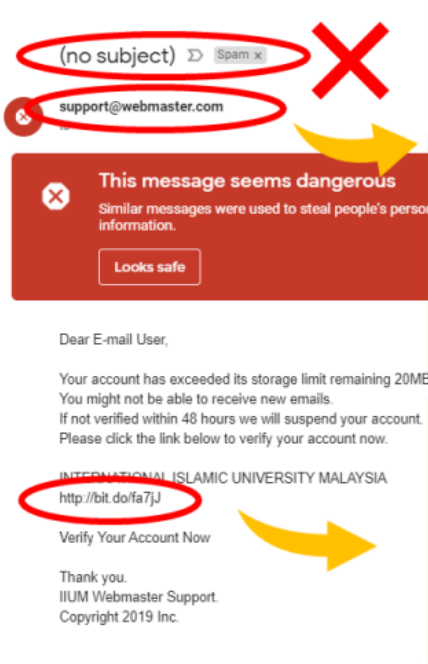


HOW DO I DIFFERENTIATE A PHISHING/SPAM EMAIL AND OFFICIAL ITD/IIUM ANNOUNCEMENT

"ITD, HOW DO I?" TIPS OF THE WEEK : HOW DO I DIFFERENTIATE A PHISHING/SPAM EMAIL AND OFFICIAL ITD/IIUM ANNOUNCEMENT



(no subject) Spam

support@webmaster.com

This message seems dangerous
Similar messages were used to steal people's personal information.

Looks safe

Dear E-mail User,

Your account has exceeded its storage limit remaining 20MB. You might not be able to receive new emails. If not verified within 48 hours we will suspend your account. Please click the link below to verify your account now.

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA
<http://bit.do/fa7jJ>

Verify Your Account Now

Thank you.
IIUM Webmaster Support.
Copyright 2019 Inc.

Subject Lines and Emails Often Include Enticing or Threatening Language or sometimes no subject at all.

Never trust an email based simply on the purported sender. Cybercriminals have many methods to disguise emails. They understand how to trick their victims into thinking a sender is legitimate, when the email is really coming from a malicious source.

It is most important to make sure that the core of the URL is correct. Be especially cautious of URLs that end in alternative domain names instead of .com or .org. Additionally, phishers use URL shorteners, such as Bitly, to bypass email filters and trick users, so be cautious of clicking on shortened URLs.

Important - Please follow these 8 guides to surf the Internet safely due to Cyber Attacks lately

IIUM Announcement <announce@iiu.edu.my>
to Iiumnet, bcc: aliiuimgp

Assalamualaikum w.b.t. Dear IIUM Community,

Cyber Attacks are increasing rapidly. Follow these 8 guides to surf the internet safely. Please be aware that cyber attacks have been increasing lately and these cyber attacks may cause big losses to individual users. We would like to ensure that we surf and use the internet safely in order to safely guard ourselves and IIUM from incurring losses. We would like to order to surf the internet safely:

1. Update your critical assets with the latest security patches and updates.
2. Warn your users not to open or click on unsolicited emails and links without attachments.
3. Ensure that anti-virus/anti-malware signatures are up to date and functioning, either the free version or paid version.
4. Review your user credentials list for any new additional unknown users.
5. If you suspect that your servers have been compromised, reset and change all usernames and passwords.
6. Perform hardening on all of your Internet-facing applications.
7. Monitor your environment closely for any anomalies.
8. Make sure your backup data is updated and is separate.

We sincerely hope everyone can implement these guides as it can protect your data, websites, computers, laptops, and the

Thank you for your kind attention, wassalam.

INFORMATION TECHNOLOGY DIVISION

Revision #1

Created Tue, Oct 29, 2019 12:33 PM by Administrator

Updated Tue, Oct 29, 2019 12:37 PM by Administrator