

From: apb-l-bounces@announce.ucsd.edu
To: apb-l@ucsd.edu
Subject: [APB-L] UC San Diego PD Community Alert Bulletin
Date: September 24, 2019 4:25:04 PM

UC SAN DIEGO POLICE DEPARTMENT

September 24, 2019

ALL ACADEMICS, STAFF AND STUDENTS AT UC SAN DIEGO

SUBJECT: Community Alert Bulletin – Theft by false pretenses (Phone Scams)

The UC San Diego Police Department would like to warn all community members of telephone and tuition scams targeting specific members of our community. Since July, victims have told us they collectively have lost over \$212,000 to suspects, who called the victims claiming they were with law enforcement in their home country. The suspects threatened the victims with detention if they did not provide the funds requested.

The following is information about scams we are seeing and/or have seen in the recent past:

Extortion Scams:

Phone scams that threaten individuals with an arrest, if they fail to meet the scammer's demands. This may include threats of arrests of international students from police in their country of origin. The phone call usually starts with a person identifying themselves as an IRS employee or police officer claiming to have an open case involving the victim in criminal activity or claiming that the victim's social security number has been used for illegal activity.

The caller then:

- Threatens the victim with an arrest and imprisonment, or future visa denial.
- Asks the victim:
 1. For their date of birth and social security number to check if they have been a victim of identity theft, "confirms" that the victim's identity has been stolen and then advises the victim to secure their funds by withdrawing their money, converting it to Bitcoin and sending it to the caller, or
 2. To purchase several gift cards (e.g., GameStop, Home Depot, etc.) and provide the serial numbers via text, or
 3. Demands the victim wire transfer funds to banks overseas as a way of proving their innocence.

General safety tips with regards to telephone scams:

- The IRS and police will NEVER ask for any form of payment, including gift cards, to avoid an arrest.
- If you are an international student, confirm any communications with your government by calling your local consulate.
- Always be suspicious of phone calls from unknown individuals or phone numbers that you do not recognize. Recognize that legitimate telephone numbers can be 'spoofed'. If in doubt, you can look up the real phone numbers and call these numbers back yourself.
- Do not conduct business over the phone with callers you do not know.
- Never share personal or financial information over the phone with someone you do not know, e.g., social security number, debit/credit/pre-paid card numbers, etc.
- If anyone contacts you and asks you to pay or send them money using Bitcoin, wire transfer, or pre-paid cards of any sort, this is probably a scam.
- If anyone calls asking for payment due to your involvement in a criminal case, hang up the phone and call your local police department.
- If you cannot verify the caller's identity, feel unsafe, or suspect criminal activity, call the UC San Diego Police Department: Non-emergency help line, (858) 534-4357.

Tuition Payment Scams:

Online scams which target college students by promising a reduction in tuition if a third-party service is used to pay their fees. Students attending institutions across the United States, including UC San Diego, have been impacted by these online tuition scams. International students have been targeted more frequently, and scammers have especially targeted students using the popular app, WeChat. Typically, scammers often promise an approximate 5% discount in tuition and requests victims transfer the scammer the reduced tuition funds. The scammers then request the victim's university credentials and attempt to pay their tuition with fraudulent or stolen credit card information. This buys the scammers time to withdraw the victim's funds because it may take several days before the credit card companies receive information that the credit card used was fraudulent or stolen. The victim then loses the funds they transferred to the scammer and still must pay their own tuition.

General safety tips regarding tuition scams:

- Never share your online credentials with anyone.
- Only use payment methods approved by UC San Diego.
- Do not to respond to third-party solicitations.
- Contact Student Financial Solutions (<https://sfs.ucsd.edu/>) if you have questions about a potential tuition discount, or an alternative form of payment that is not included on the list of ways to pay your bill.