SCAMS

created by Amanda Hakes

This presentation will discuss:

- Phishing scams
- Phone scams
- Social Security scams
- Immigration scams
- Mail / Fake check scams
- Recent scams at Binghamton University
- Resources
- Questions?

Online/Email Scams

- **Phishing Scams-** Phishing is a technique in which users are directed by an official-looking e-mail to provide personal information under false pretenses. The message appears to come from a legitimate source such as a bank, police agency, friend, or other company. The information requested may be a credit card number, social security number, ATM PIN number, password or other personal information.
- The recipient is asked to provide this information via e-mail or by visiting an official-looking website and warned that failure to do so may result in a discontinuation of service.

https://www.binghamton.edu/its/about/organization/information-security/phishing.html

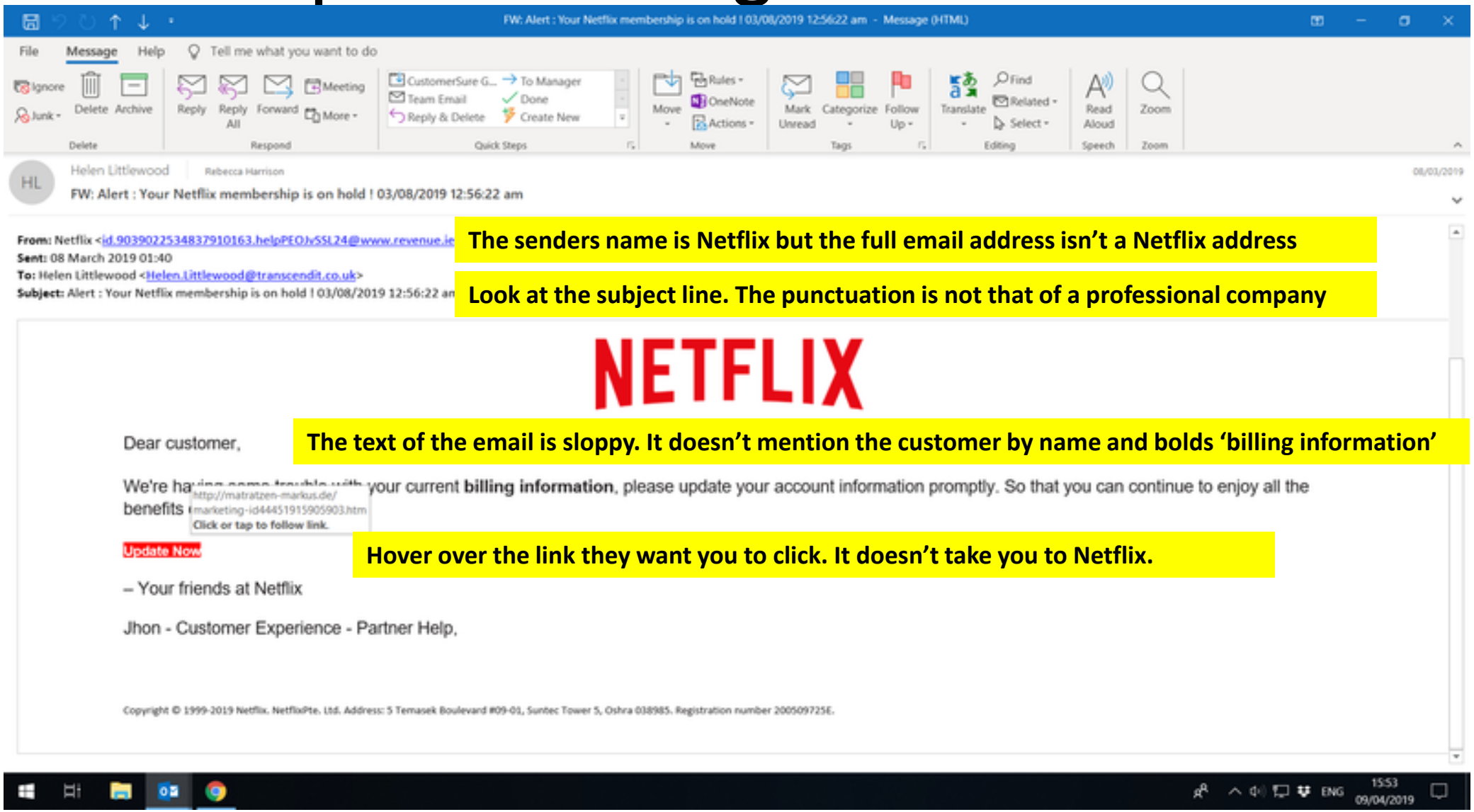
How to Recognize Phishing

Phishing emails often try to trick you into clicking a link or opening an attachment. They may

- Say they've noticed some suspicious activity or log-in attempts
- Claim there's a problem with your account or your payment information
- Include a fake invoice
- Say you're eligible for a government refund
- Offer a coupon for free stuff

https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams#recognize

How to Spot a Phishing Email



Phone Scams

- Do not trust caller ID. Phone numbers can be easily spoofed to show up on caller ID as official phone numbers.
- Don’t give the caller **ANY** personal information! Even if they have some of your information, do not give them any additional information.
- The real Social Security Administration, USCIS, IRS etc. will not contact you via phone.
- End the conversation immediately if threats and/or intimidation persists.
- If a caller tells you to meet them somewhere to make a payment, you should hang up immediately. Under no circumstances should you ever meet anyone who claims to be from a government agency to make a payment.

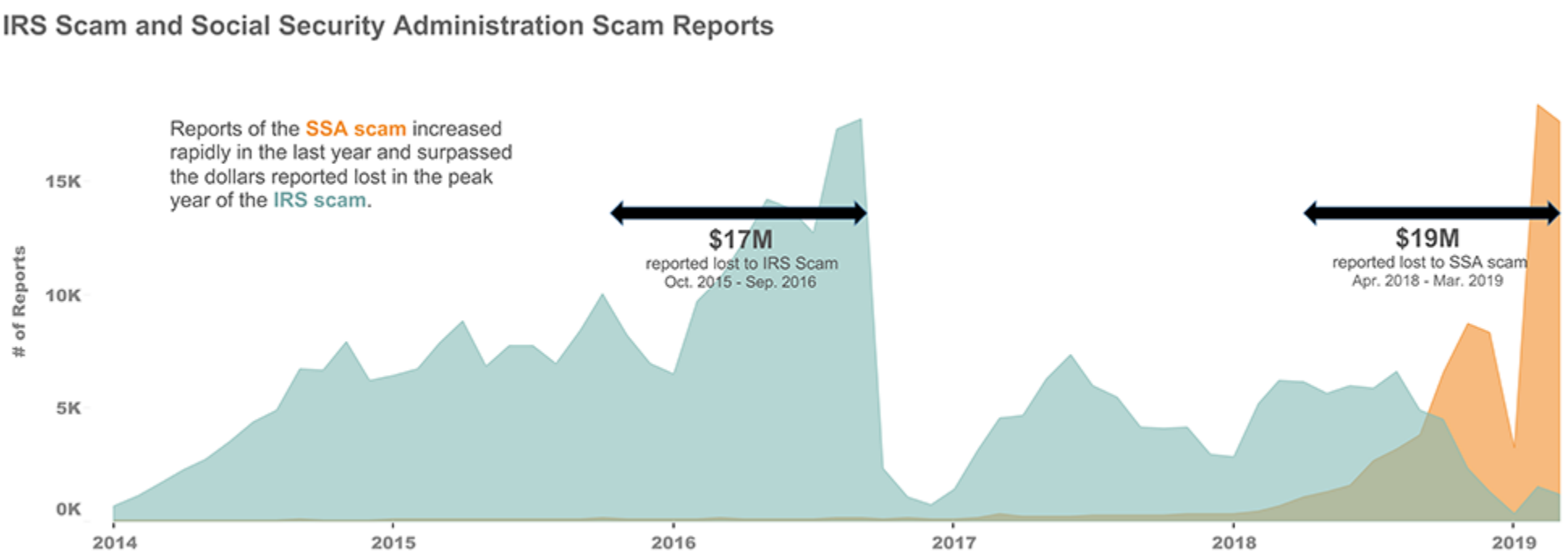
Social Security Scams

- Social Security will not send you an email or call you asking you to give them your personal information, such as your Social Security number, date of birth, or other private information.
- If someone saying they are from Social Security does call or email you requesting information, don’t respond to the message.
- Social Security will never suspend your Social Security Number, EVER!

https://youtu.be/8N96ORODZm8

Social Security Scams

- The median individual loss in 2018 was $1,500.
- People are sending money in unconventional ways such as gift cards and Bitcoin ATMs. Governments agencies will **NEVER** ask for immediate payment and **NEVER** in gift cards or Bitcoin!



Click image to open in high resolution

https://www.ftc.gov/news-events/blogs/data-spotlight/2019/04/growing-wave-social-security-imposters-overtakes-irs-scam

IMMIGRATION SCAMS

- USCIS and other government agencies will not ask for personal or password information in unsolicited e-mail messages. You should **NEVER** respond to them or click on any of the messages. These messages are phishing emails.

- If you receive a phone call from an individual claiming to work for a U.S. government agency (IRS, ICE, Dept. of Homeland Security, etc.), ask for the caller's name, badge ID, phone number and request that you call them back. If they insist you cannot call them back, **hang up**. If they tell you that this is your only opportunity to resolve the issue and if you hang up you will be arrested or deported, **DO NOT BELIEVE THEM**. Hang up and come to the ISSS office. If it is after hours, contact the University Police.

Mail and Fake Check Scams

- Do not cash or deposit any checks sent to you from someone you do not know. Many times scammers claim they do not have a U.S. bank account and if you deposit the money in your account, they will let you keep a portion of the money. After you cash it and send them the money back, the check will bounce and you will be liable for the full amount of the check and the bounced check fee.
- Similar to this, there have recently been employment scams where fake employers are contacting and “hiring” students, then wanting them to deposit a check in their bank account to pay for equipment purchases. This is a scam and is not legitimate work. As a reminder, any off-campus work requires ISSS authorization!
- Do not send cash in the mail! If you are ever told to send cash to fix an immigration issue, hang up. Do not send cash!

Recent Scams at Binghamton

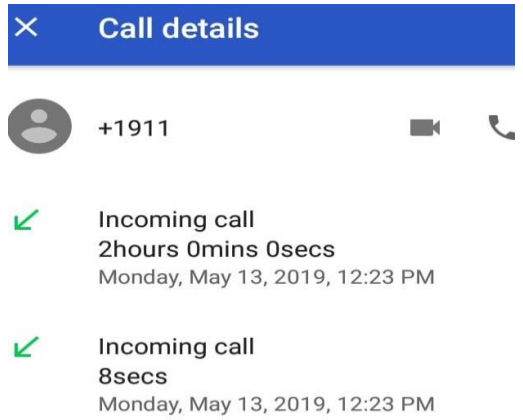
A student received a call from a spoofed number that came up on their phone as '911'. Upon answering, they were told they violated immigration regulations by not completing a specific immigration form when entering the U.S. The caller identified themselves as a USCIS agent and gave a phony badge number and had a foreign accent. The person proceeded to use scare tactics stating the student would go to jail and the police were outside their house watching the student. The student stated they would come to the ISSS office, and the caller said the police were at the ISSS office. All of this was FALSE information used to scare the student into giving the caller what they wanted, which was gift cards for "payment".

The student ended up buying gift cards totaling over $1,200 out of fear and lost that money. This was a scam.

The ISSS is here to HELP you, you can always come to our office for assistance. If we are closed, call the campus police non-emergency phone number: 607-777-2393.

Government agencies will **NEVER** ask for payments in gift cards!

*Note the caller ID is spoofed and is +1911!



Recent Scams at Binghamton

Many students have received emails regarding employment opportunities that sound too good to be true. They promise flexible hours, good wages and say they got your contact information from an administrator at Binghamton University.

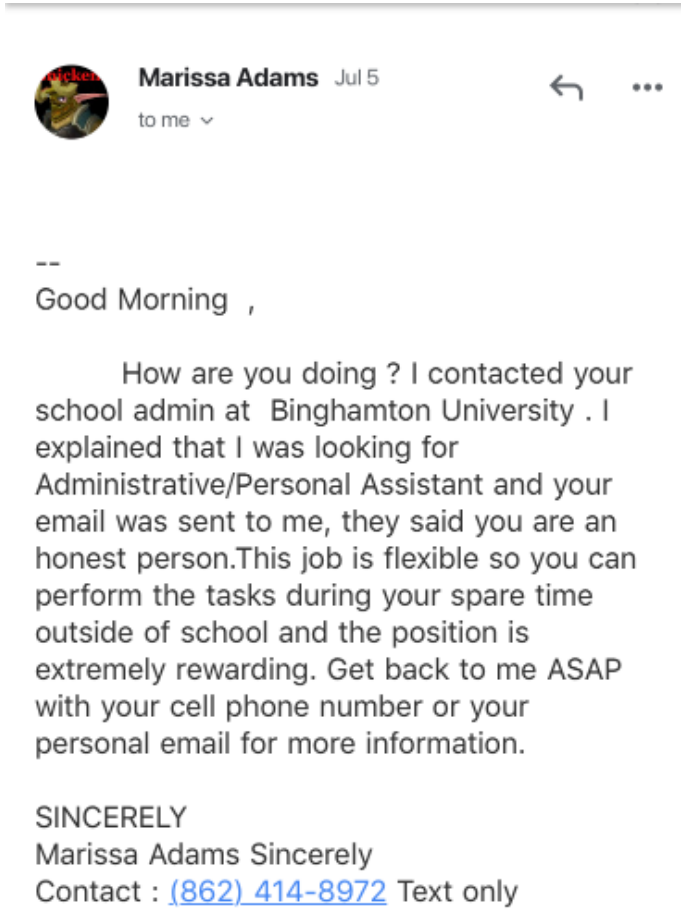
This is not true, it is a scam!

You should delete emails like this and not respond.

Binghamton University employees never give out your information to any off-campus employers or agencies.

As a reminder, you cannot work off campus without ISSS authorization!

If you do not know if it is a true employment opportunity, you should contact the Fleishman Center. You can visit their office in UU-133 or email hirebing@binghamton.edu. They will review any job description, offer, email etc.



Marissa Adams Jul 5

to me

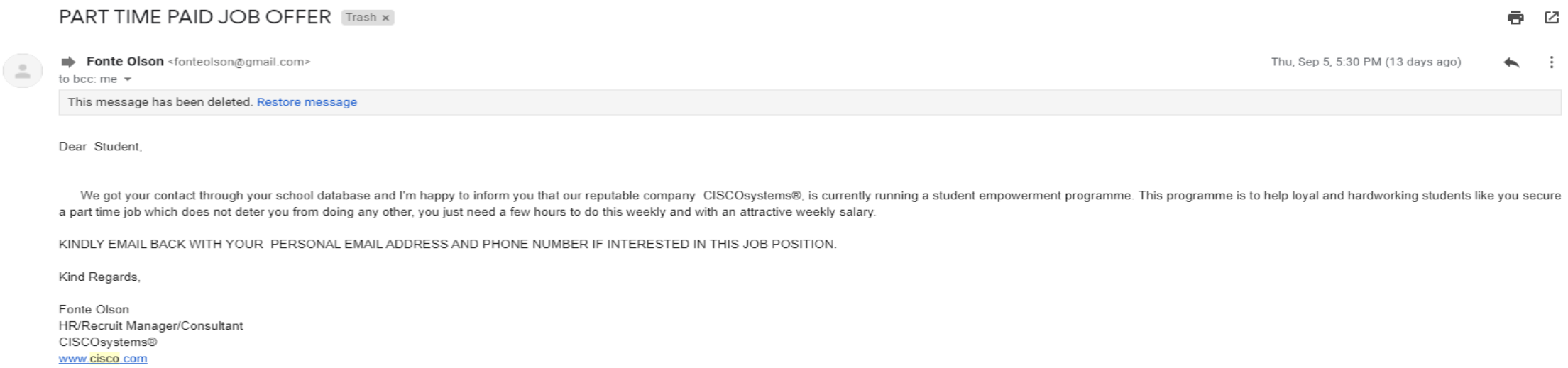
--

Good Morning ,

How are you doing ? I contacted your school admin at Binghamton University . I explained that I was looking for Administrative/Personal Assistant and your email was sent to me, they said you are an honest person.This job is flexible so you can perform the tasks during your spare time outside of school and the position is extremely rewarding. Get back to me ASAP with your cell phone number or your personal email for more information.

SINCERELY
Marissa Adams Sincerely
Contact : (862) 414-8972 Text only

Recent Scams at Binghamton



PART TIME PAID JOB OFFER Trash ×

Fonte Olson <fonteolson@gmail.com> Thu, Sep 5, 5:30 PM (13 days ago)
to bcc: me

This message has been deleted. Restore message

Dear Student,

We got your contact through your school database and I'm happy to inform you that our reputable company CISCOsystems®, is currently running a student empowerment programme. This programme is to help loyal and hardworking students like you secure a part time job which does not deter you from doing any other, you just need a few hours to do this weekly and with an attractive weekly salary.

KINDLY EMAIL BACK WITH YOUR PERSONAL EMAIL ADDRESS AND PHONE NUMBER IF INTERESTED IN THIS JOB POSITION.

Kind Regards,

Fonte Olson
HR/Recruit Manager/Consultant
CISCOsystems®
www.cisco.com

Many students have received this email from someone claiming to work at Cisco, which is a legitimate company; however, this email is a scam.

After many students responded seeking further information they were mailed a check anywhere from $800-$1,200 from a random address on the return address. If you receive anything like this you should NOT cash the check and take it to University Police immediately.

If you deposit it in your account and follow the scammers instructions the check will eventually bounce and you will be liable for thousands of dollars to your financial institution.

- No Government agency will ever ask for payment in a gift card!
- Gift cards are for gifts. They are not for payments.
- If someone tells you that you can pay for a immigration, tax or other problem to go away by paying with a gift card, hang up the phone immediately!

https://www.youtube.com/watch?v=HfHI6ToZff4

Reminders

- It’s ok to TALK ABOUT SCAMS. Many people recognize scams but may get caught off guard because scammers are so persuasive and aggressive. Talking to friends/classmates to spread the word may help educate them on scams they may not know about and help them from falling victim to scammers.

- Remember, being targeted by a scam can be a traumatic event. The University Counseling Center is here to help. Contact them for an appointment at 607-777-2772.

Resources

- Come to the ISSS, 142 Old Champlain, Floor 1R or call 607-777-2510
- If outside ISSS office hours, contact University Police at their non-emergency phone 607-777-2393
- If you have questions about a job email, offer or posting visit the Fleishman Center in UU-133 or email hirebing@binghamton.edu.
- Read the ISSS Newsletter
- If you have a questionable email, report it to ITS by forwarding to security@binghamton.edu.
- Visit the ITS Phish Tank for the latest Binghamton directed phishing scams. https://www.binghamton.edu/its/about/organization/information-security/phishing.html
- If your Social Security Number has been exposed or misused, visit https://identitytheft.gov/ssa or call the SSA Fraud Hotline 1-800-269-0271
- Report gift cards used in scams at FTC.gov/giftcards
- Report any type of scam or fraud to ftc.gov/complaint or call 1-877-FTC-HELP

Questions?