

Le “mode espion” de Google que personne ne connaît

Le Google Dorking ou Google Hacking Database

On pense parfois que les cybercriminels pour s'introduire dans des entreprises ou pour trouver des fuites de données utilisent des outils très complexes et dur d'accès. Parfois oui, mais sachez que parfois ils utilisent Google, ce n'est pas une blague ! Il y a une discipline entière qui s'appelle le Google Dorking ou le Google Hacking Database. Vous allez voir qu'en détournant certaines fonctions de Google on peut accéder à des trucs de malade et vous allez péter un câble. Si vous avez un site web, peut-être allez-vous faire des petits changements de configuration et si vous n'avez pas de site web, c'est le moment de vous présenter notre partenaire au-dessus : Switch. Ce sont des hébergeurs français qu'on aime beaucoup parce qu'ils ont une seule offre unique tout inclus : il se passe disque limité, transfère mensuel illimité, support 7 jours sur 7, une interface très épurée, un nom de domaine offert, bref on essaiera pas de vous faire passer sur un plan supérieur avec des trucs limités. Là, il y a tout doux : 48 giga de ram, c'est carré, et vous avez un code promo M15 avec 15% de réduction dans la description.

En quoi consiste le Google Dorking ?

En quoi ça consiste ? Je le disais, ça consiste à faire des requêtes de recherche avancées sur Google pour trouver des informations cachées ou des informations qui ne devraient pas

vraiment être en clair ou qui devrait être derrière un mot de passe et un nom d'utilisateur une protection. Mais alors, question Mathieu, dis-moi qu'est-ce que c'est que la recherche avancée de Google ? Moi j'utilise Google, je tape des mots, je clique sur Recherche. En fait, tu peux spécifier plein de petits chances spécifiques dans Google pour avoir des résultats beaucoup plus précis. Par exemple, si tu mets des doubles côtes dans ton mot, ça veut dire, enfin, dans ton expression, ça veut dire que il faut que toute cette expression apparaisse dans une phrase soit exact pour pour rechercher dans Google.

Une mise en garde

Mais juste avant ça, une petite mise en garde. Je vous raconte l'histoire de Bluetooth, c'est un journaliste à cœur, on va dire, et il s'est fait condamner pour avoir cherché sur Google. Qu'est-ce qui s'est passé ? En fait, c'était en 2012. Il a accédé à l'extranet de l'Agence Nationale de Sécurité Sanitaire de l'Alimentation de l'Environnement et du Travail et en extrait 8000 fichiers pour un total de quasiment 8 Go et publie 250 Mo, mais c'était accessible. Il y a eu un procès et il a été condamné. La Cour de Cassation a rendu un arrêt qui aujourd'hui fait jurisprudence et qui c'est pour ça que nous on est obligé de prendre des précautions aujourd'hui, c'est qu'il a été rendu coupable de cette maintenance dans une base de données automatisée de données et aussi pour vol d'information parce qu'il en a fait des copies, il les a téléchargé sur son ordinateur. Mais si tu accèdes à la donnée sans la télécharger, alors là, c'est légal. Globalement, en fait, c'est un peu comme c'est un peu comme une maison. Finalement, c'est ta recherche Google, tu as totalement le droit de le faire, sauf à partir du moment où tu cliques, tu tiens à ce que j'ai vraiment le droit d'y être, si c'est non, alors arrière. Et puis si vous tombez sur un truc vraiment parce que là, on va aussi l'utiliser de façon tout à fait innocente, mais voilà, si vous tombez sur le truc, vous pouvez aussi

contacter l'autorité et un peu le référence vous trouvez des failles. Parce que parce que comme ça, ça vous évitera d'avoir des ennuis parce qu'il y a la si derrière ou la CNIL aussi, exactement, il y a des problèmes de redonner. Je vous ai demandé à chacun de faire des petites recherches de vos meilleurs dents.

Exemples de Google Dorking

<

Source : [Underscore_](#) | Date : 2023-01-09 19:43:47 | Durée : 00:14:22

Description de la vidéo :

faites vraiment attention quand vous utilisez ça Merci à 02switch d'avoir sponsorisé la vidéo ! Je vous laisse découvrir leur offre ...

→  Accéder à [CHAT GPT](#) en cliquant dessus