SearchCloudSecurity.com

Frank Abagnale: No technology can beat a social engineering attack

by
Rob Wright
Site Editor
Published: 07 Jun 2016

Today's identity and access management technology may be improving, but Frank Abagnale says nothing will beat a good, old fashioned social engineering attack.

Abagnale, whose exploits as a young confidence man were made famous in his best-selling book Catch Me If You Can *and the movie adaptation from Steven Spielberg, was the opening keynote speaker at the Cloud Identity Summit 2016 in New Orleans this week. After being arrested and jailed at the age of 21 for writing more than $2 million in forged checks and committing numerous social engineering schemes, he began assisting the federal government with forgery and fraud investigations and has worked with the FBI for more than 40 years. Abagnale is considered one of the foremost authorities in fraud, forgery and secure authentication.*

He's also been involved with several security technology companies over the years. Abagnale spoke at the Cloud Identity Summit about his work with a new security startup, Trusona, which launched this year with what it calls "insured authentication" technology for financial transactions. Trusona's TruToken card reader device plugs into smartphones and can provide several layers of authentication to guarantee the identity of the person making the transaction.

Abagnale spoke with SearchCloudSecurity at the event about Trusona, the evolution of social engineering, and why, in his words, "technology breeds crime." Here are excerpts from the conversation with Abagnale.

How did you get involved with Trusona?


Frank Abagnale

Frank Abagnale: I met Ori Eisen [founder and CEO at Trusona] about 15 years ago when he was head of global security for American Express, and I quickly realized he was probably the most knowledgeable guy I had ever met in my career when it came to cybercrime and technology. So 15 years ago I told him he really needed to leave American Express and go start his own business. He had some great ideas for fraud detection technology and I told him he really needed to go out and do that. And eventually he took my advice and started a company called 41st Parameter. And in doing so, the day he made that decision, he asked me, "If I do this, will you be my advisor?" and I said absolutely. So 10 years later he had 160 employees and the company's technology was used by just about every bank, airline and retailer in the United States. A couple years ago he sold the company to Experian for more than $300 million. And I figured that would be the end of Ori; he'd be done and retired. But after only a few months he called me up and said he wanted to do what I always said we should do. And what I've said is there will never be a foolproof system until you can come up with the ability to guarantee 100% that a person on the other end of a transaction is in fact that person. He said "I think I can do that." So he asked me to come back as his advisor, and after 10 years together at 41st Parameter we got back together and started working on this technology.

What was your role in building Trusona's technology?

Abagnale: The best description was one Ori gave to a reporter in Hong Kong. The reporter said, "You have a long-term relationship with Frank, but he doesn't write code." And Ori's response was, "Yeah, and I'm not a criminal." Ori said that our whole career together has been playing chess together. He comes up with the technology and says, "Here's what I developed" and then I go and try to beat or screw it up somehow, and then we go back and try to fix it until we get to the point where it's foolproof. And that's basically what we do. And he's developed some incredible technology with Trusona and I think it's the first time ever that, whether you're operating a nuclear power plant or a CIA agent sending information, there's technology that can guarantee that the person you're talking to is that individual. And what's nice is it's not complicated to understand or use.

But it's not completely foolproof, correct?

Abaganale: Yes. Whenever we go through these exercises of the technology, and someone says, "Wow, you can't beat it," I have to say, "Well, there are two exceptions." First, there is no technology in the world, nor will there ever be, that beats social engineering. So if I call you and pretend I'm Bank of America and tell you to go through all the steps for Trusona and you follow my instructions, then I'm going to get to you. And the second is if I had a gun to your head, and I told you to do this, then you're going to do it. We try to account for some of those things [with TruToken]. So, for example, you can pick a certain card that if you swipe it, it will tell Trusona that you're under duress.

Why hasn't something like this been done before? Why hasn't the financial services industry addressed these issues before they became a problem with things like the SWIFT attacks?

Abagnale: I've been at the FBI for 40 years. I've worked with banks all over the world. I deal mainly with crimes against the federal government today. So if you look at Medicare and Medicaid, last year they paid out over $100 billion in fraudulent claims. The IRS paid out $5.6 billion [in fraudulent college credits] last year. The government has become an easy target because they don't have the technology that the banks have in place; they don't have a board of directors, they don't have stock holders and they're not in the business of making a profit. So they're a very easy target, and they have all the money. The banks at least try to do the best they can to prevent these things from happening, but a lot of times they don't put the effort into preventing the right things from happening. It seems like every breach that occurs is because someone in the company did something they weren't supposed to do. Those things don't need to occur. It's human error. And you almost have to eliminate the human being, because that's the weak link.

How do you account for a social engineering attack? It seems like these threats are much more complex these days. Should people always be skeptical?

Abagnale: It's not about being skeptical. It's just being smart enough to know the signs and do the right thing. I read an article a couple days ago about an unfortunate case where a woman in Australia went swimming at night in a lagoon that had signs that said don't swim, crocodiles are everywhere. And a crocodile attacked her. And one of the politicians in the area said, "You cannot legislate against human stupidity."

It feels like cybercriminals know that there are a lot of people doing stupid things and that they can take advantage of it. But do you think social engineering techniques are more advanced today than 30 or 40 years ago?

Abagnale: Some people used to say that I'm the father of social engineering. That's because when I was 16 years old, I found out everything I needed to know -- I knew who to call and I knew the right

questions to ask -- but I only had the use of a phone. People are still doing the same things today 50 years later, only they're using the phone, they're using the mail system, they're using the internet, email, cloud. There's all this other stuff, but they're still just doing social engineering. And that's the biggest threat to something like Trusona, and that'll never go away.

How much has the technology today made it easier for cybercriminals and hackers to take advantage of people?

Abagnale: Technology, to me, breeds crime. You look at what I did 40 or 50 years ago, and it's 4,000 times easier to do today. When I forged checks, in order for me to print a full color check from, say, a major airline, I had to have a Heidelberg printing press, which would take up the size of [the keynote ballroom]. It's a million-dollar press and you've color separation, negatives, plates, type settings and all of that. But as you know, today I can open a laptop, go to the company's corporate website, capture their logo and their images and design a beautiful, full-color check in 10 minutes. And then print it out on a color printer. So technology has made things a lot easier, and all criminals have done is conform to that. The important thing is this: You can't develop technology and say, "Here's my foolproof technology, you can't beat it, goodbye." You have to constantly go back and stay on top of it all the time. You can't just develop it and walk away and be done with it. You have to constantly be aware of things that can happen to it and how people are going to try to beat it.

07 Jun 2016