Recent Phishing Attempts

SUFFOLK UNIVERSITY BOSTON

Here are some recent phishing attempts

Suffolk University drops over a half million (that's right over 500,000) phishing and virus emails every day. However, some do get through to your mailbox. We ask that you help us by being aware of phishing email attempts.

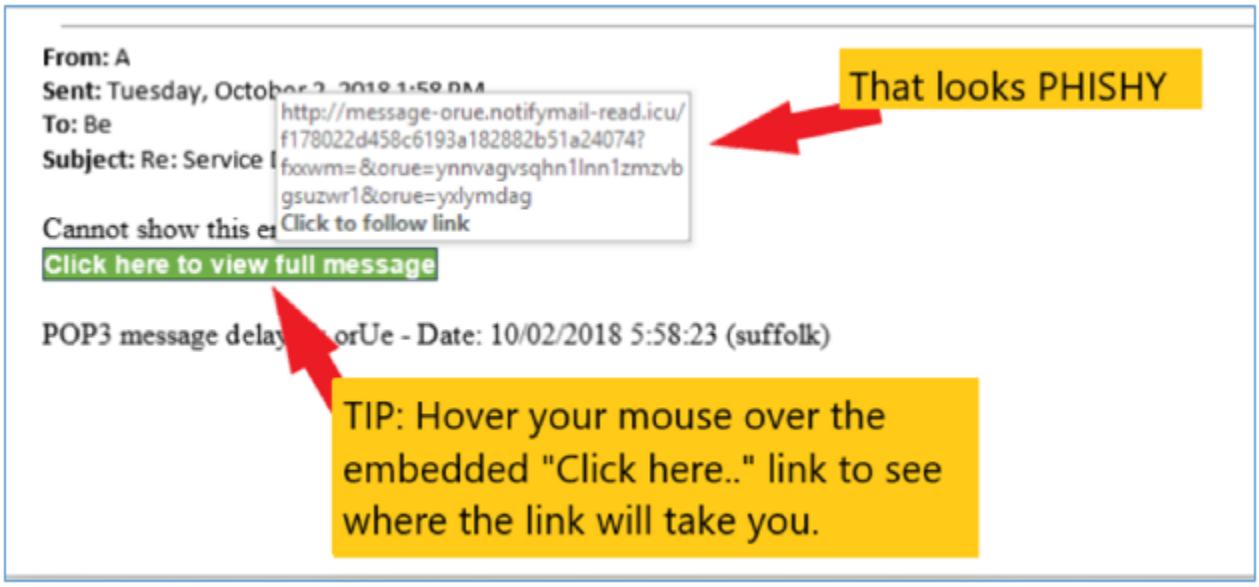
What does a Phishing email look like?

Phishing emails are typically unsolicited and have

- a generic greeting
- warning of some sudden change in an account
- and requires you to verify personal or private information that you still use the service.

These emails either include directions to reply with private information, or provide a link to a malicious web site to verify your account. Emails claiming very sudden changes or those that use poor spelling and grammar are clear warning signs of a fraudulent phishing email.

RECENT PHISHING ATTEMPTS



Oct 2 - Notice the following phishy things:

Phishing attempt to get you to click on an embedded URL web link. Notice that this link just ask to "Click here.." trying to mask where it is going to send you. This link would potentially install malware on your machine or request user credentials. Notice that if you hover your mouse over the link it would direct you to the PHISHING site. This site is obviously not Suffolk and you were not expecting the email, even if the message was addressed to you.

June 5 - Notice the following phishy things:

Phishing attempt an unexpected package is waiting for you. A package of malware. Was this a package you were expecting? Do not be fooled by email with attachments. This one you can see the attachment was removed because it was detected as malware.

From: Andrews, Amy [mailto:Amy.Andrews@sabre.com]
Sent: Tuesday, May 17, 2016 9:51 AM
To: Andrews, Amy <Amy.Andrews@sabre.com>
Subject: RE: Staff Information (MAY-2016 Bullentin)

:PASSWORD EXPIRES IN 45 MINUTES

:YOUR ARE REQUIRED TO CHANGE ACCOUNT PASSWORD IMMEDIATELY TO UPDATE :ACCOUNT/PROFILE OR ACCOUNT WILL BE DISABLED.

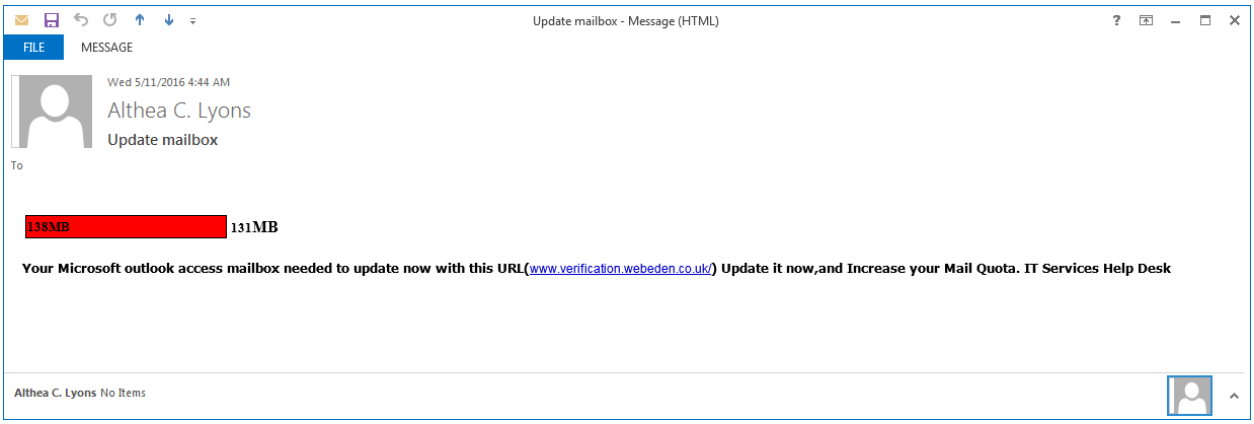
:Click on: http://www.owaresetpasscode.me/ to Update Account.

:Call the Support Center-HELP for information about any OWA :Gateway service

:Incident Report No: 110028371
:Case ID: 77MDC/ITS
:Group: Faculty/Staff
:Admin Key: XXX09273
:Date:17-05-2016

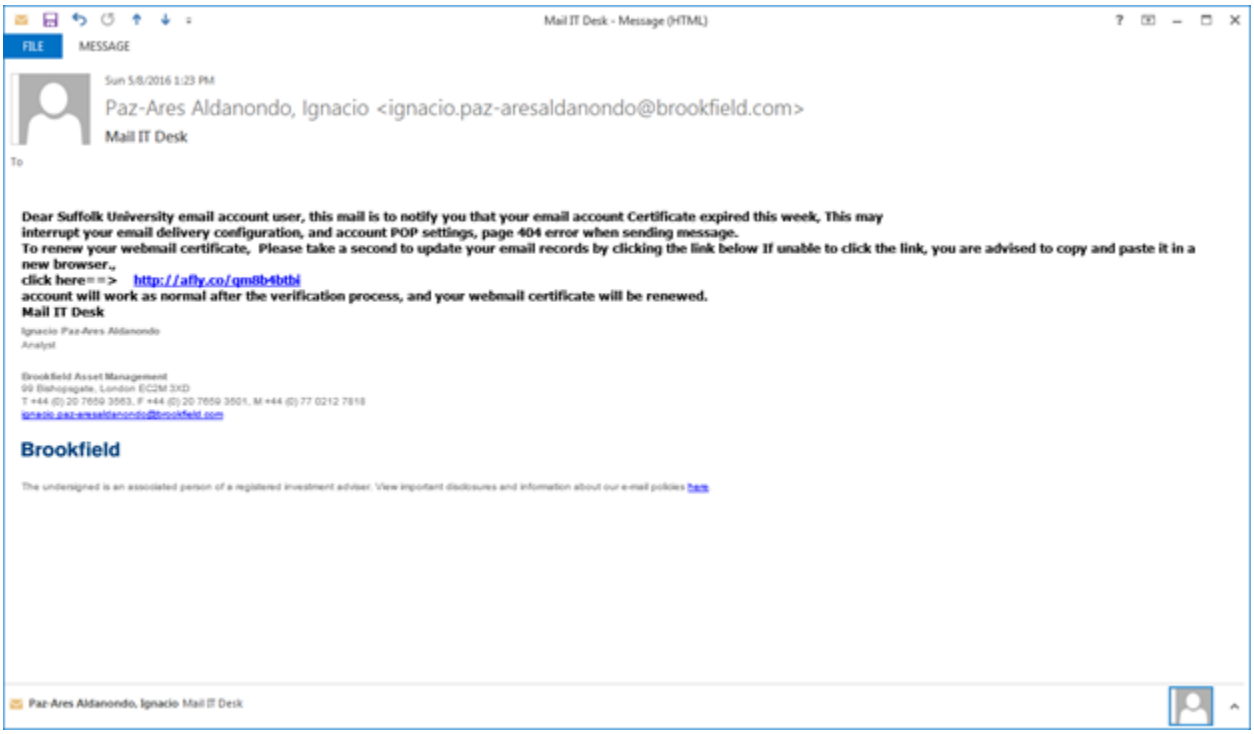
May 17 - Notice the following phishy things:

Phishing attempt filled with warning and urgency that your "PASSWORD EXPIRES IN 45 MINUTES" with a pretend Incident report number. The email addresses "From:" and "To:" name are @sabre.com, The URL(web link in the email) would send you to a web site that is definitely not Suffolk.edu.



May 11 - Notice the following phishy things:

Phishing attempt filled with warning and urgency that your mailbox needs updating "now" . The URL(web link in the email) would send you to a web site located in the United Kingdom - definitely not Suffolk.edu.

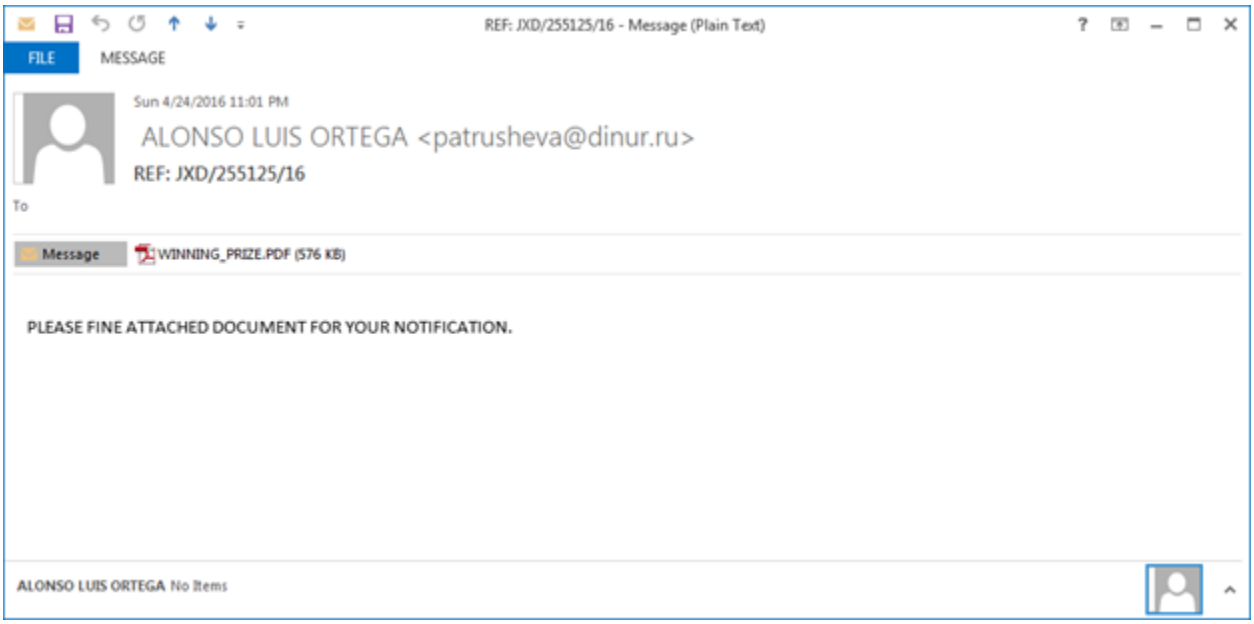


May 8 - Notice the following phishy things:

Phishing attempt to indicate you may have web email problems unless you complete the "verification process" and the email is coming from "Brookfield Asset Management" that's not Suffolk. The URL (web link in the email) asking you to "click here" and sending you to a short hidden link "http[//]afly[.]co" definitely not Suffolk.edu

May 8 - Notice the following phishy things:

Phinshing attempt filled with urgency to "update now" and "failure .. will lead to SUSPENSION .. Immediately". The URL (web link in the email) asking you to "click here" and sending you to a short hidden link "http[//]afly[.]co" definitely not Suffolk.edu



April 24 - Notice the following phishy things:

Phishing attempt indicating you won something! Wait really? "PLEASE FINE" poor grammar and spelling. Email address is from "@dinur.ru" Russia. Attachment is definitely nothing you were expecting. This attachment is PDF with a virus .

What should I do if I receive a Phishing email attempt?

Just delete the message. Do not respond in anyway. Always be skeptical when someone is requesting information, and never email your password, bank account numbers, social security, or credit card numbers to anyone. If it seems phishy it probably is.

How can I avoid phishing scams?

- Never send passwords, bank account numbers, social security numbers or other private information in an email.
- Avoid clicking links in emails, especially any that are requesting private information.
- Be wary of any unexpected email attachments or links, even from people you know.
- Never enter private or personal information into a popup window.
- Pay attention to the URL (the web site address in your browsers address bar). Look for 'https://' and a lock icon in your browser address bar and confirm the web site address before entering any private information on a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling

What should I do if I have been scammed by phishing?

Contact the organization that was the target of the scam. Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future. For Suffolk University accounts contact the Help Desk (617)557-2000. If you suspect a bank or credit card account may have been compromised, contact that institution to check your account immediately and request a credit report.