DPS Guidance on Scams & Fraud for University of Rochester International Students & Scholars

While at Rochester we hope that you will not be contacted by someone attempting to <u>scam</u> or <u>defraud</u> you. As is true anywhere, there are people who will 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.
- You may also receive a letter.
- The scammer may tell you that you owe money or have committed some kind of fraud.
- The scammer will use fear, threats, and intimidation to get what they want, which is access to your personal information. (credit or bank account information).
- The scammer may try to force you to take immediate action.
- A scam that may include punishment (often threats of deportation or arrest) for not acting immediately.
- A scammer will try to keep you on the phone for a long time and will not let you hang up to call back later, in order to pressure you for personal information or account numbers.
- A scammer may 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 providers attempting to collect a 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, that attempt to get credit card information 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.
- A scammer my pose as a government official (Embassy representative, consulate or police) asking for money to "take care of a problem" or to "help you get out of trouble".

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 (ICE/USCIS) or any federal agency will never call you regarding your SEVIS record and will never ask you for money or gift cards.
- Verify the identity of anyone who asks for your personal information over the phone. Ask for a caller's name, agency affiliation, ID or badge number, and phone number. Request that you call them back or respond through the agencies 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.
- Never provide personal data, such as social security number, bank account, or your address 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.
- Notify the police or Public Safety if you have any questions or think you may have been scammed.

Secure Your Information

- Store your Social Security card, Passport and important documents in a secure location; avoid carrying them 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 the International Student Office (ISO)

www.iso.rochester.edu

- 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, ISO can alert all of our international students and scholars.

Report Anything Suspicious to Department of Public Safety (DPS)

www.publicsafety.rochester.edu

• Public Safety is in regular contact with the International Students Office and can be a resource to help navigate questions you may have.