CHAPITRE 8 :

SÉCURITÉ EN LIGNE

SÉCURITÉ EN LIGNE

UNE MULTITUDE DE SATELLITES TOURNE AUTOUR DE LA TERRE, ET ILS SONT DE PLUS EN PLUS NOMBREUX.

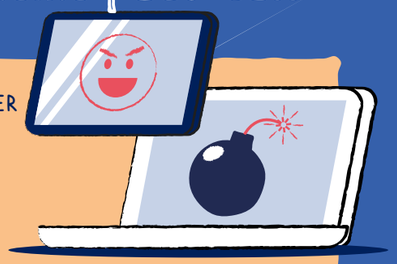
Ils permettent d'améliorer les prévisions météorologiques, de diffuser la télévision, de recevoir des appels téléphoniques dans des endroits éloignés, de se connecter à Internet, d'embarquer des expériences scientifiques et bien d'autres choses encore, comme le suivi du changement climatique.

Mais les satellites font face à des menaces : leur environnement est rude, il y a des risques de collision spatiale... Et ils pourraient aussi se faire pirater par quelqu'un qui voudrait récupérer leurs données, ou provoquer leur dysfonctionnement.

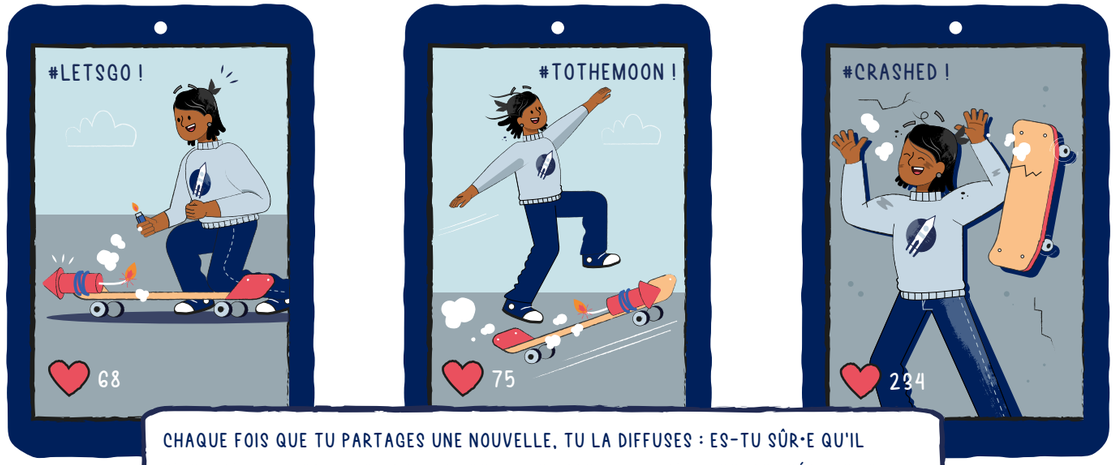
LES SATELLITES SONT SÛRS TANT QUE NOUS LES CONCEVONS DE MANIÈRE À ÉVITER LES PROBLÈMES, QUE NOUS VEILLONS À CE QU'ILS SOIENT UTILISÉS CORRECTEMENT ET QUE NOUS DISPOSONS DES OUTILS (TELS QUE LES MOTS DE PASSE) ET DES HABITUDES NÉCESSAIRES POUR LES PROTÉGER.

Il en va de même pour toi!

SI TU SURFES EN LIGNE, QUELQUES OUTILS ET RÈGLES SONT À SUIVRE POUR RESTER EN SÉCURITÉ. TOUT D'ABORD, LES MOTS DE PASSE : ILS SONT LA CLÉ DE TA VIE NUMÉRIQUE. TES MOTS DE PASSE EMPÊCHENT LES GENS DE VOIR TOUT CE QUE TU AS FAIT ET ÉVITENT QUE D'AUTRES PERSONNES SE FASSENT PASSER POUR TOI EN LIGNE. TES COMPTES EN LIGNE, ET TON SMARTPHONE SI TU EN AS UN, DOIVENT TOUJOURS ÊTRE PROTÉGÉS PAR DE BONS MOTS DE PASSE.



Mais adopter un bon comportement en ligne ne consiste pas seulement à assurer ta sécurité : il s'agit aussi de ta responsabilité personnelle.



CHAQUE FOIS QUE TU PARTAGES UNE NOUVELLE, TU LA DIFFUSES : ES-TU SÛR·E QU'IL S'AGIT D'UNE INFORMATION DIGNE DE CONFIANCE PROVENANT D'UNE SOURCE SÉRIEUSE ? CHAQUE FOIS QUE TU PARTAGERAS UNE PHOTO DE TOI, ELLE SERA ACCESSIBLE AU PUBLIC : EST-IL ACCEPTABLE QUE DES PERSONNES, Y COMPRIS TON FUTUR EMPLOYEUR ET TES FUTURS COLLÈGUES, LA VOIENT ?

Oserais-tu dire ce que tu as écrit si tu parlais à une personne en face de toi ? Chaque fois que tu cliques sur un lien, un serveur enregistre qu'un nouveau clic a été effectué... et il donne généralement plus de visibilité - donc plus d'influence ou d'argent - à celui qui se trouve derrière ce lien. Quels sont les sites web et les groupes que tu souhaites soutenir ?
En d'autres termes, tu dois considérer le monde en ligne comme un monde réel, où chaque action a un impact sur les autres et où tu as une responsabilité. C'est un monde où des actions bien choisies peuvent aider les autres, et où des actions mal choisies peuvent nuire aux autres.

Chaque fois que tu écris un commentaire, il sera lu par de vraies personnes avec de vrais sentiments.

Enfin, sache que l'intimidation et le harcèlement sont des problèmes importants en ligne. Si tu te sens blessé·e par le comportement des autres, parles-en immédiatement à quelqu'un en qui tu as confiance, comme un parent, un enseignant ou un ami. Ne garde pas le problème pour toi. Cherche du soutien. Tu n'es pas à blâmer pour les humiliations que tu subis, tu n'as donc pas à en avoir honte. Tu peux conserver les messages et les captures d'écran comme preuves, mais n'essaye pas de répondre ou de riposter. Le mieux est de se désengager, voire de bloquer les messages des personnes qui t'ont blessé·e.

De nombreux pays disposent d'une ligne d'assistance téléphonique contre le cyberharcèlement. Recherche la ligne d'assistance téléphonique dans ton pays et appelle-la pour obtenir des conseils.

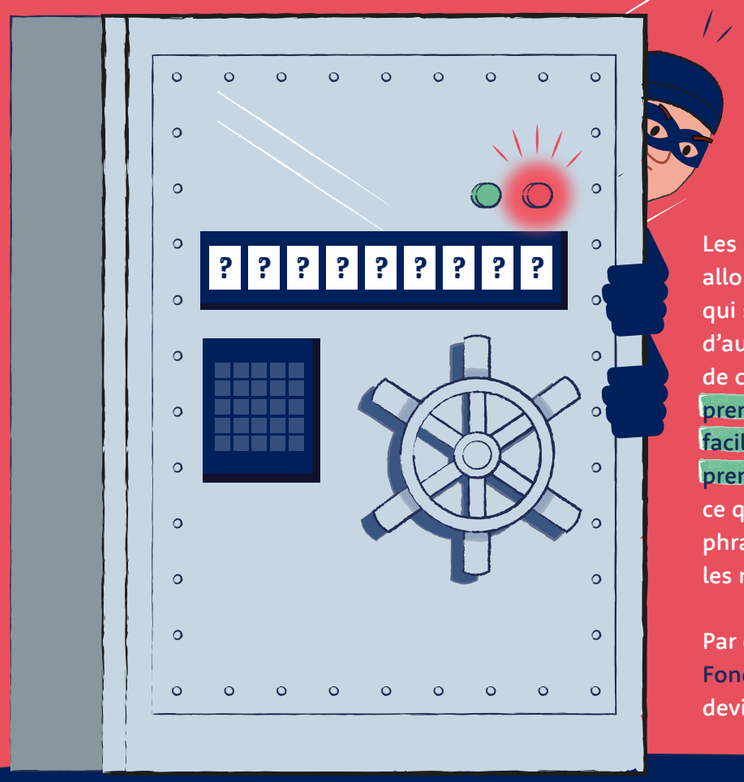
EXPRIME-TOI!

CONTRE LE HARCÈLEMENT

SI TU ES TÉMOIN DE HARCÈLEMENT, NE LE LAISSE PAS PASSER... PRENDS POSITION ET SOUTIENS LA PERSONNE QUI EST VISÉE. LE SIMPLE FAIT DE RECEVOIR UN MESSAGE GENTIL PEUT ÊTRE D'UN GRAND SECOURS POUR UNE PERSONNE QUI SE SENT ATTAQUÉE ET SEULE.

ACTIVITÉ 1

TON MOT DE PASSE : QU'IL SOIT LOOOOOONG



Les mots simples sont faciles à pirater, nous allons donc devoir créer un mot de passe qui soit long et n'ait de sens pour personne d'autre que toi. Il existe plusieurs façons de créer un mot de passe. En voici une: prends une phrase dont tu te souviendras facilement et écris seulement les deux premières lettres de chaque mot. Veille à ce qu'il y ait quelques majuscules dans ta phrase, afin que ton mot de passe mélange les minuscules et les majuscules.

Par exemple : "Je lis un livret de la Fondation Airbus !" le mot de passe deviendra : JeliunlidelaFoAi. Super !

CONSEIL PRO

IL NE FAUT JAMAIS ÉCRIRE TON MOT DE PASSE SUR UN PAPIER OU UN DOCUMENT : IL NE DOIT RESTER QUE DANS TA TÊTE ... OU DANS TON LOGICIEL DE GESTION DES MOTS DE PASSE.

ACTIVITÉ 2

ET QU'IL SOIT FORT !

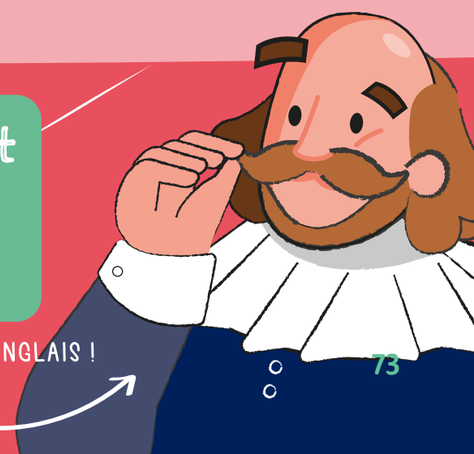
Tu peux remplacer certains mots par des chiffres qui leurs ressemblent.
Dans l'exemple précédent, tu peux remplacer "un" par 1, ce qui en fait un mot de passe plus fort : Jeli1lidelaFoAi. Et comme la phrase originale était terminée par un point d'exclamation, ajoutons-le à la fin :

Jeli1lidelaFoAi!

Ce mot de passe sera difficile à pirater !
Il est facile à retenir pour toi,
mais impossible à deviner pour les autres.

Peux-tu deviner quelle phrase était derrière le mot de passe 2beorno2be,thisthequ ?

C'EST LA CITATION LA PLUS CÉLÈBRE DE SHAKESPEARE, EN ANGLAIS !



ACTIVITÉ 3

ENQUÊTER TOI-MÊME

Que pouvons-nous trouver sur toi en ligne ?

Imagine que la directrice d'une entreprise que tu adores soit sur le point de te proposer le job de tes rêves...

Avant de te le proposer, la directrice aimerait vérifier qui tu es.
Elle cherche donc sur Internet toutes les informations, photos, vidéos, commentaires, etc. qu'elle peut trouver sur toi. Que va-t-elle trouver ?

Eh bien, tu peux le vérifier : fais quelques recherches sur toi-même, sur Internet. Y a-t-il quelque chose que tu ne voudrais pas que la directrice lise ? Des choses qui pourraient la surprendre, et l'empêcher de te donner le job de tes rêves ? Si la réponse est oui, il est temps de supprimer au plus vite ces photos, vidéos et commentaires... N'oublie pas que tu peux modifier tes paramètres de confidentialité sur les réseaux sociaux, pour choisir qui peut voir tes publications.

Et bien sûr, le mieux est d'éviter de poster des informations potentiellement embarrassantes !

Ressources supplémentaires : Pour obtenir d'autres conseils sur la sécurité en ligne, consulte les articles, vidéos et autres ressources des sites Web suivants *Jeunesse j'écoute* et *Cyberaide* !