OUCH! | Juillet, 2017

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

OUCH!

Dans ce numéro...

Jouer en ligne de manière sûre et sécurisée

Vue d'ensemble

Le jeu en ligne est un excellent moyen de s'amuser, mais il s'accompagne également de risques particuliers. Dans ce numéro, nous vous indiquons ce que vous pouvez faire pour vous protéger et protéger votre famille lorsque vous jouez en ligne.

Editeur invité

Steve Armstrong est un instructeur certifié SANS et le fondateur de Logically Secure. Il est également l'architecte de CyberCPR, une plateforme de gestion des incidents. Il est actif sur Twitter en tant que **@Nebulator** et travaille avec de nombreuses grandes entreprises de jeux à travers le monde : accomplir ses rêves d'enfants et ses rêves professionnels !

Assurer sa sécurité

Ce qui rend le jeu en ligne tellement accrocheur est le fait de pouvoir jouer et communiquer avec d'autres joueurs partout dans le monde. La plupart du temps, vous ne connaissez même pas les autres joueurs. Et alors que la grande majorité des joueurs en ligne veulent s'amuser, tout comme vous, il n'en demeure pas moins qu'il y a aussi ceux qui veulent nuire. Voici quelques petites choses que vous devriez faire afin de demeurer en sécurité.

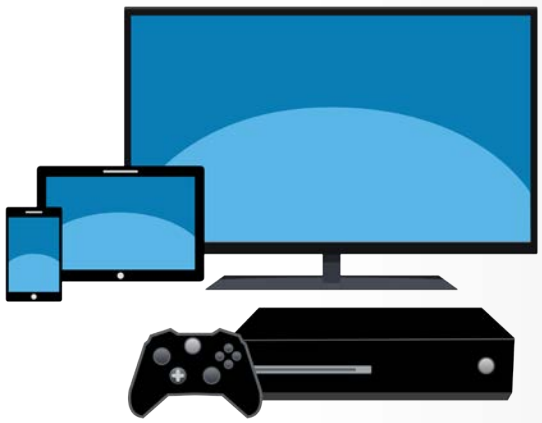
- Méfiez-vous de tout message vous demandant de faire quelque chose, tel que de cliquer sur un lien ou télécharger un dossier. Tout comme le phishing, les criminels vont essayer de vous berner et vous inciter à faire des choses qui infesteront votre ordinateur. Si un message vous semble bizarre, urgent ou trop beau pour être vrai, méfiez-vous qu'il ne s'agisse pas d'une attaque.
- Beaucoup de jeux en ligne ont leurs propres marchés financiers où vous pouvez échanger, troquer ou même acheter des produits virtuels. Tout comme dans la vraie vie, il y a des fraudeurs sur ces systèmes qui essayeront de vous inciter à donner de l'argent ou même essayeront carrément de vous voler. N'achetez que sur les marchés qui jouissent d'une bonne réputation.
- Utilisez une phrase de passe forte pour tous vos comptes de jeux. De cette façon, les attaquants ne peuvent pas simplement deviner vos mots de passe et prendre en charge vos comptes. Si votre jeu offre une vérification en deux étapes, utilisez-la. Par ailleurs, tous vos comptes en ligne doivent avoir un mot de passe différent. De cette façon, si un jeu est compromis, vos autres comptes restent sécurisés. Vous ne pouvez pas vous souvenir de tous vos mots de passe ? Pensez à utiliser un gestionnaire de mot de passe.

Sécuriser votre système

Les criminels peuvent essayer de pirater ou de prendre le contrôle de l'ordinateur sur lequel vous jouez, vous devez prendre des mesures pour le protéger.

Jouer en ligne de manière sûre et sécurisée

- Sécurisez votre ordinateur en utilisant systématiquement la dernière version du système d'exploitation ainsi que celle du logiciel de votre jeu en ligne. Tout comme votre système d'exploitation et les navigateurs web, les logiciels de jeux anciens ou obsolètes possèdent souvent des vulnérabilités connues que les agresseurs pourront exploiter afin de pirater votre ordinateur. En vous assurant de la mise à jour régulière de votre ordinateur et de vos applications de jeux, vous éliminez la plupart de ces vulnérabilités connues.
- Equipez-vous d'un anti-virus, assurez-vous qu'il soit mis à jour et qu'il vérifie tous les dossiers que vous utilisez, en temps réel.
- Ne téléchargez vos logiciels de jeux que sur des sites reconnus. Si vous installez un logiciel de jeu, assurez-vous de le télécharger sur le site du vendeur ou sur un site connu, réputé et auquel vous faites confiance. Très souvent, les criminels vont créer une fausse version ou une version infectée d'un jeu qu'ils distribueront via leur propre serveur. Si vous installez une de ces versions, les criminels auront tout pouvoir sur votre ordinateur.



La clé pour jouer en ligne en toute sécurité est d'utiliser des mots de passe forts, sécuriser votre ordinateur et utiliser le bon sens lorsque vous recevez des messages ou des requêtes étranges.

- Les extensions de jeux, souvent développées par la communauté, sont fréquemment utilisées pour ajouter de nouveaux modules. Les criminels infectent parfois ces extensions avec des logiciels malveillants que les antivirus peuvent avoir du mal à détecter. De la même manière que vous téléchargez vos jeux, assurez-vous aussi de télécharger les extensions sur des sites de confiance. De plus, si une extension requiert la désactivation de votre anti-virus, ou vous oblige à changer vos firewalls, ne l'utilisez pas.
- Les marchés noirs sont apparus pour soutenir les activités frauduleuses. Au-delà du fait qu'ils soient immoraux, beaucoup de programmes frauduleux sont eux-mêmes des rootkits, sans conteste le plus dangereux des logiciels malveillants. N'installez et n'utilisez jamais de logiciels frauduleux.
- Vérifiez le site web du logiciel de jeu en ligne que vous utilisez. Beaucoup de sites de jeux en ligne possèdent une section dans laquelle ils vous expliquent comment assurer votre sécurité et celle de votre système, suivez leurs conseils.
- Enfin, soyez aussi prudent en jouant sur vos appareils mobiles que vous l'êtes sur votre ordinateur. Les cybers criminels commencent de plus en plus à s'attaquer aux appareils mobiles.

Pour les parents ou tuteurs

Les enfants ont besoin d'une protection et d'une éducation supplémentaires lorsqu'ils jouent en ligne. L'éducation et un dialogue ouvert avec vos enfants est la meilleure des stratégies pour les protéger. Une des astuces pour faire parler votre enfant est de lui demander de vous expliquer le fonctionnement de son jeu, demandez-lui de vous faire une démonstration

Jouer en ligne de manière sûre et sécurisée

et de vous décrire ce qu'est une partie de jeu type. Vous pouvez même jouer avec lui. Aussi, demandez-lui de vous décrire les différentes personnes qu'il rencontre en ligne. Très souvent, le jeu en ligne peut être une grande part de la vie sociale de votre enfant. En lui parlant (et en l'incitant à vous parler), vous pouvez détecter un problème et le protéger de manière beaucoup plus efficace que n'importe quelle technologie.

- Connaitre les jeux auxquels ils jouent et assurez-vous que ces jeux soient bien adaptés à son âge.
- Limitez la quantité d'informations que vos enfants partagent en ligne. Par exemple, ils ne devraient jamais partager leur mot de passe, leur âge, leur numéro de téléphone ou leur adresse personnelle.
- Envisagez d'avoir leur ordinateur de jeu dans une zone ouverte où vous pouvez les surveiller. En outre, les enfants plus jeunes ne devraient pas jouer dans leur chambre ou tard dans la nuit.
- L'intimidation, le langage grossier ou d'autres comportements antisociaux peuvent poser problème. Gardez un œil sur vos enfants, s'ils semblent bouleversés après avoir joué à un jeu, ils peuvent avoir été agressés en ligne. S'ils sont intimidés en ligne, faites-leur cesser de jouer au jeu et faites-les jouer dans des environnements plus adaptés aux enfants, ou faites-les jouer à des jeux en ligne avec seulement des amis de confiance.
- Découvrez si les jeux de votre enfant prennent en charge les achats dans l'application et renseignez-vous sur les types de contrôles parentaux qu'ils fournissent.

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.answer.ch et http://answersecurity.com/

Sources

Sécuriser votre réseau domestique :	https://securingthehuman.sans.org/ouch/2016#february2016
Ingénierie sociale :	https://securingthehuman.sans.org/ouch/2017#january2017
Phrases de passe :	https://securingthehuman.sans.org/ouch/2017#april2017
Gestionnaires de mots de passe :	https://securingthehuman.sans.org/ouch/2015#october2015
Vérification en deux étapes :	https://securingthehuman.sans.org/ouch/2015#september2015

Comité de rédaction : Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Traduit par : Marilyn Combet