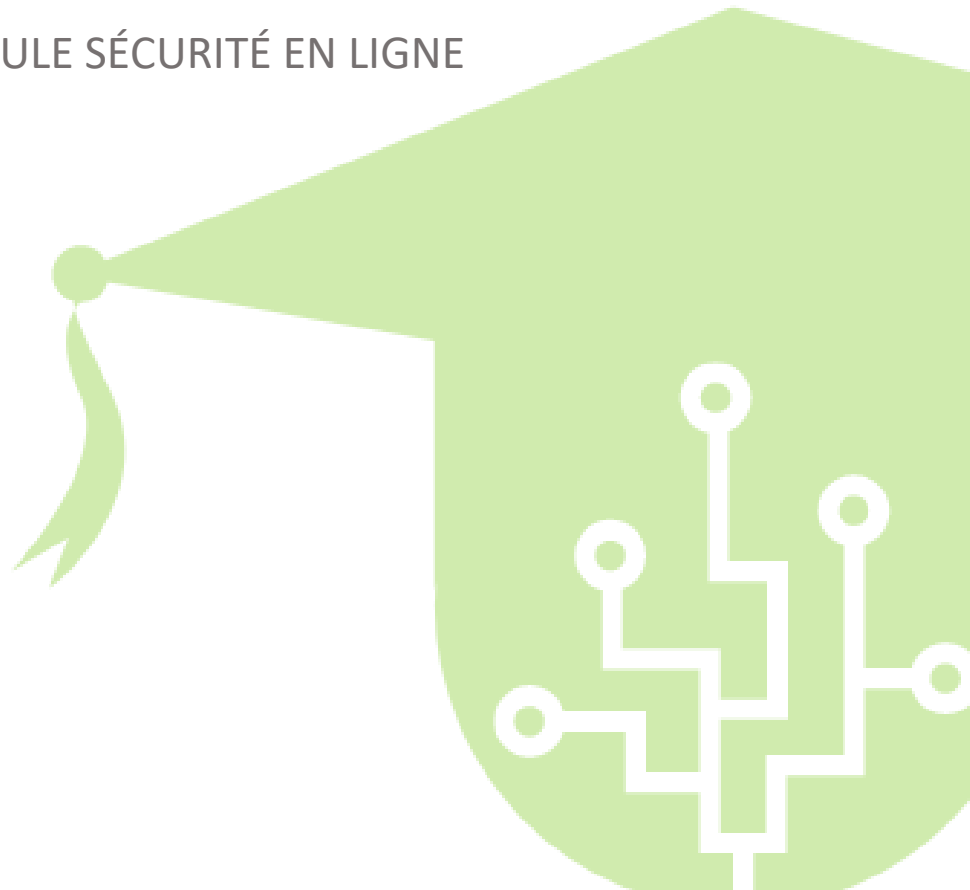
L2D

MEDIA LITERACY COMPETENCES FOR YOUTH WORKERS

LIGNES DIRECTRICES POUR UNE UTILISATION SÛRE DE L'INTERNET

MODULE SÉCURITÉ EN LIGNE



Titre :	LIGNES DIRECTRICES POUR UNE UTILISATION SÛRE DE L'INTERNET
Mots clés :	Sécurité en ligne, Sécurité Internet, Confidentialité numérique, Cybersécurité, Pratiques en ligne sûres, Protection des informations personnelles, Sécurité des données, Gestion des mots de passe, Menaces en ligne, Signalement des abus, Paramètres de confidentialité
Préparé par .	
Langue :	Anglais
Objectifs :	• Définir la sécurité en ligne : Expliquer le concept de sécurité en ligne et son importance dans le monde numérique d'aujourd'hui. • Identifier les menaces en ligne : Aidez les apprenants à reconnaître les différentes menaces en ligne telles que l'hameçonnage, les logiciels malveillants, l'usurpation d'identité, la cyberintimidation et les escroqueries. • Comprendre les préoccupations en matière de protection de la vie privée : Sensibiliser les participants à l'importance de la protection des informations personnelles en ligne et aux conséquences potentielles des atteintes à la vie privée. • Développer des mots de passe forts : Enseigner les techniques de création de mots de passe forts et uniques pour renforcer la sécurité des comptes. • Se prémunir contre les tentatives d'hameçonnage : Fournir des stratégies pour détecter et éviter d'être victime de courriels, de messages et de sites web d'hameçonnage. • Sécuriser les profils de médias sociaux : Proposez des lignes directrices pour ajuster les paramètres de confidentialité, contrôler le partage d'informations personnelles et gérer les demandes d'amis. • Promouvoir une communication en ligne sûre : Enseignez des méthodes efficaces pour communiquer en toute sécurité sur les médias sociaux, les forums et les plateformes de messagerie, en insistant sur le fait qu'il faut éviter de partager des détails sensibles. • Développer l'esprit critique : Favoriser la capacité à évaluer les informations et les sources de manière critique, en particulier dans le contexte des "fake news" et de la désinformation en ligne. • Faire face au harcèlement en ligne et à la traque : Proposer des conseils sur la manière de réagir et de signaler les cas de harcèlement en ligne ou de traque.

Résultats de l'apprentissage :	
Index du contenu :	1. SÉCURITÉ SUR INTERNET 1.1.DÉFINITION DE LA SÉCURITÉ SUR INTERNET 1.2.COMPRENDRE LE CHAMP D'APPLICATION ET L'IMPORTANCE 1.2.1. Champ d'application de la sécurité sur Internet 1.2.2. Importance de la sécurité sur Internet 1.3.ÉVOLUTION DES CONCEPTS DE SÉCURITÉ SUR L'INTERNET 1.4.Les éléments clés d'une expérience en ligne sûre 2. MENACES EN LIGNE 2.1.LES TYPES DE MENACES EN LIGNE 2.2.RECONNAÎTRE LES SIGNES D'ALERTE 2.3.LES CONSÉQUENCES DE L'IGNORANCE DES MENACES EN LIGNE 3. PROTECTION DES INFORMATIONS PERSONNELLES 3.1. IMPORTANCE DE LA PROTECTION DE LA VIE PRIVEE 3.2.GESTION SÉCURISÉE DU COMPTE EN LIGNE 3.3.PARTAGE RESPONSABLE DES MÉDIAS SOCIAUX 4. NAVIGUER EN TOUTE SÉCURITÉ DANS LES MÉDIAS SOCIAUX 4.1.RÉGLAGE DES PARAMÈTRES DE CONFIDENTIALITÉ 4.2.GÉRER LES DEMANDES D'AMIS ET LES MESSAGES 4.3.SIGNALER ET BLOQUER LES COMPTES ABUSIFS 5. CYBERSÉCURITÉ ET DISPOSITIFS MOBILES 5.1.SÉCURISER LES SMARTPHONES ET LES TABLETTES

	5.2. AUTORISATIONS D'UTILISATION DES APPLICATIONS ET ACCÈS AUX DONNÉES 5.3. PROTÉGER LES APPAREILS MOBILES CONTRE LE VOL ET LA PERTE
Développement du contenu :	1. SÉCURITÉ SUR INTERNET 1.1. DÉFINITION DE LA SÉCURITÉ SUR INTERNET La sécurité sur Internet, également connue sous le nom de sécurité en ligne, est la pratique qui consiste à adhérer à des lignes directrices applicables, à acquérir une compréhension globale de la technologie moderne et à protéger de manière proactive ses appareils numériques pour se défendre contre les divers aspects malveillants du monde en ligne. Alors que le nombre d'utilisateurs de l'internet continue d'augmenter dans le monde, diverses parties prenantes, notamment les gouvernements, les organisations et les fournisseurs d'accès à l'internet, se préoccupent de plus en plus de la sécurité des populations vulnérables, telles que les enfants, les adolescents et les personnes âgées, lorsqu'elles s'aventurent dans le vaste domaine virtuel. Des statistiques alarmantes révèlent que plus de 45 % des utilisateurs de l'internet ont déclaré avoir été victimes d'une forme ou d'une autre de cyberharcèlement, ce qui souligne la nécessité urgente de promouvoir des pratiques en ligne plus sûres et de cultiver une culture de la responsabilité numérique. Pour répondre à ces préoccupations pressantes et plaider en faveur d'un paysage numérique plus sûr, la Journée pour un internet plus sûr est célébrée à l'échelle mondiale chaque année en février. Cet événement annuel sert de plateforme dédiée à la sensibilisation à la sécurité sur Internet, encourageant les individus et les communautés à être vigilants, informés et proactifs dans leurs interactions en ligne. Les gouvernements, les organisations à but non lucratif et les entreprises technologiques du monde entier participent activement aux initiatives de la Journée Safer Internet, en organisant des campagnes de

	sensibilisation, des ateliers éducatifs et des événements interactifs afin de doter les internautes des connaissances et des compétences nécessaires pour naviguer en toute sécurité dans le monde en ligne. Au Royaume-Uni, la campagne Get Safe Online s'est imposée comme une force de premier plan dans la promotion de la sécurité sur l'internet. Grâce au parrainage essentiel de l'agence gouvernementale Serious Organized Crime Agency (SOCA) et à la collaboration de grandes sociétés Internet telles que Microsoft et eBay, la campagne vise à donner aux internautes des conseils pratiques et des ressources pour se protéger contre les cybermenaces. Grâce à des informations, des conseils et des outils facilement accessibles, Get Safe Online s'efforce d'améliorer la résilience numérique des individus, rendant la communauté Internet du Royaume-Uni plus robuste et moins vulnérable aux dangers en ligne. Alors que l'internet continue d'évoluer et de jouer un rôle de plus en plus important dans notre vie quotidienne, il devient primordial de garantir la sécurité sur l'internet. En encourageant une culture du comportement responsable en ligne, en sensibilisant le public par des initiatives telles que la Journée pour un internet plus sûr et en fournissant des ressources accessibles telles que la campagne "Get Safe Online", nous pouvons collectivement œuvrer à la création d'un environnement numérique plus sûr et plus sécurisé pour tous. Dans notre monde toujours connecté, on ne saurait trop insister sur l'importance de la sécurité sur l'internet. L'internet offre des possibilités inégalées d'apprentissage, de communication et de divertissement, mais il expose également les utilisateurs à des risques et des dangers potentiels. À mesure que la technologie progresse et que les menaces en ligne deviennent plus sophistiquées, il est essentiel pour les personnes de tous âges de rester informées et proactives en matière de sécurité sur l'internet. Pour les enfants et les adolescents, qui sont souvent des natifs du numérique, il est essentiel de

	comprendre la sécurité sur internet pour avoir des interactions en ligne responsables et sûres. Les parents, les éducateurs et les tuteurs jouent un rôle essentiel en guidant les jeunes utilisateurs d'internet, en leur apprenant les risques potentiels liés au partage d'informations personnelles, aux relations avec des inconnus et à la participation à des activités en ligne dangereuses. Pour renforcer la sécurité sur internet, il est essentiel de se tenir au courant des dernières tendances et des meilleures pratiques en matière de cybersécurité. La mise à jour régulière des logiciels et des applications, l'utilisation d'un logiciel antivirus réputé et l'activation des mises à jour automatiques peuvent renforcer la défense des appareils numériques contre les menaces émergentes. En outre, l'intégration de l'authentification multifactorielle dans la mesure du possible ajoute une couche supplémentaire de protection aux comptes en ligne. La promotion d'une communauté en ligne positive et sûre passe également par la promotion de l'empathie et du respect numériques. Encourager la gentillesse et l'empathie dans les interactions en ligne permet de lutter contre la cyberintimidation et les comportements toxiques, et de faire de l'internet un espace plus accueillant pour tous. 1.2. COMPRENDRE LA PORTÉE ET L'IMPORTANCE 1.2.1. Champ d'application de la sécurité sur Internet ● Protection contre les cybermenaces telles que les virus, les logiciels malveillants, le phishing, les ransomwares et l'usurpation d'identité. ● Protéger les informations personnelles et l'identité numérique contre les accès non autorisés et les abus. ● Naviguer de manière responsable dans les médias sociaux et faire face à la cyberintimidation ou au harcèlement en ligne.

	• Garantir la sécurité des transactions en ligne et protéger les informations financières lors d'achats ou de transactions bancaires en ligne. • Utiliser et gérer les appareils mobiles en toute sécurité afin d'éviter les violations de données et de la vie privée. • Reconnaître et éviter les escroqueries en ligne, les sites web frauduleux et les tentatives d'hameçonnage. • Enseigner aux enfants et aux adolescents la sécurité en ligne et les aider à développer des habitudes numériques responsables. 1.2.2. Importance de la sécurité sur Internet • Protection des informations personnelles et financières : Les mesures de sécurité sur Internet protègent les données sensibles, évitant ainsi l'usurpation d'identité et la fraude financière. • Préserver la vie privée et la réputation numérique : Le fait d'être attentif aux activités en ligne aide les individus à préserver leur vie privée et à protéger leur réputation numérique. • Protection contre les cybermenaces : La sensibilisation aux risques en ligne et le respect des pratiques de sécurité permettent de se prémunir contre les cybermenaces qui peuvent perturber la vie quotidienne, les activités commerciales ou compromettre des informations sensibles. • Favoriser les expériences numériques positives : La sécurité sur l'internet permet aux individus de vivre des expériences positives et enrichissantes en ligne sans craindre d'être harcelés ou victimisés. • Encourager la citoyenneté numérique : En pratiquant la sécurité sur l'internet, les individus contribuent à la construction d'une communauté numérique responsable et respectueuse. • Impact économique : Les incidents de cybersécurité peuvent avoir de graves conséquences économiques pour les particuliers, les entreprises et les gouvernements, ce qui fait de la sécurité sur l'internet un aspect essentiel de la sécurité globale. • Protéger les personnes vulnérables : La sécurité sur l'internet est particulièrement cruciale pour les

enfants, les adolescents et les populations vulnérables qui peuvent être plus sensibles aux dangers en ligne.

1.3. ÉVOLUTION DES CONCEPTS DE SÉCURITÉ SUR L'INTERNET

L'évolution des concepts de sécurité sur l'internet fait référence à la manière dont la compréhension de la sécurité sur l'internet et les mesures prises pour protéger les utilisateurs des menaces en ligne ont évolué au fil du temps. Au fur et à mesure que l'internet s'est développé et transformé, les défis posés par les cybermenaces se sont multipliés, ce qui a conduit à l'élaboration de nouveaux concepts et de nouvelles stratégies pour garantir la sécurité en ligne. Cette section se penche sur le contexte historique et les étapes clés qui ont façonné les pratiques en matière de sécurité sur l'internet.

- Les débuts de l'internet : Dans les premiers temps de l'internet, le concept de sécurité en ligne était relativement simpliste. La plupart des utilisateurs étaient des personnes ou des professionnels compétents en matière de technologie qui comprenaient les risques associés au partage d'informations personnelles en ligne. Toutefois, le grand public n'était guère sensibilisé aux cybermenaces potentielles.

- L'essor de la communication en ligne : Avec l'apparition des plateformes de communication en ligne et des médias sociaux, la sécurité sur l'internet a pris de nouvelles dimensions. Les utilisateurs ont commencé à partager davantage d'informations personnelles, ce qui a suscité des préoccupations croissantes en matière de protection de la vie privée et d'usurpation d'identité. Des concepts tels que l'hameçonnage et les courriels non sollicités ont commencé à prendre de l'importance, les cybercriminels cherchant à exploiter la confiance des utilisateurs.

- Des mesures pionnières en matière de cybersécurité : Face à la multiplication des

	menaces, les mesures de cybersécurité ont commencé à évoluer. Les logiciels antivirus, les pare-feu et les technologies de cryptage sont devenus des outils essentiels de protection contre les logiciels malveillants et les accès non autorisés. Ces premières solutions de cybersécurité ont jeté les bases de mécanismes de protection plus avancés à l'avenir. ● Campagnes et initiatives de sensibilisation : Face à la généralisation des cybermenaces, plusieurs organisations, gouvernements et entreprises technologiques ont commencé à lancer des campagnes et des initiatives de sensibilisation pour éduquer le public à la sécurité sur l'internet. Ces efforts visaient à sensibiliser le public aux risques courants en ligne et à encourager les utilisateurs à adopter des pratiques en ligne plus sûres. ● Inquiétudes croissantes concernant la cyberintimidation : L'essor des médias sociaux et de la communication en ligne a également attiré l'attention sur la question de la cyberintimidation. Avec l'augmentation des cas de harcèlement en ligne et de cyberintimidation, les efforts en matière de sécurité sur internet se sont multipliés pour faire face à cette forme d'agression numérique et soutenir les personnes concernées. ● L'internet mobile et les nouveaux défis : L'avènement des smartphones et de l'accès à l'internet mobile a introduit une nouvelle série de défis pour la sécurité de l'internet. Les risques uniques associés aux appareils mobiles, tels que les autorisations d'applications et les logiciels malveillants mobiles, ont nécessité des mesures de sécurité adaptées. ● Progrès en matière d'authentification : Les mots de passe s'étant révélés insuffisants pour protéger les comptes en ligne, l'authentification à deux facteurs (2FA) et l'authentification à plusieurs

	facteurs (MFA) ont gagné en popularité. Ces méthodes offrent un niveau de sécurité supplémentaire, réduisant le risque d'accès non autorisé. ● L'accent mis sur la culture numérique : les concepts de sécurité sur l'internet ont commencé à englober non seulement les mesures de sécurité technique, mais aussi la culture numérique et les compétences en matière d'esprit critique. L'éducation des utilisateurs à l'identification de la désinformation, des fausses nouvelles et des escroqueries en ligne est devenue vitale dans la lutte contre les menaces en ligne. ● L'essor du secteur de la cybersécurité : La sophistication croissante des cybermenaces a donné naissance à un solide secteur de la cybersécurité. Les entreprises et les professionnels spécialisés dans les services de cybersécurité, l'analyse des menaces et la réponse aux incidents ont joué un rôle crucial dans la défense contre les risques en ligne en constante évolution. ● Intégration de la sécurité sur Internet dans l'enseignement : Reconnaissant l'importance de l'éducation à la sécurité sur internet, les écoles et les établissements d'enseignement ont commencé à l'intégrer dans leur programme. Enseigner aux enfants et aux jeunes adultes un comportement responsable en ligne et la citoyenneté numérique est devenu un aspect essentiel de l'éducation moderne. L' éducation aux médias est une matière d'enseignement qui a vu le jour dans le but de fournir aux gens tous les outils nécessaires pour mieux comprendre la dynamique et les messages offerts par les médias, et pour les retravailler d'une manière indépendante et critique. Aujourd'hui, il est nécessaire d'apprendre aux gens à mieux gérer leur relation avec les médias sociaux, de les éduquer et de les former sur "quoi et comment poster" ou comment reconnaître les

	"fake news". L'utilisation d'Internet grâce aux smartphones offre un potentiel d'apprentissage infini, mais aussi des risques liés à "l'utilisation superficielle de ces outils". Les "immigrés numériques" sont les plus exposés car ils ne sont pas habitués à gérer les règles non écrites d'un monde virtuel auquel ils n'appartiennent pas. Souvent, ils ne connaissent pas les principaux systèmes de communication et n'ont pas la capacité de traiter les nouveaux messages afin d'offrir leur propre contribution à la communauté, restant ainsi des éléments passifs. 1.4. Les éléments clés d'une expérience en ligne sûre Les "éléments clés d'une expérience en ligne sûre" sont des éléments essentiels qui contribuent à créer un environnement sûr et protégé lors de l'utilisation de l'internet. Ces éléments englobent diverses pratiques, comportements et outils que les individus peuvent utiliser pour garantir leur sécurité et leur vie privée en ligne. La compréhension et la mise en œuvre de ces éléments clés sont essentielles pour une expérience positive et sûre de l'internet. ● Sensibilisation à la cybersécurité : Une bonne sensibilisation à la cybersécurité est essentielle pour une expérience en ligne sûre. Il s'agit de se tenir informé des dernières cybermenaces, de comprendre les méthodes d'attaque courantes telles que le phishing et les logiciels malveillants, et de reconnaître les signes avant-coureurs d'activités suspectes. La sensibilisation permet aux individus de prendre des décisions éclairées et de prendre les précautions nécessaires lorsqu'ils naviguent dans le monde numérique. ● Protection de la vie privée : La protection de la vie privée est un aspect essentiel de la sécurité sur l'internet. Il s'agit de faire attention aux informations partagées en ligne et d'éviter de divulguer trop de détails personnels. La protection des données sensibles, telles que les informations financières et les documents

	d'identité, est essentielle pour prévenir l'usurpation d'identité et la fraude. ● Authentification forte : Il est essentiel d'utiliser des méthodes d'authentification solides pour les comptes en ligne. Il s'agit notamment d'utiliser des mots de passe forts et uniques pour chaque compte et de tirer parti de couches de sécurité supplémentaires telles que l'authentification à deux facteurs (2FA) ou l'authentification biométrique lorsqu'elles sont disponibles. Les mesures d'authentification forte permettent d'empêcher l'accès non autorisé aux comptes et de protéger les informations sensibles. ● Pratiques de navigation sûres : Il est nécessaire d'adopter des habitudes de navigation sûres pour éviter les sites web malveillants et les menaces potentielles. Il s'agit notamment de vérifier les URL des sites web avant de saisir des informations sensibles, d'éviter de cliquer sur des liens ou des pop-ups suspects et d'utiliser des navigateurs sécurisés dotés de protections intégrées. ● Mises à jour régulières des logiciels : Il est essentiel de maintenir les logiciels, les systèmes d'exploitation et les applications à jour pour garantir la sécurité de l'expérience en ligne. Les mises à jour régulières comprennent souvent des correctifs de sécurité qui corrigent les vulnérabilités connues, ce qui rend plus difficile leur exploitation par les cybercriminels. ● Réseaux sécurisés : Il est essentiel de se connecter à des réseaux sécurisés et fiables pour protéger les données en transit. Il est essentiel d'éviter les réseaux Wi-Fi publics dépourvus de mesures de sécurité adéquates afin de prévenir l'interception potentielle de données et l'accès non autorisé.

	• Pratiques sûres en matière de médias sociaux : Il est essentiel d'être prudent lors de l'utilisation des plateformes de médias sociaux pour protéger les informations personnelles et éviter d'être victime d'attaques d'ingénierie sociale. Régler les paramètres de confidentialité, être sélectif dans les demandes d'amis et s'abstenir de partager publiquement des données sensibles sont des pratiques essentielles de sécurité sur les médias sociaux. • Vigilance contre le phishing : il est essentiel d'être vigilant contre les tentatives de phishing. Cela implique de vérifier l'identité des expéditeurs d'e-mails, de ne pas cliquer sur des liens suspects ou de ne pas télécharger des pièces jointes provenant de sources inconnues, et de signaler les tentatives d'hameçonnage. • Contrôle parental et supervision : Pour les parents et les tuteurs, la mise en place d'un contrôle parental et la surveillance des activités en ligne des enfants sont des éléments essentiels d'une expérience sûre de l'internet pour les jeunes utilisateurs. Cela permet d'assurer un accès au contenu adapté à l'âge et de protéger les enfants des contenus en ligne potentiellement dangereux. • Culture numérique et esprit critique : Le développement de la culture numérique et de l'esprit critique est essentiel pour identifier la désinformation, les fausses nouvelles et les escroqueries en ligne. Comprendre comment évaluer les sources d'information et vérifier la crédibilité du contenu contribue à une expérience en ligne plus sûre. 2. MENACES EN LIGNE 2.1. LES TYPES DE MENACES EN LIGNE

	Les types de menaces en ligne font référence aux diverses activités et attaques malveillantes qui peuvent mettre en péril la sécurité, la vie privée et l'intégrité des utilisateurs d'Internet et de leurs données. Il est essentiel de comprendre ces menaces pour prendre les précautions qui s'imposent et se protéger en naviguant dans le paysage numérique. Voici quelques types courants de menaces en ligne : **Phishing :** Le phishing est une technique trompeuse utilisée par les cybercriminels pour inciter les utilisateurs à révéler des informations sensibles, telles que des identifiants de connexion, des détails financiers ou des données personnelles. Les tentatives d'hameçonnage impliquent souvent de faux courriels, sites web ou messages qui imitent des entités légitimes afin d'inciter les victimes à fournir leurs informations. **Les logiciels malveillants :** Les logiciels malveillants sont des logiciels malveillants conçus pour infecter et endommager les appareils ou les réseaux. Ils comprennent les virus, les vers, les chevaux de Troie, les rançongiciels et les logiciels espions. Les logiciels malveillants peuvent compromettre les données, voler des informations, perturber les opérations, voire rendre les appareils inutilisables. **Ransomware :** Les rançongiciels sont des logiciels malveillants spécifiques qui cryptent les données d'un utilisateur, l'empêchant ainsi d'accéder à ses propres fichiers ou systèmes. Les cybercriminels exigent le paiement d'une rançon pour fournir la clé de décryptage, mais il n'y a aucune garantie que le paiement de la rançon entraînera la restitution des données. **Ingénierie sociale :** L'ingénierie sociale consiste à manipuler des individus pour obtenir un accès non autorisé à des informations ou des systèmes sensibles. Cela peut se faire par l'usurpation d'identité, la manipulation ou l'exploitation de la psychologie humaine pour tromper les utilisateurs et les amener à révéler des informations confidentielles. **Violation de données :** Une violation de données se produit lorsque des cyber-attaquants accèdent sans autorisation aux données d'une organisation ou d'un individu. Il peut s'agir d'informations personnelles, de dossiers financiers ou de propriété intellectuelle. Les

	violations de données peuvent avoir de graves conséquences sur la vie privée des individus et conduire à des vols d'identité ou à des pertes financières. **L'usurpation d'identité :** L'usurpation d'identité consiste à voler des informations personnelles, telles que des numéros de sécurité sociale, des détails de cartes de crédit ou des identifiants de connexion, pour se faire passer pour quelqu'un d'autre à des fins frauduleuses. Les cybercriminels peuvent utiliser ces informations volées à des fins lucratives ou pour commettre d'autres délits. **La cyberintimidation :** La cyberintimidation est une forme de harcèlement ou d'intimidation en ligne, qui se produit généralement sur les plateformes de médias sociaux ou par le biais d'applications de messagerie. Il s'agit d'envoyer des messages blessants, de répandre des rumeurs ou de partager des contenus embarrassants dans l'intention de nuire, d'intimider ou d'humilier la victime. **Attaques par déni de service (DoS) et par déni de service distribué (DDoS) :** Les attaques DoS et DDoS visent à submerger un site web ou un service en ligne d'un flot de trafic, le rendant inaccessible aux utilisateurs légitimes. Ces attaques peuvent perturber les services en ligne et entraîner des pertes financières pour les entreprises. **Attaques de type "Man-in-the-Middle" (MitM) :** Les attaques MitM impliquent l'interception et l'écoute des communications entre deux parties, telles qu'un utilisateur et un site web. L'attaquant peut alors visualiser ou manipuler les données échangées à l'insu des parties qui communiquent. **Exploits de type "jour zéro" :** Les exploits de type "jour zéro" ciblent les vulnérabilités des logiciels qui ne sont pas encore connues du fournisseur ou des développeurs. Les cybercriminels utilisent ces vulnérabilités pour lancer des attaques avant qu'un patch ou un correctif ne soit disponible, ce qui les rend difficiles à défendre. **Vulnérabilités de l'internet des objets (IdO) :** Alors que de plus en plus d'appareils sont connectés à l'internet, les vulnérabilités de l'IdO sont devenues un sujet de préoccupation. La faiblesse des mesures de sécurité des appareils IoT peut être exploitée pour

	accéder aux réseaux domestiques ou compromettre la vie privée. 2.2. RECONNAÎTRE LES SIGNES D'ALERTE Reconnaître les signes d'alerte est une compétence essentielle en matière de sécurité sur l'internet. Il s'agit d'être attentif aux indicateurs indiquant que quelque chose ne va pas ou est potentiellement dangereux lors de l'utilisation de l'internet. En reconnaissant les signes d'alerte, les individus peuvent agir rapidement pour se protéger des menaces en ligne et éviter d'être victimes d'escroqueries, de cyberattaques ou d'autres activités malveillantes. Voici quelques signes d'alerte importants à surveiller : **Communication non sollicitée :** Méfiez-vous des courriels non sollicités, des messages ou des demandes d'amis provenant de sources inconnues ou suspectes. Les cybercriminels utilisent souvent ces moyens pour lancer des tentatives d'hameçonnage ou diffuser des logiciels malveillants. **Mauvaise grammaire et orthographe :** De nombreux courriels d'hameçonnage et messages frauduleux contiennent des erreurs grammaticales, des fautes d'orthographe ou un langage maladroit. Ces erreurs peuvent être le signe que la communication ne provient pas d'une source légitime. **Demandes d'informations personnelles :** Méfiez-vous des demandes d'informations sensibles, telles que les identifiants de connexion, les données financières ou les numéros de sécurité sociale, en particulier si la demande est inattendue ou semble inutile. **Langage urgent ou menaçant :** Les messages qui utilisent un langage urgent ou menaçant pour vous pousser à agir immédiatement peuvent être des indicateurs d'une escroquerie ou d'une tentative d'hameçonnage. **Liens ou URL inhabituels :** Passez votre souris sur les liens dans les courriels ou les messages pour voir la destination réelle de l'URL. Méfiez-vous des URL raccourcis ou des liens qui redirigent vers des sites web suspects. **Adresses URL non concordantes ou fausses :** Faites attention aux URL qui semblent légitimes mais qui présentent des fautes d'orthographe ou des variations subtiles. Les escrocs peuvent utiliser des noms de domaine

qui ressemblent beaucoup à des sites web connus pour tromper les utilisateurs.

Expéditeurs de courrier électronique inconnus : Vérifiez l'identité des expéditeurs de courrier électronique, en particulier si le message contient des pièces jointes inattendues ou des demandes d'informations sensibles.

Téléchargements inattendus : Méfiez-vous des téléchargements ou des pièces jointes que vous n'avez pas initiés ou que vous n'attendiez pas, car ils peuvent contenir des logiciels malveillants.

Activité inhabituelle du compte : Examinez régulièrement l'activité de votre compte en ligne et soyez attentif à toute connexion ou transaction non autorisée.

Comportement inexpliqué du système : Si votre ordinateur ou votre appareil se comporte de manière inhabituelle, comme des pannes fréquentes, des ralentissements ou des fenêtres contextuelles inattendues, cela peut indiquer la présence de logiciels malveillants ou d'autres problèmes de sécurité.

Avertissements des logiciels de sécurité : Prêtez attention aux avertissements ou aux alertes de votre antivirus ou de votre logiciel de sécurité, car ils peuvent indiquer des menaces potentielles ou des activités suspectes.

Offres et promotions non sollicitées : Méfiez-vous des offres ou des promotions non sollicitées qui semblent trop belles pour être vraies, car il peut s'agir d'escroqueries visant à vous inciter à fournir des informations personnelles.

2.3. LES CONSÉQUENCES DE L'IGNORANCE DES MENACES EN LIGNE

Ignorer les menaces en ligne peut avoir des conséquences graves et profondes qui peuvent avoir un impact négatif sur les individus, les entreprises et même la société dans son ensemble. Le fait de ne pas s'attaquer aux menaces en ligne ou de ne pas prendre les mesures qui s'imposent peut rendre une personne vulnérable à divers cyberrisques, ce qui peut entraîner des pertes financières, des atteintes à la vie privée, des atteintes à la réputation, voire des répercussions juridiques. Voici quelques-unes des principales conséquences de l'ignorance des menaces en ligne :

	Pertes financières : Être victime d'escroqueries, d'attaques par hameçonnage ou de manœuvres frauduleuses en ligne peut entraîner d'importantes pertes financières. Les cybercriminels peuvent voler des identifiants bancaires, des informations sur les cartes de crédit ou effectuer des transactions non autorisées, ce qui entraîne des pertes sur les comptes bancaires et des difficultés financières. **L'usurpation d'identité :** Ignorer les signes avant-coureurs d'un vol d'identité peut permettre aux cybercriminels de voler des informations personnelles, telles que les numéros de sécurité sociale, les dates de naissance et les adresses. Ils peuvent utiliser ces informations volées pour commettre des fraudes financières, ouvrir des comptes au nom de la victime ou se livrer à d'autres activités criminelles, ce qui peut avoir de graves conséquences à long terme pour la victime. **Violations de données :** Le fait de ne pas mettre en œuvre des mesures de sécurité solides ou de ne pas remédier aux vulnérabilités peut entraîner des violations de données pour les individus et les organisations. Une violation de données peut exposer des informations sensibles, notamment des données clients, des secrets commerciaux ou des éléments de propriété intellectuelle, entraînant des pénalités financières, des responsabilités juridiques et une atteinte à la réputation de l'organisation. **Attaques par ransomware :** Ignorer les pratiques de cybersécurité peut rendre les particuliers et les entreprises vulnérables aux attaques de ransomware. Lorsque les systèmes sont compromis par un ransomware, des données précieuses peuvent être cryptées et les attaquants exigent le paiement de la clé de décryptage. Le paiement de la rançon ne garantit pas la récupération des données, et les victimes peuvent subir des pertes de données ou des perturbations opérationnelles. **Atteinte à la réputation :** Être la proie de la cyberintimidation ou d'attaques sur les médias sociaux peut nuire considérablement à la réputation des individus et des organisations. De fausses informations, des critiques négatives ou des contenus nuisibles diffusés en ligne peuvent nuire à la réputation d'une personne ou d'une marque, ce qui affecte la position sociale, les opportunités professionnelles et la confiance des clients. **Perte de la vie privée :** Ignorer les préoccupations en matière de protection de la vie privée peut conduire à l'exposition d'informations privées, y compris des

	conversations personnelles, des images ou des vidéos. Cette perte de vie privée peut avoir des conséquences émotionnelles et psychologiques, ainsi que des menaces potentielles de chantage. **Conséquences juridiques :** L'ignorance des cybermenaces et l'absence de mise en œuvre des mesures de sécurité nécessaires peuvent avoir des conséquences juridiques. Les personnes ou les organisations peuvent faire l'objet de poursuites judiciaires, d'amendes ou de sanctions réglementaires en cas de violation des données, de violation de la vie privée ou de non-respect des normes de cybersécurité. **Perturbation des services :** Les entreprises qui ignorent les menaces en ligne risquent de voir leurs activités perturbées. Les cyberattaques, telles que les attaques par déni de service distribué (DDoS), peuvent surcharger les sites web ou les réseaux, rendant les services inaccessibles aux clients et entraînant une perte de revenus et de crédibilité. **Impact social et émotionnel :** Ignorer la cyberintimidation, le harcèlement en ligne ou les comportements prédateurs peut avoir de graves conséquences sociales et émotionnelles pour les victimes. Cela peut conduire à l'anxiété, à la dépression, à l'isolement et même à des pensées d'automutilation. **Préoccupations en matière de sécurité nationale :** Ignorer les menaces en ligne peut dépasser le niveau individuel ou organisationnel et devenir une question de sécurité nationale. Les cyberattaques contre les infrastructures critiques ou les systèmes gouvernementaux peuvent perturber les services essentiels, compromettre des informations sensibles et porter atteinte à la stabilité nationale. 3. PROTECTION DES INFORMATIONS PERSONNELLES 3.1. IMPORTANCE DE LA PROTECTION DE LA VIE PRIVEE La protection de la vie privée est d'une importance capitale à l'ère numérique actuelle en raison de l'utilisation généralisée de la technologie et de l'internet. Elle consiste à protéger les informations personnelles, les données et les activités en ligne d'un individu contre tout accès non autorisé, toute utilisation abusive et toute exploitation. L'importance de la

	protection de la vie privée peut être appréhendée sous différents angles : **Sécurité personnelle :** La protection de la vie privée garantit que les informations personnelles sensibles, telles que les numéros de sécurité sociale, les données financières ou les adresses personnelles, restent confidentielles et sécurisées. Empêcher l'accès non autorisé à ces informations permet de prévenir l'usurpation d'identité, la fraude financière et d'autres formes de cybercriminalité qui peuvent avoir de graves conséquences pour les individus. **Confidentialité et contrôle des données :** Les individus ont le droit de contrôler la manière dont leurs données sont collectées, stockées et utilisées par les organisations. La protection de la vie privée garantit que les individus peuvent choisir en connaissance de cause de partager leurs données et consentir à ce qu'elles soient utilisées à des fins spécifiques. **Maintien de la confiance :** La protection de la vie privée est essentielle pour établir et maintenir la confiance entre les individus et les organisations. Lorsque les utilisateurs sont convaincus que leurs informations personnelles seront traitées de manière responsable et sécurisée, ils sont plus enclins à utiliser les services en ligne, à effectuer des transactions et à partager des informations en toute confiance. **Préserver la liberté individuelle :** Respecter la vie privée signifie permettre aux individus de s'exprimer librement, sans crainte de surveillance ou de discrimination fondée sur leurs activités ou préférences en ligne. La protection de la vie privée est essentielle au respect du droit à la liberté de parole et d'expression. **Prévention du harcèlement en ligne et de la traque :** La protection de la vie privée protège les individus contre le harcèlement et la traque en ligne. En limitant l'accès aux informations personnelles, les mesures de protection de la vie privée réduisent le risque d'attaques ciblées ou de cyberintimidation. **Protéger les relations personnelles :** La protection de la vie privée permet aux individus de communiquer et de partager des informations dans le cadre de relations de confiance, en garantissant la confidentialité des conversations et des interactions privées.

	Éviter l'utilisation abusive des données : La protection de la vie privée réduit le risque que les données personnelles soient exploitées à des fins autres que celles prévues par l'individu. Il s'agit notamment d'éviter les campagnes de marketing non désirées, les courriers électroniques non sollicités ou les contenus personnalisés susceptibles d'empiéter sur l'espace personnel. **Prévenir la discrimination et le profilage :** La protection de la vie privée peut contribuer à empêcher le profilage et la discrimination des individus sur la base de leurs informations personnelles ou de leur comportement en ligne. La collecte de données sans protection adéquate de la vie privée peut conduire à des prises de décision injustes et partiales. **Cybersécurité et confiance numérique :** La protection de la vie privée et la cybersécurité sont liées. Une atteinte à la vie privée peut conduire à des incidents de cybersécurité et vice versa. En donnant la priorité à la protection de la vie privée, les individus et les organisations peuvent favoriser une culture de la confiance et de la sécurité numériques. 3.2. GESTION SÉCURISÉE DU COMPTE EN LIGNE La gestion sécurisée des comptes en ligne est un ensemble de pratiques et de stratégies visant à protéger et à gérer les comptes en ligne d'une personne de manière à minimiser le risque d'accès non autorisé et d'atteinte à la protection des données. Une bonne gestion des comptes en ligne est essentielle pour préserver la confidentialité des informations personnelles, prévenir l'usurpation d'identité et sauvegarder les actifs numériques. Voici quelques aspects clés et bonnes pratiques pour une gestion sécurisée des comptes en ligne : **Des mots de passe forts et uniques :** Utilisez des mots de passe forts et uniques pour chaque compte en ligne. Évitez d'utiliser des mots de passe faciles à deviner, tels que "123456" ou "mot de passe". Créez plutôt des mots de passe complexes composés de lettres majuscules et minuscules, de chiffres et de caractères spéciaux. **Gestionnaires de mots de passe :** Envisagez d'utiliser un gestionnaire de mots de passe réputé pour générer, stocker et gérer les mots de passe en toute sécurité. Les gestionnaires de mots de passe vous aident à conserver des mots de passe forts et uniques pour chaque compte sans avoir à les mémoriser tous.

	Activez l'authentification à deux facteurs (2FA) : Dans la mesure du possible, activez l'authentification à deux facteurs pour vos comptes en ligne. L'authentification à deux facteurs ajoute une couche supplémentaire de sécurité en exigeant une deuxième forme de vérification, comme un code à usage unique envoyé à votre appareil mobile, en plus de votre mot de passe. **Surveillez l'activité de votre compte :** Examinez régulièrement l'activité de votre compte et soyez attentif à toute connexion non autorisée ou action suspecte. Si vous remarquez une activité inhabituelle, prenez immédiatement des mesures pour sécuriser votre compte, par exemple en changeant votre mot de passe et en contactant le fournisseur du compte. **Évitez les ordinateurs publics et les réseaux Wi-Fi :** Évitez d'accéder à des comptes sensibles, tels que le courrier électronique ou les opérations bancaires, à partir d'ordinateurs publics ou de réseaux Wi-Fi non sécurisés. Les ordinateurs publics peuvent stocker des identifiants de connexion et les réseaux Wi-Fi non sécurisés peuvent exposer vos données à des écoutes potentielles. **Méfiez-vous des tentatives d'hameçonnage :** Méfiez-vous des courriels, messages ou liens non sollicités qui vous demandent des informations sensibles ou vous invitent à vous connecter à vos comptes. Vérifiez la légitimité de l'expéditeur et du site web avant de fournir des informations. **Mettez régulièrement à jour les informations relatives à la récupération du compte :** Maintenez à jour les informations relatives à la récupération de votre compte, telles que les adresses électroniques ou les numéros de téléphone de remplacement. Vous pourrez ainsi retrouver l'accès à votre compte si vous oubliez votre mot de passe ou si vous rencontrez d'autres problèmes de connexion. **Réviser les paramètres de confidentialité et de sécurité :** Revoyez régulièrement les paramètres de confidentialité et de sécurité de vos comptes en ligne. Ajustez les paramètres en fonction de vos préférences et de vos besoins afin d'assurer un bon équilibre entre confidentialité et fonctionnalité. **Déconnexion et sécurisation des appareils :** Déconnectez-vous toujours de vos comptes lorsque vous avez fini de les utiliser, en particulier sur les appareils partagés ou publics.

Co-funded by the European Union

	En outre, sécurisez vos appareils personnels à l'aide de mots de passe forts ou d'une authentification biométrique. **Changez régulièrement vos mots de passe** : Pensez à changer régulièrement vos mots de passe, en particulier pour les comptes critiques tels que la messagerie électronique et les comptes bancaires. La mise à jour régulière des mots de passe ajoute une couche supplémentaire de sécurité. **Activer les options de récupération de compte :** Configurez des options de récupération de compte, telles que des questions de sécurité ou des codes de sauvegarde, pour retrouver l'accès à votre compte en cas de verrouillage. 3.3. PARTAGE RESPONSABLE DES MÉDIAS SOCIAUX Le partage responsable des médias sociaux fait référence à l'approche consciente et réfléchie du partage de contenu sur les plateformes de médias sociaux d'une manière qui respecte la vie privée, favorise les interactions positives et évite de contribuer à la désinformation ou de nuire. Il est essentiel de pratiquer un partage responsable des médias sociaux pour respecter l'étiquette numérique, favoriser une communauté en ligne positive et protéger le bien-être personnel et collectif. Voici quelques aspects clés d'un partage responsable des médias sociaux : **Protéger les informations personnelles :** Soyez prudent lorsque vous communiquez des informations personnelles sensibles, telles que votre adresse personnelle, votre numéro de téléphone ou des informations financières, sur les médias sociaux. La protection des informations personnelles permet de se prémunir contre l'usurpation d'identité et d'autres risques liés à la protection de la vie privée. **Ajuster les paramètres de confidentialité :** Vérifiez et ajustez régulièrement vos paramètres de confidentialité sur les plateformes de médias sociaux. Personnalisez l'audience de chaque message, afin de vous assurer que seul le public visé puisse voir votre contenu et interagir avec lui. **Respecter le consentement :** Obtenez le consentement des personnes avant de partager leurs photos ou leurs informations personnelles sur les médias sociaux. Tenez compte des préférences des personnes en ce qui concerne le fait d'être étiquetées dans les messages ou mentionnées dans le contenu.

	Vérifier les faits et éviter la désinformation : Avant de partager des articles, des informations ou des images, vérifiez leur exactitude auprès de sources fiables. Évitez de diffuser des informations erronées ou des contenus non vérifiés susceptibles de contribuer à la propagation de rumeurs ou de faux récits. **Veiller au moment et à la fréquence :** Évitez les partages excessifs ou inappropriés, car ils peuvent entraîner une surcharge d'informations pour les personnes qui vous suivent. Soyez attentif au moment où vous publiez vos messages afin de respecter les différents fuseaux horaires et les préférences de votre public. **Promouvoir un contenu positif :** Partagez du contenu positif, informatif ou inspirant. Le partage positif contribue à un environnement en ligne plus sain et favorise un sentiment de communauté parmi les personnes qui vous suivent. **Gérer les désaccords avec respect :** Engagez des discussions respectueuses et constructives sur les médias sociaux, même si vous n'êtes pas d'accord avec les autres. Évitez de vous engager dans des discussions en ligne ou de recourir à des attaques personnelles. **Éviter les contenus nuisibles ou offensants :** Abstenez-vous de partager des contenus susceptibles d'être offensants, discriminatoires ou préjudiciables à d'autres personnes. Soyez conscient de l'impact potentiel de vos messages sur différentes personnes et communautés. **Protection des droits d'auteur :** Respectez les lois sur les droits d'auteur et évitez de partager du matériel protégé par des droits d'auteur sans autorisation ou attribution appropriée. Mentionnez les créateurs originaux lorsque vous partagez leur travail. **Réviser le contenu partagé :** Examinez régulièrement votre contenu partagé pour vous assurer qu'il est conforme à vos valeurs et à l'image que vous souhaitez donner en ligne. Supprimez ou mettez à jour les messages qui ne reflètent plus vos perspectives actuelles. **Promouvoir la gentillesse numérique :** Faites preuve de gentillesse et d'empathie dans vos interactions sur les médias sociaux. Évitez de participer à la cyberintimidation, aux discours haineux ou à toute forme de comportement préjudiciable, ou de les propager.

Encourager une culture en ligne positive : Encouragez les autres à partager les médias sociaux de manière responsable en donnant un exemple positif. Engagez des discussions sur la citoyenneté numérique et sur l'importance d'être des citoyens numériques responsables.

4. NAVIGUER EN TOUTE SÉCURITÉ DANS LES MÉDIAS SOCIAUX

4.1. RÉGLAGE DES PARAMÈTRES DE CONFIDENTIALITÉ

L'ajustement des paramètres de confidentialité fait référence au processus de personnalisation du niveau d'accès et de visibilité des informations personnelles sur diverses plateformes, sites web et applications. Il s'agit de choisir en connaissance de cause quelles données sont partagées, avec qui elles sont partagées et comment elles sont utilisées par des tiers. En ajustant les paramètres de confidentialité, les individus peuvent mieux contrôler leur empreinte numérique et protéger leurs informations personnelles d'une exposition inutile. Voici une explication détaillée de l'importance et des étapes du réglage des paramètres de confidentialité :

Importance du réglage des paramètres de confidentialité :

Protection des informations personnelles : Le réglage des paramètres de confidentialité permet aux individus de limiter la quantité d'informations personnelles visibles par d'autres, réduisant ainsi le risque d'usurpation d'identité, de harcèlement ou d'attaques par ingénierie sociale.

Contrôle du partage des données : En personnalisant les paramètres de confidentialité, les individus peuvent contrôler les données qu'ils partagent avec les plateformes de médias sociaux, les sites web et les applications, limitant ainsi la collecte et l'utilisation de leurs informations.

Empêcher la publicité ciblée : Les paramètres de confidentialité peuvent aider les individus à refuser la publicité ciblée et le contenu personnalisé, offrant ainsi une expérience en ligne plus privée et moins intrusive.

Éviter l'utilisation abusive des données : L'ajustement des paramètres de confidentialité réduit les risques d'utilisation abusive des données par des tiers non autorisés, ce qui

	permet de se prémunir contre d'éventuelles violations et contre l'accès non autorisé à des informations sensibles. **Améliorer la sécurité en ligne :** Restreindre l'accès aux informations personnelles par le biais des paramètres de confidentialité peut renforcer la sécurité en ligne et minimiser le risque d'ingénierie sociale ou d'attaques par hameçonnage. **Marche à suivre pour ajuster les paramètres de confidentialité :** **Consultez les paramètres du compte :** Sur les plateformes de médias sociaux, vérifiez les paramètres du compte ou la section des paramètres de confidentialité pour accéder aux options de personnalisation des préférences en matière de confidentialité. **Choisissez l'audience des messages :** Déterminez qui peut voir vos messages, par exemple vos amis, les amis de vos amis ou le public. Optez pour un public plus restreint afin de limiter la visibilité de votre contenu. **Contrôler les informations du profil :** Décidez quelles informations de profil sont visibles par les autres, comme votre adresse électronique, votre numéro de téléphone ou votre date de naissance. Dans la mesure du possible, réduisez la visibilité des données sensibles. **Gérer les autorisations des applications :** Pour les applications mobiles, vérifiez et gérez les autorisations dans les paramètres de l'appareil. N'autorisez que les autorisations nécessaires pour chaque application et révoquez les autorisations pour les applications qui n'en ont pas besoin. **Refus de la collecte de données :** Certaines plateformes et certains sites web offrent la possibilité de refuser la collecte et le partage de données à des fins publicitaires. Profitez de ces options pour réduire le suivi des données. **Personnaliser le partage de la localisation :** Choisissez quand et avec qui vous partagez votre position. Désactivez le partage de localisation lorsque vous n'en avez pas besoin ou limitez-le à des applications de confiance spécifiques. **Envisagez la navigation anonyme :** Utilisez les modes de navigation privée ou incognito pour empêcher le stockage de l'historique de navigation et des cookies sur votre appareil.

	Vérifier l'accès aux applications tierces : Examinez et gérez les applications tierces qui ont accès aux informations de votre compte. Révoquez l'accès aux applications qui ne sont plus utilisées ou qui n'ont pas besoin d'être accessibles. **Soyez prudent avec les paramètres par défaut :** De nombreuses plateformes ont des paramètres de confidentialité par défaut qui peuvent être plus permissifs que souhaité. Prenez le temps d'ajuster ces paramètres en fonction de vos préférences. **Réviser et mettre à jour régulièrement :** Révisez et mettez à jour régulièrement vos paramètres de confidentialité, car les plateformes et les applications peuvent introduire de nouvelles fonctionnalités ou des changements qui affectent votre vie privée. 4.2. GÉRER LES DEMANDES D'AMIS ET LES MESSAGES Le traitement des demandes d'amis et des messages sur les plateformes de médias sociaux et les applications de messagerie implique de faire preuve de prudence, de discernement et de respect dans vos interactions avec les autres. Il est essentiel de maintenir des limites personnelles, de protéger votre vie privée et de favoriser une expérience en ligne positive. Voici quelques conseils pour traiter les demandes d'amis et les messages : **Gestion des demandes d'amis :** **Vérifier l'identité :** Avant d'accepter une demande d'amitié, assurez-vous de connaître la personne ou d'avoir des amis communs. Soyez prudent lorsque vous acceptez des demandes provenant de profils inconnus ou suspects. **Vérifier les paramètres de confidentialité :** Ajustez vos paramètres de confidentialité pour contrôler qui peut vous envoyer des demandes d'amis. Limitez les demandes d'amis aux amis d'amis ou à des groupes spécifiques afin de réduire les risques de recevoir des demandes d'inconnus. **Évitez d'accepter des étrangers :** Soyez sélectif lorsque vous ajoutez de nouvelles connexions. Évitez d'accepter des demandes d'amis provenant de personnes que vous ne

	connaissez pas personnellement, surtout si elles n'ont pas de relations mutuelles. **Bloquez ou signalez les comptes suspects :** Si vous recevez des demandes d'amis provenant de comptes suspects ou falsifiés, envisagez de les bloquer ou de les signaler aux administrateurs de la plateforme. **Examinez les informations du profil :** Avant d'accepter une demande d'amitié, examinez le profil du demandeur pour vous assurer qu'il semble authentique et qu'il correspond à vos valeurs et à vos intérêts. **Respectez les limites :** Il n'y a pas de mal à refuser des demandes d'amis si vous ne vous sentez pas à l'aise avec quelqu'un. Respectez vos propres limites et ne vous sentez pas obligé d'accepter toutes les demandes. **Traitement des messages :** **Soyez respectueux :** Répondez aux messages de manière polie et respectueuse. Traitez les autres comme vous aimeriez être traité dans une conversation en ligne. **Vérifiez les expéditeurs :** Si vous recevez un message d'un expéditeur inconnu, soyez prudent. Évitez de cliquer sur des liens suspects ou de télécharger des pièces jointes provenant de sources inconnues. **Évitez de partager des informations sensibles :** Évitez de partager des informations personnelles sensibles, des données financières ou des mots de passe par le biais d'applications de messagerie. Soyez prudent lorsque vous partagez des informations privées avec des personnes que vous ne connaissez pas bien. **Signaler les cas de harcèlement ou d'abus :** Si vous recevez des messages offensants, menaçants ou harcelants, signalez l'expéditeur aux administrateurs de la plateforme ou à l'équipe d'assistance de l'application de messagerie. **Définir la confidentialité des messages :** Réglez les paramètres de confidentialité de vos messages pour contrôler qui peut vous envoyer des messages. Limitez l'accès à la messagerie à vos amis ou contacts. **Utilisez la fonction de blocage :** Si quelqu'un vous importune ou vous envoie des messages inappropriés,

utilisez la fonction de blocage pour empêcher tout contact ultérieur avec cette personne.

Attention au ton et à l'intention : Les messages peuvent être facilement mal interprétés en raison de l'absence de ton et d'expressions faciales. Soyez attentif à votre propre communication et essayez d'éviter les malentendus.

Faites des pauses dans la messagerie : Il n'y a pas de mal à faire des pauses dans la messagerie et les médias sociaux pour se concentrer sur d'autres activités et éviter d'être submergé par le numérique.

4.3. SIGNALER ET BLOQUER LES COMPTES ABUSIFS

Le signalement et le blocage des comptes abusifs constituent une étape cruciale dans le maintien d'un environnement en ligne sûr et positif. Les comptes abusifs peuvent avoir des comportements préjudiciables, tels que la cyberintimidation, le harcèlement, les discours haineux et d'autres formes d'abus en ligne. Le signalement et le blocage de ces comptes permettent de se protéger et de protéger les autres contre leurs actions nuisibles. Voici une explication du fonctionnement du signalement et du blocage et de leur importance :

Signaler les comptes abusifs :

Identifiez les comportements préjudiciables : Si vous tombez sur un compte qui a un comportement abusif ou préjudiciable, tel que le harcèlement, les menaces ou les discours haineux, il est important de le reconnaître.

Signaler le compte : La plupart des plateformes de médias sociaux et des services en ligne disposent d'un mécanisme de signalement. Utilisez la fonction de signalement de la plateforme pour informer les administrateurs ou les modérateurs du comportement abusif.

Fournir des preuves : Lorsque vous signalez un compte abusif, il peut être utile de fournir des preuves, telles que des captures d'écran ou des liens vers le contenu offensant, pour étayer votre signalement.

Choisissez la catégorie appropriée : Les plateformes de médias sociaux proposent souvent différentes catégories de

	signalement. Choisissez la catégorie qui correspond le mieux au type d'abus que vous signalez. **Respecter les directives de signalement :** Familiarisez-vous avec les lignes directrices de la plateforme en matière de signalement afin de vous assurer que vous signalez des comptes pour des raisons valables. Évitez les faux signalements, car ils peuvent nuire à l'efficacité du système de signalement. **Bloquer les comptes abusifs :** **Protégez-vous :** Le blocage d'un compte abusif empêche ce compte d'interagir avec vous. Cela peut contribuer à protéger votre bien-être mental et à créer un espace en ligne sûr pour vous. **Empêcher les contacts indésirables :** Lorsque vous bloquez un compte, l'utilisateur derrière ce compte ne pourra plus vous suivre, vous envoyer des messages ou commenter vos publications. **L'anonymat :** Le blocage est généralement une action privée. L'utilisateur que vous bloquez ne recevra aucune notification l'informant qu'il a été bloqué. **Plus d'interaction :** Après avoir bloqué un compte, vous ne verrez plus son contenu ni ses activités, et il ne pourra plus voir les vôtres. **Pourquoi le signalement et le blocage sont importants :** **Prévenir les préjudices : le** signalement de comptes abusifs peut permettre de prendre des mesures à l'encontre du compte en question, ce qui peut empêcher que vous ou d'autres personnes ne subissent d'autres préjudices. **Application des directives de la plate-forme :** Signaler un comportement abusif permet de faire respecter les conditions d'utilisation de la plateforme et les directives de la communauté, créant ainsi un environnement plus sûr pour tous les utilisateurs. **Soutenir la santé de la communauté :** En signalant et en bloquant les comptes abusifs, vous contribuez à favoriser une communauté en ligne saine et respectueuse. **Responsabiliser les utilisateurs :** Le signalement et le blocage permettent aux individus de prendre le contrôle de

leurs expériences en ligne et de se protéger contre les interactions abusives ou préjudiciables.

5. CYBERSÉCURITÉ ET DISPOSITIFS MOBILES

5.1. SÉCURISER LES SMARTPHONES ET LES TABLETTES

La sécurisation des smartphones et des tablettes est essentielle dans le monde mobile d'aujourd'hui, où ces appareils stockent une multitude d'informations personnelles et de données sensibles. La sécurisation de ces appareils permet de se protéger contre les accès non autorisés, les violations de données et les attaques de logiciels malveillants. Voici quelques mesures clés pour assurer la sécurité des smartphones et des tablettes :

Activer la sécurité de l'écran de verrouillage : Configurez une méthode de verrouillage sécurisée de l'écran, telle qu'un code PIN, un motif, un mot de passe ou une méthode biométrique (empreinte digitale ou reconnaissance faciale). Cela permet d'empêcher tout accès non autorisé à votre appareil en cas de perte ou de vol.

Maintenez les logiciels à jour : Mettez régulièrement à jour le système d'exploitation et les applications de votre appareil. Les fabricants publient des mises à jour pour corriger les failles de sécurité. Il est donc essentiel de garder votre appareil à jour pour rester protégé contre les exploits potentiels.

N'installez que des applications de confiance : Téléchargez des applications à partir des boutiques d'applications officielles (par exemple, Google Play Store, Apple App Store) et évitez d'installer des applications provenant de sources inconnues. Les applications malveillantes provenant de sources non officielles peuvent compromettre la sécurité et la confidentialité de votre appareil.

Examinez les autorisations des applications : Soyez prudent lorsque vous accordez des autorisations à des applications. Examinez les autorisations demandées par chaque application et vérifiez si elles sont nécessaires à son fonctionnement. Évitez d'accorder des autorisations inutiles qui pourraient compromettre votre vie privée.

Utiliser un VPN sur les réseaux Wi-Fi publics **:** lorsque vous utilisez des réseaux Wi-Fi publics, pensez à utiliser un réseau privé virtuel (VPN) pour crypter votre trafic internet et protéger vos données contre d'éventuelles écoutes ou espionnages.

Navigation mobile sécurisée : Utilisez des navigateurs sécurisés qui offrent des connexions cryptées (HTTPS) pour les sites web. Évitez d'accéder à des informations sensibles, comme les services bancaires en ligne, sur des réseaux non sécurisés ou publics.

Sauvegardez régulièrement vos données : Sauvegardez régulièrement les données de votre appareil sur un service en nuage sécurisé ou sur un appareil externe. Ainsi, vos informations importantes seront en sécurité même si votre appareil est perdu, endommagé ou réinitialisé.

Évitez de cliquer sur des liens suspects : Soyez prudent lorsque vous cliquez sur des liens contenus dans des courriels, des messages ou des fenêtres contextuelles provenant de sources inconnues. Cliquer sur des liens malveillants peut conduire à des tentatives d'hameçonnage ou à l'installation de logiciels malveillants.

Utilisez des verrous d'applications pour les applications sensibles : Pensez à utiliser des verrous d'applications ou une fonction de mode invité pour restreindre l'accès aux applications ou contenus sensibles sur votre appareil. Cela constitue un niveau de sécurité supplémentaire, en particulier lorsque vous partagez votre appareil avec d'autres personnes.

Crypter les données de l'appareil : Si votre appareil le permet, activez le cryptage pour protéger vos données contre tout accès non autorisé, même si quelqu'un d'autre accède physiquement à l'appareil.

5.2. AUTORISATIONS D'UTILISATION DES APPLICATIONS ET ACCÈS AUX DONNÉES

Les autorisations d'application et l'accès aux données font référence aux autorisations demandées par les applications mobiles (apps) pour accéder à diverses fonctions et données sur l'appareil d'un utilisateur. Lorsque les utilisateurs installent et utilisent des applications sur leurs smartphones ou tablettes, ces applications peuvent nécessiter l'accès à

	certaines ressources de l'appareil et à des informations personnelles pour fonctionner correctement. Ces autorisations permettent aux applications de fournir des fonctionnalités spécifiques et d'améliorer l'expérience de l'utilisateur. Cependant, il est essentiel que les utilisateurs comprennent et gèrent ces autorisations afin de protéger leur vie privée et leur sécurité. Voici un examen plus approfondi des autorisations des applications et de l'accès aux données : **Types d'autorisations pour les applications :** Les autorisations d'utilisation varient en fonction de la fonctionnalité de l'application et de la plateforme (Android ou iOS). Les autorisations les plus courantes sont l'accès à l'appareil photo, au microphone, à la localisation, aux contacts, au calendrier, au stockage, aux SMS, aux journaux d'appels, etc. de l'appareil. Certaines applications peuvent également demander l'autorisation d'utiliser d'autres appareils connectés, tels que des périphériques Bluetooth. **Demandes d'autorisation :** Lorsque les utilisateurs installent une application, celle-ci peut demander des autorisations spécifiques dont elle a besoin pour fonctionner. Les demandes d'autorisation sont généralement présentées au cours du processus d'installation de l'application ou lorsque l'application tente pour la première fois d'accéder à une fonction particulière. Les utilisateurs peuvent accorder ou refuser ces autorisations. **Objectif des autorisations d'utilisation :** Les autorisations d'utilisation sont nécessaires pour activer certaines fonctions de l'application. Par exemple, une application de retouche photo doit avoir accès à l'appareil photo et à la mémoire de l'appareil pour capturer et enregistrer des photos. Une application de navigation a besoin d'accéder à la localisation pour fournir des indications précises. **Protection de la vie privée :** Bien que les autorisations soient souvent essentielles au fonctionnement des applications, les utilisateurs doivent être prudents et ne pas accorder d'autorisations sans tenir compte de l'objectif de l'application et sans se demander si les autorisations demandées sont raisonnables. L'octroi de permissions excessives peut potentiellement compromettre la vie privée ou permettre à des applications d'accéder à des données sensibles sans nécessité légitime. **Gestion des autorisations des applications :** La plupart des systèmes d'exploitation modernes permettent aux utilisateurs de gérer les autorisations des applications. Les utilisateurs

peuvent consulter et modifier les autorisations des applications dans les paramètres de l'appareil, ce qui leur permet d'accorder ou de révoquer à tout moment des autorisations spécifiques pour des applications individuelles.

Lire attentivement les autorisations : Avant d'accorder des autorisations, les utilisateurs doivent lire attentivement les autorisations demandées par une application. Si une application demande des autorisations qui ne semblent pas en rapport avec ses fonctionnalités, il s'agit d'un signal d'alarme, et les utilisateurs doivent faire preuve de prudence ou envisager d'utiliser d'autres applications.

Permissions et mises à jour des applications : Lors de la mise à jour d'une application, il est essentiel de vérifier les autorisations nouvelles ou modifiées. Parfois, les mises à jour d'applications peuvent introduire des autorisations supplémentaires, et les utilisateurs doivent s'assurer qu'elles correspondent à leurs préférences et à leurs besoins.

Demandes d'autorisation pour les applications iOS et Android : Bien qu'iOS et Android gèrent différemment les autorisations, les deux plateformes offrent aux utilisateurs la possibilité de gérer les autorisations dans leurs paramètres respectifs. Sur iOS, les utilisateurs peuvent consulter et gérer les autorisations dans les paramètres de l'application, sous "Confidentialité". Sur Android, les utilisateurs peuvent gérer les autorisations en allant dans "Apps & notifications" ou "Gestionnaire d'applications" dans les paramètres de l'appareil.

5.3. PROTÉGER LES APPAREILS MOBILES CONTRE LE VOL ET LA PERTE

Il est essentiel de protéger les appareils mobiles contre le vol et la perte afin de sauvegarder les informations personnelles, de prévenir l'usurpation d'identité et de préserver la confidentialité des données sensibles. Les appareils mobiles, tels que les smartphones et les tablettes, sont souvent la cible de voleurs en raison de leur portabilité et des informations précieuses qu'ils contiennent. La mise en œuvre de mesures de sécurité peut réduire considérablement les risques associés au vol ou à la perte. Voici quelques mesures importantes pour protéger les appareils mobiles :

Configurer la sécurité de l'écran de verrouillage : Activez une méthode de verrouillage sécurisée de l'écran, telle qu'un

	code PIN, un motif, un mot de passe ou une méthode biométrique (empreinte digitale ou reconnaissance faciale). Cela permet d'empêcher tout accès non autorisé à votre appareil s'il tombe entre de mauvaises mains. **Utilisez les services de recherche de mon appareil :** Activez la fonction "Trouver mon appareil" ou "Trouver mon iPhone" sur votre appareil. Ces services vous permettent de localiser, de verrouiller ou d'effacer votre appareil à distance en cas de perte ou de vol. **Maintenez les logiciels et les applications à jour :** Mettez régulièrement à jour le système d'exploitation et les applications de votre appareil pour vous assurer que vous disposez des derniers correctifs de sécurité et des dernières corrections de bogues. Les fabricants publient des mises à jour pour corriger les vulnérabilités et améliorer la sécurité de l'appareil. **Évitez de laisser vos appareils sans surveillance :** Ne laissez pas votre appareil mobile sans surveillance dans les lieux publics, tels que les restaurants, les transports publics ou les salles de sport. Gardez votre appareil sur vous ou en lieu sûr pour réduire le risque de vol. **Restez vigilant dans les endroits bondés :** Faites attention à ce qui vous entoure dans les endroits très fréquentés, en particulier là où les vols à la tire et les vols sont les plus susceptibles de se produire. Soyez prudent lorsque vous utilisez votre appareil dans des lieux très fréquentés. **Rangez votre appareil en toute sécurité à la maison :** Conservez votre appareil mobile dans un endroit sûr lorsqu'il n'est pas utilisé, en particulier à la maison. Évitez de le laisser sur un comptoir, près d'une fenêtre ouverte ou dans un endroit facilement accessible. **Utilisez des verrous d'applications pour les applications sensibles :** Pensez à utiliser des verrous d'applications ou des fonctions de mode invité pour restreindre l'accès aux applications ou contenus sensibles sur votre appareil. Cela ajoute une couche de sécurité supplémentaire, en particulier lorsque vous partagez votre appareil avec d'autres personnes. **Crypter les données de l'appareil :** Si votre appareil le permet, activez le cryptage pour protéger vos données contre tout accès non autorisé, même si quelqu'un d'autre accède physiquement à l'appareil.

	Évitez les stations de recharge publiques : Évitez d'utiliser les stations de recharge publiques ou les ports USB, car ils peuvent être compromis et présenter un risque de vol de données ou d'installation de logiciels malveillants. **Sauvegardez régulièrement vos données :** Sauvegardez régulièrement les données de votre appareil sur un service en nuage sécurisé ou sur un appareil externe. Ainsi, vos informations importantes seront en sécurité même si votre appareil est perdu, endommagé ou réinitialisé. **Utilisez des protections d'écran confidentielles :** Envisagez d'utiliser des protections d'écran pour empêcher les regards indiscrets de voir votre écran dans les lieux publics. **Enregistrer les appareils auprès des autorités :** Enregistrez vos appareils mobiles auprès des autorités locales ou des bases de données pertinentes. Cela peut faciliter le processus de récupération en cas de vol.
Glossaire :	1. Sécurité en ligne La pratique consistant à suivre des lignes directrices applicables, à comprendre la technologie moderne et à protéger les appareils numériques contre les éléments malveillants du monde en ligne. 2. Sécurité sur Internet Mesures et pratiques prises pour protéger les ordinateurs, les réseaux et les données contre les cybermenaces, telles que les logiciels malveillants, les virus et les accès non autorisés. 3. Vie privée numérique Le droit de contrôler et de protéger ses informations et données personnelles contre l'accès, l'utilisation ou le partage sans consentement. 4. La cybersécurité La protection des appareils numériques, des réseaux et des systèmes d'information contre les cybermenaces, y compris le piratage, les violations de données et les cyberattaques. 5. Pratiques en ligne sûres Ensemble de lignes directrices et de comportements que les individus doivent suivre pour garantir la sécurité de leurs activités en ligne et protéger leur vie privée. 6. Protection des données personnelles

	La protection des données sensibles et personnelles contre l'accès non autorisé ou l'utilisation abusive, la prévention de l'usurpation d'identité et de la fraude. 7. Etiquette des médias sociaux Le comportement approprié et respectueux que les individus doivent adopter lorsqu'ils utilisent les plateformes de médias sociaux. 8. Sécurité des données Mesures et protocoles pris pour protéger les données numériques contre l'accès, la modification ou la destruction non autorisés. 9. Prévention de l'usurpation d'identité Techniques et pratiques visant à protéger les informations personnelles et à empêcher les criminels de les utiliser pour usurper l'identité d'une personne. 10. Gestion des mots de passe Pratique responsable consistant à créer des mots de passe forts et uniques et à les gérer en toute sécurité pour protéger les comptes en ligne. 11. Menaces en ligne Divers risques et dangers rencontrés lors de l'utilisation d'Internet, tels que l'hameçonnage, les logiciels malveillants, les escroqueries et la cyberintimidation. 12. Sensibilisation à l'hameçonnage La capacité à reconnaître et à éviter les tentatives d'hameçonnage, où les attaquants trompent les individus pour obtenir des informations sensibles, souvent par le biais de courriels ou de sites web frauduleux. 13. Paramètres de confidentialité Les options personnalisables des plateformes en ligne qui permettent aux utilisateurs de contrôler la visibilité de leurs informations personnelles et l'audience de leur contenu. 14. Signalement des abus Processus consistant à informer les administrateurs ou les modérateurs de la plateforme d'un comportement abusif ou préjudiciable sur la plateforme, tel que le harcèlement ou les propos haineux. 15. Blocage des comptes

	L'action d'empêcher un compte abusif ou indésirable d'interagir avec vous ou de consulter votre contenu sur les plateformes de médias sociaux. 16. Transactions en ligne sécurisées Veiller à ce que les transactions en ligne, telles que les achats ou les transactions financières, soient effectuées en toute sécurité afin d'éviter les fraudes. 17. Empreinte numérique La trace de données et d'informations laissée par les activités en ligne d'un individu, y compris les messages sur les médias sociaux, l'historique des recherches et les interactions en ligne. 18. Prévention de la cyberintimidation Mesures prises pour arrêter et prévenir le harcèlement, l'intimidation ou les brimades en ligne. 19. Authentification à deux facteurs (2FA) Une couche de sécurité supplémentaire qui exige des utilisateurs qu'ils fournissent deux formes d'identification (par exemple, un mot de passe et un code unique envoyé à leur téléphone) pour accéder à un compte. 20. Des habitudes de navigation sûres Pratiques et lignes directrices visant à garantir une navigation sûre et sécurisée sur l'internet, en évitant les sites et les contenus à risque.
Bibliographie :	Conseils et règles de sécurité sur Internet (kaspersky.com) Sécurité en ligne (pour les adolescents) - Nemours KidsHealth Qu'est-ce que la sécurité en ligne ? | SWGfL Conversation sur la sécurité en ligne | LearnEnglish Teens (britishcouncil.org) Sécurité sur Internet - Wikipédia Sécurité en ligne - Conseils pour aider les enfants | Internet Matters Sécurité sur Internet : Introduction à la sécurité sur Internet (gcfglobal.org) indianjournals.com/ijor.aspx?target=ijor:ijie&volume=8&issue=2&article=001

	"Sécurité sur Internet" dans : L'encyclopédie internationale de l'éducation aux médias en ligne (researchgate.net) Recherche d'informations sur Google - Google Güvenlik Merkezi (safety.google) La sécurité en ligne - Commissaire à l'eSécurité Comment rester en sécurité en ligne : Conseils et ressources en matière de sécurité sur Internet (reviews.org)
Ressources (vidéos, lien de référence)	https://www.youtube.com/watch?v=qZE45J-MIUg&pp=ygULc2FmZSBvbmxpbmU%3D https://www.youtube.com/watch?v=aO858HyFbKI&pp=ygULc2FmZSBvbmxpbmU%3D https://www.youtube.com/watch?v=HxySrSbSY7o&pp=ygULc2FmZSBvbmxpbmU%3D https://www.youtube.com/watch?v=EyQeUwqCDWg&pp=ygULc2FmZSBvbmxpbmU%3D