OUCH! Juin 2022

Votre bulletin mensuel sur la sensibilisation à la sécurité

Jouer en ligne en toute sécurité

Ce qui rend les jeux en ligne si amusants, c'est que vous pouvez jouer et interagir avec d'autres personnes de n'importe où dans le monde, et souvent vous ne connaissez même pas les personnes avec lesquelles vous jouez. Si la grande majorité des personnes en ligne cherchent à s'amuser comme vous, il y en a d'autres qui veulent vous nuire.

Sécuriser vos données

Le plus grand risque des jeux en ligne n'est pas la technologie elle-même, mais les interactions que vous avez avec des inconnus.

- Méfiez-vous de tout message qui vous demande d'effectuer une action, comme cliquer sur un lien ou télécharger un fichier. Les attaquants utiliseront des messages dans le jeu ou des e-mails d'hameçonnage pour tenter de vous inciter à entreprendre des actions susceptibles d'infecter votre ordinateur, de voler votre identité ou vos comptes de jeu. Si un message vous semble étrange, urgent ou trop beau pour être vrai, méfiez-vous, il peut s'agir d'une attaque.
- De nombreux jeux en ligne ont leurs propres marchés financiers où vous pouvez échanger, troquer ou acheter des biens virtuels. Tout comme dans le monde réel, il existe des fraudeurs qui tenteront de vous tromper et de vous voler votre argent ou toute monnaie virtuelle que vous possédez. Ne parlez qu'avec des personnes dont la réputation est établie et fiable.
- Utilisez une phrase secrète forte et unique pour tous les comptes de jeu. De cette façon, les attaquants ne peuvent pas deviner vos mots de passe et prendre le contrôle de vos comptes. Si votre jeu/plateforme propose une vérification en deux étapes, utilisez-la. Vous ne pouvez pas vous souvenir de tous ces mots de passe? Utilisez un gestionnaire de mots de passe.

Sécurisez votre système

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

- Sécurisez vos appareils en utilisant toujours la dernière version du système d'exploitation et du logiciel de jeu ou de l'application mobile. Les logiciels obsolètes présentent des vulnérabilités connues que les attaquants peuvent exploiter et utiliser pour pirater votre appareil. Activez la mise à jour automatique lorsque cela est possible. En maintenant vos appareils et vos applications de jeu à jour, vous éliminez la plupart de ces vulnérabilités connues.

- Ne téléchargez des logiciels de jeu et des packs d'extension de jeux que sur des sites Web fiables. Les attaquants créent souvent des versions falsifiées ou infectées, puis les distribuent à partir de leur propre serveur. En outre, si un jeu ou un module complémentaire vous oblige à désactiver des outils ou des paramètres de sécurité, ne l'utilisez pas.
- Des marchés clandestins sont apparus pour soutenir l'activité de triche. En plus d'être contraires à l'éthique, de nombreux programmes de triche sont eux-mêmes des logiciels malveillants qui infecteront votre appareil. N'installez et n'utilisez jamais aucun type de logiciel ou site web de triche.
- Consultez le site Web du logiciel de jeu en ligne que vous utilisez. De nombreux sites de jeux ont une section sur la façon de se protéger et de protéger votre système.

Pour les parents ou les tuteurs

L'éducation et un dialogue ouvert avec vos enfants sont les mesures les plus efficaces que vous pouvez prendre pour protéger les enfants. Une première approche consiste à leur demander de vous montrer comment leurs jeux fonctionnent, de vous montrer à quoi ressemble un jeu typique. Vous pouvez peut-être même jouer au jeu avec eux. En outre, demandez-leur de vous parler des différentes personnes qu'ils rencontrent en ligne. Bien souvent, les jeux en ligne peuvent constituer une partie importante de la vie sociale de votre enfant. En leur parlant (et en faisant en sorte qu'ils vous parlent), vous pouvez détecter un problème et les protéger bien plus efficacement que n'importe quelle technologie. Voici quelques étapes supplémentaires:

- Informez-vous sur les jeux auxquels ils jouent et assurez-vous que ces jeux sont adaptés à l'âge de votre enfant.
- Limitez la quantité d'informations que vos enfants partagent en ligne. Par exemple, ils ne doivent jamais communiquer leur mot de passe, leur âge, leur numéro de téléphone ou leur adresse personnelle.
- Envisagez de placer leur appareil de jeu dans un endroit ouvert où vous pouvez garder un œil sur eux. De plus, les jeunes enfants ne doivent pas jouer dans leur chambre ou tard dans la nuit.
- L'intimidation, le langage grossier ou d'autres comportements antisociaux peuvent constituer un problème. Gardez un œil sur vos enfants, s'ils semblent contrariés après avoir joué à un jeu, ils ont peut-être été victimes d'intimidation en ligne. S'ils sont victimes d'intimidation en ligne, signalez-le au site de jeu et demandez-leur de jouer à des jeux en ligne uniquement avec des amis de confiance.
- Découvrez si les jeux de votre enfant prennent en charge les achats sur l'application et quels types de dérogations parentales ils offrent.

Rédacteur Invité

Charlie Goldner est le fondateur de CyberNV et un instructeur chez SANS. Il est actif sur LinkedIn et travaille en soutien aux agences gouvernementales. Il a passé de nombreuses heures à jouer sur PC et consoles au fil des ans.

Ressources

Ingénierie sociale: https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering
Une étape simple pour sécuriser vos comptes:
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blta467eb5cefbb8b36/6137f535876fcf3cb80c3438/ouch!_september_2021_one_simple_step_to_securing_your_accounts_French.pdf
Gestionnaires de mots de passe:
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt2daeb46008f7661a/604a694ba8c6585cda24db20/202004-OUCH-French.pdf
La sécurité en ligne pour les enfants: https://www.sans.org/newsletters/ouch/online-security-kids/

Traduit pour la communauté par: Juliette Busson