LIVRE BLANC TECHNIQUE · CADRE PROPOSÉ · VERSION 1.0

De la détection à la mise en œuvre

Une architecture mesurable de réponse au DNS Abuse : provenance des preuves, mesures proportionnées, responsabilité publique et recours rapide — conçue pour être testée plutôt que simplement affirmée.

Publié le 2 août 2026 · PhishDestroy Recherche · Projet soumis à consultation publique · Non soumis à un examen par les pairs

PD-WP-2026-01 · Version 1.0 · 2026-08-02
https://phishdestroy.io/fr/dns-abuse-enforcement-framework

RÉSUMÉ

PROPOSITION INDÉPENDANTE · NE CONSTITUE PAS UN PROGRAMME D'ICANN

Conclusion directe. L'écosystème contractuel de l'gTLDe présente un écart mesurable entre l'utilisation malveillante d'un domaine, validée sur le plan technique, et la mise en œuvre effective de mesures d'atténuation. Des études publiées montrent que de nombreuses campagnes de phishing se poursuivent pendant des heures, voire des jours, tandis que les procédures de conformité contractuelle peuvent s'étaler sur plusieurs jours ouvrés. Le modèle de scénario présenté montre comment ce délai augmente les gains attendus des campagnes ; la fourchette de 60 à 85 % correspond à l'estimation centrale vérifiable avancée dans l'article concernant le préjudice postérieur à la notification, et non à une statistique établie pour l'ensemble de la fraude mondiale. L'estimation technique de 100 à 150 dollars concerne la collecte et le traitement initial d'un corpus défini de données de zone, de Certificate Transparency et de flux publics, et non le coût total de l'examen juridique ou de l'application de la loi. L'article propose des preuves signées, des objectifs de réponse mesurables, une remontée automatique des cas validés, des mesures correctives proportionnées, une responsabilité publique et une procédure d'appel rapide. Il ne propose pas de donner aux signalants un accès direct aux commandes de suspension de domaine.

SOURCE PRIMAIRE
Étayé directement par un document officiel ou une étude publiée.

MODÈLE ILLUSTRATIF
Un calcul reproductible dont les données d'entrée sont des hypothèses, et non des moyennes du marché.

PROPOSITION DE POLITIQUE PUBLIQUE
Un dispositif soumis à consultation, expérimentation et révision.

01 Problématique de recherche, champ d'application et niveau de preuve

La question est plus précise que « qui a échoué ? » : **quels délais observables entre des preuves validées et une action proportionnée sont évitables, et quelle intervention réduit le préjudice subi par les victimes sans provoquer de faux positifs ni d'effets collatéraux inacceptables ?**

Le champ couvre l'écosystème contractuel des gTLD : titulaires, revendeurs, bureaux d'enregistrement, registres et fonction de conformité contractuelle d'ICANN. Les hébergeurs, CDN, navigateurs, services de paiement, plateformes publicitaires, CERT nationaux et services répressifs ne sont inclus que lorsqu'ils influent sur la chaîne des preuves ou de réponse. Les ccTLD relèvent d'une gouvernance différente et ne sont pas réputés soumis aux contrats gTLD d'ICANN.

État d'avancement des thèses principales

- Cet article analyse l'ICANN en tant qu'institution de gouvernance privée et de contrôle du respect des contrats au sein de l'écosystème de l'gTLD. L'ICANN n'est ni un organisme de régulation gouvernemental ni une autorité chargée de faire respecter la loi, mais elle accrédite les bureaux d'enregistrement, conclut des contrats avec les opérateurs de registre et veille au respect de ces accords ; ce champ d'action limité n'exonère pas l'institution de sa responsabilité.
- La fourchette de 60 à 85 % constitue une estimation quantitative centrale dans le modèle d'évaluation des préjudices présenté dans cet article. Elle est présentée comme une estimation vérifiable, dérivée d'hypothèses explicites et d'observations de cas concrets — et non comme une statistique déjà établie pour l'ensemble de la fraude mondiale. La publication d'un ensemble de données au niveau des incidents, qui aligne les horodatages relatifs à la détection, à la notification, à l'atténuation et aux préjudices, constitue la prochaine étape en matière de preuve.
- Le chiffre de 100 à 150 dollars correspond à une estimation budgétaire technique vérifiable pour la collecte continue et le triage initial d'un ensemble défini de données issues des zones accessibles, du programme « Certificate Transparency » et des flux publics sur une infrastructure standard. Il ne s'agit pas du coût d'une visibilité mondiale complète, d'un examen juridique, des recours, d'une haute disponibilité ou de la mise en application. Le document le considère donc comme une référence à reproduire à l'aide d'une charge de travail publiée, d'un inventaire des sources et d'un journal des coûts — et non comme un prix universel déjà validé. Cette distinction nuance l'affirmation sans pour autant effacer l'asymétrie des coûts faisant l'objet du test.
- La comparaison sur trois semaines présentée dans cet article porte sur le délai de mise en conformité, et non sur un accord de niveau de service (SLA) universel relatif à la suppression de sites web. ICANN's FAQ sur la conformité contractuelle précise que la plupart des types de plaintes peuvent faire l'objet de trois délais de réponse successifs de cinq jours ouvrés avant qu'une escalade formelle ne soit engagée, alors que de nombreuses campagnes malveillantes se poursuivent pendant des heures, voire des jours. Les contrats exigent par ailleurs, de manière distincte, la mise en œuvre de mesures correctives rapides et appropriées dès l'obtention de preuves permettant d'agir. [2] [4]
- Dans le cas d'un enregistrement malveillant avéré et à usage unique, `serverHold` C'est l'une des mesures correctives les plus perturbatrices au niveau de l'DNS, car elle supprime la délégation de la zone. Elle n'est pas universelle : elle peut également perturber la messagerie, les sous-domaines et les services légitimes ; les réponses mises en cache peuvent persister jusqu'à l'expiration du TTL ; et les services compromis ou partagés peuvent nécessiter des mesures d'atténuation plus ciblées. [4] [7]

CONTRIBUTION À LA RECHERCHE

La proposition est falsifiable. Un projet pilote peut comparer des cohortes de traitement et de contrôle selon le délai de triage, le délai d'atténuation, les indicateurs des pertes subies par les victimes, la récurrence, les faux positifs, le délai de révocation et les effets collatéraux.

02 Ce que révèlent les sources primaires

$165.1M

Financement des opérations d'ICANN pour l'exercice 2027

Budget adopté pour l'exercice 2027. Ordre de grandeur contextuel ; il ne s'agit pas de dépenses consacrées au DNS Abuse. [1]

191,561

Plaintes relatives au phishing et à l'usurpation d'identité enregistrées par l'IC3 en 2025

Catégorie de plaintes IC3 la plus représentée en nombre ; 215,8 millions de dollars de pertes directement imputées. [10]

24 h

Durée de vie médiane selon une étude de 2021

Résultat spécifique à cet ensemble de données portant sur 1 288 domaines de hameçonnage ; il ne s'agit pas d'une durée de vie universelle. [11]

Aucun SLA fixe

Délai universel de désactivation

Les modifications de 2024 imposent une atténuation « rapide » et « appropriée », non un délai mondial unique. [2] [3]

PROPOSITION	STATUT	CE QU'ON PEUT AFFIRMER
Le phishing relève du DNS Abuse	VÉRIFIÉ	Le phishing figure explicitement parmi les cinq catégories couvertes par les modifications contractuelles de 2024 applicables aux gTLD. [2]
Les bureaux d'enregistrement doivent agir	VÉRIFIÉ	Les bureaux d'enregistrement doivent agir rapidement lorsqu'ils disposent de preuves exploitables qu'un nom qu'ils parrainent est utilisé à des fins de DNS Abuse. [2]
Les opérateurs de registre doivent agir	VÉRIFIÉ	Les opérateurs de registre doivent agir rapidement lorsqu'ils déterminent raisonnablement, sur la base de preuves exploitables, qu'un nom enregistré est utilisé à des fins de DNS Abuse ; la mesure appropriée demeure contextuelle. [3]
`serverHold` supprime la délégation	VÉRIFIÉ	Il s'agit d'un statut EPP défini au niveau du serveur. Les réponses mises en cache par DNS peuvent subsister jusqu'à leur expiration, et cette action s'applique à l'ensemble du domaine enregistré. [7]
Tout DNS Abuse est visible dans CZDS ou CT	FAUX	CZDS et Certificate Transparency sont des capteurs précieux, mais ils ne donnent ni une vue exhaustive ni une vue en temps réel de tous les usages de domaines. [8] [9]

Le premier rapport semestriel d'ICANN sur la mise en œuvre des modifications de 2024 recense 192 enquêtes, plus de 2 700 domaines suspendus, plus de 350 pages de phishing désactivées et deux notifications formelles de manquement contractuel (Notices of Breach). Ces chiffres ne prouvent pas que les contrôles actuels suffisent, mais excluent l'affirmation absolue selon laquelle le système n'agit jamais. [5]

03 Pourquoi la latence de réponse reste un sujet de recherche légitime

Certaines campagnes de hameçonnage se déroulent sur une durée de quelques heures ou de quelques jours. Dans une étude réalisée en 2021, Bijmans et al. ont fait état d'une durée de vie moyenne observée de 45 heures et d'une médiane de 24 heures pour 1 288 domaines de hameçonnage. Une étude de 2026 portant sur des domaines de hameçonnage nouvellement enregistrés a révélé une distribution très asymétrique : sur 14 112 domaines dont la durée de vie était mesurable, la moyenne était de 8,6 jours et la médiane d'un jour. Aucun de ces échantillons ne peut être généralisé à toutes les catégories de menaces, mais les deux montrent pourquoi un processus mesuré uniquement en jours ouvrés peut passer à côté de campagnes de courte durée. [11] [12]

> **LE DÉCALAGE TEMPOREL MESURÉ**
>
> Ces études ne permettent pas de déterminer la part des préjudices financiers survenant après la notification, mais elles mettent en évidence un décalage temporel : un processus dont les premières étapes informelles de mise en conformité peuvent prendre jusqu'à quinze jours ouvrés ne peut, à lui seul, constituer une réponse aux incidents pour des campagnes dont la durée de vie médiane est proche d'un jour. Le délai de 21 jours mentionné ci-dessous correspond donc à un scénario de latence de mise en conformité, et non à une référence à un « SLA ICANN » universel.

FIGURE 1 · EXEMPLE DE RÉSULTATS CUMULÉS D'UNE CAMPAGNE

MODÈLE · ESPACEMENT TEMPOREL QUASI LOGARITHMIQUE

La courbe illustre le scénario présenté à la section 4 ; il ne s'agit pas de données de marché observées. Le placement horizontal permet de condenser les longs intervalles pour faciliter la lecture. Source : modèle reproductible dont les données d'entrée sont rendues publiques.

PRUDENCE EN MATIÈRE DE CAUSALITÉ

Une durée de vie plus courte d'un domaine ne signifie pas automatiquement qu'une perte financière a été évitée. Les acteurs malveillants peuvent déplacer leurs activités, exploiter des sites compromis, changer de canaux de diffusion ou encaisser leurs gains avant d'être détectés. L'effet de causalité doit être mesuré, et non déduit uniquement de la rapidité de la suppression.

04 L'économie des campagnes frauduleuses comme scénario reproductible

L'actif économiquement déterminant n'est souvent pas le prix d'enregistrement, mais le trafic, les créations, l'infrastructure et la confiance accumulés autour d'un domaine. Cette intuition est plausible, mais son ampleur varie selon la campagne frauduleuse. Le calculateur expose donc chaque entrée plutôt que de présenter un résultat hypothétique comme une moyenne observée.

DÉFINITION DU MODÈLE

```
visits(T)   = daily_traffic × T / 24
victims(T)  = visits(T) × conversion_rate
proceeds(T) = victims(T) × average_loss × (1 - cashout_attrition)
profit(T)   = proceeds(T) - campaign_budget
```

Calculateur de scénarios

Modifiez n'importe quelle hypothèse. Les valeurs sont données à titre indicatif et ne constituent pas des estimations du marché typique du hameçonnage.

`MODÈLE ILLUSTRATIF`

Budget de la campagne (USD)

5000

Visites quotidiennes

2000

Taux de conversion des victimes (%)

1.5

Perte moyenne par victime (USD)

2400

Taux d'attrition lié aux retraits (%)

25

Durée de l'action (en heures)

24

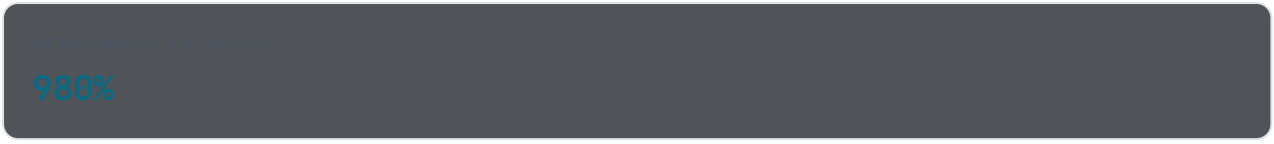
Victimes
2,000

Victimes retirées
30

Perte brute
$54,000

Perte nette estimée
$49,000

Durée de l'action
2.2 h



Le nombre attendu de victimes peut comporter une partie décimale, car le modèle exprime une espérance. Il ne tient pas compte du déclin du trafic, de la rétroaction liée à la détection, de la migration, des victimes répétées ni des distributions d'incertitude.

▶ Afficher la table source du modèle

05 Mesurer les préjudices évitables sans prétendre à la précision

La « perte après détection » ne peut constituer un critère d'évaluation utile que si les notions de détection, de transmission et de préjudice sont définies de manière cohérente. L'horodatage d'une liste noire ne constitue pas une preuve que le bureau d'enregistrement a reçu des éléments de preuve exploitables. Une transaction de portefeuille n'est pas automatiquement attribuable à un domaine donné. Le fait qu'un domaine devienne inaccessible ne permet pas d'identifier l'acteur à l'origine de ce changement.

Schéma minimal d'événement

ÉVÉNEMENT	HORODATAGE REQUIS	PREUVE MINIMALE
Première observation	`t_obs`	Capteur, hachage requête/réponse, méthode de capture, source d'horloge.
Validation technique	`t_valid`	Indicateur reproductible, identité de l'évaluateur, catégorie de menace et niveau de confiance.
Notification transmise	`t_notice`	Accusé de réception authentifié et version de l'evidence envelope.
Accusé de réception par l'acteur responsable	`t_ack`	ID du dossier et rôle destinataire : hébergeur, bureau d'enregistrement, registre, plateforme ou autorité.
Atténuation observée	`t_mitigate`	État DNS, HTTP, des paiements ou de la plateforme, mesuré depuis plusieurs points d'observation.
Recours / rétablissement	`t_restore`	Fondement de la décision, évolution des preuves et vérification du rétablissement.
Événement causant des dommages	`t_harm`	Rapport anonymisé concernant la victime, transaction identifiable ou autre élément de substitution documenté.

INDICATEUR DE RÉSULTAT PROPOSÉ

$$\text{Post-notice harm share} = \frac{\text{attributable harm with } t_{harm} > t_{notice}}{\text{all attributable harm in the observation window}}$$

Le numérateur et le dénominateur doivent suivre la même règle d'attribution. Les résultats doivent indiquer la cohorte, l'intervalle de confiance, la censure à droite, les sources manquantes, le traitement des victimes en double et la sensibilité à la fenêtre d'observation. Le terme « évitable » doit être réservé à un plan d'étude causal ou, au minimum, à une comparaison appariée — et non à tout événement survenant après la notification.

ESTIMATION CENTRALE ISSUE DE LA MODÉLISATION · 60 À 85 %

L'étude retient une fourchette de 60 à 85 % comme estimation centrale de la part des préjudices imputables survenant après la détection et la notification, dans la catégorie d'incidents modélisée. Il s'agit d'une estimation de scénario dérivée d'hypothèses rendues publiques et d'observations de cas — et non d'une statistique mesurée pour l'ensemble des fraudes à l'échelle mondiale. Elle doit être utilisée à des fins d'analyse de sensibilité jusqu'à ce qu'un ensemble de données au niveau des incidents permette d'aligner les observations, les preuves validées, les dates de survenance, d'atténuation et de préjudice. La publication de cet ensemble de données constitue le test probatoire de la thèse, et non une raison de la rejeter.

06 La carte institutionnelle : les capacités sont réparties

Aucun acteur ne voit ni ne contrôle l'intégralité de l'incident. Le bureau d'enregistrement connaît la relation avec le titulaire ; le registre contrôle le statut du domaine défini au niveau du registre ; l'hébergeur et le CDN contrôlent la diffusion du contenu ; les navigateurs et éditeurs de sécurité contrôlent les avertissements ; les prestataires de paiement et de portefeuilles peuvent interrompre les transferts ; les autorités peuvent ordonner la conservation ou la saisie. ICANN rédige et fait respecter les contrats dans l'écosystème gTLD, mais n'exploite pas de plan de contrôle EPP universel.

01 · SIGNAL

Chercheurs & capteurs

Observer les indicateurs liés au contenu, à l'infrastructure et aux victimes ; préserver leur provenance.

02 · SERVICE

Hébergeur / CDN / plateforme

Peut retirer rapidement le contenu ou en bloquer l'accès, souvent sans modifier le domaine.

03 · PARRAIN

Bureau d'enregistrement

Examine le signalement, contacte le titulaire et peut définir un statut côté client.

04 · ZONE

Opérateur de registre

Permet de gérer l'état EPP défini dans le registre ainsi que la délégation de la zone TLD.

05 · CONTRAT

Conformité contractuelle d'ICANN

Enquête sur la conformité des parties contractantes ; ne tranche pas chaque affaire de fraude.

06 · DROIT

CERT / autorités

Coordonnent la réponse et exercent les pouvoirs juridiques propres à leur juridiction.

La décentralisation des compétences n'implique pas la disparition des responsabilités. Un bureau d'enregistrement parrain ne se dégage pas de ses obligations contractuelles en déléguant la gestion des abus à un revendeur ; le registre contrôle l'état EPP défini au niveau du serveur ; l'ICANN veille au respect des obligations contractuelles. La piste d'audit doit consigner non seulement qui a agi, mais aussi qui a reçu des preuves permettant d'engager une action, qui a réorienté le dossier, qui n'a pas répondu ou qui a manqué à une obligation qui lui était assignée. L'autorité légale reste entre les mains de l'acteur habilité à appliquer une mesure ; la responsabilité s'étend également aux manquements documentés.

Concentration des financements et hypothèse vérifiable relative à un conflit d'intérêts

$165.1M

Financement des opérations de l'ICANN pour l'exercice 27

Adoption du budget de référence pour l'exercice 27. [1]

≈98.1%

les sources de revenus provenant des frais d'enregistrement et des frais de registraire

Environ 162,0 millions de dollars sur les 165,1 millions de dollars prévus dans le plan de financement. [1]

70.7%

les frais liés aux transactions uniquement

$116.8M tied to billable domain transactions. [1]

La structure de financement repose donc en grande partie sur les paiements versés par les parties contractantes dont les accords sont appliqués par ICANN, et une part importante varie en fonction des opérations d'enregistrement facturables. Cela crée une dépendance structurelle et soulève une question légitime de conflit d'intérêts. Cela *pas*, ne suffisent pas à elles seules à prouver une application délibérément laxiste de la réglementation ou une « captation réglementaire » avérée. L'hypothèse de la captation doit être vérifiée à la lumière des délais d'intervention au cas par cas, des résultats en matière d'application de la réglementation, des sanctions, de la récidive et du rôle des parties prenantes financées dans les décisions relatives aux politiques et à leur mise en œuvre.

07 Le cadre contractuel de référence pour 2024 — et ce qu'il ne précise pas

Les modifications mondiales d'avril 2024 du Registrar Accreditation Agreement et du Base Registry Agreement ont instauré des obligations expresses de lutte contre le DNS Abuse. Les bureaux d'enregistrement doivent agir rapidement lorsqu'ils disposent de preuves exploitables qu'un nom qu'ils parrainent est utilisé à des fins de DNS Abuse. Les opérateurs de registre doivent agir rapidement lorsqu'ils déterminent raisonnablement, sur la base de preuves exploitables, qu'un nom enregistré est utilisé à des fins de DNS Abuse. Dans les deux cas, la mesure appropriée dépend du contexte, de la gravité et des effets collatéraux. [2] [3]

Trois échéances souvent confondues

CHRONOLOGIE	À QUOI CELA S'APPLIQUE-T-IL ?	CE QUE CELA NE SIGNIFIE PAS
24 heures	Examen, au titre du § 3.18.3 du RAA, des signalements étayés d'activités illégales (« Illegal Activity ») adressés au contact dédié par les autorités chargées de l'application de la loi, de la protection des consommateurs, quasi gouvernementales ou similaires.	Il ne s'agit pas d'un délai universel de 24 heures pour la suspension.
« Rapidement »	Adopter une mesure d'atténuation appropriée une fois atteint le seuil applicable de preuves exploitables.	Ce terme ne correspond pas à un nombre fixe d'heures et n'impose pas le même remède dans chaque affaire.
21 jours	Peut correspondre à un délai de régularisation accordé à la suite d'une mise en demeure contractuelle officielle pour manquement.	Il ne s'agit pas de la durée de vie habituelle attribuée à chaque domaine malveillant signalé.

Cette flexibilité présente des avantages : un domaine universitaire compromis ne doit pas être traité comme un domaine de hameçonnage à usage unique nouvellement enregistré. Le problème en matière de responsabilité réside dans le fait qu'il est difficile de comparer ce qui est « rapide » et ce qui est « approprié » en l'absence d'horodatages, de catégories de cas et de codes de résultat publiés. La proposition ci-dessous prévoit des mesures d'évaluation et de contrôle sans prétendre qu'un délai unique puisse s'appliquer à tous les cas.

08 Le problème des limites : le phishing est pris en compte ; certaines escroqueries financières pourraient ne pas l'être

Le phishing relève explicitement de la définition contractuelle du DNS Abuse. La frontière la plus difficile concerne les sites qui trompent sous un nom original plutôt que d'usurper un tiers identifiable : certaines fausses plateformes d'investissement, boutiques frauduleuses, escroqueries à la récupération et manœuvres visant les signatures de portefeuilles. Selon les faits, ils peuvent relever de l'abus de contenu web, de la fraude à la consommation ou d'une autre catégorie juridique plutôt que du DNS Abuse contractuel.

> TERME DE RECHERCHE PROPOSÉ
>
> **Verified Financial Harm Abuse (VFHA)** : usage documenté d'un domaine pour obtenir, par tromperie, des fonds, des identifiants de paiement, des clés privées ou des phrases de récupération, indépendamment de toute usurpation de marque. VFHA ne relève pas de la terminologie actuelle d'ICANN et ne crée pas, à lui seul, de pouvoir contractuel.

Une consultation de politique publique pourrait déterminer si une catégorie étroitement circonscrite et étayée par des preuves, telle que VFHA, doit figurer dans de futurs contrats, un cadre intersectoriel de

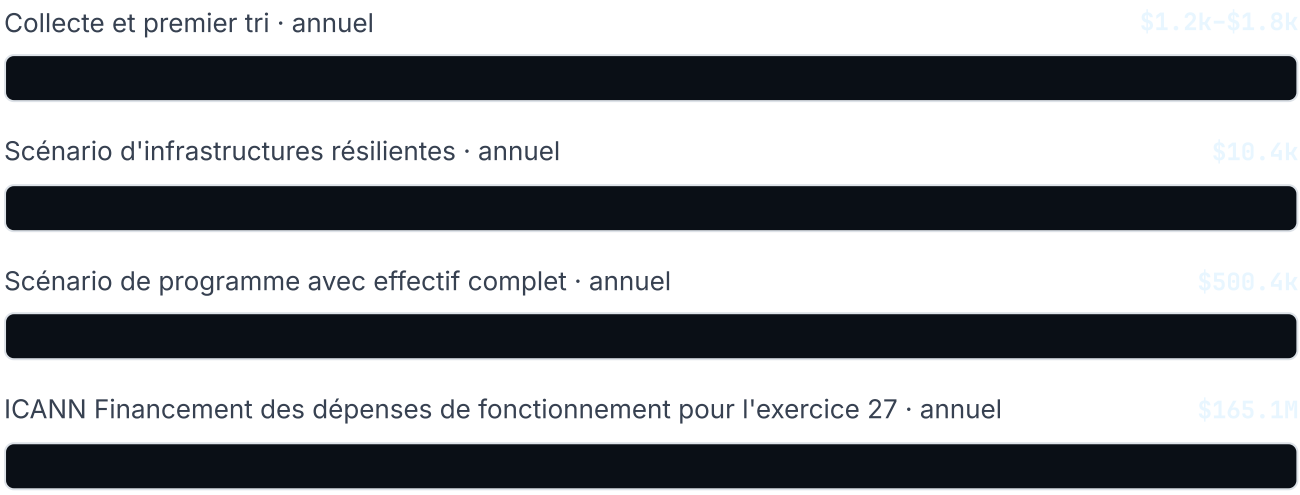
saisine ou le droit national. Toute extension devrait exiger un critère précis de préjudice, des preuves fiables, des remèdes proportionnés, un contrôle de compétence et un recours. Les qualificatifs vagues comme « arnaque » sont insuffisants.

09 Ce que l'argument de la surveillance à 100-150 $ par mois doit prouver — et ce qu'il ne peut pas prouver

Un serveur standard peut télécharger des instantanés accessibles des fichiers de zone gTLD participants et calculer les modifications localement, ingérer des événements « Certificate Transparency » sélectionnés et des flux ouverts, normaliser les chaînes de caractères, calculer des hachages et hiérarchiser les candidats. Il s'agit d'un critère de référence technique utile et vérifiable — et non d'une « surveillance complète d'Internet ». Au deuxième trimestre 2026, Verisign a fait état de 401,6 millions d'enregistrements sur l'ensemble des TLD ; le CZDS couvre les fichiers de zone gTLD participants plutôt que l'ensemble des TLD, et le CT recense les certificats ou pré-certificats enregistrés publiquement plutôt que tous les domaines actifs ou malveillants. [8] [9] [17]

CAPACITÉ	PROTOTYPE SUR INFRASTRUCTURE STANDARD	SERVICE DE PRODUCTION D'INTÉRÊT PUBLIC
Zone/CT/importation de flux	Faisable pour un ensemble de sources défini	Collecteurs redondants, contrats d'approvisionnement, surveillance des écarts
Triage des chaînes de caractères et des tables de hachage	Réalisable	Évaluation comparative, détection des dérives, études sur les faux négatifs
Rendu dans le navigateur	Petit sous-ensemble échantillonné	Flotte isolée, points d'observation régionaux, confinement des logiciels malveillants
Qualification juridique	Non incluse	Examinateurs qualifiés, cartographie des juridictions et des pouvoirs
Haute disponibilité / conservation des preuves	Généralement absent	Signatures sécurisées par un module de sécurité matériel (HSM), journaux d'audit, sauvegardes et gestion des incidents
Recours et réintégration	Non inclus	Fonctionnement 24 h/24, 7 j/7, escalade autonome et objectifs de service

FIGURE 2 · CONTEXTE D'ORDRE DE GRANDEUR — LARGEUR LOGARITHMIQUE · COÛTS NON COMPARABLES



Les largeurs logarithmiques permettent de garder les petites valeurs visibles. Les trois premiers chiffres correspondent à des hypothèses techniques ou de programme qui nécessitent un point de référence publié et ne constituent pas des devis de fournisseurs. ICANN Le financement des opérations est un chiffre vérifié à l'échelle institutionnelle. Il s'agit délibérément de budgets non équivalents : la comparaison vise à déterminer si la collecte et le tri de base représentent un coût intrinsèquement prohibitif, et non si un programme complet de mise en application coûte 100 dollars par mois.

10 Cadre proposé de réponse aux abus vérifiés

Le cadre proposé est une architecture de référence, non un « interrupteur d'arrêt » mondial automatique. Il normalise l'evidence envelope, le dossier de décision et les horodatages, tout en permettant à l'opérateur habilité de choisir la mesure efficace produisant le moins d'effets collatéraux.

01 · INGESTION

Acquérir & préserver

Collecter signalements et observations ; hacher les artefacts bruts ; synchroniser les horloges.

02 · PROVENANCE

Normaliser les preuves

Consigner l'origine, la méthode, l'historique de traitement et les dépendances des sources.

03 · VALIDER

Confirmer

Reproduire le comportement préjudiciable et identifier les éléments de preuve indépendants.

04 · ÉVALUER

Risque & effets collatéraux

Classer les enregistrements malveillants, les services compromis, l'hébergement mutualisé et la gravité.

05 · RÉPONDRE

Signaler et atténuer

Désigner le responsable, fixer un délai et déterminer la solution efficace la moins perturbatrice.

06 · RÉEXAMINER

Audit & recours

Publier les métadonnées de résultat, mesurer l'impact et faciliter une révocation rapide.

Niveaux de preuve

E1 **Signal non vérifié**

Information isolée, correspondance lexicale ou allégation fondée sur la réputation. Convient à des fins d'observation, mais ne suffit jamais à elle seule pour justifier une suspension.

E2 **Comportement reproduit**

Capture horodatée montrant un vol d'identifiants, l'injection d'un logiciel malveillant ou un parcours de transaction trompeur.

E3 **Confirmation indépendante**

Au moins deux sources véritablement indépendantes ou une preuve technique reproductible, accompagnée de vérifications de la propriété et du contexte.

E4 **Confirmation qualifiée**

Autorité, service touché, titulaire de marque ou preuves validées émanant de victimes, assorties d'une chaîne de conservation respectueuse de la vie privée.

RÈGLE D'INDÉPENDANCE

Trois flux qui reproduisent la même liste noire en amont constituent une seule source, et non trois. Le graphe de provenance doit mettre en évidence l'origine commune, la synchronisation et la republication par le fournisseur.

11

Un evidence envelope minimal et une API interopérable

L'APIe doit créer un dossier vérifiable et déclencher un compte à rebours de réponse pouvant faire l'objet d'un audit ; un déclarant ne doit pas pouvoir émettre directement une commande de suspension. Si un dossier E3/E4 concerne un enregistrement malveillant à usage unique et arrive à expiration sans décision motivée ni mesure corrective efficace, le système le transmet automatiquement à l'opérateur du registre ou à un autre acteur disposant d'une autorité contractuelle ou légale. A `serverHold` Une commande ne peut provenir que d'un acteur autorisé. L'escalade automatique et le pouvoir du registre d'intervenir en cas d'expiration constituent des modifications

proposées de la politique, et non des affirmations concernant une autorité existante. Chaque transition d'état est signée et consignée dans le journal d'audit.

POST /V1/CASES · EXEMPLE

```
{
  "indicator": {"type": "domain", "value": "example.invalid"},
  "alleged_category": "credential_phishing",
  "observed_at": "2026-08-02T06:14:22Z",
  "evidence": [
    {
      "type": "http_capture",
      "sha256": "a3f1c9…",
      "collection_method": "isolated_browser_v2",
      "source_id": "reporter:ed25519:7c2a…"
    }
  ],
  "provenance_graph": "ipfs-or-object-store:sha256:91bd…",
  "collateral_context": {
    "registered_domain_scope": true,
    "shared_service": false,
    "mail_observed": true,
    "suspected_compromise": false
  },
  "requested_action": "review",
  "reporter_signature": "ed25519:…"
}
```

Une réponse réussie renvoie l'ID du dossier, l'acteur destinataire, le niveau de preuve, les erreurs d'exhaustivité, le délai d'examen attendu et une URL publique de transparence. Aucun remède précis ne doit être promis avant qu'un acteur compétent ait évalué son pouvoir et les effets collatéraux.

12 Objectifs de réponse proposés, et non délais universels de désactivation

Les objectifs de niveau de service doivent distinguer *l'accusé de réception*, le *triage*, la *décision* et *l'atténuation effective*. Les performances deviennent ainsi mesurables sans présumer que la suspension constitue toujours la bonne issue.

PROFIL DU DOSSIER	ACCUSÉ	OBJECTIF DE TRIAGE	OBJECTIF DE DÉCISION	OPTIONS DE RÉPONSE COURANTES
Vol E3/E4 d'identifiants de paiement ou de phrases de récupération au moyen d'un enregistrement malveillant à usage unique	15 min	1 h	4 h	Blocage du contenu ; suspension par le bureau d'enregistrement ou le registre lorsqu'elle est autorisée ; avertissements du navigateur et du prestataire de paiement.
Phishing de marque E3 ou diffusion de logiciels malveillants	30 min	2 h	6 h	Retrait par l'hébergeur/CDN, atténuation au niveau du domaine, sinkhole ou avertissement selon le point de contrôle.
Domaine légitime compromis ou locataire SaaS partagé	1 h	4 h	12 h	Isolement du chemin d'accès/du compte et récupération par le propriétaire ; éviter, dans la mesure du possible, la suspension des domaines enregistrés.
Fraude financière avec classification contestée	4 h	12 h	24 h	Conservation, intervention au niveau de la plateforme ou du paiement, saisine de l'autorité compétente et décision motivée.
Signal E1 ou rapport incomplet	Auto	24 h	Aucun jusqu'à validation	Suivre, enrichir et demander des éléments justificatifs.

Il s'agit d'objectifs indicatifs. Les valeurs exactes doivent être déterminées à partir de la durée de vie observée des menaces, des effectifs, du coût des erreurs et des contraintes juridiques, puis publiées sous forme de distributions de réalisation plutôt que sous la forme d'une simple moyenne.

13 Sécurité, respect des procédures, confidentialité et modes de défaillance

Une réaction rapide, en l'absence de mesures de protection, peut transformer des données erronées en censure, en sabotage commercial ou en pannes d'infrastructure. Une architecture adéquate considère donc les faux positifs et les dommages collatéraux comme des défaillances de sécurité majeures.

MODE DE DÉFAILLANCE	CONTRÔLE OBLIGATOIRE	MESURE VÉRIFIABLE
Signalement malveillant visant un concurrent	Authentification des auteurs de signalements, réputation des sources, reproduction indépendante et sanctions en cas d'abus	Taux de signalements rejetés par auteur ; cas de manipulation confirmés
Circularité des flux présentée comme un consensus	Graphe de provenance et déduplication des sources en amont	Nombre de sources indépendantes avant et après correction de la filiation
Suspension globale d'un domaine légitime compromis	Classification de l'intention d'enregistrement et préférence pour une atténuation au niveau du chemin	Part des domaines compromis ; services légitimes touchés
Les données relatives aux victimes ou les détails de l'exploitation ont été rendus publics	Divulgation par niveaux, expurgation, pièces à conviction scellées et délais de conservation	Incidents liés à la protection de la vie privée ; résultats de l'examen des expurgations
Une mesure injustifiée persiste	Réception des recours 24 h/24 et 7 j/7, examinateur indépendant et procédure de rétablissement authentifiée	Délai médian et au 95e centile de révocation
Une suspension du registre interrompt la messagerie ou des sous-domaines	Inventaire des effets collatéraux, proportionnalité du remède et suivi postérieur à l'action	Services interrompus par action ; taux de révocation

Garanties minimales en matière de procédure régulière

1. Pour chaque mesure restrictive, le code de motif, le niveau de preuve et le décideur responsable sont consignés.
2. Le titulaire peut obtenir un exposé des motifs respectueux de la vie privée et présenter des contre-preuves.
3. Les recours d'urgence sont examinés par une personne qui n'a pas pris la décision initiale.
4. L'annulation se propage par le même canal signé que l'action d'origine.
5. Les statistiques globales relatives aux erreurs et aux restaurations sont publiques ; l'accès aux éléments de preuve sensibles reste soumis à des restrictions.

14 D'un « indice de toxicité » à un indice de qualité de la réponse permettant de rendre des comptes

Une note publique attribuée à un bureau d'enregistrement peut renforcer la responsabilité, mais les classements simplistes sont faussés par la taille du portefeuille, la couverture des flux, la composition de la clientèle et la distinction entre enregistrement malveillant et compromission ultérieure. Une note ne doit jamais justifier le blocage collectif de tous les clients d'un bureau d'enregistrement.

VECTEUR DE QUALITÉ PROPOSÉ

```
RQI = report as a vector, not a single opaque rank:

  coverage-adjusted validated-abuse rate
  median / p90 acknowledge, triage and decision times
  mitigation effectiveness and recurrence
  false-positive and reversal rates
  median / p95 appeal-resolution time
  evidence completeness and transparency rate

Always publish N, observation window, confidence intervals,
feed coverage and malicious-registration / compromise split.
```

Si un indicateur composite est nécessaire à des fins de gouvernance, les pondérations doivent être définies avant l'évaluation, soumises à des tests de sensibilité et validées rétrospectivement sur des cas mis de côté. Les résultats doivent être stratifiés par TLD, taille du bureau d'enregistrement, classe de menace et source des preuves. Le résultat obtenu est un indicateur de responsabilité — et non un verdict automatisé concernant le domaine.

15 Base publique de transparence sur le DNS Abuse, à accès gradué

Un registre de transparence peut mettre fin aux litiges concernant l'existence d'une notification, la date à laquelle elle a été transmise et les mesures qui ont été prises par la suite. La publication de toutes les données pourrait toutefois exposer les victimes, les données à caractère personnel, les méthodes d'enquête et les vecteurs d'attaque actifs. La solution réside dans un accès à plusieurs niveaux.

P

Registre public

ID du dossier, indicateur, catégorie générale, horodatages clés, niveau de preuve, rôles des acteurs, code de résultat, état du recours et hachages des artefacts scellés.

C

Vue « Partenaire contractuel »

Preuves techniques reproductibles, canal de contact, contexte connexe et consignes de conservation.

R

Vue restreinte aux autorités

Données sur les victimes, attribution financière, éléments d'enquêtes actives et chaîne de conservation non expurgée.

Chaque mise à jour est de type « ajout uniquement », horodatée et signée. Les corrections n'effacent pas l'historique ; elles ajoutent un enregistrement qui remplace le précédent. La recherche publique doit respecter les règles de conservation, empêcher l'identification massive des victimes et offrir un recours en cas de données à caractère personnel inexactes.

16 Un projet pilote de six mois assorti d'une évaluation préenregistrée

Un projet pilote utile doit être assez restreint pour être gouverné et assez vaste pour tester la chaîne causale. Périmètre suggéré : trois bureaux d'enregistrement volontaires, deux opérateurs de registre, un partenaire d'hébergement/CDN, deux flux de recherche indépendants et un comité de recours qualifié. Le protocole d'étude et les définitions des résultats doivent être enregistrés avant l'affectation des dossiers.

MOIS 1

Protocole et cartographie juridique

Définir les catégories, les autorités compétentes, les niveaux de preuve, l'analyse d'impact sur la vie privée et les conditions de cessation.

MOIS 2

Instrumenter le processus existant

Mesurer les horodatages et résultats de référence sans modifier le comportement de réponse.

MOIS 3

Expérimenter l'evidence envelope

Introduire une provenance signée, la déduplication et la classification des effets collatéraux.

MOIS 4

Tester les objectifs de réponse

Randomiser les dossiers éligibles ou déployer par paliers ; surveiller quotidiennement les erreurs.

MOIS 5

Exercer les recours et les modes de défaillance

Mener des exercices de rétablissement, des simulations de signalements malveillants menées par une red team et des audits des contrôles d’accès.

MOIS 6

Évaluation indépendante

Publier les tailles d'effet, les intervalles de confiance, les données manquantes, les événements indésirables, les coûts et les documents nécessaires à la reproduction des résultats.

Critères d'évaluation principaux de l'étude pilote

- Durée médiane et durée au 90e centile entre la mise à disposition de données validées et la mise en œuvre effective de mesures d'atténuation.
- Différence au niveau du préjudice imputable survenu après la notification ou d'un indicateur prédéfini de l'exposition des victimes.
- Taux de faux positifs, gravité des mesures injustifiées et délai médian de rétablissement.
- Récurrence chez le même titulaire, dans le même cluster d’infrastructure et au niveau de la même campagne.
- Coût opérationnel direct par cas validé et par mesure d'atténuation efficace.

RÈGLE DE DÉCISION

Ne passer à l’échelle que si le pilote démontre une atténuation effective nettement plus rapide sans dépasser les limites préenregistrées de faux positifs, d’incidents de confidentialité, de délais de recours ou de perturbations collatérales du service.

17 Conclusions et recommandations vérifiables

La réponse au DNS Abuse n’est ni un simple filtre technique ni un problème qu’une institution peut résoudre seule. Les contrats en vigueur depuis 2024 ont instauré des obligations d’atténuation substantielles, tout en laissant une marge d’appréciation importante sur les preuves, les délais et le remède. Cette latitude est nécessaire à la proportionnalité ; sans registres comparables, elle complique aussi l’évaluation des performances.

1. **Normaliser l’evidence envelope.** Adopter des champs communs de provenance, d’horodatage et de résultat pour les auteurs de signalements, bureaux d’enregistrement, registres et fournisseurs d’infrastructure.
2. **Mesurer les étapes séparément.** Publier les délais d’accusé, de triage, de décision, d’atténuation et de recours par classe de menace et niveau de preuve.

3. **Faire la distinction entre un enregistrement malveillant et une compromission.** Privilégier les mesures de remédiation au niveau du chemin d'accès ou du compte pour les services légitimes compromis, et réserver les mesures à l'échelle du domaine aux cas où celles-ci sont proportionnées.
4. **Piloter les objectifs de réponse.** Tester des objectifs horaires pour les enregistrements malveillants à usage unique et de forte confiance, plutôt que déclarer un délai universel.
5. **Publier des données de responsabilité respectueuses de la vie privée.** Utiliser un registre de transparence gradué, assorti d'historiques signés et de preuves restreintes.
6. **Évaluer l'impact causal.** Il ne faut pas conclure qu'une suspension plus rapide permet de réaliser des économies tant qu'une étude préenregistrée n'aura pas évalué l'impact sur les victimes et les répercussions.

La conclusion constructive n'est pas que le problème initial disparaît une fois que ses affirmations ont été nuancées. Elle réside dans le fait que les affirmations centrales peuvent désormais être vérifiées : la fourchette de préjudice post-détection comprise entre 60 et 85 % constitue une hypothèse quantitative explicite ; la fourchette de 100 à 150 $ constitue une hypothèse budgétaire technique vérifiable pour une couche définie de capteurs et de triage ; et les objectifs de réponse à l'échelle de l'heure peuvent faire l'objet d'un projet pilote pour les enregistrements malveillants à usage unique et hautement fiables. Publier la charge de travail, les coûts, les horodatages et les résultats, les comparer à une référence, puis mesurer les écarts et les erreurs. Une confirmation justifierait une modification des contrats et des politiques ; un rejet permettrait d'identifier quelle hypothèse s'est révélée erronée.

Note éditoriale et méthodologique. PhishDestroy est un projet indépendant et non commercial de renseignement sur les menaces. Cette publication est une proposition de politique publique et d'ingénierie, non un avis juridique, un programme d'ICANN ou un article évalué par les pairs. Les fourchettes budgétaires présentées comme des « modèles » sont des hypothèses de planification. Les affirmations issues de sources primaires sont référencées ci-dessous. Les corrections peuvent être transmises par les canaux de contact et de divulgation responsable du site.

UNE APPROCHE CENTRÉE SUR LA PERSONNE · LA RESPONSABILITÉ DOIT EMPÊCHER TANT L'INACTION QUE LES EXCÈS

Une limite personnelle au pouvoir d'exécution

Je ne demande pas — et je ne souhaite pas — avoir un accès direct à un outil de blocage de domaines. Ce pouvoir doit faire l'objet d'un contrôle indépendant, de journaux d'audit publics, d'une procédure de recours rapide et d'une possibilité de réversibilité.

Je pense qu'il existe de nombreuses entreprises compétentes et responsables auxquelles on pourrait confier certaines parties de ce travail. Au vu de mon expérience et des articles que j'ai publiés, je ne classe pas NameSilo dans cette catégorie.

Je ne conseillerais pas aux entreprises américaines légitimes de confier des fonctions sensibles liées à la lutte contre les abus ou à la sécurité à des prestataires spécifiques dont les conflits d'intérêts, les compétences ou la conduite ne résisteraient pas à un examen indépendant. Il s'agit ici d'actions avérées, et non de nationalité : une origine russe ne prouve rien en soi, tout comme l'adresse d'une entreprise américaine ne prouve rien.

Je veux que justice soit faite et que les responsables rendent véritablement des comptes pour les bureaux d'enregistrement ayant tiré des revenus de l'enregistrement et du renouvellement de domaines identifiés comme faisant partie de campagnes d'escroquerie répétées. Lorsque les preuves indiquent, au-delà d'une simple négligence, une éventuelle complicité délibérée — qu'il s'agisse d'une implication opérationnelle directe ou du rôle d'intermédiaire en connaissance de cause dont la fonction était de maintenir un domaine nuisible enregistré et en ligne malgré des avertissements répétés —, ce comportement doit faire l'objet d'une enquête indépendante et, s'il est avéré, entraîner des conséquences. Je ne présente pas ces soupçons comme des faits avérés ; mais le statut d'intermédiaire ne doit pas conférer l'immunité face à un examen minutieux.

Examiner l'enquête à l'origine de l'affaire ↗

A

Références et notes de source

[1] **ICANN : budget adopté pour l'exercice 27 (2026)** · https://www.icann.org/en/system/files/files/adopted-icann-budget-fy2027-published-2026-en.pdf

Source des 165,1 millions de dollars destinés au financement des opérations pour l'exercice 27 et composition des sources de financement.

[2] **ICANN : modification globale de 2024 du Registrar Accreditation Agreement** · https://www.icann.org/en/system/files/files/registrar-accreditation-agreement-global-amendment-05apr24-en.pdf

Source contractuelle principale des obligations des bureaux d'enregistrement relatives au DNS Abuse.

[3] **ICANN : amendement global de 2024 au contrat de registre « Base gTLD »** · https://itp.cdn.icann.org/en/files/registry-agreements/base-registry-agreement-global-amendment-05-04-2024-en.html

Source contractuelle principale régissant les obligations de l'opérateur de registre en matière d'atténuation.

[4] **Conformité contractuelle d'ICANN : avis sur les obligations relatives au DNS Abuse (2024)** · https://www.icann.org/en/contracted-parties/advisories/documents/advisory-compliance-with-dns-abuse-obligations-in-the-registrar-accreditation-agreement-and-the-registry-agreement-05-02-2024-en
Interprétation opérationnelle, exigences applicables aux signalements et exemples d'atténuation appropriée.

[5] **ICANN : mise en œuvre des exigences d'atténuation du DNS Abuse (2024)** · https://www.icann.org/en/system/files/files/icann-enforcement-of-dns-abuse-mitigation-requirements-08nov24-en.pdf
Rapport semestriel de mise en œuvre et décompte des enquêtes et mesures d'atténuation.

[6] **ICANN SSAC, SAC115 : rapport sur une approche interopérable du traitement des signalements d'abus (2021)** · https://www.icann.org/en/system/files/files/sac-115-en.pdf
Contexte sur l'interopérabilité des signalements d'abus et la qualité des preuves.

[7] **Hollenbeck, RFC 5731 : Mappage des noms de domaine EPP (2009)** · https://www.rfc-editor.org/rfc/rfc5731.html
Définition technique des valeurs d'état du domaine EPP, y compris les états définis par le serveur.

[8] **Laurie et al., RFC 9162 : Certificate Transparency version 2.0 (2021)** · https://www.rfc-editor.org/rfc/rfc9162.html
Spécification de référence du protocole et limites de CT comme capteur.

[9] **ICANN, Service centralisé de données de zone** · https://www.icann.org/en/contracted-parties/registry-operators/services/centralized-zone-data-service
Portée et modèle d'accès pour les fichiers de zone « gTLD » participants.

[10] **FBI Internet Crime Complaint Center, rapport annuel IC3 2025** · https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
Chiffres des plaintes et pertes déclarées, notamment pour le phishing et l'usurpation.

[11] **Bijmans et al., « Catching Phishers By Their Bait » (USENIX Security, 2021)** · https://www.usenix.org/system/files/sec21-bijmans.pdf
Mesures spécifiques à chaque ensemble de données concernant l'infrastructure de hameçonnage et les durées de vie observées.

[12] **Domaines nouvellement enregistrés et durée de vie des tentatives d'hameçonnage, Journal of Cybersecurity (2026)** · https://doi.org/10.1093/cybsec/tyag020
Données empiriques récentes concernant les domaines de hameçonnage nouvellement enregistrés et la répartition de leur durée de vie.

[13] **Analyse inférentielle des noms de domaine enregistrés à des fins malveillantes — INFERMAL (2024)** · https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf

Analyse financée par ICANN des enregistrements malveillants et des facteurs de l'écosystème ; limites pertinentes pour les inférences causales.

[14] **Chainalysis : tendances 2026 en matière d'escroqueries liées aux cryptomonnaies** · https://www.chainalysis.com/blog/crypto-scams-2026/

Estimation d'un fournisseur concernant les flux liés aux escroqueries sur la blockchain en 2025 ; ce chiffre n'est pas pris en compte dans le total des cas de phishing par domaine.

[15] **APWG, Rapport sur les tendances en matière de hameçonnage, 1er trimestre 2026** · https://docs.apwg.org/reports/apwg_trends_report_q1_2026.pdf

Attaques de hameçonnage et URL observées ; ces chiffres ne correspondent pas au nombre de domaines enregistrés distincts.

[16] **Centre d'information sur la cybercriminalité / Interisle, Panorama du phishing en 2025** · https://www.cybercrimeinfocenter.org/phishing-activity-numbers-may-april-2025

Distingue les attaques observées, les domaines uniques et les domaines enregistrés à des fins malveillantes.

[17] **Verisign, Rapport sur le secteur des noms de domaine, 2e trimestre 2026** · https://blog.verisign.com/domain-names/q2-2026-domain-name-industry-brief-quarterly-report/

Source des 401,6 millions d'enregistrements déclarés pour l'ensemble des TLD.