



## Plus de la moitié des mots de passe rendent les armes en 24 heures

publié le 12/07/2015

### Descriptif :

Article sur ITexpresso et recommandations de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information)

Trustwave a soumis près de 500 000 mots de passe à des tests de robustesse. **Résultat : 51% d'entre eux ont pu être craqués en à peine une journée, du fait notamment d'un manque évident de complexité.** [🔗](#)

**Les avertissements sur la faiblesse des mots de passe et les risques encourus sont le plus souvent ignorés des internautes.**

Résultat, plus de la moitié des mots de passe pourraient être « craqués » en 24 heures, selon le rapport 2015 mondial de la société de sécurité informatique Trustwave.

La firme américaine, qui a effectué des tests de robustesse sur 499 556 mots de passe hachés l'an dernier, estime que 51% d'entre eux peuvent être piratés en l'espace de 24 heures et 88% dans les deux semaines, relève Silicon.fr.

Autre enseignement de l'étude, « Password1 » est toujours le mot de passe le plus utilisé et 39% des mots de passe testés ne dépassaient pas les 8 caractères. Ces derniers ont été reconnus par les hackers testeurs de Trustwave en une journée environ.

**Dans ses recommandations** [🔗](#) sur la sécurité des mots de passe, l'Anssi (Agence nationale de la sécurité des systèmes d'information) indique : « la robustesse d'un mot de passe dépend en général d'abord de sa complexité [...] Si vous souhaitez une règle simple : choisissez des mots de passe d'au moins 12 caractères de types différents (majuscules, minuscules, chiffres, caractères spéciaux). »

Un avis partagé par Trustwave. La publication de son rapport fait suite au piratage du gestionnaire de mots de passe LastPass confirmé en début de semaine.



**Académie  
de Poitiers**

Avertissement : ce document est la reprise au format pdf d'un article proposé sur l'espace pédagogique de l'académie de Poitiers.

Il ne peut en aucun cas être proposé au téléchargement ou à la consultation depuis un autre site.