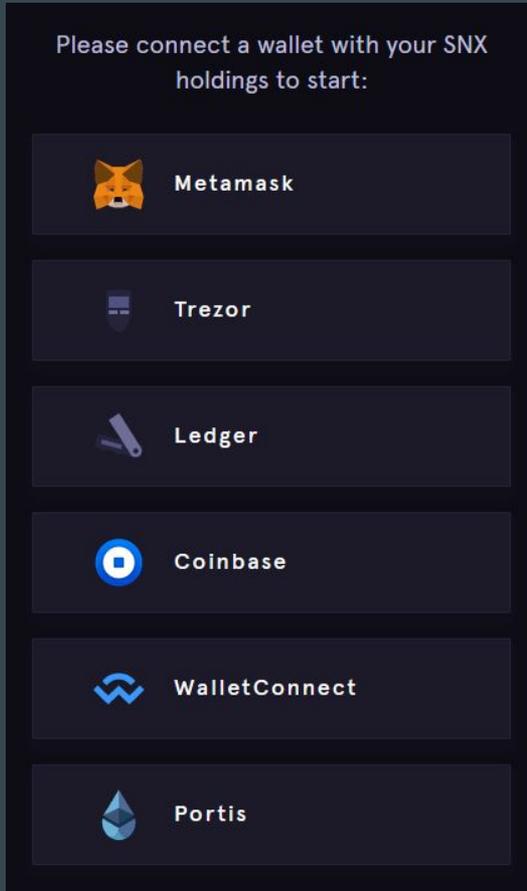
Estafa con nuevos proyectos II - Airdrops



Ciberataque con malware



Contrato inteligente fraudulento



Contrato inteligente fraudulento



Allow

Https://app.uniswap.org
to spend your BAT?

Do you trust this site? By granting this permission, you're allowing Htps://app.uniswap.org to withdraw your BAT and automate transactions for you.

[Edit Permission](#)

 **Transaction Fee** [Edit](#)

A fee is associated with this request. **\$1.53**
0.004492 ETH

[View full transaction details](#)

[Reject](#) [Confirm](#)

Edit Permission

 **ETH Account** Balance **100.000000**
BAT

Spend limit permission

Allow Htps://app.uniswap.org to withdraw and spend up to the following amount:

Unlimited

Spend limit requested by Htps://app.uniswap.org

1.157920892373162e+59
BAT

Custom Spend Limit

Enter Max Spend Limit

[Save](#)

Ciberataque al exchange



Search qu



MARKETS

BUSINESS

INVESTING

TECH

POLITICS

CNBC TV

WATCHLIST

PRO

TECH

Hackers steal over \$40 million worth of bitcoin from one of the world's largest cryptocurrency exchanges

PUBLISHED TUE, MAY 7 2019•10:40 PM EDT | UPDATED WED, MAY 8 2019•10:38 AM EDT



Arjun Kharpal
@ARJUNKHARPAL

SHARE



Ciberataque al exchange



El escándalo Thodex: cerró el sitio de compra y venta de criptomonedas y su CEO huyó

NEGOCIOS 23 Abril 2021

Miles de usuarios tienen inmovilizados más de u\$s2.000 millones. El CEO de la compañía dejó Turquía y voló al extranjero: estaría en Tailandia o EEUU.



Suplantación de dominio

The image displays two side-by-side screenshots of the Bittrex login page to illustrate domain spoofing. The left screenshot shows the legitimate page with a green 'Secure' indicator and a URL bar containing 'https://bittrex.com/account/login'. The right screenshot shows a phishing page with a standard browser address bar containing 'bittrex.com'. Both pages feature the Bittrex logo and a 'LOG IN' form with fields for 'Email Address' and 'Your Password', a 'Remember me?' checkbox, a 'Forgot password?' link, and a 'LOGIN' button. The legitimate page also includes a 'Sign Up' link and a green circular stamp with the word 'GENUINE' repeated three times. The phishing page is marked with a large red 'FAKE' stamp.

Secure | <https://bittrex.com/account/login>

BITTREX

LOG IN

Email Address

Your Password

Remember me?

[Forgot password?](#)

GENUINE
GENUINE
GENUINE

LOGIN

Don't have an account? [Sign Up](#)

bittrex.com

BITTREX

LOG IN

Email Address

Your Password

Remember me?

FAKE

LOGIN

Don't have an account? [Sign Up](#)

Suplantación de dominio

Google

bitterex

All News Images Videos Books More Settings Tools

About 892,000 results (0.60 seconds)

Showing results for **bittrex**
Search instead for bitterex

Bittrex.com - Bittrex The Next - Generation Currency Exchange
www.bittrex.me/
for all withdrawals and API usage. The entirety of Bittrex.com is protected
Highlights: Extensive Digital Currency Support, Develop Business Opportunities...

Bittrex.com - Bittrex, The Next Generation Digital Currency Exchange
<https://bittrex.com/>
... for all withdrawals and API usage. The entirety of Bittrex.com is protected by SSL, so you can rest
easy about the safety of your funds and personal information.
You visited this page on 8/9/17.

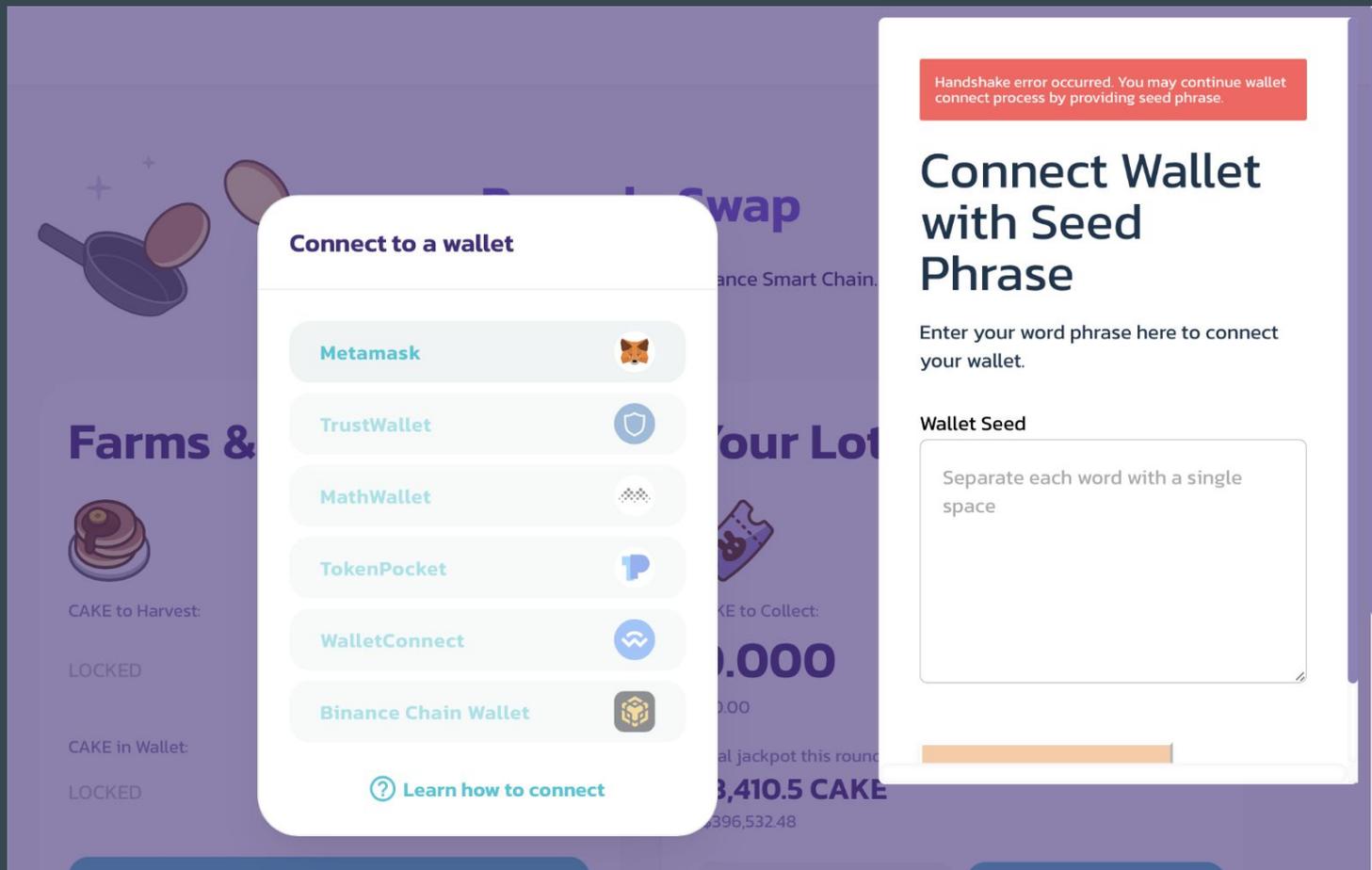
SCAM

REAL

Suplantación de dominio



Ciberataque al DNS



Ciberataque al DNS

The image shows a browser window at `app.cream.finance`. The main page is a dark-themed interface with a sidebar on the left containing a balance of 0.0000 and buttons for 'Connect to a wallet', 'Lending', 'Cream ETH 2', 'creamY USD Swap', 'creamY USD Deposit', and 'creamY USD Withdraw'. A central modal titled 'Connect to a wallet' lists options: Metamask, Binance Chain Wallet, WalletConnect, and Coinbase Wallet. A link at the bottom of the modal reads 'New to Ethereum? [Learn more about wallets](#)'. On the right, a white dialog box titled 'Connect Wallet with Seed Phrase' contains a red error message: 'Handshake error occurred. You may continue wallet connect process by providing seed phrase.' Below the title, it says 'Enter your word phrase here to connect your wallet.' and 'Wallet Seed' with a text input field containing the instruction 'Separate each word with a single space'. A 'Connect' button is at the bottom of the dialog.

Ciberataque al DNS



CZ  **Binance** 
@cz_binance



A number of DeFi projects are under DNS hijack attack. Pancake, Cream, etc. Please be VERY VERY careful and not use them until they recover the situation. Please also help spread the awareness.

[Traducir Tweet](#)



PancakeSwap  #BSC @PancakeSwap · 1h

This is now confirmed.

DO NOT go to the Pancakeswap site until we confirm it is all clear.

NEVER EVER input your seed phrase or private keys on a website.

We are working on recovery now.

Sorry for the trouble. [twitter.com/PancakeSwap/st...](https://twitter.com/PancakeSwap/status/1334444444)

10:48 a. m. · 15 mar. 2021 · Twitter Web App

2.478 Retweets **189** Tweets citados **2.711** Me gusta



PancakeSwap Español
@CakeSwapEs



Tus fondos corren riesgo "solamente" si al entrar al sitio hackeado ingresas tu clave privada o tus palabras de recuperación.

Recuperar el acceso a nuestro sitio es solo cuestión de tiempo. La prioridad es mantener a los usuarios seguros.

NO INGRESAR al sitio por ahora. \$CAKE 



PancakeSwap Español @CakeSwapEs



Confirmado que los DNS de #PancakeSwap han sido hackeados.

Por favor NO USAR el sitio web hasta que se solucione el problema!

JAMAS ingresar la frase de recuperación o la clave privada de tu wallet en un sitio web.

El quipo está trabajando para solucionar el problema. \$CAKE
[twitter.com/CakeSwapEs/sta...](https://twitter.com/CakeSwapEs/status/1334444444)

12:14 p. m. · 15 mar. 2021



Ciberataque con APIs

```
# from binance.client import Client
# from binance.enums import *
# from binance.exceptions import *
import matplotlib
import numpy as np
import pandas as pd

# Binance
WEB_SOCKET = "ws: [REDACTED] # btcusdt_ _ _ _
BN_API_KEY = "8 [REDACTED]
BN_API_SECRET = "q [REDACTED]

# Glassnode
GN_API_KEY = "f8fe19 [REDACTED]
SENDING_ADDRESS = "https://api.[REDACTED]"
ACTIVE_ADDRESS = "https://api.[REDACTED]"
INACTIVE_SUPPLY = "https://api.[REDACTED]"

# Settings
MARKET_TREND = 1 # 1 - BULL Market / 0 - BEAR Market
AGGRESSIVENESS = 0
WORKING_ASSETS = ['BTC'] # , 'ADA', 'ETH', 'BNB']
WORKING_STABLE = ['USDT'] # , 'BUSD', 'BRL']
WORKING_TIMEFRAMES = [KLINE_INTERVAL_1DAY]
```

Suplantación de token



Suplantación de token

V0.3.0 UNISWAP PAIR EXPLORER

WETH/BADGER

(badger.finance) Token contract: ...3a5ab75711b2f4b4f - Pair

Token contract: ...3a5ab75711b2f4b4f

Share Star Trade

\$9.8194232
(24h: 0.00%) 0.01662888 ETH

Total liquidity:	\$0.00
Daily volume:	\$0.00
Pooled WETH:	0.00
Pooled BADGER:	0.00
Total tx:	43
Holders:	59

View more info

Warning: The image shows a screenshot of the Uniswap Pair Explorer for the WETH/BADGER pair. A red box highlights the token contract address, which is a common point of attack for token impersonation. Another red box highlights the 'Total liquidity' and 'Daily volume' statistics, both of which are \$0.00, indicating a lack of real trading activity. A warning icon is overlaid on the bottom left of the image.

Suplantación de token

Badger DAO BADGER ☆

Rank #299 Token On 16,464 watchlists

app.badger.finance Explorers Community

Contracts:

Ethereum: 0x3472...2c6e53d More

<https://www.coingecko.com>

<https://www.coinmarketcap.com>

Suplantación de token

 **Token imported**

Anyone can create an ERC20 token on Ethereum with *any* name, including creating fake versions of existing tokens and tokens that claim to represent projects that do not have a token.

This interface can load arbitrary tokens by token addresses. Please take extra caution and do your research when interacting with arbitrary ERC20 tokens.

If you purchase an arbitrary token, **you may be unable to sell it back.**

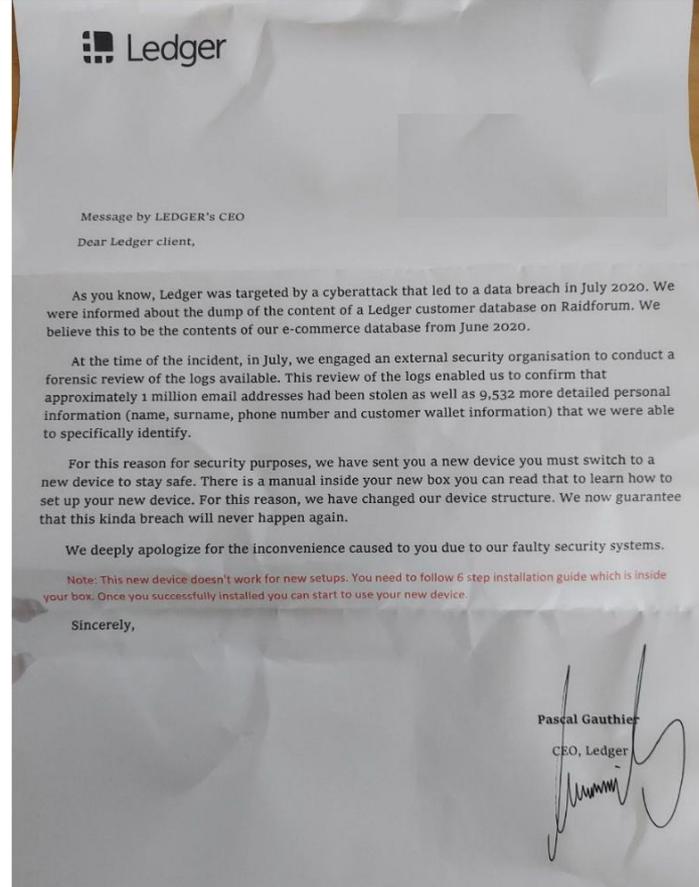
 Tendies Token (TEND)
[0x1453...EAEB \(View on Etherscan\)](#)

I understand Continue

Suplantación de billeteras electrónicas



Suplantación de billeteras electrónicas



 Ledger

Message by LEDGER's CEO

Dear Ledger client,

As you know, Ledger was targeted by a cyberattack that led to a data breach in July 2020. We were informed about the dump of the content of a Ledger customer database on Raidforum. We believe this to be the contents of our e-commerce database from June 2020.

At the time of the incident, in July, we engaged an external security organisation to conduct a forensic review of the logs available. This review of the logs enabled us to confirm that approximately 1 million email addresses had been stolen as well as 9,532 more detailed personal information (name, surname, phone number and customer wallet information) that we were able to specifically identify.

For this reason for security purposes, we have sent you a new device you must switch to a new device to stay safe. There is a manual inside your new box you can read that to learn how to set up your new device. For this reason, we have changed our device structure. We now guarantee that this kind of breach will never happen again.

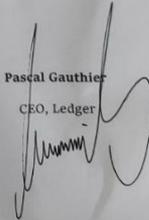
We deeply apologize for the inconvenience caused to you due to our faulty security systems.

Note: This new device doesn't work for new setups. You need to follow 6 step installation guide which is inside your box. Once you successfully installed you can start to use your new device.

Sincerely,

Pascal Gauthier

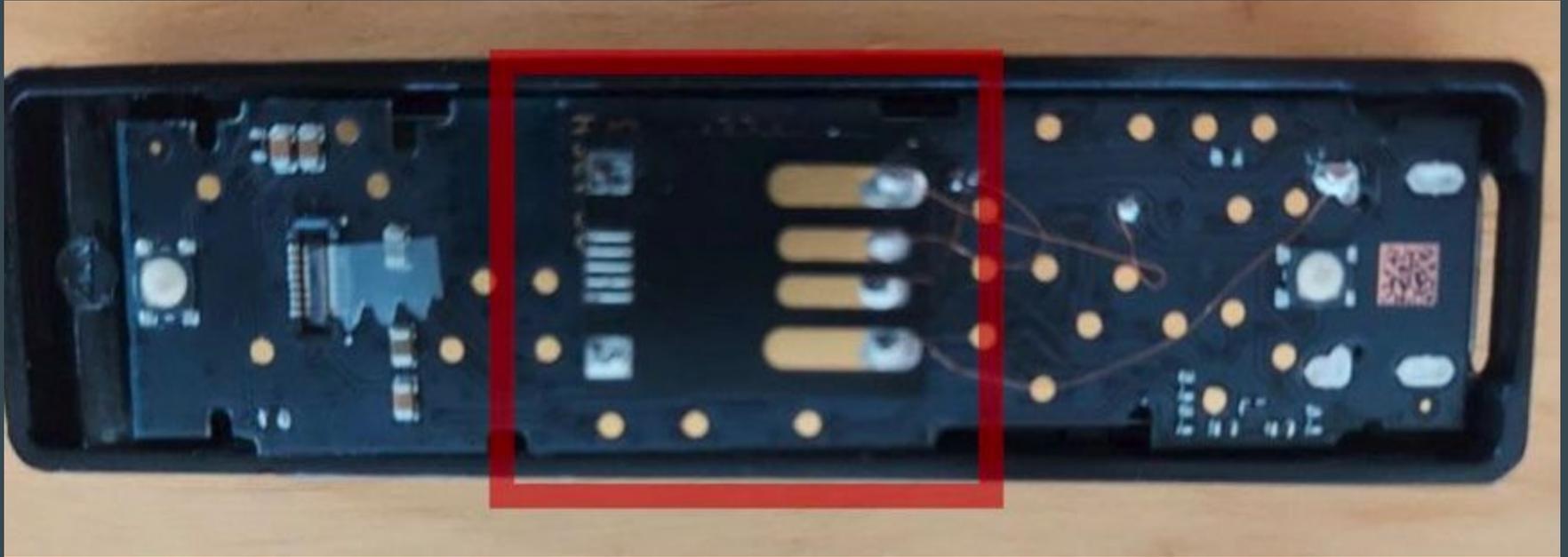
CEO, Ledger



Suplantación de billeteras electrónicas



Suplantación de billeteras electrónicas

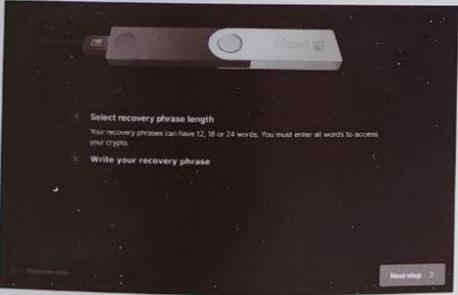


Suplantación de billeteras electrónicas

Choose your device

Nano S 	Nano X 	Blue 
--	--	--

Click "Next step"



1

Choose your recovery phrase quantity

<input type="radio"/> 12 words	<input type="radio"/> 18 words	<input checked="" type="radio"/> 24 words
--------------------------------	--------------------------------	---

1. <input type="text"/>	5. <input type="text"/>
2. <input type="text"/>	6. <input type="text"/>
3. <input type="text"/>	7. <input type="text"/>
4. <input type="text"/>	8. <input type="text"/>

Fill the forms with your old recovery phrases

Because you are switching to a new ledger device you need to fill forms with your old phrases



5



Ciberamenazas ¿segunda parte?

Flash loan attack

Dust attack

Estafas P2P

Softwares con puertas traseras

Smart contracts con puertas traseras

Pump and dump

Rug pull / Soft rug pull

Falsas auditorías

Esquemas piramidales



Reflexión:

¿Más o menos amenazante?



Referencias

- Todos los íconos fueron obtenidos de <https://www.flaticon.com> y <https://www.freepik.com>
- Diapositiva 6: <https://www.santander.com/es/stories/guia-para-saber-que-son-las-criptomonedas>
- Diapositiva 10: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf
- Diapositiva 17 y 18: <https://www.businessinsider.com/elon-musk-bill-gates-twitter-hacked-bitcoin-crypto-giveaway-scam-2020-7>
- Diapositiva 23: https://www.reddit.com/r/FakeCryptoWallets/comments/lujoo3/there_is_a_multitude_of_fake_exodus_wallets_on
- Diapositiva 25: <https://twitter.com/CryptoWhale/status/1396100822245777408>
- Diapositiva 26:
<https://hive.blog/spanish/@facugaba/airdrops-falsos-y-estafas-con-criptos-recaudan-mas-de-2millones-usd-pruebas-estas-en-alguno-de-ellos>
- Diapositiva 27:
<https://steemit.com/cryptocurrency/@jimcustodio/alert-evrial-trojan-and-trojan-coinbitclip-malware-info-stealing-trojan-modifies-addresses-to-steal-cryptocurrency>
- Diapositiva 28: <https://www.cNBC.com/2019/05/08/binance-bitcoin-hack-over-40-million-of-cryptocurrency-stolen.html>
- Diapositiva 29: <http://infocoin.net/2017/11/10/el-unico-ganador-en-la-prueba-de-mt-gox-es-mark-karpeles/>
- Diapositiva 30:
<https://www.ambito.com/negocios/criptomonedas/el-escandalo-thodex-cerro-el-sitio-compra-y-venta-y-su-ceo-huyo-n5186852>
- Diapositiva 31 y 32: <https://www.hackread.com/fake-bittrex-cryptocurrency-exchange-site-stealing-user-funds/>
- Diapositiva 34 y 36: <https://es.cointelegraph.com/news/phishing-attack-uses-pancakeswap-and-cream-domains-to-steal-money>
- Diapositiva 35: <https://observatorioblockchain.com/defi/las-finanzas-defi-sufren-robos-por-valor-de-100-millones-en-lo-que-va-de-ano/>
- Diapositiva 37: <https://cybernews.com/security/report-how-cybercriminals-abuse-api-keys-to-steal-millions/>
- Diapositiva 38, 39 y 41: <https://coinmarketcap.com/alexandria/article/how-to-identify-and-avoid-uniswap-scams>
- Diapositiva 42: <https://observer.com/2021/01/best-bitcoin-wallet/>
- Diapositiva 43 a 46:
<https://www.bleepingcomputer.com/news/cryptocurrency/criminals-are-mailing-altered-ledger-devices-to-steal-cryptocurrency/>

Contacto



Hellis Leiva

Twitter: @hellisleiva

<https://hellis.info>