While at Yale we hope that you will not be contacted by someone attempting to “scam” or defraud you of your money. As is true anywhere in the world, there are people who attempt to take advantage of international students and scholars, but with a little knowledge you can learn how to identify a scam and avoid falling victim to the scheme.

Understand the Threats

Common Scam Themes

- The caller ID or phone number looks like a government agency or police, and the caller may claim to be a government representative.
- A claim is made that you owe money or have committed some kind of fraud.
- A caller or letter will use fear, threats, and intimidation to get what they want.
- A scam requires immediate action.
- A scam includes punishment (often threats of deportation or arrest) for not acting immediately.
- A scammer will keep you on the phone for a long time and will not let you hang up to call back later.
- A scammer will ask for non-traditional payment methods such as gift cards.
- A scammer will use lots of legal-sounding language such as “federal regulations” and “visa fee” to sound as legitimate as possible.

Common Scams

- Third Party tax forms attempt to collect the refund that is rightfully yours.
- Rental scams where your deposit money is taken and no one meets you with the keys to move in.
- Online scams when purchasing items on Craigslist or EBay or through PayPal.
- Calls demanding an “international student tax” or “visa fee” which directs the victim to wire money or buy gift cards.
- A website charging fees to enter the Green Card Lottery.

Exercise Caution
In general, no government agency or reputable company will call or email you unexpectedly and request your personal information, or request advance fees for services in the form of wire transfers or gift cards.

- Department of Homeland Security may call you regarding your SEVIS record, but they will never ask for money over the phone.
- Verify the identity of anyone who asks for your personal information over the phone. Ask for a caller's name, ID badge, and phone number and request that you call them back or respond through the entity's customer service channels.
- Do not cash checks that arrive in the mail unexpectedly.
- Do not sign contracts without reading them and fully understanding the content.
- Avoid providing personal data, such as banking information or your social security number, to unknown persons over the phone or internet.
- Scammers may know basic information about you and use that as 'proof', however this information is likely easily searchable online. It's a good idea to check how much of your information is public, such as your phone number and address.
- If anyone pressures you to provide information or money over the phone, it's a scam and you should just hang up.

Secure Your Information

- Store your Social Security card in a secure location; avoid carrying it with you.
- Shred documents that list personal information such as your Social Security number and banking information.
- Avoid opening emails from unknown sources or clicking on suspicious hyperlinks.
- Equip your computing devices with strong anti-virus software and maintain strong passwords.
- Regularly check your credit reports for suspicious activity.

Report Anything Suspicious to OISS

- If you receive a concerning or suspicious call.
- If a letter arrives in the mail which includes threats for not acting.
- If an employer is acting unethically by requiring you to pay money to receive a job offer, or an employment agency is offering to create fake credentials.
- **Remember: when one person reports a scam, OISS can alert all of our international students and scholars.**

Resources for More Information:

- USCIS webpages on [how to avoid scams](https://www.uscis.gov/avoid-scams/common-scams) and also where to report a scam. If OISS is alerted, we will put notices on our [homepage](https://oiss.yale.edu) as well as our [Facebook](https://www.facebook.com/oiss.yale.edu) page.

Source URL: [https://oiss.yale.edu/taxes-legal/scams-fraud](https://oiss.yale.edu/taxes-legal/scams-fraud)

Links: