

1 — Naviguer dans un monde connecté. L'essence du cyberhéros — Les cyberhéros connaissent les risques et utilisent les médias sociaux en toute sécurité et pour le bien de tous.

2 — Protéger tes renseignements personnels. Les appareils personnels, les appareils intelligents et Internet étant devenus monnaie courante, nous les utilisons pour travailler, apprendre, faire de l'exercice, nous divertir et socialiser. Il est plus important que jamais de protéger nos renseignements personnels et de nous montrer les uns les autres de saines habitudes.

3 — Que sont les paramètres de confidentialité des médias sociaux?
Des contrôles qui déterminent qui peut voir tes publications et tes renseignements personnels

Des mesures prises pour empêcher l'accès aux bibliothèques publiques

Le processus de suppression des comptes de médias sociaux

Un moyen d'améliorer la popularité de ton profil sur les médias sociaux

4 — Des contrôles qui déterminent qui peut voir tes publications et tes renseignements personnels. Vérifie souvent les paramètres de confidentialité et restreins ce qui peut être vu par d'autres personnes.

5 — Il y a probablement plus d'informations sur toi en ligne que tu ne le penses. En voici quelques exemples : Nom complet

Date de naissance

Numéro de téléphone

Expérience de travail

Photos / lieux

6 — Que ne devrais-tu jamais mettre en ligne? (en sélectionner deux)

Souper de la veille

Votre mot de passe

Photos de chats

Numéro d'assurance sociale (NAS)

7 — Tu ne devrais communiquer ton NAS qu'à ton employeur, et jamais en ligne par courriel.

8 — Conseils pour rester en sécurité sur les médias sociaux.

Gère ton compte : Personnalise tes paramètres de confidentialité.

Examine le contenu : Réfléchis avant de publier tes messages et respecte la vie privée des autres.

Pour éviter la fraude, le vol et les escroqueries : Méfie-toi.

Ne laisse pas de comptes ouverts : Ferme ta session lorsque tu as terminé ou supprime un compte que tu n'utilises pas.

9 — Lequel des éléments suivants n'est PAS une bonne pratique sur les médias sociaux?

Prendre part à des conversations positives

Faire trop connaître des renseignements personnels et privés

Vérifier les sources d'information avant de les diffuser

Mettre à jour régulièrement les paramètres de confidentialité

10 — Faire trop connaître tes renseignements personnels et privés ou ceux de tes amis ou des membres de ta famille.

11 — La divulgation de données personnelles (doxing) est une pratique malveillante qui consiste à rechercher et à divulguer publiquement des renseignements privés. Cette pratique est souvent utilisée dans le but de harceler une personne ciblée, de l'intimider ou de lui nuire. Elle peut avoir de graves conséquences, notamment le harcèlement en ligne, l'usurpation d'identité, les dommages physiques ou l'atteinte à la réputation et à la vie personnelle d'une personne.

12 — Quel risque la divulgation de données personnelles peut-elle représenter pour une personne?

Changer la photo d'un profil en ligne

Divulguer publiquement des renseignements privés sur une personne

Inscrire automatiquement une personne à des infolettres

Augmenter le nombre de fans en ligne

13 — Les sources d'information les plus courantes pour la divulgation de données personnelles sont les profils des médias sociaux, les archives publiques, les annuaires en ligne et les informations publiques. La divulgation de données personnelles est non

seulement contraire à l'éthique, mais aussi illégale dans de nombreux territoires de compétence, car elle viole la vie privée et peut entraîner de graves préjudices.

14 — Les dangers du métavers et comment se protéger. Les gens ne sont pas toujours ce qu'ils prétendent être. Un avatar peut être n'importe qui. Des adultes peuvent se faire passer pour des adolescents et t'attirer dans des zones privées en te montrant des contenus graphiques et inappropriés. Approche-toi des autres en ligne avec prudence.

15 — Vrai ou faux. Un avatar peut-il être n'importe qui en ligne?

16 — Exact! Un avatar peut être n'importe qui. Suis les personnes qui t'inspirent, qui encouragent la positivité et le bonheur ou celles dont tu pourrais t'inspirer! Apprends à filtrer les contenus qui ne contribuent pas à ton bien-être général.

17 - Voir, c'est croire. Il ne faut pas croire tout ce qui se trouve sur Internet. Tout n'est pas vrai et il existe de nombreuses informations fausses ou trompeuses. Il est important de vérifier les faits et d'utiliser des sources fiables avant de faire confiance à ce que vous trouvez en ligne.

18 - Faut-il croire tout ce que l'on voit sur les médias sociaux ?

Oui, parce que c'est sur Internet

Non, tout ce qui est en ligne n'est pas vrai

Seulement si l'image est drôle

Oui, s'il y a beaucoup de likes

19 - Tout n'est pas réel ou vrai en ligne ! L'internet contient un mélange d'informations exactes, d'opinions, de rumeurs et même de contenus intentionnellement faux. Il est essentiel de faire preuve d'esprit critique, de vérifier les faits et d'utiliser des sources fiables pour vérifier les informations que vous trouvez en ligne.

20 - Souriez à l'appareil photo. Prendre la photo d'une personne pour les médias sociaux implique des considérations relatives à la vie privée, au consentement et au respect des limites personnelles.

21 - Est-il acceptable d'enregistrer des vidéos de ses amis et de les partager sur les médias sociaux ?

Tant que c'est pour le plaisir.

Pas sans leur consentement, car cela pourrait porter atteinte à leur vie privée et à leur confiance.

Tant que vous pensez que vos amis n'y verront pas d'inconvénient.