California State University, Northridge
Department of Police Services

CAMPUS CRIME TREND ALERT

The California State University, Northridge Department of Police Services is providing this notice of a campus crime trend in order to provide information that may help in avoiding similar crimes or provide information that may assist in solving these crimes, leading to an arrest and/or recovery of the stolen property.

EMERGENCY CONTACTS

24-hour Emergency
9-1-1

From a cell phone
9-1-1

Emergency "BLUE LIGHT" phones and yellow TTY emergency call boxes (connected to CSUN Police)

Report suspicious persons or circumstance anonymously
"We Tip Hotline" – (818) 677-TIPS (8477)

Visit us on the web:
www.csun.edu/police

07/17/2020

EMAIL PHISHING SCAMS

DATE/TIME: Monday July 13, 2020 10:54am and Wednesday July 15, 2020 6:18pm.

Two (2) victims were contacted via email regarding job opportunities for a Covid-19 Student Empowerment Program or teleworking position to stop the pandemic. The emails came from what appeared to be that of a faculty member. Both were directed to a website for Dr. Isabella Campos to enter their personal information which they did. After being accepted for the positions, electronic checks were sent to both victims to be printed and deposited in their accounts. They were then directed to withdraw cash and distribute the money via different cash apps, for which they would be able to keep some of the money for themselves. Later they learned neither check cleared and were responsible for the money withdrawn and returned (i.e., bounced) check fees.

Tips to Avoid Phishing Scams:

- To confirm if a job offer email is legitimate and was truly sent by a staff or faculty member, use the CSUN campus directory to independently verify and contact and speak with that person via their CSUN office extension before responding to the original email.
- Red flags of fraudulent email scams include the request for checks or funds to be deposited in your personal bank account and later distributed via money transfer apps/electronic or physical gift cards.
- Please **BEWARE!!!** If it seems too good to be true it probably is.
- Social Media is the main way a phisher obtains information about you and tailors their e-mails to your interests. Limit personal information you provide in your posts (school, location, full name, etc.), even if you're on private; not everyone who follows you is trustworthy.
- Think carefully before clicking on a link or image. Phishing and other malware scams rely on our habit of click first, think later.

For additional tips and to see samples of phishing scams visit the CSUN Information Technology website at
https://www.csun.edu/it/avoid-fraud-email
or by phone at 818-677-6100