Logistics and Supply Chain MultiTech R&D Centre
物流及供應鏈多元技術研發中心

17 June 2022

To whom it may concern

Phishing Emails Reminder

Recently, a number of suspicious emails that look like being sent from a department or a staff member of LSCM have been discovered. Those emails requested the recipients to provide:

1. money, gift points or other cash equivalent payments;
2. their email, bank or other accounts passwords; and/or
3. other private or personal information, etc.

by either replying to the email, or downloading an attachment file or clicking a link in the email to access a web page and filling in the above information there.

Please be careful and note that LSCM and our staff have never asked and will not ask users to transmit any money or cash equivalent payments or provide password and/or other private or personal information via email. Those phishing emails were NOT originated from LSCM or its staff members, and the sender's addresses (e.g. lscm@virginmedia.com, simon_wong@platinumonline.website, anthony_kwok@piro.sakura.ne.jp, lscm-marketing@saneloud.com, etc.) are NOT our Centre's email address.

You are advised to delete such email immediately when it is received. Don't reply to the email or click on any link or attachment contained in the message.

If unfortunately you have already responded to this kind of email, please change your password immediately.

If you have any queries, please feel free to contact our IT Security Team at the following contacts: -

Logistics and Supply Chain MultiTech R&D Centre Limited

Tel.: (+852) 3973 6200

Email: info@lscm.hk