Comment dÃ©crypter vos fichiers infectÃ©s avec Avast Ransomware Decryption Tool

CatÃ©gorie : SÃ©curitÃ©
PubliÃ© par Nendo le 27/07/2025

Ce tutoriel explique comment utiliser l'outil Avast pour rÃ©cupÃ©rer des fichiers chiffrÃ©s par un ransomware. Il commence par lâ€™identification du type de ransomware Ã lâ€™aide de lâ€™extension des fichiers ou du message de ranÃ§on. Une fois identifiÃ©, lâ€™utilisateur tÃ©lÃ©charge lâ€™outil de dÃ©cryptage correspondant depuis le site officiel dâ€™Avast. Lâ€™outil est simple Ã utiliserâ€¯: il suffit de sÃ©lectionner le dossier oÃ¹ se trouvent les fichiers chiffrÃ©s, Ã©ventuellement fournir une version originale dâ€™un fichier, puis de lancer le processus de dÃ©cryptage. Lâ€™application effectue une analyse et tente de restaurer les donnÃ©es sans les endommager. Une fois le dÃ©cryptage terminÃ©, les fichiers deviennent Ã nouveau lisibles. Ce guide permet Ã tous, mÃªme sans connaissances techniques, de dÃ©crypter rapidement vos fichiers.

Installation de Avast Ransomware Decryption Tool

1) Pour commencer, rendez-vous sur la fiche de notre site pour **TÃ©lÃ©chargez le logiciel Avast Ransomware Decryption Tool pour Windows**
2) Cliquez sur le bouton **Download** pour obtenir la derniÃ¨re version du logiciel.
3) Puis lancez lâ€™installation du logiciel.

Ã‰tape 1 : Identifier le ransomware

Avant tout, il faut savoir quel ransomware vous a infectÃ©. Voici comment le reconnaÃ®tre :
- VÃ©rifiez lâ€™extension ajoutÃ©e Ã vos fichiers (ex: **.crypt**, **.locked**, **.bart, etc.**).
- Lisez le message de ranÃ§on affichÃ© (souvent un fichier texte ou une fenÃªtre).
- Consultez le site dâ€™**Avast Decryption Tools** pour comparer les symptÃ´mes.
Information : Si vous ne savez pas identifier le ransomware, utilisez un site comme **ID Ransomware** (en ligne et gratuit).

Ã‰tape 2 : TÃ©lÃ©charger lâ€™outil correspondant

1) Rendez-vous sur : **Site Avast Ransomware Decryption Tool**
2) Dans la liste, trouvez lâ€™outil correspondant au nom du ransomware (ex : **TeslaCrypt**, **Jigsaw**, **AES_NI**, etc.).
3) Cliquez sur **TÃ©lÃ©charger** pour rÃ©cupÃ©rer lâ€™exÃ©cutable .exe.

Ã‰tape 3 : PrÃ©parer les fichiers Ã dÃ©crypter

- CrÃ©ez un dossier sur votre bureau avec **les fichiers chiffrÃ©s** Ã traiter.
- Si possible, ajoutez **une version originale non chiffrÃ©e** dâ€™un fichier (cela peut accÃ©lÃ©rer le processus de dÃ©cryptage).

Ã‰tape 4 : Lancer le dÃ©cryptage

1) Ouvrez lâ€™outil tÃ©lÃ©chargÃ© (**clic droit** > **ExÃ©cuter en tant quâ€™administrateur**).
2) Lisez et acceptez les conditions dâ€™utilisation.
3) SÃ©lectionnez :
 - Le **dossier contenant les fichiers chiffrÃ©s**.
 - Le **fichier original non chiffrÃ©** si vous en avez un (facultatif).
4) Lancez le processus avec le bouton **Start Decryption**.

InformationÂ : Lâ€™outil va analyser les fichiers, tenter de retrouver la clÃ© de dÃ©cryptage, puis restaurer les fichiers dans leur version dâ€™origine. Il crÃ©e automatiquement des copies de sauvegarde pour Ã©viter toute perte.

Ã‰tape 5 : VÃ©rifier les fichiers dÃ©cryptÃ©s

- VÃ©rifiez que vos fichiers sont bien lisibles.
- Les originaux chiffrÃ©s peuvent Ãªtre supprimÃ©s une fois le dÃ©cryptage confirmÃ©.

Petits conseils de sÃ©curitÃ©

- **Ne payez jamais la ranÃ§on** : ces outils sont gratuits et fiables.
- Mettez Ã jour votre antivirus aprÃ¨s lâ€™incident.
- Sauvegardez rÃ©guliÃ¨rement vos donnÃ©es sur un support externe.
- Ã‰vitez dâ€™ouvrir des piÃ¨ces jointes suspectes Ã lâ€™avenir.