

Educating International Students & Scholars about Common Scams

Masume Assaf, The Pennsylvania State University
Senem Bakar, American University
Christina Lehnertz, George Mason University
Bronwen Watts, Colorado State University

Recent Incidents

Chinese Students Scammed – Tuition Money

- ◆ At Penn State in 2018-19 academic year, a student convinced some students that they could save up to 10% on tuition by allowing this student to pay the tuition. She had a way to get a discount from Penn State. Several students were convinced by the fellow student and gave their Penn State User ID and password to the University access account. The fellow students could see a portion was paid, and then paid the student for her payments. Unfortunately, Penn State was contacted by the banks that some tuition payments paid by credit cards were with stolen credit cards. All of the students were recharged tuition. At this time, all but five or six students have repaid the tuition. There were a handful of Penn State students affected by the same type of scam in the 2017-18 academic year.

- ◆ University of Washington students (possibly 90) from China were defrauded of tuition money.

<https://www.seattletimes.com/seattle-news/education/tuition-scam-takes-up-to-1-million-from-uw-students/>

“... several students said a UW student from China who was well-known in the community spread word of he deal through a popular Chinese social-media app called WeChat. Because the student was active in UW student clubs for a number of years, she was widely trusted, said George Zhou, a sophomore math major

Schulz said the students were asked by the scammers to give their UW ID and password, used to get access to the student's account. The people running the scheme apparently used stolen credit-card numbers to pay a tuition bill, which generated a confirmation from the university that it had been paid. The student then would give the schemers a check or wire them money.

<https://bursar.psu.edu/credit-card-scam-targeting-international-students>

CREDIT CARD SCAM TARGETING INTERNATIONAL STUDENTS

ALERT DATE:

08/16/2018

MESSAGE:

HIGHER EDUCATION INSTITUTIONS HAVE RECENTLY SEEN A SURGE IN A NEW CREDIT CARD SCAM TARGETING INTERNATIONAL STUDENTS. IN THIS NEW SCAM, A THIRD PARTY CONTACTS STUDENTS VIA SOCIAL MEDIA (I.E., WECHAT) OR IN PERSON OFFERING TO SECURE AN ADVANTAGEOUS CURRENCY EXCHANGE RATE IF THE THIRD PARTY MAKES A CREDIT CARD PAYMENT ON BEHALF OF THE STUDENT. THE STUDENT PROVIDES ACCESS TO THEIR STUDENT ACCOUNT (USER ID AND PASSWORD), AND THE THIRD PARTY LOGS IN AS THE STUDENT TO MAKE THE PAYMENT. WHEN THE STUDENT SEES THAT THEIR BALANCE IS PAID, THEY TRANSFER PAYMENT TO THE THIRD PARTY. BECAUSE THE THIRD PARTY IS USING STOLEN CREDIT CARDS TO MAKE PAYMENTS, SEVERAL WEEKS CAN PASS BEFORE IT IS DISCOVERED THAT THE PAYMENT MADE BY THE THIRD PARTY IS FRAUDULENT. STUDENTS WHO FALL VICTIM TO THIS SCAM CAN EXPERIENCE A SIGNIFICANT LOSS OF FUNDS.

Recent scams have targeted students and scholars via numerous formats:

- Phone
- Mail
- Online
 - PayPal/Ebay, Craigslist, Email

Phone scams seem to be most prevalent and aggressive

PHONE SCAMS



PHONE

Phone scams often target specific groups of students

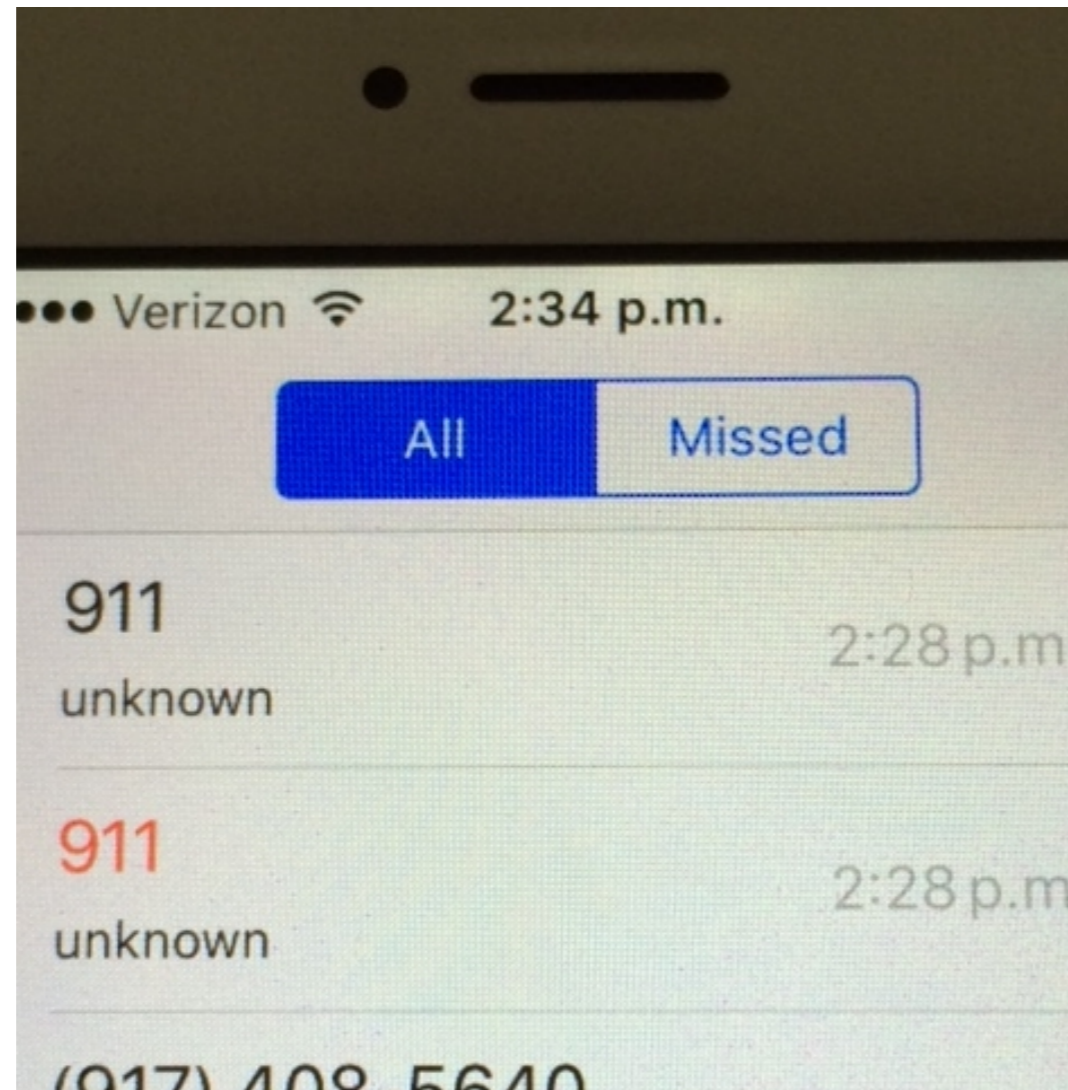
- Universities often see new students/scholars targeted in different times of varying semesters
- Chinese consulate calling
 - Chinese speakers told their passport has been stolen and told to contact Shanghai police. Then the person is accused of money laundering and other international crimes
- U.S. citizens also receive the calls but don't understand

Callers have identified themselves as officers from: local District Attorney's office, FBI, Homeland Security, Immigration, IRS, State or local police

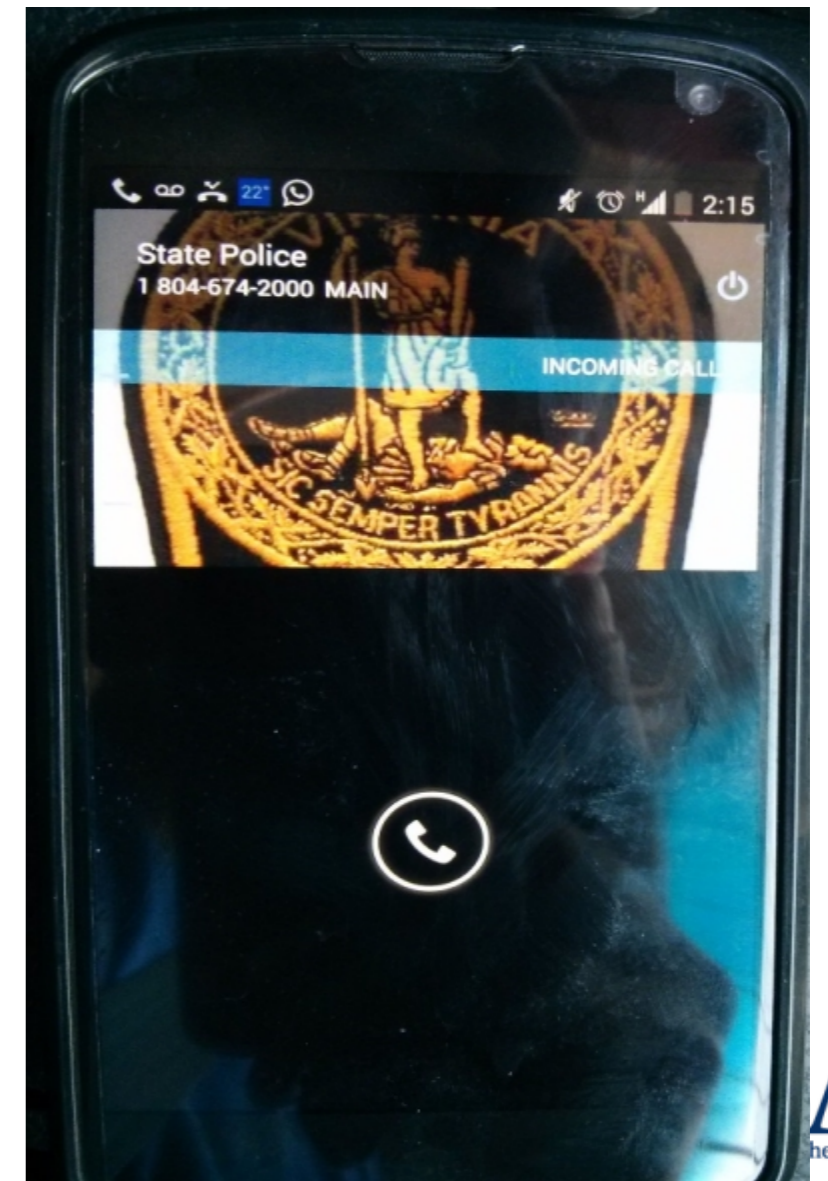
PHONE SCAMS

Recently, phone numbers appearing on caller ID are spoofing the actual agency the caller purports to be from. If student/scholar Googles or calls the number, it is a legitimate phone number.

Calls from “911” indicating student had to pay international student fee immediately or be arrested.



The number appearing in the caller ID is the number to VA state police.



PHONE

Callers are aggressive and authoritative, using key words to convince student/scholar call is legitimate, and threatening arrest and deportation if instructions are not followed.

- Students have described callers as brusque and scary, and the scammers rely on the fear they generate to convince individuals to pay immediately.

Scammers threaten to arrest student/scholar immediately if they hang up the phone or try to tell anyone about the call.

Students are told to purchase cash cards, in varying amounts, to make the payments. If the scammer successfully obtains the funds, they will often call back indicating the student/scholar owes additional money.

Scammers call individuals indicating they are from the Social Security Administration that there the SSN is suspended due to suspicious activity and there is an arrest warrant issued unless payment made to Western Union

- The SSA indicates there have been 76,000 scam calls in the past 12 months
- The SSA is not a law enforcement agency so they do not issue arrest warrants
- The SSA will never suspend SSNs according to Fraud.org
- SSA says don't trust phone's caller ID because of spoofing

International student's sister received a call that she (the international student) had been arrested and needed money for bail.

Mail Scams



Mail Scams

Letter looks like it is from IRS stating the individual should complete Form 2624 so IRS can process the tax forms and send refund

Dubious note from collection agency and student should call right away

MAIL SCAMS

Form 2624 received by student to complete the form and send to IRS.

Form **2624**
(November 2017)

Department of the Treasury - Internal Revenue Service
Consent for Third Party Contact

Go to www.irs.gov/Form2624 for the latest information.

Name(s) shown on return _____ Your social security number _____

You must use this form to authorize the IRS to contact a third party on your behalf or to revoke that authorization.

Part 1. Information Return Filed with IRS (e.g., financial institution, employment, or other payer records)

For determining an income tax liability, I authorize _____ to disclose to the IRS, for a period of three months from the date of this consent, records pertaining to any information returns filed by _____ for the taxable year _____. I understand I may revoke this consent at any time before the records are disclosed. I am mailing this consent both to the IRS and to _____.

If the payer is a financial institution, I understand a financial institution may not disclose my financial records except as permitted or required by law, a financial institution can't require this consent as a condition of doing business with it, and I may request from the financial institution a copy of a record of any disclosure the institution makes to the government.

The financial institution/employer/payer cannot be contacted on your behalf without a signed consent.

Your signature _____	Date _____	Daytime telephone number _____
Spouse's signature (if a joint account, both must sign) _____	Date _____	Daytime telephone number _____

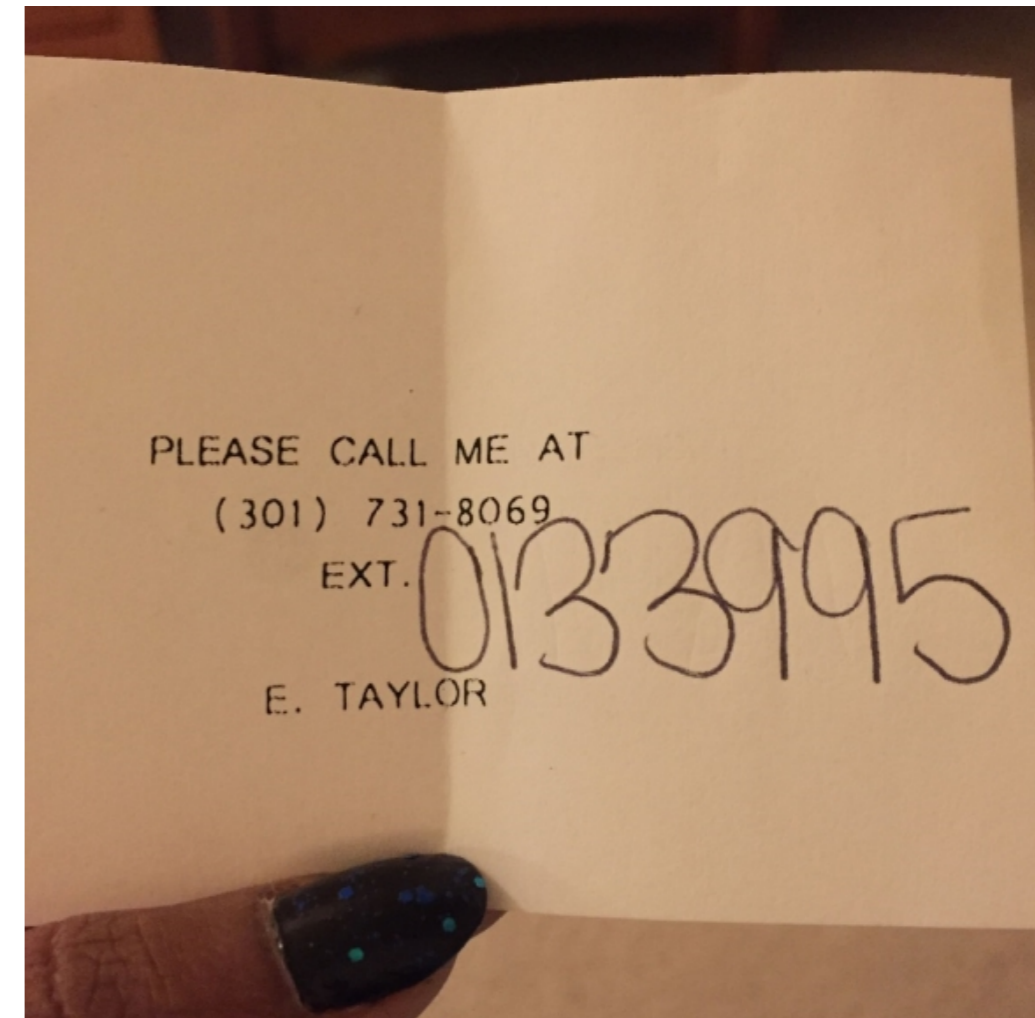
Part 2. Provide the below information to allow us to associate your consent with our records

1. Taxpayer identification number _____	2. Payer name _____	3. Account number _____
---	---------------------	-------------------------



MAIL SCAMS

Student received letter in the mail indicating to call a number. It was from someone who claimed to be from a collection agency and threatened legal action unless the student paid a fee.



Online Scams

ww ww

ww

ONLINE SCAMS

Students/scholars purchasing items on Craigslist or Ebay should also be aware of deals that are too good to be true—particularly if an item is being sold very cheaply and under normal value. Students have encountered scams when purchasing cars or renting an apartment.

- Sellers price item way below market value, and when student calls, seller indicates there is high interest and ask for immediate deposit to hold car/apartment for student. There is no car or apartment and several students have lost money this way. Students and scholars listing items for sale on similar online sites should be aware of buyers offering to pay more than the asking price, as this is often the sign of a scam.

Emails supposedly from USCIS demanding money and providing some scholar details that seem only USCIS could be sending the email.

Typical emails that all of us get to click on a link to verify university account or to extend university account access, thus providing password details. Include supposed emails from the school's bursar's office. These are phishing attempts so students should be warned early and frequently.

ONLINE SCAMS

A prominent scam occurring recently is one targeting students through social media platforms, particularly campus housing sites. Someone will create a post, or reply to an existing post, with a message about a friend looking to rent or sublease. If a student responds, the scammer will send a check for greater than the requested amount, request the difference, and the student will lose that money.

Scammers turn off commenting on the posts, so no one can warn anyone it is a scam.



ONLINE SCAMS

 **Iris WU** ▶ **university of cincinnati off campus housing**

Apr 25 · 🌐 · A friend of mine is seriously looking for a place to rent or sublease for summer, you can email her at corrinasave /@/ gmail dot com or text her phone 513 - 437 6478. Thank you!

👍 4

 **Iris WU** ▶ **College of William and Mary (W&M) Housing, Sublets & Roommates**

Apr 25 · 🌐 · A friend of mine is seriously looking for a place to rent or sublease for summer, you can email her at corrinasave /@/ gmail dot com or text her phone 513 - 437 6478. Thank you!

👍 4

 **Iris WU** ▶ **Grand Valley State University Off-Campus Housing**

Apr 8 · 🌐 · A friend of mine is seriously looking for a place to rent or sublease for summer, you can email her at corrinasave /@/ gmail dot com or text her phone 513 - 437 6478. Thank you!

👍 2

 **Jennifer Wang** ▶ **Seattle Housing, Rooms, Apartments, Roommates, Sublets, Roomster**


Apr 13 · 🌐 · A friend of mine is seriously looking for a place to rent or sublease for summer, you can email her at corrinasave /@/ gmail dot com or text her phone 513 - 437 6478. Thank you!

👍 8

 **Jennifer Wang** ▶ **San Francisco State University Off-Campus Housing**


Apr 8 · 🌐 · A friend of mine is seriously looking for a place to rent or sublease for summer, you can email her at corrinasave /@/ gmail dot com or text her phone 513 - 437 6478. Thank you!

👍 10

 **Jennifer Wang** ▶ **University of Chicago (UOFC) Housing, Sublets & Roommates**

Apr 15 · 🌐 · A friend of mine is seriously looking for a place to rent or sublease for summer, you can email her at corrinasave /@/ gmail dot com or text her phone 513 - 437 6478. Thank you!

👍 2

 **Jennifer Wang** ▶ **University of Nevada, Reno (UNR) Housing, Sublets & Roommates**

Apr 13 · 🌐 · A friend of mine is seriously looking for a place to rent or sublease for summer, you can email her at corrinasave /@/ gmail dot com or text her phone 513 - 437 6478. Thank you!

👍 5

 **Jennifer Wang** ▶ **JMU Subleasing**

Mar 18 · 🌐 · Do you have any available room or apartment to rent, share or sublease? I have a friend who is seriously looking for a place to rent or sublease asap, you can email her at corrinasave /@/ gmail dot com or text her phone 513 - 437 6478 the details about your available place. Thank you!

👍❤️ 6

How Do We Inform Our Students?

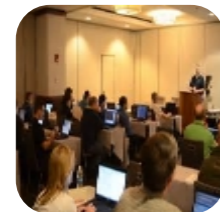
Educating students and scholars is key to prevent them from becoming victims. Our offices have developed the following resources to notify students and scholars of these issues.



Address the topic in orientations



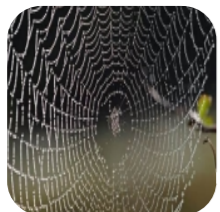
Send emails to students and scholars each semester warning/reminding them to be aware of these scams



Cover the issue in OPT workshops and presentations



Post a warning blurb on FaceBook



Create a webpage with scam information and updates



Create handouts to provide to students and scholars

The resources developed should educate students about how to recognize scams.

Inform students on common scamming themes.

- Scammers claim that students owe money or have committed some kind of fraud.
- The scammers demand immediate payment.
- Scammers have an aggressive and authoritative tone of speech and use scare tactics, threatening students with arrest and/or deportation.
- The callers are persistent and continue to call.

Warn students about scammer prototypes. Scammers generally claim to be from government agencies such as IRS, FBI, local or state police, or immigration.

Tell students that government agencies do not call students or scholars demanding immediate payment.

Advise students that although the phone numbers on caller ID may seem legitimate when Googled or called back, students should not rely on this to tell if caller is legitimate.

Inform students DHS would never send them mail asking for money.

Make it clear that students should contact ISSS immediately if they receive a suspicious phone call, email, or mail item.

While most scammers purport to be from government agencies, other scams—Craigslist, Ebay, PayPal, etc.—often work in similar ways that should be red flags for students/scholars:

- Demand immediate payment
- May threaten legal action if payment is not made

Advise students/scholars that if an offer sounds too good to be true—item being sold well beyond market value, seller willing to pay more than asking price, etc.—it is likely a scam!

How Can Students & Scholars Protect Themselves?

How Scammers Get Information

Entering on-line contests

Filling out lots of on-line surveys re: hotel stays, service, etc.

Sharing personal updates on social media

- Don't post personal info
- Narrow who can see posts
- Avoid posting rea-time updates about your whereabouts

Tossing mail without redacting personal info or shredding

Make contact information private; opt off of any campus directory. Students can usually make this request online through a student portal.

Contact ISSS immediately when receiving a suspicious or concerning call.

- Student should get the caller's name, their badge/ID number, their phone number, and tell them they will call back.

If the student/scholar has lost money due to a scam, they should contact the campus or local police department and file a report.

Register phone number with National Do Not Call Registry by calling 1-888-382-1222 or registering at <https://www.donotcall.gov/register/reg.aspx> . Report robocalls or unwanted calls.

Report any scam calls or emails FTC (1-877-382-4357) and ICE's HSI Tipline (1-866-347-2423)

Be cautious of caller ID. Scammers can mimic real numbers. Report caller ID spoofing to the Federal Communications Commission at 1-888-225-5322. Don't forget state consumer protection offices.

If the student/scholar is a victim of identity theft, they should follow federal government's recommendations: <https://www.identitytheft.gov/>

Read Citizenship and Immigration Services guidelines on how to avoid to be scammed.
<http://www.uscis.gov/avoid-scams/common-scams>

Don't give into pressure to take immediate action including notice of winning unsolicited prizes or vacation packages.

Never give personal information over the phone when you didn't make the call.

Never send money prepaid debit card or wire money if caller asks for it.

Be careful of phishing where you receive an email asking you to verify personal information

Tech Support Calling: If you didn't call for help, hang up.

IRS Calling and Threatening Arrest

- Will never call without sending several letters
- Will never ask for immediate payment and credit card information over the phone

Phone Apps to Block Robocalls

- **Robokiller**.com - \$24.99/yr. Not only blocks but keeps caller on phone.
- **Trapcall**.com – blocks
- **Nomorobo**.com – blocks callers on landline phones
- **Hiya**.com – free version (updates once a day) and subscription service (\$14.99 -updates 3x day)

Other resources already exist that you can use and/or incorporate in your materials:

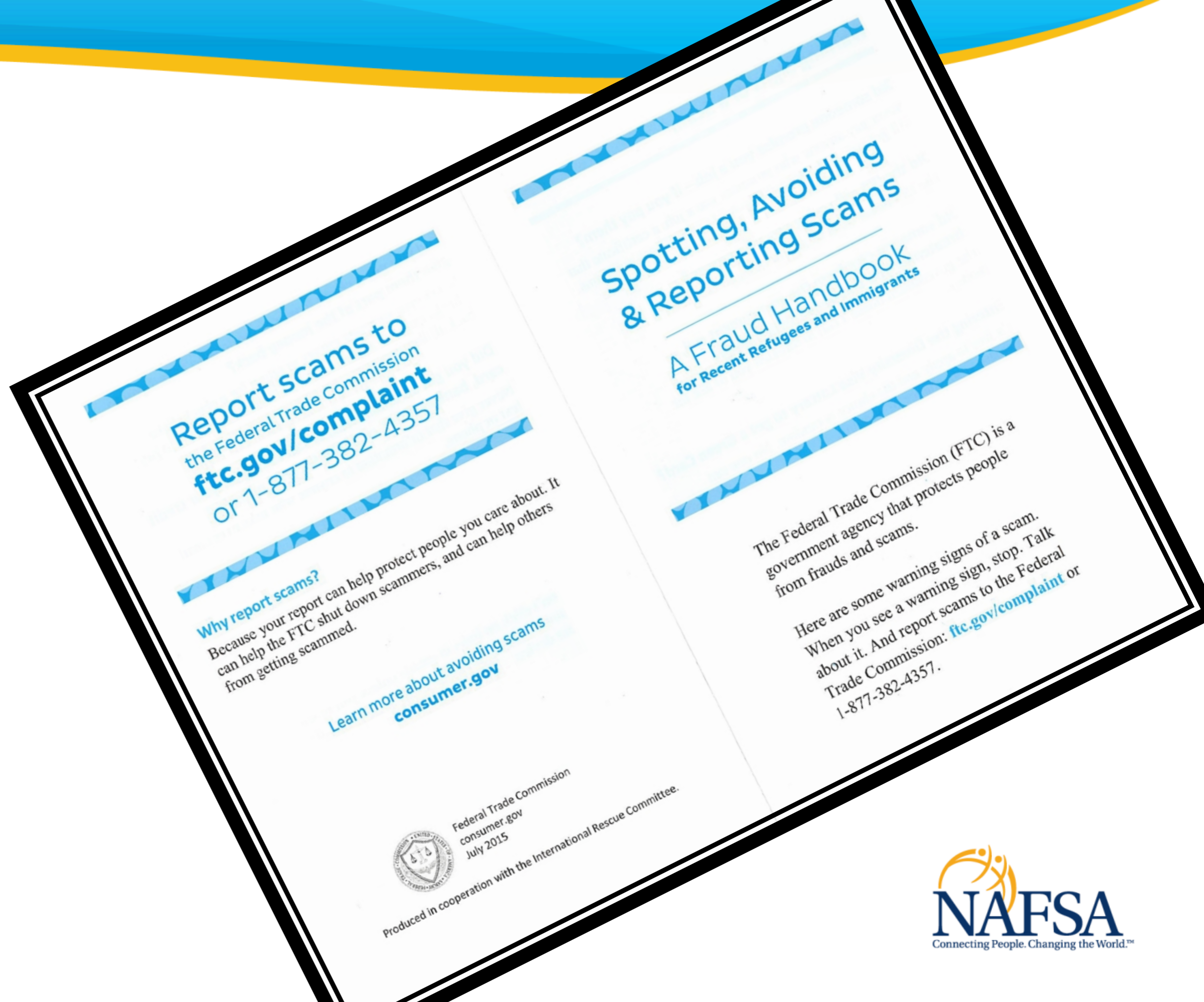
The Federal Trade Commission has several free and printable pamphlet options, including one you can customize with your logo

USCIS has a webpage devoted to avoiding common scams and a webpage with tools to avoid scams and where to report scams

SEVP has published numerous warnings and resources:
<https://studyinthestates.dhs.gov/2018/08/students-read-these-tips-to-avoid-scams>

Newspaper articles

Federal Trade Commission Brochure



Q & A

DISCUSSION

Have students and scholars on your campus been victims of other types of fraud?

What resources have you developed to help educate your international population?

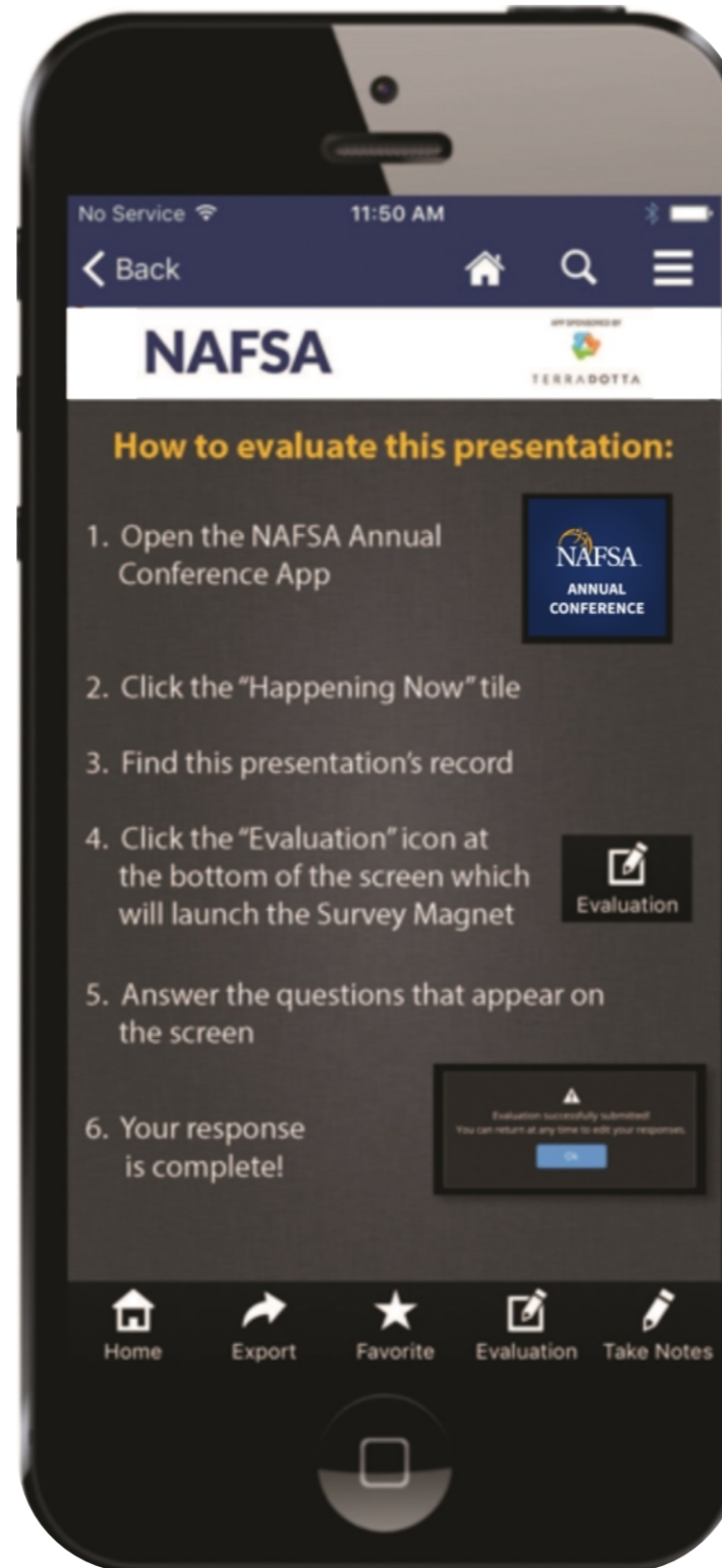


PHONE SCAMS

Partial audio of scam call purporting to be from Virginia State Police:

- **Caller:** Your account from 2009 up to 2014 and (unintelligible) on a hold of your account which is \$1,235, you know. So, for the visa (unintelligible) action, you know, against the U.S. government. For the visa, I am giving you a chance because I can't understand it. You are a student. yet I am taking a statement from you. Because your (unintelligible) is very clear. So, for the visa, sir, I am giving you a chance, right? So, I don't want to arrest you for the \$1,235. So, for the visa, sir, I am asking you, do you want to make the payment and resolve this matter outside the court or do you want to go to the courthouse for this amount?
- **Student:** So how will I make the payment?
- **Caller:** Alright, alright, so for (unintelligible) the information. Can you hold for a moment so I can transfer you to the accounting department? They're going to talk to you and they give you more information about what the government wants, and everything alright?
- **Caller:** Accounting department, for asking am I talking to, uh, (student's name)?
- **Student:** Yes.
- **Caller:** Alright, sir, I got the, uh, recording line, and I got your (unintelligible). Your amount due is \$1, 235, and you're gonna resolve this matter, am I right?
- **Student:** Can you first tell me the year for which this amount is due?
- **Caller:** That will be about your balance due of amount your education fees and that is the amount of the United States government that is due, the amount is \$1,435 which you have not paid. So, this is your cell phone number or this is your home phone number?
- **Student:** This is my cell phone number.
- **Caller:** Alright, so I'm gonna tell you one important thing sir. That would be a federal (unintelligible) recording line with my attorney and the police department. So make sure don't hang up this line because if you want to hang up this call there is a system on my computer and your arrest warrant will be issued on your name automatically. So, make sure you don't hang up this call or the recording line, ok?
- **Student:** Ok, but the thing is...but first of all how will I make the payment? I don't have, like, how do you want me...should I write you a check, is there an online place that I can go and make the payment
- **Caller:** That would be the payment procedure, which you have to follow the procedure. You have to. You are not going to make the payment through a check or through your debit card or credit card because right now there is a pre allegation on your name and (unintelligible) should be under the presumption of premium charges and we are not able to accept your debit card or a utility card. So you have to make your payment through the federal government procedure. That means you have to get the voucher card and you have to make the payment.

Please
complete this
session
evaluation
NOW!



Or FAVORITE now
and EVALUATE later!