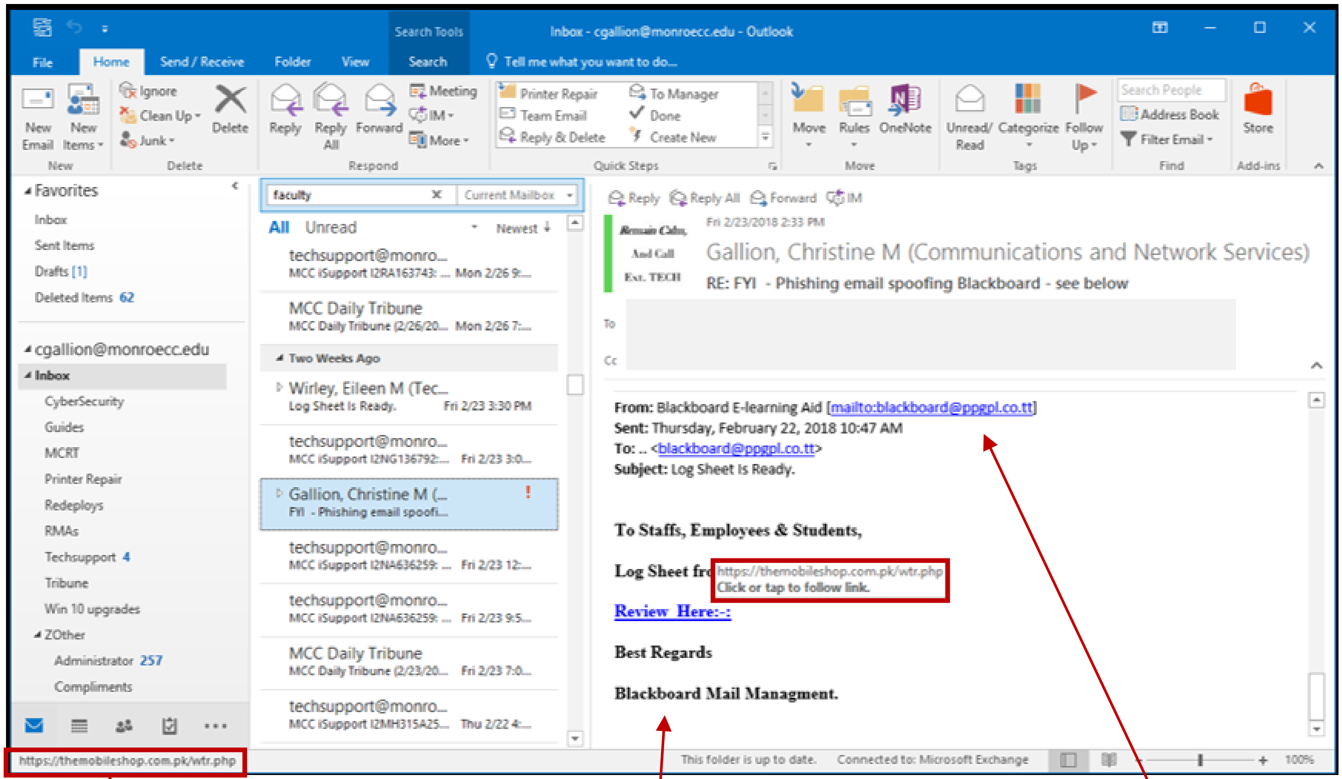
Current Phishing Attack

You should always think twice about clicking on a link in an email. Below is one of the emails from the current phishing attack.

When you hover over a link in an email the address of the link (also known as a URL) is displayed in two places in Outlook, outlined in red below. On the web version of Outlook at mymail.monroecc.edu, the link will only appear in the lower left hand corner.



Fri 2/23/2018 2:33 PM

Gallion, Christine M (Communications and Network Services)

RE: FYI - Phishing email spoofing Blackboard - see below

From: Blackboard E-learning Aid [mailto:blackboard@ppgpl.co.tt]
Sent: Thursday, February 22, 2018 10:47 AM
To: .. <blackboard@ppgpl.co.tt>
Subject: Log Sheet Is Ready.

To Staffs, Employees & Students,

Log Sheet fr

https://themobileshop.com.pk/wtr.php
Click or tap to follow link.

Review Here:-:

Best Regards

Blackboard Mail Managment.

Because this email claims to be from Blackboard:

The link address should match a monroecc.edu address or an open.suny address. The address shown here is to an unknown destination.

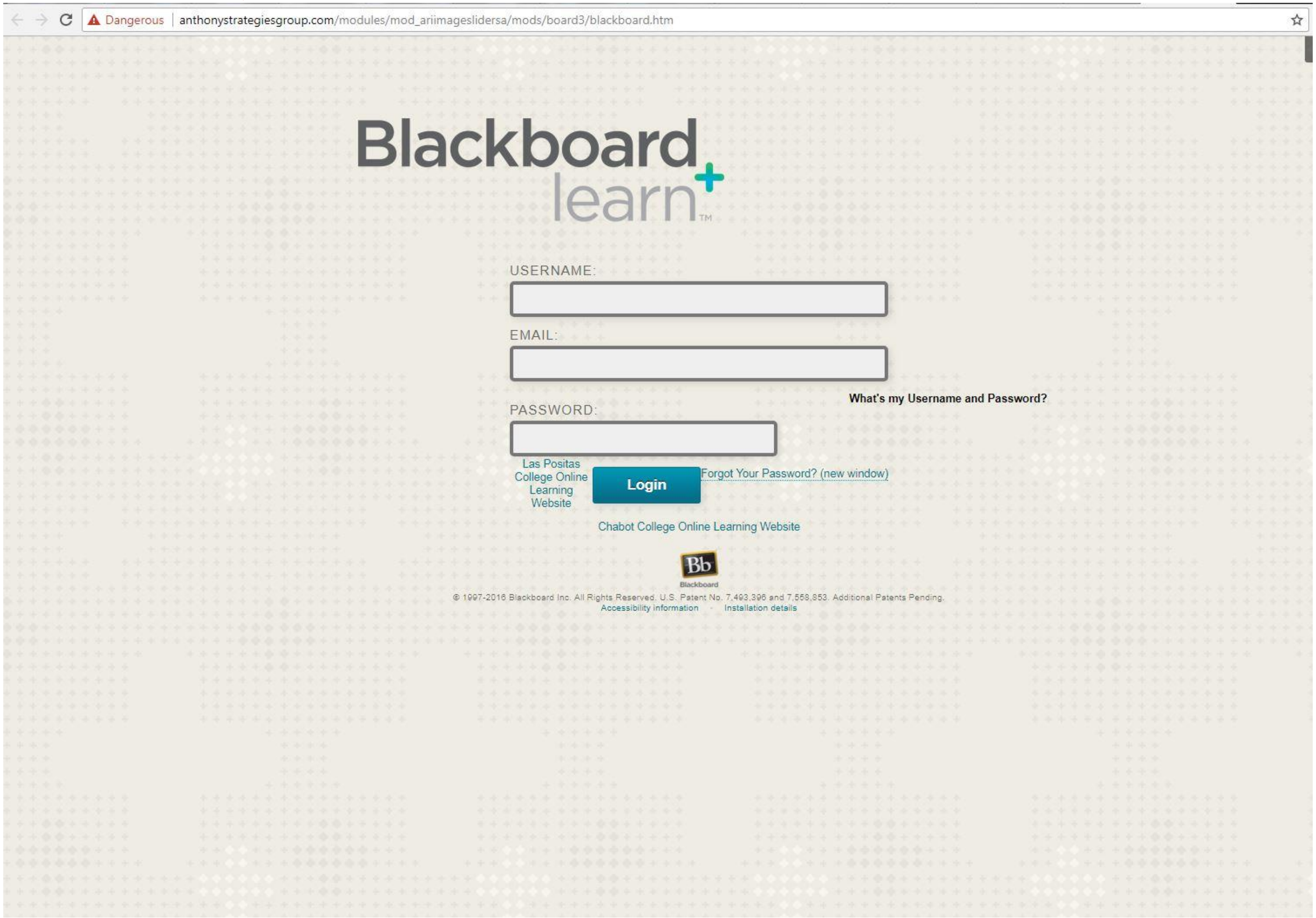
In the signature there is no contact information.

If we look at the who the email is from it should be from an @monroecc.edu or an @suny.edu address. The address shown here is from an unknown source.

You can always contact Technical Support for MCC at x8324, option 3 if you have any questions about the legitimacy of an email or if you want to report a spam email. If you know it's spam you can forward it to spamsubmission@monroecc.edu and delete it from your email.

Clicking on the link of the current phishing attempt will bring you to the very convincing site shown on the next page.

This is not a Blackboard page. Note the web address.

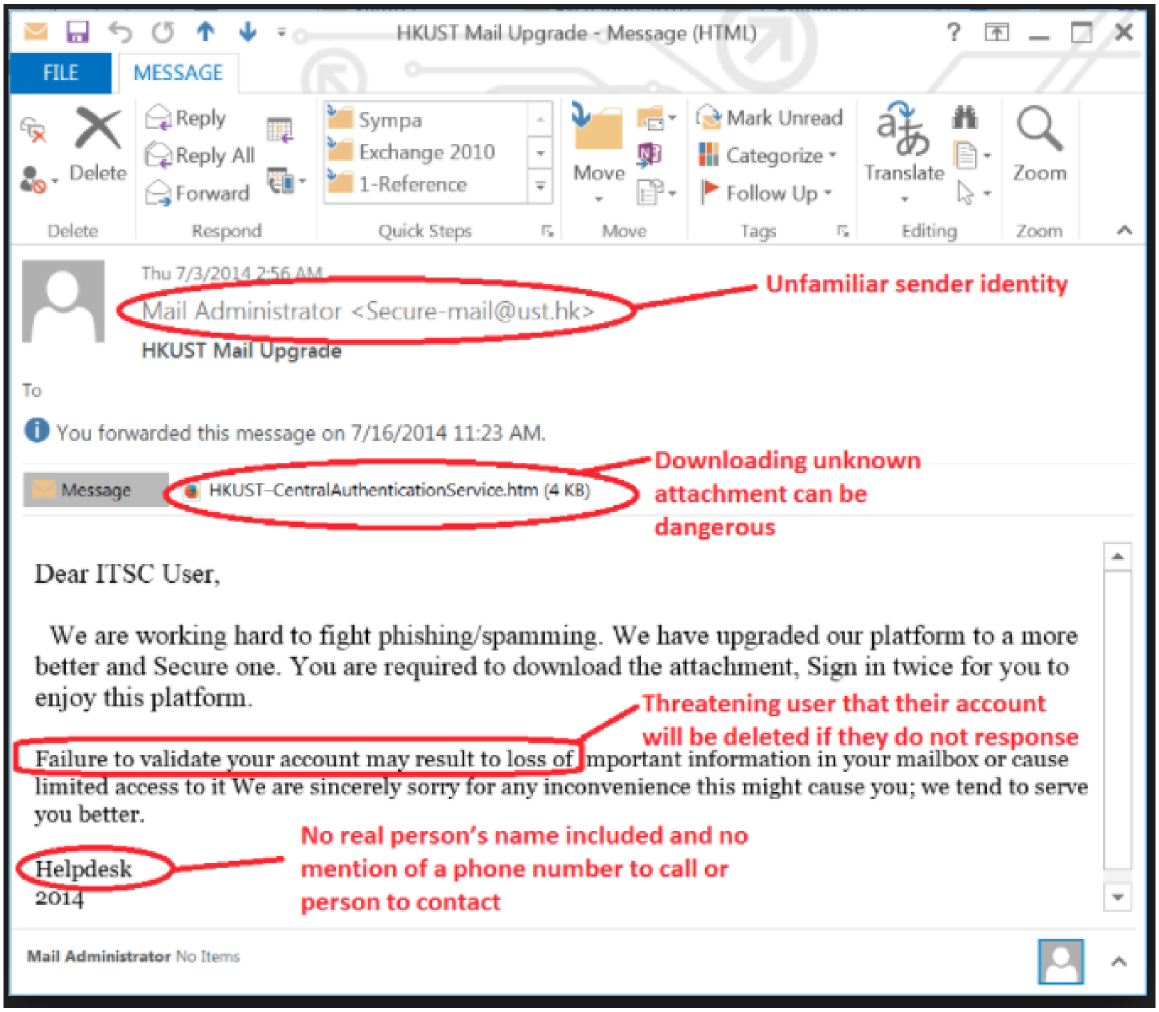


Dangerous | anthonystrategiesgroup.com/modules/mod_ariimageslidersa/mods/board3/blackboard.htm

Blackboard learn
USERNAME:
EMAIL:
What's my Username and Password?
PASSWORD:
Las Positas College Online Learning Website
Login
Forgot Your Password? (new window)
Chabot College Online Learning Website
Bb
Blackboard
Accessibility information
Installation details

© 1997-2016 Blackboard Inc. All Rights Reserved. U.S. Patent No. 7,493,396 and 7,558,853. Additional Patents Pending.

Some phishing emails are using logos to make it look like it is legitimate. There are some more examples of phishing (found on the web) on the next few pages.



Thu 7/3/2014 2:56 AM

Mail Administrator <Secure-mail@ust.hk>

Unfamiliar sender identity

HKUST Mail Upgrade

To

You forwarded this message on 7/16/2014 11:23 AM.

Message | HKUST-CentralAuthenticationService.htm (4 KB)

Downloading unknown attachment can be dangerous

Dear ITSC User,

We are working hard to fight phishing/spamming. We have upgraded our platform to a more better and Secure one. You are required to download the attachment, Sign in twice for you to enjoy this platform.

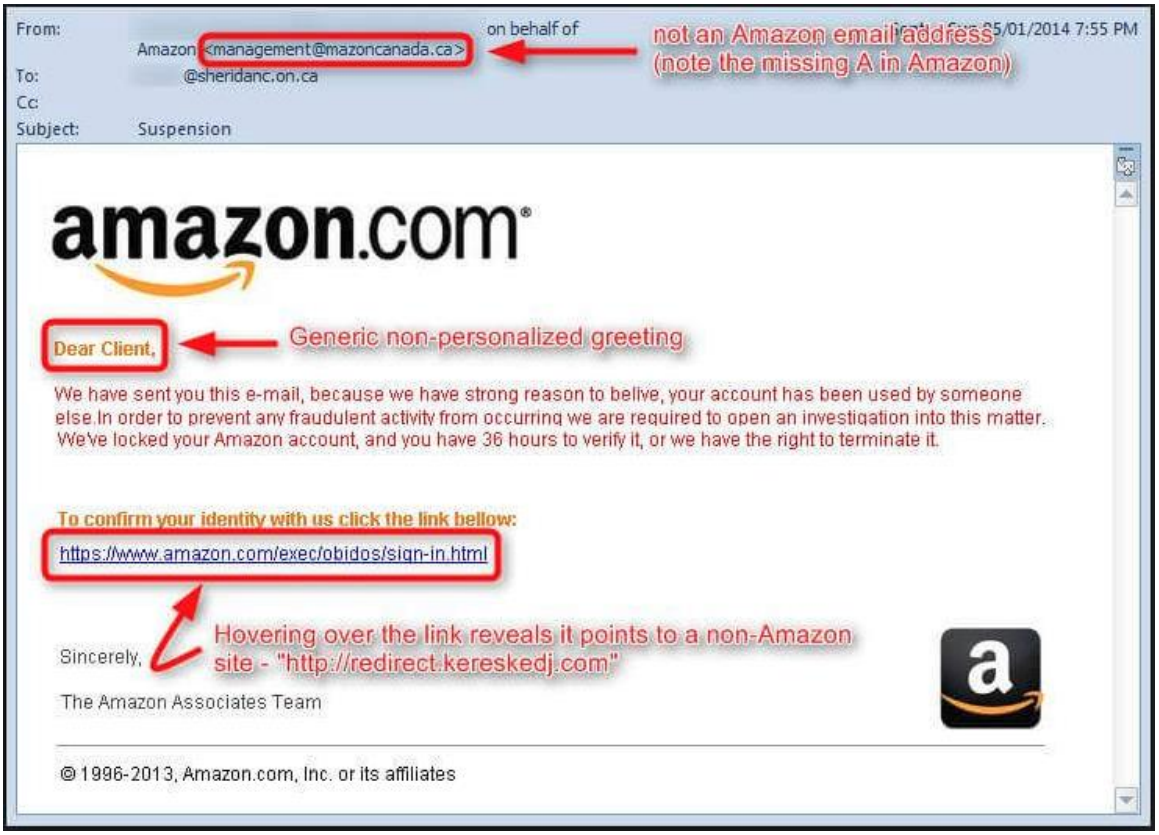
Threatening user that their account will be deleted if they do not response

Failure to validate your account may result to loss of important information in your mailbox or cause limited access to it We are sincerely sorry for any inconvenience this might cause you; we tend to serve you better.

Helpdesk
2014

No real person's name included and no mention of a phone number to call or person to contact

Mail Administrator No Items



From: [redacted] on behalf of Amazon <management@mazoncanada.ca>

5/01/2014 7:55 PM

not an Amazon email address (note the missing A in Amazon)

To: [redacted]@sheridanc.on.ca

Cc:

Subject: Suspension

amazon.com

Dear Client,

Generic non-personalized greeting

We have sent you this e-mail, because we have strong reason to belive, your account has been used by someone else.In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link bellow:

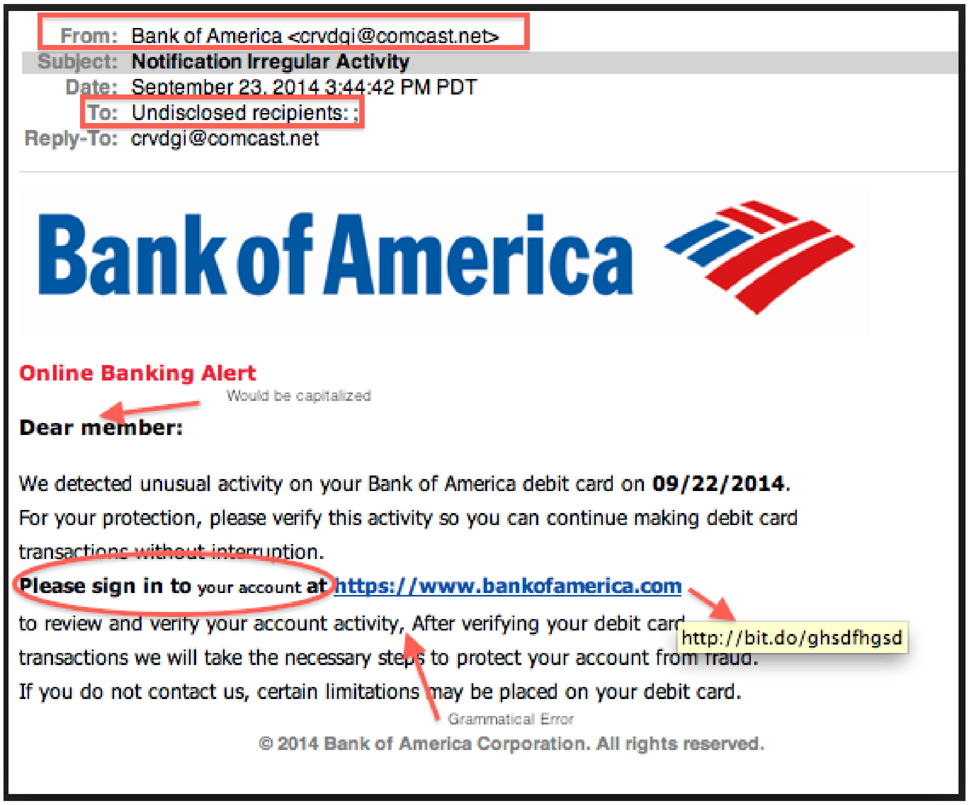
https://www.amazon.com/exec/obidos/sign-in.html

Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

Sincerely,

The Amazon Associates Team

© 1996-2013, Amazon.com, Inc. or its affiliates



From: Bank of America <crvdgi@comcast.net>
Subject: Notification Irregular Activity
Date: September 23, 2014 3:44:42 PM PDT
To: Undisclosed recipients: ;
Reply-To: crvdgi@comcast.net

Online Banking Alert

Would be capitalized

Dear member:

We detected unusual activity on your Bank of America debit card on **09/22/2014**. For your protection, please verify this activity so you can continue making debit card transactions without interruption.

Please sign in to your account **at** https://www.bankofamerica.com to review and verify your account activity, After verifying your debit card transactions we will take the necessary steps to protect your account from fraud. If you do not contact us, certain limitations may be placed on your debit card.

http://bit.do/ghsdfhgsd

Grammatical Error

© 2014 Bank of America Corporation. All rights reserved.

Hopefully these examples will help you spot phishing attacks.

As a reminder, Monroe Community College will NEVER send you an email directing you click a link and enter your MCC Network Account credentials (your username/password), and we urge you to treat ANY such requests as hacking attempts. If you know it's spam you can forward it to spamsubmission@monroecc.edu and then delete it from your email.

Additionally, no one at MCC should ever ask you for your password and you should never give anyone your password.

To see more phishing examples take the Cybersecurity Awareness Training. Go to the Technology Help tab (Tech tab) in myMCC. Click on the Cybersecurity Awareness Training link under Technology Links. On the sign in page use the dropdown to select Monroe as the campus and click on the Login button.

You can always contact Technical Support for MCC at x8324, option 3 if you have any questions about the legitimacy of an email or if you want to report a spam email.