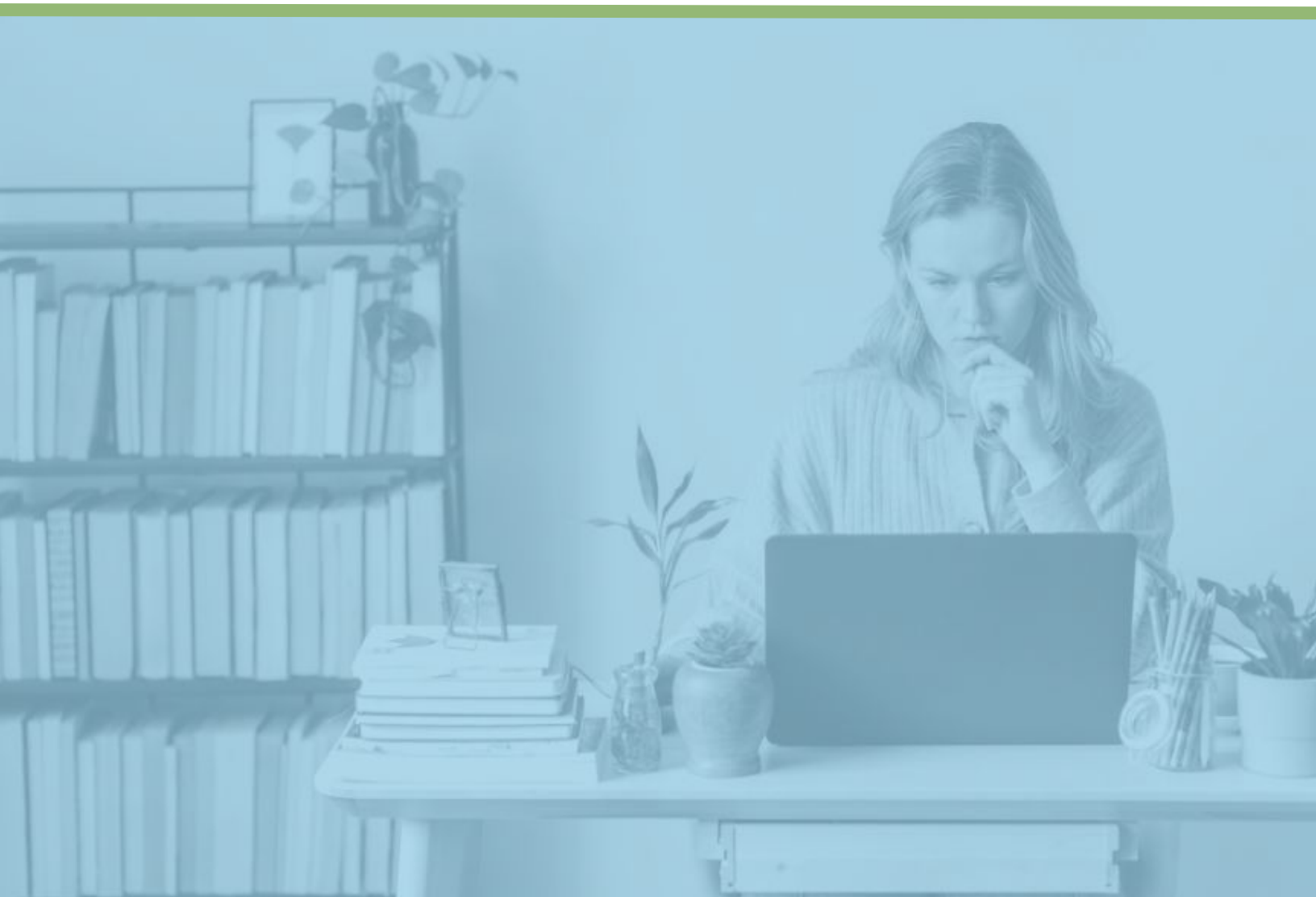
wikiHow
to do anything

L'initiative Vérifié des Nations Unies et wikiHow présentent

Comment combattre la désinformation en ligne

Un cours gratuit produit par l'initiative Vérifié des Nations Unies et wikiHow pour vous aider à reconnaitre et à lutter contre la désinformation en ligne.



wikiHow to do anything × Verified

Table des matières

1re leçon : qu'est-ce que la désinformation ?

En ligne, n'importe qui peut publier une information et atteindre de vastes audiences dans différentes régions du globe. Cela signifie que vous devez vérifier la fiabilité de ce que vous lisez et partagez. Avant de publier une information, essayez de déterminer son origine et la raison de sa diffusion. Vous éviterez ainsi de lire des informations trompeuses ou dangereuses et d'encourager d'autres personnes à les lire sur internet.

Quel genre d'informations non fiables peut-on rencontrer et comment pouvons-nous empêcher leur propagation ?

Vous avez probablement déjà eu affaire à de fausses affirmations en ligne. Il s'agissait peut-être de *fausses informations* comme celles que les gens diffusent accidentellement. Ils ne savent pas qu'elles sont fausses et y croient probablement eux-mêmes.

Vous avez peut-être aussi vu de la *désinformation*. La désinformation présente trois caractéristiques principales:

- elle est créée exprès dans l'intention de tromper le public ;
- elle est inexacte ;
- elle est diffusée dans le but de nuire.

La grande différence entre la fausse information et la désinformation réside dans les motifs qui ont poussé l'auteur à créer ou publier une fausse nouvelle.

Quand il y a une campagne de désinformation soutenue, une grande partie du public peut croire quelque chose qui est tout simplement faux. Mais vous pouvez apprendre à repérer une désinformation quand vous la voyez, afin d'aider à arrêter sa propagation et aussi alerter les autres.

Pourquoi les gens créent-ils de la désinformation ?

La désinformation n'est pas une chose nouvelle. Pendant la Seconde Guerre mondiale, les nazis avaient disposé d'un « service de désinformation » qui créait de faux plans militaires. Ces plans étaient ensuite placés en des endroits où ils pouvaient facilement être trouvés et volés par des espions étrangers qui croyaient avoir de vrais plans militaires nazis.

Aujourd'hui, la désinformation est toujours utilisée pour faire croire aux gens des choses erronées afin de servir les intérêts de quelqu'un d'autre.

La « désinformation » se présente sous différentes formes allant de l'information structurée et diffusée pour des raisons politiques (par exemple pour persuader les gens de voter d'une certaine façon ou de soutenir une cause particulière), à la diffusion de théories conspirationnistes sur la santé publique ou l'environnement. La désinformation est néfaste, car elle peut porter atteinte à de nombreux droits de l'homme, compromettre d'importantes mesures publiques ou aggraver les tensions en période d'urgence ou de conflit.

La désinformation peut également être diffusée par différents moyens.

Les particuliers, les gouvernements et d'autres organisations peuvent diffuser de fausses informations à travers des campagnes publicitaires et des réseaux sociaux, en utilisant des supports variés allant des tracts aux publicités télévisées en passant par des personnes dans les rues. En ligne, il peut être encore plus facile de diffuser ces histoires sans vérifier leur exactitude.

La désinformation peut s'appuyer sur de nombreuses motivations. Les gens peuvent la créer ou la diffuser pour gagner de l'argent ou pour promouvoir leurs objectifs politiques, leurs idées ou leurs croyances religieuses.

Quelqu'un peut publier de fausses informations affirmant qu'un candidat politique est impliqué dans des affaires de corruption. Cela peut inciter des personnes indécises à voter pour le candidat adverse.

Une personne religieuse peut publier de fausses informations selon lesquelles un groupe religieux rival est responsable du meurtre de membres de sa communauté religieuse. Les gens pourraient chercher à se venger des membres de ce groupe rival, même si l'information est fausse et que ces meurtres n'ont jamais eu lieu.

Un fabricant de compléments alimentaires peut lancer une campagne de désinformation pour présenter son produit comme un moyen « naturel » de réduire rapidement la graisse abdominale, alors qu'il n'en est rien.

Comment la désinformation peut-elle se propager aussi facilement ?

Les réseaux sociaux ont changé les méthodes d'accès à l'information et son partage. Ces réseaux sont axés sur le degré d'implication des internautes. Les messages deviennent viraux en fonction du nombre d'appréciations, de commentaires et de partages, et non de la véracité ou de l'exactitude du contenu.

Les réseaux sociaux permettent à pratiquement tout le monde d'atteindre une audience très large avec peu de frais et d'efforts. Le contenu en question est montré aux gens, qu'il ait été vérifié ou non quant à la réalité des faits et de leur exactitude.

Enfin, ces plateformes suivent votre activité en ligne et déterminent vos centres d'intérêt. Elles utilisent ensuite des algorithmes pour vous montrer plus de contenu correspondant à vos intérêts. Si vous lisez, aimez, partagez ou commentez un seul article de désinformation sur les réseaux sociaux, vous risquez d'en recevoir de plus en plus.

Quelles sont les tactiques utilisées pour diffuser la désinformation ?

Les auteurs utilisent les tactiques suivantes pour diffuser la désinformation.

- La publication de contenus hautement émotionnels rédigés pour faire réagir le lecteur.
- Des affirmations sans fondement, des informations tronquées et l'utilisation d'images ou de vidéos trafiquées.
- Les bots et les trolls qui créent et diffusent de fausses informations.
- Le piratage de compte.

Dans les prochaines leçons, vous en apprendrez davantage sur chacune de ces tactiques de diffusion de désinformation, notamment sur la manière de les identifier et les actions à mettre en œuvre pour les contrer.

Lectures recommandées pour la première leçon :

https://fr.wikihow.com/différencier-une-information-inexacte,-une-désinformation-et-une-infox

2e leçon : le contenu provocateur, spectaculaire ou étrange

Dans la première leçon, nous avons appris ce qu'est la désinformation. Pour que la désinformation se répande largement, elle doit aussi être attrayante. Dans les deux prochaines leçons, nous examinerons de plus près le contenu d’une désinformation.

L'un des moyens d'inciter les gens à partager du contenu consiste à faire appel à leurs émotions, en particulier la peur, la méfiance ou la colère. Ces émotions puissantes peuvent prendre le dessus et pousser les gens à agir sans réfléchir.

Dans cette leçon, nous allons examiner le type de contenu trop chargé d'émotions, impressionnant ou trop beau pour être vrai, qu'utilisent les gens pour désinformer, et comment on peut le reconnaitre et le contrer.

Comment reconnaitre le contenu provocateur ?

Commencez par vous demander : « Le contenu essaie-t-il de manipuler mes émotions ? Essaie-t-il de me convaincre que quelque chose est vrai sans apporter de preuves à l'appui ? » Un contenu visant en premier lieu à déclencher vos émotions peut souvent être peu fiable.

Voyons pourquoi. Selon certaines études, si nous nous sentons en colère, bouleversés, choqués ou effrayés, nous sommes plus enclins à partager des informations avec d'autres personnes. En raison du sentiment d'urgence, il est plus probable que nous partagions le contenu sans réfléchir ni vérifier qu'il est vrai.

C'est pourquoi les personnes qui veulent diffuser de fausses informations créent ou partagent du contenu conçu pour susciter de la peur, de la colère ou de la contrariété. Elles savent que si elles peuvent déclencher ce type de réaction émotionnelle, vous serez plus enclin à partager le contenu.

Par exemple, vous pourriez voir un message sur les réseaux sociaux expliquant que la 5G propage la COVID-19 et peut causer le cancer. Le message affirme que votre gouvernement est au courant de ce risque, mais qu'il installe quand même des antennes 5G dans les zones résidentielles. Il vous incite à faire passer le message pour protéger vos amis et votre famille.

Ce message répond à toutes les attentes : il vous effraie, vous encourage à vous méfier de votre gouvernement et vous incite à vous battre pour protéger vos proches.

L'instinct qui nous pousse à partager ce genre de contenu vient normalement d'un bon sentiment.

- Lorsque vous avez peur de quelque chose, votre premier instinct est probablement de prévenir les personnes que vous connaissez de cette menace.

- Lorsque vous vous méfiez d'une personne ou d'une organisation, vous voulez faire prendre conscience aux personnes que vous connaissez et aimez qu'elles ne devraient pas non plus faire confiance à cette personne ou à cette organisation.
- Lorsque vous êtes en colère contre quelque chose, vous voulez que d'autres personnes le sachent afin qu'elles vous aident à lutter contre cette menace.

Les personnes qui créent de fausses informations espèrent que vous agissiez sous le coup de vos émotions en partageant ou en commentant le contenu avant de vous intéresser de plus près à l'histoire pour en vérifier l'exactitude.

Comment se sert-on du contenu étrange ou impressionnant pour faire de la désinformation ?

Parfois, vous voyez du contenu qui semble trop beau pour être vrai. Mais si ce contenu correspond à ce que vous pouvez déjà croire, vous serez plus enclin à vous laisser convaincre. Les psychologues appellent cela le *biais de confirmation*.

Le biais de confirmation fait partie de la nature humaine, tout le monde est touché. Mais cela ne veut pas dire que vous devez forcément y succomber.

Si vous voyez des informations qui correspondent à vos propres idées préconçues, faites une pause et évaluez les informations de plus près avant d'agir.

Rappelez-vous : si quelque chose semble « trop beau pour être vrai », c'est probablement le cas.

Le biais de confirmation peut vous amener à négliger des détails qui sont ridicules et exagérés. Si vous preniez le temps de réfléchir un instant, vous réaliseriez que le message est trop scandaleux pour y croire.

Par exemple, vous pouvez voir un article sur les réseaux sociaux indiquant que l'Antarctique a de plus en plus de glace au lieu d'en perdre. L'article cherche à « prouver » que le changement climatique est une supercherie. Mais si vous prenez le temps de réfléchir, vous vous rendrez compte que ce n'est pas possible, et une recherche en ligne vous montrera que ce n'est pas vrai.

Les personnes qui créent de fausses informations espèrent que vous ne prendrez pas le temps de réfléchir. Elles souhaitent que vous agissiez sous le coup de l'émotion et que vous partagiez immédiatement le message. Leur travail est de faire circuler de fausses informations et elles veulent que vous fassiez leur travail pour elles.

Comment contrer la désinformation découlant d'un contenu provocateur ou impressionnant ?

Le moyen le plus simple de résister à ces tentatives de manipulation de vos émotions est de **faire une pause**. Respirez profondément pendant quelques secondes pour vous calmer, puis faites appel à votre raison pour évaluer l'information.

Pendant votre pause, posez-vous les questions suivantes.

- **Quelle est la source de cette information ?** Si ce n'est pas clair dans le message lui-même, cherchez l'information sur internet. Vérifiez si vous pouvez confirmer que d'autres sources importantes partagent la même information. Si la source de l'article a un parti pris politique, consultez ce que disent les journalistes d'un média du camp adverse.
- **Qui a publié cette information ?** Efforcez-vous de déterminer si cette personne est un expert ou une référence dans son domaine (comme un scientifique ou un universitaire, ou un journaliste référençant des recherches fiables). Si vous ne pouvez pas déterminer les antécédents de l'auteur de l'article, il n'est peut-être pas digne de confiance.
- **Pourquoi voulez-vous partager cette information ?** Si votre intention est d'informer les gens de quelque chose, vérifiez d'abord le contenu. Ainsi, les gens sauront qu'ils peuvent toujours se fier aux informations que vous publiez.

Lisez et vérifiez **toujours** tout ce que vous partagez sur les réseaux sociaux. Parfois, les gens jettent un coup d'œil à un titre et partagent immédiatement l'article sans cliquer dessus et le lire. C'est un moyen facile de tomber dans la désinformation destinée à déclencher une réaction émotionnelle, ne vous laissez donc pas faire. Si vous n'avez pas le temps de lire l'article, ne le partagez que lorsque vous l'aurez fait. Si le contenu de l'article est exact, vous pourrez toujours le partager plus tard.

3e leçon : allégations fabriquées, sélection de preuves et images ou vidéos manipulées

Dans la 2e leçon, nous avons examiné certaines méthodes utilisées par les auteurs de désinformations pour déclencher une réaction émotionnelle afin d'inciter les lecteurs à en diffuser le contenu sans réfléchir.

Ces auteurs tentent également d'employer des preuves et des sources douteuses pour convaincre les lecteurs de la véracité d'une affirmation fabriquée de toutes pièces. Parfois, ils sélectionnent des faits et les présentent de manière trompeuse. Ils peuvent aussi manipuler des images ou des vidéos, ou les sortir de leur contexte.

Dans cette leçon, nous allons voir comment les gens propagent leur désinformation vous faisant croire que des faits et des recherches fiables soutiennent leurs fausses affirmations.

Comment reconnaitre les affirmations fabriquées ?

Abordez tout ce que vous voyez sur internet avec un scepticisme sain. Si un article énonce un « fait », recherchez une source crédible qui le confirme. Une recherche sur le titre ou sur quelques mots-clés de l'article vous donnera accès à d'autres publications qui vous aideront à faire votre vérification.

Vous pouvez également essayer de rechercher quelques mots-clés de l'article en leur ajoutant le mot « faux ». Cette recherche fera apparaitre des articles de vérification des faits en haut de la liste.

Les personnes qui créent de la désinformation peuvent prétendre que leurs fausses informations proviennent d'une agence gouvernementale ou d'une organisation internationale bien connue, comme la NASA ou l'OMS. Allez directement sur le site Web de cette agence et recherchez les informations pour les vérifier.

Une personne qui diffuse de la désinformation peut également prétendre que son affirmation s'appuie sur les déclarations d'un expert, sans le nommer ni l'identifier. Une preuve de ce type n'en est pas vraiment une, car personne ne peut la vérifier.

Si vous ne trouvez pas de source fiable pour étayer le contenu du message, optez pour la sécurité et ne le partagez pas.

Les images ou vidéos hors contexte

Lorsque vous voyez une image en ligne que vous n'avez jamais vue auparavant, demandez-vous si elle reflète la totalité de l'information. Manque-t-il quelque chose qui normalement devrait y être ?

Supposons que vous examiniez la photo d'un enfant qui pleure sous le regard d'une infirmière. La légende dit : « Les vaccins nuisent aux enfants. » Mais est-ce vraiment ce que montre la photo ?

Sans connaitre le contexte de l'image, vous ne pouvez pas savoir si l'enfant pleure à cause d'un vaccin ou pour une autre raison.

Vous pouvez conclure que l'allégation est fabriquée, car rien dans la photo ne montre qu'un enfant est affecté par un vaccin. La personne qui a publié la photo veut vous montrer un enfant qui pleure, et, en raison de la légende, elle espère que vous arriverez à la conclusion qu'elle vous propose.

La sélection de preuves

Parfois, les auteurs des désinformations choisissent quelques éléments vrais et les utilisent pour appuyer une affirmation totalement erronée. Si vous replacez ces éléments dans leur contexte, vous verrez qu'ils ne soutiennent pas du tout l'affirmation en question.

Lisez vous-même la source. Comparez-la au contenu et demandez-vous si celui-ci reflète fidèlement les informations contenues dans la source. Y a-t-il une omission qui pourrait changer la conclusion proposée ?

Par exemple, imaginez un message affirmant que le changement climatique est une supercherie, accompagné d'un graphique montrant une faible variation des températures sur une année.

Il s'agirait d'une sélection de preuve, car l'auteur n'a examiné que les données d'une année et non celles de plusieurs décennies. Si vous placez ces données dans un contexte plus large portant sur de nombreuses années, la conclusion correcte serait que le changement climatique est vraiment une réalité.

Les images ou les vidéos manipulées

Les auteurs de désinformations manipulent également des images ou des vidéos pour qu'elles semblent étayer leurs fausses affirmations. Certaines de ces manipulations sont très techniques et il est difficile de les détecter.

Parfois, les auteurs ne modifient même pas l'image ou la vidéo, mais se contentent de lui donner un nouveau titre ou une nouvelle description. Par exemple, des utilisateurs de réseaux sociaux ont diffusé une vidéo de 2012 montrant une jeune palestinienne affrontant des soldats israéliens et ont prétendu qu'il s'agissait d'une jeune ukrainienne affrontant des soldats russes en 2022.

Il peut être difficile de vérifier de faux messages de ce type, toutefois une recherche d'image inversée vous montrera la même image en ligne, mais dans des contextes différents. Comparez ces images et les informations qu'elles contiennent pour vérifier l'authenticité du message que vous lisez.

Comment pouvons-nous contrer les fausses allégations ?

Avant de partager une information, aussi factuelle ou fiable qu'elle puisse paraitre, vérifiez-la toujours. Si vous ne pouvez pas le faire, ne la partagez pas, c'est aussi simple que cela.

Si vous souhaitez mieux connaitre le contenu auquel vous avez accès, voici quelques moyens de le faire.

Commencez par les sites Web de vérification des faits. Ils font le travail à votre place et vous permettent de déterminer rapidement et facilement la véracité d'une information. En voici quelques-uns à ajouter à vos favoris et à garder à portée de main.

- Snopes : ce site réalise des vérifications de faits et analyse toutes sortes d'affirmations en ligne, de canulars, de légendes urbaines et de rumeurs. Ce site couvre tout.
- Africa Check : ce site fait des vérifications de faits et analyse des articles concernant le continent africain.
- Alt News India : ce site est spécialisé dans la vérification des faits et analyse des articles parus dans les grands médias indiens et les réseaux sociaux.

Pour les **articles,** allez à la source originale selon la nature du contenu.

- Le contenu de reportages sera vérifié et fiable quand il provient d'organes d'information connus et fiables tels que *le New York Times*, *BBC News*, *Deutsche Welle* ou *The Hindu*.
- Les articles scientifiques publiés dans des revues universitaires évaluées par des pairs sont généralement considérés comme fiables.

Pour les **images**, effectuez une recherche inversée d'images afin de trouver des copies de la même image en ligne. Ces copies vous aideront à vérifier la date de création de l'image et à trouver sa source initiale.

Pour les **vidéos**, utilisez YouTube Data Viewer, créé par Amnesty International, pour trouver la date et l'heure exactes du téléchargement de la vidéo, ainsi que sa vignette. Vous pouvez effectuer une recherche d'image inversée de la vignette pour trouver éventuellement des versions plus anciennes de la même vidéo.

Encore une fois, si vous ne pouvez pas vérifier les informations contenues dans un message, **ne le partagez pas**. Si l'une de vos connaissances le partage, contactez-la et dites-lui qu'il s'agit probablement d'une désinformation. Et n'oubliez pas que le fait de commenter un message, même pour dire qu'il contient des informations fausses, le fera connaitre à un public plus large. Il est donc préférable de ne pas interagir avec lui.

Par contre, vous pouvez le signaler à la plateforme de publication en utilisant le lien sur le message. Cela ne prend que quelques secondes et le compte que vous signalez ne saura pas que vous l'avez fait.

Vous ne pourrez peut-être pas empêcher les gens de créer de la désinformation, mais vous *pouvez* contribuer à ralentir sa propagation.

4e leçon : les bots et les trolls

Dans la 3e leçon, nous avons appris comment les gens utilisent des affirmations inventées, des preuves sélectives et des images ou des vidéos déformées pour créer de la désinformation. Dans cette leçon, nous allons nous intéresser à deux moyens connexes de diffusion de la désinformation : l'utilisation de robots et de trolls.

Des milliers de comptes « bots » ou « trolls » créent des millions de messages de désinformation qui sèment le désordre et la confusion. Les bots et les trolls interagissent également avec les utilisateurs sur les plateformes de réseaux sociaux, principalement par le biais de commentaires et de messages privés. Les personnes qui ne savent pas ce qu'ils sont les suivent, ce qui risque de propager davantage leur désinformation.

Cela peut être dangereux. Par exemple, la désinformation concernant une bande de kidnappeurs d'enfants, diffusée sur le service de messagerie mobile WhatsApp, a provoqué des actes de violence en Inde.

Pour aider à stopper la propagation de ce type de désinformation néfaste, il est bon de savoir ce que sont les bots et les trolls, pourquoi ils sont utilisés et comment les repérer.

Qu'est-ce qu'un bot ?

Un bot est simplement un programme informatique qui gère un compte sur une plateforme de réseau social.

Les programmeurs conçoivent le programme du bot pour qu'il comprenne, apprenne et réponde au texte. Cette *intelligence artificielle* (IA) permet au bot d'interagir avec d'autres comptes de la même manière qu'une personne réelle le ferait. Plus la programmation est sophistiquée, plus le bot semblera réel.

Comment reconnaitre un bot ?

De manière générale, vous pouvez reconnaitre un bot en prenant quelques minutes pour consulter son compte.

Allez sur la page principale du compte et vérifiez les éléments suivants.

- **La photo de profil :** les comptes bots n'ont généralement pas de photo de profil. S'ils en ont une, c'est souvent une image générique d'un paysage ou d'un animal mignon.
- **Le nom de l'utilisateur :** les comptes bots ont souvent un nom d'utilisateur qui semble généré de façon aléatoire, comme « Xchtkrz7942 ». Il peut également s'agir d'un nom courant suivi de chiffres, comme « ChrisJones82 » ou « John87924 ».

- **L’activité du compte :** les comptes bots sont beaucoup plus actifs que l'utilisateur moyen. Si le compte publie plusieurs messages en quelques secondes, c'est un signe qu'il est automatisé.
- **Le schéma d'activité :** les comptes bots publient fréquemment à intervalles réguliers, de jour comme de nuit. Ils ne suivent pas les schémas typiques d'un humain, dont le compte reste souvent inactif pendant les heures où il travaille ou est en train de dormir.
- **Le ratio d'abonnés :** les comptes bots suivent n'importe qui et tout le monde pour développer leur réseau. En général, ils suivent beaucoup de personnes, mais n'ont pas beaucoup d'abonnés.
- **Les hashtags :** les comptes bots utilisent *beaucoup* de hashtags pour essayer de rendre un message viral. La plupart des hashtags utilisés sont « tendance » au moment où le contenu est publié. Souvent, les hashtags n'ont aucun rapport avec le contenu.
- **La qualité du contenu :** les comptes bots n'ont typiquement pas de contenu original. Leurs publications sont plutôt des copies exactes des publications d'un autre compte. Les articles sont aussi souvent répétitifs et peuvent même afficher exactement le même contenu plusieurs fois par jour.

Un seul signe n'est pas suffisant pour dire que le compte est un bot, mais plusieurs signes réunis doivent vous alerter. Regardez le compte dans son ensemble et si vous avez le moindre doute, suivez votre instinct !

Comment protéger notre flux d’actualité des bots ?

Surveillez les demandes d'amis ou de suivi sur les réseaux sociaux. S'il s'agit d'un compte quelconque que vous ne connaissez pas, vérifiez l'historique des publications et les informations relatives au compte avant d'accepter la demande et de le suivre.

Si vous pensez qu'un compte est un bot, signalez-le à Facebook, Instagram ou Twitter et bloquez le compte.

Enfin, si quelqu'un que vous connaissez partage de fausses informations provenant d'un bot, dites-le-lui ! Vous pouvez commencer par lui demander s'il connait le propriétaire du compte. S'il répond par la négative, dites-lui que vous pensez qu'il

s'agit d'un bot.

Vous pouvez dire : « Toutes les publications sont en fait identiques, encore et encore. Il s'agit probablement d'un bot. Si j'étais toi, je le supprimerais et je veillerais à ne plus partager d'informations provenant de ce compte. »

Qu'est-ce qu'un troll ?

La grande différence entre les bots et les trolls est que les trolls sont des *personnes réelles*. Un troll est une personne qui provoque intentionnellement des conflits en ligne. Il veut offenser, créer la confusion ou détourner l'attention des gens. Certains trolls travaillent pour d'autres personnes, mais de nombreux autres sont indépendants.

Les trolls sont souvent actifs dans les fils de commentaires des publications. Ils peuvent énerver les gens en attaquant leurs propos. Ils font également des commentaires extrêmes pour inciter les autres à les attaquer.

Lorsque les trolls publient leur propre contenu, il s'agit généralement de quelque chose d'extrême, conçu pour mettre les gens en colère ou les contrarier.

Comment reconnaitre un troll ?

Tout comme pour les bots, la page du compte principal d'un troll contient des indices sur son identité. Cherchez les éléments suivants.

- **La photo de profil :** les comptes de trolls n'ont pas de photo de profil ou en ont une qu'ils ont clairement téléchargée sur internet.
- **Le nom de l'utilisateur :** les comptes de trolls ont souvent un nom d'utilisateur humoristique. Ils peuvent également usurper le nom d'une personnalité publique, comme un compte portant le nom d'utilisateur « Elon Muskk » ou « B1ll G@tes ».
- **L'activité du compte :** en général, les comptes de trolls ont peu de publications, car l'essentiel de leur activité consiste à commenter les publications des autres. Le moment ainsi que la fréquence de leurs commentaires peuvent donner l'impression qu'ils sont en ligne en permanence.

- **Les informations personnelles :** les comptes de trolls ne possèdent souvent pas d'informations personnelles ni de photos. S'ils ont des publications, vous ne verrez probablement pas de commentaires de la part d'utilisateurs qui semblent les connaitre.
- **L'ancienneté du compte :** en général, les comptes de trolls sont très récents. Il ne faut souvent pas longtemps pour qu'un compte de troll soit signalé et fermé par une plateforme, ce qui signifie tout simplement que le troll doit créer un nouveau compte.

Comment protéger votre fil d'actualités des trolls ?

Vous avez peut-être déjà entendu le conseil « Ne nourrissez pas les trolls. » C'est un bon conseil, peu importe ce que dit le troll !

Même lorsqu'ils ne diffusent pas de désinformation, les trolls aiment énerver les gens et provoquer la confusion. Ils n'atteindront pas leurs objectifs si vous refusez d'entrer dans leur jeu.

La meilleure réponse à un troll est de ne pas répondre du tout. N'oubliez pas que si vous répondez à un troll dans un fil de commentaires, vous faites connaitre ce contenu à un public plus large. S'il vous agresse, bloquez son compte pour ne plus jamais voir ses commentaires. Vous pouvez également signaler le compte à la plateforme.

Il est recommandé d'informer les autres utilisateurs qu'un compte est un troll. Si vous voyez quelqu'un se disputer avec un troll dans un fil de commentaires, vous pouvez l'encourager à ignorer le troll. Les trolls ne méritent pas qu'on leur accorde du temps.

Lecture recommandée pour la 4^{e} leçon :

https://fr.wikihow.com/identifier-un-troll-sur-Internet
https://www.wikihow.com/What-Is-a-Bot

5e leçon : les comptes piratés

Dans la 4e leçon, nous avons appris comment les gens utilisent des bots et des trolls pour faire circuler de fausses informations sur internet, en particulier sur les réseaux sociaux.

En général, les bots et les trolls opèrent via des comptes fraichement créés. Toutefois, les personnes qui souhaitent diffuser de fausses informations peuvent également pirater des comptes existants et en prendre le contrôle.

Dans cette leçon, vous apprendrez ce qu'est le piratage, la manière de l’utiliser pour désinformer, et les raisons pour lesquelles il est si populaire. En outre, vous saurez comment reconnaitre un compte piraté et ce que vous devez faire lorsque vous en voyez un. Enfin, vous apprendrez à protéger vos propres comptes contre le piratage.

Qu'est-ce que le piratage ?

Le piratage consiste à obtenir un accès non autorisé à un compte existant.

Le moyen le plus simple d'y parvenir est de deviner le mot de passe du propriétaire du compte. Cela est particulièrement facile si le titulaire du compte utilise un mot de passe très simple, tel que « motdepasse1234 ». Toutefois, les pirates ont aussi recours à des programmes sophistiqués pour décoder des mots de passe plus complexes.

Une fois qu'un pirate a réussi à avoir accès à un compte, il change généralement le mot de passe et l'adresse e-mail de récupération afin d'y avoir toujours accès. Il devient alors difficile pour la personne qui a initialement ouvert le compte de le récupérer.

Pourquoi le piratage informatique est-il si populaire ?

Si quelqu'un souhaite répandre de fausses informations, il pourrait créer son propre compte sur les réseaux sociaux et y publier ce qu'il veut. Cependant, il rencontrerait un problème : il n'a pas d'abonnés.

Les informations qu'il va publier n'iront donc pas très loin et ne seront pas vues par un grand nombre de personnes. Alors, comment peut-il obtenir plus d’abonnés ?

Le piratage est un moyen rapide. Après tout, les comptes existants disposent déjà de bases d'abonnés, en espérant qu'elles sont actives.

Ces comptes ont également une bonne réputation auprès de leurs abonnés. Les gens font confiance aux titulaires de ces comptes et aux informations qu'ils partagent.

Si un pirate informatique obtient l'accès à un tel compte, il lui sera beaucoup plus facile de faire de la désinformation.

Comment reconnaitre un compte piraté ?

Il est très facile de savoir si votre compte a été piraté. Dans la plupart des cas, il vous sera impossible d'y accéder, car votre mot de passe aura été modifié. Vous pourrez également recevoir un e-mail de la plateforme vous avertissant que votre compte a été consulté sur un appareil inconnu.

Mais qu'en est-il des comptes que vous suivez ? S'ils sont piratés, pouvez-vous le savoir ? C'est un peu plus délicat, mais voici quelques éléments à prendre en compte.

- Vous recevez un message direct étrange ou inhabituel du compte. Par exemple, vous pouvez recevoir un message d'une personne que vous voyez tous les jours au travail et qui commence par : « Ça fait longtemps qu'on ne s'est pas vu. »
- Le compte publie des messages à des heures qui ne cadrent pas avec les habitudes de son titulaire.
- Les messages sont étranges au regard de la personne qui possède le compte. Par exemple, un message d'un ami écologiste affirmant que le changement climatique est une supercherie.
- Le compte fait des commentaires ou répond à d'autres commentaires de manière étrange ou déroutante, par exemple des commentaires hostiles à un ami proche.

Comment pouvez-vous contrer la désinformation provenant de comptes piratés ?

Si vous suivez un compte qui, selon vous, a été piraté, **ne partagez et ne commentez** aucune de ses publications jusqu'à ce que le propriétaire initial ait récupéré son compte.

Dans la mesure du possible, contactez le propriétaire du compte par téléphone ou par e-mail et faites-lui savoir que vous pensez que son compte de réseau social a été piraté.

Il devra sans doute contacter la plateforme pour vérifier son identité et récupérer son compte.

Proposez-lui de publier un message sur votre propre compte pour informer les gens que le compte a été piraté. Cela est particulièrement utile si vous avez beaucoup d'abonnés en commun.

Si vous ne connaissez pas le mail ou le numéro de téléphone du propriétaire du compte, signalez le compte à la plateforme.

Comment pouvez-vous vous protéger contre le piratage ?

Tout le monde est potentiellement vulnérable aux pirates, même les « petits » comptes qui n'ont pas beaucoup d'abonnés.

Heureusement, il y a quelques mesures simples que vous pouvez prendre pour rendre votre compte moins attrayant pour les pirates. Examinons-les plus en détail.

- Activez **l'authentification à deux facteurs**. Après avoir saisi votre mot de passe pour vous connecter à votre compte, la plateforme envoie un code à un numéro de téléphone que vous aurez fourni. Il est impossible d'accéder à votre compte sans saisir ce code.
- Utilisez un **mot de passe sécurisé**. Les mots de passe les plus sécurisés sont composés de lettres minuscules et majuscules aléatoires, ainsi que de chiffres et d'autres caractères, tels que * ; & ou $. S'ils réduisent les risques de piratage de votre compte, ils sont également difficiles à mémoriser. Votre navigateur vous proposera des mots de passe sécurisés et les remplira automatiquement à partir d'un fichier crypté. Vous pouvez également télécharger un gestionnaire de mots de passe si vous souhaitez avoir accès à vos mots de passe sécurisés sur plusieurs appareils.
- Utilisez **différents mots de passe** pour chaque compte que vous possédez. Le gestionnaire de mots de passe de votre appareil vous facilite la tâche. L'emploi de mots de passe différents permet simplement de vous assurer que si des pirates accèdent à l'un de vos comptes, ils ne pourront pas accéder aux autres.

- **Changez vos mots de passe** au moins une fois par an. Plus longtemps vous utilisez le même mot de passe, plus vous laissez de temps aux pirates de le découvrir. Si quelqu'un a réussi à accéder à votre compte, changer votre mot de passe implique un retour à la case départ.

Savoir comment reconnaitre les comptes de réseaux sociaux piratés et comment protéger les vôtres vous donne un autre moyen de lutter contre la désinformation.

Lectures recommandées pour la 5e leçon :

https://fr.wikihow.com/ne-pas-se-faire-pirater-(hacker)-sur-internet
https://fr.wikihow.com/protéger-son-compte-Facebook-des-pirates-informatiques
https://fr.wikihow.com/savoir-si-on-a-été-piraté

Félicitations, vous avez terminé le cours !

Nous sommes convaincus que vous avez appris des éléments précieux pour identifier et ralentir la propagation de la désinformation. Êtes-vous prêt à tester vos connaissances ? Faites notre quiz sur le cours pour montrer ce que vous avez appris !

Faites le quiz !