What's next

Enterprise

The fight against fraud

Brett Beranek
Posted November 16, 2020

Recently I had the privilege of sitting down with a very special guest, Robert Ross, a tech investor, father, and now fervent SIM Swap prevention advocate after losing just shy $1M in less than 1 hour at the hands of a fraudster.

The goal of our discussion was really to allow Rob to share how the attack unfolded, how it affected him and his family, and what he's been learning behind the scenes to help educate both enterprises and consumers.

It happened very quickly

On a Friday night in late 2016, Rob was sitting at home and received a notification from his financial institution for a withdrawal request. At the time, he happened to be looking at both his mobile phone and his laptop. Rob noticed in real-time he had gone from being logged in to his email to being logged out, and looking at his mobile phone, he noticed he had no service. Right away, he knew something was gravely wrong but did not have any idea about the impending implications.

Rob immediately went to his local Apple store and spent countless hours with his carrier, financial service providers, and other stakeholders. It was then that he learned about SIM swapping for the first time.

Rob's case follows a typical SIM swap attack. First, the fraudster contacted Rob's mobile carrier, pretending to be Rob. Then the fraudster convinced the support agent to port Rob's phone number to a new SIM number. Once complete, the fraudster requested password resets on Rob's email and financial accounts and had them sent by text message. Because the fraudster had swapped the SIM associated with Rob's mobile number to one he controlled, all of these one-time passwords were sent to the fraudster's device. In mere minutes, the fraudster had full access to all of Rob's accounts.

This could have been prevented if Rob's mobile carrier had been using biometric security factors to validate the person's identity trying to make the SIM swap. Instead, the carrier's lax authentication processes allowed the fraudster to easily take over Rob's phone, gain access to his accounts, and steal his life savings.

The search for answers and the resulting impacts

Rob learned over the next few days that the million dollars in his account were converted from USD to bitcoin and withdrawn in its entirety. Consider for a moment your entire life's savings gone in minutes. For Rob, this meant his daughter's college fund, home savings, retirement planning were all erased; he felt gutted and uncertain where to go. The physical and mental impacts were significant and ranged from lack of sleep to emotional agony. Rob's not alone; in fact, many fraud victims have seen devastating effects, such as divorce and severe mental health effects.

Rob worked with several agencies to forensically discover the perpetrator. There is one fraudster facing 21 felony counts for the crime against Rob and 11 other victims, but unfortunately, the lion share of Rob's nest egg was not recovered.

Rob was not the only person impacted; these types of crimes affect the entire family. Rob shared a poignant conversation with his then high school age daughter that he had concerns about paying for college, and how their lifestyle had to be adjusted given their new financial reality, which meant fewer vacations, time together, holidays, etc. and how the breach of all his personal documents exposed her social security number, driver's license, and passport information, potentially opening the door for further fraud in the future.

Turning to prevention and education

Throughout this entire ordeal, Rob has been working to educate himself, consumers, and organisations on the importance of technology tools that can remove the guesswork for contact centre agents and protect them and their customers from social engineering. He started an organisation to help others called Stopsimcrime.org. His main goal is to message the importance of reliable processes and technical solutions, so this never happens again.

Rob shared he is a long-time customer of Schwab and was pleased to know they use Voice ID for authentication. "All I have to do is say, '*my voice is my password*,' and it provides me with a feeling of security, that they have gone the extra step to protect me, using my voice and voice attributes to verify I am who I say I am."

Rob Ross:

Do you feel that most telco's are currently taking this issue seriously enough and addressing it

aggressively enough given that it primarily impacts other accounts owned by the consumer (financial, email, social media, etc.), but has little impact on their telco accounts (cable, phone, internet, tv)? If not, what is the best way for technology providers like Nuance to help convince them that it is time to take additional action?

Brett Beranek:

Telcos do recognize the risk SIM swap poses to consumers. But it is taking time to see them recognize their own responsibility in fighting this phenomenon. The lack of significant financial losses and regulations is certainly one of the main reasons why telcos aren't moving as quickly as financial institutions or even retailers when it comes to modernizing their authentication strategy. Fortunately, in the past months, we are starting to see a shift. Telcos are starting to join the fight against fraudsters and corporate social responsibility is driving innovation on the authentication front. For businesses like Nuance, the best approach is to keep educating on the risks account takeovers represent and to give a voice to victims. Because in the end, telcos will act because they feel it's the right thing to do, and not only on the basis of mitigating financial losses, which is not significant enough on its own to drive change.

RR:

Where customers choose not to opt into Voice ID and/or organisations don't have the investment to deploy scaled Voice ID solutions, what can you offer to minimize SIM Swap risk?

BB:

Even if legitimate customers aren't enrolled in voice biometrics, it is still possible for a telco to passively analyse every call where a customer asks for a SIM change and compare the voice with a list of known fraudster voices. Within seconds of the call, the customer service agent will be notified there is a risk and can take specific measures or escalate the call to the fraud team. This fraud first approach to voice biometrics deployments has proven to bring a lot of value while being a quicker and easier deployment. In such a deployment, all fraud investigation techniques become available, such as data mining or voice clustering.

To hear more about Rob's story or what companies can do to protect against SIM Swap and fraud, listen to the 30-minute discussion.

Tags: biometrics, fraud prevention, SIM swap

More Information

Want to know more?
Visit us to learn more about Nuance's voice biometrics solutions
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