

Ce que les attaquants savent déjà de vous (OSINT)

Avant d'attaquer, on se renseigne. Découvrez votre empreinte numérique avec les yeux d'un fraudeur — et réduisez-la.

9 min de lecture · Niveau Intermédiaire · cyberionis.fr/ressources/empreinte-numerique

Toute attaque ciblée commence par du renseignement en sources ouvertes — l'OSINT : site web, réseaux sociaux, registres publics, fuites de données. En une heure, un attaquant reconstitue votre organigramme, vos outils, vos fournisseurs et les adresses email de toute l'équipe. Faire ce travail sur soi-même, avant lui, révèle exactement ce qui alimentera le prochain phishing ciblé ou la prochaine fraude au président.

1. Ce qu'une heure de recherche révèle sur une PME type

- L'organigramme : dirigeants et fonctions via les registres légaux (societe.com, Pappers) et LinkedIn — y compris qui tient la comptabilité, cible n° 1 des fraudes au virement
- Le format des emails : deux adresses trouvées suffisent à déduire prenom.nom@entreprise.fr pour toute l'équipe
- Les outils utilisés : offres d'emploi (« maîtrise de Sage, environnement Microsoft 365 »), signatures d'emails, mentions du site — de quoi crédibiliser un faux support technique
- Les absences et événements : congés annoncés sur LinkedIn, salons, déménagements — les fenêtres idéales pour une fraude « urgente »
- Les fuites de données : mots de passe associés aux adresses de l'entreprise dans les fuites passées, revendus quelques euros
- L'exposition technique : sous-domaines oubliés, services exposés (RDP, caméras), certificats — visibles via des moteurs spécialisés comme Shodan

CAS CONCRET

Recette d'une fraude au président réussie, ingrédients 100 % publics : le dirigeant annonce sur LinkedIn sa participation à un salon à l'étranger ; la comptable est identifiable sur le site « votre contact facturation » ; le format email est déduit du site. Le premier jour du salon, elle reçoit un email urgent et confidentiel « du dirigeant en déplacement »... Chaque élément du scénario a été fourni par l'entreprise elle-même.

2. Auditer sa propre empreinte

- Googler l'entreprise et ses dirigeants (entre guillemets), y compris en pages 2-5 et sur les images
- Vérifier les adresses email de l'équipe sur haveibeenpwned.com — et traiter les mots de passe concernés
- Passer en revue les réseaux sociaux de l'entreprise ET les profils publics des collaborateurs clés avec un œil d'attaquant
- Relire son site web : trombinoscopes détaillés, adresses email individuelles en clair, documents PDF

avec métadonnées

- Faire vérifier l'exposition technique (sous-domaines, services ouverts) par votre prestataire — ou un audit dédié
- Refaire l'exercice une fois par an : l'empreinte repousse

3. Réduire — sans disparaître

L'objectif n'est pas l'invisibilité (le site doit vendre, LinkedIn doit recruter) mais la maîtrise : savoir ce qui est public, retirer l'inutile, et neutraliser ce qui ne peut pas l'être.

- Préférer les adresses de fonction (contact@, compta@) aux adresses nominatives sur le site public
- Sensibiliser les collaborateurs exposés : ce qu'un post « en congés deux semaines ! » ou « fier de notre nouvelle infrastructure » offre à un attaquant
- Nettoyer les métadonnées des documents publiés (auteur, logiciel, chemins internes)
- Fermer les sous-domaines et services oubliés révélés par l'audit
- Surtout : puisque l'information publique alimentera toujours l'ingénierie sociale, ancrer les procédures qui la rendent inoffensive — vérification téléphonique des virements, signalement des demandes inhabituelles

4. Surveiller dans la durée

- Alerte de surveillance de domaine sur haveibeenpwned (gratuite) : notification à chaque nouvelle fuite touchant vos adresses
- Alertes Google sur le nom de l'entreprise et des dirigeants
- Surveillance des dépôts de domaines proches du vôtre (cybersquatting : cyberionis-fr.com...) utilisés pour le phishing — des services le font, votre registrar parfois aussi
- En cas d'usurpation détectée (faux profil, faux site) : signalement à la plateforme, au registrar, et plainte si nécessaire

L'essentiel à retenir

- 01 Faire l'exercice OSINT sur sa propre entreprise une fois par an
 - 02 Vérifier les adresses du domaine sur haveibeenpwned et traiter les fuites
 - 03 Remplacer les emails nominatifs par des adresses de fonction sur le site
 - 04 Sensibiliser les collaborateurs exposés à ce que révèlent leurs publications
 - 05 Faire auditer l'exposition technique (sous-domaines, services ouverts)
 - 06 Ancrer les procédures qui neutralisent l'ingénierie sociale
-

Questions fréquentes

Chercher ces informations sur sa propre entreprise est-il légal ?

Oui : l'OSINT sur sources ouvertes est légal — c'est la consultation d'informations publiques. La limite pénale est franchie quand on tente d'accéder à des systèmes (deviner des mots de passe, exploiter une faille) : cela relève du test d'intrusion, qui exige une autorisation écrite, même sur sa propre infrastructure si elle est hébergée chez un tiers.

Peut-on faire retirer des informations qui nous concernent ?

Partiellement : le RGPD donne aux personnes un droit à l'effacement auprès des sites et moteurs (formulaires de déréférencement Google), efficace pour les données personnelles obsolètes. Les registres légaux (dirigeants d'entreprise), eux, sont publics par nature — certaines données peuvent être rendues non diffusables (adresse personnelle des dirigeants via l'INPI) : pensez-y.

Faut-il interdire aux salariés de mentionner l'entreprise sur LinkedIn ?

Irréaliste et contre-productif — LinkedIn sert aussi votre visibilité. La bonne approche est la sensibilisation ciblée : les fonctions exposées (direction, finance, IT) comprennent ce que leurs publications offrent à un attaquant, et l'entreprise cadre dans sa charte ce qui relève du confidentiel (projets, outils, organisation interne).

Pour aller plus loin

Have I Been Pwned — surveiller son domaine — haveibeenpwned.com/DomainSearch

INPI — rendre confidentielle l'adresse des dirigeants — www.inpi.fr

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

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