The Security Division of EMC

# Accompagner ses enfants en ligne en toute sécurité *:*
## *bonnes résolutions pour une e-rentrée réussie*


Dans le cadre de sa campagne pédagogique de sensibilisation au bon usage d'Internet *« Internet, Les Autres et Moi »,* lancée en mars 2013 et destinée aux jeunes et à leurs parents, RSA présente ses recommandations pour une rentrée connectée réussie.

Période charnière, la rentrée annonce pour plusieurs millions d'élèves et leurs parents l'adoption de nouvelles habitudes et de nouveaux usages, notamment en ligne. A savoir : Internet est l'un des premiers outils d'aide au travail à la maison pour les enfants de 11 à 17 ans, qui sont **98%** à l'utiliser pour chercher des informations et **95,3%** pour faire du travail scolaire*.

Pourtant, sans quelques règles et conseils simples, Internet peut devenir une source de dangers pour les enfants qui n'ont pas toujours les bons réflexes face à des contenus inadaptés.

**Et les parents dans tout cela ?**


Pour les parents qui souhaitent mettre toutes les chances de réussite du côté de leurs enfants, pas question non plus de faire l'impasse sur les nouvelles technologies. Comment gérer la jungle des réseaux sociaux, leur smartphone devenus un objet transitionnel, les pseudos, avatars et autre photos téléchargées en masse ?

Et comment s'assurer que son équipement informatique tiendra la distance, lorsque l'on n'a pas de connaissance particulière pour se protéger efficacement?

RSA
The Security Division of EMC

Voici quelques conseils simples pour aborder la rentrée en toute sérénité :

### 1/ Faire d'internet une activité familiale

Instaurez un dialogue et créez un partage familial autour des usages de l'Internet. Pour cela, placez l'ordinateur dans un lieu de passage et n'hésitez pas à vous intéresser à ce que votre enfant fait sur la toile, que cela concerne ses devoirs ou ses relations sociales.

D'autre part, ne pas laisser votre enfant seul sur internet est le meilleur moyen de réduire les risques de sécurité, car vous serez plus à même de repérer un contenu inapproprié ou suspect.

**ATTENTION : passer trop de temps devant un écran peut limiter la concentration et donc la vigilance !**

## 2/ Réseaux sociaux : sélectionner avant de poster


RSA
The Security Division of EMC

Les cybercriminels utilisent de plus en plus les réseaux sociaux pour récupérer des informations sur nous, nos goûts et nos habitudes. Pour se protéger, certains choisissent de boycotter ces plates-formes, mais cette technique à ses limites. En effet, que vous autorisiez ou non vos ados à s'inscrire, ils peuvent quand même exister sur les réseaux sociaux à travers leurs amis qui partagent des photos, des vidéos…

Acceptez donc dès maintenant que Facebook, Twitter, Instagram ou encore Youtube vont faire partie de votre vie. Mais si votre enfant est inscrit à l'un de ses services, il y a de fortes chances qu'il y partage aussi des informations personnelles anodines… ou pas !

C'est pourquoi il est essentiel de définir ensemble les informations qui se partagent et celles qui doivent rester secrètes, quelles photos poster sans risque, mais également apprendre à gérer une multiplicité d'identités.

**LE CONSEIL** : **ces plates-formes disposent toutes d'outils pour supprimer des contenus inappropriés (les vôtres mais aussi ceux postés par d'autres internautes).**

**N'hésitez pas à vous en servir !**

**Partagez en gardant toujours à l'esprit qu'Internet est un espace public.**

## 3/ Faire de votre ordinateur un environnement sécurisé

Les logiciels et fichiers malveillants ont pour but de voler vos informations bancaires, vos mots de passe ou encore vos contacts. Un anti-virus et un pare-feu peuvent vous protéger contre la plupart d'entre eux. Les plus connus, qu'ils soient payants ou gratuits, sont téléchargeables directement sur Internet et s'installent en quelques clics.

N'hésitez pas à également à faire appel à un logiciel de contrôle parental. Ils vous sont souvent proposés par votre fournisseur d'accès, et même si leur fonctionnement n'est pas infaillible, ils filtrent certains contenus inadaptés et permettent de suivre l'activité de vos enfants sur Internet.

**ATTENTION : ces outils sont à mettre à jour régulièrement pour rester efficaces.**

## 4/ Créer des mots de passe sécurisés

Que ce soit "monprénom" ou "123456", de nombreux internautes, enfants comme adultes, utilisent des mots de passe simples à retenir pour eux… mais aussi pour ceux qui souhaiteraient pirater leurs comptes en ligne. Choisir un mot de passe compliqué ne veut pas forcément dire qu'il sera impossible à retenir. Aidez-vos enfants à créer des combinaisons plutôt que des éléments simples (comme par exemple « monprénom+monanimaldecompagnie » ou « monprénom+madatedenaissance) et alternez chiffres, lettres minuscules et lettres majuscules.

**ATTENTION : le mot de passe perd toute son utilité si on le partage avec ses amis.**

## 5/ Apprendre à trier les emails

Les criminels sont doués pour créer des sites web, des emails ou des publicités qui semblent venir d'une source que vous connaissez mais qui sont en réalité des leurres. Apprenez à vos enfants à détecter les indices comme une adresse d'expéditeur inhabituelle (même si le nom de l'expéditeur est connu) ou des cadeaux qui semblent trop beaux pour être vrais (voyages, gadgets informatiques, etc.).

**ATTENTION : en cas de doute, soyez méfiants ! Evitez le plus possible de cliquer sur un lien contenu dans un e-mail.**


RSA
The Security Division of EMC

*Ces données sont tirées d'une étude commanditée par RSA en partenariat avec l'association Internet Sans Crainte et réalisée par l'IFOP en janvier 2013 à l'occasion du Safer Internet Day dans le cadre de la campagne « Internet Les Autres et Moi » centrée sur les usages d'Internet par les jeunes (11 à 17 ans) et leurs parents.
Retrouver l'ensemble des résultats de l'étude et les conseils de RSA sur le site internet d'information dédiée à la campagne : disponible ici

**Qui est RSA ?**

Depuis plus de 25 ans, RSA, la division sécurité d'EMC, protège les ressources numériques des entreprises et œuvre pour un Internet plus sûr partout dans le monde. RSA dispose d'un centre de commande anti-fraude et anti Cybercriminalité qui surveille 24/24 et 7j/7 les menaces venant d'Internet : phishing (hameçonnage), virus, trojans, logiciels espions… Ce centre a déjà contribué au démantèlement de nombreux réseaux mafieux sur internet. Expert dans la lutte contre les menaces qui émergent chaque jour sur Internet, RSA est à l'origine de la campagne pédagogique de sensibilisation au bon usage d'Internet : « Internet, les autres et moi », lancée à l'occasion du Safer Internet Day 2013.

**Contact:**
Hotwire pour RSA
Marion Delmas / Mariana Maal
01 43 12 55 62 / 49
Hotwire.emcfr@hotwirepr.com