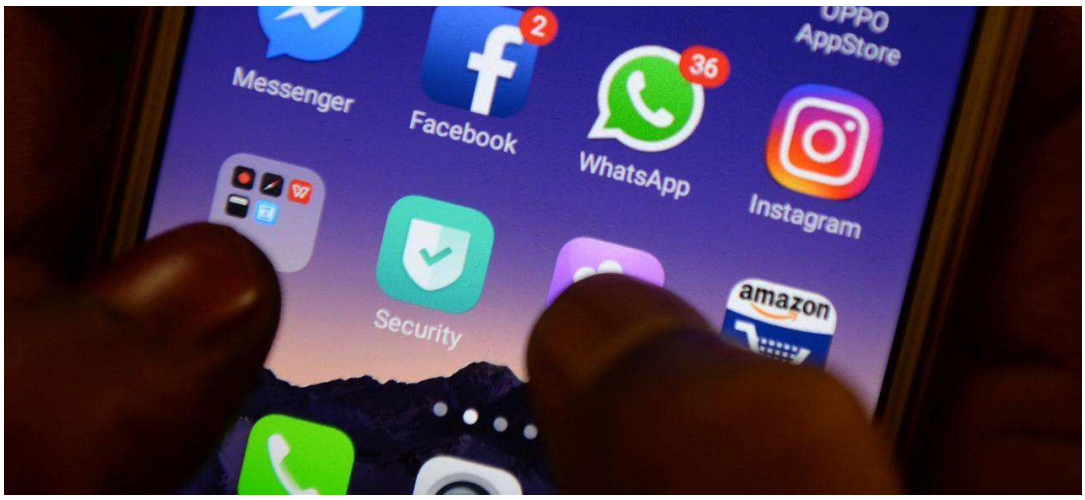
L'organisme qui supervise le Web annonce la mort à venir des mots de passe

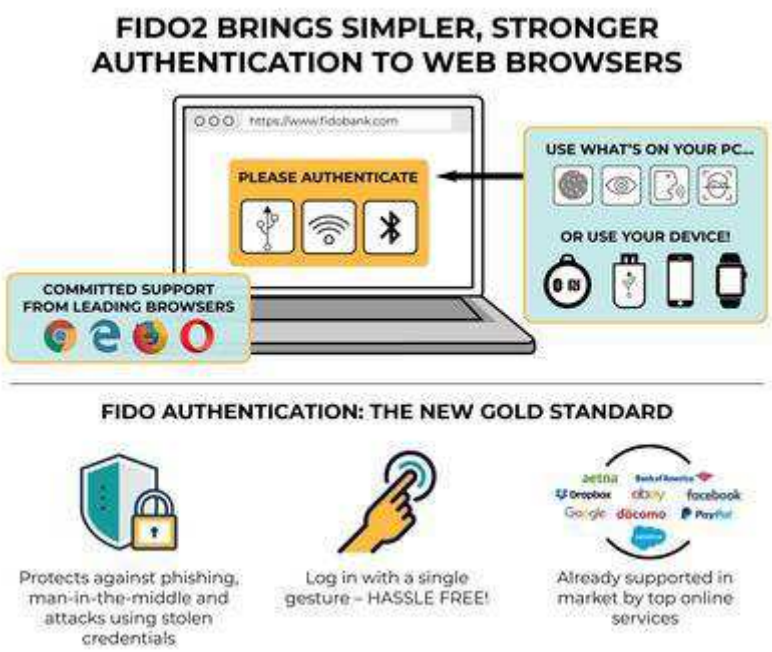


Nos habitudes d'authentification sur le web vont évoluer avec le déploiement de ce nouveau standard. - Crédits photo : ARUN SANKAR/AFP

Tech & Web (http://premium.lefigaro.fr/secteur/high-tech) | Par Marius François (#figp-author)
Mis à jour le 13/04/2018 à 14h52

Le consortium international W3C a approuvé un nouveau standard dont le déploiement va permettre d'améliorer la sécurité des usages en ligne.

Le mot de passe appartiendra bientôt au passé et c'est une bonne nouvelle. Le World Wide Web Consortium (W3C), l'organisation qui gère les standards du Web, a annoncé la mise en place d'un nouveau modèle d'authentification. Il concernera notamment l'accès aux banques en ligne, aux réseaux sociaux ou encore aux sites d'e-commerce. L'institution internationale, qui réunit plus de 400 grandes organisations liées au web, prévoit de déployer la connexion par biométrie et périphériques mobiles. Le grand public verra sa mise en place dans les prochains mois et années. Il faut en effet laisser le temps aux développeurs d'adapter les sites à ce nouveau standard. Jugés aisément piratables et peu fiables, les mots de passe devraient, quant à eux, progressivement tirer leur révérence.



Avec la nouvelle authentification FIDO2, les mots de passe devraient disparaître. - Crédits photo : World Wide Web Consortium

Associé au **FIDO** (https://www.fidoalliance.org/), un standard d'authentification, le W3C a dû mettre d'accord **les représentants de plus de 30 entreprises** (https://www.w3.org/2000/09/dbwg/details?group=87227&order=org&public=1) comme Airbnb, Alibaba, Apple, Google ou encore le français Orange. Il était question de mettre au point un système d'authentification simplifié pour l'utilisateur et qui améliore la sécurité des comptes.

Les utilisateurs auront le choix entre deux modes d'authentification: soit depuis un périphérique externe (smartphone, badge NFC, **clé USB** (http://www.01net.com/tests/test-yubico-yubikey-neo-la-cle-usb-pratique-pour-securiser-vos-comptes-google-et-facebook-5617.html), montre connectée), soit directement depuis leur ordinateur par biométrie (reconnaissance d'empreinte, de visage, d'iris ou de la voix). Certaines de nos machines embarquent déjà les équipements nécessaires (lecteur d'empreinte, webcam), ils vont peu à peu se démocratiser. Pour ce qui est de la reconnaissance d'iris, elle nécessite des caméras de bonne qualité et un logiciel particulier, peu communs sur les appareils grand public. Néanmoins, certains smartphones haut de gamme **comme le Galaxy S9** (http://www.samsung.com/fr/smartphones/galaxy-s9/performance/#intelligent-scan) en sont déjà pourvus. Une fois lancés par l'utilisateur, ces systèmes enverront une signature numérique au site pour accéder au service. Comme le rapporte **01net** (http://www.01net.com/actualites/ce-nouveau-standard-va-t-il-enfin-nous-permettre-de-nous-debarrasser-des-mots-de-passe-1416559.html), ce standard attendait l'approbation du W3C depuis 2015.

L'organisation annonce avoir déjà convaincu de nombreux acteurs du numérique comme les navigateurs Chrome, Edge, Mozilla et Opéra ainsi que des plateformes à l'instar de Facebook, ebay ou Google. Facebook et Google justement se sont déjà équipés de ce mode d'authentification en complément du mot de passe. Les entreprises vont peu à peu déployer le standard FIDO2, par le biais de l'**API WebAuthn** (https://www.w3.org/TR/2018/CR-webauthn-20180320/) (une interface logicielle) récemment mise à disposition des développeurs.

Les mots de passe, «maillon faible» de la sécurité en ligne

«Alors qu'il y a de nombreux problèmes de sécurité en ligne et que l'on ne peut tous les résoudre, l'usage des mots de passe est l'un des maillons les plus faibles», explique Jeff Jaffe, dirigeant du consortium. En effet, de nombreux internautes ne respectent pas les règles de création de mots de passe les plus élémentaires ou se font piéger par des hackers.

» LIRE AUSSI - Comment choisir un bon mot de passe? (http://www.lefigaro.fr/secteur/high-tech/pratique/2016/11/24/32002-20161124ARTFIG00075-comment-choisir-un-bon-mot-de-passe.php)

L'organisation explique que la sécurité en sera donc renforcée. Le standard FIDO2 serait la solution contre le phishing, les attaques de l'homme du milieu (interceptions de communications) et les usurpations d'identité. Le **phishing** (https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/Phishing-hameconnage-ou-filoutage), par exemple, est un hameçonnage de l'internaute invité par un e-mail spam à donner des informations un site web frauduleux imitant parfaitement un site de confiance. Avec WebAuthn, il sera difficile à exécuter car le nom de domaine du service est lié au système d'authentification par cryptage. En somme, si un pirate essaie de récupérer des données via un faux site, le système ne transmettra pas la signature numérique de l'internaute. Aujourd'hui, les données d'identification comme le mot de passe transitent jusqu'au site web. S'il s'agit d'un faux, le pirate peut donc les récupérer. Si certains regretteront la nécessité d'avoir un périphérique sur soi ou de devoir faire une manipulation pour accéder à un service en ligne, le gain de sécurité sera une réelle plus-value selon le W3C.

(http://plus.lefigaro.fr/page/marius-francois-0)
Marius François (http://plus.lefigaro.fr/page/marius-francois-0)
Journaliste
Suivre (http://plus.lefigaro.fr/fpservice/follow/membre/8132503124224559636736912743501 3/3363197)
Journaliste au Service Tech & Web
Twitter : @marius_francois (https://twitter.com/marius_francois)