ASTUCES ET CONSEILS UTILES FACE AU HARCÈLEMENT EN LIGNE

Les organisations de défense des droits humains qui mènent des activités de plaidoyer en ligne sont confrontées à des menaces de plus en plus dangereuses. Ces menaces, qui prennent la forme de langage grossier dans les commentaires et lignes ou de menaces personnelles à l'encontre du personnel, visent à porter atteinte à la crédibilité des organisations et à limiter l'espace public disponible pour défendre une cause. Dans ce guide, nous fournissons quelques conseils et astuces utiles vis-à-vis du harcèlement en ligne, ainsi qu'une liste de ressources auxquelles les organisations peuvent se référer pour faire face au harcèlement en ligne.

QU'EST-CE QUE LE HARCÈLEMENT EN LIGNE ?
(PEN America, n.d.)

Le harcèlement en ligne prend plusieurs formes, du *trolling* individuel aux attaques organisées qui sont moins visibles. Connaître les différentes formes de harcèlement en ligne permet de mieux se préparer à y faire face et de répondre efficacement à l'attaque.

- *Trolling* : publication répétitive de commentaires polémiques ou haineux en ligne par un individu dont l'intention est de chercher à attirer l'attention, de nuire intentionnellement à une cible, de susciter des troubles et/ou la controverse, et/ou de se joindre à un groupe de trolls qui ont déjà débuté une campagne de *trolling.*
- *Doxing* : abrévation de "*dropping docs*" – cet acte consiste à publier des informations personnelles sensibles d'une personne en ligne pour la harceler, l'intimider, l'extorquer, la traquer ou voler son identité. Ces informations peuvent inclure des numéros de sécurité sociale, des numéros de téléphone, des adresses postales, des photos personnelles, des informations relatives à l'emploi, des adresses électroniques et des informations personnelles sur des proches.
- Cyberharcèlement : comportement de harcèlement commis de manière répétée ou régulière qui causent généralement à la personne visée de la peur, de l'anxiété, des humiliations ou une détresse émotionnelle extrême.
- Usurpation d'identité : les harceleur·euse·s créent des comptes fictifs sur les réseaux sociaux généralement dans le but de publier des déclarations offensantes ou polémiques en utilisant le nom de la victime. L'objectif de ce comportement est de diffamer ou de discréditer la victime, souvent en convainquant d'autres personnes de croire les faux propos qui sont attribués à la victime. Ce type de comportement peut ensuite inciter d'autres personnes à commettre des actes de harcèlement en ligne. Le *trolling* par usupartion d'identité peut également se produire lorsqu'un·e harceleur·euse se fait passer pour quelqu'une que la victime connaît dans le but de l'offenser ou de la blesser.
- Autres formes de harcèlement : piratage, envoi en masse de messages, etc.

COMMENT PRÉVENIR LE HARCÈCELEMENT EN LIGNE ?
Doucet-Bon (2019)

Voici quelques-unes des meilleurs pratiques pour se prémunir contre le harcèlement en ligne :

- Mettez régulièrement à jour vos logiciels et applications.
- Créez des mots de passe sécurisés. Adoptez des mots de passe d'au moins 16 caractères (même si la limite du nombre de caractère minimal fixée par les sites internet est inférieure), utilisez un mot de passe différent pour chaque application et changez-les au moins tous les six mois. Il est nécessaire de créer ses propres questions de sécurité car celles suggérées sont souvent trop

simples. Assurez-vous également que vous n'avez pas donné la réponse à la question sur un compte public.

- Ne vous connectez jamais à une application via Facebook, Gmail ou autre.
- Ne donnez pas accès aux applications à vos contacts. N'autorisez la géolocalisation seulement lorsque vous le jugez nécessaire. Dans ce cas, ne l'autorisez seulement lors de l'utilisation de l'application.
- Utilisez une application sur internet pour téléphoner comme Google Voice, par exemple.
- Protégez-vous contre le *sim swapping*. On parle de *sim swapping* lorsqu'un pirate appelle l'opérateur de la victime en se faisant passer pour elle, déclare avoir perdu son téléphone et demande que les appels et messages entrants soient redirigés vers une autre carte sim. Pour vous protéger du *sim swapping*, demandez à votre opérateur téléphonique d'associer un mot de passe à votre compte.
- Utilisez une messagerie cryptée : Signal, Telegram, WhatsApp ou Wire. Il est important d'utiliser une messagerie cryptée en particulier si vous souhaitez travailler sur des sujets à risque.
- Protégez-vous contre le *doxing*. Veillez à ne pas laissez d'informations personnelles sur votre biographie lorsque vous participez à des conférences ou à d'autres évènements publics. Suivez vos informations personnelles en utilisant les alertes Google : vous serez notifié si quelqu'un partage vos informations en ligne.
- Séparez votre vie privée et votre vie professionnelle. Choisissez une plateforme pour votre vie personnelle et une autre pour votre vie professionnelle. Afin de protéger vos comptes, toutes les messageries offrent désormais un accès facile pour modifier les paramètres de confidentialité. Évitez de poster des photos de famille ou de votre maison sur des comptes publics.
- Cryptez vos courriels sensibles. Pour cela, demandez à votre fournisseur. L'une des méthodes les plus simple est Mailvelope à partir de Gmail.
- Sécurisez vos envois de documents sensibles. Les individus peuvent notamment utiliser GlobaLeaks. Vous pouvez également proposer à votre entreprise d'utiliser Secure Drop.
- Sécurisez votre VPN. Une sécurité à deux niveaux est essentielle.

Le site internet du Citizen Lab offre des conseils personnalisés pour protéger votre présence et/ou vos informations en ligne : https://securityplanner.org.

COMMENT FAIRE FACE AU HARCÈLEMENT EN LIGNE ?

(Institute For War and Peace Reporting, 2019, p.210)

Signalez le commentaire ou la publication en question, comme le recommande Facebook. Fournissez autant de détails et d'informations contextuelles que possible. Les utilisateur·trice·s peuvent suivre l'avancée du processus à l'adresse https://www.facebook.com/report.

Bloquez les harceleur·euse·s. Cela les empêchera de vous envoyer des demandes, des vous envoyer des messages et de voir les mises à jour qui sont publiées sur votre fil d'actualités. Les utilisateur·trice·s ne sont pas averti·e·s lorsqu'elles et ils sont bloqué·e·s, mais elles et ils peuvent s'en rendre compte quand elles et ils ne sont soudainement plus en mesure de contacter une cible.

Signalez l'incident et gardez le numéro de dossier pour effectuer un suivi, comme le recommande Twitter aux utilisateur·trice·s qui sont la cible de harcèlement en ligne. Sur Twitter, il est possible de signaler un tweet spécifique ou un profil.

Faites des captures d'écran avant de bloquer les harceleur·euse·s sur les plateformes afin de conserver des preuves des abus. Une fois que les harceleur·euse·s sont bloqué·e·s, il devient beaucoup plus difficile de recueillir des preuves. Il peut être demander aux utilisateur·trice·s de fournir des preuves lorsqu'un incident fait l'objet d'une enquête.

Documentez les incidents dans un journal de bord.

- La documentation peut être utile ultérieurement pour faire des liens entre les différents incidents qui se sont déroulés sur une période spécifique ou qui sont arrivés à plusieurs personnes dans l'organisation.
- La documentation peut révéler des schémas d'abus ou d'autres attaques en ligne que vous n'auriez peut-être pas remarqué autrement. Ces schémas peuvent être utiles pour identifier les harceleur·euse·s ou pour établir des liens entre certains types d'incidents et certaines actions de votre part ou de votre organisation.
- Lors du signalement et de l'enquête sur des incidents sur les réseaux sociaux, des preuves, telles que des captures d'écran et des noms de profil peuvent être demandées.
- Vous pouvez regrouper les informations en suivant ce modèle (Institute For War And Peace Reporting, 2019, p.216) :

Date	
Heure	
Résumé de l'incident	
Plateforme	
URL	
Capture d'écran (nom du fichier ou copier-coller le fichier)	
Description des captures d'écran et du contenu	
Niveau de risque	*Expliquez de manière précise le niveau de risque car ce champ est très subjectif et moins explicite que les autres.*
Actions de suivi	
Notes	

RESSOURCES SUPPLÉMENTAIRES SUR LE HARCÈLEMENT EN LIGNE

Vous trouverez ci-dessous une liste de lectures complémentaires pour vous aider à faire face au harcèlement en ligne :

RÉFÉRENCES CITÉES

Doucet-Bon P, « Journalisme : harcèlement en ligne, ça n'arrive pas qu'aux autres », 19 septembre 2019, via https://www.meta-media.fr/2019/09/19/journalisme-harcelement-en-ligne-ca-narrive-pas-quauxautres.html.

Institute For War And Peace Reporting, "Holistic digital security training curriculum for women human rights defenders", 2019, via https://cyberwomen.com/en/cyberwomen/cyberwomen.pdf.

PEN America, "Defining "Online Harassment": A Glossary of Terms", non daté, via ONLINE HARASSMENT FIELD MANUAL : https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-ofterms/.

AUTRES RESSOURCES

Feminist Frequency, "Speak Up & Stay Safe(r): A Guide to Protecting Yourself from Online Harassment, non daté, via https://freedom.press/training/preventative-mobile-security-tips-activists/.

Frontline Defenders, "Workbook on Security: Practical Steps for Human Rights Defenders at Risk", 2011, via https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-humanrights-defenders-risk.

PEN America, "Online Harassment Field Manual", non daté, via https://onlineharassmentfieldmanual.pen.org/.

PEN America, "Protecting Information from Doxing", non daté, via https://onlineharassmentfieldmanual.pen.org/protecting-information-from-doxing/.