CATCHING PHISH

The FIC worked with the Asset Forfeiture Unit, SARS, the South African Police Service, the South African Banking Risk Information Centre and various banking institutions to uncover a phishing scam.

Phishers clone bank accounts using sophisticated devices. After the phishers have identified a potential phishing victim, they contact SIM swappers to block the owner's cell phone number so that account holders do not receive transaction notifications. This allows the phishers to log into the victim's account and transfer money out of it. The money is then immediately withdrawn from different ATMs, after which the ATM cards are discarded. The mobile service provider employees are paid for assisting with the SIM swap, while the rest of the money is deposited into the accounts of the main phishers.

With the FIC's assistance, law enforcement arrested some of the subjects and seized laptops and cell phones. Three of the perpetrators have been sentenced to between 15 and 20 years in prison.