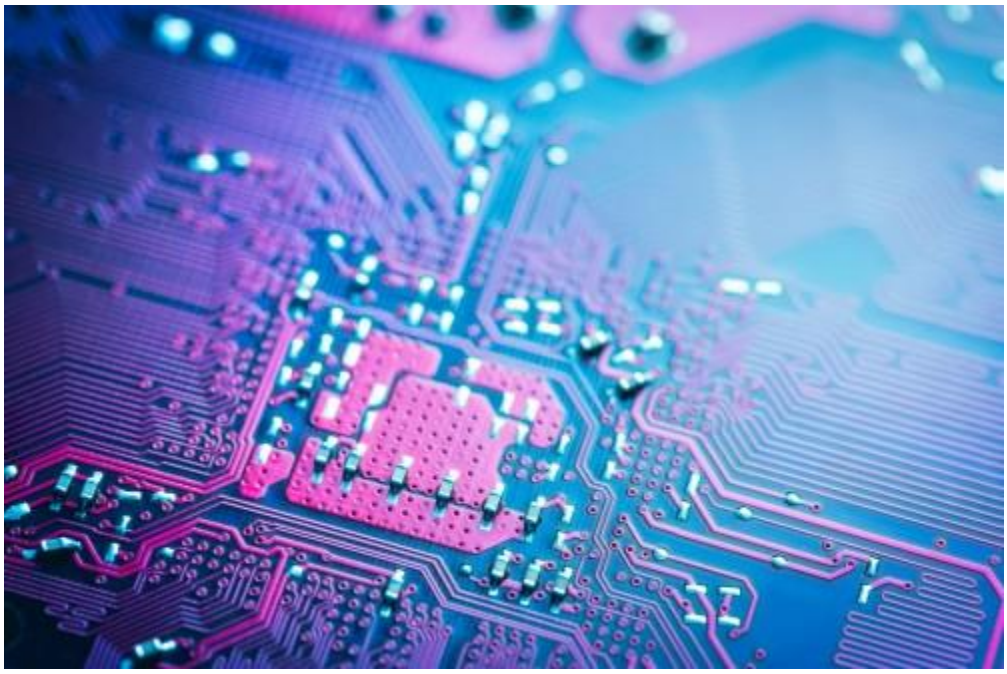
Sungula Nkabinde

Tech

International cybercrime fighter warns SA

Frank Abagnale on the dangers of what is now a multi-billion dollar industry.

Sungula Nkabinde | 5 August 2015 10:56



According to reformed fraudster and FBI consultant Frank Abagnale, South Africa's growing online presence makes it a fertile ground for cyber criminals. Abagnale, whose life provided the inspiration for the feature film *Catch Me If You Can*, is an expert on fraud, security and identity theft and started working for the FBI nearly 40 years ago, when he was removed from prison to help the unit catch other fraudsters.

Speaking to the media at Experian's Insight Conference held on Tuesday, Abagnale revealed that cybercrime costs the global economy hundreds of billions of dollars a year, and that South Africa was now the second most targeted country in the world for internet fraud and phishing attacks.

Cybercrime worldwide is a billion dollar industry, he said, citing a Russian gang that makes $20 billion dollars a year engaging in it, which is more than most US corporations.

"In the United States fraud has cost the economy $950 billion a year. Last year, Medicare (US health care provider) paid out R100 billion in fraudulent refunds. That's already 10% of their budget," said Abagnale. "Our Internal Revenue Service, the tax collector, paid out $5.6 billion in tax returns to people using someone else's identity. We had $7.7 billion paid in unemployment fraud to people who said they were unemployed but were in fact working and $16 billion to people claiming to living under to poverty level, but were not."

Michelle Beetar, MD of Experian South Africa, said that in South Africa, R1 billion is lost as a direct result of identity theft. If you include white collar crime, it's a R6 billion industry. This was according to a new report launched by Experian, which analysed findings from 255 key decision makers from 195 telecoms and financial services organisations in eight regions across Europe, the Middle East and Africa. The report also revealed that three in ten people surveyed had been a victim of credit card fraud.

Abagnale said he only deals with cybercrime that is in the realm of billions, meaning many of the fraudsters simply get away with crimes because they operate at a smaller threshold. He said it was unwise to look at examples in Russia and America and assume that it would not come to one's own jurisdiction, explaining that technology had opened the world up to everyone and that governments, institutions, banks and retailers needed to take a proactive approach – learning from other countries/companies' experiences – instead of a reactive one.

Said Beetar in a statement from Experia: "The rapid rise in demand for online banking, combined with very little security on devices, meant there were huge opportunities for cyber criminals, leaving many people and businesses exposed and extremely vulnerable."

Protecting yourself

While Abagnale admits to holding nothing against social media platforms like LinkedIn, Facebook and Twitter, "they make it much easier for criminals". If you're on Facebook and you've listed your date of birth and where you were born, and a head-and-shoulders image of yourself, criminals will already have 98% of the information they need to steal your identity, he said.

"Criminals are not looking for a challenge, they're looking for an opportunity to exploit. If you make it difficult for them, they'll simply move on to the next target, and that applies to whether you're a bank, retailer, a government or a consumer."

Beetar said it was important for everybody to get their free annual credit report, because that was the best way to check whether their identity had been stolen and any accounts had been opened in their name without their prior knowledge.

For more tips on how to protect yourself from cybercrime, check Abagnale's site.

People are at the root

Abagnale said security breaches come down to human error. All breaches occur because someone in a company, government agency or institution has done something they were not supposed to do or failed to do something they were supposed to do. (For example - an employee reads an e-mail or goes to a website or the company fails to put in the proper technology to keep the breach from occurring.)