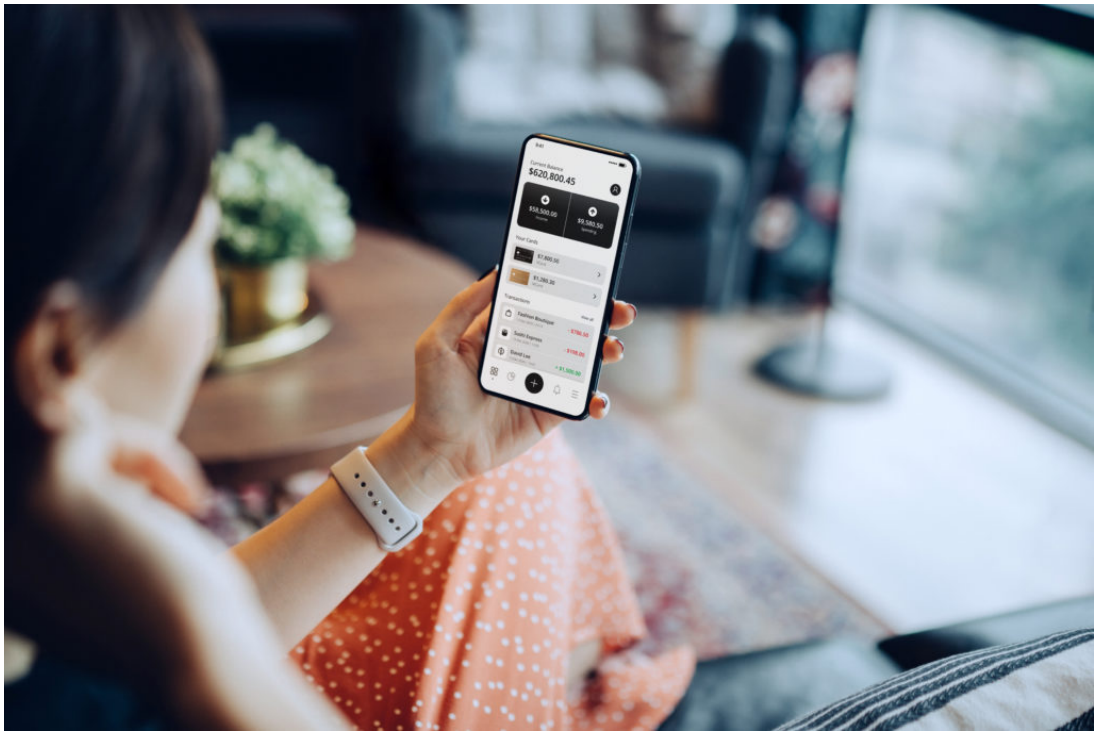
NUANCE | WHAT'S NEXT BLOG

Autentification biométrique et prévention, Engagement client omnicanal

Le moment est venu de repenser l'authentification des clients

Brett Beranek | Vice President & General Manager, Security & Biometrics

18 novembre 2021



Les méthodes d'authentification fondées sur les connaissances, auxquelles nous faisons confiance pour nous protéger, ne sont pas à la hauteur. Cependant, l'heure de la victoire des pirates n'a pas encore sonné. Car l'authentification biométrique permet aujourd'hui aux entreprises de protéger les consommateurs comme vous et moi, tout en leur offrant une expérience client de meilleure qualité.

Tous les ans, les consommateurs victimes de piratage perdent des milliards à travers le monde. En début d'année, une enquête internationale menée par Nuance a révélé qu'un cinquième des personnes interrogées avaient été victimes de piratage au cours des 12 mois précédents. Et le problème ne fait qu'empirer : le responsable de la sécurité d'une banque de détail avec qui j'ai discuté récemment parle d'une augmentation de 400 % des tentatives de piratage pendant la pandémie de COVID-19.

Beaucoup trop de personnes et d'entreprises s'appuient encore sur des outils d'authentification qui ne sont plus adaptés. Et les bouleversements survenus au cours des 19 derniers mois ont créé de nouvelles opportunités pour les fraudeurs. Il est plus urgent que jamais d'abandonner les méthodes traditionnelles d'authentification des clients, comme les codes PIN et les mots de passe, au profit de facteurs plus puissants comme la biométrie.

Un mot de passe ne peut jamais être fort.

Il est très facile pour les criminels d'acheter codes PIN, mots de passe et autres informations personnellement identifiables (IPI) sur le dark web. Et plus « l'hygiène » des mots de passe est négligée, plus ces informations dérobées sont précieuses pour les pirates.

Notre enquête a révélé que, malgré tous les efforts de publicité et de sensibilisation consacrés à la cybersécurité, 76 % des consommateurs n'utilisent toujours pas un mot de passe différent par site web ou par marque avec lesquels ils interagissent. Par ailleurs, seuls 18% prennent en considération les indications garantissant le niveau de sécurité du mot de passe et choisissent l'option la plus forte.

Si les méthodes d'authentification traditionnelles ne parviennent pas à apporter une sécurité adéquate, elles devraient au moins pouvoir offrir une bonne expérience client.

Or, rien n'est moins vrai. Les méthodes d'authentification fondées sur les connaissances (KBA) ne forment quasiment aucun obstacle pour un fraudeur déterminé, qui dispose toujours de toutes les informations dont il a besoin. En revanche, ces méthodes sont très contraignantes pour les vrais clients qui, souvent, perdent ou oublient les informations censées vérifier leur identité. *Vous rappelez-vous* le nom de famille de votre instituteur ou votre numéro client à 16 chiffres ?

Les répondants à l'enquête affirment que les méthodes d'authentification traditionnelles nuisent à l'expérience client. Près d'un tiers (31 %) sont frustrés par les majuscules / minuscules et les caractères spéciaux, et 30 % ont régulièrement des problèmes pour retrouver leur nom d'utilisateur, code PIN ou mot de passe et doivent les réinitialiser.

L'heure est à l'authentification biométrique

Pour remédier aux vulnérabilités inhérentes aux méthodes KBA traditionnelles, beaucoup d'entreprises se tournent vers l'authentification biométrique. Des solutions telles que Nuance Gatekeeper vérifient l'identité des personnes sur la base de caractéristiques qui leur sont spécifiques et uniques. Ces facteurs ne peuvent être oubliés, volés ou usurpés, ce qui les rend à la fois plus sûrs et plus pratiques.

Alors que les appareils biométriques, comme les dispositifs d'identification digitale ou faciale, sont bien connus et largement adoptés par les consommateurs, leur utilité n'en est pas moins intrinsèquement limitée ; si je veux vérifier le solde de ma carte de crédit à partir du smartphone de ma femme, par exemple, je ne peux le faire que si j'ai enregistré sur son appareil l'empreinte de mon doigt ou mon visage.

L'utilisation de ces appareils génère également des vulnérabilités, notamment par rapport au piratage chez les personnes âgées : un adulte sans scrupules pourrait très bien, par exemple, s'inscrire sur l'appareil d'un de ses vieux parents et utiliser ensuite son visage pour se connecter aux comptes bancaires de ce senior (et les vider).

Les entreprises préfèrent à ces méthodes l'authentification biométrique sur serveur. Elles font appel à la biométrie vocale et comportementale pour authentifier les clients à tout moment, où qu'ils soient et quelle que soit la manière dont ils s'engagent – et, simultanément, pour détecter les fraudeurs, peu importe le dispositif ou l'identité derrière lesquels ils se cachent.

Les moteurs de biométrie vocale, par exemple, analysent la parole naturelle d'une personne, en extraient des centaines de caractéristiques et les comparent à une bibliothèque d'"empreintes vocales" appartenant à des clients ou à des pirates. Les moteurs les plus perfectionnés peuvent effectuer cette analyse en moins d'une seconde, simplement à partir du son de votre voix quand vous expliquez à un agent qui vous êtes et pourquoi vous appelez. Dès que l'agent se voit confirmer que vous avez été authentifié, il peut se concentrer sur l'aide à vous apporter, sans plus avoir à vérifier votre identité.

Les solutions de biométrie comportementale analysent la façon dont les gens tapent sur leur clavier, glissent les doigts sur leur portable, utilisent une souris ainsi que de nombreux autres facteurs propres à leur comportement numérique. Elles sont idéales pour l'authentification continue dans les canaux de communication numériques, car elles peuvent rapidement repérer les sessions qui ont été frauduleusement détournées.

La biométrie conversationnelle – le nouveau venu dans la prévention du piratage – offre un autre type de paramètre permettant de déterminer si une personne est bien celle qu'elle prétend être. Ces solutions analysent les constructions de phrases des gens, leur choix de mots voire les émojis qu'ils utilisent, et sont dès lors particulièrement adaptées à l'identification du piratage par scripts.

L'authentification biométrique s'avère bénéfique pour

tous

Bonne nouvelle pour les professionnels de la sécurité et de la lutte contre le piratage : 50 % des personnes interrogées dans le cadre de notre enquête se disent plus à l'aise qu'avant la pandémie avec l'utilisation de la biométrie comme moyen d'identification. Deux personnes sur cinq (38 %) déclarent faire confiance à une forme ou autre de biométrie pour s'authentifier.

Les clients apprécient la façon dont la biométrie supprime les contraintes lors de leur interaction avec les marques, car ils n'ont plus à mémoriser leurs identifiants ni à passer par des réinitialisations de mot de passe.

En combinant la biométrie et d'autres facteurs d'authentification dans une approche de la sécurité structurée en couches et supportée par IA, les organisations peuvent évaluer en temps réel le risque de toute interaction. Il en résulte une réduction spectaculaire des temps de traitement moyens, des coûts des centres de contact et des pertes dues au piratage.

Le géant des télécommunications Telefónica a même utilisé la biométrie vocale pour s'assurer que ses clients les plus vulnérables puissent accéder au service prioritaire dont ils ont besoin en cas de problèmes de connectivité. Le système détermine l'âge de l'appelant à partir du son de sa voix et achemine les appels des personnes âgées directement vers un agent disponible pour leur fournir une assistance immédiate.

Construire un avenir plus sûr

J'espère que d'ici l'année à venir l'authentification biométrique sera encore plus répandue qu'aujourd'hui. Et qui sait, à mesure que de plus en plus d'entreprises adoptent, pour protéger leurs clients, des approches en couches, alimentées par IA, il arrivera peut-être un jour où nous n'aurons plus du tout besoin de les sensibiliser.

Tags: Mois de sensibilisation à la cybersécurité, Nuance Gatekeeper, Prévention de la fraude

More Information

Désireux d'en savoir plus sur nos solutions d'authentification?

Découvrez comment Nuance combine l'authentification biométrique et la prévention par IA, avec Gatekeeper, sa solution unifiée omnicanal.

Learn more

About Brett Beranek

Brett Beranek est responsable de la sécurité et de la biométrie chez Nuance. Avant de rejoindre Nuance, il a occupé, au cours des dix dernières années, divers postes de développement commercial et de marketing dans le domaine des logiciels de sécurité B2B. Brett Beranek possède une vaste expérience des technologies biométriques, notamment en tant qu'associé fondateur de Viion Systems, une start-up spécialisée dans le développement de solutions logicielles de reconnaissance faciale pour le marché des entreprises. Brett Beranek a également une expérience approfondie d'un large éventail d'autres technologies de sécurité, y compris la biométrie des empreintes digitales, l'analyse vidéo pour l'espace de sécurité physique et la technologie de reconnaissance des plaques d'immatriculation. Il est titulaire d'un Bachelor of Commerce, Information Systems Major, de l'université McGill, ainsi qu'un certificat de marketing exécutif de la Sloan School of Management du Massachusetts Institute of Technology.

View all posts by Brett Beranek