#DigitSafe

Renforcer les espaces numériques sûrs et la résilience

Manuel sur la résilience numérique

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

Contents

Introduction

Le projet « #DigitSafe-Boosting digital safe spaces and resilience » vise à donner aux jeunes les moyens de devenir des citoyens numériques capables de résilience et de prudence, leur permettant ainsi de relever certains défis et de lutter contre les effets négatifs de l'ère numérique. Ce projet fait suite à l'objectif 4 « information et dialogue constructif » de la stratégie de l'UE en faveur de la jeunesse 2017-2027.

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 matière de résilience numérique.

Le but de ce projet est également d'atteindre les trois objectifs suivants :

1. Promouvoir la citoyenneté numérique chez les jeunes des pays participants, en accord avec la stratégie de l'UE en faveur de la jeunesse 2017-2027, en leur communiquant des informations pratiques et concises en matière de sécurité, de confidentialité, de discours de haine et de cyberharcèlement.
2. Fournir aux jeunes les compétences nécessaires pour améliorer leur résilience numérique, en particulier à ceux qui ont moins d'opportunités ou qui manquent souvent d'informations et de connaissances en matière de données.
3. 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 moderne 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 guide consacré à la résilience numérique offrira des conseils exhaustifs et unifiés, grâce à des informations et des conseils pratiques (notamment des ressources juridiques, psychologiques, de formation et d'apprentissage ouvert), et formulera des recommandations clés pour aider les jeunes à acquérir une connaissance plus approfondie de leurs droits, des risques et des menaces numériques dans le contexte de ces sujets. Ce projet contribuera également à informer des possibilités et des ressources disponibles pour développer les compétences permettant de faire face aux problèmes que pose actuellement la vie numérique des jeunes. Dès lors, il donnera aux jeunes les moyens de devenir des citoyens numériques engagés et de favoriser un monde numérique plus sûr. Enfin, il rassemblera une grande quantité d'informations, en les regroupant de sorte qu'elles soient plus utiles et plus complètes.

#DigitSafe
Boosting digital safe spaces and resilience

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

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 plusieurs aspects selon les caractéristiques spécifiques 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 » 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 trois participants clés suivants :

- L'**auteur** : personne qui mène l'agression.
- La **victime** : personne qui subit l'agression.
- 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.

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.
Les caractéristiques clés du cyberharcèlement qui facilitent son identification et sa compréhension sont les suivantes :

- 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.
- L'acte 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.

- L’agression est répétitive 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 téléphones portables

Les Plateformes de Messagerie

Les Plateformes de Jeux

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 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 d'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)

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.

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.

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

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.(4)
- **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.

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

Le Centre de recherche sur le cyberharcèlement 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.

À l'attention des plus jeunes:

- 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.

- 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.
- 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.
- 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.
- 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 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.

À l'attention des enseignants et des parents:

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 le Cyberbullying Research Center en 2021 « Cyberharcèlement: comment l'identifier, le combattre et y répondre en 2021 » a donné une 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.

En d'autres termes, il est important de ne pas se contenter de l'éducation formelle, mais d'utiliser les activités extrascolaires et non officielles dans les écoles pour combattre et prévenir le cyberharcèlement d'un point de vue créatif.

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. »

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. 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 Recommandation : comment se comporter avec les victimes de cyberharcèlement ?

(Procédures, empathie, importance de l'écoute, soutien émotionnel, soutien psychologique)

Lorsque vous êtes vous-même une victime:

Si vous êtes victime de cyberharcèlement, nous vous conseillons cette une série d'étapes à suivre :

- Demandez de l'aide: tout d'abord, vous devez parler ; discutez-en avec vos proches ou avec des professionnels!
- Signalez 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.
- Protégez-vous: 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, supprimez votre compte ou modifiez votre pseudonyme.

- Répondez et rappelez 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-lui savoir 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.
- Coupez les ponts: Ne vous liez pas d'amitié avec ceux qui sont méchants et n'essayez pas 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.
- Ne réagissez pas: Les personnes qui harcèlent sur Internet cherchent à vous faire réagir. Toutefois, 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.
- Contactez 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.

- Déposez 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.
- Signalez 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).

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 une intelligence émotionnelle afin qu'ils puissent acquérir des compétences en matière de conscience de soi et 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 sur les médias numériques
- Apprenez-leur à réfléchir avant de publier du contenu.
- 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. 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, engagez la conversation sur ce qui se passe dans le calme, et écoutez-le. Prenez votre temps pour comprendre exactement ce qui s'est passé et le contexte dans lequel cela s'est produit.

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 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.

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 Measures 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 en soient la cible.

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.

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.

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 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 (5).

((5) Code of Conduct- Illegal Online Hate Speech Questions and Answers, (European Commission 2016)
https://ec.europa.eu/info/sites/default/files/code_of_conduct_hate_speech_en.pdf

2.2 Comment éviter le 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 d'empêcher les discours de haine(6):

- **Faites une pause** - retenez-vous d'écrire des commentaires haineux et/ou de partager un tel contenu;
- **Vérifiez 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;
- **Soutenez** - prenez publiquement position et faites preuve de solidarité envers les victimes du discours de haine;

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

- **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.

www.un.org/en/hate-speech/take-action/engage

2.3 Comment signaler le discours de haine ?

Les utilisateurs peuvent directement signaler 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. 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.

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 ;
- Parler à quelqu'un en qui vous avez confiance, par exemple un parent, un ami, ou un enseignant.

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.

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

1 **L'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.

2 Le 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).

3 Le phishing

Le phishing (ou hameçonnage) est 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.

4 La fraude sur Internet

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.

5 Arnaques dans les cartes de vœux

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 e-mail 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.

6 La fraude 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 des 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.

7 Les escroqueries sur les sites de rencontre

Les escroqueries sur les sites de rencontre en ligne sont un autre exemple typique de fraude sur Internet et 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.

8 L'escroquerie sur les frais de loterie

L'escroquerie sur les frais de loterie est autre forme courante de fraude sur Internet. Elle se fait par e-mail et 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.

9 Prince du Nigéria

L'arnaque du Prince du Nigéria 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.

10

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.

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.

https://www.facebook.com/help

Twitter

- Dans le Centre d'assistance de Twitter, 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.

https://help.twitter.com/en

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.

- 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.

https://help.instagram.com/

TikTok

- Si vous avez des questions, des préoccupations ou des problèmes concernant votre profil, vous pouvez trouver des informations et de l'aide ici. 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 ». Les étapes sont très faciles à suivre, il vous suffit de trouver l'option « signaler un problème » et de suivre les instructions.

https://support.tiktok.com/en/

3.4. Comment éviter les risques liés à la protection des données ?

L'une des choses les plus importantes à faire pour protéger nos données est d'avoir un mot de passe robuste. 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. 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.

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 pourra ensuite s'en servir.

Comment protéger vos données personnelles ?

1 Sécurisez vos comptes

2 Protégez votre navigation sur Internet

3 Utilisez un logiciel antivirus sur votre ordinateur

4 Mettez à jour vos logiciels et appareils

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

6 Désactivez le Bluetooth lorsque vous ne l'utilisez past

7 Soyez très prudent lorsque vous partagez des informations personnelles

8 Méfiez-vous des imposteurs

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

10 Personnalisez les paramètres de confidentialité de vos réseaux sociaux

11 N'oubliez pas de vous déconnecter

12 N'ouvrez pas de courriels provenant d'inconnus

13 N'enregistrez pas de mots de passe dans votre navigateur

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

15 Choisissez un fournisseur de courrier électronique sûr et réputé

4. Conclusion

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 le discours de haine : il sert également de guide pour prévenir, réagir et signaler ces types d'abus.

#DigitSafe
Boosting digital safe spaces and resilience

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

Questions et Informations:

info@digit-safe.com

www.digit-safe.com