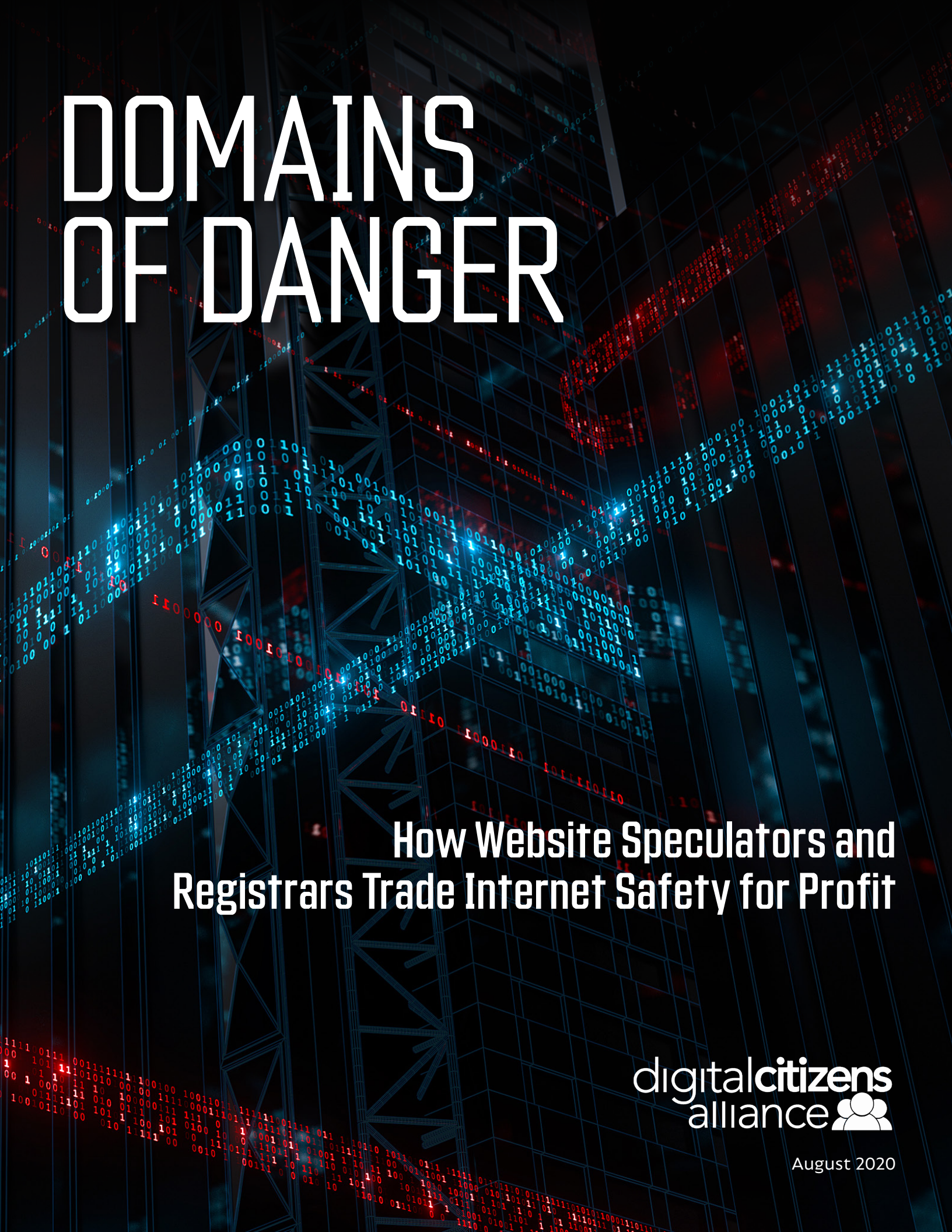


DOMAINS OF DANGER

How Website Speculators and Registrars Trade Internet Safety for Profit

digitalcitizens alliance

August 2020

Table of Contents

Since the first website 35 years ago, more than 375 million domain names have been registered, creating platforms for everything from commerce to communications to charities. But as the Internet took a dark turn in the last decade, those with the most to gain from a booming market – website speculators, registrars, and domain agents – have increasingly let bad actors have their run at domain names designed to scam, harm, and worse.

Digital Citizens supports a free and open Internet, but with that freedom comes responsibility. Just as "Platform Accountability" has become a call to action for Internet leaders Google and Facebook to do a better job of protecting users from harms facilitated by their services, the leading domain name providers should also take a greater responsibility for a safer Internet.

A Digital Citizens three-month investigation, spurred by reports of rampant fraud and price-gouging related to the COVID-19 pandemic, found that little to no effort is made to police domains whose sole purpose would be to scam (such as coronavaccinefree.com), endanger those most vulnerable (such as underage-girls-escorts.biz), or entice those seeking dangerous drugs (such as oxycodone-no-prescription.biz).

Digital Citizens easily acquired those names, and more, from registrars (the companies that have the right to create and sell domain names to the public). When some names were taken, so-called domain brokers, who help acquire names already taken, are more than ready to help even when informed the buyer wants to create a scam site (such as we told DomainAgents, a domain name buying service, when seeking its help to acquire coronavaccine.com).

This report also explores the no-holds-barred world of so-called domainers, the website speculators whose sole purpose is to snap up potentially valuable names and sell them at a premium – regardless of whether the name might have public interest benefits (as was the case with coronavirusinfo.com, which a domainer purchased at the start of the COVID crisis and immediately put up for auction for a minimum price of $5,000). In another instance, Digital Citizens investigators attempted to purchase daterapedrug.com, but were informed that it would cost $4,745 to do so. Instead, Digital Citizens was able to purchase date-rape-drug.com from Namecheap, a domain registrar called out by a leading cyber security company of sponsoring malicious domains.

Combined, these results reflect an industry, much like dominant online platforms, that is basing its sketchy dealings on what it can do, rather than what it should do to foster a healthy Internet. And much like the platforms that ignored public sentiment and policymaker concern over behavior that put profits over consumer safety, the domain industry may regret it.

As part of its investigation, Digital Citizens looked at how the domain industry addresses three issues of concern to policymakers and citizens: sex trafficking, dangerous drugs, and COVID scams and price gouging. Digital Citizens also conducted a research survey to explore Americans' perspectives on whether registrars and domainers should adopt a higher standard of care when it comes to potentially dangerous domains.

Digital Citizens reinforces that domain operators acting without regard to consumer and Internet safety do so at their own risk. Google and Facebook ignored similar warnings over the last decade and now face consumer protection, business and antitrust investigations by the Department of Justice and at least 48 state attorneys general.

This report is not about the legality of the domain operators' actions, but how by acting blind to the domain names they offer they can enable criminals and bad actors to seamlessly operate. Just as with the platforms, only time will tell if the leaders of the domain industry – companies such as GoDaddy and Domain.com, and others with the most to lose – take the initiative to raise the bar.

COVID AND DOMAINS: PROFITING FROM FEAR AND PANIC

The global coronavirus pandemic spurred widespread fear and uncertainty, and a clamor for information about prevention and treatment. This created a huge opportunity for bad actors who are more than happy to exploit this state of affairs for their own ill-gotten gains. Indeed, Digital Citizens has previously found videos on YouTube and ads on Facebook and Instagram purporting to sell coronavirus vaccines and personal protective equipment (PPE).

The ease with which bad actors can use online service providers is a chronic problem in the online environment. Katie Conner, a spokeswoman for Arizona Attorney General Mark Brnovich, recently said: "With social media, scammers can quickly spread the news about a fake miracle cure or fake product. We have seen just about everything in the last couple weeks, That's why we really want consumers to remember there is no cure for COVID-19." And a new report from activist group Avaaz found that "[g]roups and pages that spread misleading health news attracted an estimated 3.8 billion views on Facebook in the past year."

While abuses enabled by consumer facing platforms like Facebook and Google grab most of the headlines, the lesser-known domain name industry appears to suffer from similar problems. Digital Citizens found it easy to register domains such as "coronavaccinefree.com" and was encouraged to bid on domains such as "coronavaccine.com" even after telling a domain broker, "I know there is not a real vaccine but want to sell something anyway."

The lack of due diligence conducted by a number of these companies with respect to their commercial customers has real world consequences. The Federal Trade Commission has received more than 137,000 complaints related to the coronavirus with consumer losses exceeding $90 million.[1] In one example, the authorities shut down "coronavirusmedicalkit.com," – a domain registered with Namecheap - for peddling a "free" vaccine for a $4.95 shipping fee.

[1] https://public.tableau.com/profile/federal.trade.commission#!/vizhome/COVID-19andStimulusReports/Map

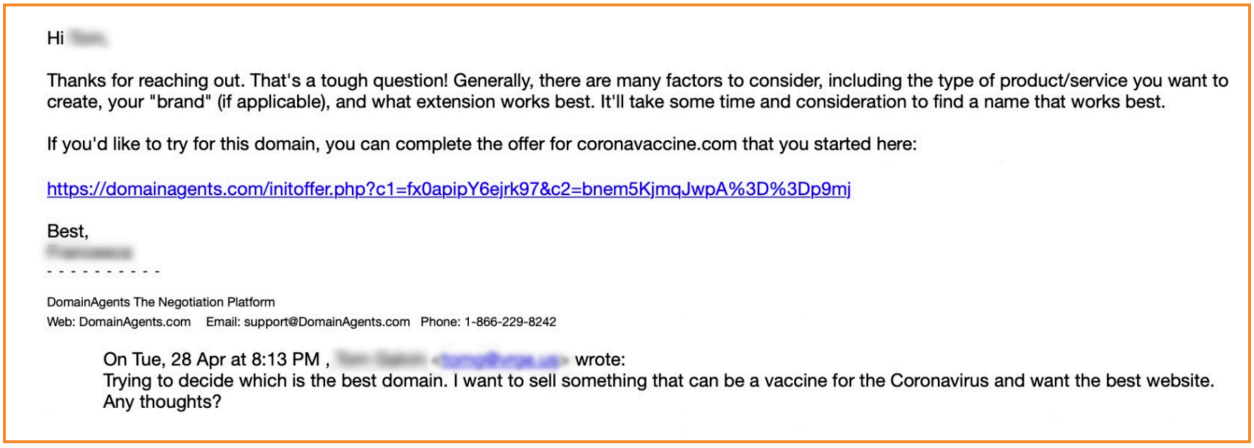
Given the opportunity for fraud and the risk it creates for public health, the need for business responsibility has never been greater. And yet, some domain name businesses are turning a blind eye to obvious attempts to scam those desperate for a solution to the deadly virus.

The domain name industry's vulnerability to COVID-19 related exploitation is no secret. Indeed, threat intelligence firm DomainTools recently created a free website offering "a curated list of high- risk COVID-19-related domains to support the community during the coronavirus crisis." Its data reveals that more than 100,000 registered domains related to the COVID-19 crisis had been flagged by DomainTools as "high risk" with more than two-thirds scoring 99 out of 100 on their risk scale. The score "predicts how likely a domain is to be malicious."

The risks caught the eye of U.S. policymakers. Senators Hirono, Booker, and Hassan sent a letter in April to the leaders of eight domain name registrars and hosting providers asking them "to explain the steps their companies are taking to combat misinformation about the coronavirus pandemic." They went on to note "it is critical that domain name registrars like yours exercise diligence and ensure that only legitimate organizations can register coronavirus-related domain names and domain names referencing online communications platforms."

After receiving response letters, Sen. Hirono told Morning Consult: "Too many domain name registrars and other Internet companies are putting their heads in the sand as cybercriminals and scammers try to exploit this pandemic by luring people to fraudulent coronavirus-related websites."

As part of its investigation, Digital Citizens reached out to DomainAgents, a company that brokers the sale of domain names already registered. After exploring what it would take to acquire "coronavaccine.com," DomainAgents reached out to a Digital Citizens investigator offering to help acquire the name. As you can see from the screenshots below, the fact that Digital Citizens expressed a willingness to offer a vaccine that clearly doesn't exist didn't faze the agent.



Hi [redacted],

Thanks for reaching out. That's a tough question! Generally, there are many factors to consider, including the type of product/service you want to create, your "brand" (if applicable), and what extension works best. It'll take some time and consideration to find a name that works best.

If you'd like to try for this domain, you can complete the offer for coronavaccine.com that you started here:

https://domainagents.com/initoffer.php?c1=fx0apipY6ejrk97&c2=bnem5KjmqJwpA%3D%3Dp9mj

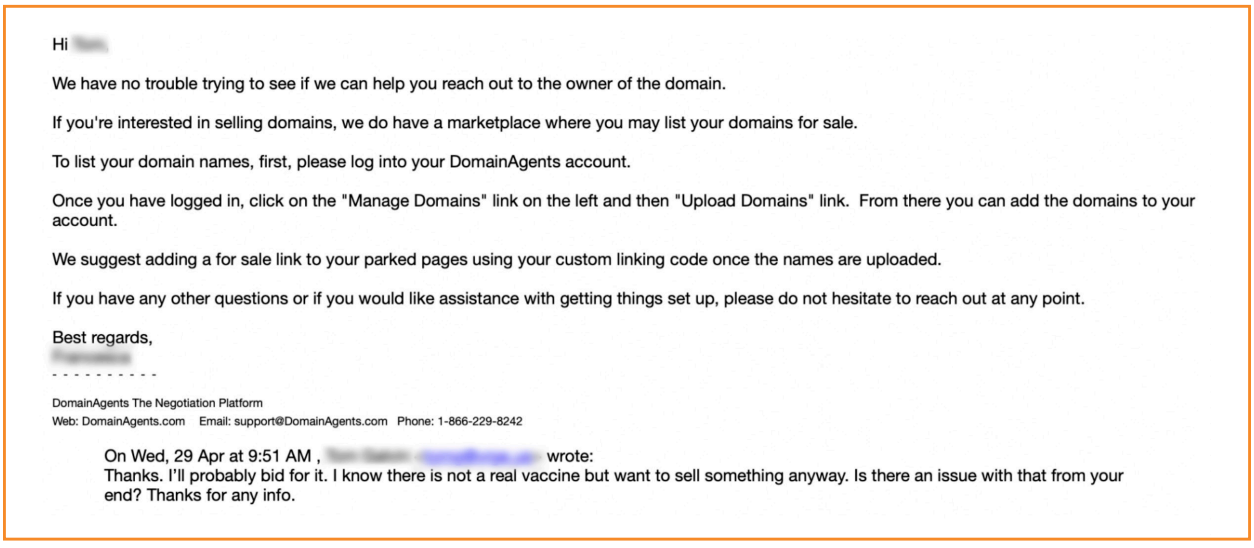
Best,
[redacted]
- - - - - - - - - -

DomainAgents The Negotiation Platform
Web: DomainAgents.com Email: support@DomainAgents.com Phone: 1-866-229-8242

On Tue, 28 Apr at 8:13 PM , [redacted] wrote:
Trying to decide which is the best domain. I want to sell something that can be a vaccine for the Coronavirus and want the best website. Any thoughts?

IMAGE 1

The Digital Citizens investigator then got more explicit that it was a scam. But that didn't change the response from the DomainAgents representative.



Hi [redacted],

We have no trouble trying to see if we can help you reach out to the owner of the domain.

If you're interested in selling domains, we do have a marketplace where you may list your domains for sale.

To list your domain names, first, please log into your DomainAgents account.

Once you have logged in, click on the "Manage Domains" link on the left and then "Upload Domains" link. From there you can add the domains to your account.

We suggest adding a for sale link to your parked pages using your custom linking code once the names are uploaded.

If you have any other questions or if you would like assistance with getting things set up, please do not hesitate to reach out at any point.

Best regards,
[redacted]
- - - - - - - - - -

DomainAgents The Negotiation Platform
Web: DomainAgents.com Email: support@DomainAgents.com Phone: 1-866-229-8242

On Wed, 29 Apr at 9:51 AM , [redacted] wrote:
Thanks. I'll probably bid for it. I know there is not a real vaccine but want to sell something anyway. Is there an issue with that from your end? Thanks for any info.

IMAGE 2

While this is perhaps the most egregious example, the ease of acquiring domain names that can be used for scams is alarming. Digital Citizens acquired multiple domain names from the following registrars:

- coronavirus-cure-for-sale.biz — Google
- Getcoronavaccines.com — Google
- Bleachcoronaviruscure.com — Google
- Freecoronavaccine.net — Domain.com
- Coronavaccinefree.com — Domain.com
- Freecurenow.com — Name Cheap
- Freecure.org — Name Cheap
- Buycovidcure.net — GoDaddy

To warn consumers, Digital Citizens launched an initiative about the dangers of COVID scams.

Users visiting the aforementioned websites received the following "offer":

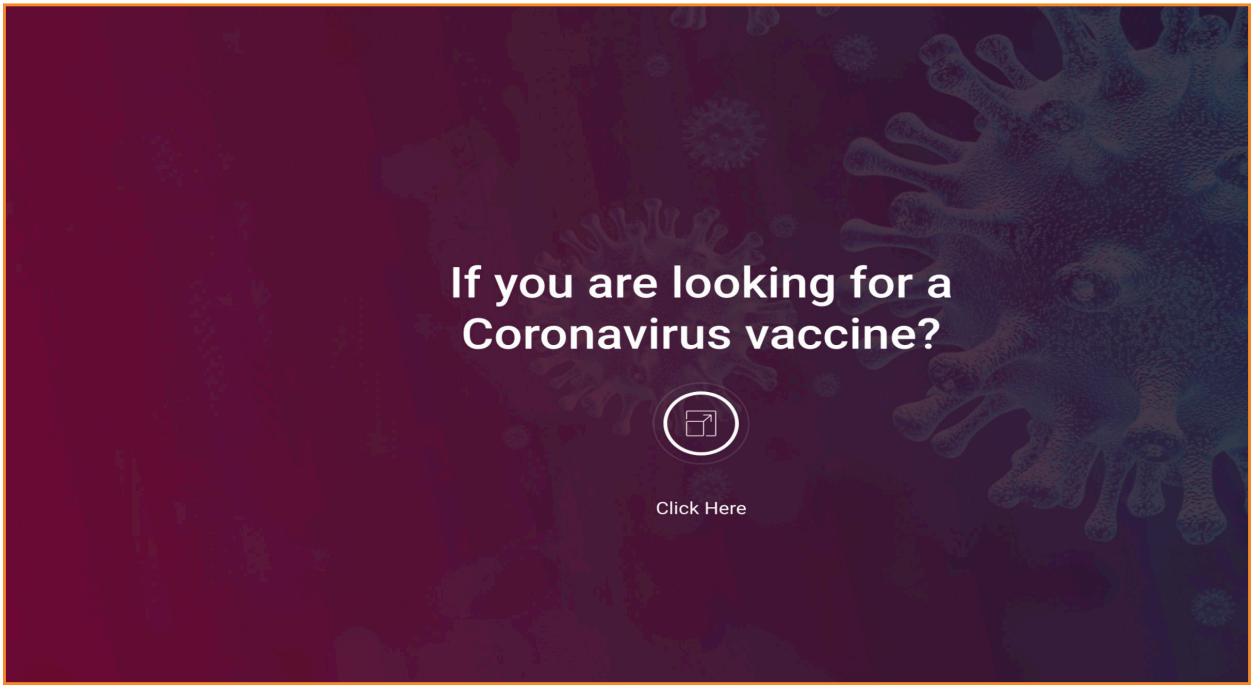


IMAGE 3

When visitors click for a vaccine, they are directed to a Digital Citizens warning page that includes information about online scams:

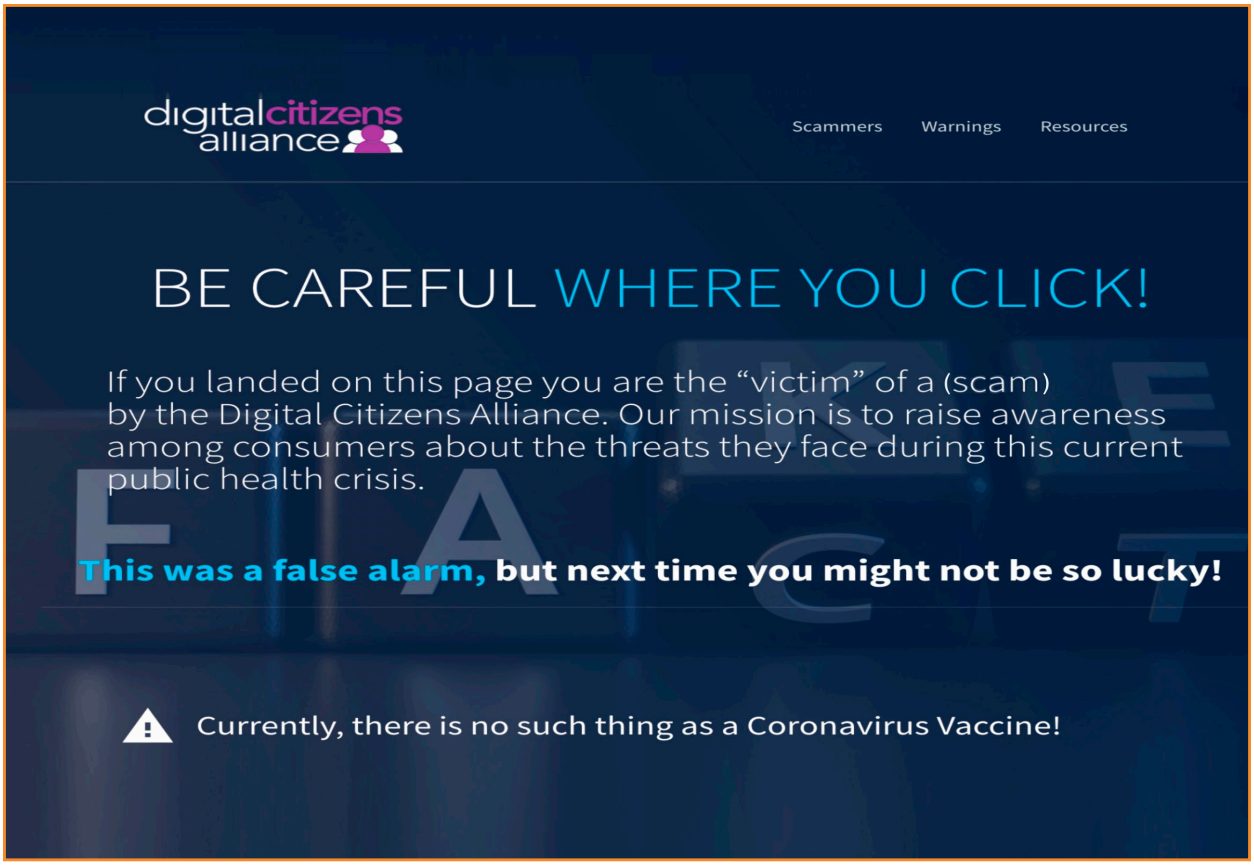
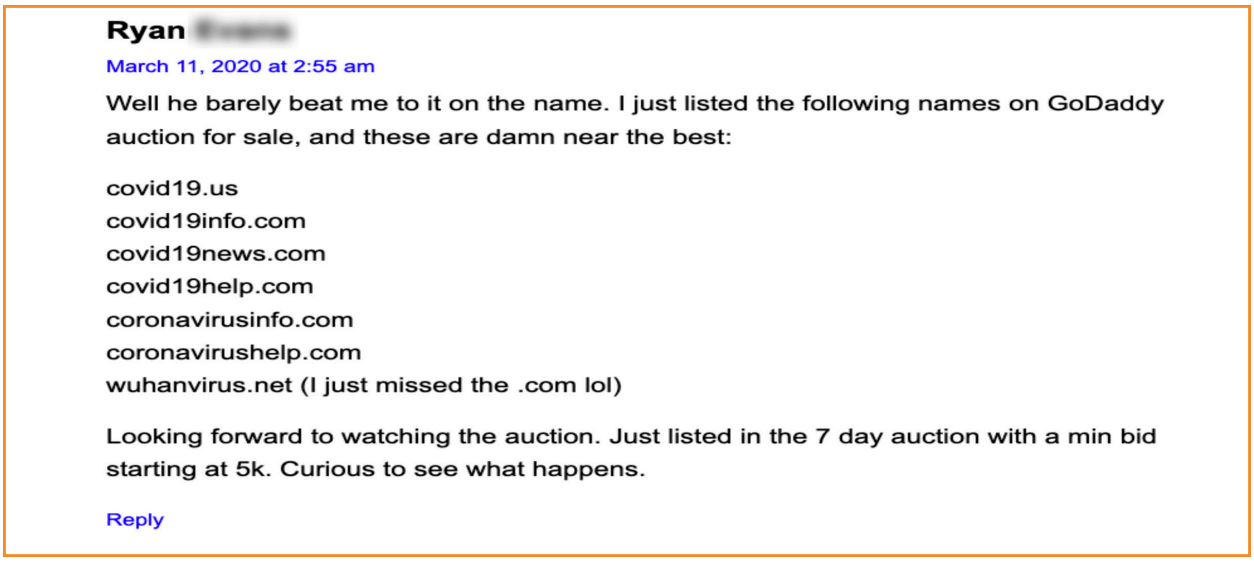


IMAGE 4

It is worth pointing out that the domain coronaviruscure.biz was acquired through Google Domains, a subsidiary of the advertising giant. While Google has launched high-profile efforts to identify online coronavirus scams, it's also potentially enabling them through its domain business.

The COVID crisis also put a spotlight on what can be an unseemly "domainer" market of those who purchase sometimes thousands of names in hopes of turning them around for a profit. In the early days of the crisis, domainers purchased popular COVID- related names. In the following message board, two domainers discuss names and potential returns:



Ryan [redacted]

March 11, 2020 at 2:55 am

Well he barely beat me to it on the name. I just listed the following names on GoDaddy auction for sale, and these are damn near the best:

covid19.us
covid19info.com
covid19news.com
covid19help.com
coronavirusinfo.com
coronavirushelp.com
wuhanvirus.net (I just missed the .com lol)

Looking forward to watching the auction. Just listed in the 7 day auction with a min bid starting at 5k. Curious to see what happens.

Reply

IMAGE 5

Just like those who scoop up popular show or movie tickets for resale, domainerscan warp the market by hoarding popular names and in this case crowd out those who may have had a philanthropic purpose to use a domain such as coronavirusinfo. com to spread helpful information. But instead of it costing $17.95, it would now cost that would-be philanthropist a minimum of $5,000 to launch that website.

Just like any market, bad actors learn who are the go-to players. The National Association of Boards of Pharmacies ("NABP") recently reported that "many COVID-related rogue pharmacies are registered with known 'safe haven' registrars." In the report, NABP cites that more than 50 percent of the rogue sites it identified had their domain registered by Hosting Concepts.

There are many who would say that the "free market" should reign in the domain industry, and it would be a legitimate point to make. But it speaks to the responsibility of the domain industry – in this case GoDaddy – to determine whether to conduct enhanced due diligence when offering clearly risky domains for sale.

As long as the number of COVID cases continues to grow, scammers and domainers will capitalize on Americans' fear and uncertainty. In July, the Federal Bureau of Investigation issued a renewed warning about a surge of COVID-related scams.

Consumers need to be on the alert; domain industry operators have to do better.

Sex Trafficking & Domains

Pootential coronavirus scam sites are not the only shady domains that bad actors can get easily and quickly. It shouldn't be easy to acquire domains that explicitly promote sex trafficking.

It is.

In roughly ten minutes, Digital Citizens purchased the following names:

• Jailbaitmarket.biz	Name Cheap
• Girlsforsale.biz	Name Cheap
• Sextrafficking.so	Name Cheap
• Trackingsexslaves.com	Name Cheap
• Barely18girlsforsale.biz	Google
• Underage-girls-escorts.biz	Google

Below is a screenshot of the purchase of barely18girlsforsale.biz. Note how Google, the domain provider, offers suggestions on the best way to ensure the domain isn't misunderstood.

IMAGE 6

It should go without saying that it's unlikely that a sex trafficker would register a domain as blatant as the ones Digital Citizens acquired, but if these names prompt no scrutiny, imagine what savvy and unscrupulous sex traffickers can do?

Since the crackdown on Craigslist and takedown of Backpage.com, which had facilitated child sex trafficking, other websites have surfaced. In June 2020, the owner of the website CityXGuide.com was charged in a 28-count indictment alleging it was a leading source of online advertisements for prostitution and sex trafficking.

And it goes beyond domains promoting sex trafficking. Namecheap had no qualms registering for Digital Citizens the domain date-rape-drug.com, but only after offering to sell the original request, daterapedrug.com, to an investigator for $4,745.

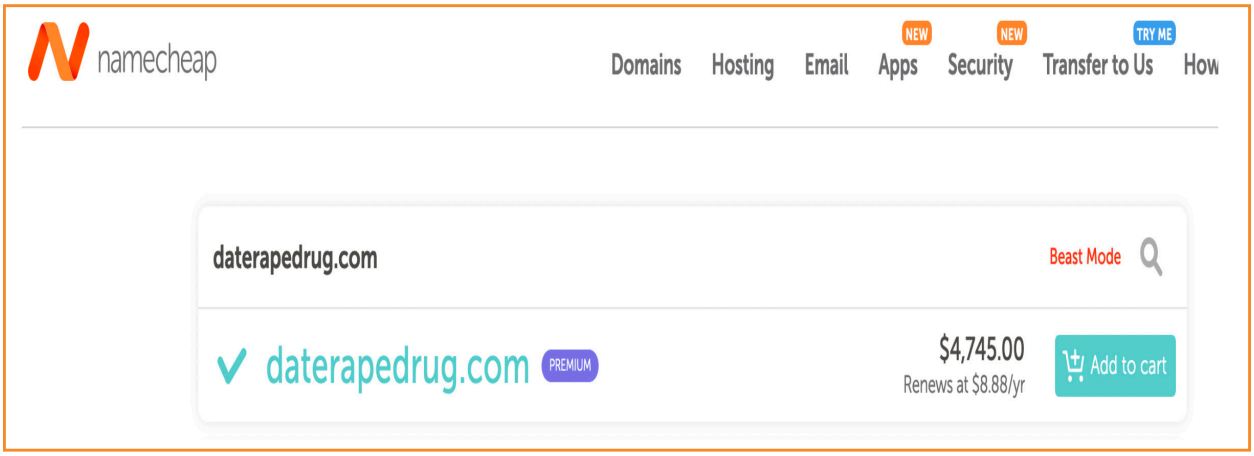


IMAGE 7

Digital Citizens reiterates the point it made at the start: it shouldn't be easy to acquire domains that explicitly promote sex trafficking. The fact that it is, and that domains such as date-rape-drug.com (or it's pricier counterpart daterapedrug.com) are readily available, reflects the need for the principle that the domain name industry must act responsibly.

Dangerous Drugs and the Domain Industry

The responsibility chasm in the domain industry is never more clear than when it comes to the online promotion and sale of dangerous drugs such as opioids. On the one hand, some domain registries (the wholesalers of domain names) announced that they will work with government authorities to suspend websites suspected of illegally selling opioids. On the other hand, registrars and brokers have no issue selling domains that promote the sale of opioids without a prescription.

The opioid crisis has prompted federal and state authorities to crack down on the illegal sale of the drugs online. Starting in 2013, Digital Cit- izens raised alarms about how easy painkillers could be bought online. And the organization has worked with state attorneys general to raise awareness about the proper disposal of opioids and other drugs.

That is why it's so concerning to see how easy registrars make it to purchase domains such as buy-oxycontin-online.us (Google) and oxycodone-no-prescription.biz (Namecheap).

Besides facilitating the domain registration of buy-oxycontine-online.us, Google also suggests other domain purchases to promote the online sale of opioids.

IMAGE 8

Why is this significant? Because according to experts, 97 percent of websites offering opioids operate illegally. Given Google's checkered history of promoting illegal online sales, it stands to reason they should be more careful. In 2011, the advertising giant paid $500 million to settle allegations that it aided Canadian pharmacies illegally marketing drugs in the United States. The case started when conman David Anthony Whitaker helped the FBI launch an undercover investigation into how Google helped him overcome safeguards against the illegal sale of drugs.

The effort to curb the illegal sale of drugs online is an area where progress has been made, strengthened only more by a program that enables government authorities to flag websites suspected of illegal drug sales. That is why it's so important to remain vigilant.

But the domains Digital Citizens purchased show how easily the effort to keep opioids and other drugs out of the hands of minors and those at risk can backslide. The domain industry can and should play a critical role in keeping illegal drugs off the Internet.

SEARCHING FOR RESPONSIBILITY IN DOMAIN WILD WEST

Digital Citizens has been here before.

In its 2013 report, "Google & YouTube and Evil Doers: Too Close for Comfort," Digital Citizens raised alarms about how the ad engine allowed – and profited – from a myriad of illegal or dangerous behavior. The report closed with a call for Google to take responsibility: "It is critical they are proactive in this regard; this is not the time or place for government to intervene. But we, the Digital Citizens, can hold them accountable."

Google now faces a reckoning for failing to heed the call for greater responsibility.

To be sure, the domain industry is not Google, nor will it be a lightning rod. But the examples laid out in this report will hopefully be taken seriously by domain industry operators. Over the last decade, the domain industry has been seemingly taken over by domainers and those who don't consider stewardship of the Internet a core principle. That is troubling.

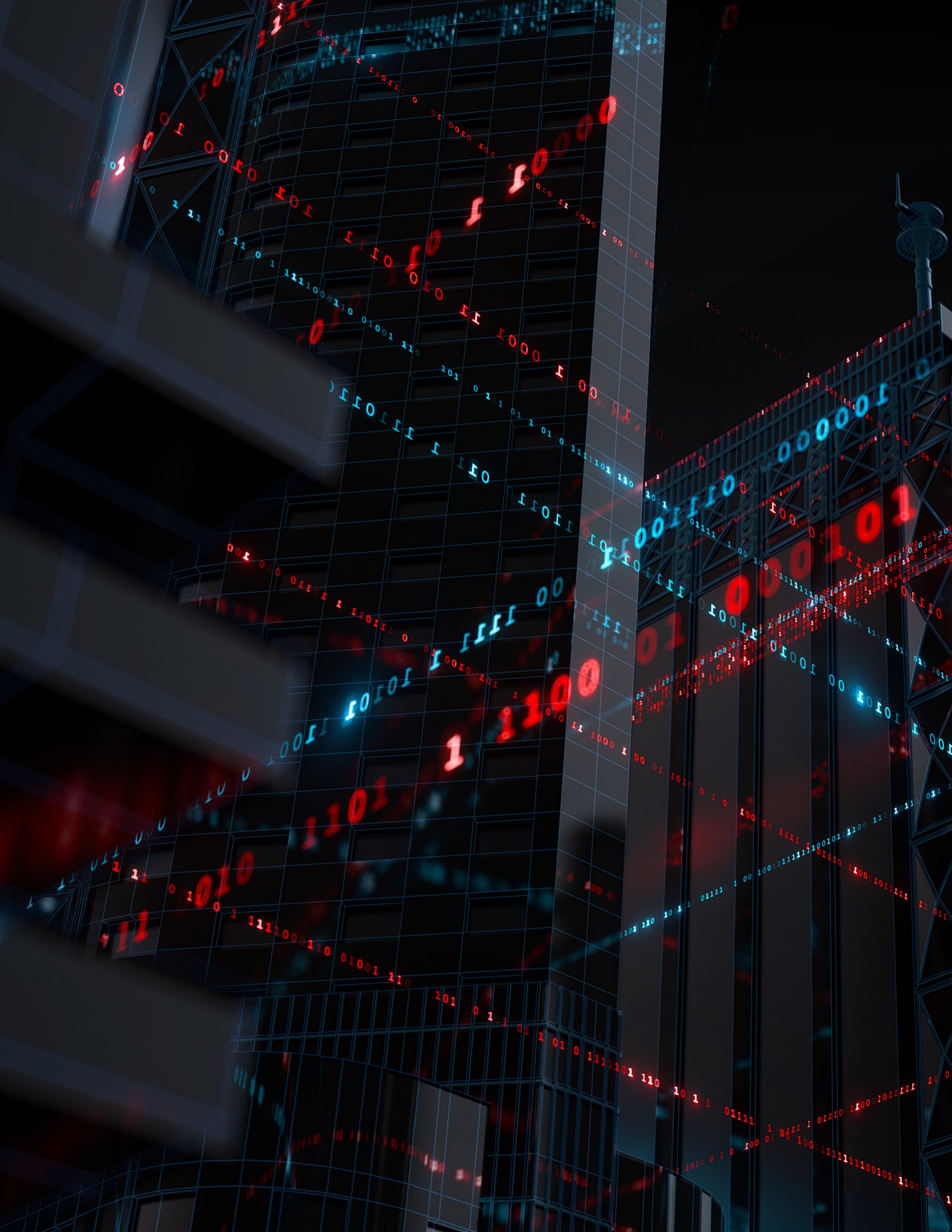
There is still time to recalibrate the system. Industry leaders should come together to identify the most dangerous ways bad actors are manipulating the unregulated domain market.

There are also mechanisms that could be put in place to put a "hold" on names that could be used to provoke violence, hate speech, or be a platform for malicious and illegal activity. Registrars should impose a review on domains that fit that criteria.

Unfortunately, a number of domain registrars do the opposite and turn a blind eye or even welcome malicious registrations. And domain domainers seemingly only factor in one thing: profit. That is not a recipe for the long-term health of the industry.

Domain name industry participants, government and other stakeholders should come together to craft solutions to these problems. Because just as any domain name can be registered, doesn't mean it should be, or that registrars have to do it. The industry, its stakeholders, and its self-regulatory forum, the Internet Corporation for Assigned Names and Numbers (ICANN) should work together to promote a domain name system that takes public safety, responsibility and accountability seriously. And if ICANN is unwilling or unable to do, then governments may need to step into the breach.

There is an opportunity for these businesses to do better and we need them to. We live in a time of crisis, fear, uncertainty, and misinformation – a toxic mix that leads to fraud and risks for those seeking to keep themselves safe. There has never been a more important time for online companies to demonstrate responsibility. We urge them to do so.



About Digital Citizens Alliance

The Digital Citizens Alliance is a nonprofit, 501(c)(6) organization that is a consumer-oriented coalition focused on educating the public and policymakers on the threats that consumers face on the Internet. Digital Citizens wants to create a dialogue on the importance for Internet stakeholders—individuals, government, and industry—to make the Web a safer place.

Based in Washington, DC, the Digital Citizens Alliance counts among its supporters: private citizens, the health, pharmaceutical and creative industries as well as online safety experts and other communities focused on Internet safety. Visit us at digitalcitizensalliance.org

digitalcitizens alliance