Anti-Abuse Report Q4 2025

This quarter, we examine bit-flipping (also known as bit-squatting), a lesser-known but documented vulnerability. While the mechanism may seem obscure, the threat is well-documented: the first comprehensive study on bit-squatting dates to 2011, and numerous cases have been observed since. Unlike traditional domain squatting techniques that exploit user error, bit-squatting targets machine-to-machine communication with a significant element of randomness, making it particularly challenging to detect and mitigate.

Bit-Squatting: When Hardware Failures Mislead Users

What is Bit-Squatting?

Bit-squatting exploits the fundamental building blocks of computing: binary digits, or bits. Every piece of digital information consists of strings of 0s and 1s, including domain names. For instance, identity.digital translates to binary as:

- 01101001 01100100 01100101 01101110 01110100 01101001 01110100 01111001 (identity)
- 00101110 (the dot)
- 01100100 01101001 01100111 01101001 01110100 01100001 01101100 (digital)

When a single bit flips from 0 to 1 (or vice versa), the resulting string produces a different domain name. For example, changing one bit in “identity” yields 01101000 01100100 01100101 01101110 01110100 01101001 01110100 01111001, which translates to “hdentity.” While users are unlikely to manually type “hdentity.digital,” such single-bit variations can occur through hardware failures and environmental factors.

Real-world examples demonstrate the prevalence of bit errors. In December 2024, cosmic radiation struck a flight computer, flipping a single bit and forcing an emergency landing. More commonly, router memory can become unstable during high temperatures, causing transient bit errors. A user might type “example.com,” but a faulty router could transmit “extmple.com” instead. If a malicious actor has registered “extmple.com” and hosts a convincing replica of the legitimate site, the user can be compromised without ever making a typing error or realizing the exploit has occurred.

Thought Leadership 1

Abuse Reporting Statistics 3

Action Timeline 4

Our Expertise.....5

Trusted Notifiers 6

LEA Requests and Court Orders 7

Beyond Theory: A Measurable Threat

An attack dependent on cosmic rays, temperature fluctuations, and hardware sensitivity might seem primarily theoretical. However, the scale of the internet transforms this low-probability event into something much more real. The proliferation of internet-connected devices, combined with billions of users and the difficulty of detecting bit-squatted domains, creates a much larger surface area vulnerable to exploitation.

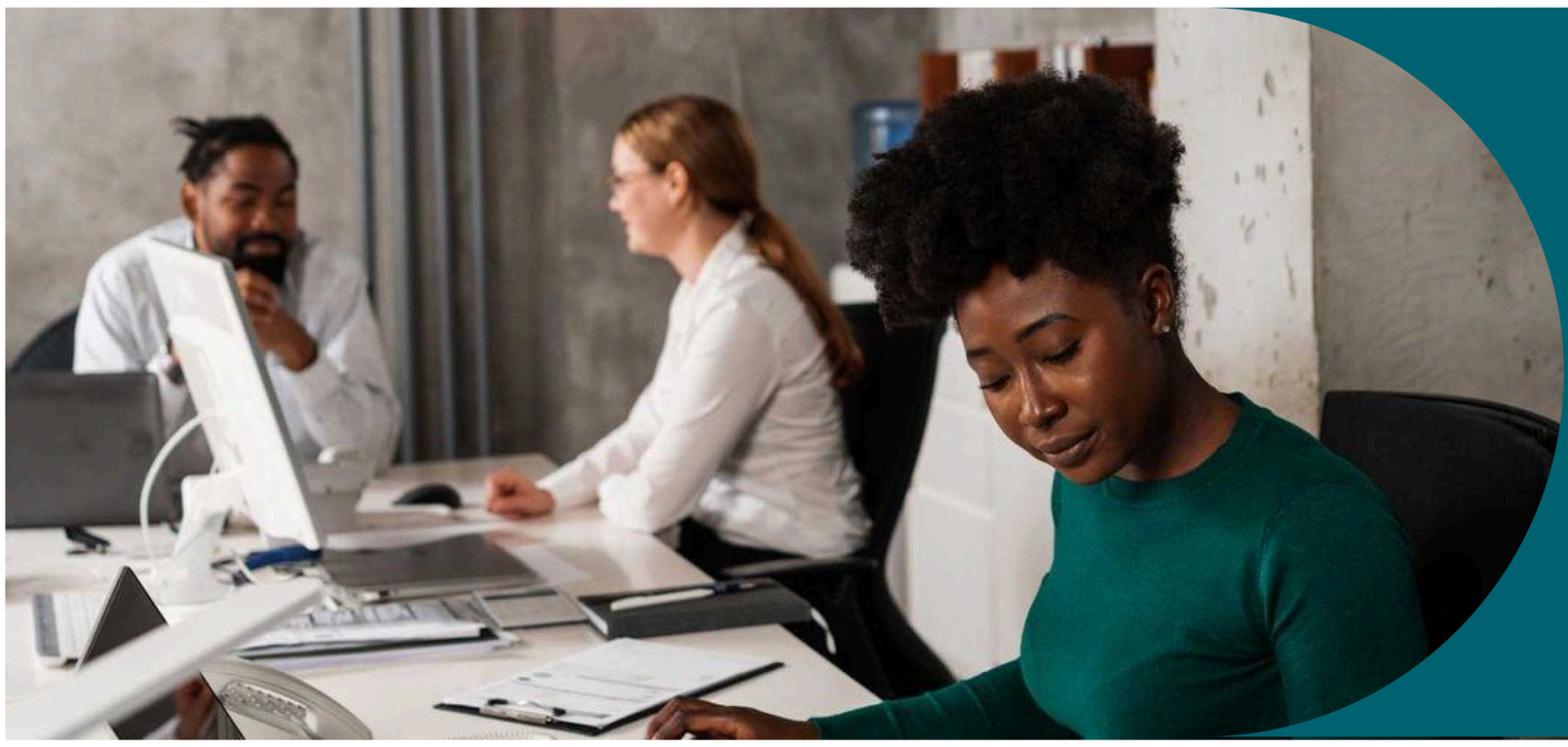
The threat escalates when targeting content delivery networks (CDNs), which serve high volumes of traffic and often use URLs not directly associated with the content owner's brand. For example, this newsletter is hosted at https://cdn.prod.website-files.com/644d37e47398154bd8f7a45e/68472eb869885f8818134954_anti-abuse-report-q1-2026.pdf. Any bit-squatting attack on "website-files.com" could potentially affect not only readers of this document but all clients using the same CDN infrastructure.

Protecting Against Bit-Squatting

Stay vigilant. If a webpage appears suspicious, despite the domain name looking correct, do not enter sensitive personal information. Reload the site or manually re-enter the URL.

Recognize the scope. While bit-squatting may appear rare and highly technical, research demonstrates it occurs in web application caches, DNS resolvers, and proxy servers. Standard security measures such as SSL certificates and TLS protocols are ineffective against this attack vector. One researcher documented 52,317 bit-squat requests from 12,949 unique IP addresses, with an average of 59 unique IPs per day making HTTP requests to 32 bit-squatted domains. Analysis confirmed these requests were not typos or manually entered URLs, and some exhibited multiple bit errors.

Consider defensive registration. Organizations should consider registering common bit-flip variations of their domains to prevent brand abuse. Unlike traditional typosquatting patterns based on predictable user errors, bit-squatting generates different character combinations. Online bit-flip generators can help identify potential threat vectors. Once identified, register these variations through your registrar before malicious actors can exploit them.



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.

85,852
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)	31,286 21,917 918 12,366	21,207	3,474	24.70%	66,487
Malware	Abuse List Report API Submissions Third Party Reports (email or abuse form) Manual Submissions	4,840 329 61 34	620	22	0.72%	5,264
Pharming	Any	0	0	0	0%	0
Botnets	Any	1,005	624	40	0.73%	1,005
Spam (as a delivery mechanism)	Spam Traps Third Party Reports (email or form)	0 64	58	1	0%	64
Denial-of-Service Attacks	Any	0	0	0	0%	0
Child Sexual Abuse Material	IWF Third Party Reports (email or form)	200 0	62	34	0.07%	200
Promotion, encouragement, sale, or distribution of prescription medication without a valid prescription in violation of applicable law	Third Party Reports (email or form)	710	185	36	0.22%	710
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	0	0	0	0%	0
Incitement to violence or other unlawful actions	Third Party Reports (email or form)	53	43	0	0.05%	53
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	415 62,900 426 2,943	63,842	566	74.36%	66,684

Action Timeline

0hrs

Registrar took action **PRIOR** to registry escalation	**559** cases	**541** domains
Registry took action **PRIOR** to registrar escalation (protective hold)	**1,663** cases	**1,884** domains

24hrs

Registrant or third party remediation (e.g. compromise fix, hosting etc.)	**228** cases	**158** domains
Registrar response provided reasonable explanation (no further action taken)	**772** cases	**1,515** domains
Registrar took action **POST** registry escalation	**759** cases	**1,337** domains

72hrs

Registry took action **POST** registrar escalation	**697** cases	**2,276** domains
Compromised / Platform (registry intervention deemed inappropriate)	**108** cases	**72** domains

4,830
Cases closed*

7,532
Unique domains affected (closed)**

1,884
Domains placed on protective holds (within 24 hrs of report)

0.05%
Percent of all ID domains

14.6M
Number of all ID domains in current Q

4,149
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		62	0	0
Domains Suspended	Registrar	7	0	0
	Registry	32	0	0
Remediated (confirmed by IWF or registrar)		18	0	0
Closed / Remediated Other		10	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	7	32	2	30

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.

1	1	0	2
# 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®