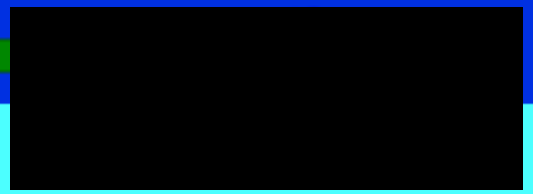
RECOGNIZING AND AVOIDING SCAMS



ONLINE / EMAIL SCAMS

- Phishing emails often try to trick you into clicking a link or opening an attachment.
- The message appears to come from a legitimate source. 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 discontinuation of a service.

https://www.binghamton.edu/its/about/organization/security/phishing.htm

PHONE SCAMS

- Do not trust caller ID. Phone numbers can be easily spoofed to show up on caller ID as official phone numbers.
- ' R Q ¶ W J L Y H W K H F D O O H U D Q \ S H U V R Q D O L Q I R U
- The real Social Security Administration, USCIS, and IRS will not contact you unexpectedly via phone. If you make an appointment with the Social Security office they will call you back to make an appointment.
- If a caller tells you to meet them somewhere to make a payment, you should hang up immediately.
- The U.S. government will never text you asking for personal information.

SCAMS IMPERSONATING U.S. OFFICIALS

- USCIS and other government agencies will not ask for personal or password information in unsolicited e-mail messages.
- If you receive an unexpected phone call from an individual claiming to work for a U.S. J R Y H U Q P H Q W D J H Q F \ D V N I R badge ID, phone number and request that you call them back.
- The Social Security Administration will never suspend your Social Security Number.

MAIL AND FAKE CHECK SCAMS

- Do not cash or deposit any checks sent to you from someone you do not know.
- There have recently been employment scams where fake employers are contacting and ³ K L U L Q J ´ V W X G H Q W V W K H Q Z D deposit a check in their bank account to pay for equipment purchases. This is a scam and is not legitimate work.
- Do not send cash in the mail! If you are ever told to send cash to fix an immigration or IRS issue, hang up. Do not send cash!

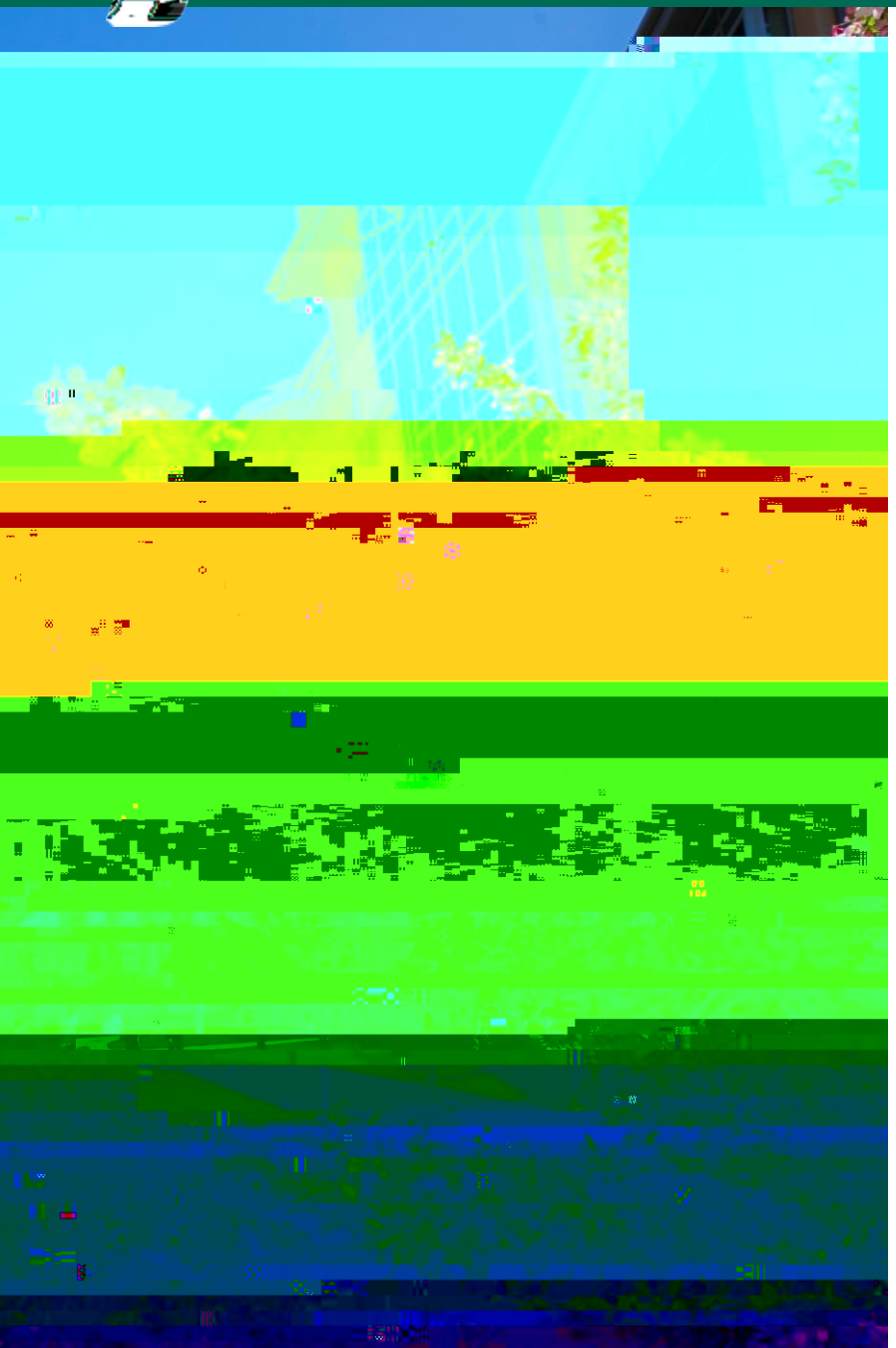
CORONAVIRUS SCAMS

- Ignore offers for vaccinations and home test kits. - Scammers are selling products to treat or prevent COVID-19 without proof they work.
- Stay informed! ±Only use sites like https://www.coronavirus.gov/ , https://www.usa.gov/coronavirus or https://coronavirus.health.ny.gov/home to get the latest information.
- , I \ R X J H W D F D O O I U R P ³ 1 < 6-3 &7 R Q W D F W L Q J ´ **PLEASE answer the phone.**
- Be aware of scams: a contact tracer will never:
  - ask for your Social Security number
  - ask for any private financial information
  - ask for credit card information
  - send you a link without proper authentication procedures

https://www.ftc.gov/coronavirus/scams-advice

RECENT SCAMS AT BINGHAMTON

- Students received an email offering employment that sounds too good to be true and saying they got the student's name from an administrator. This is not true. If you get an unsolicited job offer, it's probably a scam.
- A student received a call that appeared to be from 911 on their cell phone. The caller claimed they were about to be deported and used many scare tactics. They told the student that if they went to the ISSS office, police were waiting there to arrest them. The student was scared and paid a large amount of money in gift cards.
- Students from China have been targeted by phone scammers impersonating Chinese police officers, Chinese government officials, or employees at banks in China. The caller claims that the student has been involved with illegal activity or has been the victim of identify theft. They then ask for personally identifying information and may demand payment of thousands of dollars to resolve the problem.



RESOURCES

- Call the ISSS at 607-777-2510 or email us at ISSS@Binghamton.edu
- If outside ISSS office hours, contact University Police at their non-emergency phone 607-777-2393
- The University Counseling Center can be contacted for an appointment at https://www.binghamton.edu/counseling or call for an appointment at 607-777-2772.
- If you have questions about a job email, offer or posting call the Fleishman Center 607-777-2400 or email hirebing@binghamton.edu
- 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/

QUESTIONS?

Employment: intl.work@binghamton.edu

Extending Your I-20 or DS-2019:intl.extend@binghamton.edu

Health Insurance: intl.insure@binghamton.edu

All Other Questions: isss@binghamton.edu

Advising Hours: Call 607-777-2510

- Monday & Tuesday: 10:00am-11:45am
- Wednesday & Thursday: 1:30pm-3:30pm