

**From:** jesse@yourpersonalcryptoassistant.com  
**Sent:** Friday, October 15, 2021 10:42 PM  
**To:** 'jesse@yourpersonalcryptoassistant.com'  
**Subject:** Save Your Crypto and other thoughts - from Your Personal Crypto Assistant

Welcome back. I hope you are enjoying these occasional emails – as always all feedback positive and negative is greatly appreciated. Feel free to forward to others that you think might enjoy reading this. If you'd like to be removed, just reply and tell me...

**Save Your Crypto** – I was interviewed yesterday by [Lee Siler \(The Stock Dr's Prescription\)](#) about the story of Erick and Molly Richardson who had [21 Bitcoin stolen](#) earlier this year. The theft occurred some months back, but it's in the news because of people complaining Coinbase's customer support now. For me, I'm not worried about a customer support issue, I'm concerned about people having their crypto stolen. I feel bad for the Richardson's and as I mentioned in my last email I have been doing some work recently helping people manage and protect their coins. I have some tips here to get you started, but if you want more help please feel free to email me specific questions - I'm happy to answer. For more detailed assistance I can set up a consulting appointment and we can go as deep as you like.

The first set of things to do is for any online account – not just your crypto exchange, but all your online financial accounts, brokerage, IRAs, Banks, Credit Unions, Credit Cards.

1. Use strong passwords. At least 10 characters long and preferably 12 or more, using lower case, UPPER CASE, special characters like “#!+” and digits like 12345. Of course “12345” is not a good password, and any words found in a dictionary, or proper names should not be used. Random is best, but could be hard to remember, so -
2. Use a [password manager](#). This is a program that encrypts all your other passwords and you only need to remember one master password.
3. Do NOT reuse passwords. If a criminal gets your user id / password to a game account or your public library account – they may go ahead and try the same password at financial institutions.
4. Use two factor authentication if available (2FA). The most common version of this is getting an SMS text message on your phone with some second code to enter. This is better than not doing 2FA, but there are [SMS weaknesses](#). Generally an authenticator app on your phone or a dedicated hardware token is a better option.
5. Don't believe me on the above – [ask Harvard](#). Seriously. After writing the above, I was looking for a good link to add in for strong passwords and found Harvard's recommendations.

For crypto you can also keep your wealth off the exchanges and in your own wallet(s). You keep the private keys and have ultimate control. You may have heard the phrase - Not Your Keys Not Your Coins, you keep the keys safe and no one can take away your coins. Think of this as keeping cash in your wallet instead of money in the bank (online account). It's good to have some walking around money, but you also don't want to keep your life savings in your purse or the wallet in your pocket, so -

1. Move your long term savings to a different wallet than your normal every day account and protect it more strongly. Think of this like a safe in your house.
2. One way to protect your savings wallet is to have it be a ['cold' wallet](#) – one that is not normally connected to the internet. The most common way to do cold wallets today is to use a hardware device to allow you to do your crypto transactions 'offline'. These generally look like a USB stick and keep your private keys from being accessible online. If your desktop, laptop or phone is hacked and your private keys are there, the hacker has access to your crypto. If the private keys are on an external hardware device you are still protected.

There is a less common but another interesting approach to protecting a crypto wallet. Just like a business checking account may have 3 officers authorized to sign checks, and each check needs two signatures to be valid, you can set up a crypto account with multiple signatures required. You can configure a 2 of 3 wallet and then keep the keys in different locations to protect against theft or loss. There are now companies beginning to offer solutions based on this to help you guard your crypto.

In summary – protect your property – but be careful not to be too paranoid and protect your crypto so well that even you can't figure out how to get back to it. Just like the horror stories of people getting their savings stolen, I've heard many stories of people losing and/or forgetting the information they need and not being able to get to their crypto.

**El Salvador** hasn't been in the news much recently and I was trying to learn how things are going there. It seems to me that most El Salvador reporting is just a mirror - those who want to see success see the successes and those who want to point out

the failures see those instead. One article I found on [NASDAQ.com](https://www.nasdaq.com) was reasonably balanced but missed a spot of what I think is amazing news. They reported on the remittances (when citizens working overseas send money to their families back home) and the importance of them to the economy – approximately \$6 billion per year, 25% of annual GDP. The article mentioned that \$2 million per day is now being sent via the new bitcoin app (Chiva) introduced in El Salvador. Curiously, they didn't do the math to mention that at \$2 million per day that's about 10% of remittances are now in Chiva. So in less than a month the new app already has 10% market share of remittances – wow! Watch out Western Union and other money transfer companies.

If you are investing in crypto now, I suggest caution. Bitcoin is heading back up and recently broke \$60,000 again. It's easy to get caught up in the hype and excitement and FOMO (fear of missing out) and buy, buy, buy. Crypto has been very volatile and is likely to stay that way for quite some time. I don't think you should avoid buying in now, just make sure you think things through and manage your risk. There are a huge number of coins and tokens out there and I expect many, most to fail and eventually go to zero. As in my last email I continue to purchase more crypto as I see favorable entry points (buy the dip), but am mostly focused on Bitcoin, Ethereum and a limited number of other coins. Personally, I remain long term bullish on crypto and still expect new all-time highs by year's end.

I enjoy sharing my thoughts and what I'm doing, but only for your education. I don't offer financial, legal or tax advice. You need to evaluate your own situation and risk tolerance and as always it's important to DYOR (Do Your Own Research) and not put any money into crypto that you are not willing to lose.

I enjoy answering crypto questions, so feel free to email me or call me, I like to help. Personal instruction and assistance is my specialty – so if you or someone you know is looking for more than an email response to a question I can also provide one on one consulting and have a number of [consulting packages](#).

Thanks,

Jesse

Jesse Markowitz

(407) 900-9453

[Jesse@YourPersonalCryptoAssistant.com](mailto:Jesse@YourPersonalCryptoAssistant.com)

<https://YourPersonalCryptoAssistant.com>

Helping you understand and excel with Bitcoin and other crypto technologies

PS: If you want to hear me join Lee Siler on his radio show, the interview that taped yesterday should air this weekend on the Florida Man network. In the [Florida panhandle](#), it's on 103.1FM Saturday at 1pm EDT. In [Orlando](#), it's on 660AM / 105.5 FM Sunday at 7am. You can also listen to it as a podcast on [Spotify](#), [Apple](#), [Overcast](#) and probably other podcast platforms.