Author: Maya Fisher-French

New wave of fraud targeting bank customers

Fraud continues to pose the risk of serious financial losses for banking customers. All indicators are pointing towards the fact that there are new scams and an increasing number of the victims, warns Reana Steyn, the Ombudsman for Banking Services (OBS).

The basic modus operandi of these scams is not new. However, over the years, there is a constant change in the execution techniques that fraudsters have applied. “The success of these scams, and their evolution, is heavily guided by how the consumer will react in each situation,” advised Steyn.

Steyn highlighted two recent matters that were investigated by her office where two private banking customers fell victim to the same scam under the exact same circumstances. The story behind convincing the victims to disclose their confidential banking information was new. However, the basic scam remained the same, as did the results.

The New Phishing MO Scam

Mr M* advised that he received emails SUPPOSEDLY from the South African Post Office (Post Office). The emails informed him that he had unclaimed packages waiting for him at the Post Office Head Office. He advised THE REPRESENTATIVE IN THE EMAIL that he in fact had a package at the Post Office which he was aware of and had not collected yet. Mr M then received an SMS from the Post Office advising him to pay a fee of R42.50 for the package to be released and sent to his nearest Post Office.

Mr M followed the instructions on the link he received, and the link opened to a payment option on an OFFICIAL Post Office Payment page. He then inserted his card details and received an “Approve It “message on his cell phone. He accordingly approved the transaction. Immediately thereafter, he received another “Approve It “message from his bank and he noticed the word Singapore and realised that he was being defrauded. He immediately reported the fraud to his bank and instructed the bank not to release the pending transaction of R16 061.80. However, since the transaction was authorised with the use of the card details and the “Approve It “message, the bank had already released the transaction and refused any liability for the loss that was suffered. Mr M then reported the incident to the OBS and asked for assistance with his complaint against the bank.

The OBS determined that Mr M had in fact made the payment himself and approved the transaction through his Banking App. The OBS further found that although Mr M advised that he thought he was making a payment for R42.50, however, the message he received from the bank for the authentication of the payment read: “YOU ARE ABOUT TO MAKE AN ONLINE PURCHASE OF CHF 1, 000.00 AT BIGO LIVE”. Since it was clear from the message that the payment was not to the Post Office and that the purchase amount was not R42.50, the OBS found against Mr M and concluded that he was unfortunately a victim of a phishing scam where he willingly compromised his confidential banking details.

Fraud claims/losses for OBS complaints exceed R295 million in 2021

Steyn warned that banking fraud has become a very lucrative business for online scammers. The banking fraud matters investigated by her office in 2021 alone (the amounts claimed as losses by the victims of the various types of banking scams) exceeded R295 million. "This is an extremely worrying trend, especially when considering that these funds are mostly lost by individuals and small businesses who, in the majority of cases, are not in a financial position to suffer any kind of financial setback. In addition to the negative effects of Covid-19 on finances, most of these victims will sadly never be able to recover from these financial losses," says Steyn.

The Ombudsman confirmed that it was unfortunate that, in most of these matters, the amounts that were claimed were not recovered as they had already been withdrawn by the fraudsters. In fact, Steyn reiterated that the losses were largely due to the victims falling hook line and sinker to typical and well-publicised scams.

The latest wave of scams to look out for in 2022

According to the OBS' 2021 records, the Ombudsman received and investigated over 2 880 banking fraud related cases. This was a significant increase of 7.5% from the fraud cases that were investigated in 2020. Most of these matters were due to bank customers falling victim to internet banking fraud, credit card fraud, current account fraud, and ATM card swap scams.

Steyn advised that these scams are avoidable and called on bank customers to be extra vigilant in 2022 to ensure that they (individuals and businesses) do not suffer significant financial losses over a scam that could have been avoided had someone taken the time to consider the possibility that they are being defrauded. Never provide confidential banking details to a stranger over the phone or enter these details on a link received via email or SMS. Finally, never accept assistance from a stranger at an ATM, Steyn cautioned.

Steyn emphasised the point that no legitimate caller or email from the bank will ever ask a bank customer to provide their card number, passwords, and especially an OTP over the call or a link. She further advised consumers to refrain from using any links that are received to make payments. Consumers should be extra vigilant when it comes to a link where you are instructed to put in your banking account details that can be used to access the funds from your account.

A Call from the Ombudsman to raise more awareness

The OBS called on all banking customers, banking institutions and other stakeholders to partner with each other in 2022 to educate the public and raise awareness about the various scams that target banking customers (consumers and small businesses).

Steyn advised that the power to prevent these scams lies mostly with consumers as they are the ones being targeted. As such, the scams and the techniques that are used are created to take advantage of the vulnerabilities that the fraudsters have identified.

While there has been some consumer awareness and education regarding the scams that are currently being used and how they committed, Steyn added that over the years, the number of fraud victims has not decreased. According to Steyn, this is an indication that more vigorous action must be taken by institutions like the OBS, Banks, and (very importantly) the media, to assist, warn and educate South African consumers.

Steyn stated that consumers played the most critical role in ensuring that they do not fall victim to scams. According to her, Banks can never ensure that consumers do not provide their confidential banking information to strangers, nor can the fraudsters be prevented from trying their luck to deceive customers into providing them with the keys to their vaults. The responsibility is on customers to always remain vigilant and suspicious, especially when requested to provide their confidential banking details that they know can be used to access the funds in their accounts.

Fraud Detection Systems and Insurance by Banks

To combat the scourge of fraud, Banks have, over the years, created and introduced various fraud detection systems. The aim of these systems is to monitor and detect unusual transactions and prevent them where possible. This will hopefully minimise the number of fraud losses that are suffered by consumers. However, while these systems have proven to be valuable in preventing fraud in most instances, Steyn warns these measures do not guarantee that all fraudulent transactions can or will be detected. Therefore, if it is found that you as a customer provided your confidential banking details to the fraudster (and as a result, funds were withdrawn from your account) you will suffer the loss should the transaction not be detected and stopped by the bank.

Steyn continued and advised that such losses are not for the banks to absorb through their insurance. She advised that her office had on previous occasions received some matters where customers believed that the banks were insured for the losses suffered by clients through banking scams. “This is incorrect. The only time the bank will be held liable by the OBS is when the losses suffered by the customer were because of the bank’s negligence or wrongdoing,” warned Steyn.

Lastly, Steyn encouraged the consumers to do their utmost to eliminate the scourge of banking fraud by educating themselves about the various banking fraud threats that do exist. She warned that unless consumers assume the responsibility to educate themselves about banking scams (thus protecting their livelihoods), these scams will continue to grow as fraudsters will identify this as an ongoing lucrative vulnerability which only leads to increased profits.

Knowledge is power

The nature of the fraud landscape is that there is a specific theme to all of the scams that fraudsters use, it is the execution of these schemes that change all of the time.

Here are some tips that the public can use when presented with a possible fraudulent scheme:

Tips:

- banks will never ask you to confirm your confidential banking information over the phone;
- if you receive a phone call requesting confidential or personal information, do not respond and end the call. Contact your banks fraud hotline immediately;
- if you receive an OTP on your phone without having made a transaction, it is likely that it is a fraudster who has used your personal information. Do not provide the OTP to anybody. Contact your banks fraud hotline immediately;
- do not click on links or icons in unsolicited emails or SMSs.
- do not make payments into an unknown person/merchants' account without first verifying their authenticity. If you are unsure, go to your nearest bank branch and speak to a representative;
- when doing online shopping, only use your card to make payments on secure websites;
- while transacting, always keep an eye on the ATM card slot to ensure that your card is not removed, skimmed and replaced without your knowledge;
- Report lost and stolen cards immediately.
- be alert to your surroundings. Do not use the ATM if there are loiterers or suspicious people in the vicinity. Also, take note that fraudsters are often well-dressed, well-spoken and respectable looking individuals;
- key in your PIN in such a way that no one else can see it e.g., cover your PIN when punching in the numbers even when alone at the ATM as some criminals may place secret cameras to observe your PIN; and
- don't let anyone stand too close to you in order to keep both your card and PIN safe.
- entering a PIN, as it could be in "cardless transaction" mode.

Following these tips should protect you against becoming a victim of fraud.

ENDS