5ème techno COLLEGE

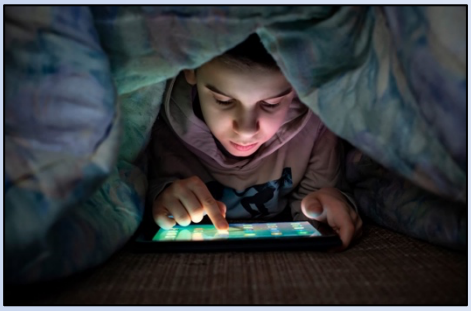
Réseaux sociaux

CDI

Je retiens … *CYBERDEPENDANCE / CYBERHARCELEMENT / CYBERSECURITE*
INFO FAKE NEWS / DROIT A L'IMAGE / VIE PRIVEE ET DONNEES PERSONNELLES

La cyberdépendance, ou cyberaddiction, est une dépendance excessive aux écrans, comme les smartphones et les ordinateurs, souvent liée à des activités en ligne telles que les jeux vidéo ou les réseaux sociaux.

Les signes de cette dépendance incluent le temps excessif passé sur les écrans, l'obsession pour les appareils, l'anxiété liée à la peur de manquer des événements en ligne, ainsi que des symptômes physiques et émotionnels comme la fatigue et l'anxiété.



Pour prévenir ou traiter la cyberdépendance, il est important de prendre conscience de ses habitudes numériques, de limiter le temps passé sur les écrans, de rechercher un soutien auprès d'adultes de confiance, et éventuellement de recourir à une thérapie ou à des médicaments prescrits par un médecin.

Des pratiques telles que l'arrêt des écrans avant le sommeil et le partage de repas sans écrans, ainsi que l'engagement dans des activités alternatives, peuvent également contribuer à rétablir un équilibre sain entre vie numérique et vie réelle.

Le cyberharcèlement se manifeste par des attaques répétées via des moyens numériques, visant souvent les jeunes et prenant diverses formes telles que l'intimidation ou la diffusion de rumeurs. En cas de cyberharcèlement, il est crucial d'en parler à des adultes de confiance et de signaler les contenus inappropriés.

Des ressources telles que le numéro d'assistance de l'association E-Enfance peuvent fournir un soutien et des conseils. Sur le plan légal, le cyberharcèlement est sévèrement puni, avec des peines allant jusqu'à deux à trois ans d'emprisonnement et des amendes considérables.

Il est essentiel pour les témoins de soutenir la victime. Pour prévenir le cyberharcèlement, il est recommandé d'être vigilant en ligne et d'encourager un environnement respectueux.

Réseaux sociaux

Je retiens …

La cybersécurité englobe les pratiques et technologies visant à protéger les systèmes informatiques contre les cybermenaces, tandis que la cyberdéfense se concentre spécifiquement sur la détection, la réponse et la neutralisation des attaques en temps réel.

Les pirates informatiques peuvent être classés en trois catégories principales : les Black Hats, motivés par des intentions malveillantes, les White Hats, professionnels de la sécurité, et les Grey Hats, intermédiaires entre les deux.

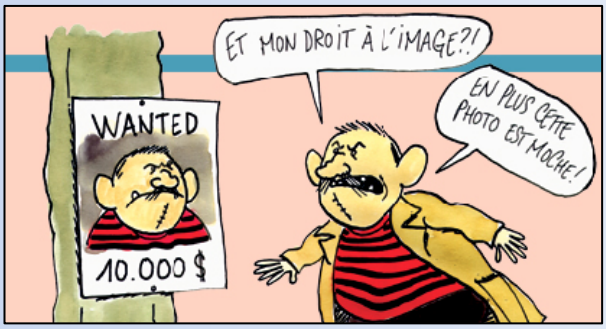
Les malwares, ou programmes malveillants, sont des logiciels conçus pour endommager ou exploiter des systèmes informatiques. Les exemples incluent les virus, les vers et les chevaux de Troie, qui ont des objectifs différents, tels que la destruction de données ou le vol d'informations.

Une adresse IP est une étiquette numérique attribuée à chaque appareil sur un réseau, et un hacker peut l'utiliser pour surveiller l'activité en ligne ou lancer des attaques.

Le droit à l'image confère à chacun le contrôle sur l'utilisation de sa propre image, nécessitant le consentement préalable pour toute diffusion de photos ou vidéos, sauf exceptions légales telles que les contextes publics ou journalistiques.

Pour partager des photos en ligne, le consentement des amis et de leurs parents mineurs est indispensable.

Les images libres de droits, disponibles sous des licences Creative Commons, peuvent être utilisées sans restriction.



En cas de publication non consentie, plusieurs recours sont possibles, incluant la demande de retrait à la personne concernée ou aux plateformes en ligne, avec des sanctions légales pouvant aller jusqu'à 45 000 € d'amende et un an de prison.

Réseaux sociaux

Je retiens …

Une infox, également connue sous le nom de fake news, est une fausse information diffusée dans le but de tromper ou manipuler. Avec la prolifération des réseaux sociaux, les infox se propagent rapidement. Il est crucial de ne pas partager toutes les informations trouvées en ligne.

Pour vérifier la fiabilité d'une information, il est recommandé de se poser plusieurs questions, notamment sur l'auteur, l'objectif, la nature du site, les sources et la cohérence des détails. Pour vérifier une image, il est possible d'utiliser la recherche d'images inversée sur des moteurs de recherche comme Google.

Je peux supprimer des photos de moi publiées sans mon consentement en demandant tout simplement à la personne qui l'a publiée de la retirer. Si ce n'est pas possible, alors je peux demander le retrait de l'image au site qui l'héberge.

Il est également possible de contacter le 3018 qui aide et donne des conseils.

Si rien ne se passe :

- Faire un recours à la CNIL pour opposition à la diffusion de son image.
- Les parents peuvent porter plainte à la police ou la gendarmerie.

La vie privée se réfère à notre sphère personnelle et intime, éloignée de la sphère publique visible sur les réseaux sociaux.

Il est crucial d'éviter de publier des éléments tels que son adresse réelle, des informations intimes ou des photos compromettantes.

L'e-réputation, ou cyber-réputation, est l'image que les internautes se font d'une personne à partir des traces qu'elle laisse sur Internet, qu'elles soient maîtrisées ou non.

Toutes ces traces et données d'individus et même d'entreprises ou d'administrations sont stockées dans des **DATA CENTERS**, centres de stockage hyper sécurisés représentants d'immenses propriétés physiques. Aussi pour mieux connaitre le profil des internautes, les cookies informatiques sont de petits fichiers stockant des données personnelles utilisées par les sites web pour personnaliser l'expérience utilisateur et proposer des publicités ciblées. Un data center est un centre de stockage sécurisé des données provenant d'entreprises, d'administrations et d'individus, représentant d'immenses propriétés physiques.

Il est également possible de supprimer définitivement ses propres comptes sur les plateformes concernées.

Chacun a « le droit à l'oubli »