



## LES BONNES PRATIQUES POUR SE PROTÉGER DES STEALERS

-  Ne **pas télécharger**, ni utiliser de logiciels, d'applications et de vidéos piratés ou **d'origine douteuse** qui peuvent souvent contenir un virus.
-  Ne **jamais désactiver votre antivirus** à la demande d'un logiciel.
-  Face à un **message suspect** (inattendu, alarmiste, aguicheur...), **ne pas ouvrir les pièces jointes** ou cliquer sur les liens.
-  **Mettre régulièrement à jour** vos appareils, logiciels et applications.
-  **Utiliser des mots de passe forts** qui ne disent rien sur vous et différents pour chaque accès afin d'éviter des piratages en cascade.
-  Deux sécurités valent mieux qu'une : **activer la double authentification** lorsque cela vous est proposé.
-  **Ne pas stocker vos mots de passe de manière non sécurisée** : post-it, fichiers textes, messages brouillons, notes sur votre smartphone...
-  Utiliser un **gestionnaire de mots de passe** ou un trousseau d'accès sécurisés, stockés de préférence en local, pour conserver vos mots de passe en sécurité. Vous n'aurez ainsi à retenir qu'un mot de passe pour accéder à l'ensemble de vos comptes.
-  Ne **jamais sauvegarder vos mots de passe dans le navigateur** d'un ordinateur partagé.
-  **Se déconnecter systématiquement de votre compte** après utilisation, pour éviter que quelqu'un puisse y accéder après vous.

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :  
[www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)

