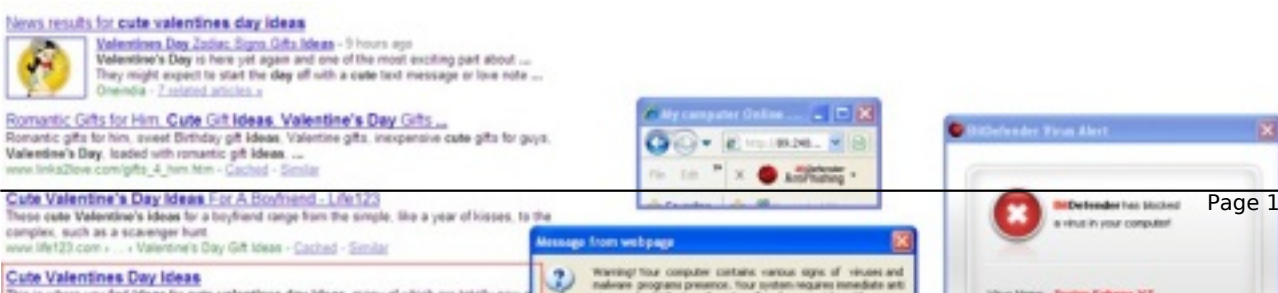


Publié le : 12/2/2010 0:00:00



À chaque « analyse », le nombre d'infections détectées augmente, afin de convaincre les utilisateurs de la nécessité d'enregistrer le faux programme antivirus. Une fois installé, il modifie le contenu de plusieurs fichiers système et déclenche l'affichage de nombreuses fenêtres pop-up avertissant de problèmes système et d'infections imaginaires. Il demande aussi constamment à l'utilisateur d'acheter ou de renouveler une licence.

[Vous pouvez voir ici les actions de ce](#) « joli cadeau »

Afin de protéger vos systèmes et données pour éviter de les compromettre, veuillez suivre les cinq conseils ci-dessous :

• Installez et activez une solution pare-feu et antimalware fiable ainsi qu'un filtre antispam, comme celles proposées par BitDefender.

• Mettez à jour votre antimalware, votre pare-feu et votre filtre antispam aussi souvent que possible avec les dernières définitions de virus et signatures de fichiers et d'applications suspectes.

• Analysez votre système fréquemment

• Vérifiez régulièrement votre système d'exploitation : téléchargez et installez les dernières mises à jour de sécurité et les outils permettant de supprimer des malwares, ainsi que les autres patches et fixes disponibles.

• Ne téléchargez pas et n'enregistrez pas de fichiers provenant de sources inconnues ; même s'ils proviennent d'une source fiable, évitez d'ouvrir et de copier des fichiers sur votre système sans avoir lancé auparavant une analyse antimalware complète.