Identifying fraudulent "phishing" email

"Phishing" refers to email that attempts to fraudulently acquire personal information, such as your account password or credit card information. On the surface, the email may appear to be from a legitimate individual, but it's not.

Never send personal information in an email. This includes SSN, DOB, mother's maiden name, credit card information, account passwords, etc. Lehman College will never ask you for this information by email. This document contains a number of resources to help you learn about the risks of email scam and teaches you how to recognize a scam email.

What is Phishing or a Phishing email?

Phishing is a type of online fraud in which a scammer uses an e-mail or website to illicitly obtain confidential information. Phishing scams frequently involve a copycat website designed to mimic that of a legitimate organization, often a college/university asking users to transmit sensitive data.

Phishing email is a form of an email message that asks you to reply to the message with confidential information, such as your user ID and password. Never respond to any email with confidential information. CUNY or Lehman College will never ask for this information via email. Many times these webpages look like legitimate sites, such as **Email Account Verification, URGENT WARNING! – ACT FAST NOW, Bank of America, or Pay Pal**, but they are not. When you provide your user ID and password, this information is captured by the phisher who can then use it to log into the legitimate site.

How do I identify phishing scams?

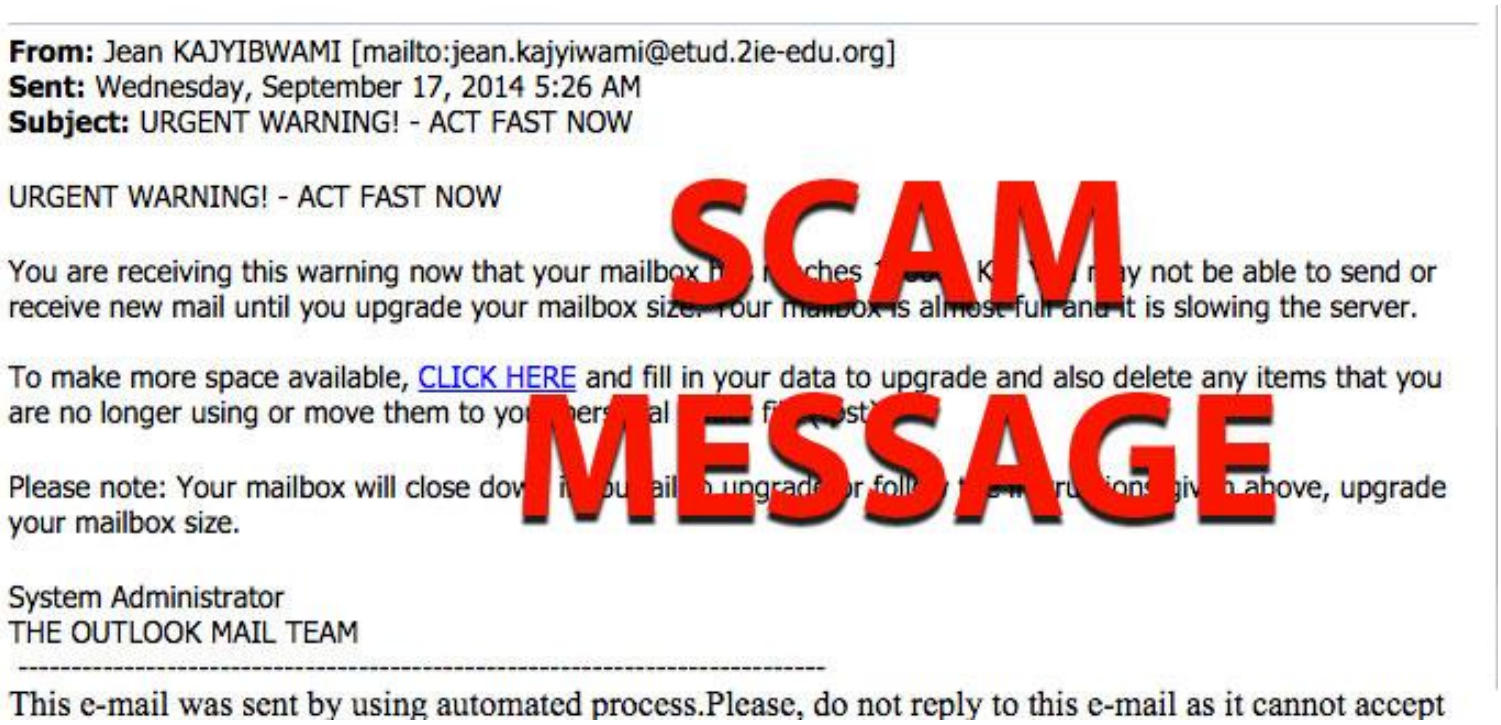
If you are unsure if an email is legitimate, read this document or contact our Help Desk before replying or clicking on a link. Keep in mind that CUNY or Lehman College IT Division will never request your username or password or any other personal information such your SSN, DOB, mother's maiden name, credit card information, account passwords, or extensive personal information by email.

Phishing emails:

- May show the sender on behalf of someone.
- Generally require you to take quick action, such as verifying your account to prevent it from being deactivated.

Be particularly vigilant during holidays or during significant events since attackers heighten their activity during these times.

Sample of a phishing email:



From: Jean KAJYIBWAMI [mailto:jean.kajyiwami@etud.2ie-edu.org]
Sent: Wednesday, September 17, 2014 5:26 AM
Subject: URGENT WARNING! - ACT FAST NOW

URGENT WARNING! - ACT FAST NOW

You are receiving this warning now that your mailbox h[illegible] ches [illegible] K[illegible] y not be able to send or receive new mail until you upgrade your mailbox size. Your mailbox is almost full and it is slowing the server.

To make more space available, CLICK HERE and fill in your data to upgrade and also delete any items that you are no longer using or move them to yo[illegible]al [illegible] f[illegible]st)

Please note: Your mailbox will close dow[illegible] ail to upgrad[illegible] follo[illegible] ru[illegible]ions giv[illegible] above, upgrade your mailbox size.

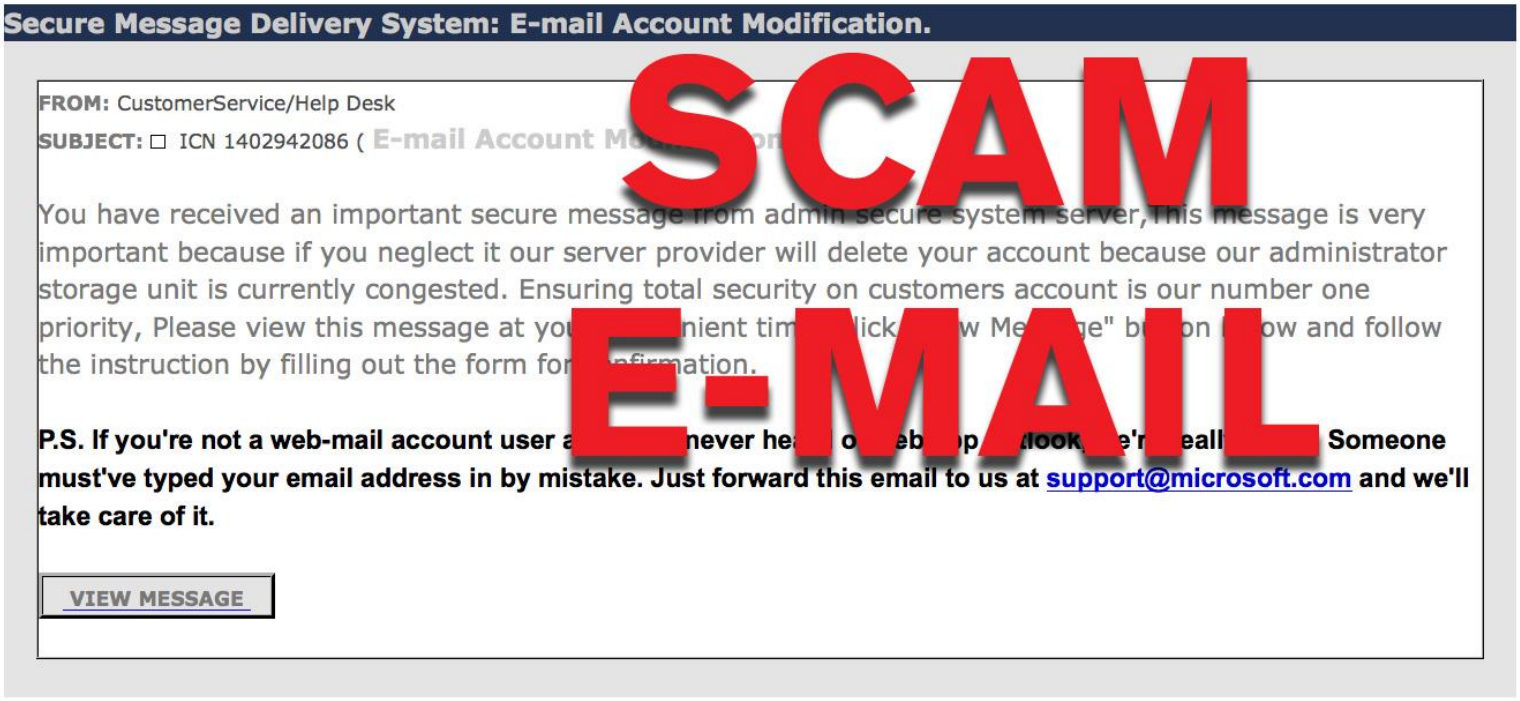
System Administrator
THE OUTLOOK MAIL TEAM

This e-mail was sent by using automated process.Please, do not reply to this e-mail as it cannot accept

SCAM MESSAGE

Another sample of a phishing email:

From: Betty Spradley <bspradley@lcisd.org>
Date: Friday, January 31, 2014 at 8:14 AM
To: Betty Spradley <bspradley@lcisd.org>
Subject: RE: E-MAIL ACCOUNT VERIFICATION



How to Protect Yourself?

Here are some best practices that will help protect you and your information:

- Beware of messages that claim your account has been suspended.
- Be suspicious of any email containing urgent requests for personal or financial information.
- **DO NOT** click on suspicious or shortened links.
- Be suspicious of email messages and other electronic communications from sources you do not know or recognize.

- Never reply to any email that asks you for your personal information such as social security number, usernames and passwords, account numbers, and date of birth, regardless of now official it may appear.
- Have the latest security software updates (patches) installed and keep your anti-virus software up to date.
- If an email communication looks suspicious, or too good to be true, it probably is. **Delete the message immediately**.
- Report any suspicious emails.

Getting Help

For additional assistance, the following resources are available:

- Contact IT Center Help Desk (Carman Hall 108 or in the Library or (718) 960-1111 or help.desk@lehman.cuny.edu)
- http://www.antiphishing.org/
- http://security.cuny.edu