

Fraud detectives – The banking scam

by Costa John

There has been a noticeable increase of late in what is being touted as the banking scam. This is according to Nico Theron, a legal adviser of fraud detection company Alchemy Business Consultants. He says, “I am currently dealing with six matters that have come up in the last week, where large companies as well as auditors and accountants are being taken for a ride.”

He explains how the scam works. “An organisation receives a letter from a company they believe to be one of their trusted suppliers. The letter advises them of a change in banking details. This is followed up by a friendly call to make sure the company received the letter. The organisation then makes a payment to the false banking details, and shortly afterwards the real supplier phones to follow up on payment which they never received. It turns out the banking details were fraudulent and the money is gone.”

Once the money is paid in, the criminals can draw it in a relatively short period of time. “This is a very difficult matter to investigate because their identity is unknown, and it is a long process to get access to the bank account.”

through to a fraudulent call centre, where they will confirm the change.”

Another spin-off of this scam occurs when an organisation that regularly deals with a trusted client on a cash basis, receives a fraudulent application for a credit account. Because the organisation has been dealing with this purported client for a long period of time the credit application is approved. A criminal then comes to purchase goods on credit, and once they are delivered they are gone. **S**

For more information visit
www.alchemyconsultants.co.za

“I am currently running with **six matters that have come up in the last week**, where large companies as well as auditors and accountants are being taken for a ride”

Theron points out that with internet transfers it does not matter what account name you input, it is the bank account number that matters, so the fraudulent banking details could say the name of the real supplier, but if the account number is wrong the supplier will not receive the money.

“This type of scam is not perpetrated by the same person. In all six matters that we are dealing with at the moment it seems to be different people committing each crime.”

He highlights that these fraudsters often have some internal connection with the companies involved. “The insider could be a staff member of the organisation or the supplier organisation. They often know the amount which needs to be paid to the supplier, and they use fraudulent letterheads.”

He warns that whenever you get any letter stating a change in banking details, you need to check with the company and ensure that their details have indeed changed. “Do not under any circumstances phone the number on the letter. That is often a different number which is routed

