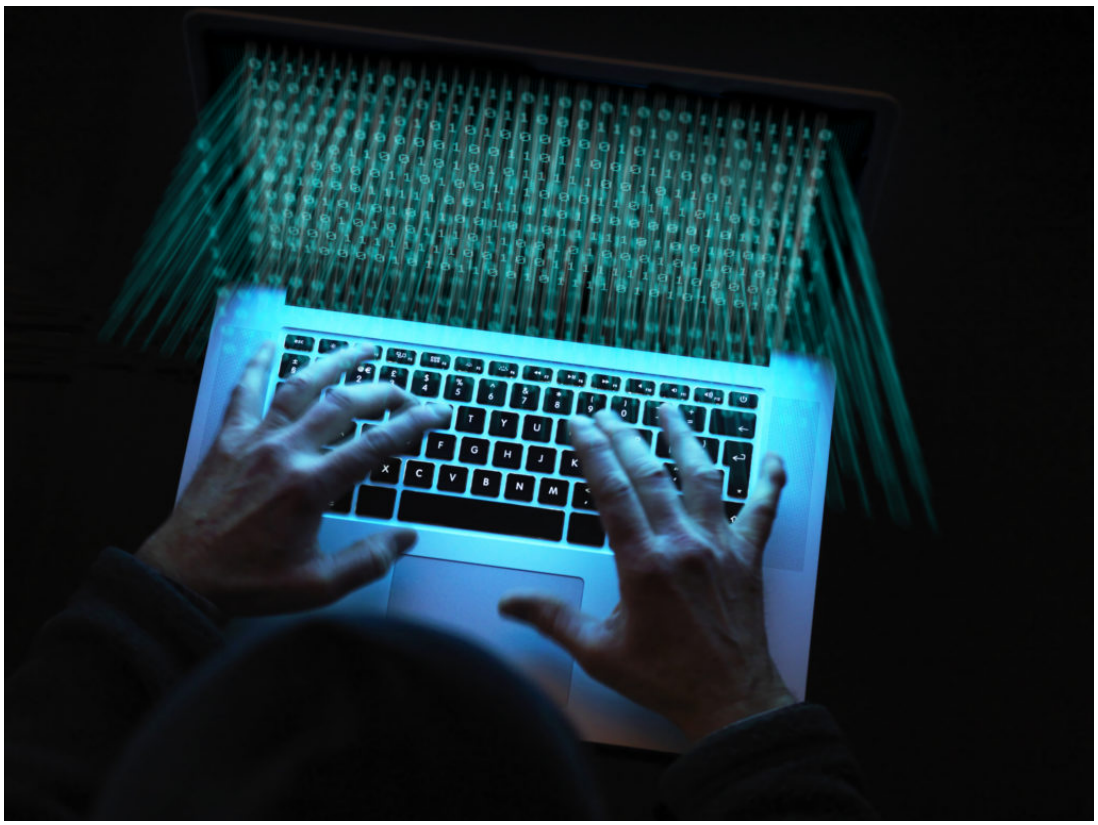
NUANCE | WHAT'S NEXT BLOG

Autentification biométrique et prévention, Engagement client omnicanal

La lutte contre la fraude

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

17 novembre 2020



Après avoir perdu 1 million de dollars en moins d'une heure, Robert Ross, investisseur dans la technologie et père de famille, est devenu un fervent supporter de la prévention des tentatives d'échange de carte SIM ou SIM Swap. Ecoutez l'entretien qu'il a eu avec Brett Beranek de Nuance.

Récemment j'ai eu la chance de m'entretenir avec Robert Ross, investisseur dans la technologie et père de famille. Après avoir perdu 1 million de dollars en moins d'une heure, celui-ci est devenu un fervent supporter de la prévention des tentatives d'échange de carte SIM ou SIM Swap.

Rob nous a raconté les circonstances de l'attaque, les répercussions pour lui-même et sa famille et ce qu'il en retient pour mieux informer les entreprises et les consommateurs.

Tout s'est passé très vite

Fin 2016, un vendredi soir, alors qu'il était chez lui, Rob a reçu un avis de retrait de fonds de la part de sa banque. Il a alors consulté son smartphone et son PC portable. Rob a constaté qu'il n'était plus connecté à sa messagerie. Son smartphone n'était plus non plus en service. Il a compris que quelque chose n'allait pas mais de se doutait pas encore des implications de la situation.

Rob s'est rendu dans son Apple store et a passé des heures à discuter avec l'opérateur, ses interlocuteurs financiers et d'autres contacts encore. C'est là qu'il a entendu parler de la pratique de SIM swapping pour

la première fois.

Rob a en effet été victime d'une attaque type d'échange de carte SIM. Le fraudeur a contacté l'opérateur mobile de Rob en se faisant passer pour lui. Il a convaincu l'agent de porter le numéro de Rob sur un nouveau numéro de carte SIM. Une fois cela fait, il n'avait plus qu'à demander à réinitialiser les mots de passe des comptes d'e-mail et bancaires de Rob. Ainsi le fraudeur a reçu directement les mots de passe à usage unique par sms. En quelques minutes, il avait accès à l'ensemble des comptes de Rob.

Ceci aurait pu être évité si l'opérateur mobile de Rob avait utilisé des facteurs de sécurité biométrique pour vérifier l'identité du demandeur de l'échange de carte SIM. Malheureusement, les processus d'authentification insuffisants de l'opérateur ont permis au fraudeur de prendre le contrôle du smartphone de Rob et de lui voler ses économies d'une vie.

La recherche de la vérité et les conséquences à déplorer

Rob a appris dans les jours suivants que le million de dollars sur son compte avait été converti en bitcoin et retiré intégralement. Imaginez que toutes vos économies disparaissent en quelques minutes. Pour Rob, cela représentait le financement des études de sa fille, son plan d'épargne-logement, sa future retraite. Il était totalement désemparé, ne dormait plus et souffrait émotionnellement. De nombreuses victimes de fraude confirment ces effets dévastateurs, avec parfois à la clé un divorce et de graves troubles pour la santé mentale.

Rob a sollicité plusieurs agences et administrations pour identifier le criminel. Un fraudeur a été accusé de 21 délits au détriment de Rob et de 11 autres victimes. Malheureusement, Rob n'a pu récupérer son pécule.

Bien entendu, c'est toute la famille de Rob qui a souffert. Il a dû apprendre à sa fille alors étudiante qu'il n'était pas sûr de pouvoir payer l'université, qu'ils allaient devoir adapter leur mode de vie à cette nouvelle réalité financière, ce qui signifiait moins de vacances, de loisirs, de temps passé ensemble. De plus, le fait que ses documents personnels aient été compris avait exposé son numéro de sécurité sociale, son numéro de permis de conduire et les détails de son passeport, ce qui pouvait laisser craindre de futures fraudes.

Le choix de la prévention et de l'information

Pendant toute cette épreuve, Rob n'a cessé de s'informer et de sensibiliser les consommateurs et les entreprises à la nécessité de déployer des outils technologiques pour protéger les agents des centres de contact et leurs clients des techniques d'ingénierie sociale. Il a créé une organisation baptisée Stopsimcrime.org pour insister sur l'importance de processus fiables et d'adopter des solutions techniques pour éviter que ces crimes puisent se reproduire.

Client de longue date de Schwab, Rob apprécie qu'ils utilisent l'authentification vocale. « J'ai juste à dire « ma voix est mon mot de passe » et je sais que je suis en sécurité, qu'ils peuvent vérifier les attributs de ma voix et être certains que je suis bien qui je prétends être. »

Rob Ross :

Trouvez-vous que les opérateurs prennent cette question au sérieux alors même que les attaques visent surtout les autres comptes du consommateur (bancaires, e-mail, réseaux sociaux, etc.) plus que ses comptes téléphoniques, internet, tv ? Quels sont les moyens dont Nuance et d'autres disposent pour les convaincre d'agir ?

Brett Beranek :

Les opérateurs de télécom reconnaissent le risque d'échange de carte SIM pour les consommateurs. Mais ils tardent à assumer leur propre responsabilité dans la lutte contre ce phénomène. Le fait qu'ils n'accusent pas de pertes financières majeures et le manque de réglementations expliquent qu'ils tardent à moderniser leur stratégie d'authentification par rapport aux institutions financières ou même aux enseignes de commerce. Heureusement, les choses changent depuis quelques mois et les politiques de

responsabilité sociale d'entreprise des opérateurs incitent à innover sur le front de l'authentification. Pour des entreprises comme Nuance, la meilleure approche consiste à sensibiliser aux risques d'usurpation de comptes et à donner la parole aux victimes. En effet, au final, les opérateurs de télécom se sentiront obligés d'agir parce que cela leur semblera juste, plus que pour éviter des pertes financières jugées insuffisantes.

RR :

Quand les clients n'optent pas pour l'authentification vocale (Voice ID) ou que les entreprises ne déploient pas de solutions Voice ID, que peut-on faire pour limiter le risque d'échange de carte SIM ?

BB :

En l'absence de biométrie vocale, un opérateur peut toujours analyser passivement les appels de clients qui demandent un échange de carte SIM et comparer la voix avec les voix de fraudeurs connus. En quelques secondes, l'agent du service client sera averti du risque et pourra prendre des mesures ou faire monter l'appel à l'équipe en charge de la lutte contre la fraude. Les déploiements de solutions de biométrie vocale sont simples, rapides et efficaces dans la lutte contre la fraude. Toutes les techniques sont alors disponibles, data mining, voice clustering, etc.

To learn more about Rob's story or techniques to combat SIM swapping and fraud, listen to this 30-minute discussion or contact Nuance Communications.

Tags: Fraude SIM

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