INTERNET ET SES DÉRIVES

Télévision, consoles de jeux, téléphones portables, ordinateurs et autres tablettes : les outils numériques sont utilisés de plus en plus, et de plus en plus tôt. Un enfant de trois ans est capable de se servir d'un écran tactile, et même de naviguer sur Internet. Mais attention !… ce n'est pas sans danger, et nous autres parents devons poser des règles pour préserver intimité, sphère familiale et santé.

Les jeunes qui sont nés à partir de 1995 ont toujours baigné dans l'univers numérique. C'est la « génération écran », familière avec le monde virtuel, même si elle n'en maîtrise pas forcément tous les rouages.
Chaque jour, les 9-16 ans passent en moyenne deux heures sur Internet, et deux de plus devant la télé ou sur une console de jeux.

Internet est un formidable outil de découverte, d'information, de partage, de communication, de divertissement. Cependant, l'utilisation d'Internet peut s'accompagner de pièges auxquels nos enfants peuvent être exposés. Par conséquent, il convient de faire preuve d'un minimum de prudence, afin d'éviter à nos enfants (aussi bien qu'à nous mêmes) de se retrouver victimes de ces dérives...

A) Les principaux pièges d'Internet

1 - L'usurpation d'identité

C'est le fait d'utiliser les identifiants (pseudonyme et mot de passe) de quelqu'un d'autre pour pirater son compte, dans le but d'utiliser son image, faire des choses malhonnêtes en son nom, fouiller dans son ordinateur ou l'endommager à distance (en y envoyant un virus informatique).

2 - Les mauvaises rencontres

Nous devons veiller à ce que nos enfants n'aient pas d'échanges avec un inconnu, quelque soit l'âge qu'il prétend avoir. En effet, certains adultes peuvent se faire passer pour des enfants sur les sites de discussions en ligne, les réseaux sociaux, les forum, les blogs ou les jeux en ligne. Leur but est de dialoguer avec les enfants, gagner leur confiance, obtenir des renseignements, des photos, voire même un rendez-vous…

3 - Les réseaux sociaux

Les réseaux sociaux très prisés des mineurs sont Skype, Facebook, Twitter, MySpace, Ask, Instagram et Snapchat.
Si les réseaux sociaux sont généralement réservés aux plus de 13 ans, c'est parce que des pédopsychiatres ont déterminé que les moins de 13 ans n'ont pas la construction mentale et le recul suffisants pour affronter des dérives, sans conséquences fâcheuses sur leur équilibre.

Gendarmerie nationale
Brigade de Prévention de la Délinquance Juvénile des Yvelines
12 rue Benjamin Franklin – 78000 VERSAILLES
Tél : 01.39.67.50.54 – Email : bpdj.ggd78@gendarmerie.interieur.gouv.fr

Or, les réseaux sociaux sont souvent vecteurs de messages malsains ou malveillants, d'injures, de propos diffamatoires, de discriminations, ou même de harcèlement (moqueries, chantage, menaces).
Les parents dont l'enfant est inscrit sur un réseau social doivent veiller à ce que leur enfant ne diffuse pas d'informations ou de photos personnelles, et qu'il n'accepte pas des inconnus en « amis ».

B) Quelques précautions pour éviter ces pièges

1 - Tous les ordinateurs verrouillés

Tout d'abord, il convient pour nous autres parents de créer notre propre session d'utilisateur, sur chaque ordinateur (et tablette numérique) du domicile. Nous pouvons ainsi protéger notre session personnelle avec un code d'accès, afin de la rendre inaccessible à nos enfants, et donc de nous garantir l'impossibilité pour ces derniers de se connecter sur Internet en notre absence.

Nous pouvons en profiter pour créer une session d'utilisateur pour chaque enfant. On est ainsi à même de définir le niveau de sécurité adapté à nos enfants, en installant un logiciel de contrôle parental sur leur session.

2 - L'installation d'un logiciel de contrôle parental

Notre enfant peut se retrouver confronté à des images obscènes ou violentes, que ce soit en « zappant » seul sur les chaînes de télévision, ou bien au gré de sa navigation sur Internet, ou encore à l'occasion d'intrusions inopinées de ce genre d'images sur l'écran d'ordinateur ou de tablette.

Depuis 2006, tous les fournisseurs d'accès à Internet ont l'obligation de fournir à leurs clients un système de contrôle parental gratuit, par simple téléchargement sur leur page d'accueil.

Il convient donc d'installer un logiciel de contrôle parental, afin de bloquer l'accès aux sites à caractère pornographique ou violent, en filtrant les images et autres documents obscènes ou de nature à choquer nos enfants.

Un logiciel de contrôle parental se présente sous 2 modes possibles : le mode « enfant » et le mode « adolescent » :
- en mode « enfant », ces systèmes permettent de restreindre l'accès de notre enfant à une sélection de sites au contenu vérifié et adapté à son âge ;
- en mode « ado », le logiciel refuse seulement l'accès à certains sites au contenu jugé inapproprié.

3 - Les écrans dans une pièce commune

Un logiciel de contrôle parental ne suffit pas : il ne nous dispense pas de surveiller la navigation de notre enfant sur Internet. Pour ce faire, il nous est fortement conseillé d'installer l'ordinateur ou la tablette numérique dans une pièce à vivre, et de limiter son usage à cette pièce.
Cela nous permet de garder un œil sur ce que fait notre enfant, et il lui sera plus pratique de s'adresser à nous pour des remarques ou des questions.

Protéger nos enfants des dérives d'internet passe par le dialogue avec eux.
Accompagner nos enfants sur Internet les aidera à devenir prudents, responsables, autonomes et capables d'éviter les pièges.

Gendarmerie nationale
Brigade de Prévention de la Délinquance Juvénile des Yvelines
12 rue Benjamin Franklin – 78000 VERSAILLES
Tél : 01.39.67.50.54 – Email : bpdj.ggd78@gendarmerie.interieur.gouv.fr

4 - Temps de connexion Internet limité

Il est aussi vivement recommandé d'astreindre nos enfants à une durée maximale de navigation sur Internet. Au besoin, les logiciels de contrôle parental nous permettent aussi de bloquer l'accès à Internet pendant certaines plages horaires au quotidien, ou certains jours de la semaine.

5 - Des identifiants sûrs

Ensuite, il est important de s'assurer que notre enfant ait un pseudonyme et un mot de passe sûrs, c'est à dire qui ne révèlent aucun renseignement personnel (son identité, son âge ou le nom de sa commune). De même qu'on tient à savoir où nos enfants vont dans la rue et à connaître leurs amis, on se doit de savoir où il vont sur Internet et de connaître les gens avec qui ils y sont en contact.

6 - Une webcam sécurisée

Des adultes mal intentionnés peuvent chercher à convaincre l'enfant d'allumer la webcam. Même quand l'enfant refuse, il peut arriver que certains personnes mal intentionnées parviennent à prendre à distance le contrôle de la webcam pour visualiser l'enfant : il peut s'agir de pédophiles, ou de personnes (mineurs comme majeurs) qui cherchent à filmer l'enfant dans le but d'exercer un chantage.
L'idéal est de penser non seulement à éteindre systématiquement la webcam, mais aussi à mettre un cache par dessus.

7 - Précautions minimum pour les réseaux sociaux

Quel que soit le réseau social sur lequel les enfants peuvent être inscrits, il est important que nous autres parents nous assurions au moins d'avoir nous-mêmes un accès libre au profil de nos enfants, et que les paramètres de confidentialité de leur profil soient verrouillés au maximum.

Gendarmerie nationale

Brigade de Prévention de la Délinquance Juvénile des Yvelines
12 rue Benjamin Franklin – 78000 VERSAILLES
Tél : 01.39.67.50.54 – Email : bpdj.ggd78@gendarmerie.interieur.gouv.fr