4.

RÉDUISEZ VOS TRACES

Le navigateur de votre téléphone conserve beaucoup d'informations à votre sujet – votre localisation, vos recherches, les sites que vous utilisez – et peut les révéler. Vous pouvez reprendre le contrôle sur certaines d'entre elles grâce à quelques modifications.

Les téléphones, les tablettes et les ordinateurs sont généralement fournis avec des navigateurs déjà installés et sans égard pour votre vie privée. Au lieu de vous en servir, vous pouvez **télécharger et utiliser un navigateur qui protège votre activité en ligne par défaut** et bloque les pisteurs.

Pour plus de confidentialité, vous pouvez installer des « add-ons et des extensions » supplémentaires (ce sont des modules pour votre navigateur, faciles à installer, qui **peuvent protéger les données de votre activité en ligne plus encore**).

5.

RETIREZ VOTRE IDENTIFICATION ET CELLE DES AUTRES

Vous avez déjà participé à l'accumulation de données de vos ami·es en les identifiant sur des photos ou dans des publications ? Réduisez leur trace visible (et soulagez votre conscience au passage) en **retirant cette identification** sur autant de photos et publications que possible.

Donnez l'exemple ! Encouragez vos proches et vos collègues à vous imiter et à reprendre le contrôle de toutes leurs données éparpillées. Si nous nous y mettons tous ensemble, la désintoxication sera plus facile.

Produit par

TACTICAL TECH

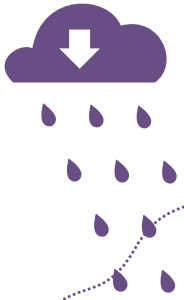
Avec le soutien de

Firefox

datadetoxkit.org
#datadetox

Pour bloquer les publicités espionnes et les pisteurs invisibles, installez uBlock Origin (pour Chrome, Safari et Firefox) ou Privacy Badger (pour Chrome, Firefox et Opera).

Pour que votre connexion aux sites soit la plus sûre possible, installez HTTPS Everywhere : une extension qui vous garantit le chiffrage et la protection de vos communications sur de nombreux sites internet de grande envergure. Si vous utilisez Safari et souhaitez bénéficier de cette fonctionnalité, définissez un moteur de recherche par défaut qui soit autre que Google (par exemple DuckDuckGo) et qui vous redirigera automatiquement vers des connexions chiffrées.



DATA DETOX KIT

CONTRÔLEZ LES DONNÉES DE VOTRE SMARTPHONE

pour améliorer votre vie privée en ligne

Si vous réfléchissez à ce que vos données peuvent révéler à votre sujet, cela peut vous sembler négligeable : peu importe que l'on sache que vous aimez la musique country, que vous adorez les chaussures ou que vous organisez vos vacances une année à l'avance.

Mais le problème vient de ce que l'on fait avec vos données. Lorsqu'elles sont accumulées sur la durée, elles font **émerger des schémas numériques intimes :** vos habitudes, vos déplacements, vos relations, vos préférences, vos opinions et vos secrets sont révélés à ceux qui les analysent et en tirent profit, comme des entreprises et les courtiers en données.

En lisant ce Data Detox (détox de données), vous aurez un aperçu du fonctionnement et des causes de ce phénomène, ainsi que des mesures concrètes pour **limiter les traces que vous laissez sur internet.**

C'est parti !

1.

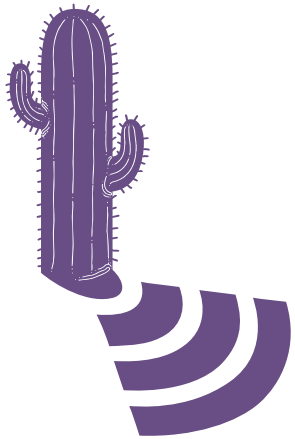
CHANGEZ LE NOM DE VOTRE APPAREIL

Vous avez peut-être donné un nom pour le Wi-Fi votre appareil, son Bluetooth ou les deux. Peut-être même que son nom a été généré automatiquement lors de l'installation.

Cela signifie que « Téléphone d'Alex Chung » est le nom qui apparaît au propriétaire du réseau Wi-Fi et, si votre Bluetooth est activé, à toute personne à proximité dont le Bluetooth est également activé.

Vous ne donnez pas votre nom à tout le monde en entrant dans un café, un restaurant ou un aéroport, alors pourquoi votre téléphone devrait-il le faire ?

Vous pouvez **modifier le nom de votre téléphone** et lui en donner un **qui vous identifie moins directement**, mais qui soit tout de même unique et personnel. Voici comment faire :



iPhone:
Modifier le nom du téléphone :
Réglages → Général → Informations → Changez le nom de votre téléphone

Android:
Modifier le nom du Wi-Fi :
Paramètres → Wi-Fi → Menu → Options avancées / Plus → Wi-Fi Direct → Menu → Configurer l'appareil → Renommer l'appareil
Modifier le nom du Bluetooth :
Paramètres → Bluetooth → Activez le Bluetooth s'il est désactivé → Menu → Renommer cet appareil → Désactivez le Bluetooth

2.

EFFACEZ LES TRACES DE VOTRE LOCALISATION

Vos données de localisation peuvent vous sembler sans importance, mais une fois rassemblées, elles peuvent révéler vos habitudes ainsi que **d'importantes informations à votre sujet**, comme votre lieu de résidence, votre lieu de travail et les lieux que vous aimez fréquenter avec vos ami·es. C'est pour cela que les courtiers de données et de nombreuses entreprises s'y intéressent.

Vous pouvez **consulter les permissions de chaque application** et **désactiver les services de localisation**. Cherchez les applications qui n'en ont pas besoin pour fonctionner (votre localisation est-elle vraiment nécessaire pour tel et tel jeux ?) et celles auxquelles vous ne souhaitez pas la donner :

Android:
Paramètres → Applications → Définissez l'accès aux données de localisation individuellement

iPhone:
Réglages → Confidentialité → Services de localisation → Définissez l'accès aux données de localisation individuellement

3.

METTEZ DE L'ORDRE DANS VOS APPLICATIONS

Vos applications de médias sociaux, de jeux et de météo s'intéressent à vos données... et elles peuvent en recueillir beaucoup.

Effacer toutes les applications que vous n'utilisez jamais peut s'avérer être une excellent méthode de détox pour votre vie en ligne.

Ce nettoyage vous permet également de libérer de l'espace sur votre téléphone, de réduire votre consommation de données et de prolonger la durée de vie de votre batterie. En fonction de l'application, cela peut même améliorer les performances générales de votre appareil.

Android:
Paramètres → Applications → Sélectionnez l'application que vous souhaitez désinstaller → Désinstallez-la

iPhone:
Maintenez appuyé sur une application jusqu'à ce qu'elles s'agitent toutes et qu'une petite croix apparaisse au coin supérieur gauche de chaque application.
Pour supprimer une application, appuyez sur la petite croix.
Pour revenir à la normale, appuyez sur le bouton principal.

4.

PROTÉGEZ VOS DONNÉES IMPORTANTES

De la même manière que vous prenez soin des objets de valeur chez vous, prenez soin des données que vous stockez en ligne.

Un **nettoyage ciblé** est parfait pour effectuer quelques améliorations rapides. Cherchez des informations précises dans votre messagerie ou tout autre compte et supprimez-les : des numérisations de vos pièces d'identité, vos coordonnées bancaires ou vos informations d'assurance maladie, par exemple. Si vous pensez avoir besoin de ces données et documents par la suite, vous pouvez toujours les télécharger ou les imprimer avant de les supprimer de votre messagerie.

Un **nettoyage en profondeur** sera plus efficace. Il est bon d'en faire un par an. Archivez toutes les données de vos comptes de messagerie ou de médias sociaux, téléchargez-les et supprimez-les de vos comptes pour repartir de zéro.

Conseil : Supprimer ne suffit pas, videz votre corbeille et effacez les fichiers temporaires !

À vous de décider si vous voulez enregistrer vos archives et documents sur un service de cloud ou les conserver sur un disque dur externe ou une clé USB. Employez la méthode qui vous convient le mieux et, quel que soit votre choix, faites en sorte de ne pas perdre vos données et de les protéger avec un mot de passe robuste.

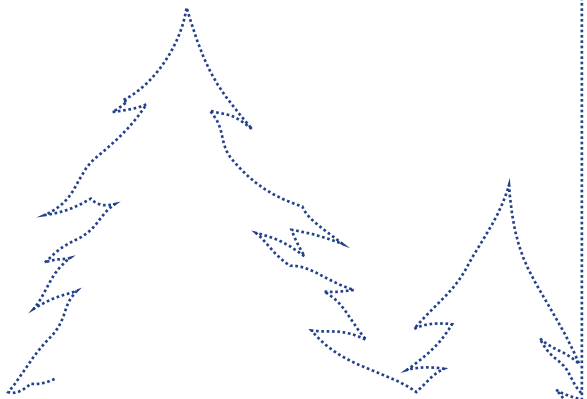
5.

PASSEZ LE MESSAGE

Lorsque vous sécurisez vos comptes, renforcez vos mots de passe et nettoyez vos données, ce sont **tous·tes celles et ceux à qui vous êtes connecté·es qui en bénéficient et gagnent en sécurité.**

Lorsque vous nettoyez vos comptes de messagerie et de médias sociaux, réfléchissez à ce que vous pourriez télécharger et supprimer qui pourrait aider vos proches et collègues : les coordonnées bancaires de votre sœur, le code de la porte de votre bureau, ou encore une numérisation du passeport de votre fils sont des données qui, si elles tombaient entre de mauvaises mains, pourraient vous causer bien des soucis.

Passez le message ! Il suffit de suivre quelques étapes simples pour améliorer votre sécurité en ligne. Faites passer ce Data Detox (détox de données) à vos proches ou vos collègues pour les aider à changer leurs habitudes à leur rythme.



DATA DETOX KIT

CHANGEZ VOS PARAMÈTRES

pour protéger vos données

Si internet ne servait qu'à échanger des photos de chiens en costumes de dinosaures, nous n'aurions pas besoin de mots de passe. Mais sur internet, vous pouvez aussi payer vos factures, renouveler vos ordonnances et vous enregistrer sur les listes électorales. Réfléchissez à toutes les données personnelles et importantes que vous faites transiter par internet et que vous stockez sur vos appareils. **Pourquoi devraient-elles moins bien protégées que vos clés ou votre portefeuille ?**

Il existe un bon moyen d'empêcher les autres d'accéder à vos données importantes : **choisissez des mots de passe difficiles à deviner.** La plupart du temps, aucune compétence technique n'est nécessaire pour accéder à vos comptes. Il suffit de quelques tentatives pour deviner un mot de passe, ou d'utiliser un programme qui le fait automatiquement.

Et lorsqu'une personne a accès à un compte, elle peut essayer d'utiliser le mot de passe de ce dernier pour accéder à d'autres comptes, rassembler des informations sur vous et vos habitudes, prendre le contrôle de vos comptes, voire de votre identité en ligne.

En suivant ce Data Detox (détox de données), vous trouverez des mesures concrètes pour améliorer votre sécurité en ligne.

Allons-y !

Produit par
TACTICAL TECH

Avec le soutien de
Firefox

datadetoxkit.org
#datadetox

1.

VERROUILLEZ LA PORTE DE VOTRE UNIVERS NUMÉRIQUE

La protection de votre téléphone, tablette ou ordinateur, sera toujours meilleure avec n'importe quel type de verrouillage que sans. Et à l'image des différents types de verrous que vous pouvez avoir à vos portes, **certains écrans de verrouillage sont plus robustes que d'autres.**

De tous les verrouillages existants, les mots de passe longs et uniques sont la meilleure protection. Cela signifie que si vous utilisez un mot de passe pour protéger votre appareil, il doit comprendre des lettres, des chiffres et des caractères spéciaux.

Si vous déverrouillez votre téléphone tout simplement en faisant glisser votre doigt sur votre écran, vous pouvez augmenter le niveau de sécurité en passant à un long mot de passe. Si vous utilisez un motif de verrouillage, pourquoi ne pas en choisir un plus long ? Votre code PIN est 1234 ? Vous pourriez lancer des dés sept fois et utiliser les chiffres obtenus en guise de code PIN.

Une petite modification peut avoir un énorme impact sur le contrôle que vous avez sur vos appareils.

2.

RÉGLEMENTER LES ACCÈS

Pour créer des mots de passe de qualité, c'est simple. Il suffit de respecter quelques règles de base. Vos mots de passe doivent être :

Longs : **les mots de passe doivent être composés de 8 caractères au minimum. Pour un mot de passe encore plus sécurisé, employez entre 16 et 20 caractères !**

Uniques : **chaque mot de passe – pour chaque site – doit être différent.**

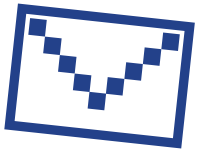
Aléatoires : **vos mots de passe ne doivent pas suivre un schéma logique ou être trop faciles à deviner. Un gestionnaire de mots de passe vous sera donc très pratique.**

Les meilleurs mots de passe sont composés de lettres, de chiffres et de caractères spéciaux. Il n'y a toujours pas de meilleur conseil pour créer un mot de passe robuste et difficile à deviner. Certains systèmes ne vous permettent toutefois pas d'utiliser des caractères spéciaux (comme @#$%-=+), mais une longue combinaison de lettres et de chiffres sera toujours meilleure qu'un mot de passe plus court.

La solution idéale est d'utiliser un **gestionnaire de mots de passe** pour générer et stocker tous vos mots de passe. Il s'agit d'un logiciel — comme 1Password ou KeePassXC, qui sont recommandés par des experts en matière de sécurité — dont la fonction principale est de protéger vos identifiants et autres données sensibles.

3.

AJOUTEZ UN DEUXIÈME VERROU



En instaurant une vérification en deux étapes (2FA) ou une authentification multi-facteurs (MFA), même si quelqu'un trouve votre mot de passe, **il lui manquera probablement les informations d'authentification associées pour accéder à votre compte.**

Consultez les paramètres de sécurité des sites et applications que vous utilisez le plus souvent pour voir si cette fonctionnalité est disponible. Commencez par les plus importants — les applications bancaires, ou les services de messagerie que vous utilisez pour récupérer les informations d'accès à vos autres comptes.

Google:
Connectez-vous à myaccount.google.com → Sécurité → Validation en deux étapes → Commencer

Facebook:
Menu → Paramètres → Sécurité et connexion → Utiliser l'authentification à deux facteurs

Conseil : Au moment d'établir un niveau de vérification supplémentaire, vous devrez sélectionner un autre moyen de confirmer votre identité. Évitez de choisir les SMS (messages textuels envoyés à votre téléphone), au cas où vous perdriez votre téléphone. Un e-mail est généralement plus fiable.

4.

FAITES-VOUS ENTENDRE

Si le côté addictif ou persuasif des sites que vous fréquentez ou des applications que vous utilisez, ou encore les informations erronées qu'ils diffusent, vous déplaisent, vous pouvez contacter les entreprises responsables par e-mail ou sur Twitter pour leur exprimer votre désaccord concernant leurs méthodes. Lorsque les entreprises sont sommées d'agir par ce qu'elles ont de plus précieux, leurs utilisateurs, elles sont plus disposées à changer.

Si vous considérez que votre voix ne compte pas, il vous reste un atout de taille : utiliser un site ou une application différent·e. Si vous avez communiqué votre mécontentement vis-à-vis des méthodes d'un site ou d'une application et que vous cessez aussitôt de l'utiliser ou que vous la supprimez – et qu'assez de gens suivent le mouvement – **les entreprises le remarqueront.**

5.

RÉPANDEZ LE MESSAGE

Faites passer ! Il est facile de l'oublier, mais cela peut avoir un impact considérable. Parlez à vos proches et vos collègues de ce que vous découvrez, vous pouvez même leur proposer de vous accompagner dans cette détox !

Changer ses habitudes vis-à-vis de son téléphone n'est facile pour personne. Le plus important est de trouver la méthode qui vous convient et correspond à votre mode de vie. Essayez-vous à différentes choses afin de trouver la solution qui vous satisfait, puis changez vos habitudes en fonction de vos besoins. Il n'y a pas de solution miracle.

Et pour finir, parlez de vos choix autour de vous. Si vous choisissez de mettre vos écrans de côté tous les jours à partir de 20 h, dites-le à vos proches afin qu'ils privilégient les appels au lieu de vous contacter sur votre application de messagerie.

Restez ouvert·e au dialogue et posez de questions, vous pourrez ainsi trouver l'équilibre qui vous convient en ligne.

DATA DETOX KIT

CHANGEZ LES RÉGLAGES PAR DÉFAUT

pour accroître votre bien-être en ligne

Quand vous êtes-vous « déconnecté·e » de la technologie pour la dernière fois, que ce soit pour une journée ou même une heure ? Si vous êtes en ligne en permanence, vous n'êtes pas seul·e. Comment faire en sorte que le temps passé sur votre appareil en vaut la peine ?

Pour commencer, vous devez savoir que vous n'êtes pas responsable de l'attrait irrésistible de vos appareils ! Croyez-le ou non, vos sites et applications préféré·es sont conçu·es de telle façon que chaque fonction, couleur et son ont été « optimisé·es » pour vous y scotcher et vous pousser à y retourner.

Vous voulez trouver un meilleur équilibre entre votre vie en ligne et hors ligne ? C'est ce que vous propose cette partie du Data Detox (détox de données).

Allons-y !

Produit par
TACTICAL TECH

Avec le soutien de
Firefox

datadetoxkit.org
#datadetox

1.

PROFITEZ DU MOMENT PRÉSENT

C'est plus facile à dire qu'à faire. Rester ancré·e dans le présent est un défi quotidien. Comme s'il fallait régulièrement entraîner un muscle dans notre cerveau pour le renforcer. Vous pouvez commencer en prenant conscience de votre rapport à vos appareils.

Combien de temps passez-vous sur votre téléphone ?

Si la réponse ne vous satisfait pas, vous pouvez tirer parti de paramètres et de stratégies pour reprendre le contrôle sur vos appareils.

Si votre but est de passer moins de temps sur Facebook, Instagram ou Snapchat, changez leurs paramètres et leurs permissions pour obtenir un résultat à votre convenance. Certaines applications, comme Instagram, disposent d'une option permettant de mettre en place un rappel lorsque vous atteignez la limite d'utilisation quotidienne que vous vous êtes fixée.

Instagram:
Profil → Menu → Paramètres → Compte → Votre activité → Rappel quotidien

Si les sons, les vibrations ou les clignotements de votre téléphone vous perturbent lors de conversations hors ligne, vous pouvez les désactiver temporairement, retourner votre téléphone, ou encore le mettre hors de vue dans votre poche ou votre sac.

2.

IDENTIFIEZ LES ARTIFICES

La conception persuasive, aussi appelée « interface truquée », est une conception s'appuyant sur des connaissances en psychologie et employée afin de vous pousser à souscrire à quelque chose, à acheter quelque chose ou à fournir plus d'informations personnelles que prévu.

Parmi les méthodes de conception persuasive, on compte l'emploi de certaines couleurs, la position de boutons, des textes confus ou des informations incomplètes. Ces artifices sont parfois évidents, mais ils peuvent aussi être plus difficiles à repérer. Si vous pouvez en retrouver partout, c'est bien parce que ces astuces fonctionnent - elles nous font cliquer, souscrire ou acheter plus souvent et nous font revenir.

Vous pouvez déjouer les pièges de vos applications de plusieurs manières.

Reconnaissez les manipulations : pour commencer, vous pouvez simplement prendre conscience des techniques utilisées.

Capturez et partagez : prenez des captures d'écran dès que vous trouvez des exemples de conception persuasive en ligne et partagez-les avec vos amis (sans y inclure d'informations personnelles, pensez à votre vie privée !). Vous pouvez également demander aux entreprises de changer leurs méthodes.

Restez calme : si une page d'achat comporte un compte à rebours, réfléchissez au caractère urgent de votre achat. Si vous cliquez sur un bouton sans vraiment le vouloir, pensez à la formulation ou aux couleurs utilisées par le service. Si vous vous sentez perdu·e, ne considérez pas tout de suite en être responsable — réfléchissez aux mots employés par le site ou l'application utilisé·e, ils sont parfois ambigus.

3.

RESTEZ VIGILANT·E VIS-À-VIS DES MÉDIAS

Tout comme vous pouvez vous détacher des fonctionnalités conçues pour vous pousser à faire défiler (votre fil d'actualités) ou cliquer, vous pouvez également prendre le recul nécessaire pour détecter les articles et publications qui cherchent à vous tromper.

Vous devez déjà être sensible aux problèmes de « d'informations erronées » et de « fausses informations ». Vous pouvez éviter les informations erronées en prenant l'habitude de vous poser des questions critiques concernant les articles que vous lisez, surtout s'ils vous semblent surprenants, scandaleux ou trop beaux pour être vrais.

Ce qui compte, c'est de vérifier quelles informations sont vraies ou fausses, surtout si vous comptez les partager à vos proches.

De quel site proviennent les informations ?
Qui les a écrites (et quand) ?
Que dit l'article au-delà de son titre ?
À quelles sources fait-il référence ?

Si vous pensez qu'il s'agit d'informations erronées et que vous voulez en empêcher la diffusion, la plupart des plateformes disposent d'une fonction vous permettant de signaler une publication. Profitez aussi de la situation pour vous demander si vous voulez rester abonné·e au compte ayant publié ces informations.

DATA DETOX KIT

5.

CHERCHEZ LA VÉRITÉ SUR INTERNET

Le terme infox se rapporte à différents types d'informations fausses ou inexactes, telles que les satires, le contenu non vérifié ou n'ayant pas bénéficié de recherches suffisantes, les canulars et les arnaques.

Au mieux, ce peut être un mème amusant (un mème est un élément culturel ou comportemental qui se transmet d'un individu à un autre par imitation ou par d'autres moyens non génétiques). Au pire, ce peut être une information médicale incorrecte ou une fausse information politique.

Même en faisant de votre mieux pour approfondir et poser des questions critiques sur les articles que vous lisez, vous pouvez vous sentir perdu·e. Mais sachez que vous n'êtes pas seul·e !

Mobilisez toutes les ressources disponibles
Qu'un site internet ne reconnaisse pas ses erreurs ne veut pas dire qu'il n'en fait pas. Les publications les plus fiables sont celles qui accordent le plus d'attention aux faits et qui emploient plusieurs personnes, voire des départements entiers, pour vérifier les informations.

Cherchez les sources qui corrigent leurs erreurs lorsqu'elles en font. Et lorsqu'elles indiquent les mises à jour en début d'article et les partagent sur les médias sociaux, vos recherches seront facilitées.

6.

SORTEZ DE VOTRE BULLE DE FILTRES

Une fois que les sites internet et les applications auront constitué votre profil, vous risquez de vous retrouver dans une bulle de filtres. C'est ce qu'il se produit lorsque les différentes plateformes vous proposent des articles similaires à ceux auxquels vous vous êtes intéressé·e auparavant. Quel est l'impact de cette situation ?

Être dans une bulle de filtre a l'effet d'exposer chaque individu à des informations, des titres, des articles et des publicités différentes, comme l'article interactif Blue Feed, Red Feed (graphics.wsj.com/blue-feed-red-feed) le montre.

Si vous savez que vous consultez du contenu sélectionné par algorithme dans les bulles de filtres de vos applications et sites internet, vous vous demandez sans doute comment sortir de ces bulles ?

Changez vos habitudes et variez vos sources
Un bon moyen de sortir de sa bulle de filtres est de s'inscrire à des services qui regroupent des actualités et des informations provenant de différentes sources et offrant plusieurs points de vue différents. Les flux RSS, les forums et les listes de diffusion regroupant divers sujets et opinions pourront vous aider dans ce sens.

DATA DETOX KIT

6 CONSEILS POUR ÉVITER LES INFORMATIONS ERRONÉES EN LIGNE

Les applications, les sites internet et les médias en ligne peuvent être très indispensable pour s'informer, trouver des astuces et se détendre. Mais il est parfois difficile de ne pas se laisser distraire par tant de contenu et de trouver ce que l'on cherche vraiment.

Il peut aussi être compliqué de distinguer la réalité de la fiction face à une vidéo, une image ou un article en ligne. Des tests de personnalité, qui cherchent à faire un profil de vous, aux titres sensationnalistes et aux photos retouchées ou aux vidéos qui peuvent vous présenter une tout autre réalité, ce que l'on voit en ligne n'est pas toujours vrai.

Dans ce Data Detox, vous découvrirez des sujets et des tendances liées aux informations erronées, en commençant par un examen approfondi de votre responsabilité, puis d'explorer la situation dans son ensemble, ainsi que des conseils pour bien vous y retrouver.

C'est parti !

datadetoxkit.org **#datadetox**

Produit par
TACTICAL TECH

Les partenaires du projet
Save the Children 100 ANNI
IFLA

Financé par l'Union européenne

1.

PRENEZ CONSCIENCE DE L'IMPACT QUE VOUS AVEZ

Posez-vous la question suivante : **« Quelle influence ai-je en ligne ? »** Quand avez-vous vu pour la dernière fois un article, un titre, une vidéo ou une image, qui amuse ou qui choque, que vous avez immédiatement partagé avec vos amis ? Des chercheurs ont mis en évidence que les histoires et les images qui avaient le plus de chances d'être virales sont celles qui génèrent des émotions fortes : la peur, le dégoût, la stupeur, la colère ou l'angoisse. Si vous avez partagé quelque chose de ce genre encore ce matin, ne vous sentez pas coupable !

Le partage crée des liens
Le partage est une forme de participation. Lorsque vous partagez quelque chose (quoi que ce soit), vous participez à sa diffusion qui peut devenir virale. Si ce que vous avez partagé se révèle faux, par exemple, voulez-vous vraiment que l'on vous y associe ? Avant de partager un lien, réfléchissez à son contenu : allez-vous diffuser de fausses informations, du contenu néfaste ou toxique ?

2.

RÉFLÉCHISSEZ BIEN AVANT DE REMPLIR UN TEST DE PERSONNALITÉ

Quand avez-vous vu pour la dernière fois un questionnaire (en texte ou en images) de ce genre :

- Quelle décennie vous représente le plus ?
- Quelles seraient vos vacances idéales ?
- La liste n'en finit pas !

Ce questionnaire amusant était peut-être conçu pour vous divertir, mais il est tout à fait possible que ses questions aient été pensées pour recueillir des données afin de vous catégoriser selon de soi-disant modèles psychométriques. Vos réponses à une question sur votre personnage préféré des Simpson, tout comme vos habitudes d'utilisation susceptibles d'être surveillées par votre navigateur internet, vos applications ou tout autre objet connecté (par exemple, une carte de fidélité), permettent aux analystes de données de se faire une idée de votre personnalité, de ce qui compte pour vous, et de la manière de vous influencer pour acheter une paire de chaussures (par exemple)... Ou encore de constituer votre profil pour trouver des moyens d'influencer votre vote lors des prochaines élections.

Gardez plus de secrets
Lorsque vous pensez à vos renseignements personnels, les premières choses qui vous viennent à l'esprit sont sans doute vos mots de passe, vos numéros d'identification et de compte. Mais d'autres informations sont tout aussi personnelles, par exemple ce qui vous fait peur, ce qui vous agace, ou encore vos ambitions. Ces informations peuvent avoir beaucoup de valeur pour les analystes de données, leur révélant ce qui vous touche profondément. Réfléchissez bien avant de donner ce genre d'informations dans un sondage ou un questionnaire.

3.

NE MORDEZ PAS À L'HAMEÇON

Le **piège à clic (click bait)** est un terme utilisé pour décrire les titres surfaits (sensationnalistes), malhonnêtes, ou mensongers, utilisés pour vous inciter à cliquer sur le lien en question. Plus un article, une vidéo, ou une image génère d'attention, plus son auteur pourra gagner d'argent. Cela signifie que les créateurs peuvent être incités à utiliser n'importe quel moyen pour vous faire lire, voir ou partager leur contenu.

En fonction du profil que les plateformes que vous utilisez (par exemple Facebook et Instagram) ont constitué de vous, vous pourrez tomber sur des titres créés sur mesure **pour vous émouvoir** afin de vous pousser à cliquer.

Les pièges à clic vont parfois de pair avec les informations erronées, mais pas toujours. Lorsque vous commencerez à reconnaître des titres pièges à clic, vous verrez qu'il en existe partout sur YouTube, sur les blogs et dans les tabloïdes.

Remontez jusqu'à la source
Lorsque vous tombez sur un lien piège à clic, ne vous arrêtez pas au titre. Si le lien semble sûr, suivez-le et trouvez le nom de l'auteur, la date de publication et les sources auxquelles il fait référence. Il se peut que l'article indique quelque part que son contenu est payant, ou qu'il s'agisse de contenu publi-rédactionnel, ou encore qu'il soit classé comme contenu éditorial. Ces informations vous permettront de décider de l'importance que vous accorderez au contenu.

4.

ATTENTION AUX TRUCAGES (FAKES)

Les **hypertrucages (deep fakes)** sont des séquences vidéo, audio, ou des images qui ont été modifiées, généralement pour remplacer le visage, les mouvements ou les paroles d'une personne. Bien que le terme soit récent, ce type de trucages existe depuis bien longtemps. Il est encore plus facile de créer des trucages très simples (cheap fakes) : du contenu trompeur peu élaboré et peu coûteux, dont la création se résume à l'utilisation d'un titre incorrect pour une photo ou une vidéo, ou de vieux contenus pour illustrer un événement actuel.

Vous pensez peut-être qu'il est impossible de combattre le contenu falsifié, mais vous pouvez commencer par un geste crucial : garder les pieds sur terre.

Gardez les pieds sur terre et explorez
De même qu'avec un piège à clic, ne prenez rien pour argent comptant. Si une vidéo ou une photo vous semble surprenante ou scandaleuse, ne vous laissez pas décontenancer et rappelez-vous que les apparences sont trompeuses. Si vous constatez qu'une image apparaît souvent dans votre fil d'actualités ou si vous l'avez reçue plusieurs fois, saisissez cette occasion pour en trouver l'origine véritable.

Vous vous poserez alors plus de questions : qui l'a publiée (quel site, quel auteur) ? Quand a-t-elle été publiée ? Si c'est une image, faites une recherche inversée sur TinEye pour voir où elle apparaît.

Recoupez vos informations avec d'autres sources fiables avant de les considérer comme authentiques et de les partager avec vos proches.