



Forum: Propositions de logiciels

Topic: Dashlane : gestionnaire des mots de passe

Subject: Re: Dashlane : gestionnaire des mots de passe

Publié par: tignothe

Contribution le : 07/03/2018 00:06:39

Bonjour,

Citation :

DANHY

Comment peut-on être certain de l'inviolabilité des mots de passe, qui sont, d'après ce que je comprends, stockés sur le Cloud ?

Tout simplement parce que le « mot de passe maître qui sert à « chiffrer » la « base de donnée » (la totalité des mots de passe qui se retrouve sur les serveurs de Dashlane) ne sort pas de l'appareil où il a été conçu. Il n'est même pas mémorisé sur le PC (pas de transmission de ce mot de passe sur les serveurs de Dashlane).

En d'autres termes, seul le créateur de ce mot de passe maître est capable de « déchiffrer » sa base, et ce mot de passe maître ne va jamais se balader sur les serveurs de Dashlane. Donc pas de sueurs froides à avoir.

Le fait que la base de donnée aille se promener sur les serveurs Dashlane ne change rien à l'affaire. Double sécurité, il faut posséder ce mot de passe maître et en plus que l'appareil sur lequel le déchiffrement se fait soit autorisé pour que l'opération se fasse. Les opérations de « chiffrement » « déchiffrement » se font en local

Personnellement je suis utilisateur de Keepass version 2.38 (Ubuntu) et ma base de donnée est en local (chiffrée) sur mon PC, et sur Dropbox et Hubic pour que je puisse la récupérer notamment sur mon Iphone avec une Apps qui va bien. Ce petit voyage sur le cloud se fait après un « chiffrage » en AES (avec une clé 256 bits) et Twofish (avec des blocs de 128 bits et une clé de 256 bits).

Pour ce qui concerne Dashlane,

Citation :

Dashlane explique le chiffrement <https://frblog.dashlane.com/chiffrement-dashlane/>

Jusqu'à preuve du contraire, personne ne peut se vanter d'avoir pu « cracké » cette norme AES 256.

Donc on peut avoir confiance en Dashlane.