

Peddling For Profit

How Website Retailers Enable Bad Actors to Become the Master of Illicit Domains





Table of Contents

Executive Summary	2
Registering Without Concern	6
Illegal Guns	7
Stolen Credit Cards	8
Opioids	8
Malware	11
How Registrars Operate vs. What Internet Users Want	13
Online Crime Hits Americans Hard, and They Worry More Is Coming	14
Restoring Trust in our Digital Institutions	16

Executive Summary

The internet is an unprecedented platform for speech, expression, commerce, entertainment, and more. But in recent years, the absence of rules and regulations in the digital realm upon which we depend offline has become increasingly problematic. Digital Citizens has worked hard to shine a light on these abuses and the potential harms to consumers – whether it be exploiting social media platforms to advertise illegal COVID scams and recruit jihadists or demonstrating how piracy websites are used as bait to spread malware to consumers.

Abuse of consumer-facing platforms and websites like Facebook and YouTube understandably grabs the media and public's attention, given our familiarity with these services. But the internet is a much deeper and layered ecosystem of service providers which all play a role in the ultimate delivery of content and services to consumers – whether it be legitimate commerce or illegal and dangerous conduct or products and services.

Lesser known but vital players in this ecosystem are the companies that enable businesses, organizations, and individuals to establish a digital presence by acquiring a domain name. That industry is made up of registries, which administer hundreds of domain names such as .com, .org, and .biz and act as wholesalers; the domain name registrars, who offer specific domain names (such as digitalcitizensalliance.org) to consumers; and brokers, which operate in a robust secondary market where users can acquire a domain name that's already registered.

There is a close relationship between the registrars that serve as a first step to acquiring a domain name and the brokers who fuel the secondary market. Registrars partner with brokers, as Namecheap does with Domain Agents, or offer to purchase the name on the secondary market itself on behalf of customers, as both GoDaddy and Network Solutions do.

It's a crucial aspect of the internet: if websites are the buildings and locations we visit on the internet, domain names are their street signs. With more than 400 million domains in existence, they are the foundation of the online neighborhoods we visit to shop, connect with friends and family, support causes, and entertain ourselves. And it's often used to build and support illegal enterprises that are shielded against accountability by lackadaisical or non-existent verification efforts by domain retailers.

Indeed, more than a year after domain name sellers [promised to crack down on the sale of domains](#) on what would appear to be illegal or sketchy businesses, domain registrars and brokers remain willing to help would-be "entrepreneurs" create an online presence to peddle what would appear to be illicit goods and services, a Digital Citizens Alliance investigation has found. While the selling of these domains is legal, it raises questions about whether these registrars and brokers should take greater responsibility for keeping the Internet safe.

DigitalCitizens investigators found it easy, for example, to register domains that, on their face, would suggest illegal activities - such as [oxycodone-no-prescription.com](#) and [buyillegalassaultweapons.co](#). Willing retailers not only offered the names but, in some instances, offered to create an online advertising campaign to promote the venture. When a specific domain name offering to sell stolen credit cards was taken, a broker was ready to acquire the domain.

This indifference towards selling domain names for would-be illegal or illicit activity is troubling. It can make it easier for criminals and other bad actors to engage in activities that put the lives of adults and minors in harm's way. And it places these domain sellers at odds with Internet users, who have growing expectations that retail companies offering services make efforts to vet their business customers.

In its "Domains of Danger" 2020 report, Digital Citizens [spotlighted how COVID-related scams were made easier](#) by the ability to register misleading domains offering cures and vaccines. Over a year later, little has seemingly changed. Digital Citizens registered dozens of domain names for alarming potential businesses, such as [Malwareforsale.com](#) and [hitmanforhire.info](#). If the domain was taken, brokers that control the lucrative secondary market were willing to facilitate its acquisition for a substantial premium.

Digital Citizens purposefully registered and sought to purchase on the secondary market egregious domain names to test how registrars and brokers would react, as there are conceivably some uses for these domain names that don't involve illegality. But in these instances, the registrars raised no questions about the intended use of domains that, on their face, seemed likely to be used for illicit or dubious purposes. Nor did they appear to engage in any due diligence to determine the identity and motives of the would-be buyer. This seeming indifference to who their customers are and what they do with high-risk domain names runs contrary to what Americans expect from technology companies that enable digital commerce. According to a survey conducted by YouGov¹, there is a significant disconnect between consumers' low expectations regarding the steps these companies are currently taking to safeguard against abuse of their services and how consumers would like them to behave. Indeed, in that survey, only 39 percent said they believe technology companies closely verify the identity of their business customers. But double that amount, 82 percent, report that the companies *should* closely verify business customers.

Given that fraud, scams, and viruses that cause harm, such as ransomware, are getting increasing attention from law enforcement and the public alike, domain registrars and brokers are playing with fire if they continue to register domain names that appear to be for the potential purpose of illicit online activities. In Europe, momentum is growing to mandate that companies that provide services to businesses do a better job of verifying the identities of commercial actors using their services.

For example, the European Council and Parliament of the European Union [reached a preliminary agreement on the so-called Digital Services Act](#) to implement "Know Your Business Customer" (KYBC) rules on some online e-commerce marketplace providers. KYBC requires them to take measures to verify users of their services engaged in commercial activity. Similar measures to provide access to accurate WHOIS data for domain names are currently under consideration as part of a pending EU information security directive, known as "NIS2." And in September 2021, the U.S. Department of Commerce issued an Advanced Notice of Proposed Rulemaking seeking comment on potential regulations requiring online service providers to take meaningful steps to verify the identity of businesses paying for their services.

¹ Survey was conducted among 1,000 Americans aged 18+ through YouGov's online panel from March 1-7, 2022. The respondents were matched to a sampling frame on gender, age, race and education constructed by stratified sampling from the full 2019 American Community Survey (ACS).

And the data shows, that consumers overwhelmingly support proposals like "Know Your Business Customer." According to the same YouGov survey, 82 percent of Americans support proposals to require tech companies to check and verify their business customers' identities, and 6 in 10 of those say they *strongly* support these regulations.

Europe and the United States may be separated by a large ocean. Still, just as the internet knows no borders, the movement towards greater accountability by registrars and brokers doesn't. For that reason alone, it would be wise for these companies to take notice.

Registering Without Concern

Let's start with the obvious. With over 400 million domain names, it's a challenge for registrars to dedicate staff to review each domain as it is purchased. But the volume of domains registered or sold by registrars or brokers can't be a blanket excuse to avoid accountability. It comes down to this: just because these domains can be legally registered, should well-known domain operators allow them to be?

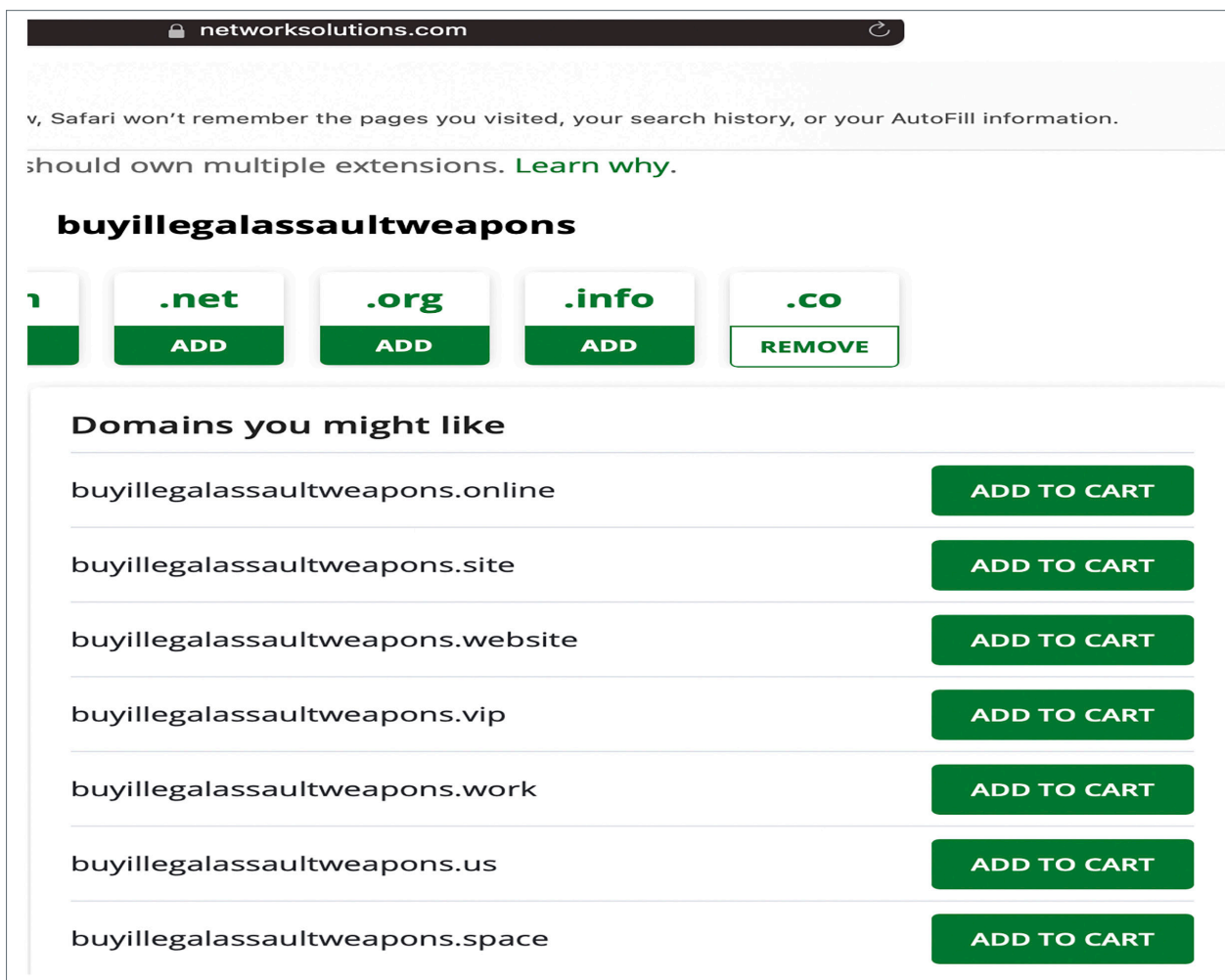
Case in point: domains offering stolen credit cards – such as **buystolencreditcards.com** – would appear on their face to be offering an illegal product. Yet, it is easily registered.

This apparent indifference is even more troubling given that the existence of "high risk" domains is well-known to the industry. Respected online security research firm DomainTools has cataloged and analyzed domains, assigning scores (1-100) to better gauge their potential for abuse – with a score of 70 or higher denoting "high risk." But carrying a high volume of "high risk" domains doesn't appear to trigger an increased sense of responsibility by some companies selling them. For instance, almost 5.8 million of Namecheap's 26.3 million domains (22 percent) score 70 or more – and yet a Digital Citizens investigator easily registered **buystolencreditcards.com** from Namecheap (as chronicled later in the report).

Illegal Guns

Guns are the leading cause of death among children in the United States. While online gun sales are legal, the purchases are regulated by the Bureau of Alcohol, Tobacco, Firearms, and Explosives. Yet it's easy to acquire a domain that blatantly offers illegal guns. For example, Network Solutions registered **buyillegalassaultweapons.co** – then proposed a slew of other domains with “buyillegalassaultweapons” in the name. Once again, the sale is legal. The question is whether this is the type of business a domain registrar wants to be associated with.

Image 1. “buyillegalassaultweapons” Domains for Sale.



The screenshot shows a web browser window with the address bar displaying "networksolutions.com". The page content includes a notification about Safari's privacy settings, a search bar, and a list of domain options for "buyillegalassaultweapons".

buyillegalassaultweapons

1 .net .org .info .co
ADD ADD ADD REMOVE

Domains you might like

buyillegalassaultweapons.online	ADD TO CART
buyillegalassaultweapons.site	ADD TO CART
buyillegalassaultweapons.website	ADD TO CART
buyillegalassaultweapons.vip	ADD TO CART
buyillegalassaultweapons.work	ADD TO CART
buyillegalassaultweapons.us	ADD TO CART
buyillegalassaultweapons.space	ADD TO CART

Image 1

GoDaddy enabled Digital Citizens to register **untraceablegunsforsale.com**, then, within minutes, its web builder tool enabled investigators to create a potential website design.

Image 2. "untraceablegunsforsale" Domains for Sale

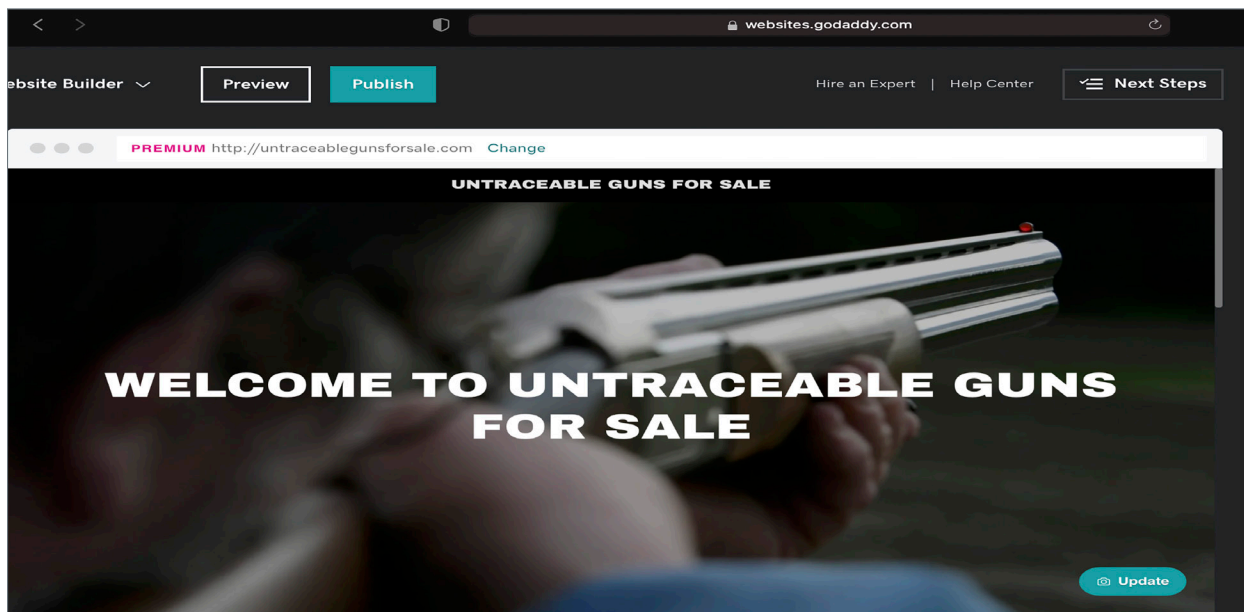


Image 2

For hopefully self-explanatory reasons, Digital Citizens didn't publish the website.

Stolen Credit Cards

Domains offering stolen credit cards – such as [buystolencreditcards.com](#) – would appear on their face to be offering an illegal product. But Namecheap registered the name on behalf of Digital Citizens investigators. Digital Citizens then tested whether the broker Domain Agents would help another investigator acquire it. The broker canceled the deal at one point, but shortly after, it agreed to try to acquire [stolencreditcardsforsale.com](#).

Opioids

The [opioid crisis continues to take the lives of over 100,000 Americans a year](#). But that doesn't mean it's hard to get a domain name to sell them. Namecheap registered the domain [buyopioidswithoutrx.biz](#) for investigators.

Image 3. Buying The “buyopiodswithoutrx” Domain

Domain Registration buyopiodswithoutrx.biz	1 year	\$15.98 \$4.98	MANAGE
ICANN fee		\$0.18	
Free Domain Privacy	1 year	\$0.00	MANAGE
Initial Charged		\$5.16	
Total Charged		\$5.16	

Image 3

GoDaddy registered the domain **oxycodone-no-prescription.com**.

Image 4. Buying "oxycodone-no-prescription.com" domain via GoDaddy

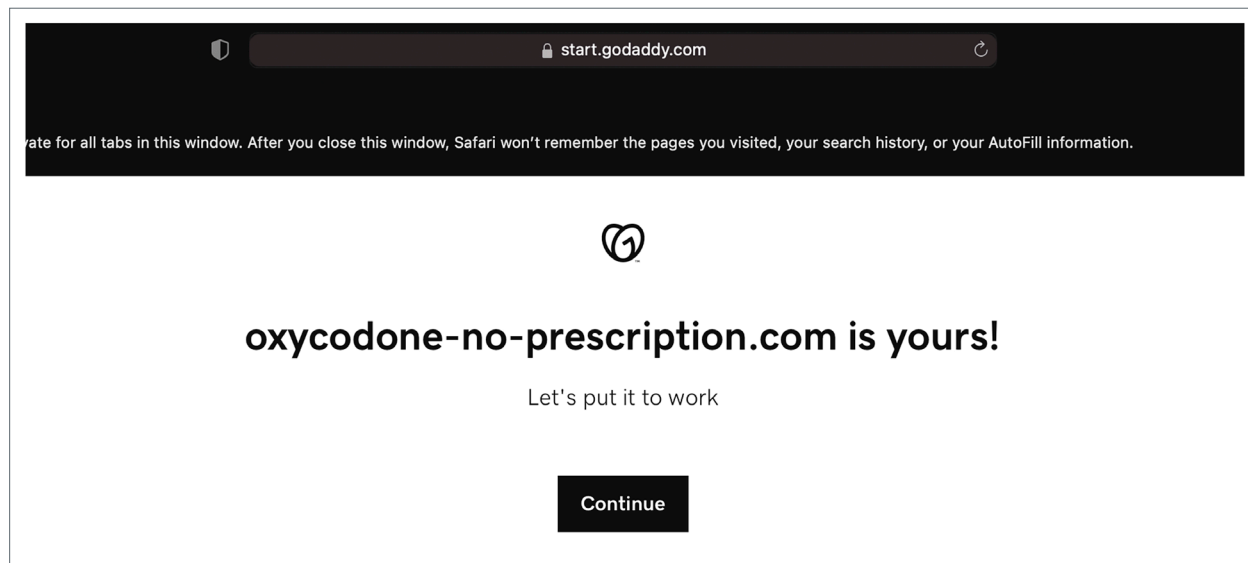


Image 4

In each case, again, while the registration process itself was legal, the likely use of the domain seems clear.

It went a step further. GoDaddy also offered to help the new domain holder make a profit on oxycodone-no-prescription.com by selling it on a GoDaddy-controlled secondary market site:

Image 5. Researcher Buys "oxycodone-no-prescription.com"

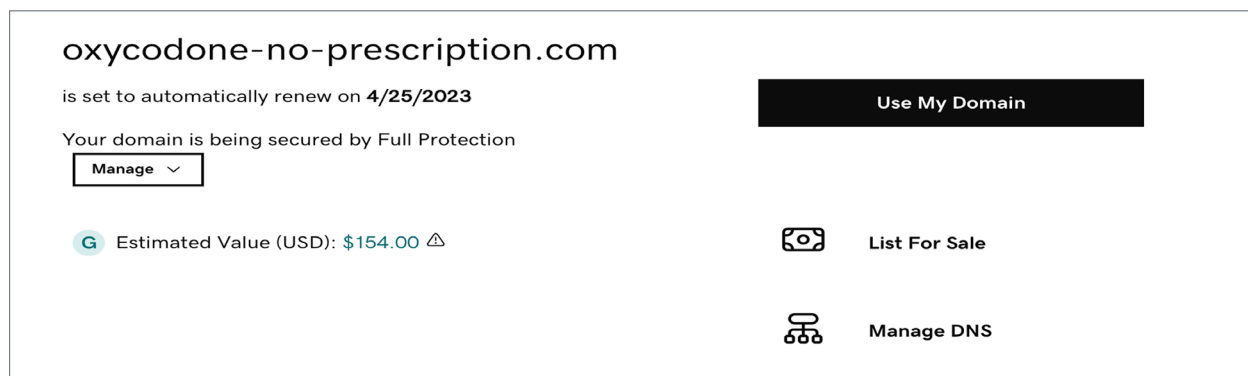


Image 5

Image 6. GoDaddy Suggests Selling "oxycodone-no-prescription.com"



Image 6

Malware

Ransomware attacks are wreaking havoc across the world. In February, cyber security authorities warned that in 2021 there was a [spike in high-impact attacks against critical infrastructure](#) across the globe. And a February 2022 research survey warned that 75 percent of small to mid-sized companies [would be forced to close their doors if targeted by a ransomware attack](#). And it's not just businesses who are worried: two-thirds of Americans (64 percent) reported to YouGov that they are concerned about malware attacks online. As a vital part of the critical infrastructure, the domain industry places a heavy focus on cyber security but still doesn't hesitate to register domains that claim to sell malware.

Malwareforsale.com is a straightforward name, leaving no ambiguity over its purpose. And it was registered with ease with Namecheap.

Image 7. Buying “Malwareforsale.com” on Namecheap

Item	Duration	Price	Action
Free Domain Privacy	1 year	\$0.00	MANAGE
Domain Registration	1 year	\$13.98 \$8.98	MANAGE
malwareforsale.com			
ICANN fee		\$0.18	
Free Domain Privacy	1 year	\$0.00	MANAGE
Initial Charged		\$18.32	
Total Charged		\$18.32	

Image 7

To see if other names would give pause to a registrar, investigators tried **dangerousmalwareforsale.co**. And Google, which prides itself on its efforts to [combat ransomware](#), registered it.

GoDaddy, Network Solutions, Google, Namecheap, and other companies mentioned in this report consider themselves leaders in the domain industry. Yet, these consumer-facing companies seem reluctant to take the lead in identifying domains that could be dangerous.

The dozen or so domains referenced in this report are just a sample of what Digital Citizens was able to register. Ultimately, they were registered to test whether registrars and brokers put safeguards against potential bad actors establishing an apparently nefarious website. It's fair to say, based on this investigative exercise, the answer is a resounding no.

How Registrars Operate vs. What Internet Users Want

In this report, Digital Citizens did learn something: Internet users are looking for the industry to step up. That is partly due to experience. Two-thirds of those who responded to the YouGov survey reported having been victims of an online crime or violation such as credit card or identity theft, data breach, scam, or ransomware.

For that reason, many Internet users tend to be once bitten, twice shy. More than three-quarters of the survey's 1000 respondents said they closely evaluate websites where they use their credit cards or supply personal data. That scrutiny is at odds with how retail domain providers vet their customers.

Just 13 percent of Americans believe tech companies are very closely checking and verifying their business customers' IDs before selling them services. And they have suspicions as to why some businesses hide their identity from service providers: more than half said it's likely they hide their identity to violate privacy laws (63 percent), avoid law enforcement (56 percent), or avoid taxes (56 percent).

Internet users are looking for diligence. Eighty-Two percent of Americans report that they'd like companies selling tech services to business websites to regularly verify the identity of the company operators, with 54 percent believing these obligations would protect consumers from scammers, hackers, and thieves.

What's more, consumers don't believe verifying business customers is too much to ask of online service providers. Seventy-six percent of Americans believe that tech companies that offer business services have the know-how and resources to verify those customers.

The survey results overwhelmingly demonstrate that lawmakers and regulators have the public's support when proposing rules and regulations designed to make it harder for bad actors to conduct illegal business online.

Online Crime Hits Americans Hard and They Worry More Is Coming

While we know millions of Americans have experienced some kind of online attack, the numbers still tell a disturbing, troubling story. More Americans told researchers they have had their credit card information stolen or compromised (33 percent) than those who said they've never been a victim of online crime (32 percent). Consider the reaction if we surveyed pedestrians at some of the busiest intersections in U.S. cities and more said they had been robbed there than those who said it was safe? But that's not the whole story - 1 in 4 said they had been infected with malware from a website or browser and 1 in 5 said they were victims of a data breach.

The history of criminality could threaten the long-term viability of the internet as we know it. Eight-in-10 Americans are concerned about criminals using fake IDs to sign up for online services. We know the criminals often use fake identities to sign up for the online services used to run websites like those shared in this report. Nearly two-thirds of respondents said criminals likely use fake IDs to illegally collect people's data or identities.

This leads us to the role tech companies could or should play in restoring Americans' confidence in the internet. When asked if tech companies should closely check and verify the identities of their business customers - an overwhelming 82 percent said they should, while less than half (43 percent) of respondents thought companies were actually doing that. Six-in-10 believe financial institutions have shown that checking and verifying ID is practical and effective.

Furthermore, Americans had some definite ideas on how companies could keep Americans safer:

- When asked if companies should be required to check and verify the identity of foreign business websites, 82 percent said yes. Interestingly, when asked about U.S.-based websites, again 82 percent said companies should have to check and verify them as well.
- 82 percent of companies selling tech should have to recheck and verify ID to stop cybercriminals from doing a bait and switch.
- 79 percent said tech sellers should terminate support for a website not sharing proper ID.

YouGov interviewed 1,325 respondents who were then matched down to a sample of 1,000 to produce the final dataset. The respondents were matched to a sampling frame on gender, age, race, and education. The frame was constructed by stratified sampling from the full 2019 American Community Survey (ACS) 1-year sample with selection within strata by weighted sampling with replacements (using the person weights on the public use file).

This survey was conducted March 1-7. The MOE is +/- 3.81.

Restoring Trust in our Digital Institutions

A recent [piece](#) in *The Atlantic* about the challenges today's internet poses to a well-functioning democratic society offers the following solution (among others):

Banks and other industries have "know your customer" rules, so they can't do business with anonymous clients laundering money from criminal enterprises. Large social media platforms should be required to do the same.

The author's observation rings true for domain name registrars and brokers who sell high-risk domain names to any buyer, including criminals and bad actors, counting on their laissez-faire approach to identity verification. And brokers, who, [according to DomainAgent CEO Ryan McKegney](#), "represent neither the buyer nor the seller," are more focused on the potential profits they can reap on the secondary market for domain names, which can reach five, six, and even seven figures – whether or not the buyer is up to no good.

Consumers want and deserve better. And based on the wave of scrutiny regarding online harm, governments are increasingly inclined to give it to them. Registrars operate in a lightly regulated market; secondary market players face no regulation. Will that continue? That's likely up to whether they wake up to a changing world that expects more of them – and that means stepping up their efforts to ensure their marketplaces serve legitimate businesses and consumers instead of registering dangerous domains just because someone can.

In short, the ground is shifting. To understand how much, consider how the EU's Digital Services Act – which seeks to broadly reign in online abuse in part facilitated by tech companies – would have been received in the United States a decade ago when Google and Facebook were corporate darlings before Cambridge Analytica exposed a world of data

exploitation. Russia used the United States' openness as an election-year weapon against its citizens. As the YouGov survey clearly shows, consumers now expect far more from online service providers.

This brings us back to the prospect of the principles of the EU's Digital Services Act being adopted in the United States – regulations that would have been inconceivable just years ago.

Yet, The Washington Post urged U.S. policy leaders earlier this year [to bone up on the EU's vision for tech regulation](#): "U.S. legislators should study the Digital Services Act because it could inform whatever rules they write, and they should also study it because some of its rules will likely *become* the rules here."

Those rules speak to the frustration that domain name retailers such as GoDaddy, Google, and Namecheap deploy sophisticated systems to offer customers domain names they might like – yet seemingly don't dedicate those resources to prevent abuse.

This is not to say that every provocative name is dangerous – it's just that nearly all of these retailers don't seem to bother to check. If domain registrars and brokers don't see the benefit in knowing their customers, they may be forced to by policymakers fed up with waiting for them.



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

