Caught him: An interview with cyber security expert and "Catch Me If You Can" Author, Frank Abagnale, Jr.

by Cory Davenport, Contributing Writer
February 8 2019 11:23 AM


DEUS MEUS
ET OMNIA
OSF®
HEALTHCARE

GODFREY - Famous author and current cyber security expert Frank Abagnale, Jr. came to Lewis and Clark Community College Thursday night to discuss a bit about his most-noted work "Catch Me If You Can" as well as the evolving world of cyber security.

Here is an interview with Abagnale conducted by Riverbender.com. Questions asked to him are in bold.

What does it take to catch up with the trends in cyber security?

You know I've been with the FBI now for 43 years, so when I went to the Bureau back in 1974 out of prison, there was no cyber crime. Everything was about counterfeiting and forgery and things like that, and that I knew a lot about, but as time went on, things changed, and I had to change with those things, as crime started to change, I had to learn how the new crimes worked, always asking myself, “how would I use this if I had this technology? How would I defeat this if I was trying to do it?” and my whole career has been based on just moving along with that – as crime moved along, I'd learn those crimes and how those crimes worked and what motivates people to do them and how they do them and all that, but again, yeah, you have to stay one step ahead at all times.

Have you seen anyone reach your level like when you were doing that kind of thing?

Yeah, I have to laugh sometimes when they say – when I read that they say – I'm “The World's Greatest Con Man, and I say, “OK, I was a single 16-year-old kid. It was two-and-a-half million dollars, which most of it was recovered because I was too young to spend it all.” However, there are people who take billions of dollars – the Madoffs of the world – and of course most of the politicians in Washington, I couldn't strike a match to with that, so you know, I'm not the world's greatest con man.

What is the new cutting edge of what people are using? What would we be surprised about?

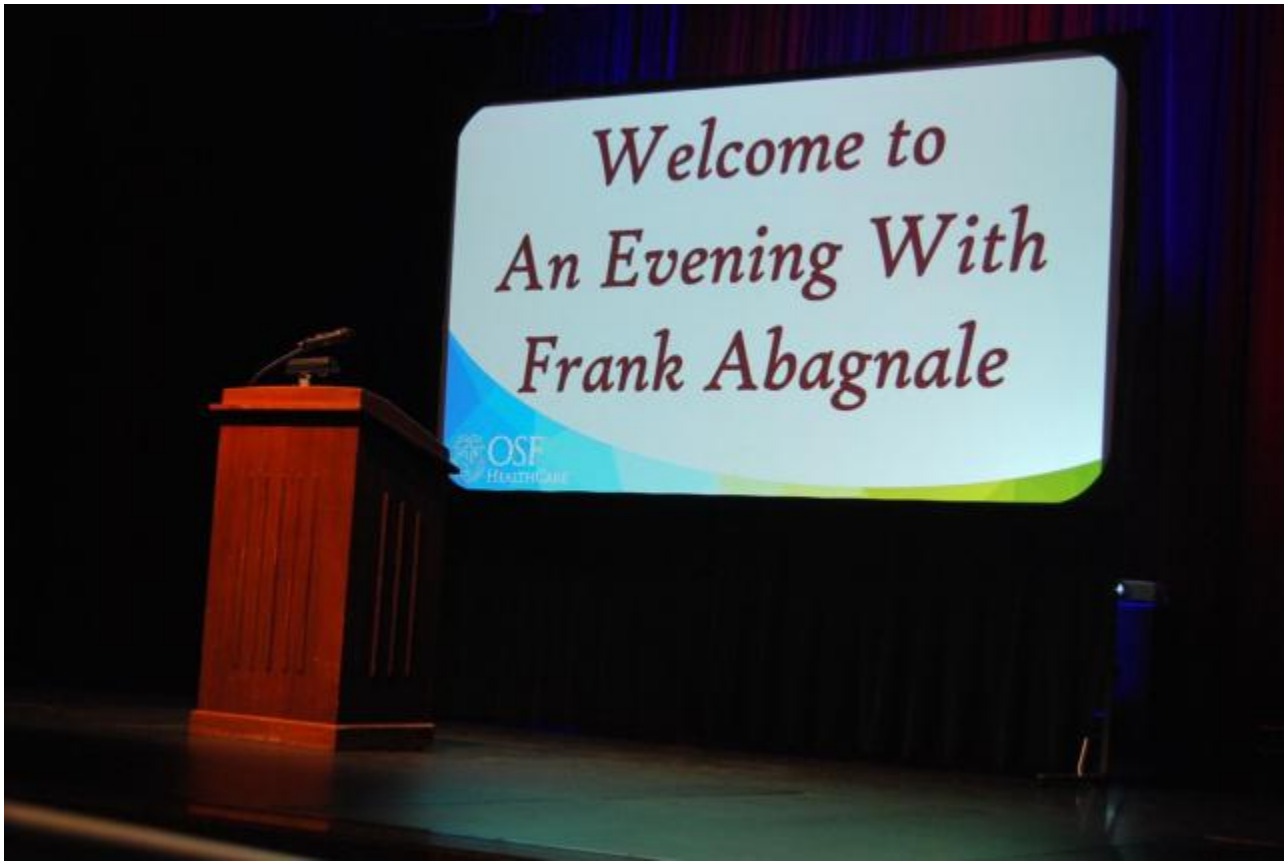
I think it's just that we keep developing devices that we use for convenience purposes without taking it to the final step and asking “how would someone misuse this?” So when you have a device in your home that you can talk to, and ask it “what's the weather today?” and order things from Amazon – it's voice-activated. So, I can easily hack into that and I hear everything that you say in your house. I could turn the cameras on you, so that I could see everything that's going on in your house. All these things are developing. Because they're not expensive, a lot of the technology that would be needed to protect them is not in there. So people take these things and think they're safe, but they're very easily manipulated. So that's probably the scariest part – that we never take everything to the final step.

So what do you think we'll have to do to counter the 5G "Internet of Things?"

Well, I think we have to start worrying about the fact that we can now shut someone's pacemaker off, but we have to be within 35 feet of them. We can pull over a vehicle, and shut it off because that's 240 computer components in it. We can lock someone in a car, turn on the airbag, we can lock the windows. You got to put that in the wrong hands of someone before you expand from 35 feet, which is now the limit to maybe a mile, maybe five miles, maybe 500 miles. Those are the things that are going to get real scary. Technology is only going to get scarier and be more misused. It's not going to get better.

How much do you know about the technology of things? Do you know about their usage, or also about their innards and coding?

I work as an adviser to a company that – I do this with a lot of technology companies – they are the ones that do develop the technology, but at the end, they want to make sure it's secure, so they hire me to test it. So the CEO of a company called Trusona, which is a no passwords technology, he once said to an NBC reporter, "now what about Frank Abagnale? You worked with him for many years, he was your adviser on some of these projects, but Frank Abagnale doesn't write code." He said, "no, he doesn't write code." But he said "I'm not a criminal. I will never be able to think like Frank Abagnale thinks." He said, "I can develop the best software in the world, but only he can decide whether he can defeat it, beat it, or find a way around it." So he said, "I always tell people my relationship with Frank is that we play chess. So I develop something and then he comes in and goes, 'you know, I could do this, and I could get around that.' So I go back and fix it and he comes back and says 'well I know you built this wall, but I could still do this. Until the day he says to me, 'I think it might shut it up for now, but he said I still bring him back every year, because in a year something else may have come up." That's, you know, that's the whole thing, you continue to have that mind, or you don't have that mind to look at things, and with the FBI, I've worked with agents in my life on cases that they look at as one way, and I look at it totally in a different way.


Welcome to
An Evening With
Frank Abagnale
OSF
HEALTHCARE

Do you ever think about going back into that world a little bit?

Being married for 40-plus years, and having three sons with five grandchildren, my oldest boy is an FBI agent. You know, I think – as I told someone earlier today – people are amazed by what I did between 16 and 21. I, personally, at 70 am totally amazed that I did it, went to prison, but where my life went after that is what did it.

So, how did the FBI receive you after all that?

I think Steven Spielberg did a wonderful job in the scene where what's supposed to be the Washington Field Office where I walk in. Of course, back in those days, it was all males, they were all white, they were Harvard graduates, Yale graduates, there were lawyers, there were accountants, where they all stood up with animosity when I walked into the room, and Steven Spielberg showed that. So it took years to get their trust and build credibility, but having taught at the FBI Academy has helped a great deal. It's part of what I do, because every new agent that comes in there has had me as an instructor, so he knows me from day one, he knows who I am, and I think it's helped and gone a long way in building credibility. I've taught now two generations of FBI agents, so when they go out in the field, they all know who I am, and they know my background.

Are there any safe technology measures that you can say are actually catching up with the tech itself?

We have to eliminate passwords. Passwords are for tree houses. Passwords were invented in 1964, so I was 16 years old, I didn't even start doing anything, and here we are at 70 they're still using passwords to gain access. So, Trusona is a great, new technology backed by Microsoft that eliminates the need for passwords, and that is very fast catching on. So you may have seen an ad on TV with Serena Williams where she's jogging and doesn't have a wallet or anything, but she sees a necklace she likes, so she goes over to the Chase ATM and she presses an app on her phone, and she gets her money. She has no card, she has no password, but she uses her phone to identify who she is, and that kind of technology is very quickly catching on, so I think in the next two or three years, we'll see the elimination of passwords – not only in this country, but around the world.

Is the U.S. leading the way in technology? What about other powerhouses like Japan, South Korea and the rise of China?

I think they're right behind us, and I think that we need to make sure we do stay ahead. I think they do a lot of things that we do no recourse for. So, for example, when you look at some of these hacks like Microsoft, Marriott and the OPM hack, they're obviously state-sponsored hacks, but instead of doing anything about it, we accept it. I always say, “hey, why don't we go shut off all the streetlights; the traffic lights in China for 20 minutes to let them know that we can do that?” We don't do that, so they're not really afraid of us, but I think we should be more aggressive when they do do something just to counteract that.

So do you investigate state-sponsored things like that?

I get involved with a lot of breaches and things that fall under what I do. I work with agents in the field. Sometimes those companies bring me in to ask me what happened and what's going on, so since the TJ Max breach back about 14 years ago, I've been involved in a lot of those breaches since then, and one things I've found is that – and I mentioned that to the audience today – every breach occurs because somebody in that company did something they weren't supposed to do, or somebody in that company failed to do something they were supposed to do. Hackers don't cause breaches. People do. Hackers just wait for doors to open. These companies leave all their doors open, so these hackers get the information...

People are basically honest, and because they are honest, they don't have a deceptive mind. So, when they get an email that is a fishing email, they think it's legitimate. They're not sitting here going, “oh this could be a scam, somebody is trying to get information from me.” None of those things ever enter their mind, unless you've taught them and you've shown them how they work, then they understand it. So, I deal a lot with elderly folks. I've been involved with the AARP as their ambassador for years. I do a podcast out of Washington every Wednesday that deals with crimes against seniors. And basically, I have learned if I teach seniors about these scams and how they work, they don't fall for them. Those robo-calls, Publishers Clearing House scam, grandparents scam, but I I tell them this is how it works – I just finished writing a new book. It will be out in August from Random House about scams against the elderly. When I write a book, I give all my advance and all my royalties to a charity. So I gave all that money to AARP. They have a fraud-watch network to put it to build that network. But the book is a great book – simple to read, but if you're an older person, you'll read about all these scams, so when the phone rings, and they say it's the IRS, you'll say you know this scam and have read about it. That's what it takes – is educating people.

What about countries around the world, do you keep up with their security?

Yeah, a lot of all of these – that Marriott breach, that was a state-sponsored breach. So was that OPM breach or that Chinese breach. Those were a lot of countries. The whole thing – I was telling somebody this today – the whole concept of a “con man” like I was back in the 50 years ago, which stood for “confidence man.” You had to be well-dressed, well-spoken, charming. People had to like you, they had to trust in you. That's what it was all about. Today the people who commit these crimes are sitting in their pajamas with a cup of coffee on their laptop in their kitchen in Moscow. They never see the victim. The victim never sees them, so there's no emotion involved. Even the con man might have said, “I got enough from him, I can't rip this guy off anymore. I took a lot of his money, and it's starting to bother my conscience. These people have nothing, because they have no visible contact with you, whatsoever. So that is why so much of it is so bad that they'll take every penny you have.

Leanne Guthrie also contributed to this story.