OUCH! | Juin 2015

La Newsletter mensuelle de Sensibilisation à la Sécurité destinée aux utilisateurs informatiques

OUCH!

Dans ce numéro...

Eduquer les enfants à la sécurité informatique

Contexte

Pour les enfants d'aujourd'hui, le nombre de façons leur permettant d'accéder à internet et d'interagir avec les autres est effarant. Les nouveaux services de réseaux sociaux apparaissent aussi vite que les mauvaises herbes et il existe un nombre croissant d'applications et de jeux qui se connectent à internet. De plus, beaucoup d'écoles migrent vers des services tels que Google Drive et exigent qu'une partie voire la totalité du travail se fasse via internet et que les devoirs soient soumis en ligne. Les enfants grandissent littéralement «connectés». Alors qu'il existe beaucoup d'avantages à cela, ces opportunités ne sont pas sans risques. Dans cette newsletter, nous explorons trois domaines à risques pour les enfants et ce que vous pouvez faire pour les aider à rester en sécurité.

Editeur invité

Bob Rudis est un scientifique spécialisé dans la sécurité des données à Verizon. Auteur du Rapport 2015 sur la violation des données, il est également l'heureux père de quatre enfants. Bob a construit et mené des campagnes de sensibilisation engageantes et efficaces dans plusieurs sociétés figurant dans le classement du Fortune 100. Vous pouvez suivre Bob sur Twitter sous le pseudo **@hrbrmstr**.

Les risques

1. **Comportement** : Lorsque les enfants interagissent avec les communautés en ligne ou dans des mondes virtuels, ils peuvent adopter des comportements qu'ils n'auraient jamais adoptés dans la vraie vie. L'absence de contact physique peut générer un sentiment d'anonymat puissant, particulièrement chez les enfants. Ils sont souvent tentés de s'exprimer d'une manière qui peut blesser les autres enfants, comportement appelé cyber-intimidation. Aussi, vos enfants peuvent également devenir les victimes des autres qui sont volontairement méchants ou blessants.

2. **Contact** : Les enfants sont pratiquement toujours en communication avec les autres, que ce soit à travers les sms, l'interaction à travers les communautés en ligne ou les jeux dans les mondes virtuels. L'absence de présence physique leur fait souvent oublier que l'individu de «l'autre côté» n'est pas forcément qui il prétend être et n'a pas non plus nécessairement les meilleurs intérêts à cœur. Les prédateurs rôdent dans ces rues numériques et useront de quelque tactique que ce soit pour créer une relation avec leurs victimes potentielles, souvent en se faisant passer eux-mêmes pour des enfants.

3. **Contenu** : Les moyens ne manquent pas pour capturer ou poster une vidéo, un son une image ou un message texte sur internet. La tentation pour les enfants de s'exposer plus que nécessaire ou de partager des informations personnelles sur eux ou sur d'autres membres de leur famille, sans en réaliser les conséquences, est très réelle. Les enfants ne réalisent sans doute pas les dangers du vol d'identité ou les infections par les logiciels malveillants lorsque les autres leur demandent de répondre à des questions précises ou leur demandent de cliquer sur des liens. Enfin, nous sommes à une époque où nous ne pouvons pas «défaire» ce qui a été partagé ou publié en ligne. Les enfants pensent

Eduquer les enfants à la sécurité informatique

que Kik, Instagram, Snapchat et autres publications sont éphémères, mais toutes ces publications peuvent réapparaître et les hanter, eux ou d'autres membres de leur famille, plus tard dans leur vie future.

Eduquer les enfants

La première chose que vous pouvez faire pour protéger vos enfants est de leur parler. Soyez au courant de ce qu'ils font sur internet, éduquez les sur les risques d'aujourd'hui et ce qu'ils doivent savoir pour se protéger.

La clé pour protéger les enfants en ligne est de les éduquer sur les dangers auxquels ils font face et de vous assurer que non seulement vous leur parlez mais qu'ils vous parlent aussi.

1. **La sécurité à la maison** : Même avec une grande mobilité, c'est tout de même à la maison que le comportement de sécurité face à internet s'apprend. Plus vous commencerez à communiquer tôt, dans un sens comme dans l'autre, mieux ce sera. Ayez des conversations régulièrement sur les problèmes de sécurité en ligne, et vous pouvez également aller jusqu'à leur montrer les méfaits par des cas concrets et réels. Si vous ne savez pas ce que font vos enfants, demandez-leur simplement. Jouez au parent ignorant et demandez-leur de vous montrer les dernières technologies et comment ils les utilisent. Les enfants adorent le fait d'enseigner et ils s'ouvriront plus facilement. Par exemple, peut-être sont-ils sur Instagram, demandez-leur de vous montrer comment Instagram fonctionne, demandez-leur de vous créer un compte afin que vous puissiez les suivre. Non seulement vous apprenez et contrôlez ce que font vos enfants, mais en plus vous facilitez grandement le fait qu'ils viennent vous parler. De plus, assurez-vous, dans la mesure du possible, que toute activité en ligne prenne place dans des endroits centraux de la maison et mettez en place des créneaux horaires pour l'activité. En utilisant des ordinateurs dans des endroits centraux de la maison, les enfants sont moins enclins à adopter des comportements dangereux. Aussi, pensez à une station de recharge centrale pour les appareils mobiles, et instaurez une règle selon laquelle tous les appareils mobiles seront laissés à cet endroit lorsque les enfants iront se coucher.

2. **La sécurité avec les autres** : Lorsque les enfants sont en dehors de la maison, ils sont plus exposés. Aidez-les à comprendre que vos «cyber-règles» s'appliquent où qu'ils soient et n'hésitez pas à communiquer vos restrictions à la personne à qui vous faites confiance pour s'occuper de vos enfants. S'ils ont des appareils mobiles, vérifiez les modes d'utilisation (temps et bande passante) pour vous assurer qu'ils ne profitent pas de l'absence de restrictions lorsqu'ils ne sont pas à la maison. Vous ne pourrez pas empêcher toutes les infractions aux règles, mais votre bienveillance reviendra à l'esprit de vos enfants lorsqu'ils navigueront sur leurs appareils mobiles.

3. **La sécurité par le nombre** : Vous n'êtes pas seuls dans cette cyber-surveillance et vous devriez engager d'autres parents, gardiens, frères et sœurs, professeurs et amis pour garder un œil sur les comportements potentiellement dangereux. Essayez de les encourager à se maintenir au niveau des enfants et encouragez-les à interagir de façon positive s'ils constatent que leurs enfants empruntent une voie dangereuse.

Eduquer les enfants à la sécurité informatique

Enfin, lorsque les enfants font des erreurs, envisagez les plutôt comme des expériences desquelles il faut apprendre plutôt que d'entamer directement une action disciplinaire. Expliquez-leur « pourquoi », à chaque fois, et rappelez-leur également que vous essayez simplement de les protéger des dangers dont ils ne sont pas encore conscients. Dites-leur bien qu'ils sont libres de venir vous voir s'ils font l'expérience de quelque chose de désagréable ou inconfortable lors d'une interaction en ligne, encouragez-les même à faire des captures d'écran pour éventuellement vous les montrer. Assurez-vous aussi qu'ils se sentent pleinement en confiance pour venir vous parler lorsqu'ils réalisent qu'ils ont fait quelque chose d'inapproprié. Maintenir une communication ouverte et active dans la vraie vie est le meilleur moyen pour aider les enfants à rester en sécurité dans le monde numérique d'aujourd'hui.

Ressources publiques

N'utilisez jamais les ordinateurs publics, tels que ceux que l'on trouve dans les halls d'hôtels, les librairies ou les cybers cafés. Vous n'avez aucune idée de qui a pu utiliser cet ordinateur avant vous, il se peut que cette personne ait, volontairement ou involontairement, infecté cet ordinateur. Lorsque cela est possible, n'utilisez que des appareils que vous contrôlez et auxquels vous faîtes confiance pour vos activités en ligne. Si vous n'avez d'autre choix que d'utiliser un ordinateur public, n'utilisez aucun service qui vous demande de vous identifier ou d'entrer un mot de passe.

Version Française

La division sécurité de ANSWER S.A. offre des services de Conseil, d'Audit et d'Architecture en sécurité des systèmes d'information. Ces activités sont accompagnées d'une veille active sur les solutions de sécurité du marché permettant ainsi à ses consultants de répondre efficacement aux problématiques de ses clients.
Pour en savoir plus, veuillez vous référer aux liens suivants :
http://www.answersolutions.ch et http://answersecurity.com/

Sources

Cyber Smart : http://www.cybersmart.gov.au/Parents.aspx
OnGuard Online : http://www.onguardonline.gov/topics/protect-kids-online
StaySafeOnline : https://www.staysafeonline.org/stay-safe-online/for-parents/raising-digital-citizens
Securing Kids Panel :
http://www.rsaconference.com/media/into-the-woods-protecting-our-youth-from-the-wolves-of-cyberspace

Comité de rédaction : Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Traduit par : Marilyn Combet