Interisle

Phishing Landscape 2025

A Study of the Scope and Distribution of Phishing

INTERISLE CONSULTING GROUP SEPTEMBER 2025

CONTENTS

EXECUTIVE SUMMARY

Phishing defrauds millions of Internet users every year.

Cybercrime continues to grow unabated around the world, breaking annual records for both incident numbers and economic damage. In 2024, the Federal Bureau of Investigation reported some $16.6 billion in direct financial losses from cybercrime in the U.S., a 33% rise over the previous year. At the global level, some projections estimate total losses in 2025 to reach a staggering $1.2–$1.5 trillion, factoring in both direct and indirect costs.

Phishing, the practice of using messages and fraudulent websites to pose as a trusted party in order to ensnare victims, is the most commonly use tactic to perpetrate these crimes. Phishers currently thrive in an environment where it is cheap and easy to acquire the Internet resources needed to conduct attacks—including domain names, subdomains, and hosting–with minimal risks and few deterrents.

This report is Interisle's fifth annual analysis of phishing attack data and the abuse of Internet resources that enable them. For this study we analyzed data from nearly 4 million phishing reports collected by respected threat providers between May 2024 to April 2025. We then used data from our previous studies to create year-over-year comparative measures and five-year analyses of key trends.

Each year we have witnessed significant growth in the annual number of attacks and shifts in the tactics criminals use to perpetrate them—and this year is no exception.

Our analysis shows that:

The total number of phishing attacks grew to nearly 2 million unique attacks worldwide, up by over 60,000 attacks compared to last year.

The number of unique domain names reported for phishing rose by 38% over last year, to over 1.5 million domains. This is the third year in a row that more than 1 million domains have been reported for phishing and the highest number since we began research five years ago.

The vast majority of domain names used in attacks were specifically acquired for criminal purposes. 77% of all domain names used for phishing were maliciously registered and the total number of malicious registrations increased by 36% over last year. Nearly nine out of ten domains reported in the new gTLDs were maliciously registered.

Subdomain abuse fell markedly as domain name abuse grew. The number of subdomains used in attacks fell by 44% off last year's record high.

Chinese phishers tapped preferred local suppliers to acquire resources for the Unpaid Toll Scam. Of the 37,000 Unpaid Toll Scam attacks we analyzed, 65% were registered at a single domain registrar, 49% in a single TLD, and 33% at a single hosting company – all located in China.

Over half of all phishing attacks reported worldwide were hosted with US-based companies. The United States has been the top hosting location for phishing attacks for five years in a row.

Phishers currently thrive in an environment where permissive policies and business practices make it cheap and easy for criminals to acquire the Internet resources needed for attacks with minimal risk and few deterrents.

Effective anti-abuse measures are urgently needed across the domain name, subdomain, and hosting ecosystems to curb criminal access to these resources. These should include proactive, front-end protections to prevent abuse before it occurs, as well as stronger, more efficient mitigation mechanisms where phishing is detected.

Our recommendations include:

Verify Customer Information – Research by Interisle and others has shown that stronger customer verification requirements correspond to lower rates of abuse. Industry should use address verification tools and screen for bogus and inaccurate registration data at the time of registration or sign-up.

Implement Requirements for Bulk Registration and High-Volume Account Creation – Phishers consistently exploit low-friction, high-volume access to Internet resources, including domain names and subdomains. Customers requiring high-volume services should undergo vetting and enhanced identity checks and limits should be placed on the number of registrations or accounts that can be created over short periods.

Proactively Identify and Act on Suspicious Abuse Patterns – Attackers often abuse resources in conspicuous patterns. Providers should monitor for and investigate suspicious behavior before registrations and accounts are activated. To improve mitigation, providers should also identify and suspend all related accounts and registrations tied to discovered phishers.

Implement Stronger Policy Goals and Require Corrective Action – ICANN policy should aim to measurably reduce malicious registrations, raise industry operating standards, and increase accountability for abuse. Providers with high abuse rates should be required to improve performance or face penalties, including possible deaccreditation.

Introduction

Cybercrime and phishing attacks continue to grow unabated around the world, setting new records in the number of reported incidents and associated economic losses.

According to the US Federal Bureau of Investigations (FBI), cybercrime inflicted over $16.6 billion in direct financial losses on US consumers and businesses alone in 2024 – a new high representing a 33% increase over 2023 – and more than $50.5 billion in direct losses over the last five years. At the global level, some experts project 2025 direct financial losses from cybercrime at $150 - $250 billion, with damages of a staggering $1.2 - $1.5 trillion when including indirect costs such as business downtime and broader economic impacts. Others, however, place the global impact at nearly 10 times these estimates.

According to the US Cybersecurity and Infrastructure Security Agency (CISA), more than 90% of successful cyberattacks begin with a phishing attack, making it one of the most pervasive, effective, and costly forms of cybercrime. Cybercriminals use phishing as a means to conduct consequent illegal and malicious activities, including theft, fraud, ransomware, malware, and distributed denial of service attacks (DDoS), and to steal sensitive corporate and national security information. As a gateway tactic of choice, phishing contributes substantially to the steep and growing global impact and losses inflicted by cybercrime.

This is Interisle's fifth annual Phishing Landscape report. For the past five years we have analyzed global incidents of phishing, how cybercriminals acquire key resources needed to conduct attacks (including domain names, subdomains, and hosting), and the top brands attackers exploit to build trust with victims. Each year we have

What is phishing?

A phishing attack is a perpetration of fraud that begins with an attempt to lure a party to a fake web site where a convincing impersonation of a merchant, brand, or product causes the party to submit or reveal personal data, a user account, or credit/financial information to the criminal attacker.

In most cases, the lure is a URL. A user who clicks on the URL is like a fish that takes the bait, not realizing that there's a barbed hook within. However, just as fishers adapt to water conditions by using hand lines, rods, or nets to fish, criminals are quick to adopt any delivery method(s) that promise to reach more potential victims.

Historically, the means of delivering the phishing lure to a user has been electronic mail. Today, delivery mechanisms include text or messaging apps (a.k.a., "smishing"), voice messaging ("vishing"), and social media posts, messaging, or comments. Phishers now also include QR codes in YouTube videos or posted notices.

Bottom line: phishers will do whatever it takes to put a malicious URL in front of the largest potential victim pool.

witnessed significant growth in the annual number of attacks and shifts in the tactics criminals use to perpetrate them – and this year is no exception.

For our 2025 report, we collected and analyzed nearly four million phishing reports from four widely respected data threat providers (Anti-Phishing Working Group (APWG), OpenPhish, PhishTank, and Spamhaus.) From this data we identified nearly two million distinct phishing attacks perpetrated during our study period of May 2024 to April 2025, up 3% from last year. 7.5 million unique attacks were launched over the past five years. Alarmingly, we found quarterly phishing attacks grew an astonishing 423% between our first measurements taken in 2020 and our most recent in 2025.

The Unpaid Toll Scam, which aims to defraud drivers by impersonating billing notices from US state tollway services, was among the most audacious attacks perpetrated by phishers this past year. Delivered through text message and conducted at massive scale through Chinese commercial Phishing-as-a-Service (PhaaS) providers, the attacks captured national attention and ensnared tens of thousands of victims in 2024 alone. Our report provides analysis and insight into how this scam is conducted and where these criminals are sourcing their attack resources.

Using the data from our previous annual studies, this year we also provide a 5-year overview of comparative results and measurements, including in the areas of across domain names, subdomains, and hosting resource abuse and the most frequently impersonated brands. Finally, based on our data and analysis, we provide recommendations on how resource abuse prevention and mitigation efforts can curb criminal exploitation and disrupt the growing scourge of phishing and impact of cybercrime.

Key Results

MEASUREMENT	MAY 2023 TO APRIL 2024	MAY 2024 TO APRIL 2025	% CHANGE
Total number of phishing attacks	1,897,952	1,963,390	+ 3%
Number of phishing attacks associated with malicious domain registrations	1,053,735	1,366,158	+ 30%
Unique domain names reported for phishing	1,117,670	1,542,922	+ 38%
Number of maliciously registered domain names reported for phishing	878,111	1,192,794	+ 36%
Top-level domains where phishing domains were reported	720	790	+ 10%
gTLD registrars with domains under management reported for phishing	1,951	2,033	+ 4%
All registrars with domains under management reported for phishing	3,047	3,125	+ 3%
Hosting networks where phishing web sites were reported	4,284	4,065	– 7%
Number of phishing attacks using a subdomain provider	454,948	256,026	– 44%

A *phishing attack* is a phishing site that targets a specific brand or entity. Our measure *Phishing Attacks* quantify the number of unique phishing sites used in attacks, and therefore the scope of phishing activity. In our research, the phishing attacks metric is the most important indicator of positive or negative change over time.

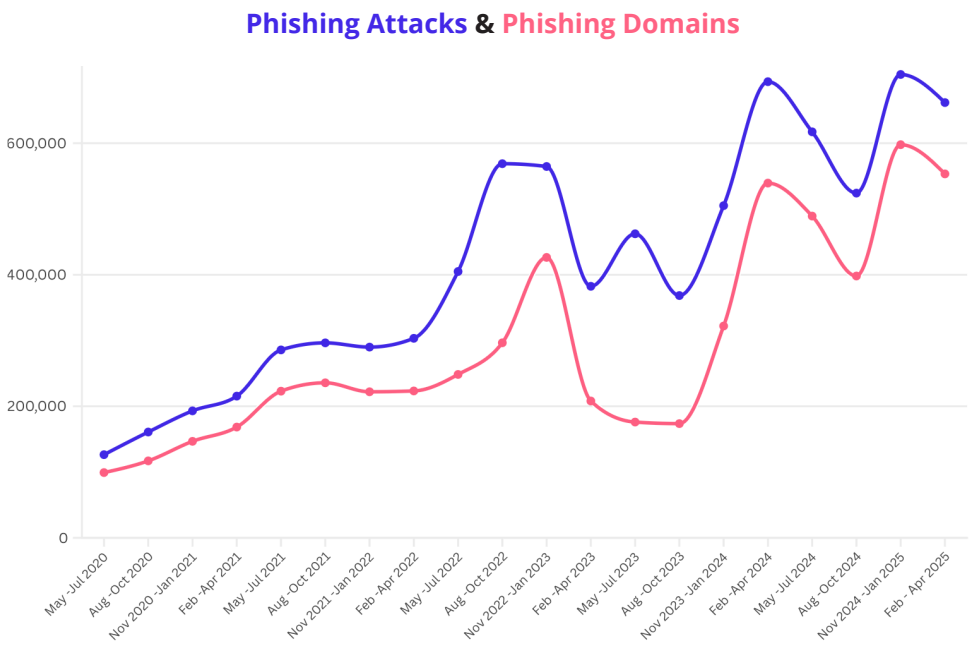
We observed an increase of 65,438 reported phishing attacks over the previous study period. This was a slightly larger increase than we observed in last year's report; which showed the lowest increase (47,560) since we began measuring phishing attacks in May 2020.

Many phishing attacks go undetected or are not included in our source data. Each threat intelligence provider only has a certain window of visibility into the problem, phishers use a variety of techniques to evade detection, and research indicates that adding new data sources always increases the number of detected phishing sites. Consequently, the total size of the phishing problem is almost certainly greater than our data indicates – our numbers indicate a *lower bound* of the overall phishing problem.

The number of phishing attacks, as well as the number of domain names used for phishing, continues to rise.

More than one million unique domain names were reported for phishing, for the third year in a row.

Domain names are essential resources for phishers. Users are accustomed to seeing domain names in URLs and suspicious should they see Internet addresses. Phishers often impersonate brands or companies by including near-



or exact matches to these names in their domain names or web site host names.

The notable drop in February 2023 shows the effect of the shutdown of ccTLD registry Freenom, which had been used by phishers to register large numbers of domain names. We observed significantly decreased phishing activity hosted at subdomain providers (*e.g.,* free website operators). We examine this later, in the section *"Subdomain Providers"*.

We saw a marked increase in the number of phishing domains that we were able to classify as maliciously registered compared to our previous report. We saw an even larger increase (38%) in the total number of phishing domains compared to our previous report.

Nearly 37% of the domains used for phishing in our study data were registered in bulk.

This is up from 27% in our previous report. Cybercriminals sometimes register and use hundreds to thousands of registered domain names at a time. These registrations are conspicuous and indicate that criminals are able to obtain large numbers of domain names at will.

We examine this later, in the section *"Bulk Registrations"*.

One major subdomain provider had a significantly reduced number of phishing attacks, but other important subdomain providers hosted increasing numbers of attacks.

Subdomain providers offer services to users on a domain name that the provider owns. Users receive their own DNS space, using a third level domain of the form: *subdomain.domainname.tld*. **Thirteen percent of all reported phishing attacks took place using resources at subdomain providers.** These phishing attacks are often difficult to mitigate and pose persistent problems for phishing targets.

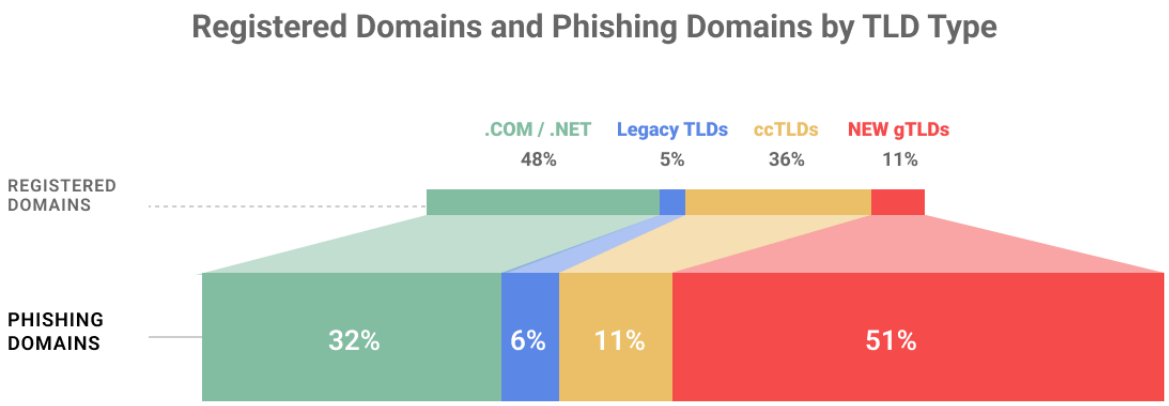
The statistics that we present in this report include both absolute metrics (*e.g.,* the number of domain names registered in a particular TLD that appear on a blocklist) and relative metrics (*e.g.,* a phishing score, representing the number of those domain names as a proportion of the total number of domains registered in that TLD).

The number of *maliciously registered domain names* is based on our determination that a domain name was purposely registered by a phisher to perpetrate a phishing attack.

Domains reported for phishing increased by 38% year-over-year.

To obtain yearly measurements for TLDs or gTLD registrars, we performed a de-duplication of domain names and URLs that appeared in more than one quarter. For more information about how we process phishing reported through our feeds, see the Terminology and FAQ pages at the Cybercrime Information Center.

37% of phishing domains were registered in bulk.



Top Level Domains

For our study, we divided the overall domain name space into four market segments:

- .COM and .NET
- Country-code domains (ccTLDs)
- Legacy gTLDs: those gTLDs other than .COM and .NET that were delegated before 2013 (*e.g.,* ORG, .BIZ, .INFO. ASIA)
- new gTLDs, delegated from 2014 to the present (*e.g.,* .XIN, .BOND, .CYOU, .TOP)

According to DomainTools, at the end of April 2024, there were over 360 million registered domains in all TLDs. We observed phishing in 790 of the nearly 1600 existing TLDs during the current study period. A comparison of the market share against phishing domains reported in each market segment is insightful:

New gTLDs now represent 11% of the market and 51% of phishing domains reported. This is a dramatic change from 2021 when the new gTLDs represented 9% of the market and 21% of phishing domains reported. The new gTLD market segment includes gTLDs with unrestricted registration policies (open to anyone) and *community gTLDs* that restrict registration eligibility to certain types of entities or users. Nearly all phishing-related DNS abuse is concentrated in new gTLDs with unrestricted registration policies. We examine the effects that registration policies have in mitigating phishing in the section *"Domain Registration Policies Matter"*.

The market share of .COM/.NET decreased slightly in 2025, but phishing domains reported in COM and NET decreased more significantly from 37% to 32% compared to last year and has significantly declined from the 54% we reported in our 2020 study.

Market share and percentage of phishing domains reported in the legacy gTLDs were relatively unchanged from our 2024 study.

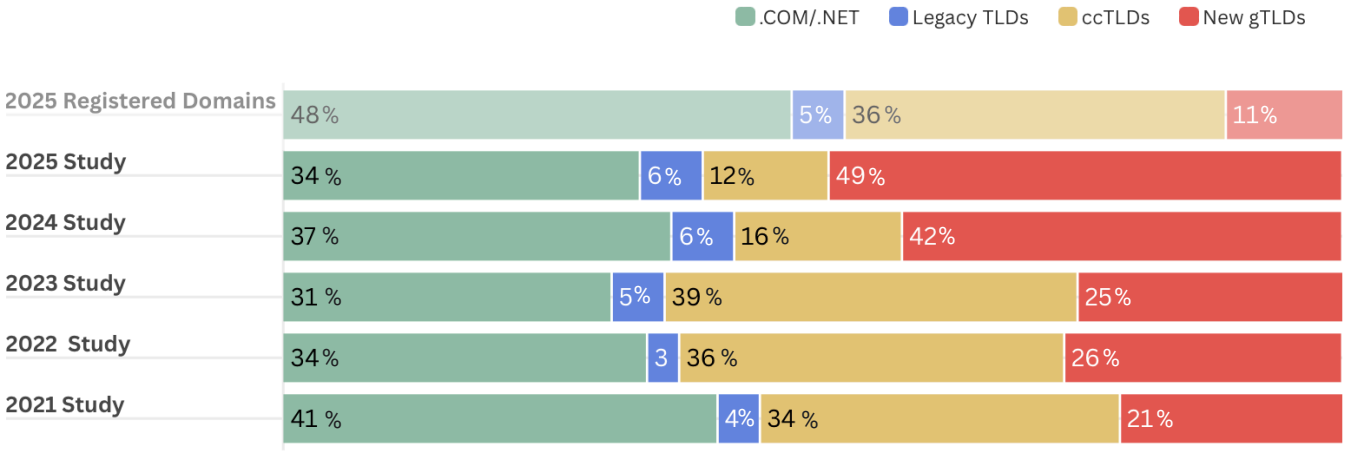
Phishing domains reported in ccTLDs decreased significantly, from 15% in our 2024 study to 11% this year. ccTLDs have a significant market share but little phishing compared to other market segments. The ccTLDs market share essentially held steady and the ccTLDs now have the lowest percentage of phishing domains reported by market segment.

The ccTLDs market segment had the lowest combined phishing attack and combined phishing domain scores:

COMBINED PHISHING SCORES	CCTLD SCORES	.COM/.NET SCORES	LEGACY GTLDS SCORES	NEW GTLDS SCORES
Phishing Attack Score	**23.9**	36.3	58.0	**244.9**
Phishing Domain Score	**14.0**	29.2	50.5	**203.6**

In our 2024 Cybercrime Supply Chain study, we determined that verification requirements on domain registrations correlate with lower cybercrime and malicious

Proportion of Phishing Domains by Namespace Segment



registrations. In the section *"Domain Registration Policies Matter"*, we repeat our analysis of registration policies looking at phishing domains only.

Ranking of TLDs by Phishing Domains Reported

The complete Top 20 TLD rankings for this yearly study period are posted at the Cybercrime Information Center. In that ranking:

- The most exploited TLD, .COM, is also the largest TLD, with 155M domains under management and 455,297 phishing domains reported.
- Together, the gTLDs that rank #2 to #7 – .TOP, .BOND, .XYZ, .SHOP, .INFO, and .XIN – have *more* phishing domains reported (478,449) but the combined domains under management of these gTLDs is a small fraction of .COM's (15.4M of 154M, or 10%).
- Only three ccTLDs appear in the top 20: .CN, .CC, and .RU
- We observed a 524% increase in .BOND, where nearly all the registrations were processed by a single registrar, Key-Systems (IANA ID 1345).
- All but one of the top 20 TLDs (.CN) offered registrations to any individual or legal entity, irrespective of their nationality, place of residence, organization or entity type, or area of operations.
- Previously unranked .XIN, had 42,724 phishing domains reported in 2025 (and only 9 in 2024). Nearly all of these were registered at Dominet (HK) (IANA ID 3775).

The top five TLDs ranked by phishing domains reported appear in the table below:

2025 RANK	TLD	REGISTRY OPERATOR	2025 DOMAINS IN TLD	PHISHING DOMAINS REPORTED
1	.COM	Verisign	154,712K	**455,297**
2	.TOP	Jiangsu Bangning	3,525K	**187,749**
3	.BOND	ShortDot	454K	**79,875**
4	.XYZ	XYZ.COM	4,220K	**73,509**
5	.SHOP	GMO Registry	3,322K	**50,052**

A five-year comparison of TLDs shows that:

- .COM, the largest TLD, had the highest number of phishing domains reported each year.
- Three commercialized ccTLDs – .TK, .GA, and .ML – were prominent among the top five TLDs until their operator Freenom was sued and the registries stopped processing domains registrations.
- The TLDs .XYZ and .CN have had historically high rankings.

5–YEAR COMPARISON OF TLDS WITH HIGHEST NUMBER OF PHISHING DOMAINS REPORTED				
2021 Study	**2022 Study**	**2023 Study**	**2024 Study**	**2025 Study**
1 .COM	**1 .COM**	**1 .COM**	**1 .COM**	**1 .COM**
2 .TK	2 .CN	2 .CN	**2 .TOP**	**2 .TOP**
3 .XYZ	**3 .SHOP**	3 .ML	**3 .XYZ**	**3 .BOND**
4 .ML	**4 .XYZ**	**4 .TOP**	4 .CN	**4 .XYZ**
5 .GA	5 .TK	5 .TK	5 .INFO	**5 .SHOP**

Ranking of TLDs by Score

Raw counts can be deceiving. For example, a study that only compares the number of crimes committed in New York City to the number committed in Albany, NY doesn't consider that the population of Albany is barely 100,000 and New York City has nearly 8.5 million people. A study that uses a *per capita* comparison would show that the total crime rate in Albany is 165% higher than New York City. The number of crimes *is* important, but it is not sufficient to conclude that one city is mitigating crime better than others.

Similarly, if we only compare and rank TLDs by the number of phishing domains reported, very large TLDs like .COM and .CN will invariably be victims of a numbers bias. It's important to consider the size of TLDs as a factor as well.

To compare phishing incidences in a set of TLDs with varying sizes, we use a Phishing Score which is the number of phishing domains reported per 10,000 domains in a TLD. Like a *per capita* comparison, phishing score compares whether a TLD has a higher or lower incidence of phishing relative to other TLDs of varying sizes.

The TLDs with the highest rates of phishing were:

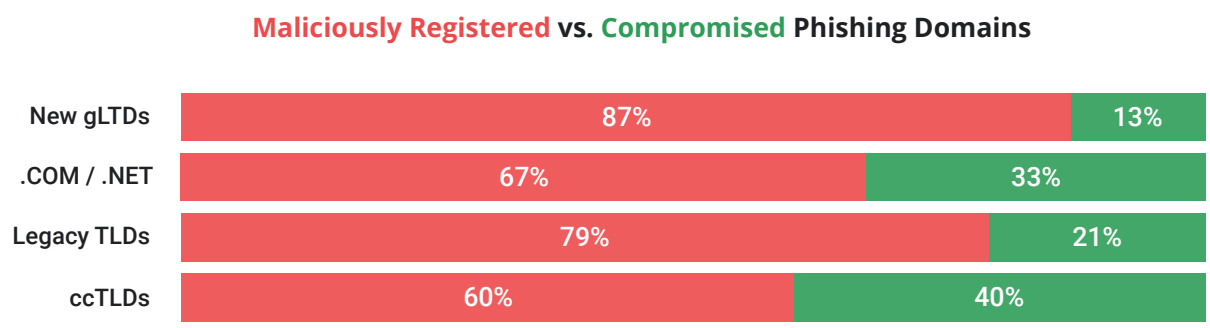
2025 RANK	TLD	2025 DOMAINS IN TLD	PHISHING DOMAIN SCORE
1	.XIN	40K	**10,810.2**
2	.BOND	454K	**1,759.0**
3	.HELP	44K	**1,077.7**
4	.WIN	83K	**796.1**
5	.CFD	324K	**747.8**

The top five TLDs in this study period all had higher phishing scores than any TLD in our 2024 study. The most exploited TLD, .XIN, had the highest phishing score (10,810.2) we have ever reported. Domain names used in Unpaid Toll Scam phishing campaigns account for most of the abuse in .XIN. Nearly all of these .XIN phishing domains were registered at Dominet (HK) (IANA ID 3775).To put these scores into perspective, **the phishing scores of the Top 5 TLDs range from 25 to 365 *times* that of COM's phishing score of 29.6.**

A 5-year ranking of the TLDs with the highest phishing domain scores reported appears below:

5–YEAR COMPARISON OF TLDS WITH HIGHEST PHISHING DOMAINS REPORTED				
2021 Study	**2022 Study**	**2023 Study**	**2024 Study**	**2025 Study**
1 .CYOU	1 .SUPPORT	1 .REST	1 .LOL	**1 .XIN**
2 .BAR	2 .BAR	2 .LIVE	**2 .BOND**	**2 .BOND**
3 .BEST	3 .SHOP	3 .SUPPORT	3 .SUPPORT	**3 .HELP**
4 .CASA	4 .WORK	4 .ML	4 .TOP	**4 .WIN**
5 .BUZZ	5 .LIVE	5 .CYOU	5 .SBS	**5 .CFD**

Forty-nine TLDs appeared in the Top 20 phishing domain scores over the 5-year period. Forty-two of these were new gTLDs, of which seven were operated by Binky Moon (including .FINANCE, .SUPPORT, .FYI, .DIGITAL, .ZONE) and seven by XYZ.COM (including .XYZ, .LOL, .MONSTER, and .PICS).



Domain names in TLDs with high scores represent a high risk for users and organizations. A person is more likely to encounter a dangerous domain when they click on a hyperlink in an email message or visit a web site address that contains a domain name registered in a TLD with a high yearly phishing score.

High scores represent a liability for registry operators. High yearly phishing domain scores erode the reputation of a TLD. Legitimate registrants have learned to avoid TLDs that have poor reputations and risk-averse organizations have resorted to blocklisting entire TLDs.

Phishing registration activity in TLDs over time

Over a five-year period, 36 TLDs appeared at least once in the Top 20 for most phishing domains reported and 49 TLDs appeared in the Top 20 for highest phishing domain scores.

Ten TLDs – .SHOP, .ONLINE, .XYZ, .CN, .ORG, .RU, .TOP, .COM, .NET, and .INFO – have appeared in the Top 20 for phishing domains reported in each of our five studies and three – .BEST, .TOP, and .BUZZ – appeared in the Top 20 for highest phishing domain scores.

We again note that, except for .CN, these TLDs offer registrations to any individual or legal entity, irrespective of their nationality, place of residence, or area of operations.

Malicious Domain Registrations Across the Domain Name Space

For our studies, we call a phishing domain purposely registered to carry out a criminal act a *malicious domain registration*. We categorize domains as malicious registrations based on methodology that is published at the Cybercrime Information Center.

During our 2025 reporting period,

- 77% of domain names reported for phishing were maliciously registered.
- Nearly 9 of 10 phishing domains reported in the new gTLDs were maliciously registered.
- .COM/.NET and the ccTLD market segments have the lowest percentages of maliciously registered domains. This is likely associated with their long-established market presence and a higher percentage of legitimate, annually renewed, registrations.

The top five TLDs with the highest proportion of malicious registrations were new gTLDs and had malicious registration rates of 96% or higher:

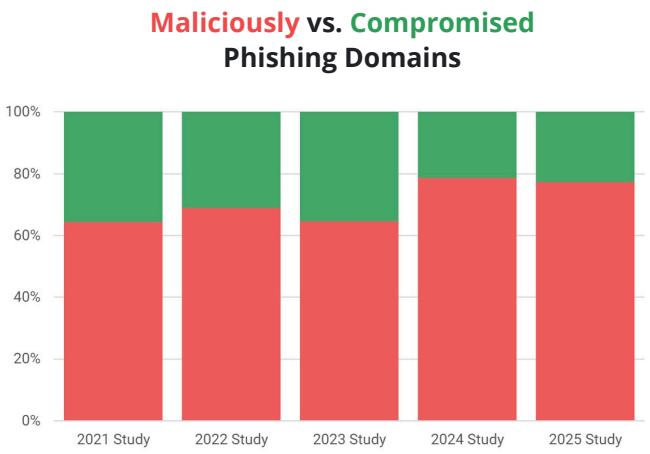
2025 RANK	GTLD	PHISHING DOMAINS	MALICIOUS PHISHING DOMAIN REGISTRATIONS	% PHISHING DOMAINS MALICIOUSLY REGISTERED
1	.XIN	42,724	42,681	100%
2	.BOND	79,875	79,690	100%
3	.CFD	24,241	23,219	96%
4	.TODAY	14,440	13,831	96%
5	.LOL	24,187	23,122	96%

The top five ccTLDs with the highest proportion of malicious registrations represented a mix of business models and geographies.

2025 RANK	CCTLD	PHISHING DOMAINS	MALICIOUS PHISHING DOMAIN REGISTRATIONS	% PHISHING DOMAINS MALICIOUSLY REGISTERED
1	**.CC**	24,550	22,252	**91%**
2	**.RU**	31,312	25,682	**82%**
3	**.US**	8,067	5,972	**74%**
4	**.CO**	6,996	5,070	**72%**
5	**.DE**	9,065	6,169	**68%**

In total, 80 TLDs were determined to have a 75% or high percentage of malicious phishing domain registrations. This included 74 new gTLDs, 2 legacy TLDs and 4 ccTLDs

Over time we have seen the percentage of maliciously registered phishing domains increase, as depicted here:



While the yearly percentage of malicious domains over all TLDs (ccTLDs and all gTLDs) ranges from 64% to 79%, we note that for the new gTLDs, this range is 87% to 93%.

A 5-year ranking of the TLDs with the most malicious phishing domains reported:

A 5-YEAR RANKING OF THE TLDS WITH THE MOST MALICIOUS PHISHING DOMAINS REPORTED:				
2021 Study	**2022 Study**	**2023 Study**	**2024 Study**	**2025 Study**
1 .COM	**1 .COM**	**1 .COM**	**1 .COM**	**1 .COM**
2 .TK	2 .SHOP	2 .ML	**2 .TOP**	**2 .TOP**
3 .ML	3 .TK	**3 .TOP**	**3 .XYZ**	**3 .BOND**
4 .GA	**4 .XYZ**	4 .CN	4 .SHOP	**4 .XYZ**
5 .XYZ	5 .ML	5 .LIVE	5 .INFO	**5 .XIN**

Thirty-seven TLDs appeared in the Top 20 malicious phishing domains over the 5-year period. Of these twenty-four were new gTLDs, four were legacy TLDs, and nine were ccTLDs.

Of the twenty-four new gTLDs, five were operated by ShortDot – .ICU, .BOND, .CFD, .SBS, and .CYOU – and three by Registry Services – .CLUB, .VIP, and .WORK.

Of the nine ccTLDs, five were the Freenom commercialized ccTLDs – .CF, .GA, .GQ, .ML, and .TK.

Five TLDs, all of them new gTLDs, were in the Top 20 for phishing domains and have at least 80% of those TLDs' domains maliciously registered for more than two of the five years:

- .INFO – four of the five years
- .TOP – four of the five years
- .LIVE – four of the five years
- .SHOP – three of the five years
- .XYZ – three of the five years

Domain Registration Policies Matter

Many ccTLDs require proof of identity to register domains. For example, individuals (natural persons) may be asked to provide a state personal identification number or passport to prove residency, citizenship, or real connection to the country. Businesses may be asked to provide a commercial registration, proof of presence in the country, or a VAT number.

To determine whether such registration requirements affect malicious domain registration levels, we studied two sample sets of ccTLDs – 25 countries in the European Union, and 25 in the Asia-Pacific region for which we had phishing data – to investigate whether there is a correlation between conditions imposed upon domain registrations and low phishing numbers or scores.

For each ccTLD, we collected the registration requirements for these from the country's network information centers (NICs) and domain registrars authorized to process registrations for the country.

We grouped the EU ccTLD and Asia ccTLD sets into three registration requirements categories. The composite scores for thewse sets appear in two tables:

REGISTRATION REQUIREMENTS IN EU CCTLD SET	COMPOSITE PHISHING DOMAIN SCORE OF CCTLDS IN CATEGORY	COMPOSITE MALICIOUS PHISHING DOMAIN SCORE OF CCTLDS IN CATEGORY
NONE Any individual or legal entity, irrespective of their nationality, place of residence, area of operations	4.5	2.9
OPEN with requirements Any individual or legal entity, irrespective of their nationality, place of residence, area of operations BUT subject to some form of identity verification	4.6	2.9
RESTRICTED, strict requirements Proof of residency or business presence in country or EU	4.5	1.9
COMPOSITE SCORE	4.5	2.6

REGISTRATION REQUIREMENTS IN ASIA CCTLD SET	COMPOSITE PHISHING DOMAIN SCORE OF CCTLDS IN CATEGORY	COMPOSITE MALICIOUS PHISHING DOMAIN SCORE OF CCTLDS IN CATEGORY
NONE Any individual or legal entity, irrespective of their nationality, place of residence, area of operations	31.4	19.6
OPEN with requirements Any individual or legal entity, irrespective of their nationality, place of residence, area of operations BUT subject to some form of identity verification	29.5	10.6
RESTRICTED, strict requirements Proof of residency or business presence in country.	2.8	0.8
COMPOSITE SCORE	25.2	10.2

We used ICANN Registry Agreements list to find new gTLDs that restrict registration eligibility to certain types of entities or users. This set includes gTLDs that subject registrants to some form of identity verification (Open, with requirements) and those that impose strict requirements.

COMMUNITY GTLDS	COMPOSITE PHISHING DOMAIN SCORE	COMPOSITE MALICIOUS PHISHING DOMAIN SCORE
City and Regional gTLDs* **.BARCELONA, .BERLIN, .BZH, .CAT, .CORSICA, .EUS, .GAL, .HAMBURG, .MADRID, .OSAKA, .PARIS, .QUEBEC, .RIO, .SCOT, .SWISS, .TIROL, .WEIN** *Only 12 of 17 had domains reported for phishing	1.9	0.5
Professional gTLDs* **.ARCHI, .ECO, .MUSIC, RADIO, .SPA, .SPORT** *Only 3 of 6 had domains reported for phishing	4.1	3.1
High Security gTLDs* **.BANK, .INSURANCE, .NGO, .ONG. PHARMACY, .REIT, .VERSICHERUNG** *Only 2 of 7 had domains reported for phishing	5.2	3.0

To this set we added 10 legacy gTLDs: .INFO, .PRO, .ASIA, .COM, .NET, .TEL, .ORG, .BIZ, .NAME and .MOBI. We then added the 25 new gTLDs with the highest phishing domain scores in our 2025 data.

Combined, these gTLDs provide a basis for comparison against the EU and Asia ccTLD sets.

GTLD CATEGORY	COMPOSITE PHISHING DOMAIN SCORE	COMPOSITE MALICIOUS PHISHING DOMAIN SCORE
Legacy gTLDs (10)	31.2	21.6
New gTLDs (25)	320.5	285.2
Community gTLDs (30)	2.2	0.9
Composite score (65)	52.0	40.6

When we compared the scores for the EU, Asia and gTLD sets we observed that:

- The EU ccTLDs have the lowest composite phishing domain scores relative to the Asia and gTLD sets.
- Strict registration requirements appear to reduce malicious phishing domain scores across all sets. The Asia ccTLDs and ICANN community gTLDs (particularly, the city and regional community gTLDs) have the lowest malicious phishing domain scores.
- The gTLD set had the highest composite phishing domain score and malicious phishing domain score.
- The phishing scores for Asia ccTLDs that were open with registration requirements are biased by .CN and .ID. The phishing scores of .CN and .ID may be due to a difference between their stated registration policy and how those policies are implemented in practice.
- TLDs with no registration restrictions had the highest scores irrespective of set.

Overall, we conclude that requirements of some form or another are effective in deterring malicious registrations. This is particularly the case for EU and Asia ccTLDs but community gTLDs with registration requirements based on the geography, type, or affiliation of a user or entity are successful in mitigating phishing or otherwise have policies that make them less attractive to phishers. However, we note cases where some requirements or strict policies did not reduce abuse of domains for phishing as one would expect. From this, we conclude that policies matter, but they must be enforced.

Phishers Like Cheap

Our data from May 2020 to April 2025 show that cheap domains are attractive to phishers.

We used comparative pricing data published by TLD-list.com and complemented these data with fees published by ccTLD registries that process registrations directly. We used the Cheapest Price History chart from TLD-list.com for each TLD to confirm that the fees have been offered frequently during our yearly study period.

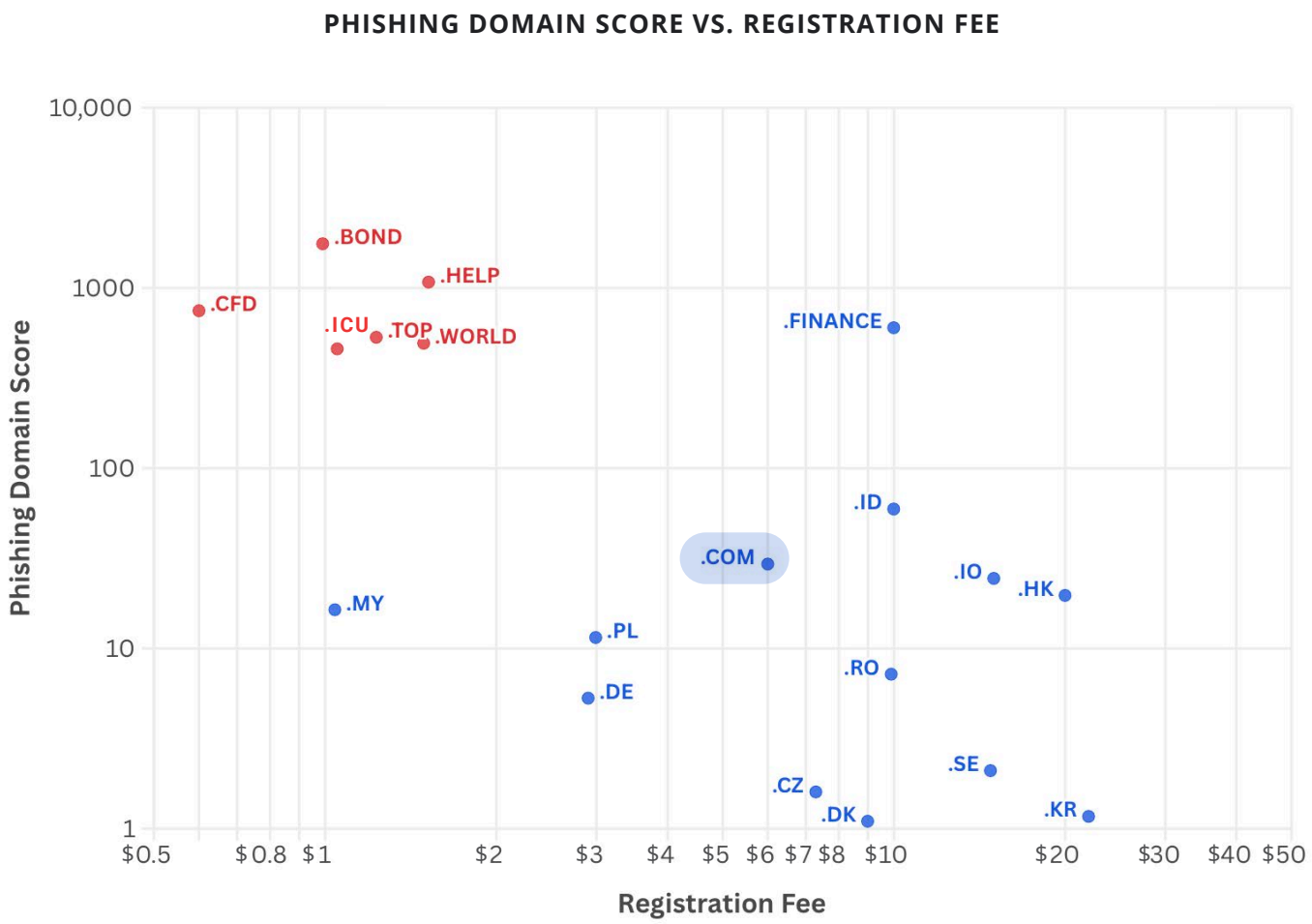
Comparing our TLD sets, we observe that:

ccTLD registration fees are generally higher than those of gTLDs. Only four ccTLDs (.NP, .MY, .CN, .IN) offered registrations for US$6 or less. 18 new gTLDs in our set offered (non-promotional) registrations for under US$2, and 24 of the 25 in our set offered registrations for under US$6.

Registration fees in the EU ccTLD set had little influence on phishing scores. All the TLDs in the EU ccTLD set had low scores relative to the other sets. The highest phishing score in this set was 11.5.

TLDs in the new gTLD set with very low registration fees generally attract phishing. The new TLDs in our study set all offered registrations for under US$10. The lowest phishing score in this set was 236.5, more than twenty times the *highest* phishing scores in the EU ccTLD set. The new gTLDs that offered registrations below US$2 generally had the highest phishing scores.

A scatter plot of the three TLD sets shows that, generally, TLDs with the low registration fees have high phishing scores:



Subdomain Providers

Our analysis reveals that **13% of all reported phishing attacks took place using resources at subdomain providers.** These phishing attacks are difficult to mitigate and pose persistent problems for phishing targets. **While one major provider had a significantly reduced number of phishing attacks mounted on its services, other important subdomain providers hosted increasing numbers of attacks.** Subdomain service providers must have preventative, proactive ways to prevent the mass exploitation of their services, and to provide quick anti-abuse monitoring and takedown capabilities.

Subdomain providers give customers services on a domain name that the provider owns. This gives users their own DNS space, using a hostname of the format:

subdomain.domainname.tld

Some of these providers offer website building or hosting services. Others offer free DNS management so the customer can point the hostname to other hosting. Phishers use the services to build and maintain phishing sites.

These phishing attacks pose persistent problems because:

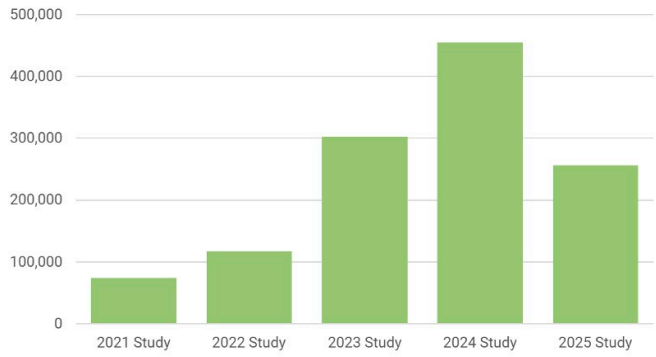
- Most of these services offer free accounts, which attracts phishers.
- Subdomain service providers often do not deploy effective, proactive measures to keep criminals from creating accounts and abusing their services. For example, they often lack effective account or identity validation procedures at sign-up.
- Only the subdomain service providers can effectively mitigate these phishing attacks. Most lack highly responsive abuse mitigation, which is a cost to the provider.
- As a result, phishers can abuse these services repeatedly and at scale.

Some of these providers have chosen this abuse situation. They wish to attract usage, and to provide low barriers and user-friendly features to customers. Abuse is an unfortunate, inevitable side-effect of their business plans.

Some phishing kits — software used by phishers to launch and manage their phishing sites — integrate the use of subdomain providers, allowing the phishers to sign up for and use subdomains in an automated fashion. This allows the phishers to launch large numbers of attacks, and to abuse these services repeatedly and at scale.

In the latest study period, **there were 256,026 phishing attacks created on 701 second-level domains operated by subdomain providers**. The number of such attacks reported by our sources was down notably over the last year – there were 454,947 attacks reported in our 2024 study, which was 24% of all phishing attacks.

Phishing Attacks Using Subdomain Providers



The decrease was due almost entirely to a drop in reports about phishing on Google's services — notably its Blogger service, which provides third-level domains on *blogspot.com* and *blogspot.cctld* domains.

89% of the subdomain-provider attacks occurred on domains operated by just ten providers, which shows how the choices made by a few companies can affect the phishing landscape.

The top ten providers were:

2025 RANK	PROVIDER	DOMAINS	2024 PHISHING ATTACKS	2025 PHISHING ATTACKS	% CHANGE
1	Cloudflare	pages.dev, workers.dev, trycloudflare.com, r2.dev	10,057	**43,857**	**+ 157%**
2	Webflow	webflow.io	3,067	**33,418**	**+ 980%**
3	Google	blogspot.com and blogspot.xx on 66 ccTLDs. web.app, firebaseapp.com, page.link, googleapis.com, appspot.com, doubleclick.net, cloudfunctions.net	258,347	**30,703**	**– 88%**
4	Weebly	weeblysite.com, weebly.com	24,736	**29,934**	**+ 21%**
5	GitBook	gitbook.io	n/a	**21,981**	**+**
6	Vercel	vercel.app	5,663	**21,442**	**+279%**
7	Github (Microsoft)	github.io	11,485	**20,211**	**+76%**
8	Duck DNS	duckdns.org	60,913	**9,653**	**–84%**
9	CentralNIC	ru.com, sa.com, za.com, com.de, us.com, eu.com, uk.com, cn.com, jp.com, de.com, gb.net, ae.org, uk.net, jpn.com, br.com	12,563	**6,243**	**–50%**
10	Glitch	glitch.me	4,903	**4,707**	**–4%**

#2 Webflow is a newcomer to our rankings. Webflow offers a software-as-a-service (SaaS) platform that allows users to design, build, and launch websites without coding. Like many website-building platforms, Webflow offers free sub-domains and hosting, on which its customers can place their sites.

#5 Gitbook is another newcomer to our rankings. Gitbook is a documentation platform, and started providing free and paid-plan subdomains on gitbook.io to its customers in 2024. Gitbook is not related to Github, which is #7 on our list. Github is a Microsoft subsidiary, a code repository and developer platform that offers free subdomains and project hosting on GITHUB.IO.

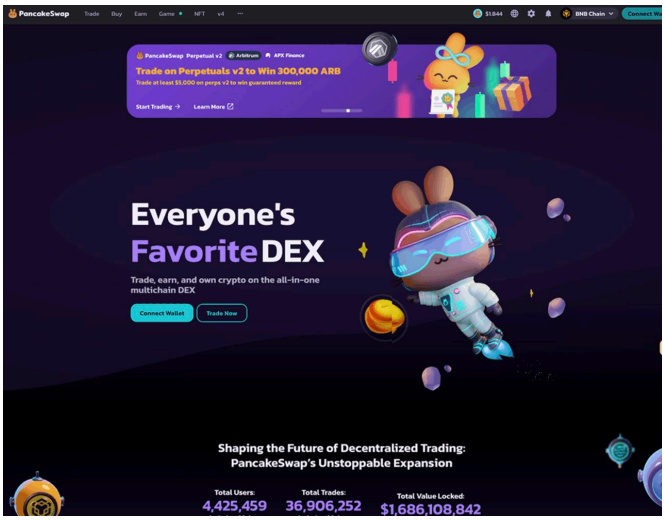
5-YEAR RANKING OF SUBDOMAIN PROVIDERS MOST PHISHING REPORTED:				
2021 Study	**2022 Study**	**2023 Study**	**2024 Study**	**2025 Study**
1. Google	**1. Google**	1. DuckDNS	**1. Google**	**1. Cloudflare**
2. Hostinger	2. DuckDNS	**2. Google**	2. DuckDNS	**2. Webflow**
3. Weebly	**3. Weebly**	3. Hostinger	**3. Weebly**	**3. Google**
4. DynDNS	4. Hostinger	**4. Weebly**	4. CentralNIC	**4. Weebly**
5. ChangeIP	5. no-ip.com	5. Replit	5. Hostinger	**5. GitBook**

Case Study: Vercel

Cloud application company Vercel saw a 279% increase in the abuse of its free subdomain service, and hosted more than 21,000 phishing attacks on its services over the year. Vercel offers developer tools and cloud infrastructure. When a customer signs up for a free account and begins a project, Vercel automatically assigns it a subdomain on vercel.app based on the user's project name. This is an attractive feature for phishers, who can choose phishing-friendly project names and get corresponding subdomains and free hosting.

For example, phishers obtained hundreds of subdomains to attack users of the cryptocurrency exchange PancakeSwap, creating subdomains such as

https://pancake-swapv2.vercel[.]app/
https://pancakeswapclaim6754[.] vercel[.]app/
https://v3-pancakeswap.vercel[.]app



Above: phishing attack hosted at https://v3-pancakeswap[.]vercel[.]app, December 20, 2024

Phishers also used Vercel's service to attack companies such as Facebook, on subdomains including:

https://**violation-policy-meta-ticket-id6398549**.vercel[.]app/

and they created subdomains with misleading security terms, such as:

https://**challenge-captcha-ten-10**.vercel[.]app

Phishing from Outer Space: The InterPlanetary File System

Phishing using the InterPlanetary File System (IPFS) exploded in 2023-2024, when we found it was used to host 19,387 phishing sites, up from 1,475 attacks in 2022-2023. In our 2024-2025 data, only 7,898 phishing attacks using IPFS were reported — a decrease of 60%.

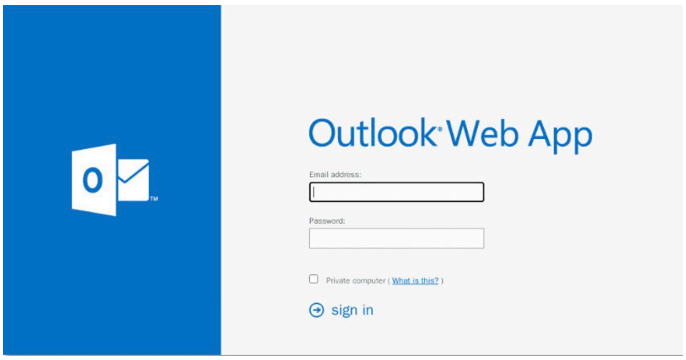
The InterPlanetary File System (IPFS) is a decentralized data storage and delivery network based on peer-to-peer (P2P) networking. It's an example of "Web3" technologies, which are generally based on the concept of decentralization and often incorporate blockchain technology. Instead of having a central server that holds and distributes a Web site or data file, IPFS is a decentralized system of user-operators who hold copies of data. Any user in the network can serve a file by its content address, and other peers in the network can find and request that content from any node that has it.

Major web browsers do not currently support the IPFS protocol, so providers operate "gateways" to help people access IPFS content. A gateway is an IPFS peer that accepts HTTP requests for IPFS content IDs, allowing users to use their default browsers to access the IPFS content on a standard domain name.

An example of one of these IPFS content IDs represented as a URL is:

http://bafkreial7xm2noknyl6vrni7v7wr2ij7p7t2f3qknuhsvsytjekcf7jwq4.ipfs.flk-ipfs[.]xyz

That URL was created on Fleek's pubic IPFS gateway. It was used to make this phishing site accessible through web browsers:



In our latest data set, most of the IPFS-hosted phishing was routed through gateways operated by just three companies:

2025 RANK	PROVIDER	DOMAINS	2024 PHISHING ATTACKS	2025 PHISHING ATTACKS
1	IPFS Foundation / Protocol Labs	dweb.link and ipfs.io	8,743	**4,642**
2	Cloudflare	cf-ipfs.com and cloudflare-ipfs.com	4,351	**2,036**
3	Fleek	flk-ipfs.xyz, fleek.co, fleek.cool	2,405	**993**
4	Consensys	infura-ipfs.io	2,381	**52**

While IPFS is sometimes touted as a technology that is "permissionless, trustless, censorship resistant, and free of centralized gatekeepers," a phishing site hosted on IPFS can be effectively neutralized if a gateway operator simply stops making the URL resolve on its standard DNS domain. To make that happen, gateway providers are using the Bad Bits Denylist. This is a blocklist of IPFS IDs that IPFS gateway operators can refuse to serve, if they choose to. The Denylist is used to curb phishing, malware distribution, copyright violations, and other abuses, and is operated by Protocol Labs, which invented the IPFS protocol and also operates two popular gateways. We will continue to monitor phishing on IPFS.

Domain Registrars

Most domain names used to host phishing attacks are registered by phishers for the express purpose of committing crimes. Domain name registrars that have the highest rates of phishing abuse tend to be the ones that offer low prices or offer high-volume registrations services. The gTLD registrars with the most domains used for phishing attacks were:

2025 RANK	REGISTRAR	REGISTRAR IANA_ID	gTLD DOMAINS UNDER MANAGEMENT	PHISHING DOMAINS
1	NICENIC	3765	141K	**114,493**
2	NameSilo	1479	4,481K	**114,317**
3	Dominet (HK)	3775	766K	**96,650**
4	NameCheap	1068	18,701K	**83,587**
5	Key-Systems	1345	1,216K	**75,713**

NICENIC, with less than 150,000 domains under management, had more phishing domains reported (114K) than the largest registrar GoDaddy (66K reported in 65 million registrations) and #2 NameSilo (114K reported in 4.5 million registrations).

Domains reported for phishing at #3 Dominet (HK) increased by 477%. Most of these were associated with Unpaid Toll scam campaigns.

Key-Systems had 74,737 .BOND domains names reported for phishing. This caused the registrar to enter to Top 5 rankings.

The Top 20 Registrar rankings for this yearly study period are posted at the Cybercrime Information Center.

Notably, 75% of the Top 5 slots over the past 5 years were held by repeat entrants. NameCheap and NameSilo have appeared in the Top 5 in each of our five annual studies. GoDaddy appeared annually from 2021 through 2024 but dropped to #6 in 2025.

5–YEAR COMPARISON OF REGISTRARS WITH MOST PHISHING DOMAINS REPORTED				
2021 Study	**2022 Study**	**2023 Study**	**2024 Study**	**2025 Study**
1. NameCheap	**1. NameCheap**	**1. NameSilo**	**1. NameSilo**	**1. NICENIC**
2. NameSilo	2. GoDaddy	2. PDR	2. GoDaddy	**2. NameSilo**
3. GoDaddy	**3. NameSilo**	**3. NameCheap**	3. Onamae	**3. Dominet (HK)**
4. PDR	4. DNSpod	4. GoDaddy	4. PDR	**4. NameCheap**
5. Tucows	**5. Dominet (HK)**	5. Sav.com	**5. NameCheap**	**5. Key-Systems**

Below we use the metric phishing domain score to compare gTLD registrars by highest incidence of phishing relative to others. The highest-scoring gTLD registrars for this period were:

2025 RANK	REGISTRAR	REGISTRAR IANA_ID	GTLD DOMAINS	PHISHING DOMAINS	PHISHING DOMAIN SCORE
1	NICENIC	3765	140K	114,493	**8,192.4**
2	Aceville	3858	44K	6,706	**1,534.5**
3	Dominet (HK)	3775	766K	96,650	**1,261.4**
4	WebNic	460	849K	61,700	**727.1**
5	OwnRegistrar	1250	327K	21,983	**673.3**

NICENIC International, a registrar in Hong Kong, again topped the registrar rankings by phishing domain score, with a highest score (8,192.4) we have reported. Nearly all the NICENIC domains reported for phishing were in .COM (80%), .NET (10%), or .ORG (7%). More than 45,000 of these domains were hosted on IP addresses assigned to CLOUDFLARE-NET (AS13335).

Case Study:
Unpaid Toll Scams on Domains at Dominet (HK)

Through most of 2025, a Chinese threat group known as XinXin used a Phishing as a Service (PhaaS) infrastructure, LUCID, to offer a service where phishing attacks were promulgated via text messages sent from large mobile device farms. The service was used to impersonate U.S. toll road systems and numerous postal, courier, or package delivery services. Specifically, the attacks delivered text messages via Apple iMessage or Android RCS and by design. bypassed telecom filtering techniques to increase success. Victims of these scams unwittingly disclose their credit card and personal data. XinXin has also been using Darcula for its operations and offers its subscribers weekly licenses via Telegram.

Interisle reported in a March 2025 substack post that the toll scams often utilized deceptively composed domain names. In our 2025 study data, we identified 37K scam domains containing strings such as EZ-pass, EZpass, EZdrive, SunPass, etc.; of these,

- 24K were registered using Dominet (HK) registrar (IANA ID 3775), a Hong Kong company, the registrar was formerly Alibaba.com Singapore E-Commerce Private Limited
- 18.5 K of the domain names were registered in .XIN, Elegant Leader Limited (HiChina Group Ltd., Alibaba Group Holding Ltd.)
- 5.5K of the domain names were registered in .TOP, managed and operated by Jiangsu Bangning Science & Technology Co., Ltd. in Nanjing, China.

The scam sites were mainly hosted on IP addresses assigned to Chinese operators:

- 12.3K were hosted on IP addresses assigned to TENCENT-NET-AP-CN (AS132203),
- 2.1K on IP addresses assigned to ALIBABA-CN-NET (AS45102), and
- 7.6 were hosted on a DNS redirection service, CLOUDFLARE-NET (AS13335), so the IP address of the host is hidden.

What is Phishing-as-a-Service (Phaas)?

Phishing as a service (PhaaS) is an outsourced commercial cybercrime offering that allows parties without infrastructure or technical expertiseto conduct a sophisticated phishing attacks. According to Barracuda, PhaaS attacks spiked in the first quarter of 2025, driven in part by the massive Unpaid Toll Scam.

Typically offered in dark web marketplaces, PhaaS providers offer buyers access to ready-made phishing campaigns, including fake login, automated tools for sending phishing emails, managing stolen data, registering domain names, and hosting malicious sites, faciliitating large-scale attacks for clients with minimal investment.

Many offer services on a subscription or pay-per-use basis, lowering the barriers to entry and exit for this type of criminal activity, making the cybercrime business broadly accessible to low-skill attackers.

PhaaS is a significant, growing threat because it facilitates highly sophisticated attacks at scale, with many providers offering customization options to target specific organizations, industries, or individuals, increasing the successs rate of phishing campaigns.

Our figures underreport the total number of domain names registered for this scam. The Unpaid Toll scammers have also used domains that do not contain these strings and for many such domains, we did not receive sufficient metadata to associate domains with these scam campaigns.

Our available data demonstrates how phishing has become an internationalized, commercialized business conducted on an industrial scale. The domain name and hosting industries need to respond quickly when a nexus of this kind appears in order to successfully mitigate phishing at this level. Without coordinated anti-abuse measures, the widespread exploitation of domain and hosting resources that fuel these massive attacks will continue.

Bulk Registrations

Phishers often register large numbers of domain names, in batches – a practice called "bulk registration." At least 37% of the domains name used for phishing were bulk registered. These registrations are highly conspicuous and indicate that criminals are able to obtain large numbers of domain names at will.

Legitimate, law-abiding domain name registrants rarely need to register more than a small set of domain names at a time. Two notable classes who do are trademark owners, who register domain names for promotional, rebranding, or product/service launches, and "domainers" or domain speculators, who buy and sell domain names for profit. The domains registered by legitimate registrants are rarely blocklisted for phishing. In contrast, cybercriminals regularly register hundreds to thousands of domains at a time, and do so repeatedly, which they use to run large phishing and spamming campaigns.

We consider a set of domains to be bulk registered if at least ten domains reported to our phishing feeds were registered through the same registrar, with less than ten minutes between consecutive domain registrations. Using these criteria, we found 70,541 sets of bulk registrations, registered at 174 different gTLD registrars (compared to 9,081 sets, registered at 97 different registrars, in our previous report). These domains are almost always generated by a script and often include or entirely consist of random characters, or random dictionary words jammed together.

The registrars associated with the highest number of bulk-registered phishing domains were:

2025 RANK	REGISTRAR	IANA ID	BULK-REGISTERED DOMAINS	SETS	LARGEST SET (# OF DOMAINS)
1	Dynadot	472	**768,090**	7,033	4,386
2	Gname	1923	**586,743**	8,900	1,982
3	GoDaddy	146	**475,512**	8,929	1,431
4	NameSilo	1479	**268,206**	6,574	712
5	NameCheap	1068	**211,998**	5,719	826
6	GMA d/b/a Onamae	49	**166,921**	1,753	17,591
7	Dominet (HK)	3775	**158,325**	3,423	6,306
8	Spaceship	3862	**102,387**	1,678	2,664
9	Domain International	3863	**82,814**	2,571	2,044
10	NICENIC	3765	**67,697**	3,038	282

It should be noted that the number of sets, and the total number of domains registered in these sets, is under-counted. Our data set consists of only domain names that were reported to our phishing feeds. Many more domain names were involved in these bulk sets than we know about. Certainly, many were registered in these sets and used for phishing, but they were not detected and reported. And our data set does not include domains registered for (illegal) spamming campaigns.

Note also that some (criminal) registrants register smaller sets of domains – sometimes 20 at a time – but register sets regularly, sometimes every day over a period of days, or every week, and thereby consume large numbers of domains over time. Seemingly dissociated sets are sometimes the work of one threat actor, which can sometimes be revealed by analysis of the hosting, domain patterns, and other telltale signs. In the past, investigators could associate and aggregate sets based on registrant contact data. Because of ICANN policy, contact data is now rarely available for gTLDs, making it hard to identify and quickly mitigate phishing campaigns.

The gTLD registrars who sponsored the largest single sets of bulk domain registrations were:

2025 RANK	REGISTRAR	IANA ID	BULK-REGISTERED DOMAINS	SETS	LARGEST SET (# OF DOMAINS)
1	GMO d/b/a Onamae	49	166,921	1,753	**17,591**
2	Dominet (HK)	3775	158,325	3,423	**6,306**
3	Dynadot	472	768,090	7,033	**4,386**
4	eName	1331	16,436	142	**4,305**
5	Key-Systems	1345	67,293	1,791	**3,677**
6	Spaceship	3862	102,387	1,678	**2,664**
7	July Name	3855	9,267	135	**2,295**
8	Domain International	3863	82,814	2,571	**2,044**

In the previous report, there were only three gTLD registrars that had a set comprising at least 1,000 bulk registered domains. For this reporting period, however, there were twenty gTLD registrars that had a set of at least 1,000 bulk registered domains – nearly a 7-fold increase.

When bulk registration services are available, phishers can acquire domains at will, in large numbers. The sets of domains acquired via bulk registrations are easily identified by domain registration and passive DNS data. Registrars are in the best position to identify suspicious registrations, *e.g.,* from domain creation data and registrant contact data (and possibly domain name composition) and should bear responsibility for mitigating this malicious behavior.

Case Study:
Dynadot Inc. Bulk Registrations

Dynadot had the most bulk registered domains of all gTLD registrars.

On 30 March 2025, Dynadot received 5,131 bulk domain registrations, in eight separate sets. These domains were subsequently added to blocklists.

Half of these domain names were five-character domain names registered in 35 different TLDs, including: .PET, .BLOG, .WTF, .TOWN, .CARE, .TRADE, and .SOY. These were all either five random alphabetic characters (such as *dczwg.pet* and *oiwky.town*) or five random numeric characters (such as *86468.wtf* and *68352.blog*).

Nearly a quarter of these domain names were 16-character domain names registered in .COM – all were 16 random hexadecimal characters (such as *a831df6dc1e3321b.com* and *def5e20ecba92b2d.com*).

Case Study:
GMO Bulk Registrations

Among all gTLD registrars, GMO had the largest set of bulk registered domains. This set contained 17,591 domain names, registered at GMO between 01:11 and 11:10 on 19 February 2024 and was reported to the phishing feeds in our 2025 data. There was an average of 30 domains registered each minute in that 10-hour period.

These domains comprised eight random alphabetic characters (such as *jyqeecog.lol* and *ejmtuzej.lol*), almost all in the .LOL gTLD.

We note that 17,562 of these domains were also reported to our phishing feeds in our 2024 data. This is the largest set of bulk registered domains in any of our 5 yearly studies.

Hosting Networks

We studied where phishing sites were being hosted to identify the network operators that have been most exploited by phishers. This tells us where the phishing activities were hosted. For this analysis, we identified the IPv4 addresses (DNS A records) where phishing sites were hosted, the address block (allocation) of each address, and the Autonomous System Number (ASN) that administers that address allocation. Our data contained no IPv6 addresses reported for phishing, and thus only show results for phishing hosted on IPv4 addresses only.

We found phishing in 4,065 hosting networks. **The five ASNs with the most reported phishing attacks were:**

2025 RANK	HOSTING PROVIDER	AS NUMBER	# ROUTED IPV4 ADDRESSES	PHISHING ATTACKS
1	Cloudflare	13335	2,694K	**539,911**
2	Amazon	16509	210,264K	**163,160**
3	Shenzhen Tencent	132203	2,640K	**97,974**
4	Alibaba (US)	45102	6,407K	**51,335**
5	Fastly	54113	1,229K	**42,450**

The Top 20 ASN rankings for this yearly study period are posted at the Cybercrime Information Center.

A comparison of hosting networks with most phishing attacks shows that only one ASN has appeared in each of the past five years among the Top 5 ASN rankings:

5-YEAR COMPARISON OF HOSTING NETWORKS WITH MOST PHISHING DOMAINS				
2021 Study	**2022 Study**	**2023 Study**	**2024 Study**	**2025 Study**
1. NameCheap	**1. Cloudflare**	**1. Cloudflare**	**1. Cloudflare**	**1. Cloudflare**
2. Cloudflare	2. UnifiedLayer	2. Quadranet	2. Google	**2. Amazon**
3. UnifiedLayer	3. Microsoft	3. ColoCrossing	**3. Amazon**	**3. Shenzhen Tencent**
4. Google	4. NameCheap	4. Google	**4. Fastly**	**4. Alibaba (US)**
5. Digital Ocean	5. Google	5. UnifiedLayer	5. IQWeb	**5. Fastly**

Cloudflare's AS13335 had the most phishing attacks reported for the fourth year in a row. The San Francisco-based provider offers a reverse proxy service that protects its customers from denial-of-service attacks. This proxy service prohibits observers from seeing the real hosting locations behind this defense network. Phishers continue to take advantage of this service, using Cloudflare's service and nameservers to hide the hosting locations of their phishing pages from security responders. Cloudflare also provides subdomain services and hosting that were used by phisher reverse proxies.

Google dropped out of the top five after rising to #2 in our 2024 study. Most of the phishing attacks reported in Google's AS15169 were hosted on IPv4 addresses that Google uses to host its Blogger service. Please see the *"Subdomain Providers"* section for more about phishing at Blogger.

Hackers exploited Amazon Web Services to launch phishing campaigns. Amazon uses AS16509 to host Amazon Web Services (AWS). Phishers exploited misconfigured AWS accounts, which contributed to the large number of reported phishing attacks in this ASN.

The rise of #3 Shenzhen Tencent (AS132203) and #4 Alibaba (AS45102) is related to Unpaid Toll scam campaigns. Please see the section *"Case Study: Unpaid Toll Scams on Domains at Dominet (HK)"* for more about this largely SMS-based phishing campaign.

Phishers exploited #5 Fastly's content delivery network and security services. Domains (including phishing domains) resolve to the IPv4 addresses of Fastly's edge routers and "good traffic" is forwarded to Fastly customers' web sites. Phishing pages that are front ended by Fastly's service are thus reported as being hosted at IP addresses allocated to Fastly and not its customer's IP addresses. Phishers are thus taking advantage of Fastly's redirection service much as they have of Cloudflare's reverse proxy service.

The gross numbers of phishing attacks such as those reported above are significant and a simple equation: more phishing attacks means more damage and victimization.

As we did for TLDs, we use a proportional scoring metric to compare ASNs of different sizes. The metric *Phishing Attacks Score* – phishing attacks reported per 10,000 IP

addresses assigned to an ASN – compares whether an ASN has a higher or lower incidence of phishing relative to other ASNs and allows comparisons of ASNs of varying sizes.

2025 RANK	HOSTING PROVIDER	AS NUMBER	# ROUTED IPV4 ADDRESSES	PHISHING ATTACKS	PHISHING ATTACK SCORE
1	Cloudflare	13335	2,694K	**539,911**	**2,004.0**
2	Namecheap	22612	133K	**14,871**	**1,115.5**
3	SonderCloud	133199	68K	**6,128**	**906.7**
4	FranTech	53667	54K	**3,201**	**589.8**
5	Dimension Network	59371	79K	**4,133**	**522.5**

Cloudflare remains #1. Phishers have consistently exploited Cloudflare's reverse proxy service to hide their fake sites for the past five years. Cloudflare's free plan includes reverse proxy and global content delivery network services. A GitHub module provides a complete starter guide for employing the reverse proxy. The module description includes a section, IP Address Detection, where the author explains that "Because your site will be proxied via Cloudflare, the global variable $_SERVER["REMOTE_ADDR"] will contain a CloudFlare IP address, not the client IP." These characteristics are attractive to phishers.

Phishing attacks in #2 NameCheap (AS22612) are fewer in number but the ASN's attack score is second only to Cloudflare.

61% of the phishing attacks hosted in #3 SonderCloud's ASN targeted the United States Postal Service. 635 attacks used domains that contained the string "usps" and the remainder of this 61% were pseudo-randomly generated domain names. One-third of the domains associated with SonderCloud addresses were registered at Dominet (HK).

Phishing attacks hosted in #4 FranTech's ASN targeted Canada Post. 758 phishing attacks that targeted Canada Post used domain names registered at NameSilo and were also hosted at FranTech.

Nearly all the domain names used in phishing attacks hosted in #5 Dimension Network were pseudo-randomly generated. Two-thirds of these were registered in .COM or .CC.

Where in the World Do We Find Most Phishing?

We geolocated the IP addresses of phishing sites. In 2025, over one million phishing attacks in our study data were hosted on IP addresses geolocated to the United States. China was a distant second at 156,000.

Nine countries have been ranked in the top five for hosting the most phishing attacks over the past five years:

5–YEAR COMPARISON OF COUNTRIES HOSTING MOST PHISHING ATTACKS				
2021 Study	2022 Study	2023 Study	2024 Study	2025 Study
1. US	**1. US**	**1. US**	**1. US**	**1. US**
2. GB	**2. DE**	2. GB	**2. HK**	**2. CN**
3. NL	**3. RU**	**3. RU**	**3. CN**	**3. DE**
4. DE	**4. CN**	4. CY	4. NL	**4. HK**
5. RU	5. NL	5. DE	**5. RU**	**5. RU**

Hosting operators in the US have been consistently abused by phishers over our five-year measurement period. This is particularly true of providers that largely operate on US infrastructures and who offer services that create impediments for first responders and investigators. For example, reverse proxy services (*e.g.,* CloudFlare), redirection services (*e.g.,* Fastly), free web hosting (*e.g.,* Google Blogger sites), developer accounts (Amazon AWS), and email services (Microsoft 365).

China, Germany, Great Britain, and the Russian Federation have each occupied a top five spot in three of our five-year measurement periods.

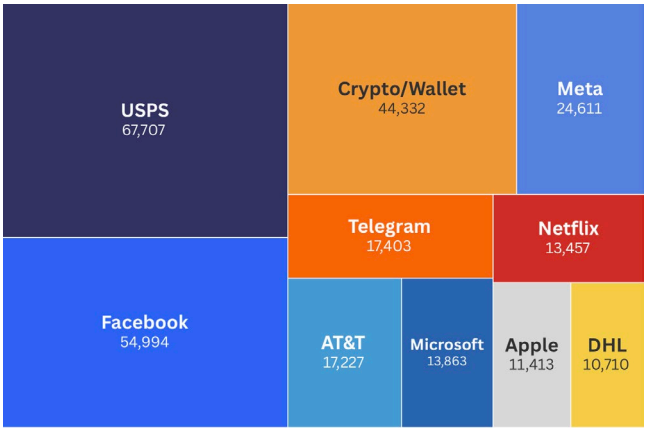
The Most-Phished Brands

The U.S. Postal Service was the brand that was phished the most often, and Meta was the company that suffered the most phishing attacks.

The U.S. Postal Service (USPS) has been a heavily impersonated brand for years. In 2024-2025, our sources reported that the USPS was attacked on 67,707 phishing sites. These phishing sites impersonated the USPS brand and tried to fool Internet users into thinking they were doing business with the USPS. Those attacks were mounted on 62,197 unique domain names.

Meta's Facebook was the most-attacked brand in our 2023-2024 study. In 2024-2025, Meta's brands—Facebook plus Instagram, WhatsApp, and Meta itself—were impersonated across 89,680 phishing sites.

Top Phished Brands May 2024 – April 2025



More than half of the domains used to attack the USPS — 32,124 to be exact — were in the .TOP TLD, operated by the Chinese company Jiangsu Bangning Science & Technology Co., Ltd. The .TOP registry received a breach letter from ICANN in July 2024. The breach letter charged the .TOP registry with problems beginning in April 2024, including failure to fulfill its abuse reporting and mitigation responsibilities, for failure to pay its ICANN fees, and other contractual breaches. ICANN then gave .TOP five time extensions to "cure" these problems, stretching into May 2025. During that year period, tens of thousands of phishing attacks on the USPS, using .TOP domains, took place. On 2 June 2025, ICANN announced that .TOP Registry had cured its contractual breaches, had instituted improved response procedures, and had developed "a proactive monitoring system to detect the use of .TOP domain names for DNS Abuse."

Over the last five years, the most-attacked brands were:

5–YEAR COMPARISON OF MOST PHISHED BRANDS				
2021 Study	**2022 Study**	**2023 Study**	**2024 Study**	**2025 Study**
1. Facebook	**1. Facebook**	**1. Facebook**	**1. Facebook**	**1. United States Postal Service**
2. Microsoft	2. Amazon	2. Mitsubishi UFJ NICOS	2. Gazprom	**2. Facebook**
3. Outlook	3. Microsoft	**3. United States Postal Service**	**3. United States Postal Service**	**3. Crypto/ Wallet**
4. Amazon	4. WhatsApp	4. NICOS	4. Microsoft	**4. Meta**
5. Apple	5. Apple	5. Microsoft	5. AT&T	**5. Telegram**

Use of Brand Names in Domain Names and URLs

Phishers continue to use company, service, and product names in phishing URLs to deceive victims. They embed the names of brands in domain names that they maliciously register for phishing attacks, and in hostnames and URL paths. **These are often tell-tale signs of phishing, and can be used by hosting providers, third-level domain providers, and domain name registrars and registry operators to find potential phishing sites.**

Of the 1,542,922 unique domain names used for phishing in 2024-2025, **8.9% contained a prominent brand name, spelled exactly (137,860 domains).** We found domains that contained exact matches for 762 well-known brands.

The United States Postal Service's real web site is at USPS.GOV, and "USPS" was contained in 32,353 domains names used for phishing, the most for any brand. "Apple," "DHL," "Coinbase," and "Amazon" were the next-most-frequently appearing brand strings.

In addition, phishers register many second-level domains that contain misspellings of brand names, attempting to foll unwary Internet users. We did not perform a near-match analysis to count these domains.

Phishers also frequently place brand names elsewhere in URLs — in subdomains and in URL paths — in the hopes that it will deceive unwary victims. Many Internet users do not have the knowledge needed to recognize the domain name in a URL, and some do not check the URL at all. That is why phishers also register domain names and use URLs that contain no brand name, or even consist of nonsense characters.

Use of Internationalized Domain Names (IDNs) for Phishing

Data continues to show that the unique characteristics of Internationalized Domain Names (IDNs) are seldomly used to facilitate phishing. Phishers do occasionally take advantage of them, though, because IDN spoofing can fool the human eye, and these domains can evade automated detection by security programs that do not recognize the words they are constructed to represent.

IDNs are domain names that contain one or more non-ASCII characters. Such domain names can contain letters with diacritical marks such as and ü, or be composed of characters from non-Latin scripts such as Arabic, Chinese, or Cyrillic. IDN TLDs allow the entire domain name to be in non-Latin characters, including the TLD extension.

In an *IDN homographic attack*, a phisher seeks to deceive Internet users by exploiting the fact that characters in different language scripts may be nearly (or wholly) indistinguishable, thereby allowing the phisher to spoof a brand name. These look-alike domains can be displayed in browser address bars if IDN display is enabled.

For example, this IDN spoofs the cryptocurrency site **bitpay.com** by substituting the character "į" for the Latin "i":

xn--btpay-b4a.com ⟶ bįtpay.com

In the 2024-2025 data:

- There were 2,655 unique internationalized domain names, used to make 2,706 attacks. This is just 0.17% of all the domains used for phishing during the 2024-2025 study period.
- 78% of those domains (2,076) appear to be malicious registrations. However, not all the malicious registrations were homographic attacks.
- The 2,655 domain names were in 81 TLDs: 31 new gTLDs, 26 ccTLDs, 18 IDN TLDs, and 6 legacy gTLDs

The most-targeted brands were two Turkey-based online casinos: Jojobet (jojobet.com) and Holiganbet (holiganbet.com). Many of these domains included a number. About half were registered at a Turkish registrar: Atak Domain Bilgi Teknolojileri A.Ş. (IANA ID 1601).

Examples included:

xn--jojobt999-zf7d.com ⟶ jojobẹt999.com

xn--holganbet1085-djb.com ⟶ holîganbet1085.com

Recommendations

Phishing attacks, and the abuse of internet resources that enables them, have grown at an alarming rate over the past five years. This surge in phishing significantly contributes to the rising global cost of cybercrime and the harm inflicted on individuals, businesses, and the economy at large.

Despite the scale and visibility of the problems, however, effective anti-abuse measures remain largely unimplemented. Phishers are currently thriving in an environment where it is cheap and easy to acquire attack resources, with minimal risk and few deterrents. The Unpaid Toll Scam exemplifies how growing criminal enterprises are exploiting unchecked access to launch large-scale attacks that cause widespread harm.

Like pollution, Internet resource abuse — and the cybercrime it facilitates — is an economic negative externality imposing steep costs on society.

Reasonable, effective anti-abuse measures are urgently needed across the domain name, subdomain, and hosting ecosystems to limit criminal access to these critical resources. To be effective, these must include *proactive*, *front-end measures to prevent abuse* before it occurs, as well as stronger, more *efficient mitigation mechanisms* on the back end when incidents of abuse are detected.

We recommend the following actions:

1. Verify Customer Registration Information

Stronger and more effective measures to verify customer registration information should be adopted across the domain name, subdomain, and hosting industries. Our research, which has been corroborated by ICANN's INFERMAL study, has consistently found a strong correlation between stricter verification requirements and lower rates of abuse.

Cybercriminals frequently provide false or suspicious customer information. Industry should use address verification tools and screen for bogus and inaccurate registration data at the time of registration or sign-up. These practices are already widely used across e-merchant and other online industries, where international address verification services and identity verification tools are used to screen customer data for pennies per transaction.

In the domain name industry specifically, we recommend ICANN adopts the European Union NIS 2 Directive standards. NIS 2 requires that registries and registrars take steps to ensure accurate and complete registration information and recommends risk-based approaches to screen for problems. European ccTLD registries are using automated screening tools and risk-based evaluations to meet these requirements and are showing that this approach is effective, practical, and efficient.

2. Implement Requirements for Bulk Registration and High-Volume Account Creation

Phishers consistently exploit low-friction, high-volume access to Internet resources, including domain names and subdomains. Our research has consistently shown that bulk registration is a key method attackers use to acquire domain names, accounting for over a third of all phishing-related abuse. In this study and prior research, we found hundreds of instances where phishers registered thousands of malicious domains at a time at a single registrar, over very short timeframes. ICANN's INFERMAL study, conducted independently, found a similarly high correlation between bulk registration and phishing.

Registrants wishing to bulk register domain names should be vetted and required to prove their identity before accessing these services. Registrants associated with prior malicious registration activity should be denied. Registries and registrars should also routinely scrutinize high-volume transitions for suspicious registration behavior and suspend accounts found to engage in abuse. Limits should also be considered for the number of registrations that can be submitted at one time and over short durations.

Subdomain providers should also adopt measures to prevent abusive high-volume account creation, cancel

abusive accounts where identified, and require customer verification to access high-volume services.

3. Proactively Identify and Act on Suspicious Abuse Patterns

Phishers often abuse resources in other conspicuous, identifiable patterns beyond falsified account information and excessive, high-volume registrations. These include, for example, registering nearly identical domain names and subdomains with small sequential variations, registering algorithmically generated nonsense names and names containing or confusingly similar to known brands, and using identical registration information across multiple abusive registrations and accounts, among others.

Domain name, subdomain, and hosting providers should implement procedures and tools to proactively identify and act on such suspicious patterns to increase the efficiency and effectiveness of abuse mitigation and prevention.

As a routine step in abuse mitigation, providers should search for all associated registrations and accounts tied to discovered phishers and suspend the abuser's entire portfolio of holdings. This will increase the efficiency and effectiveness of mitigation efforts by shutting down multiple vectors of malicious activity associated with bad actors.

In terms of proactive abuse prevention, automated systems have already been deployed by some domain name registries to detect and place a hold on suspicious registrations before they can inflict harm, such as the EURid Abuse Prevention and Early Warning System (APEWS). Real-time abuse monitoring tools should be further developed and adopted broadly across the domain industry and other sectors. The continuing development of AI is likely to make these systems continually more effective and agile, promising to keep up with evolving abusive registration tactics.

4. Require Corrective Action

ICANN's anti-abuse policy goals should be aimed at a clear, measurable outcome: reducing DNS abuse, specifically the number of malicious domain name registrations. Each year, however, our research finds the amount of domain name abuse increasing and a high level of consistency in the registries and registrars with high abuse rates.

In the DNS market today—which is shaped by ICANN policy—there are simply too few disincentives for resource providers to take business from cybercriminals. Absent reasonable rules, the pressure to gain and retain market share and deliver return on investment in these highly competitive markets provides little incentive to curb such behavior. This is of particular concern given ICANN's plan to further expand gTLDs, as additional pressure on competition and prices will exacerbate already growing abuse problems and related harms.

This should include requiring registries and registrars with consistently high abuse rates to improve performance or face penalties such as increased fees, suspended or reduced ability to process registration, and possible deaccreditation. In addition, ICANN should also review its contracts to identify and revise provisions that may unintentionally reduce the financial or operational risk of processing abusive domain name registrations.

About the Authors

Greg Aaron is an internationally recognized authority on the use of domain names for cybercrime, and is an expert on domain name registry operations, DNS policy, and related intellectual property issues. Mr. Aaron is Senior Research Fellow for the Anti-Phishing Working Group. As a member of ICANN's Security and Stability Advisory Committee (SSAC), he advises the international community regarding the domain name and numbering system that makes the Internet function. He works with industry, researchers, and law enforcement to investigate and mitigate cybercrime, and is also a licensed private detective. He was the Chair of ICANN's Registration Abuse Policy Working Group (RAPWG) and has been a member of ICANN's EPDP Working Group, which created registration data access policies. He was the senior industry expert on a team that evaluated the policy and technical qualifications of more than one thousand new gTLD applications to ICANN in 2012-2013. He has created products and services used by organizations to discover and track Internet-based threats, and has managed large top-level domains around the world, including .INFO, .ME, and .IN. He is President of Illumintel, Inc., a consulting company. Mr. Aaron is a *magna cum laude* graduate of the University of Pennsylvania.

David Piscitello has been involved in Internet technology and security for more than 40 years. Until July 2018, Mr. Piscitello was Vice President for Security and ICT Coordination at ICANN, where he participated in global collaborative efforts by security, operations, and law enforcement communities to mitigate Domain Name System abuse. He also coordinated ICANN's security capacity-building programs and was an invited participant in the Organisation for Economic Co-operation and Development (OECD) Security Expert Group. Dave is an Associate Fellow of the Geneva Centre for Security Policy. He served on the Boards of Directors at the Anti-Phishing Working Group (APWG) and Consumers Against Unsolicited Commercial Email (CAUCE). He is the recipient of M3AAWG's 2019 Mary Litynski Award, which recognizes the

lifetime achievements of individuals who have significantly contributed to making the Internet safer.

Karen Rose is an internationally recognized expert in Internet policy, technology, and development with over 25 years in the field. Since 2017, she has consulted on a range of Internet policy, digital economy, and new technology issues. From 2006 to 2016, Karen was a senior executive at the Internet Society (ISOC) where she led the organization's work to expand Internet access, infrastructure, and related policy capacity around the world, as well as the organization's research on emerging Internet issues. Earlier in her career, Ms. Rose served at the U.S. Federal Communications Commission (FCC) and the National Telecommunications and Information Administration (NTIA). While in government, she was co-author of the U.S. policy statement and related agreements that globalized management of the Internet Domain Name System (DNS) and led to the creation of the Internet Corporation for Assigned Names and Numbers (ICANN). Ms. Rose previously served on the board of Netnod, one of Europe's most recognized Internet exchange point operators, and on the .US domain stakeholder advisory committee. She currently serves on the advisory panel for AfChix, an African organization dedicated to advancing women in tech.

Dr. Colin Strutt has published and spoken extensively on networking technology, name collisions, enterprise management, eBusiness, and scenario planning, and has represented the interests of Digital Equipment, Compaq, and the Financial Services Technology Consortium in national and international industry standards bodies. He holds six patents on enterprise management technology and has more than forty years of direct experience with information technology, as a developer, architect, and consultant, with recent work including design and operation of a regional public safety network, providing technical expertise relating to patents, and analysis of world-wide Internet use. Dr. Strutt holds a B.A. (with First Class Honours) and Ph.D. in Computer Science from Essex University (UK).

Acknowledgments

The authors extend thanks to:

- Spamhaus and OpenPhish, for their kind contribution of data for this study.
- The PhishTank and the APWG eCrime Exchange communities, for their collaborative efforts to identify phishing.
- Domain Tools, for access to historical and bulk parsed WHOIS and the IRIS investigations platform.
- April Lorenzen and Zetalytics, for access to passive DNS data.
- Saeed Abu-Nimeh for access to the Seclytics Predictive Threat Intelligence platform.
- John Levine, for operational support.
- All the security personnel who fight phishing.

About Interisle Consulting Group

Interisle's principal consultants are experienced practitioners with extensive track records in industry and academia and world-class expertise in business and technology strategy, Internet technologies and governance, financial industry applications, and software design. For more about Interisle, please visit: www.interisle.net