Privacy and Security

INTERNET BANKING PLATFORM

The privacy and security of our clients when transacting via our new internet banking facility is of the utmost importance to us.

We will therefore not share any of your personal information with a third party without your express prior authorisation, or unless compelled to do so in terms of a valid Order of Court or a mandatory statutory requirement.

Should you have any concerns regarding privacy issues, you are welcome to contact our Compliance Department at telephone number (011) 634-4000.

Information transmitted over an unsecured link or communication system is susceptible to unlawful monitoring, distortion or access. For your safety you must always follow the security instructions provided to you via the various communications and service channels, and published from time to time on our website.

You must never disclose your pin number or password to any person, including any staff member of The South African Bank of Athens Limited, or to any person claiming to work for or represent the bank in any way.

We will never ask you for your pin number or password, and you should never reply to an e-mail purporting to have been sent from the bank in which any personal information is requested from you. You must furthermore always log off from the Online banking website after finishing with your transactions.
We also recommend that you regularly update and check your computer's anti-virus software and security settings. Failure to do so may expose you to a security risk.

Contact our Helpline or IT Department immediately in the event that you suspect a security breach or any abnormal activity or online behaviour whilst utilising our Online Banking facility.

grobank

Grobank Limited Reg. No.: 1947/025414/06
Authorised Financial Services Provider (FSP 5865)
Registered Credit Provider (NCRCP 6)

There are two types:

- Larger numbers of computer users can be victimized because it is not necessary to target individuals one by one and no conscious action is required on the part of the victim. In one form of pharming attack, code sent in an e-mail modifies local host files on a personal computer. The host files convert URLs into the number strings that the computer uses to access Web sites. A computer with a compromised host file will go to the fake website even if a user types in the correct Internet address or clicks on an affected bookmark entry
- A particularly ominous pharming tactic is known as domain name system poisoning (DNS poisoning), in which the domain name system table in a server is modified so that someone who thinks they are accessing legitimate websites is actually directed toward fraudulent ones. In this method of pharming, individual personal computer host files need not be corrupted. Instead, the problem occurs in the DNS server, which handles thousands or millions of Internet users' requests for URLs. Victims end up at the bogus site without any visible indicator of a discrepancy.

Frequently asked questions:

How do I know it is a pharming scam?

- You would typically receive a phishing e-mail message with official-looking bank logos or other identifying information taken directly from the bank website.
- The e-mail will include an attachment containing the virus, which will be activated once opened.
- Alternatively, the e-mail will contain a link to a website which will download the virus to your computer once the link has been clicked on.
- Once the virus is installed on your computer, and you try to access Internet Banking, either by manually typing in the address or by a saved bookmark, it is possible that a pharming attack could cause your browser to unobtrusively redirect to a fraud website which would resemble a legitimate bank website.

What should I do if I get caught in a pharming scam?

- Logon to the internet banking site and change your details or contact the internet banking help desk.

Prevention Tips:

- Update your browser with the latest software updates and security patches.
- Use secure Web sites for sharing personal information.
- Regularly check your bank statements for purchases that you did not make.
- Report fraudulent websites to the bank.

DEPOSIT AND REFUND SCAM

In this type of scam, sellers of goods will accept the fraudulent proof of "cash" payments provided by the fraudsters. After releasing the goods on receipt of proof of "cash" payment, a customer will discover that the payment was by way of a fraudulent cheque and not cash when the cheque is reversed from the buyer's account.

Scams involving altered deposit slips have evolved to take advantage of electronic banking. A fraudster posing as a buyer will place an order for an item. A "cash" payment would be made into the unsuspecting seller's account. In reality a fraudulent cheque is deposited and the copy of the deposit slip is altered to reflect a cash payment.

This proof of payment is provided to the seller. The seller is subsequently offered a plausible excuse as to why the order cannot be taken up. The fraudulent 'buyer' then asks the seller to make an electronic refund of the payment (made by cheque) into a nominated account. The cheque is eventually returned by the bank, leaving the seller out of pocket.

Prevention Steps:

- Do not accept any faxed or photocopied proof of payment. Do not make withdrawals against unclear cheques. A credit on your bank statement does not mean that the funds are available; it is merely an indication that a deposit has taken place. Banks are entitled to debit an account with the amount of an unpaid or dishonored cheque.
- Contact the bank to check the clearance of cheque.
- Be critical about any kind of refund request.

BENEFICIARY MAINTENANCE SCAM

The beneficiary maintenance scam involves perpetrators contacting clients, and requesting them to amend their beneficiary details. This is done either by an email request for information or by luring you to a fake website.
Perpetrators create a false document using a legitimate company's details, and then request the client to update their beneficiary details on internet banking. The documents presented include letterheads, fax headers, invoices and statements which compare well to the company's legitimate documents, and appear to be genuine.

The client subsequently pays money into the fraudulently opened accounts. The frauds are generally discovered a few months later when the creditor queries non-payment of accounts. By this time, the funds have been withdrawn from the fraudulent account, and there is no possibility of a recovery. The information required to perpetrate these frauds are usually obtained from intercepted post, rubbish bins, websites, etc.

Prevention Tips:

- Customer should use the 'bank approved beneficiary' option when loading beneficiaries for large corporate entities wherever possible.
- If you receive a request of this nature, please confirm it with the company or entity.
- Refrain from using the contact details quoted on such requests and instead use the contact information already stored in your records.

Note: In case you come across through any of the above mentioned scams, please call the bank urgently on 0861102205 or e-mail us at Internetbankingsupport@grobank.co.za