In 1964, Frank Abagnale, a runaway teen in New York City, was running out of options. Authorities were after him for truancy and writing bad checks. He was broke and struggling to survive, but he possessed three tremendous, natural gifts—a brilliant mind, a prodigious talent for social engineering, and prematurely grey hair that made him look a little older than his peers. So at 16, Abagnale obtained a Pan American Airlines pilot uniform, created a fake airline ID, and began a remarkable five year crime spree.
Between the ages of 16-21, he flew an estimated 1 million miles for free on commercial aircraft in the cockpit jump seat (no, he didn’t fly the planes), touching down in 26 countries around the world. While still legally a minor, Abagnale created several identities and passed himself off as a pediatrician in Georgia (no children were hurt), an attorney in Louisiana (where he worked a year for the State Attorney General), and a college professor in Utah (teaching sociology at Brigham Young University). Also during this 5-year span, he forged $2.5 million in checks, was “wanted” by the FBI, and matured into one of the world’s most daring con men and escape artists of all time.

Crime doesn’t pay, of course. Abagnale was finally arrested in 1969 in France at age 21 on an Interpol warrant from Sweden. After serving time in France and Sweden, he was sentenced to 12 years in U.S. federal prison. Four years into that prison term, at the age of 26, the U.S. government offered to release Abagnale on the condition he works for the FBI for the remainder of his sentence. He did that, and much more.

Today at 64, Frank Abagnale is one of the world’s most respected authorities on forgery and embezzlement. Mr. Abagnale has been associated with the FBI for over 35 years. He lectures extensively at the FBI Academy and for the FBI field offices. Abagnale is a faculty member at the Department of Justice National Advocacy Center. More than 14,000 financial institutions, corporations, and law enforcement agencies use his fraud prevention programs. And in the past 31 years, Abagnale has worked with 65% of America’s Fortune 500 companies.

FS-ISAC KnowledgeShare recently “caught up” with Mr. Abagnale.

**AS EMPLOYEES, WHAT DO WE NEED TO KNOW ABOUT PHISHING?**

**FA:** The main thing is that security really is your responsibility. The greatest harm that can come to a financial institution and its customers is through an employee who does something he or she wasn’t supposed to do, and unintentionally creates an opportunity for cybercriminals. We can develop all of the technology in the world and roll out the most sophisticated and secure technology, but we must rely on human beings to operate it. And if we have just one person who is a weak link in the chain, the whole system is at risk.

**WHICH COUNTRY’S HACKERS ARE THE MOST DANGEROUS FOR BANKS? IS IT THE CHINESE? RUSSIANS?**

**FA:** In 37 years of working with the FBI and teaching at the FBI academy, I’ve never found the master criminal. There is no master criminal. There’s no master hacker sitting in Nigeria or Hong Kong. For every breach I’ve investigated, worked on, and written about – whether it’s for MasterCard, the Veteran’s Administration, Hotels.com, LexisNexis, etc. – each one happened because someone at that company did something they weren’t supposed to do.
SO BEHIND EVERY SUCCESSFUL HACKER IS A CARELESS INSIDER?

**FA:** Right. What master hackers will tell you when you interrogate them, is that they typically can’t access a financial institution’s network. It’s basically impossible. The technology in place makes hacking into it almost impossible without “help” from an inside person. Many banking corporations employ thousands of people, and that means at some point, someone may inadvertently open the door. So all the hackers do is sit and wait for it to open.

**WHAT DO YOU MEAN BY AN EMPLOYEE "OPENING THE DOOR?"**

**FA:** In companies that have experienced breaches, you find that an employee clicked on an email they shouldn’t have opened, or they went online and clicked on a pop-up ad to look at something they shouldn’t have looked at. These things can happen at companies where employees are told many times not to do these things, and they’ve taken training, but they’ve gone ahead and done something to open the door anyway.

**CAN YOU SHARE AN EXAMPLE OF AN EMPLOYEE WHO UNWITTINGLY AIDED A HACKER?**

**FA:** Sure. Last year someone hacked into South Carolina’s Department of Revenue and stole the tax returns of 3.5 million of the state’s citizens. This is about everyone in the state, including myself. These hackers have my Social Security number and my wife’s Social Security number. And for those citizens with minors at home, they have their children’s Social Security numbers. If we paid our taxes by check, the criminals now know where we bank, and they have our account numbers and signatures. If we paid by credit card, they have our credit card numbers.

**AN EMPLOYEE WAS AT FAULT FOR THE HACK?**

**FA:** On the day that incident occurred, the local news interviewed me. The reporter said, “The Department of Revenue claims they didn’t do anything wrong and somebody just hacked into their system and stole this information.” I said, “No, Miss. First of all, that’s impossible. Someone at that office had to do something for this to occur.”

...AND? WERE YOU RIGHT?

**FA:** Two months after the interview, the Secret Service concluded their investigation of the hack. It turns out an employee took a laptop home that they weren’t supposed to take, got online, and someone got into their system.

**HAVE THE HACKERS STOLEN FROM YOUR ACCOUNTS?**

**FA:** Not yet. The governor of South Carolina provided every citizen of the state with a credit monitoring service for two years. But most criminals who steal masses of data actually warehouse it for about three years. Just like wine, the longer you hold onto stolen data without using it, the more valuable it becomes.

**WOULD YOU SAY TECHNOLOGY IS MAKING US MORE OR LESS SECURE?**

**FA:** There’s no question that technology breeds crime. It always has; it always will. It’s 5,000 times easier today to commit fraud than it was back in the 1960s when I did it. When I forged checks 40 years ago, it required a $1 million printing press. I had to build scaffolding on the side of it so I could
operate it by myself. There were color separations, negatives, plates, typesetting chemicals. Today’s crook simply opens a laptop, goes to a corporate website, captures their logo, designs a check, goes to the company’s annual report and gets the CFO’s or CEO’s signature, scans it and puts it on the check, and then calls the bank and asks for their routing/wiring information. In some ways, technology makes it much easier for criminals. But we can also use technology to combat crime. We just always have to stay one step ahead of the criminals.

IS THERE ANYTHING ELSE WE CAN DO TO FOIL PHISHERS AND SOCIAL ENGINEERS?

FA: Yes. Be careful when using social media. Employees don’t want to have the attitude that, “I’m secure at work, but at home I can do whatever I want.” I strongly recommend carrying that security mindset into your home, and sharing it with your children, family, and friends. For example, there’s software anyone can buy online called “Phone Creeper.” If you’re on Facebook and you have a cell phone, Phone Creeper allows someone to track all of your movements. Right now there are about 7.5 million children under the age of 13 on Facebook, and about 5 million of them are under 10 years old. So if your child is on Facebook and has a cell phone, someone with this Phone Creeper software can track your child’s location.

ANYTHING ELSE?

FA: If I have Google’s PittPatt software on my iPhone and I take a picture of you – let’s say you’re a complete stranger who walks by me in the airport – PittPatt will take me to your Facebook page in 7.5 seconds. And if I get to your Facebook page and your home page tells me where you were born and your date of birth, I’m now 98% on my way to stealing your identity. So I always tell young people, first of all, limit the amount of photos you have on your Facebook page, because the more photos you post, the better the facial recognition software works. Also, avoid posting a frontal, straight on, passport-type photo of yourself, because facial recognition software gets better and better every day.

"There's no question technology breeds crime. It's 5,000 times easier to commit fraud today than it was back in the 60s..."