ProtÃ©ger sa ligne, 5 conseils pratiques pour les Gamers.
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 17/10/2013 11:30:00

Lâ□□industrie du jeu vidÃ©o, comme beaucoup dâ□□autres, a rÃ©cemment Ã©tÃ© la cibleÂ de groupes de cybercriminels. Dans cette bataille, les utilisateurs seÂ retrouvent parfois dÃ©lestÃ©s de leurs donnÃ©es les plus personnelles.

Selon Kaspersky Lab, les Gamers franÃ§ais sont victimes de prÃ¨s de 30000 attaques par an. Pour limiter les risques, Kaspersky propose 5 conseils faciles et surtout rapides Ã mettre en place.

1. Attention aux liens douteux

De nombreux jeux multijoueurs disposent de leur propre serveur de messagerie et fonctionnent uniquement sâ□□ils sont connectÃ©s Ã Internet. Le nombre de joueurs et le volume dâ□□informations disponibles peuvent reprÃ©senter une aubaine pour les pirates informatiques Ã la recherche de victimes peu mÃ©fiantes. Pour Ã©viter les risques, il est prÃ©fÃ©rable de ne pas cliquer sur les liens et de ne pas ouvrir les piÃ¨ces jointes envoyÃ©es par un utilisateur non identifiÃ©. De mÃªme, il est plus prudent de ne pas tÃ©lÃ©charger un nouveau logiciel avant dâ□□avoir vÃ©rifiÃ© sa lÃ©gitimitÃ©, afin dâ□□Ã©viter quâ□□il endommage potentiellement le matÃ©riel informatique. En effet, dâ□□aprÃ¨s le rapport trimestriel global de Kaspersky Lab Ã paraÃ®tre en novembre, les produits Kaspersky Lab ont dÃ©tectÃ© en France prÃ¨s de 11 millions dâ□□incidents sur Internet entre aoÃ»t et septembre 2013, gÃ©nÃ©rÃ©s par des malwares.

2. Patchs et mises Ã jour

Il est impÃ©ratif de ne pas oublier de mettre Ã jour le systÃ¨me de son ordinateur, Smartphone ou tablette, au risque de voir les risques dâ□□infection par un virus ou un malware dÃ©multipliÃ©s. Pour les Ã©viter, une seule solution : chaque fois quâ□□une mise Ã jour logicielle est disponible, il faut lâ□□installer !

3. Utiliser des mots de passe forts

Un mot de passe doit Ãªtre sÃ©curisÃ©â□¦ et multiple ! Il est essentiel dâ□□utiliser une variÃ©tÃ© de mots de passe uniques compliquÃ©s pour chaque site sur lequel un profil est crÃ©Ã©. Si la sÃ©curitÃ© dâ□□une plate-forme de jeux venait Ã Ãªtre compromise, comme cela a pu arriver, un mot de passe fort pourrait bien Ãªtre le seul rempart entre les pirates et les donnÃ©es personnelles des utilisateurs (informations bancaires, vols dâ□□avatars, etc.) disponibles sur dâ□□autres sites Web.

4. Eviter les bornes Wi-Fi publiques

Il est tentant dâ□□Ãªtre connectÃ© en permanence Ã son jeu vidÃ©o prÃ©fÃ©rÃ©, depuis chez soi bien sÃ»r, mais aussi Ã lâ□□aÃ©roport ou encore Ã lâ□□hÃ´tel. Cependant, les connexions Wi-Fi gratuites proposÃ©es dans les lieux publics sont le plus souvent configurÃ©es de faÃ§on Ã ce que tout le monde puisse se connecter, ce qui implique de rÃ©duire le niveau de sÃ©curitÃ© au minimum. En consÃ©quence, les cybercriminels intÃ©ressÃ©s par les donnÃ©es personnelles des internautes nâ□□ont plus quâ□□Ã imaginer des attaques pour intercepter les donnÃ©es qui circulent, non cryptÃ©es pour la plupart. Pour les joueurs en ligne, le risque est encore plus grand. AccaparÃ© par le jeu, il est facile dâ□□oublier que dâ□□autres applications ou sites Internet sont ouverts et diffusent des informations personnelles. La prudence est donc de mise pour Ã©viter les surprises Ã la fin de la partie.

5. Mieux vaut prÃ©venir que guÃ©rir

Les Smartphones, ordinateurs et tablettes utilisÃ©s pour jouer doivent Ãªtre Ã©quipÃ©s des outils qui pourront les protÃ©ger, comme par exemple un antivirus ou un anti-malware. Lorsquâ□□il sâ□□agit de conserver ses donnÃ©es personnelles, il est prÃ©fÃ©rable dâ□□adopter la rÃ¨gle dâ□□or Â« mieux vaut prÃ©venir que guÃ©rir Â».