FUTURA

Apple, Google et Microsoft signent la fin des mots de passe (Techpod #40)

Podcast écrit par Sylvain Biget et lu par Emma Hollen

Bonjour à toutes et à tous et bienvenue dans Techpod, la chronique audio de Futura dédiée à l'actualité des technologies et de la mobilité. Je suis Emma Hollen, et aujourd'hui on va parler de la fin des mots de passe.

[*Musique technologique, journalistique*]

123456, azerty, … et pourquoi pas loulou. Ça a l'air d'une blague, mais tous les ans le palmarès des mots de passes les plus utilisés en France ne témoigne ni d'une grande créativité ni d'un grand renouveau. Il faut dire qu'avec la multitude des réseaux sociaux, des applis bancaires, des identifiants numériques pour tous les services publics, des gadgets connectés et des abonnements en ligne, ça fait beaucoup de comptes d'utilisateurs à mémoriser. Si c'est facile, on ne se trompe pas mais la sécurité en pâtit, et si c'est compliqué on ne retient pas et combien d'entre nous ont déjà abandonné un compte en ligne dans les oubliettes d'internet, incapables de retrouver le mot de passe lié à une messagerie Hotmail ou Caramail délaissée depuis des années ? Heureusement, les applications de gestionnaires de mot de passe se démocratisent et retiennent, voire créent pour vous, les mots de passe les plus complexes et impossibles à mémoriser – bon, si tant est que vous reteniez quand même celui du gestionnaire. Mais voilà, le problème avec cette solution, c'est que lorsque vous essayez de vous connecter sur un autre appareil que le vôtre, c'est toujours le même cirque : impossible de vous souvenir des mots de passe à 15 lettres et 8 chiffres que Chrome ou Dashlane ont choisi pour vous. Mais rassurez-vous, cette folie des sésames et des multiples identifications, c'est bientôt terminé ! En effet dès l'an prochain, le fameux mot de passe devrait commencer à disparaître progressivement. Comment ? Grâce à une norme baptisée FIDO2, qui émerge depuis plusieurs années. C'est sur ce protocole que Microsoft, Apple et Google se sont entendus. Chose rare, les colosses de l'informatique ont accordé leurs violons pour intégrer ce système dans tous leurs produits. Le FIDO2 sert tout bonnement à supprimer la notion de mot de passe. Hé oui, car malgré les apparences, même le mot de passe le plus costaud reste un maillon faible. Il est systématiquement envoyé vers un serveur pour l'authentification, et il y est aussi stocké. Mot de passe fort ou faible, c'est finalement le plus souvent lors du piratage de la base de données utilisateurs d'un service en ligne que les hackers font leur razzia sur les sésames. Alors comment procéder pour sécuriser un compte sans mot de passe ? En combinant plusieurs technologies. Vous l'avez remarqué, aujourd'hui les capteurs d'empreinte digitale sur les smartphones et même les ordinateurs sont devenus monnaie courante. Ils sont associés au mot de passe et ajoutent une couche de protection pour activer l'appareil. On retrouve également la reconnaissance faciale, ou encore le code PIN et même les dessins.

[*Nouvelle musique technologique*]

À la différence des services en ligne, tous ces systèmes mémorisent un identifiant biométrique ou un code directement sur l'appareil. Et cet identifiant est comme gravé à l'intérieur. Il n'en sort jamais. On élimine ainsi le maillon faible de la chaîne, le stockage des mots de passe sur des serveurs vulnérables. Bien, mais ce genre de protocole permet seulement de débloquer un appareil, pas de se connecter à Facebook, alors comment s'y prend-on pour résoudre ce problème ? Eh bien, à l'avenir, pour vous connecter en ligne, il vous faudra utiliser un petit composant appelé Webauthn. Que son nom barbare ne vous inquiète pas, il a déjà été intégré à presque tous les navigateurs du marché ces dernières années. Cela signifie qu'il peut être utilisé par n'importe quel site. Android, iOS, macOS et Windows 10/11 l'exploitent aussi désormais. Ce procédé remplace le mot de passe par un jeu unique de deux clés de chiffrement. L'une est publique et reste chez le service en ligne, l'autre est privée et ne quitte jamais votre appareil. Il ne vous reste alors plus qu'à toucher le capteur biométrique de votre ordinateur ou de votre portable, ou encore à montrer votre visage pour activer cette clé privée et déverrouiller l'accès via la clé publique distante. Et si ces explications vous semblent trop compliquées, retenez simplement que d'ici quelques années, vous n'aurez plus à mémoriser tous ces mots de passe, mais simplement à poser le bout de doigt sur un capteur et ça va nous changer la vie !

[*Musique de conclusion douce, évocatrice d'un jeu vidéo*]

Merci d'avoir suivi cet épisode de Techpod. Pour ne rien manquer à l'actualité technologique et scientifique, je vous invite à suivre Fil de Science et nos autres podcasts sur Apple Podcasts, Spotify, Google Podcasts ou encore Amazon Music. N'hésitez pas à nous laisser un commentaire et un like, ou une note, pour nous aider à améliorer notre travail et à le faire connaître. Pour le reste, on se retrouve mercredi prochain pour toujours plus d'actualités technologiques, et d'ici là bonne semaine à toutes et tous.