

8

Attention aux risques
liés à l'utilisation
des logiciels piratés.



Le piratage de logiciels est une affaire sérieuse, en plus d'enfreindre la loi et les droits de propriété intellectuelle des créateurs de logiciels, vous pouvez mettre votre PC à risque de dommages et de menaces de sécurité.

Il existe plusieurs méthodes pour obtenir et utiliser des logiciels contrefaits. Ceux couramment utilisés sont : l'obtention et l'utilisation de « clés contrefaites de produit », l'obtention de programmes « Générateur de clé » et les utiliser pour créer des clés de produits, et l'obtention des « outils de craque » et de les utiliser pour contourner les mécanismes d'attribution et d'activation de licences.

Qu'est-ce que le piratage logiciel ?

Le piratage logiciel est l'utilisation, la copie ou la distribution non autorisée d'un logiciel soumis à des droits d'auteur. Il peut prendre différentes formes :

- **Copie illicite de logiciels achetés en toute légitimité (piratage par l'utilisateur final) ;**
- **Accès illégal à un logiciel protégé (craquage) ;**
- **Reproduction et/ou distribution de contrefaçons ou de logiciels non autorisés (généralement par Internet).**

Les logiciels font partie des œuvres protégées par le code de la propriété intellectuelle. Dans ce qui suit, nous allons focaliser sur les risques techniques liés à l'utilisation des logiciels piratés.

Risques techniques d'utilisation des logiciels piratés :

1. Les logiciels piratés peuvent provoquer une panne de votre système. Ils entraînent une perte de temps. Vous pouvez perdre des données ou des fichiers irremplaçables.
2. Lorsque vous utilisez la copie illicite d'un logiciel, vous ne pouvez pas bénéficier des mises à jour du produit. Or, les mises à jour sont indispensables pour assurer la sécurité des logiciels : chaque année, les éditeurs publient des dizaines de « correctifs sécurité » ou des « patches » améliorant le fonctionnement de leurs logiciels. Si, cependant, vous utilisez des logiciels contrefaits, vous ne pourrez pas incorporer ces correctifs et serez vulnérable face à d'éventuelles attaques.
3. Les logiciels piratés sont souvent incomplets et manquent de documentation. De plus, certains logiciels téléchargeables sur Internet sont en fait des versions bêta (de test) qui ne comportent pas toutes les fonctionnalités. Les pièces manquantes peuvent être parfois fatales : les versions bêta étant destinées à l'essai, rien ne garantit qu'elles ne mettent pas en péril le bon fonctionnement de votre ordinateur.

4. Les logiciels piratés peuvent ne pas fonctionner correctement ou être entièrement défectueux, ce qui entraîne une surconsommation des ressources de votre entreprise et une augmentation des coûts informatiques.

5. En cas de problème, vous ne pouvez pas avoir recours au support technique de l'éditeur.

6. Les logiciels contrefaits peuvent être malveillants, par exemple contenir des chevaux de Troie, des virus ou des spywares qui s'infiltreront sur votre ordinateur et font usage de vos informations personnelles sans votre autorisation, qu'il s'agisse de vos numéros de carte de crédit ou de comptes bancaires, de vos mots de passe ou de vos carnets d'adresses. Les informations volées peuvent être exploitées immédiatement par des usurpateurs d'identité.

De même, un vendeur qui propose de violer la loi ne s'arrêtera probablement pas au piratage de logiciels. Toute donnée de carte de crédit ou information personnelle que vous communiquez peut être exploitée par des voleurs d'identité.

Comment se mettre à l'abri des logiciels piratés ?

Pour éviter d'être victime des pirates de logiciels, il est recommandé :

- D'acheter les logiciels uniquement auprès de sociétés connues.
- Lorsque vous faites des achats en ligne, assurez-vous que le site Web est légitime. Sur la page d'accueil du site de vente, cliquez sur l'icône de verrouillage qui apparaît sur le cadre de votre fenêtre de navigateur et affichez le certificat de sécurité.
- Si un prix affiché semble trop attractif, méfiez-vous. Méfiez-vous également des prix extrêmement faibles et vérifiez l'authenticité du site.





http://www