#DigitSafe

Renforcer les espaces numériques sûrs et la résilience

Manuel sur la résilience numérique

Co-funded by the Erasmus+ Programme of the European Union

#DigitSafe

“#DigitSafe-Boosting digital safe spaces and resilience" vise à donner aux jeunes les moyens de devenir des citoyens numériques résilients et sûrs, leur permettant de relever certains des défis et des impacts négatifs de l'ère numérique.

Partenaires du projet:

CONEXX-EU

inova aspire

CESUR
Tu Centro Oficial de FP

alma radio 101.9

Co-funded by the
Erasmus+ Programme
of the European Union

Introduction

Le projet ***#DigitSafe-Boosting digital safe spaces and resilience*** fait suite à la stratégie de l'UE en faveur de la jeunesse pour la période 2019-2027, en accord avec l'objectif 4 de l'UE en matière d'information et de dialogue constructif. Ce projet vise à donner aux jeunes les moyens de devenir des citoyens numériques capables de résilience et de se protéger, leur permettant ainsi de relever certains défis et de lutter contre les effets négatifs de l'ère numérique.

Le but du projet #DigitSafe est de promouvoir une compréhension plus approfondie parmi les jeunes, en particulier parmi les groupes de jeunes les plus vulnérables, concernant les deux thèmes clés que sont la cybersécurité & le discours de haine, d'une part, et la sécurité & la vie privée, d'autre part. Le projet vise également à créer des espaces communs et des pratiques numériques plus sûrs et de renforcer leurs capacités en termes de résilience numérique.

Ce projet vise également à atteindre les trois principaux objectifs suivants:

- **Premièrement, promouvoir la citoyenneté numérique chez les jeunes des pays participants,** en accord avec la stratégie de l'UE en faveur de la jeunesse pour la période 2019-2027, en leur donnant des informations pratiques et concises en matière de sécurité, de confidentialité, de discours de haine et de cyberharcèlement.
- Ensuite, fournir aux jeunes les compétences nécessaires pour **améliorer leur résilience numérique**, en particulier à ceux qui ont moins d'opportunités, qui manquent souvent d'informations et de connaissances en matière de données.
- Enfin, développer une méthodologie innovante qui permet de retranscrire les informations pertinentes rassemblées dans un manuel unique en une **campagne de sensibilisation publique multicanal,** et ce, en utilisant les pratiques, les langages, les outils et les tendances de communication audiovisuelle les plus répandus chez les jeunes.

Une stratégie multimédia et multicanal qui profite de la création de contenu actuel et du grand nombre de possibilités accessibles à chaque utilisateur que propose le paysage actuel des réseaux sociaux, et qui vise à renforcer la capacité des jeunes à faire des choix rationnels, en toute connaissance de leurs droits numériques.

Ce manuel de résilience numérique consacré au cyberharcèlement, au discours de haine, à la sécurité et à la protection de la vie privée, offrira de manière approfondie et unifiée, des conseils, des informations pratiques (ressources juridiques, ressources psychologiques, astuces, ressources d'apprentissage ouvertes et autres ressources de formation) et des recommandations clés sur différentes questions pour que les jeunes acquièrent une connaissance plus approfondie de leurs droits, des risques numériques et des menaces dans le contexte de ces thématiques.

Ce projet permettra de sensibiliser les jeunes aux possibilités et aux ressources disponibles permettant de développer des compétences pour faire face aux problèmes liés à la vie numérique contemporaine.

Cette initiative permettra aux jeunes de devenir des citoyens numériques engagés et de favoriser un monde numérique plus sûr. Enfin, ce projet rassemblera une grande quantité d'informations, en les unifiant de manière plus efficace et plus compréhensible.

Ce guide sera divisé en deux modules:

1. **Cyberharcèlement & Discours de Haine**
2. **Sécurité & Confidentialité**

Cela fournira non seulement des informations sur le cadre juridique, la sensibilisation et la prévention, mais aussi des lignes directrices sur les actions à entreprendre ainsi que des conseils et des recommandations.

1. Cyberharcèlement

1. CYBERHARCÈLEMENT

1.1 Qu'est-ce que le cyberharcèlement ?

Au niveau européen, il existe plusieurs définitions du cyberharcèlement ou la cyberintimidation, celles-ci intègrent un ou plusieurs aspects selon les caractéristiques spécifiques de chacun des pays dans lesquels l'étude a été réalisée (en Belgique, en Bulgarie, aux Pays-Bas et en Espagne). Cependant, l'étude développée en 2016 par le département thématique des droits des citoyens et des affaires constitutionnelles dépendant du Parlement européen « Le cyberharcèlement chez les jeunes »[1] a abouti à une définition assez précise et homogène qui peut être utilisée au niveau transnational dans l'Union européenne:

"Le cyberharcèlement désigne les situations dans lesquelles l'intimidation a lieu sur Internet, principalement via les téléphones portables et les réseaux sociaux. Le cyberharcèlement correspond donc à un acte tout aussi agressif et intentionnel, réalisé par l'utilisation des technologies de l'information et des communications (TIC)."

Comme pour le harcèlement hors ligne, le cyberharcèlement implique généralement les 3 participants clés suivants, le comportement doit se produire intentionnellement et à plusieurs reprises et il doit y avoir un déséquilibre dans les relations de pouvoir entre l'agresseur et la victime:

1. **L'auteur**: *Personne qui mène l'agression.*
2. **La victime**: *Personne qui subit l'agression*
3. **Les témoins**: *Personnes qui voient ce qui se passe entre le harceleur et la victime, mais qui ne sont pas directement impliquées dans l'intimidation.*

[1] Céline Château. (2016). *Cyberbullying among Young people.* European Parliament*. Parlement* européen. Disponible ici : https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_FR.pdf

En ce qui concerne les personnes impliquées, il est important de souligner qu'il existe une différence importante entre le harcèlement et le cyberharcèlement. En effet, l'auteur (le harceleur) peut rester anonyme en cas de cyberharcèlement, il peut se cacher sous une fausse identité (ou l'identité de quelqu'un d'autre) et il pourrait même y avoir plusieurs personnes cachées derrière cette identité.

Toutefois, le cyberharcèlement laisse une trace électronique; qui peut servir de preuve et de moyen d'arrêter un tel comportement. Malheureusement, malgré ces différences, le harcèlement en personne et le cyberharcèlement se produisent souvent en parallèle.

En outre, certaines caractéristiques clés du cyberharcèlement facilitent son identification et sa compréhension:

Le cyberharcèlement est malveillant et jamais accidentel. Le but du cyberharcèlement est clair et conscient: nuire à la victime, la blesser, l'humilier et la faire souffrir physiquement ou mentalement.

Il se produit à partir d'une position de puissance. Le cyberharceleur a toujours un avantage et occupe une position de supériorité. Selon l'environnement dans lequel se déroule le cyberharcèlement, l'acte pourrait, par exemple, être commis par un groupe contre une victime seule. De même, les agresseurs peuvent profiter d'une victime inoffensive ou vulnérable, incapable de se défendre.

Il est répétitif et a pour objectif d'intimider, de susciter la colère ou d'humilier les victimes. Une action agressive, mais isolée n'est pas considérée comme du cyberharcèlement. On parle donc de cyberharcèlement lorsque l'agression est répétée encore et encore contre la même personne (ou les mêmes personnes).

La numérisation, et donc internet, a multiplié les canaux par lesquels le harcèlement peut être réalisé. Les canaux les plus courants pour agresser les victimes de cyberharcèlement sont:

- **Les réseaux sociaux**
- **Les plateformes de messagerie**
- **Les plateformes de jeux**
- **Les téléphones portables**

Afin de clarifier les actions qui relèvent du cyberharcèlement, voici quelques exemples d'actions illégales:

- Diffuser des mensonges ou publier des photos/vidéos embarrassantes de quelqu'un sur les réseaux sociaux.
- Envoyer des messages offensants ou des menaces via des plateformes de messagerie.
- Envoyer des messages malveillants sous l'identité de quelqu'un d'autre.

1.2. Découvrez toute la portée du cyberharcèlement et ses conséquences. Sensibiliser et apprendre à l'identifier:

Identifier le cyberharcèlement

L'une des principales façons de lutter contre le cyberharcèlement est de pouvoir l'identifier et de prêter attention aux signes avant-coureurs. Il n'existe pas de définition mondialement acceptée du cyberharcèlement au niveau international ou au niveau européen. Toutefois, la Commission européenne définit le cyberharcèlement comme:

'Harcèlement verbal ou psychologique répété commis par un individu ou un groupe à l'encontre d'autrui par le biais de services en ligne et de téléphones mobiles .'[2]

[2]Cyberbullying among Young People, direction générale des politiques internes (Parlement européen), 2016, p. 8.

Selon le Conseil de l'Europe, le cyberharcèlement se distingue des autres types de harcèlement en raison du risque d'exposition publique, du rôle complexe des observateurs et de la taille de l'audience fournie par les technologies numériques et la communication.[3]

WiredSafety**, l**e plus grand groupe de sécurité, d'éducation et d'aide en ligne au monde, n'est pas d'accord avec la proposition selon laquelle le cyberharcèlement doit être « répété » pour être qualifié de cyberharcèlement. Certains incidents graves de cyberharcèlement n'ont peut-être pas besoin d'être répétés pour être qualifiés de cyberharcèlement. Par exemple :

- Le sex-intimidation, soit le harcèlement sexuel par message ou les atteintes importantes à la réputation (par exemple, les attaques liées à l'orientation sexuelle, à l'activité sexuelle et d'autres types d'atteintes à la réputation qui peuvent être considérées comme de la diffamation)
- Les menaces de mort ou les menaces de lésions corporelles graves à la victime ou à une personne proche et dont le but est de faire souffrir la victime.[4]

Afin de créer un monde plus tolérant et plus sûr en ligne, le cyberharcèlement doit être abordé à plus grande échelle, tant au niveau individuel qu'organisationnel.

Selon un rapport publié en 2016 par le Parlement européen, l'implication directe des enfants dans la création de solutions et de politiques relatives au cyberharcèlement a été reconnue comme l'une des méthodes les plus efficaces pour faire face à ce problème.[5]

[3]https://www.coe.int/fr/web/campaign-free-to-speak-safe-to-learn/preventing-bullying-and-violence [consulté le 27/05/2022)

[4]Bullying, Perspectives, Practices and Insight, ancie Richardson, Elizabeth Milovidov, Roger Blamire, Conseil de l'Europe (2017)

[5]Cyberbullying among young People, direction générale des politiques internes (Parlement européen), 2016, p. 11

En outre, un rapport de 2017 au Conseil de l'Europe a conclu que, pour lutter contre le cyberharcèlement, la voix des jeunes devrait être représentée et entendue aux niveaux européen et national.[6] Il est donc évident que la voix des jeunes devrait se trouver au premier rang de ces discussions.

Les conséquences du cyberharcèlement ne peuvent pas être prises à la légère ou considérées comme de simples blagues, car non seulement cela revient à ignorer les émotions et la souffrance de la victime, mais aussi à banaliser ce type violence dans le milieu numérique. Les conséquences du cyberharcèlement peuvent durer pendant de nombreuses années et toucher les victimes à bien des égards.

Dans certains cas extrêmes, le cyberharcèlement peut même conduire au suicide. Le consortium #DigitSafe est parvenu à ces conclusions à la suite de recherches intensives menées dans quatre pays européens et grâce aux témoignages de victimes de cyberharcèlement recueillis par le projet. Le rapport *Social Networks and Cyberbullying* développé par le Centre commun de recherche (CCR) a permis de comprendre l'ampleur des conséquences du cyberharcèlement chez les personnes qui en souffrent. Le cyberharcèlement peut principalement entraîner des:

- **Conséquences mentales et émotionnelles**

Les victimes peuvent se sentir tristes, honteuses, gênées, stupides, déprimées, en colère ou encore anxieuses. Les victimes perdent généralement leur intérêt pour les choses qu'elles aimaient, elles développent une moindre estime de soi ou se sentent isolées, incapables de communiquer avec leurs proches. Parfois, les victimes de cyberharcèlement peuvent devenir des « victimes-agresseurs »: elles reproduisent le comportement d'un agresseur en intimidant les autres[7].

[6]Bullying, Perspectives, Practices and Insight, ancie Richardson, Elizabeth Milovidov, Roger Blamire, Conseil de l'Europe (2017) p. 44

[7] Centre commun de recherche (2013). Social Networks and Cyberbullying among Teenagers. https://publications.jrc.ec.europa.eu/repository/handle/JRC80157

En d'autres termes, il y a une réelle possibilité que le cyberharcèlement provoque un profond préjudice psychologique chez les victimes. Ces victimes sont [8]:

1. Plus susceptibles de souffrir de **dépression** et **d'anxiété.**
2. Plus susceptibles de souffrir de mauvais résultats scolaires et de problèmes de comportement à l'école.
3. Plus susceptibles de rencontrer des **difficultés à développer des compétences démocratiques de base telles que l'empathie, le respect des autres, l'ouverture à d'autres cultures et croyances, la tolérance et la confiance en soi s'ils ont été victimes de violence.**

- **Conséquences physiques**

Le stress et l'anxiété peuvent entraîner des **problèmes physiques** chez la victime comme la fatigue provoquée par des troubles du sommeil ou l'apparition de réels **troubles de santé** tels que des maux d'estomac ou des maux de tête.

- **Conséquences juridiques**

Le sentiment qu'ils sont ridiculisés ou intimidés par d'autres empêche souvent les victimes de cyberharcèlement de signaler ou d'essayer de résoudre le problème. Ce sentiment, associé à la lente évolution de la qualification juridique du crime, a pour conséquence une impunité fréquente et encourage la répétition de ces actes.

Pour combattre le cyberharcèlement, la sensibilisation est essentielle. La première étape dans l'identification du cyberharcèlement est d'avoir une définition claire de ce que cela implique. Par ailleurs, en Europe, afin de prévenir le cyberharcèlement, des décisions politiques ont été prises et de nombreux programmes ont été définis et mis en œuvre.

[8]https://www.coe.int/en/web/campaign-free-to-speak-safe-to-learn/preventing-bullying-and-violence [consulté le 27/05/2022)

Néanmoins, en raison de la portée de ce phénomène, les institutions européennes doivent poursuivre leurs recherches, légiférer et encourager des actions collectives et individuelles pour y faire face[9].

À l'attention des plus jeunes

Le Centre de recherche sur le cyberharcèlement[10] a développé une série de conseils structurés concernant la façon de procéder pour prévenir le cyberharcèlement et de nous protéger en tant qu'utilisateurs. La prévention est toujours la meilleure option pour lutter contre ce problème. Dès lors, nous avons sélectionné ces conseils précisément parce que la plupart d'entre eux ont des caractéristiques beaucoup plus orientées vers les enfants que les jeunes adultes:

- **Soyez au courant des paramètres de confidentialité**

Les sites de réseaux sociaux ou autres applications modifient et mettent à jour fréquemment leurs paramètres de confidentialité. Veillez à vous familiariser avec les nouvelles options de configuration de profil et limitez autant que possible vos informations aux personnes en qui vous avez réellement confiance.

- **Restreignez l'accès à vos coordonnées**

Ne donnez pas votre adresse e-mail ou votre numéro de téléphone à des personnes que vous ne connaissez pas. En outre, gardez votre adresse e-mail et votre numéro de téléphone hors des sites de réseaux sociaux. Vous ne savez jamais qui pourrait y avoir accès et vous ne pouvez pas faire confiance à vos « amis » ou « abonnés ».

[9]Rizza C, Martinho Guimaraes Pires Pereira A. Social Networks and Cyber-bullying among Teenagers. 25 881 EUR. Luxembourg (Luxembourg) : Bureau des publications de l'Union européenne; 2013. JRC80157

[10] Cyberbullying Research Center. (2021.) https://cyberbullying.org/preventing-cyberbullying-adults

- **Apprenez à respecter les règles de savoir-vivre d'Internet**

Pour éviter d'éventuels problèmes avec d'autres utilisateurs d'Internet, apprenez les conventions sociales liées à l'interaction sur la toile. Par exemple, n'écrivez pas tout en majuscules, car vous pourriez donner l'impression de crier pour certains. Évitez également d'utiliser le sarcasme en ligne, car il peut être facilement mal interprété.

- **N'envoyez pas de photos ou de vidéos inappropriées**

Rappelez-vous que le petit ami ou la petite amie d'aujourd'hui ne le sera peut-être plus forcément demain. Vous ne souhaitez pas qu'une personne disposant de photos ou vidéos inappropriés de vous les partage sur la toile avec le reste du monde. Ne prenez pas le risque de devoir vous inquiéter à ce sujet.

- **Faites une recherche Google avec votre nom**

Vous devriez toujours savoir ce qu'on dit de vous. Il est souvent surprenant de trouver que des informations, normalement confidentielles, apparaissent dans des bases de données publiques, dans de nouveaux articles ou sur des pages de réseaux sociaux qui ont été référencés par les moteurs de recherche.

- **N'acceptez pas les demandes d'amis d'inconnus**

Si vous ne connaissez pas la personne qui vous envoie une demande d'ami ou d'abonnement, ignorez-la. La plupart des sites et applications de réseaux sociaux vous donnent également la possibilité de bloquer l'utilisateur si vous le souhaitez.

- **Utilisez les paramètres de contrôle du site**

Désactivez les options de recherche sur certains sites de réseaux sociaux pour empêcher toute personne lambda de vous chercher ou de vous envoyer des messages. Cela vous permet d'avoir plus de contrôle sur vos échanges en ligne, car vous êtes le seul à pouvoir l'initier.

- **Protégez vos informations**

Si vous utilisez un ordinateur public ou une connexion sans fil, assurez-vous de vous déconnecter de n'importe quel site sur lequel vous vous trouvez lorsque vous quittez cet ordinateur, et ce, même pendant une minute.

D'ailleurs, faites-le aussi sur vos autres appareils mobiles s'il y a une chance que quelqu'un vienne et utilise votre compte pour être drôle ou malicieux. Ne donnez pas de mots de passe à qui que ce soit et changez votre mot de passe fréquemment. En outre, assurez-vous que votre téléphone et votre tablette ont un code d'accès et sont verrouillés.

- **Soyez sceptique lors des interactions en ligne**

Même parmi les personnes en qui vous avez confiance, il est risqué de révéler trop d'informations parce que vous ne savez jamais avec certitude si la personne avec qui vous pensez communiquer est vraiment là ou si elle est seule.

- **Protégez-vous de vous-mêmes et des autres**

Rappelez-vous que certaines personnes ont beaucoup de temps à perdre et tout ce qu'elles veulent faire, c'est rendre la vie des autres misérables. Ne les laissez pas faire. Évitez de mettre en ligne trop d'informations personnelles ou privées qui pourraient être utilisées pour vous harceler ou vous humilier. Évitez également toute forme d'interaction avec les harceleurs. Car comme le veut le bon sens: ne donnez pas aux trolls d'Internet de quoi vous atteindre!

<u>À l'attention des enseignants et des parents</u>

En raison des conséquences que cet acte peut avoir sur ses victimes, il est important que les associations, les écoles, les lieux de travail et les citoyens s'engagent à lutter contre le cyberharcèlement. La recherche développée par Cyberbullying Research Center en 2021 « Cyberharcèlement : comment l'identifier, le combattre et y répondre en 2021 »[11] donne une

[11]Hinduja S. et Patchin J.W. (2021). Cyberbullying : Identification, prevention and Response https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2021.pdf

explication détaillée de la manière dont les enseignants et les parents pourraient s'attaquer au cyberharcèlement en matière d'identification et de prévention :

Éduquer la communauté vers une utilisation responsable des dispositifs, tout en mettant l'accent sur la citoyenneté numérique, est peut-être l'étape préventive la plus importante pour les établissements d'enseignement et ses professeurs. Inculquer la discipline aux étudiants qui se lancent dans des actes de harcèlement ou de menace et leur faire savoir que ce qu'ils font n'est pas une simple erreur; c'est un crime.

Il est essentiel d'inclure dans divers domaines, des programmes d'enseignement ; un contenu en ligne approprié pour discuter du cyberharcèlement et d'autres menaces numériques.

En outre, les messages de prévention pourraient être renforcés dans d'autres matières, en particulier dans celles qui utilisent la technologie et les outils numériques. Il est crucial d'établir et renforcer un environnement de respect et d'intégrité dans les établissements d'enseignement, un lieu où les violations et le harcèlement sont traités de manière formelle ou informelle.

De plus, de nos jours, l'élaboration de stratégies nouvelles et créatives pour lutter contre le cyberharcèlement devient de plus en plus importante, en particulier pour faire face à des formes mineures de harcèlement et les éviter. Les chercheurs Sameer Hinduja et Justin W. Patchin (2021) du Centre de recherche sur le cyberharcèlement en donnent différents exemples:

"Les étudiants peuvent être invités à créer des affiches contre le cyberharcèlement et à les exposer dans toute l'école, ou une vidéo d'annonce de service public (PSA) qui véhiculent un message contre le harcèlement et/ou un message de gentillesse.

Les étudiants plus âgés pourraient être invités à faire une brève présentation aux étudiants plus jeunes concernant l'importance d'utiliser la technologie de manière éthique.

Le but ici, encore une fois, est de condamner le comportement (sans condamner l'enfant) tout en envoyant le message au reste de la communauté scolaire que le harcèlement, sous n'importe quelle forme, est inacceptable et ne sera pas toléré".[12]

En d'autres termes, l'apprentissage formel ne se suffit pas à lui-même. En effet, il est également nécessaire d'introduire, dans l'apprentissage formel, des activités d'apprentissage non formel et informel afin dans le but de combattre et de prévenir le cyberharcèlement dans un cadre ludique.

Par ailleurs, les parents *"doivent apprendre à leurs enfants, par leurs paroles et leurs actes, qu'ils souhaitent tous le même résultat final: mettre fin au cyberharcèlement et que la vie ne devienne pas encore plus difficile."*[13]

Le Centre de Recherche sur le Cyberharcèlement (https://cyberbullying.org/) souligne à quel point il est essentiel, en tant que parent, de ne pas négliger le point de vue de leurs enfants, mais de valoriser leur récit et leur opinion. **Il est essentiel que les victimes de cyberharcèlement et les témoins sachent que les adultes, puisqu'ils sont au courant de la situation, « interviendront rationnellement et logiquement, et ne feront pas empirer la situation ».**[14]

Comment les parents devraient-ils réagir s'ils découvrent que leur propre enfant harcèle sur internet? Tout d'abord, ils doivent lui expliquer en quoi ce comportement provoque et cause du mal dans le monde réel. Après cela, les parents devraient être en mesure de lui donner la possibilité de passer à autre chose et de mettre fin à ce comportement.

[12] Hinduja S. et Patchin J.W. (2021). Cyberbullying : Identification, prevention and Response https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2021.pdf

[13] Hinduja S. et Patchin J.W. (2021). Cyberbullying : Identification, prevention and Response https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2021.pdf

[14]Hinduja S. et Patchin J.W. (2021). Cyberbullying: Identification, prevention and Response https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2021.pdf

Les chercheurs Sameer Hinduja et Justin W. Patchin (2021) proposent aux parents « de favoriser l'empathie en les mettant intentionnellement dans des situations qui les rendent inconfortables et qui peuvent adoucir leur cœur ».

Les enfants ont besoin de savoir que chaque action, même si elle se fait en ligne, a de graves conséquences. Du côté des parents, il est essentiel de commencer à prêter une plus grande attention au comportement et aux actions de leurs enfants en ligne.

1.3. Conseil: comment se comporter avec les victimes de Cyberharcèlement ? (Procédures, empathie, importance de l'écoute, soutien émotionnel, soutien psychologique) :

La compilation des procédures et des conseils sur la manière de procéder a été principalement façonnée par les propositions, plus que complètes, du Cyberbullying Research Center et d'Amnesty Jeunes (https://jeunes.amnesty.be/).

Lorsque vous êtes vous-même une victime

Si vous êtes victime de cyberharcèlement, nous aimerions vous conseiller avec une série d'étapes à suivre:

- **Demander de l'aide**

Tout d'abord, vous devez parler: discutez-en avec vos proches ou avec des professionnels !

- **Signaler le contenu**

Si le cyberharcèlement s'est produit sur un réseau social, signalez le contenu à cette plateforme. Ce n'est pas toujours efficace, mais il est important que le réseau social sache qui est l'accusé afin qu'il puisse agir, parfois après plusieurs signalements.

- **Se protéger**

Modifiez votre mot de passe, renforcez la confidentialité de vos messages, supprimez les informations personnelles telles que votre adresse e-mail, votre numéro de téléphone ou des liens vers d'autres comptes.

- ***À titre temporaire, supprimer votre compte ou modifier votre pseudonyme***

Essayez de vous déconnecter des réseaux sociaux pendant un certain temps, bloquez la personne qui est à l'origine du cyberharcèlement.

- **Répondre et rappeler à la personne qui vous harcèle le cadre juridique en soulignant que le harcèlement en ligne constitue un crime punissable par la loi.**
- **Si cela se produit dans le milieu du travail, parlez-en à votre employeur**

Faites savoir à votre employeur si la personne qui vous harcèle est un collègue de travail, ou si l'intimidation se produit sur un forum ou un blog lié au travail. Si le harcèlement vous empêche de faire votre travail, votre employeur doit le savoir.

- **Couper les ponts.**

Ne vous liez pas d'amitié avec ceux qui sont méchants et n'essayez de les convaincre à se rapprocher de vous. Si vous sentez que vous avez besoin de répondre à la personne qui vous harcèle, faites-le respectueusement. N'essayez pas de rationaliser ou de vous lier d'amitié avec quiconque est cruel envers les autres.

- **Ne pas établir de relation**

Les personnes qui harcellent sur internet cherchent à vous faire réagir. Le problème est que si vous réagissez avec agressivité, le harceleur peut se servir de cette réponse et continuer (voire aggraver) le cyberharcèlement. De plus, votre réaction pourrait avoir des conséquences.

- **Contacter le fournisseur d'accès Internet (FAI)**

Si votre harceleur a été identifié, essayez de contacter son fournisseur d'accès à Internet. Le FAI peut alors contacter la personne ou peut-être directement fermer son abonnement à Internet.

- **Déposer une plainte en se rendant au commissariat de police**

Conservez des preuves de cette agression (par exemple, des captures d'écran). La police prendra note de votre plainte et de toutes les informations relatives à votre plainte et les consignera dans un rapport. Elle vous remettra ensuite une copie du rapport et un certificat de plainte. Le rapport est ensuite envoyé au parquet, c'est-à-dire aux magistrats chargés des enquêtes. Demandez le numéro du procès-verbal pour pouvoir suivre l'affaire et savoir quel parquet (de quelle commune) est compétent.

- **Signaler publiquement le cyberharcèlement**

Partagez des captures d'écran de l'agresseur (assurez-vous de cacher le nom d'utilisateur et la photo de profil de celui-ci afin que vous ne soyez pas accusé de diffamation).

<u>En tant que collègue (au travail ou à l'école)</u>

Dans ce domaine, l'ONGI Save the Children[15] a très justement indiqué quelques recommandations concernant la façon d'agir en cas de harcèlement :

- Il est possible que vous ressentiez de la peur ou du rejet dans une telle situation, mais <u>prenez des mesures</u>.
- Si vous voyez que vous ne pouvez pas l'arrêter par vous-même et que ce n'est pas la meilleure chose à faire, <u>demandez de l'aide à un adulte ou à une personne responsable.</u> Il ne s'agit pas ici d'être une « balance », mais plutôt de soutenir ceux qui en ont besoin.
- <u>Soutenez le collègue</u> qui est victime de harcèlement. Personne ne mérite d'être maltraité.

[15]Save the Children. Conseils destinés étudiants concernant la façon de faire face au harcèlement. https://www.savethechildren.es/publicaciones/consejos-para-estudiantes-frente-al-bullying-o-acoso-escolar

- Proposez d'organiser une formation ou de développer du matériel pour sensibiliser votre établissement d'enseignement ou votre entreprise afin de combattre le cyberharcèlement et de demander de l'aide.

En tant qu'enseignant

Les enseignants doivent prêter attention à différents signes qui peuvent indiquer qu'un enfant est victime de cyberharcèlement. Parmi ces signes, on retrouve une augmentation ou une diminution rapide de l'utilisation des appareils, ou encore une réponse dictée par les émotions à ce qui se passe sur leur appareil. Si un enfant cache son écran ou son appareil lorsque d'autres sont proches et évite toute discussion, il faut le prendre en compte.

En outre, les enseignants doivent également aider les enfants à identifier, à réagir et à éviter le cyberharcèlement. Voici quelques recommandations:

- La communication est très importante, donc **si vous pensez qu'un enfant est victime de cyberharcèlement, parlez-lui en privé et posez-vous des questions à ce sujet.** Vous pouvez également en parler à un parent. Les enseignants peuvent faire office de médiateurs entre l'enfant, les parents et l'école.
- **Promouvoir un environnement sûr en classe.** Aider les enfants à développer l'intelligence émotionnelle afin qu'ils puissent acquérir des compétences en matière de conscience de soi et les compétences d'autorégulation et apprendre à avoir de l'empathie envers les autres.
- Encouragez les élèves à prêter attention aux signes qui peuvent les aider à comprendre quand quelque chose les met mal à l'aise, inquiets, tristes ou anxieux a lieu sur les médias numériques.
- Apprenez-leur à réfléchir avant de publier quelque chose.
- Expliquer aux étudiants les trois façons dont ils peuvent et devraient répondre s'ils sont témoins de cyberharcèlement : si vous soutenez la victime de harcèlement, vous êtes un bon ami, si vous essayez de mettre fin au cyberharcèlement, vous faites preuve de solidarité et si vous êtes victime de cyberharcèlement, vous devez le signaler à un adulte.

En tant que parent

Il est très probable que les enfants ne reconnaissent pas qu'ils sont victimes de cyberharcèlement parce qu'ils pourraient en avoir honte. Il est très courant que les jeunes souffrent en silence. Ils peuvent craindre que les parents réagissent en limitant leur accès à internet, ils peuvent se sentir gênés de ne pas pouvoir résoudre ce problème de harcèlement eux-mêmes, ils peuvent avoir peur que les parents gèrent les choses et aggravent la situation, ou qu'ils ne comprennent pas le problème.

Pour ces raisons, si les parents voient des signes chez leurs enfants, ils doivent agir immédiatement. Tout d'abord, **essayez de parler avec votre enfant et écoutez-le.** La meilleure façon de le faire est de l'engager dans la conversation sur ce qui se passe dans le calme. Prenez votre temps pour comprendre exactement ce qui s'est passé et le contexte dans lequel cela s'est produit.

Il est très important pour votre enfant que vous ne minimisiez pas la situation. Étant donné que les réseaux sociaux sont devenus une extension de la vie quotidienne des enfants, un commentaire ou un texte désagréable peut être dévastateur pour eux. Afin de renforcer la confiance entre vous, félicitez votre enfin d'avoir fait le bon choix et de vous en avoir parlé.

Une fois que vous êtes au courant de la situation, **offrez du réconfort et un soutien inconditionnel,** car les victimes de cyberharcèlement éprouvent souvent un sentiment d'isolement. Montrez à votre enfant que cette situation peut être traitée d'une manière qui n'implique pas de représailles. Faites en sorte que votre enfant se sente en sécurité, il doit être la priorité absolue, ainsi que de lui faire savoir que ce n'est pas de sa faute.

Après cela, **essayez de recueillir autant de preuves que possible**. Imprimez ou faites des captures d'écran ou encore des enregistrements de conversations, de messages, d'images, de vidéos et d'autres éléments qui peuvent servir de preuve évidente pour démontrer que votre enfant est victime de cyberharcèlement. Tenez un journal de tous les incidents pour aider au déroulement de l'enquête. En outre, **gardez des notes sur les détails pertinents** tels que l'emplacement, la fréquence, la gravité du préjudice, la participation de tiers ou les témoins, ainsi que le contexte.

L'étape suivante **consiste à contacter le fournisseur de contenu**, car le cyberharcèlement viole toujours les Conditions d'utilisation de tous les fournisseurs de services légitimes. Ils devront donc prendre des mesures à ce sujet afin que votre enfant n'en souffre plus.

Si le harceleur est un camarade de classe ou va à la même école que votre enfant, vous devriez en **informer l'école dès que possible**, car l'établissement pourrait avoir établi des règles pour répondre à la problématique.

Les parents peuvent également contacter la police dans le cas où la procédure susmentionnée ne permettrait pas à la situation de s'améliorer.

Si nécessaire, essayez de demander une aide psychologique pour votre enfant. Les enfants peuvent bénéficier d'un entretien avec un professionnel de la santé mentale. Ils préfèrent peut-être dialoguer avec un tiers qui peut être considéré comme plus objectif.

1.4. Mesures de prévention

Il n'y a pas de moyen infaillible qui empêcherait un enfant d'être victime de cyberharcèlement. Cependant, il existe différentes façons de réduire la probabilité qu'ils soient touchés.

Tout d'abord, **il est important d'utiliser des mots de passe** pour tout et de ne pas les partager avec qui que ce soit. Un bon moyen d'améliorer la sécurité des enfants sur internet est d'utiliser les outils et paramètres de confidentialité fournis par les réseaux sociaux.

Nous devons nous assurer que les enfants sont conscients des paramètres et des outils de confidentialité offerts par ces derniers et parcourir chaque réseau social pour définir les paramètres de confidentialité sur le mode le plus sécurisé. Par conséquent, les comptes devront être privés, afin qu'il soit impossible de les taguer, etc.

Les enfants doivent savoir qu'il est important de garder les informations personnelles privées. Ils ne doivent jamais partager leur adresse, leur numéro de téléphone portable ou leur adresse e-mail sur internet. Ils doivent faire attention à partager trop d'informations sur l'endroit où ils vont à l'école, surtout s'ils ont des « amis » ou des « abonnés » sur les réseaux qu'ils ne connaissent pas très bien.

Ils doivent également savoir qu'ils doivent se déconnecter lors de l'utilisation d'appareils publics tels que des ordinateurs publics ou des ordinateurs portables à l'école ou à la bibliothèque. Cela comprend la déconnexion de la boîte mail, des comptes sur les réseaux sociaux, de leur compte scolaire ou de tout autre compte qu'ils peuvent ouvrir.

Enfin, et c'est peut-être le plus important, **les enfants devraient être conscients que s'ils deviennent victimes de cyberharcèlement, ils doivent le signaler à leurs parents ou à leurs enseignants.**

1.5. Comment signaler le cyberharcèlement (cadre juridique, institutions, ONG, etc.)

L'un des aspects les plus marquants du signalement du cyberharcèlement réside dans le fait que la plupart des pays européens ne disposent pas d'une législation spécifique à ce sujet.

Malgré son importance, le grand nombre de cas et les inquiétudes parmi les jeunes, la législation n'a pas encore progressé dans ce domaine. Le travail des institutions et des organisations est donc essentiel pour aider à identifier les cas, les dénoncer et apporter un soutien aux victimes.

En Belgique

- **Cadre juridique**

Le cyberharcèlement est considéré comme une « infraction pénale » en Belgique, et fait donc l'objet de sanction pénale. Néanmoins, comme dans de nombreux autres pays, il n'existe pas de loi pénale spécifique en matière de cyberharcèlement.

Cependant, cela ne signifie pas que l'infraction pénale reste impunie, mais plutôt qu'elle passe par d'autres lois belges:

Art. 442 bis du Code pénal belge = Harcèlement.

"*Quiconque profère en public des mensonges préjudiciables à l'honneur ou à la réputation d'autrui commet une infraction à l'article 442 du Code pénal belge*".

Art. 422 bis du Code pénal belge = « stalking ».

Art. 145.3bis de la loi du 13/06/2005 en ce qui concerne les communications électroniques, la diffamation et l'atteinte à l'honneur.

Art. 448 du Code pénal belge = Injures publiques.
Art. 383 du Code pénal belge = outrage public à la pudeur.

Dans le monde du travail, le cyberharcèlement est un phénomène relativement récent et inexploré, malgré l'utilisation omniprésente des technologies de l'information et de la communication dans les environnements et modalités de travail. La Convention de l'OIT sur la violence et le harcèlement, 2019 (n° 190), et la Recommandation n° 206 qui l'accompagne, ont récemment été adoptées et incluent dans leur champ d'application la violence et le harcèlement survenant également « par le biais de communications liées au travail, y compris celles rendues possibles par les technologies de l'information et de la communication ». En Belgique, ces dispositions sont intégrées dans la législation nationale concernant la sécurité et la santé au travail (SST).

- **Institutions et ONGs**

En Belgique, si le cyberharcèlement se produit dans un établissement d'enseignement, des règlements intérieurs permettent à ces établissements de prendre des mesures à ce sujet.

En outre, il existe des associations et des plateformes qui offrent un soutien et une orientation aux victimes qui cherchent de l'aide avant la procédure judiciaire qui, dans la plupart des cas, est complexe, difficile et éprouvante pour les adolescents.

L'application **CyberHelp** (https://smartcity.brussels/news-750--the-cyberhelp-app-combats-cyberbullying)

Il s'agit du résultat d'une initiative commune de la police fédérale belge, de l'Université Mons et de la Fédération Wallonie-Bruxelles. Il s'agit donc d'une **application contre le cyberharcèlement**, permettant de le signaler via votre propre smartphone. L'application comprend un bouton qui permet aux jeunes victimes de harcèlement de faire une capture d'écran de leur historique de conversation avec un cyberharceleur et un second bouton par lequel ils peuvent ensuite, envoyer ce contenu aux personnes chargées de gérer de telles situations au sein de leur établissement d'enseignement.

En 2021, l'équipe de CyberHelp présentera l'application à 12 000 élèves lors d'une centaine de visites dans des écoles de Wallonie et de Bruxelles.

Amnesty Jeunes Belgium (https://jeunes.amnesty.be/)

Télé-Accueil Bruxelles (https://tele-accueil.be/bruxelles/)

Télé-Accueil est un **service d'écoute et de chat par téléphone**. Toute personne souhaitant trouver « quelqu'un à qui parler » trouvera en composant le 107, une oreille attentive, gratuite, et ce, 24 heures sur 24, 7 jours sur 7, dans l'anonymat et la confidentialité. C'est une excellente option pour les victimes qui, par gêne ou ne sachant pas comment faire face au cyberharcèlement, à la cybercriminalité ou aux discours de haine, peuvent bénéficier d'une assistance et d'une personne qui les écoute et les conseille.

En Espagne:

En cas de cyberharcèlement, il y a plusieurs choses dont il faut être conscient. Tout d'abord, ne répondez pas aux messages de cyberharcèlement, ne les transférez pas et bloquez la personne qui vous harcèle. Il est important de conserver des preuves de cyberharcèlement. Notez les dates, les heures et les descriptions de ces actes.

Il est possible de signaler l'intimidation à la fois sur la plateforme où elle a lieu, mais aussi légalement, par exemple à la police.

Lorsque vous signalez un cas sur une plateforme, examinez d'abord ses conditions générales ou ses sections sur les droits et responsabilités. Celles-ci décrivent les contenus qui sont ou ne sont pas appropriés. Ensuite, signalez le cyberharcèlement auprès du site de réseaux sociaux afin qu'il puisse prendre des mesures contre les utilisateurs qui violent les conditions d'utilisation.

En revanche, lorsque le cyberharcèlement implique des menaces de violence, de la pédopornographie ou l'envoi de messages ou de photos sexuellement explicites, ou encore de harcèlement et de crimes haineux, il est considéré comme un délit. Dans ces cas, il convient de le signaler à la police.

Il existe des associations qui offrent un soutien et une aide aux enfants ou aux adolescents et à leurs familles qui ne savent pas comment faire face à cette question ou comment le signaler. Par exemple :

Cybersmile (https://www.cybersmile.org/who-we-are).

Il s'agit d'une organisation à but non lucratif engagée pour le bien-être numérique et la lutte contre toutes les formes d'intimidation et d'abus en ligne.

AEPAE (https://aepae.es/plan-nacional).

Il s'agit d'une association visant à prévenir l'intimidation en Espagne. L'objectif de cette association est de développer chez les enfants et les adolescents des comportements préventifs visant à résoudre les conflits dans le milieu scolaire.

INFOACOSO (https://infoacoso.es/telefonos-de-ayuda-contra-el-acoso-y-el-bullying).

Cette association propose un guide sur son site Web sur la façon d'agir si vous êtes victime de cyberharcèlement et où appeler pour le signaler, en fonction de la communauté autonome d'Espagne dans laquelle vous vivez.

Aux Pays-Bas:

Aux Pays-Bas, les institutions et organismes suivants peuvent vous aider si vous êtes victime de cyberharcèlement :

- **MiND** (https://www.mindnederland.nl/) la ligne d'urgence contre la discrimination sur Internet qui enregistre et évalue les signalements de discrimination sur Internet.
- Contactez un service de lutte contre la discrimination dans votre région. Toutes les communes des Pays-Bas disposent d'un service anti-discrimination auquel vous pouvez vous adresser pour poser une question ou déposer une plainte pour discrimination.
- Appelez la ligne d'assistance nationale contre la discrimination (0900 235 5345)
- Contactez la police si vous avez été harcelé, intimidé, menacé ou pire encore.

Certains des services mentionnés ci-dessus sont spécifiques aux personnes qui ont été victimes de discrimination. La discrimination est généralement définie comme le traitement inégal d'une autre personne en raison de son origine ethnique, de son sexe, de son genre ou de ses caractéristiques génétiques. La discrimination est interdite par la législation européenne:

Article 21 : *"Toute discrimination fondée sur le sexe, la race, la couleur, l'origine ethnique ou sociale, les caractéristiques génétiques, la langue, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à une minorité nationale, la fortune, la naissance, le handicap, l'âge ou l'orientation sexuelle est interdite".*[16]

Comme le cyberharcèlement peut prendre de nombreuses formes, vous pouvez avoir l'impression d'être victime de cyberharcèlement qui n'est pas spécifiquement discriminatoire. Dans ce cas, voici quelques suggestions:

[16]Article 21 de la législation européenne : Non-discrimination https://fra.europa.eu/fr/eu-charter/article/21-non-discrimination - :~:text=EU Charter of Fundamental Rights,-Previous title&text=1.,2

- Signaler le cyberharcèlement à l'école/au travail (si vous êtes victime de harcèlement de la part de quelqu'un sur votre lieu de travail/d'enseignement) ;
- Stop Online Bullies est un programme d'intervention conçu par les Pays-Bas pour les victimes de cyberharcèlement ayant un faible niveau d'éducation, et dont l'objectif est d'apprendre aux victimes à faire face au cyberharcèlement et à ses effets négatifs;
- Bloquer et signaler le cyberharcèlement sur vos réseaux sociaux ;
- Bloquer et signaler le numéro du harceleur ;
- Demander des informations à votre service de police local ;
- Déposer un rapport officiel auprès de la police (si cela est perçu comme la meilleure solution après discussion avec le service de police).

Aux Pays-Bas, des responsabilités spécifiques sont confiées aux écoles pour combattre et prévenir le cyberharcèlement. Par exemple, le programme KiVa vise à améliorer la sécurité des élèves dans les écoles et a été financé par des subventions du ministère néerlandais de l'Éducation.

IL s'agit d'un programme de recherche et de lutte contre le harcèlement basé sur des preuves. KiVa (https://www.kivaprogram.net/) a été développé à l'origine par l'Université de Turku, en Finlande, et a été introduit dans des écoles du monde entier. Il repose sur trois éléments principaux : la prévention, l'intervention et le suivi.[17]

- **Prévention**. des actions préventives comme le programme KiVa sont menées dans les écoles pour se concentrer sur la prévention au cyberharcèlement.
- **Intervention**. Les techniques d'intervention de KiVA ciblent les enfants qui ont été directement impliqués dans des actes de harcèlement. L'objectif est de fournir aux écoles et aux élèves des outils **orientés vers les solutions**.
- **Suivi annuel.** Les enquêtes annuelles menées auprès des élèves et du personnel des écoles partenaires de KiVa servent à contrôler l'efficacité du programme et à fournir des informations pour améliorer le travail de lutte contre le harcèlement.

[17]En quoi consiste KiVa? https://belgique.kivaprogram.net/

Des programmes tels que KiVa permettent de tirer des leçons et de les appliquer auprès de citoyens et d'organisations du monde entier. Il est évident qu'il est essentiel de se concentrer sur les mesures préventives pour s'assurer que toutes les formes de harcèlement soient traitées.

Ces mesures peuvent être appliquées aux cas de cyberharcèlement à travers des campagnes d'éducation. Ces mesures garantissent que les internautes soient capables d'utiliser internet en toute sécurité.

En Bulgarie

Les cybercrimes, y compris le cyberharcèlement, les risques concernant la vie privée et la sécurité en ligne sont signalés au département de la cybercriminalité du ministère de l'intérieur bulgare. Il s'agit d'un dispositif de signalement des cas non urgents de cybercriminalité (consacré principalement à la cyberfraude et à la pédopornographie). Le programme est contrôlé par le département de la cybercriminalité (www.cybercrime.bg) au sein de la direction générale de la lutte contre le crime organisé du ministère de l'Intérieur.

Un formulaire en ligne permet de signaler les cas de cyberharcèlement, de cyberfraude et de pédopornographie. Pour les cas urgents, il est conseillé d'appeler le numéro d'urgence: 112.
Site web: www.cybercrime.bg
Téléphone: 112 (en cas d'urgence)

Il existe également un dispositif géré par l'État pour soutenir et conseiller les enfants et les jeunes sur différents sujets, notamment le cyberharcèlement, les discours de haine et les risques relatifs à la vie privée et à la sécurité en ligne. Il s'agit de la **ligne téléphonique nationale pour les enfants** 116 111, qui est gérée et administrée par l'Agence nationale pour la protection de l'enfance dans le but de soutenir tous les enfants et leurs familles en Bulgarie. Les opérateurs qui répondent aux appels sont des psychologues qualifiés qui, 24 heures sur 24 et 7 jours sur 7, de manière anonyme et totalement gratuite, sont prêts à écouter, soutenir, conseiller et guider les appelants sur toutes les questions qui les préoccupent.

2. Discours de haine

2. DISCOURS DE HAINE

2.1. Qu'est-ce que le discours de haine?

Il n'existe pas de définition universellement acceptée du discours de haine. Dans cette section, nous présenterons quelques définitions qui sont décrites à la fois dans la législation de l'UE et par des organisations de premier plan qui luttent contre les discours de haine.

Le discours de haine, phénomène illégal, est défini par la législation européenne comme

'l'incitation publique à la violence ou à la haine sur base de certaines caractéristiques, dont notamment la race, la couleur, la religion, l'ascendance et l'origine nationale ou ethnique'.

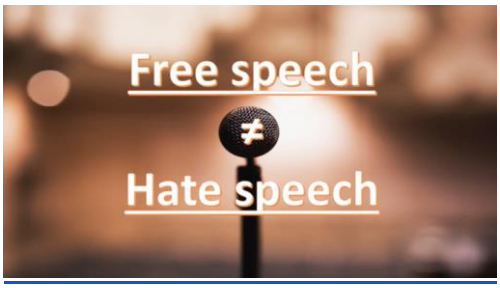
Bien que la décision-cadre porte sur le racisme et la xénophobie, la majorité des États membres ont étendu leur législation nationale à d'autres motifs tels que l'orientation sexuelle, l'identité de genre et le handicap.

L'INACH (le principal réseau de lutte contre la cyberhaine dans l'UE et dans le monde) définit le discours de haine comme:

'Des déclarations publiques discriminatoires et/ou diffamatoires, intentionnelles ou non ; l'incitation volontaire à la haine et/ou à la violence et/ou à la ségrégation fondée sur la race, l'ethnie, la langue, la nationalité, la couleur de la peau, les convictions religieuses ou l'absence de croyance, le sexe, l'identité sexuelle, l'orientation sexuelle, les opinions politiques, le statut social, la naissance, l'âge, la santé mentale, le handicap ou la maladie d'une personne ou d'un groupe.'

Le droit européen protège la liberté d'expression, ce qui amène certains à penser qu'il existe une zone floue entre la protection de la liberté d'expression et la pénalisation des discours de haine. De nombreux experts estiment que ce prétendu « conflit d'intérêts » entre la pénalisation du discours de haine et la protection de la liberté d'expression est mal interprété. En réalité, le Pacte international relatif aux droits civils et politiques (PIDCP) interdit « tout appel à la haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination, à l'hostilité ou à la violence. » Cette courte vidéo explique davantage cette idée fausse et les raisons pour lesquelles la liberté d'expression n'est pas un droit absolu.

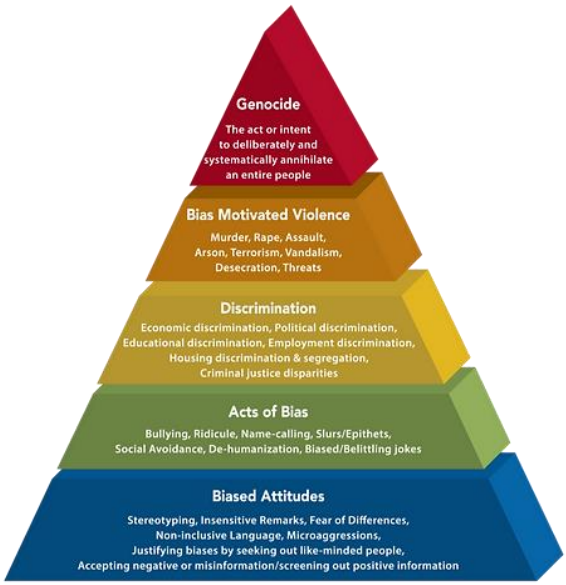
Cette courte vidéo explique davantage cette idée fausse et pourquoi la liberté d'expression n'est pas absolue.



https://www.youtube.com/watch?v=V0HhyVLX0ZA

La « Pyramide de la haine » (voir ci-dessous) représente le danger de toutes les formes de discours de haine[18] :

La pyramide de la haine est utilisée pour illustrer la façon dont le discours de haine a historiquement été un précurseur de la violence extrême et continue de l'être. Son but est de mettre en évidence la menace que les discours de haine peuvent représenter pour les autres en alimentant la pyramide de la haine et de la violence. La lutte contre les discours de haine est donc essentielle pour créer un monde plus pacifique et plus tolérant.



[18] https://www.rightsforpeace.org/hate-speech

2.2. Comment prévenir le discours de haine

Les discours de haine sont abordés au niveau de l'UE par la Directive sur les Services de Médias Audiovisuels (DSMA), celle-ci exige des autorités nationales de chaque pays de l'UE qu'elles veillent à ce que les programmes de médias audiovisuels ne contiennent pas d'incitation à la haine.[19]

En outre, au niveau de l'UE, la Commission a convenu avec Facebook, Microsoft, Twitter et YouTube d'un « code de conduite visant à lutter contre les discours de haine illégaux sur internet ». Le respect de ce code de conduite fait l'objet de contrôle régulier par un réseau d'organisations dans l'ensemble de l'UE.[20]

Comment pouvez-vous, au niveau individuel, lutter contre les discours de haine?

Une façon de lutter contre les discours de haine est de **bloquer et de signaler les propos haineux que vous rencontrez en ligne** (voir la section suivante sur les recommandations pour signaler les discours de haine).

Les Nations Unies recommandent de s'engager à adopter les pratiques suivantes afin de prévenir les discours de haine[21] :

- **Faites une pause:** retenez-vous d'écrire des commentaires haineux et/ou de partager un tel contenu;
- **Vérifier les faits:** assurez-vous de repérer les informations fausses et biaisées avant de diffuser de la désinformation ;
- **Laissez place au défi:** propagez votre propre contre-discours et contestez le discours de haine dans la mesure du possible ;

[19]Code of Conduct – illegal online hate speech Questions and answers https://ec.europa.eu/info/sites/default/files/code_of_conduct_hate_speech_en.pdf

[20] Code de conduite de l'UE pour lutter contre le discours de haine illégal en ligne https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_fr

[21] Nations Unies : comment réagir face aux discours de haine ? https://www.un.org/en/hate-speech/take-action/engage

- **Soutenez:** prenez publiquement position et faites preuve de solidarité envers les victimes du discours de haine ;

- **Signalez:** consultez les lignes directrices communautaires des plateformes de médias sociaux que vous utilisez et signalez les cas de discours haineux qui enfreignent ces directives. Pour les cas plus graves, vous pouvez déposer une plainte auprès de la police (par exemple, lorsqu'il y a incitation à la violence) ;

- **Sensibilisez:** partagez des ressources éducatives et des campagnes publiques ou engagez la conversation avec vos amis et votre famille ;

- **Engagez-vous:** songez à joindre à une ONG ou une initiative qui s'efforce de lutter contre les discours haineux au sein de votre communauté.

Pour en savoir plus sur les discours de haine et les moyens de les prévenir, faites le test en répondant à ce quiz des Nations Unies : https://www.un.org/en/hate-speech/take-action/test-yourself

2.3. Comment signaler le discours de haine

L'INACH est un réseau de premier plan au sein de l'UE et dans le monde entier qui œuvre à la lutte contre la cyberhaine. Il s'agit d'une fondation de droit néerlandais, basée à Amsterdam, qui compte 32 membres issus de 28 pays. Son site Web propose une plateforme de signalement en ligne pour dénoncer tout incident de cyberhaine. En plus d'offrir un service de plaintes et de signalement contre la cyberhaine, l'INACH utilise les données de toutes les plaintes reçues pour rédiger des rapports et des analyses. Ce faisant, l'INACH cherche à influencer le public, les entreprises de réseaux sociaux et les institutions internationales qui contribuent à faire pression sur la législation internationale contre la cyberhaine.

En plus de signaler des cas de cyberhaine via INACH, les utilisateurs peuvent également signaler directement tout incident de discours haineux par le biais du réseau social dans lequel ils le rencontrent. Le site web du Conseil de l'Europe fournit des informations sur la procédure de signalement les canaux des réseaux sociaux.[22]

[22] Signalement sur les plateformes des réseaux sociaux https://www.coe.int/fr/web/no-hate-campaign/reporting-on-social-media-platforms

Dans certains cas, il n'est pas nécessaire d'avoir un compte pour signaler un incident. Par exemple, sur Facebook, vous pouvez remplir un formulaire en ligne sans être inscrit ou connecté à un compte Facebook.

Certains pays européens ont mis en place des procédures et des mécanismes nationaux de signalement des discours de haine, des crimes de haine et de cyberharcèlement dans le cadre de la campagne « Mouvement contre le Discours de haine » du Conseil de l'Europe. Vous trouverez la liste des pays et leurs procédures signalement sur le site web du Conseil de l'Europe.
Voici d'autres suggestions pour signaler les discours de haine:

- Signaler le discours de haine à la police.
- Signaler à un organisme faisant autorité, par exemple, à un tribunal civil ou administratif.
- Par exemple, MiND est le centre national de signalement aux Pays-Bas pour les discours haineux et les contenus discriminatoires ;
- Parlez à quelqu'un en qui vous avez confiance, par exemple un parent, un ami, ou un enseignant.

3. Cybersécurité et confidentialité

3. CYBERSÉCURITÉ ET CONFIDENTIALITÉ

3.1. Pourquoi la protection des données à caractère personnel est-elle importante?

La notion de protection des données à caractère personnel est définie dans l'article 4, paragraphe 1, du Règlement général sur la protection des données: les données à caractère personnel constituent toutes les informations relatives à une personne physique identifiée ou identifiable.

'Les noms et les adresses e-mail sont évidemment des données personnelles. Les informations de localisation, l'origine ethnique, le sexe, les données biométriques, les croyances religieuses, les cookies Web et les opinions politiques peuvent également constituer des données personnelles. Dans les paragraphes suivants, nous explorerons plus en détail les types de données qui nécessitent une protection.'

La protection des données est importante, car elle empêche l'utilisation abusive des informations d'une personne ou d'une organisation, elle vise à éviter différents dangers de confidentialité et de sécurité, tels que les activités frauduleuses, le piratage, le phishing (ou hameçonnage) et l'usurpation d'identité (décrit dans la section suivante).

Le type de données qui nécessitent une protection:

Les informations essentielles telles que **les noms, les adresses, les adresses e-mail, les numéros de téléphone, les informations de santé ou les coordonnées bancaires** sont toutes des données qui doivent être soigneusement stockées et protégées. Si de telles informations tombent entre de mauvaises mains, elles peuvent compromettre la sécurité des personnes sous de nombreuses formes, y compris l'intégrité personnelle, la sécurité physique et la sécurité financière. Les informations volées peuvent également être utilisées pour créer de faux profils et commettre des fraudes.

Voici des exemples de données à caractère personnel:

- Un prénom et un nom de famille ;
- Une adresse de domicile ;
- Une adresse électronique telle que name.surname@company.com ;
- Un numéro de carte d'identité ;
- Données de localisation (par exemple, la fonctionnalité de localisation sur un téléphone portable) * ;
- Une adresse IP (Internet Protocol) ;
- Un identifiant de cookie* ;
- L'identifiant publicitaire de votre téléphone ;
- Données détenues par un hôpital ou un médecin, qui peuvent être un élément permettant d'identifier une personne de manière unique.

Voici des exemples de données qui ne sont pas considérées comme des données à caractère personnel:

- Un numéro d'immatriculation de société ;
- Une adresse électronique telle que info@company.com ;
- Des données anonymes, soit les données à caractère personnel rendues anonymes de sorte que la personne ne soit plus identifiable ou ne sont plus considérées comme des données à caractère personnel. Pour que les données soient réellement anonymes, l'anonymisation doit être irréversible.

Qui est responsable de la protection de nos données?

La protection des données est un moyen de protéger les informations importantes de la corruption, la compromission ou la perte. La protection des données est d'autant plus importante que la quantité de données créées et stockées ne cesse de croître à un rythme sans précédent.

Par conséquent, les organisations qui stockent et gèrent des informations personnelles doivent garantir qu'elles sont protégées contre la corruption, la compromission ou les pertes.

Dans l'Union européenne, le règlement général sur la protection des données (RGPD) (https://gdpr-info.eu/) protège les données à caractère personnel des citoyens de l'UE. Il s'agit de la loi sur la confidentialité et la sécurité la plus stricte au monde. Bien qu'elle ait été rédigée et adoptée par l'Union européenne (UE), elle impose des obligations aux organisations où qu'elles soient, tant qu'elles visent ou collectent des données relatives à des personnes de l'UE. Le règlement est entré en vigueur le 25 mai 2018.

Éléments clés de la protection des données

Un modèle très important de protection des données est la triade de la CIA, où les trois lettres du nom représentent les trois éléments de la protection des données: confidentialité (*confidentiality*), intégrité (*integrity*) et disponibilité (*availability*). Ce modèle a été développé pour aider les personnes et les organisations à développer une approche holistique de la protection des données. Les trois éléments sont définis de telle sorte:

- Confidentialité: Les données ne sont récupérées que par des opérateurs autorisés disposant d'informations d'identification appropriées.
- Intégrité: Toutes les données stockées au sein d'une organisation sont fiables, précises et ne font l'objet d'aucune modification injustifiée.
- Disponibilité: Les données stockées sont sûres et facilement disponibles chaque fois que cela est nécessaire.

Selon le règlement général sur la protection des données, il existe également plusieurs principes de protection des données à caractère personnel que les organisations responsables doivent respecter:

- **Légalité, équité et transparence:** le traitement doit être légal, équitable et transparent pour la personne concernée.
- **Limitation de la finalité:** le responsable du traitement doit traiter les données aux fins légitimes spécifiées explicitement à la personne concernée lorsque vous les avez collectées.
- **Minimisation des données:** le responsable du traitement ne devrait collecter et traiter que les données absolument nécessaires aux fins spécifiées.

- **Exactitude:** le responsable du traitement doit garder les données à caractère personnel exactes et à jour.
- **Limitation du stockage:** le responsable du traitement ne peut stocker des données d'identification personnelle que pendant la durée nécessaire pour réaliser l'objectif spécifié.
- **Intégrité et confidentialité:** le traitement doit être effectué de manière à assurer la sécurité, l'intégrité et la confidentialité appropriées (par exemple en utilisant le cryptage).
- **Responsabilité:** le responsable du traitement des données doit être en mesure de pouvoir démontrer la conformité au RGPD de tous ces principes.

L'importance de la protection des données augmente alors que la quantité de données créées et stockées ne cesse de croître à un rythme sans précédent. La tolérance pour les périodes de non-fonctionnement susceptibles de rendre impossible l'accès à des informations importantes est minime.

Comme expliqué ci-dessus, les organisations qui collectent, stockent et gèrent les données personnelles sont responsables de garantir que ces données ne sont pas utilisées à mauvais escient et qu'elles sont à la disposition du personnel autorisé à tout moment. Le RGPD le garantit au moyen d'exigences juridiques et de sanctions concrètes pour les organisations qui ne les respectent pas. De plus, les individus peuvent préserver la sécurité de leurs données contre les tentatives non souhaitées d'accès à leurs données par des tiers, ainsi que protéger leur vie privée contre les personnes avec lesquelles ils ne consentent pas à partager leurs informations personnelles.

3.2. Types de menaces et de crimes liés aux données personnelles et à la vie privée.

- **Usurpation d'identité**

L'usurpation d'identité **est un crime qui consiste à obtenir les renseignements personnels ou financiers d'une autre personne dans le but d'utiliser son identité et ensuite commettre une fraude**, par exemple, en effectuant des transactions ou des achats non autorisés.

L'usurpation d'identité est commise de différentes manières et ses victimes se retrouvent généralement avec des dommages à leur crédit, à leurs finances et à leur réputation.

L'usurpateur d'identité peut utiliser vos renseignements pour demander un crédit, remplir une déclaration d'impôt ou obtenir des services médicaux. Ces actes peuvent nuire à votre statut de crédit et vous coûter du temps et de l'argent pour retrouver votre réputation.

L'usurpation d'identité se produit lorsque quelqu'un vole vos informations personnelles, telles que votre numéro de sécurité sociale, votre numéro de compte bancaire ou vos informations de carte de crédit. Cet acte peut être commis de différentes manières. Certains usurpateurs d'identité passent au crible les poubelles à la recherche de compte bancaire et de relevés de carte de crédit. D'autres méthodes plus sophistiquées permettent d'accéder aux bases de données des entreprises pour voler des listes d'informations sur les clients. Une fois que les usurpateurs disposent des informations qu'ils recherchent, ils peuvent ruiner la cote de crédit d'une personne et la réputation d'autres informations personnelles.

Les usurpateurs d'identité utilisent de plus en plus la technologie informatique pour obtenir les renseignements personnels d'autres personnes dans le but de commettre des fraudes d'identité. Pour trouver de telles informations, ils peuvent fouiller les disques durs d'ordinateurs volés ou jetés; pirater des ordinateurs ou des réseaux informatiques; accéder aux documents publics informatisés; utiliser des logiciels malveillants de collecte d'informations pour infecter les ordinateurs; parcourir les sites de réseaux sociaux ; ou utilisez des adresses e-mail ou des messages frauduleux.

Types d'usurpation d'identité

Usurpation d'identité à caractère financier

Dans ce cas-ci**, une personne utilise l'identité ou les informations d'une autre personne pour obtenir des crédits, des biens, des services ou des avantages**. Il s'agit la forme la plus courante de vol d'identité.

Usurpation d'identité liée à la sécurité sociale

Si les usurpateurs d'identité obtiennent votre numéro de sécurité sociale, ils peuvent l'utiliser pour demander des cartes de crédit et des prêts et ne pas payer les soldes impayés. Les fraudeurs peuvent également utiliser votre numéro pour recevoir des indemnités médicales, d'invalidité et autres.

Usurpation d'identité pour des raisons médicales

Dans ce cas-ci, une personne se fait passer pour une autre personne pour obtenir des soins médicaux gratuits.

Usurpation d'identité synthétique

L'usurpation d'identité synthétique est un type de fraude dans lequel **un criminel combine des informations réelles (généralement volées) et fausses pour créer une nouvelle identité, qui sera ensuite utilisée pour ouvrir des comptes et réaliser des achats frauduleux.** L'usurpation d'identité synthétique permet au criminel de voler de l'argent à des sociétés de cartes de crédit ou aux prêteurs qui accordent un crédit basé sur la fausse identité.

Usurpation d'identité de mineurs

Dans ce cas-ci, quelqu'un utilise l'identité d'un enfant pour diverses formes de gain personnel. Cette pratique est courante, car les enfants n'ont généralement pas d'informations qui pourraient représenter un obstacle au fraudeur.

Celui-ci peut utiliser le nom de l'enfant et le numéro de sécurité sociale pour obtenir une résidence, trouver un emploi, obtenir des prêts ou éviter une arrestation suite à un mandat d'arrêt non exécuté. **Souvent, la victime est un membre de la famille, l'enfant d'un ami ou une autre personne proche de l'auteur.** Certaines personnes volent même les informations personnelles d'êtres chers décédés.

Usurpation d'identité à des fins fiscales

L'usurpation d'identité à des fins fiscales se produit lorsque quelqu'un utilise vos informations personnelles, y compris votre numéro de sécurité sociale, **pour produire une fausse déclaration fiscale en votre nom et obtenir un remboursement.**

Usurpation d'identité dans le cadre pénal

Dans ce cas-ci, **un criminel se présente comme une autre personne lors d'une arrestation** pour tenter d'éviter une citation à comparaître, d'empêcher la découverte d'un mandat acté en son vrai nom, ou d'éviter une arrestation ou un casier judiciaire.

Usurpation d'identité relative au chômage

Quelqu'un utilise vos renseignements personnels pour demander (et recevoir) des prestations de chômage.

- **Harcèlement sexuel en ligne**

Le harcèlement sexuel en ligne est défini comme un **comportement sexuel non désiré sur n'importe quelle plateforme numérique et il est reconnu comme une forme de violence sexuelle.**

Le harcèlement sexuel en ligne englobe un large éventail de comportements où des contenus numériques sont utilisés (images, vidéos, publications, messages, pages) sur une variété de plateformes (privées ou publiques). Le harcèlement sexuel en ligne peut entraîner un sentiment de menace, d'exploitation, de pression, d'humiliation, de bouleversement, de sexualisation ou de discrimination à l'égard d'une personne.

Types de harcèlement sexuel en ligne:

Partage d'images et de vidéos intimes sans consentement

Les images et vidéos à caractère sexuel d'une personne sont partagées ou prises sans son consentement. Cela comprend une série de comportements, tels que:

- Images/vidéos à caractère sexuel prises sans consentement (pratique appelée « creep shots » ou encore « upskirting »)
- Images/vidéos sexuelles prises avec le consentement de la personne, mais partagées sans son consentement (« revenge porn » ou « pornodivulgation »)
- Actes sexuels non consentis (par exemple, le viol) enregistrés numériquement (et potentiellement partagés)

Exploitation, contraintes et menaces

Situation où une personne reçoit des menaces sexuelles, et est contrainte de participer à un comportement sexuel en ligne ou fait du chantage avec du contenu sexuel. Cela comprend une série de comportements, tels que:

- Harceler ou faire pression sur une personne sur internet pour qu'elle partage des images sexuelles d'elle-même ou se livre à un comportement sexuel en ligne (ou hors ligne).
- Utiliser la publication de contenu sexuel (images, vidéos, rumeurs) pour menacer, contraindre ou faire chanter quelqu'un (« sextortion »).
- Écrire des menaces de nature sexuelle sur internet (par exemple, menaces de viol) ;
- Inciter d'autres personnes à commettre des violences sexuelles en ligne.
- Inciter quelqu'un à participer à un comportement sexuel et ensuite en partager les preuves.

Harcèlement à caractère sexuel

Une personne est prise pour cible par un groupe ou une communauté et en est systématiquement exclue à cause d'un contenu sexuel qui l'humilie, la bouleverse ou la discrimine. Cela comprend une série de comportements, tels que:

- Les commérages, rumeurs ou mensonges sur le comportement sexuel publiés en ligne, soit en nommant directement quelqu'un, soit en faisant indirectement allusion à quelqu'un.
- Le langage à caractère sexuel offensant ou discriminatoire et les injures en ligne.
- Usurper l'identité de quelqu'un et porter atteinte à sa réputation en partageant des contenus sexuels ou en harcelant sexuellement d'autres personnes.
- Partage non consenti d'informations personnelles en ligne pour favoriser le harcèlement sexuel (pratique appelée « doxing » ou « divulgation de données personnelles »).
- Être victime d'intimidation en raison de son genre et/ou de son orientation sexuelle réelle ou présumée.
- Le « body shaming », pratique qui consiste à critiquer quelqu'un pour son apparence physique.
- Forcer une personne à rendre publique son orientation sexuelle ou son identité de genre sans son consentement.

Sexualisation non désirée

Situation où une personne reçoit des demandes sexuelles, des commentaires et du contenu indésirable. Cela comprend une série de comportements, tels que:

- Commentaires à caractère sexuel (par exemple sur des photos) ;
- Campagnes virales à caractère sexuel qui incitent à la participation ;
- L'envoi de contenu sexuel à quelqu'un (images, emojis, messages) sans son consentement ;
- Avances sexuelles malvenues ou demandes de faveurs sexuelles ;

- « Blagues » de nature sexuelle ;
- Évaluer le degré d'attractivité ou d'activité sexuelle d'une autre personne ;
- Modifier les images d'une personne pour leur donner un aspect plus sexuel.

Ce type de harcèlement peut donner à la victime un des sentiments de:

- Menace ou de peur
- Abus
- Pression
- Violation de sa dignité
- Humiliation ou de dégradation
- Honte ou de jugement
- Bouleversement
- Sexualisation
- Discrimination en raison de leur genre ou de leur orientation sexuelle
- Culpabilité ou de responsabilité

L'expérience et les conséquences du harcèlement sexuel en ligne sont propres à chaque personne et peuvent être ressenties à la fois à court terme, mais peuvent également avoir des répercussions à long terme sur la santé mentale et le bien-être. Les conséquences à long terme peuvent être amplifiées par une nouvelle victimisation, par exemple si le contenu est partagé en ligne une nouvelle fois, ou parce que le traumatisme initial de l'incident refait surface beaucoup plus tard. Il est important de reconnaître qu'il n'y a pas qu'une seule et même façon pour une jeune personne d'être victime de harcèlement sexuel en ligne et que cela peut également affecter les autres personnes qui en sont témoins.

- **Phishing (ou hameçonnage)**

Les attaques de phishing sont **une pratique qui consiste à envoyer des communications frauduleuses qui semblent provenir d'une source fiable**. Cette attaque est généralement réalisée par e-mail.

L'objectif est de voler des données sensibles telles que les cartes de crédit et les informations de connexion ou d'installer des logiciels malveillants sur l'ordinateur de la victime. Le phishing est un mode de cyberattaque courant que chacun devrait connaître afin de se protéger.

Parfois, les hackers se contentent d'obtenir vos données personnelles et vos informations de carte de crédit pour en tirer un profit financier. Dans d'autres cas, les e-mails de phishing sont envoyés pour recueillir les informations de connexion des employés ou d'autres détails qui seront utilisés dans des attaques plus malveillantes contre quelques personnes ou une entreprise spécifique.

Le phishing commence par un e-mail frauduleux ou toute autre communication destinée à attirer la victime. Le message est présenté comme provenant d'un expéditeur de confiance. S'il réussit à tromper sa victime, celle-ci est amenée à fournir des informations confidentielles, souvent sur un site Web illégal. Parfois, des logiciels malveillants sont également téléchargés sur l'ordinateur de la cible.

Les cybercriminels commencent par identifier un groupe d'individus qu'ils veulent cibler. Ensuite, **ils créent des e-mails et des messages texte qui semblent légitimes, mais contiennent en fait des liens dangereux, des pièces jointes ou des leurres qui incitent leurs cibles à entreprendre une action inconnue et risquée.**

Dans les risques liés au phising, on trouve notamment:

- Le vol d'argent de votre compte bancaire
- Des débits frauduleux sur les cartes de crédit
- La perte d'accès à des photos, vidéos et fichiers
- De faux messages sur les réseaux sociaux publiés depuis votre compte
- Des Cybercriminels se font passer pour vous auprès d'un ami ou un membre de votre famille, les mettant ainsi en danger

En bref:

- **Les phishers utilisent fréquemment des émotions comme la peur, la curiosité, l'urgence et la cupidité pour inciter les destinataires à ouvrir des pièces jointes ou à cliquer sur des liens.**
- **Les attaques de phishing sont conçues pour sembler provenir d'entreprises et de personnes légitimes.**
- Les cybercriminels innovent en permanence et deviennent de plus en plus sophistiqués.
- Il suffit d'une attaque de phishing réussie pour compromettre votre réseau et voler vos données, c'est pourquoi **il est toujours important de "réfléchir avant de cliquer".**

Afin d'éviter le phishing, l'entreprise informatique américaine CISCO (https://www.netacad.com/) donne les conseils suivants:

1. **Évitez les expéditeurs inconnus.** Vérifiez les noms et les adresses e-mail avant de répondre ;
2. Ne faites pas confiance aux liens ou **pièces jointes dans les spams.**
3. **Méfiez-vous des e-mails avec l'objet "urgent".**
4. Méfiez-vous des messages avec des **erreurs d'orthographe ou de grammaire.**
5. **Ne vous laissez pas séduire par des "offres".** Elles sont généralement trop belles pour être varies.
6. **Envisagez d'utiliser un fournisseur de messagerie sécurisée**.
7. **Ne donnez jamais d'informations personnelles ou financières** pour donner suite à une demande dans un e-mail.
8. Lorsque vous recevez un e-mail d'une institutions connues (gouvernement, banques, votre médecin), **allez directement à la source au lieu de cliquer sur les liens dans l'e-mail.**
9. **Méfiez-vous des salutations génériques, telles que "Cher monsieur" ou "Chère madame".**
10. Assurez-vous de comprendre **la politique de votre fournisseur de services en matière de suivi et d'arrêt du phishing.**
11. Ne donnez pas accès à votre ordinateur à un inconnu ou à une aide non sollicitée.

- **<u>Fraudes et escroqueries sur Internet</u>**

La fraude sur Internet consiste à utiliser **des services en ligne et des logiciels ayant accès à Internet pour escroquer ou profiter des victimes.** Le terme « fraude sur Internet » recouvre généralement les pratiques cybercriminelles qui se produisent sur Internet ou par e-mail, y compris les crimes tels que l'usurpation d'identité, le phishing et d'autres activités de piratage conçues pour escroquer les gens.

Les escroqueries sur Internet qui ciblent les victimes à travers des services en ligne représentent des millions de dollars d'activités frauduleuses par an, et les chiffres ne cessent d'augmenter à mesure que l'utilisation d'Internet se développe et que les techniques cybercriminelles deviennent plus sophistiquées.

Les cybercriminels utilisent divers supports et stratégies d'attaque pour réaliser des fraudes sur Internet. Dans ces supports, **on trouve notamment des logiciels malveillants, des services d'adresses e-mail et de messagerie instantanée pour diffuser ces logiciels malveillants, des sites Web piratés qui volent les données des utilisateurs, ainsi que des escroqueries par hameçonnage complexes et de grandes envergures.**

La fraude sur Internet peut être divisée en plusieurs types d'attaques clés, notamment:

Phishing (expliqué en détail ci-dessus) : l'utilisation d'e-mail et de messagerie en ligne pour inciter les victimes à partager des données personnelles, des identifiants de connexion et des détails financiers;
Violation de données: le vol de données confidentielles, protégées ou sensibles d'un emplacement sécurisé et les transférer dans un environnement non fiable. Cela inclut les données volées aux utilisateurs et aux organisations;
Déni de service (DoS): interruption de l'accès du trafic à un service, un système ou un réseau en ligne pour provoquer une action malveillante;
Logiciels malveillants: l'utilisation de logiciels malveillants pour endommager ou désactiver les appareils des utilisateurs ou voler des données personnelles et sensibles;

Ransomware: il s'agit d'un type de malware qui empêche les utilisateurs d'accéder aux données essentielles et qui ensuite exige un paiement contre la promesse de restaurer l'accès. Les ransomwares sont généralement transmis via des attaques de phishing.
Le Business Email Compromise (BEC): il s'agit d'une forme complexe d'attaque visant les entreprises qui effectuent fréquemment des paiements par virement. Cet acte compromet les vraies adresses e-mail grâce à des techniques d'ingénierie sociale pour soumettre des paiements non autorisés.

Voici quelques exemples:

- **Arnaques dans les cartes de vœux**

De nombreuses escroqueries sur Internet se concentrent sur des événements populaires pour escroquer les personnes qui les célèbrent. Il s'agit notamment des anniversaires, de Noël et de Pâques, événements généralement marqués par l'envoi de cartes de vœux par email aux amis et aux membres de la famille. Les hackers profitent généralement de cette situation en installant un logiciel malveillant dans une carte de vœux électronique, qui se télécharge et s'installe sur l'appareil du destinataire lorsqu'il ouvre la carte de vœux.

- **Escroqueries par carte de crédit**

La fraude par carte de crédit se produit généralement lorsque des hackers acquièrent frauduleusement les coordonnées de cartes de crédit ou de débit de personnes dans le but de voler de l'argent ou de faire des achats.

Pour obtenir ces données, les escrocs utilisent souvent des offres de cartes de crédit ou de prêts bancaires trop beaux pour être vrais, afin d'attirer les victimes. Par exemple, une victime peut recevoir un message de sa banque lui disant qu'elle peut bénéficier d'une offre de prêt spéciale ou qu'une importante somme d'argent a été mise à sa disposition sous forme de prêt.

Ces escroqueries ne cessent de tromper les consommateurs, malgré la prise de conscience générale que de telles offres sont trop belles pour être vraies, et ce pour une bonne raison.

- **Escroqueries sur les sites de rencontre en ligne**

Un autre exemple typique de fraude sur Internet concerne la multitude d'applications et de sites de rencontres en ligne. Les hackers se concentrent sur ces applications pour inciter les victimes à envoyer de l'argent et à partager des données personnelles avec leurs nouveaux partenaires. Les escrocs créent généralement de faux profils pour interagir avec les utilisateurs, développer une relation, gagner lentement leur confiance, créer une histoire fictive et demander à l'utilisateur une aide financière.

- **Escroqueries sur les frais de loterie**

Une autre forme courante de fraude sur Internet est l'escroquerie par e-mail qui annonce aux victimes qu'elles ont gagné à la loterie. Ces arnaques informent les destinataires qu'ils ne peuvent réclamer leur prix qu'après avoir payé une petite somme.
Les escrocs des frais de loterie rédigent généralement leurs e-mails de manière à ce qu'ils semblent crédibles, ce qui n'empêche pas de nombreuses personnes de tomber dans le panneau. L'escroquerie cherche à faire croire aux victimes que leur rêve de gagner de grosses sommes d'argent est devenu réalité, même si elles n'ont jamais acheté de billet de loterie. Par ailleurs, aucune loterie légitime ne demande aux gagnants de payer pour recevoir leur prix.

- **Le prince du Nigéria**

Tactique classique de fraude sur Internet, la méthode d'escroquerie du prince nigérian reste courante et florissante malgré une grande sensibilisation.

L'arnaque utilise le scénario d'une riche famille ou d'une personne nigériane qui souhaite partager sa richesse en échange d'une aide pour accéder à son héritage. Elle utilise des tactiques de phishing pour envoyer des e-mails qui décrivent une histoire émouvante, puis attire les victimes en leur promettant une récompense financière importante.

L'escroquerie commence généralement par une demande de petite somme pour l'aider dans ses démarches juridiques et administratives, suivies de la promesse d'une grosse somme d'argent plus tard.

L'escroc demandera inévitablement des frais plus importants pour couvrir d'autres tâches administratives et des frais de transaction, accompagnés de documents de certification à l'apparence authentique. Cependant, le retour sur investissement promis n'arrive jamais.

Conseils pour éviter les fraudes et les escroqueries sur Internet:

Il est essentiel de ne jamais envoyer d'argent à une personne rencontrée sur Internet, de ne jamais partager des détails personnels ou financiers avec des personnes qui ne sont pas légitimes ou dignes de confiance, et de ne jamais cliquer sur des hyperliens ou des pièces jointes dans des e-mails ou des messages instantanés. Une fois touchés, les internautes devraient signaler l'activité des arnaqueurs sur internet et les emails de phishing aux autorités.

La fraude par carte de crédit peut également être évitée en gardant un œil attentif sur ses comptes bancaires, en mettant en place des notifications sur l'activité des cartes de crédit, en s'inscrivant à un service de surveillance du crédit et en utilisant des services de protection des consommateurs. Si un utilisateur est victime d'une fraude à la carte de crédit, il doit le signaler aux autorités judiciaires compétentes et aux agences d'évaluation du crédit.

Spam

Le spam est un **type de communication numérique non désirée et non sollicitée qui est envoyée massivement.** Le spam est souvent envoyé par e-mail, mais il peut aussi être distribué par des messages texte, des appels téléphoniques ou des réseaux sociaux.

Le spam n'est pas un acronyme pour désigner une menace informatique, bien que certains aient été proposés, par exemple, « stupid pointless annoying malware ». Le terme « spam » a été inspiré par un sketch des Monty Python dans lequel les acteurs déclarent que tout le monde doit manger la marque de corned-beef « spam », qu'il le veuille ou non.

De même, toute personne possédant une adresse e-mail doit malheureusement être dérangée par des messages de spam, que cela nous plaise ou non.

Les spammeurs utilisent de nombreuses formes de communication pour envoyer en masse leurs messages indésirables. Certains d'entre eux sont des messages de marketing colportant des produits non sollicités. D'autres types de spams peuvent propager des logiciels malveillants, vous inciter à divulguer des informations personnelles ou vous effrayer en pensant que vous devez payer pour vous sortir d'ennuis.

Les filtres antispam des e-mails interceptent beaucoup de ces types de messages, et les opérateurs téléphoniques vous avertissent souvent d'un « risque de spam » de la part d'appelants inconnus. Que ce soit par e-mail, par SMS, par téléphone ou par les réseaux sociaux, certains messages de spam arrivent à passer, et vous devez être capable de les reconnaître et de les éviter. Vous trouverez ci-dessous plusieurs types de spams dont il faut se méfier:

- E-mails de phishing (déjà décrits ci-dessus).
- **Usurpation d'e-mails:** les e-mails usurpés imitent, ou usurpent, un e-mail provenant d'un expéditeur légitime, et vous demandent d'effectuer une action quelconque. Les usurpations bien exécutées contiennent une marque et un contenu familiers, souvent ceux d'une grande entreprise bien connue comme PayPal ou Apple.
- **Les escroqueries du support technique:** dans une escroquerie du support technique, le message de spam indique que vous avez un problème technique et que vous devez contacter le service d'assistance technique en appelant le numéro de téléphone ou en cliquant sur un lien dans le message.
- **Le malspam:** abréviation de « malware spam » ou « malicious spam », le malspam est un message de spam qui envoie un malware sur votre appareil. Les lecteurs peu méfiants qui cliquent sur un lien ou ouvrent une pièce jointe se retrouvent avec un type de logiciel malveillant, notamment un rançongiciel, un cheval de Troie, un robot, un voleur d'informations, un cryptomineur, un logiciel espion ou un enregistreur de touches. L'une des méthodes les plus courantes consiste à inclure des scripts malveillants dans une pièce jointe de type familier, comme un document Word, un fichier PDF ou une présentation PowerPoint. Une fois la pièce jointe ouverte, les scripts s'exécutent et récupèrent la charge utile du malware.

- **Appels et textes indésirables**: avez-vous déjà reçu un appel automatique ? Il s'agit de spam téléphonique. Un message texte d'un expéditeur inconnu vous incitant à cliquer sur un lien inconnu? C'est ce qu'on appelle le spam par SMS ou « smishing », un mot-valise composé de « SMS » et de « phishing ».
  Si vous recevez des appels et des SMS indésirables sur votre Android ou votre iPhone, la plupart des grands opérateurs vous offrent la possibilité de les signaler. Le blocage des numéros permet également de lutter contre le spam mobile.

Cyberpiratage

Toute personne qui utilise un ordinateur connecté à internet est exposée aux menaces que représentent les pirates informatiques et les cyberprédateurs. Ces malfaiteurs en ligne utilisent généralement des escroqueries telles que le phishing, des spams ou des messages instantanés, ainsi que de faux sites web, et ce, dans le but de diffuser des logiciels malveillants dangereux sur votre ordinateur et de compromettre votre sécurité informatique.

Les pirates informatiques peuvent également essayer d'accéder directement à votre ordinateur et à vos informations privées si vous n'êtes pas protégé par un pare-feu. Ils peuvent surveiller vos conversations ou parcourir le back-end de votre site web personnel. Généralement déguisés sous une fausse identité, les prédateurs peuvent vous inciter à révéler des informations personnelles et financières confidentielles, ou bien pire encore.

Lorsque votre ordinateur est connecté à internet, le logiciel malveillant qu'un pirate a installé sur votre PC transmet discrètement vos informations personnelles et financières à votre insu et sans votre consentement. En outre, un cyberprédateur peut se jeter sur les informations privées que vous avez involontairement révélées. Dans les deux cas, ils pourront:

- Détourner vos noms d'utilisateur et mots de passe
- Voler votre argent et créer une carte de crédit et des comptes bancaires à votre nom
- Détruire votre réputation
- Demander de nouveaux numéros d'identification personnels (PIN) ou des cartes de crédit supplémentaire

- Effectuer des achats
- S'ajouter ou ajouter un pseudonyme qu'ils contrôlent en tant qu'utilisateur autorisé afin de faciliter l'utilisation de votre compte
- Obtenir des avances de fonds
- Utiliser et abuser de votre numéro de sécurité sociale
- Vendre vos informations à d'autres tiers qui les utiliseront à des fins illicites ou illégales

Afin de vous protéger de ces menaces, vous pouvez prendre les mesures suivantes:

1. **Vérifiez continuellement l'exactitude des comptes personnels et traitez immédiatement toute anomalie.**
2. Soyez **extrêmement prudent** lorsque vous entrez dans des salons de discussion ou que vous affichez des pages Web personnelles.
3. **Limitez les informations personnelles** que vous publiez sur vos pages Web personnelles.
4. Surveillez attentivement les demandes d'« ami » ou de connaissances en ligne pour le comportement abusive.
5. **Gardez vos informations personnelles et financières hors des conversations en ligne.**
6. Soyez **extrêmement prudent lorsque vous acceptez de rencontrer en personne un "ami"** ou une connaissance en ligne.
7. **Utilisez un pare-feu de nouvelle génération.**
8. **Mettez régulièrement à jour votre système d'exploitation**.
9. **Augmentez les paramètres de sécurité de votre navigateur.**
10. **Évitez les sites Web douteux.**
11. **Ne téléchargez que des logiciels à partir de sites auxquels vous faites confiance.** Évaluez soigneusement les logiciels gratuits et les applications de partage de fichiers avant de les télécharger.
12. **N'ouvrez pas les messages d'expéditeurs inconnus**.
13. **Supprimez immédiatement les messages que vous soupçonnez d'être un spam.**
14. Assurez-vous que les meilleurs logiciels de sécurité sont installés sur votre PC.
15. Utilisez une protection antivirus.
16. Utilisez une protection antispyware.

Cyberintimidation

La cyberintimidation désigne **l'utilisation d'Internet et d'autres technologies pour harceler ou traquer une autre personne en ligne.**

Ce harcèlement en ligne, qui est une extension du cyberharcèlement et du harcèlement en personne, peut prendre la forme d'e-mails, de messages texte, de messages sur les réseaux sociaux, etc., cette pratique est souvent méthodique, délibérée et continue.

La plupart du temps, les interactions ne se cessent pas, même si la victime exprime son mécontentement ou demande à la personne de s'arrêter. **Le contenu destiné à la victime est souvent inapproprié et parfois même troublant, ce qui peut donner à la personne un sentiment de peur, de détresse, d'anxiété et d'inquiétude.**

En ce qui concerne la cyberintimidation, les personnes qui la commettent utilisent une variété de tactiques et de techniques pour harceler, humilier, intimider et contrôler leurs victimes. En fait, beaucoup de ceux qui se livrent au cyberharcèlement sont doués pour la technologie et la créativité et trouvent une multitude de façons de tourmenter et de harceler leurs cibles. Voici quelques exemples de ce que peuvent faire les personnes qui pratiquent la cyberintimidation:

- **Publier des commentaires grossiers, offensants ou suggestifs en ligne ;**
- **Suivre la cible en ligne** en rejoignant les mêmes groupes et forums ;
- Envoyer des messages ou des **e-mails menaçants, autoritaires ou obscènes** ;
- Utiliser la technologie pour menacer ou faire chanter sa victime ;
- **Identifier la victime sur des publications de manière excessive**, même si elle n'a rien à voir avec celle-ci ;
- Commenter ou aimer tout ce que la victime poste ;
- **Créer de faux comptes pour suivre la cible sur les réseaux sociaux ;**
- Envoyer sans cesse des messages à la victime ;
- **Pirater ou détourner les comptes en ligne de la cible ;**
- Tenter d'obtenir des faveurs sexuelles ou de photos explicites ;
- Envoyer des cadeaux ou des objets non sollicités à la cible ;

- **Publier des informations confidentielles en ligne ;**
- Publier ou diffuser des photos réelles ou fausses de la cible ;
- **Bombarder la victime avec des photos sexuellement explicites d'eux-mêmes ;**
- Créer de faux messages destinés à humilier à la victime ;
- Suivre les mouvements en ligne de la cible en installant des dispositifs de suivi ;
- **Pirater l'appareil photo de la victime sur leur ordinateur portable ou son smartphone afin de la filmer secrètement ;**
- Continuer à harceler même après avoir été prié d'arrêter.

Tout comme le harcèlement, le cyberharcèlement peut avoir un large éventail de conséquences physiques et psychologiques sur les personnes visées. Par exemple, il n'est pas rare que les personnes harcelées en ligne ressentent de la colère, de la peur et de la confusion. Elles peuvent aussi avoir du mal à dormir et même se plaindre de problèmes d'estomac.

Les moyens de lutter contre la cyberintimidation sont très similaires à ceux recommandés pour prévenir d'autres cybermenaces, car elles sont toutes liées et fonctionnent de manière similaire. Voici quelques-uns de ces conseils:

Créez des mots de passe forts. Assurez-vous d'avoir des mots de passe forts pour tous vos comptes en ligne ainsi que des mots de passe forts pour vos appareils. Ensuite, programmez un rappel sur votre téléphone pour changer régulièrement vos mots de passe. Choisissez des mots de passe difficiles à deviner, mais faciles à retenir pour vous.
Veillez à vous déconnecter à chaque fois. Cela peut sembler fastidieux, mais veillez à vous déconnecter de votre boîte mail, de vos comptes sur les réseaux sociaux et de vos autres comptes en ligne après les avoir utilisés. Ainsi, si quelqu'un parvenait à s'introduire dans votre appareil, il n'aurait pas facilement accès à vos comptes.

- **Surveillez vos appareils.** Ne laissez pas votre téléphone sur votre bureau au travail ou ne vous éloignez pas d'un ordinateur portable ouvert. Il suffit d'une minute ou deux pour que quelqu'un installe un dispositif de localisation ou pirate votre appareil. **Veillez donc à garder vos dispositifs en votre possession ou à les sécuriser d'une manière ou d'une autre.**

- **Soyez prudent avec le wifi public**. Sachez que si vous utilisez le wifi public dans les hôtels ou au café du coin, vous vous exposez à des risques de piratage. Essayez de vous abstenir d'utiliser le wifi public ou investissez dans un VPN.
- **Adoptez des habitudes de sécurité en ligne.** En d'autres termes, faites-vous une priorité d'accepter uniquement les demandes d'amis de personnes que vous connaissez et gardez vos publications privées. Vous devriez également envisager d'avoir une adresse e-mail réservée à votre activité en ligne. Utilisez cette adresse lorsque vous faites vos achats en ligne ou que vous vous inscrivez à des programmes de fidélité.
- **Profitez des paramètres de sécurité.** Passez en revue chacun de vos comptes en ligne et plus particulièrement vos comptes sur les réseaux sociaux ; assurez-vous que vous utilisez les paramètres de confidentialité les plus stricts possibles. Vous pouvez même définir des paramètres qui empêchent les internautes de vous taguer ou de publier des photos de vous sans autorisation.
- **Créez des pseudonymes génériques.** Plutôt que d'utiliser votre nom complet en ligne, envisagez de créer un pseudonyme ou un nom sans genre. Ainsi, il sera plus difficile pour les internautes de vous retrouver. Vous devriez également laisser en blanc les sections facultatives, comme votre date de naissance ou votre ville natale.
- **Gardez des emplacements sécurisés**. Pensez à désactiver les paramètres de géolocalisation dans les photos. Vous devriez également vous abstenir de publier votre position en temps réel et publier plutôt des photos montrant où vous avez été a posteriori.
- **Soyez prudent avec les sites de rencontres en ligne**. Évitez d'utiliser votre nom complet sur ces sites. Vous devriez également éviter de communiquer des informations personnelles telles que votre nom de famille, votre adresse, votre adresse e-mail et votre numéro de téléphone avant de rencontrer quelqu'un en personne et d'établir un niveau de confiance.
- **Effectuez un contrôle des réseaux sociaux**. C'est toujours une bonne idée de passer en revue vos comptes sur les réseaux sociaux et de supprimer les photos ou les publications qui donnent trop d'informations sur vous ou qui créent une image que vous ne voulez pas diffuser.

- N’oubliez pas non plus que, même si vous avez bloqué une personne sur les réseaux sociaux, elle peut toujours voir votre compte en utilisant le compte d’une autre personne ou en créant un faux profil.

Les moyens de faire face à la cyberintimidation, au cas où cela se produirait déjà, sont notamment:

- **Dites à la personne d’arrêter.** Répondez une seule fois à la personne qui vous harcèle et dites-lui d’arrêter de vous contacter. Vous n’avez pas besoin de dire quoi que ce soit de précis ou d’expliquer votre réponse, demandez-lui simplement de ne plus jamais vous contacter.
- **Bloquez la personne.** Assurez-vous de bloquer la personne qui vous harcèle en ligne à partir de tous vos comptes. Vous devriez les bloquer sur les réseaux sociaux et sur votre smartphone.
- **Refusez de répondre à tout contact.** Si la personne qui vous harcèle continue à trouver des moyens de vous contacter, ne répondez pas à ce qu’elle publie ou vous envoie.
- **Changez d’adresse e-mail et de pseudonymes.** Envisagez d’obtenir une nouvelle adresse e-mail et de changer vos pseudonymes en ligne afin qu’il soit plus difficile pour la personne qui vous harcèle de vous atteindre.

Si vous avez demandé à la personne qui vous harcèle d’arrêter et que son comportement persiste, il est important de prendre des mesures à son encontre. Vous devez par exemple contacter les autorités compétentes et recueillir des preuves de ses agissements. **Vous pouvez également envisager de prendre contact avec un avocat.**

Les forces de l’ordre de votre région peuvent vous indiquer si vous pouvez faire autre chose pour garantir votre sécurité. Voici les points clés qui devront être abordés lorsque vous agirez:

- **Conservez des preuves de tout ce dont vous êtes victime.** Même si vous avez envie de tout supprimer, il est important de conserver des copies de tout ce que la personne qui vous harcèle a envoyé. Faites une copie pour vous-même et une copie pour les forces de l’ordre.

- **Prévenez la police locale.** Il est important de prévenir la police et de déposer une plainte officielle si vous êtes victime de cyberharcèlement. Même s'ils ne peuvent rien faire dans l'immédiat, il est important d'avoir une plainte officielle dans le dossier si le comportement persiste ou s'intensifie.

- **Signalez-les au site ou au service qu'ils ont utilisé**. Si la personne qui vous harcèle vous a harcelé par l'intermédiaire de Facebook, Instagram, Twitter, Snapchat, YouTube, Gmail ou une autre méthode, informez les autorités compétentes de la situation. Bien souvent, ces organismes prennent les plaintes pour cyberharcèlement très au sérieux et traiteront le problème.

3.3 Comment signaler les menaces de cybersécurité sur les réseaux sociaux ou dans les institutions?

Tous les réseaux sociaux ont mis en place des procédures permettant de signaler différents types de menaces en matière de cybersécurité, notamment les discours de haine en ligne, l'usurpation d'identité, le harcèlement sexuel, la cyberintimidation, etc. Vous trouverez ci-dessous des informations sur certains des réseaux sociaux les plus fréquentés:

- **Facebook**

Les problématiques de sécurité sur Facebook sont classées en plusieurs catégories. Il peut s'agir d'un contenu abusif ou d'une page haineuse que vous souhaitez signaler, ou encore d'une personne qui se fait passer pour vous sur Facebook, etc. La meilleure solution pour signaler un contenu abusif ou un spam sur Facebook est d'utiliser le lien Signaler à côté du contenu lui-même.

Pour signaler un profil:

1. Accédez au profil que vous souhaitez signaler en cliquant sur son nom dans votre fil d'actualité ou en le recherchant ;
2. Cliquez sur « … » à droite et sélectionnez « signaler ce profil » ;

3. Pour donner votre avis, cliquez sur l'option qui décrit le mieux en quoi ce profil est contraire aux normes de la communauté, puis cliquez sur « suivant » ;
4. En fonction de vos remarques, vous pourrez ensuite soumettre un rapport à Meta. Pour certains types de contenu, Facebook ne vous demande pas de soumettre un rapport, mais il utilise vos commentaires pour aider ses systèmes à se perfectionner. Cliquez sur « terminer ».

Pour signaler une publication:

1. Allez sur la publication que vous voulez signaler.
2. Cliquez sur « … » en haut à droite de la publication.
3. Cliquez sur « signaler la publication ».
4. Pour donner votre opinion, cliquez sur l'option qui décrit le mieux la façon dont cet article va à l'encontre des normes communautaires de Facebook. Cliquez sur « suivant ».
5. En fonction de vos commentaires, vous pourrez alors soumettre un rapport à Meta. Pour certains types de contenu, Facebook ne vous demande pas de soumettre un rapport, mais il utilise vos commentaires pour aider ses systèmes à progresser. Cliquez sur « terminer ».

Pour signaler une photo ou une vidéo:

1. Cliquez sur la photo ou la vidéo pour l'agrandir. Si le profil est verrouillé et que vous ne pouvez pas afficher la photo en grand, cliquez sur « signaler la photo ».
2. Cliquez sur « … » à droite de la photo ou de la vidéo.
3. Cliquez sur « signaler la photo » s'il s'agit d'une photo, ou sur « signaler la vidéo » s'il s'agit d'une vidéo.
4. Sélectionnez l'option qui décrit le mieux le problème et suivez les instructions à l'écran.

Pour signaler un message qui va à l'encontre des normes communautaires de Facebook:

1. À partir de n'importe quelle page de Facebook, cliquez sur l'icône « Messenger » en haut à droite.
2. Ouvrez le message.

3. Si vous avez ouvert le message en tant que fenêtre contextuelle, cliquez sur l'icône de réglage ;
4. Cliquez sur « il y a un problème » ;
5. Pour donner votre opinion, cliquez sur l'option qui décrit le mieux la façon dont ce message va à l'encontre des normes communautaires de Facebook ;
6. En fonction de votre opinion, vous pourrez alors être en mesure de soumettre un rapport à Meta. Pour certains types de contenu, Facebook ne vous demande pas de soumettre un rapport, mais ils utilisent vos commentaires pour aider leurs systèmes à progresser.

<u>Pour signaler une page:</u>

1. Allez sur la page que vous souhaitez signaler en cliquant sur son nom dans votre fil d'actualité ou en le recherchant ;
2. Cliquez plus en dessous de la photo de couverture de la page ;
3. Sélectionnez « signaler la page » ;
4. Pour donner votre opinion, cliquez sur l'option qui décrit le mieux la façon dont cette page va à l'encontre des normes communautaires de Facebook ;
5. En fonction de votre opinion, vous pourriez alors être en mesure de soumettre un rapport à Meta. Pour certains types de contenu, Facebook ne vous demande pas de soumettre un rapport, mais ils utilisent vos commentaires pour aider leurs systèmes à s'améliorer.

<u>Pour signaler un groupe:</u>

1. Accédez au groupe que vous souhaitez signaler en cliquant sur son nom dans votre fil d'actualité ou en le recherchant ;
2. Cliquez plus en dessous de la photo de couverture du groupe ;
3. Sélectionnez « signaler un groupe ».

<u>Pour signaler un événement:</u>

1. À partir de votre fil d'actualité, cliquez sur « événements » dans le menu de gauche ;
2. Cliquez sur l'événement que vous voulez signaler ;

3. Cliquez sur « … » et sélectionnez « signaler l'événement ».
4. Pour donner votre opinion, cliquez sur l'option qui décrit le mieux la façon dont ce profil va à l'encontre des normes communautaires de Facebook ;
5. En fonction de votre opinion, vous pourrez alors être en mesure de soumettre un rapport à Meta. Pour certains types de contenu, Facebook ne vous demande pas de soumettre un rapport, mais ils utilisent vos commentaires pour aider leurs systèmes à progresser.

<u>Pour signaler un commentaire:</u>

1. Allez sur le commentaire que vous voulez signaler ;
2. Cliquez sur « … » à côté du commentaire ;
3. Cliquez sur « signaler ce commentaire ».
4. Pour donner votre opinion, cliquez sur l'option qui décrit le mieux la façon dont ce commentaire va à l'encontre des normes communautaires de Facebook. Si vous ne voyez pas d'options adaptées, cliquez sur « autre » pour en rechercher plus ;
5. En fonction de votre opinion, vous pourrez alors être en mesure de soumettre un rapport à Meta. Pour certains types de contenu, Facebook ne vous demande pas de soumettre un rapport, mais ils utilisent vos commentaires pour aider leurs systèmes à s'améliorer.

<u>Pour signaler une annonce sur Facebook:</u>

1. Accédez à l'annonce que vous souhaitez signaler en cliquant sur son nom dans votre fil d'actualité ou en la recherchant ;
2. Cliquez sur « … » à côté de l'annonce que vous souhaitez signaler ;
3. Cliquez sur « signaler l'annonce », puis suivez les instructions à l'écran.

- **Instagram**

Signaler une publication:

Si vous voyez une publication, un message ou un compte qui, selon vous, va à l'encontre des directives communautaires d'Instagram, vous pouvez le signaler. Vous pouvez signaler des éléments de contenu individuels en appuyant sur les trois points au-dessus d'une publication, en maintenant votre doigt sur un message ou en vous rendant sur un compte et pour le signaler directement à partir du profil. Pour plus d'informations, consultez les pages d'aide d'Instagram ici https://help.instagram.com/.

Signaler un compte:

Les comptes qui enfreignent les directives communautaires d'Instagram peuvent être signalés via l'application ou via le formulaire en ligne. Pour plus d'informations, vous pouvez consulter les pages d'aide Help Center.

Signaler un commentaire:

1. Si vous voyez un commentaire qui est un spam ou qui vise à vous intimider ou à harceler, vous ou quelqu'un d'autre, signalez-le.
2. Ouvrez la conversation dans l'application Instagram.
3. Appuyez et restez enfoncé sur le message que vous souhaitez signaler.
4. Appuyez sur « signaler ».
5. Sélectionnez la raison pour laquelle vous signalez le message, puis appuyez sur « envoyez le signalement ».
6. Pour plus d'informations, rendez-vous sur les pages d'aide Help Center.

Signaler un message:

Si vous recevez un message qui vous semble inapproprié, appuyez et maintenez le message pour le signaler. Pour plus d'informations, rendez-vous sur les pages d'aide Help Center.

Signaler une story:

1. Si vous voyez une story de quelqu'un et pensez que cela va à l'encontre des directives communautaires d'Instagram, vous pouvez la signaler.
2. Ouvrez la story;
3. Appuyez sur les 3 points en bas de la photo ou de la vidéo que vous souhaitez signaler.
4. Appuyez sur « signalez », puis suivez les instructions à l'écran.
5. Pour plus d'informations, rendez-vous sur les pages d'aide Help Center.

- **TikTok**

Si vous avez des questions, des préoccupations ou des problèmes concernant votre profil, vous pouvez trouver des informations et de l'aide ici TikTok Help Center (https://support.tiktok.com/en/). Dans la section « sécurité », vous pouvez cliquer sur « signaler un problème », « signaler une vidéo LIVE », « signaler commentaire LIVE », « signalez une vidéo », « signaler un commentaire », « signaler un message direct », « signaler un son », « signaler un hashtag », ou encore « signaler quelqu'un » https://privacytiktok.zendesk.com/hc/en-us/requests/new . Les étapes sont très faciles à suivre, il vous suffit de trouver l'option « signaler un problème » et suivre les instructions.

Pour toute question, préoccupation ou complication concernant la politique de confidentialité ou la cybercriminalité au sein de TikTok, vous pouvez trouver de l'aide ici. Vous serez redirigé vers un formulaire en ligne où vous pourrez solliciter des informations sur vos données, signaler une violation de la vie privée ou poser des questions sur un problème particulier de confidentialité.

- **Twitter**

Dans le Centre d'assistance de Twitter (https://help.twitter.com/en/safety-and-security), vous pouvez trouver des informations et de l'aide en cas de comptes volés ou piratés, mais aussi concernant la vie privée, les spams ou les faux comptes, les contenus sensibles et offensants, les comportements abusifs et leurs signalements.

Pour signaler un Tweet:

1. Accédez au Tweet que vous souhaitez signaler sur twitter.com ou depuis l'application Twitter pour iOS ou Twitter pour Android ;
2. Sélectionnez l'icône « … » ;
3. Sélectionnez le Tweet ;
4. Sélectionnez à qui s'adresse ce signalement : moi-même, une autre personne ou un groupe de personnes spécifique, ou tout le monde sur Twitter ;
5. Ensuite, Twitter vous demandera de fournir plus d'informations sur le problème que vous signalez. Twitter peut également vous demander de sélectionner des Tweets supplémentaires sur le compte que vous signalez afin qu'ils aient un meilleur contexte pour évaluer votre signalement ;
6. Twitter s'assurera ensuite de l'exactitude de vos informations en confirmant ce que vous signalez, ainsi que le contexte supplémentaire que vous avez partagé et les règles qui seraient enfreintes ;
7. Twitter inclura le texte des Tweets que vous avez signalés dans les e-mails de suivi et les notifications qui vous seront adressés. Pour ne pas recevoir ces informations, vous pouvez décocher la case située à côté de Mises à jour concernant ce signalement susceptible de montrer ces Tweets ;
8. Une fois que vous aurez soumis votre rapport, Twitter vous recommandera des mesures supplémentaires à adopter pour améliorer votre expérience sur Twitter.

Pour signaler un compte :

1. Allez dans le profil du compte et sélectionnez l'icône « … ».
2. Sélectionnez « signaler ».

3. Sélectionnez qui est la cible du compte: Moi-même, quelqu'un d'autre, ou un groupe de personnes.
4. Ensuite, Twitter vous demandera de fournir des informations supplémentaires sur le problème que vous signalez. Ils peuvent également vous demander de sélectionner des Tweets à partir de ce compte afin qu'ils aient un meilleur contexte pour évaluer votre signalement.
5. Twitter s'assurera ensuite de l'exactitude de vos informations en confirmant ce que vous signalez, ainsi que le contexte supplémentaire que vous avez partagé et les règles qui seraient enfreintes.
6. Twitter inclura le texte des Tweets que vous avez signalés dans les e-mails de suivi et les notifications qui vous seront adressés. Pour ne pas recevoir ces informations, vous pouvez décocher la case située à côté de Mises à jour concernant ce signalement susceptible de montrer ces Tweets.
7. Une fois que vous avez envoyé votre signalement, Twitter vous recommandera des mesures supplémentaires à adopter pour améliorer votre expérience sur Twitter.

<u>Pour signaler un message ou une conversation :</u>

1. Sélectionnez la conversation dans vos messages privés et trouvez le message que vous souhaitez signaler. (Pour signaler l'intégralité de la conversation, cliquez sur l'icône « … »).
2. Sélectionnez l'icône d'information « i » et sélectionnez « signaler @username » ;
3. Si vous sélectionnez « les propos tenus sont inappropriés ou dangereux », Twitter vous demandera de fournir des informations supplémentaires sur le problème que vous signalez. Ils peuvent également vous demander de sélectionner des messages supplémentaires à partir du compte que vous signalez afin qu'ils aient un meilleur contexte pour évaluer votre signalement.
4. Une fois que vous avez envoyé votre signalement, Twitter vous recommandera des mesures supplémentaires à adopter pour améliorer votre expérience sur Twitter.

- **Quand est-ce considéré comme un crime?**

<u>En Espagne:</u>

En Espagne, **les sanctions des délits de cybersécurité vont de cinq ans de prison à des amendes pouvant aller jusqu'à 2.700 €.**

Le harcèlement devient un crime lorsque quelqu'un réduit de façon répétitive le sentiment de sécurité d'une personne et lorsqu'il fait en sorte que la victime se sente humiliée, insultée, menacée. Sans surprise, toute personne qui commet ce délit doit faire face à plusieurs sanctions allant de trois mois à deux ans d'emprisonnement ou au paiement d'une amende à la victime ; il s'agit d'un montant journalier fixé par les juges. Une amende journalière de 15 € pendant six mois représente un total de 2.700 €.

La **divulgation de secrets** a également des conséquences en Espagne puisqu'il s'agit d'un crime grave. Toute personne qui, « sans l'autorisation de la personne concernée, diffuse, divulgue ou transfère à des tiers des images ou des enregistrements audiovisuels » peut également être passible d'une peine d'emprisonnement ou d'amendes. La diffusion d'images à caractère sexuel est encore plus grave et peut avoir d'autres conséquences.

Par ailleurs, il est nécessaire de mentionner **l'usurpation d'identité**. Il s'agit de l'appropriation de l'identité d'une personne. En d'autres termes, il s'agit de se faire passer pour cette personne, d'endosser son identité auprès d'autres personnes. Par exemple, la création d'un compte sur un réseau social dont le but de se faire passer pour une autre personne afin de collecter des informations ou à toute autre fin. Elle est passible d'une peine d'emprisonnement allant de six mois à trois ans.

Il faut mettre un terme à ces menaces de cybersécurité. C'est pourquoi, en Espagne, il existe un moyen de lutter contre ce phénomène au niveau juridique. En premier lieu, **toute victime qui souhaite agir doit d'abord rassembler des preuves de ce qui se passe, puis le signaler au commissariat de police le plus rapidement possible.** Après avoir vérifié ces preuves, la police vous contactera et évaluera la situation. S'ils le jugent opportun, le rapport déclenchera une nouvelle procédure et des actions en justice seront lancées.

En Belgique:

La cybersécurité est le résultat d'un ensemble de mesures de sécurité qui minimisent le risque de perturbation ou d'accès non autorisé aux secteurs des technologies de l'information et de la communication (TIC). Elle comprend toutes les mesures raisonnables et acceptables visant à protéger les TIC des citoyens, des entreprises, des organisations et du gouvernement contre les cybermenaces. La cybersécurité implique la protection des systèmes (tels que le matériel, les logiciels et les infrastructures connexes) et des réseaux, ainsi que des données qu'ils contiennent.

L'évaluation nationale des risques (2018-2023) du Centre de crise belge considère la cybersécurité comme l'un des principaux risques auxquels la Belgique sera confrontée dans les années à venir. À l'intérieur de ce cluster, la cybercriminalité et le piratage informatique sont considérés comme des risques prioritaires au niveau national.

Cette définition est tirée du Centre pour la sécurité Belgique[23,] l'autorité nationale en matière de cybersécurité belge, qui précise également les 4 principales menaces auxquelles la cybersécurité tente de faire face : les services militaires et les services de renseignement étrangers, le terrorisme, le piratage informatique et la cybercriminalité.

Dans ce rapport, la cybersécurité sur laquelle nous nous concentrerons sera principalement liée au piratage informatique et à la cybercriminalité en raison de leurs méthodes d'attaque les plus communément utilisées, ainsi que les réseaux sociaux, en raison de leurs conséquences directes sur la sécurité de chaque citoyen, y compris les jeunes.

En juillet 2016, la directive sur la sécurité des réseaux et des systèmes d'information (SRI) (https://www.itgovernance.eu/nl-be/nis-directive-be) a été adoptée, et a été ensuite traduite dans la loi belge le 7 avril 2019 : loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt public pour la sécurité publique. L'article 7 de cette directive (reproduit à l'article 10 de la loi belge sur les SRI) impose aux États membres d'élaborer une stratégie nationale pour la sécurité des réseaux et des systèmes d'information.

[23]Centre for Cyber Security Belgium (2022, mai).Cybersecurity Strategy Belgium 2.0 2021-2025. Disponible : https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_UK_WEB.pdf

Jusqu'à la publication de la loi belge sur les réseaux et les systèmes d'information (NIS) en mai 2019, le pays ne disposait pas d'une législation complète sur la cybersécurité. Cette étape importante a été franchie grâce à l'Agence de l'Union européenne pour la cybersécurité (ENISA) qui contribue à la politique informatique de l'UE, renforce la fiabilité des produits, services et processus TIC grâce à des systèmes de certification de cybersécurité, coopère avec les États membres et les organes de l'UE et aide l'Europe à se préparer aux défis cybernétiques de demain. En outre, nous pouvons souligner la législation suivante qui sera utilisée en fonction de la cybercriminalité poursuivie :

- Code pénal belge : art. 550 (b) "Piratage", art. 210bis "Fraude informatique" ;

- Loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques.

-Directive (UE) 2016/1148 du 6 juillet 2016 concernant des mesures visant à assurer un niveau commun élevé de sécurité des réseaux et des systèmes d'information dans l'Union.

-La loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.

- Arrêté royal du 12 juillet 2019, portant exécution de la loi du 7 avril 2019, établissant le cadre du réseau de sécurité et des systèmes d'information d'intérêt général pour la sécurité publique.

- Règlement (UE) 2019/881 du 17 avril 2019 relatif à l'ENISA

- Règlement d'exécution (UE)2018/ 151 de la Commission du 30 janvier 2018 fixant les modalités d'application de la directive UE 2016/1148 du Parlement européen et du Conseil en ce qui concerne une spécification supplémentaire des éléments à prendre en compte par les fournisseurs de services numériques dans la gestion des risques de sécurité.

Aux Pays-Bas:

En 2021, près de 2,5 millions de personnes aux Pays-Bas âgées de 15 ans ou plus ont déclaré avoir été victimes de cybercriminalité, ce qui représente près de 17 % de la population!

Le parlement néerlandais a adopté une législation sur la cybercriminalité qui empêche les points suivants :

- Article 138a: Toute personne qui accède intentionnellement et illégalement à un système automatisé de stockage ou de traitement de données, ou à une partie d'un tel système ;
- Article 138 b: l'entrave grave et illicite au traitement des données ;
- Article 232: la falsification de tout porte-jeton électronique ayant une valeur probante et l'utilisation de ces jetons comme s'ils étaient authentiques.

La cybercriminalité est définie comme "la criminalité impliquant des formes numériques d'usurpation d'identité, de fraude lors d'achats ou de ventes en ligne, de piratage et de cyberharcèlement (diffamation, harcèlement, chantage et menace de violence commise en ligne)." [24]

Les cybercrimes relatifs à la vie privée des individus, des organisations et des gouvernements sont considérés comme des délits par la loi néerlandaise (conformément aux articles ci-dessus). Les cybercrimes couramment signalés aux Pays-Bas sont :

- Le piratage
- La fraude liée aux achats en ligne
- Le cyberharcèlement[25]

Les cybercrimes les plus courants, identifiés par le gouvernement néerlandais, sont les suivants[26] :

- Le phising : utilisation de faux e-mails pour obtenir des informations personnelles des internautes ;

[24] Les Pays-Bas en chiffres: https://longreads.cbs.nl/the-netherlands-in-numbers-2020/what-about-cyber-crime/#:~:text=Hacking%2C%20online%20shopping%20fraud%20and%20cyber%20bullying&text=Hacking%20was%20most%20common%2C%20mentioned,such%20as%20stalking%20or%20threats.
[25] Ibid.
[26] Formes de cybercriminalité : https://www.government.nl/topics/cybercrime/forms-of-cybercrime

- L'Utilisation abusive de renseignements personnels (usurpation d'identité) ;
- Le piratage : fermer ou utiliser abusivement des sites web ou des réseaux informatiques ;
- La diffusion de la haine et l'incitation au terrorisme ;
- La diffusion de pédopornographie ;
- Le pédopiégeage ou « grooming »: faire des avances sexuelles aux mineurs.

Le National Cyber Security (NCSC) (https://english.ncsc.nl/) est chargé de superviser la sécurité numérique aux Pays-Bas[27]. Pour ce faire, ils :

- Surveillent en permanence toutes les sources suspectes sur Internet ;
- Conseillent les organisations sur la façon de se protéger contre les menaces en ligne ;
- Contrôlent les évolutions de la technologie numérique et mettent à jour les systèmes de sécurité.

En Bulgarie

La « cybercriminalité » (également appelée « criminalité informatique » ou « criminalité de haute technologie ») doit s'entendre comme « actes criminels commis par l'utilisation de réseaux de communications électroniques et de systèmes d'information, ou contre de tels réseaux et systèmes ».

En fait, le terme désigne trois catégories d'actes criminels. La première concerne les formes traditionnelles de criminalité telles que la fraude ou la contrefaçon, bien que, dans le contexte de la cybercriminalité, cette catégorie se réfère en particulier aux infractions commises par l'intermédiaire de réseaux de communications électroniques et de systèmes d'information (« réseaux électroniques »).

La deuxième concerne la publication dans les médias électroniques de contenus illicites (tels que la pédopornographie ou les contenus incitant à la violence et liés aux discours de haine et à la discrimination).

[27] Lutte contre la cybercriminalité aux Pays-Bas : https://www.government.nl/topics/cybercrime/fighting-cybercrime-in-the-netherlands

Le troisième comprend les crimes spécifiques aux réseaux électroniques, tels que les attaques contre les systèmes d'information, le déni de service et le piratage.

La Bulgarie a ratifié la Convention sur la cybercriminalité adoptée par le Conseil de l'Europe en 2001 et ses protocoles. Sur cette base, le Code pénal bulgare comprend des définitions et des sanctions relatives à la cybercriminalité. Le Code criminel décrit différents types de cybercriminalité:

- La cyberfraude est définie à l'article 212 bis
- Une forme spéciale de destruction et d'endommagement à l'aide d'outils numériques est définie à l'article 216, paragraphe 2
- Une manière spécifique de violation du secret de la correspondance est définie à l'article 171.
- La pédopornographie est également spécifiquement considérée comme un crime.
- Les cybercrimes décrits au chapitre 9 du Code pénal (art. 319a à 319 f du Code pénal). Ils affectent les relations publiques qui assurent le bon fonctionnement des ordinateurs, des systèmes informatiques, des ressources informatiques et des réseaux informatiques, ainsi que la création et l'utilisation licites de l'information.Il s'agit notamment de l'accès non autorisé, de l'altération, des dommages, de la destruction de données ou de programmes, de l'introduction d'un virus ou de la propagation de mots de passe.
- La première concerne la copie ou l'utilisation de données informatiques sans autorisation en obtenant un accès non autorisé aux ressources informatiques (article 319 bis).
- Le type suivant de criminalité informatique est la contrefaçon ou la destruction d'un programme ou de données informatiques (article 319 ter). Cela inclut l'ajout, la modification ou la suppression d'un programme informatique ou de données informatiques, ce qui les rend inauthentiques ou incompatibles avec les programmes et données originaux.
- L'introduction d'un virus informatique dans un ordinateur ou un réseau d'information est visée à l'article 319d, paragraphe 1, du Code pénal.
- L'article 319e, paragraphe 1, du Code pénal prévoit la distribution de mots de passe informatiques ou de systèmes, lorsque cela conduit à la divulgation de données à caractère personnel ou de secret personnel. La peine est d'un an de prison.

En termes de confidentialité et de sécurité en ligne, il est important de mentionner que la réglementation bulgare est liée au GDPR, qui est réglementé par la Commission pour la Protection des Données Personnelles (https://www.cpdp.bg/). Il s'agit d'un organisme public indépendant qui protège les citoyens dans le traitement de leurs données personnelles et dans l'accès à ces données, et qui contrôle le respect de la loi sur la protection des données personnelles.

Il s'agit d'un organe indépendant et collégial, composé d'un président et de quatre membres. Les membres de la commission et son président sont élus par l'Assemblée nationale sur proposition du Conseil des ministres pour un mandat de 5 ans et peuvent être réélus pour un autre mandat. L'un des rôles les plus importants de la Commission est de transmettre les questions liées à la violation du GDPR à la Cour de justice de Bulgarie.

3.4 Comment éviter les risques liés protection des données

L'une des choses les plus importantes à faire pour protéger nos données est d'avoir un mot de passe fort. Il sera très utile, car, de nos jours, les cybercriminels ne cessent d'imaginer des moyens innovants pour pirater les comptes et s'emparer des données personnelles. Parmi les conséquences potentielles des mots de passe faibles, on peut citer les violations de données, l'usurpation d'identité, le détournement d'ordinateur, le chantage et la violation de la vie privée.

Par conséquent, afin d'éviter que les internautes ne subissent ces désagréments, vous trouverez ici des instructions pour créer un mot de passe robuste sur lequel vous pouvez compter.

- **N'utilisez jamais d'informations personnelles.** Cela peut sembler évident, mais beaucoup de personnes utilisent leurs propres informations lors de la création de leur mot de passe. Il est recommandé de ne pas utiliser de noms, d'anniversaires, d'adresses ou de numéros de téléphone.
- **Inclure une combinaison de lettres, de chiffres et de symboles.** Plus vous utilisez de caractères aléatoires, plus votre mot de passe sera complexe.

- **Favoriser un mot de passe long.** Cela réduira les chances d'être victime d'une cyberattaque.
- **Ne jamais réutiliser les mots de passe.** Les internautes sont habitués à toujours choisir le même mot de passe. C'est une grave erreur, car cela les expose à des attaques de type « credential stuffing » (attaque qui consiste à voler des listes d'identifiant et des mots de passe).
- **Évitez d'utiliser des mots réels**. Les pirates utilisent des programmes malveillants qui peuvent exploiter chaque mot figurant dans les dictionnaires pour craquer les mots de passe. Par conséquent, l'utilisation de mots inventés peut aider à créer un mot de passe robuste et sûr.

De plus, afin de protéger vos informations, il est recommandé **d'utiliser uniquement les sites Web auxquels vous avez confiance**. Beaucoup de personnes ne savent pas comment vérifier si un site Web est sûr ou non, c'est pourquoi vous trouverez quelques conseils à ce sujet.

1. Tout d'abord, **vérifiez si l'URL est correctement orthographiée**, si elle est sécurisée par la mention « https » et si elle comporte un indicateur de vérification, tel qu'un cadenas.
2. Deuxièmement, **les sites Web qui semblent dangereux le sont généralement**. Si le propriétaire du site n'investit pas dans l'apparence et l'expérience de l'utilisateur, il n'investit probablement pas dans la sécurité du site. Par conséquent, ces sites sont donc sujets à des logiciels malveillants, qui pourraient menacer votre sécurité.
3. Troisièmement, **vous devez pouvoir vérifier que des informations de contact sont disponibles ainsi qu'une politique de confidentialité accessible**. Ces informations se trouvent généralement tout en bas de la page d'accueil. Un autre conseil utile est de consulter les témoignages et les avis d'autres personnes sur le site afin de connaître les expériences vécues par d'autres personnes lors de l'utilisation de ces sites.

Il existe également d'autres pratiques qui peuvent mettre en danger la sécurité numérique, comme **l'utilisation du WIFI public**. Il est vrai que ce service que certains hôtels et aéroports proposent est gratuit, mais il a un prix. Ces bornes WIFI gratuites permettent aux pirates de se placer entre la personne qui l'utilise et le point de connexion.

Au lieu de parler directement grâce à la borne, les gens envoient leurs informations à le hacker, qui s'en sert ensuite. Les pirates ont alors accès à toutes les informations que les gens envoient sur l'internet: e-mails importants, informations sur les cartes de crédit et identifiants de sécurité. Une fois que les hackers disposent de ces informations, ils peuvent accéder à vos systèmes comme s'ils étaient vous.

Pour éviter d'être piraté de la sorte, il est recommandé de ne pas utiliser le WIFI lorsque vous n'en avez pas besoin et, si vous devez utiliser ce type de connexion, connectez-vous avec un VPN. Le VPN est un réseau privé virtuel qui permet de crypter efficacement vos informations. Si vous avez vraiment besoin d'utiliser ce WIFI gratuit, essayez de ne pas faire de transactions bancaires, d'achats ou de travail en ligne. Vous pouvez également désactiver le Bluetooth et le partage de fichiers.

Comment protéger vos données personnelles?

1. **Sécurisez vos comptes**

Au cours de la dernière décennie, les violations de données et les fuites de mots de passe ont frappé de grandes entreprises telles que Facebook, Home Depot, Marriott, Yahoo, etc. Les institutions gouvernementales ont également souffert de cyberattaques par lesquelles des tiers non autorisés ont obtenu l'accès aux informations personnelles des citoyens (par exemple, l'attaque contre l'Agence nationale des revenus bulgare en 2019). Si vous avez des comptes en ligne, il est possible que des pirates aient divulgué les données d'au moins l'un d'entre eux. Pour le vérifier, vous pouvez rechercher votre adresse électronique sur le site **Have I Been Pwned?** (https://haveibeenpwned.com/) afin de la croiser avec des centaines de violations de données (une « violation » est un incident au cours duquel des données sont exposées par inadvertance dans un système vulnérable, généralement en raison de contrôles d'accès insuffisants ou de défaillances de sécurité dans le logiciel).

Il existe d'autres moyens d'identifier les signes possibles qu'un compte a été piraté, que votre identité a été volée ou que vos données ont été violées d'une autre manière. Renseignez-vous sur les signes avant-coureurs d'une violation potentielle et créez des réflexes pour surveiller la sécurité de vos données personnelles afin d'identifier les attaques ou violations potentielles avant qu'elles ne deviennent dévastatrices.

Lisez les conseils de protection des données et les informations décrivant les signes avant-coureurs fréquents d'une violation ou d'un piratage des données, comme cette liste de "**15 signes que vous avez été piraté: comment se défendre?"** (https://www.csoonline.com/article/3617849/15-signs-youve-been-hacked-and-how-to-fight-back.html).

Si votre compte a été piraté, vos données perdues ou votre appareil volé, voyez-y une occasion d'apprendre. Déterminez exactement ce qui a mal tourné et comment vous auriez pu protéger vos données en prenant de meilleures précautions. Pendant que vous réparez les dégâts, c'est le moment de prendre du recul et de vous poser une question plus fondamentale: quelle était la raison de la violation?

S'il s'agissait de votre compte bancaire, la réponse peut être évidente. Dans d'autres cas, comme celui de la boîte e-mail, les raisons peuvent être multiples: par exemple, l'utiliser pour envoyer des spams, demander de l'argent à vos contacts ou obtenir des réinitialisations de mot de passe sur d'autres services. Un hacker peut même essayer d'accéder à votre entreprise. Comprendre pourquoi vous avez été ciblé peut aussi parfois vous aider à comprendre comment vous avez été piraté.

Une façon de renforcer le niveau de sécurité numérique et de protéger nos données personnelles est d'utiliser un gestionnaire de mots de passe pour générer et retenir des mots de passe différents et complexes pour chaque compte; c'est l'une des mesures les plus importantes que les gens puissent prendre pour protéger leur vie privée et leur sécurité aujourd'hui. **LastPass** (https://www.lastpass.com/) et **1password** (https://1password.com/) peuvent vous aider à le faire, et ce en générant des mots de passe, en surveillant les comptes pour détecter les failles de sécurité, en proposant de changer les mots de passe faibles et en synchronisant vos mots de passe entre votre ordinateur et votre téléphone. **N'utilisez pas de numéros de sécurité sociale, de numéros de téléphone, d'adresses ou d'autres informations d'identification personnelle comme mots de passe.**

Nous vous suggérons également d'utiliser, dans la mesure du possible, l'authentification en deux étapes pour vos comptes en ligne. La plupart des banques et des principaux réseaux sociaux proposent cette option.

Comme son nom l'indique, l'authentification en deux étapes nécessite deux étapes : la saisie de votre mot de passe et la saisie d'un numéro auquel vous seul avez accès. Par exemple, la première étape consiste à vous connecter à Facebook avec votre nom d'utilisateur et votre mot de passe.

Lors de la deuxième étape, Facebook vous envoie un code temporaire par SMS ou, mieux encore, par le biais d'une application comme Google Authenticator, que vous devrez ensuite saisir pour vous connecter.

2. Protégez votre navigation sur internet

Les entreprises et les sites web suivent tout ce que nous faisons en ligne. Chaque publicité, chaque touche des réseaux sociaux et chaque site web recueille des informations sur votre localisation, vos habitudes de navigation et bien plus encore. Les données collectées en disent plus sur vous que vous ne pensez.

Même si vous ne partagez pas publiquement vos informations personnelles sur les réseaux sociaux, il y a de fortes chances que les sites web que vous visitez régulièrement fournissent toutes les données dont les publicitaires ont besoin pour déterminer le type de personne que vous êtes. C'est en partie pour cela que les publicités ciblées restent l'une des innovations les plus troublantes d'Internet.

Une extension de navigateur comme **uBlock Origin** (https://ublockorigin.com/) bloque les publicités et les données qu'elles rassemblent. L'extension uBlock Origin empêche également les logiciels malveillants de s'exécuter dans votre navigateur et vous offre un moyen simple de désactiver le verrouillage des publicités lorsque vous souhaitez favoriser les sites que vous savez sécurisés. Vous pouvez combiner uBlock avec **Privacy Badger** (https://privacybadger.org/), qui bloque les trackers, et les publicités n'apparaîtront pas partout. Pour ralentir encore plus les publicités des trackers, désactivez les publicités basées sur les centres d'intérêt d'Apple, Facebook, Google et Twitter. De nombreux sites Web proposent des moyens de refuser la saisie des données, mais vous devez le faire manuellement. Cela n'éliminera pas complètement le problème, mais réduira considérablement la quantité de données collectées.

L'installation de l'extension **HTTPS Everywhere** (https://chrome.google.com/webstore/detail/https-everywhere/gcbommkclmclpchllfjekcdonpmejbdp) contribue également à protéger vos informations personnelles. Elle vous dirige automatiquement vers la version sécurisée d'un site lorsque celui-ci le prend en charge, ce qui rend difficile pour un pirate (surtout si vous utilisez une connexion Wi-Fi publique dans un café, un aéroport ou un hôtel) de surveiller numériquement ce que vous faites.

3. **Utilisez un logiciel antivirus sur votre ordinateur**

Les virus ne sont peut-être pas aussi courants qu'il y a dix ans, mais ils existent toujours. Les logiciels malveillants présents sur votre ordinateur peuvent causer toutes sortes de ravages, qu'il s'agisse de fenêtres pop-up gênantes, de minage clandestin de bitcoins ou de recherche d'informations personnelles. Si vous risquez de cliquer sur des liens douteux ou si vous partagez un ordinateur avec plusieurs personnes dans un même foyer, il est utile de configurer un logiciel antivirus, en particulier sur les ordinateurs Windows. Si votre ordinateur fonctionne sous Windows 10, vous devriez utiliser le logiciel intégré de Microsoft, **Windows Defender**. Vous pouvez également disposer d'une mesure de protection supplémentaire si vous installez un programme antivirus.

4. **Mettez à jour vos logiciels et appareils**

Les systèmes d'exploitation des téléphones et des ordinateurs, les navigateurs Web, les applications les plus utilisées et même les appareils domestiques intelligents font l'objet de fréquentes mises à jour qui apportent de nouvelles fonctionnalités et des améliorations en matière de sécurité. Ces mises à jour de sécurité sont généralement bien plus efficaces pour déjouer les pirates que les logiciels antivirus.

Les trois principaux systèmes d'exploitation peuvent se mettre à jour automatiquement, mais vous devriez prendre le temps de vérifier que les mises à jour automatiques sont bien activées sur le système d'exploitation de votre choix: Windows, macOS ou Chrome OS. Bien qu'il soit frustrant d'allumer votre ordinateur et de devoir attendre une mise à jour qui risque de fermer le logiciel que vous utilisez, les avantages en termes de sécurité en valent la peine.

Votre téléphone dispose également d'options de mise à jour automatique, mais vous devez parfois approuver manuellement l'installation des mises à jour.

5. **N'installez pas de logiciel que vous ne connaissez pas et dans lesquels vous n'avez pas totalement confiance**

Chaque application étrange que vous installez sur votre téléphone et chaque extension de navigateur ou logiciel que vous téléchargez à partir d'un site web douteux représente une autre faille potentielle en matière de confidentialité et de sécurité.

D'innombrables applications mobiles suivent votre localisation partout où vous allez et récoltent vos données sans vous demander votre consentement, même dans les applications pour enfants. Contentez-vous de télécharger les logiciels et les extensions de navigateur directement auprès de leurs créateurs et des applications officielles.

Vous pouvez voir quelles applications ont accès à votre localisation, à vos contacts, à votre microphone et à d'autres données. Désactivez les autorisations lorsqu'elles n'ont pas de sens: par exemple, Google Maps a besoin de votre localisation pour fonctionner, mais pas votre application de notes.

À l'avenir, pensez aux autorisations des applications lorsque vous installez un nouveau logiciel; si une application est gratuite, il est possible qu'elle collecte et vende vos données.

6. **Désactivez le Bluetooth lorsque vous ne l'utilisez pas**

La technologie Bluetooth offre des avantages incroyables au monde de la téléphonie mobile, mais elle ouvre également la porte à de nombreuses failles. La plupart des menaces exploitant la connectivité Bluetooth dépendent de la connexion Bluetooth active, et si elles ne sont généralement pas dévastatrices ou dangereuses, elles sont certainement dérangeantes et peuvent être sérieuses. Les attaques Bluetooth dépendent de l'exploitation du processus de demande et d'octroi de permission qui constitue l'épine dorsale de la connexion Bluetooth.

Quelles que soient les fonctions de sécurité de votre appareil, la seule façon d'empêcher complètement les pirates d'exploiter ce processus de demande et d'octroi d'autorisations est de désactiver la fonction Bluetooth de votre appareil lorsque vous ne l'utilisez pas (il ne suffit pas de le mettre en mode invisible ou indétectable, mais plutôt en le désactivant complètement).

7. **Soyez très prudent lorsque vous partagez des informations personnelles**

Ce conseil s'applique aussi bien au monde en ligne qu'au monde hors ligne : qui vous demande vos informations personnelles, comme votre numéro de sécurité sociale ou les informations de votre carte de crédit ? Pourquoi en ont-ils besoin? Comment vont-ils les utiliser ?

Quelles mesures de sécurité ont été mises en place pour garantir la confidentialité de vos informations personnelles? Vous devez répondre clairement à toutes ces questions importantes avant de fournir vos données personnelles à quiconque.

8. **Méfiez-vous des imposteurs**

Dans le même ordre d'idées que le conseil précédent, de nombreux imposteurs tentent d'inciter des consommateurs peu méfiants à divulguer leurs informations personnelles confidentielles en se faisant passer pour leur banque, leur société de cartes de crédit ou toute autre entité. Cela peut se faire par téléphone ou en ligne, par le biais d'e-mails de phishing ou de sites web conçus pour imiter l'aspect et la présentation de l'entreprise authentique. **Assurez-vous de savoir qui a accès à vos informations personnelles ou financières.**

Ne donnez pas d'informations personnelles au téléphone, par courrier ou sur Internet, à moins d'avoir pris l'initiative du premier contact ou de savoir à qui vous avez affaire. Si une entreprise affirme avoir un compte chez vous et envoie un courriel demandant des informations personnelles, ne cliquez pas sur les liens contenus dans le courriel. Tapez plutôt le nom de l'entreprise dans votre navigateur Web, allez sur son site et contactez-la par le biais du service clientèle. Vous pouvez également appeler le numéro du service client figurant sur votre relevé de compte. Demandez si l'entreprise a vraiment envoyé une demande.

9. Ne partagez pas trop d'informations sur les plateformes de réseaux sociaux

Les réseaux sociaux sont devenus un mode de vie pour de nombreuses personnes, mais partager trop d'informations personnelles sur vos profils de réseaux sociaux peut être dangereux. Par exemple, de nombreux hackers ont réussi à deviner des mots de passe grâce à des méthodes d'essai et d'erreur, en combinant des informations courantes (telles que les noms des enfants, les adresses et d'autres détails) facilement trouvées sur les profils des utilisateurs. **Ne publiez pas d'informations qui vous rendraient vulnérable**, comme votre adresse ou des informations sur votre emploi du temps ou vos habitudes. Si vos contacts publient des informations sur vous, assurez-vous que l'ensemble de ces informations ne dépasse pas ce que vous accepteriez que des inconnus sachent.

Soyez également prudent lorsque vous publiez des informations, y compris des photos, à propos de vos contacts.

10. Personnalisez les paramètres de confidentialité de vos réseaux sociaux

Les réseaux sociaux comme Facebook permettent aux utilisateurs de personnaliser leurs paramètres de confidentialité. Sur Facebook, par exemple, vous pouvez choisir qui peut voir le contenu que vous publiez et qui peut voir les informations de votre profil, telles que votre lieu de travail, votre date de naissance et votre ville natale.

Choisissez toujours le niveau de confidentialité le plus élevé possible pour vous assurer que vos données personnelles ne se retrouvent pas entre les mains de personnes mal intentionnées. Le contenu que vous publiez en ligne sera présent sur le long terme, mais vous pouvez personnaliser les paramètres de confidentialité sur la plupart des sites de réseaux sociaux. Ces paramètres déterminent qui peut vous contacter et qui peut voir les informations que vous publiez.

Faites preuve de prudence: même s'il est amusant de partager des informations, gardez à l'esprit votre réputation en ligne. Et si vous divulguez trop d'informations publiquement, elles pourraient être utilisées par des usurpateurs d'identité et servir à détourner votre identité.

11. N’oubliez pas de vous déconnecter

La connexion aux services en ligne est obligatoire lorsque vous souhaitez accéder à vos comptes personnels, mais de nombreux utilisateurs oublient de se déconnecter lorsqu’ils ont fini d’utiliser un service. Lorsque vous accédez à des sites Web basés sur des comptes via un ordinateur public (ou un appareil partagé), veillez à vous déconnecter du service à la fin de la session. Ce n’est pas parce qu’un nouveau site web est consulté après une visite sur un site auquel vous vous êtes connecté que l’utilisateur suivant ne peut pas appuyer sur le bouton retour et accéder à votre compte connecté. Certains sites sont également configurés pour sauvegarder automatiquement les informations, alors vérifiez si cette fonction peut être désactivée.

12. N’ouvrez pas d’e-mail de personnes que vous ne connaissez pas

Si vous recevez un e-mail d’une source ou d’une personne que vous ne reconnaissez pas, ne l’ouvrez pas et évitez absolument de cliquer sur les liens ou les fichiers joints.

Il existe une règle d’or pour traiter les messages de spam: s’ils ressemblent à un message de spam, c’est probablement le cas; supprimez-les donc sans cliquer ni télécharger quoi que ce soit. Ces messages peuvent contenir un logiciel qui indique à l’expéditeur que vous avez ouvert l’e-mail, confirmant ainsi que vous avez un compte actif, ce qui peut conduire à davantage de messages indésirables. Certains programmes malveillants peuvent voler votre adresse électronique et l’utiliser pour renvoyer des pourriels sous l’apparence d’une adresse légitime. Par exemple, les imposteurs peuvent se faire passer pour quelqu’un que vous connaissez, comme un ami, un parent ou un collègue. Si le message en question semble provenir d’une personne que vous connaissez, contactez-la en dehors de votre boîte mail.

13. N’enregistrez pas de mots de passe dans votre navigateur

La pratique courante qui consiste à « enregistrer les mots de passe » dans les navigateurs est dangereuse. En effet, si quelqu’un s’empare de votre ordinateur ou de votre téléphone portable, il pourra facilement accéder à tous les comptes pour lesquels vous avez enregistré des identifiants de connexion dans votre navigateur.

Bien que cela puisse rendre la connexion plus pratique, c'est une habitude risquée en termes de protection des données. Gardez un œil sur ces fenêtres pop-up et assurez-vous de les désactiver.

14. Ne vous connectez pas à d'autres sites en vous identifiant via vos comptes sur les réseaux sociaux

Cela semble être une option pratique: il suffit de s'inscrire à un site Web ou à un service en ligne en utilisant son compte Facebook ou LinkedIn, et tant que vous êtes connecté à ce réseau social, la connexion au site tiers est rapide et facile.

Cependant, cela peut mettre en péril votre vie privée. Bien que ce soit une option pratique, se connecter à un autre compte avec votre nom d'utilisateur et votre mot de passe Facebook peut impliquer la transmission à l'autre site de toutes les informations que Facebook a recueillies à votre sujet.

Pire encore, si quelqu'un détourne vos informations de connexion au réseau social, il peut également avoir accès à ces comptes tiers.

15. Choisissez un fournisseur de courrier électronique sûr et réputé

Assurez-vous que votre fournisseur de courriel garantit une sécurité suffisante. Vous devez vous assurer que votre fournisseur d'e-mail utilise une méthode d'authentification comme **DMARC** pour empêcher le phishing et minimiser les risques.

La bonne nouvelle, c'est que Google, Yahoo, Microsoft et AOL utilisent cette méthode. Dès lors si vous utilisez l'une de ces messageries en ligne, vous êtes sur la bonne voie pour minimiser les risques en matière de confidentialité et de sécurité.

4. Éducation non formelle

4. ÉDUCATION NON FORMELLE

Dans cette section, nous mentionnerons les contextes nationaux des moyens non formels de sensibiliser à la cyberintimidation et aux discours de haine:

- **Pays-Bas**

Il existe d'autres façons non formelles dont les citoyens sont devenus plus conscients des problèmes liés à la sécurité en ligne. La cybersécurité n'est pas seulement évoquée dans une éducation formelle ou spécifique. En effet, la prise de conscience peut être effectuée de différentes manières, comme par le biais d'articles d'actualité, d'influenceurs en ligne, **de parents** et **d'enseignants** ou de la prise de parole de victimes.

Cybersécurité et confidentialité

La lutte ou la réglementation de la cybersécurité et de la vie privée est souvent associée aux institutions et organes officiels ou à l'éducation formelle. Toutefois, l'éducation non formelle à ce sujet a également une influence.

Chantal Stekelenburg (https://twitter.com/mifare_lady) membre de l'ONG américaine **« Women in Cybersecurity Community Association (WICCA) »** (https://womenofwicca.nl/) est très suivie sur les réseaux sociaux. Elle aborde des thèmes tels que la cybersécurité et s'efforce à encourager les femmes à se passionner pour la sécurité, voire à devenir expertes en la matière.

Cyberharcèlement

Ceux qui abordent le thème du cyberharcèlement, qu'ils soient influenceurs ou non, ont permis à beaucoup d'avoir un regard nouveau sur le sujet, mais aussi d'apprendre.

Beaucoup de jeunes ont souvent honte de s'exprimer de manière formelle ou officielle, par exemple en rédigeant des rapports ou en alertant le personnel de leur école ou d'autres institutions. Ainsi, les approches non formelles sont utiles, car elles permettent aux personnes qui ont été victimes de cyberharcèlement de s'identifier aux autres, de se sentir moins seules et plus susceptibles de s'exprimer.

Un article de presse de 2018 a rapporté qu'une cour d'appel néerlandaise a édicté une peine de prison pour un homme reconnu coupable de cyberharcèlement envers de nombreux jeunes, hommes et femmes, dont beaucoup viennent des Pays-Bas. Il avait fait pression sur les jeunes femmes pour qu'elles accomplissent des actes sexuels devant les webcams. Cette histoire a été très médiatisée et peut être considérée comme un exemple clair d'éducation non formelle en matière de cyberharcèlement et de cybercriminalité: **plus on accorde de l'attention à des cas similaires, plus importante est la prise de conscience, permettant ainsi aux jeunes d'être plus aptes à les éviter et à les signaler.**

Discours de haine:

L'importance de l'éducation non formelle s'étend aux discours de haine, car il est vital que les gens s'expriment contre ce phénomène. D'importantes campagnes ont été organisées sur ce sujet.

Une action a été menée dans le cadre de la **Campagne Jeunesse contre le Discours de Haine** (https://www.coe.int/en/web/no-hate-campaign) du Conseil de l'Europe dont le but a été de mobiliser les jeunes dans la lutte contre les discours de haine et ainsi de promouvoir les droits de l'homme.

- ## Espagne

Il est impossible de ne pas mentionner le rôle essentiel de la culture, des influenceurs ou encore des grandes campagnes de marketing lorsque l'on aborde les moyens éducatifs non formels de sensibilisation au cyberharcèlement et aux discours de haine en Espagne.

Cyberharcèlement

Beaucoup s'identifient aux influenceurs. En effet, de par ses millions d'adeptes, cette nouvelle profession est capable d'atteindre une cible plus élevée grâce aux réseaux sociaux et autres plateformes en ligne. La méthodologie est simple et efficace: tout en surfant sur ses réseaux pendant son temps libre, l'utilisateur reçoit, par le biais des influenceurs, des informations relatives au cyberharcèlement sans faire aucun effort supplémentaire.

En Espagne, il existe de nombreux exemples d'influenceurs qui ont utilisé leur notoriété pour sensibiliser au cyberharcèlement. Par exemple, le roman ***Y luego ganas tú*** **(paru chez *Nube de Tinta*)** est un recueil de nouvelles dans lequel les auteurs (5 influenceurs espagnols) racontent, à travers leurs propres histoires et fictions qui s'inspirent de la réalité, le problème du harcèlement scolaire.

Un phénomène qui prend toujours plus d'ampleur: aujourd'hui, un étudiant espagnol sur deux affirme avoir déjà été victime de harcèlement ou de cyberharcèlement. Ces influenceurs, Javier Ruescas (@javier_ruescas), Manu Carbajo (@karbajo), Jedet Sánchez (@lajedet), María Herrejón (@hersimmar) y Andrea Compton (@andreacomptonn) sont populaires en Espagne pour leur lutte pour les droits sociaux et la visibilité LGBT.

Le podcast **Estirando el chicle** (https://www.youtube.com/c/Estirandoelchicle?app=desktop), dirigé par Carolina Iglesias y Victoria Martín, est un exemple supplémentaire des initiatives mises en œuvre dans la lutte contre le cyberharcèlement. Dans ce podcast, de nombreuses personnes célèbres sont questionnées sur des sujets tels que le cyberharcèlement ou que la visibilité LGBT.

Considéré comme « un programme inédit tant dans le langage que dans l'approche, mêlant humour, interviews et contenus sociaux sans retenue », ce podcast a gagné en reconnaissance grâce à de nombreux prix tels que le prix Ondas pour le meilleur podcast ou programme de diffusion numérique.

En outre, il serait également pertinent de mentionner la célèbre marque de shampooing Head&Shoulders qui a également contribué à la lutte contre le harcèlement. Dans la campagne '**Stop Bullying'** (https://www.hys.es/es-es/frena-el-bullying/) (« Non au harcèlement »), de nombreuses personnalités publiques espagnoles, comme Marta Pompo ou Ibai Llanos, tentent de sensibiliser le public en racontant leurs propres expériences de discours de haine sur les réseaux sociaux.

En outre, un microsite éducatif sera ajouté au site web de la marque, où l'on pourra retrouver tant des conseils pour les élèves, les enseignants et les parents afin de les amener à adopter un rôle actif dans les situations de harcèlement que des clés pour résoudre ces conflits.

- **Belgique**

Depuis la Belgique, nous souhaitons entreprendre une campagne de communication contre le cyberharcèlement chez les jeunes et mettre en évidence l'un de ses influenceurs les plus importants:

Campagne WAT WAT TEGEN PESTEN

La plateforme **WAT WAT** (https://www.watwat.be/) travaille main dans la main avec des influenceurs et des jeunes pour discuter du harcèlement chez les jeunes à l'aide de conseils et d'expériences. Vous pouvez par exemple démarrer une conversation concernant le cyberharcèlement avec WAT WAT, qui vous répondra automatiquement sur la messagerie de Facebook. Être harcelé ou harceler, *troller* ou pas, le choix est à vous.

La plateforme a mené une campagne au cours de la « semaine contre le harcèlement » flamande pour sensibiliser les enfants et les jeunes à ce qu'est le harcèlement, à ce que vous pouvez faire pour y remédier et à ses conséquences.

De vraies histoires ont été partagées publiquement: Angel, 16 ans, a été forcée de manger des déchets par ses harceleurs. Dans la semaine contre le harcèlement, Angel, ainsi que Yasmien Naciri, 27 ans, Margot, 22 ans et Jorrit, 23 ans, ont partagé leur histoire et dévoilent leurs cicatrices après des années de harcèlement. Ces histoires courageuses incitent les jeunes à réfléchir, à en parler et à s'entraider.

Wat Wat exhortait tout le monde à agir encore plus contre l'intimidation. Faites entendre votre voix grâce aux affiches de la campagne dans les salles de classe, par exemple, afin de faire de l'intimidation un sujet de discussion et utilisez le hashtag #tegenpesten (#nonauharcèlement).

Angèle (angele_vl), la chanteuse belge la plus célèbre du moment et l'influenceuse belge la plus suivie sur Instagram avec 3,6 millions d'abonnés (Statista, 2019), est engagée dans l'enseignent égalitaire et dans la lutte contre les discours de haine contre les femmes et la communauté LGBTI+, vision qui se reflète dans ses chansons.

- ## Bulgarie

Le cyberharcèlement a été abordé par le biais de plusieurs campagnes et organisations en ligne qui œuvrent à sa prévention et à la sensibilisation des jeunes, des parents et des enseignants à cette question sociale. Un exemple d'une telle campagne en ligne est les lignes directrices sur le cyberharcèlement élaborées par **Safenet.bg** (https://cyberbullying.safenet.bg/).

Ici, de manière très visuelle, les jeunes peuvent voir des exemples de cyberharcèlement, peuvent partager leurs expériences et signaler un incident via le lien fourni. Ils peuvent également lire des informations utiles, des conseils et des astuces concernant cette problématique.

Safenet.bg dispose également d'une chaîne YouTube (https://www.youtube.com/@safenetbg948) où sont publiées des vidéos sur le cyberharcèlement, sur les discours de haine en ligne, etc., et dont le but est de sensibiliser les jeunes à ces questions de manière plus attrayante et plus visuelle.

La société de télécommunications **Yettel** a également créé une chaîne YouTube (https://www.youtube.com/@YettelBulgaria) en 2020, où sont publiées des vidéos pour les jeunes les informant des différents risques en ligne auxquels les jeunes peuvent faire face, tels que les faux profils, le cyberharcèlement, les liens dangereux, les risques présents sur Tik-Tok, YouTube ou dans les jeux, etc.

5. Conclusion

5. CONCLUSIONS

Tout au long de ce manuel, le cyberharcèlement et le discours de haine ont été expliqués et contextualisés. Leurs définitions peuvent varier d'un pays à l'autre, mais les deux notions sont considérées comme une agression envers autrui. Dans le cas du harcèlement en ligne, il y a normalement trois acteurs: l'auteur, la victime et les témoins. Dans le cas du discours de haine, il est plus difficile d'établir un schéma unique, mais cette problématique, elle aussi, implique une personne qui en discrimine une autre.

Ce manuel présente différentes façons d'identifier, de traiter et de signaler le cyberharcèlement et les discours de haine. Toutefois, votre comportement dépendra de qui est la victime (vous-même, un collègue, vos enfants, etc.), tout en s'inscrivant dans le cadre juridique du pays où l'action se passe.

En Espagne, par exemple, vous pouvez rapporter à la police un cas de cyberharcèlement alors qu'aux Pays-Bas il existe une ligne d'assistance nationale contre la discrimination. En outre, il a été expliqué pourquoi des concepts tels que la protection des données ou la triade « confidentialité, intégrité et disponibilité » sont importants ainsi que des types de menaces à la vie privée telles que l'usurpation d'identité, le harcèlement sexuel en ligne, les phishings ou autres fraudes.

En conclusion, ce manuel ne propose pas seulement des définitions ou des concepts clés concernant le cyberharcèlement et les discours de haine: il sert également de guide pour prévenir, réagir et signaler ces types d'abus.

6. Références

6. RÉFÉRENCES

101 Data Protection Tips: How to Keep Your Passwords, Financial & Personal Information Online Safe in 2022. (2022, May 26). Digital Guardian. https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe

A, D. (2020). Cyberbullying (for Parents) - Nemours KidsHealth. Nemours KidsHealth. L https://kidshealth.org/en/parents/cyberbullying.html

A, D. (2020). Cyberbullying (for Parents) - Nemours KidsHealth. Nemours KidsHealth. https://kidshealth.org/en/parents/cyberbullying.html

(2018). Report security vulnerabilities | TikTok Help Center. TikTok. https://support.tiktok.com/en/safety-hc/reporting-security-vulnerabilities/reporting-the-security-vulnerabilities

Assistant Secretary for Public Affairs (ASPA). (2019b, December 4). Report Cyberbullying. StopBullying.Gov. https://www.stopbullying.gov/cyberbullying/how-to-report

Assistant Secretary for Public Affairs (ASPA). (2021, May 21). Tips for Teachers. StopBullying.Gov. https://www.stopbullying.gov/cyberbullying/tips-for-teachers

C, S. (2021). Password security: How to create strong passwords in 5 steps. Norton. https://us.norton.com/internetsecurity-privacy-password-security.html

Caroline Rizza. (2013). Social networks and Cyber-bullying among teenagers: EU Scientific e political report. https://doi.org/10.2788/41784

Celine Chateau. (2016). Policy department Citizen¡s rights and constitutional affairs. https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf

Center, C. R. (2021, October 18). Preventing Cyberbullying: Top Ten Tips for Adults Who Are Being Harassed Online. Cyberbullying Research Center. https://cyberbullying.org/preventing-cyberbullying-adults

CISCO. (2021). Think Before You Click [Slides]. CISCO. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/phishing-program-infographic.pdf

Commission for Personal Data Protection, available. (2019). FOLD. https://www.cpdp.bg/?p=element&aid=12

Convention on Cybercrim (No. 185). (2001, November). Convention on Cybercrime. https://rm.coe.int/1680081561

Cyberbullying Research Center. (2022). Cyberbullying Fact Sheet: Identification, Prevention, and Response. https://cyberbullying.org/cyberbullying-fact-sheet-identification-prevention-and-response

Defining online sexual harassment. (2021, December 15). Childnet. https://www.childnet.com/what-we-do/our-projects/project-deshame/defining-online-sexual-harassment/

Digital Guardian. (22–05-26). 101 Data Protection Tips: How to Keep Your Passwords, Financial & Personal Information Online Safe in 2022. https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe

Facebook - Meld je aan of registreer je. (2018). Facebook. https://www.facebook.com/unsupportedbrowser

Griffin, M. (2020, March 5). Advice on what to do if your child is a victim of cyber bullying. Laya Healthcare. https://www.layahealthcare.ie/thrive/family/what-to-do-if-your-child-is-victim-of-cyber-bullyi/

How to Protect Your Digital Privacy. (2019). The Privacy Project Guides - The New York Times. https://www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy

Identity Theft. (2022, June 12). Investopedia. https://www.investopedia.com/terms/i/identitytheft.asp

Instagram Help Center. (2018). Instagram. https://help.instagram.com/192435014247952?helpref=uf_permalink

J. (2013). Social Networks and Cyber-bullying among Teenagers. JRC Publications Repository. https://publications.jrc.ec.europa.eu/repository/handle/JRC80157

L. (2021, 28 enero). Ciberdelincuencia en el código penal - Letslaw. LetsLaw. https://letslaw.es/ciberdelincuencia/

L.J. (2022, June 2). Delitos en redes: de cinco años de cárcel a multas de hasta 2.700 euros. Diario Noticias de Álava. https://www.noticiasdealava.eus/vivir-on/internet-y-ciencia/2022/04/24/delitos-redes-consecuencias/1183252.html

Lex.bg - P—P°PєPsPSPë, PïCЂP°PIPëP»PSPëC†Pë, PєPsPSCЃC,PëC,CґC†PëCЏ, PєPsPґPµPєCЃPë, PґCЉЂCЂP¶P°PIPµPS PIPµCЃC,PSPëPє, PïCЂP°PIPëP»PSPëC†Pë PïPs PïCЂPëP»P°PiP°PSPµ. (2017). Lex.Bg. https://www.lex.bg/laws/ldoc/1589654529

P. (2020). Why is Data Protection Important? PECB. https://pecb.com/article/why-is-data-protection-important

S, G. Cyberstalking: Prevention, Consequences, and Coping. (2021, August 17). Verywell Mind. https://www.verywellmind.com/what-is-cyberstalking-5181466

Safety and security. (2018). Twitter. https://help.twitter.com/en/safety-and-security

W, The Dangers of Hacking and What a Hacker. (2020). © Copyright 2004 - 2022 Webroot Inc. All Rights Reserved. S https://www.webroot.com/us/en/resources/tips-articles/computer-security-threats-hackers

What Is Internet Fraud? Types of Internet Fraud. (2019). Fortinet. https://www.fortinet.com/resources/cyberglossary/internet-fraud

What is personal data? (2018, August 1). European Commission - European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

What Is Phishing? (2022, May 5). Cisco. https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html#%7Ehow-phishing-works

Wilkey Oh, E. (2020, March 15). Teachers' Essential Guide to Cyberbullying Prevention. Common Sense Education. https://www.commonsense.org/education/articles/teachers-essential-guide-to-cyberbullying-prevention

Ф. (2009). Киберсигурност. Фондация. https://www.netlaw.bg/bg/a/kiber-sigurnost

Si vous voulez en savoir plus sur #Digitsafe, visitez notre site web www.digit-safe.com

Ou contactez-nous à info@digit-safe.com

www.digit-safe.com
info@digit-safe.com