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)

Banking Information Form

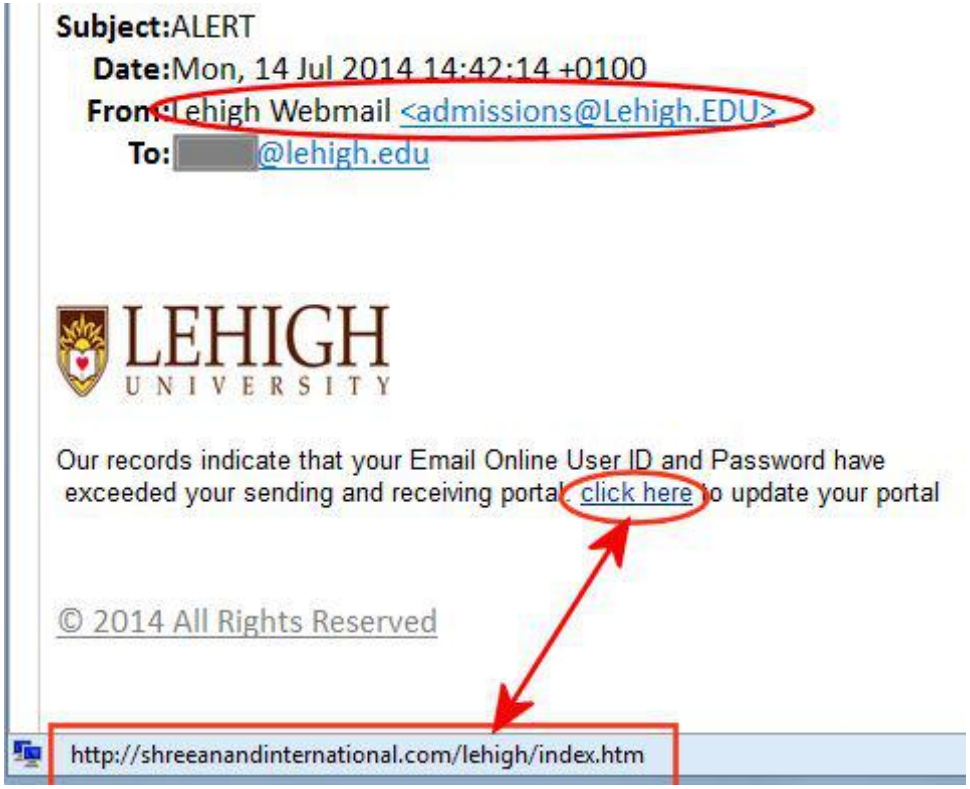
Wednesday, July 23, 2014 - 10:15

This is the form included with the "Irregular Activities Verification" scam message.

Fake Exceeded Your Sending and Receiving Portal Message

Monday, July 14, 2014 - 12:25

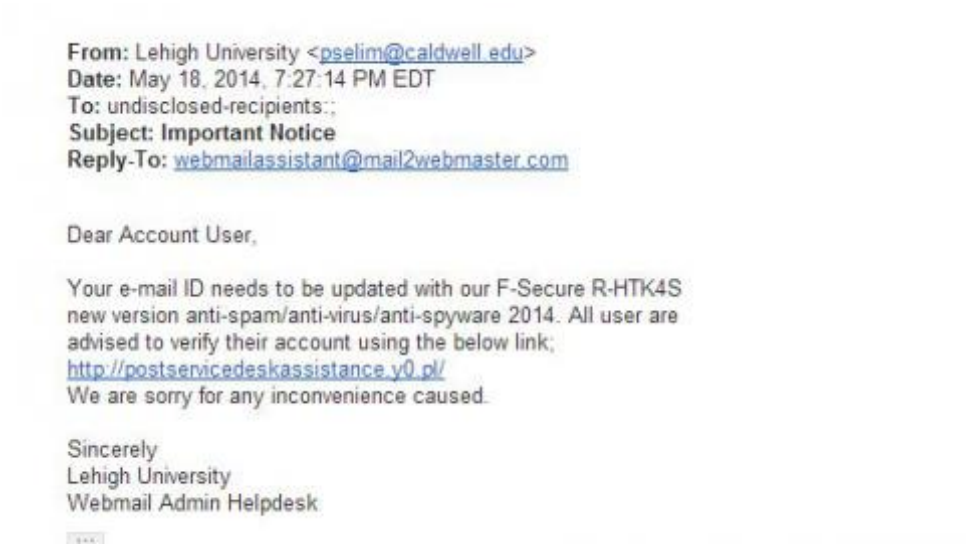
This message is a clever attempt to obtain your credentials through claiming your email has exceeded it's sending and receiving limits on the Campus Portal. Notice the tell-tale signs of phishing highlighted in the example. Message claims to be from Lehigh Webmail, but address is Admissions (both false). If you hover over the link, you will see it attempts to take you to a domain shreenandinternational.com, not an actual Lehigh web site. Do NOT click on the link!



Fake Anti-Virus Update

Tuesday, July 1, 2014 - 12:23

This message attempts to get you to sign into your lehigh account in order to update a fake "anti-spam/anti-virus/anti-spyware" software called "F-Secure R-HTK4S". It is an attempt to steal your lehigh credentials.



From: Lehigh University <pselim@caldwell.edu>
Date: May 18, 2014, 7:27:14 PM EDT
To: undisclosed-recipients:;
Subject: Important Notice
Reply-To: webmailassistant@mail2webmaster.com

Dear Account User,

Your e-mail ID needs to be updated with our F-Secure R-HTK4S new version anti-spam/anti-virus/anti-spyware 2014. All user are advised to verify their account using the below link;
http://postservicedeskassistance.y0.pl/
We are sorry for any inconvenience caused.

Sincerely
Lehigh University
Webmail Admin Helpdesk

Fake eFax

Tuesday, July 1, 2014 - 12:21

This message tries to get you to click on a link by claiming that you have received a fax message online. Some of the links on the page are copies of legitimate links, but the trap is a very deceptive link. On the surface, the link text says "http://**www.efax.com**/fax/fax_view.aspx?fax_id=7132159010", which looks like a reasonable link.

eFax.com

Fax Message[Caller-ID: 610-758-4983]

You have received a 1 page fax at 2014-02-18 05:30:20 CDT.

* The reference number for this fax is min1_did13-1329191075-7132159010-49.

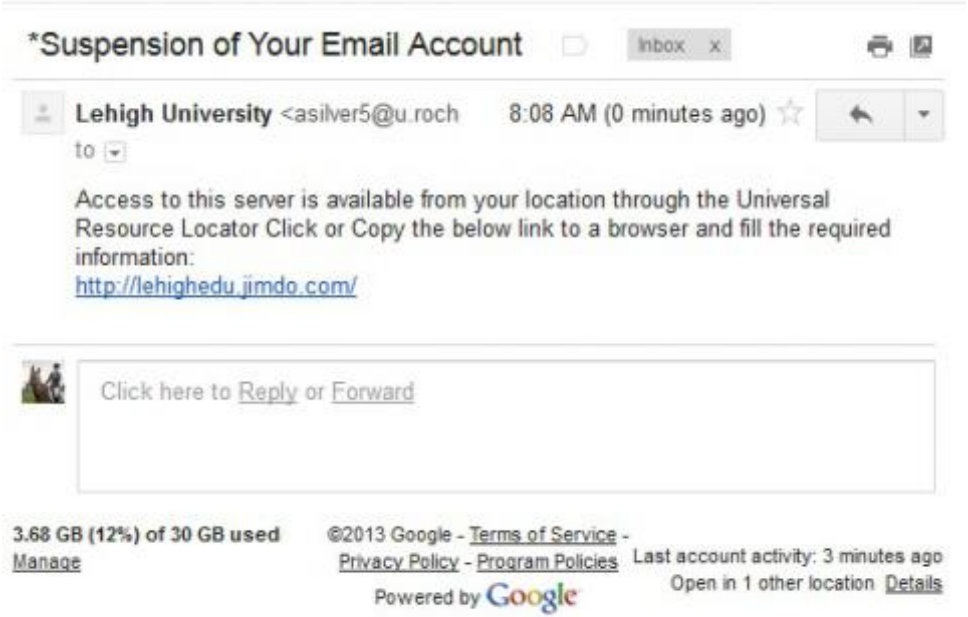
View this fax online, on our website : http://www.efax.com/fax/fax_view.aspx?fax_id=7132159010
Please visit www.eFax.com/en/efax/twa/page/help if you have any questions regarding this message or your service.

Thank you for using the eFax service!

Email Suspension

Tuesday, September 24, 2013 - 00:00

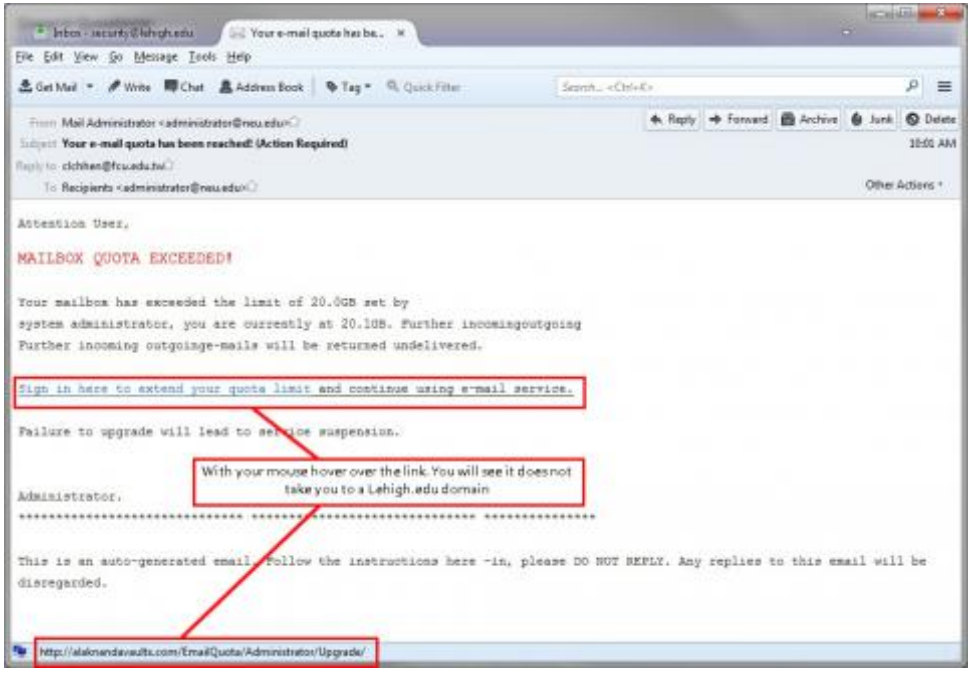
This message claims that your email is suspended and provides a link -- note that the link is NOT in the lehigh.edu domain and that it lacks punctuation.



Fake Mail Quota Warning

Friday, September 13, 2013 - 00:00

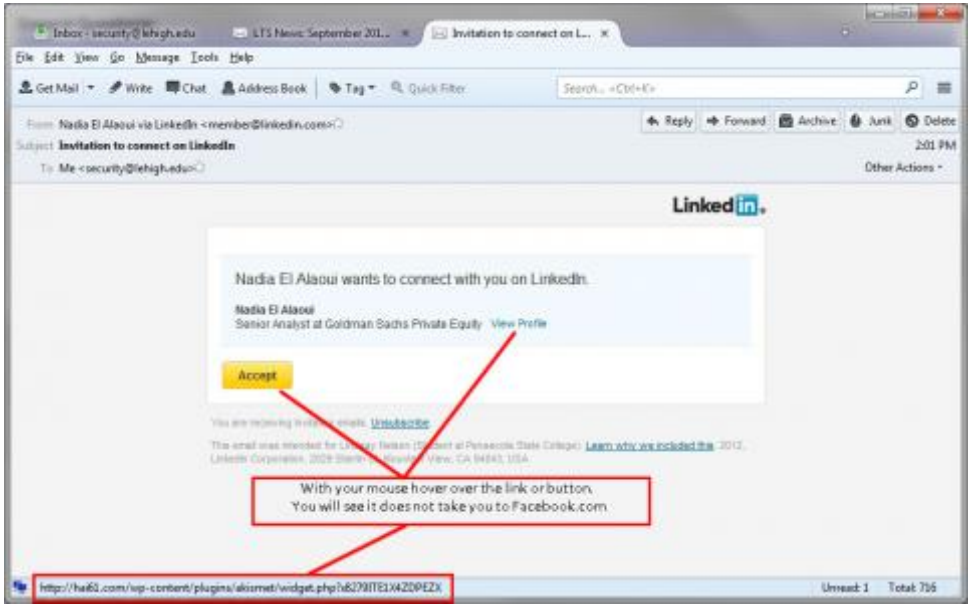
This message fraudulently tells you that your email quota has been exceeded. The message is not from Lehigh and the link takes you to a non-Lehigh site which may have malicious software. Delete this message. NOTE: you can hover over links to see that it does not go to a real lehigh domain. You can also check your (legacy, not Gmail) mail quota by going to your Lehigh Account web page linked at the bottom of the main Lehigh and Inside Lehigh web pages.



Fake LinkedIn Announcement

Friday, September 13, 2013 - 00:00

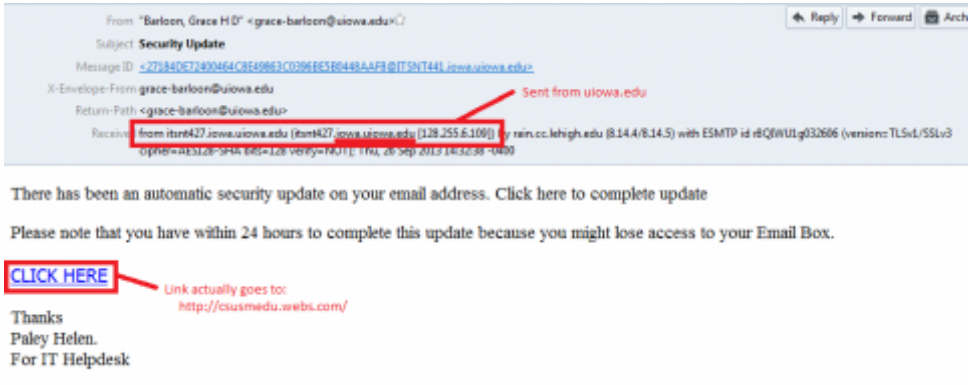
This message purports to be from the social media site LinkedIn, suggesting that someone wishes to connect with you. This message is a fraud, as can be seen by examining the destinations of the links in the message (they do not go to LinkedIn). Delete this message; do not click on any of the links or attempt to reply.



Fake Security Update

Sunday, September 1, 2013 - 00:00

This message falsely indicates a security update requires your action to complete, and that if not responded to within 24 hours, you may lose your email. This message is a fraud, by examining the destinations of the link in the message you will notice they go to some other domain, 'webs.com'. Delete this message; do not click on any of the links or attempt to reply.



Account Expiration Fraud

Monday, August 26, 2013 - 00:00

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 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.

Subject: Account Update
Date: Mon, 26 Aug 2013 08:48:42 -0500
From: Lehigh University <incopy@Lehigh.EDU>

ACCOUNT ALERT

Your Account Is About To Expire

Click Here To Read

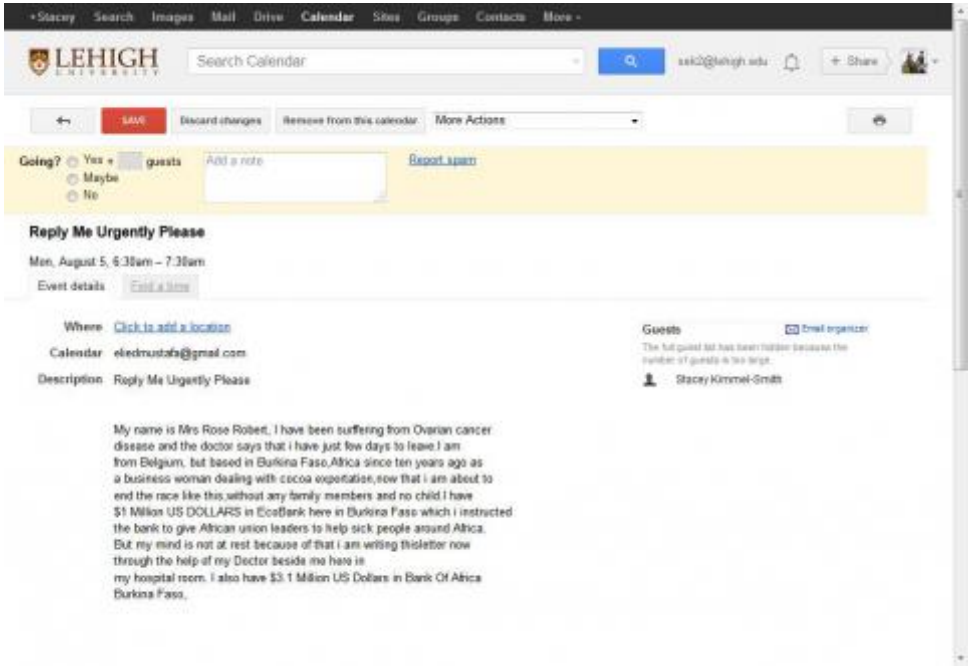
Sincerely,

Lehigh University

Calendar Phishing

Monday, August 5, 2013 - 00:00

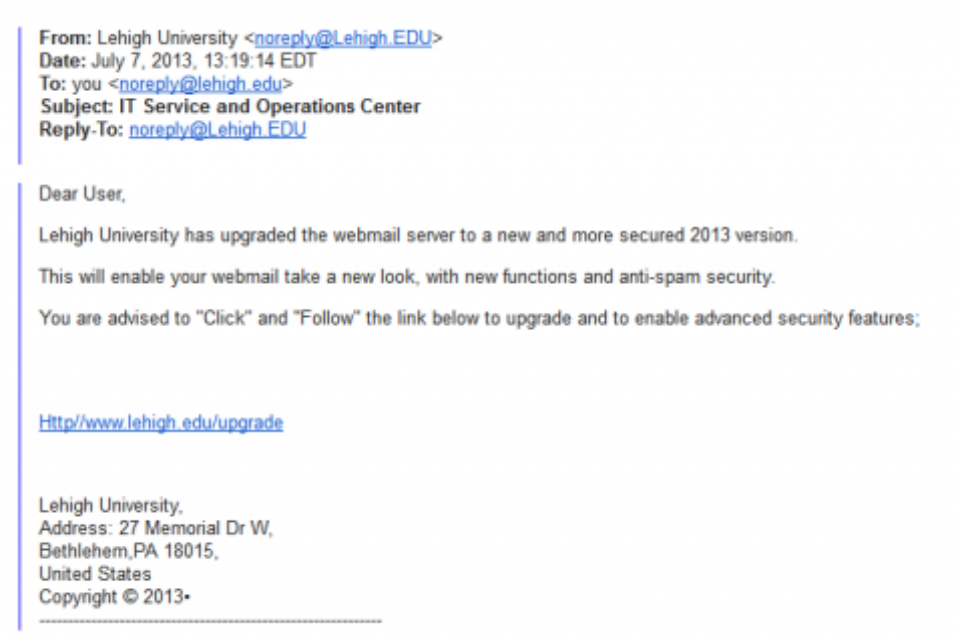
This is a calendar event that appeared on a staff member's Lehigh Google Calendar, and a variation on the theme of email phishing. Delete calender events that may appear in your calendar.



IT Services and Operations (Fraud)

Monday, July 8, 2013 - 00:00

This message fraudulently tells the you, the recipient, that the webmail server has been upgraded and that you should click and follow the links to take advantage of new security features. While the text appears to be a legitimate link if you hover over the link you see that it takes you to a non-Lehigh server and likely one that will do harm to your identity or your computer.



From: Lehigh University <noreply@Lehigh.EDU>
Date: July 7, 2013, 13:19:14 EDT
To: you <noreply@lehigh.edu>
Subject: IT Service and Operations Center
Reply-To: noreply@Lehigh.EDU

Dear User,

Lehigh University has upgraded the webmail server to a new and more secured 2013 version.

This will enable your webmail take a new look, with new functions and anti-spam security.

You are advised to "Click" and "Follow" the link below to upgrade and to enable advanced security features;

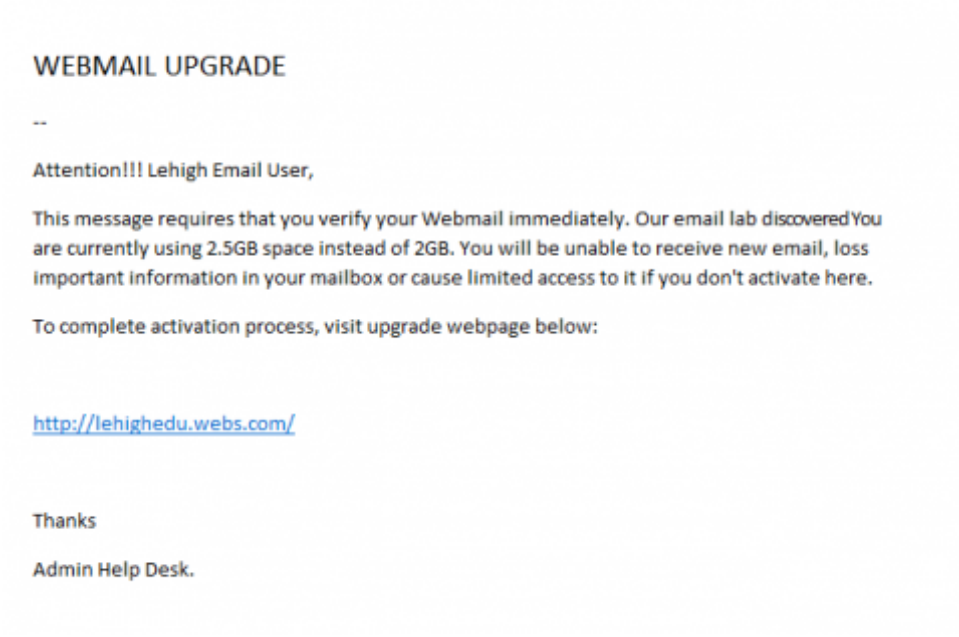
Http//www.lehigh.edu/upgrade

Lehigh University,
Address: 27 Memorial Dr W,
Bethlehem,PA 18015,
United States
Copyright © 2013•

Webmail Upgrade Fraud

Friday, June 21, 2013 - 00:00

This message indicates that you are using more space for web mail than you have been allocated. It threatens that unless a link is clicked to upgrade the account, the account holder will be unable to receive email. Notice that the message is signed "Admin Help Desk" (no such thing), refers to "email labs" (again, no such thing), and that the link points to someplace that is not lehigh.edu. Clicking the link can result in having your account credentials compromised. This email should be regarded as SPAM and deleted.



WEBMAIL UPGRADE

--

Attention!!! Lehigh Email User,

This message requires that you verify your Webmail immediately. Our email lab discoveredYou are currently using 2.5GB space instead of 2GB. You will be unable to receive new email, loss important information in your mailbox or cause limited access to it if you don't activate here.

To complete activation process, visit upgrade webpage below:

http://lehighedu.webs.com/

Thanks

Admin Help Desk.

Account Security Breach Violation

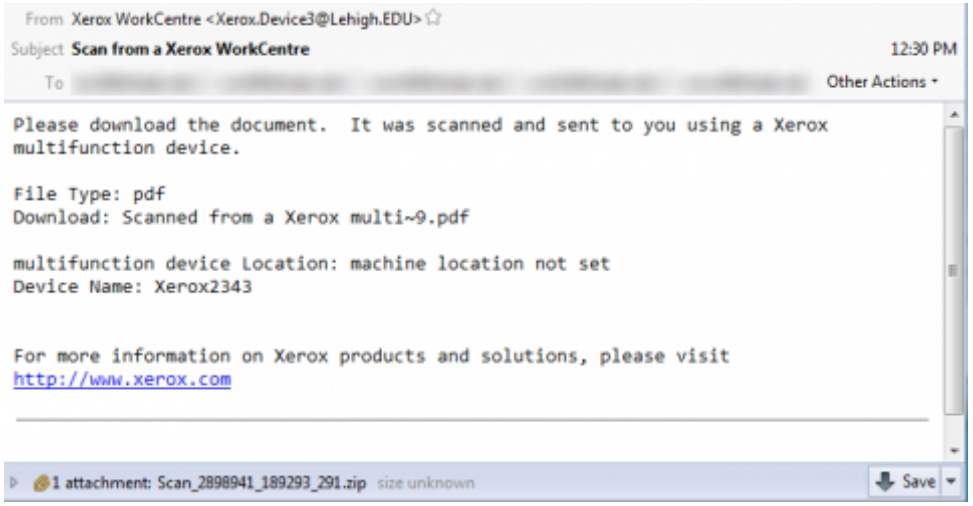
Thursday, June 13, 2013 - 00:00

This message purports to be a "Lehigh Web Notice" about a security breach to your account. It threatens that unless a link is clicked to verify the account, the account holder will be unable to send email. Clicking the link can result in having your account credentials compromised. This email should be regarded as SPAM and deleted.

Xerox Scan Fraud

Wednesday, June 12, 2013 - 00:00

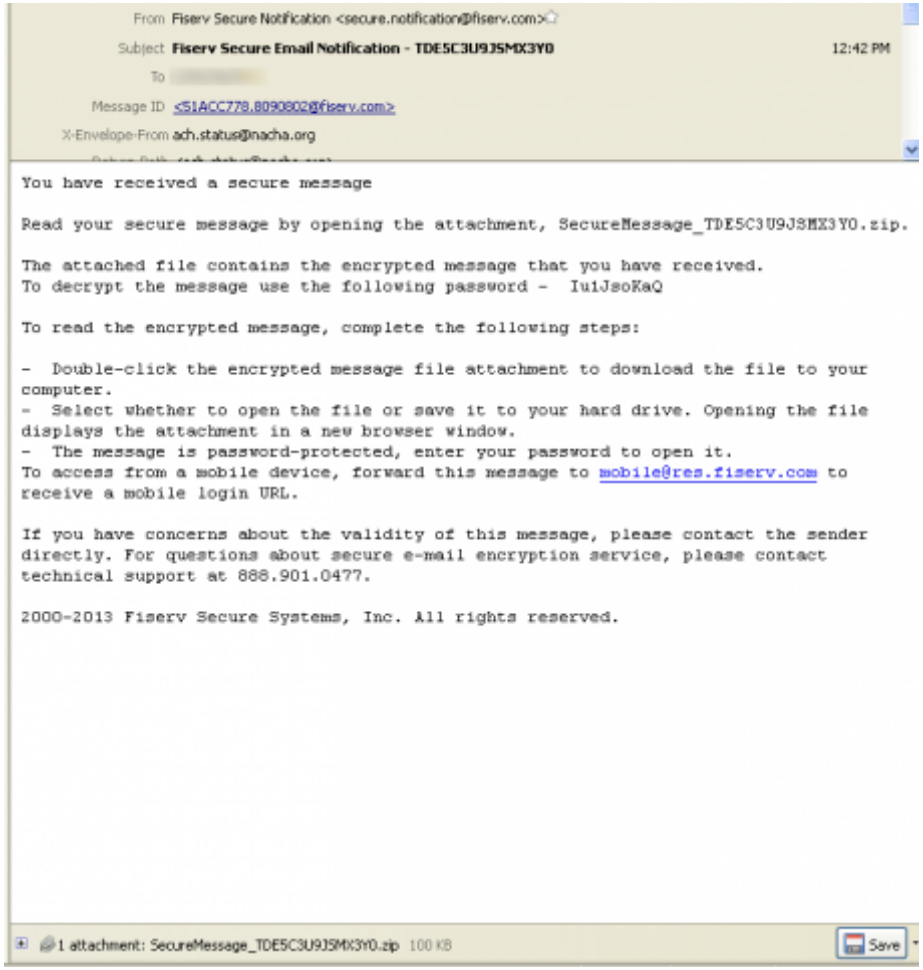
This message pretends to be an email message sent by a multifunction printer/scanner/fax machine as the result of scanning a document. The message claims that the document is a PDF, but the attachment is actually a ZIP archive (note the extension at the end of the file name). The key principle here is that any message you weren't expecting should be regarded as suspect--if you didn't just scan a document, why would you be receiving this? If you aren't sure, don't click on any links or open any attachments.



Secure Message Fraud

Monday, June 3, 2013 - 00:00

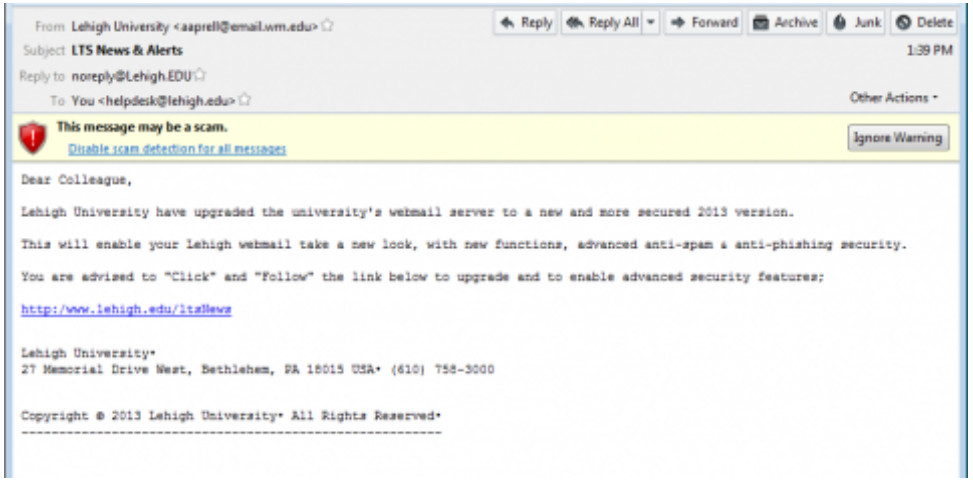
This message purports to be a transmission of a secure message from a company called "fiserv.com," a mobile banking services company. The sender address, however, is "nacha.org," which is a completely different (and unrelated) group that oversees the ACH network (a key player in electronic fund transfers). The NACHA name has been used for some time as a cover for fraudulent mailings of various types (see https://www.nacha.org/node/983). This particular mailing is an attempt to get you to open and execute an infected attachment.



Fake Upgrade Alert (again)

Thursday, May 16, 2013 - 00:00

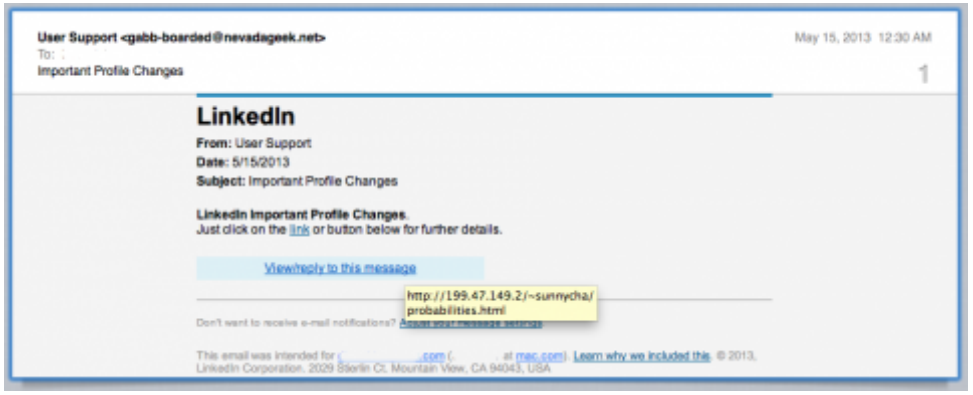
This message is a version of the same scam we have seen before. The screenshot shows that, depending upon your mail client, and whether it blocks images, the message can look slightly different. Note that the link, which purports to go to http:/www.lehigh.edu/ItsNews (this URL does not exist and is not even correctly-formed, as the slash following the colon should be two slashes) actually goes to http://www.123contactform.com/form-580146/Lehigh.



Fake LinkedIn "Important Profile Changes" Alert

Wednesday, May 15, 2013 - 00:00

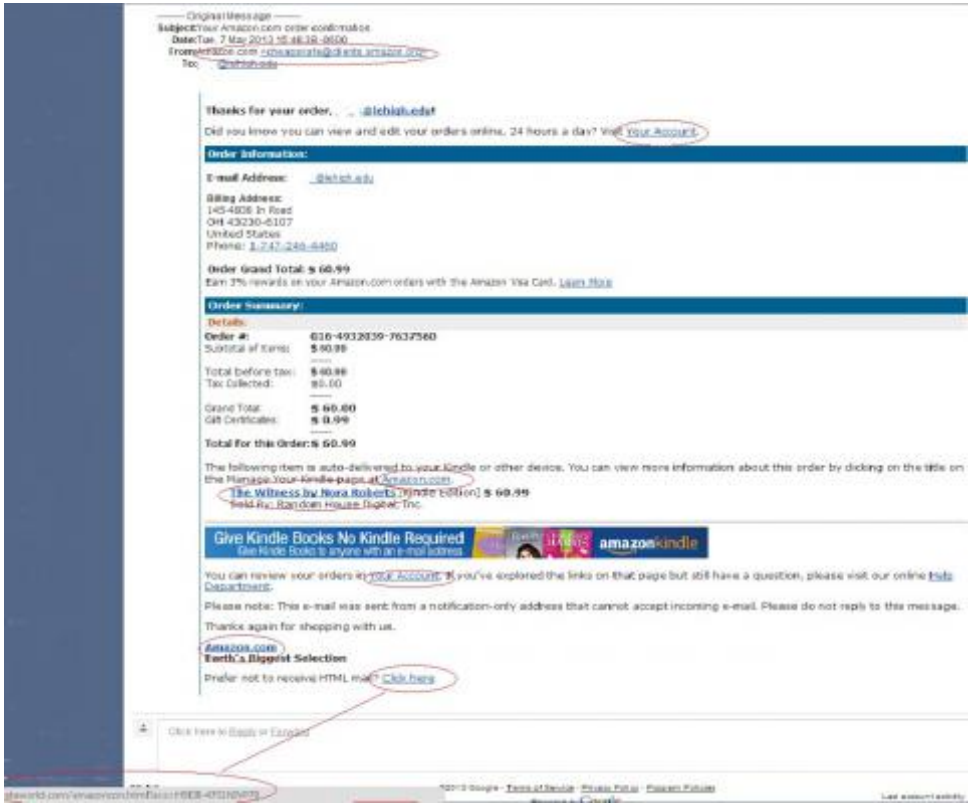
This email attempts to trick you into clicking on a link. It purports to be from LinkedIn, and it looks very realistic (the graphics are all exactly like those in real LinkedIn messages, and there are no apparent errors in grammar or style). But the link, whose address is http://199.47.149.2/~sunnycha/probabilities.html, does not point to a LinkedIn address (it does not even point to a named server, but just an IP address!). This email should be regarded as SPAM and deleted.



Fake Amazon Kindle Order Confirmation

Wednesday, May 8, 2013 - 00:00

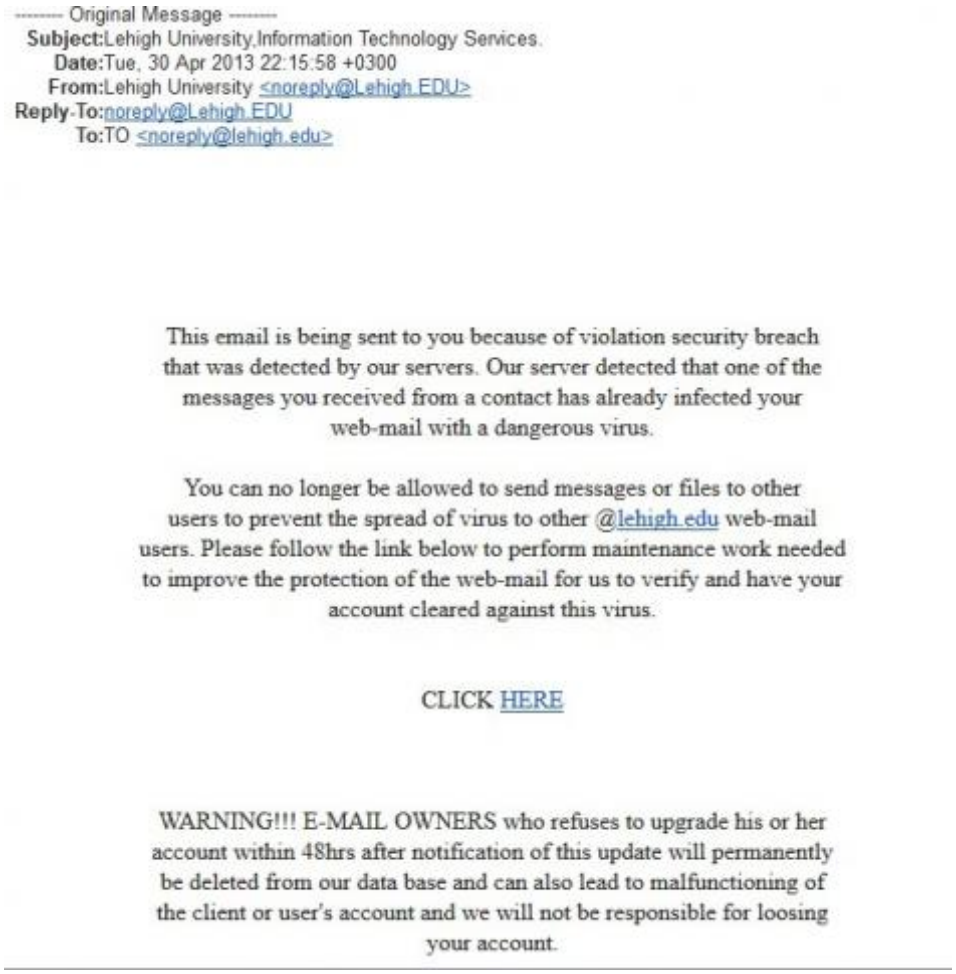
This email appears to come from Amazon, but note the email address is not amazon.com, but rather amazon.org. The links all point to code on the myataworld.com domain. This email should be regarded as a phishing attack with intent to infect your computer and obtain data. Do not click any links and delete it immediately.



"Violation Security Breach"

Tuesday, April 30, 2013 - 00:00

This email tells you that your webmail has been infected with a dangerous virus. It is a fake.



-------- Original Message --------
Subject: Lehigh University,Information Technology Services.
Date: Tue, 30 Apr 2013 22:15:58 +0300
From: Lehigh University <noreply@Lehigh.EDU>
Reply-To:noreply@Lehigh.EDU
To:TO <noreply@lehigh.edu>

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 web-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 web-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 "Verify Mailbox and Increase Quota" Alert

Sunday, April 28, 2013 - 00:00

This email tricks you into thinking there is a problem with your mailbox and quota and encourages you to click the link to fix it. Do not click on the link. Note also the improperly sized Lehigh graphic. This email should be regarded as SPAM and deleted.

Subject:Mailbox Update
Date:Sun, 28 Apr 2013 17:31:15 +0300
From:Lehigh Unversity <upgrade@Lehigh.EDU>
To:Recipients <upgrade@lehigh.edu>

LEHIGH UNIVERSITY

This message requires that you verify your mailbox and increase its quota. You are currently running on 23GB instead of 20GB Due To Hidden Files and Folders in Your Mailbox. You will be unable to receive new email, Loss Important Information in Your Mailbox Or Cause Limited Access to It if not verified. To complete this verification simply :

Clicking Here

Failure to do this will violate the Lehigh University Web-mail email terms & conditions. This will render your account inactive.

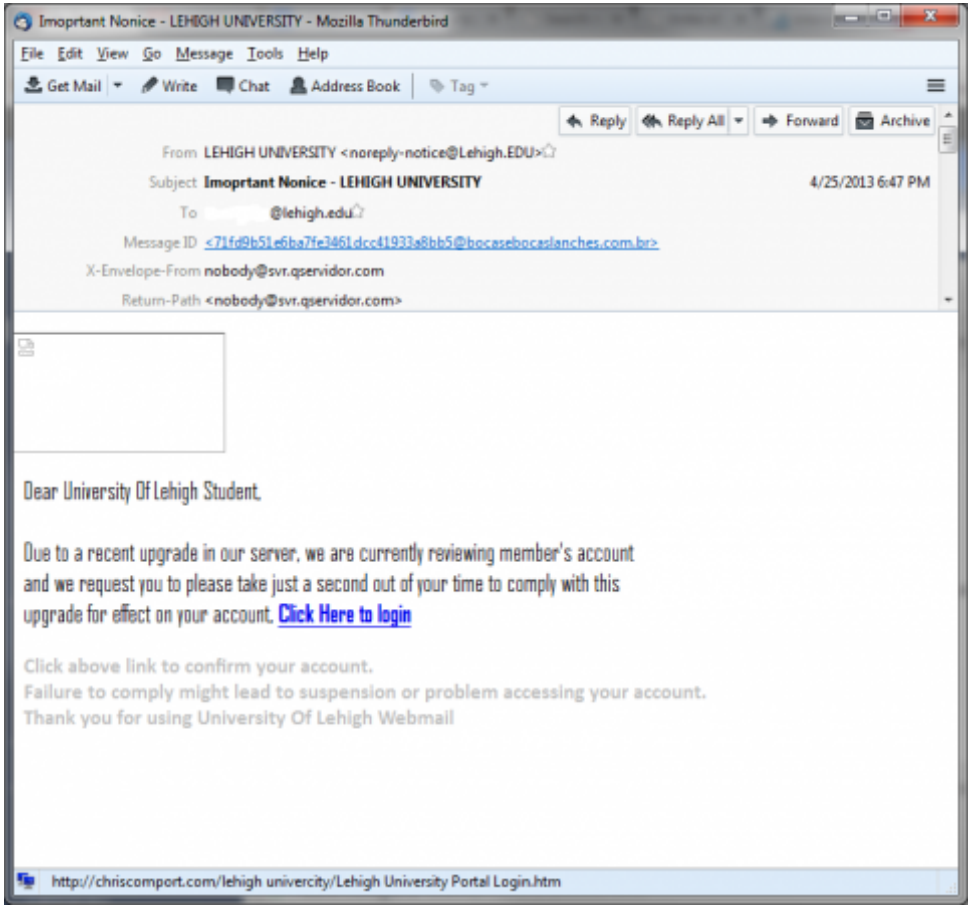
LEHIGH UNIVERSITY

Thanks
Lehigh University
27 Memorial Drive West
Bethlehem, PA 18015
(800) 523-0565

Fake "Account Update" Alert

Friday, April 26, 2013 - 08:01

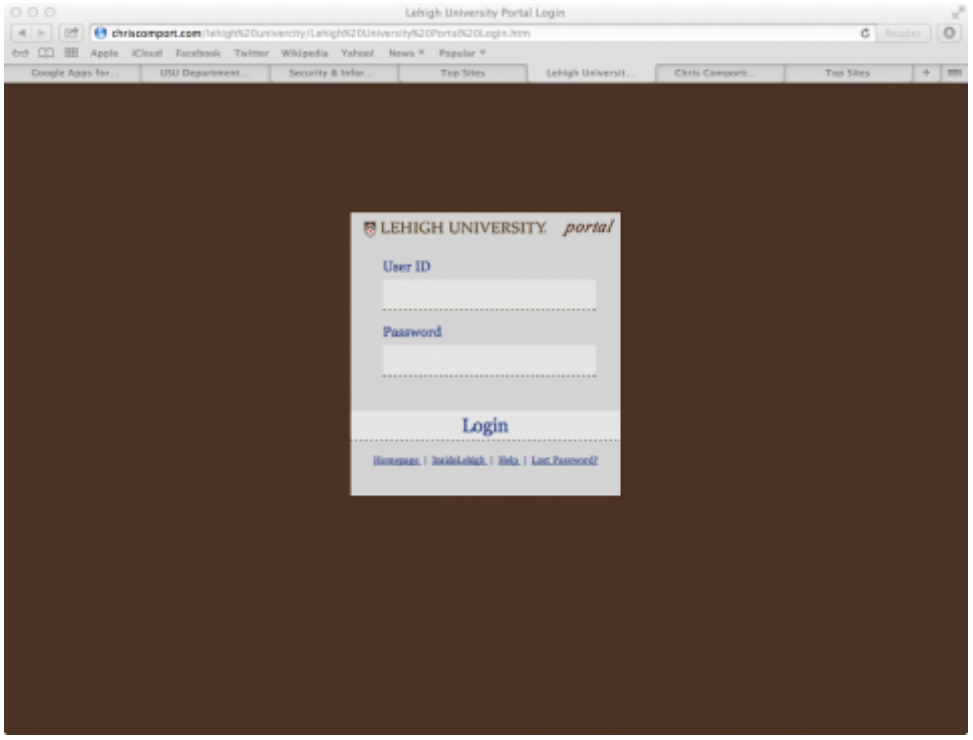
This email implies that as a result of an upgrade, you need to log in to your account to check out the "effect". It provides a link to the supposed login page (LTS would not do this--users should know where the login page is, and should know not to click on links in email messages). Notice that this link goes to a page in a non-Lehigh domain (the page looks very much like our portal login page--but if you pay attention to the web address, it can't possibly be a Lehigh page). This email should be regarded as SPAM and deleted.



Fake Portal Login Page

Friday, April 26, 2013 - 08:00

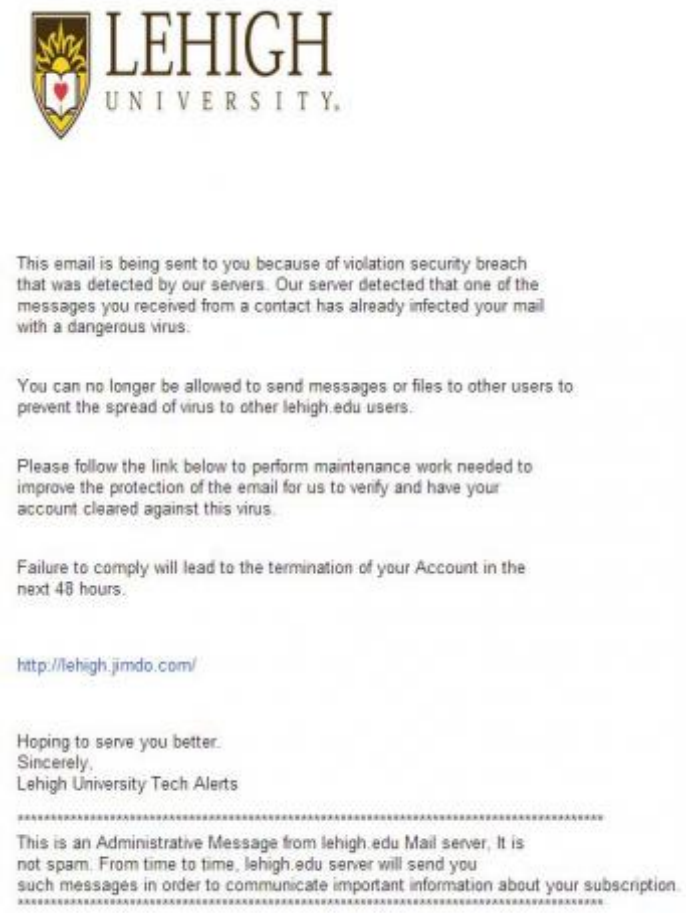
This is the fake portal login page that the fake "Account Update" alert message links to. It looks almost perfect. But notice the address, "chriscomport.com". This page is not real and you should not enter any information whatsoever into this page.



Fake "Security Breach" Alert

Friday, April 19, 2013 - 00:00

This email is quite similar to yesterday's fake Upgrade Alert message, even using the same Subject line. However this message attempts to create a sense of urgency by claiming that your account will be closed if you take no action. That should be a red flag, as LTS will never threaten you with account closure. Also notice that the link at the bottom of the email is pointing to a non-Lehigh domain. This email should be regarded as SPAM and deleted.



Fake Upgrade Alert

Thursday, April 18, 2013 - 00:00

This email purports to be a notification from LTS about upgrades to the Lehigh web-mail servers. As a security precaution, Library and Technology Services no longer sends emails with links in them. If you get an email claiming to be from us, and directing you to follow a link, you may safely assume it is fraudulent, and should delete it immediately.

Subject:LTS Help Desk
Date:Thu, 18 Apr 2013 15:36:38 +0300
From:Lehigh University <LTS-helpdesk@Lehigh.EDU>
Reply-To:noreply@Lehigh.EDU
To:You <LTS-helpdesk@lehigh.edu>

LEHIGH UNIVERSITY.

Dear Colleague,

Lehigh University have upgraded the University's Web-mail servers to the new and more secured 2013 versions.

This will enable your webmail take a new look, with new functions and anti-Spam Security.

You are hereby advised to upgrade to the University's 2013 Web-mail version to enable advanced features.

Please "Click" and "Follow" the instructions on the link below for the required Upgrade;

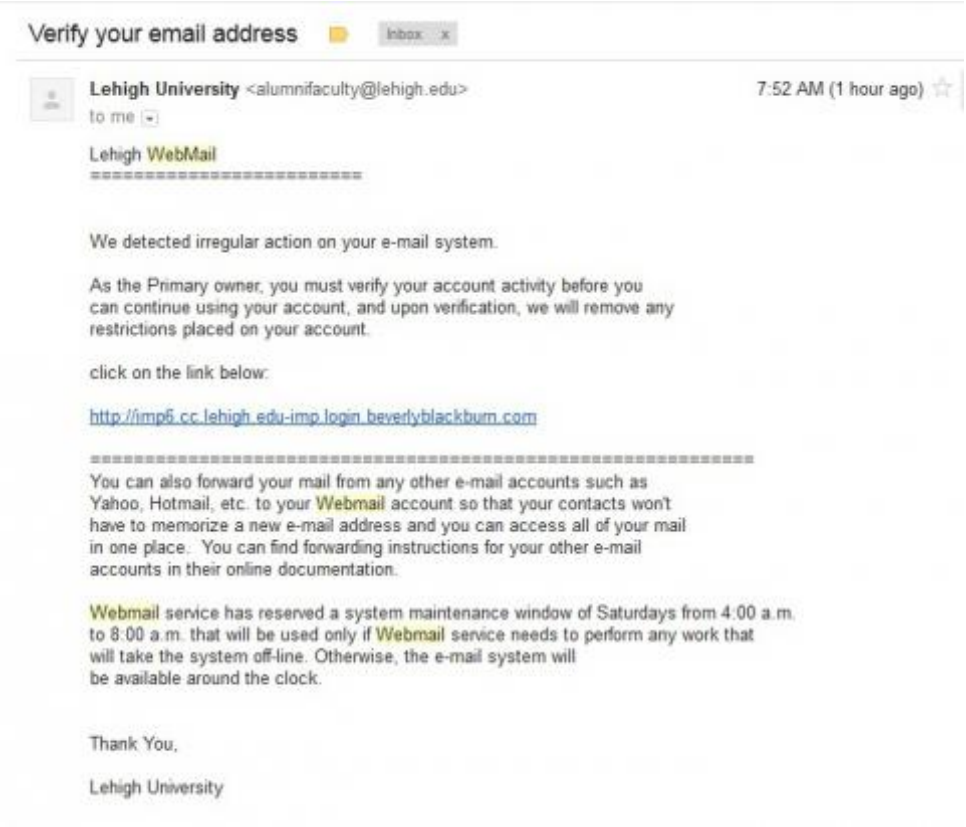
http:/Lehigh.edu/LTS/Helpdesk/

Lehigh University•
27 Memorial Drive West, Bethlehem, PA 18015 USA• (610)758-3000

Fake "Irregular Action" / Verify Address Alert

Thursday, April 4, 2013 - 08:01

This clever phishing example looks like it is from Lehigh. If you hover over the link, notice that the server address - the part between the double-slash and the next slash - is not the lehigh.edu domain (it starts out like a Lehigh web address, but it actually ends with "beverlyblackburn.com"!). Very tricky. If you were to follow this link (DON'T), you'd see a fake webmail login page (shown elsewhere in this list). NOTE: LTS will not send links in email, and we will not ask for your password!



Verify your email address Inbox x

Lehigh University <alumnifaculty@lehigh.edu> 7:52 AM (1 hour ago)

to me

Lehigh WebMail

==========

We detected irregular action on your e-mail system.

As the Primary owner, you must verify your account activity before you can continue using your account, and upon verification, we will remove any restrictions placed on your account.

click on the link below:

http://imp6.cc.lehigh.edu-imp.login.beverlyblackburn.com

==========

You can also forward your mail from any other e-mail accounts such as Yahoo, Hotmail, etc. to your Webmail account so that your contacts won't have to memorize a new e-mail address and you can access all of your mail in one place. You can find forwarding instructions for your other e-mail accounts in their online documentation.

Webmail service has reserved a system maintenance window of Saturdays from 4:00 a.m. to 8:00 a.m. that will be used only if Webmail service needs to perform any work that will take the system off-line. Otherwise, the e-mail system will be available around the clock.

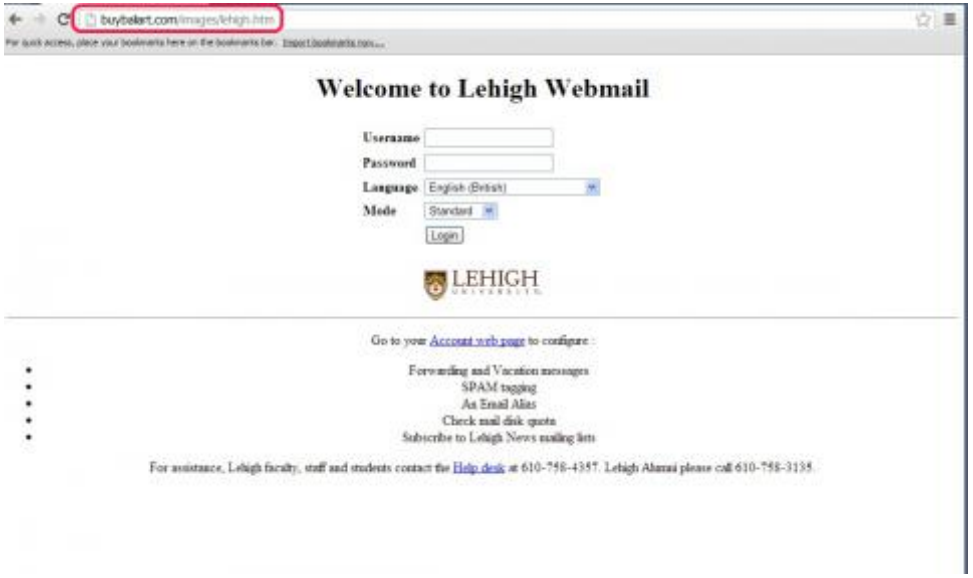
Thank You,

Lehigh University

Fake Lehigh Webmail Login

Thursday, April 4, 2013 - 08:00

This web form is attempting to look like a Lehigh secure web page. Note that the web address (URL) is not in the lehigh.edu domain.



Fake Lehigh Account Information Form

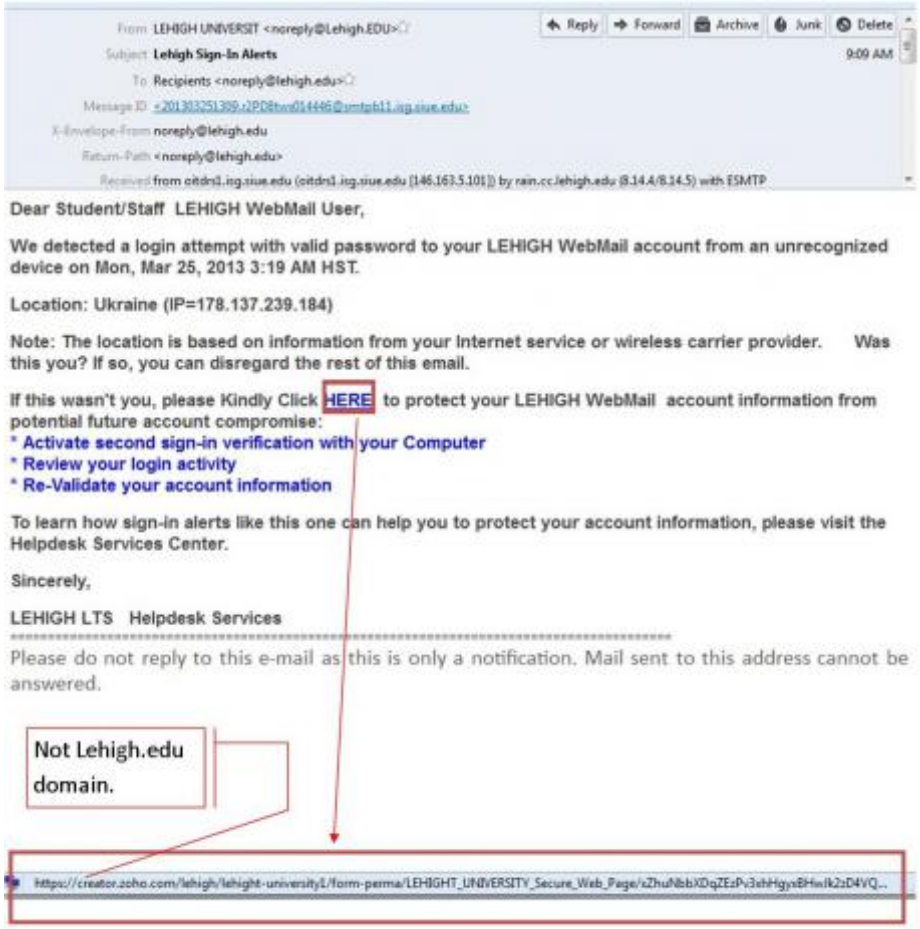
Monday, March 25, 2013 - 00:00

This web form is attempting to look like a Lehigh secure web page. Note that the web address (URL) is not the lehigh.edu domain. There are also a number of misspelled words, including Lehigh.

Fake Lehigh LTS Account Compromise Alert

Monday, March 25, 2013 - 00:00

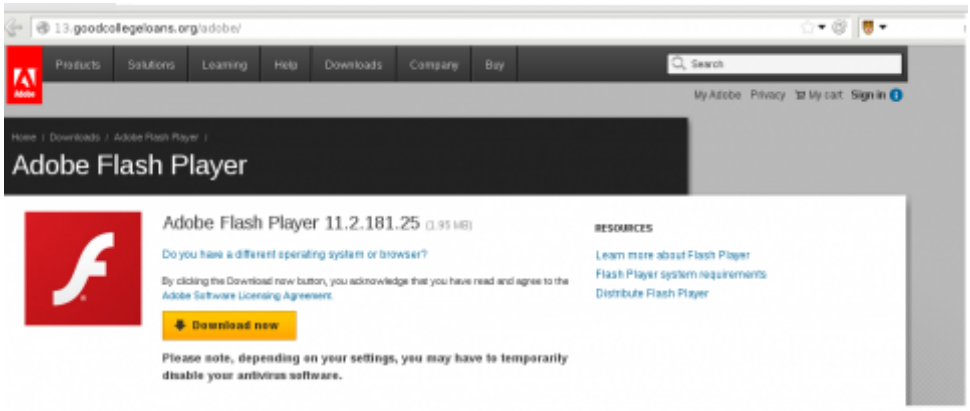
This clever phishing example looks like it is from Lehigh LTS - note that if you hover over the link, it is not the lehigh.edu domain. NOTE: LTS will not send links in email, and we will not ask for your password!



Fake Adobe Website

Thursday, March 21, 2013 - 00:00

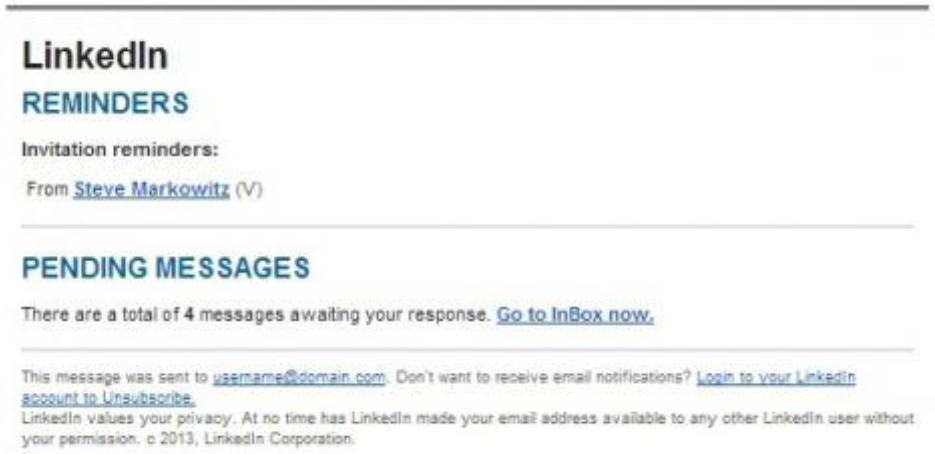
This phishing scheme takes users to a fake Adobe site. Note the web address, whose domain is "goodcollegeloans.org."



LinkedIn Email

Thursday, March 21, 2013 - 00:00

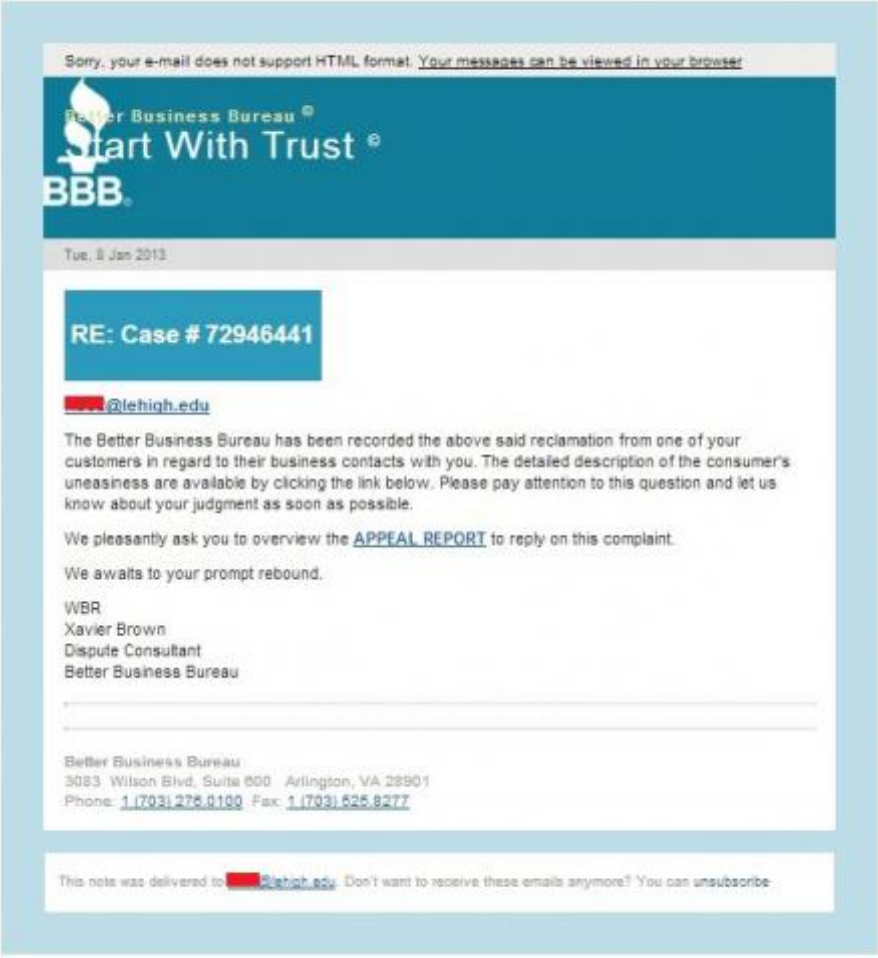
Many at Lehigh are using LinkedIn for professional networking. This example looks very much like the email messages received daily from LinkedIn.



Better Business Bureau Claim Email

Thursday, March 21, 2013 - 00:00

Phishers often use scare tactics to encourage people to click before they think! This is an example of a messages that appears to come from the Better Business Bureau.



Sorry, your e-mail does not support HTML format. Your messages can be viewed in your browser

Better Business Bureau ®
Start With Trust ®
BBB®

Tue, 8 Jan 2013

RE: Case # 7946441

[redacted]@lehigh.edu

The Better Business Bureau has been recorded the above said reclamation from one of your customers in regard to their business contacts with you. The detailed description of the consumer's uneasiness are available by clicking the link below. Please pay attention to this question and let us know about your judgment as soon as possible.

We pleasantly ask you to overview the APPEAL REPORT to reply on this complaint.

We awaits to your prompt rebound.

WBR
Xavier Brown
Dispute Consultant
Better Business Bureau

Better Business Bureau
3033 Wilson Blvd, Suite 600 Arlington, VA 28901
Phone: 1 (703) 276.0100 Fax: 1 (703) 525.8277

This note was delivered to [redacted]@lehigh.edu. Don't want to receive these emails anymore? You can unsubscribe

Amazon Order Confirmation

Wednesday, March 20, 2013 - 00:00

Clicking on the links in this fake Amazon Order Confirmation will take you to a compromised site that will infect your computer.

amazon.com

Order Processing Confirmation

Greetings [redacted]@lehigh.edu,

Thank you for shopping with us. We have to inform ya that secondpity shipped your item, and that this completes your order.. If you need to return an good from this shipment or manage other orders, please visit Your Orders on Amazon.com.

Your estimated shipment delivery date is:
Friday, September 21, 2012

Why tracking information may be not available?

Your order was delivered to:

539 S Louis Dr , App. 8B
S Maria, KY
United States

This shipment have no an associated delivery number of tracking.

Conveyance Information

$771.69

Samsung XVT3D23, SV 46-Inch 720p 100 Hz Cinema 3D LED-LCD HDTV with 3D Blu-ray Player and Three Pairs of 3D Glasses
Sold by: onner
Condition: used - acceptable

Item Subtotal:	$771.69
Shipping & Handling:	$23.99
Total Before Tax:	$771.69
Shipment Total:	**$771.69**
Paid by Check:	$771.69

Returns are easy. Visit our Online Return Center
If you need further assistance with your order, please visit Merchant Contact Form

We hope to see you again soon!
Amazon.com

Unless otherwise noted, items are sold by Amazon LLC. Learn more about tax and good provider information

This email was sent from a notification-only address that cannot accept incoming email. Please don't reply to this message.

Income Tax Return Payment Receipt

Wednesday, March 20, 2013 - 00:00

This message purports to be a rejected electronic income tax refund. It attempts to trick you into downloading and opening an infected Word document.

Your Federal Tax remittance (ID: 57378473347676), recently sent from your checking account was returned by The Electronic Federal Tax Payment System.

	Rejected Tax transaction
Tax Transaction ID:	57378473347676
Reason	See details in the report below
Income Tax Transaction Report	tax_report_57378473347676.doc (Microsoft Word Document)

Internal Revenue Service P.O. Box 996 Augusta 38914 NY

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