SHOTS HEARD ROUND THE WORLD BOÎTE À OUTILS

Guide sur la manière de se préparer, de se défendre et d'aller de l'avant après une attaque des antivax.

1ÈRE PARTIE : QUI SOMMES-NOUS 5

2ÈME PARTIE : CE QUE VOUS POUVEZ FAIRE EN CAS D'ATTAQUE 6

Vous préparer 6
Disposer de renforts 6
Analysez votre présence en ligne 6-7
Préparer votre lieu de travail, votre bureau ou votre institution 7
Contrôler la sécurité de vos comptes en ligne 7
Connaître les paramètres de votre plateforme 7
Recherchez-vous sur Google 7
Vous défendre 9
Les 10 mesures les plus importantes à prendre en cas d'attaque 9
Mesures spécifiques à chaque plateforme 9-10
Aller de l'avant après une attaque 10
Organiser toutes les captures d'écran 10
Débriefing 10
Mesures spécifiques à chaque plateforme 11
Que faire si vous êtes victime de doxing 11
Mesures spécifiques 11
Ressources 12

3ÈME PARTIE PRENEZ SOIN DE VOUS 14

Santé mentale 14
Ressources pour le traitement de la santé mentale 14
Ressources pour la prévention du suicide 14
Ressources sur l'intimidation et le harcèlement en ligne 14
Solidarité 15
Histoires de personnes qui ont réussi à déjouer des attaques en ligne 15
Sécurité physique 15
Éteignez Internet si vous le pouvez 15

4ÈME PARTIE : CONNAÎTRE LES RÈGLES 16

Les lois 16
Identifier la nécessité de faire appel aux forces de l'ordre 16
Identifier le besoin de soutien juridique 17
Ressources pour trouver un avocat 17
Aperçu des lois fédérales 17
Ressources publiques 17
Conditions d'utilisation 17
Termes spécifiques à la plateforme 17

SHOTS HEARD ROUND THE WORLD BOÎTE À

Dans le monde en ligne actuel, de nombreux professionnels de santé mettent leur expertise à disposition sur les réseaux sociaux pour aider les patients à obtenir des informations de qualité. Trop souvent, ces professionnels de santé sont harcelés, intimidés et attaqués.

Avec cette boîte à outils, nous mettons à votre disposition des compétences et des informations pour vous permettre de vous **préparer**, de vous **défendre** et d'**aller de l'avant** après une attaque des antivax sur diverses plateformes en ligne. Nous espérons vous aider à vous prendre en main et vous donner les ressources nécessaires pour continuer à défendre la cause des vaccins en ligne.

QUI SOMMES-NOUS

Shots Heard Round the World (Shots Heard ou SH) est une cavalerie numérique à réaction rapide destinée à protéger les pages des médias sociaux des prestataires de soins et des cabinets médicaux.

Nous sommes un réseau à réponse rapide à but non lucratif dûment contrôlé, fondé sur des données concrètes, ayant pour objet de lutter contre les attaques des antivaccins sur les pages des réseaux sociaux, les sites web et les sites d'évaluation des prestataires de soins, des cabinets médicaux, des hôpitaux et de systèmes de santé complets. **Si vous défendez la science des vaccins, nous vous défendrons.**

Nous savons de première main que la valeur de ce type de réseau virtuel à réponse rapide est à la fois immense et profonde. Lisez l'histoire de nos fondateurs.

Shots Heard est géré par le personnel de « Public Good Projects », une organisation à but non lucratif vouée à la lutte contre les problèmes de santé publique les plus urgents dans le monde.

CE QUE VOUS POUVEZ FAIRE EN CAS D'ATTAQUE

VOUS PRÉPARER ET ÉVITER

Il existe une série de mesures à mettre en oeuvre lors de la création de votre présence en ligne et de votre prise de position en faveur des vaccins qui vous permettront d'éviter d'être pris pour cible par les antivax ou d'être préparé en cas d'attaque.

Disposer de renforts

- Rejoignez dès aujourd'hui la cavalerie numérique « Shots Heard Round the World »
- Email Join@shotsheard.org
- Adhérez au Facebook Group privé de Shots Heard
- Apprenez à connaître la communauté - consultez les anciennes publications de soutien, de camaraderie et de formation

Analysez votre présence en ligne

- Ne nourrissez pas les trolls : Pour empêcher l'afflux de commentaires négatifs, ignorez les commentateurs négatifs, harceleurs et intimidants
- Évitez les combats inutiles et réagissez avec prudence : Si vous avez l'intention de réagir à un commentaire antivax, choisissez les conversations en vous basant judicieusement sur le contexte.

Voici quelques éléments à prendre en compte :

- Le commentateur est-il de bonne foi ? Est-il ouvert à une conversation productive ? Est-ce qu'il vous provoque ?
- Connaissez-vous cette personne ou avez-vous confiance en elle ?
- A-t-elle une longue histoire de publications antivax et fait-elle partie de groupes correspondants ?

Construisez un réseau de confiance

- Devenez « ami » ou « follower » de profils qui ont affiché une attitude positive et peuvent être des alliés
- Encouragez les avis positifs sur votre lieu de travail

Préparez votre lieu de travail, votre bureau et/ou votre institution

- Téléphones : formez votre personnel à identifier les signes d'attaque, à la manière de réagir et quand informer un responsable
  - Si vous recevez sans arrêt des appels téléphoniques négatifs ou grossiers ou des canulars :
    - Si possible ignorez votre téléphone, mettez-le sur vibreur ou éteignez-le
    - S'il s'agit d'une ligne à laquelle vous devez répondre, déterminez s'il s'agit d'un appel négatif, et si tel est le cas, raccrochez et rejetez poliment l'appel
    - Notez le nombre d'appels mal intentionnés ainsi que les numéros de téléphone et les messages
- Apprenez à reconnaître les signes d'une attaque imminente sur les réseaux sociaux
  - Le personnel responsable de la surveillance des comptes doit être formé à rechercher :
    - Un pic ou un volume plus élevé que d'habitude de commentaires négatifs
    - Des commentaires inhabituellement grossiers ou déplaisants en provenance de nouveaux comptes
    - Des liens ou des captures d'écran de votre page publiés sur des sites de groupes antivax ou par des pages antivax
    - Des gens qui, dans les commentaires de vos pages, incitent d'autres antivax à s'attaquer à vous
    - Des commentaires négatifs en provenance de comptes suspects, anonymes ou de type bot
    - Des antivax qui vous contactent par le biais d'autres plateformes

Contrôlez la sécurité de vos comptes en ligne :

- Activez l'authentification à deux facteurs pour tous les comptes qui la prennent en charge
- Utilisez des mots de passe forts et différents ou un gestionnaire de mots de passe

Renseignez-vous sur les paramètres de votre plateforme en cas d'attaque :

Sachez comment limiter ou désactiver rapidement les commentaires, bloquer les comptes insultants, rendre votre profil privé, signaler les comptes insultants et effacer les commentaires insultants (voir les liens dans la section « Vous défendre » ci-dessous).

Quelques tactiques préventives pour éviter et décourager les attaques :

1. Envisagez de rendre vos comptes privés :
   Instagram Confidentialité
   Twitter Confidentialité
   Tiktok Confidentialité
2. Affirmez votre activité en ligne
   Yelp
   Google My Business
3. Activez les notifications par e-mail - cela vous permettra de savoir rapidement si une attaque se prépare
   Facebook Notifications
   Yelp Notifications
   Google My Business Notifications

« Googlez-vous » et « dé-doxez-vous » vous-même

Le doxing est une pratique qui consiste à identifier ou à publier des informations privées sur quelqu'un, notamment dans l'intention de le punir ou de se venger. Il est important de savoir si des informations à caractère personnel vous concernant sont publiquement accessibles en ligne. Ces informations peuvent vous rendre plus vulnérable au doxing.

Conseils ***du New York Times***:

1. Faites une recherche sur vous-même sur des moteurs de recherche tels que Google et supprimez autant d'informations que possible des sources qui apparaissent
2. Retirez les informations vous concernant sur les sites de recherche de personnes ou de courtiers de données
3. Rendez vos réseaux sociaux privés

VOUS DÉFENDRE

De nombreux professionnels de santé ont été attaqués en ligne, notamment après avoir partagé des informations véridiques et scientifiquement fondées. Bien que cela puisse être frustrant, dérangeant et potentiellement angoissant, vous surmonterez cela comme nombre de vos collègues l'ont fait par le passé.

Si vous êtes attaqué, voici 10 mesures importantes à prendre immédiatement :

1. Souvenez-vous : Vous surmonterez cette épreuve et vous n'êtes pas seul.

2. Informez-nous et demandez un soutien.

3. N'entrez pas en relation avec les attaquants.

4. Désactivez les notifications des médias sociaux.

5. Renforcez vos paramètres de confidentialité sur la plateforme et sur les pages de l'attaque.

6. Faites des captures d'écran et sauvegardez toutes les attaques, y compris les commentaires négatifs, les avis frauduleux et autres contenus du même type.

7. Signalez et bloquez les attaquants et supprimez les commentaires négatifs.

8. Faites connaître vos entreprises sur Yelp et sur Google.

9. Informez votre employeur ou vos employés de la situation.

10. Prenez des pauses pour prendre soin de vous et de votre santé mentale.

Mesures spécifiques à la plateforme :

Facebook
Renforcez vos paramètres de confidentialité
Désactivez les messages des visiteurs
Désactivez les avis et les recommandations sur Facebook
Signalez les messages d'intimidation, de doxing ou de désinformation

Instagram
Rendez votre profil privé
Signalez les messages d'intimidation, de doxing ou de désinformation

Twitter
Protégez vos tweets (rendez votre compte privé)
Signalez les messages d'intimidation, de doxing ou de désinformation
Bloquez les comptes agressifs

Tiktok
Renforcez les contrôles de la confidentialité
Signalez et supprimez les commentaires d'intimidation, de doxing ou de désinformation

Yelp
Signalez les avis frauduleux
Signalez les utilisateurs

Google Reviews (Avis Google)
Signalez les avis frauduleux

ALLER DE L'AVANT APRÈS UNE ATTAQUE

Les attaques peuvent se terminer progressivement ou rapidement mais dans tous les cas vous remarquerez que les réactions négatives diminuent lorsque la mobilisation des antivax faiblit, lorsqu'ils sont bloqués ou se désintéressent du sujet. Lorsque vous remarquez cela, il est important de prendre le temps de vous reposer, de nettoyer vos pages et de vous organiser.

- Organisez toutes les captures d'écran et tous les enregistrements de l'attaque
- Faites le point avec le personnel, les modérateurs ou les membres de votre famille qui ont accès à votre page ou ont été témoins de l'attaque. Assurez-vous de recueillir toutes les preuves, analysez la capacité de chacun à aller de l'avant et vérifiez la santé mentale de chacun.

Mesures spécifiques à la plateforme:

Facebook
- Bloquez les pages d'entreprise restantes

Instagram
- Supprimez les commentaires négatifs

Twitter
- Masquez les réponses | API Twitter | Docs

Tiktok
- Supprimer les commentaires

Yelp
- Signalez tous les avis frauduleux de Yelp

Google Reviews
- Envoyez un message directement sur Twitter à @Googlemybiz; décrivez brièvement l'attaque et demandez de l'aide
- Répétez le point 1 si nécessaire (parce que cela peut être vraiment nécessaire)
- Essayez également : Demandez la suppression d'un avis - Android - Google My Business Help

QUE FAIRE SI VOUS ÊTES VICTIME DE DOXING

Mesures plus spécifiques :

1. Signalez les pages et les commentaires offensants au site web ou à la plateforme (il existe en général une option « signaler » sur la page/le commentaire)
2. Rendez vos comptes sur les réseaux sociaux privés
3. Documentez les cas de doxing à l'aide de captures d'écran
4. Faites une recherche sur vous-même dans les moteurs de recherche (Google, Bing, Firefox, etc.) et retirez les informations vous concernant des sources qui apparaissent
5. Contactez le service client du site de recherche de personnes ou du courtier de données pour demander la suppression de vos informations
6. Supprimer un contenu de Google - Aide juridique
7. Définissez des alertes pour votre nom complet sur Google : Alertes Google - Surveillez le web à la recherche de nouveaux contenus intéressants
8. Faites une recherche sur vous-même sur les sites de tchat en ligne tels que Reddit et 4Chan
9. Changez tous vos mots de passe pour renforcer la sécurité

Si le doxing se transforme en menaces de violence sérieuses, contactez les autorités locales et le FBI Ressources :

- Globalsign.com: Comment éviter le doxxing
- Berkely.edu: Protégez-vous du doxing
- DHS.gov: How to prevent online harassment from "Doxxing" (Comment prévenir le harcèlement en ligne dû au doxing)
- NYT: A Guide to Doxxing Yourself on the Internet (Guide d'auto-doxing sur Internet)
- NYT: Social Media Security & Privacy Checklists (Check-lists sur la sécurité et la confidentialité des réseaux sociaux)
- NYT: Doxxing Curriculum Guide (Guide pédagogique sur le doxing)
- FBI complaint form (Formulaire de dépôt de plainte du FBI)

PRENEZ SOIN DE VOUS

SANTÉ MENTALE

Être attaqué peut provoquer un sentiment d'isolement. Sachez que vous n'êtes jamais seul et qu'il y a toujours de l'espoir et la lumière au bout du tunnel. **Merci pour votre travail qui consiste à fournir des soins médicaux et des informations factuelles en ligne.**

Ressources pour le traitement de la santé mentale

- Ressources des CDC pour les personnes à la recherche d'un traitement
- Ressources pour la prévention du suicide : si vous avez des pensées suicidaires, demandez de l'aide à des prestataires locaux ou appelez l'une des lignes d'assistance suivantes
- National Suicide Prevention Lifeline (Ligne d'assistance nationale pour la prévention du suicide)
- American Foundation for Suicide Prevention (Fondation américaine pour la prévention du suicide)
- Suicide Prevention Resource Center (Centre de ressources pour la prévention du suicide)
- National Institute of Mental Health (Institut national de santé mentale)

Online bullying and harassment resources

- Cyberbullying Research Center (Centre de recherche sur le cyberharcèlement): Resources
- HeartMob by Hollaback: Know Your Rights (« HeartMob by Hollaback » Connaître vos droits)

SOLIDARITÉ

Nous pouvons vous mettre en contact avec d'autres personnes ayant été victimes d'attaques. Veuillez nous contacter si vous êtes intéressé.

Histoires de gens qui ont surmonté des attaques en ligne avec succès :

- 1. Lisez notre histoire sur shotsheard.org

SÉCURITÉ PHYSIQUE

- Si vous ne vous sentez pas en sécurité chez vous, peut-être pouvez-vous aller chez un ami ou un parent avec lequel vous vous sentirez plus en sécurité
- Alertez les agents de sécurité de votre lieu de travail ou de votre lieu de résidence
- Si vous avez reçu des menaces, appelez la ligne de non-urgence de votre poste de police local

Ressources au cas où vous vous sentez menacé physiquement là où vous vous trouvez :
Vous pouvez signaler toute menace directe ou doxing au FBI. Vous trouverez le bureau local du FBI ici

ÉTEIGNEZ INTERNET SI VOUS LE POUVEZ

Faites des activités qui vous procurent du bien-être : sortez, faites de l'exercice, préparez-vous un repas, lisez, passez du temps avec les gens que vous aimez.

Si cela vous donne un sentiment de sécurité et de confort, envisagez de désactiver **toutes les notifications de tous les comptes des réseaux sociaux.**

CONNAÎTRE LES RÈGLES

Il peut s'avérer utile de comprendre les lois qui régissent tous les types d'attaques en ligne, le doxing et le cyberharcèlement pouvant frapper les professionnels de santé. Les lois et leur application varient d'un État à l'autre. Vous trouverez ci-dessous un aperçu juridique général sur ce sujet. Veuillez noter qu'il ne s'agit pas de conseils juridiques et que cela n'a pas pour but de remplacer l'assistance d'un avocat.

LES LOIS

Identifier la nécessité de faire appel aux forces de l'ordre

- Si vous avez le sentiment que votre sécurité est menacée, appelez le 911

Selon le Pen America's online harassment guide, la police est vraisemblablement plus à même de vous aider d'une manière ou d'une autre dans le cas des formes suivantes de cyberharcèlement :

- Vous avez reçu ou avez été désigné nommément dans des menaces directes de violence. (Les menaces qui suggèrent une heure, un lieu ou un endroit sont plus susceptibles d'être prises au sérieux par les forces de l'ordre).
- Un agresseur en ligne a publié des images de vous à caractère explicitement sexuel sans votre consentement.
- Vous avez été harcelé par voie électronique (voir ci-dessous).
- Vous connaissez votre harceleur et souhaitez demander une ordonnance restrictive.

Dans les cas où une action en justice n'est pas immédiatement engagée, le fait de signaler le harcèlement aux forces de l'ordre peut aider à établir une trace écrite en vue d'une action ultérieure.

- Vous pouvez signaler un harcèlement en ligne au FBI ici
- Signaler des menaces et des délits au FBI
- Contacter le bureau local du FBI

Identifier le besoin d'aide juridique

- Étapes d'une action en justice

Ressources pour trouver un avocat

- Annuaire de référence des avocats par État

Aperçu des lois fédérales pertinentes

- Loi fédérale relative à la prévention du harcèlement
- Lois relatives au doxing

Ressources publiques

- Lois de chaque État sur le harcèlement
- Pour une présentation plus détaillée de chaque État

CONDITIONS GÉNÉRALES D'UTILISATION ET DE SERVICE

La plupart des plateformes interdisent les messages et les contenus qui intimident, harcèlent ou révèlent publiquement des informations à caractère personnel de leurs utilisateurs.

Conditions générales des plateformes

- Facebook
- Instagram
- Twitter
- TikTok
- Yelp
- YouTube
- Google Reviews

Merci de nous soutenir dans notre mission de reprendre la science en main, de protéger la santé publique et de défendre les prestataires pro-vaccins - un post, un tweet, une photo à la fois.

Nous sommes là pour vous !