Ciberamenazas al usar criptomonedas

Noviembre de 2021

Agenda

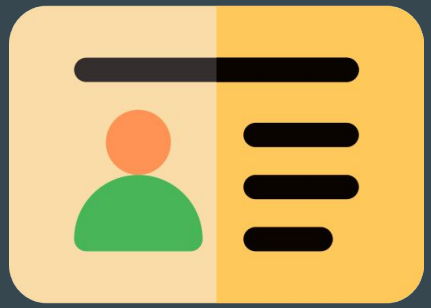
Quién soy.

¿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.

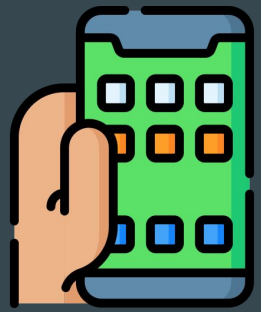
Wallet

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”

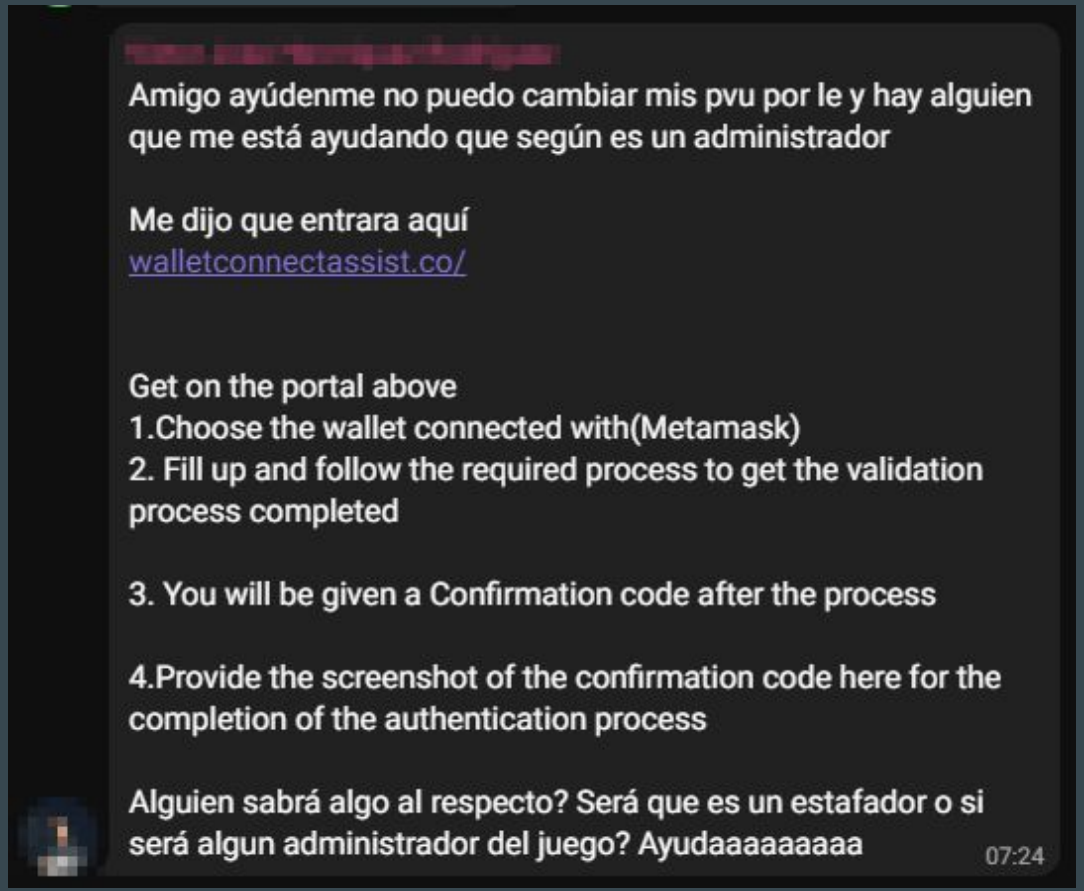
Ciberamenaza

...

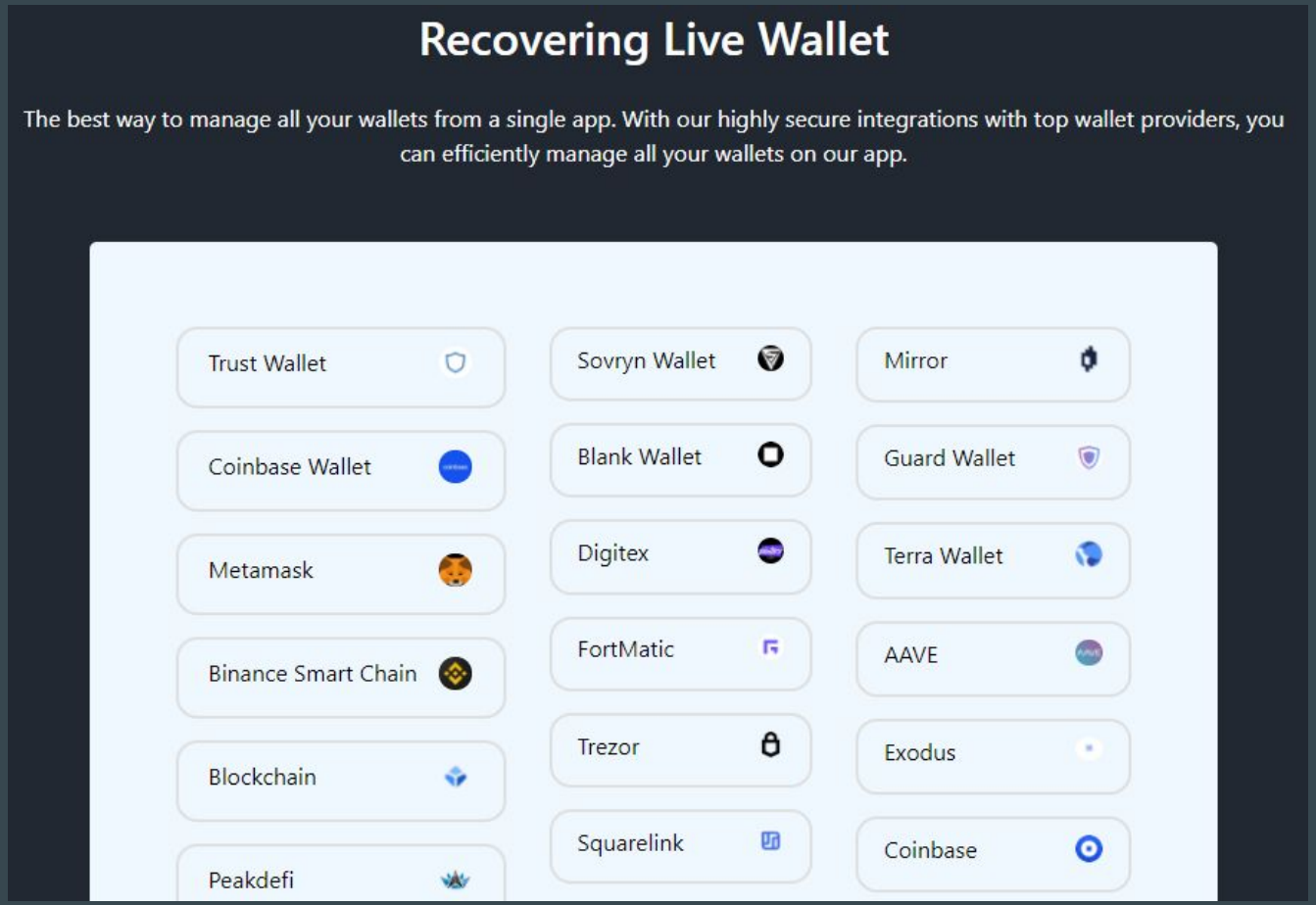
"Circunstancia desfavorable que **puede** ocurrir y que (...) tiene consecuencias **negativas** sobre los **activos** provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor"

Ingeniería social - RRSS I

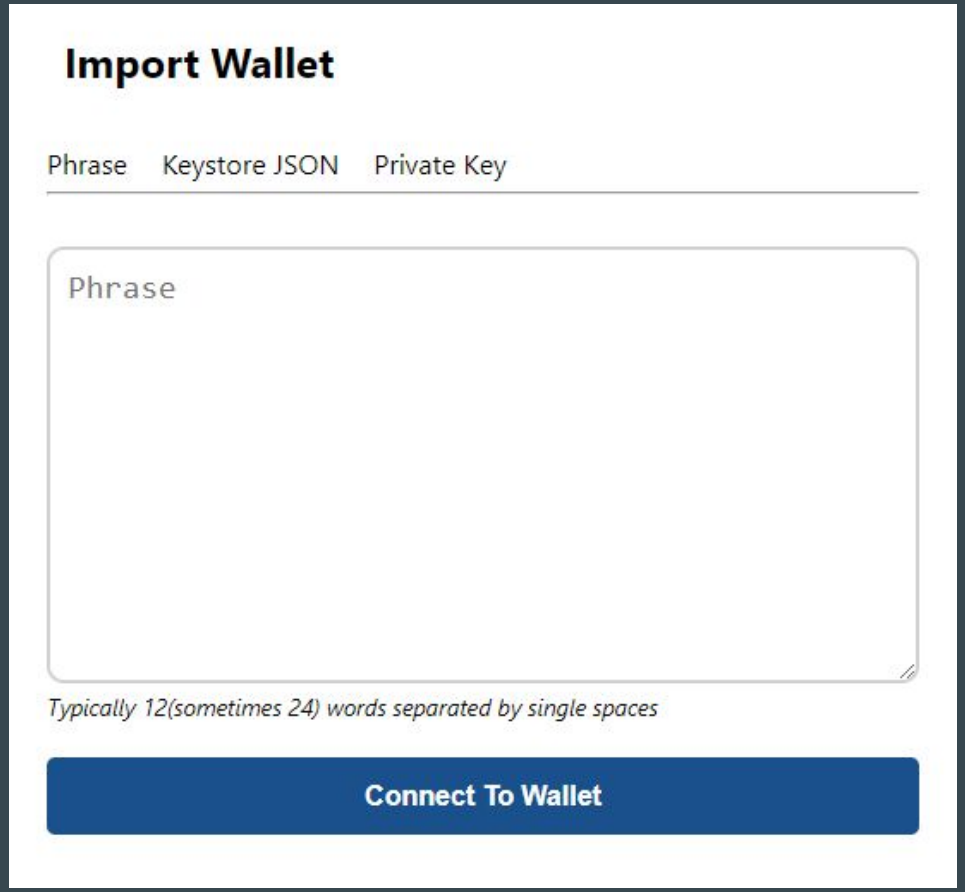
Ingeniería social - RRSS I



Ingeniería social - RRSS I

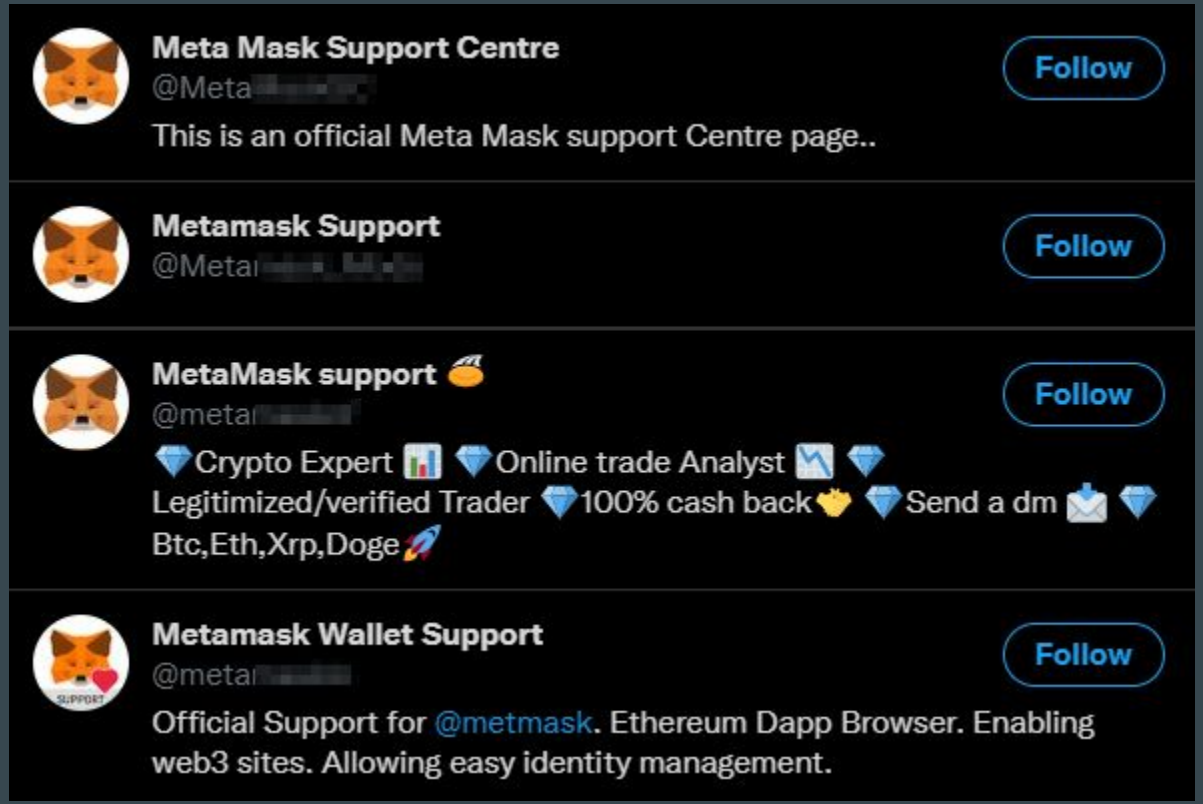


Ingeniería social - RRSS I



Ingeniería social - RRSS II

Ingeniería social - RRSS II



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

Ingeniería social - RRSS IV

CARDANO

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

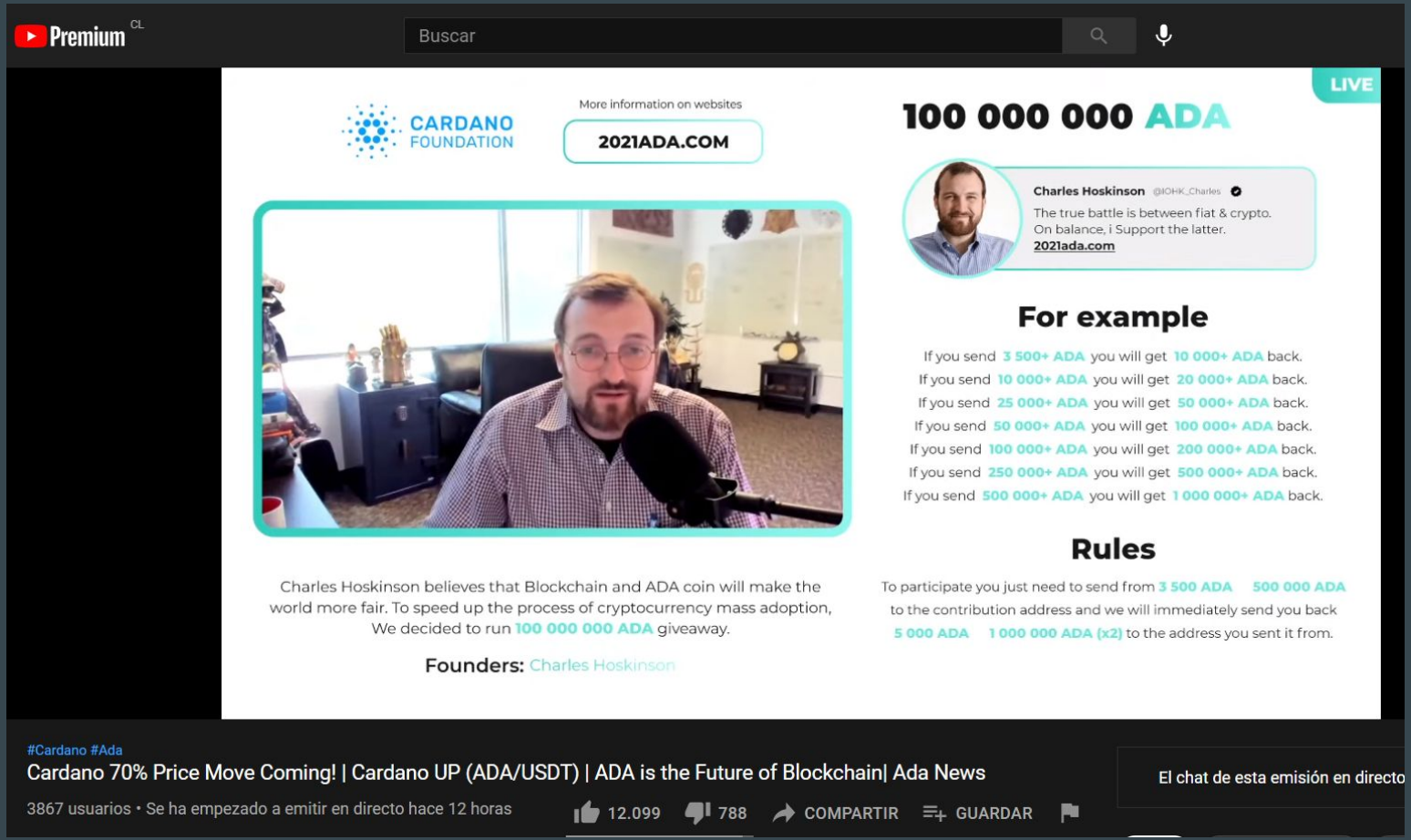
- Marketplace
- Price Predictions
- Live Event
- 100 000 000 ADA
- Giveaway

Charles Hoskinson

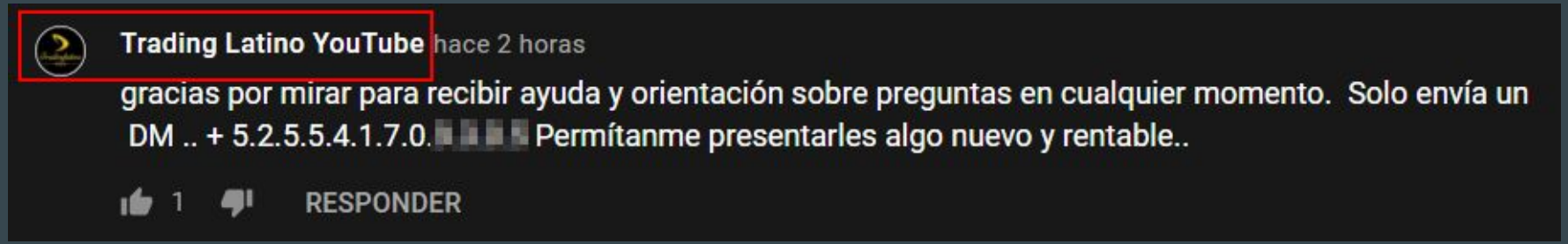
Event 2021

Cardano (ADA)	100 000 000 ADA
Dollar (USD)	200 000 000 USD

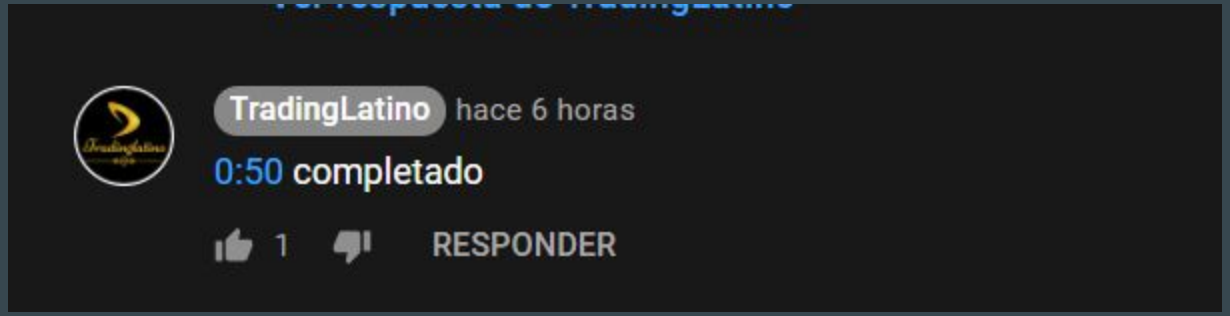
Ingeniería social - RRSS IV

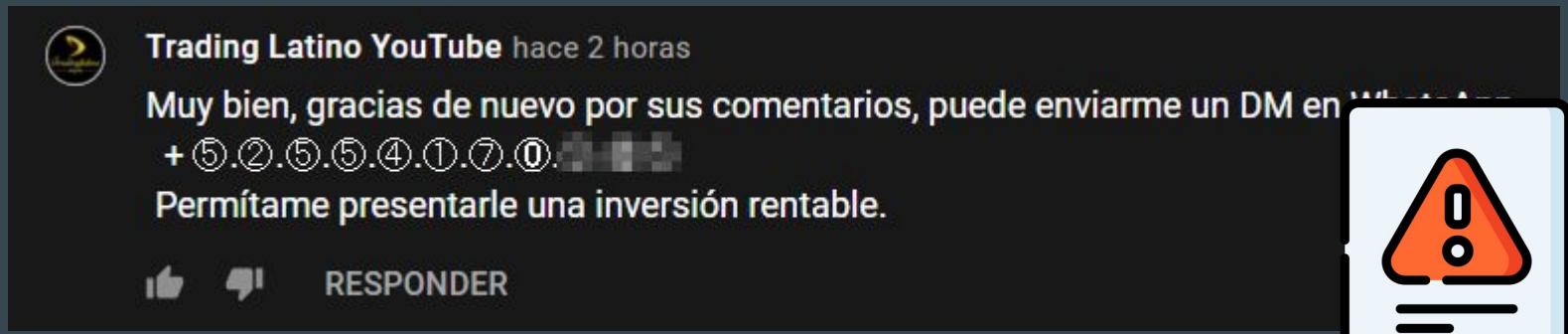


Ingeniería social - RRSS V



Ingeniería social - RRSS V





Suplantación de billeteras de software

Exodus Wallet : Crypto Wallet BTC ETH ...
[illegible] • Finance

Exodus Wallet : Bitcoin Ethereum Dash E...
[illegible] • Finance
4.9★ 100+

Exodus: Crypto Wallet Token ERC20 tok...
[illegible] • Finance

Suplantación de billeteras de software

EXODUS

EXODUS CRYPTO BTC ETH WALLET TRX USDT

[redacted] Finanzas

Todos

Esta app está disponible para tu dispositivo

Agregar a la lista de deseos

INFORMACIÓN ADICIONAL

Actualizado	Tamaño	Instalaciones
July 16, 2021	10M	1+
Versión actual	**Requiere Android**	**Calificación del contenido:**
6.045	4.4 y versiones posteriores	Todos Más información
Permisos	**Informe**	**Ofrecida por**
Ver detalles	Marcar como inadecuado	[redacted]

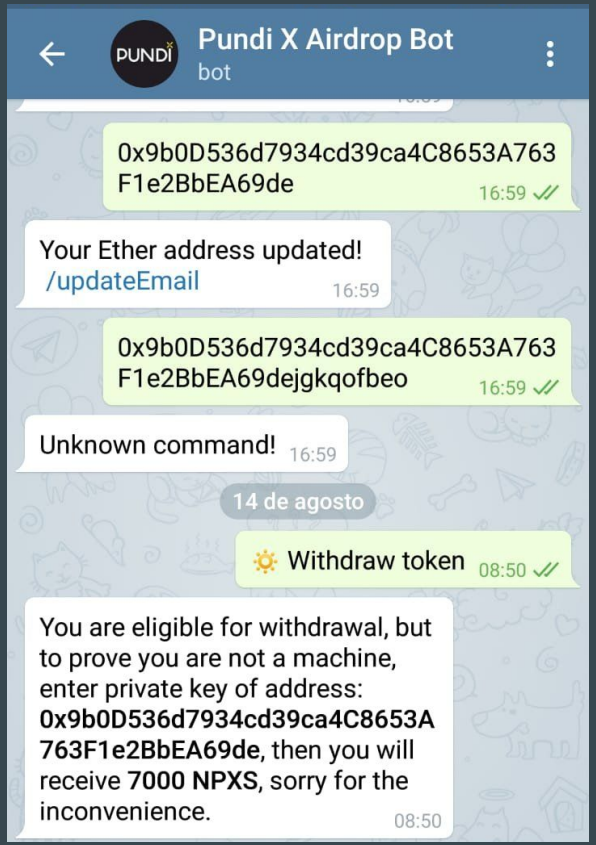
Desarrollador

[redacted]67@gmail.com

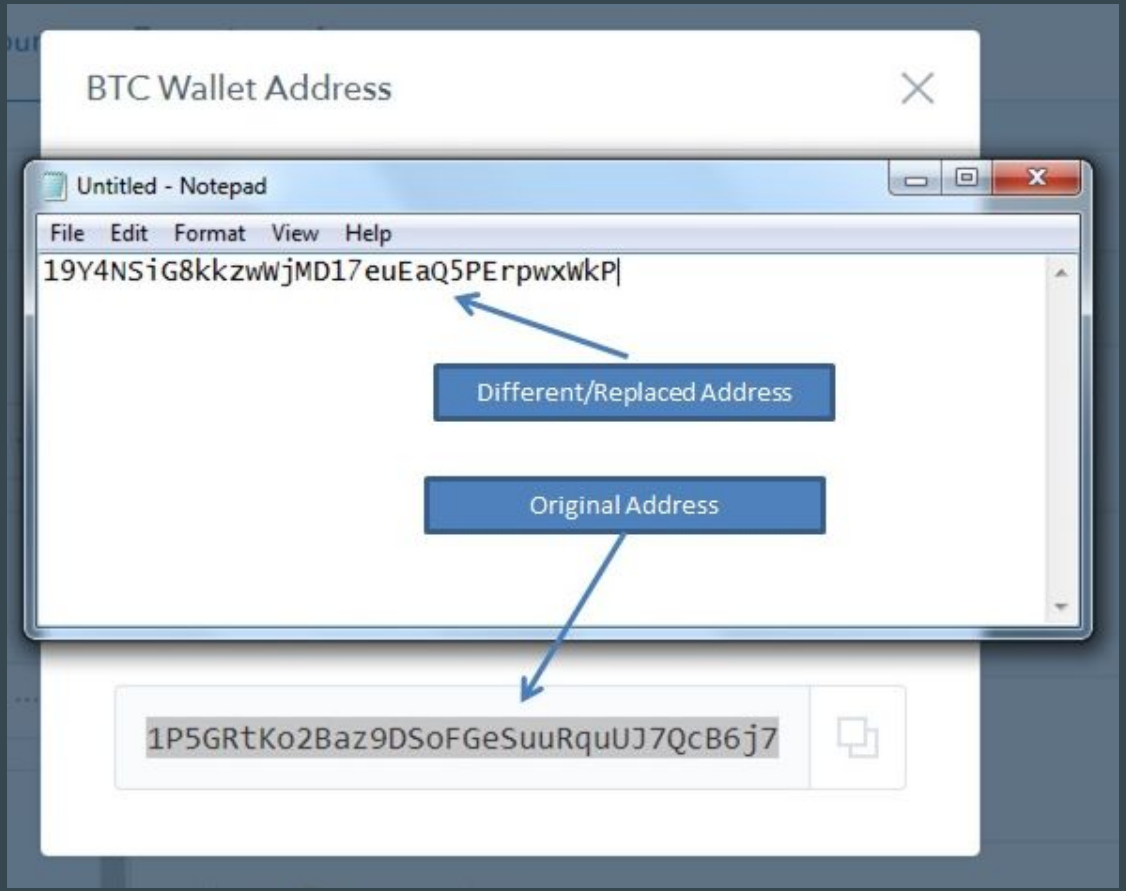
Política de Privacidad

Estafa con nuevos proyectos I - Exit Scam

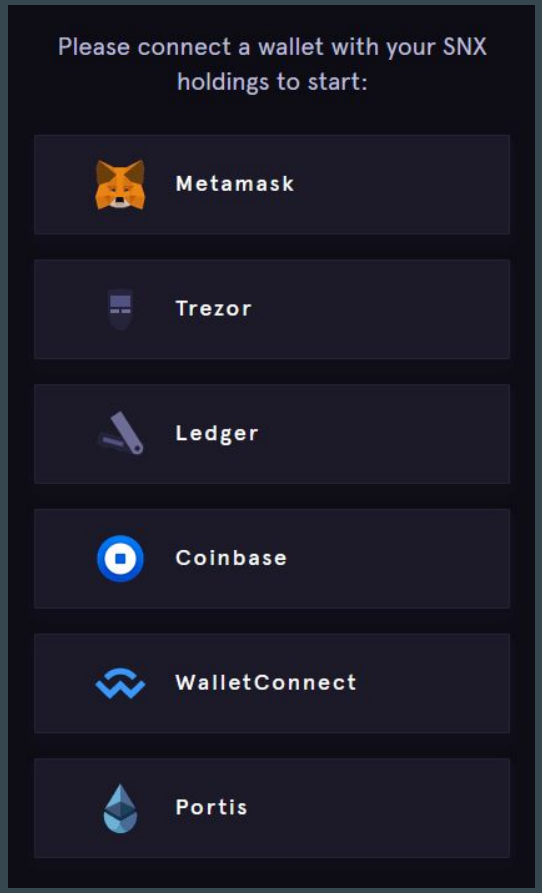
Estafa con nuevos proyectos II - Airdrops

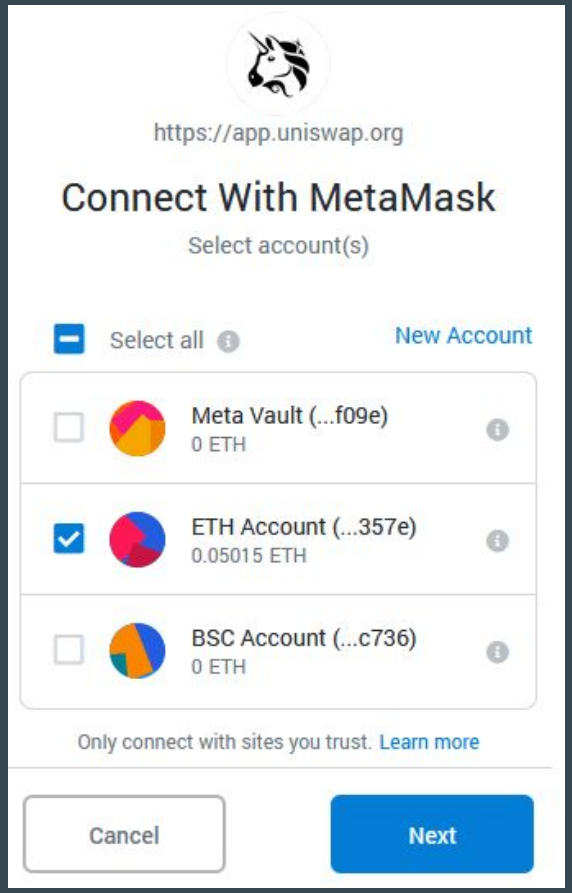


Ciberataque con malware

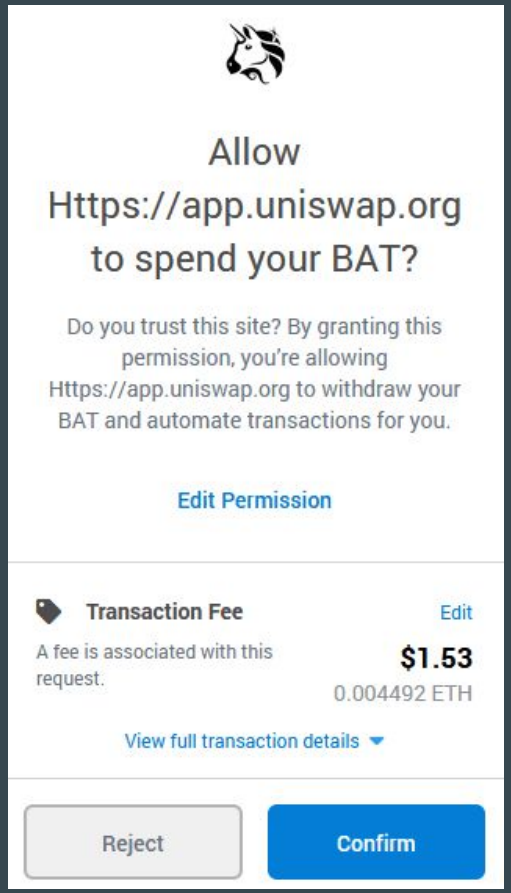


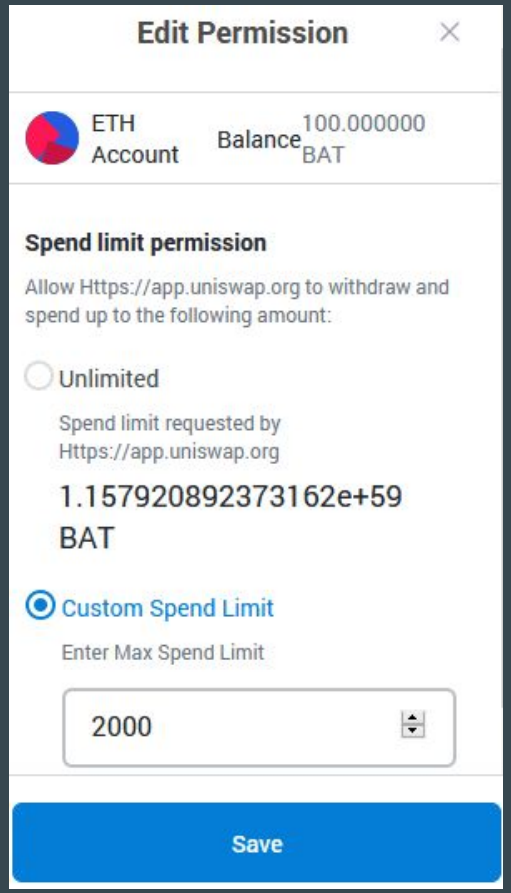
Contrato inteligente fraudulento





Contrato inteligente fraudulento





Ciberataque al exchange

CNBC

Search quo

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

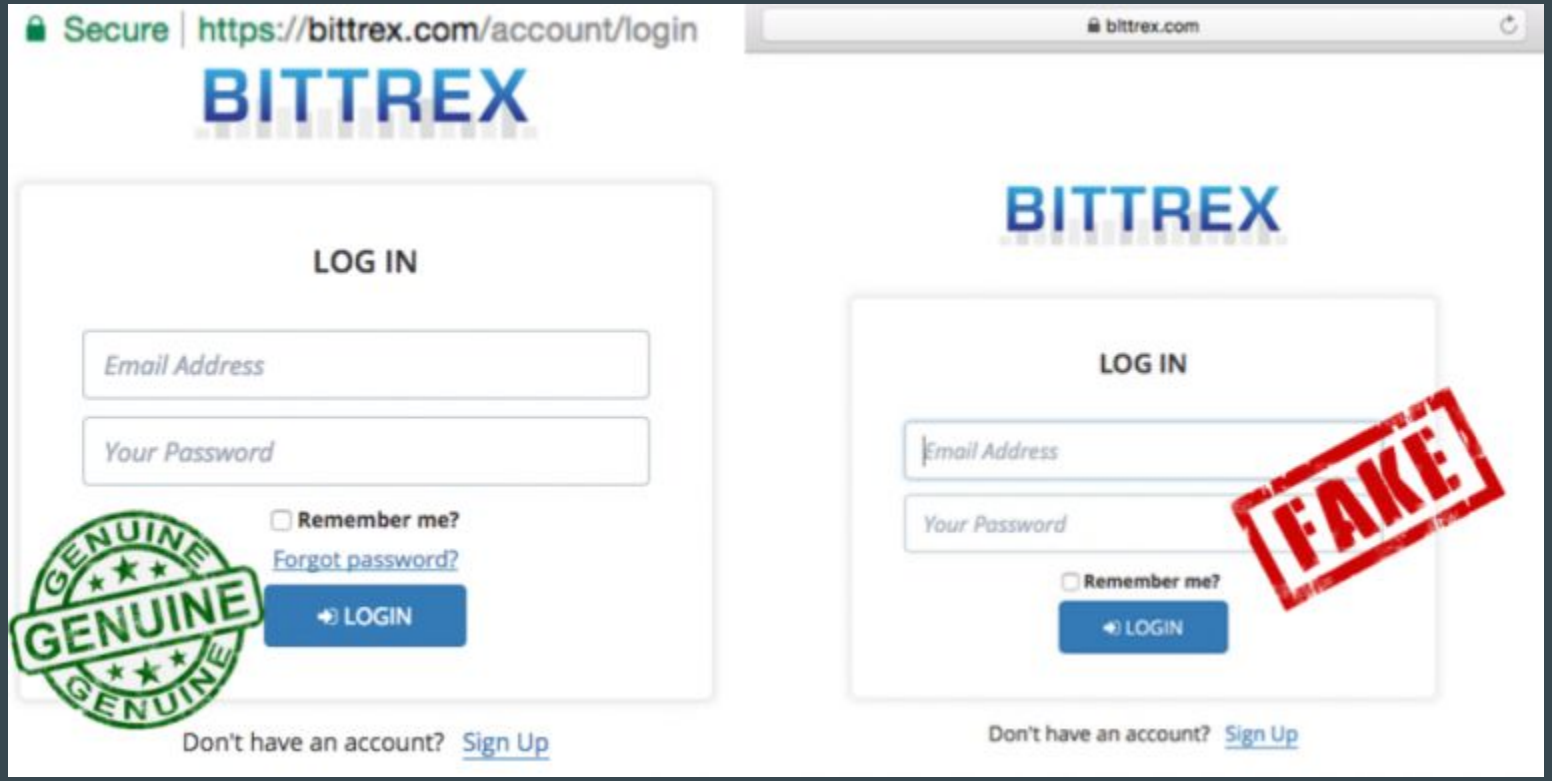
Cierre del exchange

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

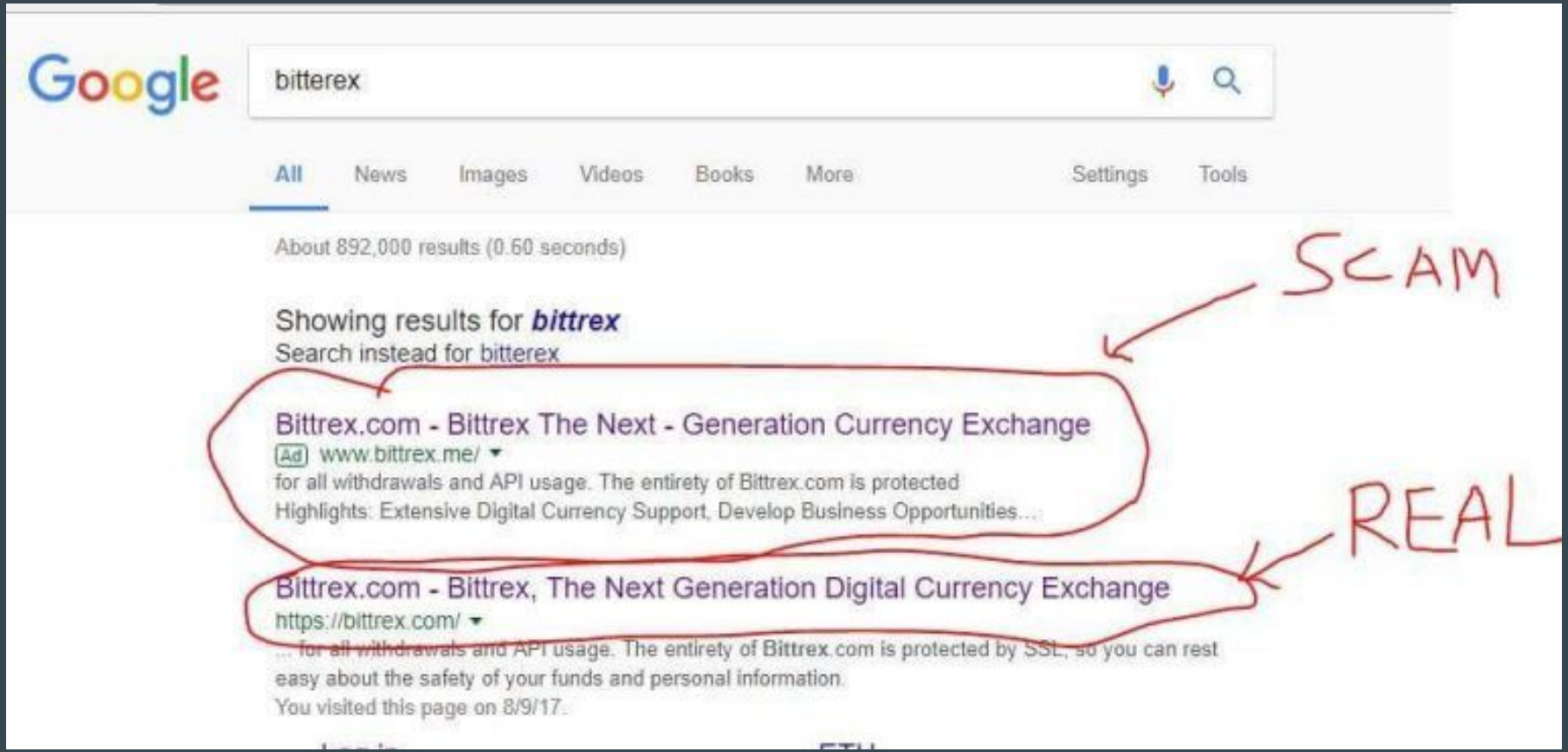
NEGOCIOS 23 Abril 2021

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.

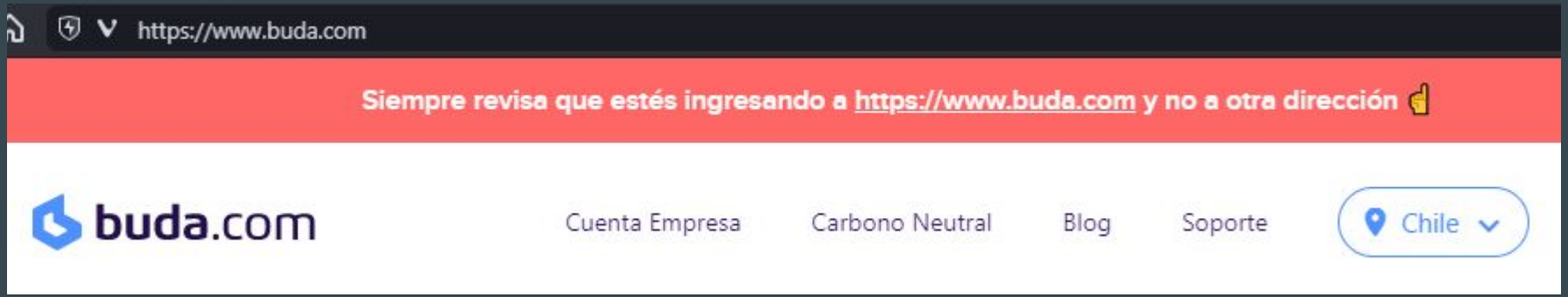
Suplantación de dominio



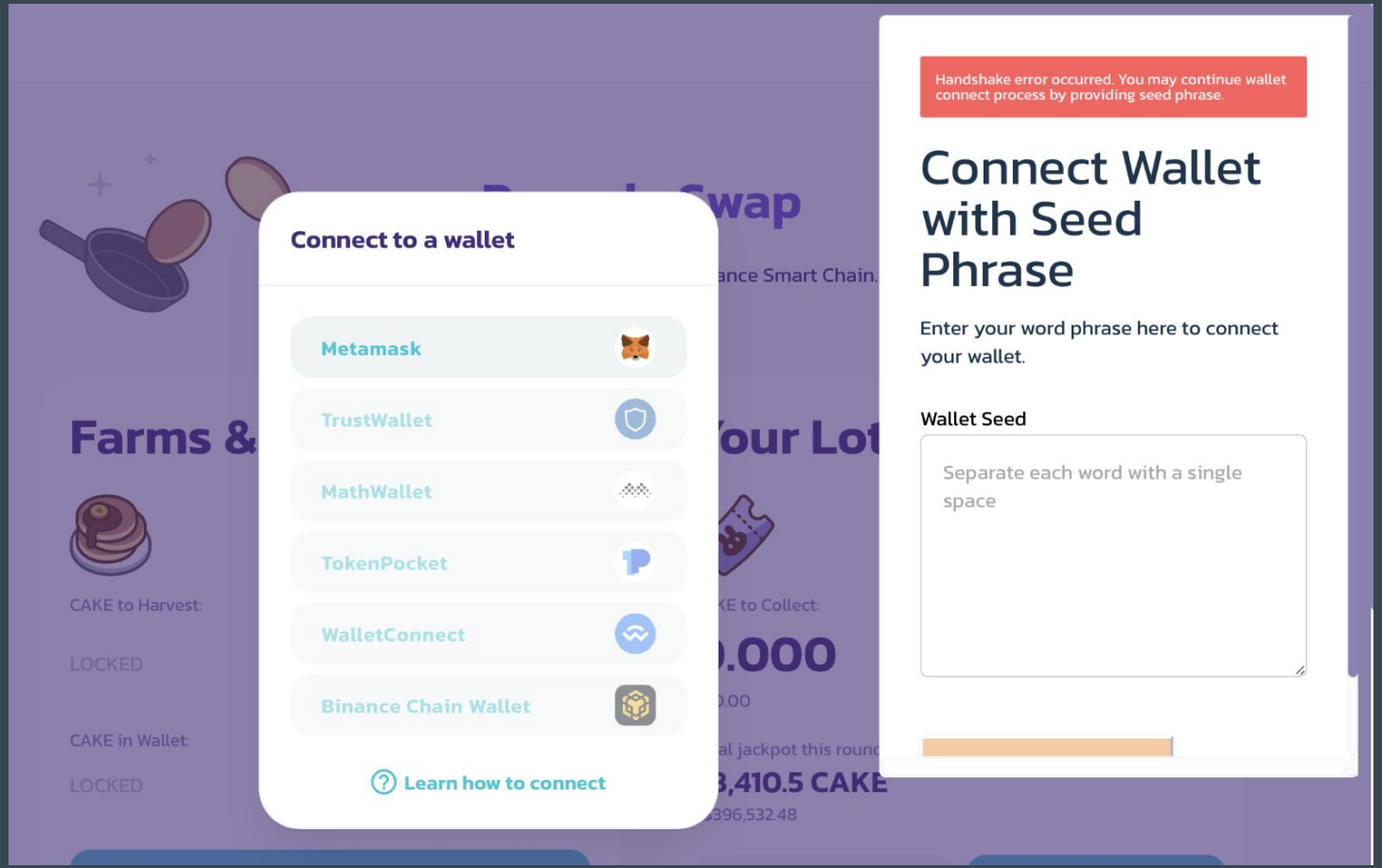
Suplantación de dominio



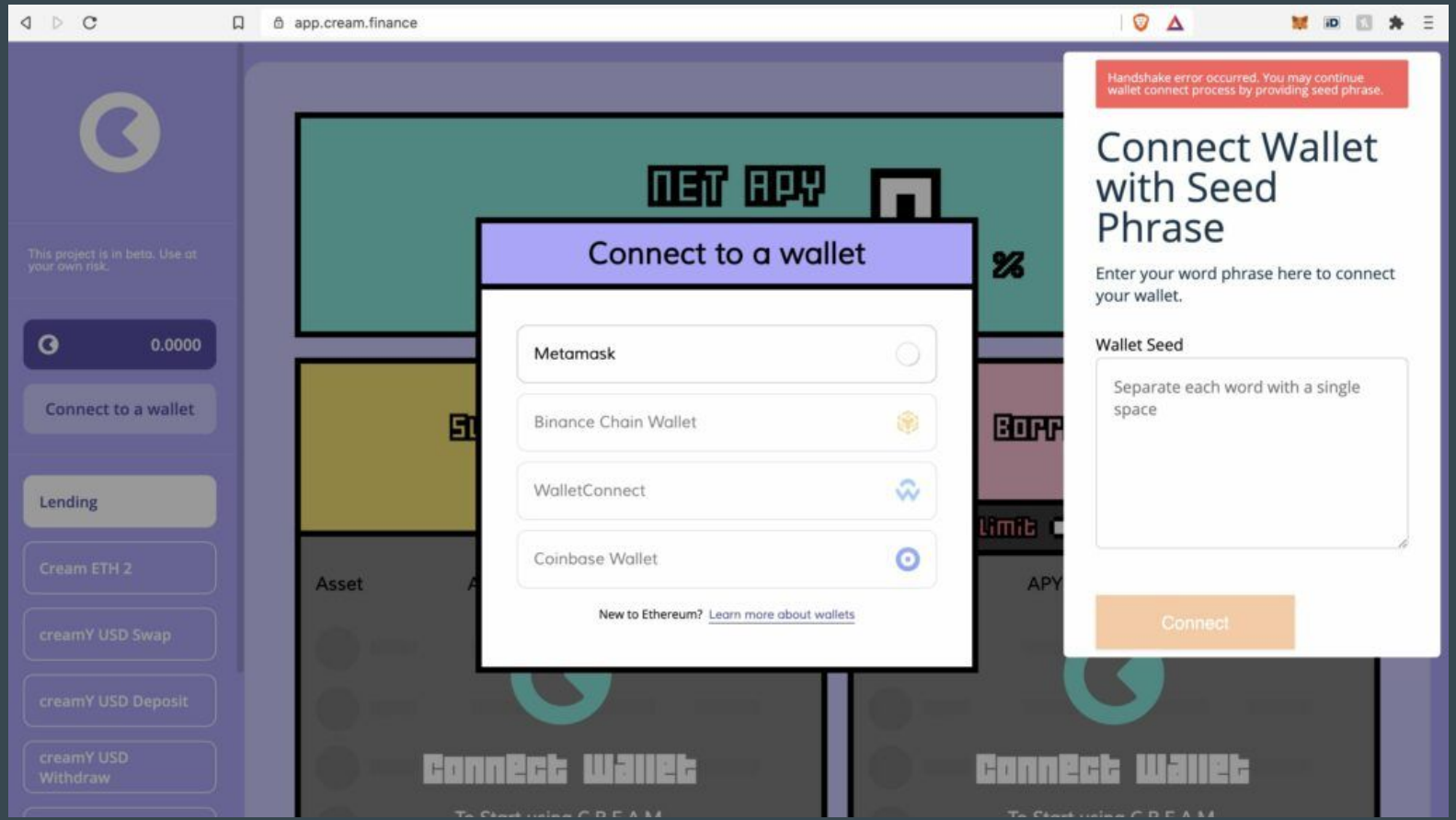
Suplantación de dominio



Ciberataque al DNS



Ciberataque al DNS



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...

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 trabajndo para solucionar el problema. $CAKE
> twitter.com/CakeSwapEs/sta...

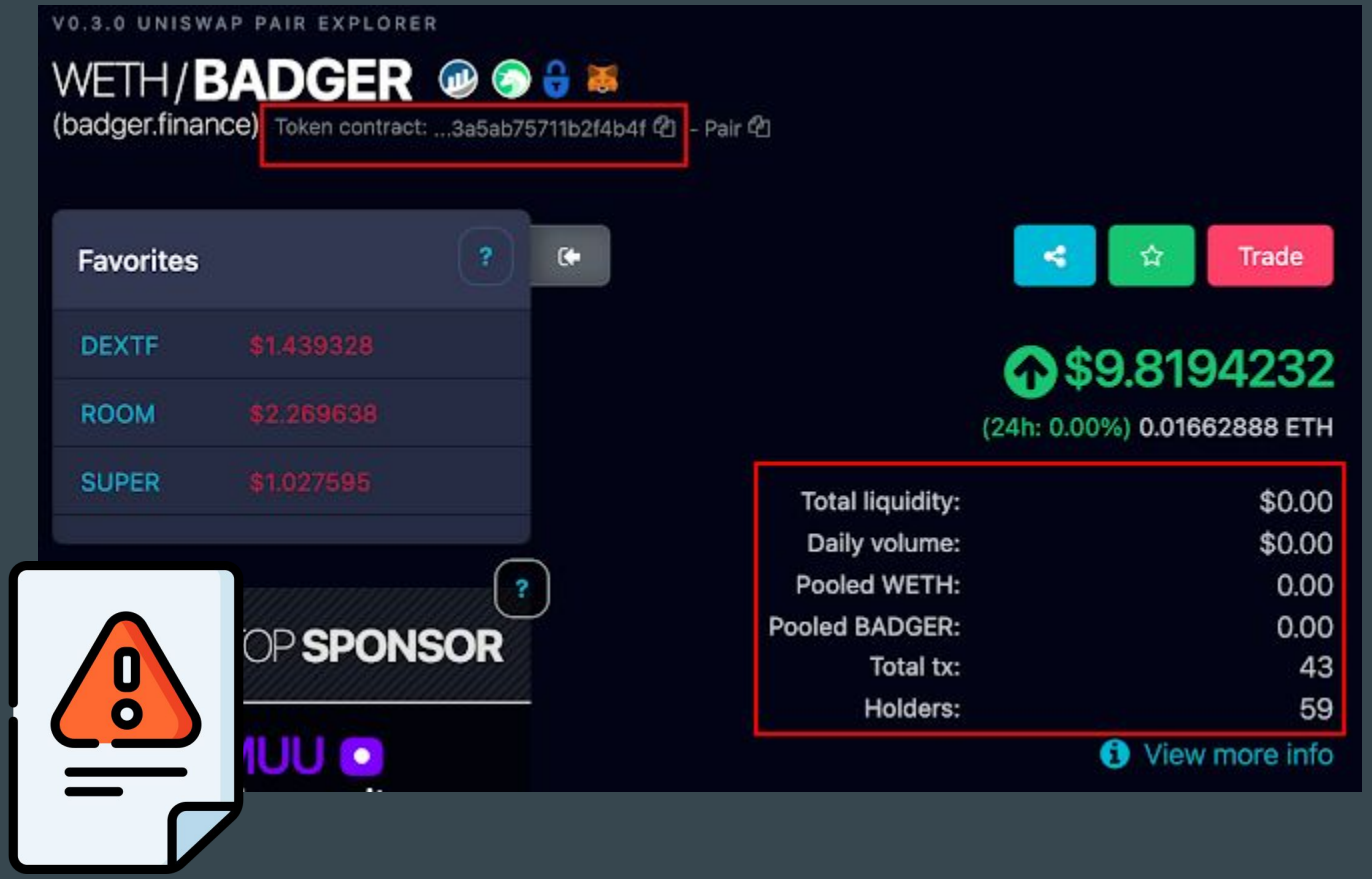
12:14 p. m. · 15 mar. 2021

Ciberataque con APIs

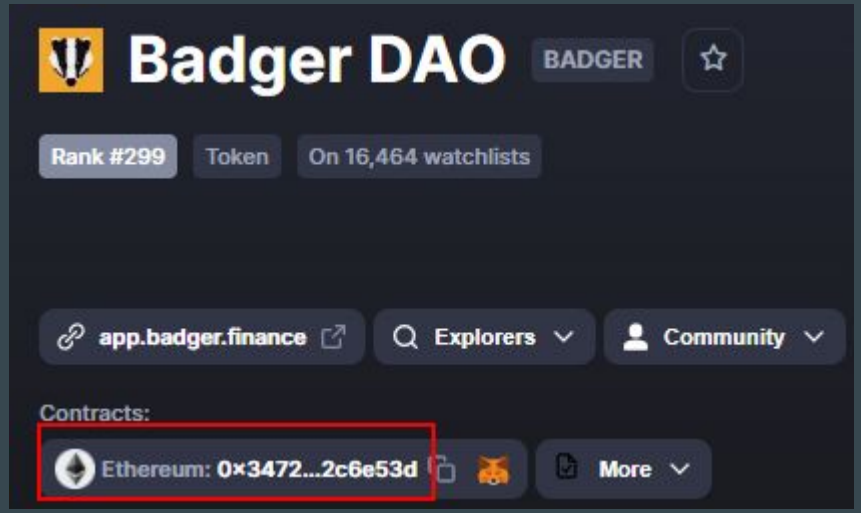
```
# from binance.client import Client
# from binance.enums import *
# from binance.exceptions import *
import matplotlib
import numpy as np
import pandas as pd

# Binance
WEB_SOCKET = "ws
BN_API_KEY = "8
BN_API_SECRET = "q

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

# 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



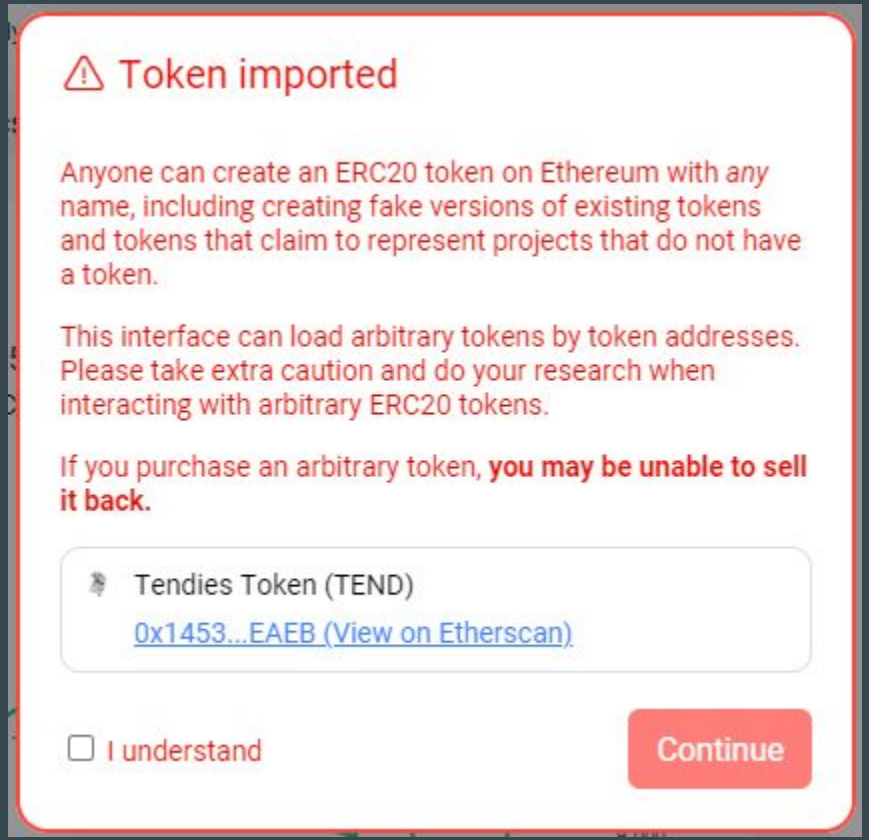
Suplantación de token



https://www.coingecko.com

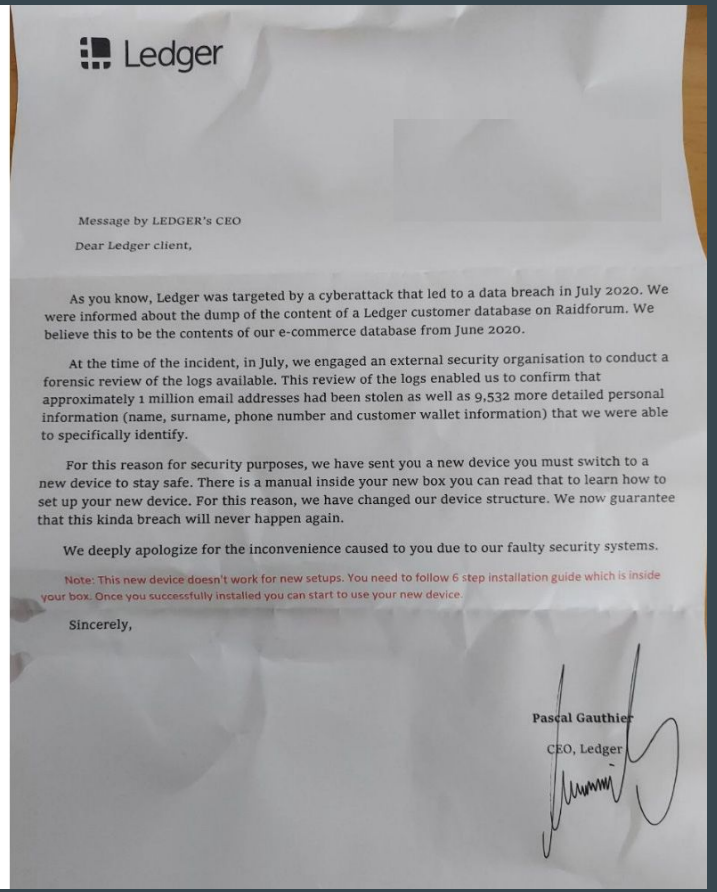
https://www.coinmarketcap.com

Suplantación de token



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 kinda 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.

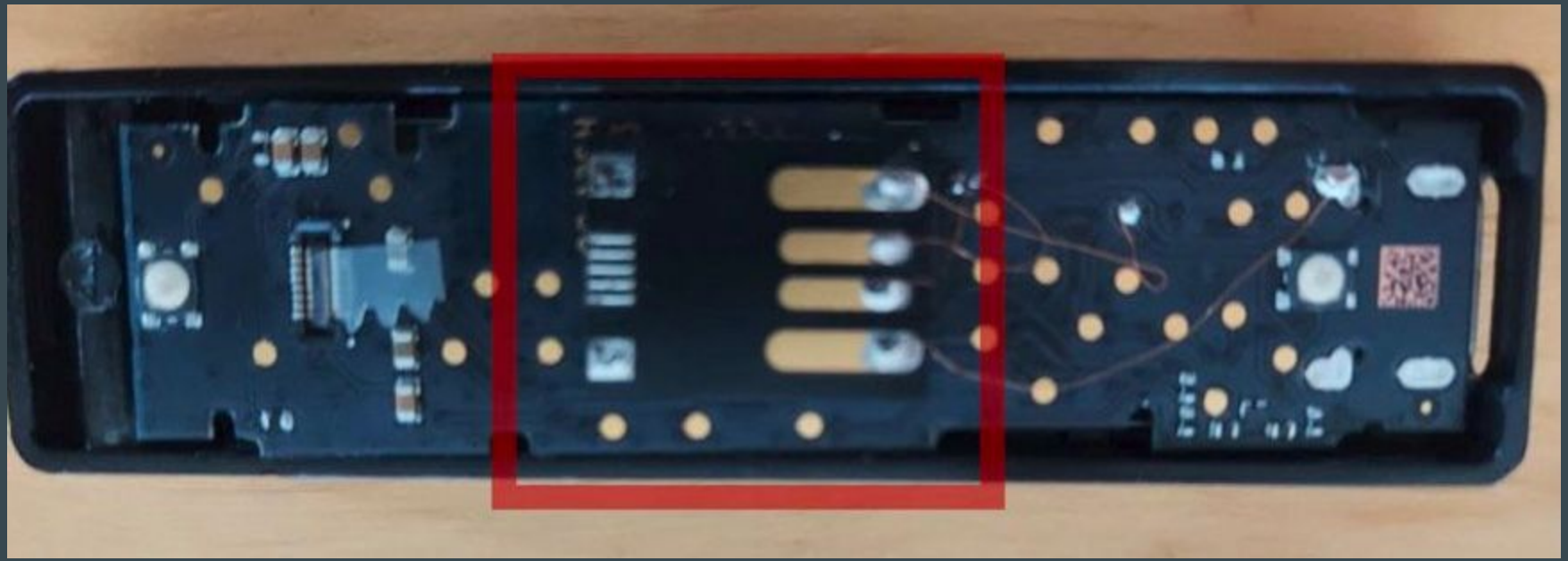
Sincerely,

Pascal Gauthier

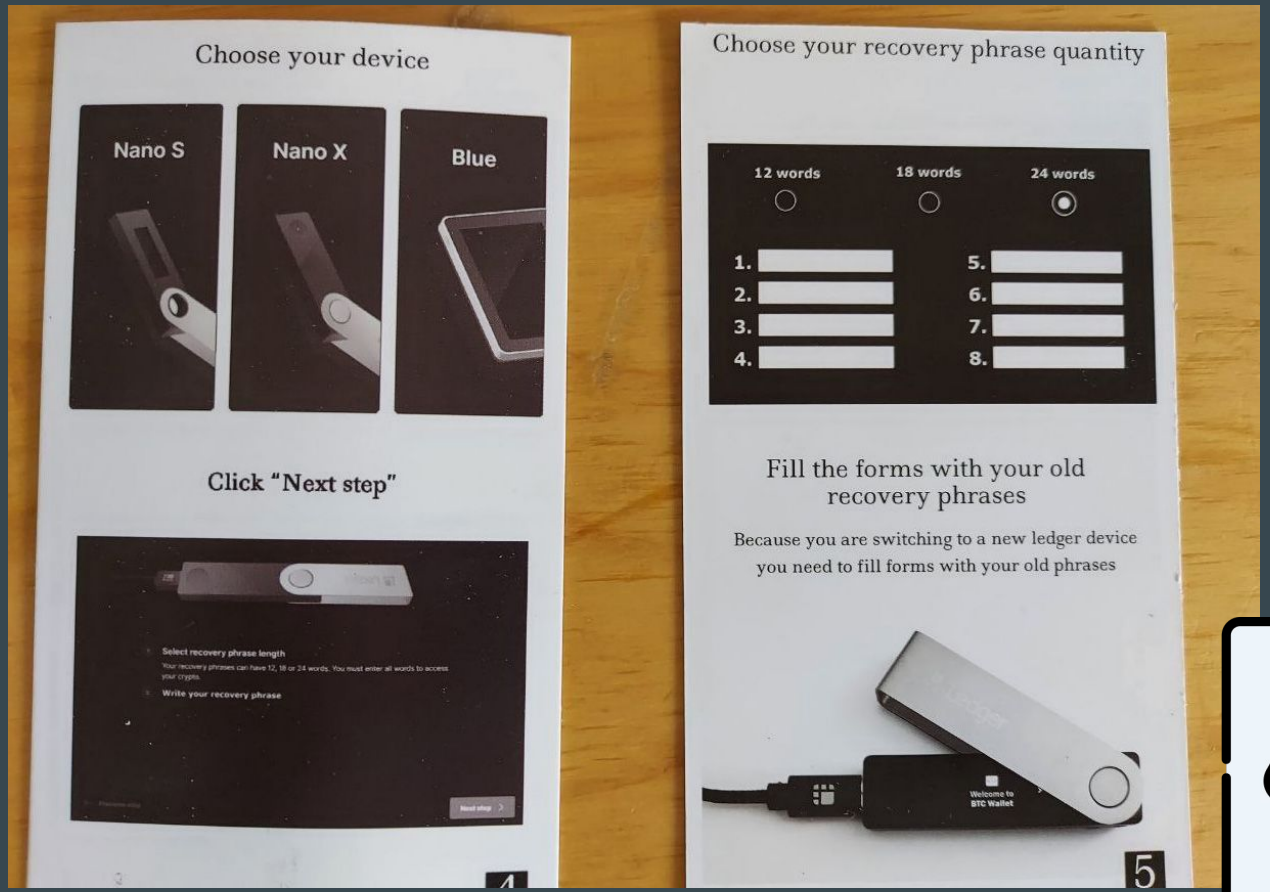
CEO, Ledger

Suplantación de billeteras electrónicas

Suplantación de billeteras electrónicas



Suplantación de billeteras electrónicas



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