CECS 378 Semester Project

Social Engineering: ID Card Duplication

Group 6

Social Engineering

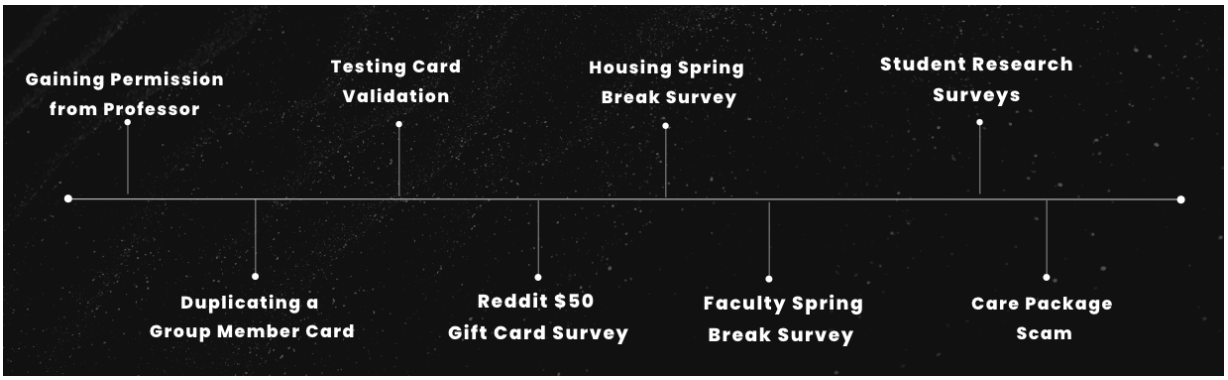
Professor Louis Uuh

Han Pham	026502812
Denise Martinez	025892631
Victoria Macali	026340182
Brenden Smith	026245997
Corbin Marino	025865448
Justin Wagers	025403155
Shane Khan	027283956

Introduction

The mission behind our Semester Project project is to essentially use social engineering to collect credentials and duplicate ID cards in order to get access to private information, beachbucks and/or locations. Social engineering is defined as the use of deception to manipulate individuals into divulging confidential or personal information for fraudulent purposes/criminal activities. The goal of the project was to successfully duplicate into a physical card, collect information and test the duplicated ID cards, and lastly attempt to gain access into user-restricted areas.

The general timeline should go as follows: gaining permissions, purchasing our MSR reader/writer device, read/writing into a blank ID card, testing card validation, revising ID card prototypes, creating mass surveys, and lasting retesting of our ID cards with the information we collected. For February (iteration 1), we focused on gathering the appropriate MSR reader/writer devices, multiple kinds of ID cards, and learning how to use the MSR device by attempting to duplicate cards with our own ID numbers. For early March (iteration 2), we focused on testing whether the duplicated ID cards can get access to restricted areas and how to improve our duplicated ID cards. For mid March to April (iteration 3), our team focused on creating multiple surveys (reddit, housing, email poof, care package, and student research surveys), demonstrating a demo of a duplicated ID card in use, and finishing the paper and presentation.

Visual of the timeline


The roles of the project are detailed in the table below.

Project Roles	
Name	**Tasks**
Shane Khan	● Launched a Qualtrics Survey about student cyber safety on Discord, and gathered around x # of Student ID's. ● Created a Discord server, where meetings/notes were taken. ● At times, try to make meetings to work on projects.
Corbin Marino	● Used a command line email spoof trick to send to a small pool of professors a survey to collect their faculty id numbers. ● This involved configuring a lazy script and an smtp server in order to get a full email address spoof.
Justin Wagers	● Launched a Qualtric Survey on Reddit, where an anonymous survey was posted. Upon completion of the survey along with a voluntary request for student ID, would be put in a raffle for a $50 dollar gift card from Amazon. ● Researched and experimented with the card reader, by swiping and inserting in different machines around campus that used "Beach Bucks". ● Found Appropriate Supplies for Project such as, Card Reader, ID

	cards, etc.
Victoria Macali	● Found Appropriate Supplies for Project such as, Card Reader, ID cards, etc. ● Created flyers with QR codes and posted them around the housing area of CSULB to gather Student ID's. ● Experimented with loading information onto Blank Cards, Guest Campus ID Cards and Rewriting on Student Campus IDs.
Han Pham	● Coordinated a Program Schedule ● Found Appropriate Supplies for Project such as, Card Reader, ID cards, etc. ● Oversaw the whole development of this project, including weekly checks in times. ● Posing as survey takers on campus to collect student id numbers.
Denise Martinez	● Launched a Qualtric Survey, consisting of a random Student Survey and gathered 2 amounts of student ID's in the process. ● Assisted in posting flyers around Parkside and Hillside housing for the Housing Survey
Brenden Smith	● Contributed technical explanations for some of the concepts to the write-up and presentation. ● Assisted with survey creation and deployment. ● Edited and published the presentation video

<u>Iteration 1:</u> ***Purchased MSR Reader/Writer Device, duplicating ID cards, testing on BeachBucks Machine***

March 15, 2022

After analyzing multiple Student IDs we discovered that cards Issued in 2019 have track 2 and 3 information. While cards Issued in 2022 have only track 2 information. Track 2 is the space where information is stored for chip and/or magnetic strip. Track 3 is known to be unused in the scope of RFID Cards and the information stored on Track 3 might not even be physically present on the card itself. After reading this information we came to the conclusion that Track 3 is not needed to duplicate student ID/ faculty ID cards in order to successfully gain access to swipe based events.

When swiping cards we noticed a very clear pattern. The Track 2 information stored on every CSULB Student ID Card is a 15-digit number, with the first 9 digits being every person's unique Student ID number. Following the SID combination is the 6 digit sequence of 84500* (with * representing an ever changing digit for all SIDs). With only having the knowledge of two Student ID numbers, we were able to brute force the ending digit for two cases of Student IDs.

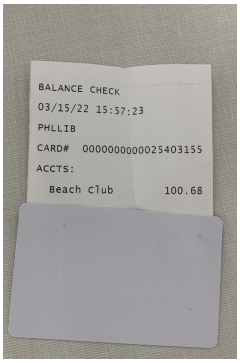
Name	**ID Number**	**Ending Sequence**
E****** ******	026588859	845002
A***** *****	029121701	845001

The same process was used for brute forcing Professor Uhh's Campus ID

L**** ***	006720049	845001

We first tested the cards against a campus card reader. On the first floor of the University Library we tested reading SID against BeachBucks balance machines and Printing Service Computers. From here we were able to gather if the card was valid and see the potential spending limit per student. From here we were able to copy Justin’s Student ID Card in order to access his CSULB Campus Currency - BeachBucks.

Name	**Student ID**	**Ending Sequence**
J***** ******	025403155	845001

Receipt of justin's beachbuck accounts


BeachBucks Machine Spoof Concept

After our team discovered that the fake student identification card had the ability to read off a student's BeachBucks balance from the BeachBucks balance machine, we came up with the idea to attempt to access that data remotely, without the need to use the machine. However, we did not end up completing this idea because of some obstacles we encountered.

- We deduced that the API is hosted and provided by Blackboard. Even if we were able to trace the API endpoints, there is a very high chance that since Blackboard is a reputable company. The company took basic security precautions to lock down their API from unauthorized use. If this was the case, we would have to pretend to be the BeachBucks machine to get any useful information.
- To the best of our knowledge from the class, it could be possible to conduct a man in the middle attack to intercept data from the BeachBucks machine. However, we would have to be on the same network as the machine. On top of this, it would only allow us to intercept data, not to make our own requests independent of the host machine.

<u>Iteration 2:</u> Testing access into restricted facilities with duplicate ID cards, improving our ID cards by implementing blank cards with Chips

March 16, 2022 - April 16, 2022

The discovery of successful SID duplication sparked the idea of copying a SID card in order to gain access to a housing building. We tried many attempts to try to gain access to the CSULB Beachside Atlantic Housing Facility. (Note: The Beachside Housing Card Reads use RFID Tap Technology)

V******* ******	026340182	845004

Attempt #1

- Copy Victoria's SID onto a blank card
- Result : The Track 2 information stored on the card is not picked up by the RFID Reader.

Attempt #2

- Copy Victoria's SID onto a blank card with a Chip with hopes of a stronger connection.
- Result: The Track 2 information stored on the card is not picked up by the RFID Reader.

Attempt #3

- Copy Victoria's SID onto CSULB Issued Guest Card

Blank Bookstore giftcard	999709250845000

- Result: The Track 2 information stored on the card is not picked up by the RFID Reader.

Attempt #4

- Copy Victoria's SID onto CSULB Issued Student ID Card, Replaced Current Student Information with Victoria's sequence.

- Result: The Track 2 information stored on the card is not picked up by the RFID Reader.

Attempt #5

- Use RFID reader to see what information is being processed during the “tap” process.

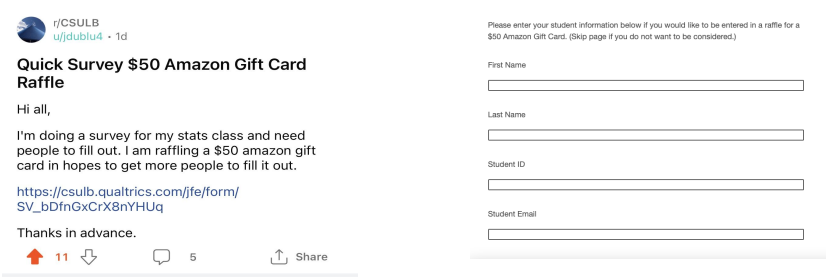
We attempted to gain access by purchasing a new set of RFID chip cards which we hypothesized would hold a stronger magnetic connection. In the end we realized that this was not the case, it was not that the RFID signal was not strong enough, rather that the information being read was not coinciding with the information stored on the Housing Database. It was as if we were not placing anything near the reader, the information was not being processed since there was no coexisting match. However we do not believe that our duplication technique failed, as all swiping related events which used a magnetic strip would work perform as expected.

<u>Iteration 3:</u> Collecting credentials and private information from various surveys, providing demo of duplicated ID card in use

Reddit Survey

In an attempt to gather more student ID numbers to clone onto ID cards, a Qualtrics survey was launched and posted to r/CSULB with a request for their student information along with random questions. In 24 hours, 81 surveys were collected. Of the 81 surveys collected, 65 student IDs were obtained. After testing some of the ID numbers at random, they followed the same ending sequence as the previous IDs tested (84500X).

Reddit Survey and Results

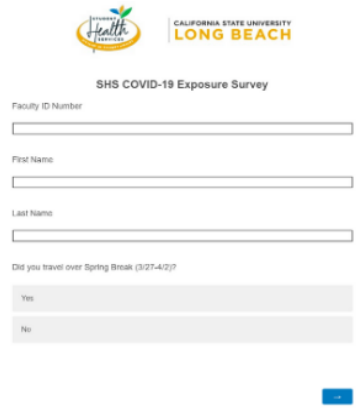
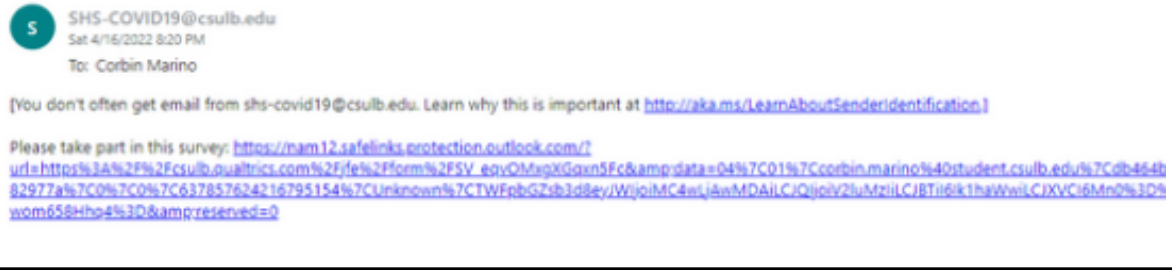


IPAddress	Q9	Q8	Q7	Q6	Q13
IP Address	First Name	Last Name	Student ID	Student Email	How long is your commute to campus?
{"importId":"ipAddress"}	{"importId":"QID9_TEXT"}	{"importId":"QID8_TEXT"}	{"importId":"QID7_TEXT"}	{"importId":"QID6_TEXT"}	{"importId":"QID13"}
108.185.6.75	Soo	Ahn	29452174	Soo.ahn01@student.csulb.edu	15-30 minutes
47.147.141.247	Chanrocharta	Thon	28072874	Chanrocharta.Thon01@student.csulb.edu	15-30 minutes
47.147.148.88	Monik	Patel	29343481	Monikkishor.patel01@student.csulb.edu	Under 15 minutes
172.58.19.156	David	Lopez		davidlopez1.1997@gmail.com	15-30 minutes
75.84.116.188	Sabrina	Bobadilla	28334720	SabrinaBobadilla01@student.Csulb.edu	30 minutes - 1 hour
68.126.222.120	Kelly	Ajiatac	25858862	kelly.ajiatac@student.csulb.edu	30 minutes - 1 hour
99.8.3.54	Arely	Barrettos	27272859	arely.barrettos@student.csulb.edu	30 minutes - 1 hour
47.152.124.115	Sheila	Hayati	26893990	sheila.hayati@student.csulb.edu	I live on campus
172.56.16.210	Katherine	Chang	27692949	katherine.chang@student.csulb.edu	30 minutes - 1 hour
104.28.50.178					15-30 minutes
172.58.20.48	Yennyfer	Zelaya	27888677	Yennyfer.Zelaya@student.CSULB.edu	Over 1 hour
47.146.240.177	Jocelyn	Magana	28362358	jocelyn.magana01@student.csulb.edu	I live on campus
174.81.8.182	Richard	Huang	17849869	richard.huang@student.csulb.edu	15-30 minutes
172.114.45.82	Edith	Magana	26315716	Edith.magana@student.csulb.edu	15-30 minutes
45.51.63.68	Daisy	Tapia	26514746	daisy.tapia@student.csulb.edu	30 minutes - 1 hour
134.139.201.183	Raymond	Trieu	18521283	Raymond.trieu@student.Csulb.edu	30 minutes - 1 hour
76.166.144.34	Allan	Hernandez	29264763	Allan.hernandez02@student.csulb.edu	30 minutes - 1 hour
134.139.201.194	David	Tran	28678011	David.tran10@student.csulb.edu	I live on campus
107.185.75.213	Ilene	Ortiz	28671459	Ilene.ortiz01@student.csulb.edu	Over 1 hour
134.139.201.137	Jaden	Anzuetto	27510052	jaden.anzuetto@student.csulb.edu	Over 1 hour
45.50.31.54	Niamh	Velosso	30303856	niamh.velosso01@student.csulb.edu	I live on campus
174.193.132.176	Audrey	Arias	27505892	audrey.arias@student.csulb.edu	15-30 minutes
47.157.247.172	vesena	le	26855641	vesena.le@student.csulb.edu	15-30 minutes
47.149.201.122	Savannah	McCorkle	26997020	savannah.mccorkle@student.CSULB.edu	Under 15 minutes
47.147.129.52	Jessica	Quang	26201589	jessica.Quang@student.csulb.edu	Under 15 minutes
76.89.183.39	John Dave	Flores	18421453	johndave.flores@student.csulb.edu	30 minutes - 1 hour
99.66.231.163	Sofia	Uribe	28964544	sofia.uribe01@student.csulb.edu	15-30 minutes
73.118.246.161	Khloe	Johnson	25373812	Khloe.johnson@student.csulb.edu	Under 15 minutes
71.9.6.185	Stephanie	Nguyen	25595321	Stephanie.nguyen08@student.csulb.edu	15-30 minutes
172.90.185.50	Itzel	Contreras	13865941	Itzel.contreras@student.csulb.edu	30 minutes - 1 hour
24.205.44.196	Graciela	Guerrero	18788040	Graciela.guerrero@student.csulb.edu	30 minutes - 1 hour
172.114.149.65	Ruben	Gaona	16883475	Ruben.Gaona@student.csulb.edu	30 minutes - 1 hour
23.242.61.144	Christie	Vo	27501940	christie.vo@student.csulb.edu	15-30 minutes
71.93.208.119	Alejandro	Gonzalez	26168803	alejandro.gonzalez02@student.csulb.edu	Under 15 minutes
138.229.202.128	Ellie	Sasalusikul	25083634	ellie.sasalusikul@student.CSULB.edu	15-30 minutes
47.151.13.191	Ryan	Hoang	17680115	Ryan.Hoang@student.csulb.edu	15-30 minutes
45.48.158.107	Brandon	Nguyen	16707026	Brandon.Nguyen13@student.csulb.edu	30 minutes - 1 hour
162.204.120.130	Andy	Nguyen	26497677	Andy.Nguyen13@student.csulb.edu	15-30 minutes
172.58.17.15	Audrey	Romero Castellanos	26946216	Audrey.romerocastellanos@student.csulb.edu	Under 15 minutes
47.156.205.57	Matthew	Johnson	15850144	Matthew.johnson02@student.csulb.edu	15-30 minutes
134.139.201.48	Alais	Ashcraft	28584417	Alais.Ashcraft01@student.csulb.edu	I live on campus
70.93.132.177	Ashley	Abrego	16648784	Ashley.abrego@student.csulb.edu	15-30 minutes
45.48.153.186	Dylan	Sakamoto	17143709	dylan.sakamoto@student.csulb.edu	15-30 minutes
172.226.7.19	Ikem	Anyanwu	28005768	Ikem.anyanwu01@student.csulb.edu	15-30 minutes
150.195.38.185	taeawn	huyck		thuyck@gmail.com	Under 15 minutes
174.195.132.91	Moises	Rivera	25637207	moises.rivera01@student.csulb.edu	15-30 minutes
107.127.21.64	Chinar	Pusalkar	17950811	chinar.pusalkar@student.csulb.edu	15-30 minutes
47.148.76.99					30 minutes - 1 hour
45.51.53.226	Nguyen	Van	25909056	nguyen.van@student.csulb.edu	30 minutes - 1 hour
47.147.137.74	Darshan Umesh	Elibote	29320757	darshan.elibote01@student.csulb.edu	Under 15 minutes
23.243.196.45	LeAnh	Ly			
23.243.196.45	LeAnh	Ly	28667338	leanh.ly01@student.csulb.edu	15-30 minutes
172.58.22.212	Sahar	Soltani	26445001	Sahar.soltani@student.csulb.edu	30 minutes - 1 hour
73.71.226.216	Amos	Ryan		janettingalianh@gmail.com	15-30 minutes
76.20.78.82	Ivory	Riggin		ajohnlariohymanlang@gmail.com	30 minutes - 1 hour
97.93.102.11	Bennett	Bualeridge		thomassteleinjenem@gmail.com	15-30 minutes
23.240.7.135	Caitlin	Galias	29088252	Caitlin.Galias01@student.csulb.edu	30 minutes - 1 hour
107.77.229.18					15-30 minutes
172.58.21.193	Michael	George			30 minutes - 1 hour
134.139.201.146	Yesenia	Cota	27697824	yesenia.cota01@student.csulb.edu	30 minutes - 1 hour
107.77.231.183					I live on campus
107.77.231.183	Christian	Balasoro	26529475	christian.balasoro@student.csulb.edu	I live on campus
71.149.146.140					Under 15 minutes
172.58.20.233	Adrian	Diaz	8898693	adrian.diaz01@student.csulb.edu	15-30 minutes
47.149.213.242	Roxana	Moreno	28599075	Roxana.moreno01@student.csulb.edu	15-30 minutes
134.139.201.154	Sandra	Duong	28120272	sandra.duong01@student.csulb.edu	I live on campus
98.147.150.65	Tammy	Nguyen	17826131	tammy.nguyen@student.csulb.edu	15-30 minutes
104.32.107.1	Alexa	Banos	26670499	alexabanos@gmail.com	Over 1 hour
23.243.105.100	Jenny	Truong	26588872	Jenny.Truong@student.csulb.edu	15-30 minutes
172.58.23.92	Jonathan	Dhauw	29376449	Jonathan.dhauw01@student.CSULB.edu	15-30 minutes
134.139.201.162	Kay	Kim	27032666	ahjung0101@gmail.com	I live on campus
12.89.24.194	Flavio	Avila	25469442	flavio.avilamota@student.csulb.edu	30 minutes - 1 hour
172.58.27.47	Shadman	Zahir	25405651	Shadman.Zahir@student.csulb.edu	15-30 minutes
45.27.24.61	Haley	Nikcevich	29532059	haleynikcevich@gmail.com	30 minutes - 1 hour
47.155.160.120	Julie	Belousow	26670590	julie.belousow@student.csulb.edu	15-30 minutes
134.139.201.149	Amanda	Phong	28987437	Amanda.phong01@student.csulb.edu	15-30 minutes

Email Spoofing Survey

We attempted to get faculty ID numbers by sending a Qualtrics survey under the disguise of the SHS-COVID19@csulb.edu email. We randomly selected many faculty from gathering emails that were publicly available on the csulb website. This survey was a post spring break survey that involved the user to input their ID number, name, and check yes or no on whether they traveled over spring break.

We used an open source project on github called lazy script and the kali linux terminal in order to perform the spoof of the email. A smtp server was set up using smtp2go.com in order to actually fake the SHS-COVID19 email. Unfortunately, no recipient of the email fell for the email and took the survey. During testing of this process the emails went directly to inbox and did not get flagged as junk, however we may think the security system picked up on this after many emails were sent out and there is a possibility that some went to recipients' junk folder.

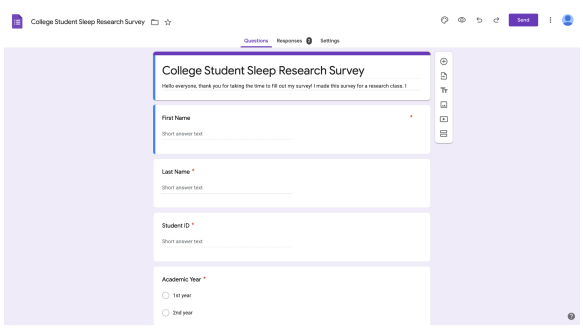
Email Spoofing Images



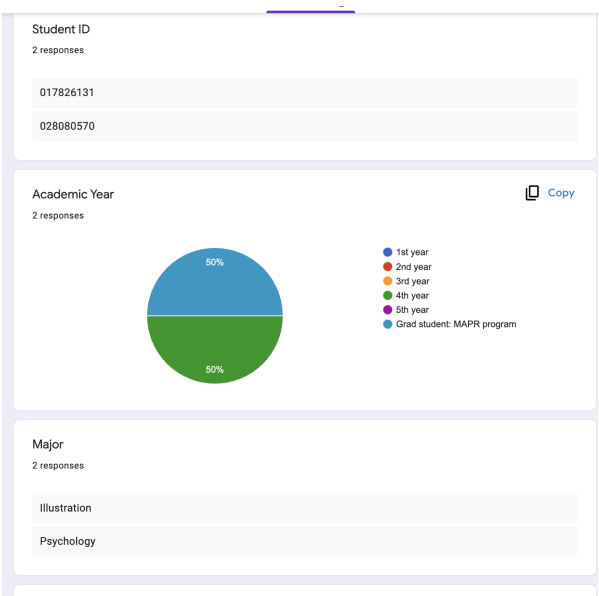
Student Research Survey

Another way of gathering student IDs is through posing as a research student. It is common to receive an email from research students asking for you to participate within their research. Posing as research students brings a realistic situation, therefore this position holds a certain level of automatic trust from a victim. This is a form of social engineering where we trick the user into thinking we are a trustworthy source.

This survey was deployed through Reddit to take advantage of being anonymous. The results were not as much as we anticipated since we only got two responses. On the other hand this approach was still beneficial since we managed to collect the full name, academic year, and student ID of those respondents.

Student Research Survey Images

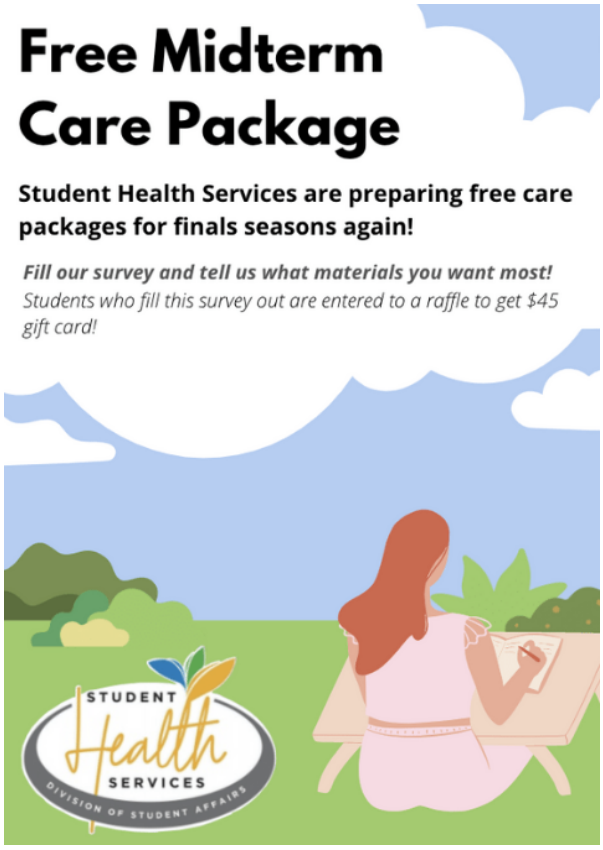




Care Package Survey

Another survey we created was a care package survey. This survey is based on a previous survey we have seen on campus. During March, the Student Health Services were giving away essentials for students to aid them for the midterm season. Items such as scantrons, chips, bars, pens, pencils, coffee, and even personal hygiene items (i.e. soap. pads, tampons) were provided. The Student Health Services found what items students wanted by collecting information during the Week of Welcome and the Cultural Week of Welcome.

Inspired by this care package event, we also created a survey where we could ask what items students wanted for finals season. In addition to asking what items students wanted, we also collected emails, names, and ID numbers. The incentive of the survey is that those who filled it out got entered in a raffle to win a $45 gift card. The survey was posted on Reddit and got no results.

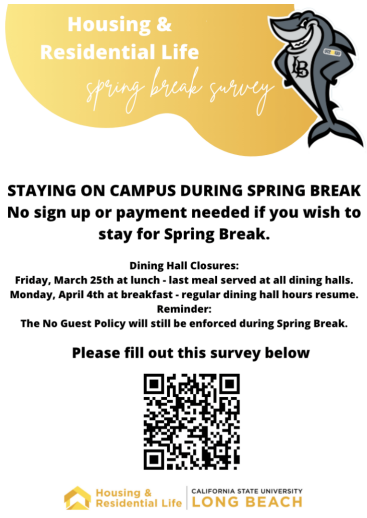
Care Package Survey	

Housing Survey

The week prior to Spring Break we plastered the posters all around the Campus Housing Buildings. During this time we tried to find vulnerabilities within the housing key readers. Through this we were able to gain access to the Parkside North Rooftop with a non-Parkside resident ID. A second event was using a Parkside ID card to enter the Beachside Parking Lot. After further research we uncovered that there is an extra layer of encryption for those who live in housing, and only one card can be activated at a given time to provide access. Which prevented us from successfully making a duplicate card without the knowledge of the primary card holder.

In keeping with the theme of Social Engineering, confidence is key. After placing our posters nearby bulletin boards, after a day our posters were placed inside of the bulletin boards and moved around for more optimal viewing by RA's. This shows that the RA's do not check the validity of programs and will organize any flyer as desired. Sadly, very few housing students felt inclined to fill out the survey without an incentive (i.e. gift card or giveaway).

Housing Survey Images



Challenges We Faced

The first challenge we had as a group was trouble picking out the correct RFID cards. For the cards we did have, we had to make 3 cards for each ID. Since some areas around CSULB didn't support TAP, and only swiping. We utilized brute forcing but no pattern led us to use something faster. The second challenge we faced was with the BeachBucks machine, our group was trying to collect many Student ID’s remotely, with that being said, Blackboard most likely has basic API security in place, and we would not be able to access the network needed to perform a man in the middle attack. The third challenge we faced was not getting enough faculty ID's. Based on our research it's shown that faculty won't give their ID"s whereas students were open to give it up for a chance at a $50 dollar Amazon gift card.

Future Implementations

The first implementation we would aim to create is a script that detects CSULB security precautions. From this we have access to every Student ID that has been registered through theBeachBucks machine. The second future implementation comes from the idea of when we were brainstorming ways to gain Student ID Numbers, we found out that the CSULB FTP Folder displays every student who has registered to have a website hosted through the school’s domain. From here we aim to check if the Campus ID number is valid and connect them to Student Name.

Results/Conclusion

The online surveys for getting the student ID numbers proved to work really well. We were able to gather a lot of student ID numbers and we can associate them to a name. We posted other surveys that people can take by scanning a QR code, but these did not work as well as the ones posted online. Sadly, our email spoofing attempt to get faculty to take a survey failed as well. Our process of duplicating ID cards to be able to write any ID number to it and get that card to be functionable was a success. The ID cards worked really well in any swiping instances. Unfortunately, when it came to card tap services, the cards were not being read correctly. The access we gained with these fake ID cards was the ability to see beach bucks balance and be able to spend this balance wherever beach bucks are taken.