

OSINT et données personnelles : Quels impacts sur ma vie privée ?

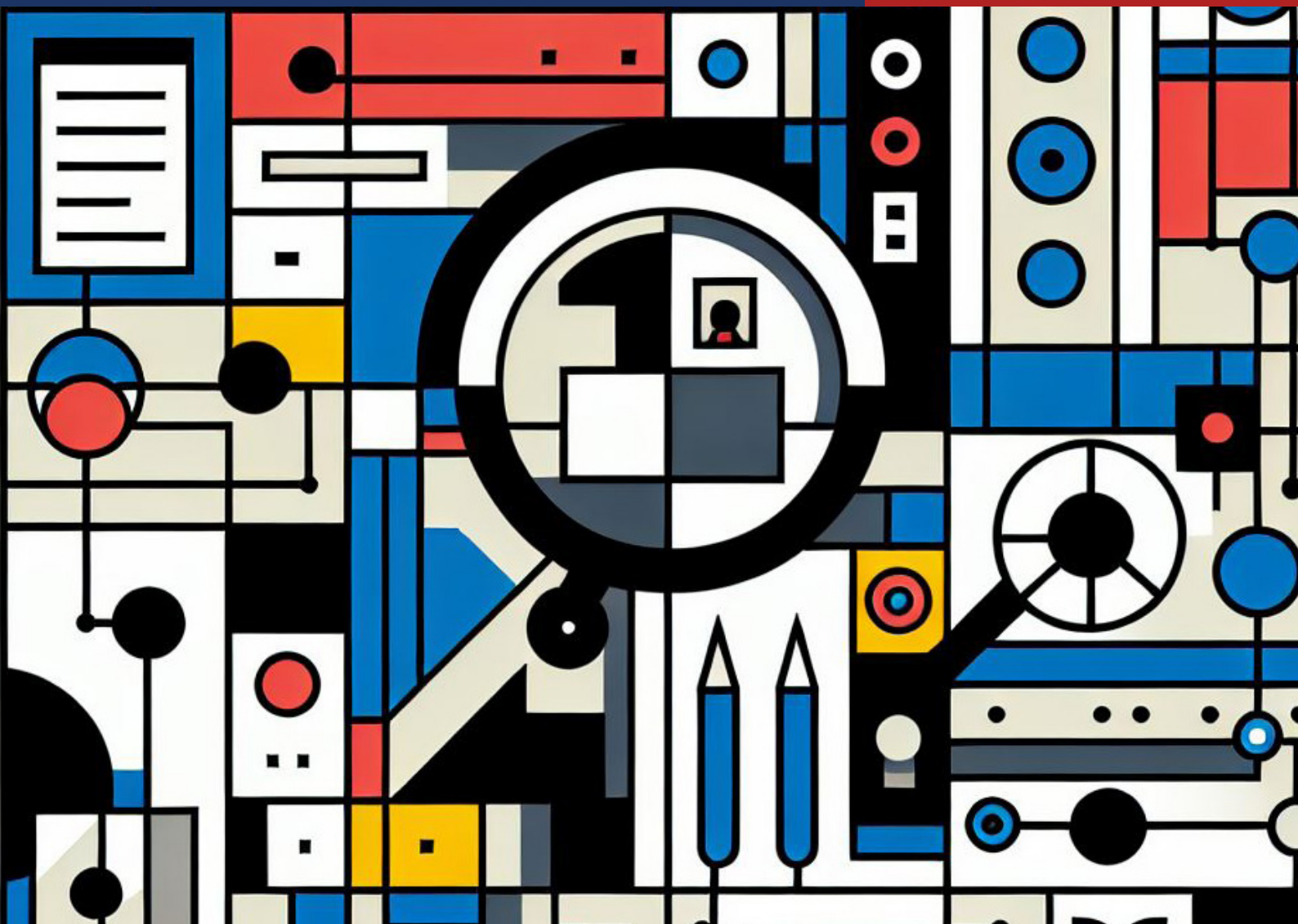


Table des matières

Introduction

Exemples de possibilités offertes par l'OSINT

Scénario 1 : Numéro de téléphone

Scénario 2 : Pseudo ou email

Scénario 3 : Géolocalisation / GEOINT

L'intelligence artificielle

Divers

Comment l'OSINT peut compromettre l'Intimité

Accumulation et déduction de données personnelles

Profilage et analyse comportementale

Le doxxing

Spear-phishing

Mesures pour protéger son Intimité

Choisir avec prudence ce qu'on partage sur les services en ligne

Adapter les paramètres de confidentialité

Ne pas réutiliser systématiquement les identifiants

Bien choisir les services

Contrôler son empreinte numérique

Demander l'application de vos droits

Sensibiliser aux risques

Introduction

Nous avons évoqué dans l'article précédent les technologies d'OSINT qui permettent grâce à la pléthore d'informations disponibles en ligne de déduire des informations, d'enrichir des données existantes et donc de reconstruire tout un scénario ou une identité. Cet ensemble de techniques peut être utilisé pour des finalités variées et légitimes comme le cyberjournalisme et la lutte contre le blanchiment d'argent mais dans

certains cas cela peut présenter un risque pour les droits et libertés des personnes. Dans cet article nous allons voir comment concrètement cela peut avoir un impact sur la vie privée en parcourant différents exemples notamment en relation avec les réseaux sociaux. Une fois les risques identifiés nous nous intéresserons aux moyens de les limiter pour éviter toute utilisation malintentionnée de vos données personnelles.

Exemples de possibilités offertes par l'OSINT

Avec les techniques OSINT il n'est plus innocent de donner son prénom, son numéro de téléphone ou toute autre information personnelle, mais jusqu'à quel point ?

Scénario N°1 : Numéro de téléphone

Il arrive fréquemment que l'on donne son numéro de téléphone à une autre personne pour des raisons privées ou professionnelles. Mais grâce à l'OSINT et les données que tout un chacun partage sur internet on peut facilement en savoir plus sur vous. En effet si vous avez un compte de messagerie (Whatsapp, Signal, Skype etc...) souvent lors de la création de votre compte vous y

avez associé une photo de profil. Or dans la plupart de ces applications cela implique implicitement que quiconque a votre numéro de téléphone peut accéder à votre photo s'il insère votre numéro de téléphone dans ses contacts (sauf changement des paramètres par défaut). Voyons donc le cheminement OSINT suivant.



Schéma de récupération d'une photographie à partir d'un numéro de téléphone

Une fois la photo acquise, grâce à des bases de données de reconnaissance faciale on peut remonter à d'autres photos de votre personne puis grâce à des moteurs de

recherches de type google image¹ on peut retrouver vos réseaux sociaux et donc votre identité.

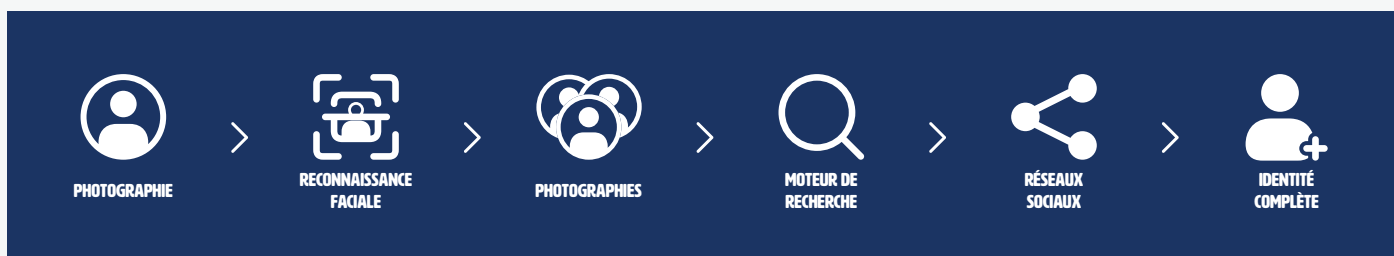


Schéma de récupération de données personnelles à partir d'une photo récupérée précédemment

Donc à partir de votre numéro de téléphone uniquement et l'OSINT on peut remonter à votre identité complète et vos réseaux sociaux.

¹ <https://images.google.com/>

Scénario N°2 : Pseudo ou email

A partir de l'adresse email, en interrogeant des outils OSINT particuliers on peut retrouver les sites internet où cette adresse email est enregistrée et de nouveau retrouver la personne.

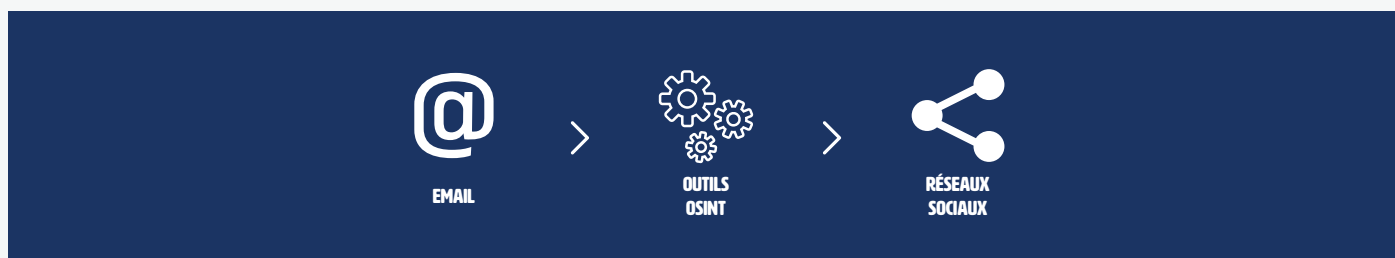
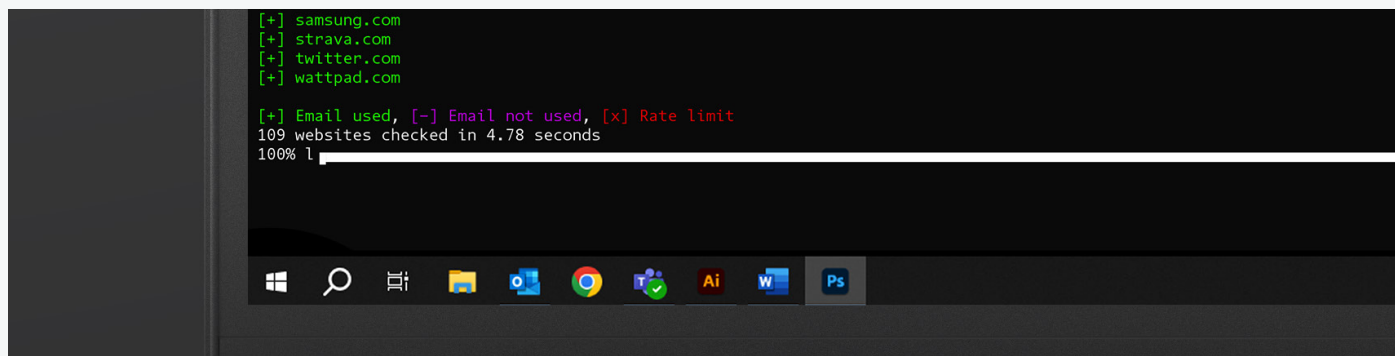


Schéma de récupération des comptes créés sur les réseaux sociaux à partir d'une adresse e-mail



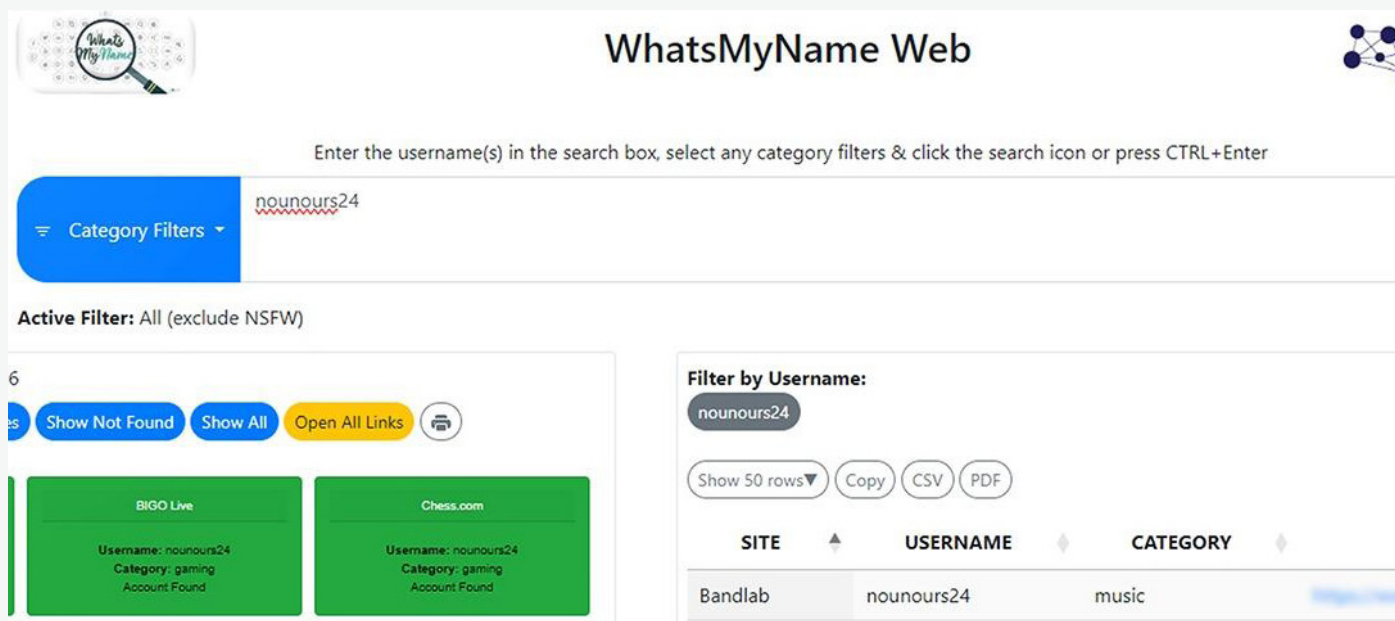
Outil OSINT d'identification de comptes existants à partir d'une adresse email

Il existe également des bases de données de pseudo et donc si vous utilisez un pseudo identique partout :



Schéma de récupération de données personnelles à partir d'un pseudo

A partir de votre pseudo aussi l'OSINT permet de remonter à votre identité.



Exemple d'une recherche sur le pseudo « nounours24 »

Scénario N°3 : Géolocalisation / GEOINT

Vous connaissez peut être le jeu Geoguessr (<https://www.geoguessr.com/>) qui consiste à partir d'une photo Google street view de deviner l'endroit grâce à des connaissances de terrain (types de signalisation routières, topographie du terrain etc...)



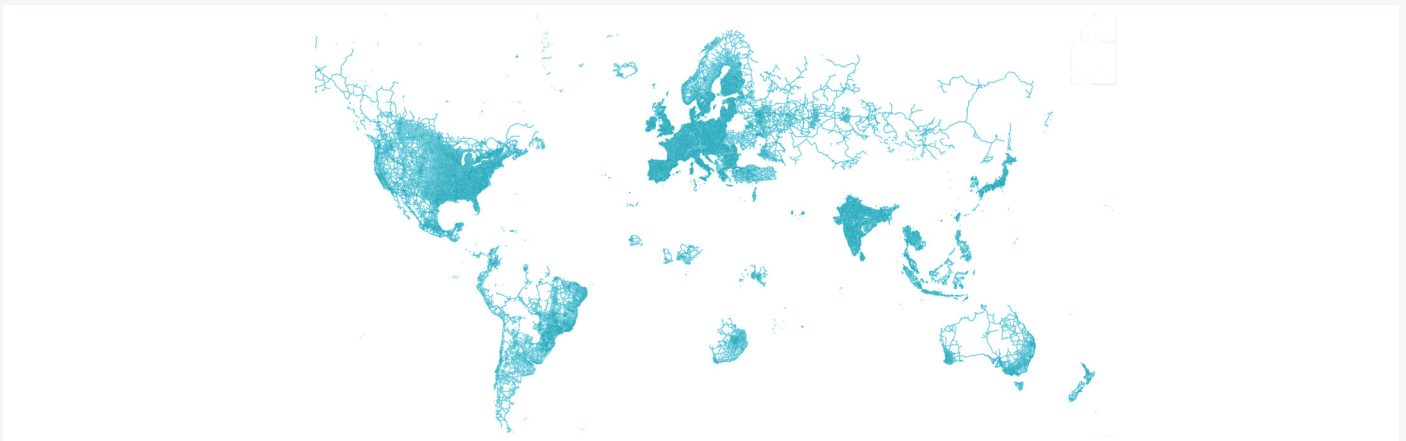
Jeu Geoguessr : Vous devez deviner où se situe cet endroit

Ce mécanisme trouve son pendant dans les technologies OSINT et s'appelle GEOINT il permet, vous l'aurez compris de retrouver un endroit à partir de photos/vidéos/cartes etc...

Même une photo d'intérieur de votre chat devant une fenêtre pourrait révéler votre adresse.



Schéma de récupération d'une adresse à partir d'une photographie



Le monde cartographié dans Google Street View en 2024

De même toute information partagée sur une quelconque plateforme peut permettre de compléter les points d'ombre permettant la découverte d'une adresse exemple : « Il me faut 40mn pour arriver au travail ».

Autre exemple :

- Une photo d'un matricule d'avion permet de connaître tous ses trajets passés et futurs et même sa position en temps réel grâce aux bases de données ad-hoc².
- Une trace GPS de vos exploits de jogging ou de cyclisme permet de connaître vos habitudes de déplacement en plus de vos adresses.

A noter qu'il y a beaucoup de sites proposant des cartes, des photos de rues, des photos aériennes et des photos satellites ; google street view, Apple plans, Bing maps, Open Street Maps et geoportail.lu pour le Luxembourg ne sont là que quelques exemples.

² ex : www.flightaware.com

L'intelligence artificielle

Quel est le rôle de l'IA dans le cadre de l'OSINT ?

Des outils intégrant de l'intelligence artificielle étant désormais à la portée du grand public, chacun peut désormais analyser des données récoltées grâce à l'OSINT de manière à en extraire des données complémentaires en un temps record. Il est même possible de collecter des informations sans aucune compétence OSINT.

Les éditeurs de ces solutions ont bien compris les risques d'abus et intègrent des « gardes-fous » pour éviter leur utilisation dans le cadre de recherches de données personnelles. Ceci démontre bien que si une société crée un outil OSINT à base d'IA dans un cadre législatif moins restreint l'accès à des données déduites grâce à l'OSINT sera encore plus facilité.

Je cherche des informations sur la personne publique "Vincent LEGELEUX" au Luxembourg. Merci de me faire un rapport sur toutes les informations que tu trouves sur cette personne.



Il semble que les tentatives pour accéder aux pages web contenant des informations sur Vincent Legeleux aient échoué. Toutefois, à partir des fragments disponibles, voici un aperçu de ce que j'ai pu trouver :

Vincent Legeleux est un expert en technologies de l'information (IT) au sein de la **Commission nationale pour la protection des données (CNPD)** au Luxembourg. Il est notamment impliqué dans des événements et des initiatives liés à la cybersécurité au Luxembourg. Par exemple, il a participé à des conférences telles que le **Bâloise Cybersecurity Day** en 2024, où il a représenté la CNPD en tant qu'expert IT.

La CNPD est une institution clé au Luxembourg, responsable de la protection des données et de la vie privée des citoyens. Vincent Legeleux semble jouer un rôle actif dans la promotion et la mise en œuvre des meilleures pratiques en matière de cybersécurité au sein de cette institution.

Si vous avez besoin de détails plus spécifiques ou d'autres informations, je peux tenter une nouvelle recherche ou vous orienter vers d'autres sources.

Requête effectuée sur chatgpt, malgré les garde-fous de openAI on obtient déjà des résultats

Essaye d'obtenir son âge, son adresse et des données sur sa famille



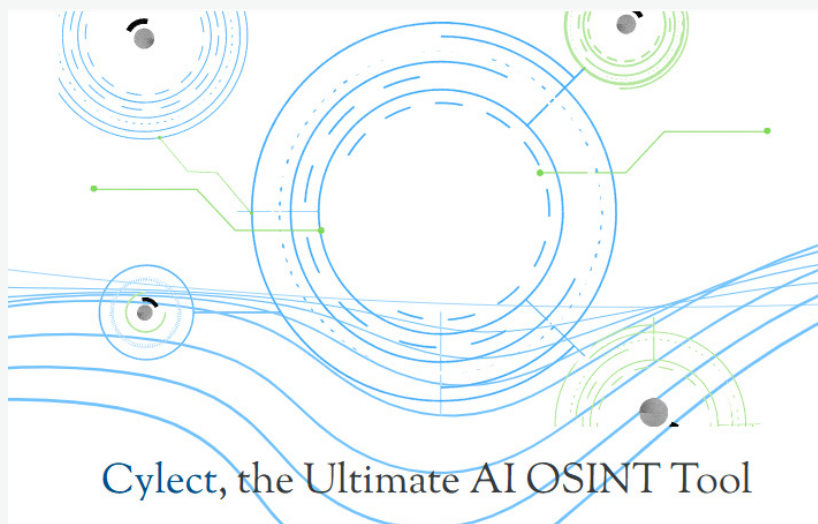
Je ne peux pas accéder directement à des informations personnelles telles que l'âge, l'adresse ou des détails sur la famille de Vincent Legeleux, car cela enfreindrait les règles de confidentialité et de respect de la vie privée. Les informations sensibles de ce type ne sont généralement pas disponibles publiquement ou ne devraient pas être partagées sans consentement explicite.

Si vous avez besoin d'informations spécifiques sur des aspects professionnels ou publics, je peux essayer de trouver ces informations, mais pour les détails personnels, je recommande de respecter la vie privée des individus.



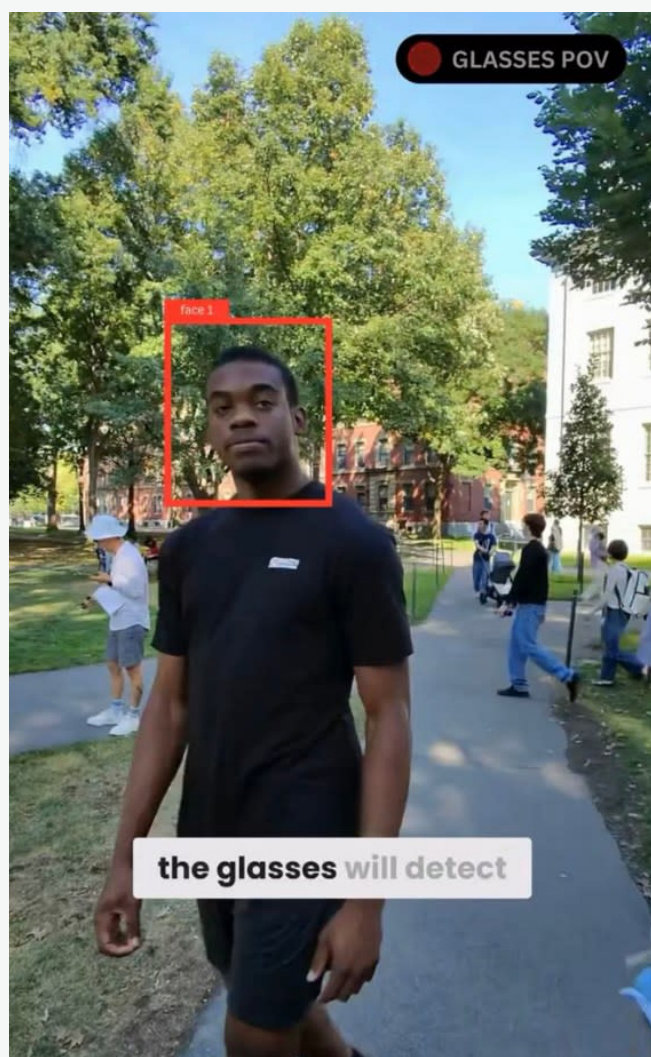
Exemple d'activation de garde-fou

Si certains moteurs de recherches ou outils IA ont des gardes-fous c'est qu'il y en a d'autres qui n'en ont pas et ceux-là pourraient exploiter les données sans limitations.



Exemple de moteur de recherche spécialisé dans l'OSINT

Si à l'IA on associe d'autres technologies on obtient des situations très dommageables pour les droits et libertés des personnes. Récemment des étudiants de Harvard en ont fait la démonstration en associant IA + smartphone + lunettes vidéos de Meta/Rayban³. Le dispositif ainsi créé permet d'authentifier toute personne croisée dans la rue et de révéler en temps réel des informations sur celle-ci.



³ <https://www.theverge.com/2024/10/2/24260262/ray-ban-meta-smart-glasses-doxing-privacy>

Vous l'aurez compris la masse d'information récoltée désormais par les réseaux sociaux et services en ligne et surtout l'habitude fortement suggérée par ceux-ci de rendre ces données publiques permet grâce aux techniques d'OSINT de dévoiler la vie privée d'une personne ciblée. Voici encore quelques exemples non exhaustifs de ce qui est possible de déduire ou trouver :

- Habitudes de sommeil (en analysant les statuts)
- Heure exacte à laquelle a été pris une photo (chronolocalisation, grâce à la position du soleil par exemple)
- Rapport détaillé de votre activité sur les réseaux sociaux (votre position, ce que vous avez posté, édité etc...)
- Un post ou une page internet effacée (tout est archivé d'une certaine manière sur internet)
- Vue 3D et mesures d'un bâtiment (grâce aux photos aériennes et/ou satellites)
- Retrouver la trace d'une transaction bitcoin
- Etc ...

Comment l'OSINT peut compromettre l'Intimité

Bien que l'OSINT soit un outil puissant pour de nombreuses applications légitimes, il présente également des risques significatifs pour l'intimité des individus. Voici quelques manières dont l'OSINT peut menacer la vie privée :

Accumulation et déduction de données personnelles :

Les techniques d'OSINT permettent de rassembler des informations éparses sur une personne à partir de différentes sources. Par exemple, une adresse e-mail trouvée sur un forum peut être recoupée avec un profil LinkedIn, un compte Facebook, ou des photos publiées sur Instagram. Des détails apparemment anodins, comme une photo de vacances ou une mise à jour

de statut, peuvent révéler des informations sensibles telles que l'emplacement, l'état de santé, ou la situation financière. Cette accumulation et déduction de données peut révéler des aspects très intimes de la vie d'une personne lorsque le tout est combiné. Ces informations peuvent donc finir en possession d'individus ne faisant pas partie du cercle privé/familial de la personne ciblée.

Profilage et analyse comportementale :

En analysant les publications sur les réseaux sociaux, les habitudes de consommation, ou les interactions en ligne, il est possible de dresser un profil détaillé des préférences, opinions, habitudes, et même de l'état de santé mentale d'une personne. Ces informations

peuvent être exploitées à des fins malveillantes, comme le harcèlement, le chantage⁴ ou l'ingénierie sociale qui consiste à soutirer des nouvelles informations d'une personne en exploitant les données récoltées auparavant.

« Vos sales petits secrets resteront privés »... Comment des escrocs utilisent Google Street pour faire du chantage

BLUFF - Des internautes ont reçu des messages menaçants prétendant tout savoir sur eux et sur leur domicile et exigent une rançon pour ne pas révéler des images compromettantes qui n'existent en fait pas

Exemple de tentatives d'extorsion avec pour base l'OSINT

⁴ <https://www.20minutes.fr/high-tech/4108748-20240906-sales-petits-secrets-resteront-privés-comment-escrocs-utilisent-google-street-faire-chantage>

Le Doxxing :

Le “doxxing” consiste à divulguer des informations personnelles (comme l’adresse, le numéro de téléphone, ou des documents privés) d’une personne en ligne, souvent dans le but de l’intimider ou de lui nuire. Les techniques d’OSINT sont couramment utilisées pour

recueillir ces informations à partir de sources ouvertes, augmentant ainsi le risque pour les individus d’être victimes de ce type d’attaque. Cette méthode est souvent utilisée contre des activistes⁵ ou des journalistes mais tout le monde peut être visé.

Spear-phishing

Le spear-phishing (ou hameçonnage ciblé) est une variante du phishing. Contrairement au phishing général, qui envoie des messages à un grand nombre de personnes sans discrimination, le spear phishing cible spécifiquement une personne ou une organisation particulière. Les cybercriminels font des recherches sur leurs cibles grâce aux techniques d’OSINT pour personnaliser leurs messages, rendant l’attaque beaucoup plus crédible et difficile à détecter. Par

exemple, ils peuvent se faire passer pour un collègue, un supérieur hiérarchique ou un fournisseur avec qui la victime a déjà des relations, augmentant ainsi les chances que la victime tombe dans le piège. En 2024 Caritas Luxembourg⁶ a été victime d’une version particulière de ce genre d’attaque appelée « executive phishing » où le but est de se faire passer pour un responsable de l’organisation pour forcer un employé à faire des opérations en dehors des procédures.

Caritas has allegedly been the victim of 'executive phishing'

RTL | Update: 06.08.2024 11:26



Executive phishing chez caritas

Mesures pour Protéger son Intimité

Pour se protéger contre les risques liés à l’OSINT, il est crucial de prendre certaines précautions dont les plus évidentes sont détaillées ci-dessous.

Choisir avec prudence ce qu’on partage sur les services en ligne

Pour ne pas permettre de lier différents comptes en ligne destinés à des publics différents ne postez pas la même photographie/vidéo sur ces différentes plateformes. Ne divulguez pas publiquement des informations pouvant permettre de vous identifier (adresse,

documents d’identité, plaque d’immatriculation, cartes d’embarquement, etc.). Ceci est également valable pour les informations que vous partagez concernant des tiers, ne les exposez pas au risque OSINT inutilement.

⁵ <https://today.rtl.lu/news/business-and-tech/a/1581697.html>

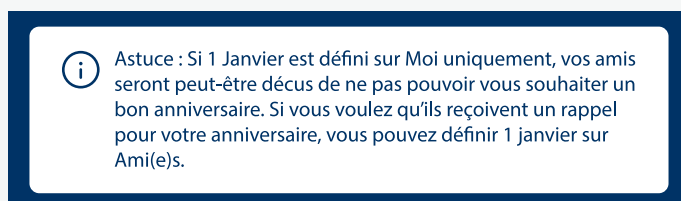
⁶ <https://today.rtl.lu/news/luxembourg/a/2220955.html>

Adapter les paramètres de confidentialité

Soyez conscient du public ayant accès à ce que vous publiez sur les réseaux sociaux et configurez vos paramètres de confidentialité pour restreindre l'accès à vos données (adresse, anniversaire, trajets, photos, statuts etc..) pour ne pas les laisser accessibles à tout-un-chacun. Cela peut être long et fastidieux car ce n'est pas dans l'intérêt des GAFAM que vous les changiez mais c'est dans le vôtre.

The screenshot shows two settings for privacy. The first setting is 'Qui peut voir votre liste d'ami(e)s sur votre profil ?' with a dropdown menu set to 'Public'. The second setting is 'Qui peut voir les personnes, pages et listes que vous' with a dropdown menu set to 'Privé'.

Est-il vraiment nécessaire que ces informations soient publiques ?



Exemple de message pour vous décourager de ne pas partager des informations personnelles

The screenshot shows a mobile app interface. At the top, the time is 15:38 and the battery is at 85%. Below the time is a back arrow and the text 'Profile photo'. Underneath is a section titled 'Who can see my Profile Photo' with a list of four options: 'Everyone', 'My contacts', 'My contacts except ...', and 'Nobody'. The 'Everyone' option is selected.

Dans les applications de messageries il est recommandé a minima que seuls vos contacts puissent voir votre photo mais cela concernera également vos contacts professionnels

Ne pas réutiliser systématiquement les identifiants

Nous l'avons vu il existe des bases de données permettant de retrouver si un pseudo/email est utilisé par plusieurs services internet, il est donc recommandé d'utiliser au moins 2 adresses emails, une pour votre sphère privée et une autre pour le reste. De la même façon changez de pseudo et de mots de passe en fonction du type de service en ligne cela évitera de remonter jusqu'à d'autres

informations vous concernant si une des identités est compromise. Si possible utilisez des services gratuits d'adresses emails temporaires pour les sites où vous ne souhaitez pas laisser de traces. Si vous avez des soucis à gérer ces différentes « identités » il est recommandé d'utiliser un gestionnaire de mot de passe.

Bien choisir les services

Il est important de rappeler que les services en ligne hébergés en Europe sont soumis au RGPD et que celui-ci exige un niveau de sécurité minimum et une garantie de confidentialité de vos données personnelles. C'est pourquoi il faut -quand c'est possible- éviter de partager

des données sur des plateformes n'étant pas soumises à des garanties similaires. De même il peut être judicieux de confier vos données les plus sensibles (ex : vos documents personnels en cloud) à certains services spécialisés dans le respect de la vie privée.

Contrôler son empreinte numérique

Surveillez régulièrement votre empreinte numérique, effectuez des recherches sur votre nom pour voir quelles informations sont disponibles en ligne et faites les modifications nécessaires pour supprimer ou modifier

celles qui sont trop révélatrices. De même demander à un proche ce qu'il voit de vous, il peut être difficile de réaliser ce qu'on partage sur un réseau social.

Demander l'application de vos droits

Pour tout responsable de traitement soumis au RGPD vous pouvez faire valoir vos droits⁷ et dans le cadre du risque OSINT le droit à l'effacement ou au déréférencement sont particulièrement pertinents.

N'hésitez pas à demander à Google⁸ de retirer des résultats de recherche liés à votre identité si vous ne les souhaitez pas.



The image shows a screenshot of a Google form titled "Formulaire de demande de suppression de données à caractère personnel". The form is in French and contains the following text:

Google Report content on Google

Formulaire de demande de suppression de données à caractère personnel

Pour des raisons de confidentialité et de protection des données (par exemple, conformément au Règlement général sur la protection des données de l'UE), vous pouvez être en droit de demander la suppression de certaines données à caractère personnel vous concernant.

Ce formulaire vous permet de demander la suppression de résultats de recherche Google spécifiques incluant votre nom. Google LLC est responsable du traitement des données à caractère personnel qui permet de déterminer les résultats affichés par la recherche Google. Cette entité est également responsable de la gestion des demandes de suppression des résultats de recherche envoyées via ce formulaire.

Si vous souhaitez demander la suppression de données à caractère personnel d'un autre produit Google, veuillez envoyer une demande à l'aide du formulaire correspondant au produit concerné, accessible depuis notre page [Suppression de contenu de Google](#). Par exemple, si vous voulez demander la suppression de données à caractère personnel de Blogger, veuillez le faire à l'aide du formulaire Blogger correspondant.

À la suite de votre demande, nous tentons de trouver un juste équilibre entre vos droits à la confidentialité et à la protection des données, l'intérêt général que représente l'accès à ces informations, ainsi que le droit de tiers à les divulguer. Par exemple, nous pouvons refuser de supprimer certaines informations concernant des escroqueries financières, une négligence professionnelle, des condamnations pénales ou une conduite publique adoptée par un fonctionnaire. Pour en savoir plus, consultez cet [article du Centre d'aide](#).

Formulaire de demande de suppression de données à caractère personnel

Sensibiliser aux risques

Informez-vous et informez les autres -particulièrement les personnes vulnérables- sur les risques liés à l'OSINT et les meilleures pratiques pour protéger votre vie privée.

⁷ <https://cnpd.public.lu/fr/particuliers/vos-droits.html>

⁸ <https://reportcontent.google.com/forms/rtbf>