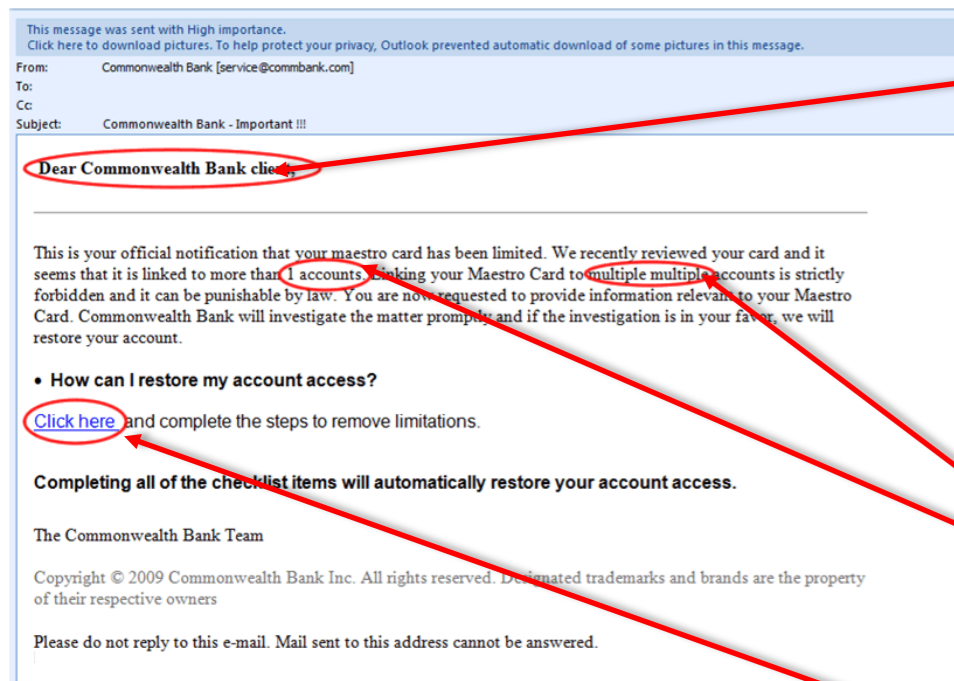


Phishing...

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.



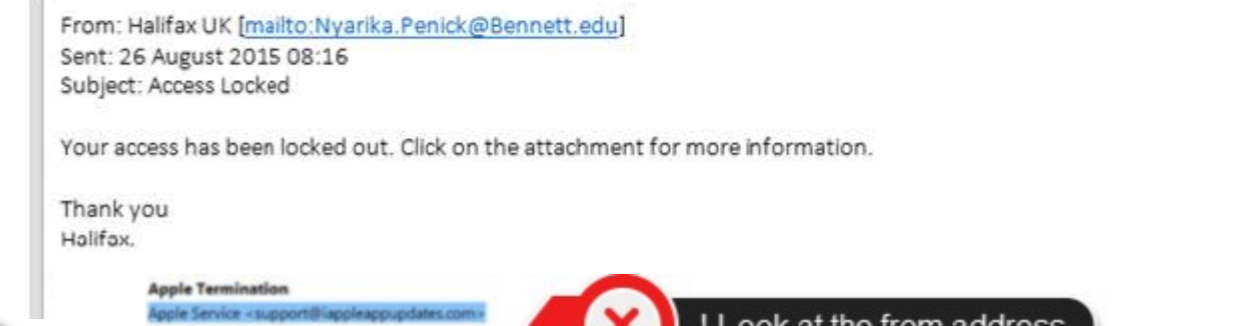
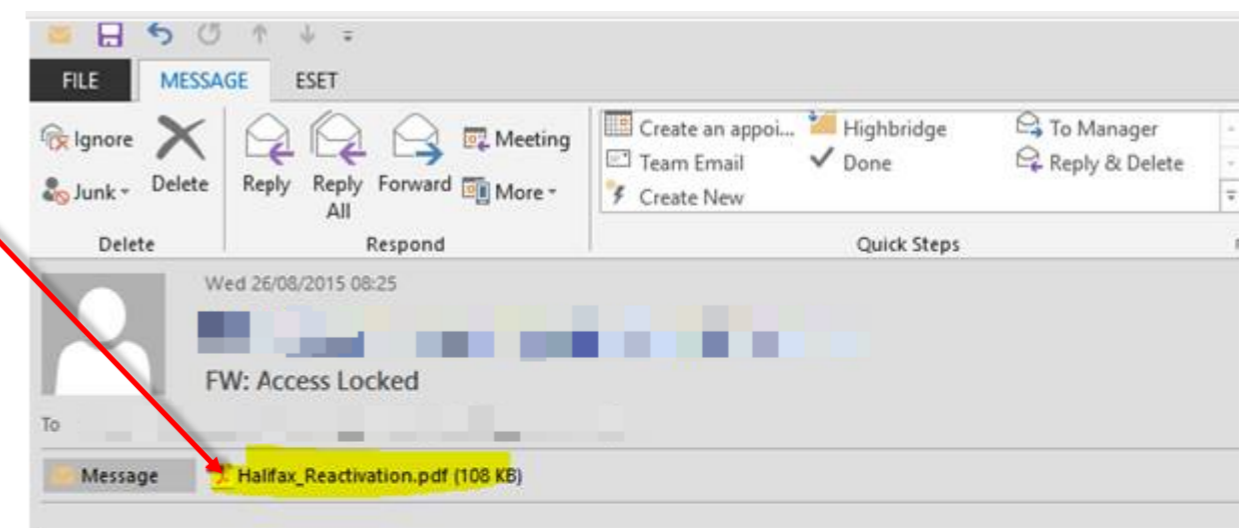
Notice how the email isn't addressed to anyone specific...
This is a common trait of phishing and spam email

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.

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>