How grandee of banking Anthony Loehnis fell prey to web fraudsters

Dominic Kennedy, Investigations Editor

March 30 2019, 12:01am, The Times

Anthony Loehnis, a former Bank of England executive director, with his son, Barney, and wife, Jennifer. "One feels a fool"

A gang of online scammers has stolen tens of thousands of pounds from the bank accounts of a retired executive director of the Bank of England.

Anthony Loehnis described the trick, in which fraudsters posed as BT staff protecting his computer, as "mental colonisation".

For four days the team tried to keep him cut off from the outside world by occupying his landline and instructing him to stay away from his computer, mobile and tablet while a bogus firewall program was downloaded.

"With hindsight I think, 'How could I have been so naive?'," he said. "But they are extremely plausible, these people."

Mr Loehnis, 83, of Oxford, is a grandee of the City of London, having been executive director at Threadneedle Street for eight years during the 1980s, a vice-chairman at SG Warburg & Co and chairman of Alpha Bank London from 2005 to 2015. When talking with relatives he has compared himself to King

Lear. He decided to speak out to warn others who may conclude that if he can be a victim, anybody can.

The scam involved a technique known as “vishing” in which criminals use their voices over a telephone to fish for personal information.

The attack began on Tuesday last week when Mr Loehnis received a phone call at home, claiming that technical problems required the delivery of a new broadband router that would arrive in 48 hours. The fraudsters said that in the meantime they had to install their strongest anti-virus software. They asked him to download a program enabling remote connection to his PC so that they could add the protection. He did so and they were in.

The bogus BT characters speaking with Mr Loehnis were “Ben” who reported to “Aaron”, along with “Jason” who was supposedly in charge of a regional team. There was a pretence that they were in a call centre in India.

Mr Loehnis, an Old Etonian, has a sharp mind and embraced the internet. He took his wife Jennifer’s advice to switch to First Direct, a remote banking specialist, because of its reputation. “I was fed up with the bad service I had from Coutts for years,” he said. “I had been with them since the age of 12.”

On the second and third days of the attack, the retired banker was asked to move money from his account with First Direct to accounts he keeps in sterling, euros and dollars with Citibank. The transfer was supposedly to help the police to catch a hacker in the act of taking money from a cash dispenser.

Mr Loehnis was shown an alleged Interpol photo of the criminal, whose name appeared to be Ukrainian. He believed that he was doing his civic duty. “I was assisting them and the police in capturing him,” he said.

The conman using the name Aaron told Mr Loehnis that the operation worked and the hacker had admitted to detectives that he had taken sums from the banker’s First Direct account.

When Mr Loehnis complained that the downloading was slow, he was promised £204 in compensation and free BT telephone and broadband for six months. He said that this was not enough to compensate for the disruption: without a phone he had been forced to cancel lunch and a yoga class. He had fallen under the spell of the fraudsters. Aaron encouraged him to go to the First Direct account website to see if the compensation had been credited. When he logged into his accounts, however, the screen went blank.

On the fourth morning, the security software stated that it was only 70 per cent downloaded. Mr Loehnis opened his banking websites to discover that tens of thousands of pounds were gone. “I realised I had been cleaned out,” he said. “One feels just ‘what a fool’.”

The case has been reported to the banks and Action Fraud, the national reporting centre for cybercrime. Investigators are expected to examine the destination of the sums, transferred to accounts, some with Romanian names, and a Warsaw bank. Some accounts had English names indicating that they were paying for old people’s homes, hospital beds and back support. “I have financed, according to this, the whole of the Romanian national health,” he joked grimly.

He need not be so hard on himself. Paul Breen, of the Westminster Professional Language Centre, who has studied such cases, found that the process was usually scripted with fake scenarios that create confusion.

Dr Breen’s report *A Dance of Deceit* suggests that victims believe there is an emergency that “is under control and in the safe hands of the fraudster”.

Citibank said that the case was under investigation and it was in regular contact with its client. First Direct said: “We take fraud extremely seriously.”