Comment éviter les PUP

Si vos utilisateurs téléchargent des logiciels sur leurs ordinateurs, il est possible que, sans le savoir, ils encombrent leurs machines de PUP. Une petite formation pourrait permettre d'économiser du temps de nettoyage (sans parler des ressources informatiques).

Voici ce que vos utilisateurs et vous devez savoir à propos des PUP.

Qu'est-ce qu'un PUP ?

CE N'EST PAS : un bébé chien.

C'EST : l'acronyme de programmes potentiellement indésirables, Potentially Unwanted Programs en anglais.

Un PUP est un logiciel que les utilisateurs **ne souhaitaient** probablement **pas installer** sur leur ordinateur.

FONCTIONNEMENT :

- ralentit l'ordinateur en raison de nombreux processus en arrière-plan
- affiche de nombreuses publicités dérangeantes
- ajoute des barres d'outils qui prennent de la place sur le navigateur
- collecte des informations privées

COMMENT SONT TOUCHÉS VOS UTILISATEURS :

Les PUP sont souvent associés à des logiciels volontairement installés par les utilisateurs. En cliquant rapidement pendant une installation, l'utilisateur peut facilement rater les petits caractères et « accepter » les applications supplémentaires.

Les spywares, adwares et dialers sont des **types de PUP.**

Les PUP sont parfois appelés **bundlewares, junkwares ou PUA** (applications potentiellement indésirables).

Les **PUM** sont des modifications potentiellement indésirables. Elles changent les paramètres par défaut de l'ordinateur.

Les PUM peuvent être réalisées par des applications légitimes et des malwares. Toutefois, les modifications effectuées par des malwares sont plus susceptibles de poser problème.

Vos utilisateurs ne se rendent peut-être même pas compte de ces modifications.

Contexte

Les concepteurs de PUP estiment que puisqu'ils incluent toutes les informations de consentement nécessaires dans l'accord de téléchargement, les PUP ne devraient pas être associés à des logiciels espions ou à toute autre forme de malware.

TÉLÉCHARGER

(Parce que tout le monde lit les accords de téléchargement, n'est-ce pas ?) Ainsi, McAfee a créé le terme doux et moins agressif **« programmes potentiellement indésirables ».**

Critères de détermination des PUP

Pour déterminer si un programme est un PUP, les ingénieurs de sécurité examinent une liste de mauvais comportements. Certaines applications entrent dans la catégorie des PUP en raison de leurs **multiples infractions**, d'autres en raison d'**une importante violation**.

GRATUIT

CLIQUEZ ICI

Infractions publicitaires

- Publicité intrusive ou hors contexte
- Pop-ups ou pop-unders
- Insertion, superposition ou remplacement de publicité
- Publicité sans attribution clairement identifiée
- Publicités non clairement définies comme des publicités
- Redirection vers le site d'un concurrent

Infractions de téléchargement

- Trop de raccourcis sur le bureau
- Regroupement
- Cases pré-cochées
- Utilisation abusive de la mention « recommandé » à côté d'une option
- Procédure de désinstallation indisponible ou difficile
- Emplacements d'installation non standard
- Composants additionnels de navigateur non affichés dans le gestionnaire des suppléments

Infractions sur Internet

- Résultats de recherche altérés
- Barre d'outils sans valeur
- Moteurs de recherche ou pages d'accueil détournés
- Insertions de signets

Programmes sur liste noire

- Nettoyeurs, optimiseurs et défragmenteurs de registres
- Programme d'optimisation et de mise à jour des pilotes

Conseils pour éviter les PUP

Reconnaître les « dark patterns »

Les dark patterns sont des interfaces utilisateur délibérément conçues pour tromper l'utilisateur.

Recherchez les **cases pré-cochées** (des programmes tels que Unchecky analysent les accords de logiciels tiers et décochent les options installant des programmes potentiellement indésirables (PUP) mais ils sont susceptibles de ne pas tout détecter).

Attention aux programmes ajoutant un « sceau » non officiel en tant qu'indicateur de crédibilité.

Ignorer | Suivant | Annuler

Regardez si l'interface pousse à certaines actions (bouton « ignorer » grisé pour inciter à cliquer sur le bouton de couleur vive « suivant »).

ACHETER

Attention aux mauvaises consignes : les sociétés **peuvent essayer de cacher** des options gratuites ou moins chères.

Lisez attentivement les CLUF

- N'acceptez pas des conditions d'utilisation concernant un ensemble de programmes.
- Lisez le titre au-dessus des clauses pour vous assurer que le Contrat de Licence Utilisateur Final (CLUF) que vous acceptez ne concerne que le programme que vous avez téléchargé à l'origine.
- Si ce n'est pas le cas, vous pouvez refuser et poursuivre le processus d'installation.

Lisez attentivement les instructions de l'assistant d'installation

- Lisez les informations dans la **barre de navigation supérieure** de l'assistant d'installation pour retenir les noms des programmes indésirables.
- **N'acceptez pas les paramètres d'installation standard, rapide, par défaut** ou autres paramètres d'installation recommandés.
- **Choisissez toujours l'installation personnalisée.** Les assistants d'installation peuvent parfois qualifier cette installation d'avancée entre parenthèses mais il s'agit en fait d'un dark pattern. **Les paramètres personnalisés ne sont pas avancés.**

Augmentez la sécurité

- Installez un bloqueur de publicités/bloqueur de fenêtres contextuelles
- Installez des produits contre les programmes malveillants et espions

En savoir plus sur malwarebytes.org/resources/

Malwarebytes