National Computer Board

Computer Emergency Response Team of Mauritius

(CERT-MU)

Phishing Email Alert

Phishing Email Targeting the MCB Ltd.

Detected on: May 09, 2014

Updated on: May 09, 2014

Severity Rating: High

Scam Overview:

Email title	***"We placed hold on your account"***
Scam target	MCB Ltd
Sender	mcb@277262.mcb.mu
Scam objective	Getting account information of users – User id, Password & Transaction Password
Phishing link	http://iib-mcb.com/mcb/ENULogin/MCB.htm
Is link masked?	No
Phishing site IP	23.229.145.165 – GoDaddy.com

Methodology

Phishing emails are circulating on behalf of MCB Ltd, with the subject: ***"We placed hold on your account".*** In the email, users are being informed that the MCB is migrating to a new server and will shut down the previous server accordingly. Therefore, users wishing to activate their account on the new server should click on the phishing link provided in the email to login.

A copy of the email is presented below for your reference.

-----Original Message-----
From: MCB [mailto:mcb@277262.mcb.mu]
Sent: Friday, May 9, 2014 4:32 AM
Subject: We placed hold on your account

....
Dear valued customer,

We have migrated your account to the new MCBISO2 Server. We shall shutdown the previous server accordingly. This is a procedure to further protect our clients.

Your kind attention is required to activate your account on the new server below to avoid account being suspended or closed.

Activate Account on Server Now :
http://iib-mcb.com/mcb/ENULogin/MCB.htm

Sincerely,

MCB Internet Banking
Mauritius Commercial Bank © 2014

When users click on the link, they are directed to the **phishing website** where they are asked to submit their account credentials.

The phishing website is copied below for your reference.

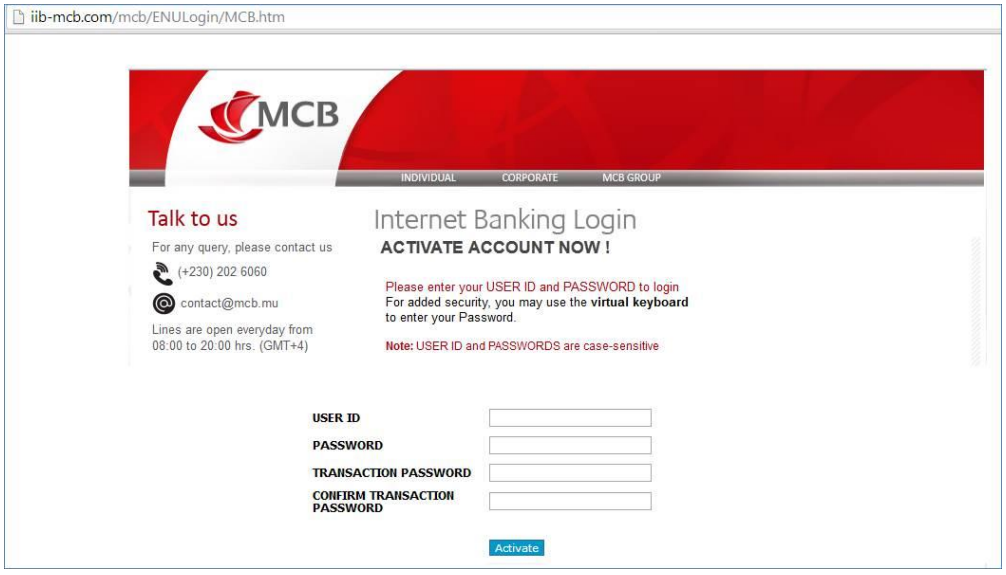

Image 1

Recommendations

1. Carefully review any email asking for personal information. If you are contacted to verify account information, call the institution that apparently sent you the email to verify if it is its policy to send account inquiries using email.
2. Make sure the email is from the intended website.
3. Open another browser page and manually type the URL mentioned in the email. If it is a phishing website, it returns a blank page. This indicates that this is not the legitimate website.
4. Entering the URL into a browser window would give you a log-in page even though you have not finished typing the whole URL.
5. Check if the site uses "HTTPS" and has the small padlock icon at the end of the address bar and at the bottom of the right page.
6. Practice safe and secure emailing. Never open an email from a sender you do not recognize and be extra cautious with email from unknown senders with blank or gibberish subject lines.
7. If you receive an email that is obviously a phishing email, do not open it. If you do open it, do not click on the enclosed link.
8. An email stating that your email account will be closed can look convincing. However, upon closer inspection, note the inconsistencies in capitalization, punctuation, spelling and grammar present in the email.
9. Notify the institution about the email or report it to the CERT-MU.

Contact Information

To report a phishing incident, you can contact CERT-MU on the following:

Hotline No: (+230) 800 2378

Fax No: (+230) 208 0119

Incident: incident@cert-mu.gov.mu

Website: http://www.cert-mu.org.mu