

06.02.2026

# OSINT et usurpation d'identité : quand les données publiques deviennent une menace

**Jamais les informations personnelles n'ont été aussi accessibles qu'aujourd'hui. Or, on ignore souvent que les cybercriminels exploitent méthodiquement le renseignement open source (OSINT) pour collecter des identités, créer des profils et mettre en place des arnaques. Combinée à l'usurpation d'identité, cette pratique constitue une menace sérieuse.**

## Qu'est-ce que l'Open Source Intelligence (OSINT) ?

L'OSINT désigne la collecte et l'analyse systématiques d'informations provenant de sources publiquement accessibles. Il ne s'agit pas ici de données piratées, mais de contenus disponibles en libre accès sur le web, souvent publiés par les victimes elles-mêmes. Prises isolément, ces données semblent tout à fait anodines, mais une fois recoupées, elles permettent de dresser un profil très précis.

Les principales sources d'OSINT sont :

- les réseaux sociaux (Facebook, Instagram, TikTok etc.)
- les registres et annuaires publics
- les sites web, forums et espaces de commentaires
- les images, vidéos et leurs métadonnées
- les anciennes fuites de données accessibles en ligne

## Comment fonctionne l'OSINT concrètement ?

Les cybercriminels utilisent l'OSINT de manière ciblée et structurée. Tout commence par une recherche ciblée d'informations accessibles au public : nom, adresse email, numéro de téléphone ou nom d'utilisateur. Ces données sont ensuite recoupées avec l'activité sur les réseaux sociaux (posts, photos, interactions). D'autres informations telles que l'employeur, les loisirs ou les lieux fréquentés peuvent encore enrichir l'analyse. De cette mosaïque de détails émerge peu à peu un profil complet qui révèle les habitudes de vie, les contacts et le cercle de confiance de la cible. C'est sur cette base que les malfaiteurs mettent au point des attaques avec des scénarios crédibles, lorsqu'ils ne procèdent pas directement à une usurpation d'identité pure et simple. Tout le processus repose sur des informations obtenues légalement, mais détournées à des fins criminelles.

## Comment limiter les risques ?

S'il est pratiquement impossible de se prémunir totalement contre les attaques OSINT, vous pouvez en réduire considérablement la portée. Comment ? En vérifiant régulièrement les paramètres de confidentialité de vos comptes sur les réseaux sociaux et en faisant preuve de retenue lorsque vous partagez des contenus personnels. Pensez aussi à contrôler, voire à supprimer si nécessaire, vos anciens profils, publications et photos. Parallèlement, il est recommandé de ne pas utiliser les mêmes pseudonymes et adresses email sur toutes les plateformes. En particuli-

er, il convient de vous méfier des demandes ou messages qui contiennent étonnamment beaucoup de détails personnels, car ces derniers n'ont d'autre but que de vous mettre en confiance. La règle d'or est la suivante : moins vos données sont accessibles publiquement, plus il sera difficile de les détourner.

## **Conclusion**

L'OSINT révèle tout le potentiel des informations publiquement accessibles, pour le meilleur comme pour le pire. Entre de mauvaises mains, ces données deviennent une arme au service de l'usurpation d'identité et des escroqueries ciblées. Avoir conscience des données que l'on laisse derrière soi lors de ses activités en ligne est le premier pas pour renforcer durablement sa sécurité numérique.