

GUIDE

# OSINT : maîtriser l'exposition numérique de vos dirigeants

---

Ce qu'un attaquant trouve sur vos dirigeants — et  
comment reprendre le contrôle

---

**Sedona Radar — audit de sécurité externe automatisé**

Sedona AI    Lecture ~12 min    Édition 2026    [sedona-ai.com](https://sedona-ai.com)

**A**vant d'attaquer une entreprise, un adversaire commence par ses dirigeants. En quelques heures et sans jamais franchir la moindre porte fermée, il reconstitue leurs adresses, leurs mots de passe fuités, leur entourage, leurs habitudes — de quoi rendre une fraude au virement crédible ou piéger un assistant. C'est l'OSINT : le renseignement en sources ouvertes. Ce guide explique ce qu'un attaquant voit réellement de vos dirigeants, où passe la frontière légale, et surtout comment réduire cette exposition, méthodiquement.

### À retenir

- L'OSINT exploite uniquement des informations publiquement accessibles — mais l'agrégation de miettes anodines suffit à construire une attaque ciblée.
- Le point d'entrée le plus courant : des identifiants réutilisés et déjà présents dans des fuites publiques (credential stuffing).
- Les dirigeants sont des cibles privilégiées de la fraude au virement (BEC) : leur autorité rend l'ingénierie sociale efficace.
- L'OSINT est légal en France tant qu'il n'y a ni accès non autorisé à un système, ni collecte déloyale, ni atteinte à la vie privée. Le doxing, lui, est un délit.
- Vous disposez de leviers concrets : MFA, gestionnaire de mots de passe, cloisonnement perso/pro, déréférencement et droit à l'effacement.

## 01 Ce qu'un attaquant voit de vous

Le renseignement en sources ouvertes (OSINT) consiste à collecter et recouper des informations librement accessibles : réseaux sociaux, registres publics, fuites de données, métadonnées de documents, moteurs de recherche. Prise isolément, chaque donnée semble anodine. Agrégée, elle dessine un portrait exploitable : e-mail professionnel (souvent au format prénom.nom déductible), fonction et organigramme via LinkedIn, mots de passe issus de fuites, entourage, déplacements, centres d'intérêt.

**~1,96 Md**

Adresses e-mail uniques exposées dans un seul jeu de données de fuites (combolists de credential stuffing) indexé fin 2025, accompagnées de 1,3 milliard de mots de passe.

Have I Been Pwned / Troy Hunt, novembre 2025

**68 %**

Part des compromissions impliquant un facteur humain (erreur, ingénierie sociale, usage d'identifiants volés).

Verizon, 2024 Data Breach Investigations Report (DBIR)

# 31 %

Part des compromissions impliquant l'usage d'identifiants volés — souvent récupérés dans des fuites publiques et réutilisés.

Verizon, 2024 Data Breach Investigations Report (DBIR)

# 5 629

Violations de données personnelles notifiées à la CNIL en 2024 (+20 % sur un an) ; le nombre de violations touchant plus d'un million de personnes a doublé.

CNIL, bilan des violations de données 2024

## 02 De la donnée exposée à l'attaque

L'exposition n'est pas une fin en soi pour l'attaquant : c'est un carburant. Voici les chaînes d'attaque les plus fréquentes visant les dirigeants.

- Credential stuffing : un mot de passe fuité sur un site grand public est rejoué sur la messagerie professionnelle, car réutilisé.
- Spear-phishing : un e-mail sur mesure, nourri de détails réels (projet en cours, nom d'un collaborateur), déjoue la méfiance.
- Fraude au virement (BEC / « arnaque au président ») : usurpation du dirigeant pour ordonner un virement urgent et confidentiel au service comptable.
- Usurpation d'identité et fraude au CEO sur messageries et réseaux sociaux, en s'appuyant sur des photos et un ton crédibles.

# 55,5 Md\$

Pertes mondiales déclarées liées à la fraude au virement par compromission d'e-mail (BEC), cumulées sur 305 033 incidents signalés (2013–2023).

FBI IC3, Business Email Compromise: The \$55 Billion Scam (2024)

### Pourquoi les dirigeants ?

Un dirigeant cumule autorité (ses demandes sont exécutées sans discussion), visibilité (informations publiques abondantes) et accès (validation de paiements, secrets stratégiques). C'est le meilleur rapport effort/gain pour un attaquant.

## 03 Ce qu'est — et n'est pas — l'OSINT

L'OSINT défensif consiste à regarder votre organisation avec les yeux d'un attaquant, à partir des seules sources ouvertes, pour corriger ce qui est exposé. Il ne s'agit jamais d'accéder à un compte, de contourner une authentification ou d'exploiter une faille : cela relèverait de l'intrusion, sanctionnée par l'article 323-1 du Code pénal.

### La frontière : OSINT vs doxing

Divulguer des informations permettant d'identifier ou de localiser une personne en l'exposant à un risque est un délit (doxing, art. 223-1-1 du Code pénal), puni de 3 ans d'emprisonnement et 45 000 € d'amende — jusqu'à 5 ans et 75 000 € si la victime est dépositaire de l'autorité publique, journaliste, ou vulnérable. Une démarche OSINT légitime vise à protéger, avec le consentement de la personne concernée.

Chez Sedona, un audit OSINT est réalisé sur consentement écrit, centré sur l'exposition publique des personnes, et débouche sur des recommandations de réduction — pas sur une collecte à charge.

## 04 Auto-évaluation : votre exposition en 8 points

- ☐ Vos adresses e-mail (perso et pro) apparaissent-elles dans une fuite connue ? Vérifiez sur [haveibeenpwned.com](https://haveibeenpwned.com).
- ☐ Vos profils LinkedIn / réseaux sociaux exposent-ils l'organigramme, vos déplacements, votre entourage à un public non maîtrisé ?
- ☐ Réutilisez-vous un même mot de passe sur plusieurs services (dont un compte grand public déjà fuité) ?
- ☐ Le MFA est-il activé sur la messagerie, la banque et les accès d'administration ?
- ☐ Vos documents publiés en ligne (PDF, présentations) contiennent-ils des métadonnées sensibles (auteur, chemins internes, logiciels) ?
- ☐ Vos comptes personnels et professionnels sont-ils strictement cloisonnés (adresses, appareils, mots de passe) ?
- ☐ Des informations personnelles excessives vous concernant subsistent-elles dans les résultats de recherche à votre nom ?
- ☐ Une procédure interne impose-t-elle une double validation, par un canal distinct, pour tout virement inhabituel ou urgent ?

## 05 Réduire l'exposition : le plan d'action

### 1 Fermez les portes déjà ouvertes

Recensez vos comptes exposés (Have I Been Pwned), changez tout mot de passe fuité, et adoptez un mot de passe unique par service via un gestionnaire — cela neutralise le credential stuffing.

- 2

**Généralisez le MFA**  
Activez l'authentification multifacteur partout, en privilégiant une clé physique ou une passkey plutôt que le SMS (vulnérable au SIM swapping).
- 3

**Cloisonnez perso et pro**  
Séparez strictement adresses, appareils et comptes personnels et professionnels : une fuite d'un côté ne doit pas ouvrir l'autre.
- 4

**Maîtrisez votre empreinte publique**  
Restreignez la visibilité sur les réseaux sociaux, limitez la publication de déplacements et d'informations familiales, purgez les métadonnées avant toute mise en ligne.
- 5

**Exercez vos droits**  
Demandez le déréférencement des liens excessifs associés à votre nom et l'effacement des données non nécessaires (art. 17 du RGPD).
- 6

**Mettez en place une surveillance**  
Activez des alertes de fuite (notifications HIBP) et une veille sur votre nom et votre marque, pour détecter une exposition avant qu'elle ne serve à une attaque.

## 06 Vos droits pour reprendre la main

| Levier               | Effet                                                                                                                  | Base                       |
|----------------------|------------------------------------------------------------------------------------------------------------------------|----------------------------|
| Droit à l'effacement | Suppression des données personnelles qui ne sont plus nécessaires ou traitées de façon illicite ; réponse sous 1 mois. | Art. 17 du RGPD            |
| Déréférencement      | Retrait d'un lien des résultats de recherche associés à votre nom (le contenu source reste en ligne).                  | Jurisprudence / CNIL       |
| Signalement doxing   | Poursuite pénale en cas de divulgation malveillante de données vous exposant à un risque.                              | Art. 223-1-1 du Code pénal |

### Un audit vaut mieux qu'une intuition

Vous ne pouvez pas corriger ce que vous ne voyez pas. Un audit OSINT dresse l'inventaire réel de votre exposition et de celle de vos dirigeants, puis le traduit en actions prioritaires.

## § Sources

1. Have I Been Pwned / Troy Hunt — jeu de données « Synthient » (nov. 2025) — <https://www.troyhunt.com/2-billion-email-addresses-were-exposed-and-we-indexed-them-all-in-have-i-been-pwned/>

2. Verizon — 2024 Data Breach Investigations Report (DBIR) — <https://www.verizon.com/business/resources/reports/dbir/>

3. CNIL — Violations massives de données en 2024 — <https://www.cnil.fr/fr/violations-massives-de-donnees-en-2024-quels-sont-les-principaux-enseignements-mesures-a-prendre>

4. FBI IC3 — Business Email Compromise: The \$55 Billion Scam (2024) — <https://www.ic3.gov/PSA/2024/PSA240911>

5. Légifrance — Code pénal, art. 223-1-1 (doxing) — [https://www.legifrance.gouv.fr/codes/article\\_lc/LEGIARTI0000043974282](https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI0000043974282)
6. CNIL — Le droit à l'effacement — <https://www.cnil.fr/fr/le-droit-leffacement-supprimer-vos-donnees-en-ligne>
7. CNIL — Le déréférencement d'un contenu dans un moteur de recherche — <https://www.cnil.fr/fr/le-dereferencement-dun-contenu-dans-un-moteur-de-recherche>

## Que révèle une recherche à votre nom ?

L'audit OSINT de Sedona évalue l'exposition numérique de vos dirigeants à partir de sources publiques — mots de passe apparus dans des fuites, informations privées accessibles, empreinte en ligne — avec l'accord écrit de chaque dirigeant concerné. Vous recevez un rapport confidentiel. À partir de 1 900 € HT.

**Demander un audit OSINT**

[sedona-ai.com/contact?service=osint](https://sedona-ai.com/contact?service=osint)