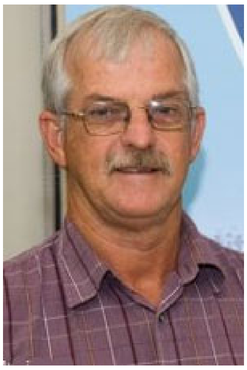
BIZCOMMUNITY

NMMU moves to minimise internet fraud

By Musa Mkalipi

4 Jun 2013

A team of researchers in the School of Information and Communication Technology at the Eastern Cape's Nelson Mandela Metropolitan University has come up with a solution to mitigate SIM swap fraud and fraudulent internet banking transactions, using just a USB stick.



Prof Rossouw Von Solms is the leader of the research team at NMMU. (Image:MyPE)

Like others around the world, South Africans are not immune to internet crime. The NMMU innovation is a solution to help people to avoid falling prey to fraudsters, and will also make it possible to carry out secure internet banking from any computer, even a public one in an internet café.

The technology is based on a custom-built operating system residing on the USB drive, and into which the client computer boots. The system is used solely to do online banking, and can't be cracked, hacked or broken into, according to NMMU.

The bank will issue the device in the same manner as a credit card or debit card is issued currently. The USB stick is unique in that it incorporates a SIM card and a modem. The bank sends a text message containing a security code to the user's phone, which offers double protection.

When a client wants to do online banking via the computer, he or she plugs in the banking stick but will first need to enter a PIN number to prove authenticity, after which a communication link is created between the client and the bank that cannot be compromised.

"We are currently experimenting with a fingerprint reader on the banking stick to offer maximum protection," said Prof Rossouw von Solms, a cyber-security specialist and leader of the research team that created the technology. "Thus the bank will know that it is me doing banking as only I have this unique banking stick."

Cutting down on internet banking risks

According to Von Solms, the USB stick could be a potential solution to most current online banking risks - if not all of them. "More than one thousand cases of online banking fraud have been reported over the last few months," he said.

Von Solms added that South African banks are currently running a fairly secure internet banking system, but that the systems are deployed in an insecure environment where clients are not always aware of the risks, and need to be educated as to what steps to take to prevent themselves from being victims of internet banking fraud.

Putting together the solution took about 18 months. The university is doing similar solution-based research in the information and security field, but specifically from an educational point of view. Von Solms said that primary schools, old age homes, and corporate environments are taught about the basic principles of information security. "The main message is to make them information- and cyber-aware," he said.

According to Von Solms, fraudsters use the practice of phishing to get your pin and password to access your bank account. This means that they lure people to a dubious - but authentic-looking - website using emails from what appear to be well known and trustworthy sites, ask them to enter their security details, and then capture those details.

"When you enter your user ID and password for internet banking, your details are transferred to a secret destination," said Von Solms. Once the fraudsters have these details, they are able to gain access to your funds. Illegal SIM swaps have become widespread to intercept one-time-pin codes sent by banks to online clients to finalise a transaction.

Mary-Ann Chetty, innovation manager in NMMU's department of technology transfer, said that the university approached two of the country's major banks, demonstrated the technology and offered it to them, but neither was interested. "According to them, 'one more click' is not acceptable to their online clients," she said in a statement.

A third bank has been approached and negotiations are under way. "We really hope after all the media buzz that has appeared lately, banks will be more serious about taking the solution," said Von Solms. He added that the team needs a bank to work with them to develop this technology, tweak and implement it.

Internet banking fraud on the rise

A report on banking services compiled by Clive Pillay from the Ombudsman for Banking Services, says that in 2012, South African internet fraud rose by 3% and mobile banking fraud by 8%. The report also said the growing trend is linked with the rising use of mobile phone banking technology in the country.

The ombudsman urged banks not to compromise on security and control in the banking environment, in order to provide a reliable payment system.

While victims may take steps to protect themselves, it is difficult for them to identify internet fraudsters as they are usually nameless and faceless.

In 2009 only 45 cases of internet banking fraud were reported by the banking ombudsman. In 2010 the number rose to 484 cases. By 2011 there were 591 complaints on record.

In 2012, banking fraud complaints constituted 20% of the complaints handled by the ombudsman. Of these complaints, 1 335 were from Absa, 1 260 from First National Bank, 845 from Standard Bank, 648 from Nedbank and 252 from Capitec Bank, according to Pillay's report.

How to protect yourself

According to business publisher ITWeb Africa, African nations such as Uganda and Nigeria have announced deadlines for SIM registration, to combat criminal activity. However, in a country like South Africa where these registrations exist, criminals still find a way to scam. Millions are being stolen from clients even with such monitoring.

Criminals use online accounts or credit card details to make fraudulent transactions, and online fraud of any form can have serious financial consequences including damage to a person's credit record.

By diligently following a few recommended steps, people can minimise the risk to themselves, their banking details and their funds:

- Protect your personal and account information at all times;
- Never give your cheque account or credit card to unknown callers, as this could be a scam. No credible institution will ask for sensitive details over the phone;
- Never give out your ATM, debit card or credit card number;
- Report lost or stolen cheques immediately;
- If an email claims to be from a bank, but the email address is from a Gmail account or similar, it doesn't come from the bank.
- Check the grammar and spelling of such messages - often they will be riddled with errors;
- If you suspect that your credit or debit card has been compromised, cancel it immediately and request a replacement.