INTELLIGENT
CRYPTOCURRENCY

CYBER SECURITY - PROTECT YOUR DATA & ASSETS ONLINE

IMPORTANT LEGAL DISCLAIMER:

All content and information provided here in and on our website https://www.intelligentcryptocurrency.com, hyperlinked sites, associated applications, forums, blogs, social media accounts and other platforms ("Site") is for general information and educational purposes only. All content is the personal opinion of the author only.

We make no warranties of any kind in relation to our content and services, including but not limited to accuracy, security and updates.

No part of the content and services that we provide (including this very newsletter) constitutes financial advice, legal advice, taxation advice or any other form of advice meant for your specific reliance for any purpose, nor any dealing in (or promotion of) securities for which a licence is required.

Any use or reliance on our content and services is solely at your own risk and discretion. By using the service at Intelligentcryptocurrency.com you agree to indemnify Intelligentcryptocurrency.com, it's owners, agents, authors and representatives from any and all claims and responsibilities. You should always conduct your own research, review, analyse and verify our content and services before relying on or using them and consult a licensed financial planner.

Trading and investing in cryptocurrencies is a highly risky activity that can lead to major losses exceeding your initial capital, please therefore consult your financial advisor before making any decision.

Never invest more than you can afford to lose.

No content on our Site is meant to be a solicitation or offer to invest or participate in any cryptocurrency tokens or fund raises of any sort.

BY PROCEEDING YOU AGREE TO HAVE READ, UNDERSTOOD AND ACCEPTED THE ABOVE DISCLAIMER

Table of Contents

Contents of this Report

IMPORTANT REMINDER: YOU SHOULD ALWAYS CONSULT A LEGAL, TAX, FINANCIAL, BUSINESS OR OTHER PROFESSIONAL ADVISER REGARDING ALL MATTERS CONCERNING CRYPTOGRAPHIC TOKENS AND YOUR OWN PERSONAL FINANCIAL SITUATION BEFORE MAKING ANY DECISION TO APPLY TO PURCHASE, TO PURCHASE OR TO HOLD OR TO SELL ANY KIND OF CRYPTOGRAPHIC TOKENS.

Cryptocurrency Security & Online Privacy

Since cryptocurrencies are digital, it's very important to properly secure your computer hardware, but also to develop high-security habits to protect your data and property as much as possible.

Here are several simple ways that you can protect your data and property online:

Encrypted Email & Email Practices

Forget about using free accounts like Gmail, Yahoo and Hotmail. They're not safe and secure in our opinion.

Setup an encrypted email for yourself on a site like Protonmail.com (it's free for a basic account and for a small fee you can get more features and upgrade to premium).

It's a good idea to have a separate email account for various purposes. E.g. for sensitive logins related to finances, create a separate account and use that account only for that purpose.

Then you may want to have an email that you hand out to personal contacts, as well as an email for business purposes, as well as an email for signing up to newsletters and websites.

(Protonmail Plus allows you to have multiple addresses within your main interface, so this allows you to setup different addresses within your main inbox so you can view everything in one place.

Be very careful when opening and clicking on links in emails sent to you.

Always verify that the send-from domain is the actual person or company you want to hear from. E.g. If you're receiving email from Paypal, check the send-from domain is @paypal.com. If it's anything else, it's usually spam or a scam.

After you've verified the send-from address and it checks out, usually it's better to actually type in the address of the company's domain rather than click a link, just to be safe. So, instead of clicking on the link in the email from Paypal, just go to your browser and go to https://paypal.com. This is especially important when dealing with bank accounts and cryptocurrency exchanges.

2 Factor Authentication (2FA)

2FA is an additional security layer that requires you to obtain a code (which typically changes every 30 seconds). This way, even if someone knows or hacks your password, they would not be able to access your account without the 2FA code.

Many sites, including email, cryptocurrency exchanges and social media platforms allow for 2FA security.

Tip: do not use the sms 2FA if given as an option. Your phone number could be cloned or sim-swapped, it is not secure.

The most common smartphone app for 2FA is Google Authenticator. You simply install this on your phone and follow the instructions to setup 2FA on the account in question. Usually this means scanning a QR code with the GA app.

You will also get a one-time emergency backup code in case you lose your GA and this way it allows you to enter your account with this code. KEEP THIS CODE SAFE… anyone who has it can access your account if they know your password (preferably keep it somewhere written down on paper, in a safe location).

Pro tip: when setting up 2FA on GA, get yourself a 2nd phone as a backup. GA is not transferable so if you lose your phone, you lose all your 2FA and need to reset it manually using the backup codes (a big headache). But, if you have 2FA on another phone or tablet, you can simply use this to help make the transfers easier. When setting up your 2FA, do it on both devices simultaneously.

Virtual Private Network (VPN)

The technical aspects behind how the internet works is complicated and there's no need to know the ins and outs.

In simple terms, when you connect to the internet, there's an IP address. This could be compared to the street number and address of your home.

If you connect to the internet without a VPN, this IP address is public and could be traced back to your ISP (internet service provider) and reveal all sorts of private data.

A VPN is software that acts as a bridge between your connection and the internet, so that it masks your IP address and adds a layer of protection that helps reduce the data that's publicly visible.

A good VPN shouldn't cost more than $10 per month, and typically allows for multiple devices to be used at the same time (computer, phone, tablet etc).

Ideally you want to always be using a VPN, especially when connecting to public networks.

VPN recommendations:

https://protonvpn.com
https://nordvpn.com
https://satoshivpn.com

Protect Your Personal Information

An easy way for hackers to gain access to your information is by using all the information you put online against you.

Be very conscious of the information you share online, especially private personal information such as your full name, phone number, address, family members, names of pets etc.

Something as simple as a photo showing your home address could be used against you.

Unless absolutely necessary, I'd advise against ever revealing anything private or sensitive online.

Consider that if there's someone with bad intentions, if you're sharing your life in public on social media and for example you're sharing that you're on vacation, then a bad person could use that to know that you may not be at home, which leaves a vulnerability. If you feel the need to share your vacations and travel plans publicly on social media, it's a good idea to do it after you've actually had the vacation.

Even when it comes to ordering physical mail, if you get mail delivered to your home address, it's safer to get yourself a mailbox or mail forwarding service so that you never have to reveal your home address to 3rd parties online when ordering things.

If you're based in the US, https://privacy.com/ is a service that allows you to generate virtual credit cards that mask your real card details so that even if someone gets the masked card details, they can't do anything with it. It adds another layer between you and the 3rd party.

Passwords

Most people tend to use a single password for all their logins. And on top of that, the password tends to be something easy to guess like a pets name, date of birth, spouse name etc.

Using the same password as all your logins is obviously bad because if anyone gets a hold of your single password, then all the places that password is used can be compromised.

Of course, make sure you've also setup your 2FA, and it's a good idea to have a separate email that you only use for logins of services. This email should not be used as a general email address and should also not be used to sign up to free services or mailing lists.

I recommend using a password manager like LastPass, that allows you to generate very complex and hard-to-guess passwords without having to remember them all.

You simply need to create one complex password to access your lastpass, and then all your other passwords are stored there.

You can even take this to the next level and have a physical Yubikey (USB device) that needs to be plugged in when you access your LastPass.

To create a complex password, use more than 12 characters, with capitalization, numbers, special characters and multiple words.

E.g. I@mverySm@rtsince12121992!!^%^

Dedicated Cryptocurrency Computer

While not mandatory, if you have more than 5 figures worth of cryptocurrency it's a good idea to get yourself a dedicated computer that you only use to transact in cryptocurrency and login to exchanges.

Again, the idea behind doing this is that by limiting the exposure to only cryptocurrency exchanges, it reduces the potential for getting malware or being hacked.

Do not use this computer for anything else. no email, messengers, social platforms, software downloads or anything of the sort.

Personally I like Apple computers and think they are more secure than Windows computers, so an entry-level Macbook laptop would be perfect for this purpose. The actual make and model of the computer is up to you though.

Another alternative (although I haven't personally tested it) is https://puri.sm/.

Supposedly it's focused on privacy, without Windows or Apple operating systems.

Private Internet Browser (BRAVE)

As mentioned earlier, using the internet reveals a lot of data about yourself.

The less data you reveal, the better it is. Google Chrome and Internet explorer are common internet browsers, but unfortunately they track almost everything you do. A much more private internet browser is called BRAVE.

Brave browser looks and feels almost exactly like Google Chrome, except that it's faster and blocks a whole lot of trackers and scripts by default.

It's free to install, faster and much more private. It'll take 10 minutes to setup and you'll be used to it in no time at all. It also works on your smartphone.

Highly recommended.

Click here to download BRAVE browse.

Storing Backup Phrases & Private Keys

When it comes to storing your 2FA and cryptocurrency backup phrases, seed recovery phrases and private keys, here's a good rule of thumb:

NEVER store backup phrases or private keys anywhere digital.

This means do not keep it in your email, Evernote, notepad, or even make a photo of it.

Anything digital can be compromised, and if someone gets access to your private keys or backup phrases they could take all of your cryptocurrency and you have no way to get it back.

Do not ever enter your private key in a random website. There are virtually no requirements of ever having to enter your private key other than to access your funds (so the only place you tend to enter your private key is when you want to restore a wallet).

A recommendation is to write down your private key or seed phrase with pen and paper, laminate it, keep it in a fireproof box and have at least 2 backups in separate, secure locations (like a safe deposit box somewhere).

Alternatively you could use something like https://cryptosteel.com which would reduce the risk of water damage, fire damage, getting eaten by animals etc.

BEWARE OF SCAMS!

There are plenty of scammers online, and the crypto space is a breeding ground for scams due to lack of regulation and plenty of newbies who don't quite understand all the technology.

The best attitude to adopt is if something sounds too good to be true, it usually is.

Nobody is going to give you free money.

Nobody can guarantee you a big ROI or guaranteed yield (even though they will).

People who talk with 100% certainty about anything should be avoided.

Always do your own due diligence and never reveal private information to strangers.

If you have any doubts at all, ask someone you trust.

You can also head over to the IC Discord chat groups and ask other members what they think of the matter, you may get some sobering advice that could save you a pretty penny.

IMPORTANT LEGAL DISCLAIMER:

All content and information provided here in and on our website https://www.intelligentcryptocurrency.com, hyperlinked sites, associated applications, forums, blogs, social media accounts and other platforms ("Site") is for general information and educational purposes only. All content is the personal opinion of the author only.

We make no warranties of any kind in relation to our content and services, including but not limited to accuracy, security and updates.

No part of the content and services that we provide (including this very newsletter) constitutes financial advice, legal advice, taxation advice or any other form of advice meant for your specific reliance for any purpose, nor any dealing in (or promotion of) securities for which a licence is required.

Any use or reliance on our content and services is solely at your own risk and discretion. By using the service at Intelligentcryptocurrency.com you agree to indemnify Intelligentcryptocurrency.com, it's owners, agents, authors and representatives from any and all claims and responsibilities. You should always conduct your own research, review, analyse and verify our content and services before relying on or using them and consult a licensed financial planner.

Trading and investing in cryptocurrencies is a highly risky activity that can lead to major losses exceeding your initial capital, please therefore consult your financial advisor before making any decision.

Never invest more than you can afford to lose.

No content on our Site is meant to be a solicitation or offer to invest or participate in any cryptocurrency tokens or fund raises of any sort.

BY PROCEEDING YOU AGREE TO HAVE READ, UNDERSTOOD AND ACCEPTED THE ABOVE DISCLAIMER