UBA

Launce Moses

Launce Moses is Group Director of Audit and Control at United Bank for Africa, reporting to the board of UBA and the CEO. He is responsible for Internal Control, Audit and Fraud Prevention & Investigations across the Group.

Published September 2009

All you need to know to ensure Safe and Secure ATM Transactions

BACKGROUND

The introduction of Automated Teller Machine (ATM) brought succor to Nigerian banking environment as long queues in the banking halls began to wane, as most customers opted to transact through that channel. This relief however did not last long as incidents of fraud resulted in a decline in customer confidence on ATMs. In this report, Launce Moses, Group Director, Audit & Control UBA plc identified some of the common tricks that ATM fraudsters are using to dupe innocent victims.

PHISHING

Recently, several ATM card customers have received emails purportedly from Interswitch (the switching company in Nigeria) and the Central Bank of Nigeria, stating that there has been an upgrade of service, and in some instances that the company has improved its security features and hence the need for the customer to immediately click on a link provided to ensure that his/her card is usable.

The link leads to a website which appears very authentic and details requested on the website include card number, name of card holder, PIN number and other details that fraudsters require to make a 'copy' of the card. Once this data is received by the fraudster on this bogus website, the details are fed into a card encoding machine and encoded onto the magnetic stripe of any plastic card. This card becomes a 'clone' of the individual's ATM card and is thereafter used by the fraudsters to withdraw funds from any ATM across the country.

These fraudulent emails are also called 'Phishing' emails. Years ago, they were in bad, broken English and emanated mostly from Central and Eastern parts of Europe and the erstwhile Soviet Bloc countries using a 'Yahoo' or 'Hotmail' email identities. More recently, the fraudsters have become more sophisticated in creating authentic looking email IDs of the Central Bank of Nigeria and Interswitch. They have also created websites that appear genuine to the ordinary consumer.

Consumers must be aware that, BANKS AND CARD COMPANIES WOULD NEVER ASK FOR A CARDHOLDER'S PIN NUMBER and are therefore urged to call their bank on the BANK'S customer service line (not on the number provided on the fraudulent email!) and confirm the authenticity of the request. Consumers are advised to immediately delete such emails and advise friends to do the same.

SHOULDER SURFING

> ***Fraudsters need some critical data such as card number, expiry date and the PIN number before they can clone the card. One of the simplest ways to get this information is to observe a card holder at the ATM machine.***

Quite often, there are one or two members of the gang who are watching customers at ATMs in crowded places. In most instances, these fraudsters are baby faced youngsters who one would never suspect. Quite often they are seen punching away numbers in their mobile phones with the information that they have gained. The data is sent to a gang member who is typically in another state, who rapidly prepares a 'cloned' card (it only takes a few minutes) and sets off to the closest ATM to make a withdrawal!

SOCIAL ENGINEERING

In some instances, the fraudster tricks a card holder into showing him his/her card. He lures the customer into a conversation and comments on the state of the card – for example that the card looks 'damaged' and that the customer should change the card. The fraudster would then ask the customer to check the card for damages. The fraudster would have gained confidence from his prey using various tactics such as offering assistance to the customer who perhaps would have tried to use the ATM without success or perhaps the customer who is not familiar with use of ATM machine and requires assistance.

Social engineering involves gaining trust – hence the fraudster poses as a member of staff or even security guard! Quite simply –customers should never part with their cards! It is akin to cash – would you handover over your purse or wallet to a stranger?

The following simple tips can help you from falling prey to fraudsters.

- Firstly – be vigilant. When you are in a crowded place, keep an eye out for people around you and note if there are any who seem to be hanging around without making any transactions or who appear to be working in a gang.
- Secondly, take out your card only after you reach the ATM machine and do not disclose the front or back of the card to anyone.
- Thirdly, shield the ATM keypad whilst entering your PIN.
- Finally, choose a PIN that is not easy and that involves moving of your hand across the entire keypad. Do not choose numbers such as '0000' or '2222' or '4567' – it is easy to spot such PINs from a distance!

Regulators also have a role to play with regard to the easy availability of Card Encoding machines. In developed countries, these devices are illegal. However, today, these devices are available 'freely' in Nigeria and off the internet.

As an industry, Nigeria is moving towards a more secure 'Chip and PIN'. The 'Chip and PIN' stores data on the chip of the card rather than the magnetic strip of the card. This chip is similar to the Chip used for mobile SIM card and is more difficult to 'clone'. This is the standard that the entire industry is moving towards. Very soon, magnetic strip cards will not be in use anymore in Nigeria and consumers will once again enjoy the convenience of ATM transacting! Till that day, be vigilant and protect your ATM card.

LINK

http://www.thisdayonline.com/nview.php?id=151390