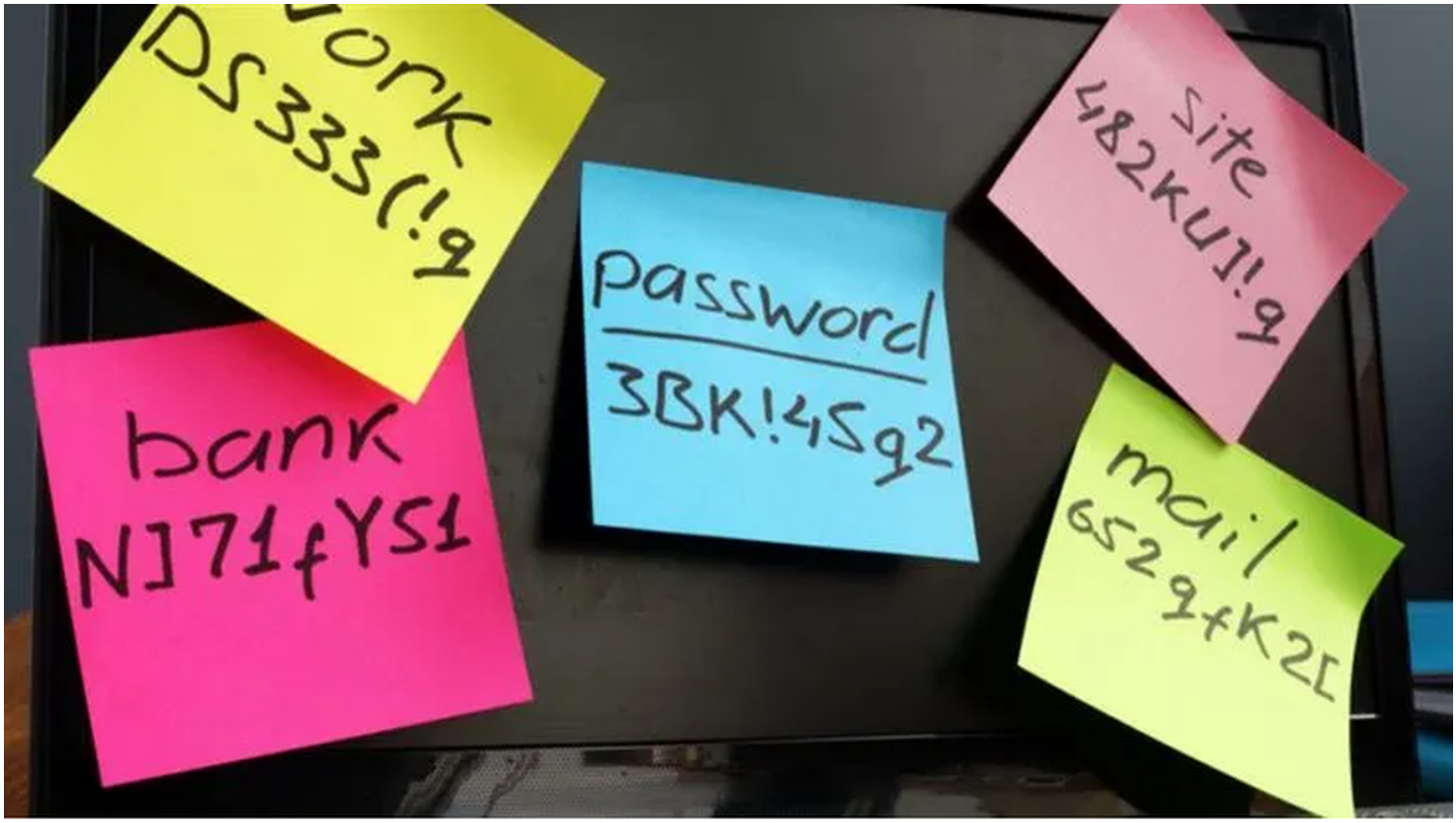
De nombreux sites Web importants permettent aux utilisateurs d'avoir des mots de passe faibles
Malwarebytes

Pieter Arntz :



Une nouvelle étude qui examine l'état actuel des politiques de mots de passe sur Internet montre que bon nombre des sites Web les plus populaires permettent aux utilisateurs de créer des mots de passe faibles.

Pour l'étude de Georgia Tech, les chercheurs ont conçu un algorithme qui détermine automatiquement la politique de mot de passe d'un site Web.
À l'aide de l'apprentissage automatique, ils ont pu voir la cohérence des exigences et des restrictions de longueur pour les chiffres, les lettres majuscules et minuscules, les symboles spéciaux, les combinaisons et les lettres de départ.
Ils pouvaient également voir si les sites autorisaient les mots du dictionnaire ou les mots de passe connus pour avoir été piratés.

À l'aide de cet outil, ils ont trouvé :

- 12 % des sites Web qu'ils ont consultés n'ont aucune exigence en matière de longueur de mot de passe.
- 3 sur 4 ne répondent pas aux normes minimales, ce qui signifie qu'elles :
    - Autoriser les mots de passe très courts

- Ne bloquez pas les mots de passe courants
- Utiliser des exigences obsolètes comme des caractères complexes

Plus de la moitié des sites Web de l'étude acceptaient les mots de passe de six caractères ou moins, et 75 % d'entre eux n'exigeaient pas le minimum recommandé de huit caractères.
Environ 12 % des sites Web n'avaient pas d'exigences de longueur et 30 % ne prenaient pas en charge les espaces ou les caractères spéciaux.

Donner ce genre de liberté aux utilisateurs, c'est leur demander d'être dupés.
Comme nous l'avons souligné il y a quelque temps, même les utilisateurs férus de technologie, comme les administrateurs informatiques, ont recours à des mots de passe horribles lorsqu'ils en ont l'occasion.

Les raisons de ne pas appliquer les normes sont évidentes.
La plupart des sites Web se soucient davantage de la satisfaction du client que de la sécurité, et vous pouvez deviner lequel est le meilleur pour les affaires.

Les utilisateurs n'aiment pas les mots de passe, d'autant plus que la situation des mots de passe a été aggravée par des règles ridicules et inutiles, telles que demander aux utilisateurs de choisir des mots de passe qui suivent des formules, ou forcer les utilisateurs à changer leur mot de passe tous les quelques mois.
Ces deux règles ont été discréditées, mais continuent de nous hanter.
Les formules réduisent le nombre de mots de passe possibles parmi lesquels un utilisateur peut choisir, et les réinitialisations régulières des mots de passe encouragent les utilisateurs à choisir des mots de passe conformes à un modèle prévisible, ce qui peut faciliter la devinette des mots de passe, ce qui est le contraire de ce que nous voulons.

Si vous souhaitez en savoir plus à ce sujet, lisez « Pourquoi (presque) tout ce que nous vous avons dit sur les mots de passe était faux ».
L'article résume comment une grande partie de ce qu'on vous a dit sur les mots de passe au fil des ans était soit erronée (changez vos mots de passe aussi souvent que vos sous-vêtements), soit malavisée (choisissez des mots de passe longs et compliqués), soit contre-productive (ne réutilisez pas les mots de passe).

Nous pensons que nous devrions nous éloigner complètement du modèle qui oblige les utilisateurs à créer et à mémoriser des mots de passe.
Il est temps de passer à quelque chose de plus sûr ET de plus convivial.
Et ce n'est pas comme si ces systèmes n'existaient pas (bonjour les clés d'accès), nous avons juste besoin de les adopter plus largement.

Activons l'authentification multifacteur (MFA) là où nous le pouvons, même si nous pensons que l'utilisation d'un mot de passe comme premier facteur n'ajoute pas beaucoup de sécurité supplémentaire à la procédure de connexion.
Et si nous devons nous fier uniquement aux mots de passe, essayez d'utiliser un gestionnaire de mots de passe.
Ils vous aident à créer des mots de passe complexes et à les mémoriser pour vous.

Le rapport complet des chercheurs sera présenté lors de la conférence de l'ACM sur la sécurité informatique et des communications (CCS) à Copenhague, au Danemark, plus tard ce mois-ci.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20231204
"C'est ensemble qu'on avance"