What's next

Entreprise

Tendances de sécurité et de prévention de fraude pour 2021

Chaque année, toujours plus d'utilisateurs peu méfiants sont victimes d'un cybercrime ou d'une fraude et la pandémie n'arrange rien avec des volumes sans précédent d'interactions en ligne, d'opérations bancaires ou encore d'achats en ligne. C'est dans ce contexte que nous proposons nos prédictions de cybersécurité pour 2021.

Brett Beranek
Posted 7 Janvier 2021

Chaque année, toujours plus d'utilisateurs peu méfiants sont victimes d'un cybercrime ou d'une fraude et la pandémie n'arrange rien avec des volumes sans précédent d'interactions en ligne, d'opérations bancaires ou encore d'achats en ligne. C'est dans ce contexte que nous proposons nos prédictions de cybersécurité pour 2021.

Les DSI visionnaires vont opter pour l'authentification sans mot de passe avec le double objectif de mieux satisfaire le client et de renforcer la sécurité de l'entreprise

Les consommateurs veulent une expérience numérique facile et sûre, sans mot de passe. Les mots de passe et codes pins à entrer au quotidien (ex : e-mail, guichets automatiques) appartiennent au passé. Maintenant que les consommateurs privilégient les canaux en ligne pour tout ou presque, opérations bancaires, réseaux sociaux, divertissement et achats, ils aspirent à vivre une expérience plus sophistiquée et sûre. Depuis des années, les mots de passe induisent un faux sentiment de sécurité, surtout avec l'explosion du nombre et de la variété des appareils proposant des applis, où il faut sans cesse rentrer les mêmes données, et qui créent des vulnérabilités et le risque de vol. Les entreprises doivent convaincre leurs

clients qu'elles prennent leur sécurité au sérieux. Les consommateurs ont pris la mesure des risques qui entourent leur identité. Ils vont en attendre plus des entreprises avec lesquelles ils font des affaires. Il ne sera plus possible de justifier les décisions par le ROI seul. La question de la sécurité conditionne désormais la rétention et la fidélisation des clients, ainsi que la responsabilité sociale d'entreprise.

La nécessité d'une approche intégrée de prévention de la fraude et d'authentification pour éviter les risques d'une biométrie faillible sur les appareils utilisés

Les clients vont exiger des protocoles de sécurité capables de les identifier à coup sûr sans risquer d'être trompés par un usurpateur. Les technologies qui n'authentifient pas l'identité de la *véritable personne* qui interagit avec les mesures de sécurité sont délaissées. L'authentification par mot de passe, code pin ou confirmée par SMS ne suffit plus. Ces informations sont trop faciles à obtenir. Il faut à présent instaurer des technologies biométriques, de reconnaissance vocale, comportementale, d'empreintes digitales, de rétine, pour sécuriser la présence en ligne. Puisqu'ils utilisent des smartphones depuis plusieurs années maintenant, les clients sont souvent à l'aise avec l'authentification des empreintes et du visage. Malheureusement, la plupart de ces méthodes d'authentification biométrique sur l'appareil n'ont pas de réel impact pour bloquer les fraudeurs. Non seulement, il n'est plus possible de savoir à coup sûr qui a créé l'empreinte biométrique et les empreintes sont limitées à un seul appareil, ce qui empêche de les valider à l'échelle de plusieurs canaux et de les porter d'un appareil à un autre. Toute leur valeur réside dans leur gratuité. C'est la biométrie côté serveur, comme la biométrie vocale, qui est la plus efficace en termes de lutte contre la fraude et de fluidité de l'expérience client.

L'intelligence artificielle de pointe va permettre à la biométrie de régler des problèmes de sécurité de plus en plus complexes

Cette année, Telefónica, S.A., multinationale espagnole des télécommunications et l'un des plus grands opérateurs mobiles au monde, a sollicité Nuance pour le déploiement de la biométrie vocale afin d'analyser les tonalités vocales des clients pour savoir s'ils ont 65 ans et plus. L'opérateur a ainsi pu fournir une protection exceptionnelle contre la fraude à ses clients dont le groupe d'âge les expose davantage à la fraude. La technologie va non seulement permettre aux entreprises de prioriser ou d'adapter leurs services à certaines catégories démographiques, mais aussi de renforcer leurs efforts de prévention de la fraude en ajoutant d'autres contrôles biométriques.

Il faudra redoubler de moyens de sécurité pour lutter contre les nombreuses tentatives de fraude induites par le télétravail

Maintenant que les entreprises privilégient le télétravail à l'instar de ce que *Harvard Business Review* a récemment appelé "The Work From Anywhere Future" (nov-déc 2020), la fraude va surtout viser les télétravailleurs et les agents en première ligne, mais il faut aussi tenir compte du risque de fraude au travail. Des employés sans surveillance, ayant accès à des informations personnelles, pourront être tentés de frauder et voler de précieuses informations

à leur employeur. Les conditions sociales et économiques difficiles sont un terreau favorable pour cette fraude au travail. Forrester Research se fait l'écho de ce sentiment en prédisant que 33% des compromissions de données seront le fait d'initiés, contre 25% aujourd'hui. Les entreprises vont devoir réagir vite pour combattre les imitations vocales (clonage ultra réaliste) et les voix fictives ou deep voices (création par l'intelligence artificielle de discours, accents, tons de voix, pour produire une voix artificielle) et sécuriser comme il se doit les interactions avec leurs collaborateurs. Il faudra aussi que les mesures de sécurité traditionnelles fassent preuve d'une performance optimale avec autant d'individus en dehors des murs et pare-feu de l'entreprise.

La relation client passera essentiellement par la vidéo et le virtuel

Maintenant que les consultations, transactions et interactions virtuelles sont devenues la norme entre les marques et les consommateurs, il est nécessaire que les canaux numériques soient suffisamment sûrs et fluides pour que ces interactions soient satisfaisantes. La relation client par vidéo est une tendance nouvelle dans le contexte de la COVID-19 qui oblige à instaurer la biométrie vocale pour authentifier les clients. Par exemple, constatant la multiplication des transactions virtuelles, la banque IBK (Industrial Bank of Korea) a adopté la technologie de biométrie vocale de Nuance pour proposer une méthode robuste et sophistiquée d'authentification client. Avec des taux de validation 100% cohérents, IBK révolutionne littéralement l'expérience de banque numérique.

2021 pourrait bien ętre une année caractérisée par une plus grande sécurité numérique source de tranquillité d esprit. Les façons de faire traditionnelles, aussi fondamentales et rudimentaires que le mot de passe en ligne, ne suffiront plus. Les systčmes de sécurité biométriques fondés sur des caractéristiques vérifiables, comme l iris de la personne, ses empreintes digitales ou sa voix, vont venir remplacer les codes subjectifs facilement volés et utilisés ŕ mauvais escient. Les entreprises qui généraliseront ces pratiques vont faire faire un saut quantique ŕ leurs protocoles de sécurité et opérer une transition plus douce vers une présence numérique nettement mieux sécurisée.

Tags: Biométrie, Customer Experience, digital security, IA, sécurité numérique

More Information

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