

The Beginner's Guide to **Protecting Your Crypto**

Securing your crypto using cold storage and learning crypto security best practices is more important than ever. Learn how to get started with our beginner's guide.

[Read more >>](#)



A person with long dark hair is writing in a notebook on a wooden desk. The image is overlaid with a semi-transparent blue filter. Two vertical purple lines are positioned on either side of the text.

Cold storage refers to the practice of **keeping cryptocurrency offline** minimizing the risk of hacking and digital theft.

About Us

CryptoConsultz is a full service cryptocurrency and Web3 consulting firm servicing both individuals and businesses. Whether your new to crypto or looking for a team of experts to up your crypto game, our specialists are here to help.

Security through knowledge is now a key tenant of the firm but we've got a variety of services to help you meet your investment goals.

01 History

We're the leading source for crypto education. Founded in 2017 and featured on major news outlets such as CNN, CNBC, Bitcoin.com and more!

02 Intro to Cold Storage

Learn what cold storage is and why its important. Keep your private key safe with CryptoConsultz.

03 Types of Crypto Threats

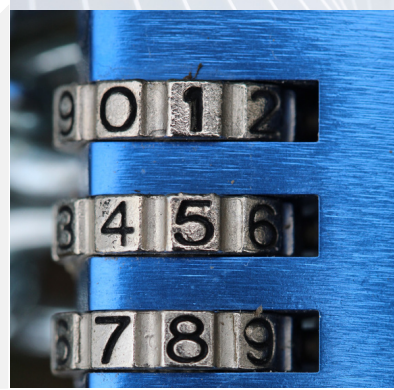
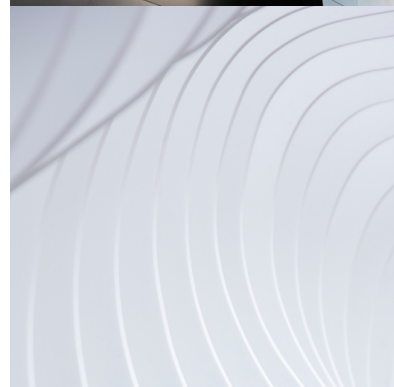
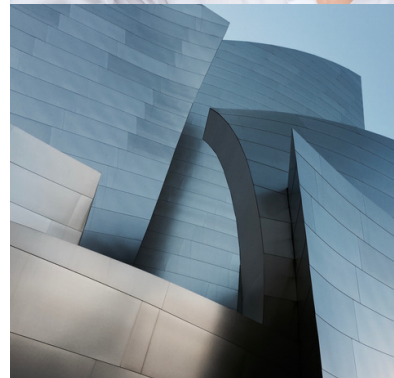
Understand the various types of threats lurking in cyberspace and how you can protect yourself.

04 Why not an exchange?

Learn how you are high risk if you're using an exchange to hold your crypto.

05 Where do I start?!?

Unsure where to get started? We'll give you actionable steps to jumpstart your crypto security and cold storage plan.



All that fun **Legal Stuff**



COPYRIGHT © 2023

See full [Terms of Service](#) & [Privacy Policy](#) for more information.

Information provided through informational consulting sessions, written or electronic delivery of content is for informational purposes only and should not be considered legal or financial advice. You should consult with an attorney or other professional to determine what may be best for your individual needs. CryptoConsultz LLC does not make any guarantee or other promise as to any results that may be obtained from using this service. No one should make any investment decision without first consulting his or her own financial advisor and conducting his or her own research and due diligence. To the maximum extent permitted by law, CryptoConsultz LLC disclaims any and all liability in the event any information, commentary, analysis, opinions, advice and/or recommendations prove to be inaccurate, incomplete, or unreliable or result in any investment or other losses. Customers are required to review Terms of Service, Legal Considerations, Risk & Disclaimer carefully prior to use of CryptoConsultz LLC services.

Your use of the information provided or materials is at your own risk.

The Company does not recommend purchasing Tokens, Coins or other forms of currency or property for speculative investment purposes. Cryptocurrency, virtual/digital currency, and Tokens are sold as digital assets, similar to downloadable software, digital music and the like. The Company does not recommend that you make such purchases unless you have prior experience with cryptographic tokens, blockchain-based software and distributed ledger technology and unless you have taken independent professional advice.

The Company does not provide any opinion or any advice to purchase, sell, or otherwise transact with virtual/digital currency and the presentation, publication or communication of all or any part of the Available Information shall not form the basis of, or be relied upon in connection with, any contract or investment decision.

NO ADVICE

No part of the Available Information should be considered to be business, legal, financial or tax advice regarding the Company, the coins/tokens/digital currency/virtual currency or any of the matters to which all or any part of the Available Information relates. You should consult your own legal, financial, tax or other professional advisor regarding the Available Information.

LIMITATION OF LIABILITY

In no event shall the Company or any current or former employees, officers, directors, partners, trustees, representative, agents, advisors, contractors, or volunteers of the Company (hereinafter the "Company Representatives") be liable for: (i) any loss of profits, lost savings or incidental, indirect, special or consequential damages, arising out of your use or inability to use the services or products offered by the Company or the breach of any of these Terms by you or by any third party; (ii) any security risk such as hacker attacks, loss of password, loss of private key, or similar; (iii) mistakes or errors in code, text, or images involved in the in any of the Available Information; or (iv) any information contained in the Available Information or any expectation promise representation or warranty arising (or purportedly arising) therefrom; (v) any losses resulting from the volatility in pricing of Coins, Tokens, Cryptocurrency, Virtual/Digital Currency or other currency in any countries and on any exchange or market (regulated, unregulated, primary, secondary or otherwise); (vi) any losses or damages arising out of or in connection with the purchase, use, sale or otherwise of the Coins, Tokens, Cryptocurrency, Virtual/Digital Currency or other currency; or (vii) arising out of or in any way connected to your failure to properly secure any private key to a wallet containing Coins, Tokens, Cryptocurrency, Virtual/Digital Currency or other currency, (collectively, the "Excluded Liability Matters").

NO REPRESENTATION & WARRANTIES

The Company does not make or purport to make, and hereby disclaims, any representation, warranty or undertaking in any form whatsoever to any entity or person, including any representation, warranty or undertaking in relation to the truth, accuracy and completeness of any of the information set out in the Available Information.

RESTRICTIONS ON DISTRIBUTION AND DISSEMINATION OF THE AVAILABLE INFORMATION

The distribution or dissemination howsoever of all or any part of the Available Information may be prohibited or restricted by the laws, regulatory requirements and rules of certain jurisdictions. In the case where any such restriction applies, you are responsible for informing yourself in respect of the same and for observing any such restrictions which are applicable to your possession and/or dissemination of all or any part of the Available Information at your own expense and without liability to the Company. Persons to whom a copy of all or any part of the Available Information which has been distributed or disseminated, provided access to or who otherwise have all or any part of the Available Information in their possession shall not circulate it to any other persons, reproduce or otherwise distribute any information contained herein for any purpose whatsoever nor permit or cause the same to occur.



History

In 2016, Nicole DeCicco was a single mom working as a nurse, mining Ethereum in her garage. Her career change occurred after a hacker stole 323 ETH from her, worth well over \$1 million. Driven to make cryptocurrency education more accessible, DeCicco launched CryptoConsultz in 2017. She's passionate about helping others navigate the crypto investing landscape successfully while minimizing the risk of hacking, scams and other common pitfalls in this rapidly evolving industry.

Featured on major news outlets like CNN, CNBC, and more!

[Check us out here >>](#)

We're here to help!

Crypto Security

Learn how to protect your investment using the most effective security devices and strategies. We're the market leaders in crypto security training

Portfolio Management

Let's grow together! We will start with an analysis of your current portfolio, and then compare it to a projection based on your targets, values, and risk tolerance to help you get to where you want to go!

Incident Analysis

Have you been a victim of crypto fraud or a scam? We're here to help. At CryptoConsultz we have experts with extensive experience in fraud investigations.

General Crypto & Blockchain Education

New to crypto? We've got everything you need. Our efficient, personalized training sessions will get you comfortable with the basics, including wallets, exchanges, and general blockchain principles.

Crypto Taxes

Our team of experts are here to help you with all your crypto tax needs, from filing your taxes to getting the best return on your investment.

Business Services

We help businesses create, accept, and utilize cryptocurrency tokens to improve and grow their business operations.





Why cold storage?

Because private keys and other sensitive information are not stored online, hackers have no way to access them. This makes it much more difficult for them to steal your funds or otherwise gain unauthorized access to your wallet.



WHAT IS COLD STORAGE?

Cold storage refers to the practice of keeping a reserve of cryptocurrency offline, in order to protect it from hacking and other forms of digital theft.

WHY COLD STORAGE?

By keeping private keys and other sensitive information offline, you can protect your funds from the many threats that exist on centralized exchanges, including hacking, phishing, and malware attacks.



WHAT TYPE OF COLD STORAGE?

There are several different types of cold storage solutions available, ranging from hardware wallets and paper wallets to cold storage coins. Each of these options has its own pros and cons. Learn what's best for your crypto investments.

Introduction to **Crypto Security**

THE FIRST STEP TO TAKING CONTROL OF YOUR CRYPTO ASSETS IS EDUCATION

Understand the risks of crypto investments and learn how to minimize them.

There's a multitude of risks associated with investing in and holding digital assets. Issues with centralized exchanges, hacking, phishing, malware attacks and user error are just a handful of threats causing serious vulnerabilities for crypto investors.

Cold storage is a critical component of your cryptocurrency security plan, particularly for those who hold significant amounts of digital assets. By keeping your private keys and other sensitive information offline, it makes it much more difficult for attackers to access your funds and gives you full control of your assets.

In this eBook, we will explore the different types threats crypto investors are up against, show you what cold storage options you have available and explore the steps you can take to set up and manage your own cold storage wallet.

Crypto security is more than just cold storage though. Learn what other steps to take to protect your crypto assets now!



Introduction to **Crypto Security**

UNDERSTANDING PRIVATE KEYS

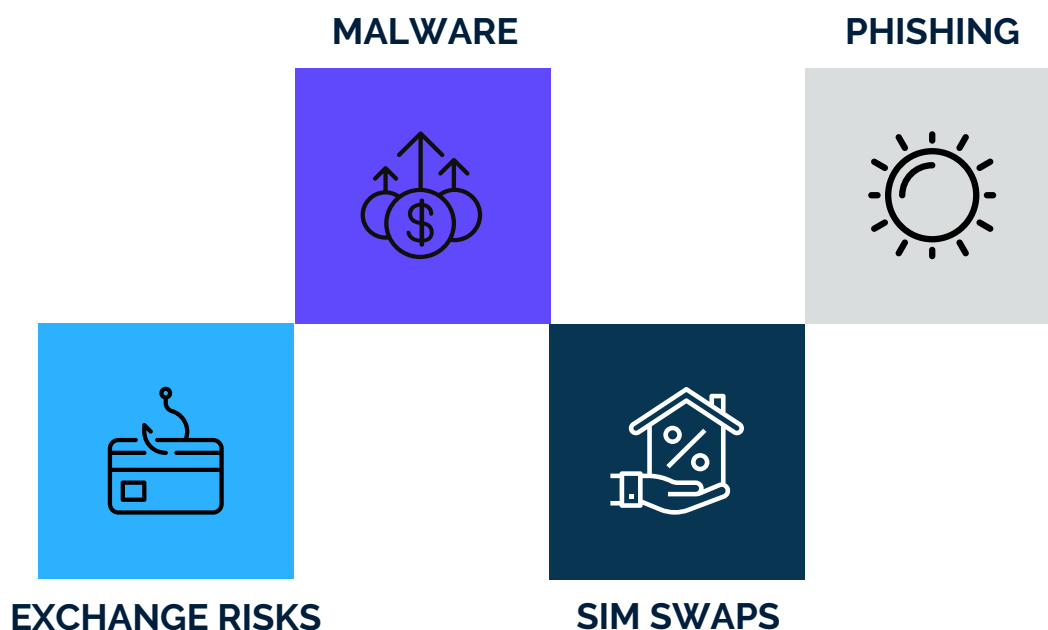
Your private key is like the password to unlock your crypto wallet.

We have a saying in the crypto investment world, "Not your keys, not your funds." Anyone that has access to your private key has access to your crypto.

When you invest with a centralized exchange, you typically aren't given access to your private key which means you only have access to your funds at the discretion of the exchange.

Cold storage protects your private key and gives you full control over your crypto for the ultimate level of security and self-custody.

TYPES OF CRYPTO THREATS



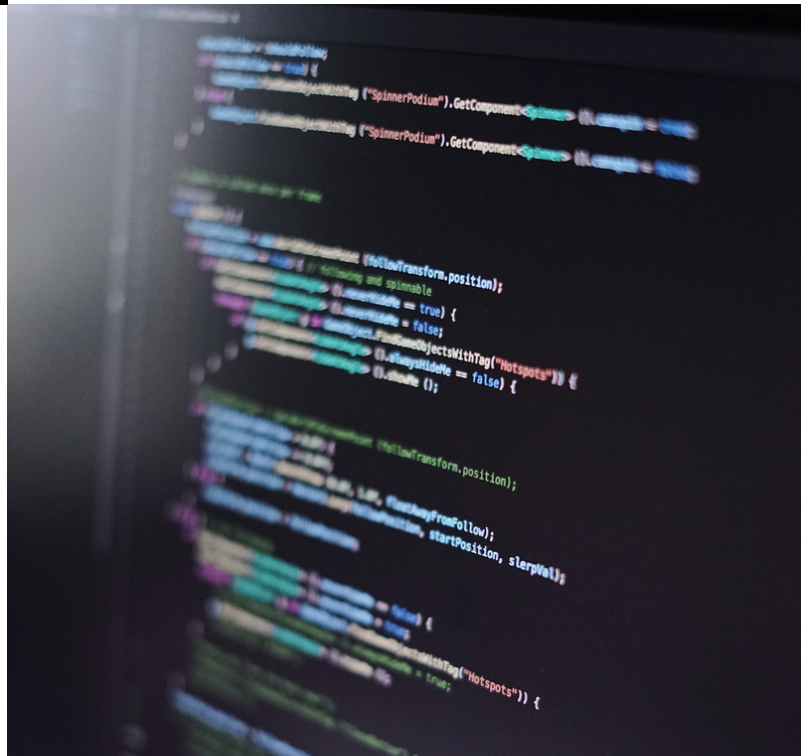


HACKING

The term hacking refers to unauthorized access to a computer system or network. It involves stealing private keys or login credentials to gain access to wallets or exchanges and steal users' funds.

MALWARE

Malware refers to any type of software designed to harm or exploit a computer system, network, or device. Malware can be used to steal private keys, login credentials, or cryptocurrency wallets.



SIM SWAPS

SIM swapping is a social engineering technique where an attacker convinces a mobile carrier to transfer the victim's phone number to a SIM card under the attacker's control. This can be used to access the victim's cryptocurrency accounts by intercepting verification codes sent via SMS.



PHISHING

Phishing is the act of tricking people into revealing sensitive information such as login credentials or private keys by posing as a trustworthy entity. In the crypto world, phishing attacks can take the form of fake exchanges, wallets, copycat websites or malicious emails.

IP TRACKING

IP tracking is the act of monitoring internet traffic to identify the location and activities of a user. IP tracking can be used to determine the IP addresses associated with a particular wallet or exchange account and potentially trace the user's identity.



USER ERROR

User error refers to mistakes made by cryptocurrency users, such as sending funds to the wrong address or storing private keys insecurely. This can result in the loss of funds or the compromise of the user's account.

Dangers of Centralized Exchanges



There are several dangers associated with using centralized cryptocurrency exchanges, which are operated by a single entity that holds custody of user funds and manages the exchange's trading activities

Dangers of Centralized Exchanges

When using a centralized exchange, users must rely on the exchange's management to protect their funds and make sound trading decisions. Users have no direct control over their assets, and if the exchange's management makes poor decisions or engages in fraudulent activities, users may suffer losses.

There are several dangers associated with using centralized cryptocurrency exchanges, which are operated by a single entity that holds custody of user funds and manages the exchange's trading activities. Several high-profile exchanges have been hacked or shut down in the past, resulting in millions of dollars in losses for users.

Cryptocurrency exchange platforms can restrict access to investors' funds, go bankrupt, or face liquidity problems. Exchanges can face outages, restrictions by region or delist tokens which can fluctuate with the rapidly evolving regulatory landscape. Users are often given very little notice and locked out of their accounts, sometimes indefinitely! Worse yet, they typically offer little to no customer support and/or extremely long wait times.

Every time you access your cryptocurrency online using an exchange platform you are opening the door of vulnerability to a hacker. Not only is an exchange vulnerable to these risks but you, as the user, are even more exposed. Exchanges DO NOT take responsibility for vulnerabilities on the user end which is typically what occurs when you hear of someone being hacked.

Centralized exchanges are subject to regulatory oversight, which can impact their operations and the ability of users to access their funds. In some cases, exchanges may be forced to comply with regulations that restrict user activities or impose fees on transactions.

Centralized exchanges can experience technical difficulties or downtime, which can prevent users from accessing their funds or executing trades. This can result in significant losses for users who are unable to react to changes in the market.

Cold storage reduces the risk of losing your investments due to exchange-related issues, making it a more secure option. By using cold storage, you have complete control over your private keys and can access your funds at any time, without depending on an exchange.



UP NEXT

How to **Get Started** with Cold Storage



Here's How to Get Started:

Follow these steps to get started and remember CryptoConsultz is here to help along the way. Don't waste valuable time and resources buying the wrong products, fumbling around with setup or, worse yet, making a mistake and losing your crypto assets! Work with one of our experts today!

STEP 01

Choose a cold storage solution (or solutions) that work best for you.

STEP 02

Set up your cold storage device.

STEP 03

Transfer your crypto funds from your exchange or hot wallet to your cold wallet.



NEED HELP?

Getting started on the right track can be overwhelming!

Our team of experts can assess your individual situation, determine where your vulnerabilities are, help you pick the right products, guide you through set up and teach you safe practices while moving your crypto to cold storage.

Our crypto security package does more than protect your crypto, it helps you secure your online footprint in all areas of your digital activity.

Get one on one assistance with your dedicated crypto expert.

GET HELP



Here's How to Get Started

✓ CHOOSE A COLD STORAGE SOLUTION

The first step in setting up cold storage is to pick a solution that meets your needs. Consider all the assets in your portfolio. There's not a one size fits all cold storage solution for all crypto assets.

✓ SET UP YOUR DEVICE

The setup process for your cold storage device is highly device dependent. This is a crucial step in the process and it's important you follow all the instructions carefully.

✓ TRANSFER CRYPTO FUNDS

The final step in setting up cold storage is to transfer your cryptocurrency from an online wallet (such as an exchange wallet) to your offline wallet.

✓ SAFE & SOUND

Store your cold storage device and any other sensitive information you generated in a secure location such as a fireproof safe.



It is important that you follow the instructions for your chosen cold storage solution. Mistakes can happen.

Be sure you don't become your own worst enemy. It's important you learn the fundamentals of crypto technology and work with an expert before moving your crypto funds.

Work with a CryptoConsultz consultant for help.

[LEARN MORE >>](#)

Getting Started with Cold Storage

Which type of cold storage device should I use?

There are several different types of cold storage solutions available, ranging from hardware wallets and paper wallets to cold storage coins. Each of these options has its own pros and cons. **The most suitable choice for you will depend on your specific needs and circumstances.**

Factors that guide your decision on which cold storage device, or better yet devices, you will use include the number and type of cryptocurrencies you are holding, your short and long term plans for your portfolio, your level of technical expertise, your diversification strategy and the level of security you are comfortable with.

In general terms, choose a well known, time tested cold storage option and steer clear of new wallet technologies or companies. Never buy from a third party seller, not even Amazon. Do your research and enlist an expert such as a CryptoConsultz consultant to be sure you're choosing the right products. Be sure you are well versed on how to use the option you choose BEFORE you transfer funds.

DON'T BYPASS CYBERSECURITY FOR COLD STORAGE

Not all crypto threats are minimized with cold storage alone.

Prioritize your cybersecurity and be sure you've created layers of security no matter what type of solution you choose.

Cold storage doesn't provide the protection you need from a number of other threats including malware, IP tracking, SIM swaps, key logging and a variety of other rapidly evolving threats.

Consider purchasing seed phrase backup devices and a dedicated crypto-only laptop before getting started.

Consider a full cybersecurity evaluation and personalized security plan with CryptoConsultz

[Learn More](#)

Getting Started with Cold Storage

SETTING UP YOUR COLD STORAGE DEVICE

The setup process is a critical step and is highly device dependent. Follow all the instructions carefully. Be sure you have your dedicated crypto notebook on hand and choose a time to set up the device where you'll be focused and uninterrupted. Stay focused and take your time to minimize the chance you'll make any mistakes.

You might be asked to generate a seed phrase, secret key, a PIN and other important bits of information during set up. It's imperative you keep any information generated in a safe place. You may need to install software for the device onto your dedicated laptop or PC, update firmware, anti-malware and/or download specific apps onto the device itself.

It sounds like a lot of work but as long as you've taken the time to learn crypto fundamentals it doesn't require a technical wizard and it's not extremally time consuming. If you're feeling a little overwhelmed and/or some of the terminology is too technical, you should enlist the help of a professional. Once your device is set up properly it's **mostly** smooth sailing from here!

TRANSFERRING FUNDS TO COLD STORAGE

Transferring your funds from your hot wallet or crypto exchange wallet is the most crucial step in the process. It's easier than you think to **make a mistake**. Be sure you are transferring the same type of cryptocurrency to the right type of wallet. For example, do not send Ethereum to a Bitcoin wallet and visa versa.

Blockchain transactions are irreversible! Double and triple check wallets addresses and take your time before hitting that send button!

Need help?

CryptoConsultz can guide you through your cold storage set up and help you learn how to execute a crypto transaction using your new device.

[Learn More](#)

Cold Storage Options

HARDWARE WALLETS

A hardware wallet is a physical device, such as a USB drive or dedicated hardware device, that stores your private keys offline. Hardware wallets are generally considered to be one of the most secure forms of cold storage.

The gold standard for crypto cold storage!



PAPER WALLETS

A paper wallet is simply a printout of your private keys, typically accompanied by a QR code that can be scanned to access your funds. Paper wallets are cheap and easy to create, but they can be easily lost or damaged, don't have a PIN code to protect them and are considered less secure than hardware wallets.



CRYPTONOTES & COINS

Physical coins & cryptonotes are similar to paper wallets but more secure and durable. They typically protect your private key with a tamper-evident holographic film with material designed for longer term use. Private keys are still easily accessible without a PIN to protect them. They make great gifts and are great for storing smaller amounts of cryptocurrency.



BEST PRACTICE ALERT

Never buy a hardware wallet or cold storage device from a third party, including Amazon! Always buy directly from the manufacturer. Hackers resell cold storage devices pre-loaded with malware and repackage them.

Frequently Asked Questions

What happens if I lose my device?

If you lose your hardware wallet or it becomes non-functional at any point do not fret! That's what your seed phrase (otherwise known as your backup key, backup phrase, secret phrase, etc.) is for! Just purchase a new hardware device and you can choose to set it up using the seed phrase. It essentially becomes a copy of your original device! This is why your seed phrase is so important. If you lose your device and can't find your seed phrase you won't have access to your crypto.



BEST PRACTICE ALERT

Keep your seed phrase safe by making two copies, storing one copy in a dedicated crypto notebook and keeping it in a fireproof safe or other secure location.

What if my device is stolen?

Most cold storage devices are secured using a PIN you generate upon set up. This adds an additional layer of security to the device. Please be aware that your seed phrase allows access to your device without a PIN and therefore is the most important bit of information to keep in a secure location.

If your hardware wallet has been stolen and/or you're otherwise concerned someone has access to your device be sure you transfer your funds to a NEW wallet immediately! In other words, backup a new device using the seed phrase and then transfer to a completely new hardware device that has a new seed phrase.



BEST PRACTICE ALERT

Store your hardware wallet in your fireproof safe when you are not actively using it.



Frequently Asked Questions

Is it still possible for my crypto to get stolen if I use a cold storage device?

It's important to note that, like any investment, cold storage is not entirely foolproof. Risks include lost/stolen devices and seed phrases and user error.

It's important to note that cold storage alone will not protect you from all of these risks. We highly recommend you work with a CryptoConsultz security expert to be sure you are taking every precaution to secure your funds.

I'm technically challenged and afraid I'm going to make a mistake. Is cold storage really the right choice for me?

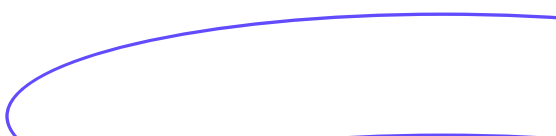
User error is one of the most common risks in crypto investing. When dealing with a rapidly evolving new technology it's easy to make a huge mistake with the push of a button. User error is NOT unique to cold storage and you are NOT necessarily at a higher risk when using a hardware device. One of the best ways you can prevent user error is to understand the basics of the technology.

Be sure you are intimately familiar with terms like private key, public key, seed phrase, backup phrase, transaction ID, block explorer, etc. It's imperative you know the differences between a centralized and a decentralized exchange and the risks that go along with each one. You'll also need to fully understand the difference between a wallet, the different kinds of wallet options out there and the risks involved with each one.

If these terms seem a little blurry to you or you don't know what they mean at all it's essential you work with a cryptocurrency consultant, attend a CryptoConsultz webinar or check out our variety of eBooks to gain a deep understanding of the basics BEFORE you venture any further down the crypto rabbit hole!

Is there a lot of work involved with maintaining or using my cold storage device?

No! That's the beauty in cold storage. Transacting in crypto using your cold storage device is easy and much more secure, even if you are a frequent crypto trader. Many of our clients choose to have one device for their long term holdings and another device for funds they would like to use to buy, sell and trade crypto on a regular basis. Whether you decide to let your hardware device collect dust in your safe or use it on a regular basis to manage your portfolio, it's the GOLD STANDARD for crypto security.



Get In Touch

www.cryptoconsultz.com

info@cryptoconsultz.com



971-808-2309

