La sécurité d'abord

Comment puis-je assurer ma sécurité en ligne ?
Internet est un outil fantastique. Tu peux y rencontrer de nouvelles personnes, contacter des gens que tu connais déjà, apprendre tout plein de choses et t'amuser de ouf. Mais tu dois **toujours rester prudent**, parce que tu cours de grands et de petits risques. BOUH.

diggit

proximus

Les risques pour ton ordi

Tout comme tu dois être attentif quand tu marches dans la rue, tu dois aussi **toujours faire gaffe en ligne**. Si un malware comme un Cheval de Troie attaque ton ordi, des programmes et des gens malintentionnés peuvent y pénétrer et mal utiliser tes données.

Comment cela arrive-t-il ?

- Par des sites web normaux qui sont **“infectés”**
- Par des logiciels qui **ne sont pas mis à jour**
- Par des **pièces jointes “infectées”** dans un e-mail
- Par des comptes de réseaux sociaux **mal protégés**
- Parce que tu n’as pas **d’antivirus** et/ou de firewall

Ce dernier est facile à régler ! Sais-tu que Windows contient d’office les programmes **Windows Defender** et **Windows Firewall** ?

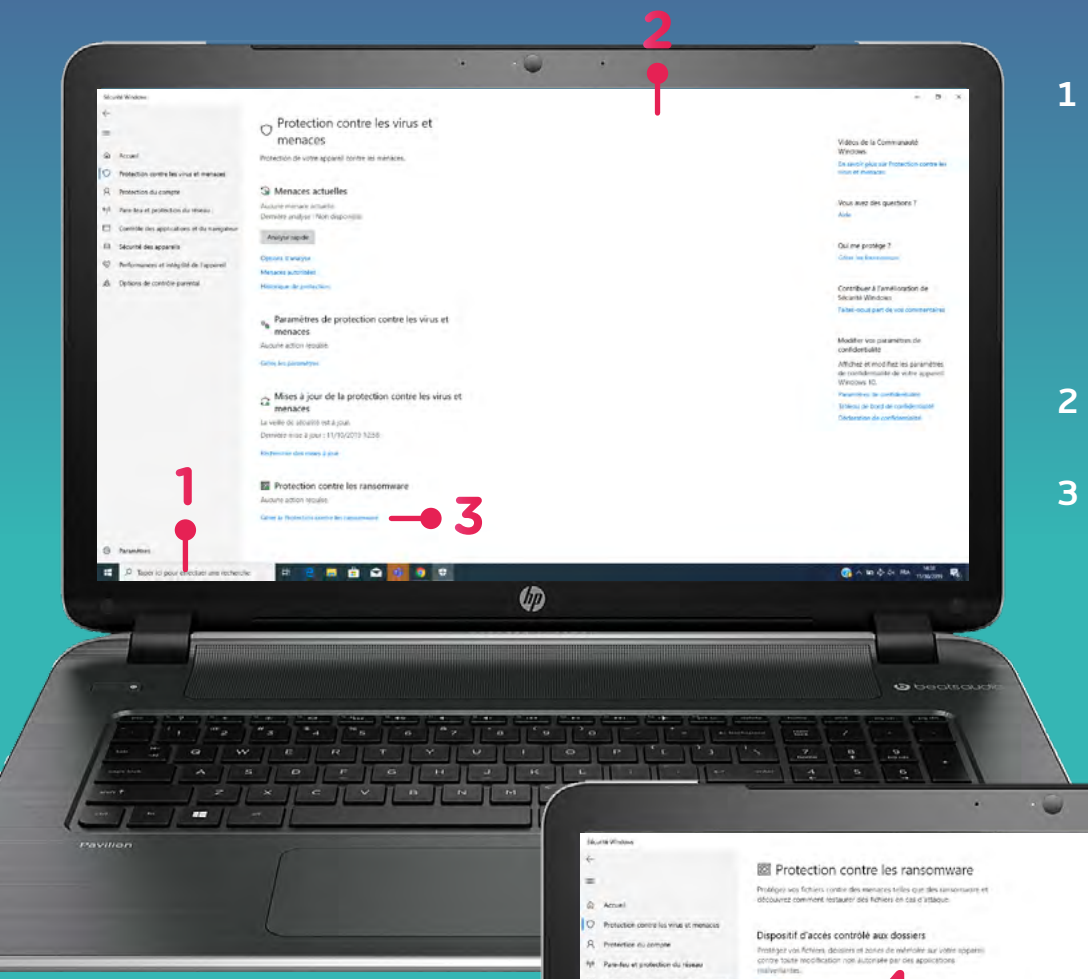
Zone de danger!

Le malware est un nom qui recouvre toutes sortes de logiciels dangereux. Ils peuvent endommager ton ordi ou voler des informations sensibles. Tes mots de passe, par exemple ! Ça craint. 👻

Le Cheval de Troie en est un exemple. Il ressemble à quelque chose de fiable, que tu crois connaître. Mais dès que tu le laisses rentrer, il casse tout. Et il cause beaucoup de dommages à ton ordi.

Un enfant averti en vaut 10 !

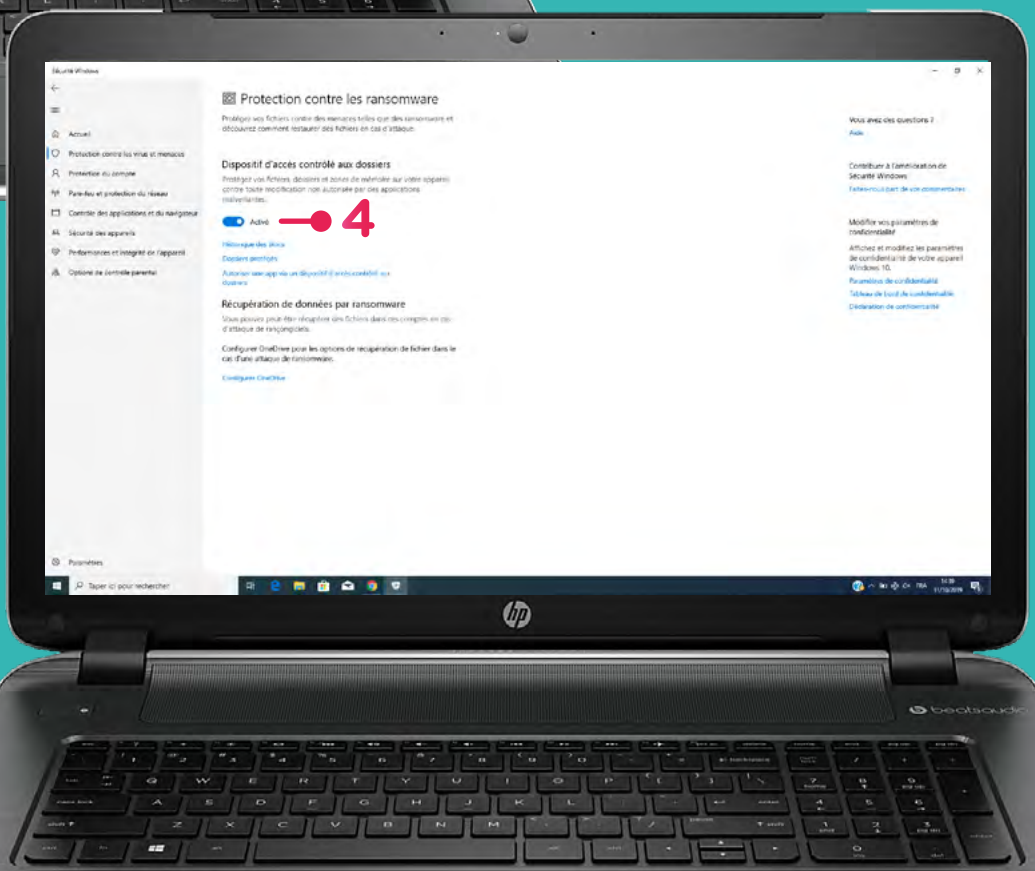
Comment fonctionne Windows Defender ?



1 Tape “Windows Defender” dans la barre de recherche de ton bureau en bas à gauche et presse Enter (uniquement si tu as Windows, évidemment).

2 Voilà à quoi ressemble Windows Defender.

3 S’il est écrit “Désactivé”, il faut juste cliquer sur la barre grise pour activer Windows Defender Antivirus.

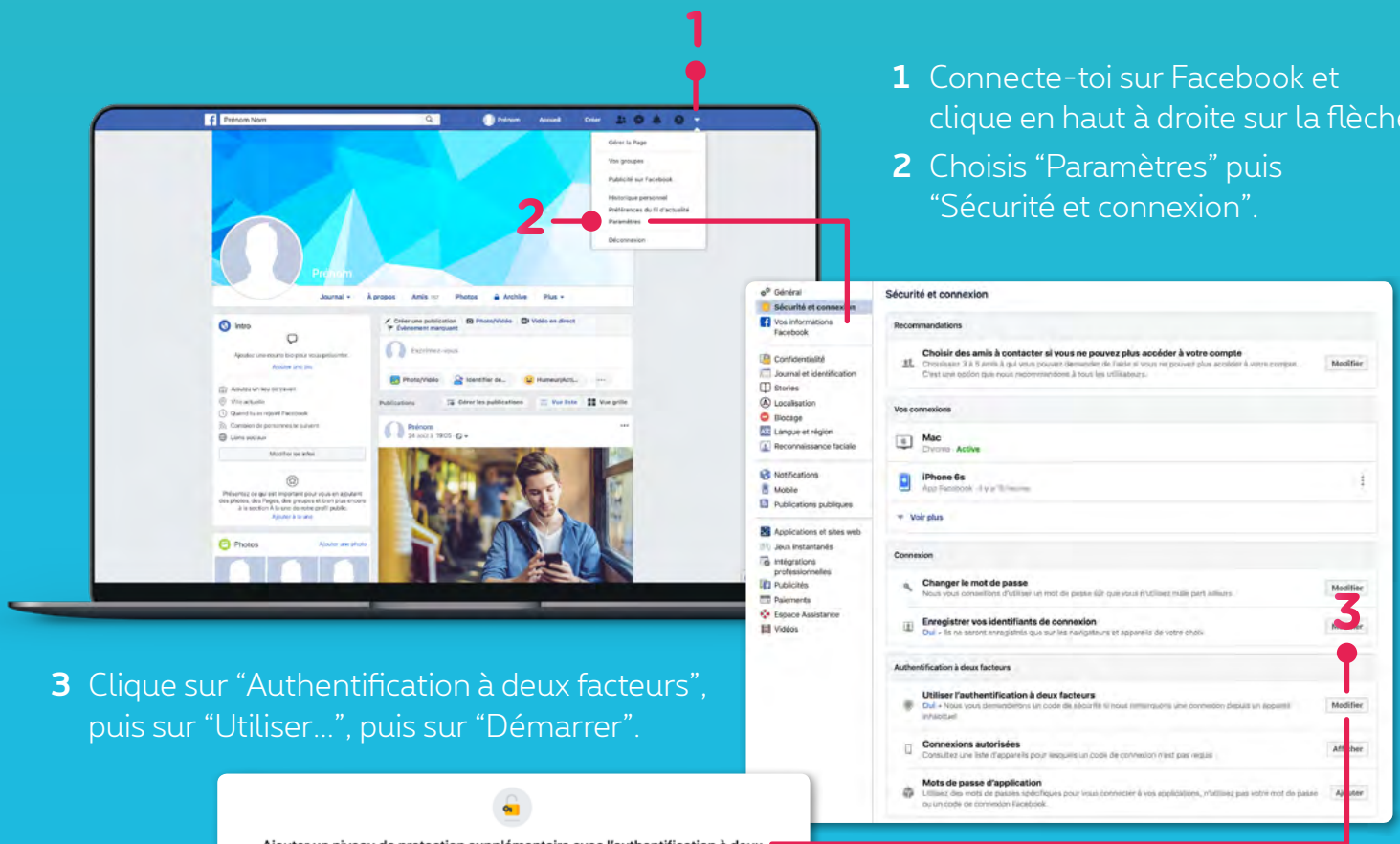


4 Alors encore cliquer sur “Scan rapide”. Le programme recherchera les fichiers infectés et, ensuite, tu pourras les effacer.

Ouf, tu as sauvé ton ordi ! Quel **héros digital !** 🤠

En sécurité sur les réseaux sociaux

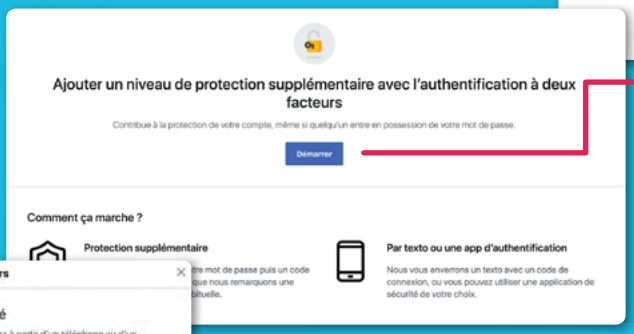
Pour empêcher des gens mal intentionnés d'accéder à tes réseaux sociaux, plusieurs plateformes proposent une option qui s'appelle l' **"authentification à deux facteurs"**. C'est un terme compliqué, mais il s'installe facilement. Prenons Facebook pour l'expliquer.

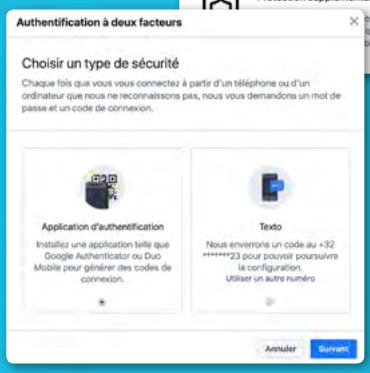


1 Connecte-toi sur Facebook et clique en haut à droite sur la flèche

2 Choisis "Paramètres" puis "Sécurité et connexion".

3 Clique sur "Authentification à deux facteurs", puis sur "Utiliser...", puis sur "Démarrer".





4 Choisis "Texto" pour recevoir un code de sécurité sur ton G et clique sur "Suivant".

5 Un code est envoyé au numéro de téléphone que tu as donné. Complète-le ici. Clique sur "Suivant". Voilà, l'authentification à deux facteurs est prête ! A partir de maintenant, tu recevras un code à chaque fois que tu te connecteras d'un smartphone ou d'un ordi inconnu.

Plus sûr que sûr !

Mot… de passe !

Ton **mot de passe** est un élément super important de ta sécurité en ligne.

Donc, ne choisis pas un mot de passe qu'on peut deviner facilement comme :

- Ton propre nom (bah oui !) ou celui de ton chien (sorry, Dark Vador !)
- Ta date de naissance ou le numéro de ta maison
- Des séries logiques comme "abcdef" ou "**54321**"
- "Mot de passe"

Important : ne garde jamais un papier avec ton mot de passe à un endroit visible ! Il faut le retenir par coeur.

Ton mots de passe est top secret !

Ne donne jamais ton mot de passe à quelqu'un d'autre. **Jamais ! Jamais ! Jamais !** Même pas à ton meilleur ami ou à ta meilleure amie. Vous êtes très proches, mais ton mot de passe est ton secret à toi. Tu ne partages pas ta brosse à dents non plus, hé ?

Sûr de sûr

Chut… ne le dis pas aux autres : un mot de passe sûr se compose d'au moins 12 caractères. Et le mieux, c'est de mélanger des minuscules et des majuscules, des chiffres et des caractères spéciaux. **MonChien@boie20fois** ? Facile à retenir, difficile à trouver !

Conseils de sécurité pour ton ordi

En résumé :

- N'ouvre jamais un e-mail ou une pièce jointe qui paraît suspect. Avec un titre bizarre, pas de sujet, un expéditeur inconnu… Utilise ton bon sens !
- Sur les réseaux sociaux, ne clique jamais sur un lien bizarre. Demande à l'expéditeur si le lien vient bien de lui !
- Si tu dois compléter des données personnelles sur un site web, vérifie d'abord s'il y a un https:\\ dans le lien en haut de ta fenêtre. Comme ça, tu es certain que ce site est bien protégé. Et que tes données sont en mains sûres.

Permis ? Possible ?

Comment rester en sécurité sur Internet? Tu sais très bien ce qui est permis ou pas. Mais on va le répéter au cas où. On ne sait jamais...

Si tu ne fais pas attention, tu peux rencontrer sur Internet des gens que tu préfèrerais ne pas rencontrer, comme dans la vie réelle. Ça peut être des gens qui ne respectent pas tes limites, qui sont méchants ou qui demandent de l'argent. Voici comment te préparer.

À l'attaque !

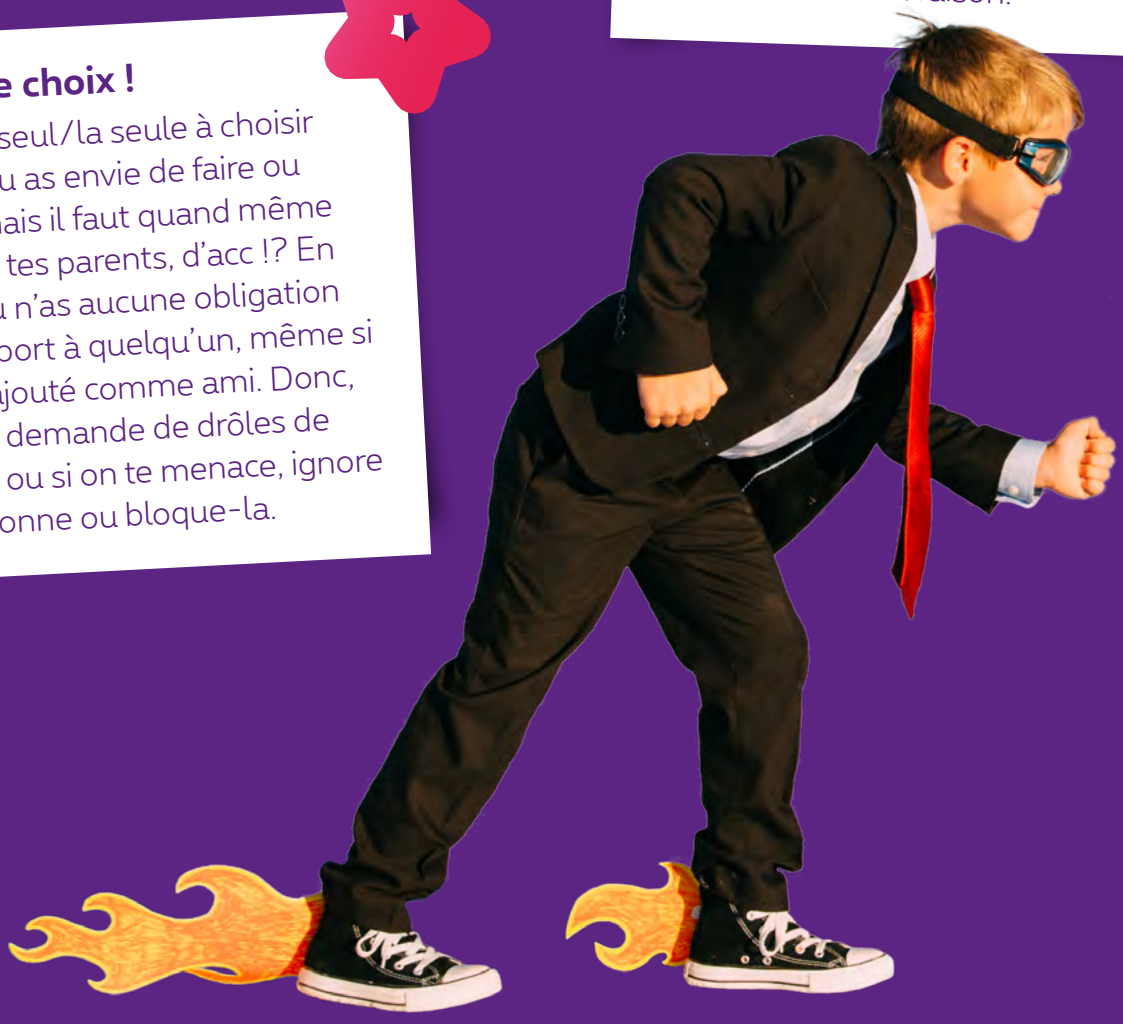
Un vrai détective !

Sur Internet, il circule beaucoup d'infos qui sont complètement fausses. #FakeNews. Si tu lis quelque chose qui semble incroyable, utilise ton bon sens. Tu peux toujours vérifier l'info en demandant à tes parents ou en cherchant sur Google. Tu ne sais pas comment ? Va voir "J'sais tout!" !

Tu peux aussi recevoir de fausses infos par e-mail. Ça ne t'est pas déjà arrivé qu'un prince d'un pays lointain veuille t'offrir sa fortune ? Ou que tu as gagné au lotto, alors que tu n'y joues même pas ? Si ça te semble trop beau pour être vrai, tu as souvent raison.

Tu as le choix !

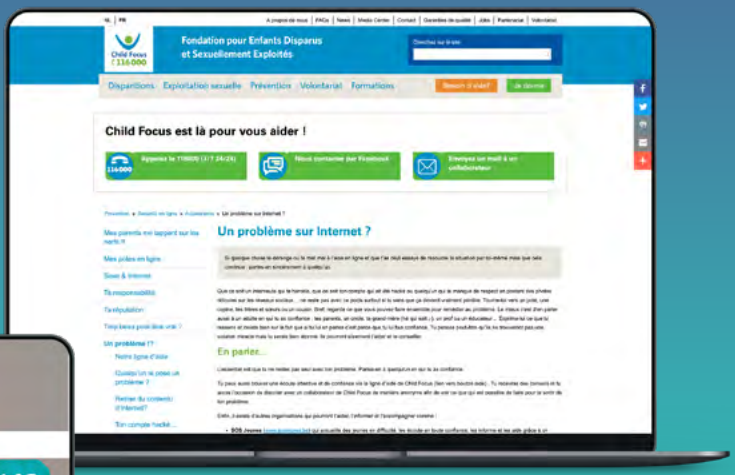
Tu es le seul/la seule à choisir ce que tu as envie de faire ou pas – mais il faut quand même écouter tes parents, d'acc !? En ligne, tu n'as aucune obligation par rapport à quelqu'un, même si tu l'as ajouté comme ami. Donc, si on te demande de drôles de photos ou si on te menace, ignore la personne ou bloque-la.

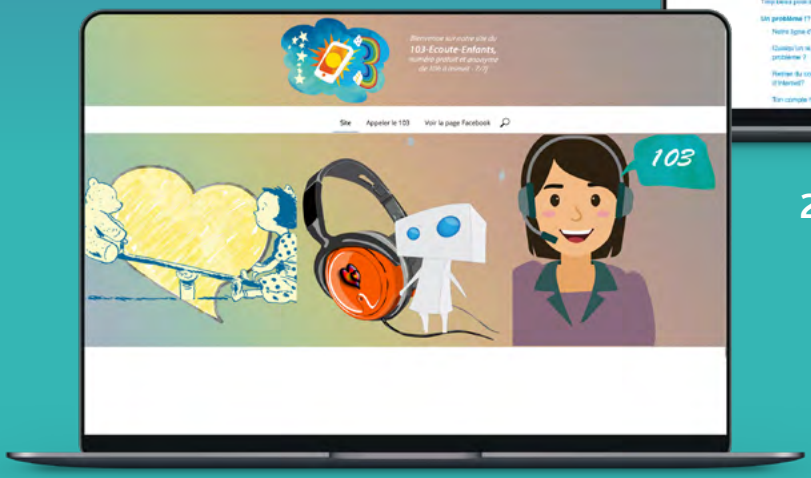


Le cyber-harcèlement, c'est non !

Quelqu'un te harcèle ou dit du mal de toi en ligne ?
Tu peux signaler ce comportement.

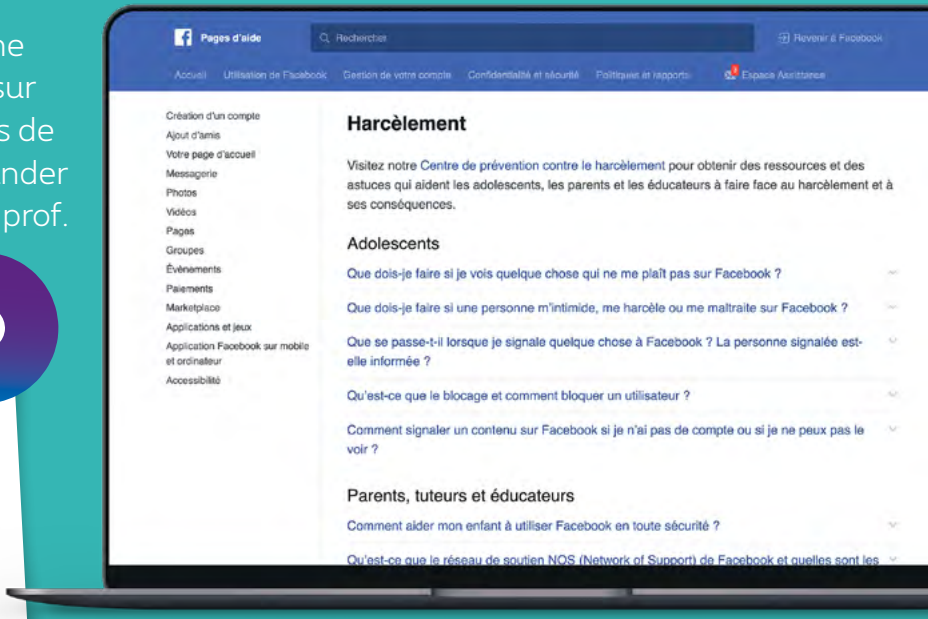
1 Tu trouveras une écoute attentive et une personne de confiance chez **Child Focus** : tu peux les contacter via leur site web, en téléphonant au numéro gratuit **116000**, par e-mail ou via Facebook.





2 Tu peux envoyer un e-mail sur le site web **www.103ecoute.be** ou y chatter avec quelqu'un. Tu peux aussi téléphoner **au numéro gratuit 103**.

3 C'est aussi possible sur la plateforme des réseaux sociaux. Par exemple, sur **Facebook**, tu peux signaler des faits de harcèlement et tu peux aussi demander l'aide d'un parent, d'un ami ou d'un prof.



Tu n'es pas seul(e) !

Tu as fait quelque chose en ligne dont tu as honte ou que tu trouves bête ? N'hésite pas un instant et parles-en avec une personne en qui tu as 100% confiance pour que vous trouviez ensemble une solution. Tout le monde a droit à l'erreur, non ?

Can you diggit? Yes, you can!

proximus