

# LET'S TALK MONEY

Issue 12



## Don't get caught by a phishing scam.

Phishing is the act of sending an e-mail, in which the sender falsely claims to be from a legitimate organization, in an attempt to scam the recipient into disclosing private information. These e-mails are typically not personalized and ask for information such as credit card numbers, bank account information, Omang / Passport numbers, and passwords that can be used for identity theft.

The content of these Phishing e-mails typically include upsetting or exciting statements that prompt recipients to react immediately. In the case of some current Phishing scams, the hoax e-mail appears to the recipient to be coming from an employee of the organization and coerces the recipient into clicking on a website link. This link directs the recipient to a cloned version of the organization's website where the recipient is asked to supply their Internet banking username and password.

Often users are not even aware that they have fallen victim to a Phishing scam as the cloned site appears genuinely authentic by using parts of the real website as well as a site re-direction gimmick. Internet users are advised to be extremely cautious when receiving such e-mail and to ignore it completely.

Victims of fraud often expect the organization, which has had its logo or name illegally used in a Phishing scam, to accept responsibility for any losses or damages incurred as a result of responding to a fraudulent e-mail. However, the targeted organization cannot be held liable as victims provide information out of their own free will. If you are unsure about the authenticity of an e-mail, rather report it to your bank for investigation.

Although the Internet's convenience has made it a popular channel for a wide range of business transactions, it brings with it a great deal of risk and vulnerability to users. While advances in technology have helped improve security over the Internet, it has also provided criminals with countless new opportunities. Bank Gaborone encourages its customers to be aware of Phishing scams and to consider the following security precautions:

- Never reply to an e-mail requesting personal information
- Instead of following the hyperlink on an e-mail, rather type in the URL e.g. [www.bankgaborone.co.bw](http://www.bankgaborone.co.bw)), which will take you directly to the website
- Ensure the website address (URL behind the link) is prefixed with 'https' and not only 'http' as the 's' indicates a secure site
- Verify that you are visiting a secure website by checking the security certificate. Check the e-mail for grammatically incorrect language, as this is often an indicator of a fraudulent e-mail
- Check that the e-mail is signed by a company official
- Ensure that you have an updated anti-virus and spyware programme and perform regular system scans
- Avoid using public terminals for Internet banking
- Be aware of the high risk of interception during a wireless connection

Banks are required to verify all client information in an attempt to curb money laundering. Please be cautious when you are contacted via e-mail or telephone to verify your information as financial institutions should only ask you to verify personal information in a Bank branch with trained staff.

We take Internet security seriously and are constantly looking for innovative ways to improve our security measures. If you have any information on a fraud scam, or if you have been a victim of fraud, please e-mail [info@bankgaborone.co.bw](mailto:info@bankgaborone.co.bw).

For further information about this article or Bank Gaborone products and services, please contact one of our branches:  
Mall Branch +267 367 1600, Game City Branch +267 318 1077,  
Francistown branch +267 244 2323 or  
e-mail us at [info@bankgaborone.co.bw](mailto:info@bankgaborone.co.bw)

Plot 5129 • Queens Road • The Mall  
Private Bag 00325 • Gaborone  
Tel: +267 367 1500 • Fax: +267 390 4007  
[www.bankgaborone.co.bw](http://www.bankgaborone.co.bw)



**Bank Gaborone**

Growing together.