BitDefender : Les conseils de sÃ©curitÃ© de BitDefender pour la Saint-Valentin
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 10/2/2010 0:00:00

Laissez quelquâ□□un de spÃ©cial sâ□□emparer de votre cÅ□ur, pas de votre identitÃ© .
BitDefenderÂ®, Ã©diteur de solutions de sÃ©curitÃ© antimalwares, met en garde aujourdâ□□hui les adeptes des sites de rencontres en ligne contre le risque accru que constitue la recherche de lâ□□Ã¢me sÅ□ur sur Internet et leur vulnÃ©rabilitÃ© potentielle face Ã lâ□□usurpation dâ□□identitÃ© et aux arnaques en ligne.

Sâ□□il est vrai quâ□□il existe de nombreux services de rencontres en ligne fiables et sÃ©rieux, il est conseillÃ© aux utilisateurs de faire preuve de la plus grande vigilance lorsquâ□□ils choisissent le site correspondant le mieux Ã leurs attentes. Avant de vous inscrire, recherchez des tÃ©moignages positifs et des avis sur le site Internet, ainsi que les conseils dâ□□une personne de confiance ayant dÃ©jÃ utilisÃ© ce service.

BitDefender met Ã©galement en garde contre le danger de souscrire Ã un service de rencontres proposÃ© via du spam, qui peut entraÃ®ner vol dâ□□identitÃ© ou la rÃ©ception de courrier indÃ©sirable supplÃ©mentaire.

Â« *Rencontrer la personne idÃ©ale le jour de la Saint Valentin grÃ¢ce Ã un service de rencontres en ligne est un conte de fÃ©es qui peut vite tourner au cauchemar* Â» dÃ©clare **Catalin Cosoi**, spÃ©cialiste antispam BitDefender. Â« *Pour Ã©viter dâ□□Ãªtre victimes de dÃ©lits informatiques, il est recommandÃ© dâ□□utiliser uniquement les sites ayant des politiques de confidentialitÃ© claires, garantissant lâ□□anonymat et la confidentialitÃ© des informations transmises.* Â»

Lorsque vous commencez Ã utiliser un service de rencontres en ligne, indiquez aussi peu dâ□□informations personnelles que possible et employez un pseudonyme Ã la place de votre

vÃ©ritable nom. CrÃ©ez et utilisez si vous le pouvez un nouveau compte e-mail, afin de prÃ©server la sÃ©curitÃ© de votre compte personnel et de vos informations professionnelles. Les utilisateurs ne devraient jamais rÃ©vÃ©ler dâ□□informations sensibles telles que leurs adresses personnelles, professionnelles, leurs numÃ©ros de tÃ©lÃ©phone, etc.

Â« *MÃªme les informations les plus insignifiantes, comme le nom de jeune fille de votre mÃ¨re ou celui de votre premier animal de compagnie, peuvent Ãªtre exploitÃ©es par des cybercriminels. Bien que ces informations semblent anodines, elles peuvent servir Ã obtenir le mot de passe dâ□□une adresse e-mail ou dâ□□un compte bancaire en ligne. Nâ□□indiquez jamais de donnÃ©es bancaires telles que des numÃ©ros de comptes bancaires, de cartes de crÃ©dit, ou leur code confidentiel* Â» ajoute **Catalin Cosoi.**

Dâ□□autres e-menaces liÃ©es Ã la Saint-Valentin peuvent Ã©galement comprendre :

â□¢ DiffÃ©rents types de spam diffusÃ©s via des rÃ©seaux sociaux, et dirigeant vers des sites web malveillants diffusant chevaux de Troie, faux logiciels antivirus (rogue), keyloggers et autres malware.

â□¢ E-mails de spam exploitant la Saint-Valentin pour promouvoir des biens et des services.

â□¢ PiÃ¨ces jointes tentant dâ□□installer diffÃ©rents malwares sous lâ□□innocente apparence dâ□□un petit film amusant (dont la lecture requiert un codec spÃ©cial), dâ□□un diaporama ou dâ□□une e-carte.

BitDefender propose les conseils suivants pour garantir la sÃ©curitÃ© de votre ordinateur et de vos donnÃ©es personnelles :

â□¢ Nâ□□ouvrez aucun e-mail provenant dâ□□une source inconnue. De nombreux virus se diffusent via des e-mails. En cas de doute, demandez toujours une confirmation Ã lâ□□expÃ©diteur.

â□¢ Nâ□□ouvrez pas immÃ©diatement les piÃ¨ces jointes des e-mails dont lâ□□objet est suspect. Enregistrez-les plutÃ´t sur votre disque dur et analysez-les avec un programme antivirus Ã jour.

â□¢ Supprimez toutes les chaÃ®nes dâ□□e-mails et messages indÃ©sirables. Ne les transfÃ©rez pas et ne rÃ©pondez pas Ã leurs expÃ©diteurs. Ces messages sont considÃ©rÃ©s comme du spam et peuvent surcharger le trafic Web.

â□¢ Mettez Ã jour votre systÃ¨me et vos applications le plus souvent possible. Certains systÃ¨mes dâ□□exploitation et certaines applications peuvent Ãªtre configurÃ©s pour Ãªtre mis Ã jour automatiquement. Nâ□□hÃ©sitez pas Ã utiliser cette fonctionnalitÃ©. Un systÃ¨me qui nâ□□est pas Ã jour est souvent vulnÃ©rable aux menaces.

â□¢ Ne copiez aucun fichier provenant dâ□□une source inconnue ou non fiable. VÃ©rifiez la provenance des fichiers que vous tÃ©lÃ©chargez et assurez-vous quâ□□ils ont Ã©tÃ© analysÃ©s par un programme antimalware.

â□¢ Utilisez une solution de sÃ©curitÃ© intÃ©grÃ©e avec un module antimalware, antispam et un pare-feu, ainsi que des fonctionnalitÃ©s avancÃ©es comme le filtrage web et la protection contre le vol dâ□□identitÃ©.