Troubles du spectre autistique : guide de sécurité en ligne

[Source : wizcase.com]

Par John Bennet

Des personnes de tous horizons et de toutes origines peuvent être victimes du harcèlement en ligne et de la cybercriminalité. Toutefois, des études ont révélé que les personnes atteintes de troubles du spectre autistique (TSA) sont plus exposées que les autres aux menaces en ligne.

> *Les* TSA *sont un trouble du développement qui affecte le comportement et la communication. Les personnes atteintes de troubles du spectre autistique mènent une vie relativement normale, mais peuvent avoir besoin de supervision et manquer de discernement – un trait identifié comme dangereux lorsqu'elles sont livrées à elles-mêmes dans le cyberespace*.

Les enfants et adultes atteints de TSA ne sont pas seulement vulnérables vis-à-vis des autres. En effet, ils sont également susceptibles de développer des habitudes compulsives en ligne et dépendances à Internet, et d'être davantage affectés par l'exposition à un contenu inapproprié.

Tout le monde devrait se sentir en sécurité en ligne. Il est donc extrêmement important de vous assurer que votre sécurité en ligne est adéquate, et de faire constamment preuve de vigilance sur Internet.

Pour vous aider à naviguer facilement et à limiter votre vulnérabilité aux attaques, jetez un œil à notre Guide de sécurité Internet pour les personnes atteintes de TSA. (Partager sur Facebook)

Sommaire :

Problèmes en ligne courants

De nombreuses menaces pèsent constamment sur le cyberespace. Familiarisez-vous avec, et faites preuve d’une vigilance extrême. Nous vous conseillons vivement de disposer d’un plan d’action. Vous trouverez ci-dessous les problèmes en ligne les plus courants auxquels se heurtent les personnes atteintes de TSA, ainsi que des conseils pour vous aider à maîtriser la situation.

1 Le harcèlement en ligne

Le harcèlement en ligne, ou cyber-intimidation, est une tendance de plus en plus courante sur Internet, et qui touche particulièrement les enfants et personnes atteintes de TSA. Les harceleurs utilisent des plates-formes numériques, telles que des réseaux sociaux ou forums de chat sur Internet, pour harceler et intimider leurs victimes. Parfois, ce harcèlement peut dégénérer en menaces et harcèlement dans le monde réel. N’importe qui peut être la cible du harcèlement en ligne, quel que soit son âge, son origine ou son mode de vie.

Selon le Journal de la recherche en santé mentale sur les déficiences intellectuelles (Journal of Mental Health Research in Intellectual Disabilities), les personnes présentant une déficience intellectuelle ou développementale sont plus exposées aux risques de harcèlement en ligne. L’alliance anti-harcèlement a également révélé que les personnes handicapées étaient plus susceptibles d’être victimes de harcèlement en ligne.

Des efforts supplémentaires sont déployés afin de comprendre le phénomène et contribuer à créer un environnement en ligne plus sûr. Toutefois, le harcèlement en ligne n’est pas toujours facile à reconnaître.

Il est parfois difficile de transmettre le même niveau de signification et de contexte à l’écrit qu’à l’oral. Pour cette raison, il n’est pas toujours évident de savoir si une personne essaye de harceler de manière intentionnelle, ou s’il s’agit d’un malentendu. Cependant, si quelqu’un vous envoie des messages abusifs, ou tente de vous intimider ou de vous faire honte en ligne, il est fort probable qu’il s’agisse de harcèlement en ligne.

Les effets du harcèlement en ligne à long terme

Le harcèlement peut affecter votre estime de soi et/ou votre santé mentale. Le harcèlement continu est susceptible de vous pousser à vous isoler, limitant vos interactions avec vos amis et proches. Si rien n’est fait, le harcèlement en ligne peut avoir un impact profond et durable.

Même si cela semble effrayant, cela ne devrait pas vous empêcher d’explorer en ligne et de vous faire des amis via Internet.

Les différents types de harcèlement en ligne

Le harcèlement en ligne présente de nombreuses facettes. Sa forme la plus fréquente est l’envoi de messages abusifs par e-mail, SMS et chat. Toutefois, les harceleurs en lignes peuvent vous atteindre de nombreuses autres manières.

Le harcèlement en ligne peut également se manifester sous les formes suivantes :

- Une personne qui propage des rumeurs sur vous en ligne, auprès de vos amis ou même d’inconnus
- Quelqu’un qui publie des statuts et commentaires dans l’intention de vous humilier ou d’altérer la façon dont les autres vous perçoivent.
- Des menaces à votre intention adressée via les réseaux sociaux et d’autres moyens de communication en ligne
- Quelqu’un qui utilise son profil en ligne pour partager des informations, vidéos ou photos de vous sans votre consentement ou après leur avoir demandé d’arrêter.
- Une personne qui utilise vos profils et informations en ligne pour vous harceler en ligne et/ou dans la vie réelle.

- Quelqu’un qui pirate vos comptes en ligne ou se fait passer pour vous avec l’intention d’utiliser votre nom et votre réputation pour propager du contenu inapproprié ou préjudiciable. Cette pratique est connue sous le nom de « fraping ».

Comment prévenir le harcèlement en ligne ?

Des recherches récentes indiquent que le harcèlement en ligne a tendance à se produire lorsque certains facteurs de risque ne sont pas évités. Bien qu’il soit difficile de mettre fin au harcèlement en ligne, vous pouvez prendre des mesures pour éviter de devenir une victime.

La première étape consiste à modifier les paramètres de vos comptes de réseaux sociaux afin que vos profils soient uniquement accessibles aux personnes que vous connaissez et en qui vous avez confiance. Les harceleurs en ligne sont opportunistes par nature, et vous êtes donc davantage exposé au harcèlement en ligne si des inconnus peuvent facilement vous contacter.

De même, vous devriez toujours éviter d’ouvrir des messages ou d’accepter les demandes d’amis de personnes que vous ne connaissez pas. La possibilité de se cacher derrière un écran d’ordinateur pour attaquer quelqu’un protège souvent les harceleurs en ligne des conséquences concrètes de leurs actes. Ils s’en prennent donc à une personne qui n’appartient pas à leur cercle social, ou qu’ils ne connaissent pas.

- Sécurisez vos comptes de réseaux sociaux. Définissez vos niveaux de sécurité sur « amis uniquement » afin que les inconnus ne puissent pas voir votre profil ni vous envoyer de messages.
- Ne publiez pas d'informations personnelles en ligne. Ne publiez jamais d'informations telles que votre localisation, votre adresse, votre numéro de téléphone, votre école ou votre lieu de travail. Cela contribuera à

prévenir le harcèlement en ligne, et empêchera les harceleurs de vous contacter face à face ou par téléphone.
- Si quelqu’un vous envoie des messages abusifs, ne mordez pas à l’hameçon. L’objectif principal de la plupart des harceleurs est d’obtenir une réaction de leur cible. Si vous répondez, cela risque de les inciter à continuer. Par conséquent, mieux vaut s’abstenir de leur donner ce qu’ils veulent. En l’absence de réponse, la plupart des harceleurs abandonneront et vous laisseront tranquille.
- Signalez-les. Si quelqu’un vous harcèle ou s’en prend à une personne de votre entourage, signalez-le à l’équipe d’assistance de la plateforme. Un membre du personnel examinera le contenu et décidera de le supprimer ou de le laisser. Dans des cas plus graves, la plateforme peut même prendre des mesures contre le harceleur en le bloquant ou en lui interdisant l’accès.
- Bloquez le harceleur. Bloquer quelqu’un l’empêchera d’accéder à votre profil et de vous contacter dans le futur.
- Parlez-en. Informez un ami de confiance ou un proche de la situation. Il pourra peut-être vous aider ou vous prodiguer des conseils utiles.

2 Comprendre le contexte des messages en ligne

Les malentendus en ligne

Il est possible de mal interpréter une situation lorsque vous communiquez avec quelqu’un par Internet. Vous pouvez facilement passer à côté du contexte ou du sens du commentaire d’une personne en l’absence d’indices sociaux, ce qui peut faire dévier la discussion en ligne, voire même provoquer un conflit.

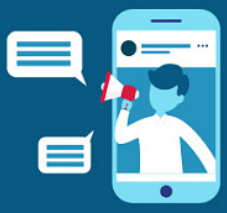
Voici les meilleures pratiques pour éviter les malentendus en ligne :

- N’oubliez pas que tout ce que vous lisez en ligne n’est pas vrai, et que toutes les personnes auxquelles vous parlez ne sont pas honnêtes.
- Si quelque chose n’est pas clair, demandez à la personne de clarifier ce qu’elle veut dire avant de partager votre opinion.
- Utilisez des sources fiables pour vérifier les faits et informations afin d’éviter de partager des informations inexactes.
- Souvenez-vous de faire preuve de politesse et de calme, même lorsque vous êtes certain que quelqu’un a tort ou vous manque de respect.
- Contactez les administrateurs et modérateurs des groupes et forums pour assurer la médiation des discussions en ligne en cas de malaise ou de conflit.

Certains forums en ligne comme Talk About Autism, sont spécialement conçus pour permettre aux personnes atteintes de TSA de discuter et se faire des amis. La plupart de ces forums ont des modérateurs qui suivent les discussions et sont formés pour offrir une médiation en cas de malentendu.

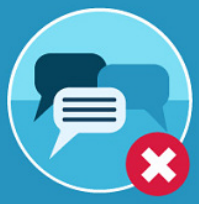
12 astuces pour mieux communiquer sur les réseaux sociaux et en ligne

L’utilisation des réseaux sociaux présente de nombreux avantages, en particulier pour les personnes atteintes de troubles du spectre autistique, qui peuvent avoir des difficultés à interagir avec les autres. Toutefois, le fait de publier toutes vos informations sur les réseaux sociaux s’accompagne souvent d’inconvénients. Voici 12 astuces pour vous aider à mieux communiquer en ligne et minimiser le risque de malentendu.



12 Ways to Improve Social Media and Online Communication

1. Never add your boss, teacher, or supervisor on social media.



2. Never comment about your workplace online.

3. Refrain from posting content that might negatively change people's opinion of you.

4. Always meet new online friends during the day and in a public place.

5. Don't hack into other people's accounts or websites.

6. Don't believe everything that you read online.

7. Don't compare your life with someone else's on social media.

8. Always be polite in your online discourse and avoid arguments.

9. Don't type in all CAPS.

10. Use Emoji's and GIFs to help express yourself.

11. Block people that make you uncomfortable.

12. Never send explicit photographs of yourself.

1. N’ajoutez jamais votre patron, enseignant ou superviseur sur les réseaux sociaux. Si vous êtes amis en ligne, ils pourront voir le contenu de votre profil, ce qui pourrait donner lieu à des interprétations erronées de votre personnalité. Si leur opinion sur vous est affectée par ce qu’ils voient, cela pourrait vous empêcher d’obtenir une promotion.
2. Ne publiez jamais de commentaires en ligne concernant votre entreprise, en particulier si vous vous plaignez. Cela peut vous sembler innocent, mais pourrait vous coûter votre emploi si votre patron ou vos collègues en avaient vent. En outre, la plupart des entreprises interdisent désormais les publications concernant le travail sur les réseaux sociaux.
3. Évitez de publier du contenu qui pourrait fausser l’avis des autres sur vous, par exemple des coups de colère. Les employeurs potentiels consultent généralement vos profils en ligne et peuvent fonder leur opinion sur ce qu’ils voient, même si cela ne représente pas vraiment votre personnalité.
4. Donnez toujours rendez-vous à vos nouveaux amis en ligne pendant la journée et dans un lieu public. Informez toujours quelqu’un du lieu de rendez-vous, de la personne que vous rencontrez et de tout changement de lieu. Pour une rencontre encore plus sûre, vous pouvez demander à un ami de confiance ou un proche de vous accompagner. Évitez les endroits isolés, et n’allez jamais chez la personne. Si quelque chose vous semble louche, n’hésitez pas à partir.
5. Protégez vos mots de passe et évitez de pirater les comptes ou sites Web d’autres personnes, même si vous en avez la possibilité. Les personnes atteintes de TSA se retrouvent souvent victimes d’une personne manipulatrice qui leur demande d’enfreindre la loi ou de pirater un ordinateur, ce qui est illégal.
6. Ne croyez pas tout ce que vous lisez en ligne, en particulier sur les réseaux sociaux. De nombreux utilisateurs propagent de fausses nouvelles et informations sur Internet, et ont tendance à exagérer pour que leur vie semble parfaite.
7. Ne comparez pas votre vie à celle des autres sur les réseaux sociaux. Souvenez-vous que vous voyez uniquement les moments forts de leur vie, et non leurs activités quotidiennes.
8. Faites toujours preuve de politesse dans votre discours en ligne et évitez les conflits, même lorsque vous estimez que l’autre personne a tort.
9. N’oubliez pas que la plupart des internautes considèrent que les majuscules sont l’équivalent numérique de crier. Dans cette optique, l’utilisation de majuscules peut être perçue comme impolie.
10. Vous pouvez utiliser des émoticônes, ou emojis, pour mieux exprimer le contexte et le sens de vos mots. Par 5La surcharge sensorielle sur Internetexemple, l’ajout d’un smiley souriant à la fin d’une phrase montrera que vous êtes de bonne humeur ou sympathique.
11. Si quelqu’un vous met mal à l’aise ou en danger, mettez fin à la situation et bloquez-le.
12. N’envoyez jamais de photos explicites de vous-même, et ne transmettez jamais des photos de quelqu’un d’autre. Si vous partagez des photos sans consentement ou d’un mineur, vous enfreignez la loi et vous vous exposez à des poursuites judiciaires.

3 Devenir la victime d’une arnaque, d’une manipulation ou d’un piratage

Les arnaqueurs et hackers font malheureusement partie du quotidien en ligne. En termes simples, certaines personnes ont de mauvaises intentions et souhaitent manipuler les autres à leur avantage.

Ils feront semblant de vouloir devenir votre ami, voire même un compagnon sentimental potentiel. Ils mettront tout en œuvre pour établir une relation afin de gagner votre confiance, puis de vous arnaquer !

Les arnaqueurs, hackers et cybercriminels peuvent avoir différents motifs. Par exemple, ils peuvent essayer de vous convaincre de leur envoyer de l’argent ou de commettre un crime à leur place.

Ils peuvent également essayer d’obtenir vos informations personnelles, par exemple les informations de votre passeport, afin d’usurper votre identité ou de se faire passer pour vous en ligne.

Les meilleures pratiques pour éviter les arnaques et la manipulation

- Ne communiquez à personne vos informations personnelles telles que votre adresse, votre numéro de téléphone ou votre numéro de carte d’identité.
- Ne divulguez jamais vos informations bancaires ou de carte de crédit en ligne. N’oubliez pas que des arnaqueurs peuvent vous contacter en se faisant passer pour votre banque. Votre banque ne vous contactera jamais pour vous demander des informations personnelles et confidentielles.
- Ne communiquez à personne votre lieu de travail ou d’études, ou celui de vos amis et proches.
- Pensez à utiliser un pseudonyme au lieu de votre vrai nom. De nombreuses personnes utilisent leur premier et deuxième prénom ou s’inventent un nouveau nom.
- Faites preuve de prudence lorsque vous acceptez de rencontrer des personnes que vous avez connues en ligne.
- N’envoyez jamais d’argent à quelqu’un que vous avez rencontré en ligne. Si quelqu’un vous demande de lui envoyer de l’argent, il essaye probablement de vous arnaquer.
- Ne cliquez jamais sur des liens vers des sites Web que vous ne reconnaissez pas, car ils risquent de vous amener sur un site susceptible de compromettre la sécurité de votre ordinateur.

Si vous pensez avoir été victime d’une arnaque, contactez immédiatement votre banque et l’organisme local chargé de l’application de la loi.

Play it Safe (ne prenez pas de risques)

Le Centre sur l’enseignement secondaire pour les élèves atteints de troubles du spectre autistique (Center on Secondary Education for Students with Autism Spectrum Disorder) a créé un acronyme facile à retenir pour rester en

sécurité en ligne : Play it Safe, qui signifie « Ne prenez pas de risques » en anglais.

PLAY IT SAFE

P **Personal information** - never share your personal information online.

L **Let a friend or family** member know if someone has asked you for this information, or if you don‘t feel safe.

A **Attachments** - remember that email attachments might contain malware that can damage your computer and harvest your private information. Don‘t open them unless it’s a file that you have been expecting from someone that you trust.

Y **Your feelings are important**. If something makes you feel uncomfortable or unsafe, stop and let somebody know.

I **Information** - remember that not everything you read online is true.

T **Take breaks** from your computer often to socialize, stretch, and give your eyes a rest.

S **Spend your money safely**. Don‘t buy things from unfamiliar stores or links, and don‘t send people money.

A **Act politely** and don‘t say things online that you wouldn‘t say in real life.

F **Friends online should stay online** - if someone asks to meet up, tell them no.

E **Enjoy** yourself and have fun!

Personal information (Informations personnelles) : Ne partagez jamais vos informations personnelles en ligne.

Let a friend or family member know if someone has asked you for this information, or if you don‘t feel safe (Informez un ami ou proche si une personne vous a demandé ces informations ou si vous ne vous sentez pas en sécurité).

Attachments (Pièces jointes) : Souvenez-vous que les pièces jointes peuvent contenir des malware susceptibles d’endommager votre ordinateur et de recueillir des informations confidentielles. Ne les ouvrez pas, sauf s’il s’agit d’un fichier que vous attendiez de quelqu’un en qui vous avez confiance.

Your feelings are important (Vos sentiments sont importants) : Si quelque chose vous met mal à l’aise ou en danger, mettez fin à votre activité et informez quelqu’un.

Information : N’oubliez pas que tout ce que vous lisez en ligne n’est pas vrai.

Take breaks from your computer often to socialize, stretch, and give your eyes a rest (Faites régulièrement des pauses pour interagir avec d’autres personnes, vous étirer et reposer vos yeux).

Spend your money safely. (Dépensez votre argent prudemment) : N’achetez rien dans des boutiques ou en suivant des liens inconnus, et n’envoyez jamais d’argent.

Act politely and don‘t say things online that you wouldn‘t say in real life. (Faites preuve de politesse et ne dites pas en ligne des choses que vous ne diriez pas dans la vie réelle.)

Friends online should stay online (Les amis en ligne doivent le rester) : Si quelqu’un souhaite vous rencontrer, refusez.

Enjoy yourself and have fun! (Amusez-vous !)

4 L’exposition à du contenu inapproprié

Certes, le Web offre une incroyable richesse de contenu passionnant et instructif. Malheureusement, il s’accompagne de la même profusion de contenu inapproprié et préjudiciable. Vous risquez en effet de tomber sur des images violentes ou pornographiques, ainsi que du contenu illégal que la plupart des gens préfèrent éviter. L’accès à des choses telles que la pornographie infantile, même par mégarde, peut avoir des conséquences juridiques désastreuses. Vous devez donc vous protéger.

Outils de blocage du contenu inapproprié

1. SafeSearch :

La fonctionnalité SafeSearch de Google bloque le contenu explicite dans vos résultats de recherche Google. Bien qu'elle ne soit pas toujours précise à 100%, elle vous permet de filtrer des éléments tels que la pornographie et les images explicites lorsque vous naviguez sur Google, que ce soit sur votre tablette, votre téléphone ou votre ordinateur.

Configuration de SafeSearch :

Cliquez sur le bouton « paramètres » de votre page d'accueil Google, puis accédez aux paramètres de recherche. Sous Filtres SafeSearch, cochez la case à côté de l'option « Activer SafeSearch » et assurez-vous de cliquer sur Enregistrer avant de quitter.

Vous pouvez consulter le guide Google SafeSearch pour savoir comment l'activer sur votre dispositif Android ou iOS.

2. Filtres Internet :

Les filtres Web comme Net Nanny surveillent les sites que vous consultez pour en bloquer le contenu inapproprié. Vous pouvez personnaliser les éléments à filtrer, et même établir une liste blanche de sites Web que vous considérez comme sûrs. Il s'agit d'un excellent outil pour les adultes qui souhaitent filtrer le contenu peu sûr au travail, ainsi que pour les parents qui souhaitent protéger leurs enfants en ligne.

3. Bloqueurs de publicité et de fenêtres émergentes :

Nous avons tous entendu des histoires d'amis surpris en flagrant délit pile au moment où une fenêtre émergente explicite et inattendue s'affichait à l'écran. Vous pouvez éviter ces incidents potentiellement désastreux en installant un bloqueur de fenêtres émergentes et de publicité sur votre navigateur.

4. Protection anti-virus et anti-malware :

Certains virus et malware provoquent l'ouverture de fenêtres émergentes à des moments inopportuns. Un bon antivirus à jour protégera non seulement votre ordinateur des infections préjudiciables, mais vous protégera également du contenu inapproprié.

5. Liens :

Évitez de cliquer sur des liens que vous ne reconnaissez pas. Même si le message vous est envoyé par un ami, ne cliquez pas sur un lien que vous ne reconnaissez pas ou que vous n'attendez pas. Vous recevrez souvent des messages spam par SMS et par e-mail vous invitant à cliquer sur un lien pour accéder à un site Web ou même à un cadeau. Toutefois, tout ce que vous

risquez de gagner est un virus ou une arnaque.

5 La surcharge sensorielle sur Internet

Les personnes qui présentent une sensibilité sensorielle peuvent souffrir d'une surcharge provoquée par les dispositifs électroniques et Internet. Les bruits forts, les rétroéclairages lumineux, la musique inattendue et la lecture automatique de vidéos ne sont que quelques-uns des éléments irritants susceptibles de conduire à une surcharge.

Heureusement, vous pouvez prendre certaines mesures pour minimiser cet impact sensoriel.

- Réglez les niveaux de luminosité de votre écran et investissez dans une application qui bloque la lumière bleue sur votre dispositif. Votre écran prendra une teinte légèrement orangée, mais il est indispensable de bloquer la lumière bleue pour atténuer les effets du rétroéclairage sur nos sens. Des applications pour bloquer la lumière bleue sont disponibles sur la plupart des dispositifs, et vous aideront même à vous endormir plus rapidement et à réduire l'impact des migraines provoquées par la sensibilité à la lumière.
- Désactivez la lecture automatique des fichiers audio et vidéo sur vos plates-formes de réseaux sociaux.
- Investissez dans un clavier et une souris « silencieux » pour réduire le bruit lors de la frappe.
- Le bruit blanc est un excellent outil pour apaiser les sens. Cela peut également atténuer des sons irritants, comme le bourdonnement de votre ordinateur ou vos voisins bruyants ! Des vidéos de bruit blanc sont disponibles gratuitement sur YouTube, ou vous pouvez également acheter une machine à bruit blanc.

6 La dépendance à Internet

L'attrait et la facilité des rencontres en ligne peuvent avoir un impact négatif sur votre volonté d'interagir avec les autres dans le monde réel. La dépendance en ligne est un problème grave qui touche de nombreuses personnes. Des études indiquent que les personnes sujettes à des comportements obsessionnels présentent un risque plus élevé de développer une dépendance à Internet. Les personnes atteintes de TSA et de troubles anxieux présentent un risque particulièrement élevé.

L'explication est simple : Internet offre un refuge, et un moyen facile de rencontrer et communiquer avec les autres. Si la plupart de vos amis sont sur Internet, c'est là que vous voudrez passer le plus clair de votre temps.

Il est essentiel pour votre santé physique et mentale de développer et maintenir des relations dans le monde réel. Internet est un outil formidable, mais s'il vous empêche de passer du temps avec vos amis et proche, il est peut-être temps de faire une pause.

Conseils de prévention de la dépendance à Internet :

- Établissez une limite de temps lorsque vous êtes sur votre ordinateur. Vous pouvez par exemple créer une alarme au bout d'une heure ou deux, et vous déconnecter lorsque le temps est écoulé.
- Créez une liste de projets et réservez du temps chaque jour pour vos amis et proches, ou pour des passe-temps et de l'exercice physique. Incluez le temps que vous prévoyez de passer en ligne dans votre liste, mais planifiez d'autres activités pour votre temps libre.
- Assurez-vous d'avoir terminé toutes les autres tâches que vous devez effectuer, par exemple les tâches ménagères, avant de vous connecter chaque jour.
- Utilisez des applications spécialement conçues pour vous rappeler de faire une pause. Des programmes tels que Offtime contrôlent votre navigation et vous montrent le temps passé sur les réseaux sociaux. Vous pouvez même les configurer pour bloquer certains sites, tels que Facebook, à certaines heures de la journée.
- Désactivez les notifications push de vos réseaux sociaux sur votre téléphone ou tablette. Ainsi, vous les recevrez uniquement lorsque vous vous connectez, et non lorsque vous êtes en train de faire autre chose.

Si vous pensez être victime d'une dépendance à Internet, vous pouvez demander à votre médecin de vous orienter vers un thérapeute expérimenté, qui sera à même de vous prodiguer d'autres conseils.

7 Comment vous protéger sur les réseaux sociaux populaires ?

Vous trouverez ci-dessous un bref guide qui vous aidera à rester en sécurité sur les réseaux sociaux les plus populaires. Nous vous expliquons leurs risques, et comment modifier les paramètres de votre compte pour éviter le contenu explicite, les arnaqueurs, les faux profils et les harceleurs en ligne.

Facebook

Quels sont les principaux risques sur Facebook ?

- Sur Facebook, les arnaqueurs peuvent facilement se lier d'amitié avec vous et vous leurrer en utilisant de faux profils.

- Il existe un risque moyen à élevé d’être exposé à des liens pointant vers des sites Web de hameçonnage de vos informations personnelles.
- Les harceleurs en ligne utilisent souvent Facebook pour harceler leurs victimes.
- Même si cela est contraire aux politiques de Facebook, vous pouvez être exposé à des publications explicites non détectées par leurs filtres de contenu.
- Des fonctionnalités telles que la lecture automatique vidéo peuvent déclencher une surcharge sensorielle.
- En général, les réseaux sociaux peuvent créer une dépendance.

Astuces pour vous protéger sur Facebook

Évitez d’utiliser vos informations personnelles :

Bien que Facebook vous demande votre prénom et votre nom, évitez de les utiliser dans la mesure du possible. De nombreux internautes utilisent un pseudonyme ou créent un faux nom de famille. Ainsi, il sera plus difficile de vous retrouver sur d’autres plateformes ou dans la vie réelle.

Évitez de trop personnaliser votre section « À propos ». N’indiquez jamais votre lieu de résidence, de travail ou d’études à Facebook.

Si vous utilisez un dispositif avec GPS, n’autorisez pas Facebook à publier votre localisation. Pour ce faire, le moyen le plus simple consiste à empêcher Facebook d’accéder aux informations de localisation de votre dispositif. Ce paramètre est généralement disponible sur votre dispositif sous Paramètres > Confidentialité > Services de localisation.

Rendez votre compte privé :

Assurez-vous que votre profil est configuré comme « privé », afin que seuls vos amis puissent voir votre statut et vous envoyer des messages. Cela réduit les risques de harcèlement en ligne en vous permettant de choisir qui peut vous contacter. N’oubliez pas que les personnes que vous ne connaissez pas pourront tout de même lire les commentaires que vous faites sur les publications de vos amis et pages publiques.

Comment limiter l’accès à vos publications à vos amis :

Une fois la boîte de dialogue de statut ouverte, cliquez sur le menu déroulant des paramètres de confidentialité dans la barre inférieure. Vous aurez le choix entre « amis » ou « public ». Si l’option par défaut est « amis », cela signifie que seuls les amis que vous avez acceptés verront cette publication. Si l’option est définie sur « public », cliquez dessus et sélectionnez « amis » avant de cliquer sur le bouton Publier.

Comment rendre votre profil privé :

Connectez-vous à Facebook et cliquez sur la flèche en haut de votre page dans la barre d'accueil. Sélectionnez « Paramètres ».

Une fois la page des paramètres chargée, sélectionnez « Confidentialité » dans la barre latérale. Cela chargera deux catégories de paramètres de confidentialité que vous pourrez modifier.

Deux options de confidentialité sont proposées sous « votre activité ». Pour une confidentialité optimale, configurez-les comme suit :

Qui peut voir vos futures publications ?

Ce paramètre doit être défini sur « amis » pour que les inconnus ne puissent pas voir vos mises à jour de statut privées.

Limiter l'audience des publications que vous avez ouvertes aux amis de vos amis ou au public ?

Si vous choisissez « amis », cela augmentera la confidentialité de toutes vos publications précédentes, de sorte que les inconnus ne pourront plus les voir.

Ensuite, vous pouvez choisir la manière dont les gens peuvent vous trouver et vous contacter.

Qui peut vous envoyer des invitations à devenir amis ?

Si vous ne souhaitez pas recevoir de demandes d'amis de la part d'inconnus, définissez cette option sur « amis de vos amis ». Malheureusement, il n'y a aucun moyen d'éviter complètement les invitations, mais cela en réduira considérablement l'occurrence.

Qui peut voir votre liste d'amis ?

Pour une sécurité optimale, définissez ce paramètre sur « amis » ou « moi uniquement ».

Qui peut vous trouver en utilisant l'adresse email/le numéro de téléphone que vous avez fourni(e) ?

Si vous craignez que des inconnus ou harceleurs vous trouvent via votre adresse e-mail ou numéro de téléphone, définissez ce paramètres sur « amis ». Vos amis peuvent déjà vous contacter par l'intermédiaire de votre compte, et n'ont donc aucune raison de vous chercher d'une autre manière.

Souhaitez-vous que les moteurs de recherche externes à Facebook indexent votre profil ?

Si vous sélectionnez « oui » pour cette option, les gens pourront trouver

votre page Facebook en cherchant votre nom sur Google ou tout autre moteur de recherche. Pour une sécurité optimale, sélectionnez « non ».

À présent, accédez à vos paramètres « journal et identification » (« timeline and tagging ») pour finaliser le processus.

Qui peut publier dans votre journal ?

Pour empêcher les inconnus (et harceleurs) de publier dans votre journal, vous pouvez définir cette option sur « moi uniquement ». Toutefois, cela empêchera également vos amis de publier dans votre journal.

Qui peut voir ce que d'autres personnes publient dans mon journal ?

Ici encore, définissez ce paramètre sur « amis » ou « moi uniquement » afin que les inconnus ne puissent pas voir les publications d'autres personnes dans votre journal.

Évitez les harceleurs :

Si quelqu'un utilise Facebook pour vous harceler, vous pouvez l'empêcher de voir votre profil ou de vous contacter. Il vous suffit d'accéder à son profil et de sélectionner le menu déroulant représenté par trois petits points en haut de sa page. Ensuite, sélectionnez « bloquer ». Il ne pourra ni trouver, ni consulter votre profil, et il ne saura pas que vous l'avez bloqué.

Évitez le contenu inapproprié :

Dans la plupart des cas, le logiciel de censure de Facebook filtre le contenu inapproprié et préjudiciable de votre feed. Toutefois, vous pouvez également configurer Facebook pour filtrer les commentaires contenant des mots spécifiques et les éliminer de votre journal.

Revenez à vos paramètres « journal et identification », puis dans la catégorie « journal », sélectionnez l'option « Masquer les commentaires contenant certains mots ». Vous pourrez alors créer une liste de mots, de termes et même d'émoticônes que vous souhaitez éviter dans votre journal. Facebook se chargera de les bloquer à votre place.

Faites une pause :

Vous pouvez vous déconnecter de Facebook à tout moment, mais vous pouvez également désactiver temporairement votre compte pour une absence prolongée. L'intégralité de vos amis, publications et photos resteront dans votre profil pendant votre absence, mais personne d'autre ne pourra accéder à votre compte ou vous envoyer de messages jusqu'à votre prochaine connexion. C'est une excellente solution si vous souhaitez vous distancier des réseaux sociaux sans pour autant perdre votre contenu et vos souvenirs.

Pour désactiver votre compte, rendez-vous dans Paramètres > Général > Gérer le compte > Désactiver votre compte.

Twitter

Quels sont les principaux risques sur Twitter ?

- Twitter est un centre névralgique de l’activisme social et politique, ce qui peut parfois être éprouvant.
- De par la nature extrêmement diversifiée du contenu de Twitter, vous risquez de tomber sur des tweets explicites ou provocateurs de temps en temps.
- Les discussions sur Twitter aboutissement souvent sur des disputes passionnées, et les utilisateurs risquent d’être victimes de harcèlement en ligne.
- Comme tous les réseaux sociaux, Twitter peut potentiellement créer une dépendance et interférer avec votre vie quotidienne.

Astuces pour vous protéger sur Twitter

Rendez vos tweets privés :

Lorsque vous définissez votre profil Twitter et vos publications sur privé, elles seront uniquement visibles pour vos « followers ». Lorsque qu’une nouvelle personne vous suit, Twitter vous envoie une notification et vous demande d’approuver ou de refuser sa demande. Toutefois, les comptes qui vous ont suivi avant de protéger vos tweets pourront toujours voir et interagir avec votre profil, sauf si vous les bloquez.

Pour protéger vos tweets, rendez-vous dans la section confidentialité des Tweets dans vos paramètres de confidentialité et de sécurité, et cochez la case à côté de « Protéger mes tweets ». Cliquez sur le bouton Enregistrer, saisissez votre mot de passe pour confirmer, et c'est tout bon !

Par ailleurs, vous pouvez faire en sorte que les personnes qui disposent de vos informations de contact ne puissent pas vous trouver sur Twitter à moins que vous ne les suiviez au préalable. Dans la page des paramètres de confidentialité et de sécurité, décochez les deux options de détectabilité.

Empêchez Twitter de publier vos informations de localisation :

À chaque fois que vous créez un tweet, vous pouvez choisir si Twitter publie ou non votre localisation. Par défaut, Twitter ne communiquera pas votre localisation à moins que vous n'ayez déjà opté pour le service.

Évitez les harceleurs en ligne :

Le processus de blocage d'un utilisateur sur Twitter s'apparente à celui de Facebook. À partir de son profil, cliquez sur l'icône « Plus » (trois points verticaux), puis sélectionnez « Bloquer » dans le menu. Ensuite, cliquez à nouveau sur « Bloquer » pour confirmer. Les personnes que vous avez bloquées ne peuvent ni suivre, ni voir votre profil Twitter. Twitter ne leur enverra pas de notification lorsque vous les bloquerez. Toutefois, si elles consultent votre profil, elles recevront un message les informant du blocage.

Évitez le contenu inapproprié :

Le meilleur moyen de vous assurer d'éviter le contenu que vous ne souhaitez pas voir sur Twitter est de suivre uniquement les personnes qui sont déjà vos amis, et de consulter uniquement le contenu de votre feed Twitter principal. Si vous explorez la fonctionnalité de recherche de Twitter ou examinez les hashtags, vous serez vulnérable au contenu inapproprié. Par défaut, Twitter affiche un avertissement avant d'afficher du contenu qu'il considère comme peu sûr pour un environnement professionnel. Toutefois, cet outil n'est pas précis à 100% et certains tweets peuvent passer à travers le filtre de Twitter.

Faites une pause :

La désactivation de votre compte Twitter est une solution permanente. Si vous souhaitez vous distancier de Tweeter à court terme, mieux vaut vous déconnecter. Vous pouvez désactiver complètement votre compte, mais vous risquez de perdre votre profil et vos tweets antérieurs.

Instagram

Rendez votre compte privé :

À l’heure de publier des photos personnelles sur Instagram, la confidentialité est importante. Vous ne souhaitez sans doute pas que des inconnus puissent accéder à vos informations personnelles ou utiliser vos photos pour se faire passer pour vous en ligne.

Heureusement, vous pouvez rendre toutes vos publications privées et uniquement visibles pour vos amis. Pour ce faire, accédez à vos paramètres, puis sélectionnez « confidentialité du compte » et activez « compte privé ».

Les utilisateurs devront désormais vous envoyer une demande d’abonnement que devrez approuver avant qu’ils puissent consulter vos publications, vos abonnés et vos listes d’abonnements. Si une personne vous suivait avant de rendre votre compte privé et que vous souhaitez l’empêcher de voir vos futures publications, vous devrez la bloquer.

Évitez les harceleurs en ligne :

Comme la plupart des plateformes de réseaux sociaux, Instagram vous permet de bloquer facilement quelqu’un. Il vous suffit d’accéder au profil de la personne concernée, de cliquer sur le bouton « Plus » (représenté par les petits points) et de sélectionner « Bloquer ».

Une fois que vous bloquez quelqu’un, il ne pourra plus trouver votre profil, vos publications ou vos histoires. Instagram n’informera pas les utilisateurs bloqués.

Évitez le contenu inapproprié :

Bien que la publication de contenu explicite soit contraire aux politiques d’Instagram, certains utilisateurs ne se privent malheureusement pas de le faire. Comme pour Twitter, le meilleur moyen d’éviter de tomber sur du

contenu explicite est de consulter uniquement le profil des personnes en qui vous avez confiance et d’éviter d’explorer les hashtags.

Faites une pause :

Si vous souhaitez vous distancier un peu de votre compte Instagram, connectez-vous à partir d’un navigateur Internet mobile ou de bureau, accédez à votre profil, puis cliquez sur « modifier le profil ». Sélectionnez « Désactiver temporairement mon compte » et suivez les instructions. Tous vos abonnés et votre contenu vous attendront patiemment jusqu’à ce que vous soyez prêt à vous reconnecter.

8 Les rencontres en ligne et les TSA

Les rencontres en ligne sont un excellent moyen de vous faire de nouveaux amis, voire plus si affinités, mais s’accompagnent de dangers non négligeables. Les personnes que vous rencontrez via des sites de rencontre en ligne ne sont pas toujours celles qu’elles prétendent être, et les « catfish » sont très répandus.

Un « catfish » est une personne qui crée un profil de rencontre en ligne en se faisant passer pour quelqu’un d’autre. Elle peut utiliser un faux nom, de fausses images et une fausse histoire, entre autres, pour que vous vous représentiez une image mentale d’une personne qu’elle n’est pas.

Online Dating Safety

If you're using the internet to date, **remember:**

Speak with the person **before meeting**

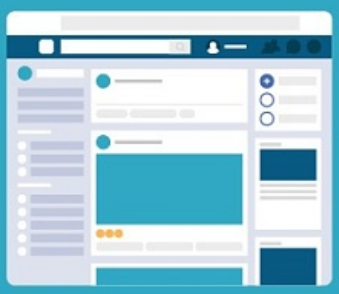
Meet in a busy public space

Don't rely on the date for a ride

Don't give personal information, like your address

Meet them over **video chat,** or on **the phone,** to verify that they are **the person in their pictures**

Add them on **Facebook** so **you can check out** their profile, pictures, and friends to get a **clearer picture** of **who they are.**



Il n’est pas toujours évident d’identifier les « catfish ». Par conséquent, vous trouverez ci-dessous des astuces pour vérifier si quelqu’un vous ment sur son identité.

Si vous faites des rencontres sur Internet, gardez à l’esprit les conseils suivants :

- Prenez toujours le temps de discuter avec quelqu’un et d’apprendre à le connaître avant d’accepter de le rencontrer en personne.
- Demandez-lui de discuter par vidéo ou téléphone pour vérifier qu’il s’agit bien de la personne sur la photo. Les personnes qui n’ont rien à cacher concernant leur identité n’émettent généralement aucune objection, et seront également rassurées de leur côté.
- Demandez-lui également de l’ajouter sur Facebook si vous avez un compte. Vous pourrez ainsi consulter son profil, ses photos et ses amis pour vous faire une meilleure idée de son identité.
- Proposez toujours un lieu public animé comme lieu de rencontre, par exemple un café en journée. Assurez-vous que d’autres personnes soient présentes pour vous aider en cas de problème, et envisagez de demander à un ami ou à un proche de vous accompagner.
- Ne communiquez jamais d’informations personnelles telles que votre adresse, même si la personne propose de venir vous chercher.
- Assurez-vous de pouvoir vous rendre au lieu de rendez-vous de manière autonome et en toute sécurité. Ainsi, vous n’aurez pas à demander à la personne de vous raccompagner si le courant ne passe pas.

9 Comment savoir si quelqu’un est vraiment la personne qu’il prétend être ?

La plupart des gens que vous rencontrez en ligne disent la vérité sur leur identité, mais certains peuvent utiliser de faux profils conçus pour vous attirer et vous manipuler. Heureusement, il est généralement facile de vérifier si une personne ment sur son identité grâce à quelques astuces simples.

Vérifiez leur photo :

Vérifiez si leur photo de profil est celle d’une personne réelle.

Si vous retrouvez la même personne sur d’autres photos de leur compte, il est probable qu’elles soient sincères. Vous pouvez enregistrer l’une de ces photos sur votre ordinateur et utiliser la recherche d’image inversée de Google pour voir si elle apparaît ailleurs en ligne.

Si vous la trouvez sur de nombreux sites, la photo est peut-être volée. Toutefois, si elle apparaît uniquement sur leur profil, il y a de fortes chances qu’il s’agisse d’une photo d’eux.

Vérifiez leur nombre d’amis :

Ont-ils d’autres amis sur leur compte ? Si vous êtes leur seul ami, ils utilisent peut-être un faux profil pour vous atteindre.

S’ils ont d’autres amis, ces derniers publient-ils des choses dans le journal ou sur le profil de la personne en question susceptibles d’indiquer qu’ils se connaissent vraiment ? Dans le cas contraire, cette personne utilise peut-être un faux profil pour attirer plusieurs cibles qui ne l’ont jamais rencontrée auparavant.

Vérifiez les mises à jour de leur statut et leurs publications :

Leurs mises à jour de statut sont-elles régulières, et concernent-elles leur vie quotidienne ? Ou publient-ils principalement des liens et publicités ? S’ils publient principalement des liens et annonces, ils utilisent probablement un faux profil pour arnaquer des gens ou vendre quelque chose.

Secret:

Vous ont-ils demandé de ne parler d’eux à personne ? Le cas échéant, cela indique qu’ils pourraient avoir de mauvaises intentions et ne sont pas de vrais amis.

Argent:

Vous ont-ils demandé de l’argent, ou vous ont-ils dit qu’ils se trouvaient dans une situation délicate et qu’ils avaient besoin d’une aide financière ? Le cas échéant, ils se font probablement passer pour un ami pour vous arnaquer.

Si vous pensez que votre ami en ligne n’est pas la personne qu’il prétend être, cessez immédiatement de lui parler et bloquez son compte.

10 Indicateurs de dangers potentiels en ligne

Si vous vous sentez contrarié, mal à l’aise ou en danger, votre situation en ligne pourrait être sérieusement menacée. Il est important d’écouter votre for intérieur et de mettre fin à la situation avant qu’elle ne se dégrade. Vous devrez peut-être bloquer la personne responsable de ce sentiment, ou solliciter l’aide d’un tiers, par exemple un proche ou la police.

Si l’un de vos amis en ligne n’est pas cohérent dans ses propos, il est possible qu’il mente sur son identité. Vous pouvez appliquer les astuces ci-dessus pour vérifier s’il vous dit la vérité, et dans le cas contraire, le supprimer de votre réseau en ligne.

Le harcèlement en ligne est courant sur les réseaux sociaux. Si une personne

se montre cruelle envers vous ou d’autres personnes, elle n’en vaut pas la peine. Nous vous conseillons de signaler les commentaires cruels à l’administrateur du site Web, puis de la bloquer pour l’empêcher de vous contacter ultérieurement.

Si quelque chose semble trop beau pour être vrai, c’est probablement le cas. Méfiez-vous toujours des arnaques. Si un inconnu ou ami vous propose quelque chose qui vous semble louche, par exemple un cadeau en échange d’un clic sur un lien, évitez-le à tout prix. En cas de doute, vous pouvez faire des recherches sur Google ou même sur Snopes.com pour savoir s’il s’agit d’une arnaque.

11 Astuces pour améliorer la sécurité de vos enfants sur Internet

Tous les parents devraient se soucier de la sécurité de leurs enfants sur Internet, que ces derniers soient atteints de TSA ou non. Voici quelques astuces et conseils pour vous aider à garantir la sécurité de vos enfants en ligne et éviter certains des dangers d’Internet.

Ways to Improve Your Child's Internet Safety

Keep your family's computer in a communal space.

Create posters of internet safety tips and hang them by your computer.

Educate your child about online safety.

Roleplay different scenarios with your child.

Set rules for time allowed on the computer to avoid internet addiction.

Put all electronics away about two hours before bed to help improve your child's sleep.

Use internet content filters to monitor and restrict your child's browsing activity.

Install child-friendly internet browsers.

Casually ask them about their online friends and what they've been talking about.

Establish a plan with them on what they should do if they encounter a cyberbully.

Provide them with a checklist of the information that they are not allowed to give out over the internet.

- Laissez l’ordinateur de votre famille dans un espace commun, par exemple le salon ou la cuisine. Ainsi, vous pouvez garder un œil sur les cercles de relations en ligne de vos enfants.
- Créez des rappels visuels et affiches avec des conseils de sécurité sur Internet, et affichez-les à proximité de votre ordinateur. C’est également une excellente occasion d’aborder la sécurité Internet avec vos enfants et de vous mettre d’accord sur certaines règles.
- Informez vos enfants sur la sécurité en ligne, assurez-vous qu’ils en comprennent l’importance et renouvelez régulièrement leurs connaissances.
- Créez différents scenarios avec vos enfants pour leur apprendre à réagir face aux dangers en ligne dans un environnement sécurisé. Vous pouvez créer un compte sur la plate-forme qu’ils utilisent et l’utiliser pour leur envoyer des messages dans le cadre du jeu de rôle, afin de le rendre plus réaliste.
- Rédigez et tenez-vous à une liste stricte de temps d’utilisation d’Internet afin de prévenir les problèmes de dépendance à Internet. Vous pouvez même diviser le temps en ligne en différentes catégories, par exemple le jeu ou les études, et l’intégrer également à la liste.
- Rangez tous les dispositifs électroniques environ deux heures avant le coucher afin de favoriser un sommeil de qualité.
- Utilisez des filtres de contenu Internet comme Net Nanny pour surveiller et limiter l’activité de navigation de vos enfants. Ces programmes limiteront également leur accès au contenu inapproprié et à tout autre site Web que vous décidez de bloquer.
- Installez des navigateurs Internet adaptés aux enfants, comme par exemple KidSplorer. Ils sont visuellement attrayants pour les enfants et sécurisent leur navigation sur Internet. Comme avec un filtre de contenu, ils pourront uniquement accéder aux sites Web que vous avez spécifiés et bloqueront même l’accès à Internet à certaines heures.
- Établissez un plan d’action avec eux pour qu’ils sachent comment réagir et à qui s’adresser en cas de harcèlement en ligne.
- Posez-leur naturellement des questions sur leurs amis en ligne et les sujets dont ils parlent, comme si vous leur demandiez comment s’est passé leur journée à l’école.
- Fournissez-leur une liste de contrôle des informations qu’ils ne sont pas autorisés à communiquer par Internet, par exemple leur nom complet, leur date de naissance, leur adresse et le nom de leur école.

12 Conclusion

Pour résumer, l’essentiel est de s’assurer que vous êtes en sécurité sur Internet. Renforcez vos mesures de sécurité en ligne. Informez-vous et restez vigilent.

Les personnes qui présentent des TSA sont plus exposées que les autres aux menaces en ligne. Nos conseils pour rester en sécurité en ligne sont donc d’autant plus importants pour elles.

Les harceleurs et arnaqueurs en ligne feront malheureusement toujours partie du décor sur Internet. Il est donc de votre responsabilité de prendre les

précautions nécessaires pour vous protéger des attaques.

Suivez nos conseils pour repérer les situations suspectes, et prenez des mesures pour vous protéger si vous vous sentez menacé.

Ce Guide de sécurité Internet traite des domaines clés à surveiller et de la manière de faire face aux menaces. Profitez de votre temps en ligne, mais n’oubliez pas de redoubler de prudence sur Internet !