Global Education Office (GEO)
2120 Mesa Vista Hall
MSC06 3850 1 University of New Mexico
Albuquerque, NM 87131-0001
Phone (505) 277-4032 ♦ Fax (505) 277-1867
Email: iadvisor@unm.edu Web: https://isss.unm.edu/

DON'T GET SCAMMED!!! CYBERCRIMES AND IDENTITY THEFT

COMMON CYBERCRIMES AND TELEPHONE SCAMS TARGETED AT INTERNATIONALS

1. **Phishing:**
   - E-mails disguised as legitimate organizations requesting personal information and threatening to terminate your account or do something negative unless you respond by clicking on their link.
   - E-mails that offer you big riches if you provide your account information.
   - E-mails requesting confirmation of your payment details for an order you may (or may have not) placed.

Be very suspicious of these e-mails, as phishing scammers are clever and often use the exact logos of companies with which you may do business, such as a major retailer or financial institution. Never click through a link on any e-mail unless you personally know the sender.

2. **IRS refund, debt owed, or threat to report you to immigration authorities:**
   - You receive an e-mail telling you that the IRS (tax agency of the US government) has a refund for you. All you have to do is click through the e-mail and provide your bank account information.
   - You receive a telephone call from a person claiming to be working for the government. The caller threatens to deport you or report to immigration authorities unless you wire money immediately.

Be aware that the IRS or other government agency will never contact you via email or telephone. If they need to reach you, they will send a letter to your home address. You can always ask to meet in person and see ID.

3. **Lottery scam:**
   - E-mail, letter or check telling you that you have won a lottery-even if you didn't buy a ticket. To collect the reward, you must provide your bank account number to deposit the funds.

4. **Calls to "confirm" your personal information:**
   - A legitimate bank will never call and ask you for your full account numbers or to confirm your PIN number. The consumer is the party that initiates contact.
   - To ensure legitimacy of the call, hang up and call the bank directly. This way, you initiated the contact.

5. **Fake jury duty:**
   - Phone call to inform you that you missed jury duty and he or she needs to confirm your personal information. Only US citizens are eligible to serve on a jury.

6. **Medical identity theft:**
   - Telephone call or email claiming to be calling from your doctors' office or health insurance. Typically asking for personal information such as dates of birth and social security numbers.
   - Do not share your medical history over email or telephone. Do it in person and only with people who need this information to provide you medical services.
   - When you go to the doctor, make sure records are kept in a secure area.
   - Don't provide your Social Security number unless there is a good reason to do so.
   - Be sure your insurance ID does not have a Social Security number on it.

IDENTITY THEFT

1. Definition: Identity theft happens when someone steals your personal information and uses it without your permission.
   - This is a serious crime that can wreak havoc with your finances, credit history, and reputation — and can take time, money, and patience to resolve.

- It is almost always committed to facilitate other crimes, such as credit card fraud.
- Personal identifying information such as name, date of birth, social security number, and bank account numbers are extremely valuable to identity thieves.

2. Signs of possible identity theft:
   - Withdrawals/missing funds from your bank account that you can't explain.
   - You don't get your bills or other mail, or you get mail in someone else's name.
   - Merchants refuse your checks or your request for credit is declined.
   - Debt collectors call you about debts that aren't yours.
   - You find unfamiliar accounts or charges on your credit report.
   - Medical providers bill you for services you didn't use.
   - Your health plan rejects your legitimate medical claim because the records show you've reached your benefits limit.
   - A health plan won't cover you because your medical records show a condition you don't have.
   - The IRS notifies you that more than one tax return was filed in your name, or that you have income from an employer you don't work for.
   - You get notice that your information was compromised by a data breach at a company where you do business or have an account.
   - You are the victim of a robbery or burglary.

RESOURCES

1. If your credit has been stolen, place an initial fraud alert with the three credit bureaus:

Equifax www.equifax.com 1-800-525-6285	Experian www.experian.com 1-888-397-3742	TransUnion www.transunion.com 1-800-680-7289

2. After placing the initial fraud alert, you are entitled to a free credit report from each of the three credit reporting companies. Carefully review it and dispute unauthorized purchases.

3. Create an identity theft report listing all the unauthorized purchases or accounts created in your name. Keep track of all the steps you have taken in response to the identity theft. This identity theft report will help you deal with credit reporting companies, debt collectors, and businesses that gave the identity thief credit or opened new accounts in your name. The report may also help you get fraudulent info removed from your credit report.

4. File a police report about the identity theft and get a copy of the police report or the report number.

HOW TO KEEP YOUR PERSONAL INFORMATION SECURE

1. Do not overshare your information. Do not provide your personal information just because it is requested by employers, vendors or medical provides. Always ask, "Why do you need this information?"
2. Store your personal information securely, especially your social security number. Never carry your social security card in your wallet or purse.
3. Maintain appropriate security on your computers and other electronic devices.
4. Properly dispose of personal info.
5. Limit what you carry.
6. Opt-out of prescreened offers of credit and insurance by mail. You can opt out for 5 years or permanently. Call 1-888-567-8688 or optoutprescreen.com.
7. **Try not to enter private information on a public computer or network. If you have to use a public computer, make sure to delete browsing, search, and download history before you log out.**