OUCH! | Mars, 2015

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

Jouer en ligne est une super façon de s'amuser, toutefois cela s'accompagne 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.

Rédacteur Invité

Jake Williams est le fondateur et le consultant principal chez Rendition Infosec, un instructeur certifié SANS et également co-auteur de plusieurs cours SANS. Il est présent sur twitter sous le pseudo **@MalwareJake** et il tient un blog : **malwarejake.blogspot.com**.

Assurer votre sécurité

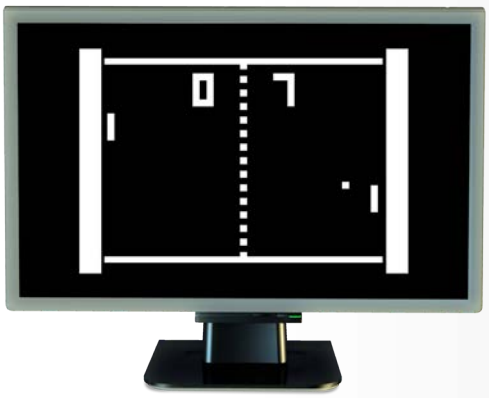
Ce qui rend le jeu en ligne tellement accrocheur est le fait que vous puissiez jouer et communiquer avec d'autres joueurs partout dans le monde. La plupart du temps, vous ne connaissez même pas les autres joueurs. Et alors que la grande majorité des joueurs en ligne veulent s'amuser, tout comme vous, 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 délinquants 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.
- Faites attention lors de vos transactions lorsque de l'argent réel est engagé pour effectuer des achats sur les jeux en ligne, et vice versa. N'achetez que sur les marchés réputés et qui jouissent d'une bonne réputation.
- Limiter les informations que vous ou vos enfants partagez en ligne. Ne partagez jamais d'informations personnelles telles que vos mots de passe ou adresse personnelle.
- Beaucoup de sites, tels que les banques en ligne, utilisent des questions de sécurité afin de confirmer votre identité. Les délinquants ont la réputation de pouvoir obtenir la réponse à ces questions de sécurité en devenant ami avec leurs victimes lors de jeux en ligne. Souvenez-vous que vous n'êtes en aucun cas tenus de répondre aux questions que les gens vous posent lorsque vous jouez en ligne.

Assurer la sécurité de votre ordinateur / vos comptes

L'étape suivante consiste à sécuriser l'ordinateur sur lequel vous jouez. Les délinquants vont essayer de prendre la main sur votre ordinateur ou sur vos comptes de jeux, vous devez les protéger.

Jouer en ligne de manière sûre et sécurisée



La clé pour rester sécurisé tout en jouant en ligne est d'utiliser des mots de passe forts, de sécuriser votre ordinateur et d'utiliser votre bon sens quand vous parlez à des inconnus ou lorsque vous recevez des messages ou des demandes en ligne.

- Utiliser un mot de passe fort aussi bien pour votre ordinateur que pour vos comptes de jeux en ligne. De cette manière, les agresseurs ne pourront pas simplement deviner votre mot de passe et prendre la main sur vos comptes. Si votre jeu vous propose une identification en deux temps, acceptez-la. De plus, assurez-vous que chacun de vos comptes de jeux en ligne possède un mot de passe différent. Ainsi, si l'un de vos jeux est compromis, les autres demeurent sécurisés.
- Sécurisez votre ordinateur en utilisant systématiquement la dernière version du système d'exploitation ainsi celle du logiciel de jeu en ligne. Tout comme votre système d'exploitation et les navigateurs web, les logiciels de jeux anciens ou périmés 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, auquel vous faites confiance et réputé. Très souvent, les agresseurs 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 agresseurs auront tout pouvoir sur votre ordinateur.
- Les extensions de jeux, souvent développées par la communauté, sont fréquemment utilisées pour ajouter de nouveaux modules. Les agresseurs infectent parfois ces extensions avec des logiciels malveillants que les anti-virus 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-agresseurs commencent de plus en plus à s'attaquer aux appareils mobiles.

Jouer en ligne de manière sûre et sécurisée

Pour les parents

Si vous êtes parents, assurez-vous que vos enfants suivent point par point les recommandations mentionnées ci-dessus (pour les plus jeunes, vous devrez peut-être le faire pour eux). De plus, parlez des risques à vos enfants. 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 et 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.

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/

Ressources

Ingénierie sociale :	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201411_fr.pdf
Attaques par phishing :	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201302_fr.pdf
Gestionnaires de mots de passe :	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201310_fr.pdf
Qu'est-ce qu'un anti-.virus ? :	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201412_fr.pdf
Rester sécurisé en ligne :	https://www.staysafeonline.org/stay-safe-online/for-parents/gaming-tips

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