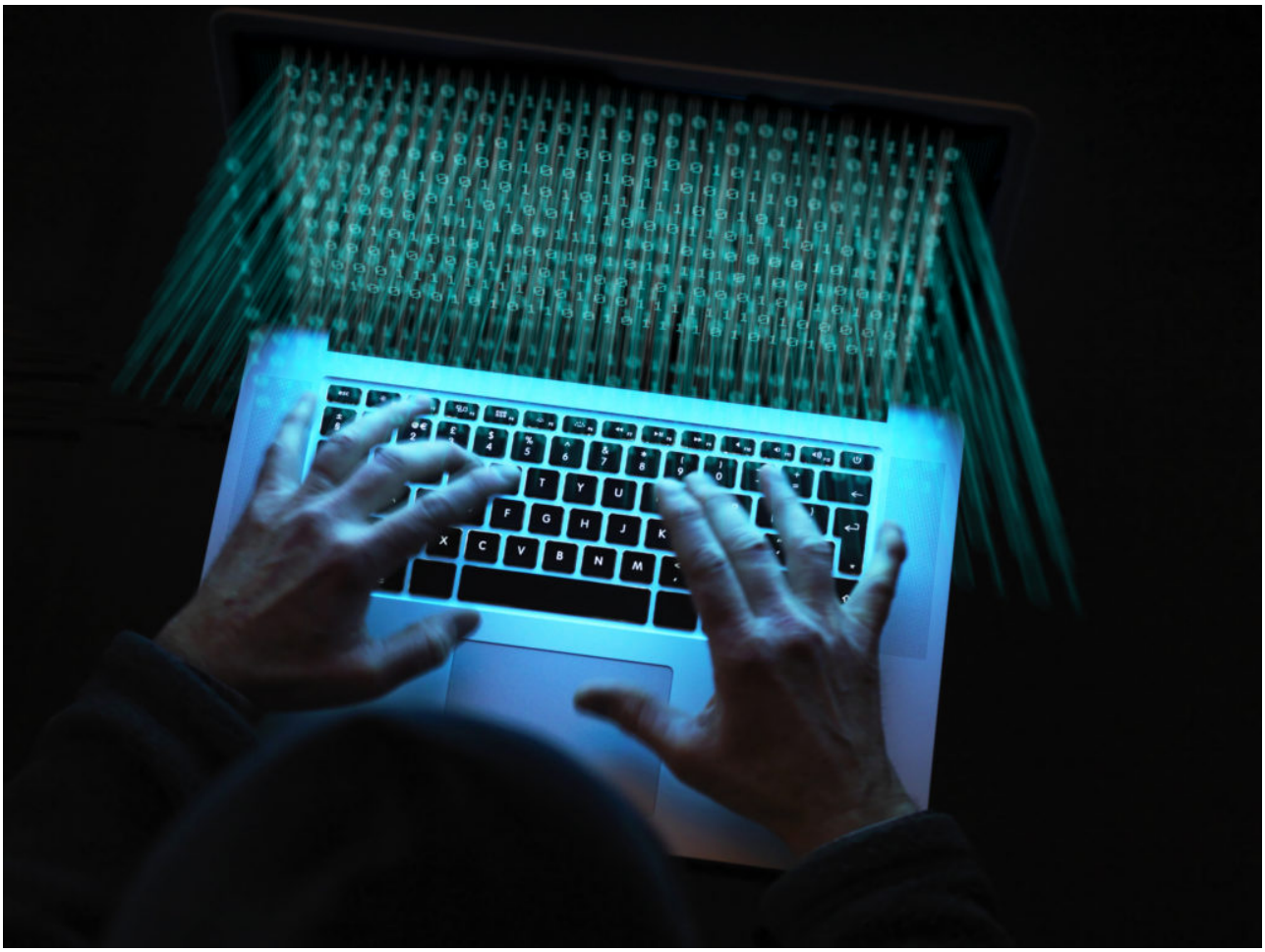
What's next

Enterprise

Die wahren Kosten von Betrug

Robert Ross, Tech-Investor, Familienvater und, durch den Verlust von knapp einer Million US-Dollar innerhalb von weniger als einer Stunde, leidenschaftlicher Verfechter Präventionsmaßnahmen gegen SIM-Swapping . Hören Sie seine Geschichte in diesem von Brett Beranek (Nuance) geführten Interview.

Brett Beranek
Posted 17 November 2020



Kürzlich hatte ich das Privileg, ein Gespräch mit einem sehr speziellen Gast zu führen: Robert Ross, Tech-Investor, Familienvater und, durch den Verlust von knapp einer Million US-Dollar innerhalb von weniger als einer Stunde, mittlerweile auch ein leidenschaftlicher Verfechter von Präventionsmaßnahmen gegen SIM-Swapping.

In diesem Gespräch erzählte mir Rob ausführlich, wie die Betrugsattacke ablief, was sie bei ihm und seiner Familie bewirkte und was er inzwischen über die Hintergründe dieser Masche gelernt hat – mit dem Ziel die Aufklärung von Unternehmen und Verbraucher zu unterstützen.

Alles geschah sehr schnell

Ende 2016 erhielt Rob eines Freitagnachts zu Hause von seiner Bank die Mitteilung, dass Geld von seinem Konto abgehoben wurde. Zu diesem Zeitpunkt blickte er gleichzeitig auf sein Mobiltelefon und seinen Laptop. Rob bemerkte sofort, dass er von seinem E-Mail-Konto abgemeldet war und sah im Sperrbildschirm seines Mobilgeräts, dass kein Telefondienst mehr angezeigt wurde. Er wusste sofort, dass etwas nicht stimmte, hatte aber nicht die geringste Ahnung von den drohenden Folgen.

Rob, der bisher noch nie etwas von SIM-Swapping gehört hatte, besuchte sofort den nächsten Apple Store und führte unzählige Gespräche mit seinem Mobilfunkanbieter, seinen Finanzdienstleistern und anderen Parteien.

Robs Betrugsfall folgte genau dem typischen Ablauf eines SIM-Karten-Swap-Angriffs: Als erstes kontaktierte der Betrüger den Mobilfunkanbieter von Rob und gab vor, Rob zu sein. Dann überzeugte er den Support-Mitarbeiter, die Mobilnummer von Rob auf eine andere SIM-Karte zu transferieren. Anschließend forderte der Betrüger per Textnachricht einen Reset der Passwörter des E-Mail-Kontos und der Bankkonten von Rob an. Da der Betrüger die Mobilnummer der SIM-Karte von Rob mit einer von ihm kontrollierten Nummer ausgetauscht hatte, wurden alle diese Einmalpasswörter an sein Gerät versandt. In nur wenigen Minuten hatte der Betrüger uneingeschränkten Zugriff auf alle Konten von Rob.

Dieser Betrug hätte verhindert werden können, wenn der Mobilfunkanbieter von Rob für die Überprüfung der Identität der Person, die den SIM-Swap anforderte, biometrische Sicherheitsfaktoren genutzt hätte. Doch die laxen Authentifizierungsverfahren des Anbieters ermöglichten dem Betrüger auf einfache Weise, das Mobiltelefon von Rob durch sein eigenes zu ersetzen, auf dessen Konten zuzugreifen und die gesamten Ersparnisse zu stehlen.

Die Suche nach Antworten und die Folgen für die Familie

Rob erfuhr innerhalb der nächsten Tage, dass die gestohlene Million von US-Dollar in Bitcoins umgetauscht und dann in voller Höhe von seinen Konten abgehoben wurde. Man stelle sich einmal vor: Die Ersparnisse eines gesamten Lebens, innerhalb von Minuten verschwunden; die Ausbildungsrücklagen für die Tochter, Bausparanlagen, Rentenpläne. Rob war am Boden zerstört und wusste nicht, wie es weitergehen sollte. Die physischen und psychischen Auswirkungen waren immens; sie reichten von Schlaflosigkeit bis hin zu emotionalen Schmerzen. Rob ist kein Einzelfall, denn viele Betrugsopfer haben ihre Ehe in die Brüche

gehen sehen und Suizidgedanken gehegt. Die Folgen sind verheerend.

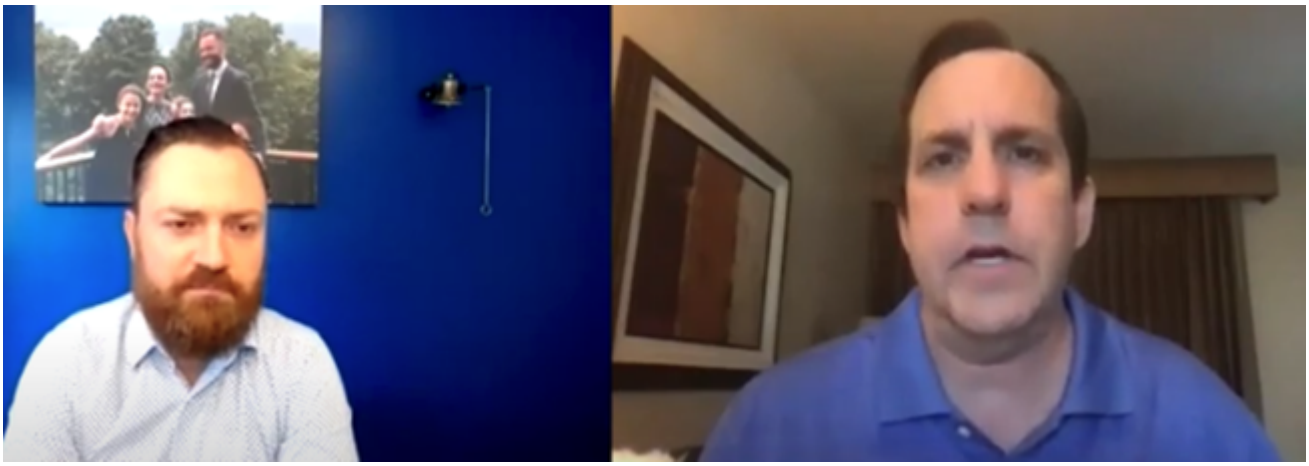
Rob arbeitete gemeinsam mit verschiedenen Behörden an der Identifizierung des Täters. Aktuell steht der Betrüger wegen 21 kriminellen Betrugsfällen in Verbindung mit Rob und elf anderen Geschädigten unter Anklage, doch der Hauptanteil seiner Ersparnisse konnte Rob leider nicht retten.

Rob war aber nicht die einzige betroffene Person; diese Art von Verbrechen hatte Auswirkungen auf die gesamte Familie. Rob führte ein Gespräch mit seiner Tochter, die zu diesem Zeitpunkt auf der High School war. Er sprach mit ihr über seine Sorgen, die Gebühren für die Uni nicht zahlen zu können, und wie sie ihr Leben der neuen finanziellen Lage würden anpassen müssen. Das bedeute, weniger Urlaubsreisen und weniger gemeinsame Zeit. Der Diebstahl aller seiner persönlichen Unterlagen habe aber auch ihre Sozialversicherungsnummer sowie Führerschein- und Reisepassdaten offengelegt und damit Tor und Tür für zukünftige weitere Betrugsversuche geöffnet.

Neuorientierung in Richtung Prävention und Aufklärung

Während seines gesamten Leidensweges befand sich Rob im Lernmodus. Neben seinem eigenen Lernprozess arbeitet er auch daran, Verbraucher und Unternehmen über die zentrale Bedeutung von Technologien aufzuklären, die Call-Center-Agenten eine Gewissheit statt Vermutungen vermitteln und somit sie selbst und den Verbraucher vor Betrügern schützen. Mit dem Ziel, anderen zu helfen, gründete er eine Organisation mit dem Namen Stopsimcrime.org. Das Kernanliegen dieser Organisation ist die öffentliche Verbreitung der wichtigen Funktion von soliden Prozessen und technischen Lösungen für eine endgültige Unterbindung von Betrugsversuchen dieser Art.

Rob merkte noch an, dass er als langjähriger Kunde von Schwab sehr froh darüber sei, dass dieses Unternehmen die biometrische Spracherkennung zur Authentifizierung einsetze. „Ich muss nur sagen, meine Stimme ist mein Passwort. Dieser zusätzliche Schritt, meine Stimme und deren Merkmale als Nachweis meiner Identität zu nutzen, vermittelt mir ein Gefühl der Sicherheit.“



Frage aus dem Publikum

Glauben Sie, da primär die Konten der Kunden (Finanzen, E-Mail, soziale Medien usw.) statt die Konten ihrer Anbieter (Kabel, Telefon, Internet, Fernsehen) betroffen sind, dass die Telekommunikationsanbieter aktuell dieses Problem ernst genug nehmen, um es aggressiv anzugehen? Falls nicht, was wäre die beste Methode für Technologieanbieter wie Nuance, daran mitzuarbeiten, diese zu überzeugen, dass es an der Zeit ist, zusätzliche Maßnahmen zu ergreifen?

Antwort von Brett

Telekommunikationsunternehmen kennen das Risiko eines SIM-Karten-Swap für Verbraucher. Es braucht jedoch Zeit, bis sie ihre eigene Verantwortung bei der Bekämpfung dieses Phänomens erkennen. Die fehlende Bedrohung erheblicher finanzieller Verluste und der Mangel an Regularien zählen mit Sicherheit zu den Hauptgründen, dass Telekommunikationsanbieter bezüglich einer Modernisierung ihrer Authentifizierungsstrategie nicht so schnell reagieren wie Finanzinstitute oder sogar Händler. Glücklicherweise erkennen wir diesbezüglich in den letzten Monaten ein Umdenken. Telekommunikationsfirmen beteiligen sich mittlerweile vermehrt am Kampf gegen Betrüger, und das Konzept der sozialverantwortlichen Unternehmensführung ebnet Innovationen den Weg an die Authentifizierungsfront. Der beste Ansatz für Unternehmen wie Nuance ist, weiterhin über Risiken einer Kontokaperung aufzuklären und den Opfern eine Stimme zu verleihen. Die Telekommunikationsanbieter werden schließlich aus dem Gefühl heraus handeln, das Richtige zu tun, und nicht mit der Motivation, finanzielle Verluste zu begrenzen, denn diese allein sind nicht signifikant genug für eine Verhaltensänderung.

Frage aus dem Publikum

Was könne Sie für eine Minimierung des SIM-Swap-Risikos tun, falls Kunden sich gegen eine biometrische Stimmauthentifizierung entscheiden oder Unternehmen keine Mittel für die Investition in eine schrittweise Einführung dieser Technologie haben?

Antwort von Brett

Selbst wenn Kunden sich nicht für den Service Stimmbiometrie registrieren, hat der Telekommunikationsanbieter die Möglichkeit, jeden Anruf, bei dem der Kunde eine SIM-Änderung anfordert, zu analysieren. Die Stimme des vermeintlichen Kunden wird dann mit den Stimmen aus einer Liste von eindeutig identifizierten Betrügern verglichen. Innerhalb von Sekunden wird der Support-Mitarbeiter informiert, ob ein Risiko besteht. Er kann dann spezifische Maßnahmen ergreifen oder den Anruf an die zuständige Abteilung weiterleiten. Dieser erste Ansatz der Stimmbiometrie für eine Betrugserkennung hat sich als sehr wertvoll erwiesen und lässt sich schneller und einfacher implementieren. Mit dieser Form der Implementierung sind alle Techniken der Betrugserkennung, wie Data-Mining oder Voice-Clustering, verfügbar.

Tags: Biometrie, SIM swap

More Information

	Hören Sie sich das 30-minütige Gespräch an. Erfahren Sie mehr Learn more

About Brett Beranek

Brett Beranek is responsible for overseeing every aspect of the security and biometric business at Nuance. Prior to joining Nuance, he has held over the past decade various business development & marketing positions within the enterprise B2B security software space. Beranek has extensive experience with biometric technologies, in particular in his role as a founding partner of Viion Systems, a startup focused on developing facial recognition software solutions for the enterprise market. Beranek also has in-depth experience with a wide range of other security technologies, including fingerprint biometrics, video analytics for the physical security space and license plate recognition technology. He has earned a Bachelor of Commerce, Information Systems Major, from McGill University as well as an Executive Marketing certificate from Massachusetts Institute of Technology's Sloan School of Management.

View all posts by Brett Beranek