



'Prevention, Verification, and Education'

FRANK ABAGNALE ON FRAUD

Frank Abagnale is a renowned Cybersecurity and Fraud Prevention Expert and Bestselling Author, while his story is the inspiration for Steven Spielberg's 2002 film, *Catch Me If You Can*, starring Leonardo DiCaprio and Tom Hanks.

Over the last forty years, Frank has shared his rare blend of knowledge and expertise with hundreds of organisations, financial institutions, and government agencies around the world. He continues to lecture extensively on combatting cyber fraud and has been associated with the FBI for over four generations as he continues his mission of fraud prevention and making the world a safer place.

Here he shares his personal philosophy of prevention, verification, and education when fighting fraud in an information and data-heavy world.

“We have seen scams increase during the pandemic by more than 400% in the United States”

Q You have an incredibly unique life story which people still to this day are fascinated by. How did your experiences between the ages of sixteen and twenty-one shape the life you now live?

A I know that most people will have seen the movie, the Broadway musical, or read the book, and that they are fascinated by all the things I did as a teenage boy between those ages of sixteen and twenty-one, but I am now seventy-two! When I look back on my life, I am amazed, not by what I did as a teenage boy, but by the fact that I was caught, which I knew I would be, and I went to prison and served time, and then for the last forty-four years I have worked with the federal government and the FBI. During my career, I have conducted over 3000 seminars around the world, and I have had the opportunity to develop a great deal of technology that went into paper and plastic which is used all over the world for securing credit cards, checks and negotiable instruments. For the last twenty years, I have spent a great deal of time advising technology companies on creating software for financial institutions for fraud detection, which is used in 80 countries around the world. I've also done a lot of work with seniors to make sure that they are not being taken advantage of through all types of scams.

I have been married to my one and only wife for forty-four years. I have three sons, of which one son is an FBI agent who has been in the FBI for fifteen years, and I have six grandchildren. So, when I look at my life, I am kind of amazed that I did those things and where my life has brought me.

Q Technology is often a solution to fraud, but it has presented unprecedented opportunities for attack and fraudulent activity in recent years; how would you advise businesses test their technologies and technological capabilities for ways in which it might be used negatively against them?

A This is especially important and is not done nearly enough around the world. We develop a lot of technology, especially consumer related technology, without ever going to the final step and asking the questions: How would someone defeat this technology? How would someone misuse this technology? We

“Criminals are not looking for challenges, they are looking for opportunities, if you make it easy for them to steal from you, they will”

are in such a rush because of return on investment for marketing purposes, that we push all these things out of the door without ever doing anything about it.

In the private sector, outside of the government, I have spent most of my time as an adviser for technology companies because they were smart enough to realise that before they released their technology into the market place, they needed to understand how someone could misuse their technology. And that is exactly what I do – I play chess with technology. I go into companies and look at how I can manipulate their software and then they go away and fix the problem.

I explain to people all the time that there is no 100% safe or secure technology. If you believe that you have a fool proof system, you have failed to take into consideration the creativity of fools, there will always be someone who is able to get around the technology – what I try to do is tell that company that we have to make it so difficult that it would be compared to moving the Empire State building over two blocks in two weeks. Criminals are not looking for challenges, they are looking for opportunities; if you make it easy for them to steal from you, they will. You can make it difficult for them to do that and that is what I have always tried to accomplish when working with companies.

My whole philosophy for the last forty-four years of educating people is based on three things, **prevention, verification, and education.**

Insurance is great, but reputation is not insured. Once you lose your money, you're not going to get your money back, so it would be much wiser not to lose it to begin with and that's why prevention is so important.

Verification, because today you have to verify everything.

And finally, education, which is the most powerful tool when fighting crime. If you can educate people about fraud, then they will be prepared.

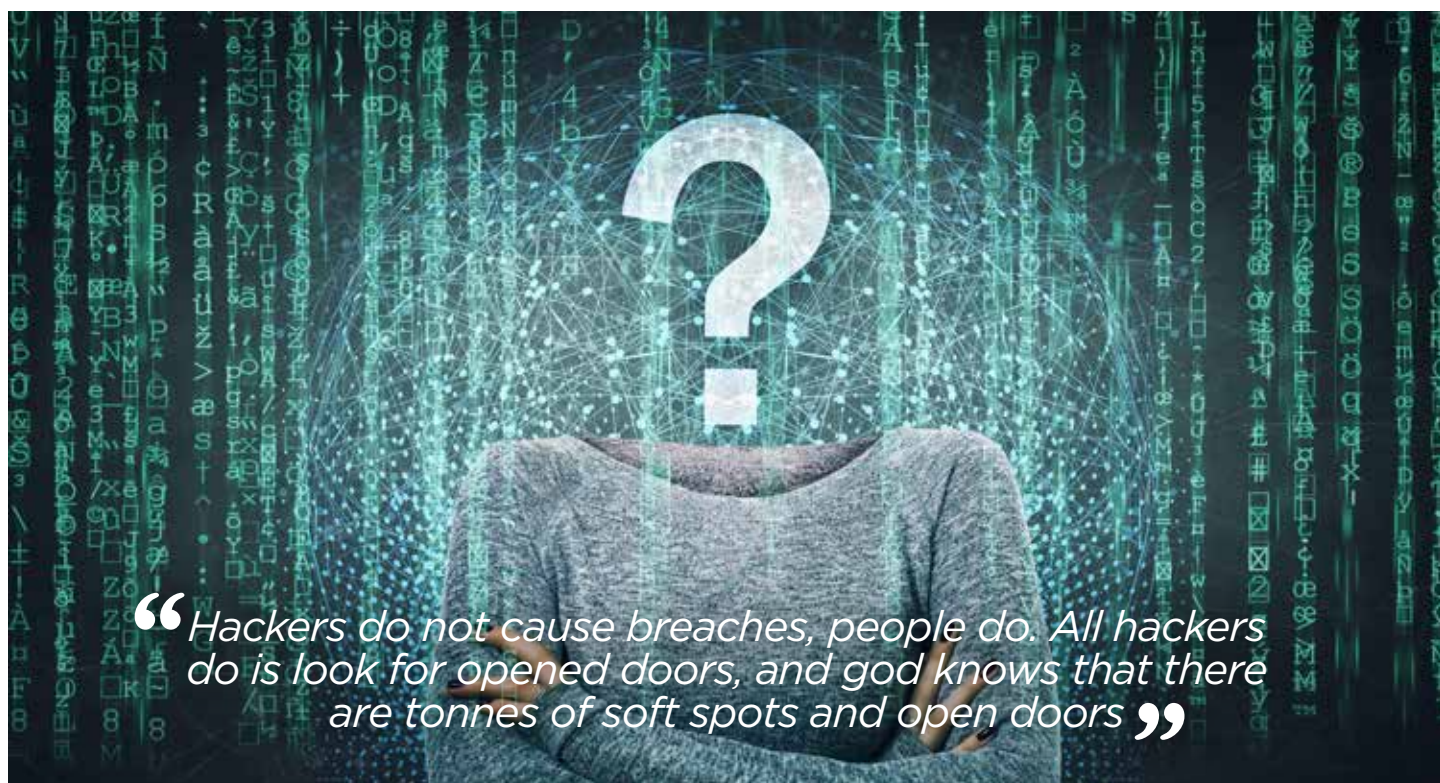
Q The Internet of Things and sensors are widely used throughout peoples' homes and their personal devices to gather data regarding customer behaviours – while that type of connectivity is useful, are we actually creating pockets of vulnerability and increasing customer risk? And do you think those businesses that utilise that type of software are aware of their responsibility in doing so?

A Absolutely. There is no question whatsoever that the UK and the European Union have done a great job of keeping some of that information private and keeping an eye on companies that are trying to track information. The US could have learned from their actions.

I tell people all the time, if you have a device in your house and you talk to it, it is very easy to manipulate that device so that I can hear everything that you're saying in your house. All our devices are connected to the internet which means that they are open to someone anywhere in the world who could breach them. I explain to people that every breach, and believe me, I have worked many breaches in my work with the FBI, going back to TJMAXX some years ago, all the way up to our current breaches of Facebook, Capital One Bank and Marriott Hotels; every breach occurs because somebody in that company did something that they weren't supposed to do, or someone in that company failed to do something they were supposed to do. Hackers do not cause breaches, people do. All hackers do is look for opened doors, and god knows that there are tonnes of soft spots and open doors.

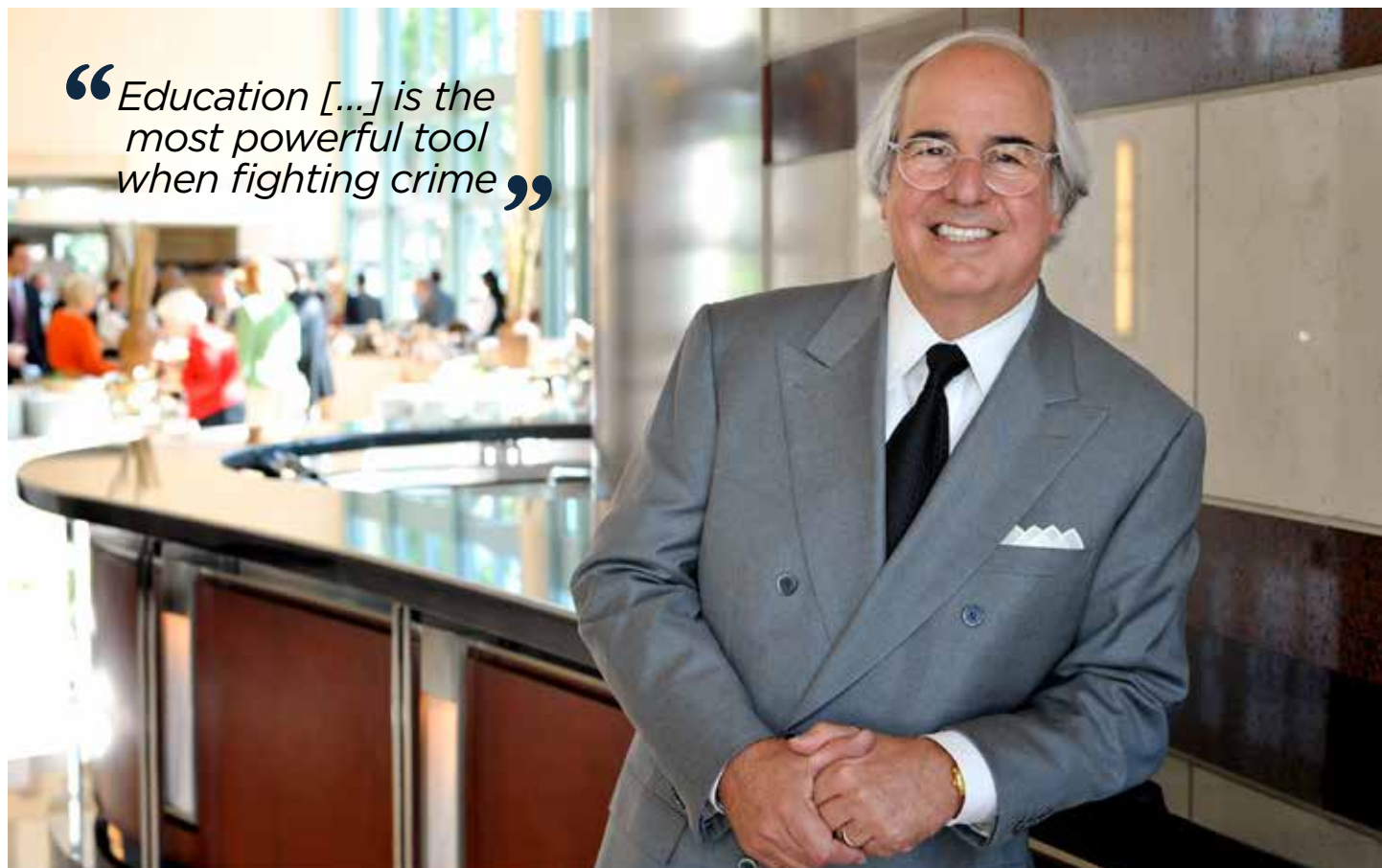
Q In terms of breaches made by employees, whether negligently or purposefully, how can companies prevent these types of breaches? Does there need to be more investment in training to get the balance right between technology and people?

A There certainly needs to be more investment in educating people, but it comes down to the attitude of people. Many



“Hackers do not cause breaches, people do. All hackers do is look for opened doors, and god knows that there are tonnes of soft spots and open doors”

“Education [...] is the most powerful tool when fighting crime”



businesspeople assume that this won't happen to them or they don't want to spend the money, so they leave themselves open to be victimised. They become the loose links or soft spots that criminals look for.

My advice is to make sure you have backups as that is the best strategy for recovery. Update your software; use company issued devices, prepare for the worst case scenario, use strong passwords, employ multi-factor authentication, reject requests from unknown sources, and tell your employees to take care when clicking on links, opening attachments and downloading software.

Remember, criminals are always looking for opportunities, they are not looking to spend a lot of time overcoming a challenging system, but when we open all these doors, they have unlimited opportunities.

Q We are facing a global pandemic, and a crisis is the perfect time for fraudsters to increase their attacks. What effect is Covid-19 having on fraudulent activity, especially in terms of cybersecurity?

A You have to remember that scammers follow the headlines. We have seen scams increase during the pandemic by more than 400% in the United States. But what has really surprised me during this pandemic, which I have never seen before, and I have been dealing with scams for four generations, is that there are a lot of malicious scams. These are scams that make no one any money; there is no profit, only malicious intent. Sometimes scams aren't about money but about people trying to cause physical harm and disruption.

Q In previous interviews, you've spoken about always looking ahead and anticipating crimes of the future – what do you think you will be investigating five years from now?

A It is going to get scary, because, as I remind people all the time, up until now, cybercrime has all been about money and data – it is either about stealing money or stealing data, because data is

money. It is a financial crime, but unfortunately, I believe over the next five years or so, it is going to be much more of a black crime.

The day of the conman, the confidence man, is gone. He was well dressed, well-spoken, had good vocabulary, a likeable character, and he swindled people by getting them to believe in him and trust him. He had a little bit of compassion and emotion because he got to know you. But, today, you are dealing with someone that is in their pyjamas on their laptop in their kitchen thousands of miles away. They will never see you and you will never see them. There is no emotion or compassion, and so consequently we see these horrible things that go on and I'm afraid that that will only get worse.

Q You have spent over four decades working with the FBI, has there ever been a security system you couldn't get around or is there always a way in?

A Unfortunately there is always a way in. It is a question of difficulty and whether it is worth the time and energy to get in. As I stated before, it is my belief that there is no fool proof system - if you believe you have a fool proof system, you have failed to take into consideration the creativity of fools. What you should try and do is make your system so secure that no matter who looks at it, that it is not worth the time and energy it would take to get around that system.

Q If you could give one key piece of advice to the insurance industry what would it be?

A I always remind people that if you make it easy for someone to steal from you, the chances are that someone will, so don't make it easy. Be a little smarter, be a little wiser, and a better businessperson today than you were twenty years ago – you have to be.

Frank W. Abagnale
is an Author, Lecturer and Consultant.