# **Rentrée des classes : cinq conseils pour aider les enfants à surfer en toute sécurité**

Avec la fin toute proche des vacances, de nombreux enfants vont reprendre le chemin de l’école et utiliser internet et leur smartphone pour leurs devoirs et leurs rendez-vous. Comme il est bien sûr important à nos yeux que les enfants agissent de manière sûre et réfléchie lorsqu’ils sont en ligne, il nous a semblé bon de partager les 5 conseils suivants pour la rentrée des classes.

Si vos enfants ne connaissent pas encore ces conseils, prenez le temps de les parcourir avec eux pour que cette année scolaire aille de pair avec une excellente expérience en ligne.

**1) Ne partagez pas en ligne ce que vous ne partageriez pas dans la vraie vie**

Beaucoup de choses sont partagées en ligne comme si elles n’étaient échangées qu’entre deux parties. Or, il s’agit bien de messages publics (ou partagés publiquement) qui peuvent être lus par tous.

Tout ce que vous postez en ligne peut aussi subsister très longtemps. Si vous ne voulez donc pas que tout le monde (y compris votre grand-mère) lise ou voie certaines choses « honteuses » ou personnelles, ne les postez pas ! Même si l’appli dit que certains posts disparaîtront, les techniques de contournement ne manquent pas.

Enfin, ne perdez pas de vue la puissance de vos posts ou de vos paroles, même en ligne. Tout bon citoyen en ligne sait que tout ce que vous pouvez dire sur les autres peut avoir un impact important. Soyez donc toujours poli et retenez que si vous ne voulez pas que les autres parlent de vous d’une certaine manière, vous ne devez pas le faire non plus.

**2) Gardez vos posts privés et limitez votre profil au minimum**

Avez-vous bien vérifié la confidentialité de vos profils sur les réseaux sociaux ? Voici quelques conseils pour verrouiller vos profils Facebook et Instagram.

D’une manière générale, il est conseillé de limiter l’accès à votre profil aux amis, de manière à toujours savoir précisément qui peut voir vos posts. Il existe également de nombreuses options de confidentialité selon les réseaux sociaux. Il est donc bon de toujours garder à l’œil vos propres paramètres de confidentialité et de les contrôler de temps à autre.

Retenez que, même si vous postez en privé, vous n’aurez jamais tout à fait la garantie que ces informations seront conservées en sécurité. Quelqu’un pourrait par exemple réaliser une capture d’écran et la partager. Soyez aussi prudent avec les informations que vous partagez, comme votre adresse, votre ville, votre adresse e-mail ou des informations personnelles. Ces informations sont accessibles à tous et vous ne voulez bien évidemment pas que tout le monde puisse en disposer.

**3) C’est bien de partager… mais pas vos mots de passe !**

Les mots de passe doivent être uniques et personnels.

Avoir le même mot de passe pour toutes vos applis et sites internet est bien sûr plus facile. Mais dans la réalité, si quelqu’un connaît votre adresse e-mail et votre mot de passe à un seul site, il aura accès à tout.

Cela arrive souvent lorsque des sites sont piratés. Les hackers ne savent que trop bien que beaucoup de personnes réutilisent leurs mots de passe et une fois qu’ils ont piraté un site, ils essaient ces mots de passe sur d’autres sites.

Partager des comptes et des mots de passe avec des amis n’est pas non plus une bonne idée. Si vous partagez un compte avec un ami et si son téléphone est volé ou piraté, tous vos comptes seront également menacés. Dans ce cas, la solution est simple : ne partagez pas de comptes !

**4) Téléchargez avec prudence**

Comparez votre téléphone ou votre ordinateur à votre propre corps : vous ne mangeriez pas n’importe quelle nourriture trouvée dans la rue. De la même façon, vous devez également faire preuve de prudence avec ce que vous mettez sur votre appareil. Certains programmes ou applis peu fiables risquent ainsi d’endommager sérieusement votre téléphone ou ordinateur, voire mettre dans certains cas des informations personnelles en danger.

Soyez donc prudent quand vous cliquez sur quelque chose, qu’il s’agisse d’un e-mail en apparence sympa, d’un questionnaire ou d’un logiciel gratuit. Le plus sûr pour votre téléphone consistera à télécharger des applis à partir des app stores officiels et non depuis n’importe quel site internet.

**5) Pensez à bien fermer votre session**

Si vous n’utilisez plus une appli ou un site internet, veillez à bien vous déconnecter. Cela sera surtout important si vous utilisez un ordinateur public à l’école ou à la bibliothèque, voire dans un magasin. Dans le cas contraire, vous permettrez à la personne suivante d’accéder librement à votre compte Facebook ainsi qu’à vos e-mails personnels.

Utiliser un mot de passe pour votre téléphone est également recommandé. Même si cela peut paraître compliqué, les avantages l’emporteront clairement sur les inconvénients.

Vous éviterez ainsi qu’un voleur ne puisse utiliser vos applis et les informations sur votre compte. Cela vous permettra aussi d’éviter des blagues de vos amis s’ils viennent à s’emparer de votre téléphone.

Un mot de passe est un moyen super simple mais aussi très efficace pour empêcher que d’autres personnes ne postent des messages sous votre nom ou même ne fassent des achats à l’aide de votre compte. Un simple mot de passe peut vous éviter bien des problèmes (évitables).

**Vous avez d’autres conseils à nous donner ?**

Vous avez des conseils que vous aimeriez partager avec nous pour aider les enfants à surfer en toute sécurité ? Nous serons ravis de les entendre.