

*Feel free to download this document for reading, sharing, or whatever you wish!*

### **An essential quote to begin with...**

*“There is a principle which is a bar against all information, which is proof against all arguments, and which cannot fail to keep a man in everlasting ignorance - that principle is contempt prior to investigation.” - William Paley (1743-1845)*

### **\*\* Disclaimer \*\***


This post is for the purpose of sharing my experience of what happened to me while using the Ledger Nano S wallet. This is a complete and honest presentation of everything that I have gathered since my robbing. This post is not meant to make any decisions for you nor attempt to persuade you to buy or not buy a Ledger wallet. What you want to do with your money is up to you. It's likely that many other wallets have similar faults (and maybe worse) but I am only giving my experience of the wallet I used — which happens to be Ledger Nano S. I'm not here to please either side (pro or anti Ledger) but only to share the story and warn others of the possibility. This is not an attempt to fear monger or spread any FUD - fear, uncertainty, doubt. If you experience any FUD after reading this than that is on you. *All personal names have been removed for privacy purposes.*

While reading this information I encourage two things...

1. Release all of your biases, limiting beliefs, and information that you have been **told** (emphasis on told) about what is possible or not up until this point.
2. Avoid taking anything personally. There is no reason to take anything personally unless something mentioned is true about you or it is challenging a bias of yours. If it is taken personally then it should be internal work that is done and not attacking someone else on the internet.

### **Story Time**

I purchased the Ledger Nano S in Jan of 2018. \*Pictured below. I took these pictures recently so I can't show that it came sealed but it did come sealed.\*

ORDER DATE Jan 04, 2018	ORDER NUMBER 282797270378- 1778720756018	SOLD BY <a href="#">pcloud6434</a> (1 item)	<a href="#">View order details</a> <a href="#">View seller's other items</a> More actions ▾
	FACTORY SEALED (TAX FREE) Ledger NANO S Cryptocurrency Hardware Wallet (282797270378) <a href="#">Add note</a>	ITEM PRICE: US \$99.00	
<a href="#">Buy similar</a>			

The reason I purchased the device on eBay is because Ledger was on back order. And of course I couldn't wait to buy a completely safe wallet to store my coins so I paid extra for this one.

This was during the rigged crypto bull run (aka massive theft) of late 2017 - early 2018. The ledger I bought was 100% legit and the seller bought it for the purpose of selling it during the bull run to those who wanted "safety" for their coins — which were sky rocketing in value at that time.

Here are all of the pictures of my Ledger Nano S

# Ledger Nano S

Cryptocurrency hardware wallet





# Ledger Nano S

Cryptocurrency hardware wallet

Ledger Nano S is a hardware wallet based on a Secure Element for storing cryptocurrencies, embedding a screen to check and secure digital payments.



BITCOIN



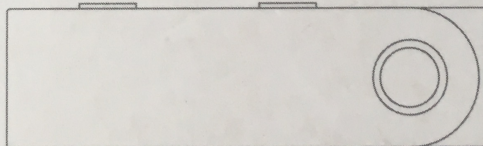
ETHEREUM

fido™

AUTHENTICATION

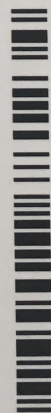


USB



OPEN SOURCE & DEVELOPER FRIENDLY

INSTALL 3<sup>RD</sup> PARTY APPS OR BUILD YOUR OWN



3760027781234

Ledger

Paris, Vierzon, San Francisco







**Did you notice?**

There is no anti-tampering sticker on this box.

A cryptographic mechanism checks the integrity of your Ledger device's internal software each time it is powered on.

The Secure Element chip prevents any interception or physical replacement attempt. Ledger devices are engineered to be tamper-proof.

**MORE INFORMATION**

[www.ledgerwallet.com/genuine](http://www.ledgerwallet.com/genuine)

**Recovery sheet**

Confidential document

Store this document in a safe place

Welcome  
**Ledger Nano S**

**Getting started**

Ledger Nano S

Thank you for choosing a Ledger product



## Did you notice?

There is no anti-tampering sticker on this box.

A cryptographic mechanism checks the integrity of your Ledger device's internal software each time it is powered on.

The Secure Element chip prevents any interception or physical replacement attempt. Ledger devices are engineered to be tamper-proof.

MORE INFORMATION

[www.ledgerwallet.com/genuine](http://www.ledgerwallet.com/genuine)



MORE INFORMATION  
[www.ledgerwallet.com/genuine](http://www.ledgerwallet.com/genuine)

## Recovery sheet

Confidential document

Store this document in a safe place



# Getting started

Ledger Nano S

Thank you for choosing a Ledger product

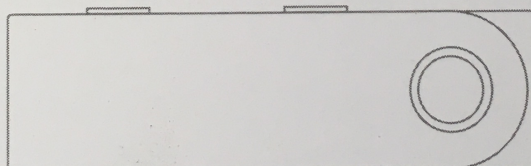


## CONFIGURE MY DEVICE

Get started at

[start.ledgerwallet.com](https://start.ledgerwallet.com)

and follow the instructions to  
configure your device.



**GET ASSISTANCE**

[www.ledgerwallet.com](https://www.ledgerwallet.com)

Contact support team

[support@ledgerwallet.com](mailto:support@ledgerwallet.com)

If this person sold me a scam ledger they would have stolen my coins long ago, when they were worth far more! It came sealed and with no words, other than the words that the device gives during set up, which I wrote down and no one has ever seen, and there has been no digital exposure anywhere.

I moved all coins to the wallet and began to use it. Everything worked perfectly for almost two years. I would check my coins, buy or sell, every month or so with no issues. I thought I had the perfect wallet. But now I know there isn't a perfect wallet, especially digitally.

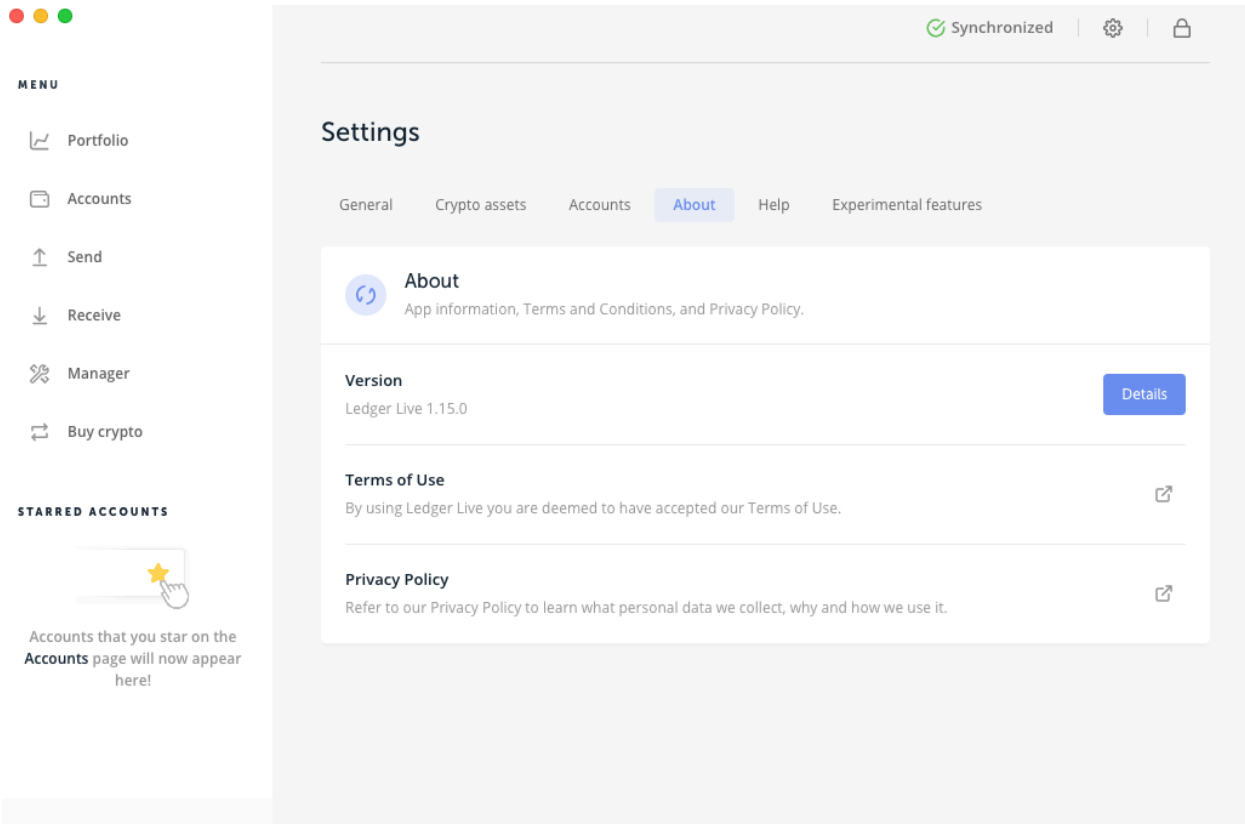
The following is everything that happened from September 26th 2019 (The day I updated my Ledger Live App, Device Firmware, and the device reset) up until now.

**Note:** The specific coins don't really matter as ANY coin that would've been stored with the wallet would have been (and were) stolen. Shit coin, scam coin, fanboy coin, god coin, etc — all would've been robbed. So I encourage you to not focus on the specific coins but see the big picture.

**Note:** There is no way for me to prove to you that I kept all of my keys safe or that I updated the ledger live app and my firmware on September 26th (there was no camera recording me to prove the former and the Ledger app and Ledger device does not list the date of update) Please know that I've always kept everything safe and the dates listed are exact.

On September 26th 2019, I used the Ledger Live App. I chose to click update on the app and it then suggested that I update the firmware on my Nano S device as well. I did the updates. The device then reset itself. Here is the pic of the version I updated to before being robbed..(1.15.0)





Here is the firmware on the Ledger Nano S device that I updated to (1.5.5) (MCU 1.7)  
-- Funny to see the word "**Secure**" on the device. Hahahaha!



Secure Element >  
1.5.5

I was then forced to put my 24 words into the device to reconfigure it. I had to do this to view any of my coins or make a transfer. I then made a transfer and then got off. Not to go back on Ledger Live until October 21st 2019.

Here is the last transfer I made to my Ledger...on Sept 26th 2019, after the update... 500 TUSD

The screenshot shows the Ledger Live interface. On the left, there is a section titled "STARRED ACCOUNTS" with a sub-header "Accounts that you star on the Accounts page will now appear here!". The main area displays a transaction history. The top transaction is dated "September 26, 2019" at "07:46" and shows a transfer from "VeriCoin" to a specific address, resulting in a balance change of "- USD 202.42". Below this, another transaction is dated "September 26, 2019" at "17:17", showing a "Received" transaction from "TrueUSD" to the same address, with a balance change of "+ TUSD 500" and "+ USD 498.50". A third transaction is dated "September 20, 2019" at "11:50", also showing a "Received" transaction from "TrueUSD" to the same address, with a balance change of "+ TUSD 50" and "+ USD 50.52".

I didn't get back onto Ledger Live to look at my balances until October 21st 2019. Here is what I saw right away (the great free fall)...



I then scrolled down and saw this... Note the date...Only two days after my device and app update! Also note the times of the transactions...pretty quick user here ;) — all coins sent to addresses that aren't mine.



Synchronized | ⚙️ | 🔒

### Last operations

September 28, 2019

↑	Sent 07:55	Qtum	QVfHqVs7HHU8Q2TVhBZD2wJlMpgGcP22VW	- QTUM 143 - USD 236.65
↑	Sent 07:53	Digibyte 1	DToKM1m2Z39gUgkEwMnwWMBxs9FkBe5Ays	- DGB 30,514 - USD 235.40
↑	Sent 07:50	Ethereum 1 (legacy)	0x35293D3348b85D08d738C40574b2Eb94B8f0b12a	- ETH 1.3349 - USD 231.93
↑	Sent 07:48	Ethereum 1 (legacy)	0x0000000000085d4780B73119b644AE5ecd22b376	- ETH 0.001443 - USD 0.25
↑	Sent 07:48	TrueUSD	0x35293D3348b85D08d738C40574b2Eb94B8f0b12a	- TUSD 550 - USD 548.53
↑	Sent 07:46	Ethereum 1 (legacy)	0x905E337c6c8645263D3521205Aa37bf4d034e745	- ETH 0.0015277 - USD 0.27
↑	Sent 07:46	Medical Token Currency	0x35293D3348b85D08d738C40574b2Eb94B8f0b12a	- MTC 94,385 - USD 710.09
↑	Sent 07:46	Ethereum 1 (legacy)	0x3597bfD533a99c9aa083587B074434E61Eb0A258	- ETH 0.0015354 - USD 0.27
↑	Sent 07:46	DENT	0x35293D3348b85D08d738C40574b2Eb94B8f0b12a	- DENT 808,482 - USD 280.95
↑	Sent	Ethereum 1 (legacy)	0x998h3R87bc9dRA173990Re7afb772788R5aC8RRd	- ETH 0.0015183

I then went and checked [Tronscan.org](https://tronscan.org) — where I used the Ledger Nano S to hold coins ... Here is what I was greeted with.. a unfreeze confirmation (that I never unfroze).

← → ↻ [tronscan.org/#/transaction/b4d01d8c4a0a69436a2aa0a07d3722be594ed44e129f39060335f3cff30f551d](https://tronscan.org/#/transaction/b4d01d8c4a0a69436a2aa0a07d3722be594ed44e129f39060335f3cff30f551d) ☆ 🌐

📄 BLOG/CRAIN 📄 CONTRACTS 📄 TOKENS 📄 TRAMARKET 📄 DAPP 📄 TRON SR 📄 MORE

---

### TRANSACTION

**# Hash** [b4d01d8c4a0a69436a2aa0a07d3722be594ed44e129f39060335f3cff30f551d](#)

**Status:** CONFIRMED

**Result:** SUCCESS

**Hash:** [b4d01d8c4a0a69436a2aa0a07d3722be594ed44e129f39060335f3cff30f551d](#)

**Block:** [13144957](#)

**Time:** 9/28/2019 07:03:06

---

🔗 **Unfreeze Balance Contract** Unfreeze TRX

**Owner Address** [TG22NMFL8WQnciouioHQsPZRdGDNk9Vrus](#)

All TRX was unfrozen on the 28th, the same day as all of the wallet robbing. Also, note the time here.

Note: it takes 72 hours to unfreeze TRX in Tronscan (at least they say)

I then saw the following transfers of TRX coins...

TRONSCAN | TRON BlockChain x Submit a request - Ledger Sup x +

tronscan.org/#/transaction/7429248291bb583bbddf25dcad99e5f92100cbdd364f4e5e2139587db88b2716

BLOCKCHAIN CONTRACTS TOKENS TRXMARKET DAPP TRON SR MORE

TRX EN

### TRANSACTION

# Hash **7429248291bb583bbddf25dcad99e5f92100cbdd364f4e5e2139587db88b2716**

Status: **CONFIRMED**

Result: SUCCESS

Hash: 7429248291bb583bbddf25dcad99e5f92100cbdd364f4e5e2139587db88b2716

Block: **13145080**

Time: 9/28/2019 07:09:18

Transfer Contract TRX transfer between addresses

From **TG22NMFL8WQnciouioHQsPZRdGdnk9Vrus**

To **TMyykKj2unRCX6nqUuZvhS1wtSyXsDBaE**

Amount 560,000 TRX

TRONSCAN | TRON BlockChain x Submit a request - Ledger Sup x +

tronscan.org/#/transaction/b822b368aed394632ce56f09d811d2b6b51b701897e10f8a9a6ca2ee5daf81a8

BLOCKCHAIN CONTRACTS TOKENS TRXMARKET DAPP TRON SR MORE

TRX EN

### TRANSACTION

# Hash **b822b368aed394632ce56f09d811d2b6b51b701897e10f8a9a6ca2ee5daf81a8**

Status: **CONFIRMED**

Result: SUCCESS

Hash: b822b368aed394632ce56f09d811d2b6b51b701897e10f8a9a6ca2ee5daf81a8

Block: **13145132**

Time: 9/28/2019 07:11:54

Transfer Contract TRX transfer between addresses

From **TG22NMFL8WQnciouioHQsPZRdGdnk9Vrus**

To **TMyykKj2unRCX6nqUuZvhS1wtSyXsDBaE**

Amount 25,000 TRX

All coins sent to addresses that aren't mine. I then checked a couple other tokens I had on Tronscan...

← → ↻ tronscan.org/#/transaction/bfddc5ca60f275e835eed2957dcd83b46eca17b58ceb54f4b9c5b3dfc01e0476 ☆

### TRANSACTION

# Hash **bfddc5ca60f275e835eed2957dcd83b46eca17b58ceb54f4b9c5b3dfc01e0476**

Status: **CONFIRMED**

Result: SUCCESS

Hash: bfddc5ca60f275e835eed2957dcd83b46eca17b58ceb54f4b9c5b3dfc01e0476

Block: **13145091**

Time: 9/28/2019 07:09:51

---

↔ Transfer Asset Contract Token transfer between addresses

From **TG22NMFL8WQnciouioHQsPZRdGdnk9Vrus**

To **TMyykKj2unRCX6nqUuZvhvS1wtSyXsDBaE**

Amount 859267.378304

Token **BitTorrent** [ID:1002000]

TRONSCAN | TRON BlockChain x Submit a request - Ledger Sup x +

← → ↻ tronscan.org/#/transaction/8208709af051eaf93af0a33832c7b16b7929d7a802092f1fc00af1c0a3dba61b ☆

### TRANSACTION

# Hash **8208709af051eaf93af0a33832c7b16b7929d7a802092f1fc00af1c0a3dba61b**

Status: **CONFIRMED**

Result: SUCCESS

Hash: 8208709af051eaf93af0a33832c7b16b7929d7a802092f1fc00af1c0a3dba61b

Block: **13145118**

Time: 9/28/2019 07:11:12

---

↔ Transfer Asset Contract Token transfer between addresses

From **TG22NMFL8WQnciouioHQsPZRdGdnk9Vrus**

To **TMyykKj2unRCX6nqUuZvhvS1wtSyXsDBaE**

Amount 12475

Token **SEED** [ID:1000001]

Note the time on all of these transactions and then go back and look at the time of the ledger live transfers! Tronscan was drained before Ledger Live.

Here is the wallet that all of my tokens ended up in on Tronscan (after 4 different transfers that I clicked through) — Check out those numbers...Are they cleaning out the wallets of others as well...??



Token	Token Type	ID	Precision	Balance	Price (TRX)	Value
TRX (TRX)	-	-	6	184,638,494.809908	1	184,638,494.809908 TRX 4,086,629.36 USD
BitTorrent (BTT)	TRC10	1002000	6	25,111,911,019.91176	0.0204	512,282,984.8062 TRX 11,338,430.203 USD
Tether USD (USDT)	TRC20	-	6	11,837.910448	45.454545	538,086.833165 TRX 11,909.55 USD
WINK (WIN)	TRC20	-	6	42,568,838,300.303696	0.00754	320,969,040.78429 TRX 7,104,052.202 USD
TRONWALLET (TWX)	TRC20	-	6	304,148.139819	0.0178	5,413.836889 TRX 119.825 USD
BeatzCoin (BTZC)	TRC10	1002413	6	5,007	0.0875	438.1125 TRX 9.697 USD
TronWeeklyJournal (TWJ)	TRC20	-	8	4,000	0.00207	8.28 TRX 0.183 USD
SEED (SEED)	TRC10	1000001	0	2	1.201	2.402 TRX 0.053 USD

I then went over to Myetherwallet and signed in with my Ledger Nano S and saw all of the same transactions that I saw on Ledger Live App..

Transfers		66 total
2019-09-28 07:50:09	Tx: 0x3be92ff3c5d88cb36a407c49e194afe5897427bb55786cddb2d313ba5... From: 0x8abba06a91b0c5acd9ec1b94407436f353311423 To: 0x35293d3348b85cd08d738c40574b2eb94b8f0b12a	Ethereum -1.334012798  ETH \$ 248.87 (6.78%) -\$ 233.07 @ 174.71
2019-09-28 07:48:55	Tx: 0x21addde47edf33ed037e35b814f518cb4c66a1ebaddbdb6aa28ff6c89... From: 0x8abba06a91b0c5acd9ec1b94407436f353311423 To: 0x35293d3348b85cd08d738c40574b2eb94b8f0b12a	TrueUSD -550.00 TUSD \$ 551.22 (-0.39%) -\$ 553.37 @ 1.01
2019-09-28 07:46:50	Tx: 0x7a822eabd5aaa6ef31e70face3878933c6d1e1cafb385d8ba74e914b8... From: 0x8abba06a91b0c5acd9ec1b94407436f353311423 To: 0x35293d3348b85cd08d738c40574b2eb94b8f0b12a	Medical Token Currency -94,385.15491497 MTC \$ 872.62 (19.46%) -\$ 730.46 @ 0.01
2019-09-28 07:46:28	Tx: 0x72ff8f1967980aec485d88e608f899eebde35a34912b25b6ffb3138b63... From: 0x8abba06a91b0c5acd9ec1b94407436f353311423 To: 0x35293d3348b85cd08d738c40574b2eb94b8f0b12a	DENT -808,482.3597428 DENT \$ 203.30 (-32.86%) -\$ 302.80 @ >0.00
2019-09-28 07:46:15	Tx: 0x6e15c155b307558736362e87ded8063269d7fd5b92d1622d4c25f97... From: 0x8abba06a91b0c5acd9ec1b94407436f353311423 To: 0x35293d3348b85cd08d738c40574b2eb94b8f0b12a	BANCA Token -9,677,070.00 BANCA \$ 281.89 (-4.23%) -\$ 294.33 @ >0.00
2019-09-28 07:46:02	Tx: 0xdcc3556a0253c8b62c27bf0ccf57a84c7cd1f57d5cadc9f43ecb33315... From: 0x8abba06a91b0c5acd9ec1b94407436f353311423 To: 0x35293d3348b85cd08d738c40574b2eb94b8f0b12a	Dentacoin -10,383,349 \$ 506.52 (124.27%) -\$ 225.85 @ >0.00

They all ended up in the same wallet here...(not my wallet)

[Get widget code](#)

Address Information		Balances - <sup>Ⓢ</sup> ~ \$ 7,214.43 (+2.82%)	
Address	0x35293D3348b85D08d738C40574b2Eb94B8f0b12a	Ethereum	25.385092541009485 $\downarrow$ ETH \$ 4,735.78
Balance	25.385092541009485 $\downarrow$ ETH \$ 4,735.78	Medical Token Currency	94,385.15491497 MTC \$ 872.62 (+9.72%)
Total In	31.515996568377854 $\downarrow$ ETH	TrueUSD	550.00 TUSD \$ 551.22 (+0.64%)
Total Out	6.13090402736837 $\downarrow$ ETH	Dentacoin	10,383,349 $\wedge$ \$ 506.52 (-3.63%)
	<a href="#">view QR-code</a>	BANCA Token	9,677,070.00 BANCA \$ 281.89 (+0.37%)
		DENT	808,482.3597428 DENT \$ 203.30 (+3.03%)

After this I went and checked the other third party wallets that I had been using. Here is what I saw on VeChain's wallet VeForge...

← → ↻ vault.veforge.com ★ 👤

⬆️ Send
⬆️ Receive

Recent Activity			My Balances	
SEP 28	<span style="color: orange;">⬆️</span> Sent VET to 0xb90e66261d0b3b1b84027e946...	-286,000	<span style="color: blue;">V</span> VeChain (VET)	52.57
AUG 10	<span style="color: orange;">⬇️</span> Received VTHO from 0xa4adafaef9ec07bc4dc6de1...	+166	<span style="color: blue;">⚡</span> VeThor (VTHO)	38.44k
DEC 01	<span style="color: orange;">⬇️</span> Received VET from 0xa4adafaef9ec07bc4dc6de1...	+75,936	EightHoursToken (EHRT)	0.00

After this I went and checked the NEO O3 wallet and saw this...

BarWally (Ae1Gow...617y5s) Copy


**\$0.00**  
\$0.00 (0%)

Send Receive Scan

ASSETS

**Buy NEO today!**

Your wallet currently has no tokens.  
To get started, send some to this address.



Copy image

Ae1Gowgy4YH6Nbfqw4q5DMXeimKn617y5s

Please only send NEO, GAS, ONT, ONG, or NEP-5 tokens to this address.

Refer friends and get rewards

TRANSACTIONS

Type	Asset	Date	Amount
Sent	TKY	2019.09.28 @ 08:02	-207389.9675
To: AWCjfxDKjZntQ5cdPK9PaP5mqpai5NDyKG			
Received	TKY	2018.12.14 @ 18:12	+207389.9675

MainNet  
NEO 4553822  
ONT 7034815  
Ver 3.0.0

Here is what I saw when I checked my Stellar Lumens Stellar Account Viewer...

Stellar Account Viewer

stellar.org/account-viewer/#/dashboard

To  
Recipient's public key or address

Amount  
Amount to send lumens

Add memo [What's a memo?](#)

Fee  
0.00001 lumens

Recommended fee: [0.00001 lumens](#) [What's a fee?](#)

**Send lumens**

### Transaction History

This tool is showing all payments, including payments smaller than 0.5 XLM.

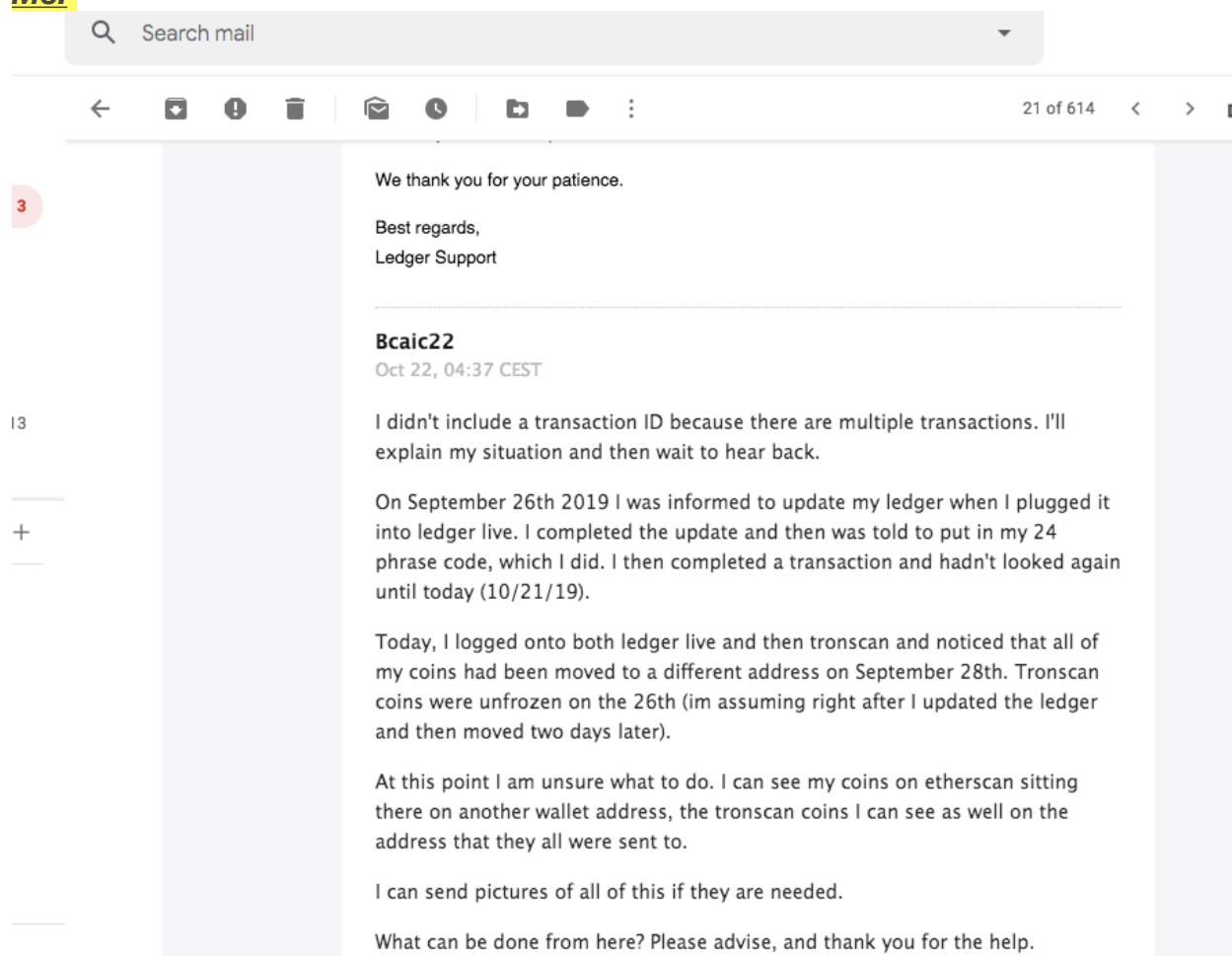
[Hide small payments](#)

Account ID	Amount	Memo	Operation ID
GBYFEWQEU56HP2Q6KEDGHCWZMXODAUIGNOSO IYM5D4BMMHDLBPNKZPDU	-14,070 XLM		<a href="#">111864549233139713</a>



After seeing all of this robbery I sent Ledger Support an email and told them what happened. Here is how it went down.. Any additional commentary by me is marked with \*\* and underlined and appears before or after the email.

**Me:**



**Ledger:** \*\*Didn't screen shot because it is too long..

"Thank you for reaching Ledger Support. My name is and I will be gladly assisting you from now.

It seems that you didn't import the correct or full 24-word recovery phrase on your Ledger device.

Could you please clarify the questions below?

- Are you able to access other crypto asset accounts created before the firmware update?
- Did you ever configure your Ledger device as a new one and change to another 24-word recovery phrase during the recent firmware update or the initialization of Ledger Live desktop? Or did you import only part of the full 24-word recovery phrase, like 12 or 18 words?

Here is the tutorial on how to recover your backup on Ledger device with your full original 24 recovery words where your crypto assets are.

<https://support.ledger.com/hc/en-us/articles/360005434914->

When you restore the backup on your device with your original 24 recovery words, you will be asked to select between 12, 18, or 24 words.

You cannot select 12 or 18 to import a Ledger 24-word backup. Ledger only generates 24 words recovery phrase that would need to be entered in their entirety.

Here is the [BIP39 English dictionary](#) where you can check the correct spelling of each of your 24 words.

Then you can import existing accounts on Ledger Live following the tutorial here.

<https://support.ledger.com/hc/en-us/articles/360006410253->

This BIP39 protocol is not specific to Ledger only. For more details about this, you can refer to [this doc](#).

You can also know more about [Ledger security in our FAQ](#).

Let us know if you have further questions.

Regards! / Cordialement! / 祝好”

**Me:**

The screenshot shows an email interface with a search bar at the top. The email content is as follows:

Here are the answers to the few questions below... underlined

3

Are you able to access other crypto asset accounts created before the firmware update?

Yes, I can access all of them still, they were all created before the last update.

- Did you ever configure your Ledger device as a new one and change to another 24-word recovery phrase during the recent firmware update or the initialization of Ledger Live desktop? Or did you import only part of the full 24-word recovery phrase, like 12 or 18 words?

13

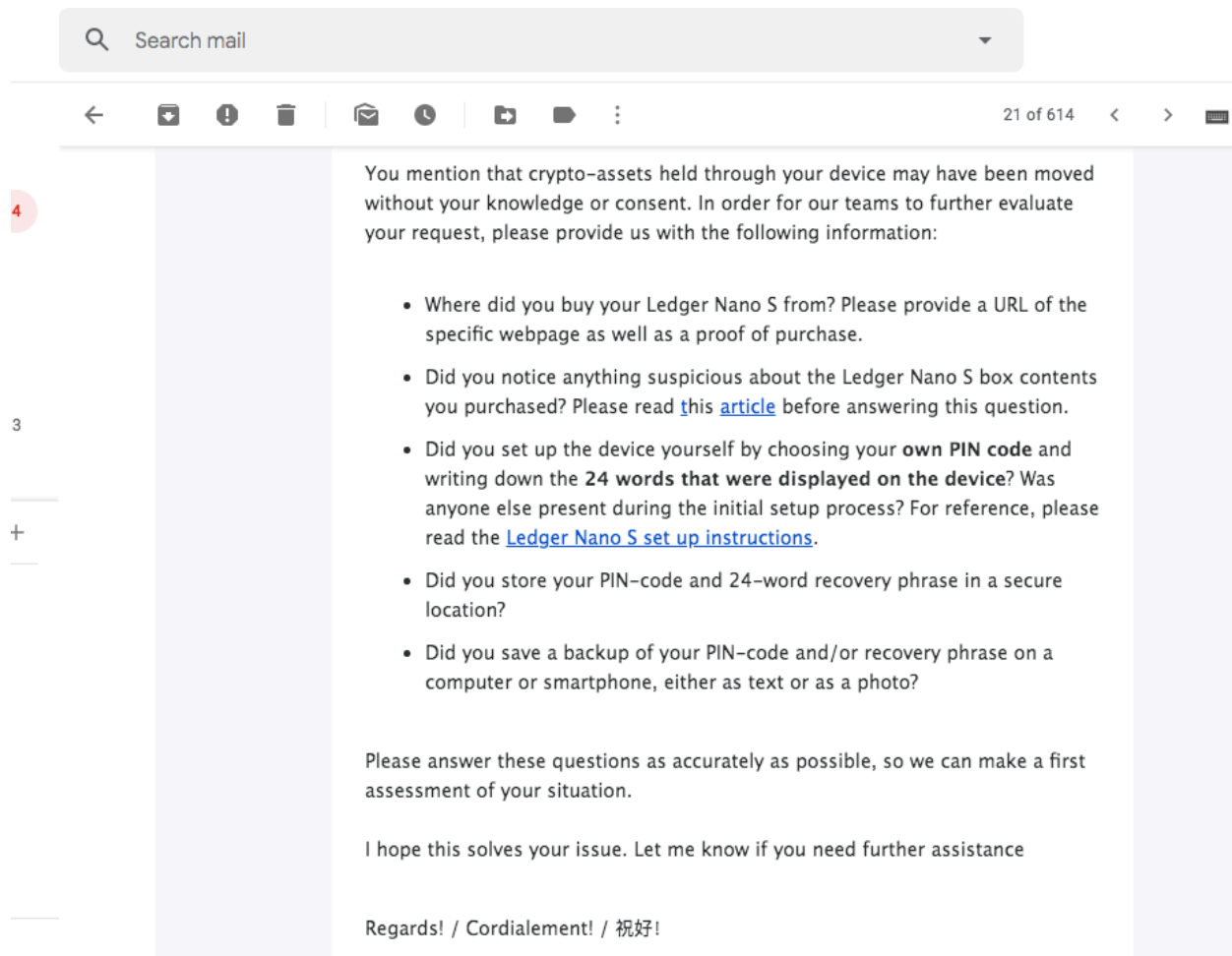
+ - I've never used any other phrase other than the 24 word recovery that was given to me on the ledger when I originally set it up in January of 2018. Last month when I updated I was instructed to put my 24 word phrase in the ledger in order to be able to use it, which I did. And then two days later all of my coins from ledger live (ETH Tokens, DGB, and QTUM) were sent to another address. The same thing happened in [tronscan.org](#). It also happened to my Neo Wallet (O3). It also did it on my stellar account viewer (XLM). I have not been able to check Veforge wallet yet because the wallet is down for maintenance (VET) but I'm sure its wiped out of there too. All these transactions were on the same exact day - sept 28th!

What should I do from here?

...

Ledger Support Oct 24, 2019, 2:04 AM ☆

**Their response to this...**



**Me:** <sup>\*\*</sup>(no pic because of size)

<sup>\*\*\*</sup>(Italic and non bold is Ledger and mine is bold and underlined)

- *Where did you buy your Ledger Nano S from? Please provide a URL of the specific webpage as well as a proof of purchase. - **I cant give the URL but I have a screenshot of the purchase from Ebay. This was a legitimate, sealed ledger, as you'll see from the attached pictures. It was during the time in early 2018 when ledger was out of devices for a while so I found a reseller on Ebay. Ive used it since Jan 2018, they would have stolen the coins back then if it came as a scam as all the coins were worth MUCH MORE.***
- *Did you notice anything suspicious about the Ledger Nano S box contents you purchased? Please read [this article](#) before answering this question. **There was nothing suspicious about the box, check attached photos! It came sealed.***
- *Did you set up the device yourself by choosing your **own PIN code** and writing down the **24 words that were displayed on the device**? Was anyone else present during the initial setup process? For reference, please read the [Ledger Nano S set up instructions](#). - **No one was present during the initial set up. I***



**followed the directions, set up my own pin code, and the wrote down the 24 words that displayed on the device during set up.**

- *Did you store your PIN-code and 24-word recovery phrase in a secure location? - **Yes, no one knows where it is, and I hardly access my accounts.***
- *Did you save a backup of your PIN-code and/or recovery phrase on a computer or smartphone, either as text or as a photo? - **No such file exists, only written on paper!***

**I've noticed that all accounts were stolen on the same day and at very close time intervals, seems hard for a single human to do. I have ALL of the proof detailed with screenshots to show my case.**

**This all happened right after I upgraded Ledger i've desktop app and the updated the software on my ledger nano S to the newest software.**

**once my ledger device was updated I was forced to reconfigure my device with my 24 words before being able to access any wallets. This was ALL done on the screen of my nano ledger S.**

**Looking forward to seeing your response to this, and will be glad to send over all proof with detail about the stolen coins.**

Thank you for the assistance on this matter!”

**Ledger:** (No pic due to size) — \*\* The inevitable dismissal email informing me of no possibility of liability and assuming it is user error... and to contact local law enforcement — that last one really made me laugh!\*\*

“Thank you for your reply.

Following a review of the elements you submitted, here is our conclusion:

As underlined in article 8 of our [Terms and Conditions](#), we would like to remind you that users of Ledger products are solely responsible for the way they use their devices and protect their data and information. Users must take all necessary steps to ensure that their PIN code and their 24-words recovery phrase remain confidential and are stored in a secure location, away from prying eyes.

Furthermore, in order to offer an optimum level of security to its users, Ledger does not have access to users’ confidential 24-words recovery phrase nor to their PIN code. Consequently, Ledger cannot be held liable for losses resulting from unauthorized third parties accessing your confidential information.

We encourage users who have been victims of fraudulent activity while using their Ledger products to contact and/or file a complaint with local law enforcement. Ledger may provide its assistance to law enforcement authorities, should they require any additional information to investigate your complaint.

All private keys that provide access to your crypto assets are derived from the 24-word recovery phrase that you've written down during the initial setup.

Anyone with access to your recovery phrase can take your crypto assets.

If indeed an unauthorized person has had access to your recovery phrase, make sure you immediately send your crypto assets to temporary accounts (e.g. an exchange) and reset your device to factory settings. You can find more information about the required procedure under section **Lost your recovery phrase?** in [this article](#).

Unfortunately, according to our Terms & Conditions, Ledger is not responsible for customers' losses.

We do not have any information regarding your wallets and accounts, which is a basic security principle. Therefore we do not have any means to track or recover your assets. Please note that, from a more general point of view, transactions on the blockchains cannot be reversed.

Thank you for your patience and comprehension.

I hope this solves your issue. Let me know if you need further assistance

Regards! / Cordialement! / 祝好”

**Me:** (no pic due to size)..\*\*(I was little mad here as anyone would be after being robbed for all of their coins) Not sure if I'll do everything I claimed in this email as I am quick to forgive.. We shall see\*\*

“\*\*Please note that anything mentioned in this email is not an attack on you personally nor anyone in the Ledger company. PLEASE forward this to anyone on your team who may be able to further or better assist me.\*\*

URGENT: Have this read by MULTIPLE members of the ledger team. And by someone who is FLUENT in English language. Have them go back to read our entire email conversation up until this point. — Thank you

URGENT: Read this email carefully!!

I appreciate your response. However, I am not a typical cowardly passive person that will accept a cookie cutter (automated) response to this issue and accept having many thousands of dollars (possibly millions in future value) stolen from me.

Being Ledger the company and Making devices and technology that holds the money of many people comes with the responsibility of ensuring it being safe. Especially if the user is following ALL guidelines of proper use. Having your customers back is part of doing good business (especially if they are following everything correctly).

Your response made it clear that my email has NOT been read and analyzed correctly. I received a automated response that has likely been sent to many customers who have

had their coins stolen — while they believed that they were safe with using a ledger device.

I have searched the web thoroughly and found all the ways in which others have been scammed for their money by using a ledger device, I found that none of their stories matched mine. I was NOT a victim of any hacking or phishing scam.

I have come to the conclusion that my coins have been stolen by someone within the ledger company (past or present), or knows how to access ledger code. It was either done manually or they set a malicious malware, spyware, etc, into the update that immediately went and began the stealing process of my coins, which started right after I updated ledger live desktop app and the firmware on ledger nano s device. All 6 of my wallets; ledger live desktop app, myether wallet, Tronscan, Veforge, O3 Neo, and stellar lumens wallet, were all cleared out on the same day — (two days after update, unfreezing of tokens began the same day as the update!!). There is no way someone would know all of this information. I kept 1-2 apps on my device at all times and hardly ever accessed any of the wallets. And kept no trace of them anywhere digitally.

I know that it is possible for someone internally to access these devices due to the closed source that Ledger is. I'm fully aware of the centralization of most wallets and anything that has to do with cryptocurrency and Ledger is NO different. — This information comes from insiders throughout the crypto community. There is NO platform or device that is 100% safe. Ledger being closed source, makes it that much more obvious that this was done from within (past or present insiders).

Ledger GAVE me the 24 words on the device during set up (I didn't choose the words myself), so of course it can be compromised from within.

I know that Ledger is not responsible in EVERY situation of lost funds, as users can easily misuse and misplace their information Or fall victim to a scam. However, none of those situations match with what has happened to me.

I am willing to supply Ledger with all screen shots and a timeline of exactly what happened. I will also give my entire 24 word phrase, my pin code for ledger nano S device, and my log in information for ledger live desktop app. I am willing to share this information because it has already been stolen anyways so it is no secret any longer, it never was a secret anyways since it can be internally compromised by Ledger. With this information a representative from Ledger can look into this situation themselves.

Upon completion of whatever examination Ledger needs to perform to see that I am being honest, I am demanding to have every single token that was stolen returned to me.

If my request isn't met I will then take both legal and personal action against Ledger for their lack of security and lack of caring about a customer/user. And their lack of taking responsibility for it.



I will take legal action by getting in contact with my legal team who deals with tech companies.

I will take personal action by spreading the word about what happened to me (in great detail). I have several connections to channels that have large followings in the crypto community and this word will be spread quickly. This information will be spread to let others know what happened to me and to let them know that at any time it can (and probably will) happen to them. I will let others know that following ledgers safety guidelines perfectly is not safe, it's still possible to be robbed.

The money that will be lost from lack of Ledger sales and a bad company reputation will be far more of a loss than the money surrendered to pay back the tokens that were stolen from me.

Im looking forward to hearing back from you with a way to resolve this issue. I sincerely hope that legal and personal action isn't needed to be taken on my part but I'm fully prepared to go that route if needed!

I would much rather spread the news about how much ledger helped me, how much ledger cares about there customers who follow directions perfectly, and that they have their customers back!

Thank you for your help”

**Ledger:** Case was sent to a new support specialist.. (no pic due to size) — \*\*This is the email admitting that the devices are useless for protection (some knew this already, some don't know this.. Remember peeps — you don't choose your own words — something to think on...)\*\* \*\*All of my previous points that they are replying to in this email will be bold and underlined\*\*)

“will now address each of your points:

**I have come to the conclusion that my coins have been stolen by someone within the ledger company (past or present), or knows how to access ledger code.**

Could you please precise what you mean by Ledger code?

As informed in this [article](#) and in [this Academy article](#), Ledger has no information linked to your accounts.

Stating that someone at Ledger stole your assets is actually a pretty serious allegation.

**It was either done manually or they set a malicious malware, spyware, etc, into the update that immediately went and began the stealing process of my coins, which started right after I updated ledger live desktop app and the firmware on**

**ledger nano s device. All 6 of my wallets; ledger live desktop app, myether wallet, Tronscan, Veforge, O3 Neo, and stellar lumens wallet, were all cleared out on the same day – (two days after update, unfreezing of tokens began the same day as the update!!). There is no way someone would know all of this information. I kept 1-2 apps on my device at all times and hardly ever accessed any of the wallets. And kept no trace of them anywhere digitally.**

It is possible that you have been the victim of a [phishing attempt](#), if that is the case this is unfortunately not Ledger's responsibility to know who is behind it. However, we always try to take any malicious website down once the information is shared with us, as you can see in this [Tweet](#) for example.

**All 6 of my wallets; ledger live desktop app, myether wallet, Tronscan, Veforge, O3 Neo, and stellar lumens wallet, were all cleared out on the same day – (two days after update, unfreezing of tokens began the same day as the update!!). There is no way someone would know all of this information. I kept 1-2 apps on my device at all times and hardly ever accessed any of the wallets. And kept no trace of them anywhere digitally.**

As explained before, if someone knows your private keys/your recovery phrase, they can easily steal all your assets as **this is the only back up to your accounts.**

**I kept 1-2 apps on my device at all times and hardly ever accessed any of the wallets. And kept no trace of them anywhere digitally.**

Someone who has access to/knows your recovery phrase do not need to own a Ledger device with apps installed to access your assets: [Anyone who gets your recovery phrase can take your crypto assets. Ledger does not store your private keys, nor ever asks for it.](#)

**I know that it is possible for someone internally to access these devices due to the closed source that Ledger is. I'm fully aware of the centralization of most wallets and anything that has to do with cryptocurrency and Ledger is NO different. – This information comes from insiders throughout the crypto community. There is NO platform or device that is 100% safe. Ledger being closed source, makes it that much more obvious that this was done from within (past or present insiders).**

**Ledger GAVE me the 24 words on the device during set up (I didn't choose the words myself), so of course it can be compromised from within.**

The Ledger Nano S and Nano X are the only hardware wallets to have received a Security Certification as you can read [here](#). Our OS (Bolos) is open source as you can [read here](#) and [here](#) as well.

**Ledger GAVE me the 24 words on the device during set up (I didn't choose the words myself), so of course it can be compromised from within.**

Private keys are equally derived from another key. The key these are derived from is called the Master Seed. Through the Master Seed, it is possible to generate an [infinite number](#) of private keys.

This [Master Seed](#) itself consists of a list of 256 bits (like flipping a coin 256 times). To make it humanly readable it can be represented with a list of 24 words as is the case for our hardware wallets. These are obtained when you first use your Ledger device. We call those 24 words the Recovery phrase.

This **Recovery phrase** (24 words) has to be carefully written down ([correct order, no misspellings](#)) and protected after you initialize your hardware wallet. That's the purpose of the **Recovery sheet**.

A [standard](#) was developed (and not by Ledger) to detail how to generate private keys from a Master Seed.

**The money that will be lost from lack of Ledger sales and a bad company reputation will be far more of a loss than the money surrendered to pay back the tokens that were stolen from me.**

**Im looking forward to hearing back from you with a way to resolve this issue. I sincerely hope that legal and personal action isn't needed to be taken on my part but I'm fully prepared to go that route if needed!**

**I would much rather spread the news about how much ledger helped me, how much ledger cares about there customers who follow directions perfectly, and that they have their customers back!**

Here I will repeat what my colleague sent to you previously:

As underlined in article 8 of our [Terms and Conditions](#), we would like to remind you that users of Ledger products are solely responsible for the way they use their devices and protect their data and information. Users must take all necessary steps to ensure that their PIN code and their 24-words recovery phrase remain confidential and are stored in a secure location, away from prying eyes.

Furthermore, in order to offer an optimum level of security to its users, Ledger does not have access to users' confidential 24-words recovery phrase nor to their PIN code. Consequently, Ledger cannot be held liable for losses resulting from unauthorized third parties accessing your confidential information.

I hope my reply provided additional insight to your request. Unfortunately, the reason why we cannot help further is not because we do not want to do so, but simply because there is nothing that can be done by Ledger at this point.



Please let me know if you still wish to contact our Legal department regarding this matter.

**Me:** (No pic due to size)

“Thank you for your fast response, I appreciate it. However I am not satisfied with this customer support case at the moment. As you hopefully understand why this is...

Im aware that it is a serious allegation to assume that someone from Ledger stole my funds, I actually stated that it was either someone from Ledger or someone that has been affiliated with ledger (past or present). It may also be someone that knows someone within the company, these are all strong possibilities and the only ones that make sense upon hours of investigation into documented reports from others who have lost their Ledger held funds in various ways — (Scams, hacks, phishing).

\*\* It’s also a serious crime (for whoever stole the funds) and a serious loss of trust in the company as whole if this isn’t resolved. Nothing personal to you; but this is why a serious allegation was made by me.

What I meant by “ledger code” is the following... “1) In programming, **code** (noun) is a term used for both the statements written in a particular programming language - the source **code** , and a term for the source **code** after it has been processed by a compiler and made ready to run in the computer - the object **code**” (<https://whatis.techtarget.com/definition/code>) — All tech has code written in it and whoever is able to access that can do anything.

This is especially true when the code is **closed sourced** and not available for the public to view and audit like other open sourced wallets are. This is why the allegation is made of someone internal or affiliated with Ledger.

I’ve already stated a few times in previous emails that I’m certain I was not a victim of a phishing attack. This all happened on the official ledger live desktop app after I updated the software and then updated my ledger device — as stated in a previous email.

Side note: I’ve seen a phishing attempt on Tronscan in the past and I instantly clicked out of that. FYI

This following statement destroys the entire purpose of having a Ledger device at all.. **“Someone who has access to/knows your recovery phrase do not need to own a Ledger device with apps installed to access your assets.”** — *The entire purpose of having the actual Ledger device is to put in your pin code and then click “accept” for any transaction. So the statement above is admitting that the physical Ledger wallet isn’t at all secure nor needed.*

My 24 phrase code was stolen by whatever happened during the firmware update on my device. I was forced to put my pin code and 24 word phrase into my ledger device in order to use my wallet after updating ledger live to its newest edition (on September 26th 2019). That same day my coins were unfrozen, two days later (September 28th 2019) all of my coins on multiple wallets were stolen.

My 24 word phrase has never seen digital format of any kind and was/is stored in a safe place; on the recovery sheet that came with my ledger nano S. — No one has seen my words.

I'm aware of what Ledgers terms and conditions say, however it appears to be a scapegoat to escape any responsibility for a failed system that actually leaves NO customers funds safe — even those who do everything exactly how Ledger recommends.

Is it possible that my case is new and hasn't been documented yet by anyone — therefore some at Ledger are unaware that this is possible? It appears this is so at the moment.

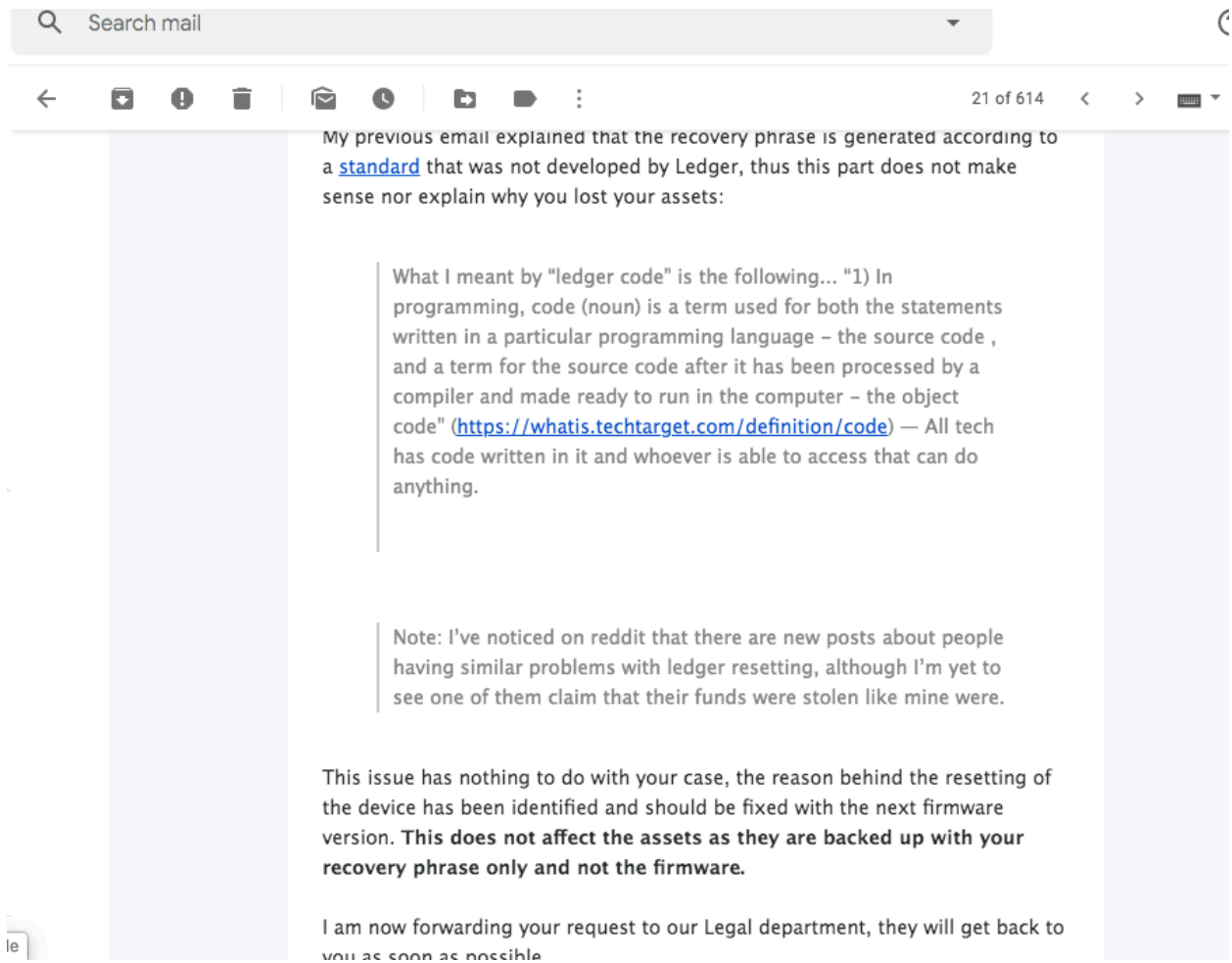
**\*\*\*\* I stated in my previous email that I'm willing to give ALL of my information to be looked at in depth by Ledger and/or their legal team (if the legal team knows how to use Ledger and all of it's supported wallets.) Someone needs to look at this or else it will be easily dismissed as just another hack or phishing robbery (as it is being dismissed as now). Is there anyone on your end that can help me with investigating all of this information that I am willing to provide??**

It would be a good idea for Ledger as a company to look into this situation that happened with my wallet. There may be others in the near future with the same issue. Not many people in the crypto world speak up when they are stolen from because it's easy for crypto companies to deny any responsibility. But once enough money is taken, as in my case, more people will be coming forward.

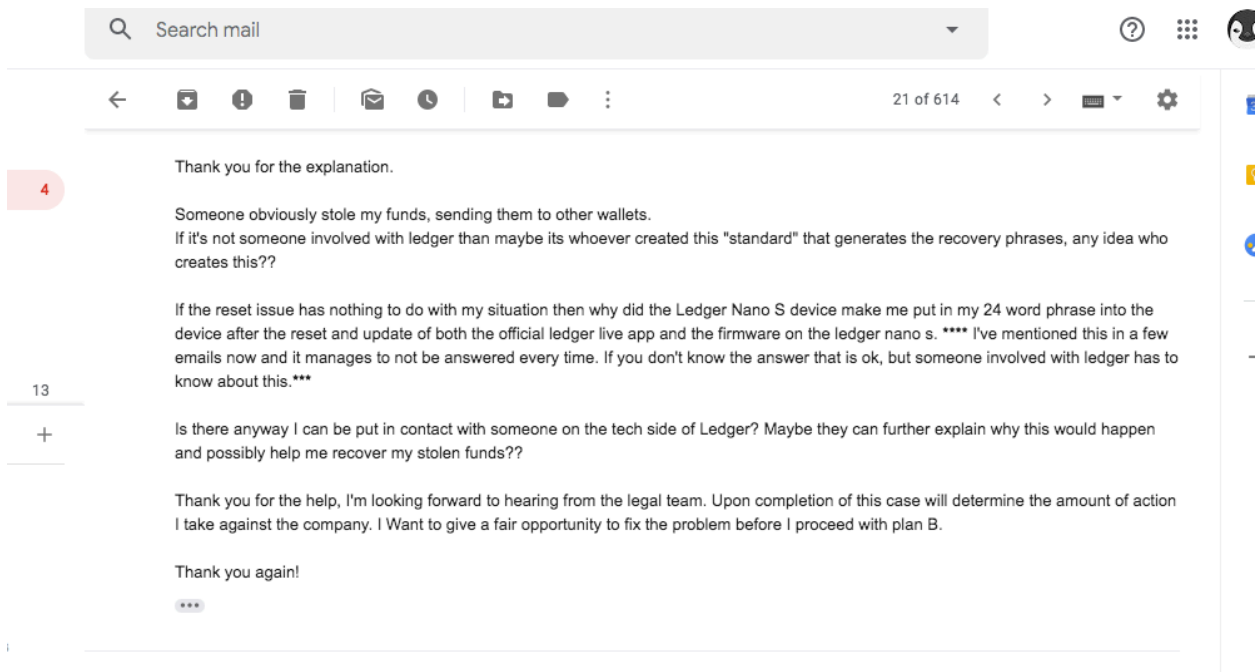
Note: I've noticed on reddit that there are new posts about people having similar problems with ledger resetting, although I'm yet to see one of them claim that their funds were stolen like mine were.

Let me know where to go from here, if you're unable to further help me then please get me in contact with someone else.  
Thank you for your time and efforts,

**Ledger:** \*\*Of course my offer to provide information was ignored. Wouldn't a company that cared actually want to look into a claim such as this?? — Scared of seeing something that might be of concern...?\*



**Me:** \*\*Me being nice and asking again for someone to look into this case\*\*



**Ledger:** (no pic due to size) \*\*ignored again and sent irrelevant information\*\* (My statements that they are replying to are in bold and underlined)\*\*

"Thank you for your reply.

**Someone obviously stole my funds, sending them to other wallets.**

**If it's not someone involved with ledger than maybe its whoever created this "standard" that generates the recovery phrases, any idea who creates this??**

Our Legal team will address all your questions regarding the standard that generates the recovery phrase. Please allow a couple of days to receive a reply. You may contact them directly at [legal@ledger.fr](mailto:legal@ledger.fr) as well.

**If the reset issue has nothing to do with my situation then why did the Ledger Nano S device make me put in my 24 word phrase into the device after the reset and update of both the official ledger live app and the firmware on the ledger nano s. \*\*\*\* I've mentioned this in a few emails now and it manages to not be answered every time. If you don't know the answer that is ok, but someone involved with ledger has to know about this.\*\*\***

**Is there anyway I can be put in contact with someone on the tech side of Ledger? Maybe they can further explain why this would happen and possibly help me recover my stolen funds??**

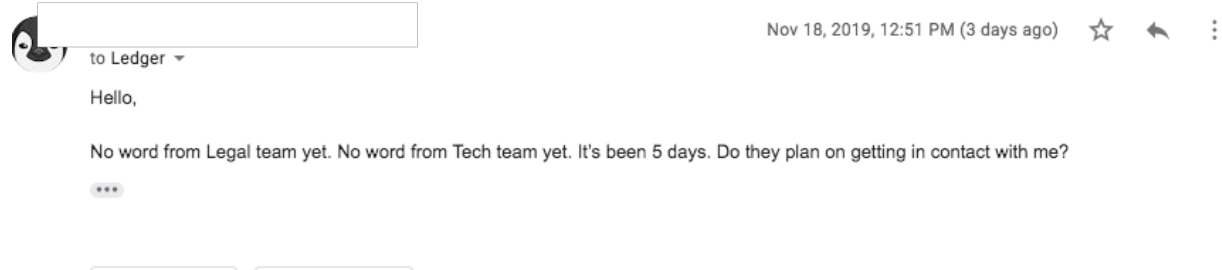
There is currently a firmware issue that triggers the device to be reset after a firmware update or when it is plugged. This happens randomly after the device gets rebooted multiple times.

This issue should be fixed if you update your device to the firmware version 1.6.0, that was launched today as communicated [here](#).

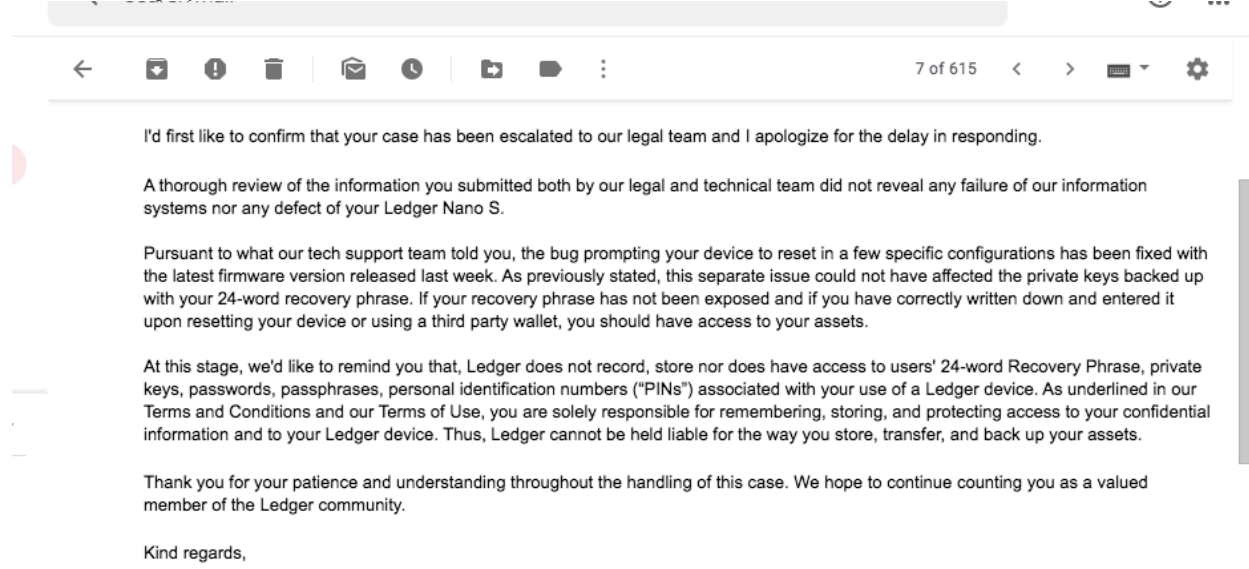


I remain at your disposal should you need additional information.  
Kind regards,

**Me:** 5 days later I had heard nothing back so I reached out again..



**Ledger:** Responded the next day... \*\*at least I'm a valued member of the Ledger community :)\*\*



**Me:** Sent this the same day and haven't heard anything back yet...

Thank you for the response.

All of my coins were sent to different addresses....So unless I have access to those addresses then I have zero access to the coins. Right now I have no access to these addresses.

My offer of giving all of my information over to ledger to be reviewed by someone who knows what they are doing is continually ignored.

This needs to be checked out by someone on the team, they may see something that they are currently considering impossible to happen or writing off as the common "user error" - which this is not user error.

Any way to get in contact with someone who can review this for me in depth?

Thanks again

...

← Reply

➡ Forward

This is where it ended. No tech team and no legal has contacted me. Im doubtful I'll be contacted again and they repeatedly ignored my offer to take all of my information and investigate this for themselves...

***All coins are out of my possession for good!!***

Here are some questions to ponder for yourselves. It's recommended to leave ALL emotions and biases out of the answers.

- Does this seem like a customer support system that really cares?? — I'll let you decide that for yourself.
- Does it concern you to know that a wallet company (any company) can easily dismiss any technical flaw as "user error"??
- Is it concerning that no matter how "safe" you have kept your information that you can still be robbed, and never get the coins back?
- How would you feel if this happened to you? — would it then still be "impossible"?

Does user error exist? — yes! And in most cases of lost (often stolen) funds it probably is user error. But user errors, hacking, phishing, and scamming, are not the only ways to lose funds. There also is the possibility of glitches and the possibility of both internal/external theft (by those who know code) and also the chance that the word phrases can be discovered.

**This happening right after an update and forced device reset makes it all the more interesting...**

If you have read this entire post and you still have a question to clear something up then feel free to message me. Or comment.  
If you're here to be a keyboard expert or bully then feel free to contact me as well — Although I cant promise I will entertain that for long.

When someone from Ledger sees this and feels they are able to further assist me please feel free to get in contact with me. I am still open to resolving this issue.

Also: What's a crypto related story of any kind worth without a donation opportunity at the end??

If you found this piece helpful and feel generous and able enough to give a donation it would be much appreciated as any tiny bit helps. And no... these are not Ledger addresses ;)

BTC — 1HXXjrNMKxuZbNPmSyBMumsw8jMARhwqNr  
ETH — 0xe307cbfb17f151a5e99c6174613e1be0a569aceb  
LTC — LdvDQ8RmkaJi8jesg3YzzMghhrpLqLd87h

Best wishes to all!