

Library & Technology Services



MENU

Recent Phishing Examples

[account compromise \(5\)](#) [account expiration \(2\)](#) [account suspension \(2\)](#) [alerts \(1\)](#) [Amazon \(2\)](#) [anti-phishing \(1\)](#) [antivirus \(1\)](#)
[BBB \(1\)](#) [calendar \(1\)](#) [certificate \(1\)](#) [complaint \(1\)](#) [courseware \(1\)](#) [email \(1\)](#) [fake \(1\)](#) [fax \(1\)](#) [finance \(1\)](#) [fraud \(1\)](#)
[help desk services \(1\)](#) [helpdesk \(1\)](#) [internship \(1\)](#) [IRS \(2\)](#) [legal matter \(1\)](#) [Lehigh \(11\)](#) [LinkedIn \(3\)](#) [login \(6\)](#)
[online banking \(4\)](#) [online ordering \(2\)](#) [password stealer \(1\)](#) [portal \(5\)](#) [quota \(3\)](#) [refund \(1\)](#) [resume \(1\)](#) [scanner \(1\)](#)
[security \(1\)](#) [social networking \(3\)](#) [tax \(2\)](#) [travel \(1\)](#) [upgrade-update \(8\)](#) [Urgent Alert Phishing \(1\)](#) [verify-validate \(6\)](#)
[virus threat \(5\)](#) [webmail \(11\)](#) [Webmail Quota Upgrade \(1\)](#) [Word document \(1\)](#)

Password Phishing Scam Messages - 5/25/2017

Thursday, May 25, 2017 - 18:05

This message fraudulently tells you your account is about to expire and tries to get you to click the link to read the message. The sender of the message is not from Lehigh and the link takes you to a non-Lehigh site which may have malicious software. Delete this message. NOTE: you can hover over links to see that it does not go to a real Lehigh domain. You can also verify if your account will soon expire by going to your Lehigh Account web page linked at the bottom of the main Lehigh and Inside Lehigh web pages.

From: **Mary Illgen** <MIllgen@wctc.edu>
Date: Thu, May 25, 2017 at 4:06 PM
Subject: Lehigh.
To:

Dear Lehigh Users,

The password associated with this account will expire shortly. To continue using this account without any changes, click on the "Keep My MAIL ACCOUNT" button below:

[MAIL ACCOUNT](#)

Please Note: This request is compulsory if you do not keep your account, it may lead to service suspension.

We apologize for any inconveniences this may have caused.

Thank you,
Lehigh university help desk.

Drob Box Phishing Scam Messages - 5/3/2017

Wednesday, May 3, 2017 - 16:53

Lehigh has been experiencing a number of phishing messages using emails with links to Drop Box documents. If you hover your mouse cursor over the link, it will show the address it is attempting to get you to go to. The messages may appear to be from people you know. If you are not expecting a file, you should immediately be suspicious and use extreme caution. If you have clicked on anything that requires a password you feel is not legitimate, it is always a good idea to reset your Lehigh password at <https://www.lehigh.edu/change>.

Hi there,

Wilson has shared a document "Signed Wire Payment Receipt.pdf" on
Dropbox with you.

[View Document Now](#)

Documents will be removed from our system upon the request of the sender.

Enjoy!

The Dropbox team

Google Phishing Scam Messages - 5/3/2017

Wednesday, May 3, 2017 - 16:37

USE EXTREME CAUTION! Lehigh and locations across the country (and possibly world-wide) have been experiencing a high volume of phishing messages using emails with links to Google Documents which use malicious code to affect your Google account. These are being caused by a compromised Google App which has now been blocked by Google, but there will be continued issues with those who were compromised before the problem was blocked.



Urgent-Important Campus Alert!

Wednesday, December 7, 2016 - 14:59


This is a phishing email intended to get you to enter credentials on a non-Lehigh web page. You will notice:

- 1) Sender is from an alleged Canadian address (uoguelph.ca)
- 2) Hovering over the link displays it goes to a non-Lehigh address.
- 3) Signed by Richard Nixon
- 4) Falsely lists our address in the signature line.
- 5) Uses urgency (you must act now) as a scare tactic to get you to respond.

Please be aware of these types of details when you see messages of a questionable nature,

LTS

Re: Urgent-Important Campus Alert! (Lehigh.Edu) Inbox x

 Elizabeth Birks <ebirks@uoguelph.ca>

to ▾

Re: Urgent-Important Campus Alert! (Lehigh.Edu)

Hello,

There's a police situation on campus, we encourage everyone to read and follow protocol.

This message is sent via secured HTML [Click Here](#) to view.

Thanks,
Richard Nixon,
Lehigh University

provides a leading-edge library and technology environment that enables flexibility, innovation, experience, research, administration, community-building and outreach.

Contact Information
Library & Technology Services
FWEM Library

BlackBoard Mail message

Tuesday, October 4, 2016 - 08:44

This is likely a message distributed to a number of universities -- Lehigh is not a BlackBoard institution (we use Moodle, or CourseSite). Note that the sender is not a Lehigh email address and the grammar is poor.



BLACKBOARD NEWS <zaratefergusson@comcast.net>

to ▾

Dear Staff, Employee & Student,

You have Two (2) important security message from BlackBoard

[Continue To View Here:](#)

***Sincerely,
BlackBoard Mail***

IT Service: Mail Exceeded Allocated Storage

Monday, July 25, 2016 - 10:15

Notice the two features identifying this as a phishing email:

- 1) The sender (highlighted) is not a Lehigh account;
- 2) the link in the email (highlighted) is to a non-lehigh web address.

Do not click on the link, and simply delete this email.

From: IT Service <clarkbakerfunding@gmail.com>
Date: Mon, Jul 25, 2016 at 7:52 AM
Subject:
To:

Attn: Lehigh University web-mail User,

We noticed that your mailbox has exceeded the allocated storage limit as set by our administrator, you will not be able to send or received email until you upgrade your allocated quota for effective use.

To upgrade your quota now, you need to Copy/click below link to fill the upgrade form.:

<http://admincentre.byethost13.com/form.php>

Failure to do this will have your account inactive.

Lehigh University Support Team.
27 Memorial Drive West, Bethlehem, PA 18015 USA · Phone: [\(610\) 758-3000](tel:6107583000)

Copyright ©2016
All rights reserved.

Phishing example from consumer Gmail account

Monday, July 25, 2016 - 08:13

Phishing example from July 25, 216. Note that sender is a generic Gmail account and the link is not Lehigh branded. The footer and greeting contains some Lehigh-specific information, but URL is not a Lehigh domain, the sender is not a Lehigh domain, and the message is sent impersonally to "undisclosed recipients."

From: IT Service <clarkbakerfunding@gmail.com>
Date: July 25, 2016 at 7:55:10 AM EDT
To: undisclosed-recipients;;

Attn: Lehigh University web-mail User,

We noticed that your mailbox has exceeded the allocated storage limit as set by our administrator, you will not be able to send or received email until you upgrade your allocated quota for effective use.

To upgrade your quota now, you need to Copy/click below link to fill the upgrade form.:

<http://admincentre.byethost13.com/form.php>

Failure to do this will have your account inactive.

Lehigh University Support Team.
27 Memorial Drive West, Bethlehem, PA 18015 USA · Phone: [\(610\) 758-3000](tel:6107583000)

Copyright ©2016
All rights reserved.

Phishing invoice with attachment

Thursday, April 14, 2016 - 11:01

Another message received by a Lehigh staff member working in a financial area. The message was personalized to the staff member and had a .doc attachment which likely contains malicious content.

----- Forwarded message -----
From: **Caroline Nicholse** <bpickel@cox.net>
Date: Wed, Apr 13, 2016 at 1:27 PM
Subject: NET-45 Invoice - Lehigh University
To:

Dear

Here's the invoice for Lehigh University. We we are hoping for your early payment of \$1,277.00.

Thanks for your business!
Nordea Bank Finland Plc, New York Branch

--

Sterling Bank

Thursday, April 14, 2016 - 10:59

Example of a spear phishing message that has been targeting financial departments at Lehigh.

----- Forwarded message -----
From: Doug Williams <chrspid@t-online.de>
Date: Wed, Apr 13, 2016 at 11:47 AM
Subject: Invoice for Lehigh University ; Attention: Controller
To:

This is a private message for the Controller, Lehigh University. If it is not you, please ignore and discard it.

Hi John Gasdaska,

Since we have not received a contract termination letter, I am assuming that you might have unintentionally overlooked our invoice 04/16000331799 (Unpaid). If you intend to bring to an end the account, just let us know. Be informed that early withdrawal penalties will apply.

Refer to the attached document for billing information.

Regards,
Doug.

Doug Williams
Sterling Savings Bank | Accounting and Billing Team
6400 Uptown Blvd Ne, Albuquerque, New Mexico, 87110
T: [866-905-9901](tel:866-905-9901) | Copyright © 2016

Re: Expiration Notice

Thursday, January 28, 2016 - 14:49

This is a bogus message about Lehigh Library Accounts. Lehigh Library accounts don't expire. Looking at the send address reveals that it's from a commercial Gmail address (ends in @gmail.com) not from a Lehigh email address, which ends in @lehigh.edu. Another clue that this is phishing message is that the URL points to a domain ending in **.ga**, NOT **lehigh.edu**.

On Thu, Jan 28, 2016 at 1:08 PM, Julie Miller <jymiller2@gmail.com> wrote:

Dear User,

This message is to inform you that your access to your library account will soon expire. You will have to login to your account to continue to have access to the library services in the new year.
You need to reactivate it just by logging in through the following URL. A successful login will activate your account and you will be redirected to your library profile.

http://library.lehigh.saea.ga/asa2.0/MyResearch_2Ltqum5JFHNfChe8hG2l8BYjMOXLf4djeoiD1V7sDUd69NjMh6fhTAQjUYni3EFv0XAvqCWXceuh3IPfUD790Psmm8/

If you are not able to login, please contact Julie Miller at jym2@lehigh.edu for immediate assistance.

Sincerely,

Julie Miller
Linderman Library
Lehigh University
[610-758-3985](tel:610-758-3985)
jym2@lehigh.edu

...

Fake request to restore service after inactiveness

Wednesday, January 27, 2016 - 15:47

Be alert to phishing messages like this example which try to fool you into clicking the link because it contains "Itshelpdesk". You will notice that the link actually goes to the domain 'moonfruit.com', and was sent from an email address reportedly from 'slu.edu', not 'lehigh.edu'. Another hint of possible phishing is the emphasis on urgency and poor grammar.

Do not click on links that you are unfamiliar with, or that don't come from lehigh.edu domains. Simply delete the message.

From: LTSHelp desk <lesnakpb@slu.edu>
Date: Wed, Jan 27, 2016 at 2:55 PM
Subject: Important message
To:

Your Email Access have been restricted, due to several hours of in-activeness on-line. For your e-mail access restoration Please verify it with the link below
<http://ltshelpdesk.moonfruit.com>

Powered By Help Desk.

Exceeded Web Mail Quota

Wednesday, December 9, 2015 - 16:28

Message falsely claims you have reached your 500MB limit on Lehigh Web Mail. You may note the sender has a .pk (Pakistan) email address. The link for Lehigh Web Mail may work, but the link to "Click Here" takes you to a non-Lehigh Google web form in an attempt to collect your username and password.

Do not click either link. Simply delete this message.

From: DR. FARHAT MUNIR <farhat.munir@umt.edu.pk>
Date: Wed, Dec 9, 2015 at 3:21 PM
Subject: lehigh update
To:

You have exceeded your webmail.lehigh.edu quota limit of 500MB and you need to expand your mail quota limit. To Upgrade Your Account [Click Here:](#)

help desk

Important Message

Monday, December 7, 2015 - 16:01

Clues that this is a phishing message and not a legitimate Lehigh email:

1. The sender's non-Lehigh email address
2. Incorrect spelling
3. The link takes you outside of the lehigh.edu domain

If you are a Lehigh Gmail user, you can report this as a phishing message:

1. At the top-right corner of the message, click the down arrow next to the Reply button.
2. Select Report Phishing from the drop-down list--the message will go directly into your Spam folder.

Subject: Important Message

Date: Mon, 7 Dec 2015 19:54:41 +0000 (UTC)

From: Lehigh University Alert <slowmotions12@comcast.net>

You have two security messages

Kindly sing in to view

[Sign In](#)

Lehigh University

Lehigh University Terror Alert***

Saturday, November 14, 2015 - 15:17

The non-Lehigh email address this was sent from, the grammatical errors and vague contextual information, and the fact that the messages requests your username and password are all clues that this is phishing scam. Always remember, LTS will never ask you for your password.

As a Gmail user, you can report this as a phishing message:

1. At the top-right corner of the message, click the down arrow next to the *Reply* button.
2. Select *Report Phishing* from the drop-down list--the message will go directly into your Spam folder.

Lehigh University IT Centre <yw0007@uah.edu>

to 

This is to notify you that the Lehigh University received a terror threat through your email concerning the University information systems shutdown. The (IT) Policy Help Center STRICTLY require mail account cleared from sending terror messages through the University email system and also to upgrade your email account for an active affiliation with cyber technology services.

You are required to provide the following information in response to this email for activation and proper verification and scrutiny:

Username:

Password:

Your email account is scheduled to be deactivated within 24 hours of "Non Compliance. After that time, you will not be able to access your mail box. Emails sent to your mailbox will be rejected.

Lehigh University
27 MEMORIAL DRIVE WEST, BETHLEHEM, PA 18015 USA ·
PHONE: [\(610\) 768-3050](tel:6107683050)
Site maintained by IT Division

Important Blackboard Message Phishing Mail

Thursday, November 12, 2015 - 10:45

This phishing mail claims to be from Blackboard Learning regarding an important course work message. It is addressed to the user, and the link also includes the user's email address in the link text. Hovering over the link will reveal that the true destination of the link has nothing to do with Lehigh University at all, and typically points to another country.

Do not click the link. Simply discard this message.

From: Member <Dots9062@stthomas.edu>
Date: Wed, Nov 11, 2015 at 1:35 PM
Subject: Notice from your faculty management (inspc@lehigh.edu)
To: inspc@lehigh.edu

Important course work message's by (Blackboard Learning)

Use the provided link below to read your message's

<https://course.blackboard.edu/login/inspc@lehigh.edu/>

Thanks

Blackboard IT Learning

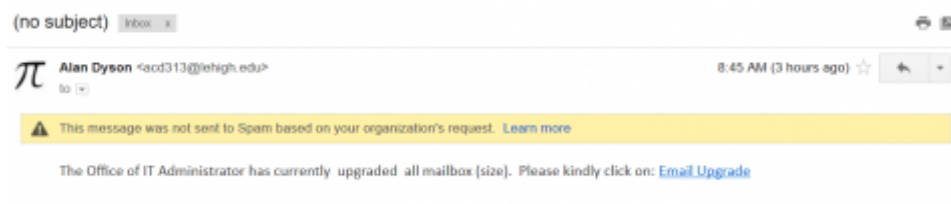
Email Upgrade

Thursday, October 22, 2015 - 13:20

Like any other phishing message you'll receive, hovering over the link shows that the it does NOT take you to a Lehigh University webpage (all Lehigh pages will end in .EDU).

Simply report it as phishing if you're a Gmail user:

1. At the top-right corner of the message, click the down arrow next to the "Reply" button.
2. Select Report Phishing--the message will go directly into Spam



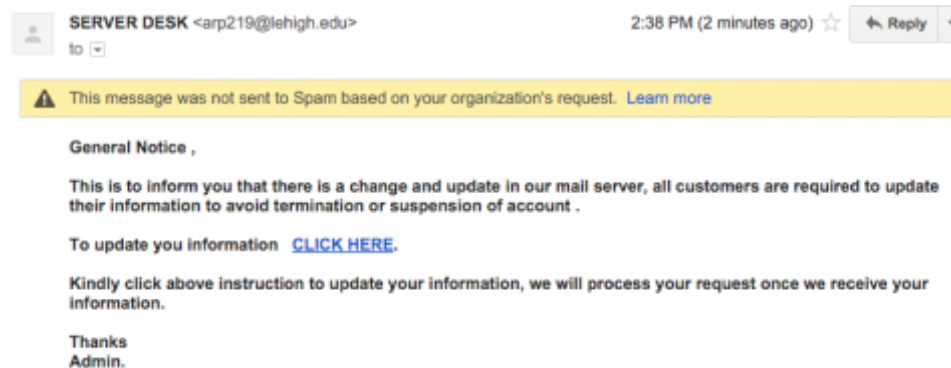
With Subject Line: DT, db, or bD

Wednesday, October 21, 2015 - 14:46

The non-Lehigh URL, <http://webbmail-vcu.bravesites.com/> (note that it ends in bravesites.COM, not LEHIGH.EDU) is a clue that this is a phishing message.

If you are a Gmail user, you can mark it as Phishing by opening the message and:

1. At the top-right corner of the message, click the down arrow next to the "Reply" button.
2. Select Report Phishing.



Dear Lehigh.edu Account User

Tuesday, September 22, 2015 - 11:03

The non-Lehigh email address (ends in @udd.cl) and non-Lehigh URL, <http://sso-cc-lehigh-edu.jimdo.com/> (note that it ends in JIMDO.COM, not LEHIGH.EDU) are clear warning signs this is a phishing message and not from the Help Desk. Grammar and punctuation errors are also always common red flags...

If you are a Gmail user, you can mark it as Phishing by opening the message and:

1. At the top-right corner of the message, click the down arrow next to the "Reply" button.
2. Select Report Phishing.

From: LTS Help Desk <esaezt@udd.cl>
Date: September 22, 2015 at 8:33:04 AM EDT
To: undisclosed-recipients;
Subject: Dear lehigh.edu Account User,

Dear lehigh.edu Account User,

This is a courtesy notice from your lehigh.edu Help Desk and it's to inform you that your email account has exceeded it's mail quota on the database server. click the following link below and also follow the instructions to verify your account.

<http://sso-cc-lehigh-edu.jimdo.com/>

Thanks,
Library & Technology Services | Lehigh University

Wells Fargo Account Scam

Sunday, September 13, 2015 - 20:09

This is a classic phishing scam using scare tactics to get you to reveal personal information. Note that the apparent sender of the message (@cyberlink.ch) is in Switzerland.

Wells Fargo Bank <capsulecorp1@cyberlink.ch>

to Recipients ▾

Download and View the attached Official Notification and reasons for the suspension of your Online Services.

You are required to proceed by following the steps below

- 1.) Downloading and Saving the attached Suspension Notice.
- 2.) Open the Suspension Notice with your web browser. You have to be connected to the Internet to view (Message is compatible with all browsers and can be viewed easily).
- 3.) Read all instructions on the Suspension Notice carefully
- 4.) Fill out all required fields and click "SUBMIT"

Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.

Please do not respond to this e-mail. If you wish to contact us via e-mail, please use secure messaging e-mail located in the Customer Service section of your Wells Fargo Bank Online Banking portal.

2015 Wells Fargo Bank Member FDIC. All rights reserved

Webmail Account Certificate?

Tuesday, September 1, 2015 - 08:23

This email, which purports to be from the "Help Desk®" with the subject "Your Mailbox" claims that you need to update and verify your Webmail certificate. It will ask you to click a link within the email to provide your credentials. This is NOT legitimate! You will never be asked by LTS to provide your credentials through a direct link within an email. Please delete this email or any similar email that hits your inbox.

From: **Help Desk®** <[redacted]@lehigh.edu>

Date: Tue, Sep 1, 2015 at 7:36 AM

Subject: Your Mailbox

To:

Your Web mail account Certificate is about to expire, not to interrupt your email delivery configuration and account POP settings when sending message.

To re-new your web mail Certificate, Please take a second to update your records

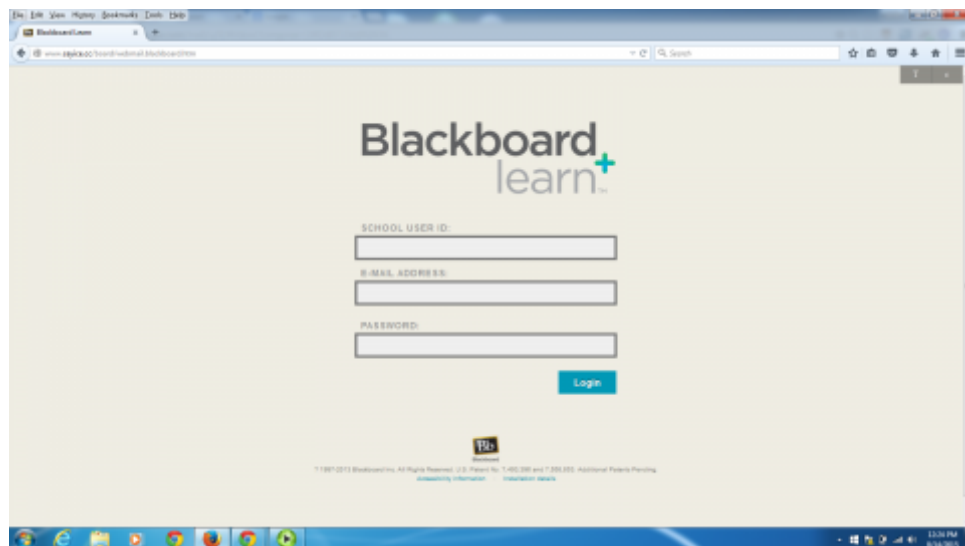
With this link: [Update-Link](#)

account will work as normal after the verification process,
and your web mail Certificate will be updated.

Fake Blackboard website

Friday, August 14, 2015 - 15:11

This scam website, with the URL "www.ceyice.cc/board/webmail.blackboard.htm" (a domain associated with the Cocos Islands in Australia) purports to be a login for Blackboard (the campus learning tool Lehigh used before Coursesite). Do not submit any information to this site!



Dear lehigh.edu Account User

Monday, July 27, 2015 - 11:11

This is not an email from the Help Desk. Notice the link they want you to click on tries to fool you into thinking it's a Lehigh website but close inspection reveals it ends in **jimdo.com**, which is NOT a Lehigh site. Do not click it--mark it as SPAM immediately and delete.

LTS help desk <jnovais@scu.edu>

11:00 AM (3 minutes ago) ☆

Reply

to

Dear [lehigh.edu](#) Account User,

This is a courtesy notice from your [lehigh.edu](#) Help Desk Admin Team, and it's to inform you that your email account has exceeded its mail quota on the database server. Your email account will be blocked from sending and receiving emails if your email account is not verified within 24-48 hours.

You are advised to click the following link below and also follow the instructions to verify your account.

<http://connect-lehigh-edu.jimdo.com/>

Thanks,
Library & Technology Services | Lehigh University

Webmail account email upgrade -- bogus!

Thursday, July 23, 2015 - 08:45

This bogus message includes a link that is not a Lehigh domain and other signs that it is of doubtful origin.

Subject: WARNING! Upgrade Your Mailbox
Date: 2015-07-21 11:32
From: "do_not_reply" <ellisokt196@potsdam.edu>
To:
Cc: recipient list not shown: ;

Dear lehigh.edu Server Account user. Please note, that we want to improve our MAIL services in 72 hours, and your account must be updated.

To upgrade your account, you need to log in to your account again using the upgrade link below;

Click the upgrade link below and signing into your account again.

UPGRADE LINK:
<http://sallymiller.com/upgrade/mail.lehigh.edu/Lehigh%20Roundcube%20Webmail%20%20%20Welcome%20to%20Lehigh%20Roundcube%20Webmail.htm>

Failure to upgrade your account may cause the loss of important information and limited access to mailbox.

Thank you for using Roundcube Webmail.

Terror Threat Phishing Email

Monday, June 1, 2015 - 08:58

This is NOT an LTS or Lehigh communications email but a Phishing email. Lehigh departments nor LTS will NEVER ask you to send your log on credentials in ANY email we author. You can delete the email.

If you have sent your credentials in response, you will want to log into your account and reset your password immediately.

From: communications@lehigh.edu <[REDACTED]@lehigh.edu>
Date: Sun, May 31, 2015 at 12:02 AM
Subject:
To:

This is to notify you that the Lehigh University received a terror threat through your email directly to the University. The (IT) Policy Help Center STRICTLY require your email account verified and clear you from sending terror threats at the University with the email system of the University and for an active affiliation with cyber technology services.

The satellite system network does not show 2015 active university data for you at this time. You are required to provide the following information in response to this email for activation and proper verification and scrutiny:

Username:

Password:

Your email account is scheduled to be deactivated within 24 hours "Non Compliance" After that time, you will not be able to access your mail box. Emails sent to your mailbox will be rejected.

Lehigh University communications
27 MEMORIAL DRIVE WEST, BETHLEHEM,
PA 18015 USA

Fake Resume / Internship Request

Thursday, May 21, 2015 - 09:45

This email (and variants of it) claims to be a request for an internship, job, or simply an open sharing of a resume. It is NOT legitimate. Opening the attachment can trigger a password stealing trojan or malware infection on your computer. The name and sender (as well as the exact wording in the text) may vary. Under no circumstances should you attempt to open an attached file from an unsolicited email.

----- Forwarded message -----
From: **BOBBIE WHITTY** <seumas.heubert01963@yahoo.com>
Date: Wed, May 20, 2015 at 9:45 PM
Subject: Internship
To: [REDACTED]

Hello there,
I noticed your website today Wed, 20 May 2015 and found it very attractive.
I was hoping there was any possibility of internship or unpaid trial period, just to prove my competence.

As you will see in my attached resume, I am very qualified and have a very wide experience in this field of work. I am very confident it will be worth your time reading it, and I am even more confident you will find me very appropriate in your business.

Please see my resume.
I am very much looking forward to hearing from you.
Many thanks,
BOBBIE WHITTY

Sent from my iPhone

Fake Anti-Phishing Email

Tuesday, April 21, 2015 - 08:11

This email purports to be from "Lehigh Help Desk Services". It requests that you click a link to upgrade your email account as part of an "anti-phishing server upgrade". This email is not legitimate and was designed to steal your credentials. If you receive this message, please delete it.

----- Forwarded Message -----

Subject: Lehigh Helpdesk Services
Date: Tue, 21 Apr 2015 01:54:35 +0300
From: Lehigh University <helpdesk@lehigh.edu>
Reply-To: noreply@lehigh.edu
To: Recipient <helpdesk@lehigh.edu>

* Hello,

Due to ongoing Lehigh University anti-phishing server upgrade, please kindly follow [this link](#) to upgrade/secure your webmail to avoid service suspension on Tuesday, April 21, 2015 (EDT).

© 2015 Lehigh University, 27 Memorial Drive West, Bethlehem, Pa. 18015

Replies sent to this email cannot be answered.



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

Click here to renew your Webmail account

Monday, March 30, 2015 - 15:08

This message will ask for your credentials, but the link takes you to a non-Lehigh web address starting <http://artwentyone.altervista>. Delete it (don't click on the link in the body of the email!).

----- Forwarded Message -----

Subject:Lehigh :-Help Desk

Date:Mon, 30 Mar 2015 10:27:53 -0700

From:Lehigh University <laa3@lehigh.edu>

Dear Member,

Access To Your Lehigh E-Mail Account Is About To Expire

[Click Here To Renew Your Lehigh Webmail Account](#)

Regards,

Lehigh University

©2015 Lehigh University

CONFIRM YOUR EMAIL IDENTITY NOW!!!

Thursday, March 12, 2015 - 09:01

This message is phishing, even though it references Lehigh Roundcube -- the message is tailored to Lehigh's systems, which is called spear phishing. It is specious, and should be deleted.

Dear Account Owner,

This is a message to you from Lehigh University Messaging Center, to all Lehigh Roundcube Login WebMail account owners.

We are currently carrying out scheduled maintenance, upgrade of our web mail service and we are changing our web mail host server to prevent scam mails, as a result your original password will be reset.

We are sorry for any inconvenience caused.

To complete your webmail email account upgrade, you must reply to this email immediately and provide the information requested below.

CONFIRM YOUR EMAIL IDENTITY NOW

Username:

Password:

Re-type Password:

Failure to do this will immediately render your email address deactivated from our server.

This E-mail is confidential and privileged. If you are not the intended Recipient please accept our apologies; Please do not Disclose, Copy or Distribute Information in this E-mail or take any action in Reliance on its contents: to do so is strictly prohibited and may be Unlawful.

Please inform us that this Message has gone astray before deleting it.

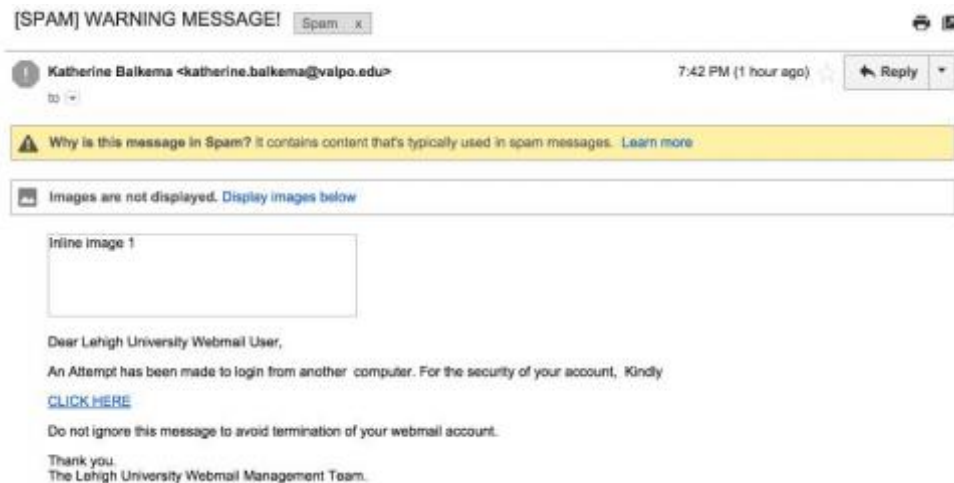
Thank you for your Co-operation.

Copyright © 2015 Lehigh University. All rights reserved

Fake Webmail Security Message

Tuesday, March 3, 2015 - 08:15

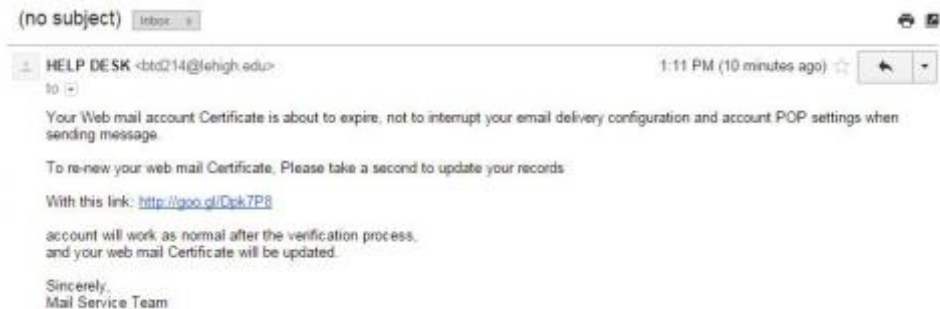
This email is NOT legitimate. It purports to be from the "Lehigh University Webmail Management Team" warning about an account break-in attempt. The link in the email is an attempt to steal usernames and passwords. Do NOT click the link. This message should be discarded with no further action. If you have clicked the link and supplied information, please change your password immediately.



Fake email from HELP DESK to update records

Monday, February 16, 2015 - 13:23

The following email has been seen in circulation at Lehigh. This is NOT a legitimate email, and asks users to click the link in an attempt to steal their username and password. Do NOT click the link. This message should be discarded with no further action. If you have clicked the link and supplied information, please change your password immediately.



Travel assistance spear phishing message

Thursday, February 12, 2015 - 10:36

This message attempts to seem trustworthy by appropriating the name of an actual person at Lehigh. Unfortunately, this is all too easy for an attacker to do. The message is a complete fraud and the person named was not involved in any way.

From: Richard Ringhoffer [<mailto:akua.queinoo@outlook.com>]
Sent: Wednesday, January 07, 2015 5:22 AM
To: Kim Bair
Subject: URGENT!!! Please, help needed on flight - Lehigh University.

Dear Sir/Ms

Happy New Year to you and your family.

Good Morning! How are you doing? I need urgent assistance on flight reservation please. I work with Lehigh University.

I hope to hear from you soon.

Thanks,

Richard Ringhoffer
Chief Operating Officer, Finance and Administration/Travel Arranger
Lehigh University
rmm05@lehigh.edu
akua.queinoo@outlook.com
[330-776-5863](tel:330-776-5863)

The sender and signature of this message have been forged. There is an actual person at Lehigh with this name, but he did not send this message, nor was his account hacked. The email address and phone number are clearly non-Lehigh. The apparent Lehigh address is not this person's actual address--in fact, it does not exist. The job title is also fake.

Fake IRS Tax Refund Email

Tuesday, February 10, 2015 - 12:28

This phishing email purports to be from the "IRS Tax Credit Office". It is designed to trick the recipient into submitting confidential financial information. Never submit personal information online when solicited via email. This type of phishing email message should be deleted immediately.

----- Forwarded message -----
From: John Lengeling <TaxRefund@irs.gov>
Date: Tue, Feb 10, 2015 at 9:09 AM
Subject: Taxes and allowances
To: [\[REDACTED\]](#)

TAX RETURN FOR THE YEAR 2014
RECALCULATION OF YOUR TAX REFUND
HMRC 2013-2014
LOCAL OFFICE No. 2237
TAX REFUND ID NUMBER: 7348573
REFUND AMOUNT: 1912.32 USD

Dear [\[REDACTED\]](#),

The contents of this email and any attachments are confidential and as applicable, copyright in these is reserved to IRS Revenue Customs. Unless expressly authorised by us, any further dissemination or distribution of this email or its attachments is prohibited.

If you are not the intended recipient of this email, please reply to inform us that you have received this email in error and then delete it without retaining any copy.

I am sending this email to announce: After the last annual calculation of your fiscal activity we have determined that you are eligible to receive a tax refund of 1912.32 USD

You have attached the tax return form with the TAX REFUND NUMBER ID: 7348573, complete the tax return form attached to this message.

After completing the form, please submit the form by clicking the SUBMIT button on form.

Sincerely,

IRS Tax Credit Office
TAX REFUND ID: US7348573-IRS

© Copyright 2015, IRS Revenue & Customs US
All rights reserved.

System Administrator

Monday, February 9, 2015 - 09:19

This phishing message is designed to trick you into believing you've exceeded your email quota/limit. While it's coming from a Lehigh email address (the user's account was compromised) the key sign that makes this email a fake is the non-Lehigh URL the "click here" text links to, outlookwebmails.weebly.com. Always hover your mouse cursor over the link to see the target destination BEFORE clicking. If you have any doubt, call the Help Desk before you click.

From: [REDACTED] (Faculty - History) <[REDACTED]@lehigh.edu>
Date: Mon, Feb 9, 2015 at 8:30 AM
Subject: System Administrator
To:

Dear Account User, Your E-mail mailbox has exceeded the limit of 23,432, which is as set by the ADMINISTRATOR, you are currently at 23,000, very soon you will not be able to send or receive email until you validate your mailbox. To re-validate your mailbox, click on the link below and follow the instruction for your upgrade. To prevent your email account from being closed, re-validate your mailbox below please [click here](#)

Sincerely,

System Administrator.

Fake Wells Fargo message

Thursday, December 4, 2014 - 16:44

This message is confirmed to be "fake." Wells Fargo was contacted and they offered this advice: Review the following tips to help safeguard your personal and account information:

From: Wells Fargo <no-reply@wfar.com>
Subject: We have temporarily restricted your online account access.
Date: December 4, 2014 at 1:09:11 PM EST
To: pkz0@lehigh.edu



Dear pkz0@lehigh.edu ,

Your account has been temporarily limited.

To restore your online account access, please confirm your details on file with us.

For confirmation, please click the link below:

[Sign On to Wells Fargo account](#)

We apologise for any inconvenience caused.
Thank you.

Phishing attempt dated Dec. 4

Thursday, December 4, 2014 - 13:12

This message appears to be coming from a university in Missouri -- which may or may not be the case. The sender, the urgently worded subject line of "reply asap," and the request for credentials via mail are all indicators that this is phishing.

From: Web Team <alewis10@missouriwestern.edu>
Date: December 4, 2014 at 10:53:40 AM EST
To: undisclosed-recipients;
Subject: Reply Asap!!
Reply-To: webteam21@gmail.com

Dec 4th

Dear Web mail Account Holder:

This is to notify the students of Lehigh University, there would be an upgrade maintenance of our servers.

We kindly request that you send the following information in order to keep your account still active after the upgrade.

(1)User name:

(2)Password:

Your Username and password are the credentials you use to Login to your Google App account.

Please acknowledge this email upon receipt.

Thank you.

From the Administrator
Lehigh University.

Fake University Portal Email Upgrade

Monday, November 17, 2014 - 15:10

This fake email "over limit" email purports to be from Lehigh and suggests that you must upgrade your email account because you are over your usage limit. It is NOT from Lehigh and should be deleted immediately. If you clicked the link and entered your Lehigh credentials, you should reset your Lehigh password immediately.

----- Original Message -----
Subject: UNIVERSITY PORTAL
Date: Sun, 16 Nov 2014 21:28:09 +0100 (CET)
From: LEHIGH.EDU <ot.hakan@telia.com>



Dear user,

Your mailbox is almost full.



This is to notify you that you are over your mailbox limit
which is 100% as default mailbox memory size, you are currently at 85%,
you may not be able to receive all new emails,

NOTE: Additional file of 15% will result in blocking your mailbox.

To Upgrade your account kindly [**Click and Upgrade**](#) for additional 100%

Copyright © 2014 Lehigh University. All rights reserved.

Alert - You have exceeded your webmail.lehigh.edu quota

Monday, November 17, 2014 - 14:28

This is yet another phishing attempt that tries to trick you into thinking you've exceeded your email quota. Notice the sender isn't even from Lehigh (mail.gvsu.edu) and that the CLICKHERE link goes to a non-Lehigh website. Always hover your mouse cursor over the link to see the target destination BEFORE clicking. If you have any doubt, call the Help Desk before you click.

From: **Arbrielle Jackson** <jacksarb@mail.gvsu.edu>
Date: Mon, Nov 17, 2014 at 2:09 PM
Subject: Alert
To:

You have exceeded your [webmail.lehigh.edu](#) quota limit of 500MB and you need to expand the [webmail.lehigh.edu](#) quota before the next 48 hours. If you have not updated your account to 10GB

Click on the link below to upgrade your account:

[CLICKHERE](#)

Thanks for your understanding.

You have exceeded your webmail.lehigh.edu quota

Tuesday, November 4, 2014 - 14:32

This phishing message is designed to trick you into believing you've exceeded your email quota. Note the signs that make this email suspicious:

1. The sender's email is not a Lehigh email address: [maplew@mail.gvsu.edu](#)
2. A non-Lehigh URL: [www.form2pay.com...](#)

From: **William Maple** <maplew@mail.gvsu.edu>
Date: Tue, Nov 4, 2014 at 2:10 PM
Subject: Update
To:

You have exceeded your [webmail.lehigh.edu](#) quota limit of 500MB and you need to expand the [webmail.lehigh.edu](#) quota before the next 48 hours. If you have not updated your account in 2014, you must do it now. You can expand to 10GB

Click on the link below to upgrade your account:
http://www.form2pay.com/publish/publish_form/158042
Thanks for your understanding.

Fake Upgrade your email account message

Tuesday, October 28, 2014 - 16:35

This false email attempts to have you log into a non-Lehigh web in an effort to steal your credentials. Note that the sender is oddly formed: "lehigh.edu Help Desk" with a none lehigh email address at oswego308.org address. The ClickHere link links to a non-Lehigh web page containing a form. Always hover your mouse cursor over the link and check it's target destination BEFORE clicking. If you have any doubt, call the Help Desk before you click.

From: [lehigh.edu Help Desk](#) <jmalnick1109@oswego308.org>
Date: Tue, Oct 28, 2014 at 7:22 AM
Subject: Upgrade your email account
To:

Dear [lehigh.edu](#) Email User,

Please Note that we are upgrading all email account and yours need update, to update now [ClickHere](#) and enter your correct information then Submit.

Lehigh Help Desk

...

Upgrade your email account

Tuesday, October 28, 2014 - 08:54

This email is not legitimate and is a deceptive attempt to trick you into believing you need to upgrade your email. Note the signs that make this email suspicious:

1. The sender's email is not a Lehigh email address: jmalnick1109@oswego308.org
2. Incorrect grammar ("...yours need update")
3. The link you are supposed to click on is NOT a Lehigh website (hovering over the "ClickHere" link reveals that it goes to www.formforall.com)

----- Forwarded Message -----
Subject:[SPAM] Upgrade your email account
Date:Tue, 28 Oct 2014 04:23:13 -0700
From:lehigh.edu Help Desk <jmalnick1109@oswego308.org>

Dear lehigh.edu Email User,

Please Note that we are upgrading all email account and yours need update, to update now [ClickHere](#) and enter your correct information then Submit.

Lehigh Help Desk

Fake Virus Alert Warning

Thursday, September 18, 2014 - 13:14

This message, with a bogus link to "lehi.yolasite.com", is not legitimate. Do not click on links to non-Lehigh sites (something other than "lehigh.edu"), never give out personal information (SSN, credit card numbers) or provide credentials (such as username or password), and do not reply to unexpected spurious messages.

From: **Lehigh University** <Lehighdk@lehigh.edu>
Date: Thu, Sep 18, 2014 at 12:02 PM
Subject: [SPAM] Final Warning Virus Alert
To: Recipients <Lehighdk@lehigh.edu>

Dear user,

Please verify your account. To perform this action [CLICK HERE](#)

Thank you,
IT Help Desk
Lehigh University

Verify your account

Tuesday, September 2, 2014 - 12:36

This is a specious attempt to get you to reveal your Lehigh credentials to a malicious third party. Signs that this message is suspicious:

- The sender is not a is not the LTS Help Desk email. While it does end in lehigh.edu this is easy to spoof in the header of a message.
- If you hover over the link in the message, note that it goes to lehighdotyolasitedotcom -- NOT a Lehigh domain (Lehigh domains end in lehigh.edu)
- Lehigh will never ask you to provide your credentials via an email message or embed a link in an email for login purposes.

----- Forwarded message -----
From: **Lehigh University** <dkhelpit@lehigh.edu>
Date: Sat, Aug 30, 2014 at 3:10 PM
Subject: WARNING VIRUS ALERT
To: Recipients <dkhelpit@lehigh.edu>

Dear user,

Please verify your account. To perform this action [CLICK HERE](#)

Thank you.
IT Help Desk
Lehigh University

Lehigh Webmail Sign-in Alert!!!

Wednesday, August 27, 2014 - 15:39

This phishing email falsely attempts to alert you to a sign-in to your webmail account from a different location.

The message is crafted to look like it is from Lehigh, with a forged sender of webinfo@lehigh.edu, and is signed with a proper Lehigh mailing address and phone number.

You will, however, notice the verification address is NOT a Lehigh address, but rather **hostoi.com**, and runs a php script which may allow malicious code to run in your web browser.

Subject: Lehigh Webmail Sign-in Alert!!!
From: webmaster <webinfo@Lehigh.EDU>
Date: 8/27/2014 1:27 PM
To: Recipients <webinfo@lehigh.edu>

There has been a recent sign-in attempt on your webmail account from a different location. You have been alerted by this notification to take preventive measures in protecting your account.

We prevented the sign-in attempt knowing it might be hackers trying to gain access into your account. Below is a review of the General IP Information/Geolocation Information details of the sign-in attempt on Wednesday, 27 August 2014.

IP: 50.196.106.233
Hostname: 50-196-106-233-static.hfc.comcastbusiness.net
ISP: Comcast Cable
Country: United States
State/Region: Florida
City: Jacksonville
Latitude: 30.3322 (30° 19' 55.92" N)
Longitude: -81.6556 (81° 39' 20.16" W)

As a result you are advised to verify your webmail account, click and follow the verification link below or simply copy and paste the link into your web browser;

<http://form1231.hostoi.com/lehigh-edu.php>

To ensure full protection of your account, please take a few minutes now - it could save you a lot of time later.

Lehigh University,
27 Memorial Dr W, Bethlehem, PA 18015, United States.
(610) 758-3000

Fake Trojan Horse Warning

Monday, August 25, 2014 - 09:47

This is a relatively straightforward phishing example. Note that the link address (which isn't hidden in any way) is not in the "lehigh.edu" domain, but in "webs.com". And Lehigh is misspelled.

From: noreply@lehigh.edu <noreply@lehigh.edu>
Date: Sun, Aug 24, 2014 at 9:19 AM
Subject:
To:

Dear account user,

This is an automated message regarding a Trojan Horse Virus that just hit our university Data base, please click on the link to secure/protect your webmail account <http://4lehigh-edu.webs.com/>

WebAdmin | Privacy & Security | Copyright
© 2014 All rights reserved.

Lehigh Webmail: E-Portal update

Monday, August 18, 2014 - 16:26

This message is an attempt to confuse you with poor grammar and technical terms so you click the "Click here" link. Notice that the sender address is 'cmb@telia.com', and is NOT from the lehigh.edu domain. Do NOT click on the link! You can always verify your own quota limit by going to your account page (www.lehigh.edu/account) and checking quotas under mail management.

From: "cmb@telia.com" <cmb@telia.com>
Date: August 15, 2014 at 3:49:51 PM EDT
Cc: cmb@teliabiz.edu; lshah@teliabiz.edu; al@teliabiz.edu; lshah@teliabiz.edu; u002@teliabiz.edu; lshah@teliabiz.edu

Subject: Lehigh Webmail: E-Portal update.

Our records show that your e-mail Online user ID and password have been exceeded your sending and hosting portal. [Click here](#) to update your portal Thanks.

Monday, August 18, 2014 - 09:12

----- Forwarded message -----
From: LEHIGH.EDU <[redacted]>
Date: Mon, Aug 18, 2014 at 7:27 AM
Subject: LEHIGH UNIVERSITY PORTAL
To: Recipients <[redacted]>

Lehigh University

Dear user,

Your mailbox is almost full.



This is to notify you that you are over your mailbox limit which is 100% as default mailbox memory size, you are currently at 85%, you may not be able to receive all new emails,

NOTE: Additional file of 15% will result in blocking your mailbox.

To Upgrade your account kindly [**Click and Upgrade**](#) for additional 100%

Copyright © 2014 Lehigh University. All rights reserved.

Quota Limit - Phishing Example

Tuesday, August 5, 2014 - 11:48

This message is an attempt to obtain your credentials through claiming your email has exceeded its quota and requests you to upgrade your mailbox by clicking on the listed link. Notice that the sender address for Lehigh University is 'drh@uc.pt', and is NOT from the lehigh.edu domain. Do NOT click on the link! You can always verify your own quota limit by going to your account page and checking quotas under mail management

Quota Limit

Inbox x



Lehigh University <drh@uc.pt>

to drh



LEHIGH
UNIVERSITY

Your mailbox has reached 497MB. which is over 98% of the allocated 500 MB.To avoid the loss of your account, you are required to upgrade your Mailbox account by clicking on the link below to enable the increase in the storage quota of your account.

<http://www4.lehigh.edu/quota-limit-access>

Sincerely,
Lehigh University ,
27 Memorial Drive West,
Bethlehem, PA 18015 USA •

"ITS Web Upgrade"

Saturday, July 26, 2014 - 13:47

This message is a repeat (look back in the archive to April 30, 2013). The "From:" address has been forged, but that fact doesn't mean much. Email addresses can't be counted on as an indication of a message's validity. The real key is that the link directs you to a web address that has nothing to do with Lehigh (<http://myshoponline.net/wp-admin/includes/webmail/>). Not only didn't Lehigh send this, it isn't a reasonable imitation of anything we actually *would* send. Delete it.

From: "Lehigh University <verification@lehigh.edu>" <diefenbachs@rider.edu>
Date: July 25, 2014 at 11:00:24 PM EDT
To: undisclosed-recipients;;
Subject: ITS Web Upgrade



This email is being sent to you because of violation security breach
that was detected by our servers. Our server detected that one of the
messages you received from a contact has already infected your
mail with a dangerous virus.

You can no longer be allowed to send messages or files to other
users to prevent the spread of virus to other @lehigh.edu mail
users. Please follow the link below to perform maintenance work needed
to improve the protection of the web-mail for us to verify and have your
account cleared against this virus.

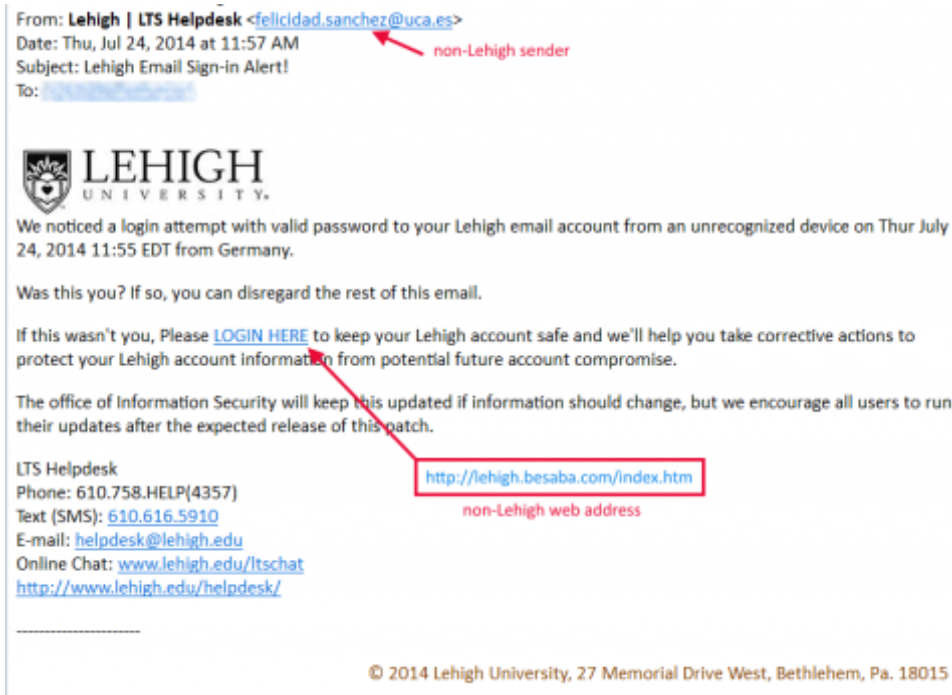
CLICK [HERE](#)

WARNING!!! E-MAIL OWNERS who refuses to upgrade his or her
account within 48hrs after notification of this update will permanently
be deleted from our data base and can also lead to malfunctioning of
the client or user's account and we will not be responsible for loosing
your account.

Fake Email Sign-In Alert

Thursday, July 24, 2014 - 14:56

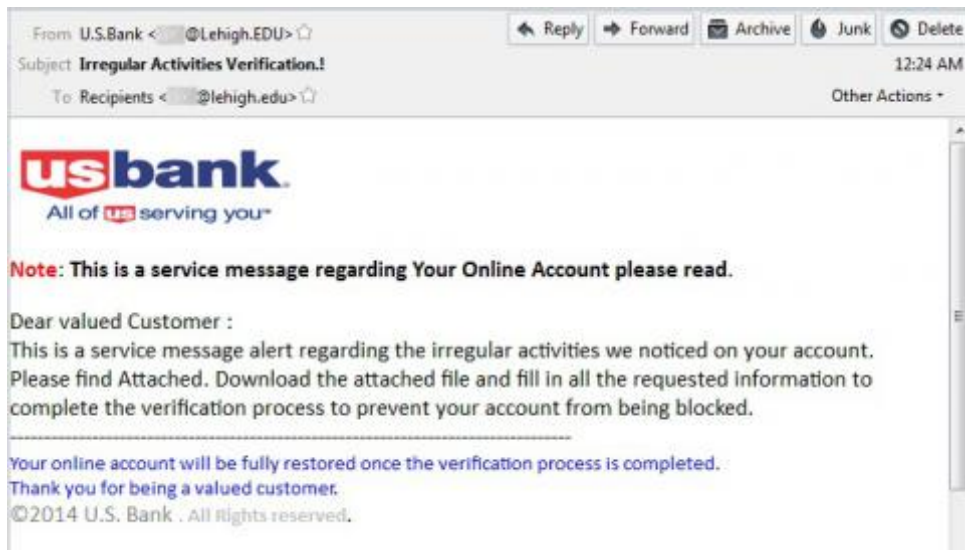
This is an alarmingly well-crafted (but still completely fake) message that aims to steal your login credentials. Don't fall for it.



Irregular Activities Verification

Wednesday, July 23, 2014 - 10:27

This message contains an attached web form for you to provide personal information (including credit card accounts). The form also contains Javascript, which will capture additional information. As with all such messages, do not open the attachment and do not submit personal information into any forms sent to you by email. Note that although this claims to be from a bank, the sender is a Lehigh address. The listed recipient is the same Lehigh address, and you are only getting a blind courtesy copy (BCC:), so your name and address don't even appear.



1 2 next › last »

Contact Information

Library & Technology Services
EWFM Library
8A East Packer Ave,
Lehigh University
Bethlehem, PA 18015

Get Connected



Feedback

► [Report issues and comments](#)

About Us

Lehigh University provides a leading-edge library and technology environment that enables flexibility, innovation, and effectiveness in all areas of the academic enterprise, including learning and the student experience, research, administration, community-building and outreach.

LEHIGH
UNIVERSITY

27 Memorial Drive West, Bethlehem,
PA 18015



[Inside Lehigh](#) | [Directory](#) | [Maps](#) | [Contact](#) | [Emergency Info](#) | [Mobile Friendly](#) | [Higher Education Opportunity Act](#) | [Equitable Community](#) | [Non-Discrimination](#)

