What is a "phishing" email or an attack?

Support Admin - 2022-05-12 - General

What is a "phishing" email or an attack?

Phishing is an attack that attempts to steal your money, or your identity, by getting you to reveal personal information -- such as credit card numbers, bank information, or passwords. This could come in the form as an email or a text message with a clickable link or an attachment.

What to do if you receive a phishing email ?

If you find the email message or the text suspicious, do not open it or click any of the links or the attachments in it.

Delete it and report to your IT services.

What to do after accidently responding to a phishing email?

The likelihood that a user might accidently respond to a phishing email is becoming inevitable.

1. Change account passwords

Do this immediately, to prevent your account being hacked.

After the attacker ties the phishing attack victim to a particular account, they will try to use similar credentials on the user’s other known accounts.

So, it’s crucial to change passwords not only for the expected compromised account but also for other associated user accounts.

2. Report the phishing incident

By reporting to relevant IT Services of your organization, you are keeping everyone aware that such an attack is taking place. Then others will be more cautious.

3. Investigate the phishing attack

Well-timed reporting of an incident—that is, as soon as a user realizes they’ve responded to a phishing email—allows information security technical staff to launch crucial information-gathering about the attack.

4. Keep an eye on your account activity

Make sure that after changing the passwords, no other activities have taken place.

Contact SLIIT ITSD for more information.