identity digital

Anti-Abuse Report Q1 2026

What is Typosquatting?

Even careful typists make mistakes, and bad actors know it. Typosquatting is the practice of registering misspelled variants of legitimate domain names to intercept misdirected traffic and exploit the users behind it.

Consider our own domain, identity.digital, as an example. Drop the "t" and you get idenity.digital, a plausible enough typo that it may not register immediately. Anyone who registers that variant can stand up a convincing clone and capture credentials, clicks, or personal data from visitors who believe they have navigated to their intended website. With modern AI tools capable of replicating a site's look and feel in minutes, the barrier to a convincing phishing operation has never been lower.

How AI Lowers the Barrier

When we asked an AI platform to generate the most likely typos for the word "identity." It returned five in seconds:

1. Identitiy (extra "i")
2. Idenity (missing "t")
3. Identiry or Idenrity (key proximity slip)
4. Identtity (double "t")
5. Idneity (transposition)

Now multiply that across every registrable string, and the scope of the attack surface comes into focus. The tooling needed to map targets is widely accessible, which makes proactive defense more valuable than ever.

How to Protect Yourself

A few consistent habits go a long way toward keeping you and your organization secure.

1. Verify URLs before submitting credentials. A brief glance before entering sensitive information is a low effort habit with meaningful security implications.
2. Use a password manager. Tools like 1Password autofill only on exact URL matches. A lookalike domain will not trigger autofill, giving you a reliable signal that the destination may not be what it appears.
3. Bookmark high value destinations. Removing manual URL entry for critical sites closes the attack vector entirely.
4. Register defensive domains. We have registered idenity.digital alongside identity.digital to take that variant off the table. Microsoft redirects microsot.com and Google redirects gooogle.com for the same reason. For any organization with meaningful web presence, defensive registration is a smart, low-cost investment.

Help Us Keep the Namespace Trustworthy

If you encounter a malicious site operating under an Identity Digital TLD, please report it to us. Maintaining a trustworthy namespace is a responsibility we take seriously across every TLD we support.

Abuse Reporting Statistics

The table below includes information about the number of reports Identity Digital has received in the last quarter about domain names in our TLDs. We may receive multiple reports about the same domain name, and multiple reports are often consolidated into one case.

102,465
Total Domains Reported

Type of Abuse	Detection Method	Number of Reports	Number of Domains Reported	Number of Domains on serverHold	% of Total Domains Reported	Number of Reports by Abuse Type
Phishing	Abuse List Report API Submissions Manual Submissions Third Party Reports (email or abuse form)	39,010 19,704 1,559 19,154	28,997	11,892	28.30%	79,427
Malware	Abuse List Report API Submissions Third Party Reports (email or abuse form)	3,205 396 181	1,220	53	1.19%	3,782
Pharming	Any	0	0	0	0%	0
Botnets	Any	992	579	41	0.57%	992
Spam (as a delivery mechanism)	Report API Submissions Third Party Reports (email or form)	13 147	145	3	0.14%	160
Denial-of-Service Attacks	Any	0	0	0	0%	0
Child Sexual Abuse Material	IWF Third Party Reports (email or form)	274 0	53	8	0.05%	274
Promotion, encouragement, sale, or distribution of prescription medication without a valid prescription in violation of applicable law	Third Party Reports (email or form)	902	144	70	0.14%	902
Illegal access of computers or networks	Any	0	0	0	0%	0
Cyber-bullying, harassment, or other forms of abuse to individuals or groups	Any	7	5	0	0%	7
Incitement to violence or other unlawful actions	Third Party Reports (email or form)	59	42	0	0.04%	59
Failure by registrant of a two-character SLD to take steps to ensure against misrepresenting or falsely implying that it is affiliated with the corresponding government or country-code manager, if such affiliation, sponsorship or endorsement does not exist	Any	0	0	0	0%	0
Holding oneself out as a licensed medical practitioner in a .doctor domain name when such license doesn't exist	Any	0	0	0	0%	0
Other	Report API Submissions Manual Submissions Third Party Reports (email or abuse form) Abuse List	592 71,568 554 969	72,437	532	70.69%	73,683

Action Timeline

0hrs

Registrar took action **PRIOR** to registry escalation	684 cases	843 domains
Registry took action **PRIOR** to registrar escalation (protective hold)	1,373 cases	5,087 domains

24hrs

Registrant or third party remediation (e.g. compromise fix, hosting etc.)	339 cases	298 domains
Registrar response provided reasonable explanation (no further action taken)	838 cases	5,937 domains
Registrar took action **POST** registry escalation	477 cases	446 domains

72hrs

Registry took action **POST** registrar escalation	715 cases	7,474 domains
Compromised / Platform (registry intervention deemed inappropriate)	29 cases	48 domains

5,107
Cases closed*

21,666
Unique domains affected (closed)**

5,087
Domains placed on protective holds (within 24 hrs of report)

0.15%
Percent of all ID domains

14.9M
Number of all ID domains in current Q

12,546
Total number of domains reported on serverHold status

* Statistics for “cases opened” vs. “cases closed” can ordinarily differ in the same measurement period

** Cases often contain multiple domains in a single escalation

Our Expertise

Detection methods, training given to staff, use of automated decision making when creating abuse cases and suspending domains

Identity Digital Abuse Team members complete continuing professional education (CPE) at least once per month, focused on topics related to anti-abuse and cybersecurity. Monthly performance audits, conducted by subject matter experts, evaluate the quality of escalations and takedowns. These audits aim to identify areas for improvement and determine additional CPE opportunities to enhance staff performance. Additionally, all staff participate in annual or quarterly security training.

We continuously evaluate abuse submissions and automatically create a case if the available evidence meets threshold standards. A team of analysts then reviews these cases and manually escalates the reports for investigation.

Trusted Notifiers

Identity Digital considers reports made to it via a number of avenues; however, there is a small category of reporters we consider “Trusted Notifiers.”

In addition to the other sources of reports described in this report, Identity Digital works with a small category of reporters we consider “Trusted Notifiers.” Identity Digital maintains formal, contractual relationships with our Trusted Notifiers.

Although each Trusted Notifier relationship is subjective and unique, the formal arrangements establish accepted standards of due process, including evidential expectations, due diligence, and ensuring reports are made to the appropriate and proximate service providers, prior to the registry being asked to intervene.

For more information on Trusted Notifiers in general please see the Contracted Party House Trusted Notifier Framework.

If you would like to discuss a potential trusted notifier relationship with Identity Digital, please contact us at compliance@identity.digital.

Identity Digital currently maintains formal trusted notifier relationships with:

Internet Watch Foundation (IWF)

The IWF securely provides us with reports of URLs using Identity Digital domains, which have been verified and confirmed as being used to access Child Sexual Abuse Material.

Motion Picture Association (MPA)

Recording Industry Association of America (RIAA)

Identity Digital receives reports of domains associated with pervasive and patently apparent copyright infringement. All reports must come with clear evidence of this pervasive infringement, and all reports must have already been made to the more proximate and appropriate service providers, such that any consideration of the registry is appropriate at that time.

In this quarter, we actioned the following reports:

		IWF	MPA	RIAA
Unique Domains Affected		53	0	0
Domains Suspended	Registrar	13	0	0
	Registry	8	0	0
Remediated (confirmed by IWF or registrar)		31	0	0
Closed / Remediated Other		4	0	0

LEA Requests and Court Orders

Orders from Competent Jurisdictions**

This table details the requests received by Identity Digital from courts or other government agencies of competent jurisdictions. These requests usually ask Identity Digital to take specific actions, such as redirecting nameservers, transferring domains to different registrars, or suspending the subject domain names.

Report Category (abuse or illegal activity)	Country	Number of Requests	Number of Affected Domains	Number of Domains Suspended	Number of Domains Transferred
Court Order	USA	2	8	0	8

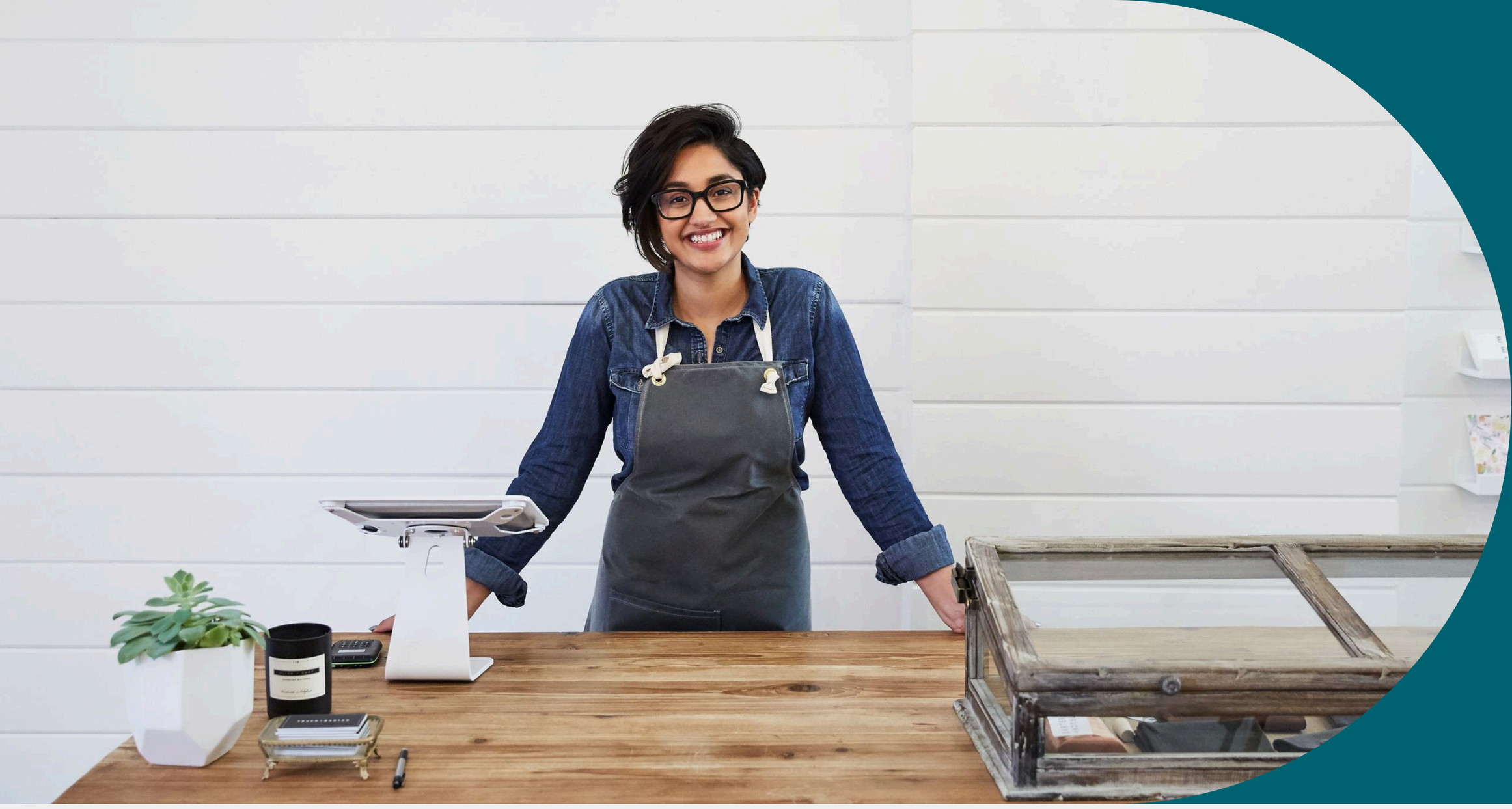
LEA Requests*

In addition to working with our Trusted Notifiers to combat abuse in our TLDs, Identity Digital collaborates directly with law enforcement authorities to help mitigate or eliminate online harms. These requests address reports of ongoing violations of registration terms such as our Acceptable Use Policy.

3	3	0	5
# of requests received	# of requests actioned	# of requests declined	# of affected domains

*This is taking down/transferring domains due to court orders

**This is requests to help mitigate DNS Abuse



.zone .travel .ride .plus .guru .cool .life .world .social

identity.digital | compliance@identity.digital

identity digital®