#CestAssez

Comment se doxxer?

Le "doxxing" est une pratique utilisée par des individus mal intentionnés et/ou des « trolls » visant à rechercher des informations personnelles sur une personne, telle que son adresse personnelle, son numéro de téléphone, son lieu de travail, l'école de ses enfants ou d'autres détails personnels. Il faut savoir qu'un grand nombre de ces informations sont accessibles via des bases de données publiques ou les réseaux sociaux.

Les journalistes sont particulièrement exposés aux risques de « doxxing » et sont susceptibles de devenir une cible de menaces et d'intimidations.

Afin de se protéger, le "self-doxxing" permet de prendre des décisions éclairées sur les informations à partager en ligne et celles qui ne le doivent pas. Ce guide vise à vous aider à minimiser les risques d'utilisation d'informations privées à votre encontre.

La démarche à adopter est celle de se positionner à la place du « Doxxer ». :

- Que cherche-t-il ?
- Où trouve -t-il des informations personnelles ? Sur quelles plateformes en particulier?
- Comment peut-il exploiter ces informations et pour en faire quoi ?

Après avoir identifié les informations à rechercher, le présent guide vous aidera à vérifier si les informations recherchées sont accessibles en ligne.

Étape 1 : Vérifier sa présence sur ls différentes moteurs de recherches

Effectuez une recherche sur Google et d'autres moteurs de recherche vous concernant afin de savoir quelles informations sont disponibles en ligne.

1. Faites défiler les différents résultats générés par le moteur de recherche pour voir quelles informations sont disponibles en ligne sur vous. Prenez le temps d'examiner les différentes sources où vous apparaissez.
2. Affiner la recherche en ajoutant des mots clés ou des indications comme le lieu de résidence, la profession, les écoles fréquentées, etc., il en résulte des données plus précises ;
3. Effectuer une recherche d'images inversées sur les moteurs de recherche en utilisant les photos de profil des différents comptes tels que LinkedIn, Twitter, Facebook et Instagram.
4. Procéder de la même manière, sur d'autres moteurs de recherche, tels que Bing, Yahoo et DuckDuckGO.

<u>Conseils de pro:</u>

- Pour affiner les résultats sur Google et Bing, on peut utiliser les opérateurs booléens, qui suivent :

Opérateurs de recherche Google et Bing		
Opérateurs	**Ce qu'il recherche**	**Exemple**
Site	Fournit les résultats des pages situées sur un site spécifique	site: linkedin.com
ET/OU	L'opérateur ET permet d'obtenir des résultats contenant deux résultats. L'opérateur OU permet d'obtenir des résultats contenant l'un ou l'autre des résultats.	"Jean Dupont" ET (Toronto OU Montréal)
L'astérisque	Cet opérateur permet d'accroître les résultats de la recherche en	"Jean * Dupont"

	isolant la racine d'un terme. La recherche devient plus vaste car elle inclut toutes les variantes de ce terme ou tous les mots de la même famille.	
Tiret	Cet opérateur permet d'exclure le texte qui le suit immédiatement.	"Jean Dupont" -site:yournewssite.com
Filetype	Filtrer les résultats de la recherche en fonction d'un type de fichier Types de fichiers courants : ● DOC/DOCX ● XLS/XLXS ● PPT/PPTX ● TXT ● JPG/JPEG/PNG (Image) ● PDF	filetype:xls intext:toi@toncourriel.com

<u>Recommandations:</u>

- Prendre le temps de réfléchir au contexte et à l'endroit où des informations personnelles sont communiquées. Par exemple, si l'on signe une pétition en ligne, des informations personnelles risquent d'être publiées.
- Des alertes Google peuvent être créées afin de recevoir des notifications à chaque nouvelle information publiée en ligne, sur vous. Pour créer des alertes Google, il faut se rendre sur l'adresse : https://www.google.com/alerts.
- Passer en revue les biographies, CV et sites web personnels afin d'identifier toute information personnelle accessible au public. Utiliser des techniques de recherches avancées en usant des opérateurs de recherche pour localiser des documents PDF, des curriculum vitae accessibles au public, etc. Pour tout CV en ligne, supprimer l'adresse personnelle, l'adresse électronique privée et le numéro de téléphone privé et remplacez-les vos coordonnées professionnelles.
- Limiter la géolocalisation du téléphone. Vérifier sur le téléphone les paramètres de chaque application.

Il est judicieux de consulter régulièrement Google ou d'autres moteurs de recherche pour vérifier vos informations disponibles en ligne.

Étape 2 : Vérifier vos réseaux sociaux

Certains paramètres sont définis comme **"publics"** par défaut, d'où la divulgation d'informations personnelles, sans consentement préalable. C'est exactement le type d'informations recherchées par les cybercriminels qui les utiliseront à votre encontre par l'intermédiaire de vos comptes sur les réseaux sociaux.

Il faut faire un choix stratégique des plateformes que vous utilisez et à quelles fins. Si vous utilisez une plateforme à des fins personnelles (exemple : partage de photos avec vos amis et votre famille sur Facebook ou Instagram), vous devez resserrer vos paramètres de confidentialité.

En revanche, si vous utilisez une plateforme à des fins professionnelles, par exemple pour suivre l'actualité sur Twitter et tweeter des informations, vous pouvez décider de laisser certains paramètres publics. Dans ce cas, il faut éviter de publier des informations et des images susceptibles de contenir des informations confidentielles, telles que votre date d'anniversaire, votre numéro de téléphone, votre localisation, votre adresse personnelle, ainsi que les noms et les photos des membres de votre famille ou de vos amis.

1. Noter les noms des différentes plateformes de médias sociaux que vous utilisez. Déterminer l'usage de chaque compte : l'est-il à des fins professionnelles, personnelles ou les deux ?

2. Passer en revue le contenu publié sur vos profils. Revenez sur vos anciennes publications et assurez-vous que vous souhaitez conserver les anciennes informations/photos. Sélectionner les informations/photos qui ne doivent plus être publiques, en les supprimant ou les archivant.

3. Examiner les différents paramètres de confidentialité et de sécurité de chaque plateforme, de manière de s'assurer que les informations partagées ne vous rendent pas vulnérables. Au besoin, ajustez vos paramètres pour limiter le nombre de personnes pouvant accéder à votre profil et à vos publications.

4. Si vous avez des comptes sur des réseaux sociaux que vous n'utilisez plus, envisagez de les supprimer ou de les désactiver.. Pour cela, utilisez des bases de données comme PeekYou ou Namecheckr pour savoir où votre pseudonyme est utilisé

5. Désactiver les paramètres de localisation sur vos différentes plateformes, afin que vos publications et photos sur les médias sociaux ne partagent pas votre position en temps réel.

Conseils de pro :

- Utilisez l'option «**Voir en tant que**» sur Facebook pour vérifier l'apparence de votre profil pour les personnes ne faisant pas partie de vos amis Facebook.
- Passez en navigation privé pour trouver vos autres plateformes sociales et voir quelles informations sont accessibles au public.

Recommandations:

- Prenez le temps d'examiner les différents paramètres de sécurité de vos plateformes sociales et de les configurer en conséquence.
- Avant de publier un contenu sur les réseaux sociaux, prenez le temps de vous assurer qu'il ne contient pas d' informations personnelles permettant de vous localiser, d'avoir accès à vos coordonnées ou des informations sur vos proches. Observez les différents angles des photos postées, peut-on avoir un indice sur le quartier dans lequel vous vivez (par exemple, votre rue est-elle repérable par un signe distinctif, un bois, une école, un magasin) ?
- Il est important de se rappeler que la famille et les amis peuvent aussi être victimes de doxxing. Si vous pensez être une personne à risque, échangez, discutez avec vos proches sur leur utilisation des médias sociaux, et des informations qu'ils peuvent révéler sur eux-mêmes et par ricochet sur vous.
- Une vérification régulière de vos comptes peut vous aider à garder le contrôle sur les informations vous concernant et disponibles en ligne.
- Si vous envisagez d'utiliser différents profils de médias sociaux à des fins professionnelles et personnelles, pensez à utiliser un pseudonyme sur votre compte personnel afin que les « trolls » aient plus de mal à vous trouver.
- Utilisez les options de blocage, de mise en sourdine ou de restriction sur vos différentes plateformes de médias sociaux si vous recevez des contenus abusifs non sollicités.
- Suivez les conseils, recommandations et mises en garde pour chaque média social, qui suit :

- Ne partagez pas d'informations en temps réel
- Assurez-vous que vos photos personnelles sont accessibles qu'à un certain groupe de personnes ;
- Masquez votre liste d'amis de la vue du public
- Déterminer qui peut vous trouver et vous contactez à l'aide de votre adresse électronique ou de votre numéro de téléphone
- Interdisez aux moteurs de recherche de créer des liens vers votre profil
- Vérifiez comment d'autres comptes peuvent interagir et publier sur votre profil
- Vérifiez qui peut vous identifier dans les publications et les photos
- Bloquez les commentaires sur certaines photos
- Évitez d'identifier les membres de votre famille et vos amis
- Supprimez ou archivez les photos qui peuvent révéler des informations personnelles

- Il est possible d'avoir un compte Instagram privé ou public
- Si vous souhaitez que votre compte reste public, assurez-vous que certains utilisateurs ne puissent pas vous identifier ou vous mentionner dans les photos, les vidéos et les commentaires
- Supprimez ou archivez les photos qui pourraient fournir des informations personnelles
- Évitez d'identifier vos proches sur vos publications personnelles
- Ne partagez vos stories personnelles, qu'avec vos amis proches ; assurez-vous que cette liste est à jour
- Instagram offre la possibilité de désactiver les commentaires, sous vos publications

- Les informations peuvent être diffusées TRÈS rapidement sur Twitter. Il est essentiel de prendre le temps de relire et de vérifier toute information avant de les publier sur cette plateforme
- Désactivez l'identification des photos et de la localisation
- Utilisez l'option de mise en sourdine des mots et des hashtags. Twitter supprimera automatiquement tous les tweets contenant ces mots ou hashtags de votre fil d'actualité
- Si vous ne souhaitez pas recevoir des messages d'un utilisateur inconnu, désactivez le paramètre « *Autoriser les demandes de messages de la part de tout le monde* »
- Modifiez qui peut consulter votre profil à l'aide de votre adresse électronique ou de votre numéro de téléphone
- Passez en revue vos anciens tweets
- Appliquez des filtres de qualité

Étape 3 : Examiner les annuaires en ligne

Address search

Recherche d'adresse

Consultez les annuaires en ligne, tels Canada411, pour vérifier si votre nom, votre adresse ou votre numéro de téléphone y figurent. Sans le savoir, votre adresse personnelle ou votre numéro de téléphone peuvent y figurer. Pour supprimer ces informations, vous devez envoyer une demande par l'intermédiaire de la plateforme. Voir les recommandations ci-dessous.

Conseils de pro :

- Lorsque vous effectuez ce type de recherche, soyez précis quant à la zone dans laquelle vous vivez. Il se peut que les résultats ne s'affichent pas si vous recherchez dans une zone trop large (par exemple, si vous habitez à Longueuil, mais que vous entrez Montréal dans la barre de recherche, vous ne trouverez pas la réponse).
- Recherchez les membres de votre famille sur cette base de données. Par inadvertance leurs noms ont pu s'afficher sur vos photos ou vos commentaires, d'où la possibilité de transfert d'informations dans ces bases de données.

Recommandations:

- Si l'information se trouve sur Canada411, la procédure de retrait est simple et rapide. Vous devez en faire la demande en cliquant sur le lien ci-dessous (il faut compter deux jours ouvrables pour que les informations soient supprimées). Vous devrez également demander à votre opérateur téléphonique de changer votre numéro de téléphone pour un numéro privé (cette demande peut prendre plus de temps) : https://www.fr.canada411.ca/help.html?key=faq.

Étape 4 : Surveiller les fuites de données

Vos informations personnelles peuvent être compromises/exposées dans le cadre d'une fuite de données. Haveibeenpwned.com vous permet de déterminer si l'un de vos comptes a été affecté par une brèche de données significative.

Recommandations:

- Modifiez immédiatement le(s) mot(s) de passe de tous les comptes concernés et ne les utilisez plus. Vous pouvez également utiliser un gestionnaire de mots de passe si vous craignez de les oublier. Un bon gestionnaire de mots de passe est généralement équipé d'une surveillance du Dark web et des brèches de données ; certains envoient des alertes proactives pour vous avertir que vos données ont été compromises.

Les bases de données publiques

Au Canada, les registres publics peuvent être conservés sur des sites relevant du provincial ou du fédéral. Les catégories de registres accessibles au grand public peuvent varier en fonction des juridictions.

Il faut noter que tous les documents publics ne sont pas tous accessibles aux citoyens. Certains peuvent nécessiter une autorisation ou un paiement pour être consultés, alors que d'autres sont protégés par les lois sur la protection de la vie privée, en particulier lorsqu'ils comportent des informations sensibles et/ou confidentielles.

De même, il est important de savoir que l'on ne peut demander la suppression d'informations publiques entrant dans *la catégorie d'informations accessibles à tous les citoyens.*

1. **Les registres de l'état civil.** Il s'agit des registres officiels des naissances, des décès et des mariages qui sont généralement conservés par le gouvernement provincial ou territorial. Si les mariages et les naissances ne sont pas accessibles au public, les décès le sont, d'où un accès aux noms de vos proches.

2. **Le rôle de l'évaluation foncière**. Ces registres contiennent des informations sur la propriété foncière, la valeur des biens et les limites des propriétés. Ils sont généralement tenus par le gouvernement provincial ou territorial.

3. **Les plumitifs.** Ces dossiers contiennent des informations sur les poursuites judiciaires, les jugements et les décisions. Ils sont généralement conservés par les tribunaux et peuvent être accessibles au public. En fonction de la nature du dossier (criminel, civil ou municipal), l'adresse et la date de naissance peuvent être divulguées.

4. **Les registres des entreprises**. Ces registres comprennent des informations sur les entreprises enregistrées au Canada (fédéral ou provincial) , telles que leur nom, leur adresse et leurs activités commerciales

5. **Les registres électoraux** sont des bases de données comprenant des informations sur l'inscription des électeurs et les résultats électoraux. Ils sont généralement conservés par le gouvernement fédéral ou provincial. Selon la province, il est possible de savoir si une personne est inscrite sur une liste électorale. Il est donc facile pour un individu de vérifier l'adresse d'une personne.

6. **Autres registres gouvernementaux**. Certains registres contiennent des informations personnelles précieuses tels que les droits personnels et réels mobiliers. Les gouvernements provinciaux gèrent ces bases de données.

Autres recommandations en matière de sécurité de l'information

- Distinguez votre adresse électronique professionnelle, de votre adresse personnelle, ainsi que vos numéros de téléphone. N'utilisez vos comptes professionnels qu'à des fins professionnelles. Soyez prudent quant aux informations d'identification incluses dans votre signature courriel.
- Utilisez l'authentification à deux facteurs, cela ajoute une couche de sécurité supplémentaire à vos comptes de médias sociaux. Un acteur de menace aura plus de difficulté à compromettre votre compte.
- Soyez prudent avec les applications tierces qui demandent l'accès à vos plateformes sociales. Ces applications peuvent parfois être utilisées pour collecter des informations personnelles.
- Utilisez une application de messagerie sécurisée si vous devez discuter avec une source ou partager des informations personnelles.
- Envisagez d'utiliser un réseau privé virtuel (RPV). Il prémunit contre l'interception des informations et protège la confidentialité de vos échanges d'informations en masquant votre adresse IP.
- Faites attention aux tentatives d'hameçonnage. Méfiez-vous des liens ou des messages suspects que vous recevez sur les réseaux sociaux. Il peut s'agir de techniques de phishing visant à voler vos informations personnelles ou vos identifiants.
- Vérifiez régulièrement les autorisations de vos applications et révoquer l'accès à toute application que vous n'utilisez plus ou en qui, vous n'avez plus confiance.

En prenant des mesures proactives visant à protéger vos informations personnelles en ligne, vous réduirez le risque d'être doxxé.

N'oubliez pas de limiter votre empreinte en ligne. De sécuriser vos comptes de réseaux sociaux ; de faire preuve de prudence lorsque vous partagez vos informations personnelles ; d'utiliser des canaux de communication sécurisés ; de prendre le temps de vous doxxer de temps en temps et d'avoir une conversation avec vos amis et votre famille sur les risques de doxxing.

Découvrir des informations personnelles en ligne peut être déstabilisant.