of the con artist and the rise of cybercrime

– a former conman and the subject of 2002 movie Catch Me If You Can
security

Frank Abagnale's early life story has been told many times. A former conman who specialised in impersonation and forgery, he was portrayed by Leonardo DiCaprio in the 2002 film *Catch Me If You Can*. His story has also been told as a book, a musical and is drawn upon in TV series *White Collar*.

At the age of 16, Abagnale posed as a pilot for Pan Am Airlines in order to wangle free flights. He later pretended to be a doctor, before masquerading as an attorney – just some of the eight different identities Abagnale claims to have assumed. Throughout this time he became a master forger of cheques, defrauding banks of millions of pounds. He was arrested at the age of 21 in France and spent six months in prison there, six months in a Swedish jail and was then deported to the US (not before he'd escaped from the aeroplane intended to transport him). After serving five years of his 12-year sentence, he was paroled on the condition that he helped the FBI uncover cheque forgers. He has since made a career as a security consultant, working closely with the FBI for almost 40 years, and launching his own company Abagnale & Associates.

Abagnale talks to WIRED about his past life as a conman, identity theft, the criminal opportunities made possible by the web and the efforts made by governments to fight cybercrime.

How would the technology available today have affected your ability to con people in your early years?

What I did was almost 50 years ago and it's about 4,000 times easier today to con people than when I did it. To forge a cheque 50 years ago, you needed a Heidelberg printed press, you had to be a skilled printer, know how to do colour separations, negatives, type-setting... those presses were 90 feet long and 18 feet high. There was a lot of work involved in creating a cheque.

fancy four-colour cheque in 15 minutes on your computer. You then go down to an office supply store, buy security cheque paper and put it in your colour printer.

Fifty years ago, information was hard to come by. When you created a cheque you had no way of knowing where in reality British Airways' bank was, who was authorised to sign their cheques and you didn't know their account number. Today you can call any corporation in the world and tell them you are getting ready to wire them money and they will tell you the bank, the wiring number, the account number. You can then ask for a copy of the annual report and on page three are the signatures of the chairman of the board, the CEO and the treasurer. It's all on white glossy paper with black ink – scanner ready art. You then just print it onto the cheque.

Technology breeds crime and we are constantly trying to develop technology to stay one step ahead of the person trying to use it negatively

of how technology breeds crime?

If I'm in the airport in London and I take out my iPhone and take a picture of you walking through the airport, I can use PittPatt – an application that used to be used by the FBI but has been bought by Google – for facial recognition. If you are on Facebook [or you are identified by your image online somewhere else, for example a company website] I can find out who you are within seconds. If you happen to tell me where you were born, your date of birth and that kind of information then I'm 98 percent of the way to stealing your identity.

So I tell a lot of the young people that you never want to put a frontal photo of yourself on your Facebook page. Use a photo with a group of friends or doing sport, but never a straight-on funnel photo of yourself.

Another example is a scam involving apps that allow you to scan and deposit cheques using an iPhone. A few weeks ago we had a man out in Kansas City who sold his home and was paid with a cheque for $583,000 (£386,000). He asked for a glass of water and then scanned the cheque with his phone to deposit it into his bank account. When the lady came back, he told her that he'd changed his mind and would prefer for her to wire him the money. He then handed the cheque back and so the buyers then wired him another $583,000.

Sometimes I wonder where these people were forty years ago when I needed them!

I think people often develop these tools and then they don't think about the negative side of them. I wish they would spend a bit of time thinking about how their technology could be used for bad purposes and then try and eliminate that possibility.

Would you say that the art of conning people in the pre-digital age, where you have to charm people and look them in the eye, has died?

Yes. In the old days, a conman would be good looking, suave, well dressed, well spoken and presented themselves real well. Those days are gone because it's not necessary. The people committing these crimes are doing them from hundreds of miles away.

The victim never meets them so it doesn't matter what he or she looks like. It doesn't involve charm any more, it's simply a matter of knowing how to use a computer and get into systems and so on.

Do you have any respect for some of the capabilities?

For example, I've been involved with the FBI for 37 years. Every case involving cybercrime that I've been involved in, I've never found a master criminal sitting somewhere in Russia or Hong Kong or Beijing. It always ends up that somebody at the company did something they weren't supposed to do. They read an email, went to a website they weren't supposed to. So they opened the door that allowed the person to get in. It's not that these people are that talented but they wait knowing that with a company of 10,000 employees someone is bound to open the door. They just wait for that door to be open.

How do you make companies understand this?

When I go into companies, I throw [USB] sticks on grounds saying 'confidential'. And then I can see all of the people who pick those sticks up and plug it into their computer. When they do that, they are greeted with a

ıd you failed". Then I explain that I could have easily got into their system. curity breach at a company it's because someone was doing something they ays have a human link that's the failure.

see as most worrying?

e is when we start getting countries using cybercrime to shut down nications systems, the internet etcetera. But crime goes to wherever there's

ice (IRS) paid out more than $5 billion in false tax returns. People use online for taxes under someone else's name and then they get the refund due to the By the time they file their own tax return, they've already paid out money and the victim has to wait around a year to get things straightened out.

Most of the perpetrators are down in Florida and Miami – mainly gangs – street gangs who have started to realise there's a lot more money doing this than in drugs. It's a lot easier and there's a lot less risk involved.

If you were still a con artist, which of the tools available now would you use?

When I did the things I did, I did them all between 16 and 21. I'm 64 years old now. When I did it I made $2.5m over a period of five years. If I was stealing identities today, I'd be looking at more like $20 million (£13m) or $50 million (£33m). If you can 'become' somebody else, what you can do is unbelievable, whether it's getting mortgages in their name, credit, jobs in their name. It's just wide-open. The internet is a wonderful thing but it opens the door to many crimes so you have to stay ahead of it.

How well are governments coping with fighting this sort of crime?

The problem you have today is that crime has become truly overwhelming and in the US white collar crime was over $950bn. It was almost a trillion dollars. So you have everything from Wall Street fraud to embezzlements to cybercrime and then you have to deal with terrorism as well. So a lot of crime is going on but there are very few resources to deal with it. This means that you have to privatise, so if you are a credit card company you are after the guys stealing $5-10 million from you. Criminals know that if they stay under certain thresholds, nobody is going to come after them. The fact that cybercrime is global makes it particularly hard. If I know someone in Russia is getting information and breaking into a bank's computer system, trying to get the Russian police to go after that person is almost impossible.

How can individuals protect themselves?

It's an education thing. I speak at a lot of universities and people are always worried about Facebook and when I explain how to use it properly they immediately go back and make those changes.

Imagine if you are 14-year-old kid and you just read a book about the Nazis. So you get on Facebook and say, "wow, I think the Nazis are cool" or "I love the Nazis". Then six years later you apply to university or a job and

What is the biggest myth about your story perpetuated by the movie *Catch Me If You Can*?

I wasn't very involved with the making of the film, but I thought Spielberg did a great job and only changed very minor things. In real life I had two brothers and a sister, he chose to portray me as an only child. In real life there was a back and forth relationship with my father (Christopher Walken in the film) but in real life once I ran away from home I never saw my parents again and my father passed away while I was in prison. And when I escaped from the aircraft I escaped from kitchen galley where they service the plane, but in the movie they had me escape from the toilet. But other than very minor things, I thought he stayed very straight to the story.

Do you ever get sick talking about the film and your early life as a conman?

I served my time and came out of prison when I was just 26, and have worked with the government for 37 years. what I did before that. So even when I'm interviewed for a newspaper article ened 40 years ago than what I've done with my life since then.

ife] negatively against me, it's just all they really know about it.

So what are you most proud of from the last 37 years?

I was very fortunate because I live in a great country where everybody gets a second chance so you can make a mistake, pay your dues, get up, brush yourself off and start all over again. I am most proud that I've been married to my wife for 37 years, brought three beautiful children into world and been a great father and husband. My proudest moment was probably when my oldest boy finished law school and went on to become an FBI agent. It was just beyond my imagination that – with my background – my own son would become an FBI agent.

***

This story originally ran ahead of Abagnale speaking at Advertising Week Europe in March 2013.

TECHNOLOGY CYBERCRIME CYBERSECURITY FBI

By JAMES TEMPERTON

TV | 30 May 2017

Global reign of terror: map plots every terrorist attack and death in real-time

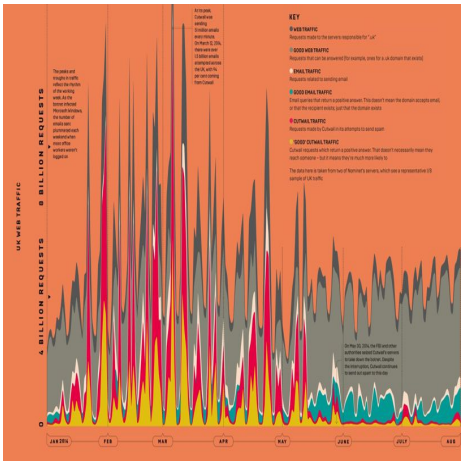
By VICTORIA WOOLLASTON

Death | 05 Jun 2017

WIRED Money 2016 Startup Stage: security and services

By JAMES TEMPERTON

WIRED Events | 05 Jul 2016



Infoporn: the rise and fall of the UK's biggest spammer

By JAMES TEMPERTON

Email | 17 Jun 2016

Quantum Computers

Quantum encrypted box hints at unhackable communication

Previous attempts at building a quantum memory storage system have been too big to be of used on a computer chip

By **ABIGAIL BEALL**

4 hours ago

Quantum-encrypted communication and quantum computing promise to be safer and more secure ways of communicating, but a variety of challenges are keeping these goals from being achieved.

But new research has taken us an inch closer to the goal.

Quantum communication involves the sharing of quantum information over long distances. But in order to crack this, first the concept of quantum memory needs to be addressed.

Quantum memory means an interaction between light and matter that allows quantum information, stored in light, to be retrieved – in a similar way to the memory in a classical computer.

Previous attempts at building a quantum memory storage system have been too big to be of use at the scale needed, the size of a computer chip.

Now researchers in China and the US have come up with quantum storage 'box', small enough to be used on a chip. The device is a nano-sized cavity, around one thousandth of a millimetre, filled with the element neodymium inside a crystal structure. The paper is published in the journal *Science*.

"The photons are stored in an ensemble of rare-earth neodymium atoms," says Andrei Faraon, from the California Institute of Technology, and co-author on the paper.

Inside, the atoms are trapped in a crystal called yttrium orthovanadate (YVO4). "The ensemble is small, and by itself would not be able to absorb the photons," says Faraon. "This is why we make an optical cavity, or resonator, in the YVO crystal, that enhances the interaction between the atoms and the light, so the absorption of photons by the atoms becomes efficient."

A scanning electron microscope image showing the nano-scale optical quantum memory device

Credit **Dr. Tian Zhong**

To store the photons, the cavity is prepared in a special way using a sequence of laser pulses. This preparation means that after the photons are absorbed they are automatically re-emitted after a certain short amount of time, or 75 nanoseconds to be precise. “To implement a quantum memory using this device, we store photons that are shaped as two pulses, early and late pulse,” says Faraon.

“Quantum mechanically the photon exist in a superposition of early and late.” This means they exist as a combination of the two phases at the same time. After the pulses are retrieved, it closely resembles the stored pulses, meaning the memory works.

Faraon hopes this new device, which is much smaller than anything made previously, will help us to crack quantum communication. “In the future it could be used to transfer information at the quantum level at long distances via optical fibres,” Faraon says. “A quantum memory is essential in most schemes to transfer quantum information at long distances.”

Quantum-encrypted communication would be much more secure than the mathematical algorithms used currently. This is because of the properties of quantum mechanics called Heisenberg’s uncertainty principle.

Currently, information can be encrypted with techniques based on mathematical algorithms. It is difficult to figure out the exact algorithm used to encrypt a piece of data, making the approach largely safe for now.

However, experts anticipate computers powerful enough to crack the codes will surface in the next 10 to 20 years. This development would mean current encryption methods would be redundant as they could easily be broken.

But there is a potential solution – and this is where quantum mechanics comes into it. Heisenberg's uncertainty principle means the act of observing a particle creates certain changes in its behaviour.

Specifically, it means we cannot know both the momentum and position of a particle to the same degree of certainty at once. Quantum encryption uses this to create encoded data in the form of light that, if intercepted, will change its behaviour. This can alert the people communicating that the security key is not safe to use.

QUANTUM COMPUTERS SCIENCE

RECOMMENDED

Star Wars Episode IX director hints at Rey's identity

By MATT KAMEN
Culture | 13 Jan 2016

China sends the world's first quantum satellite into orbit

By AMELIA HEATHMAN
Satellites | 16 Aug 2016

By EMILY REYNOLDS
Wii U | 14 Dec 2015

Solar System's most distant object hints at hidden planet

By JAMES TEMPERTON
Dwarf Planets | 11 Nov 2015