INSI

Défense numérique

Gestion des abus en ligne à l'intérieur et en dehors de la salle de rédaction

JOURNALISM | SAFETY | RESPONSIBILITY | COMMUNITY

Index

Introduction

Le secteur des médias est confronté à une vague incessante de harcèlement en ligne visant les journalistes – qu'il s'agisse d'acteurs étatiques, de réseaux criminels organisés, de bots ou de membres du public enhardis par l'anonymat. Discours haineux, désinformation et menaces de violence physique sont le quotidien de nombreux confrères. Certains sont contraints de quitter la profession ; d'autres subissent des séquelles psychologiques durables — alors même que le journalisme indépendant et approfondi n'a jamais été aussi nécessaire.

La violence numérique est notoirement difficile à contenir. Mais une chose est claire : les journalistes attendent de leurs employeurs qu'ils prennent les choses en main — avant, pendant et après les attaques — en apportant non seulement un soutien, mais aussi en prenant des actions concrètes.

Les organisations membres de l'INSI se réunissent depuis 2020 pour partager leurs approches et les leçons difficilement acquises. L'initiative Google News et Facebook ont soutenu et participé aux premières étapes de ce travail, et nous reconnaissons leur contribution.

Ce guide — rédigé pour l'INSI par Mike Christie, un acteur clé de cette démarche — s'appuie sur ces échanges et ceux qui ont suivi. En tant que responsable mondial de la sécurité chez Reuters, il a contribué à définir des normes de référence sur la manière dont les rédactions peuvent protéger leur personnel face aux menaces physiques, numériques et émotionnelles. Son travail a joué un rôle décisif dans l'élaboration des meilleures pratiques à l'échelle de l'industrie.

Ce guide est destiné aux responsables de rédaction —de l'éditorial, à la sécurité ou des ressources humaines — afin de leur fournir un cadre pratique pour atténuer l'impact des abus en ligne et se préparer si les menaces numériques se traduisent par un danger réel.

Chaque rédaction a son propre profil de risque, sa culture et ses ressources. Mais aucune ne devrait affronter seule la violence numérique. Une collaboration à l'échelle du secteur — avec un engagement des plateformes à propos de l'application des règles et la redevabilité, et avec les gouvernements sur des régulations efficaces — aura plus d'impact que des efforts isolés. L'INSI encourage tous ses membres à participer activement à ces initiatives partagées et à ancrer l'esprit de résilience collectif dans leur réponse en salle de rédaction.

Nous savons que de nombreuses rédactions connaissent déjà bien l'ampleur et la nature des abus en ligne — et que le temps leur manque. C'est pourquoi ce guide commence par les mesures applicables les plus urgentes. Il s'ouvre sur un cadre pratique de réponse au harcèlement numérique, à l'intention des responsables en charge de la sécurité et du bien-être du personnel, avant d'aborder le contexte et arrière-plan plus vastes.

En annexe, vous trouverez des listes de contrôle couvrant les principales stratégies d'atténuation, notamment l'auto-doxxing et la planification des réponses. Nous espérons que ce guide sera une ressource utile et accessible que ce soit pour les journalistes, les responsables de services et les professionnels de la sécurité.

Mesures préventives

Dans un monde hyperconnecté, les journalistes sont exposés à des risques croissants, les agresseurs exploitant les appareils liés au cloud et les données partagées sur plusieurs plateformes. Une menace vague est déjà préoccupante — mais lorsqu'elle inclut le nom de l'école d'un enfant ou la photo d'une chambre publiée en ligne par une agence immobilière, le danger devient bien réel. Une planification proactive est essentielle pour maintenir la préparation des rédactions.

1. Quantifier le problème

Réalisez une enquête au sein de la rédaction pour évaluer l'ampleur du harcèlement en ligne et des abus connexes dans votre organisation. Veillez à consulter les femmes et les journalistes issus de minorités, qui sont les plus exposés à ces abus.

2. Proposer des formations

Intégrez des informations de base sur le harcèlement en ligne, ses impacts et la réponse de votre organisation dans toutes les formations sur les environnements hostiles et les modules de cybersécurité. Vous pouvez également organiser des ateliers spécifiquement consacrés au harcèlement en ligne.

3. Créer des canaux de signalement

Faites la promotion des canaux de communication disponibles qui permettent de signaler le harcèlement en ligne, notamment lorsqu'il passe par des messages personnels ou les réseaux sociaux. Il peut s'agir d'un canal Teams ou Slack, ou simplement d'une adresse de courriel. Envisagez aussi de créer un canal où les journalistes peuvent partager leurs expériences de harcèlement en ligne : cela permettrait de repérer des tendances émergentes et de favoriser le soutien entre collègues.

Veillez à ce que l'équipe chargée de la sécurité éditoriale soit informée à l'avance de toute couverture susceptible de déclencher une campagne en ligne, au lieu d'attendre de gérer les conséquences.

4. Mener un auto-doxxing

Demandez aux journalistes d'effectuer des exercices d'auto-doxxing de base pour évaluer quelles informations sensibles peuvent être retrouvées à leur sujet en ligne. Il est impossible de faire disparaître tout ce qui a été accumulé au fil des décennies de vie en ligne — par exemple, aux États-Unis, toute personne propriétaire d'un bien immobilier verra son adresse apparaître dans les registres publics. Mais des données peuvent fuiter via des profils sociaux dont les paramètres de confidentialité ne sont pas correctement configurés. Intégrez cet exercice dans le processus d'intégration des nouvelles recrues.

5. Faire des recherches approfondies

Menez des recherches plus poussées sur les vulnérabilités numériques des journalistes très visibles ou travaillant sur des sujets sensibles. Les départements de sécurité informatique ou de gestion des risques peuvent s'en charger, ou faire appel à un prestataire externe.

6. Utiliser des services de suppression de données

Envoyez des demandes automatiques de retrait auprès des courtiers en données personnelles à l'aide de services comme DeleteMe. Bien que ces services ne soient pas disponibles dans tous les pays, souscrivez une formule entreprise pour la rédaction ou des comptes individuels. Ils n'agissent généralement pas sur la source originale des informations rassemblées, mais permettent d'en limiter la diffusion.

7. Employer des services de veille sur les menaces sécuritaires

De nombreuses organisations médiatiques utilisent des services de surveillance de marque et de réputation qui détectent les infractions au droit d'auteur, les sites ou comptes usurpateurs, et les contenus critiques pouvant nuire à leur image. Des services similaires existent pour surveiller les menaces sécuritaires pesant sur les rédactions ou les journalistes individuellement. Certains explorent le dark web et les zones moins accessibles comme les groupes de discussion sur Telegram.

8. Supprimer les anciennes publications sur réseaux sociaux

Nettoyez les commentaires publics susceptibles de compromettre la sécurité ou l'intégrité d'un journaliste, surtout s'ils datent de ses jeunes années. Des opinions politiques passées, même si elles ne sont plus d'actualité, peuvent disqualifier un journaliste pour couvrir une campagne électorale. Des photos de fêtes étudiantes peuvent poser problème s'il est amené à traiter avec des groupes ultraconservateurs. Envisagez d'intégrer cette démarche au processus d'intégration.

9. Maintenir des profils "à faible niveau de détail"

Le sourire d'un reporter télé peut faire partie de sa marque, mais un journaliste d'investigation financière a-t-il vraiment besoin d'un portrait sur ses profils ? Les photos de profil peuvent permettre d'identifier un journaliste via des logiciels de reconnaissance faciale. Les femmes journalistes, plus exposées aux abus en ligne, peuvent envisager de créer des profils neutres du point de vue du genre.

10. Séparer vie privée et vie professionnelle

Réfléchissez à la possibilité de séparer complètement les identités en ligne privées et professionnelles, en créant des comptes distincts. Les profils privés doivent être réservés à la famille et aux amis, entièrement verrouillés, et ne contenir ni sources ni collègues. Les profils professionnels doivent rester axé sur le travail, avec un minimum d'informations personnelles, en gardant à l'esprit que tout ce qui y est publié pourrait être public et utilisé par un adversaire.

11. Fournir une formation aux prises de parole en public

Proposez une formation sur la manière dont les journalistes doivent gérer leurs apparitions publiques. Les groupes d'extrême droite cherchent souvent à embarrasser ou piéger les journalistes en leur posant des questions provocatrices lors d'événements publics, puis en diffusant leurs réponses en ligne. D'autres se font passer pour des sources en proposant de faux scoops dans l'espoir de faire émerger un biais qui pourrait nuire à leur crédibilité.

12. Identifier les personnes ou groupes vulnérables

Certains journalistes peuvent avoir besoin d'un soutien ou d'une formation supplémentaire, notamment :

- Les journalistes politiques et les vérificateurs de faits
- Ceux travaillant dans des pays où le harcèlement en ligne est militarisé par l'État
- Les femmes, les personnes de couleur, les personnes LGBTQ+
- Ceux ayant une forte visibilité en ligne ; qui ont été publiquement critiqués par des personnalités ou dirigeants ; ou qui couvrent des sujets géopolitiques clivants qui ont divisés l'opinion publique.

13. Modérer les commentaires

Maintenir un espace de discussion protégé et civilisé dans les commentaires en ligne est un véritable défi qui demande des ressources dédiées. Certaines rédactions désactivent simplement les commentaires. D'autres utilisent des outils automatisés ou une combinaison d'intelligence artificielle et de modération humaine.

Les commentaires haineux visant une entreprise ou ses sites, même s'ils ne s'adressent pas à un journaliste en particulier, doivent malgré tout être surveillés s'ils expriment une intention de nuire dans le monde réel.

14. Mettre en place une équipe de réponse interdépartementale

Réagir efficacement à un cas grave de harcèlement en ligne peut nécessiter l'intervention de plusieurs départements. Impliquez-les à l'avance pour garantir une réponse coordonnée. Constituez un groupe de travail ou une cellule de crise pour gérer les incidents majeurs, qui comprenne :

- **Direction éditoriale.** Décide du déplacement d'un journaliste en lieu sûr, du recours à des services de sécurité ou aux autorités.
- **Sécurité éditoriale.** Gère toutes les menaces — physiques, émotionnelles ou numériques — pesant sur les journalistes.
- **Sécurité informatique.** Bloque les attaques, identifie leur origine, évalue leur gravité, consigne les incidents et analyse les tendances.
- **Sécurité des locaux.** Interdit l'accès des locaux ou de la salle de rédaction aux harceleurs identifiés.
- **Service juridique.** Engage des actions en justice contre les harceleurs en ligne, en tenant compte des limites liées à la liberté d'expression.
- **Ressources humaines.** Offre un soutien émotionnel ou un accompagnement psychologique aux journalistes visés ; donne son avis sur un éventuel déplacement temporaire.
- **Communication.** Prend position publiquement, par exemple en intervenant dans un fil de commentaires.
- **Soutien entre pairs.** S'assure que les journalistes concernés sont soutenus par leurs collègues.

15. Fournir des recommandations de sécurité éditoriale

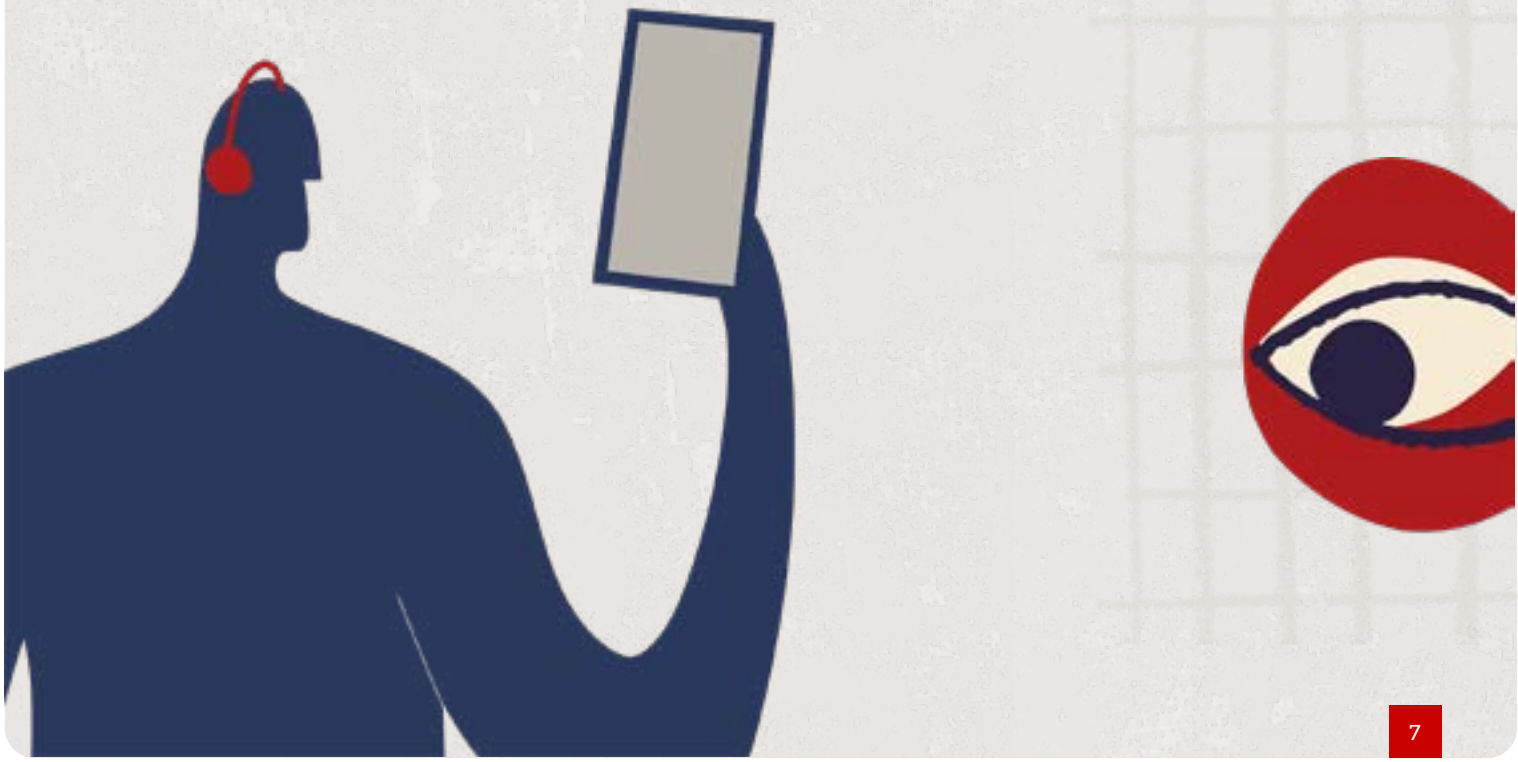
La bibliothèque interne des recommandations de sécurité de la rédaction devrait inclure des ressources sur la nature du harcèlement en ligne, ses effets, et les mesures de soutien mises en place. Les consignes de base en matière de sécurité informatique doivent également traiter du harcèlement numérique.

16. Réduire les risques

Les règlements sur le BYOD (Bring Your Own Device – utiliser son propre appareil) et le recours fréquent à des pigistes compliquent la sécurisation des dispositifs et des données dans les rédactions. Une application de messagerie sécurisée utilisée pour contacter une source sensible peut se retrouver à la fois sur l'ordinateur personnel et l'ordinateur professionnel d'un journaliste. Les échanges peuvent être sauvegardés de manière non sécurisée sur un cloud auquel l'équipe de sécurité informatique n'a pas accès.

Voici quelques moyens de réduire les risques:

- Envisagez de publier les sujets les plus controversés sans signature. Cette option est souvent rejetée par les journalistes : leurs préférences doivent être prises en compte.
- Réexaminez la politique de publication des profils détaillés de journalistes sur les sites web et l'inclusion des liens vers leurs réseaux sociaux dans les articles. Bien que cela puisse contribuer à leur désir de visibilité professionnelle, cela augmente aussi la quantité d'informations personnelles sensibles disponibles en ligne. Ces profils contiennent souvent des photos, facilitant le suivi par des individus malveillants utilisant des logiciels de reconnaissance faciale.
- Les paramètres qui permettent à un contenu de devenir viral peuvent aussi faciliter le harcèlement. Élaborez des lignes directrices sur ces réglages et réfléchissez à leur usage stratégique et sécurisé.



Mécanismes de signalement

Établir un climat de confiance avec les journalistes

Le harcèlement en ligne ne passe pas toujours par des canaux de communication contrôlés par l'entreprise, tels que les posts publiques ou les courriels professionnels. Il arrive souvent par messagerie directe sur les comptes de réseaux sociaux personnels des journalistes.

Les journalistes devraient signaler ces abus, mais s'en abstiennent souvent. Ils peuvent considérer cela comme un "risque du métier" ; craindre que cela remette en question leur intégrité, leur professionnalisme ou la véracité de leur travail, en particulier si cela soulève des doutes sur leurs qualifications ; ou redouter d'être retirés de l'enquête en cours. Il est donc essentiel de les encourager à signaler les abus. Parmi les moyens d'y parvenir:

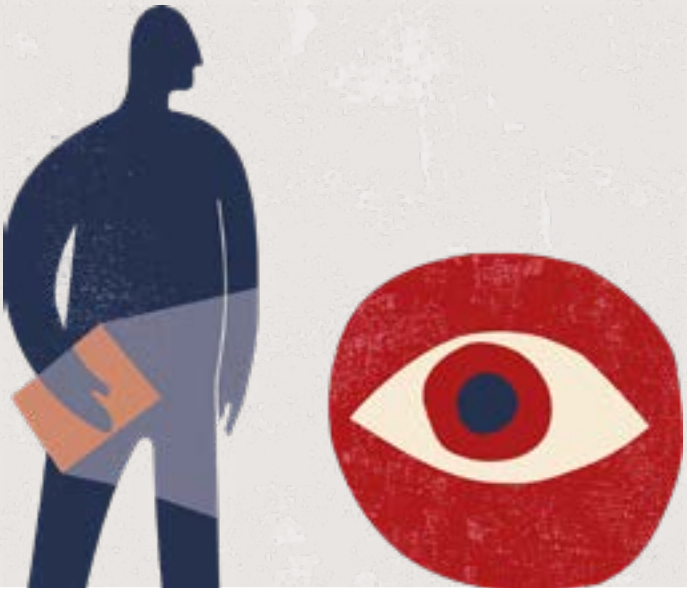
- **Formation et sensibilisation.** les journalistes ne doivent pas minimiser la gravité du harcèlement en ligne. Les formations doivent expliquer comment l'entreprise entend stopper les abus, souligner le soutien apporté aux journalistes, et les rassurer sur le fait qu'ils ne seront pas retirés d'un sujet s'ils signalent les attaques.
- **Créer des canaux de signalement.** Slack, Teams, des formulaires ou une adresse courriel dédiée peuvent être utilisés. Il est essentiel de surveiller ces canaux de signalement, sinon les journalistes perdront confiance dans le processus.

Signaler les abus aux plateformes de réseaux sociaux

Certaines entreprises de réseaux sociaux ont mis en place des portails partenaires spécifiques pour signaler des problèmes ou désigné des interlocuteurs dédiés. Ces portails offrent souvent la possibilité de signaler un compte piraté, un vol d'identifiants, un cas de harcèlement en ligne ou tout autre incident. Il peut également exister un point de contact direct au sein de la plateforme pour les utilisateurs professionnels ou institutionnels en cas de problème.

Dans d'autres cas, ce sont les utilisateurs eux-mêmes qui doivent signaler les cas de harcèlement ou les problèmes directement à la plateforme concernée.

Les responsables doivent comprendre quelles plateformes sont utilisées par leurs journalistes, et comment chaque plateforme traite les plaintes.



Mécanismes de surveillance

Le harcèlement en ligne visible publiquement peut être surveillé à l'aide d'outils permettant aux organisations de presse de détecter des menaces plus larges à l'encontre de leurs rédactions et de leurs infrastructures. Bon nombre de ces outils sont conçus pour la protection de marque. Certains peuvent explorer le dark web, le deep web ou encore les groupes de discussion sur des applications comme Telegram, en plus du web public.

Certains outils plus récents permettent également de surveiller les menaces ou attaques transmises par messagerie directe, mais cela nécessite le consentement du journaliste pour inclure ses comptes personnels dans cette surveillance.

Une autre option consiste à utiliser des outils de filtrage automatisé visant à protéger les journalistes (et autres utilisateurs) de l'impact émotionnel des messages haineux. Ces outils peuvent masquer les messages contenant certains mots ou contenus.

Ce type de modération de contenu peut être bénéfique en ce qu'il protège les cibles d'un certain préjudice émotionnel, mais il présente également un risque : celui de masquer des menaces sérieuses nécessitant une réponse. Certains outils récents basés sur l'intelligence artificielle combinent ces deux fonctions : ils protègent les journalistes tout en signalant les messages à risque.

Mécanismes de réponse

Une fois les mécanismes de signalement et de surveillance en place, les rédactions peuvent se retrouver à analyser des centaines de messages pour déterminer si certains présentent un risque concret dans le monde réel. Faire le tri parmi les harceleurs pour identifier ceux qui ont un passé criminel ou violent revient parfois à chercher une aiguille dans une botte de foin.

Voici quelques éléments à prendre en compte pour décider de la réponse à adopter:

1. Identifier les agresseurs

Google constitue souvent un bon point de départ et peut livrer des résultats surprenants. Les pseudonymes sont fréquemment utilisés sur plusieurs sites, ce qui peut permettre d'identifier un expéditeur. Des services en ligne comme Social Catfish permettent de rechercher une adresse courriel, tandis que PeekYou analyse les pseudonymes.

Le département de sécurité informatique d'une entreprise médiatique peut aussi déterminer l'emplacement d'une adresse IP. Nombre d'agresseurs utilisent toutefois des VPN pour masquer leur localisation, et créent des comptes jetables qui disparaissent dès qu'ils sont signalés.

2. Analyse des menaces et tri

Certains indicateurs montrent qu'une menace en ligne pourrait évoluer vers une violence physique:

- **Menace directe.** Une phrase comme « Je vais te tuer » est bien plus inquiétante qu'une menace indirecte telle que « Tu devrais être exécuté pour trahison », souvent protégée par la liberté d'expression.
- **Exposition accrue.** L'adresse du domicile du journaliste a-t-elle été révélée ? La divulgation de sa localisation le met-elle en danger ?
- **Dissimulation d'identité.** Un agresseur qui cache son identité sait probablement que son comportement est répréhensible. Inversement, un individu agissant sous son vrai nom peut représenter un danger car il ne réalise pas la gravité de ses actes.
- **Proximité géographique.** Une personne vivant à proximité est plus menaçante qu'un individu résidant à l'autre bout du monde.
- **Casier judiciaire ou passé violent.** L'agresseur a-t-il des liens avec des groupes extrémistes ou une autorisation de port d'armes ?
- **Escalade.** Les attaques passent-elles d'une plateforme à l'autre et se multiplient-elles ? Sont-elles de plus en plus agressives ?

- **Organisation.** L'attaque est-elle menée par un État ou un groupe structuré ? Ont-ils déjà eu recours à la violence ? Peuvent-ils engager des poursuites ou détenir un journaliste ?
- **Bots.** Soyez attentifs aux comptes récemment créés, sans historique, ou déjà impliqués dans d'autres campagnes similaires.

3. Protéger les cibles

Bloquer les agresseurs en ligne peut sembler une solution évidente pour préserver la santé mentale des journalistes. Toutefois, ce geste peut aussi provoquer une escalade invisible : les harceleurs créent souvent de nouveaux comptes pour poursuivre leurs attaques.

Une autre option consiste à confier la surveillance des comptes de réseaux sociaux à l'équipe sécurité ou au service informatique. Cependant, les journalistes peuvent être réticents à partager leurs mots de passe ou à autoriser l'accès à des messages provenant de sources sensibles.

Dans ce cas, un collègue ou un responsable éditorial pourrait assurer une surveillance intermédiaire des messages, en impliquant les spécialistes sécurité et informatique si nécessaire.

4. Agir rapidement

Les rédactions doivent agir sans délai lorsqu'elles estiment qu'un harcèlement en ligne peut déboucher sur un préjudice grave. Parmi les mesures envisageables:

- **Contacter les autorités.** Les menaces explicites doivent toujours être signalées à la police ou aux services compétents. Dans certains cas, le journaliste devra déposer plainte lui-même.
- **Verrouiller** les bureaux
- **Interdire l'accès aux agresseurs connus en les ajoutant à la liste d'individus déjà interdits**, et informer les prestataires externes ainsi que les propriétaires des locaux.
- **Sécuriser le domicile ou le lieu de résidence temporaire du journaliste** installer un système d'alarme ou souscrire à un service de sécurité privé.
- **Reloger le journaliste et sa famille dans un hôtel avec un bon niveau de sécurité** le temps que la menace soit évaluée.
- **Faire appel à des agents de sécurité privés** pour protéger les figures médiatiques très exposées.
- **Rediriger les courriels professionnels et bloquer les comptes abusifs** sur les messageries personnelles.
- **Désigner une personne en charge de la veille des menaces** reçues sur le compte du journaliste.
- **Signaler l'agresseur à la plateforme concernée.** Souvent, le journaliste devra lui-même soumettre un signalement via les outils internes du réseau social.
- **Engager des poursuites judiciaires si nécessaire.**
- **Collaborer avec d'autres rédactions ou journalistes** pour recueillir des informations utiles à l'évaluation de la menace.
- **Exprimer publiquement un soutien clair à la personne ciblée** pour renforcer sa résilience et son moral.
- **Couverture éditoriale du harcèlement.** Cela peut être une manière constructive de dénoncer une attaque, surtout si elle s'inscrit dans une tendance plus large.

5. Soutenir le ou la journaliste

Être la cible d'un flot de harcèlement peut avoir un impact émotionnel profond. Le soutien de l'organisation est essentiel pour favoriser la résilience et permettre au journaliste de continuer à exercer son métier sans peur. Parmi les mesures à envisager:

- **Mettre en place un accompagnement par les pairs ou des services de soutien psychologique** internes ou externes.
- **Affirmer clairement que l'entreprise soutient le journaliste**, qu'elle ne remet pas en cause son travail ni sa responsabilité dans les attaques subies.
- **Apporter une aide concrète pour signaler l'abus** aux plateformes ou déposer une plainte auprès des autorités.
- **Analyser en profondeur les vulnérabilités numériques du journaliste concerné**, pour s'assurer qu'aucune faille exploitable ne subsiste.
- **Réévaluer la sécurité du domicile** et décider si un déménagement temporaire est nécessaire.
- **Faire écran entre l'agresseur et le journaliste pour rediriger les abus envers l'entreprise** en publiant des déclarations officielles, en intervenant dans des fils de commentaires ou en prenant publiquement la parole.

6. Cas extrêmes

Dans certains cas, le harcèlement en ligne peut atteindre un niveau tel que la sécurité physique de toute la rédaction est menacée. Une campagne délibérée orchestrée par une personnalité politique influente visant à attiser la haine et la colère peut rendre impossible toute couverture sur le terrain, à certains événements ou dans certaines régions. Les équipes sécurité doivent être particulièrement vigilantes face à ce type d'escalade, et prêtes à porter les cas individuels devant la direction générale pour une réponse adaptée au plus haut niveau.

7. Conserver des registres et tirer les leçons

Chaque nouveau cas de harcèlement en ligne est différent et peut offrir des enseignements précieux pour mieux réagir aux attaques futures. Tenir des registres détaillés permet à l'organisation d'identifier les tendances émergentes, et de mieux justifier auprès de la direction générale ou financière l'allocation de ressources pour lutter contre ce phénomène.

Liste de contrôle pour les responsables de rédaction

Mesures préventives	Quantifier le problème	Réaliser une enquête auprès du personnel
	Former et sensibiliser	Intégrer les risques numériques dans toutes les formations de sécurité
	Établir des canaux de communication	Utiliser Teams, Slack ou des courriels dédiés
	Organiser des exercices d'auto-doxxing	Intégrer dans le parcours d'intégration ; proposer des modules d'auto-formation sur l'intranet
	Effectuer des recherches approfondies	Faire appel à un prestataire externe si besoin
	Utiliser des services de suppression de données	Souscrire à un service pour les journalistes à risque
	Mettre en place une surveillance des menaces	Employer des prestataires capables d'explorer le dark web et les groupes privés
	Nettoyer les anciennes publications	Intégrer cette étape dans le processus d'intégration
	Créer des profils "faiblement détaillés"	Intégrer dans les formations de sécurité
	Distinguer profils personnels et professionnels	Discuter avec les journalistes des moyens de séparation des comptes
	Identifier les groupes ou individus vulnérables	Proposer des ateliers spécifiques (vérificateurs de faits, journalistes politiques)
	Former aux apparitions publiques	Proposer des sessions de préparation
	Modérer les commentaires	Faire appel à un prestataire externe si nécessaire
	Mettre en place une équipe de réponse pluridisciplinaire	Impliquer l'éditorial, la sécurité, le juridique, les RH et la communication
	Fournir des recommandations en sécurité éditoriale	Publier des lignes directrices sur l'intranet
	Réduire les risques	Supprimer les photos de profils si besoin

Liste de contrôle pour les responsables de rédaction

Mécanismes de signalement	Créer un canal de communication pour signaler les attaques	Utiliser Teams, Slack, courriels
	Mettre en place des canaux de signalement aux plateformes	Utiliser les portails partenaires, les contacts directs, ou le signalement individuel
Mécanismes de surveillance	Surveiller les menaces publiques	Envisager l'intervention d'un prestataire externe
	Surveiller les messages privés	Possible via le même prestataire, avec le consentement du journaliste
	Utiliser des outils de filtrage automatique	Préserver la santé mentale sans compromettre la détection des menaces
	Modérer les fils de commentaires	Confier à un prestataire externe
Mécanismes de réponse	Identifier les agresseurs	Utiliser Social Catfish et PeekYou
	Analyser les menaces et faire un tri	Par l'équipe sécurité, éventuellement avec soutien externe
	Protéger les cibles	Confier la surveillance à des collègues si besoin
	Réagir aux menaces graves	Revoir la sécurité, alerter les autorités, accompagner le journaliste, contacter les plateformes, envisager une réponse juridique, contacter les collègues d'autres rédactions, soutenir moralement
	Soutenir le journaliste	Accompagnement par les pairs ou les responsables directs. Identifier la personne la plus adaptée pour apporter du soutien
	Tenir des registres	Le département de sécurité informatique peut coordonner cette tâche

Annexe 1. Définition du harcèlement en ligne

Le harcèlement et les abus en ligne peuvent prendre de nombreuses formes et visent à intimider, réduire au silence ou discréditer les journalistes. Ils peuvent déborder dans la sphère physique et nuire émotionnellement à leurs cibles, avec des conséquences profondes et durables.

À mesure que la technologie évolue et que l'intelligence artificielle devient plus sophistiquée, de nouvelles formes de harcèlement apparaîtront sur des canaux que nous connaissons à peine aujourd'hui. Les plateformes qui hébergent les harcèlements les plus toxiques aujourd'hui ne seront peut-être plus les principales sources d'inquiétude dans les années à venir.

Adopter une approche défensive et des stratégies proactives renforçant la résilience est plus efficace que de se concentrer sur des plateformes spécifiques ou de compter sur elles pour modérer les abus. Le harcèlement en ligne peut également soulever des questions de liberté d'expression, compliquant les interventions des autorités et rendant les plateformes réticentes à modérer le contenu.

Des définitions complémentaires peuvent être consultées auprès de: PEN America; Harvard T.H. Chan School of Public Health; Dart Center for Journalism & Trauma

Pourquoi cela compte

Les rédactions doivent protéger leurs journalistes du harcèlement en ligne pour:

- Garantir leur liberté d'informer, sans peur ou perte d'objectivité.
- Préserver leur sécurité physique et celle de leur environnement de travail.
- Soutenir leur santé mentale et leur bien-être émotionnel à long terme.

L'un des objectifs principaux du harcèlement en ligne est de réduire les journalistes au silence, de les dissuader de couvrir certains sujets, voire de les pousser à quitter la profession. Et cela fonctionne trop souvent. Une enquête de l'UNESCO menée en 2020 auprès de femmes journalistes a révélé que 30 pour cent d'entre elles s'étaient autocensurées sur les réseaux sociaux après avoir subi des attaques. Un autre sondage de l'International Women's Media Foundation (IWMF) a montré que 40 pour cent des femmes journalistes avaient cessé d'écrire sur certains sujets pour éviter les attaques, et un tiers avait envisagé de quitter la profession.

Le harcèlement en ligne constitue ainsi une menace corrosive pour la liberté d'expression, ainsi qu'une menace existentielle pour les journalistes et les rédactions qui tiennent les puissants responsables grâce à un journalisme courageux et de qualité. Dans tous les cas, il inflige un préjudice psychologique et émotionnel profond, avec des séquelles durables.

Dans certains cas, ces attaques virtuelles dégénèrent en violence physique. L'enquête de l'UNESCO a montré que 20 pour cent des journalistes interrogés dans le monde avaient subi une attaque physique liée à des violences numériques. Au Moyen-Orient, ce chiffre dépasse 50 pour cent chez les femmes journalistes ayant déclaré des abus en ligne.

L'armement du harcèlement en ligne

Dans de nombreux pays, le harcèlement en ligne est utilisé comme outil de censure et d'oppression. Des régimes autoritaires, des groupes extrémistes, des manipulateurs d'opinion ou de puissants individus peu scrupuleux s'en servent pour mobiliser des foules numériques contre des individus perçus comme opposants ou critiques. L'impact de mille messages haineux ou menaçants dépasse largement celui d'une poignée isolée. Cette tactique est redoutablement efficace pour déstabiliser, isoler et réduire au silence les cibles journalistiques.

Femmes et journalistes issus des minorités

Les femmes, les journalistes issus des minorités, les personnes LGBTQ+ ou non binaires subissent nettement plus d'abus en ligne que leurs collègues masculins blancs. Ces attaques sont souvent misogynes ou racistes. Lorsqu'une rédaction cherche à évaluer l'exposition de ses membres au harcèlement en ligne, elle doit absolument inclure ces voix dans ses enquêtes internes car elles sont généralement les cibles principales.

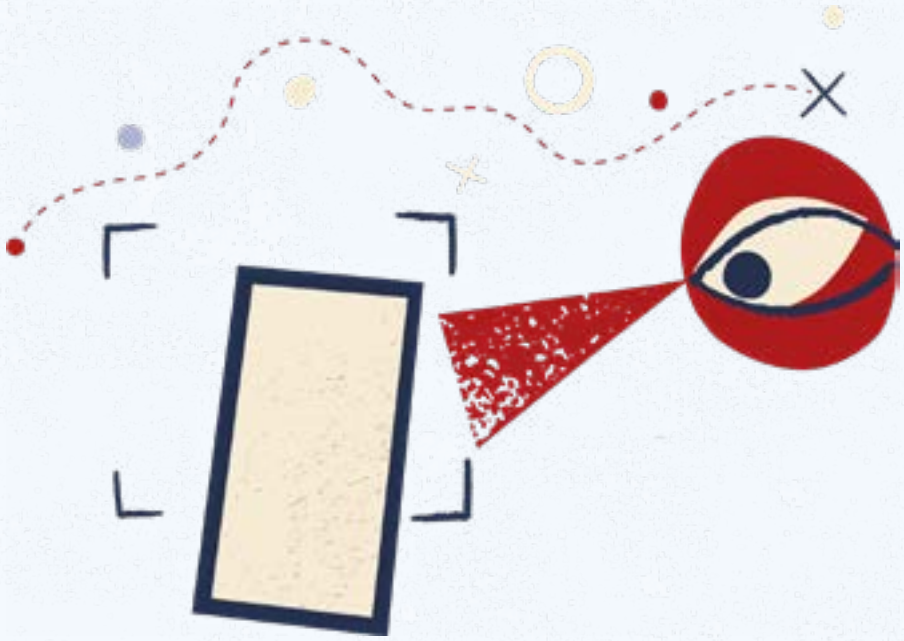
Sujets générant de la haine en ligne

Les nouvelles politiques dans les pays polarisés comme les États-Unis, c'est un déclencheur majeur de harcèlement en ligne. Les pays dirigés par des autocrates ou des gouvernements illégitimes qui utilisent souvent le harcèlement numérique comme outil de répression ou pour réduire ses dissidents au silence.

Les régions où les rivalités ethniques, tribales ou religieuses ont résulté à des conflits et où les reportages considérés critiques d'un camp ou un langage perçu comme biaisé peuvent provoquer des réactions violentes. C'est un problème assez commun, surtout s'ils sont traduits par des éditeurs hors du contexte local, qui ne sont pas familier avec les nuances du langage.

Les jeux en ligne, les investissements amateurs ou poussés par des mèmes, la musique pop et le sport suscitent beaucoup de passions qui peuvent provoquer un nombre surprenant d'abus en ligne. Autres sujets du monde réel pouvant fréquemment engendrer des zones toxiques en ligne:

- L'extrême droite et l'extrême gauche
- La misogynie
- L'antisémitisme
- Les "guerres culturelles"
- La désinformation
- Le racisme
- Les débats sur la censure et la liberté d'expression
- Les tensions géopolitiques



TYPES D'ATTAQUES EN LIGNE

Menaces de violence

Menaces d'exécution, de viol, de meurtre, de représailles contre la famille (y compris les enfants). Certaines menaces directes peuvent justifier une intervention policière mais la plupart contournent la loi ou sont protégées par la liberté d'expression.

Attaques groupées / effets de meute

Incitation à des campagnes coordonnées contre un individu. Cela peut se manifester par une multitude d'agresseurs signalant une violation des conditions de service du compte d'un journaliste aux plateformes de réseaux sociaux et obtenir sa suspension. Les gouvernements, l'armée ou les partis politiques peuvent utilisés des fermes à trolls semi officielles pour provoquer une attaque de meute.

Traque numérique (cyberstalking)

Harcèlement et intimidation prolongée d'une victime. Les traqueurs utilisent la surveillance l'usurpation d'identité ainsi que d'autres moyens de cyberharcèlement. Le cyberharcèlement est souvent un délit criminel et les journalistes ciblés devrait rechercher des conseils juridiques car les agresseurs peuvent être mentalement ou émotionnellement instables.

Doxxing

Publication de données personnelles sensibles telles que l'adresse de résidence où le nom de l'école d'un enfant. Les agresseurs publient ces informations pour inciter d'autres au harcèlement, à la surveillance, à la violence physique, ou au vol d'identité du journaliste ciblé. Le doxxing peut se manifester en particulier lorsqu'un journaliste est sur une enquête à risques élevés dans une zone dangereuse.

Imitation en ligne

Création de faux profils diffusant des propos incendiaires ou mensongers pour nuire à la réputation du journaliste ou encourager un harcèlement plus étendu. D'autres objectifs possibles sont l'escroquerie ou la manipulation de l'opinion.

Swatting

Faire de faux appels d'urgence tel qu'un meurtre ou une prise d'otages afin que la police intervienne de façon violente au domicile de la cible. Extrêmement dangereux, notamment aux États-Unis où les équipes SWAT sont lourdement armées, ce qui entraîne souvent des décès.

Annexe 2. Guide pour les journalistes confrontés à la violence numérique

Les menaces et attaques en ligne visent à réduire les journalistes au silence et à les pousser à l'autocensure. Être submergé de messages violents ou intimidants peut être effrayant et psychologiquement déstabilisant. Dans certains cas, les attaques numériques peuvent dégénérer en violence physique.

Avertissez immédiatement votre rédacteur en chef ou superviseur si vous êtes la cible d'une attaque grave.

Renforcez votre résilience face au harcèlement numérique en réduisant la quantité d'informations personnelles accessibles en ligne. Une menace vague est déjà grave, mais elle devient bien plus dangereuse si l'agresseur connaît l'école de votre enfant ou votre adresse.

Effectuez un exercice d'auto-doxxing pour repérer les données sensibles disponibles publiquement et verrouillez vos comptes sur les réseaux sociaux.

Considérez la séparation de vos identités publiques et privées en ligne. Minimisez les informations personnelles que vous partagez avec le public au travers de vos comptes professionnels tout en conservant vos comptes privés réservés à vos proches.

Sécurité numérique

Mettez à jour vos logiciels et applications

Des failles sont régulièrement découvertes dans les systèmes et logiciels qui font fonctionner nos téléphones, ordinateurs et applications dont les cybercriminels s'en emparent rapidement. Gardez tous vos appareils à jour — y compris personnels.

Ne cliquez jamais sur un lien suspect

75 pour cent des cyberattaques proviennent de courriels de phishing, liens ou pièces jointes piégés qui compromettront votre ordinateur. Si un courriel à un ton alarmiste, demande une saisie de vos identifiants, ou contient une orthographe étrange, cherchez un soutient de votre équipe de sécurité informatique ou utilisez un outil comme Dangerzone pour ouvrir les fichiers suspects de manière sécurisée ou dans un environnement bac à sable.

Utilisez un gestionnaire de mots de passe

Des logiciels pirates peuvent tester des millions de combinaisons par seconde et remplis des données publiques des comptes de réseaux sociaux d'un individu. Considérez l'utilisation d'un gestionnaire de mots de passe comme 1Password, Dashlane ou KeePassXC pour générer et stocker des mots de passe uniques et complexes pour chacun de vos comptes. Créez un mot de passe maître solide.

Vérifiez si vos comptes ont été piratés

Utilisez have i been pwned? pour savoir si vos identifiants ont été compromis dans une fuite de données. Changez immédiatement les mots de passe concernés.

Utilisez la double authentification (2FA)

Activez la double authentification. Ceci envoie un code d'accès par SMS or une appli d'authentification comme Google Authenticator ou Symantec VIP Access. Une appli est préférable au SMS, qui peuvent être interceptés si votre carte SIM est clonée.

Pensez à régulièrement évaluer les menaces à la sécurité des informations

Même un sujet anodin peut évoluer en affaire sensible. Appliquez les bonnes pratiques décrites dans ce guide dès les premières étapes de votre enquête et bien avant que le sujet demande des mesures de sécurités supplémentaires.

Utilisez un téléphone jetable

Considérez d'éviter d'emporter votre téléphone habituel lors de rendez-vous avec vos sources si l'enquête est sur un sujet sensible. Les traqueurs expérimentés peuvent utiliser vos données de localisation et celles de vos sources qui peuvent vous compromettre. Demandez à votre superviseur ou service IT si vous devriez utiliser un téléphone jetable.

Connectez vous avec un VPN

Utilisez un VPN, qui crypte vos connexions à l'internet quand vous connectez votre ordinateur portable personnel ou professionnel et votre téléphone sur les points d'accès wifi dans les hôtels et les aéroports. Protégez vos connexions sur les réseaux publics (hôtels, aéroports) avec un VPN. Proton VPN est une bonne option gratuite.

Choisissez une application chiffrée pour les messages sensibles

WhatsApp, Signal ou Wire sont de bonnes options toutefois Meta, le propriétaire de WhatsApp, conserve les métadonnées (qui avez-vous contacté et quand mais pas le contenu des messages. Telegram n'est pas chiffré par défaut à moins d'activer "message secret".

Chiffrez votre disque dur

Le disque dur de votre ordinateur devrait être chiffré par défaut. Si cela n'est pas le cas l'information contenue sur votre ordinateur peut être accédée facilement. Si le disque est chiffré et l'appareil éteint, vos données sont protégées. Faites de même pour votre téléphone.

Utilisez les versions sécurisées des sites web

Faites en sorte d'accéder des sites web sécurisés. Installez l'extension HTTPS Everywhere pour vous assurer d'utiliser les versions sécurisées. Évitez les sites en avec seulement http:// en début d'adresse au lieu de https://.

Chiffrez les fichiers sensibles

Utilisez VeraCrypt ou 7-Zip sont des programmes gratuits pour chiffrer vos documents et dossiers.

Évitez les bornes de recharge USB publiques

Préférez toujours une prise murale plutôt qu'une borne de recharge USB dans un lieu publique. À Rio pendant la Coupe du Monde en 2014, des bornes USB installées par un gang à l'aéroport servaient à siphonner les données sur les téléphones des voyageurs. Utilisez un accessoire de blocage des données pour que seule la recharge passe par le câble USB lors de l'utilisation d'une borne publique.

Surveillez vos appareils

Gardez vos téléphones et ordinateurs à proximité quand vous travaillez sur des sujets sensibles. Si vous laissez votre ordinateur non surveillé dans une chambre d'hôtel, il n'y aucun moyen de savoir si quelqu'un y a eu accès en votre absence.

Utilisez des applis comme iVerify qui offre un scan mensuel approfondi gratuit ou F-Secure Mobile Security (anciennement Lookout Lite) pour détecter les malwares sur votre téléphone ou ordinateur portable. Redémarrer votre téléphone peut éliminer certains logiciels espions installés dans la mémoire vive.

Soyez prudent aux frontières

Déplacez les données sensibles dans le cloud. Déconnectez-vous de vos comptes et applis au cas où un agent frontalier demande accès à votre téléphone ou votre ordinateur portable. Éteignez complètement vos appareils cela rendra l'accès plus difficile.

Faire face au doxxing

Des informations accessibles en ligne peuvent vous rendre vulnérable face à ceux qui n'aiment pas vos reportages. Les agresseurs peuvent rechercher de vieux posts ou publications susceptibles de nuire à votre crédibilité, ou dévoiler des données personnelles comme votre adresse. L'objectif est d'inciter d'autres personnes à vous harceler, voire à vous agresser physiquement. Certains trolls vont jusqu'à chercher à vous intimider ou vous punir en révélant des contenus sensibles ou compromettants.

- Ils peuvent même procéder à un "swatting" – appelant la police avec un faux signalement de prise d'otages
- Une critique culturelle féministe qui a contesté la domination masculine de l'industrie du jeu en ligne a été confrontée à des menaces de viol, d'attaque á la bombe et de mort
- Un troll peut aussi devenir un harceleur dans la vie réelle

Vous pourriez avoir besoin de conduire un auto-doxxing pour voir ce qui est disponible en ligne à votre sujet, que les trolls pourraient utiliser. Considérez de prendre les mesures suivantes:

Recherchez Google

Recherches sur Google, Bing, Yandex, DuckDuckGo et Baidu. Chaque moteur affiche des résultats différents, surtout si vous avez vécu à l'étranger.

Prénom Nom" OU "nom d'utilisateur"	Utilisez des guillemets pour chercher un mot ou des mots exacts. Cherchez plusieurs combinaisons de votre nom, pseudonymes fréquents et adresses courriel.
1. "Prénom Nom" -"NomMédia" 2. "Prénom Nom" "NomMédia" -site:NomMédia.com"	1. Pour exclure votre organisation médiatique "NomMédia" et voir les autres résultats enfouis dans des pages ultérieures. Le signe moins est aussi un bon moyen pour supprimer les résultats concernant d'autres personnes qui partagent votre nom. 2. Recherche les pages qui font référence à vous et votre entreprise tout en filtrant les résultats liés à son propre site.
"Prénom * Nom"	L'astérisque permet de tester pour tous les termes génériques, par exemple un deuxième prénom ou une initiale.
"(650) 656-5656" OR "6506565656"	Pour chercher votre numéro de téléphone en incluant des formats alternatifs.
"email@exemple.com" filetype:pdf	Pour trouver des documents PDF listant votre adresse mail, par exemple des publications d'anciens élèves ou des présentations anciennes.
"Prénom * Nom" 101 Rue Exemple Paris"	Pour trouver des liens avec des adresses passées, des villes, institutions, emplois et publications.
NomUtilisateur site:reddit.com	Pour trouver des commentaires sur des forums spécifiques qui ne sont pas indexés sur les moteurs de recherche

Faites aussi une recherche d'image inversée

- Sur Yandex: importez une photo de vous pour faire une recherche inversée
- Sur TinEye: importez votre photo de profil X, Facebook, LinkedIn et Instagram pour voir où vos photos sont réutilisées ailleurs

Verrouillez vos paramètres de confidentialité sur les réseaux sociaux

Les réseaux sociaux collectent des données pour la publicité ciblée. Prenez le contrôle de vos informations et la quantité collectée en ajustant vos paramètres de sécurité. Rappelez-vous que ceci peut changer et qu'il faudra les rafraichir.

Facebook

Commencez par utiliser leur outil auto-administré:

- Tapez "Vérification de la confidentialité" et suivez les étapes.
- Vérifiez qui peut voir les détails de votre profil, assurez-vous qu'aucun ne soit publique.
- Limitez la visibilité de vos posts à vos "amis", "proches" ou "moi"
- Changez votre photo de couverture car elle reste toujours publique. Remplacez-la avec une qui ne montre pas votre visage.

Puis prenez ces mesures en plus dans le "Journal d'activité":

- Faites une revue de votre chronologie. Masquez ou supprimez les contenus que vous voulez conserver confidentiel. Vérifier qu'il n'y ai pas de photos dans la revue de photo. Les photos apparaitront là si vous avez activé la reconnaissance faciale, qui peut être désactivée.
- Cliquez sur l'activité dans laquelle vous êtes tagué pour voir qui vous a tagué. En fonctions des paramètres de confidentialité de la personne qui a fait le post, cela pourrait être visible publiquement.

Ensuite

- Allez à la page de confidentialité et cliquez sur "limiter les publications récentes".
- Vérifiez qui peut voir les applications que vous utilisez et comment vous pouvez être découvert.
- Vérifiez les paramètres de confidentialité de vos amis : vos commentaires ou "likes" sur leurs pages, ainsi que leurs commentaires et "likes" sur les vôtres, peuvent être découverts même si vous n'êtes pas tagué. Un traqueur tenace peut également consulter les personnes qui vous sont liées, comme la famille et les collègues, ou les personnes avec lesquelles vous avez interagi sur des parties publiques de votre page Facebook, comme le fait d'aimer votre photo de couverture ou votre photo de profil.
- Assurez-vous d'être à l'aise avec les paramètres de vos publicités
- Dans votre profil et tags activez l'option pour voir les publications dans lesquelles vous êtes tagué avant qu'elles n'apparaissent sur votre chronologie.
- Vérifiez comment votre profil apparaît aux personnes qui vous voient en tant que fonction.

Instagram

Créez un compte professionnel et verrouillez complètement votre compte personnel/privé, en le limitant aux amis/proches.

- Activez le **mode privé** pour que seules les personnes que vous approuvez puissent voir vos publications
- Désactivez le **statut d'activité** dans les messages et les réponses aux « stories » de sorte que personne ne puisse voir quand vous êtes en ligne.
- Sur la page d'édition de profil, décochez l'option permettant à votre compte d'être suggéré sur d'autres profils.
- **Les autorisations de localisation sont contrôlées dans les paramètres de confidentialité et de sécurité de l'application sur votre téléphone. Désactivez l'accès à la localisation ou limitez-le quand vous voulez la partager.**
- Vérifiez vos options de message et story dans les « tags et mentions » et les réglages des commentaires.

LinkedIn

Comme LinkedIn est un outil professionnel de réseautage, c'est un profil public avec une photo accessible à tout le monde Cependant les agences de renseignement créent souvent de faux profils, se mettent en contact avec vous et enquêtent sur votre réseau. LinkedIn est devenu une plateforme assez populaire avec les escrocs qui publient de faux emplois, par exemple.

Les options pour sécuriser votre profil incluent:

- Sous visibilité de votre profil et de votre réseau dans les paramètres et la vie privée, assurez-vous que vous êtes à l'aise avec l'étendue de la divulgation de votre nom, de vos connexions et de votre région.
- Revoyez qui peut voir vos connexions et limitez cela à vous seul si vous êtes connecté à des sources sensibles.
- Activez le mode privé afin que les profils que vous ne connaissez pas ne puissent pas vous voir.
- Limitez qui peut voir votre courriel aux connexions de 1er degré

Puis

- Sélectionnez "non" sous "Visibilité du profil" sur LinkedIn si vous ne souhaitez pas que votre profil apparaisse sur d'autres plateformes partenaires.
- Gérez qui peut découvrir votre profil à partir de votre courriel ou de votre numéro de téléphone s'ils ne sont pas connectés à vous.
- Sous "Visibilité de votre activité LinkedIn", décidez si vous souhaitez que tout le monde sur LinkedIn suive vos mises à jour publiques ou simplement vos abonnés.

Et aussi

- Soyez également prudent avec les contacts synchronisés si vous avez des sources sensibles et envisagez de supprimer tous les éléments synchronisés dans les calendriers.
- Assurez-vous de ne pas avoir publié un ancien CV avec votre adresse personnelle
- Retirez votre lycée.

X

X est l'une des principales plateformes de harcèlement en ligne contre les journalistes et parmi les premiers attaquants qui pourraient chercher des failles dans votre armure de confidentialité.

Prenez des mesures pour protéger votre profil, y compris:

- Décider si vous souhaitez utiliser une photo qui pourrait être utilisée dans des programmes de reconnaissance faciale pour vous suivre et combien d'informations vous voulez ajouter à votre biographie.
- Évitez d'ajouter votre date de naissance à votre profil ainsi que votre localisation, qui devrait également être désactivé dans vos publications.
- Dans le menu de confidentialité et de sécurité, sélectionnez "protéger vos publications" et dans la section "public" des médias et des tags pour limiter qui peut voir vos publications. Désactivez la fonction de photo tagging.
- Décidez qui peut vous envoyer des messages dans la section des messages directs.
- Décidez si les personnes qui ont votre adresse courriel ou votre numéro de téléphone peuvent vous trouver dans la section de découverte.
- Faites attention en synchronisant les contacts de votre téléphone avec X si ceux-ci incluent des sources sensibles.
- Désactivez les annonces personnalisées et les préférences publicitaires dans la section de partage de données et de personnalisation.
- Ne pas activer l'option de personnaliser votre expérience en fonction de l'identité inférée ou de partager vos informations dans le partage de données avec des partenaires commerciaux.
- Décidez si vous souhaitez que votre contenu soit utilisé pour former Grok, l'IA d'X.

Sites personnels

Si vous possédez un site web personnel, son nom de domaine est souvent lié à votre adresse, courriel ou numéro de téléphone. C'est une option facile pour obtenir vos informations de contact.

- Allez sur DomainTools et entrez l'URL de votre site pour voir quelles informations personnelles sont publiquement visibles.
- Considérez de les cacher en utilisant un service de protection tel que Who is Guard.
- Vérifiez si votre bureau d'enregistrement offre des options gratuites ou payantes pour cacher vos données personnelles.

Comptes piratés : changez immédiatement vos mots de passe

Si vous avez été piraté, votre nom d'utilisateur et votre mot de passe ont pu être vendu et peuvent être disponibles sur le dark web.

- have i been pwned? vous indiquera si vos mots de passe et noms d'utilisateurs ont été compromis dans une fuite de données. Changez le mot de passe concerné sans délai ainsi que les autres comptes utilisant the même mots de passe/nom d'utilisateur.
- Utilisez Keeper Security ou un autre gestionnaire sécurisé pour créer des mots de passe complexes.
- Activez la double authentification via une app. Utilisez une appli plutôt qu'un SMS pour recevoir les codes 2FA.
- Préférez une messagerie sécurisée comme Gmail protégé avec YubiKey.
- Envisagez de créer un nom d'utilisateur non compromis basé sue un nouveau compte courriel que vous utiliserez uniquement à des fins spécifiques, par exemple un portail de shopping.

Courtiers en données

Des dizaines d'entreprises collectent et revendent les données personnelles. Vous pouvez vous désinscrire, mais cela peut être difficiles et nécessiter d'être répété, ce qui prend du temps.

- Optez pour des services de retrait automatique comme DeleteMe ou Optery qui feront le travail difficile pour vous.
- Utilisez l'appli Permission Slip app pour envoyer des demandes automatiques. La version payante a plus de fonctionnalités.

Annexe 3. Outils pour les journalistes et les responsables

Tool	What is it used for
Tall Poppy	Solution complète de protection contre le harcèlement en ligne : formation, réponse aux incidents, service personnalisé pour VIP
PEN America	Formations
Troll Busters	Formations et conseils spécialisés
Theseus	Analyse des menaces
DeleteMe	Suppression des informations personnelles
Permission Slip app	Suppression des informations personnelles
Mark Monitor	Protection de marque, gestion de domaines, lutte contre l'usurpation d'identité
Proofpoint	Contre l'usurpation d'identité
ZeroFox	Surveillance du dark web, détection d'usurpation d'identité
Elv.ai	Modération de contenu, surveillance des menaces
Memetica	Surveillance des menaces
Interfor	Surveillance des réseaux sociaux et des menaces en ligne
Ontic	Analyse des menaces et enquêtes
Dataminr	Surveillance des menaces
JustDeleteMe	Suppression d'anciens comptes utilisateurs
TweetDelete	Suppression d'anciens tweets/posts sur X
tweeteraser	Suppression d'anciens tweets/posts sur X
Google's PerspectiveAPI	Modération de commentaires

Other resources

- PEN America Manuel de terrain sur le harcèlement en ligne
- Zebra Crossing liste de vérification numérique facile
- Consultations individuelles sur la sécurité pas l'International Women's Media Foundation
- Le rapport des Journalistes Sans Frontières sur le harcèlement en ligne

INSI

INTERNATIONAL
NEWS SAFETY
INSTITUTE

International News Safety Institute
C/O Thomson Reuters Foundation
5 Canada Square
Floor 8
Canary Wharf
London E14 5AQ

info@newssafety. org
www. newssafety. org
@INSInews