Scams and Prevention

BANK OF ATHENS
Business and Commercial Bank

Phishing

Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication to you. It can be achieved by sending e-mails that appear to be originating from your bank. Generally, in these e-mails you are requested to change your password or enter your personal details.

Note: "Bank of Athens" will never ask you to change your password or enter your personal details by sending you an e-mail. Please call the bank urgently on **0861102205** or e-mail us at **Internetbanksupport@bankofathens.co.za** if you receive an e-mail of this nature.

Frequently asked questions:

How do I know it's a phishing scam?

There are a number of ways by which you should be able to spot a phishing scam.

- A phishing scam will ask you for personal information.
- A phishing e-mail, if clicked, will open up to an unsecured site.
- It could be a pop up window which will encourage you to enter your personal details.

What should you do if you are caught in a phishing scam? Logon to the internet banking site and change your details or contact the internet banking help desk.

Prevention Tips:

- **Be Critical:** Bank of Athens will never send you e-mails that ask for your personal information. If the bank really needs to get a hold of you to verify information, it will most likely be sent in writing.
- **Be Protected:** Never share your password with anyone.
- **Install anti-virus and anti-spyware software:** Install and update anti-virus and anti-spyware software regularly, as such software can reduce the likelihood of someone accessing your personal information stored on your personal computer or laptop.
- **Monitoring:** Monitor your account regularly and report to the bank in case of any suspicious activity.

Phishing/Voice Phishing

Not all phishing attacks require a fake website. Messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts. Once the phone number (owned by the phisher, and provided by a Voice over IP service) was dialed, prompts told users to enter their account numbers and PIN. Phishing (voice phishing) sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization.

Note: "Bank of Athens" will never ask your password or your personal details by phone. Please call the bank urgently on **0861102205** or e-mail us at **Internetbanksupport@bankofathens.co.za** if you receive an e-mail of this nature.

Prevention Tips:

It is fairly easy to avoid a Phishing scam or one conducted by e-mail, and more recently through text messaging on cell phones. Instead of calling the number listed, look up your bank account telephone number and call that number instead.

Pharming

Pharming is a scamming practice in which malicious code is installed on a personal computer or server, misdirecting users to fraudulent websites without their knowledge or consent. Pharming has been called "phishing without a lure". 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 listed 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 any of the above mentioned scams, please call the bank urgently on **0861102205** or e-mail us at **Internetbanksupport@bankofathens.co.za**.