Homeland Security

Département de la sécurité intérieure
Bureau du partenariat et de l'engagement (OPE)

Ressources pour les personnes au sujet des dangers de la divulgation d'informations personnelles ou doxing

Le 16 janvier 2024

QU'EST-CE QUE LE DOXING ?

Le Doxing fait référence à la collecte d'informations personnellement identifiables (IPI) d'une personne et à leur publication à des fins malveillantes, telles que l'humiliation publique, la traque, l'usurpation d'identité ou le ciblage à des fins de harcèlement.

EXEMPLES D'INFORMATIONS SENSIBLES

- **Nom complet**
- **Coordonnées**
- **Adresse du domicile**
- **Membres de la famille**
- **Informations sur le lieu de travail**
- **Informations financières**
- **Numéro de sécurité sociale**

SOURCES COMMUNES D'INFORMATIONS SENSIBLES

- **Publications sur les réseaux sociaux**
- **Documents immobiliers et judiciaires**
- **Annonces de mariage et nécrologies**
- **Bulletins d'information**
- **Conférences publiques**
- **Forums sur le Web, blogs et forums de discussion**
- **Réseaux non protégés**
- **Listes d'inscription des électeurs**

COMMENT PUIS-JE ME PROTÉGER CONTRE LE DOXING ?

- **Faites attention** à ce que vous publiez sur vous-même en ligne, notamment les photos et les vidéos, même s'il s'agit de publications temporaires.
- **Supprimez** les IPI (adresse, date de naissance, numéro de téléphone, etc.) de vos profils de médias sociaux.
- **Sélectionnez** vos abonnés et rejetez les demandes de toute personne que vous ne connaissez pas.
- **Demandez** la suppression de vos données personnelles des sites Web publics. Les sites Web bien connus sont par exemple BeenVerified, FastPeopleSearch, Intelius, PeopleFinders, Spokeo, TruthFinder et Whitepages.
- **Supprimez** les applications et extensions de navigateur inutiles pour éviter la collecte de vos données personnelles.
- **Limitez** le suivi de localisation sur les applications et les sites Web. Désactivez les services de localisation pour chaque application ou plateforme.
- **Activez** les fonctionnalités de confidentialité sur les réseaux sociaux, les applications et autres sites Web.
- **Configurez** la double authentification, utilisez des mots de passe complexes et ne réutilisez pas le même mot de passe pour plusieurs comptes.

Bureau OPE du DHS

COMMENT PUIS-JE ME PROTÉGER CONTRE LE DOXING ?

Demandez la suppression du contenu faux, abusif ou injurieux
Envisagez de soumettre une demande de retrait à la plateforme ou au site Web, conformément aux règles et aux exigences.

Documentez ce qui se passe
Envisagez de prendre des mesures pour préserver les preuves. Enregistrez tous les e-mails, messages vocaux et SMS que vous recevez et prenez des captures d'écran ou des photos des commentaires sur les réseaux sociaux.

Signalez l'incident
Si vous avez fait l'objet d'une menace pour votre sécurité physique ou si vous vous sentez harcelé(e) de manière criminelle, signalez l'incident aux forces de l'ordre locales, ainsi qu'à la plate-forme de médias sociaux ou à l'administrateur du site Web.

RESSOURCES ET CONSEILS SUPPLÉMENTAIRES

Meilleures pratiques de la CISA et ressources en matière de cybersécurité : cisa.gov/cybersecurity

CISA Cyber Essentials : cisa.gov/cyber-essentials

Conseil pratique CISA : Éviter les attaques d'ingénierie sociale et d'hameçonnage : cisa.gov/tips/st04-014

Informations CISA : Améliorer la sécurité des e-mails et du Web : www.cisa.gov/resources-tools/resources/enhance-email-web-security

Infographie sur les conseils de la CISA en matière de danger des réseaux sociaux pour le personnel des établissements scolaires et les autorités : https://www.cisa.gov/resources-tools/resources/social-media-threat-guidance-school-staff-and-authorities-infographic

Si vous êtes victime d'un crime en ligne, déposez une plainte auprès du Centre de traitement des plaintes contre la criminalité sur Internet (IC3) du FBI à www.ic3.gov