Just a few clicks can leave you cashless

It is very difficult to protect yourself against faceless, nameless criminals from around the world who can click, double-click and make off with your life-savings.

"They have become very sophisticated," said Colin Hill, who works on financial crimes and risk management at the SAS Institute, a "business analytics" company.

A London-based phishing gang was convicted this month of robbing a woman living in South Africa of more than R13-milli *Computerworld UK* reported.

The ubiquity of mobile and Internet banking makes it easy for fraud to cross national boundaries, said Hill.

The woman opened an e-mail she believed was from her bank and entered her banking details on the gang's phishing site

The gang used accomplices to transfer small amounts of money from the account and in that way of beat bank limits on money transfers.

"You won't even notice it is happening," Hill said.

An MTN customer lost R97,000 after an unauthorised SIM swop gave fraudsters access to his account, *Moneyweb* report last week.

The company's chief customer experience officer, Eddie Moyce, warned: "With regard to fraud committed on customers' bank accounts, there seems to be a misplaced belief that mobile network operators are liable. Please note, mobile network operators are not liable.

"This is based on the fact that, in order to commit a fraud on a customer's bank account, a fraudster must have a custome bank card or account number, or Internet banking PIN and password," said Moyce.

The company said that, because of "customer confidentiality" it could not discuss the R97,000 fraud.

"Occasionally, MTN is faced with SIM-swap fraud. MTN is doing its best, alone and in conjunction with the police, to investigate such fraud," said Moyce.

But Hill believes that the victim was not an individual target. He suspects the culprits were using a "spray and pray" approa

Hill says they had to have been hoarding information of a large number of people and waiting for a specific cellphone number to pop up on their radar and then used the corresponding banking details to drain the customer's accounts.

"To do this you must have access to a company's systems," Hill said.

Source: *The Times* via I-Net Bridge