COMMUNIQUÉ

MAURITIUS BANKERS ASSOCIATION LIMITED

PHISHING ATTEMPTS

BANKS WARN AGAINST FRAUDULENT E-MAIL AND WEBSITE

The Mauritius Bankers Association (MBA), on behalf of its Members, would like to alert bank customers to various fraudulent e-mails which ask recipients to reveal their personal information, including full names, user names and passwords for online banking users.

These e-mails which are not originated from banks, instruct the readers to visit a website via a link and input personal details as described above. **Banks would never send e-mails asking for such confidential information to be recorded online and customers should NOT respond to such e-mails, even though they are sent repeatedly. The messages should simply be deleted immediately.**

- Bank customers are reminded to ensure they are connected to a valid site before keying in any confidential personal data. Important websites should be bookmarked in the browser and accessed from there.

- If customers are in doubt or are concerned that they may have revealed their security details to fraudulent websites, they should immediately change their passwords on the bank's genuine website and contact their respective banks.

- Customers should adopt additional security measures which might be available by their bank (eg. One-Time Password, 2 factor authentication, transactional passwords, etc).

LES BANQUES METTENT EN GARDE CONTRE LES E-MAILS ET SITES WEB FRAUDULEUX

La Mauritius Bankers Association (MBA), souhaite alerter les clients des banques au sujet de divers e-mails frauduleux demandant aux destinataires de révéler des informations personnelles, dont leurs noms, les identifiants et mots de passe pour ceux qui se servent des services bancaires en ligne.

Ces e-mails n'émanant pas des banques, invitent les lecteurs à visiter un site web en cliquant sur un lien et à entrer leurs données personnelles comme indiqué ci-dessus. **Les banques n'enverraient jamais des e-mails demandant que de telles informations confidentielles leur soient soumises en ligne et les clients ne doivent pas répondre à de tels e-mails, même s'ils sont envoyés plusieurs fois de suite. Ces messages doivent être supprimés immédiatement.**

- Nous rappelons aux clients des établissements bancaires de s'assurer qu'ils sont bien connectés à un site web valide avant d'entrer n'importe quelle donnée personnelle et confidentielle. Les sites importants devraient être mis en signet dans le navigateur et accédés à partir de là.

- Au moindre doute ou si les clients sont inquiets qu'ils ont pu révéler leurs données d'accès à des sites web frauduleux, ils doivent immédiatement changer leurs mots de passe sur le site web officiel de leur banque et prendre contact avec leurs banques respectives.

- Les clients devraient adopter des mesures de sécurité supplémentaires qui pourraient être disponibles à travers leur banques (le One-Time-Password 'OTP', l'authentification à deux facteurs, les mots de passe transactionnels, etc.)

28 December 2015

Level 15, Newton Tower, Sir William Newton Street, Port Louis, Mauritius
Tel: (230) 213 2390 - 213 2391 – Fax: (230) 213 0968 – E-mail: mba@mba.mu – Website: www.mba.mu