

Cryptocurrency Scam Report



Cryptocurrency is booming, so are the scams. Learn more about the threat landscape, the attack vectors and the tactics underpinning the surge.

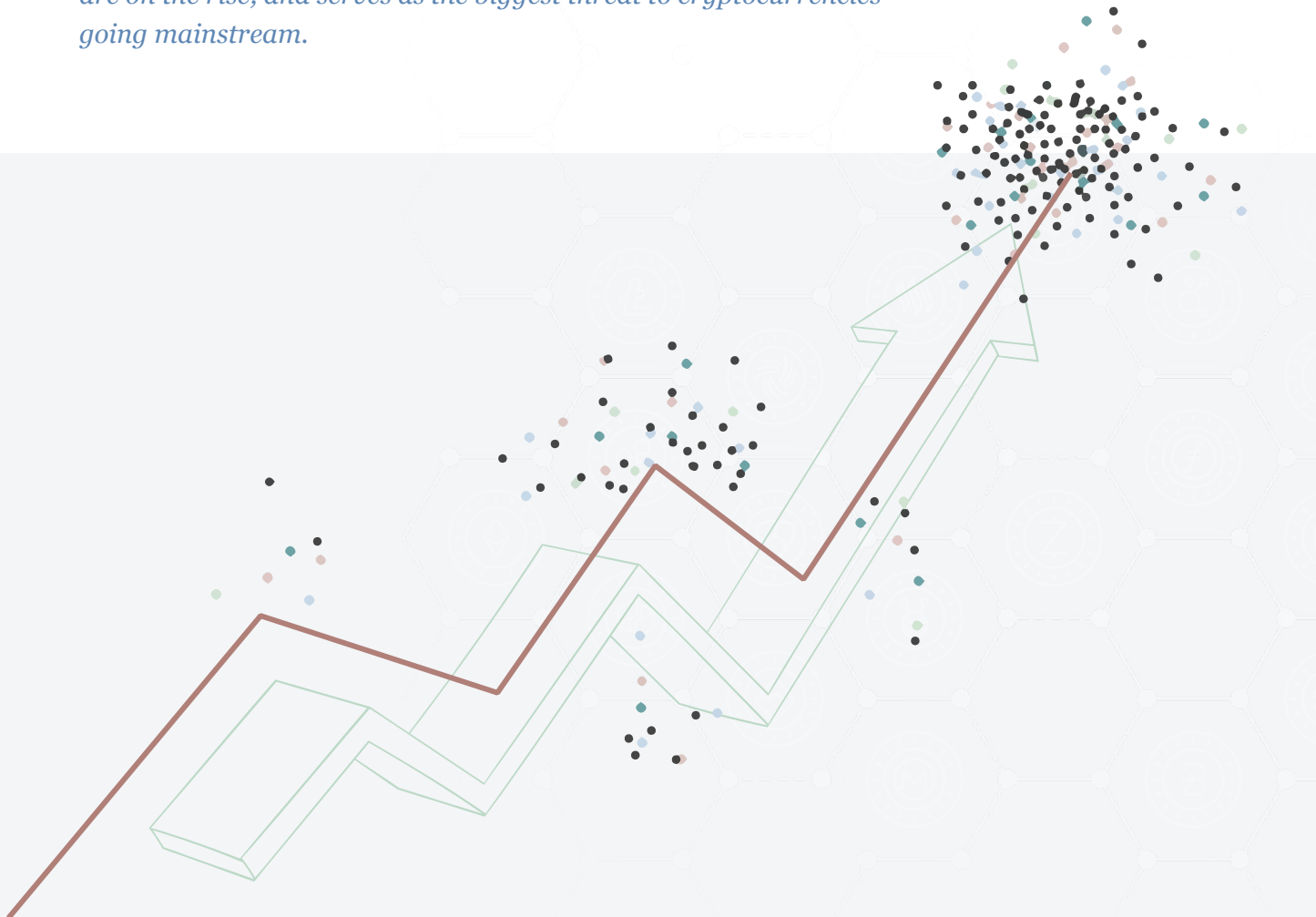
03	Executive Summary
04	Introduction
07	Cryptocurrency value and hype fuel scams...and they happen fast!
09	Crypto scammers are casting a wide net
12	Crypto scammers are in a domain gold rush
18	Lifecycle of a crypto scam
22	Beware of giveaways! Classic giveaway and airdrop scams
24	Keep an eye on your crypto wallet! Wallet validation/giveaway scams
27	Beware of Internet pick pockets! Cryptowallet theft scams
29	Stake your ground! Staking scams Proof of Staking scams
30	Keep an eye on fakes! Classic phishing scams
32	Conclusion
33	Appendix

Executive Summary

While cryptocurrency steals headlines, the fraudsters are out in force trying to steal them too.

These new currencies and ecosystems are on the cusp of going mainstream with big-time brands and personalities lining up signaling support. This digital gold rush is also attracting fraudsters who see a multibillion-dollar opportunity to scam and defraud investors. With very little regulation, protection is lacking for those who invest or transact in cryptocurrencies.

Bolster's research shows that fraud and scams related to cryptocurrencies are on the rise, and serves as the biggest threat to cryptocurrencies going mainstream.



Introduction

As Bitcoin (BTC-USD) continues to notch new highs, the buzz around cryptocurrency is hitting a feverish pitch. The buzz and highs are driven by institutional investors and speculators alike and the backing of big-time personas and brands. Elon Musk's frequent public endorsements for example, and Tesla's recent \$1.5B purchase of Bitcoin along with near-term plans to accept cryptocurrency for vehicle purchases, has provided a significant boost. And on the other end of the spectrum, the recent run-up with cryptocurrency Dogecoin (DOGE-USD), is a perfect example of speculators and frenzy at work driving up cryptocurrency values.

Naturally, none of this is lost on the hackers and scammers that troll the Internet for a quick buck, or in this case billions of bucks. In fact, the numbers we've observed with our platform are eye-opening. In 2020, we witnessed a 40% year-over-year increase in crypto-related scams to over 400,000. And looking ahead we anticipate a more than 75% increase in 2021! We observed the scams occurring across a wider range of top-level-domains, indicating a growing threat landscape.

Fraudsters are targeting unwary consumers with everything from fake sites designed to steal credentials to scams that require a small investment with the promise of a guaranteed return. Some are even promoting outright sweepstakes type scams by announcing giveaways.

Broadly there are four types of cryptocurrency scams that are proliferating.

- Fake prizes, giveaways, or sweepstakes
- Investment related scams
- Advance fee schemes
- Celebrity impersonations

Interestingly, most of the scams are also leveraging the COVID-19 pandemic and positioned as a campaign to help those who need assistance. The scams also combine different tactics, for example, a celebrity giving away cryptos for an advance fee.

This paper delves deeper into the surges we've observed. We'll examine both how cryptocurrency scams are evolving and expanding. We'll provide detailed examples of the various cryptocurrency scams we detected. And we'll conclude with tips for cryptocurrency foundations and businesses, businesses in general, and individuals on how they can keep safe as cryptocurrency goes mainstream.

Key Terms



Cryptocurrency

A digital asset designed to work as a medium of exchange wherein individual coin ownership records are stored in a ledger existing in a form of computerized database using strong cryptography to secure transaction records.



Cryptocurrency Exchange

A business that allows customers to trade cryptocurrencies or digital currencies for other assets, such as conventional fiat money or other digital currencies.



Cryptocurrency Wallet

A device, physical medium, program or a service which stores the public and/or private keys for cryptocurrency transactions.



Cryptocurrency Mining

The process in which transactions between users are verified and added to the blockchain public ledger.

Quick Facts



407,831

TOTAL NUMBER OF CRYPTO-RELATED SCAMS IN 2020



~40%

CRYPTO SCAMS: 2019/2020 YEAR-OVER-YEAR INCREASE



75%

CRYPTO SCAMS: 2021 PROJECTED INCREASE



187

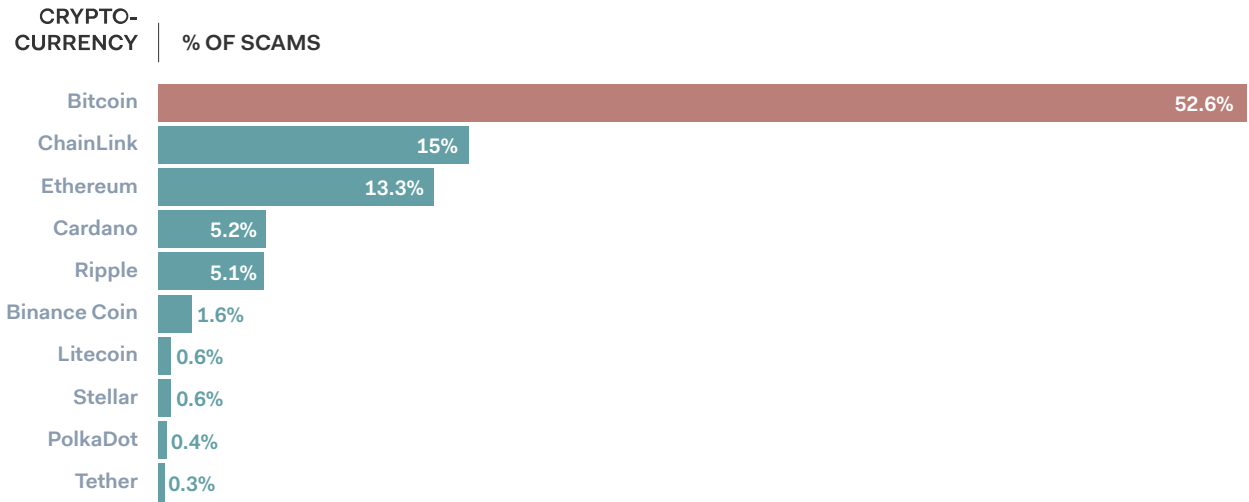
TOP LEVEL DOMAINS USED IN 2020



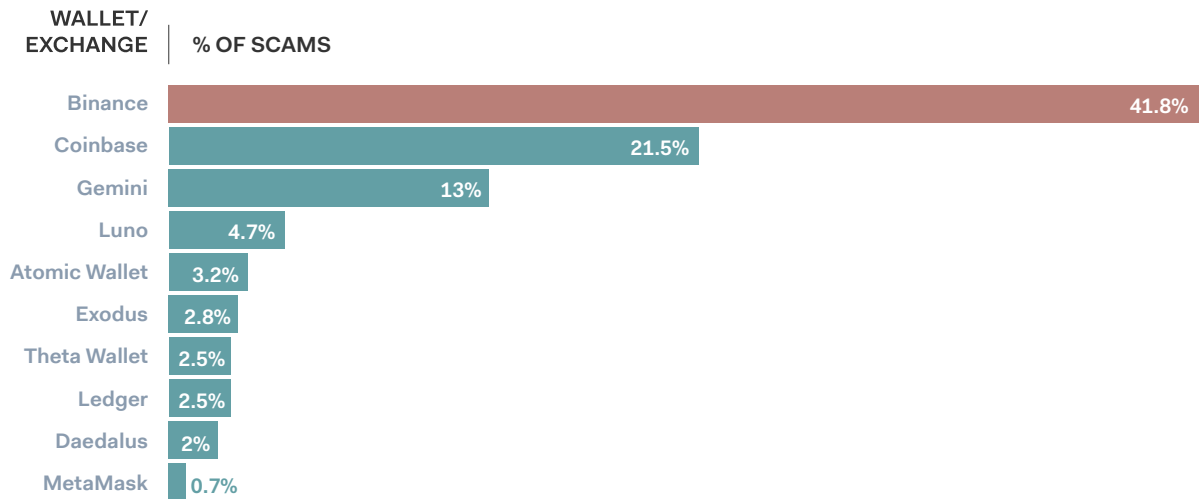
300+

PROJECTED TOP-LEVEL DOMAINS IN 2021

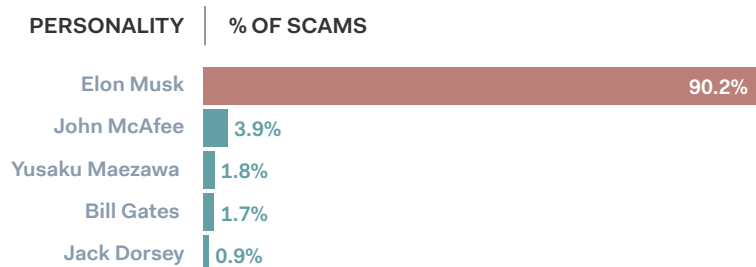
Scam Rankings by Cryptocurrency:



Phishing & Scam Rankings by Wallets/Exchanges:



Phishing & Scam Rankings by Personality:



Other notable names include Warren Buffett, Jack Ma, Cameron Winklevoss, Tyler Winklevoss.

Cryptocurrency Value and Hype Fuel Scams...and They Happen Fast!

Perhaps the starkest condition we observed is the correlation between cryptocurrency value and hype and fraud. Across virtually all the major cryptocurrencies that we monitored, we observed a direct correlation between increases in individual cryptocurrency trade volumes and value and phishing and scam related activity. Our system monitors both early indicators of phishing and scam activity, namely suspicious domain registrations in advance of scam sites being launched, as well as active phishing and scam sites. Both of these metrics demonstrated tight correlations to cryptocurrency value and hype. As a particular cryptocurrency experienced an uptick in either value or hype, fraudsters and scammers quickly came out of the woodwork to register domains and launch fraud sites. We observed it all like clockwork.

Take for example Bitcoin, the leading cryptocurrency in terms of market capitalization. You can see from the chart on the following page a direct correlation between Bitcoin value and number of Bitcoin scams during 2020 and the start of 2021. Particularly in the second half of 2020, the rapid uptick in currency value was matched by an equally alarming uptick in scam and hype related activity.

TELEGRAM CHAT GROUP: BITCOIN PUMP SIGNALS 55,739 MEMBERS

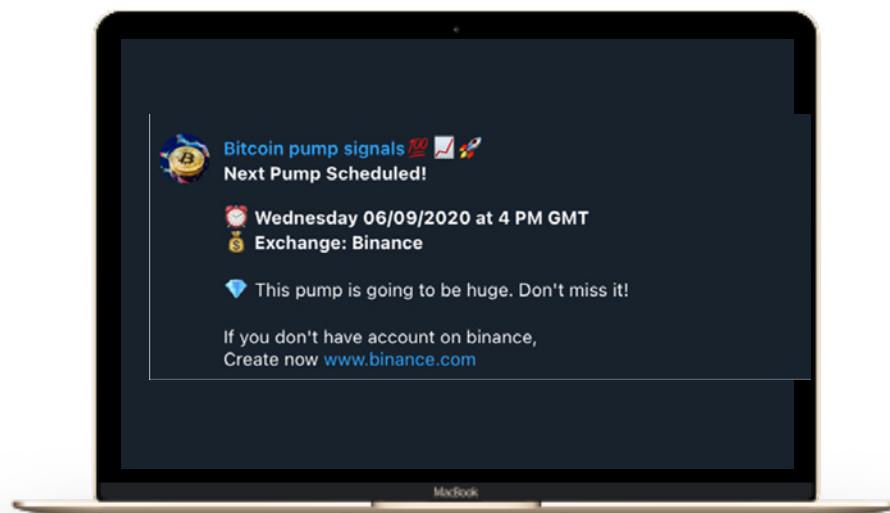
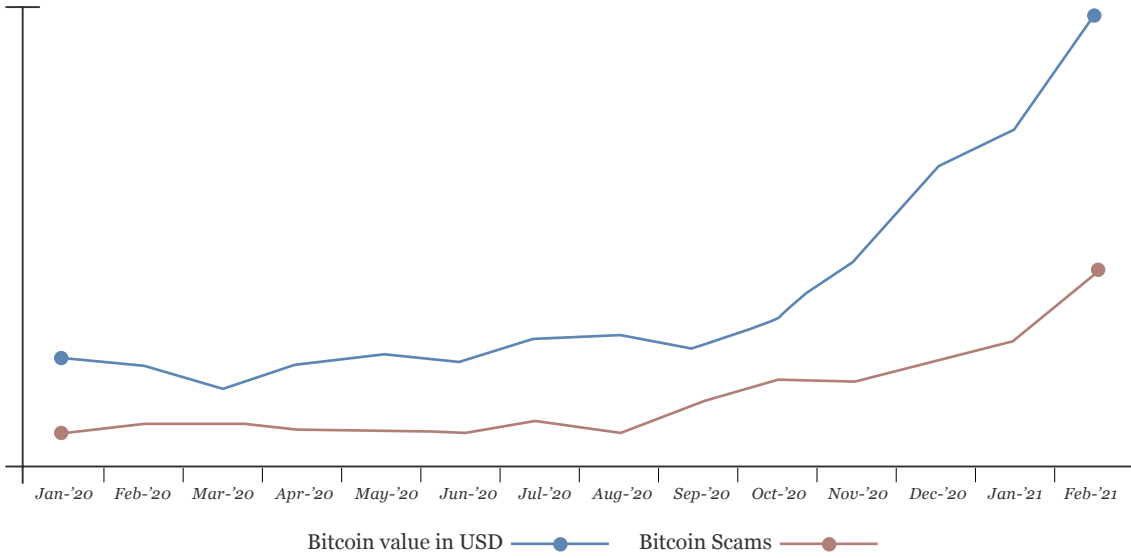


Figure 1: Bitcoin (BTC-USD) currency value vs. scam activity



Cryptocurrency Scam Report — Cryptocurrency is booming, so are the scams.

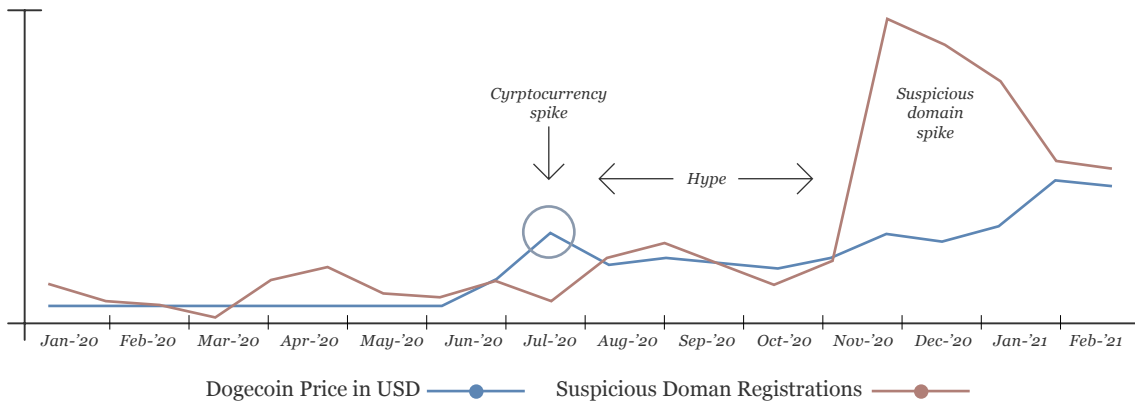
Cryptocurrency Ethereum (ETH-USD) also experienced a similar correlation with its currency value and related scam activity. Here's a snapshot for 2020:

Figure 2: Ethereum (ETH-USD) currency value vs. scam activity



And then there’s Dogecoin. Here, the cryptocurrency experienced an 800% runup in value in less than 24 hours in late January of this year driven by a spike in speculative investors and over-activity on the Reddit messaging board. The currency value run-up wasn’t lost on scammers. As you can see in the chart below, the run-up and ensuing attention triggered a tightly correlated spike in suspicious domain registrations, a leading indicator for phishing and scam attacks.

Figure 3: DOGE cryptocurrency hype vs. suspicious domain registrations



Cryptocurrency Scam Report — Cryptocurrency is booming, so are the scams.

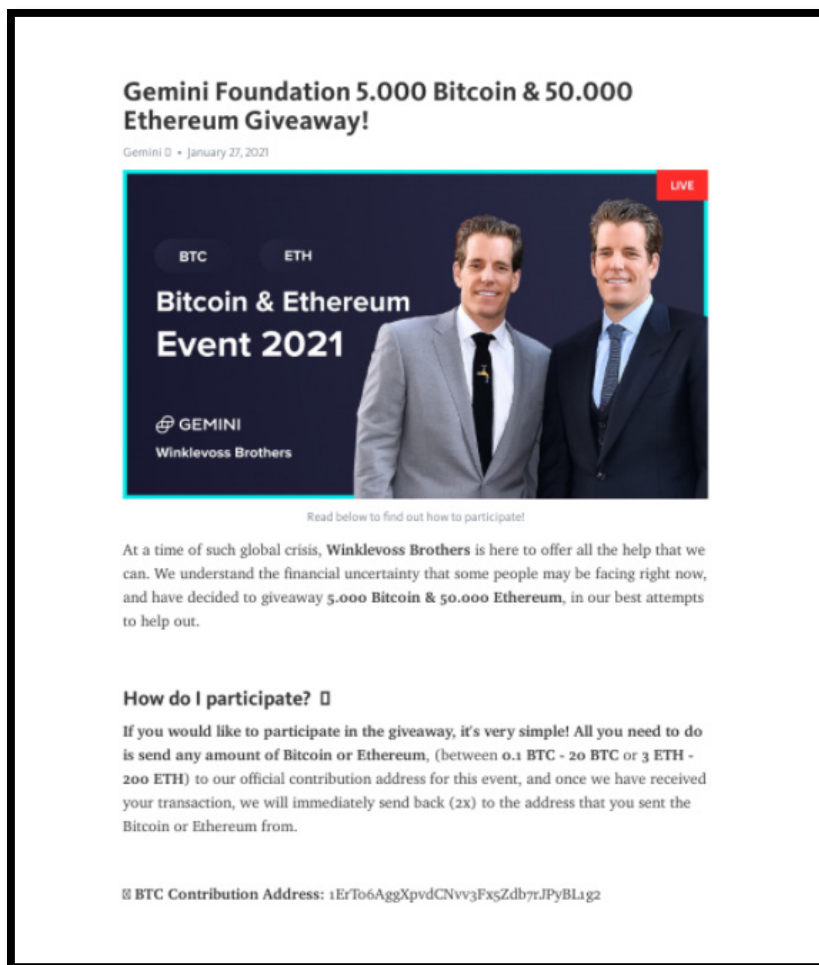
Crypto Scammers are Casting a Wide Net

Like many online scams, crypto scams use well-known techniques and playbooks. The scammers usually start by registering a domain name that could be mistaken for a legitimate web address and set up a realistic site. Though the nature of the scam varies, the common theme is that they request some sort of payment using a crypto currency. The digital nature of these scams allows bad actors to replicate and create multiple scams with minimal effort. The ease of replicating a scam allows crypto scammers to target multiple crypto currencies, and that is exactly what Bolster Research has discovered.

A great example is the Gemini Foundation Bitcoin and Ethereum Giveaway scam that Bolster Research discovered. The screenshot below promotes a giveaway by the Winklevoss brothers, who became famous first by suing Mark Zuckerberg, the founder of Facebook, for stealing their alleged business idea. Since then, they have become self-made billionaires by investing in cryptocurrencies and founding the Gemini Exchange, a place to buy, store, and trade cryptocurrencies.

CRYPTO GIVEAWAY SCAM

Cryptocurrency Scam Report — Cryptocurrency is booming, so are the scams.



Gemini Foundation 5.000 Bitcoin & 50.000 Ethereum Giveaway!

Gemini • January 27, 2021

Bitcoin & Ethereum Event 2021

GEMINI
Winklevoss Brothers

Read below to find out how to participate!

At a time of such global crisis, **Winklevoss Brothers** is here to offer all the help that we can. We understand the financial uncertainty that some people may be facing right now, and have decided to giveaway **5.000 Bitcoin & 50.000 Ethereum**, in our best attempts to help out.

How do I participate?

If you would like to participate in the giveaway, it's very simple! All you need to do is send any amount of Bitcoin or Ethereum, (between 0.1 BTC - 20 BTC or 3 ETH - 200 ETH) to our official contribution address for this event, and once we have received your transaction, we will immediately send back (2x) to the address that you sent the Bitcoin or Ethereum from.

BTC Contribution Address: 1ErTo6AggXpvdCNvv3Fx5Zdb7rJPYBL1g2

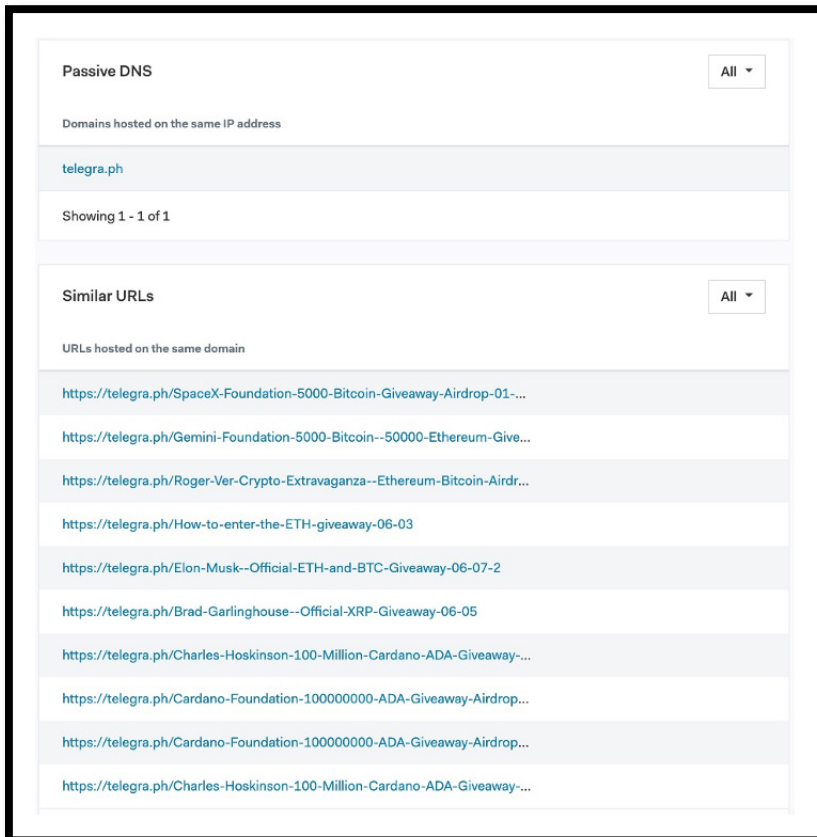
Scam URL: [hxxp://telegra\[.\]ph/Gemini-Foundation-5000-Bitcoin-50000-Ethereum-Giveaway-01-27](https://t.me/Gemini-Foundation-5000-Bitcoin-50000-Ethereum-Giveaway-01-27)

View [CheckPhish Insights](#) page

At first glance, the scam page could be mistaken for a real philanthropic campaign. The URL includes the “Gemini Foundation,” and the visuals used include real pictures of the Winklevoss brothers and official Gemini logo. It’s only when you start looking into the details of the site that you notice that this clearly cannot be authentic. Some of the giveaway signals are:

- Top level domain used is “.ph” which belongs to the Philippines
- Site is hosted in the UK (see CheckPhish Insights)
- Domain is registered through GoDaddy—a consumer service
- Multiple cryptocurrency foundation sites are hosted on the same domain

The CheckPhish Insights page also shows that there are at least 10 different crypto sites being hosted on the primary domain “telegra.ph.” The list of domain shows that the same domain and IP address are also hosting scams targeting Cardano (ADA) & Ripple (XRP) users and targeting other famous personalities like Elon Musk. Red flag!



Crypto Scammers are in a Domain Gold Rush

As the Internet has become critical for everything from education to commerce to entertainment, the international body that manages domain names, ICANN, has kept pace by expanding the number of available domains. Today, there are more than 1,400 top level domains (TLDs), and that number increases every year. The result is a crypto-scam domain gold rush as scammers try to reserve domain names to propagate their scams.

Reserving the right domain name is an important step to establishing a credible crypto scam. Because most people do not understand how domain name reservations work, seeing the currency, a celebrity, or an organization in the domain name itself tends to lend credibility to a page's legitimacy. The huge surge in suspicious domain name registrations, noted earlier, demonstrates that scammers are registering tens of thousands of domains, each of which could be used to scam investors.

Hosting companies provide services that allow individuals, organizations, or companies to make their website accessible on the Internet. Globally, there are more than 330,000 hosting companies, including companies such as Google, Amazon, and Microsoft. Most of these companies offer services that allow users to set up accounts remotely from anywhere in the world. The abundance of hosting companies means that if a site is taken down by one hosting company, the scammer can easily move to another one quickly by simply copying the website files.

This means that fighting online fraud is a constant battle for hosting companies. The sheer volume of suspicious domains and scams means that hosting providers can never proactively police every site. Since January 2020, we observed 396 different hosting providers in 58 different countries across the globe hosting crypto scams. Given the high number of scams being created, there is a high probability that the same bad actor, whether it is a group or an individual, is running multiple scams simultaneously. We see this through the concentration of hosting providers and IP address infrastructure being used. In the US alone, 125 hosting providers were used by crypto scammers. These numbers do not include hijacked or compromised servers or machines.

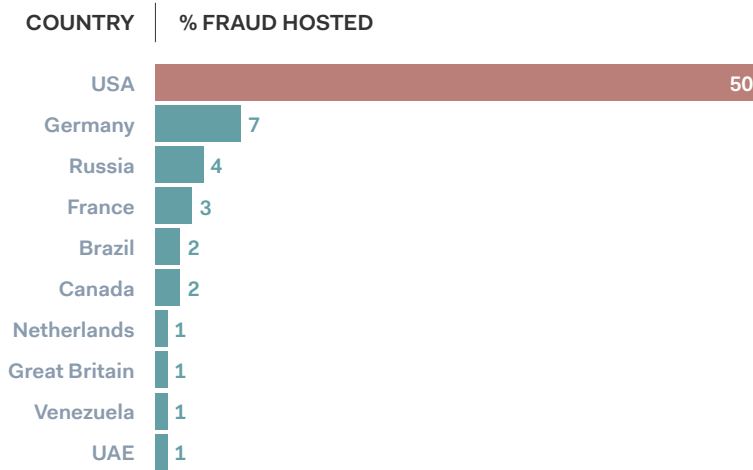
From an IP address perspective, 1,212 unique IP addresses belonging to the above 125 hosting providers were used in the US to host fraud related to crypto. This represents more than half the number (exact count being 2175) of IP address used to host crypto fraud across the globe.



We suspect that the notoriety of crypto currencies over the past year in the United States has caused a higher-than-normal concentration of crypto scams hosted domestically. Typically, Bolster Research has observed 39% of fraud campaigns being hosted in the US. The cause of the higher concentration is likely due to the increased adoption of trading apps like Robinhood making it easy for individual investors to trade cryptocurrency.

Also, despite the pandemic, the US economy has managed to remain relatively strong, and the average household wealth still continues to be one of the highest in the world. At the same time there are large numbers of households struggling, and these are the ones most susceptible to fall for a cryptocurrency scam that seems promising, but in reality is too good to be true.

Countries Where Crypto Scams are Hosted

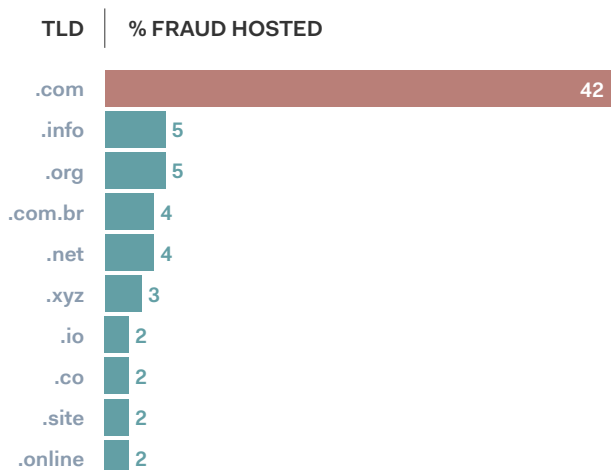


Note that this data does not reveal where the scammers themselves are. A scammer can host a fraudulent website in a country from anywhere in the world. They need not reside in the country.

Fraud across more top-level domains

Bolster Research also reveals that while attackers continue to leverage primarily the most well-known domain of “.com,” there is a growing use of less well-known top-level-domains (TLDs) to stand up malicious sites. In fact in 2020, our system detected cryptocurrency fraud on 187 different TLDs. We estimate that this number will jump to more than 300 TLDs by the end of 2021. Using multiple TLDs helps fraudsters proliferate a campaign and makes it harder for any kind of enforcement action because of the sheer number of domains to contend with.

Top Level Domains Used



Some scammers get creative and use more novel TLDs to host their scams. Below is an example of an advance fee scam using the image of Elon Musk and his association with his company Space X. The URL uses the TLD “.stream” and includes the company name.

ADVANCE FEE SCAM:

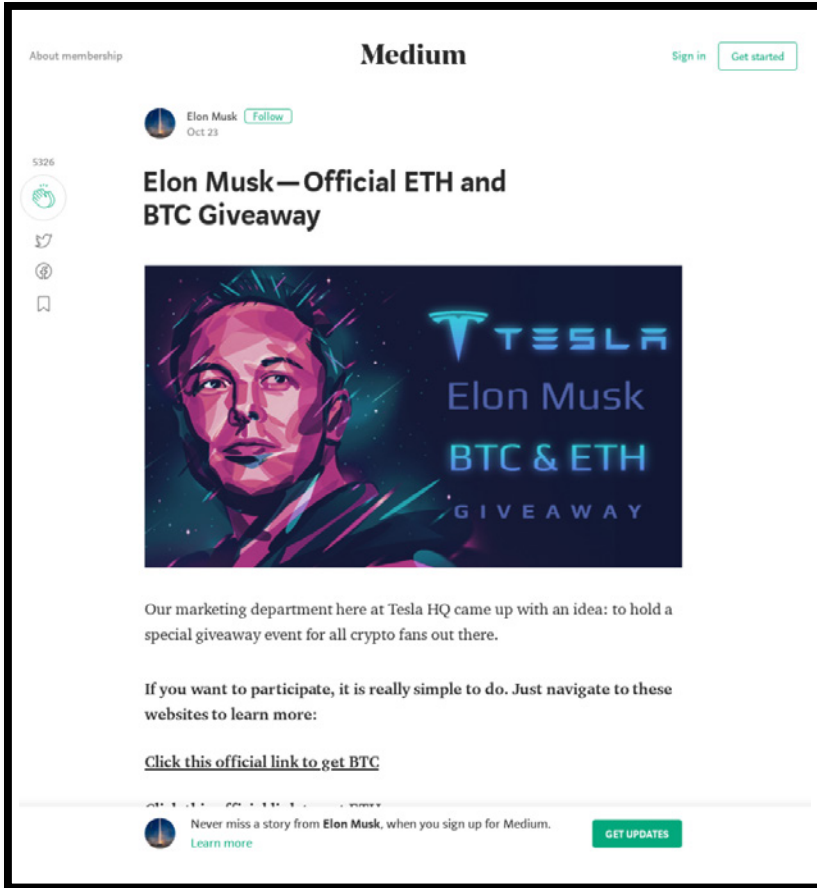


Scam URL: [hxxp://spacexdrop\[.\]stream/](http://hxxp://spacexdrop[.]stream/)
View [CheckPhish Insights](#) page

Here’s another scam that uses the TLD “.vip” to give the impression that this is Elon Musk’s personal blog site. The screen shot of the scam site clearly shows a page designed to look like a page on the popular blogging platform, Medium.

CELEBRITY IMPERSONATION SCAM

Cryptocurrency Scam Report — Cryptocurrency is booming, so are the scams.

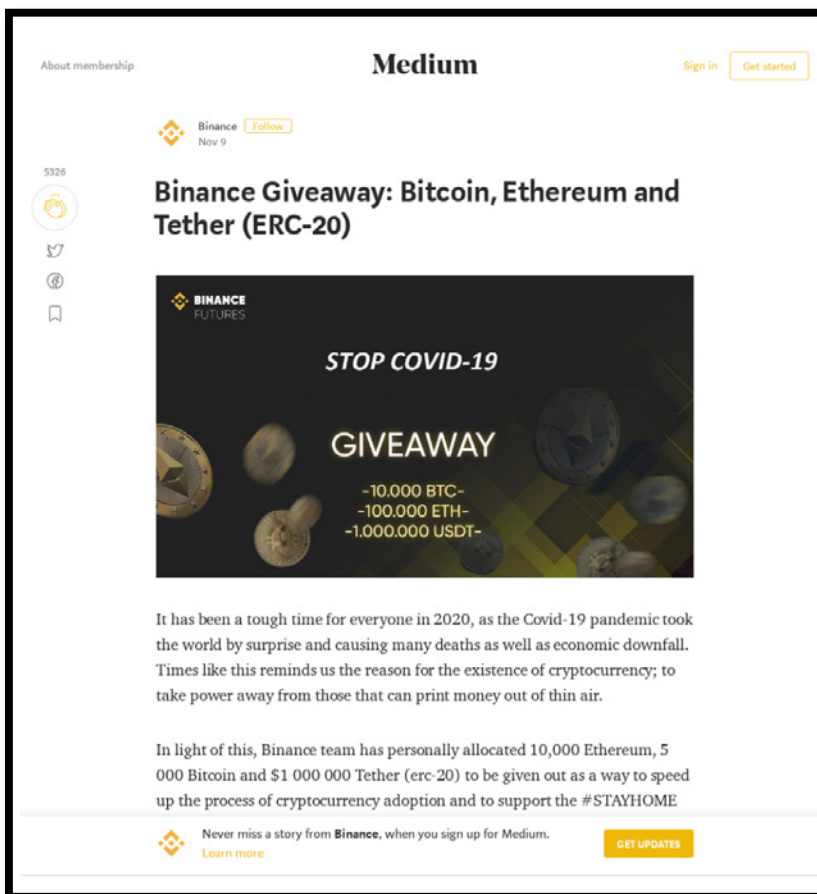


Scam URL: [http://emusk\[.\]vip/](http://emusk[.]vip/)
View [CheckPhish Insights](#) page

Some scams are just pure giveaway scams, like the screen shot below. Though there may not be any upfront fee, the scams involve you revealing your crypto current wallet information, which the criminals then use to clean out whatever balances you may have. Cryptocurrency accounts do not provide any of the fraud protections available through traditional banks or investment companies, so consumers have no recourse if they fall for one of these scams.

GIVEAWAY SCAM:

Cryptocurrency Scam Report — Cryptocurrency is booming, so are the scams.



Scam URL: [https://stayhome2020\[.\]club/](https://stayhome2020[.]club/)
 View [CheckPhish Insights](#) page

Lifecycle of a Crypto Scam

Around the world, spanning a multitude of geographies and hosting providers, scammers gear up. And while the attacks themselves are varied, the process of staging an attack is similar:

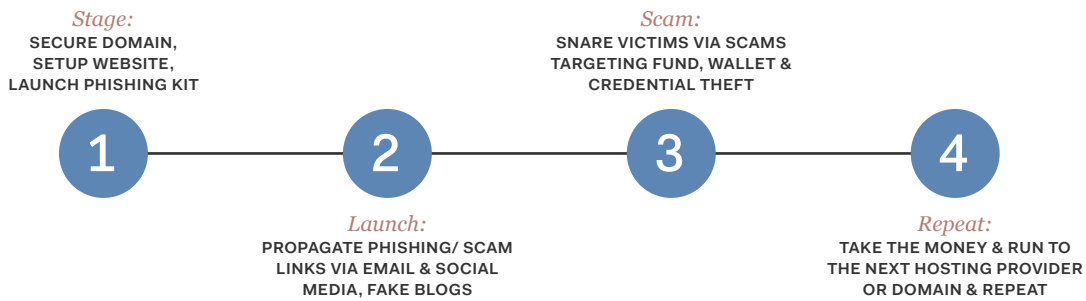


Figure 1: Lifecycle of the scam

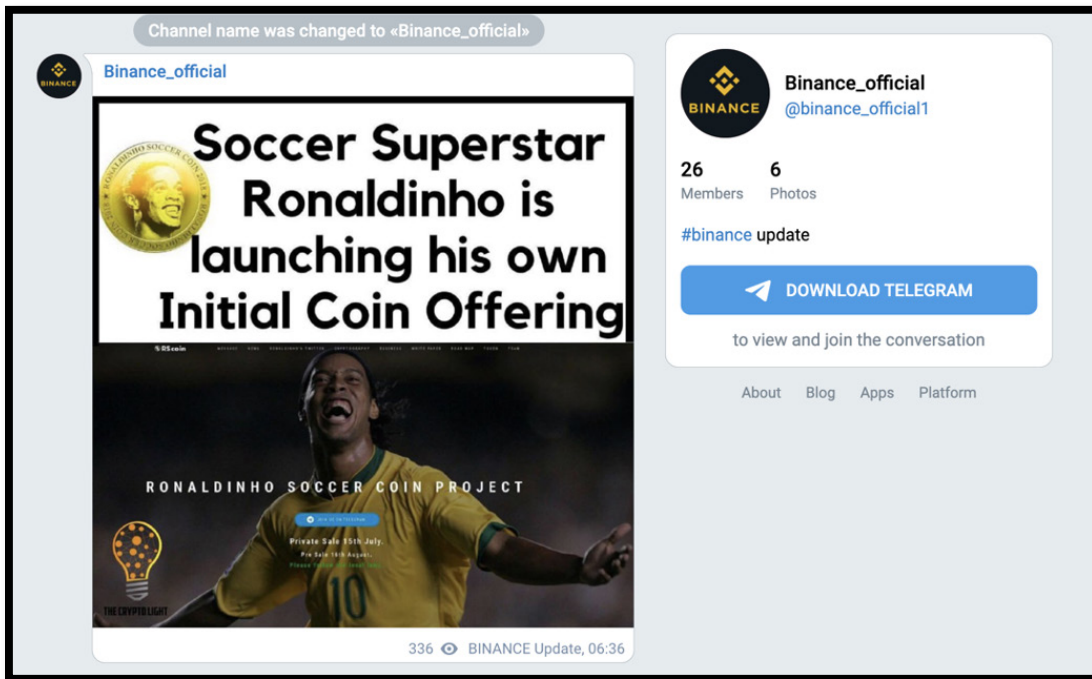
With our systems, we are able to observe the very early stages of fraudulent activity starting with the moment a fake or suspicious domain is registered. From there, we’re able to actively monitor the domain for signs of weaponization and campaign readiness. Many organizations lack this level of visibility and inherent detection capabilities, leaving them exposed well after a phishing or scam attack has been launched, and well after the damage has been done.

Propagation mechanisms

Oftentimes crypto scams are propagated through social media channels like Telegram, Twitter, Medium, Facebook and others.

On Telegram we found tens of scam pages and groups for each cryptocurrency and crypto exchange and wallet company.

Here's an example of a fake Binance group on Telegram:



Cryptocurrency Scam Report — Cryptocurrency is booming, so are the scams.

Scam URL: [hxxp://t.me/binance_official1](https://t.me/binance_official1)

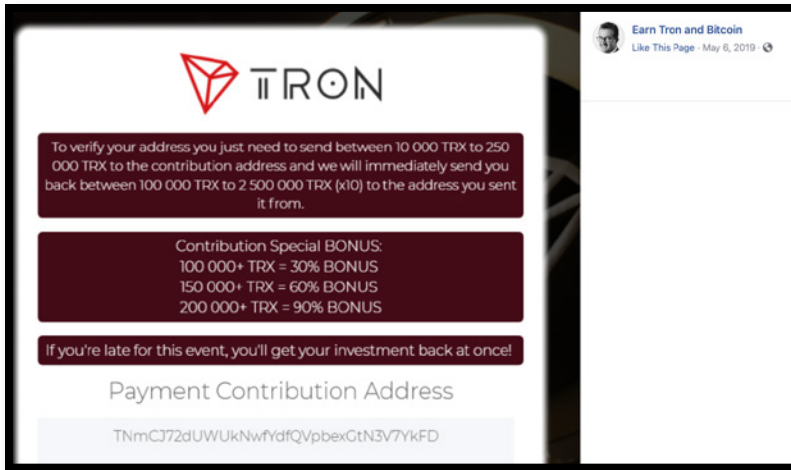
Then there's Twitter. Check out this example of someone sending a scam link around as part of a reply on Elon Musk's Twitter page.

Cryptocurrency Scam Report — Cryptocurrency is booming, so are the scams.



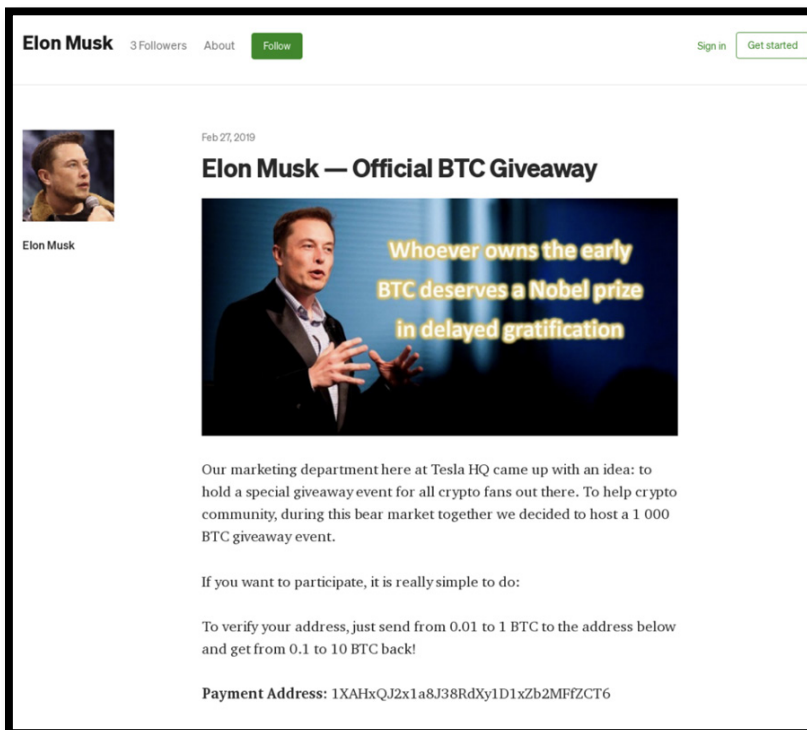
Note the URL site in the comment, elon2.site, it's a scam. View the [CheckPhish Insights](#) page to see more.

Facebook isn't immune either. Here's an address verification scam on Facebook:



Scam URL: <https://www.facebook.com/pg/thomaspowerr/posts/>

Medium articles and blog posts are also fertile ground for seeding scams. Here's a fake Elon Musk blog and address verification giveaway scam:



And as you can suspect, the scammers are getting more and more clever by the day. Read on to learn more.

Beware of Giveaways!

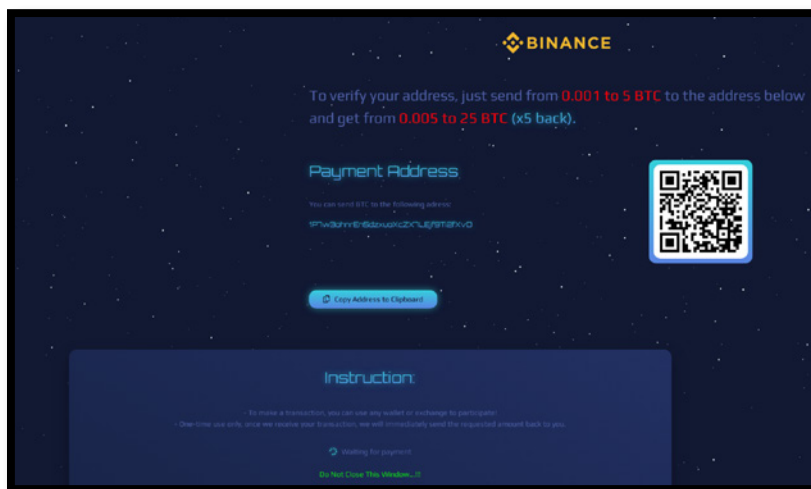
Classic giveaway and airdrop scams

Across this expanding threat landscape, we observed a wide range of scams. The most common, and shall we say classic scam, is the giveaway scam. Here, URLs appear to end users in the form of tweets, Facebook posts, and blog posts talking of an “Official Bitcoin Giveaway” or a “Get your 5000 ETH now” offer or the likes.

Virtually all of these URLs our system detects lead to scam pages targeting specific cryptocurrencies such as Bitcoin, Ethereum, Ripple or Cardano to name a few. The site will often times use either a well-known cryptocurrency exchange company or a well-known person in the crypto industry or a celebrity, to make these scams seem more legitimate. These sites often claim that “due to wanting quicker adoption of the cryptocurrency, for every X amount of crypto you send to a specific wallet address, you will get at least 2X back.” Of course, these sites have no intention of sending any cryptocurrency back to you and once you send your cryptocurrency to that wallet address, it is gone for good.

Here’s an example using the Binance name and logo to legitimize this Bitcoin giveaway scam:

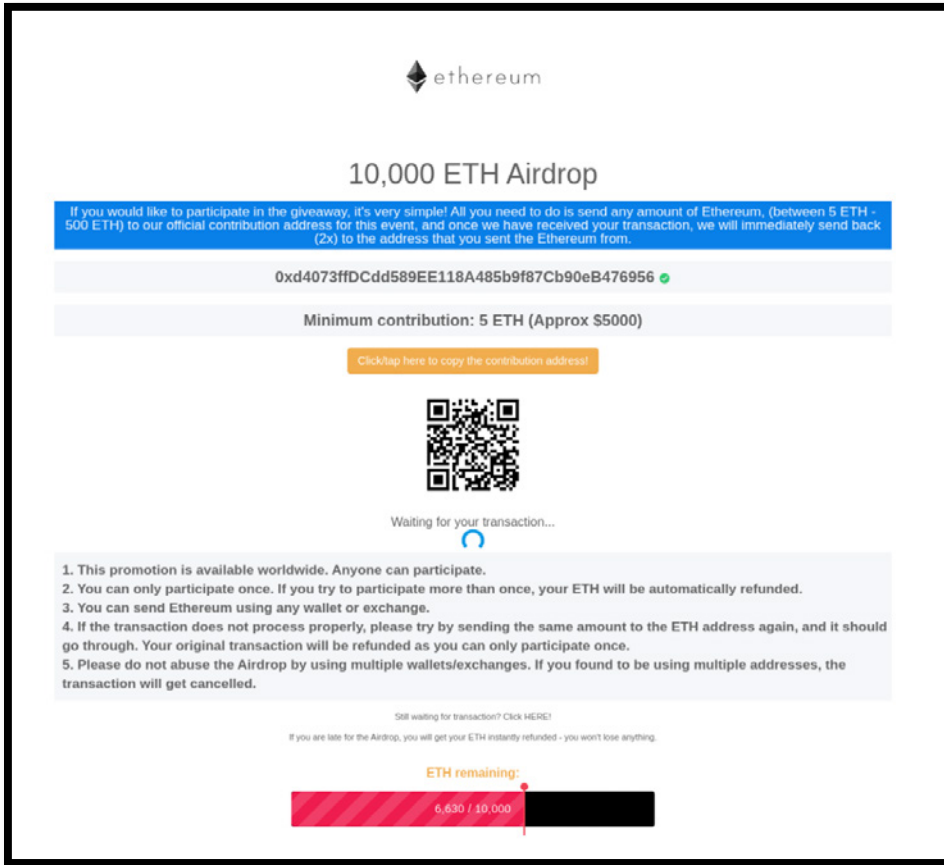
CRYPTOCURRENCY GIVEAWAY SCAM



Scam URL: [hxxp://binance-cz\[.\]epizy\[.\]com/btc/index\[.\]html?i=2](http://hxxp://binance-cz[.]epizy[.]com/btc/index[.]html?i=2)
View [CheckPhish Insights](#) page

And here's an example of an Ethereum airdrop giveaway site:

ETHEREUM GIVEAWAY SCAM



Cryptocurrency Scam Report — Cryptocurrency is booming, so are the scams.

Scam URL: [http://officialetherfoundation\[.\]com](http://officialetherfoundation[.]com)
View [CheckPhish Insights](#) page

Keep an Eye on Your Crypto Wallet!

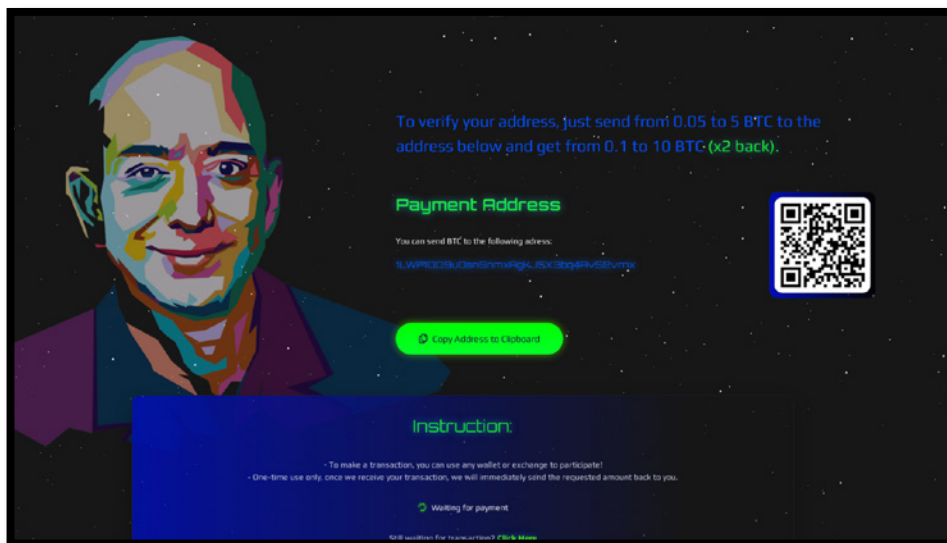
Wallet validation/giveaway scams

While the most common cryptocurrency scam is still the classic giveaway, and our system sees them all day long, our system is also detecting a growing set of scams targeting cryptocurrency wallets. Just like the physical one you might have once kept in your back pocket, cryptocurrency wallets are the digital equivalent, allowing you to store cryptocurrency and transact securely across the Internet.

One such scam builds on the giveaway scam claiming that in order to validate your wallet you need to send a certain amount of cryptocurrency to the wallet address listed on the website. Like the giveaway scam, once you send your currency to that wallet address, it's gone.

Here's an example involving Bitcoin and using Jeff Bezos's personality and his company Blue Origin in an attempt to make the transaction seem more legit:

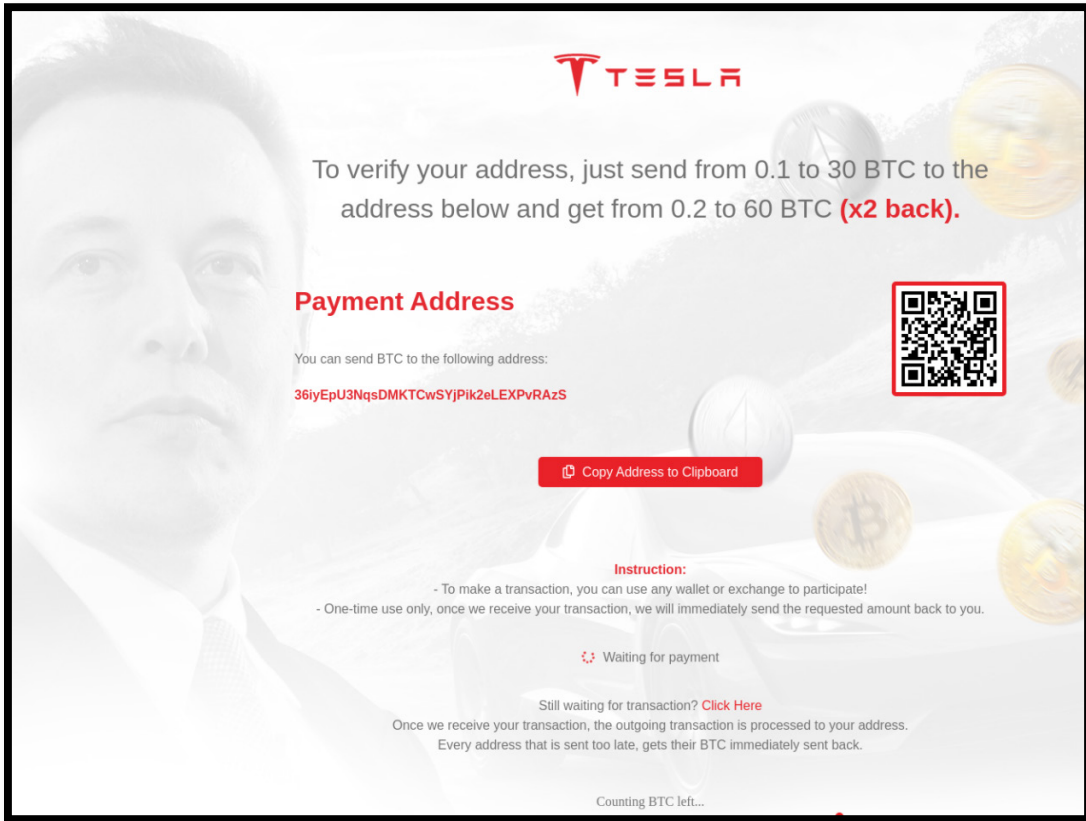
CRYPTOWALLET VALIDATION/GIVEAWAY SCAM



Scam URL: [https://www\[.\]astral\[.\]design/demo/blue-origin/](https://www[.]astral[.]design/demo/blue-origin/)
View [CheckPhish Insights](#) page

And here's a similar Bitcoin example using Elon Musk's personality and the Tesla brand:

CRYPTOWALLET VALIDATION/GIVEAWAY SCAM

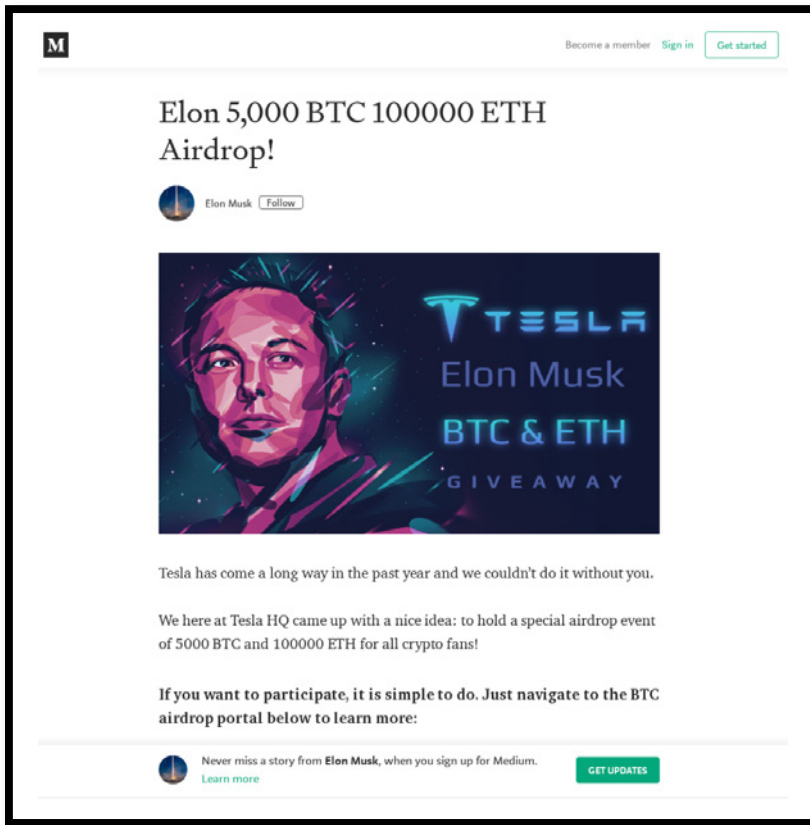


Cryptocurrency Scam Report — Cryptocurrency is booming, so are the scams.

Scam URL: [https://emuskgiveaway\[.\]com/en/btc/index\[.\]html](https://emuskgiveaway[.]com/en/btc/index[.]html)
View [CheckPhish Insights](#) page

And here's yet another example involving both Bitcoin and Ethereum and using Elon Musk's personality and the Tesla brand:

CRYPTOWALLET VALIDATION/GIVEAWAY SCAM



The screenshot shows a Medium article page. At the top left is the Medium 'M' logo. At the top right are links for 'Become a member', 'Sign in', and 'Get started'. The article title is 'Elon 5,000 BTC 100000 ETH Airdrop!'. Below the title is the author's profile, 'Elon Musk', with a 'Follow' button. The main image is a stylized, colorful portrait of Elon Musk with the Tesla logo and the text 'Elon Musk BTC & ETH GIVEAWAY'. Below the image, the text reads: 'Tesla has come a long way in the past year and we couldn't do it without you. We here at Tesla HQ came up with a nice idea: to hold a special airdrop event of 5000 BTC and 100000 ETH for all crypto fans! If you want to participate, it is simple to do. Just navigate to the BTC airdrop portal below to learn more:'. At the bottom, there is a 'Learn more' link and a 'GET UPDATES' button.

Cryptocurrency Scam Report — Cryptocurrency is booming, so are the scams.

Scam URL: [hxxp://elon-promise\[.\]com/](https://elon-promise[.]com/)
View [CheckPhish Insights](#) page

Beware of Internet Pick Pockets!

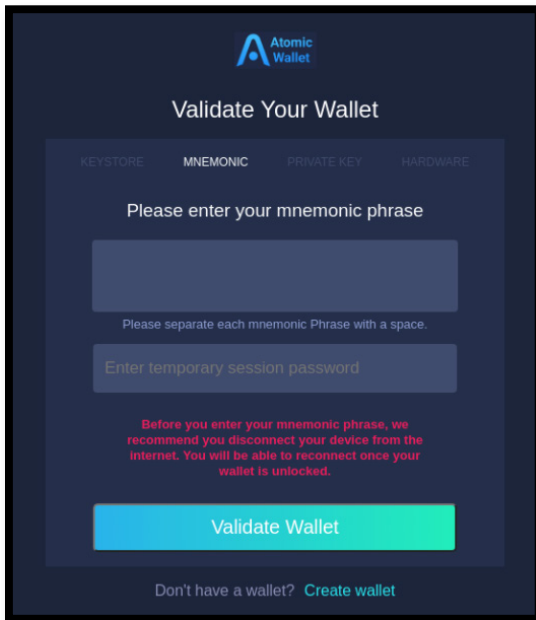
Cryptowallet theft scams

Our system also detected a more nefarious wallet validation/authentication phish. With this type of scam, crypto wallet companies are impersonated by scammers to gain access to private information needed to access a customer's crypto wallet. These sites appear to be legitimate using specific company names and logos and usually contains the company name in the domain. These sites ask for details such as a customer's keystore file, wallet password, mnemonic phrase, wallet address, BIP39/BIP44 recovery phrase, and private key...basically all the information needed for a scammer to empty your crypto wallet in a New York minute.

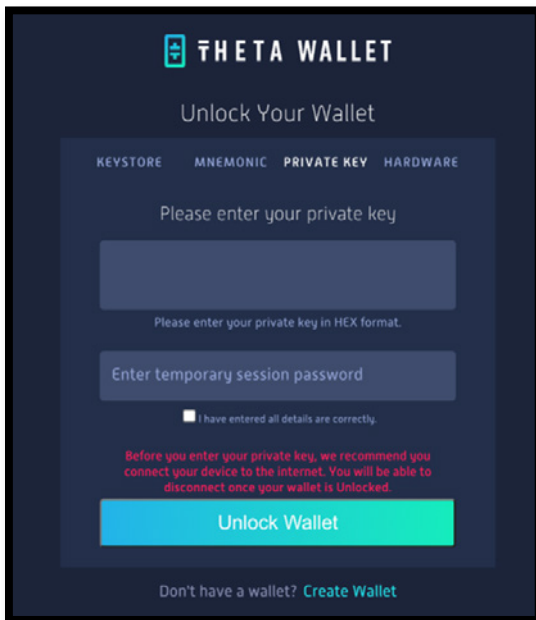
Oftentimes a phishing email will be sent to customers that spoof these wallet companies. These phishing emails make various claims about data breaches, missing information, updating information, and incorrect transactions to direct customers to these fraudulent sites. As with most phishing emails, urgency is created leaving unassuming targets little time to think before visiting these sites and giving away their private information. And beware, we've observed these types of scams targeting not only the more well-known crypto wallet companies but also the lesser well-known.

Here are two examples, one targeting Atomic Wallet and another targeting Theta Wallet customers:

FAKE ATOM WALLET VALIDATION



Scam URL: [https://www.\[.\]authenticateatomicwallet\[.\]com](https://www.[.]authenticateatomicwallet[.]com)
View [CheckPhish Insights](#) page



Scam URL: [https://www.\[.\]thetanode\[.\]online/unlock/privatekey\[.\]html](https://www.[.]thetanode[.]online/unlock/privatekey[.]html)
View [CheckPhish Insights](#) page

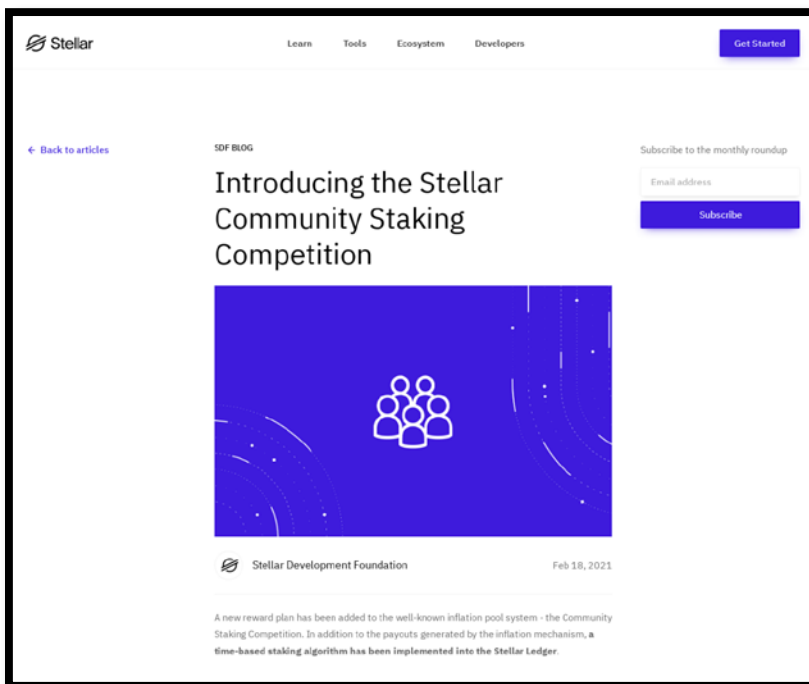
Stake Your Ground! Staking Scams

Proof of staking scams

Similar to mining, staking is a process that lets crypto holders actively participate in transaction validation on a blockchain. To earn rewards via staking, a user needs to have a minimum balance for a given cryptocurrency. Some attackers have been targeting Proof of Staking as a method of attack aimed at independent investors. Users need to be aware of all the staking websites that have emerged in recent times. While a few of them could be legitimate, most of them are scams hosted to lure crypto enthusiasts.

Here's an example. In this instance our system detected other scam pages hosted on the same domain & IP address.

STAKING SCAM SITE



Scam URL: [http://mail7-stellar\[.\]org/](http://mail7-stellar[.]org/)
View [CheckPhish Insights](#) page

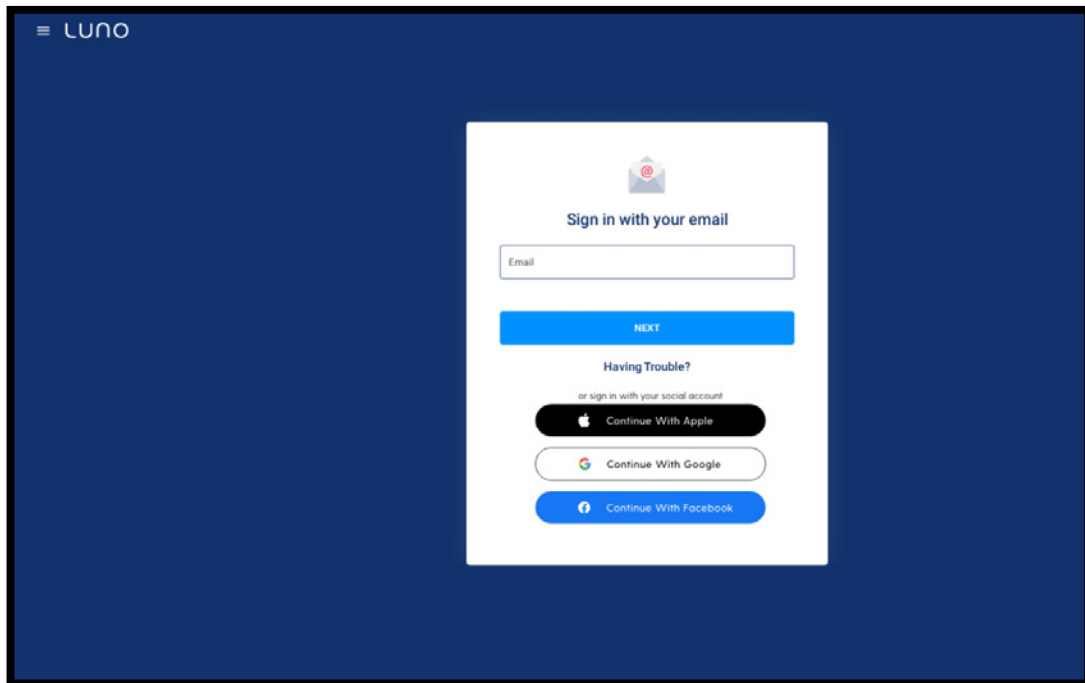
Keep an Eye on Fakes!

Classic phishing scams

And of course, there's always the flat-out fake site to beware of when it comes to cryptocurrency. Typically replicas of the real site and usually asking for username/password credentials, many of these sites employ look-alike domains that are confusingly similar to the legitimate domain and site.

Here's an example of a fake login page for Luno:

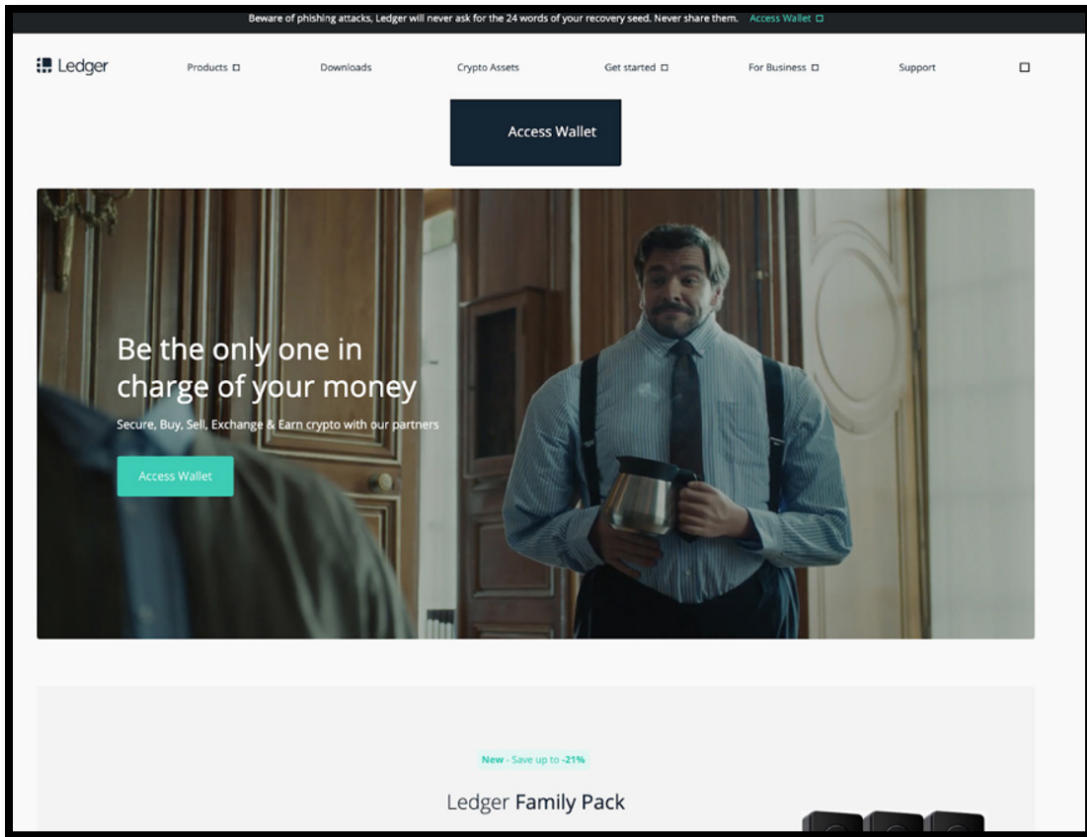
FAKE LOGIN PAGE



Scam URL: [hxxps://www\[.\]lunologinconfirmation\[.\]com/](https://www[.]lunologinconfirmation[.]com/)
View [CheckPhish Insights](#) page

And here's an example of a fake site targeting Ledger and its customers:

FAKE LEDGER SITE



Cryptocurrency Scam Report — Cryptocurrency is booming, so are the scams.

Scam URL: [https://ledgerwallet\[.\]support/](https://ledgerwallet[.]support/)
View [CheckPhish Insights](#) page

Conclusion – What Happens from Here?

Our data confirms the overwhelming volume of threats that surround the cryptocurrency industry. We don't anticipate this abating. In fact, we anticipate just the opposite. So here are a few tips and recommendations for your brand, your business and yourself.

1. For cryptocurrency foundations and business that operate directly in the cryptocurrency industry, know that you are increasingly a target. Thieves will attack your brand, mercilessly stepping on your domain and putting up fake sites to fool and scam your customers. Be prepared with systems that can detect early on brand infringements, fraud campaigns, and scams, and can help you stop them.
2. For businesses in general, recognize your employees will increasingly be targets of cryptocurrency scams through emails or through employees innocently sharing links. To stay ahead of this, consider a real-time URL scanning capability to detect and block malicious links traversing your enterprise.
3. And as an individual, well you're just as much a target. As always, it's important to practice safe web browsing and emailing and remain vigilant. Avoid clicking on any URLs sent your way if even slightly suspicious. And for safe measure, if you're uncertain about a link you're preparing to click, use a free URL scanner like [CheckPhish.ai](#) to scan the URL to get a real-time disposition. As the saying goes, better safe than sorry.

Like credit card transactions over the web, cryptocurrency is here to stay. And like with credit cards, there will always be fraud and theft to contend with. But unlike credit cards where fraud detection and prevention is well-understood, cryptocurrency's novelty has many investors in 'learn mode' and as a result raises the risk of the unsuspecting being scammed. Following these tips will help ensure your brand, business and self all remain safe. And if you need more help, contact the experts at Bolster. Their AI smarts, automated takedown capabilities and APIs will keep your organization on your toes and steps ahead of the scammers.

Appendix

1. Cryptocurrency Value vs. Scam Charts
2. Celebrity Scams – Top 5 Celebrities
3. Wallet Scams – Top 10
4. Cryptocurrency Scams – Top 10

1. Cryptocurrency Value vs. Scams

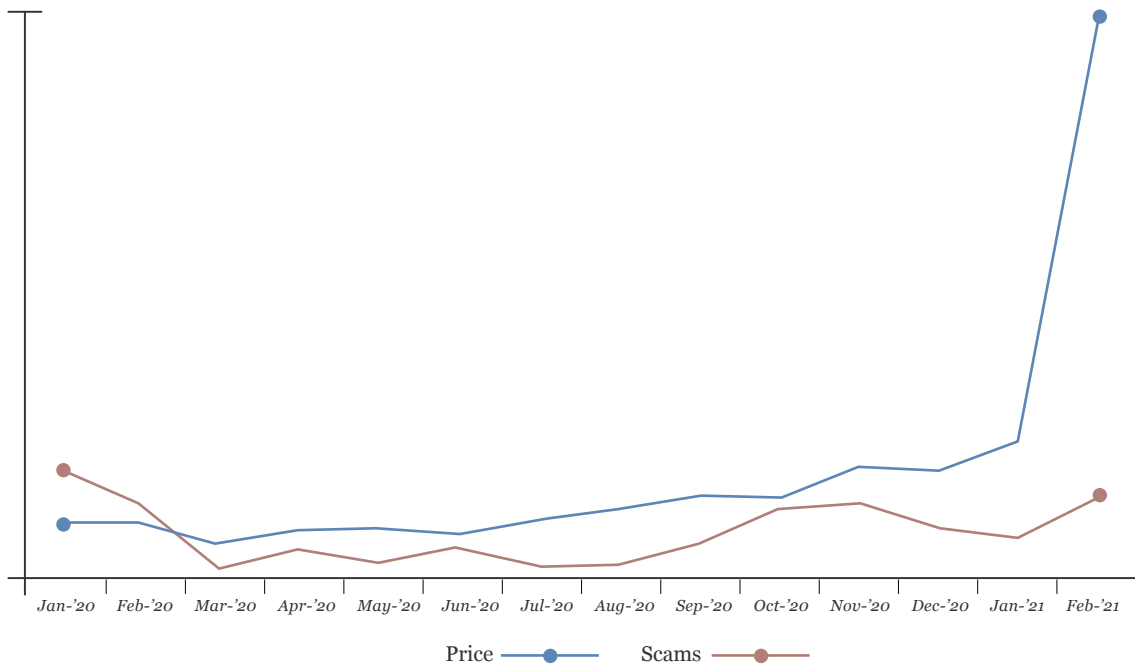
Bitcoin-See page 8

Ethereum-See page 8

Binance Coin:

Binance Coin Price vs. Scam

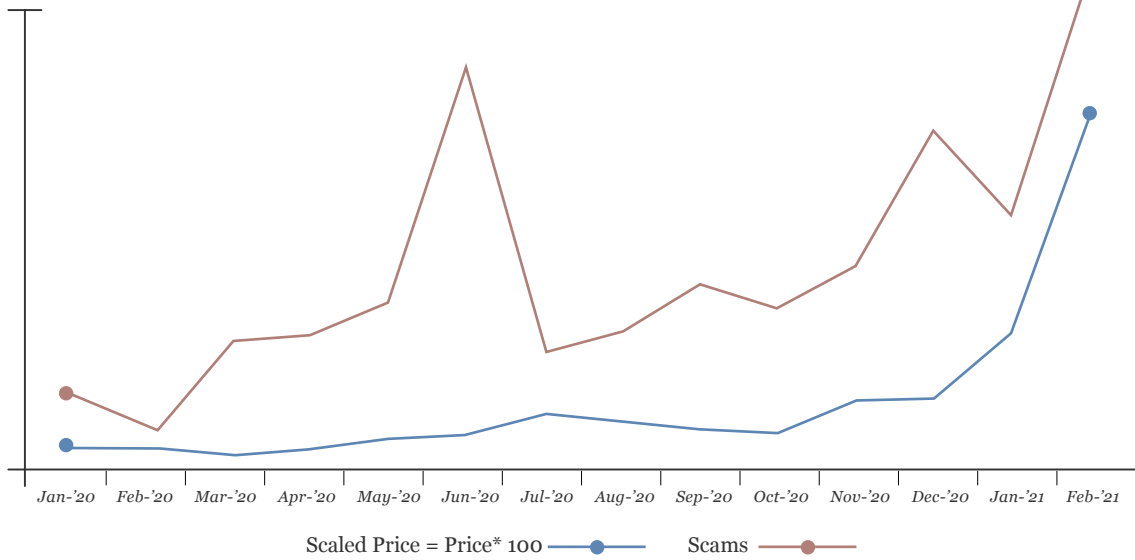
Cryptocurrency Scam Report — Cryptocurrency is booming, so are the scams.



Cryptocurrency Scam Report — Cryptocurrency is booming, so are the scams.

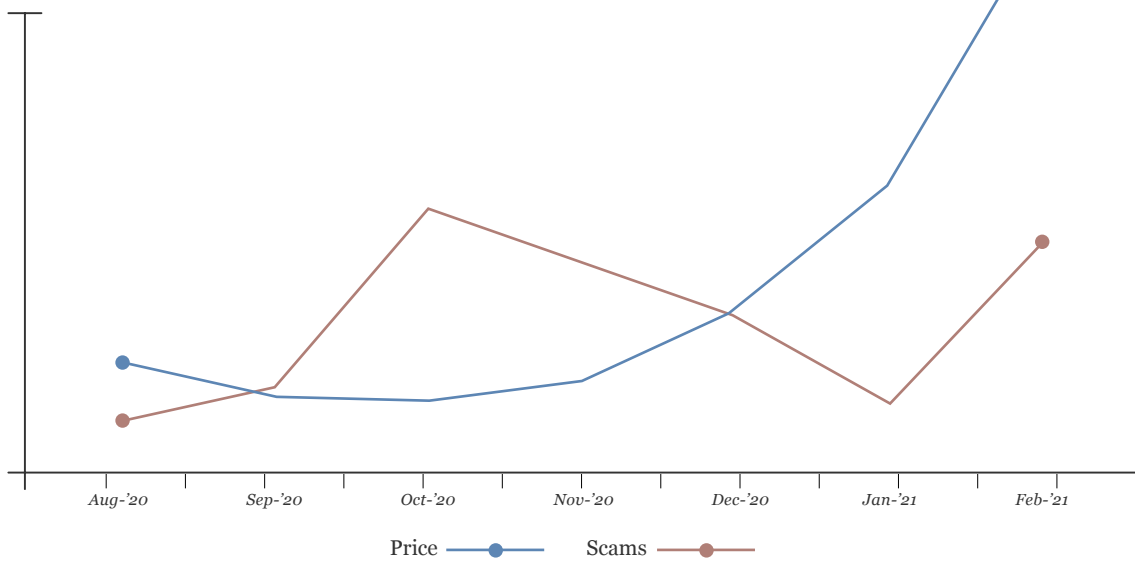
Cardano:

Cardano Scaled Price vs. Scams



PolkaDot:

Polkadot Price vs. Scams



Cryptocurrency Scam Report — Cryptocurrency is booming, so are the scams.

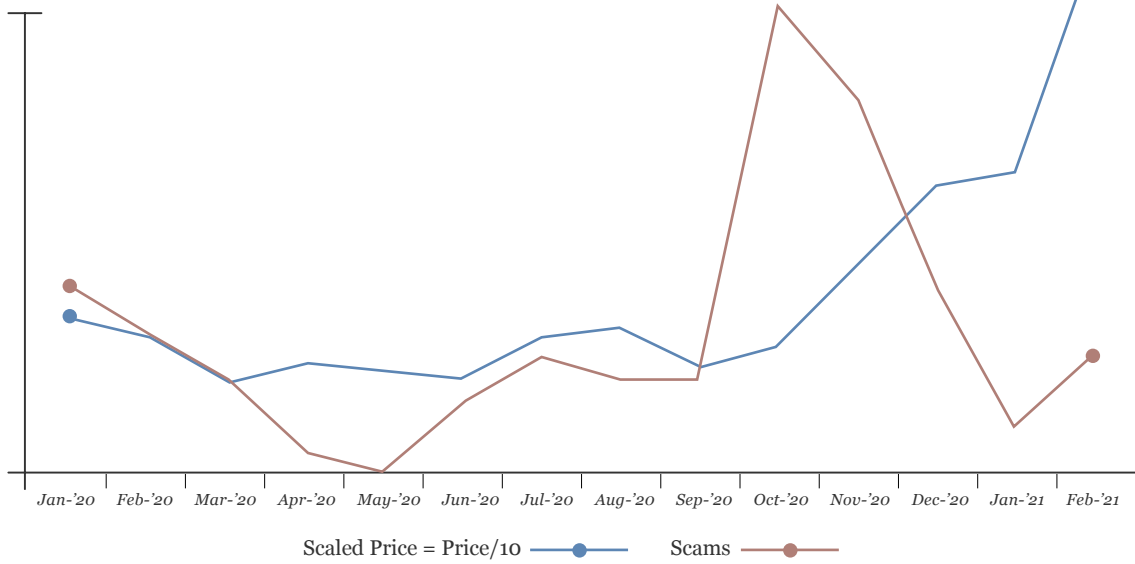
RippleXRP:

Ripple Price vs. Scams



Litecoin:

Litecoin Price vs. Scams



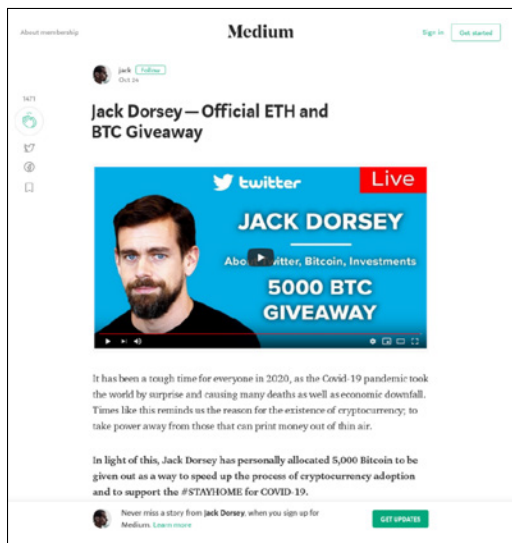
ChainLink:

ChainLink Price vs. Scams

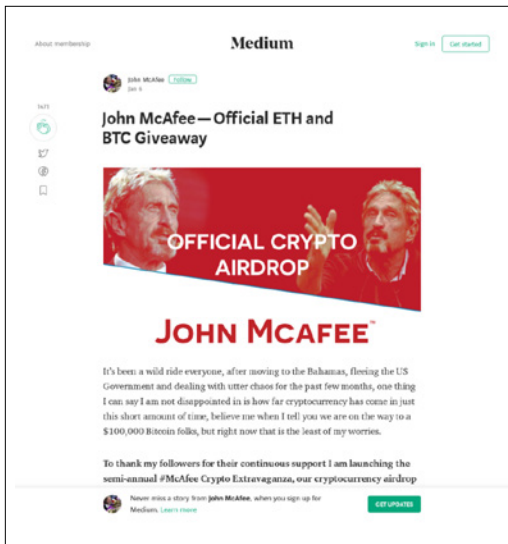


2. Celebrity Scams (Top 5)

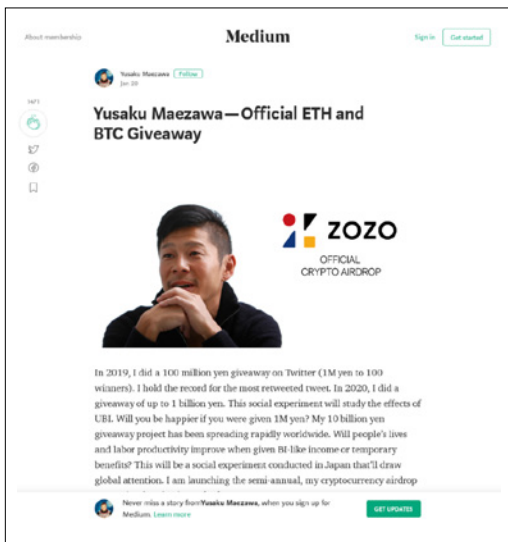
1. Elon Musk – See scam examples on [page 25-26](#)
2. Jack Dorsey:



3. John McAfee:



4. Yusaku Maezawa:



5. Bill Gates:

Bill Gates 5.000 BTC OFFICIAL GIVEAWAY by Microsoft!
Bill Gates • May 28, 2020



LIVE

5.000 BTC GIVEAWAY



Read below to find out how to participate!

At a time of such global crisis, Microsoft is here to offer all the help that we can. We understand the financial uncertainty that some people may be facing right now, and have decided to giveaway 5,000 Bitcoin, in our best attempts to help out.

How do I participate?

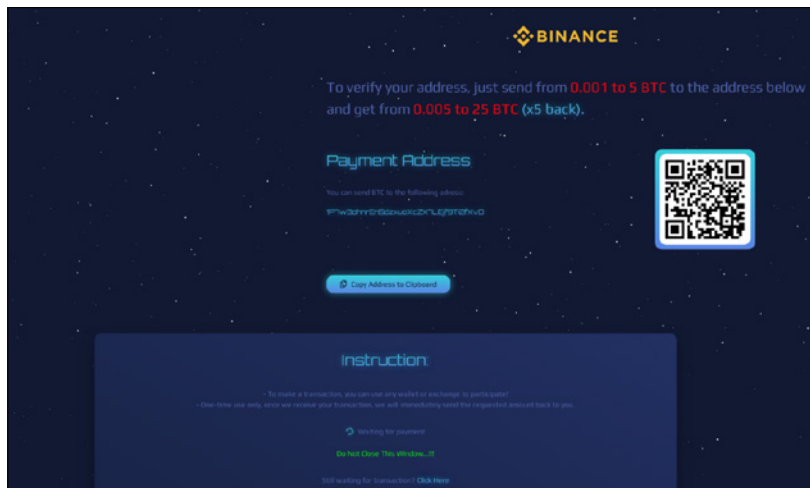
If you would like to participate in the giveaway, it's very simple! All you need to do is send any amount of Bitcoin, (between 0.1 BTC - 20.0 BTC) to our official contribution address for this event, and once we have received your transaction, we will immediately send back (2x) to the address that you sent the Bitcoin from.

► Contribution Address: 1Gates1pfGjmkUlpqD4GHxSeUvUG3b5r

◻ Send 0.1 BTC to receive 0.2 BTC back.
 ◻ Send 0.5 BTC to receive 1.0 BTC back.

3. Wallet Scams (Top 5)

1. Binance:



BINANCE

To verify your address, just send from 0.001 to 5 BTC to the address below and get from 0.005 to 25 BTC (x5 back).

Payment Address

You can send BTC to the following address:

1Fw3yYr182aw1c2K4Lp5t8HvD

[Copy Address to Clipboard](#)

Instruction

To make a transaction, you can use any wallet or exchange to participate! Once done, you only need to receive your transaction, we will immediately send the requested amount back to you.

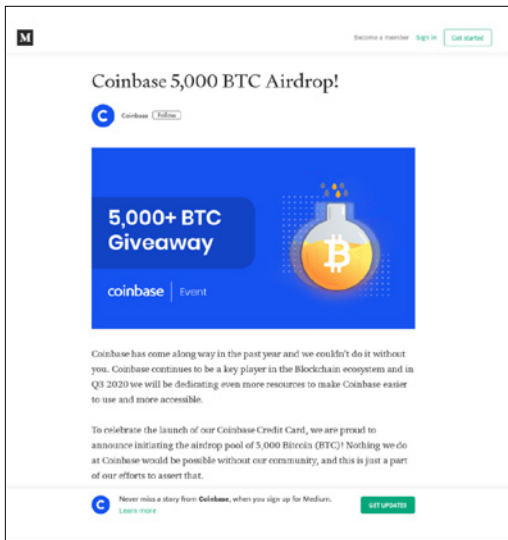
[Waiting for payment](#)

DO NOT CLOSE THIS WINDOW!!

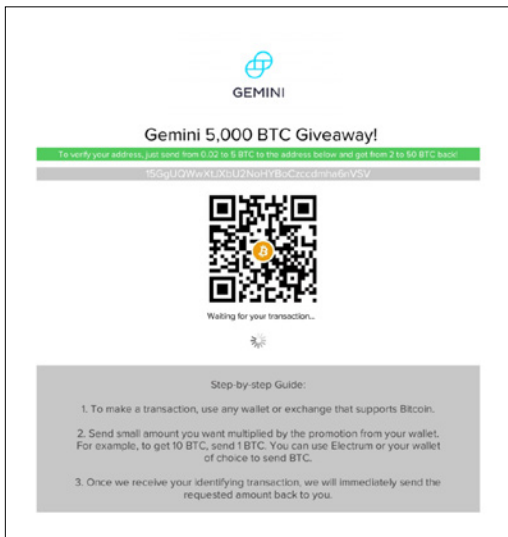
Still waiting for transaction? [Click Here](#)

Check our website and transaction, and download transaction to your wallet address.

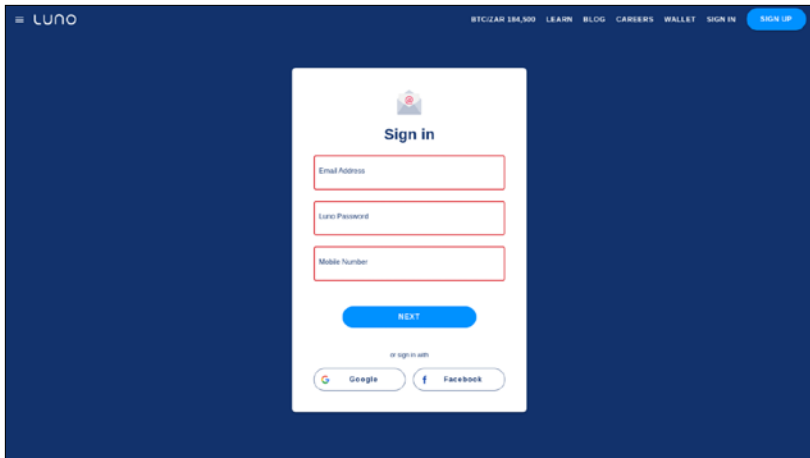
2. Coinbase:



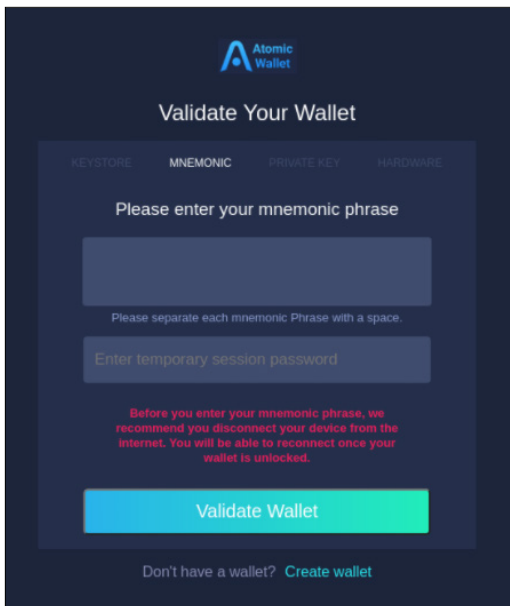
3. Gemini:



4. Luno:

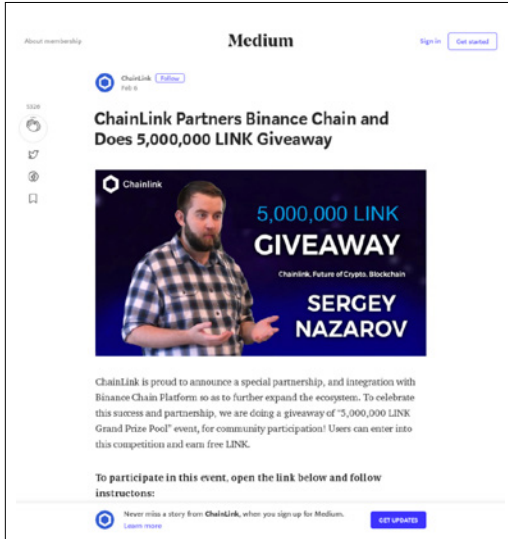


5. Atomic Wallet:

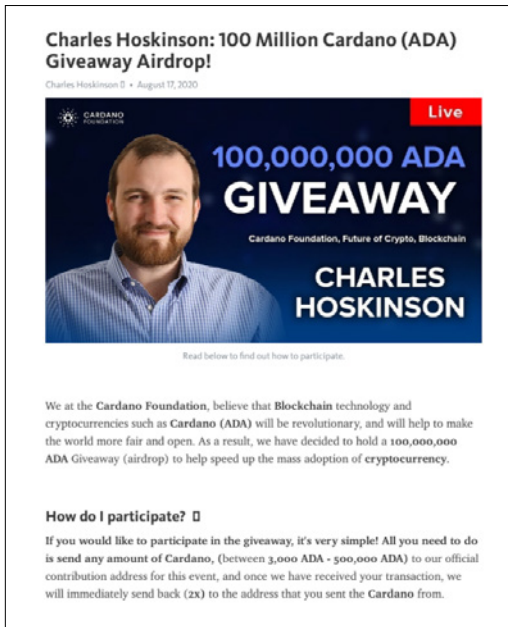


4. Cryptocurrency Scams (Top 5)

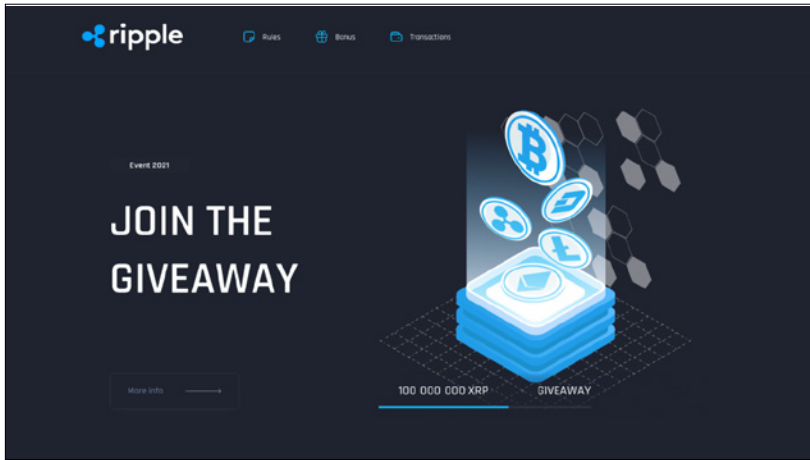
1. Bitcoin - See [paper](#)
2. ChainLink:



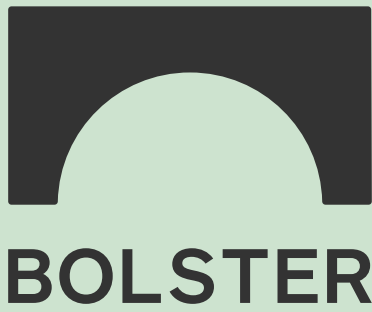
3. Ethereum – See [paper](#)
4. Cardano:



5. Ripple:



Cryptocurrency Scam Report — Cryptocurrency is booming, so are the scams.



www.bolster.ai
4966 El Camino Real, Suite #101
Los Altos, CA, USA 94022
info@bolster.ai