

Quand on se fait passer pour votre entreprise

Faux site, faux profil, fausses factures envoyées à vos clients : détecter l'usurpation de votre identité et la faire cesser.

8 min de lecture · Niveau Intermédiaire · cyberionis.fr/ressources/usurpation-identite-entreprise

Un beau matin, un client appelle : « votre facture avec le nouveau RIB, c'est bien vous ? » Non. Quelqu'un émet des factures à votre en-tête, a monté un site sosie ou démarche avec un faux profil à votre nom. L'usurpation d'identité d'entreprise attaque votre bien le plus précieux — la confiance de vos clients — et vous met en première ligne sans avoir rien fait. Détection précoce et riposte organisée limitent drastiquement les dégâts.

1. Les formes courantes

- La fausse facture à votre en-tête : vos vrais clients reçoivent « votre » facture avec un RIB modifié — souvent après compromission d'une boîte email (la vôtre ou celle d'un client)
- Le domaine sosie : cyberionis-fr.com, cyber1onis.fr — pour envoyer des emails crédibles ou héberger un site cloné
- Le faux profil : page entreprise ou profil dirigeant cloné sur les réseaux, qui démarche, « recrute » (fausses offres d'emploi collectant des données) ou arnaque en votre nom
- Le détournement administratif : usurpation du SIREN pour des locations, crédits ou inscriptions frauduleuses
- Le site cloné entier : votre catalogue copié avec un tunnel de paiement frauduleux — courant pour les e-commerçants

2. Détecter tôt

- Alertes Google sur le nom de l'entreprise, ses variantes et le nom du dirigeant
- Surveillance des dépôts de domaines proches (services de veille, parfois via le registrar) — voir notre guide domaine
- SPF, DKIM et DMARC configurés : ils empêchent l'usurpation de VOTRE domaine exact et leurs rapports révèlent les tentatives (voir notre guide)
- Prendre au sérieux le premier signalement client : « on a reçu un email bizarre de vous » est votre système d'alarme le plus précieux — remerciez, creusez
- Recherche périodique de votre marque sur les réseaux et les moteurs (l'exercice OSINT annuel — voir notre guide)

3. Riposter, dans l'ordre

- Documenter tout : captures datées, URLs, emails reçus — les preuves d'abord, la riposte ensuite
- Prévenir vos clients vite et calmement : un email officiel « des fraudeurs usurpent notre identité ; nos coordonnées bancaires n'ont pas changé et ne changeront jamais par simple email » — la transparence

protège la confiance

- Faire tomber les contenus : signalement du faux profil à la plateforme (procédures dédiées aux usurpations), du site frauduleux à l'hébergeur et au registrar, via phishing-initiative pour blocage navigateurs
- Pour un domaine sosie : procédures extrajudiciaires (Syreli pour le .fr, UDRP) — rapides et efficaces, surtout marque à l'appui
- Déposer plainte systématiquement : l'usurpation d'identité est un délit, et la plainte appuie toutes les autres démarches
- Vérifier votre propre sécurité : l'usurpation exploite souvent une vraie compromission (boîte email, données clients) — c'est le moment d'un contrôle

CAS CONCRET

Schéma classique : la boîte email d'un client est compromise ; le fraudeur y lit vos vraies factures, les reproduit à l'identique avec son RIB et les renvoie « de votre part » aux échéances habituelles. Vous n'avez RIEN été piraté — et pourtant votre nom est en cause. D'où l'intérêt du message préventif à vos clients : « tout changement de RIB de notre part se vérifie par téléphone ».

4. Prévenir : rendre l'usurpation difficile et peu rentable

- Verrouiller le domaine et ses voisins évidents ; DMARC en mode strict
- Créer vos profils officiels sur les principales plateformes, même inactifs — occuper le terrain vaut mieux que le disputer
- Informer vos clients en amont des canaux et règles officiels : « nos RIB ne changent jamais par email »
- Protéger la marque (dépôt INPI) : l'arme juridique qui accélère toutes les procédures
- Sensibiliser l'équipe à signaler toute anomalie « en votre nom » croisée en ligne

L'essentiel à retenir

01 Mettre des alertes sur le nom de l'entreprise et du dirigeant

02 Configurer DMARC et surveiller ses rapports

03 Enregistrer les domaines sosies évidents

04 Préparer le message client type en cas d'usurpation

05 Documenter, signaler, porter plainte à chaque cas

06 Envisager le dépôt de marque INPI

Questions fréquentes

Sommes-nous responsables si des clients se font escroquer « en notre nom » ?

Pas du fait de l'usurpation elle-même — vous en êtes victime. Votre exposition naît de la négligence : usurpation connue et clients non prévenus, ou compromission réelle de vos systèmes non traitée. D'où l'importance de la réaction documentée : prévenir vite, signaler, corriger — c'est aussi votre protection juridique.

La plateforme ne réagit pas à nos signalements de faux profil. Que faire ?

Utilisez les formulaires spécifiques « usurpation d'identité » (plus efficaces que le signalement générique), en fournissant des justificatifs (Kbis, pièce du dirigeant). Faites signaler aussi par plusieurs comptes. En cas d'échec persistant avec préjudice, la mise en demeure par avocat et la plainte débloquent généralement — les plateformes répondent au formalisme juridique.

Quelle différence avec le vol de notre marque par un concurrent ?

L'usurpation est frauduleuse (se faire passer pour vous) et relève du pénal + des procédures de retrait. L'utilisation d'un nom proche par un concurrent réel relève de la propriété intellectuelle et de la concurrence déloyale — terrain civil, où le dépôt de marque INPI fait toute la différence. Les deux dossiers se traitent différemment, d'où l'intérêt de bien qualifier avec un conseil.

Pour aller plus loin

Cybermalveillance.gouv.fr — l'usurpation d'identité — www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/usurpation-identite

INPI — déposer sa marque — www.inpi.fr/protéger-vos-creations/protéger-votre-marque

Un doute, une urgence, un incident ?

Cyberionis évalue votre exposition, prépare vos défenses et vous épaula pour réagir vite en cas d'attaque.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr