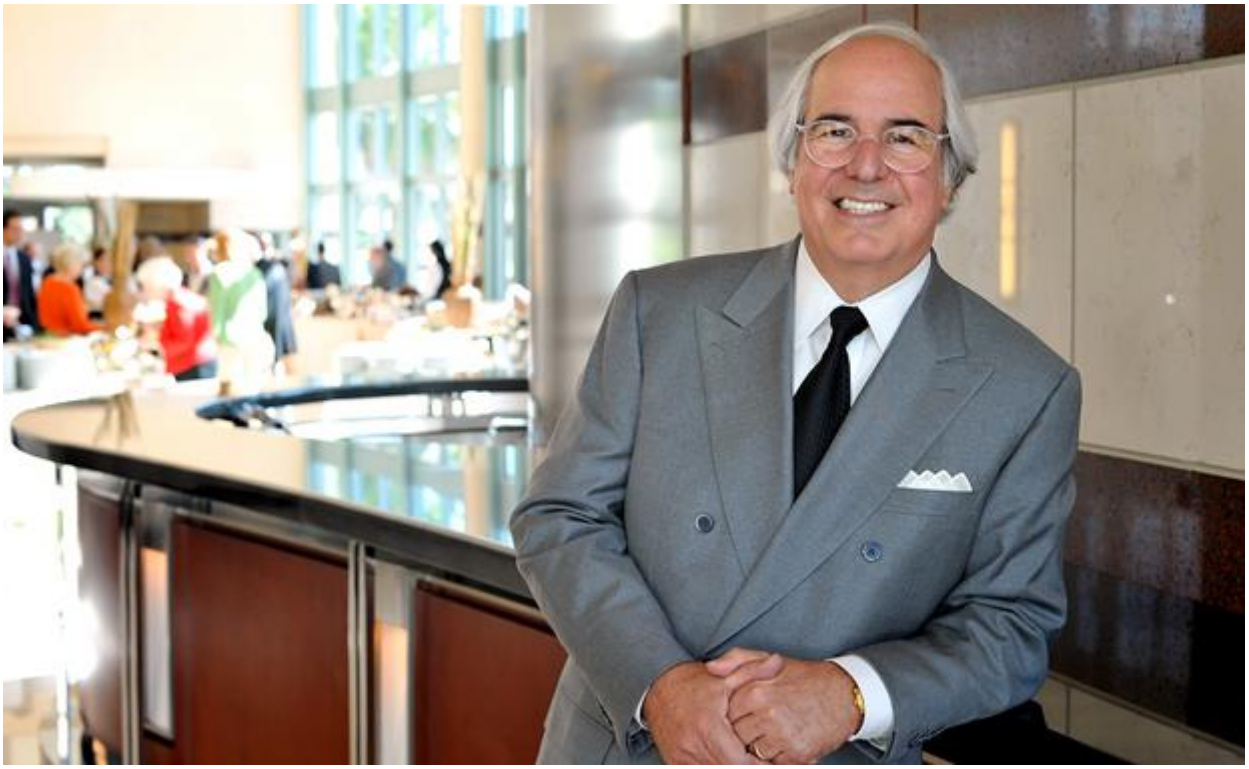
Catching Up with Frank Abagnale: “Technology Breeds Crime”

One of the world’s most respected authorities on data security shares how you can protect yourself from fraud, identity theft and other cybercrimes. BRON



A SECURE FUTURE: “Big data analytics helps uncover patterns that would be hard for any human to determine.” Photo: Abagnale

Mediaplanet: We know about malware and viruses. What other digital threats do we need to know about?

Frank Abagnale: Advanced persistent threat, or APT, is a rising attack vector that targets a specific company or even a department or a person within that company. The idea is to craft a spear phishing email that will look legit to open and infiltrate the system from within.

MP: What are some of the myths surrounding digital security?

FA: The belief that shopping online or banking online is riskier than doing it by phone, by paper or in person is hugely untrue. Many of the shoppers who think they should avoid shopping online, could very easily have their personal information compromised by shopping at a brick and mortar that was breached. The risk is everywhere and not only for online shoppers. Just think about Target.

MP: What advances in technology has pushed the digital security industry forward?

FA: The ability to recognize computers without leaving any residue on them, thus, not letting the bad guys cover their tracks easily. Also, big data analytics helps uncover patterns that would be hard for any human to determine.

MP: Where do you see the digital security industry progressing?

FA: More and more systems will become contextually aware of what are they protecting, from whom and when. Additionally, new biometric technologies will allow for better authentication in the future.

MP: How have you seen the Heart Bleed Bug impact digital security?

FA: My answer is that we all lived serendipitously for the two years the Heart Bleed Bug went on undetected. Thus, good risk managers always assume that their data has been breached, that a vulnerability such as Heart Bleed exists and then devises their security and risk management strategy in response. Do you truly believe that right now all the bugs have been fixed?

MP: How have you seen the digital security evolve during your lifetime?

FA: What I did almost 50 years ago is now 4,000 times easier to do than when I did it. Technology breeds crime, always has and always will. Fifty years ago, to print checks I needed a Heidelberg printing press which used to cost about $1 million. There were color separations, negatives, plates, typesetting and chemicals to make plates. Today, this can be done in the matter of minutes on a laptop computer, security paper from an office supply store and a laser printer.

"Good risk managers always assume that their data has been breached, that a vulnerability such as Heart Bleed exists and then devises their security and risk management strategy in response."

Fifty years ago, I would not know where the company banked, their account number or the authorized signer. Because we live in a world with too much accessible information, all one has to do today is pick up the phone, call the accounts receivable department of a company and ask for the wiring instructions. They will gladly tell you where they bank, their account routing information and account number. If you call back and ask for corporate communications, they will be happy to send you a copy of their annual report. On page 3 you will find the signatures of the CFO and Controller.

MP: We are familiar with your story from Catch Me if You Can, How did you end up working as government security consultant?

FA: I was paroled from federal prison in February of 1974. As part of the terms of my parole, I was to assist the federal government and law enforcement agencies in their fight against white collar and financial crimes. My obligation to those terms ended about 34 years ago. I have been working with the FBI for over 38 years now. One of the things I am most proud of is that my son is an FBI agent.

MP: What advice would you give to those looking to be more secure online?

FA: Change your passwords regularly, so even if they were stolen, they may not be useful. Once a month, or once a quarter, change it to something that you can remember, and yet cannot be guessed easily. Don't use dictionary words like "baseball" and don't use just numbers. What works best is to think about a sentence, and then derive a password from it that contains alphanumeric and special characters. So, if you watched the movie "Catch Me If You Can" and liked it… you can derive a password like CatchMeWas10!!!, TomHanksMakes$$$, or IsntLeoTheMan.