L'EXPLORATEUR NUMÉRIQUE

6ème

Leçon 6 : Protection et sécurité en ligne

Leçon 6

Introduction : Un adolescent peut passer parfois près de 8h par jour sur Internet (les jours sans école). Les activités sont nombreuses et parmi celles-ci, les applications de messagerie, tchat et autres réseaux sociaux permettent de continuer à communiquer avec ses amis mais aussi parfois à des inconnus. Cela n'est pas sans danger !

Nous verrons dans cette leçon des conseils à suivre pour éviter les pièges...

1) Comment reconnaître des situations de cyberharcèlement et comment y faire face ?

Harcèlement : Le harcèlement est la répétition de propos ou de comportements ayant pour but de se moquer, de rabaisser la victime. Cela provoque chez la victime une souffrance pouvant aller jusqu'à pousser au suicide.

C'est quoi le cyberharcèlement : On parle aussi de harcèlement en ligne, c'est un harcèlementqui s'effectue via internet (sur un réseau social, un forum, un jeu vidéo multijoueurs, un blog...).

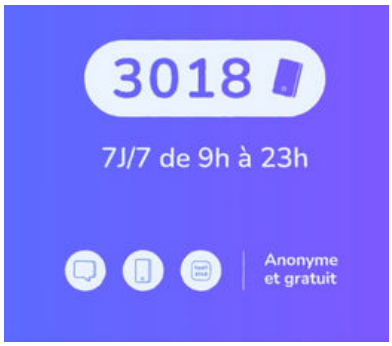
Lorsque quelqu'un est agressé sur les réseaux sociaux ou en ligne, de manière intentionnelle et répétée, par une personne ou un groupe de personnes, il s'agit de cyberharcèlement. Cela provoque chez la victime un isolement qui l'empêche de pouvoir se défendre.

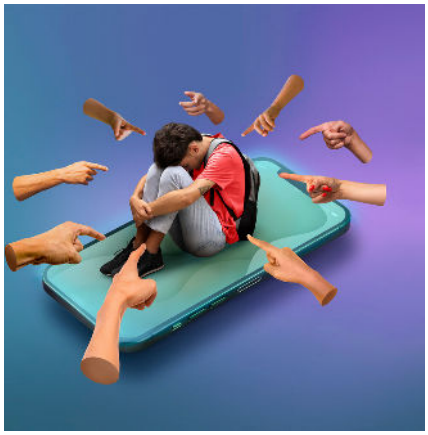
Le cyberharcèlement cela peut être des moqueries, des insultes, des menaces, des rumeurs diffusées via des messageries instantanées, des forums, des tchats, des courriers électroniques, la publication d'une photo ou d'une vidéo gênante ou humiliante. Mais aussi la création d'un groupe, d'une page sur les réseaux sociaux ou encore le piratage d'un compte. Le cyberharcèlement laisse des traces numériques.

Si une personne de votre entourage change brutalement de comportement ou s'isole cela peut être un signe de cyberharcèlement. De même, si elle montre des accès de colère inhabituels ou une perte d'appétit.

Pour l'aider le mieux est de pouvoir parler avec elle, pour qu'elle puisse s'exprimer, confier ses émotions, mettre des mots sur la situation et sortir de son isolement. Si cela n'est pas possible, vous pouvez aussi prévenir un adulte de confiance. Être témoin de cyberharcèlement est un rôle primordial, vous vous devez d'agir.

Le meilleur moyen de lutter contre le cyberharcèlement est de le faire savoir. Pour avoir de l'aide ou des conseils **contactez le 3018 par tchat ou via l'application**. C'est anonyme et gratuit.

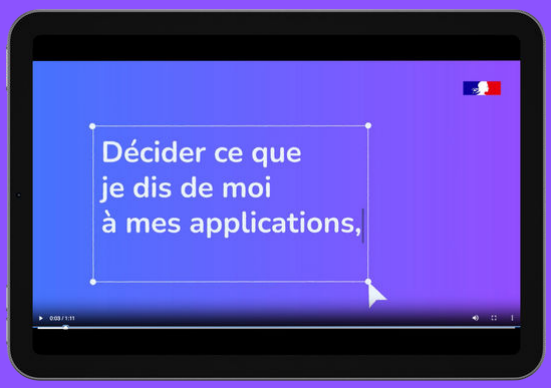




2) Décider ce que je dis de moi à mes applications, c'est possible ?

Un répertoire de contacts permet de connaître les liens que nous entretenons avec des personnes et des organisations.
La géolocalisation, une fonctionnalité disponible dans la plupart des objets connectés (smartphone, tablette ou ordinateur), permet par exemple de connaître les trajets quotidiens, les endroits favoris, de calculer un itinéraire, de partager sa position avec nos amis, d'identifier des personnes à proximité faisant partie de notre réseau.
L'état de santé peut être révélé par le nombre de nos pas, les sports que nous pratiquons, le rythme auquel nous les pratiquons, notre fréquence cardiaque et notre temps de sommeil. Tout cela, c'est notre vie privée et nous avons la possibilité de la protéger.
Certaines applications utilisent la géolocalisation, parfois plusieurs fois par minute.
Ces informations pourraient permettre d'en déduire nos habitudes et notre mode de vie dont nos lieux de vie, de travail, habitudes de fréquentation, nos déplacements.

Je regarde la vidéo suivante



3) Les données personnelles, ça nous concerne ?

Chaque jour des milliards de données sont créées et échangées.
Une donnée personnelle est une information qui permet d'identifier une personne directement ou par recoupement, c'est-à-dire en croisant plusieurs informations.

Les données personnelles sont précieuses, car elles révèlent la vie privée. Les mineurs disposent de droits pour les protéger. Dès que nous utilisons nos appareils connectés (smartphone, tablette, ordinateur, montre...) nous partageons des données personnelles.
Parmi les informations qui permettent de donner des précisions sur notre identité il y a : notre prénom, notre nom, notre date de naissance, notre visage, notre voix, ou encore notre adresse IP.
Les données personnelles sensibles sont notamment la religion, l'état de santé, les opinions politiques, l'appartenance syndicale, l'orientation sexuelle. Il est interdit de les collecter sauf exceptions prévues par la loi.

L'empreinte digitale, l'ADN, l'iris de l'œil sont des données biométriques. Légalement elles sont aussi considérées comme sensibles.

Je regarde la vidéo suivante

4) Pourquoi et comment désactiver la capacité de localisation d'un appareil mobile ?

Nous utilisons régulièrement sur nos appareils mobiles des applications ou des services utilisant la localisation par satellite comme le GPS, notamment pour nos déplacements.
Ces fonctionnalités très pratiques peuvent générer des informations sur nos habitudes de vie comme nos déplacements ou les localisations liées à nos activités personnelles ou professionnelles. Ces informations sont susceptibles d'être utilisées par des services ou des applications annexes dont nous n'avons pas réellement conscience ; avec des objectifs de ciblage publicitaire ou promotionnel personnalisés.
Notamment avec le téléphone portable que nous utilisons en permanence, il est donc important de :

- connaître les applications et services utilisant notre géo-positionnement,
- supprimer le cas échéant les historiques de localisation qu'ils produisent à une fréquence que l'on choisira,
- désactiver la fonction de localisation de l'application ou, si cela n'est pas possible, désinstaller l'application si l'on considère que son accès à notre localisation ne nous semble pas justifié ou légitime.

Je regarde la vidéo suivante

Il est donc important de connaître ces fonctionnalités et de savoir paramétrer les applications et les appareils qui les utilisent afin d'activer, désactiver ou restreindre cette capacité de géolocalisation.
D'une manière générale, pour protéger votre vie privée, désactivez complètement la localisation satellite quand vous estimez ne pas en avoir besoin.

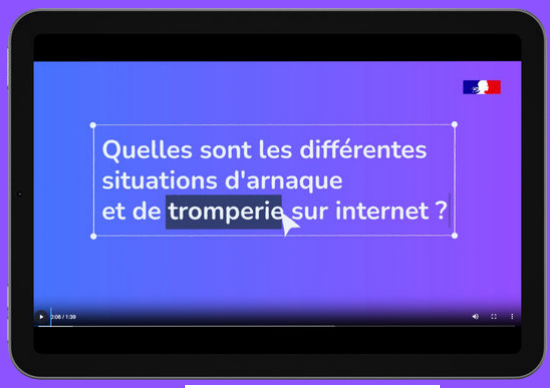
5) Quelles sont les différentes situations d'arnaque et de tromperies sur internet ?

Sur Internet, de nombreuses cybermalveillances reposent sur une tromperie où les escrocs tentent de manipuler la victime afin d'obtenir volontairement d'elle :

- des informations confidentielles comme le numéro de carte bancaire, les identifiants et mots de passe.
- des copies de documents officiels susceptibles de permettre une usurpation d'identité telle que la carte d'identité,
- des photos ou vidéos personnelles pouvant être compromettantes,
- de l'inciter à cliquer sur un lien, ouvrir une pièce jointe, ou encore installer une application pouvant amener au téléchargement d'un virus.

Pour y parvenir, les cybercriminels mettent en scène des situations crédibles destinées à provoquer un sentiment de stress, d'envie, de curiosité..., face auquel la victime peut se montrer moins vigilante et tomber dans le piège qui lui est tendu. Posts ou messages privés sur les réseaux sociaux, mails ou SMS trompeurs, sites Internet frauduleux, usurpation de l'identité d'un interlocuteur de confiance, fenêtres de fausse alerte virus vous incitant à appeler un numéro d'assistance soi-disant « gratuit » ...

Je regarde la vidéo suivante



Toutes ces situations sont destinées à vous faire réagir sans réfléchir. Alors prudence ! Pour éviter d'être victime de ces manipulations, il est capital de conserver son calme, de ne pas se précipiter et au moindre doute d'en parler à un proche de confiance ou de venir s'informer sur une plateforme officielle comme « Cybermalveillance.gouv.fr ».

L'EXPLORATEUR NUMÉRIQUE

6ème

Leçon 6 : Protection et sécurité en ligne

Leçon 6

6) Un mot de passe robuste, c'est quoi ?

Le mot de passe est le moyen le plus courant pour protéger ses données personnelles en ligne.
Choisir un mot de passe robuste pour chaque application ou service que l'on utilise, c'est protéger sa vie privée, éviter l'usurpation d'identité et le vol de données.
Pour chaque service utilisé en ligne, il faut un mot de passe différent.
Bien sûr, les mots de passe ne doivent pas être stockés sur des papiers volants, dans un carnet, ou dans un document non sécurisé.
On préfèrera utiliser un gestionnaire de mots de passe.
Un bon mot de passe doit être suffisamment complexe et unique : par exemple 12 caractères ne formant pas un mot ou une date, et utilisant 4 types de caractères différents : des minuscules, des majuscules, des chiffres et des caractères spéciaux.
On peut aussi utiliser une suite de 7 mots ne formant pas une phrase.

Je regarde la vidéo suivante