Scams & Fraud

Scams & Fraud **[1]**

While at Yale we hope that you will not be contacted by someone attempting to "scam [2]" or defraud [3] 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.

If you think you have been contacted by someone trying to commit fraud, please contact OISS **[4] and** Yale Police **[5] and follow the instructions under** Notify Authorities and Next Steps**.** OISS can help you determine if the situation is a scam.

Understand the Threats

Common Scam Themes

- A scammer will ask for payment via methods such as gift cards.
- Emails offering part time employment that look like they are from Yale faculty or staff, but are not. Before clicking into the link, use a second method to confirm the email is legitimate.
- The caller ID or phone number looks like a government agency or police.
- A caller, texter, 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 use lots of legal-sounding language such as "federal regulations" and "visa fee" to sound as legitimate as possible.

Common Scams

- Someone asks you to purchase gift cards on their behalf [6]. Do not buy gift cards for someone else per their request.
- 'Government officials' (scammers using the official numbers) call or text to ask for financial information or to notify that you have violated immigration laws.
- Employment offers that require you to purchase gift cards.
- 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 or emails demanding an “international student tax” or “visa fee” which directs the victim to wire money or buy gift cards.
- Calls or emails from someone who claims to be a government representative, and that you owe money or have committed some kind of fraud.
- 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.
- If someone asks you to buy a gift card for them, it may be a scam.

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 [7] 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.**

Notify Authorities and Next Steps

- If you are the victim of a scam or fraud, **contact** OISS **[4] and** Yale Police **[8] immediately**.
- You can also report this scam to the FTC [9] and the Connecticut Department of Consumer Protection [10].
- If you have received a fraudulent email via your Yale email address, follow the instructions on ITS's site to report it [11].
- If you are concerned that your information may have been stolen or exposed, use IdentityTheft.gov's free tool [12] to find out what you should do next. This will likely include running a free credit report [13] , placing a credit card freeze [14] or fraud alert [15], or obtaining credit monitoring services. Many credit cards offer credit monitoring services for free, so check your card benefits before paying for this service.

Resources for More Information:

- Federal Trade Commission [16] pamphlets in several languages.
- Federal Trade Commission's listing of common scams [17]
- USCIS webpages on how to avoid scams [18] and also where to report a scam [19].
- If OISS is alerted, we will put notices on our homepage [20] as well as our Facebook [21] page.

Links
[1] https://oiss.yale.edu/campus-community-life/for-students/safety-resources/scams-fraud [2] https://www.merriam-webster.com/dictionary/scam [3] https://www.merriam-webster.com/dictionary/defraud [4] https://oiss.yale.edu/about/connect-with-oiss [5] https://your.yale.edu/community/public-safety/yale-police-department [6] https://www.consumer.ftc.gov/articles/paying-scammers-gift-cards [7] http://www.annualcreditreport.com/ [8] http://your.yale.edu/community/public-safety/yale-police-department [9] https://reportfraud.ftc.gov/#/ [10] https://portal.ct.gov/dcp [11] https://cybersecurity.yale.edu/get-help/report/report-suspicious-email [12] https://www.identitytheft.gov/#/assistant [13] https://www.annualcreditreport.com/ [14] https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs [15] https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs#difference [16] https://www.consumer.ftc.gov/features/feature-0033-avoiding-scams-information-recent-refugees-and-immigrants [17] https://www.consumer.ftc.gov/features/feature-0030-pass-it [18] https://www.uscis.gov/avoid-scams/common-scams [19] https://www.uscis.gov/avoid-scams [20] http://oiss.yale.edu/ [21] https://www.facebook.com/oissatyale/