NDDCAMP PARIS 2024

8E EDITION

2024

13

SEPT

Noms de domaine & marques

Tables rondes d'experts

Juridique - Législation - Propriété intellectuelle
Cybersquatting - Second marché - Digitalisation AI
- SEO - DNS - NIS2 - Cybersécurité - Web3 - ENS

LA LETTRE DES INCORPORELS

PROGRAMME

13 SEPTEMBRE 2024 • 9H À 19H • INSTITUT F2I

22 RUE DES VIGNERONS, 94300 VINCENNES, FRANCE
(MÉTRO : BÉRAULT (LIGNE 1) / RER : VINCENNES (LIGNE A))

Sparkling .domains

BOISCHAUT MAISON DE VENTES AUX ENCHÈRES

Domstocks.com Boost your SEO with expired domains

ECOLE DSP

SUR VOTRE AGENDA EN 2025

NDDCAMP ALSACE

4E EDITION

Tables rondes d'experts

SEO, Droit, Nommage, Marques, Snap, Marché secondaire, Web3

2025

21

MARS

STRASBOURG

9H00/19H00 • SIEGE DU CIC EST

31 RUE JEAN WENGER - VALENTIN, 67000 STRASBOURG

TRAM : RIVES DE L'AAR

Intervenants du NDDCamp Alsace, 2024

Programme disponible fin 2024.

Même semaine et seulement à 45km du **CloudFest 2025**

A PROPOS


NDDCamp Paris, juin 2022

Depuis 2015, NDDCamp Paris rassemble chaque année les professionnels du nommage, noms de domaines et marques, autour de tables rondes et d'ateliers.

L'objectif de cette journée - gratuite mais sur invitation, est de diffuser dans notre milieu professionnel les dernières avancées technologiques et juridiques, mais aussi les bonnes pratiques et de débattre des thèmes d'actualité du secteur.

Depuis 2021, une deuxième conférence annuelle se tient à Strasbourg (NDDCamp Alsace) et la question du nommage est désormais étendue au Web3, où le cybersquatting et les atteintes aux droits de propriété intellectuelles concernent de plus en plus d'entreprises et nécessite une évolution de la loi.

La 8e édition parisienne est organisée en partenariat avec l'institut F2I, que nous remercions vivement d'accueillir à nouveau.

Les organisateurs

NDDCamp est une initiative menée par quatre professionnels des noms de domaine, Marc-Olivier Bernard, David Chelly, Philippe Franck et Benjamin Louis. Elle bénéficie du soutien de l'AFNIC, France Num, de Sedo et d'autres organismes de référence du secteur.

Un format original

NDDCamp est un moment de networking et d'échange de savoir. L'événement est organisé en tables rondes d'experts, sans présentations promotionnelles ni sponsorisées.
En raison de la diversité des publics, des thèmes distincts sont abordés simultanément dans deux salles.

En parallèle, chacun peut visiter les stands des exposants et les espaces de restauration, dans une atmosphère conviviale et d'échange. Les participants pourront de plus y assister à des démos, présentations d'outils, tests de versions beta, etc.

L'événement est disponible en live et replay sur Youtube, Twitter, Linkedin, Twitch et Facebook. Il bénéficie d'une large diffusion sur les réseaux sociaux, forums, médias en ligne spécialisés, blogueurs et prescripteurs.

CONTACT

Benjamin Louis
Tél. 06 12 45 66 48
Email : info@nddcamp.fr
Web : https://nddcamp.fr

S'engager pour le développement d'un internet solidaire

En 2023, la Fondation Afnic a contribué à hauteur de 1 382 690 euros à 87 projets de solidarité numérique. Depuis 8 ans, ce sont 512 projets qui ont bénéficié de plus de 10 millions d'euros. L'internet made in France est avant tout un service, le .fr, un nom de domaine sûr et accessible. Mais il est bien plus que cela. Chaque .fr contribue à financer la Fondation Afnic pour la solidarité numérique.

afnic Internet made in France

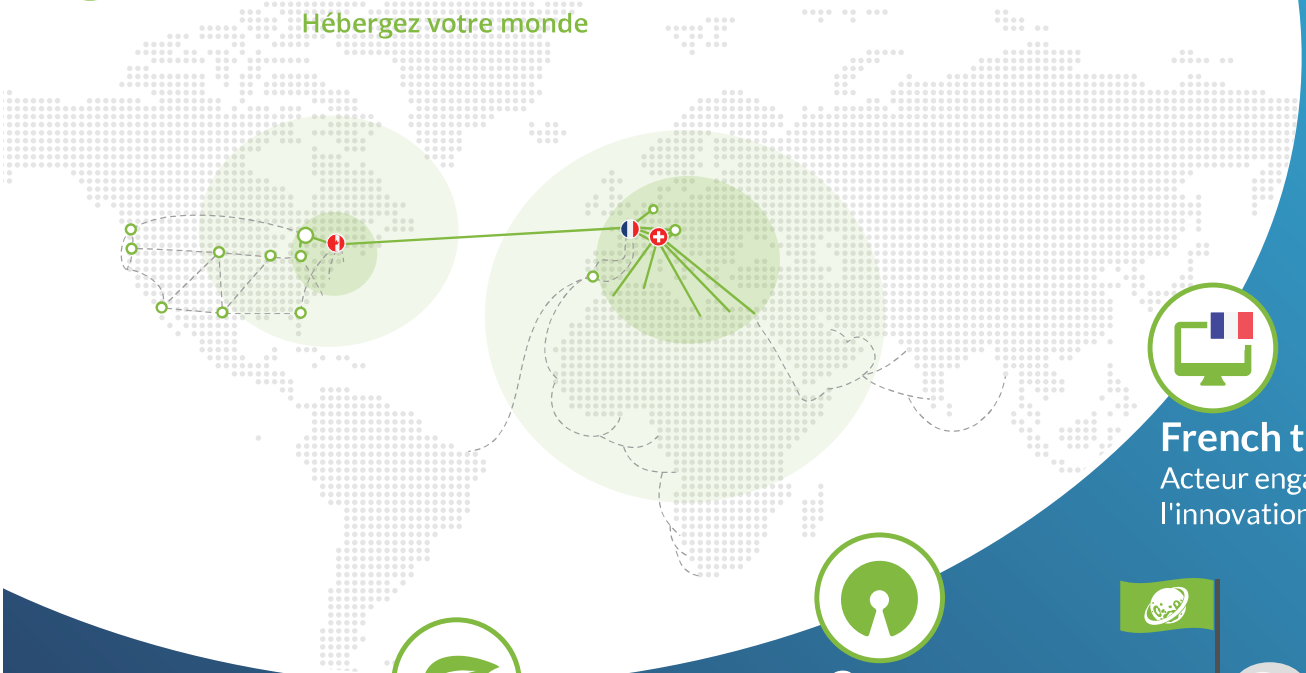
.fr

FONDATION afnic pour la solidarité numérique

Sous l'égide de Fondation de France

PlanetHoster®

Hébergez votre monde



French tech

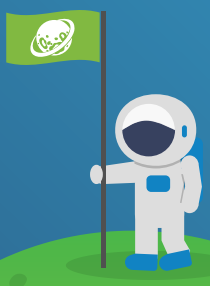
Acteur engagé pour l'innovation française.

Open source

Supporteur des technologies libres.

Eco-responsabilité

Actions durables pour l'environnement.



www.planethoster.com

AMPHI

9H00	**ACCUEIL**	Petit déjeuner networking Présentation de la journée, Discours introductifs
9H30	**TABLE RONDE** 75 MIN	Quelle gouvernance pour l'**ICANN** demain ? par **ISOC France**, avec le soutien d'**Euraleo**
11H00	**TABLE RONDE** 75MIN	**Achat-vente** d'actifs numériques, de gré-à-gré et aux enchères
12H15	**PAUSE DEJEUNER**	Buffet networking et sessions informelles
14H00	**TABLE RONDE** 75MIN	**Nouveaux enjeux** de la création de marque
15H15	**DETENTE & ATELIER**	Atelier : Cybersquatting & abus
16H15	**TABLE RONDE** 75MIN	Prochain round **ICANN**
17H00	**COCKTAIL**	Discussions networking

Accueil et détente à la Cafet

SALLE

9H00	**ACCUEIL**	Petit déjeuner networking Présentation de la journée, Discours introductifs
9H30	**TABLE RONDE** 75 MIN	Actualités **réglementaires** de la rentrée **2024**
11H00	**TABLE RONDE** 75MIN	Le **nommage Web3** (ENS) est-il utile ?
12H15	**PAUSE DEJEUNER**	Buffet networking et sessions informelles
14H00	**TABLE RONDE** 75MIN	**Google** : vers la fin d'un règne ?
15H15	**DETENTE & ATELIER**	Détente
16H15	**TABLE RONDE** 75MIN	**Mutation** des métiers du web et du SEO
17H00	**COCKTAIL**	Discussions networking

Accueil et détente à la Cafet

PROGRAMME DÉTAILLÉ

MATIN

9H00 - Accueil des participants

9H30 / 10h45 - Tables rondes

Quelle gouvernance pour l'ICANN demain ?
par ISOC France, avec le soutien d'Euraleo

Nicolas Chagny *ISOC France (modérateur) /* ***Sébastien Bachollet***
Président d'EURALO - ICANN

Actualités réglementaires de la rentrée 2024

- NIS2 : quelles obligations et quel périmètre pour la nouvelle réglementation européenne sur la cybersécurité ? Etre prêt pour son entrée en vigueur le 17 octobre 2024
- DNSSEC à un tournant : comment augmenter son adoption et est-ce vraiment une solution viable aux défis de cybersécurité modernes ?
- Gouvernance mondiale de l'internet : rôle et position de la France

11H00 / 12h15 - Tables rondes

Le nommage Web3 (ENS) est-il utile ?

- Avantages techniques des blockchains et du Web3 : un DNS via la Blockchain ?
- Ponts entre le Web3 et le Web avec les extensions du prochain round ICANN
- Difficultés liées à la duplicité des extensions
- Cybersquatting et anonymat par défaut du Web3

Achat-vente d'actifs numériques : noms de domaine, comptes de réseaux sociaux, sites Web, marques, réseaux sociaux, Web3

- Dernières données chiffrées commentées
- Quel impact de la dernière Update de Google (HCU) sur les noms de domaine expirés ?
- Tendances et stratégies gagnantes des grands acteurs du marché
- Atouts et limites des enchères

12h15 / 14h00 Déjeuner networking et ateliers

PROGRAMME DÉTAILLÉ

APRES-MIDI

14h00 / 15h15 - Tables rondes

Nouveaux enjeux de la création de marque

- Comment crée-t-on une marque ? Implications financières, juridiques et en termes de noms de domaine
- Quelle utilité des outils à base d'IA ?
- Le Nommage réinventé dans le Web3
- Derniers retours sur la lutte contre le cybersquatting

Google : vers la fin d'un règne ?

- Fuite massive d'info sur les algos de Google de mai 2024
- Procès antitrust et abus de position dominante
- Ratés successifs sur l'IA
- Concurrence sur le Search par Tiktok

15h15 / 16h - Détente networking et atelier

Cybersquatting & abus, *par Marie-Emmanuelle HAAS, avocate associée AGIL'IT & arbitre*

16h15 -17h30 Tables rondes

Prochain round ICANN

- Atouts des nTLD pour les marques, collectivités et entrepreneurs web
- Aspects techniques, organisationnels, contractuels, administratifs et financiers
- Les ambitions des acteurs du nommage Web3
- Stratégies gagnantes : analyse des best success et opportunités du moment

Mutation des métiers du web et du SEO

- Crise de la monétisation des éditeurs indépendants et de la presse
- Le search s'étend au-delà de Google
- Révolution de l'IA pour la production de contenus

17H30 - Buffet de clôture

LA LETTRE DES INCORPORELS

3 QUESTIONS À PIERRE BONIS, DIRECTEUR GÉNÉRAL DE L'AFNIC

En 2026, l'ICANN va lancer un nouveau round d'attribution d'extensions de domaine personnalisées, près de 15 ans après le précédent round de 2012. Pouvez-vous nous en expliquer l'importance ?

Pierre Bonis : Le prochain round d'attribution d'extensions de domaine de l'ICANN est une véritable opportunité pour les entreprises et les collectivités territoriales. En 2012, près de 2 000 candidatures avaient été déposées dans le monde et plus de 1 200 nouvelles extensions avaient été créées. En 2026, la réitération du processus va permettre à de nouvelles entités d'acquérir leur propre extension de premier niveau (TLD), comme un .marque ou un .région. Cela représente pour elles de fortes perspectives en termes de visibilité, de sécurité et de stratégie de marque, car elles pourront créer des espaces en ligne sécurisés, entièrement personnalisés, leur permettant de renforcer leur identité numérique, leur notoriété et la confiance des utilisateurs.

Comment l'Afnic prévoit-elle de les accompagner dans l'obtention de leur propre extension internet ?

Pierre Bonis : L'Afnic a mis en place une gamme complète de services pour accompagner les marques et les collectivités territoriales dans le processus complexe d'obtention d'une extension de domaine, et ce à chacune des étapes : de l'analyse préliminaire des besoins à la rédaction et la soumission de la candidature, et jusqu'à la gestion technique et administrative de l'extension une fois attribuée. L'Afnic est ainsi l'opérateur technique de registre n°1 en France, accompagnant près d'une quinzaine de nouvelles extensions internet génériques telles que le .leclerc pour les marques ou les .bzh et .alsace pour les territoires.

Quelles sont les attentes et défis que vous anticipez pour ce round de 2026 ?

Pierre Bonis : Nous anticipons une forte demande de la part des entreprises et des collectivités territoriales françaises, supérieure en volume à celle de 2012, et avec une bien meilleure préparation et des attentes plus précises. Les candidats arriveront plus informés sur les avantages d'avoir leur propre extension de domaine, avec des projets plus aboutis. Côté ICANN, le principal défi sera d'assurer un traitement juste et transparent de toutes les candidatures, tout en garantissant une évaluation rapide et efficace des aspects techniques, juridiques et opérationnels. L'objectif étant de tirer parti des enseignements de 2012 pour que ce nouveau round de 2026 soit toujours plus fluide, rapide, équitable et inclusif. ■

LA LETTRE DES INCORPORELS

TRANSPOSITION DE LA DIRECTIVE NIS2 : ENTRETIEN AVEC MARK FLEGG, DIRECTEUR PRODUIT CYBER CHEZ CSC

« Concrètement, NIS2 est une directive du Parlement européen visant à améliorer l'hygiène cyber au sein des États membres. C'est un peu comme le RGPD pour les technologies de l'information », explique Mark Flegg, Directeur Produit Cybersécurité chez CSC. Le résumé officiel de la Directive NIS2 préconise l'instauration d'« un niveau commun élevé de cybersécurité dans l'Union ». Cela implique l'adoption de stratégies nationales de cybersécurité, la mise en place d'autorités de gestion des crises, l'application de mesures de gestion des risques, la génération de rapports clairs et l'élaboration de plans d'action pour l'application de la législation.

« Il y a déjà eu des directives similaires qui recommandaient aux organisations d'adopter une meilleure hygiène cyber, mais il s'agissait davantage de recommandations. NIS2 est en réalité une évolution de ces directives, mais elle a cette fois été inscrite dans la loi. » Elle a été publiée en décembre 2022 et les États membres de l'UE ont jusqu'au 17 octobre 2024 pour décider de la manière dont ils l'intégreront dans la législation de leurs propres territoires.

En premier lieu, NIS2 concerne un ensemble de 10 secteurs que le Parlement Européen considère comme essentiels au fonctionnement de la société, à savoir : la sécurité économique, les communications électroniques, la finance, les fournisseurs de données, la santé, l'alimentation et l'eau, le droit et la sécurité, les transports, l'énergie et les services de protection. « Si cette liste peut sembler relativement restreinte, elle couvre en réalité toute personne ou organisation susceptible d'avoir un impact sur la société », ajoute Mark. En outre, bien qu'elle concerne uniquement les États membres de l'UE, elle s'applique également à toute organisation exerçant des activités dans l'UE, à l'instar du RGPD.

NIS2 : trois points d'action essentiels

Tout d'abord : « revoyez vos politiques de gestion du risque et assurez-vous qu'elles incluent les bureaux d'enregistrement de noms de domaine et les services DNS. Assurez-vous aussi que les organisations avec lesquelles vous travaillez sont conformes NIS2, sans quoi vous vous exposez à un risque de non-conformité », conseille Mark. Comme pour le RGPD, tout manquement entraîne des amendes salées : 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu. « Veillez également à disposer d'un DNS de niveau corporate et d'une redondance DNS », ajoute-t-il, « un plan B est nécessaire ! ».

Ensuite : « vérifiez la conformité de vos fournisseurs à la directive NIS2 et faites-le le plus tôt possible. » En matière de cybersécurité, la solidité d'une entreprise dépend de celle de son maillon le plus faible. Il est donc essentiel d'évaluer les

fournisseurs tiers de votre chaîne d'approvisionnement. Mark suggère d'évaluer les fournisseurs à l'aide d'un questionnaire d'évaluation des risques, de demander une déclaration de conformité NIS2 ou de mettre en place des accords de niveau de service (SLA).

Enfin : « mettez en place un CSIRT », préconise Mark. « Il s'agit d'une équipe d'intervention en cas d'incident de cybersécurité, qui assurera la liaison avec le CSIRT (Cybersecurity Incident Response Team) du gouvernement en cas d'incident. » Les organisations des secteurs concernés ne disposeront que de 24 heures pour signaler un incident ; aussi est-il essentiel de réunir cette équipe et de faire en sorte qu'elle soit sur la même longueur d'onde. « Il doit s'agir d'une équipe pluridisciplinaire couvrant la cybersécurité, l'IT, le droit, la gouvernance et la conformité. La cybersécurité est l'affaire de tous ; les représentants de chacun de ces domaines doivent non seulement être sensibilisés, mais aussi être prêts à agir », précise Mark.

A quelques mois de l'échéance, il est important que toutes les organisations concernées par la directive mettent en place des mesures irréprochables en matière de cybersécurité. ■

LA LETTRE DES INCORPORELS

PROTECTION DES MARQUES EN LIGNE À L'ÈRE DE LA DIRECTIVE NIS 2 : DÉFIS ET POTENTIELLES OPPORTUNITÉS

NATHALIE DREYFUS

Conseil en Propriété Industrielle et Conseil Européen en Marques, Expert agréé inter alia près le Centre d'arbitrage et de médiation de l'OMPI et le National Arbitration Forum (NAF), Expert judiciaire agréé par la Cour de cassation – Spécialité Marques
Dreyfus & associés, Paris
contact@dreyfus.fr

Le rapport d'Interisle Consulting Group du 9 août 2023 met en lumière une augmentation significative des attaques de phishing depuis mai 2020, soulignant ainsi une vulnérabilité croissante des marques en ligne.

La Directive NIS 2 vise à contrer cette menace en élargissant le champ d'application de la réglementation européenne à tous les acteurs du système de noms de domaine (DNS) et représente une révision substantielle des normes en matière de cybersécurité, susceptible d'avoir un impact conséquent sur la protection des marques en lignes.

Champ d'application volontairement large

La Directive NIS 2 élargit le cadre réglementaire de l'Union européenne en matière de cybersécurité. Elle remplace la notion d'opérateur de services essentiels (OSE) par celles d' « entités essentielles », qui fournissent des services critiques pour la société, et d'« entités importantes », fonction du nombre de salariés et du chiffre d'affaires.

Tous les fournisseurs de service DNS, les registres des noms de domaine de premier niveau, les entités fournissant des services d'enregistrement de noms de domaine, les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux sont également expressément visés.

Focus sur l'obligation d'information et les obligations de l'Article 28

L'Article 23 de la Directive NIS 2 impose aux entités essentielles et

importantes de notifier tout incident considéré comme important à l'ANSSI tels que les cas de phishing visant les employés de l'entreprise ou des partenaires, des escroqueries aux cryptomonnaies.

Une notification initiale est adressée à l'ANSSI dans les 24h suivant la prise de connaissance de l'incident. A la suite de cette dernière, une notification détaillée devra être envoyée, décrivant l'incident et son impact. Enfin, les entités essentielles et importantes seront tenues de rédiger un rapport complet dans le mois suivant l'incident.

Quant à l'Article 28 de la Directive NIS 2, il pourrait révolutionner la défense des marques en ligne, en imposant aux registres de noms de domaine de premier niveau et aux entités fournissant des services d'enregistrement de domaine de vérifier que les bases de données d'enregistrement des noms de domaine contiennent les informations nécessaires pour identifier et contacter les titulaires des noms de domaine et les points de contact qui gèrent les noms de domaine relevant des domaines de premier niveau.

Ces politiques et procédures devraient tenir compte, dans la mesure du possible, des normes élaborées par les structures de gouvernance multipartites au niveau international
La disponibilité et l'accessibilité en temps utile, des données relatives à l'enregistrement des noms de domaine pour les demandeurs d'accès légitimes sont essentielles pour prévenir et combattre les abus de DNS ainsi que pour prévenir et détecter les incidents et y réagir. Cette mesure pourrait potentiellement limiter les difficultés pour contacter les réservataires de noms de domaine frauduleux.

■

NDDCamp - Programme de la conférence & La lettre des incorporels
Pour proposer un article à paraître dans ce support, merci de contacter
Marc-Olivier BERNARD, Dir. de la publication
Tél. 06 20 10 00 56 • Email : mob@boischaut.fr
Pour devenir sponsor d'un événement NDDCamp, merci de contacter
Benjamin LOUIS, Dir. régie publicitaire et sponsoring
Tél. 06 12 45 66 48 • Email Benjamin@sparkling.alsace
Diffusé pendant dans conférences NDDCamp Paris et Strasbourg
Imprimé en Allemagne

Dreyfus
Intellectual Property in an Innovative World

Dreyfus &associés

de propriété intellectuelle à l'ère du numérique constituent des défis complexes qui ne cessent d'évoluer, nécessitant une expertise juridique spécialisée et réactive. Chez Dreyfus, notre expérience prolongée nous a enseigné que ces enjeux nécessitent une fusion unique de sagacité commerciale et de compréhension profonde des implications globales, bien au-delà des simples procédureslégalesettechniques.

Les actifs tels que les marques, les brevets, les dessins & modèles, et les noms de domaine sont des atouts précieux pour toute entreprise. Ils méritent une protection rigoureuse et une défense acharnée par des experts de premier plan. Notre équipe, armée d'une expertise pointue et d'une vision stratégique, s'engage à offrir une sécurité juridique maximale pour garantir que vos actifs numériques soient toujours un pas en avant dans cette ère numériqueenperpétuelleévolution.

Surveillance

IPweb®, Dreyfus utilise des technologies de pointe pour détecter et contrer efficacement toute atteinte à vos droits de propriété intellectuelle, comprenant des surveillances marques, noms de domaine,dénominationssocialeetdouanières.

Noms de domaine - Protection des marques en ligne

- Stratégies de conformité
- Surveillance via la plateforme Dreyfus IPweb®
- Usurpation d'identité,cybersquatting, phishing, contrefaçonetconcurrence déloyale
- Lettresdemiseendemeure,avis de suppressionet de blocage
- Gestionetauditsdesportefeuillesdenoms de domaine
- Arbitrageetlitigesrelatifsauxnomsde domaine(UDRP, DRPetautres procédures ADR)
- NouveauxgTLD:stratégieetétudes de faisabilité
- Disponibilitédesnoms de domaine, recherchesDNS, alertesdetitulaire, recherches inversées IP/DNS
- Récupérationetrachatdenoms de domaine
- Inscriptions, renouvellements, paramètres DNS

Marques - Dessins & modèles

- Recherches d'antériorités
- Dépôtetrenouvellementdemarqueset dessins & modèles
- Gestionde portefeuille de marqueset dessins & modèles
- Contrats :licences, copropriété, transactions et accordsdecoexistence
- Litigesdecontrefaçon,cybersquatting, concurrence déloyale
- Procéduresd'opposition, nullité, déchéance
- Mesures anti-piratage et anti-contrefaçon
- Surveillance et saisies douanières
- Visibilitécomplèteduportefeuille24h/24, 7j/7 sur Dreyfus IPweb®

contact@dreyfus.fr
(+33) 1 44 70 07 04

AWARDS

WWL · IP STARS from Managing IP · WTR 1000 · DÉCIDEURS MAGAZINE

Gandi Corporate Services

Disponible
Fiable
Transparent

Votre partenaire Expert en sécurité et noms de domaine au service des entreprises

Disponibilité

- Une anticipation des besoins
- Un service 24/24h et 7/7j
- Une équipe dédiée multilingue présente sur 3 continents

Fiabilité

- Une infrastructure robuste et sécurisée depuis 20 ans
- Un DNS parmi les 10 meilleures offres du marché
- Un accompagnement sans faille lors du transfert

Transparence

- Des tarifs non cachés et justes
- Une offre de services à la carte
- Une réduction significative des coûts

www.gandi.net/corporate

LA LETTRE DES INCORPORELS

HARO SUR INTERNET, L'IA ET LA 6G AUGMENTENT LE POTENTIEL DES ABUS !

En abaissant le niveau d'expertise nécessaire pour créer des abus et en démultipliant les impacts, la généralisation de l'IA générative et le déploiement de la 6G sont porteurs de risques.

ARNAUD FRANQUINET

Chief Executive Officer de Gandi
arnaud.franquinet@gandi.net

Construit initialement pour être un réseau résilient d'échanges d'information en cas d'attaque atomique, internet s'est depuis considérablement émancipé de son ambition première et a flirté, au moins au début de son ouverture au grand public, avec la double utopie libertaire d'un accès ouvert à tous et d'une autorégulation des acteurs, forme de système anarchique au sens propre du terme : accès gratuit à toute l'information, échanges bienveillants de pair à pair d'information.

Le développement de l'internet s'est basé sur ces idées simples. Son succès l'a dévié de ses idéaux : le nombre toujours croissant de transactions financières a attisé les appétits. Internet n'était pas prévu pour être à la base un espace d'échanges économiques, le droit et la réglementation y sont donc de faible portée. Cet espace, certes toujours ouvert, s'apparente de plus à une jungle.

Les entreprises présentes sur le web ont donc appris tant bien que mal à la fois à sécuriser leur espace transactionnel avec leurs clients/prospects, qui n'est pas que financier (pensons aux datas) et leurs marques, qui, utilisées à leur insu, peut provoquer des dommages considérables.

Mais le développement technologique augmente la vulnérabilité déjà intrinsèquement forte des entreprises sur le web, au moins sur deux aspects :

• le passage de la 5G à la 6G qui promet une connectivité démultipliée et ultra présente : le volume des données va s'accroitre et les points de contact se multiplier avec l'Internet des objets (IoT) mais c'est aussi la possibilité pour des attaquants de démultiplier leur force plus facilement.

• l'émergence de l'intelligence artificielle (IA) favorise la professionnalisation de la cybercriminalité en en démocratisant l'accès et en déployant son potentiel (en nombre et en qualité).

Pour contrer les menaces ouvertes par ces évolutions, un solide mot de passe et une méfiance pour les pièces jointes ne suffisent. Les marques doivent s'armer pour surveiller, identifier et répondre à ces attaques devenues quotidiennes dans certains secteurs d'activité. Mais cette surveillance ne suffit plus, il faut pouvoir anticiper et agir avant le mal.

Anticiper et créer des « domaines de confiance »

Aujourd'hui, les professionnels et les chercheurs travaillant sur ces questions alertent sur les nouveaux dangers d'Internet et développent les outils pour que le Net soit une zone de sécurité plus que de menaces.
L'idée est de pouvoir identifier des signes annonciateurs d'un mauvais usage d'un nom sur l'internet. Il s'agit de dispositifs avancés de surveillance des enregistrements de mots sensibles, de noms de domaine couplés à une sécurisation des DNS, des protocoles d'identification lors de chaque échange de mails ou d'information et la possibilité de mise en place de frontières virtuelles pour créer des "domaines de confiance" pilotés par les entreprises. La solution d'un tld « .marque » propriété de l'entreprise est une des réponses efficaces.
Les entreprises n'ont pas d'autre choix que d'anticiper et d'agir en amont de la menace mais aussi dépasser leur seule sécurité pour intégrer celle de leurs clients/prospects en leur offrant un ''domaine de confiance''. Ce sont les conditions sine qua non pour continuer à se développer sur internet. L'identité en ligne n'a jamais été autant un actif stratégique pour évoluer dans notre monde numérisé, mais surement pas dans une définition passive.

LA LETTRE DES INCORPORELS

POURQUOI LE GROUPE EASY STORE A CHOISI LWS.FR POUR SON HÉBERGEMENT WEB & E-MAIL

LWS.fr
10 rue Penthièvre 75008 Paris France
01 77 62 30 03

LWS : Bonjour Nicolas, merci de prendre le temps de partager votre expérience avec nous. Pouvez-vous nous expliquer pourquoi vous avez choisi LWS pour votre hébergement web & e-mail ?

Groupe Easy Store : Bien sûr ! En tant que dirigeant d'une entreprise, j'avais des besoins très spécifiques pour mon hébergement e-mail. Je cherchais avant tout une solution offrant 5 Go de stockage par boîte mail. C'était essentiel pour gérer efficacement tous les échanges avec mes clients et partenaires, sans avoir à supprimer constamment des e-mails pour libérer de l'espace.

LWS : Cela semble être un besoin crucial pour de nombreuses entreprises. Qu'est-ce qui vous a convaincu de choisir LWS parmi tant d'autres fournisseurs ?

Groupe Easy Store : Ce qui m'a vraiment séduit, c'est le rapport qualité-prix que propose LWS. J'avais besoin d'un service performant sans un budget qui explose. Avec LWS, j'ai trouvé exactement ce que je cherchais : un hébergement web & e-mail fiable et performant, à un tarif qui reste abordable pour une entreprise comme la mienne. D'autres fournisseurs offraient des services similaires, mais à des prix bien plus élevés.

LWS : C'est formidable d'entendre que nous avons pu répondre à vos attentes ! Qu'avez-vous pensé du support technique ?

Groupe Easy Store : Pour moi, c'était un critère décisif. Le fait que les techniciens soient basés en France a vraiment fait la différence. J'ai eu besoin d'aide à quelques reprises, et j'ai toujours été pris en charge rapidement et efficacement. C'est rassurant de savoir que vous pouvez compter sur un support local, qui comprend vos besoins et peut vous répondre en français.

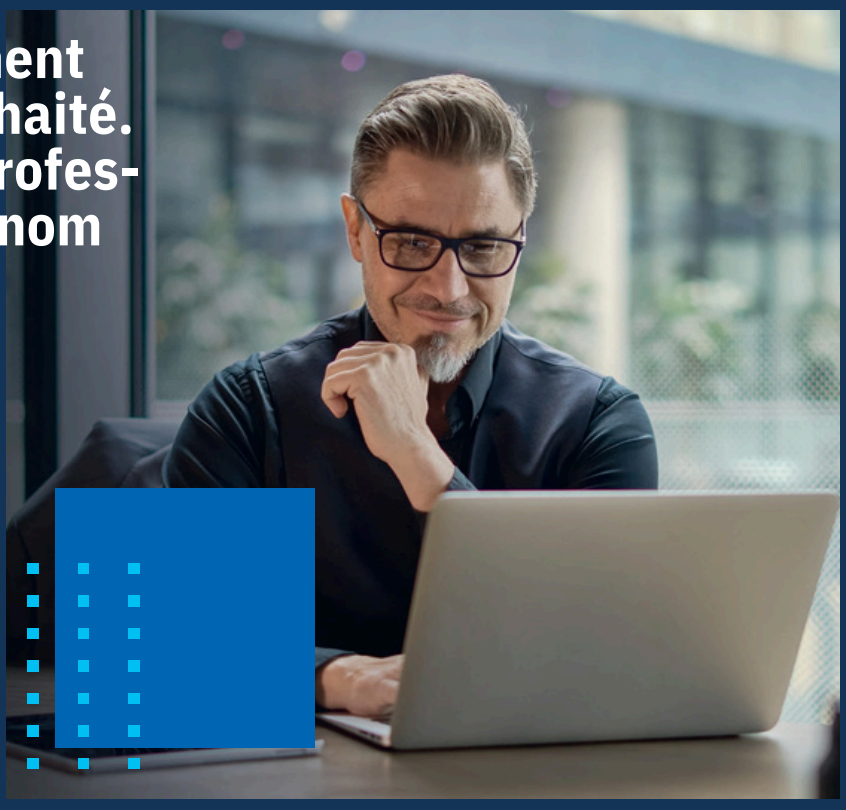
LWS : En conclusion, êtes-vous satisfait de votre choix ?

Groupe Easy Store : Absolument. LWS a su répondre à tous mes besoins : un stockage e-mail généreux, un service abordable, et un support technique de qualité. Je suis très satisfait et je recommande LWS à toute entreprise cherchant une solution d'hébergement web et e-mail fiable.

LWS : Merci beaucoup pour ce témoignage. Nous sommes ravis de vous accompagner et de contribuer au succès de votre entreprise.

■

Sécurisez tout simplement le nom de domaine souhaité. Grace à notre service professionnel de courtage en nom de domaine.



Vous êtes à la recherche du nom de domaine idéal pour votre présence en ligne? Nous le trouverons pour vous! Notre équipe de courtiers expérimentés se charge d'obtenir le domaine de vos rêves, même s'il est déjà prix. Demandez maintenant le nom de domaine souhaité:

www.sedo.com/
ser vice -de -courtage

sedo

LWS.FR

Ligne Web Services

Boostez votre présence en ligne !

Offre Hébergement Web + Nom de domaine OFFERT

.fr .com .site .store .be...

- Créateur de site facile
- Mails pro & Certificat SSL

Dès ~~2,99~~ **1,49** €/mois -50%

DÉCOUVREZ BIMI (BRAND INDICATORS FOR MESSAGE IDENTIFICATION)

BIMI (« Brand Indicators for Message Identification ») est une initiative en matière de sécurité des emails. Elle permet aux entreprises de montrer leur logo dans les courriels qu'elles envoient à leurs clients et prospects. Cette technologie vise à renforcer la reconnaissance de la marque et à améliorer la confiance des utilisateurs envers les e-mails qu'ils reçoivent.

JEAN-FRANÇOIS POUSSARD

Président, Fondateur Associé de Solidnames
jf.poussard@solidnames.fr

Comment fonctionne BIMI ?

Pour qu'une entreprise puisse utiliser BIMI, elle doit d'abord s'assurer que ses e-mails sont correctement authentifiés. Cela implique l'utilisation de protocoles comme DMARC (« Domain-based Message Authentication, Reporting & Conformance »), qui aide à prévenir les attaques de phishing et à garantir que les e-mails proviennent bien du domaine qu'ils prétendent représenter. Une fois que DMARC est correctement configuré, l'entreprise peut ajouter un enregistrement BIMI à son DNS (« Domain Name System »).

L'enregistrement BIMI contient un lien vers le logo de l'entreprise, qui doit être au format SVG (« Scalable Vector Graphics ») et respecter certaines normes de sécurité. Lorsque les fournisseurs de services de messagerie, comme Gmail ou Yahoo Mail, reçoivent un e-mail authentifié avec DMARC et BIMI, ils peuvent afficher le logo de l'entreprise à côté du message dans la boîte de réception de l'utilisateur.

La mise en place de BIMI elle-même est relativement peu coûteuse. En effet, elle repose principalement sur la création et le déploiement d'un enregistrement DNS qui pointe vers un logo au format approprié.

Toutefois, le coût augmente en fonction de la nécessité d'obtenir un certificat VMC (« Verified Mark Certificate »). Il est requis pour afficher votre logo dans certains services de messagerie, comme Gmail. L'obtention d'un VMC implique généralement des frais et une vérification de la marque, ce qui peut représenter un investissement significatif.

En règle générale, il faut compter 1 500 € HT / an pour obtenir un certificat VMC.

Les avantages de BIMI

1. Renforcement de la confiance : En affichant le logo de l'entreprise à côté des e-mails, BIMI aide à renforcer la confiance des utilisateurs envers les messages qu'ils reçoivent. Cela peut réduire les risques de phishing et d'autres types de fraudes par e-mail comme l' « email spoofing ».

2. Reconnaissance de la marque : Le logo de l'entreprise est un élément visuel puissant qui peut aider à améliorer la reconnaissance de la marque. Les utilisateurs sont plus susceptibles de reconnaître et de faire confiance à un e-mail provenant d'une marque qu'ils connaissent visuellement.

3. Amélioration de l'expérience utilisateur : En rendant les e-mails plus visuellement attrayants et en aidant les utilisateurs à identifier rapidement les messages de marques de confiance, BIMI peut améliorer l'expérience globale de l'utilisateur.

4. Différenciation : Les entreprises qui adoptent BIMI peuvent se différencier de leurs concurrents en montrant qu'elles prennent la sécurité et l'authenticité de leurs communications au sérieux.

L'avenir de BIMI dans l'écosystème de l'email

Bien que BIMI offre de nombreux avantages, il y a aussi des défis à surmonter. La mise en œuvre de DMARC peut être complexe et nécessite une compréhension approfondie des protocoles d'authentification des e-mails. De plus, tous les fournisseurs de services de messagerie ne prennent pas encore en charge BIMI, ce qui peut limiter son efficacité.

A mesure que les consommateurs deviennent plus conscients des avantages de BIMI, leur attente envers les entreprises d'utiliser de telles mesures de sécurité augmentent. Elle pousse alors davantage le marché vers son adoption.

Dans cet environnement en constante évolution, rester à la pointe de la technologie de l'email et adopter des normes comme BIMI est crucial pour garantir que les communications de marque restent sécurisées, authentiques et efficaces. ■

NOMS DE DOMAINE : UN ACTIF IMMATÉRIEL QU'IL FAUT PROTÉGER

Votre nom de domaine est le point d'accès à votre business en ligne. Pourtant, il est souvent mal considéré et relayé à un simple élément technique. Voyons un peu pourquoi et comment vous devriez prendre plus de précautions.

SÉBASTIEN ALMIRON

Directeur Commercial
& Marketing, Netim
sales@netim.com

Nom de domaine, la pierre angulaire de votre business

Votre nom de domaine est votre point d'accès principal : il doit donc recevoir une attention toute particulière.

C'est donc un élément de votre business qui doit être chouchouté et surtout pas laissé au hasard !

Il est également essentiel dès le départ de la création de votre projet de déposer votre nom de domaine en même temps que votre nom de marque pour éviter tout soucis de disponibilité par la suite.

Prendre soin de son nom de domaine passe également par la surveillance des profils de liens qui renvoient vers le site internet du nom de domaine. Des backlinks toxiques peuvent vraiment heurter le domaine et miner le référencement...

D'un point de vue financier : on le répète régulièrement, mais votre nom de domaine ne doit pas être une charge mais bien **un actif immatériel** qui va venir valoriser votre entreprise.

Quels sont les principaux risques et comment s'en prémunir ?

Vous l'aurez sans doute bien compris : il est d'une importance capitale d'accroitre le niveau de votre nom de domaine.

Voici quelques pistes pour vous aider :

- Ne pas choisir un registrar low-cost basé dans un paradis fiscal juste pour économiser 2 euros par an. Si vous avez compris que votre nom de domaine avait une réelle valeur, ne prenez pas ce risque !
- Définir un mot de passe fort pour votre compte client : c'est très basique mais si important ! Facilité avec les gestionnaires de mots de passe, optez pour une combinaison longue et complexe ce qui le rendra difficile à compromettre. Tout comme un sous-vêtement, un mot de passe ne se passe pas et on le change régulièrement
- Activation d'une méthode de double authentification (2FA) : c'est la méthode la plus sûre car elle requiert votre application pour générer le code permettant de passer la vérification.
- Activation de l'option registry block : cette option a un coût mais bloque toutes les opérations critiques sur votre nom de domaine (changement de DNS, de contacts, suppression et transfert).

Que faire des noms de domaine inutilisés ?

Vous avez enregistré des noms de domaine pour des projets, des marques ou produits qui ne sont plus d'actualité ? Voici 3 options :

- Conservation : pour la bonne et simple raison qu'ils pourraient encore vous servir dans le futur et face à la complexité de trouver des noms intéressants et disponibles, autant conserver ceux que vous possédez déjà.
- Suppression : après avoir fait des vérifications d'un point de vue SEO afin de vous être assuré que personne ne pourra récupérera vos liens ou votre trafic. Cette action étant irréversible, il est très important de bien étudier les risques et partir du principe qu'un tiers pourrait enregistrer votre nom de domaine une fois ce dernier libéré. Plus un nom de domaine est ancien, et plus il peut avoir de la valeur : il faut donc bien réfléchir.
- Les mettre en vente : ils ont eu de la valeur pour vous, donc potentiellement ils peuvent intéresser d'autres personnes et donc vous rapporter de l'argent. Il est possible de mettre en vente vos noms de domaine via une plateforme dédiée telle que Sedo (Netim permet de mettre en vente vos noms de domaine directement depuis Netim Direct). Il est également possible de revendre les marques associées aux noms de domaine.

LA LETTRE DES INCORPORELS

DES EXTENSIONS WEB3 DANS LE DNS À L'OCCASION DU PROCHAIN ROUND D'OUVERTURE DE L'ICANN : MARIAGE DE LA CARPE ET DU LAPIN OU MARIAGE DE RAISON ?

Portrait grand angle d'une famille en composition - le regard du juriste en propriété intellectuelle.

FABRICE BIRCKER

Conseil en Propriété Industrielle, Responsable Plasseraud IP Internet & Data

Comme les noms de domaine traditionnels, les noms de domaine dans la blockchain (ci-après indifféremment dénommés noms de domaine Web3, noms de domaine NFT ou encore domaines Web3 / NFT) répondent au besoin de rendre la localisation de ressources en ligne humainement communicable. Cependant, ils évoluent dans des environnements philosophiques, réglementaires et techniques très différents.

Ainsi, et pêle-mêle, les domaines NFT se caractérisent notamment par l'absence d'autorité centrale régulatrice, la possibilité de réservations à vie dans certaines extensions, l'absence de mécanisme de résolution extrajudiciaire des litiges, la possibilité de diriger vers des contenus qualifiés d'incensurables, l'absence d'équivalent au *Whols*, ou encore la capacité à être liés à des *smart contracts* lesquels peuvent entrainer des transactions irréversibles.

Pour pousser à peine le trait, à l'ordre réglementaire institutionnel établi auquel appartiennent les noms de domaine DNS, les acteurs du nommage Web3 répondent par la maxime code is law qui ne semble fixer de limite que dans le bon vouloir des « registres » et des détenteurs de domaines NFT.

Ce sentiment de liberté exacerbée a immanquablement conduit à des abus. La visite d'une place de marché de NFT montre que les réservations spéculatives de domaines Web3 sont légion.

Bien entendu, les noms de domaine NFT ne sont pas hors-le-droit, et les titulaires de marques estimant subir des atteintes ne sont pas dépourvus de moyens d'action. Toutefois, souvent ces moyens ne présentent pas la même souplesse, la même rapidité et les mêmes coûts que ceux qui ont été développés pour connaître des abus commis dans le DNS.

Dans ce contexte, le juriste en PI en charge de la protection de signes distinctifs portera un regard intéressé sur les projets de plus en plus nombreux consistant à lier des domaine NFT aux noms de domaine traditionnels. Par exemple :

- en mars 2023, le registre du **.art** annonçait la possibilité de créer des noms de domaine NFT « jumeaux » de noms de domaine DNS,
- début 2024, l'extension **.box** a été lancée, avec pour vocation d'offrir des ponts entre le DNS et le Web3, également au moyen de noms de domaine NFT / DNS « jumeaux »,
- depuis que le prochain round d'ouverture de l'ICANN se précise pour 2026, plusieurs acteurs des domaine NFT ont manifesté leur intention de candidater pour pouvoir proposer dans le DNS des extensions correspondant à celles qu'ils opèrent dans le Web3. Tel est notamment le cas des **.blockchain, .ape, .metropolis** ou encore **.pudgy**.

Les noms de domaine NFT, pour relever par nature de la blockchain, portent dans leurs gênes une volonté d'indépendance vis-à-vis des organes officiels et de toute forme de tiers de confiance. Or, ces projets conduisent leurs porteurs à soumettre leurs noms de domaine, à tout le moins ceux enregistrés dans le DNS, au contrôle d'autorités tierces.

Aussi, selon les évolutions que prendront ces projets, le juriste pourrait y voir une aubaine susceptible de participer au respect et à la mise en œuvre des droits :

- le pseudonymat pourrait être malmené par l'obligation pour les titulaires de figurer dans une base de données WhoIs, et par la prochaine entrée en vigueur de la réglementation issue de la directive NIS 2 qui fait obligation aux bureaux d'enregistrement de noms de domaine dans le DNS de tenir des base de données complètes et fiables permettant d'identifier et de contacter les titulaires. Partant, l'identification du titulaire du nom de domaine DNS pourrait conduire à celle du détenteur du domaine NFT correspondant,
- le « volet DNS » du domaine NFT sera justiciable de l'UDRP et de l'URS, ce qui facilitera le traitement des atteintes et participera à limiter leur effets, d'autant que certains registres (comme celui du .box) lient déjà le sort du domaine NFT au nom de domaine correspondant en cas de transfert ou de disparition de celui-ci. Espérons que ce sort lié se trouve généralisé.

En outre, et c'est déjà le cas, les contenus illicites mis en ligne devraient pouvoir être traités via le DSA, ce dernier visant indifféremment tous les hébergeurs, peu importe qu'ils recourent à des serveurs centralisés ou distribués lesquels sont parfois qualifiés d'incensurables.

Incidemment, et également sur le terrain du DSA, il devient tentant de qualifier de professionnels les spéculateurs détenant des centaines de noms de domaine NFT, afin de contraindre les plateformes sur lesquelles ils sont mis en vente à assurer l'identification des vendeurs.

Voir une partie des noms de domaine Web3 susceptibles d'être assujettis à une réglementation donnant prise sur eux à autre que le détenteur du wallet qui les contient, a de quoi surprendre tant est grande la rupture par rapport à l'esprit libertaire dans lequel ils ont été conçus.

Sans doute certaines entités proposant des domaines Web3 sont-elles conscientes qu'en l'état leur activité n'est adoptée que de manière confidentielle et peut susciter une certaine méfiance.

Or, la soumission aux règles de la société civile est un passage nécessaire pour faire naître la confiance indispensable à la popularisation. Cette recherche de confiance est d'autant plus fondamentale que certains acteurs aspirent à faire des domaines NFT les véhicules de l'identité en ligne.

Par ailleurs, si surprenant puisse-t-il paraître de voir des opérateurs de domaines NFT prendre un chemin pouvant les conduire à se soumettre à une réglementation « hors du code », il n'en reste pas moins qu'agir de la sorte présente l'avantage d'adhérer volontairement à des règles de droit connues et prévisibles.

A défaut, sans doute l'économie des domaines Web3 accentuerait-elle plus encore le risque de voir le Législateur s'emparer du sujet pour produire un corpus réglementaire nouveau et susceptible d'être considéré comme trop contraignant. En effet, les développements de la réglementation en matière de cryptomonnaies et de smart contracts liés à la mise à disposition de données en matière de produits connectés, montrent que la puissance publique ne reste pas longtemps sans réagir lorsque des acteurs économiques s'affranchissent par trop des règles ou sont sources de risques pour les consommateurs ou la société.

Pourtant, quitte à devoir évoluer dans un cadre réglementaire, autant le choisir dans la mesure du possible. D'aucuns déploreront un reniement de l'esprit de liberté du Web3. D'autres verront dans ce mouvement de rapprochement des domaines NFT vers les noms de domaine traditionnels, un premier pas pouvant mener à une adoption plus large d'une technologie disruptive aux avantages indéniables, mais encore marginalisée. Parfois pour se démarquer, il faut savoir rentrer dans le rang. ■

SAFEBRANDS DEVIENT BRANDSHELTER

En tant que membre de Team Internet Group, SafeBrands passe à l'étape suivante et change de nom. La société française situé à Marseille, qui a intégré Team Internet Group (anciennement CentralNic Group) en 2021, annonce une nouvelle réjouissante au NDDcamp : SafeBrands devient BrandShelter.

Il ne s'agit pas d'un simple changement de nom pour SafeBrands ; c'est l'aboutissement d'une transformation qui a commencé il y a trois ans, pour fournir aux clients un service plus large, plus complet et plus résistant grâce à la fusion avec la marque de Team Internet, BrandShelter.

L'aventure de Safebrand a commencé il y a plus de vingt ans sous le nom de Planète Marseille. Au fil du temps, les fondateurs Frédéric Guillemaut et Charles Tiné ont fait évoluer leur offre de services pour répondre aux défis de l'ère numérique, devenant Mailclub puis SafeBrands. « Chacune de ces transitions a été une étape soigneusement planifiée qui nous a rapprochés de notre objectif de fournir à nos clients la meilleure protection et le meilleur soutien pour leur identité de marque », déclare aujourd'hui Frédéric Guillemaut.

Aujourd'hui, trois ans après la dernière transformation, il est temps de passer à l'étape suivante : fusionner avec BrandShelter pour rendre les services encore plus robustes et polyvalents. BrandShelter, une marque de Key-Systems GmbH, a été lancée en Allemagne en 2009 et fait partie du groupe Team Internet depuis 2018. BrandShelter se spécialise dans l'autonomisation des entreprises du monde entier avec des solutions personnalisées de protection de marque, de surveillance et de gestion de noms de domaine.

« Notre engagement envers nos précieux clients reste inchangé. Nos équipes resteront en France pour continuer à vous servir en français, pendant les horaires européens, et avec le même dévouement que vous attendez », souligne Frédéric. « Cependant, en collaborant avec des équipes mondiales et spécialisées, nous pouvons désormais offrir des outils et des ressources qui vont bien au-delà de ce qui était disponible auparavant.

Le portail évolue en permanence pour répondre aux besoins des clients. Il offre davantage de fonctionnalités, une vue d'ensemble du portefeuille et une plus grande liberté dans le transfert des droits aux utilisateurs. L'automatisation et l'intégration sont des éléments clés de notre nouvelle offre. L'objectif n'est pas seulement de fournir aux clients des outils et des ressources, mais aussi d'être un partenaire sur lequel ils peuvent compter. L'équipe est fière d'avoir gagné la confiance de ses clients au fil des années et s'engage à la conserver.

Célébrez cette nouvelle étape avec nous et venez nous rendre visite pour en savoir plus.

SAFEBRANDS
Protecting brands in the digital era

BrandShelter

SafeBrands devient BrandShelter!

Célébration d'une nouvelle ère dans la protection des marques en ligne

- **Un héritage d'excellence:** Plus de 25 ans d'expertise en protection d'identité numérique
- **Services complets:** Stratégie globale d'optimisation de protection et de défense
- **Une dimension mondiale, une expertise locale:** Nous vous servons en français, avec des heures de travail et un dévouement à l'échelle européenne
- **Outils de pointe:** Automatisation avancée, intégration transparente, contrôle de votre portefeuille et de votre présence

Découvrez comment BrandShelter peut propulser la protection de votre marque vers de nouveaux sommets

Venez nous dire bonjour

LE CHEMIN VERS LE NOM DE DOMAINE DE VOS RÊVES

Pour réussir en ligne, un bon nom de domaine est indispensable. Cependant, dès que l'on commence à chercher un domaine approprié, on se rend vite compte que presque tous les noms de premier plan sont déjà pris. Cela s'applique désormais à tous les domaines de premier niveau établis, y compris les domaines en fr. Quelles possibilités restent alors aux entreprises pour obtenir un domaine en .fr qui répond à tous les besoins et objectifs d'une présence en ligne réussie ?

Dans de tels cas, les entreprises et les marques mondialement connues font appel au service de courtage en nom de domaine. Ils mandatent des experts courtiers pour obtenir le domaine désiré. L'avantage pour les acheteurs, est qu'ils peuvent rester anonymes. Autre avantage représente le support linguistique. Pour les domaines en .fr : dans près de 90 % des cas, les parties contractantes ne se trouvent pas dans le même pays ou ne parlent pas la même langue. En particulier, les entreprises en croissance en provenance de l'étranger, cherchant à s'internationaliser et à s'implanter sur le marché français, sont confrontées à cette barrière linguistique. Elles réalisent qu'elles ne peuvent pas progresser sans l'extension correspondante pour gagner la confiance des utilisateurs dans leur marque et augmenter le trafic vers leur site web. Plus de 40 % de tous les noms de domaines enregistrés en France sont des domaines en .fr, ce qui témoigne de la popularité de l'extension.

Voici quelques exemples d'entreprises qui ont investi dans des domaines pour renforcer leurs actions marketing et l'image de leur marque en passant par le service de courtage en nom de domaine de Sedo:

1. Entreprises dont la marque repose sur un terme générique : dentiste.fr, bistrot.fr
2. Marques étrangères connues qui se sont établies en France : action.fr, justfab.fr, homify.fr
3. PME ayant besoin de domaines courts et facilement mémorisables: qmt.fr, tel.fr

Un courtier négocie non seulement dans la langue du pays respectif, mais possède également une compétence interculturelle qui contribue à conclure des négociations réussies !

■

NOTES

NOTES

NOTES

NOTES

BOISCHAUT
MAISON DE VENTES AUX ENCHÈRES

Depuis octobre 2023

Ventes aux enchères
de noms de domaines et de sites Internet

en continu sur

INTERENCHERES ONLINE

Ventes mensuelles thématiques

Boissons - CHR - Transport - Bâtiment - Santé - Tourisme

Pour inclure des noms de domaines ou des sites Internet dans nos prochaines ventes

Contacter Marc-Olivier Bernard
06 20 10 00 56 mob@boischaut.fr

Siège
92 rue d'Angiviller
78120 Rambouillet

Salle de vente
30 rue Delambre
75014 Paris

Web : https://boischaut.fr – Tél : 01 61 08 61 00 - RCS Nanterre B 442 913 661 – Agrément 2002-363

SPONSORS

MERCI POUR LEUR CONTRIBUTION

SPONSORS OR

sedo
Buy. Park. Sell. Domains

gandi.net

csc

afnic
Internet made in France

Dreyfus
Intellectual Property in an Innovative World

netim

SCAN AVOCATS

PlanetHoster
Host Your World

SAFEBRANDS
Noms de domaine • Identité digitale • Hébergement • Certificats

LWS .FR

SPONSORS ARGENT

solid NAMES

DOTMARKET.EU
Ouvrir un monde d'opportunités digitales

KifDom

Plasseraud
INTELLECTUAL PROPERTY

inéolab

PARTENAIRES

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

[N] FRANCE NUM

SEO CAMP
L'ASSOCIATION DU RÉFÉRENCEMENT

ECOLE DSP

Internet Society
France Chapter