Phishing / Vishing / Smishing Scams via Email/SMS/Phone Call

Overview

Scammers are always looking for new ways to trick us. These scams can be difficult to detect. Sometimes scammers pose as employers or business associates. They try to gain access to your Lynn username and password, your bank account, or other information.

Definitions

Phishing

The fraudulent practice of **sending emails** or other messages purporting to be from reputable companies or portraying to be an executive or high ranking position at Lynn University in order to induce individuals to reveal personal information, such as passwords and credit card numbers and or engage to complete university business or tasks for them.

Vishing

The fraudulent practice of **making phone calls or leaving voice messages** purporting to be from reputable companies or portraying to be an executive or high ranking position at Lynn University in order to induce individuals to reveal personal information, such as bank details and credit card numbers and or engage to complete university business or tasks for them.

Smishing

The fraudulent practice of **sending text messages** purporting to be from reputable companies or portraying to be an executive or high ranking position at Lynn University in order to induce individuals to reveal personal information, such as passwords or credit card numbers and or engage to complete university business or tasks for them.

You will never be asked:

You will never be asked:

- to increase/decrease your mailbox size
- to increase/decrease the space on your One Drive or Personal Drive
- to validate/verify or confirm your Lynn login information/credentials
- to update/validate your direct deposit information
- to provide passwords
- to update a GoogleDocs or One Drive document not associated with Lynn
- to respond to a potential Job

Identifying Phishing / Vishing / Smishing Email Scams:

- The person communicating with you is not listed on the https://www.lynn.edu/campus-directory/people website.
- The person communicating with you is listed on the organization's website; however, the email address does not match the university's domain name, @lynn.edu.
- The person communicating with you is an executive or a high ranking position at the university that you normally do not interact with is asking you for a favor directly via a text/sms on your personal cell phone
- The person communicating with you is an executive or a high ranking position at the university that you normally do not interact with is asking you for a favor directly via an email on your personal email address
- The person/organization requests your bank account information to deposit large sums of money into your account.
- The person/organization sends you checks or money and asks you to buy gift cards in exchange.
- There is no face-to-face (virtual or otherwise) communication.
- The process is rushed, or the person/organization asks you to rush.
- There are spelling errors in the body of the sender's email
- Unexpected email attachments
- Poor spelling and grammar
- Hyperlinks in email
- A sender’s address that doesn’t match the name
- Request for payment or login information
- Threats
- Spoofing well-known companies
- Too good to be true
- The wording is slightly off.
- Warnings about your account being shut down
- A company logo that looks resized
- Threats of legal action
- Confirmation of shipment that you didn't order
- General salutations, not personalized
- Sudden urgency
- Inaccuracies

Do's:

- Verify the sender of a message and call them on the phone if you have to.
- Hover over web page links (URLs) in email messages to see where they link to – beware of URL shortening services (like bit.ly) that may obscure the final website destination.
- Be skeptical of messages with odd spelling/grammar, improper logos, or that ask you to upgrade or verify your account.

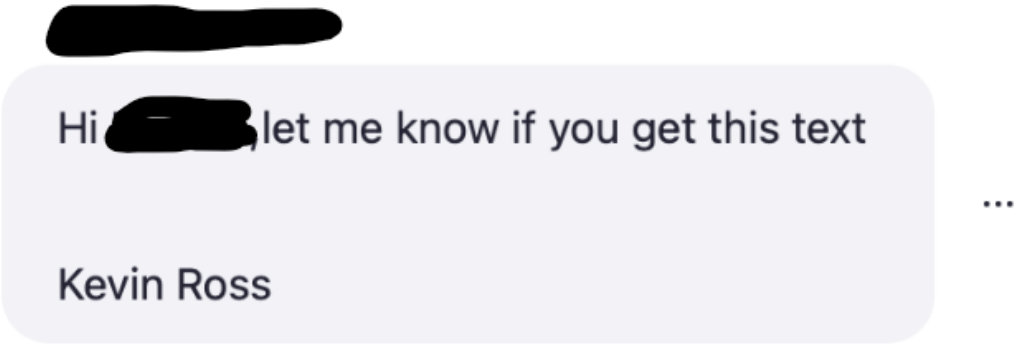
Don'ts:

- Open attachments from unknown senders.
- Click on a link from an unknown sender.
- Email someone your username or password.
- Email an attachment with sensitive university information that is not encrypted.
- Click on a link from an unknown or unexpected sender and then enter your Lynn username and password.

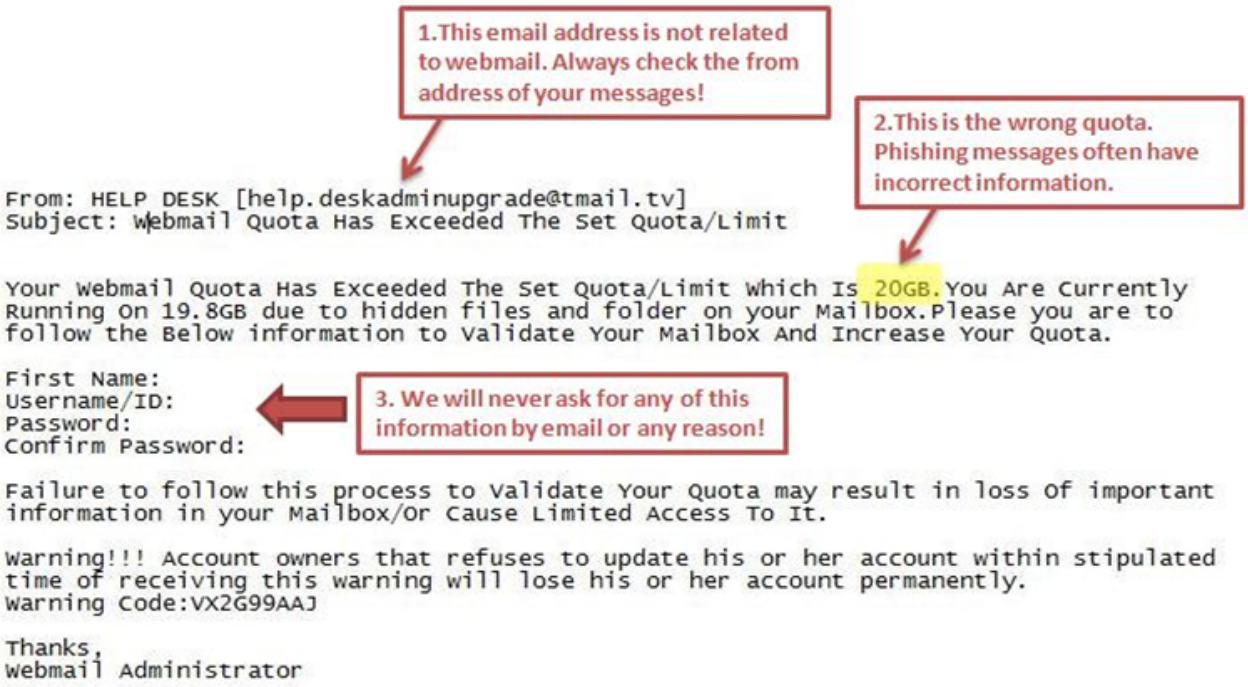
What if I clicked the link or responded?

- Change your password immediately.
- Call the IT Support desk right away
- As for procedures on what to do next
- Inform your supervisor of the incident

Smishing Examples



Phishing Email Examples



Hello!
As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

Spelling

Our system detected unusual Copyrights activity linked to your Facebook account , please follow the link bellow to fill the Copyright Law form:

http://www.facebook.com/application_form Links in email

Note: If you dont fill the application your account will be permanently blocked. Threats

Regards,

Facebook Copyrights Department. Popular company

Hello!
As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

Spelling

Our system detected unusual Copyrights activity linked to your Facebook account , please follow the link bellow to fill the Copyright Law form:

http://www.facebook.com/application_form Links in email

Note: If you dont fill the application your account will be permanently blocked. Threats

Regards,

Facebook Copyrights Department. Popular company

From: MailChimp Billing <noreply@drsha.com>
Date: February 27, 2019 at 1:35:03 PM EST
To: [redacted]
Subject: MailChimp Billing Dispute In Progress

A payment issue has been reported on your account.

Billing and sending has been disabled until the issue is resolved.

To resolve this and re-enable billing and sending, navigate to the Monthly plans or credits page in your account and re-purchase the order.

To learn more about this charge, please contact the Billing Team.

Update Billing Information

Thu 2/28/2019 2:36 PM

[redacted]

Be sure to read this message! Your personal data is threatened!

To [redacted]

You forwarded this message on 2/28/2019 2:49 PM.

Hi!

As you may have noticed, I sent you an email from your account.
This means that I have full access to your account.

I've been watching you for a few months now.
The fact is that you were infected with malware through an adult site that you visited.

If you are not familiar with this, I will explain.
Trojan Virus gives me full access and control over a computer or other device.
This means that I can see everything on your screen, turn on the camera and microphone, but you do not know about it.

I also have access to all your contacts and all your correspondence.

Why your antivirus did not detect malware?
Answer: My malware uses the driver, I update its signatures every 4 hours so that your antivirus is silent.

I made a video showing how you satisfy yourself in the left half of the screen, and in the right half you see the video that you watched.
With one click of the mouse, I can send this video to all your emails and contacts on social networks.
I can also post access to all your e-mail correspondence and messengers that you use.

If you want to prevent this,
transfer the amount of $737 to my bitcoin address (if you do not know how to do this, write to Google: "Buy Bitcoin").

My bitcoin address (BTC Wallet) is: 1GoWy5yMzh3XXBiYxLU9tKCBMgibpznGio

After receiving the payment, I will delete the video and you will never hear me again.
I give you 48 hours to pay.
I have a notice reading this letter, and the timer will work when you see this letter.

Filing a complaint somewhere does not make sense because this email cannot be tracked like my bitcoin address.
I do not make any mistakes.

If I find that you have shared this message with someone else, the video will be immediately distributed.

Best regards!

Thu 2/28/2019 2:36 PM

[redacted]

Be sure to read this message! Your personal data is threatened!

To [redacted]

You forwarded this message on 2/28/2019 2:49 PM.

Hi!

As you may have noticed, I sent you an email from your account.
This means that I have full access to your account.

I've been watching you for a few months now.
The fact is that you were infected with malware through an adult site that you visited.

If you are not familiar with this, I will explain.
Trojan Virus gives me full access and control over a computer or other device.
This means that I can see everything on your screen, turn on the camera and microphone, but you do not know about it.

I also have access to all your contacts and all your correspondence.

Why your antivirus did not detect malware?
Answer: My malware uses the driver, I update its signatures every 4 hours so that your antivirus is silent.

I made a video showing how you satisfy yourself in the left half of the screen, and in the right half you see the video that you watched.
With one click of the mouse, I can send this video to all your emails and contacts on social networks.
I can also post access to all your e-mail correspondence and messengers that you use.

If you want to prevent this,
transfer the amount of $737 to my bitcoin address (if you do not know how to do this, write to Google: "Buy Bitcoin").

My bitcoin address (BTC Wallet) is: 1GoWy5yMzh3XXBiYxLU9tKCBMgibpznGio

After receiving the payment, I will delete the video and you will never hear me again.
I give you 48 hours to pay.
I have a notice reading this letter, and the timer will work when you see this letter.

Filing a complaint somewhere does not make sense because this email cannot be tracked like my bitcoin address.
I do not make any mistakes.

If I find that you have shared this message with someone else, the video will be immediately distributed.

Best regards!

Mon 3/11/2019 7:05 PM

[redacted]@email.lynn.edu>

Incoming Doc File

To keldjoness@outlook.com

Office-365

Andrew Kosow "akosow@email.lynn.edu" sent you a Doc to review

Kindly click to **Preview**

We hope to serve you better.

Thanks,
The Microsoft account team

ADMINISTRATIVE ASSISTANT REMOTE JOB

[redacted]

Fri 1/13/2023 2:00 PM

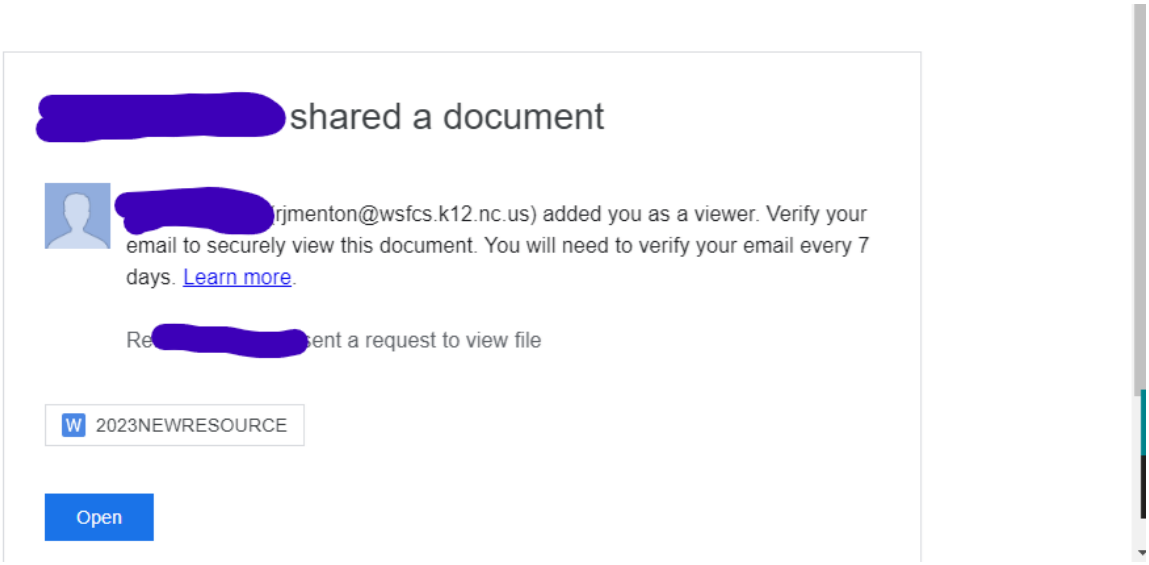
Some departments are currently hiring individuals who can assist some of their visiting professors by providing basic admin duties remotely.
The successful candidate will Liaise with staff, other departments, and/or external organization concerning matters regarding assigned work as well as coordinating with the Director.

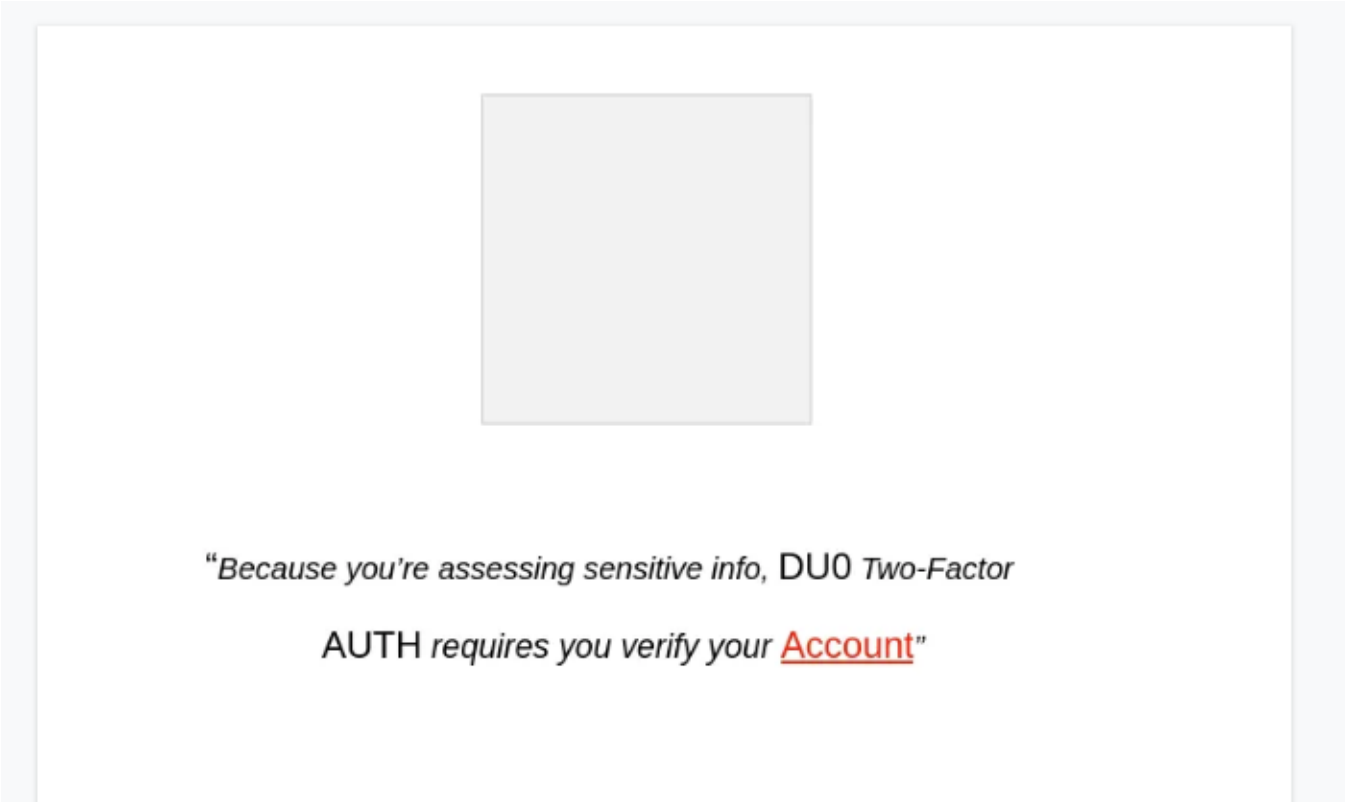
Weekly Salary:
$400 ($350 +$50 for miscellaneous including tax)

For more Information. Contact (frank.garza302@gmail.com) with your alternative "email address" as well as your school schedule.

Sincerely,
Frank Garza
Senior investment Director
(909) 366-3151
frank.garza302@gmail.com

Reply | Reply all | Forward





If you are worried that you may be the victim of a phishing email, notify your bank immediately and alert Campus Safety at 561-237-7226.