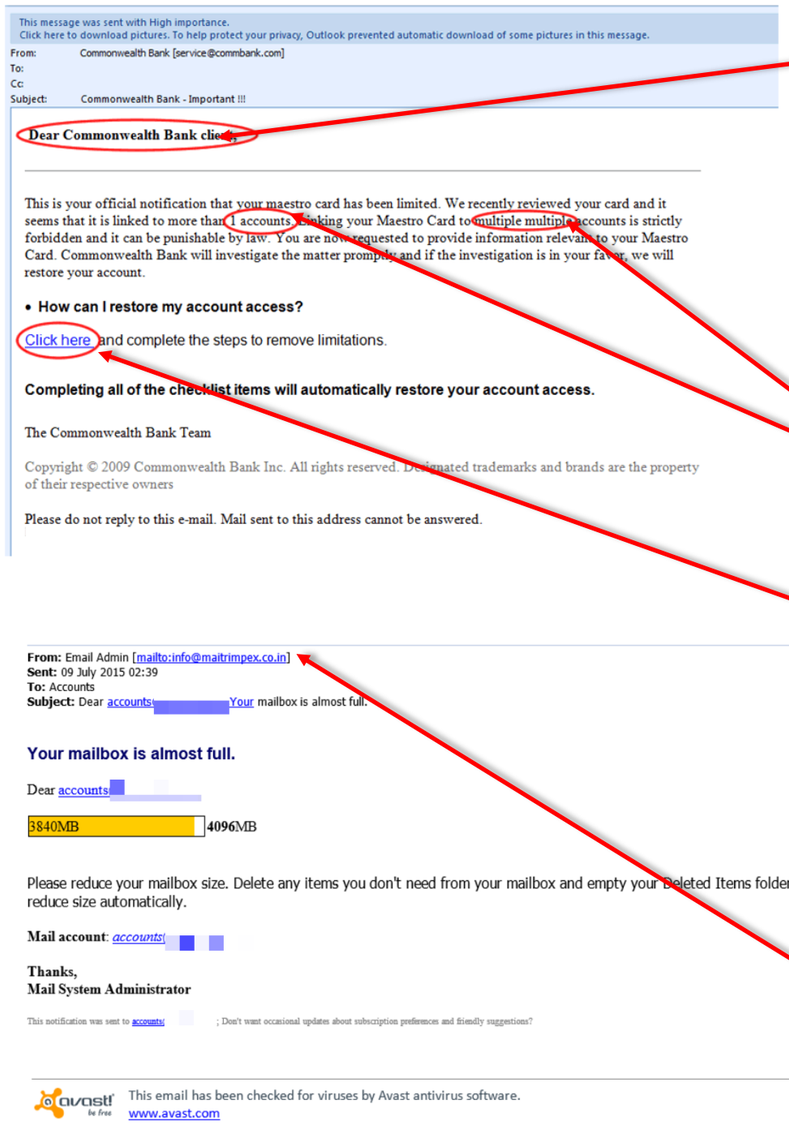
Phishing...

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting victims.

Be aware that some threats are so new, they may not yet be detectable by AV & malware vendors. Always use caution, never assume an attachment is safe. If you don't know the sender, and can't confirm the validity of the attachment: **DELETE IT!**

If you suspect that you've received a phishing or malicious email: Report it.


This message was sent with High importance.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

From: Commonwealth Bank [service@commbank.com]
To:
Cc:
Subject: Commonwealth Bank - Important !!!

Dear Commonwealth Bank client,

This is your official notification that your maestro card has been limited. We recently reviewed your card and it seems that it is linked to more than 1 accounts. Linking your Maestro Card to multiple multiple accounts is strictly forbidden and it can be punishable by law. You are now requested to provide information relevant to your Maestro Card. Commonwealth Bank will investigate the matter promptly and if the investigation is in your favor, we will restore your account.

- **How can I restore my account access?**

Click here and complete the steps to remove limitations.

Completing all of the checklist items will automatically restore your account access.

The Commonwealth Bank Team

Copyright © 2009 Commonwealth Bank Inc. All rights reserved. Designated trademarks and brands are the property of their respective owners

Please do not reply to this e-mail. Mail sent to this address cannot be answered.

Notice how the email isn't addressed to anyone specific...

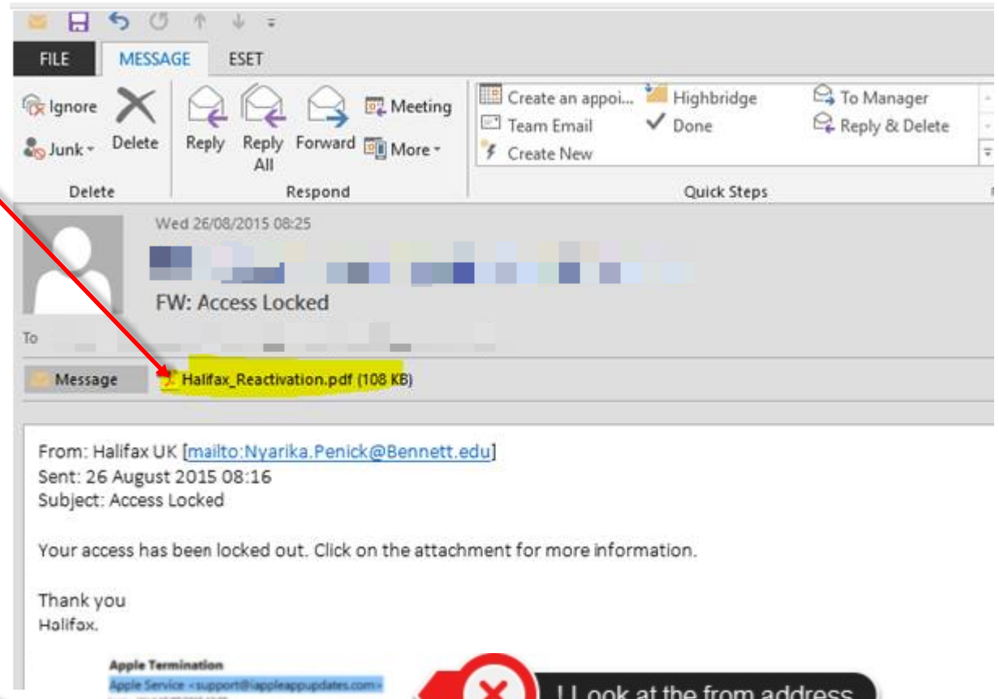
This is a common trait of phishing and spam email

Look out for malicious attachments.

In this example, the threat was so new, the AV vendor didn't detect the Trojan attachment, nor did any of the 56 AV vendors on Virus Total.

If you don't know the sender, and cant confirm the validity of the attachment, DELETE IT!

Look for spelling and grammar mistakes



The email will usually try and entice you into clicking on a link. It is this link that will either take you to a fake login page (capturing your credentials), or download a virus or piece of malware to your computer.

From: Email Admin [mailto:info@maitrimpex.co.in]
Sent: 09 July 2015 02:39
To: Accounts
Subject: Dear accounts Your mailbox is almost full.

Your mailbox is almost full.

Dear accounts

3840MB 4096MB

Please reduce your mailbox size. Delete any items you don't need from your mailbox and empty your Deleted Items folder. Click Here to do reduce size automatically.

Mail account: accounts

Thanks,
Mail System Administrator

This notification was sent to accounts ; Don't want occasional updates about subscription preferences and friendly suggestions?

avast! be free This email has been checked for viruses by Avast antivirus software.
www.avast.com

Look carefully at the From address. You may notice that these emails aren't from the companies they claim to be from, or from an email address that would having nothing to do with your IT support.

Stay Educated, Stay Informed!

For the latest news, tips & advice, follow us on twitter, or online: @the_serverninja http://the-server.ninja