Je cherche des conseils

Tout d'abord, pense à protéger tes « snaps » (messages envoyés à travers Snapchat). Pour cela, va sur la page d'accueil et clique sur l'icône « Réglages » (roue dentée en haut à droite). Va ensuite dans « Send me snaps », puis sélectionne « My friends » pour autoriser uniquement tes amis à t'envoyer des messages.

Plus généralement, il est essentiel de savoir que rien n'empêche le destinataire de réaliser une capture d'écran si son téléphone en possède les capacités. Snapchat ne garantit pas la suppression définitive des messages. Lorsque Snapchat réalise qu'une capture d'écran a été réalisée, l'expéditeur du message reçoit une notification.

Le destinataire peut également prendre une photo de l'écran avec un autre appareil, ce qui lui permettra d'éviter qu'une notification soit envoyée. Snapchat précise aussi dans sa politique de sécurité qu'il existe des moyens de récupérer des photos, même si elles ont été supprimées.

Le risque réside également dans l'apparition de publication de photos plus ou moins censurées sur des sites comme snapchatleaked.com, par des utilisateurs malveillants. Il existe également une application pour iPhone qui permet de sauvegarder automatiquement les photos ou vidéos reçues : Snap Save. Tant qu'une copie a été conservée (mis en cache) sous Snap Save, l'utilisateur peut visualiser le « snap », même s'il a été effacé sur Snapchat.Tumblr est très clair au sujet de la confidentialité du site : par défaut, tout le contenu publié sur Tumblr est public, c'est-à-dire qu'il peut être indexé par les moteurs de recherche et donc tout le monde peut le voir. Cela inclut la rubrique « À propos » dans laquelle l'utilisateur peut s'être décrit avec précision.

Il t'appartient donc de faire attention en choisissant le

contenu qui sera partagé publiquement.

Comme la plupart des réseaux sociaux, Tumblr fournit des outils pour limiter la visibilité des contenus. Il s'agit de la protection des blogs par un mot de passe qui permet de publier de manière privée. Cependant, le blog protégé par mot de passe n'est pas si facile à gérer !

Pour pouvoir utiliser cette fonctionnalité, il faut créer un blog secondaire car le blog primaire – celui qu'on créé à l'inscription – sera toujours public, sauf si l'utilisateur choisit de faire une publication privée (mais dans ce cas, il est le seul à pouvoir la voir). Pour créer un blog secondaire avec une protection par mot de passe, clique sur le menu du blog en haut à droite de ton panneau de contrôle. Clique ensuite sur « Créer un nouveau blog ». Coche la case à côté de « Protéger ce blog avec un mot de passe ». Tu peux maintenant partager ce mot de passe avec les personnes en qui tu as confiance.La sexualité est une curiosité naturelle. Aussi, il convient de relativiser. En revanche, si ta consommation devient excessive, ou si tu ne peux plus t'en passer, nous te recommandons d'en parler à un adulte. La mise en place d'un filtre parental, par exemple, peut alors t'aider.Le « thigh gap » – qui désigne l'écart entre les cuisses – est un phénomène de plus en plus répandu chez les jeunes femmes et adolescentes où il est perçu comme un critère de beauté. Imposée par la tyrannie de la minceur, cette nouvelle obsession s'avère être effectivement très dangereuse. Nous t'invitons à en parler à un adulte.C'est une prise de contact par un adulte aux intérêts sexuels déviants avec un mineur via Internet.Attention… La personne avec qui tu discutes depuis plusieurs mois n'est pas forcément celle qu'elle dit être. Tu dois donc rester vigilant(e). Nous te conseillons :

- D'être accompagné(e) au moment du rendez-vous, par exemple par un(e) ami(e).
- De rencontrer cette personne dans un lien public, en plein jour.

- D’informer tes parents de ce rendez-vous.

C’est l’ensemble des crimes et délits commis en utilisant les nouvelles technologies (tentatives d’escroquerie, harcèlement en ligne…).

En France, ce sont les autorités de police regroupées dans l’OCLCTIC (Office Central de Lutte contre la Criminalité liée aux Technologies de l’Information et de la Communication) qui traitent les signalements de ces crimes et délits : http://www.internet-signalement.gouv.fr.Il est important de savoir que Twitter est public par défaut et que les profils des utilisateurs – ainsi que leurs tweets – sont visibles par tout le monde. Cela signifie qu’une personne recherchant des informations sur Twitter peut lire les tweets qui s’y rapportent.

Il est cependant possible de rendre ses tweets privés en les protégeant, c’est-à-dire en les verrouillant de sorte qu’ils ne soient visibles qu’aux personnes acceptées par l’utilisateur pour le suivre.

Pour protéger tes tweets :

1. Va sur ton profil
2. Clique sur l’icône « Réglages » (l’icône représente une roue dentée), choisis « Paramètres », puis, dans le menu déroulant, va dans « Confidentialité »
3. Assure-toi que la case à coté de « Protéger mes Tweets » soit cochée.
4. N’oublie pas de sauvegarder les modifications.
5. Important : les abonnés (« followers ») peuvent re-tweeter les tweets protégés. Tu dois donc faire attention à bien choisir les personnes qui auront accès à ton profil et à tes tweets !

Le but est de ne pas diffuser sur Internet de détails personnels qui laisseront des traces ineffaçables et que l’on pourrait regretter d’avoir divulgués dans le futur (par

exemple, au moment de la recherche d’un emploi).Il faut créer un mot de passe fort, composé d’au moins 10 caractères, comportant des lettres et des chiffres et qui ne comporte pas d’élément en rapport avec ses données personnelles (nom, prénom, date de naissance…) ou celles d’un proche.

Le mot de passe est personnel, aussi, ne le donne à personne. De plus, lorsque tu quittes un site Internet ou un réseau social, pense toujours à te déconnecter de ta session avant de cliquer sur la croix.En cas de piratage de compte, il faut tout de suite le sécuriser en en modifiant le mot de passe. Si le compte est inaccessible, tu peux contacter le site Internet en question pour le récupérer, en passant généralement par la rubrique d’aide.

Préviens également tes amis qui peuvent, de leur côté également, signaler le piratage. Sauvegarde bien les preuves (captures d’écran des messages insultants), tu en auras besoin si tu souhaites porter plainte pour usurpation (vol) d’identité.

.C’est tout ce qui peut permettre d’identifier quelqu’un : nom, adresse, téléphone, âge, adresse email, nom de l’école fréquentée…

.Envoyer de tels SMS n’est pas un jeu et tout le monde ne trouve pas cela amusant. Si le message représente des personnes que tu connais, préviens-les et sauvegarde ce message qui pourra servir de preuve si elles portent plainte à la police. En cas de doute, un conseiller Net Ecoute t’assistera au 0820 200 000..Tu peux signaler les sites qui mettent en avant des contenus violents (images, comportements…) ou interdits par la loi à : www.pointdecontact.net. Mais rassure-toi : tu n’as rien fait de mal. Si le choc ou le malaise que tu as pu ressentir ne passe pas, n’hésite pas à en parler à un adulte.Les insultes ou injures sur internet sont punies par la loi. La victime peut porter plainte contre toi. Si tu es mineur,

la responsabilité de tes parents est également engagée. Nous te recommandons donc d'effacer le message insultant et de présenter tes excuses à la victime.Dès lors que les moqueries sont répétées ou dégradantes, nous te recommandons :

1. Avant tout, d'en parler à tes parents et de ne pas répondre aux insultes ou provocations, qui risqueraient alors d'empirer !
2. Ensuite, d'alerter le responsable de l'école ou du collège. Il avertira les autres parents des actes de leurs enfants.
3. Tu peux également bloquer et/ou signaler les personnes qui t'embêtent sur le site en question.
4. Enfin, si tu souhaites porter plainte, pense bien à imprimer les messages. Ils serviront alors de preuves.

Sur la plupart des réseaux sociaux et sites de discussion, on peut bloquer une personne qui nous importune. Sur Skype, il suffit de faire un clic droit sur ce contact et de sélectionner « Bloquer ». Sur Facebook, sur le profil de la personne en bas à gauche on peut la retirer de sa liste d'amis, ou la bloquer, ou encore la signaler en en indiquant la raison.Commence par demander à l'ami(e) de supprimer cette photo. Si elle refuse, il faut le signaler à Facebook en cliquant, lorsque tu es sur la photo, sur le bouton « Signaler ».Snapchat est une application mobile disponible sur smartphone (sous IOS et Android). Elle permet à ses utilisateurs d'envoyer des photos et des vidéos de courte durée. Les messages sont partagés avec un groupe réduit d'amis et disparaissent après avoir été visionnés par le destinataire. La durée de vie des messages va de 3 à 10 secondes, selon les paramètres choisis et il faut garder un doigt sur la photo pour la regarder.

Selon le blog de Snapchat, plus de 200 millions de messages éphémères seraient envoyés chaque jour. Cette application est destinée aux adolescents et aux jeunes adultes. Il est spécifié que l'accord des parents est recommandé pour les

mineurs âgés entre 13 ans et 17 ans.

On l'associe souvent à une appli « sexting », ce qui correspond à l'échange de photos ou de messages coquins par sms. Dans leurs efforts de s'éloigner de cette réputation, les fondateurs ont récemment créé une application pour les moins de 13 ans, « Snapkidz ». Ces derniers peuvent consulter et dessiner sur des photos sélectionnées mais n'ont pas la possibilité de les partager…Il faut que tu demandes l'autorisation de publier ces photos à tes amis, et également à leurs parents si ils sont mineurs. Autrement ils pourraient porter plainte contre toi pour le non-respect du droit à l'mage.Il est important de savoir que Twitter est public par défaut et que les profils des utilisateurs – ainsi que leurs tweets – sont visibles par tout le monde. Cela signifie qu'une personne recherchant des informations sur Twitter peut lire les tweets qui s'y rapportent.

Il est cependant possible de rendre ses tweets privés en les protégeant, c'est-à-dire en les verrouillant de sorte qu'ils ne soient visibles qu'aux personnes acceptées par l'utilisateur pour le suivre.

Pour protéger tes tweets :

1. Va sur ton profil
2. Clique sur l'icône « Réglages » (l'icône représente une roue dentée), choisis « Paramètres », puis, dans le menu déroulant, va dans « Confidentialité »
3. Assure-toi que la case à coté de « Protéger mes Tweets » soit cochée.
4. N'oublie pas de sauvegarder les modifications.
5. Important : les abonnés (« followers ») peuvent re-tweeter les tweets protégés. Tu dois donc faire attention à bien choisir les personnes qui auront accès à ton profil et à tes tweets !

Le but est de ne pas diffuser sur Internet de détails

personnels qui laisseront des traces ineffaçables et que l’on pourrait regretter d’avoir divulgués dans le futur (par exemple, au moment de la recherche d’un emploi).Il faut créer un mot de passe fort, composé d’au moins 10 caractères, comportant des lettres et des chiffres et qui ne comporte pas d’élément en rapport avec ses données personnelles (nom, prénom, date de naissance…) ou celles d’un proche.

Le mot de passe est personnel, aussi, ne le donne à personne. De plus, lorsque tu quittes un site Internet ou un réseau social, pense toujours à te déconnecter de ta session avant de cliquer sur la croix.En cas de piratage de compte, il faut tout de suite le sécuriser en en modifiant le mot de passe. Si le compte est inaccessible, tu peux contacter le site Internet en question pour le récupérer, en passant généralement par la rubrique d’aide.

Préviens également tes amis qui peuvent, de leur côté également, signaler le piratage. Sauvegarde bien les preuves (captures d’écran des messages insultants), tu en auras besoin si tu souhaites porter plainte pour usurpation (vol) d’identité.C’est tout ce qui peut permettre d’identifier quelqu’un : nom, adresse, téléphone, âge, adresse email, nom de l’école fréquentée…