Réinstallation après infection par malware Windows 7

Votre PC est infecté par un malware et vous ne savez pas comment réinstaller votre système ? Les instructions suivantes vous aideront, étape par étape, à restaurer votre PC et à réduire au minimum les risques d'une nouvelle infection.

Nous nous sommes efforcés de rédiger des instructions les plus universelles possibles, à l'attention des particuliers. Bien entendu, toutes les mesures peuvent ne pas s'appliquer à certains cas particuliers.

Les instructions font référence à Windows 7 Professionnel 32-Bit, mais restent valables également pour les versions à 64 Bit.

Pour réinstaller votre système correctement, conformément à cette fiche d'instructions, vous devez être en possession du CD d'installation Windows 7 et d'un support de stockage externe pour la sauvegarde de vos données.

Étape n°1 : déconnecter le PC du réseau

- Si votre PC est connecté au réseau à l'aide d'un câble, il suffit de retirer la fiche de ce dernier du port correspondant sur votre ordinateur.
- Si vous utilisez un réseau sans fil (WLAN), il convient de désactiver la carte réseau de votre ordinateur à partir du gestionnaire de périphériques (cliquer sur Démarrer → cliquer avec le bouton droit sur *Ordinateur* → Cliquer sur *Propriétés* → Cliquer sur *Gestionnaire de périphériques*).

Étape n°2 : sauvegarder les données personnelles

- Connectez un support de données externe en maintenant la touche « Maj » enfoncée et sauvegardez vos données personnelles. Pour cela, n'utilisez pas votre support de stockage habituel et préférez, si possible, un support de données neuf et entièrement vide.

  INDICATION : si un logiciel malveillant a infecté votre PC, celui-ci pourrait avoir également contaminé votre support externe ainsi que les données qui y sont stockées. La fonction Autorun est souvent utilisée par les malwares pour contaminer les supports de stockage externes (clés USB, etc.). Il est relativement simple de désactiver temporairement cette fonction. Pour cela, appuyez sur la touche « Maj » de votre clavier, maintenez-la enfoncée pendant que vous connectez votre support externe à votre ordinateur et ne la relâchez que quelques secondes après. Dans ce cas, la touche « Maj » empêche Windows d'exécuter automatiquement des programmes et des données présents sur le support.

Étape n°3 : réparer le secteur de démarrage principal (Master Boot Record - MBR)

Certains virus informatiques se nichent dans ce que l'on appelle le secteur de démarrage principal de l'ordinateur. Celui-ci doit donc être entièrement écrasé pour être réparé. Pour cela, utilisez l'utilitaire « Bootrec.exe » disponible dans l'environnement de restauration de Windows.

- Insérez le CD d'installation de Windows 7 dans le lecteur et redémarrez votre ordinateur.
- Si, après le redémarrage, l'ordinateur ne démarre pas avec le CD, définissez le lecteur CD comme étant le premier périphérique dans le système BIOS (cf. Manuel Carte-mère). En alternative, appuyez sur la touche « F8 » juste après le redémarrage de l'ordinateur. Vous serez ainsi dirigé vers le gestionnaire de démarrage qui vous permettra de choisir le lecteur CD.
- Le système vous demandera d'appuyer sur une touche.
- Après avoir défini la langue, l'heure, la devise, le clavier ou la méthode de saisie, cliquez sur *Suivant*.

- Cliquez sur *Réparer votre ordinateur*.
- Cliquez sur le système d'exploitation que vous souhaitez réparer puis sur *Suivant*.
- Dans la boîte de dialogue Options de récupération système, cliquez sur *Invite de commande*.
- Tapez « `bootrec.exe /fixmbr` » puis appuyez sur *Entrée*. Le secteur de démarrage principal est ainsi réparé (et libéré de tout malware).
- Fermer la fenêtre d'invite de commande et arrêtez votre PC en cliquant sur *Arrêter*. Laissez le CD d'installation de Windows 7 dans le lecteur de l'ordinateur.

Étape n°4 : réinstaller Windows 7

- Redémarrez votre ordinateur.
- Si, après le redémarrage, l'ordinateur ne démarre pas avec le CD, définissez le lecteur CD comme étant le premier périphérique dans le système BIOS (cf. Manuel Carte-mère). En alternative, appuyez sur la touche « F8 » juste après le redémarrage de l'ordinateur. Vous serez ainsi dirigé vers le gestionnaire de démarrage qui vous permettra de choisir le lecteur CD.
- Le système vous demandera d'appuyer sur une touche.
- Après avoir défini la langue, l'heure, la devise, le clavier ou la méthode de saisie, cliquez sur *Suivant*.
- Vous devez maintenant cliquer sur *Installer maintenant*.
- Indiquez ensuite les options de gestion des disques. À partir de là, vous avez la possibilité de supprimer, gérer ou formater les partitions.

  ATTENTION : lorsque vous supprimez ou formatez une partition, vous perdez toutes les données stockées sur la partition !

  INDICATION : pour vous assurer qu'il n'y a plus aucun logiciel malveillant sur votre ordinateur, il est nécessaire de supprimer les partitions existantes et d'en créer de nouvelles. Il convient ensuite de formater les nouvelles partitions crées. Notez également qu'une partition de restauration peut éventuellement être prévue par le fabricant. Celle-ci ne doit être ni supprimée ni formatée.
- Terminez l'installation de Windows 7 en définissant les réglages recommandés.
- Connectez votre ordinateur à Internet (brancher le câble).
- Faites la mise-à-jour du système d'exploitation à l'aide de Windows Update (cliquer sur *Démarrer* → *Panneau de configuration* → *Windows Update*).

Étape n°5 : installer un programme antivirus

- Installer un programme de protection antivirus provenant d'une source fiable et faites la mise-à-jour du programme à l'aide de la fonction Update.

  INDICATION : vous trouverez une liste de programmes antivirus à la page suivante www.ebas.ch/5steps_step2.

Étape n°6 : installer et mettre à jour les programmes

- Installez les programmes souhaités. Faites la mise-à-jour de tous les programmes et activez, lorsque c'est possible, la fonction de mise-à-jour automatique.

  INDICATION : prenez garde à ce que les programmes que vous installez proviennent de sources fiables (ex. : site de téléchargement du fabricant ou archive de logiciels tels que PCtipp, Heise, etc.).

Étape n°7 : analyser les données

- Maintenez la touche « Maj » enfoncée et connectez le support de données utilisé précédemment pour sauvegarder vos données personnelles.

  INDICATION : si un malware a été copié sur le support de données pendant le processus de sauvegarde, le PC risque d'être de nouveau infecté ! Pour éviter un tel scénario, il est nécessaire de maintenir enfoncée la touche « Maj » pendant la connexion du support de données à l'ordinateur (cf. Indication de l'étape 2).

- Analyser l'ensemble du système ainsi que le support externe à l'aide du logiciel antivirus installé précédemment. Si des fichiers infectés sont présents, il est nécessaire de les réparer ou de les supprimer !

  INDICATION : pour analyser le nouveau système, l'autre solution, meilleure mais plus lourde, est de vérifier le support de données externe à l'aide d'un live-cd bootable ou d'un autre système d'exploitation (ex. Linux ou macOS).

Étape n°8 : restaurer les données

- Copiez sur le PC les données que vous sauvegardées précédemment sur le support externe.

Étape n°9 : ce qu'il vous reste à faire !

- Sachant que les malwares espionnent très souvent les noms d'utilisateurs et les mots de passe, il est nécessaire de modifier les mots de passe du système ainsi que les mots de passe utilisés sur Internet (ex. sessions d'e-banking, boîte de messagerie électronique, Facebook etc.).
- Il convient par ailleurs de bien vérifier vos extraits de compte et les débits de vos cartes de crédit.

Ces instructions ont été rédigées par «eBanking – en toute sécurité!», en collaboration avec SWITCH.

eBanking en toute sécurité!

Le site Web **www.ebankingentoutesecurite.ch** vous informe gratuitement sur les mesures nécessaires à mettre en œuvre et les règles de comportement à adopter pour une utilisation sécurisée des applications d'e-banking.

SWITCH

SWITCH fournit des services Internet innovants et pratiques aux Hautes Écoles suisses et aux internautes.