DO NOT CLICK ON THAT LINK – IT MIGHT BE A PHISHING EMAIL

Category: Commercial Law,Privacy Law, Infosec, and POPIA
written by Zandile Mthabela | February 8, 2019



Many people have been swindled out of their hard-earned money due to lack of information on fraud. On a daily basis, fraudsters prowl the internet in search of their next victim. Do not become the next victim! The rule of thumb is "*if an offer looks too good to be true, it probably is*."

Joe received an email on his private email address with a link to what appeared to be his banking website. He was prompted to verify his login credentials as there was 'suspicious activity' on his account. Without thinking twice, Joe clicked on the link and punched in his username and password. Suddenly, the system seemed to have been interrupted. Another 5 minutes went by, still nothing happened. The screen went blank abruptly and Joe felt compelled to reboot his PC. He comes to realise that a large amount of money had been debited from his account. In astonishment, Joe contacted his bank only to learn that the link that he had clicked on took him to a malicious website, and his account had been hacked. Joe had accessed a phishing email. Phishing is a method of deceitfully obtaining personal information such as passwords, identity numbers, credit card details and sometimes, indirectly, money.

As a precaution, when it comes to accessing your banking website, it is always safer to type the website address in full. Never access your banking site by clicking on any link, even if it was sent by your bank. If you doubt the authenticity of the notification, rather contact your bank.

Hackers are patient, they will 'flag' your account, monitor the activity, and attack when they feel that they can lure you in.

A hacker is a person who uses computers to gain unauthorized access to data. There are ways to minimise your chances of being hacked. Although fraudsters use various methods to defraud people – (such as text messages, links, telephone calls etc.). There are steps to take when you have fallen victim to fraud, irrespective of the method. These include:

1. Stopping all contact with the scammer;
2. Changing your passwords;
3. Contacting your bank's fraud department;
4. Contacting or visiting your nearest South African Police Services department to report a crime;

5. Contacting your Banking Ombudsman. [In this instance, onus will rest on the client to prove that the bank was negligent, failing which the matter may not be pursued further.]

Are banks legally obliged to refund clients who have fallen victims to fraud?

At times, banks may refuse to refund clients on the basis that clients made the payment voluntarily.

In relation to fraudulent transactions carried out on an electronic platform, the Code of Banking Practice provides that "*a customer may be liable for losses if he or she does not inform the bank as soon as reasonably practicable after he or she discovers or believes that his or her confidential access codes or devices, if any, for accessing the e-banking services have been compromised, lost or stolen, or that unauthorised transactions have been conducted on his or her accounts.…*"

The Code of Banking Practice further provides that banks will make refunds in the following instances:

1. where unauthorised transactions have been made by a third party after the customer has reported that the relevant personal identification number (PIN) may have been compromised;
2. where the customer has informed the bank that someone else knows his or her PIN, password or unique means of personal identification;
3. when transactions not authorised by the client have been entered after the bank has been informed that a PIN has been compromised; and
4. when money is transferred from the client's account to his "electronic purse" after the bank has been informed that a PIN, password or unique means of identification have been compromised.

Exclusion of bank liability

The Code of Banking Practice provides that a bank will not be liable for any losses caused by circumstances that are beyond its reasonable control, such as the following:

1. a customer's inability to access internet banking, or any other application associated with or reliant on internet banking, at any time, or any failure or delay in providing a service via the internet;
2. a malfunction of any equipment (including telecommunications equipment) which supports the bank's automated teller machines and internet, telephone or cell phone banking service;
3. a customer's inability to access telephone or cell phone banking, or any other application associated or reliant on telephone or cell phone banking, at any time, or any failure or delay in providing a service via telephone or cell phone; or
4. a disruption of services caused by political actions or natural disasters.

But, what does the Consumer Protection Act say about such exclusions?

The CPA requires that such exclusion clauses must be drawn to the attention of a bank customer and must meet the following requirements:

1. it must be written in plain language;
2. the customer must be alerted to the exclusion in a conspicuous manner and in a form that is likely to attract the attention of an ordinarily alert consumer, having regard to the circumstances;
3. it must be brought to the attention of the consumer at the time the bank customer contract is concluded or at the time the customer is required to pay for bank services, whichever is earlier; and
4. the customer must be afforded adequate opportunity in the circumstances to receive and comprehend the exclusionary clause.

If you would like more information on the Code of Banking Practice, please access the Ombudsman brochure here.