



Un guide stratégique pour l'abandon d'un nom de domaine :

Pause – Analyse – Action





Un guide stratégique pour l'abandon d'un nom de domaine :



Pause



Analyse



Action

CSC déploie sa politique relative à la stratégie pour l'abandon d'un nom de domaine afin d'assurer la sécurité et la conformité des actifs les plus importants de nos clients. Si de nombreuses entreprises prennent le temps d'examiner quels noms de domaine elles souhaitent abandonner, elles ne disposent pas toujours de toutes les informations requises pour prendre la bonne décision. Chez CSC, il est de notre responsabilité de veiller à ce que vous compreniez les options dont vous disposez, ainsi que les risques de sécurité auxquels vous êtes exposés.

Pour vous aider à prendre une décision complexe, nous avons conçu un plan stratégique en trois étapes : **Pause – Analyse – Action.**





PAUSE

Nous souhaitons nous assurer que vous ne procédez pas à un abandon de noms de domaine trop précipitamment. Lorsque les entreprises abandonnent rapidement leurs noms de domaine, et notamment lorsque l'abandon se fait par lots, des noms de domaine importants sont invariablement supprimés accidentellement. Nous vous encourageons à prendre le temps de bien réfléchir aux noms de domaine que vous souhaiteriez abandonner, et aux risques potentiels liés aux abandons erronés.

Veillez à ce que votre prestataire de noms de domaine réalise une analyse détaillée avant d'abandonner un nom de domaine. CSC contrôle en permanence tout les abandons pour identifier les menaces potentielles et réduire les risques.

Avant d'abandonner un nom de domaine, assurez-vous d'avoir bien conscience de tous les risques potentiels :

- ✓ **Phishing** : une attaque de phishing utilisant un nom de domaine gagne en efficacité si ce nom contient votre marque.
- ✓ **Abus de marque** : les noms de domaine peuvent être utilisés pour rediriger vos clients vers un site web tiers frauduleux.
- ✓ **Récupération de nom de domaine** : au cas où le titulaire de la marque aurait de nouveau besoin du nom, il est plus rapide de l'acquérir plutôt que de perdre du temps en procédure légale
- ✓ **Collecte d'adresses e-mail (harvesting)** : les fraudeurs se contentent de réactiver la messagerie pour avoir accès à tous les e-mails envoyés à ces adresses.
- ✓ **Pannes de site web et de messagerie** : certains noms de domaine servent uniquement à héberger un sous-domaine ou sont simplement utilisés pour la messagerie
- ✓ **Fraude** : certains noms de domaine sont réactivés par des escrocs qui recueillent les coordonnées de carte bancaire ou utilisent l'accès au système pour réinitialiser d'anciens comptes de messagerie
- ✓ **Perte de revenus** : votre portefeuille contient des actifs de valeur qui peuvent être revendus



ANALYSE

CSC recommande de procéder à une analyse détaillée complète du nom de domaine afin de s'assurer qu'aucune de ses caractéristiques ne présente encore de la valeur pour vous.

Une révision détaillée inclut les éléments suivants :

Analyse d'impact par zone

- ✓ Enregistrements MX
- ✓ DNSSEC : extensions de sécurité des DNS
- ✓ DMARC : authentification des messages par rapport aux noms de domaine, génération de rapports et conformité
- ✓ Enregistrements TXT
- ✓ SPF (Sender Policy Framework) : norme de vérification du nom de domaine de l'expéditeur d'un e-mail
- ✓ DKIM (Domainkeys Identified Mail) : norme d'authentification fiable du nom de domaine de l'expéditeur d'un courrier électronique
- ✓ Certificats numériques actifs

Vérifications liées à la marque

- ✓ Correspondances des marques
- ✓ Portefeuille de marques commerciales
- ✓ Extension (pays)

Analyse du trafic

- ✓ Requêtes DNS
- ✓ Classement Alexa

Analyse de valeur

- ✓ Valeur du nom de domaine

Ces valeurs sont ensuite ventilées selon trois catégories : examen recommandé, examen facultatif ou aucune action requise. Une fois l'analyse terminée, vous pouvez prendre une décision plus informée concernant les noms de domaine que vous souhaitez abandonner.





ACTION

Une fois l'analyse terminée, nous recommandons de procéder à quelques démarches supplémentaires avant d'envoyer la demande d'abandons.



Partagez la liste avec des groupes clés au sein de l'entreprise : Services IT, sécurité, juridique et marketing. Plusieurs raisons peuvent expliquer pourquoi ces services souhaitent que l'entreprise conserve un nom de domaine particulier. Le service IT, par exemple, peut utiliser certains noms de domaine pour des besoins spécifiques inconnus des autres services (applications internes, hébergement d'un sous-domaine, etc.), et ne pas souhaiter qu'ils soient résiliés. Le service juridique peut avoir connaissance de certaines interventions qui ont nécessité l'ajout du nom de domaine dans le portefeuille. Le service sécurité peut souhaiter conserver une liste de noms de domaine dans le cadre d'une stratégie défensive visant à réduire les risques de phishing, tandis que le service marketing peut projeter de lancer un nouveau site dans les prochains mois.



Supprimez tous les détails associés du fichier de zone. Si un nom de domaine est utilisé pour la messagerie ou a un site hébergé sur un sous-domaine, la suppression du fichier de zone révélera ces utilisations avant de potentiellement abandonner le nom de domaine et d'avoir à consacrer du temps et des ressources pour le récupérer.



Envoyez la liste à votre registrar avant d'officialiser la demande d'abandons.



Utilisez un outil de surveillance de noms de domaine. Une surveillance peut permettre d'identifier des enregistrements par des tiers, et vous donne la visibilité requise pour détecter et faire interdire toute utilisation abusive de votre marque.

DISCUTONS-EN

Si vous avez des questions, ou si vous souhaitez que CSC vous assiste dans votre stratégie d'abandons de noms de domaine, vous pouvez nous contacter : <https://www.cscdbs.com/fr/contacts/>



CSC est le partenaire de confiance des entreprises du Forbes Global 2000 et des 100 Best Global Brands® en matière de gestion des noms de domaine, de services DNS et de certificats numériques, et propose des solutions de protection des marques en ligne contre la fraude. Alors que les entreprises du monde entier investissent massivement dans leur stratégie de sécurité, CSC peut les aider à identifier leurs failles de sécurité, et à sécuriser leurs noms de domaine, leur DNS et leurs certificats numériques. Les solutions de sécurité CSC protègent les entreprises des menaces de cyber-sécurité qui pèsent sur leur patrimoine numérique, et les aident à éviter les pertes de revenus, les atteintes à la réputation de leur marque ou les pénalités financières pouvant résulter d'une non-conformité aux réglementations de type Règlement général sur la protection des données (RGPD). Nous fournissons également des services de protection des marques en ligne, qui combinent la surveillance de marque et les actions ciblées en cas d'infraction. Nous proposons une approche holistique des actifs numériques et des services de protection contre la fraude pour contrer les tentatives de phishing.

 cscdbs.com/fr

Copyright ©2020 Corporation Service Company. Tous droits réservés.

CSC est un prestataire de services qui ne fournit aucun conseil juridique ou financier. Les documents présentés ici le sont uniquement à titre informatif. Veuillez consulter votre conseiller juridique ou financier afin de déterminer dans quelle mesure ces informations sont pertinentes pour vous.