Cybersecurity

Sponsored supplement to the Mail & Guardian October 28 to November 3 2016

Internet banking fraud: The scourge of SIM swaps

Customers are being blamed for cyber attacks that they can do little to prevent

COMMENT
Basie von Solms

Incidents of customers losing money through internet or online banking fraud are increasing daily. It seems that the cybercriminals are growing bolder, as the amounts stolen now often run into millions of rands per victim.

In a typical online banking transaction, the three parties involved are the customer, the customer's bank and the customer's mobile service provider. In the majority of cases, the customer's bank and the mobile service provider deny any liability for losses suffered, claiming that the customer must have compromised his or her login credentials.

While there may in some instances be negligence on the part of the customer this is often not the case in internet banking fraud. Nonetheless the banks — even after thorough investigation of the customer's computer device and inability to establish any wrongdoing or negligence on the part of the customer —persist in this attitude, frequently refusing any refund. The whole situation requires a proper review.

How transactions usually work

In a normal online banking transaction, the security approach used by banks in South Africa is a two-step process:

● Step One is to log on to the bank's internet banking website with your logon information, usually involving an account number, user name, profile number, PIN number, password and more. If this is correctly verified by the bank's system, you are given access to your banking profile and you can perform "non-sensitive" transactions like viewing a balance or transferring money between the beneficiaries defined in your profile. However, it is recognised that additional security is required to protect you while performing a "sensitive" transaction such as creating a new beneficiary, or doing a once-off payment to an account not presently in your profile, and that is when Step Two kicks in.

● In Step Two, the bank generates and sends a one-time password (OTP) to the mobile phone registered by the bank in your account. You receive the OTP, enter it into the "waiting" web page, the bank's system verifies the OTP, and allows you back into your profile. You can now perform the sensitive transaction.

Cybercriminals have perfected their attacks against this two-step process, which have a fixed pattern and basically consist of three phases.

Phase One: Logon details

In phase one of the attack, the cybercriminals obtain the logon information of a customer through various means. This can happen through a phishing attack, where the customer is tempted by a fake email claiming to come from his bank, indicating that she must log on to her online account for some reason — a link is provided which must be clicked. If the customer does this, she is taken to a faked (spoofed) website looking just like her bank's, created by the cybercriminal. She does not recognise the fake, and logs on using her logon information. The cybercriminal is now immediately in possession of the logon credentials of the customer.

In many cases, even when investigations reveal no fault on the part of the customer, banks and mobile service providers defend themselves by claiming that the customer was responsible for the compromise of his or her credentials.

However, this is simply no longer true. A customer's smartphone, tablet or computer used to interact with a bank online can be infected with malicious software (malware) without the customer having any idea that it happened. Malware infections can happen in many ways, for example by just visiting a totally legitimate website, but where this site had been itself

To page 2

Internet banking fraud: The scourge of SIM swaps

From page 5

been infected, the customer's device may also become infected. Anti-malware packages do not always recognise such an infection. The customer's device is now infected, for example by a keyboard logger, which will send every keystroke back to the cybercriminal — including the customer's logon credentials when she logs onto her online banking account.

The point is that the customer can no longer be held accountable for an infected device unless clear negligence on the part of the customer can be demonstrated — the level of sophistication of the cybercriminal is far superior to that of the customer. Banks and mobile service providers cannot and should not therefore make the straightforward assumption that the customer was involved in the compromise of her logon credentials, and certainly cannot when clear negligence can't be demonstrated.

Phase one of the attack also requires obtaining the customer's mobile number. This is extremely easy and there are many ways of doing so.

CREDITS
Editor Sipho Hlongwane
News editor Simone Wilcock
Copy subeditor Derek Davey
Layout Russel Benjamin

The contents and photographs in this supplement were sourced independently by the *Mail & Guardian* supplements team

Phase Two: The SIM swap

In phase two the cybercriminal must now engineer a situation where the OTP will be sent to him or her and not the customer. This involves a so-called SIM swap. It is important to remember that a person's mobile number is not linked to his or her physical phone device, but to the SIM card within the phone. The cybercriminal of course knows this. He or she now goes to the customer's mobile service provider with fake documents purporting to be those of the real customer, and requests a SIM swap, claiming for example that his or her phone was stolen or lost. If this SIM swap process is not very tightly controlled by the relevant service provider, the fake documents are accepted and a new SIM card is issued to the cybercriminal.

This means the mobile number is now linked electronically in the mobile service provider's database to the new SIM card — the real customer's "old" SIM card is now electronically cancelled. However, the real customer's mobile number is now linked to the new (illegal) SIM card.

The cybercriminal now inserts this new SIM card into his or her phone. This means that if the real customer's mobile number is now dialled, the cybercriminal's phone will be contacted instead. The customer's phone can no longer be reached.

The modus operandi of phase two is to do it at times when it is unlikely that the customer will be easily alerted to the SIM swap or internet banking activity on his or her account, often over a weekend. SIM swaps can be made without the customer being involved, negligent or aware.

Phase Three: The withdrawal

The cybercriminal now uses the logon information acquired in Phase One of the attack, logs into the customer's account, requests to create a new beneficiary, waits for the OTP to arrive on his or her phone, inputs the OTP, creates a new beneficiary, transfers the money into the new beneficiary account and logs off. He then withdraws the money from the account of the (new) beneficiary to which the customer's money has been transferred.

The implications

Three core implications can be drawn from the above:

- It is very clear that all three phases can take place without the customer even having the faintest clue that the attack was executed.
- Banks should face the reality that in the light of the sophistication of cyber attacks the present logon approach (as described in Step One) no longer protects customers as it was intended to. Alternative, more secure measures for this step must be rolled out as soon as possible.
- When authenticating and verifying an online banking transaction, much larger emphasis must be placed on Step Two above — the OTP approach. Step Two must be re-engineered to provide much stronger security — technically, procedurally, and regulation-wise. This will require stronger co-operation between banks and mobile service providers.

It seems that banks are well aware of these problems, because in many cases they offer to refund the customer 50% of the loss. Why would they do this if they do not understand and buy into the core statements above?

The whole situation as it presently stands sparks some burning questions.

- Is it ethical for banks to market internet banking if they do not have control and take responsibility over the whole end-to-end process? The mobile service provider has a relationship with the bank, and in sending the OTP to the customer it acts at the agency of the bank. The bank must, through formal agreements with the mobile service providers, ensure that the OTP is received only by the bank's customer, and hold the mobile operator accountable if this process is compromised.
- In the light of the above, is it ethical for banks to blame the mobile service provider and for the service provider to blame the bank if the customer is the ultimate loser?
- How can a SIM swap be performed by mobile service providers without the real customer being directly involved and personally verifying the SIM swap?
- In how many cases are insiders from the bank or mobile service provider involved in illegal SIM swaps?
- Why do banks offer 50% of the stolen amount if they do not feel they are partly to blame?
- Why do banks not issue customers with specific devices like a pager exclusively used for receiving the OTP? This will eliminate the mobile phone from the process
- How well do mobile service providers enforce the Rica requirement related to SIM card activation and SIM swaps? Does the Rica Act have to be changed to close existing loopholes?
- Why are responsible parties such as the Independent Communications Authority of South Africa and the department of justice not more visibly involved — are they missing in action?
- Why is the Public Access to Information Act not more widely utilised by the legal community to support their clients' cases? If a customer's money is transferred by an unauthorised transaction to another account, the owner of this other account is in possession of stolen property. It seems logical that the customer whose money was stolen should have the right to know the identity of the person who stole his money.
- Why are customers so often accepted as the negligent party when that is now an untenable approach?

If these questions lead to at least some discussion, something has been achieved. Cyber attacks have become so sophisticated that the assumptions made by banks and mobile service providers about their customers' role in protecting themselves from attack are not tenable any more — something must change.

Professor Basie von Solms is the director of the Centre for Cyber Security at the University of Johannesburg