Identity Theft:

A Study of Awareness amongst SJSU Students

SJSU SAN JOSÉ STATE UNIVERSITY

Harshada Bhide-Apte*,
harshada.bhide@gmail.com
010764845

Áine Cahill*,
cahillai@tcd.ie,
012055524

Niveditha Jain*,
nivedithahiriangady.jain@sjsu.edu
010471760

*College of Engineering,
San José State University,
One Washington Square,
San Jose, CA 95192-0085

Abstract

With the daily use of internet for various purposes from social interaction to banking, the threat of stolen identity has made it very important to be aware of and take precautions against Identity theft. For this purpose, we conducted a survey for the study of identity theft awareness among university level students. A survey questionnaire was composed by carefully analyzing the current issues in safety of personal identity. Safety in both financial and social accounts was the focus of the survey. It also gathered information about the type of passwords used by these students and other safety measures used over internet. Students' knowledge about common security threats like phishing attack, pharming and fraud websites was also gathered. This is an attempt to explore how seriously students take their safety.

Forty-three university students participated in this study. The study found that 97.67% of participant students were aware of the concept of identity theft. This awareness came from multiple sources like media e.g. newspapers and articles, academic course, security awareness program and personal experience. Participants were most familiar with threats like emails with links, insecure websites and downloadable software being used for identity theft. Many were also aware of safety issues related to phishing, smartphone apps and deceptive phone calls. Pharming was the least recognized method for identity theft. 95% of participants reported having no experience of their account credentials being used without permission in the past few months. Few (14%) survey participants shared their credentials so that someone they trust could use it with their permission. 63% participating students admitted they use different passwords for different accounts. The two-factor authentication also is popular. It was observed that only 54% of students log out of all websites that require passwords. Most participants did not consider themselves as possible victims of identity theft. The 'Privacy Paradox' was observed in this study, by the high levels of identity theft awareness amongst participants, but the poor security practices implemented by them.

Overall findings of this study were encouraging with more and more university students becoming aware of risks of identity theft over internet. But many people even though aware of the threat do not consider themselves as potential victims and that's why may not imply strictest safety methods leaving them vulnerable.

Keywords

Identity theft, Social media security, phishing, e-commerce safety

1 Introduction

The popularity of the Internet as a platform for social interaction, banking, financial transactions, e-commerce, education and office work has resulted in the majority of individuals having one, or multiple, e-identities.

These e-identities are generated and updated from an individual's school days and form an important part of daily life and interactions. E-identities comprise personal, and often, private or confidential information.

Identity theft occurs when an individual's identity is disclosed, distributed, modified or adopted without consent. Due to the comprehensive and private information included in e-identities, identity theft can cause serious damage to the victim. This damage may be associated with the victim's social identity, financial accounts, or educational and/or work credibility. The stolen identity could be used extensively in other crimes. This makes it highly important to spread the awareness about identity theft and how to prevent it from an early age.

Small-scale identity theft may be difficult to recognise initially, but may eventually lead to severe damage. Taking precaution at every single step, from social media accounts to university system accounts, is a necessity to prevent identity theft.

With this in mind, a survey has been conducted amongst university students in San Jose State University about their awareness and understanding of identity theft. This paper discusses student's awareness of identity theft, experience of identity theft and security-related online behaviour and also investigates students' cyber-security knowledge. This paper aspires to both analyse and draw students' attention to identity theft.

1.1 Literature Review

The Identity Theft Assumption and Deterrence Act gives the legal definition of what should be considered *Identity Theft*. This broad definition helps the prosecutors to conduct their cases in the ever-changing world of technology. However, identity theft is rarely a single crime. Usually it is used to commit a bigger crime, of severe nature. A study modeled after the FTC's original 2003 methodology, suggests that 9.3 million adults were victims of some form of identity theft in 2004 [1]. Any person of any age, gender and education, including everyone from newborns to deceased people, is vulnerable to having their identity stolen. But among the reported identity thefts incidents most of the victims are between the ages of 20 and 44.

A person's use of the Internet immediately makes them vulnerable to online identity theft [5]. The most common type of identity theft is credit card fraud, which can occur in many ways. With online banking and shopping websites, financial fraud has become more common than before [1].

The reporting of identity theft is an area in which major improvements must be made. Once a victim becomes aware of the occurrence of fraud on their account(s), it is important to file an official complaint with proper authorities. In some cases, victims may not know to whom complaints should be addressed. Furthermore, victims may not understand how urgent it is for them to take addressing actions. Depending on the identity stolen, victim often register complaints with the concerned organization but do not report this crime to the police [1]. Research indicates only 25% of victims report credit card identity theft to a police agency, while over 40% of people report these crimes to credit agencies [5].

In many cases, a victim's identity is stolen by those who have easy access to their personal information or by those with whom the victim lives in close contact (e.g. college dorms). This emphasises the importance for individuals to never disclose account access and authentication details, such as usernames and passwords, to anyone, including close friends and family. Furthermore, strong passwords and regular updating of these passwords is essential to prevent identity theft. For example, using birthday as password may make it easier for someone who knows you, to guess it, which may increase the probability of an occurrence of identity theft [1].

Identity theft usually occurs in three steps; (1) acquisition, (2) use, (3) discovery.

As per Federal Trade Commission research, there is a positive correlation between the time it takes to discover the occurrence of identity theft and the seriousness of the damage caused by this identity theft. Increased time to identity the occurrence of identity theft also reduces the possibility of an offender being caught and damages being repaired [4].

The cost of identity theft crimes extends beyond financial loss and encompasses additional soft costs such as a victim's reputation being damaged, emotional disturbance, etc. [2].

Today, social media websites including Facebook, Twitter and Snapchat are extremely popular with young people for social media and communication. A large volume of information, often very personal information, captured in text, photographs, videos and voice recordings, is exchanged over social media websites. This information exchange can play a major role in identity theft. Research conducted at Carnegie Mellon University shows that teenagers aged 15-18 years are most likely to be victims of online identity theft. Frequently, social media platforms are the gateways for identity theft.

1.2 Objective of Study and Hypothesis

The principle aims of the study are to (1) Investigate the awareness of SJSU students of online identity theft, (2) Investigate the online behavior of SJSU students in relation to security and privacy, which either increases their vulnerability or increase their protection against identity theft attacks.

It was sought to determine the degree of familiarity of SJSU students with the concept of identity theft;

- Familiarity with the concept of identity theft.
- Familiarity of safe internet practices to prevent identity theft (using strong passwords, changing passwords frequently, recognizing fraudulent websites, not responding to phishing emails, not sharing passwords and not giving access to financial and social online accounts to other people)
- Familiarity with the procedures to follow if one thinks one is the victim of an identity attack online.

It was also sought to determine how each student became aware of identity theft, e.g. through workshops, personal experience, etc.

These research aims will be explored by distributing a survey and analyzing the survey results under four headings; experience of identity theft, cyber-security knowledge and security-related online behaviour.

2 Experimental Design and Method

2.1 Method

The research was executed in a multi-stage process, including conducting a literature review, identifying the key aims to be addressed in the research, designing a survey using Qualtrics, distributing the survey to SJSU students through social media, analyzing the results of the survey using graphical and written descriptions, drawing primary conclusions from the research and presenting the results in a report.

A literature review on *Identity Theft* was conducted by analyzing the literature available on this subject on the IEEE Xplore Digital Library Database and the ScienceDirect database. Mass media articles from well-known newspapers including the New York Times and the LA Times were analysed to develop an understanding of public awareness of identity theft and the publicized attacks, victimization and advice supplied by mass media outlets in relation to identity theft. Verbal discussions and informal interviews with SJSU students on identity theft were executed to identify the key aims and trajectory of the research.

The primary aims of the research were determined: (1) To investigate the awareness of SJSU students about identity theft, (2) To identify trends in the security-related behavior of SJSU students online, which would increase their vulnerability or protection against identity theft attacks.

Twenty-two questions were designed to address the primary research questions. These questions were compiled in a single online survey, which was prepared using Qualtrics. The clear, concise questions varied in terms of the required response type, including multiple choice answers, yes/no answers, textboxes and rearranging segments in order of priority. It was ensured that all answer options for each question were mutually exclusive, but collectively exhaustive, to ensure the survey participant was clearly able to categorize their answer in multiple choice questions. The twenty-two questions were presented in a single page, so that survey participants were immediately aware of the length of the survey. It is postulated that this decreased the number of responders who commenced, but did not finish the survey.

The survey was distributed to SJSU students using social media. Three focus groups of SJSU students were identified for the survey; (1) SJSU International House residents, (2) SJSU Masters in Electrical Engineering students, (3) SJSU Masters in Computer Engineering students. For each of these three groups, a Facebook exists, on which a description of the survey, an appeal for survey participants and a URL link to the Qualtrics study was posted to attract survey participants from SJSU students in the three focus groups. There were forty-three survey recipients in total. The survey was publicized and available for SJSU students to complete for a period of three weeks, from February 23rd, 2017 to March 16th, 2017.

Upon closure of the survey access period, the survey results were analysed using tools in Qualtrics. The results data was graphically presented in Tableau using bar graphs and trend lines. Tables were also employed to display multi-dimensional, record-based data. Graphical presentation of the results was legible and clearly labelled, had a consistent color scheme, had accompanying labels and legends, and clearly expressed the key points extracted from the survey results. Basic statistical analysis was performed on the survey data to identify mean, modal, variance and categorization metrics, which summarize the data.

Results from the research were presented in a report for further distribution and long-term records.

A copy of the questions included in the survey is presented in Appendix A.

2.1.1 Participants

There were forty-three participants in the study. All the participants were SJSU undergraduate or masters-level students. The students belonged to three social and academic groups associated with SJSU, including the SJSU International House (student residential accommodation), Masters of Electrical Engineering students and Masters of Computer Engineering students.

Demographic data was not collected for this study. Hence, it is not known how the forty-three survey respondents were distributed across gender, age and academic status.

2.1.2 Tools

The survey was designed using Qualtrics. This software platform enabled answers to questions to be of the form Yes/No, multiple choice, text box or drag boxes to arrange according to priority. Qualtrics provides a simple user interface to design the survey and allows survey distribution through a simple URL distribution, which can be easily copied and pasted and clicked on for access to the survey.

Qualtrics and Tableau were employed for data analysis. Tableau enabled the data to be analysed graphically, using bar charts and trend lines. Tables were also employed for clear display of multi-dimensional data, which was best presented as records of data.

3 Results and Discussion

3.1 Results

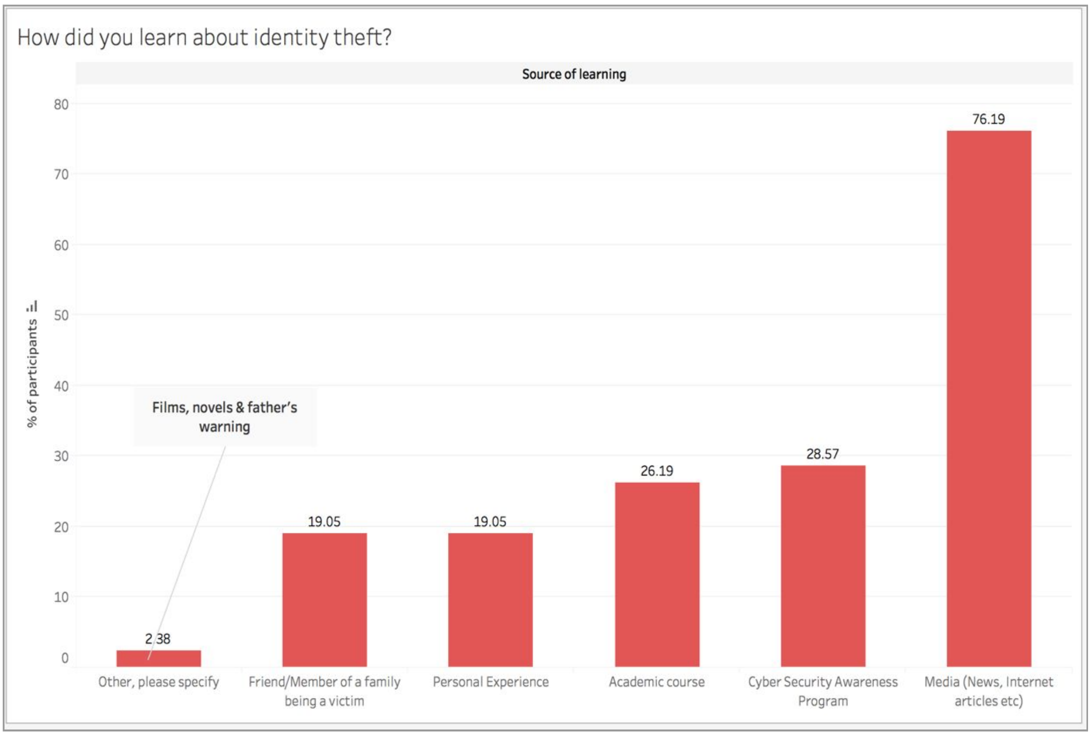


Chart 1: Source of Learning about identity theft

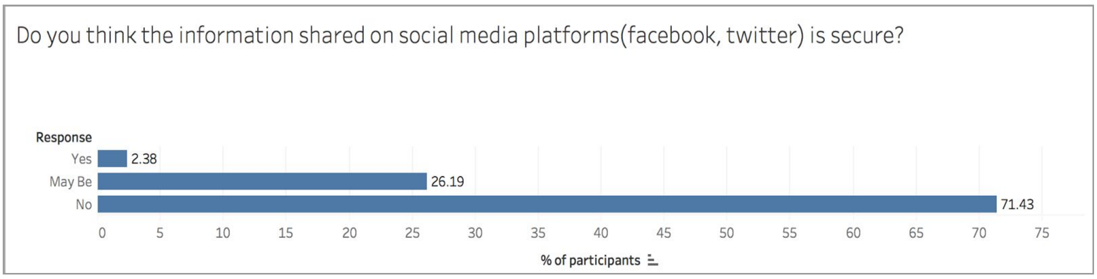


Chart 2: Social Media Security as perceived by SJSU students

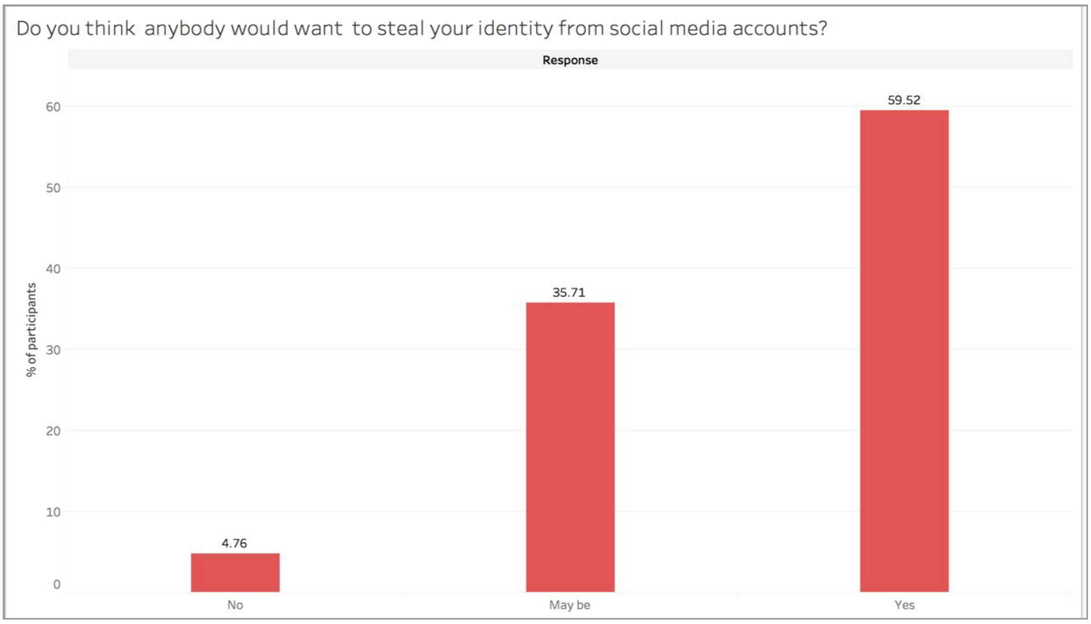


Chart 3: Possibility of identity being stolen from Social Media

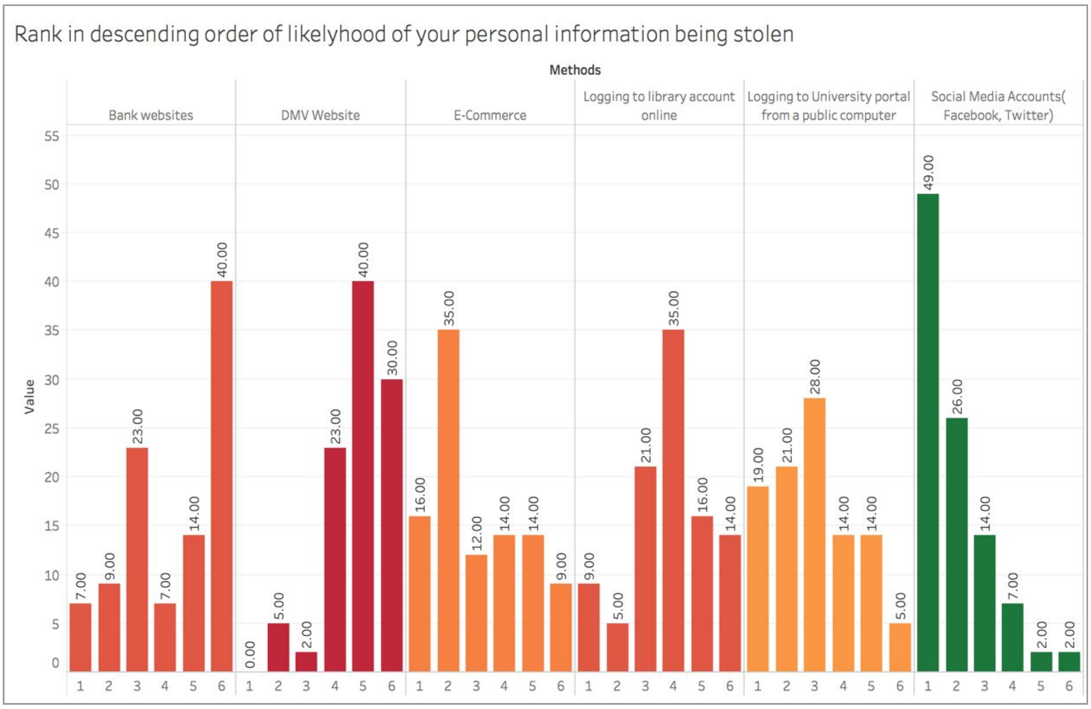


Chart 4: Likelihood of personal information being stolen

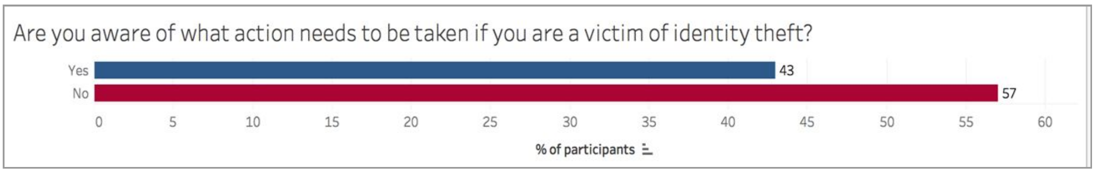


Chart 5: Aware of what actions to take if one is a identity theft victim

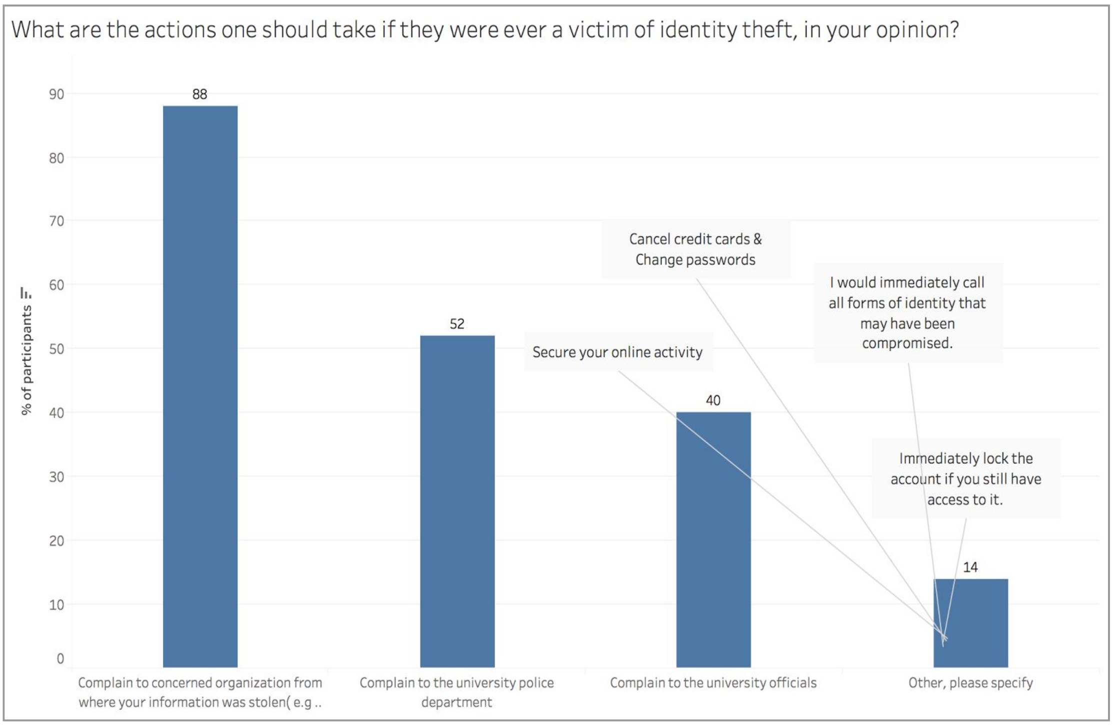


Chart 6: Actions one intend to if they were ever a victim of identity theft

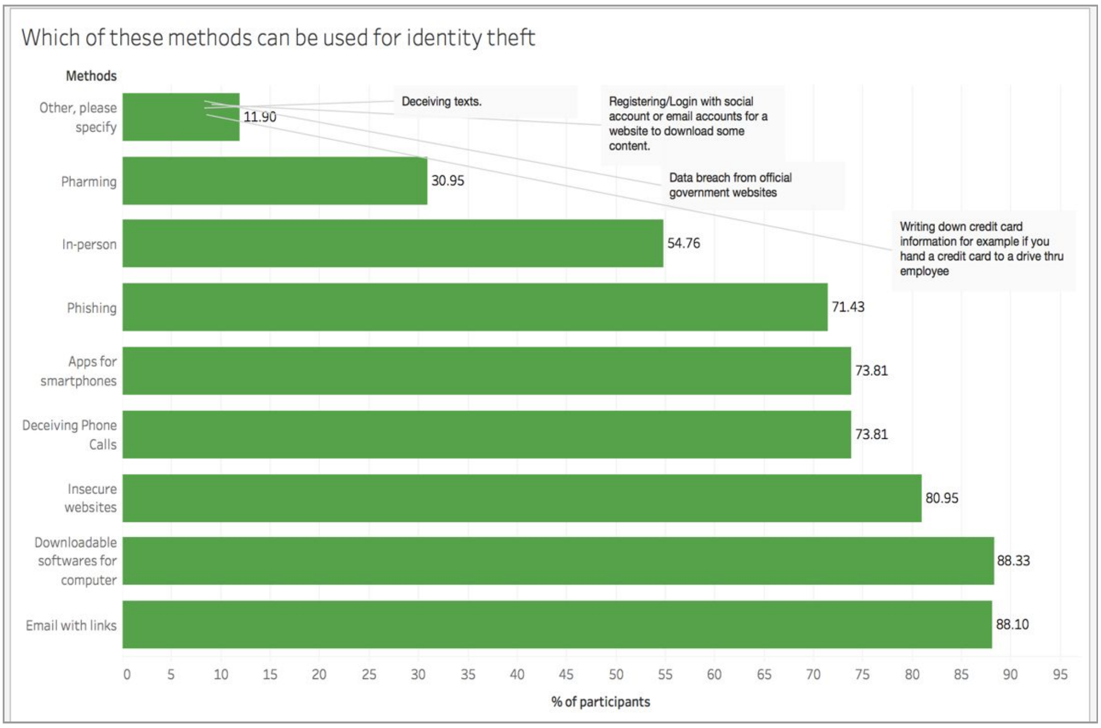


Chart 7: Methods of Identity Theft

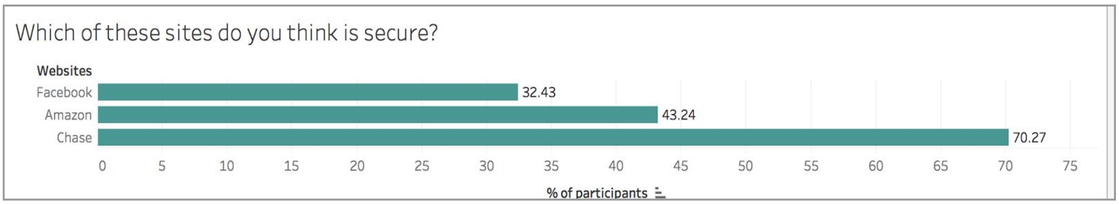


Chart 8: Sites which SJSU students believed were secure

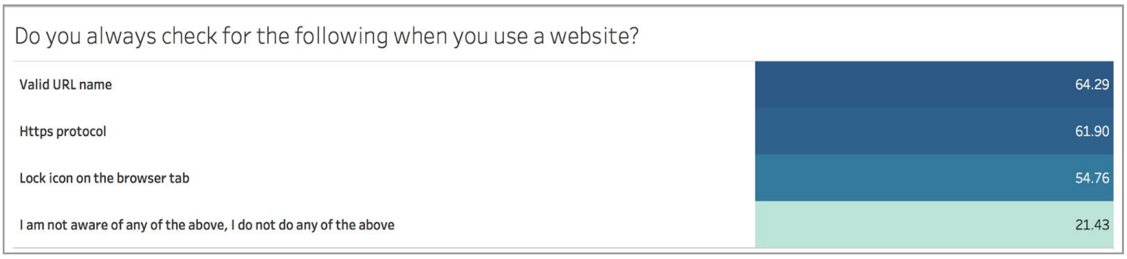


Chart 9 : Security measures student check while browsing

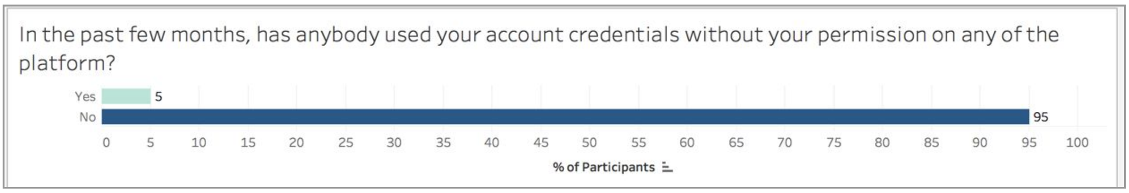


Chart 10: Identity Theft Experience

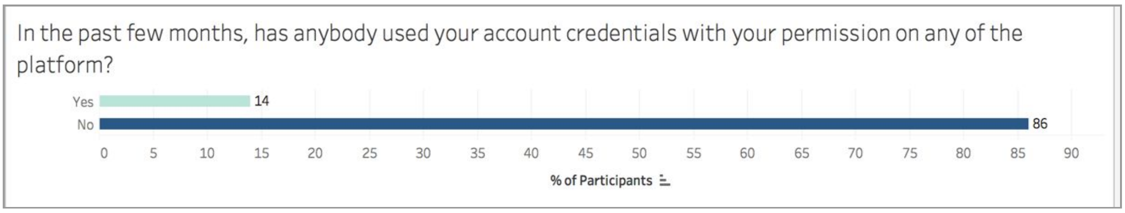


Chart 11: Participants sharing their account information with others

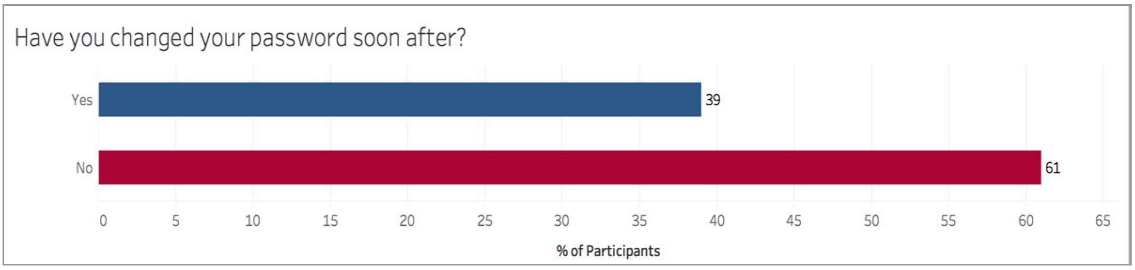


Chart 12 : Action taken after credentials being used by someone else

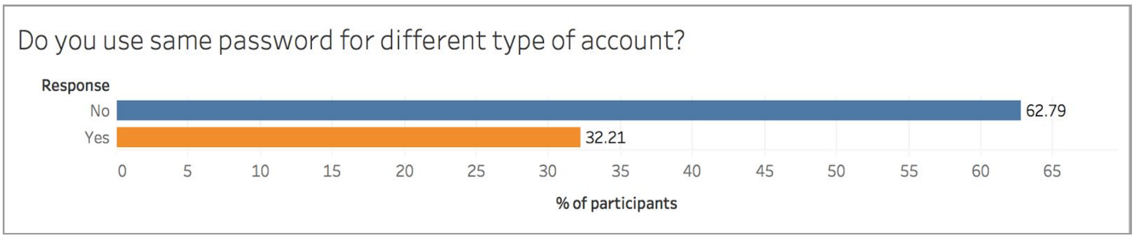


Chart 13: Password usage pattern

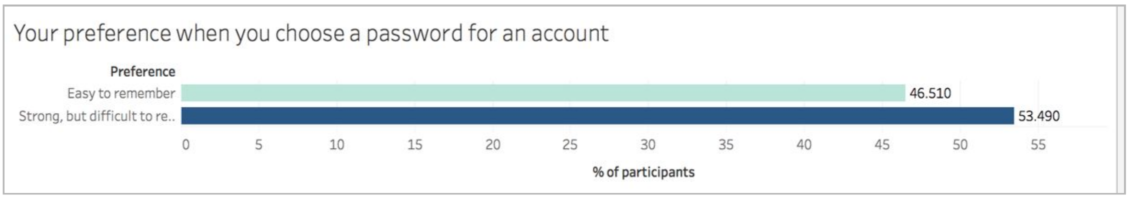


Chart 14: Password preference

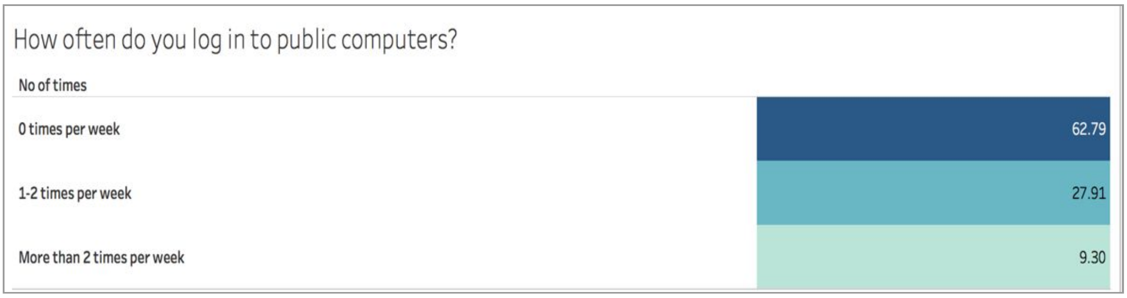


Chart 15: Logging to Public Computers

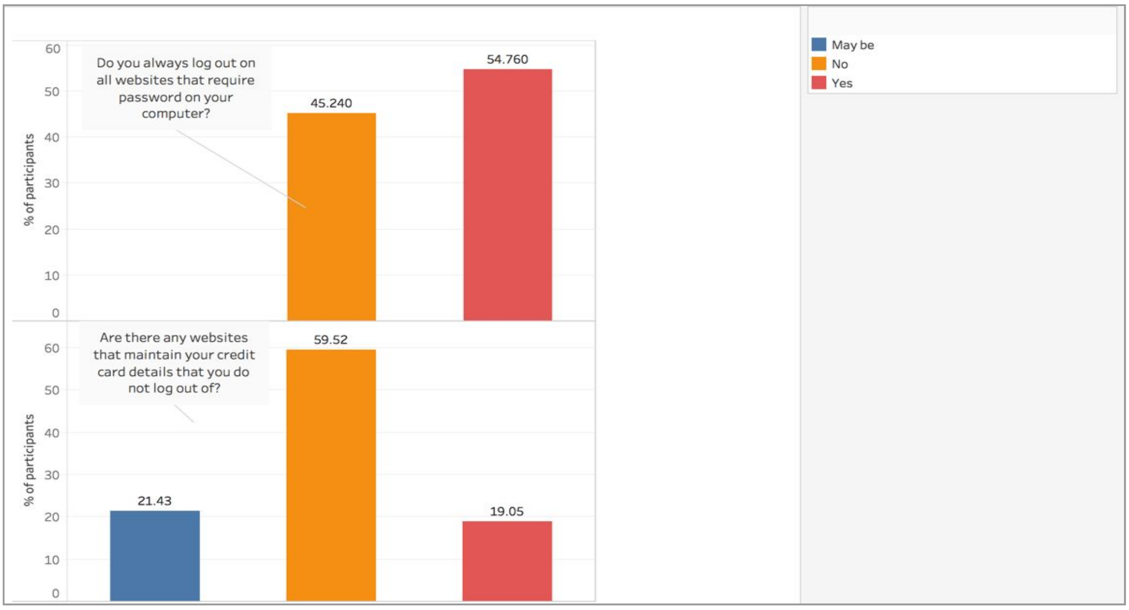


Chart 16: Log out behaviour

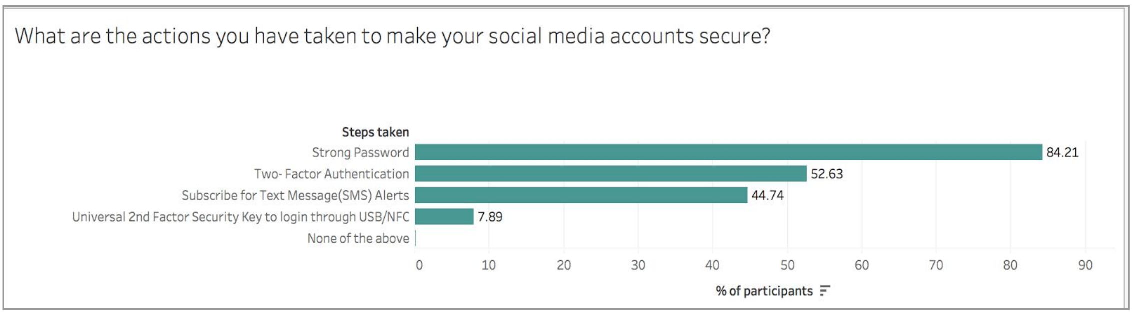
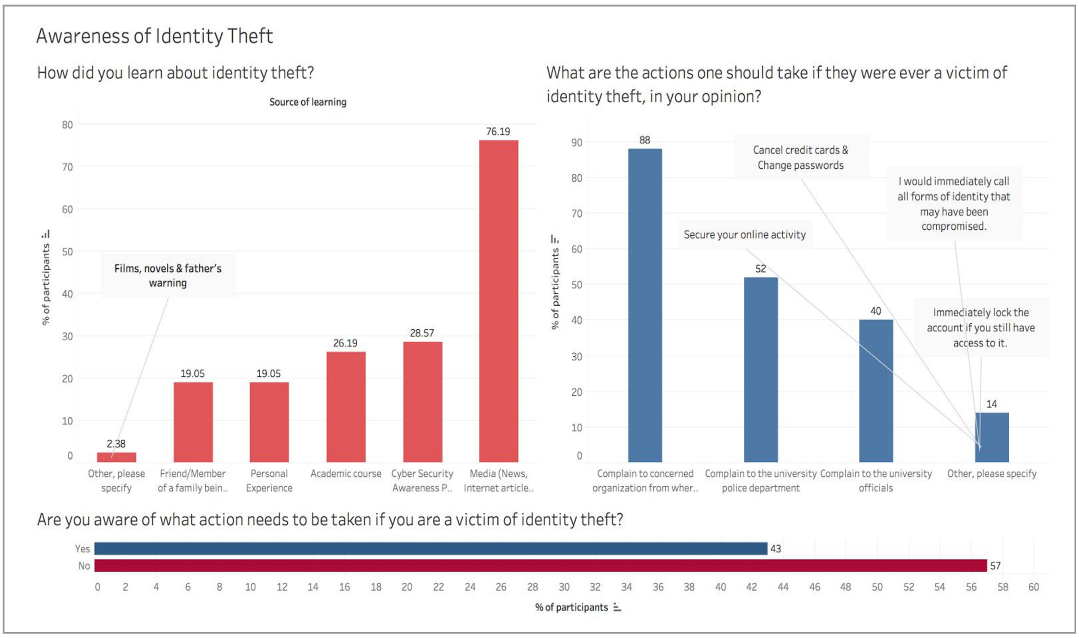


Chart 17:Actions taken to make social media accounts secure

3.2 Discussion

3.2.1 Awareness of Identity Theft



To protect oneself from identity theft and to recognize when one is the victim of an identity theft attack, one must be aware of what defines identity theft, the scenarios in which identity theft can occur, the methods employed to perform an identity theft and the actions to be taken to follow up an incident of identity theft.

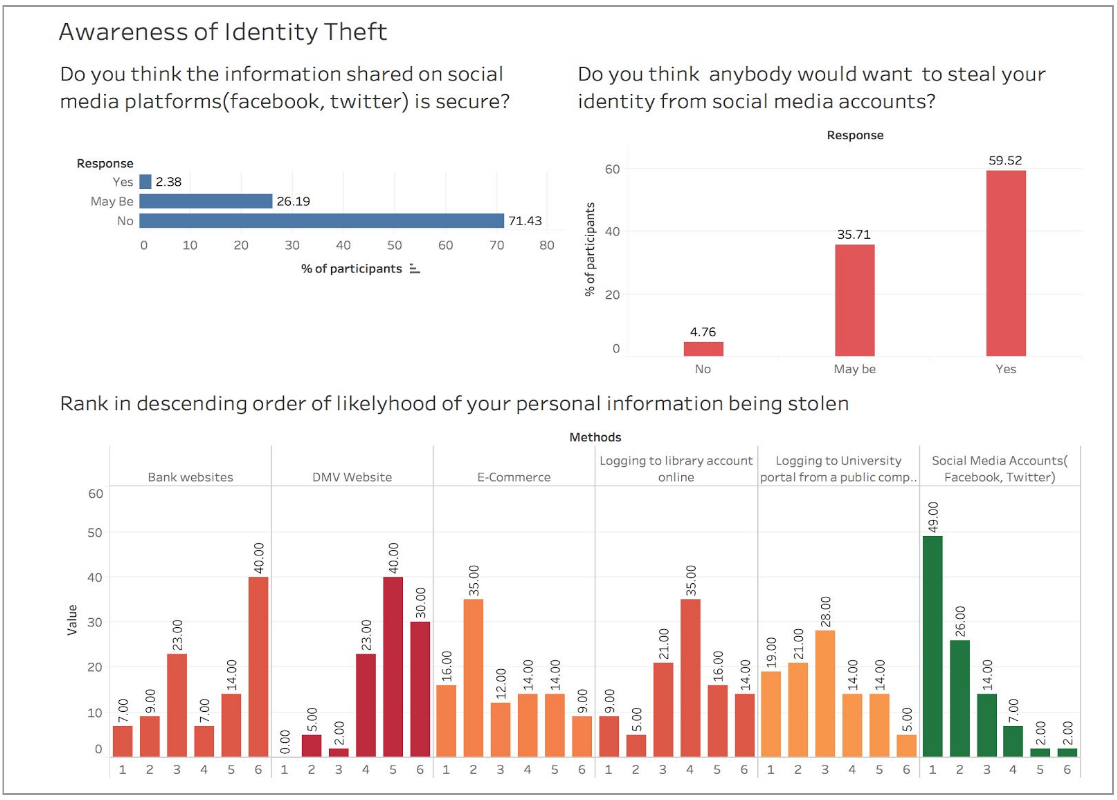
For this discussion, 'SJSU student survey respondents' will be shortened to 'SJSU students', as the survey results are postulated to extend to and be representative of the entire undergraduate and graduate SJSU student population.

From question 1 in the survey, it was found that 42 out of 43 (97.67%) of SJSU students were aware of identity theft. This result can imply that awareness of identity theft is generally very high amongst SJSU students.

This awareness of identity theft stems from multiple sources, as discovered from the results of question 2 in the survey: As per Chart 1, 76.2% of students learned about identity theft from the media, including newspapers and internet articles. Between 19% and 29% of students became aware of identity theft from an academic course, personal experience, a friend or family member being a victim of identity theft or a cyber security awareness program. One survey respondent (2%) reported exposure through films and novels, and from warnings received from his/her father.

Hence, media has the greatest influence to inform SJSU students about identity theft. This influence should be harnessed to increase awareness of identity theft to students, to inform about optimal security practices online and to make resources available to assist students if they are victim to a security attack.

Nonetheless, with 26% and 28.5% of students receiving exposure to identity theft through academic courses and cyber security awareness programs, it is clear that SJSU is reaching out to a significant portion of the student community. However, increased efforts could be made to reach out to most of the SJSU student population.



The survey also investigated the attitudes of SJSU students towards the potential for identity theft to occur.

From question 13 in the survey, it was found that as per Chart 2, 71% of SJSU students do not believe information shared on social media platforms is secure. 26% of students are unsure whether information shared on social media is secure and only one respondent reported their belief that this information sharing is secure. Therefore, over 97% of SJSU students are not convinced that social media does provide a secure platform for the sharing of information. Social media usage is very high amongst SJSU students; for socializing, sharing photographs and life events and thoughts, getting access to news stories and cooperating with peers on academic assignments and projects. Therefore, it is important to ask whether the security risks on social media perceived by students translate to proactive steps being taken by students to prevent cyber security and identity theft attacks.

From question 14 (Chart 3), it was found that 95% of SJSU students think someone may want to steal their identity from social media accounts at some stage. Only 2 survey respondents believe no one would want to steal their identity.

These results correlate very well with those of question 13, showing that for the students who believe social media is not secure for information sharing, they also believe someone may want to steal their identity through social media. This relationship also extends to those students believing social media might be, or is, secure and someone maybe, or not, wanting to steal their identity, respectively. The results show that awareness of a lack of security in social media results in students recognizing that they personally may be victim to an identity theft attack.

Question 4 asked students to rank contexts in which personal information might be stolen, in descending order from most probable to least probable. As per Chart 4, 49% of SJSU students selected social media accounts as the most likely context in which information may be stolen. 19% of students marked login portals to university public computers as being the most likely context for information to be stolen. Bank websites were identified by 40% of students as being the least likely of the presented contexts in which one's information may be stolen. However, 30% of students also selected the DMV website as being the least likely context for information theft.

These results show that SJSU students believe less 'serious' (social media) and public internet access points to be the most probable contexts for information theft. More 'serious' websites, for e-Banking and the DMV, are determined to be more secure and less at risk of information theft, by students. It should be noted that there is approximately a uniform distribution of trust in security of e-Commerce websites, from most secure to least secure, however, it is slightly skewed towards having perceived good security.

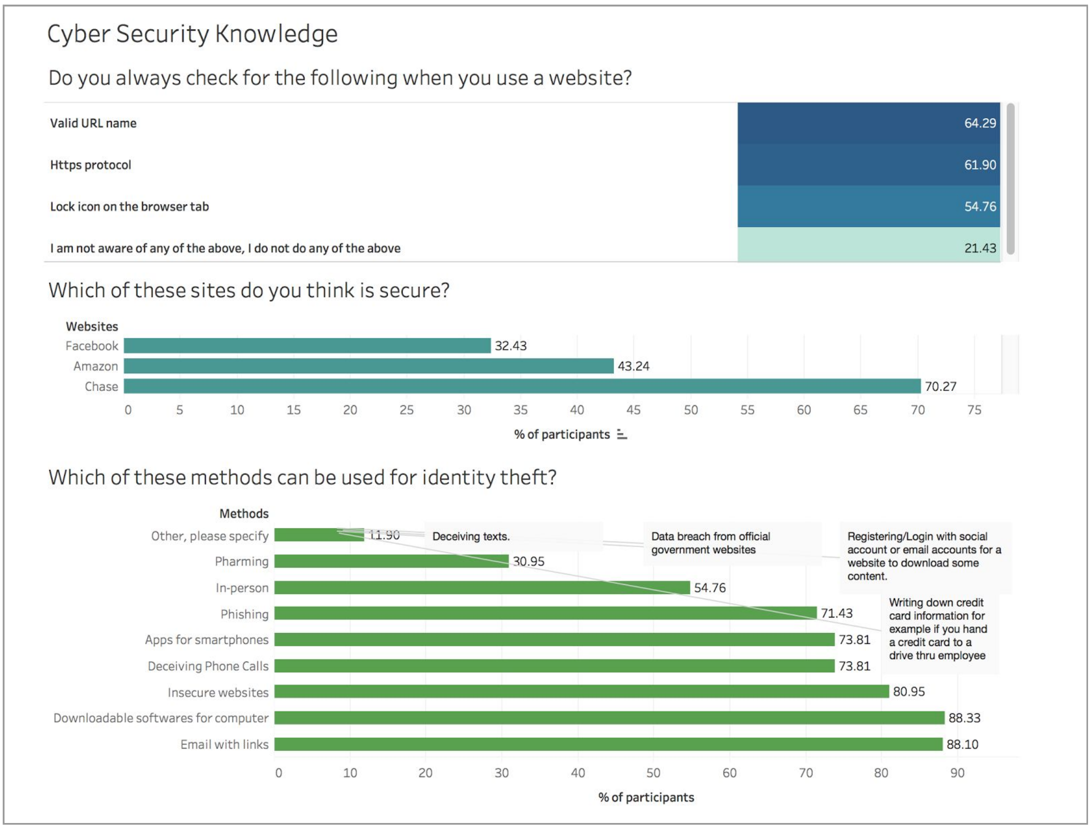
Question 22 investigated whether SJSU students would be aware of the steps required to be taken if one was the victim of an identity theft. As per chart 5, it was found that approximately half the students (57%) are not aware of the required steps to be taken. Therefore, not all students who believe they may be subject to an identity theft know what steps to take if they are subject to an identity theft attack. However, more students know how to respond to an identity theft attack than are made aware of identity attacks through academic courses and cyber security awareness programs. Therefore, some students are learning about response actions through media, friends and family and other sources. However, these informal response suggestions may not be optimal.

In question 23, SJSU students were asked to report what specific actions they would take to respond to identity theft. As per chart 6, 88% of students would complain to the concerned organization, from where one thought one’s information had been stolen. 40% of students would report the matter to university officials and 52% of students would report to the university police department. 14% of respondents suggested alternative courses of action, including immediately locking the account if one still has access to it, cancelling credit cards, changing passwords, learning more about the security breach to protect oneself against future attacks and immediately calling one’s bank and other compromised entities to cancel accounts.

These results show that most students would seek to address the identity theft attack themselves, without help from SJSU university personnel. However, approximately half of the students would also contact the university. This shows that while students are very independent, they still recognize the support structures available through SJSU. It is recommended that SJSU increase publicity of their cyber security resources to SJSU students.

It is recommended that SJSU try to educate more of the student population about identity attacks to ensure that students are correctly informed about the risks, characteristics and response mechanisms to identity theft attacks.

3.2.2 Cyber Security Knowledge



Awareness of cyber security is very important; however, a concrete knowledge of cyber security and identity theft is even more important. The study sought to briefly quantify and evaluate the level of knowledge of cyber security amongst SJSU students.

In question 3, SJSU students were presented a list of methods which could be used to steal one's identity. Students selected the methods they believed could be used for a security attack. As per chart 7, the results show that students are most familiar with emails with links, insecure websites and downloadable software being used for identity theft (80%-88% of students selected these as possible methods for identity theft). 71%-73% of students recognized phishing, smartphone apps and deceptive phone calls as being possible methods employed for identity theft. Pharming was the least recognized method for identity theft, with only 31% of SJSU students selecting it as a possible attack mechanism.

Other methods suggested by SJSU students for identity theft included receiving deceptive texts, data breaches occurring to official government websites which store one's personal information and people writing down one's credit card details when one hands them a card for payment, e.g. in a Drive-Thru restaurant. Only one student put forward the possibility that identity theft may occur not through their own actions, but through a lack of security on the part of another entity, e.g. government. This reflects the independence of SJSU students, i.e. 80% of students would try to respond to an identity theft attack by themselves, and 97% of students did not consider identity theft occurring outside of their control. However, the possibility of identity theft occurring due to a company/government data breach was not presented in question 3, so different results may have been gathered if this option was included.

In question 16, screenshots of the webpages of three insecure websites were presented; Amazon (not using HTTPS), Facebook (phishing website; invalid website domain name) and Chase (phishing website; invalid website domain name). As per chart 8, 43% of SJSU students believed the Amazon E-Commerce webpage was secure. 32% of SJSU students believed the Facebook social media webpage was secure. 70% of students believed the Chase e-Banking webpage was secure. The results show that, while SJSU students are aware of cyber security and identity theft risks, most students cannot consistently distinguish between secure and insecure webpages.

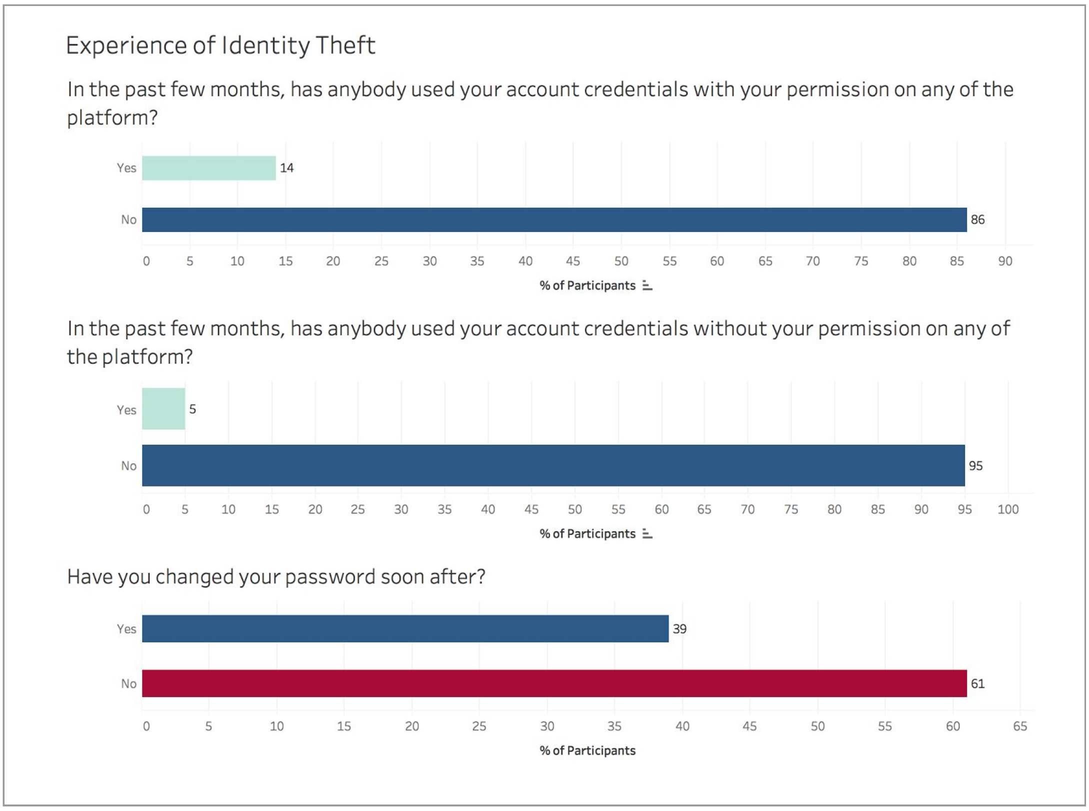
The Amazon webpage did not use HTTPS, but did have a valid domain name. This suggests approximately half (56%) of SJSU students are aware of the importance of using HTTPS when dealing with sensitive information online. However, it is postulated that SJSU students may have been more likely to mark this webpage as insecure because of its context in an identity theft survey. This postulation is made because of the lack of security awareness in the Chase webpage example.

An increasing number of students (67%) recognized the phishing webpage used for the Facebook page. 70% of SJSU students mistakenly declared the Chase e-Banking webpage to be secure, despite it being a phishing webpage like the Facebook webpage. This suggests that students may have been guessing in their answers to identifying insecure webpages. Hence, while awareness of cyber security is high amongst SJSU students, concrete knowledge about cyber security which can be utilized in real life is not high amongst SJSU students.

The results from question 16 do not reflect the assertions by SJSU students in question 17, declaring that, when using a website, as per chart 9, 62% of students check that the HTTPS protocol is being employed, 64% of students check for a valid URL name and 55% of students check for the lock icon in the browser tab. Only 21% of students admitted that they were not aware of the aforementioned methods to confirm the security of a website. The assertions made by students in question 16 about demonstrating good online security behavior conflict greatly with the poor results of students to recognize three insecure web pages in question 16. Hence, students appear to be overly confident about the knowledge and good practice in relation to cyber security. It is suggested that more hands-on practice and demonstrations are included in the cyber security awareness programs made available to SJSU students.

Actionable knowledge about cyber security is primarily obtained from formal workshops and seminars. In question 20, it was found that only 75% of SJSU students had attended a workshop or seminar on identity theft. This very low rate of attendance at formal information events on cyber security may explain the low success rate of identifying insecure web pages from question 16.

3.2.3 Experience of Identity Theft



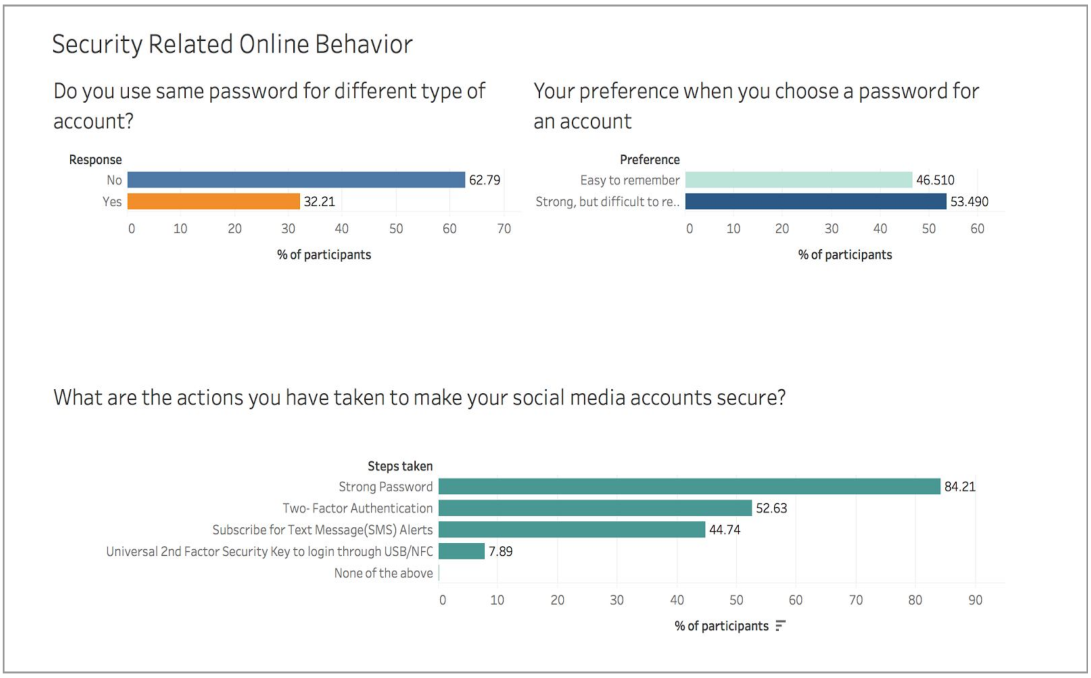
This study also investigated incidence rates of minor identity theft.

The study found in question 18 that (Chart 10) 95% of survey participants had no experience of their account credentials being used without permission in the past few months. However, 5% of SJSU students (2 survey participants) did have their account credentials used without their permission. This represents a significant number of students, particularly since only two survey participants (5%) thought someone may want to steal their identity from social media accounts. More research is required to investigate the types and contexts of identity theft attacks occurring to SJSU students.

Chart 10 shows that 14% of survey participants shared their credentials so that someone they trust could use it with their permission. Of the students who had experienced identity theft in recent months, as indicated in question 18, only 39% of students had subsequently changed their related password.

This is a very surprising result: 61% of the 14% of SJSU students who shared their password with others changed their password soon after. This demonstrates that SJSU students do not appreciate the seriousness of identity attacks and the repercussions that may ensue, or SJSU students believe that since their accounts have been compromised, the important information has already been taken, so they continue to maintain the same account. These actions allude to naivety and passivity, which should be addressed through increased awareness programs and campaigns by SJSU.

3.2.4 Security-related Online Behavior

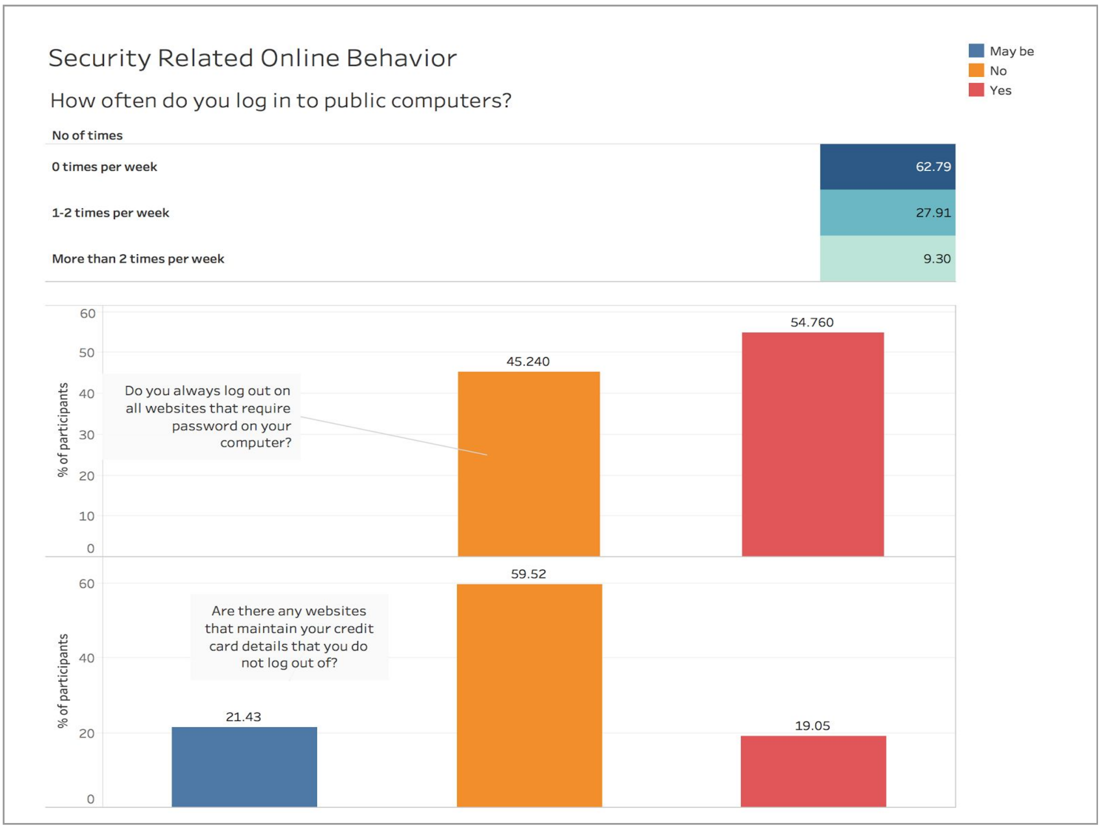


A phenomenon called the 'privacy paradox' has been discussed in the literature. The 'Privacy Paradox' refers to people having an awareness and understanding the importance of privacy and security, but behaving in an inconsistent manner by showing a lack of regard and concern for security and privacy. The 'Privacy Paradox' can be seen in the results of this survey, by the high levels of identity theft awareness amongst SJSU students, but the poor security practices and rates of recognition of insecure webpages of these students.

In question 5, the types of online accounts belonging to students was investigated. 100% of SJSU students had social media, e-Banking and email accounts. 93% of SJSU students admitted they had school portal accounts (even though 100% of SJSU students have online portal accounts). 48% of SJSU students had work-related online accounts.

Question 6 revealed that 63% of SJSU students use different passwords for different accounts. This reflects good security practices. The ability for students to remember so many passwords may be attributed to keychain management systems which are becoming more popular across operating systems on computers, tablets and smartphones.

Password creation behavior was investigated in question 8, showing that 46.5% of SJSU students choose passwords that were easy to remember, while 53.5% of SJSU students choose passwords that were strong, but difficult to remember. This demonstrates that although students acknowledge the risks of identity theft, many still chose simpler passwords for convenience of use and memorization. There is a clear trade-off between security and password-convenience/memorability exhibited in the results of this study.



It was found that 63% of students never log onto public computers in SJSU. 28% of students log onto public computers 1-2 times per week and only 9% of students onto public computers more than 2 times per week. This reflects the rising popularity of personal devices, and the subsequent separation of SJSU students from using public computer resources.

One should recall that public computers were credited as the second most likely context in which one’s information may be stolen. Hence, this belief may also be pushing students away from using public computers. For SJSU, to ensure public computing resources are used optimally and viewed as secure, these resources should be securely protected and well-advertised as being secure. It is postulated that SJSU should not invest too much money on public computer resources, due to the lack of demand for such resources.

While many online services require passwords, the results from question 10(Chart 14) revealed that only 54% of students log out of all websites that require passwords. Websites listed in the results of question 11, for which students do not log out include Facebook, Splitwise, Twitter, Amazon, Gmail, Instagram, Canvas, News websites, LinkedIn, shopping websites. It is important to note that the 68% of students do not log out of social media websites, despite these websites being ranked as the most likely context in which information might be stolen. This clearly demonstrates the 'Privacy Paradox' in SJSU students.

As per chart 14, 19% of SJSU students allow websites that they do not log out of to maintain their credit card details, and 21% of students *maybe* allow websites that they do not log out of to maintain their credit card details. This is further evidence of the 'Privacy Paradox', with only 60% of SJSU students taking the simple step to logout of websites which maintain their banking details.

In terms of other steps taken by SJSU students to secure their social media accounts (viewed as the most probably contexts for identity theft), 84% of students claim to use a strong password (despite only 53% of students explicitly declaring to create strong passwords in question 8). Two factor authentication is becoming more popular, with 53% of students employing this technique. 45% of students also subscribe for text message alerts. These results show that students are likely to own multiple devices connected to the internet and students are comfortable and familiar with cross-platform authentication over different devices.

4 Conclusion

The study found that majority of the people studying at the university level (97.67% of participant students) are aware of the concept of identity theft and its consequences. The overall understanding about the threats and security vulnerabilities of using online accounts are known to the these people. Students are taking precautions while using passwords, responding to emails and divulging information on social media (71% students think information shared on social media could be hacked/misused). Media including newspapers and online articles play an important role in making students aware of the possible issues. Academic courses are also important in generating this awareness. More than half the students (57%) are aware of the required steps to be taken in case they fall victim to a crime related to identity theft. But more awareness needs to spread in this regard. Most of the students (70%-88%) are aware of various ways in which their confidential data can be stolen like phishing attacks, malware, insecure websites etc. A considerable number (14%) of SJSU students had experienced identity theft in some or the other form. Surprisingly, only 39% of students who had experienced identity theft in recent months; had subsequently changed their related password. This shows the discrepancy between awareness about safety and taking actual preventive or counter actions against theft. Privacy Paradox is evident from the results of this survey.

Overall this survey had positive results when it comes to awareness among SJSU students about online vulnerabilities associated with identity theft. But there is much to be done to convert this awareness into actual precautions taken by individuals.

References

[1] G. R. Newman, M. McNally, “Identity Theft Literature review”, July 2005, https://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf

[2] E. Holm, “Social networking and identity theft in the digital society”, 2014 http://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1729&context=law_pub

[3] Synovate, “Federal Trade Commission—2006 identity theft survey report”, November 2007, http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf

[4] National Institute of Justice, “Identity theft - A research review”, July 2007 https://www.ncjrs.gov/pdffiles1/nij/218778.pdf

[5] Criminology and Criminal Justice Senior Capstone Project, “Prevention of Identity Theft: A Review of the Literature”, Summer 2011, http://pdxscholar.library.pdx.edu/cgi/viewcontent.cgi?article=1008&context=ccj_capstone

Appendix

A Survey Questions (22 questions)

1. Are you aware of the concept of identity theft?
   Yes/No

2. How did you get to know about identity theft?
   Media (News, Internet articles, etc.); Academic course, Personal Experience; Friend/Member of a family being a victim; Cyber Security Awareness Program; Other, please specify.

3. Which of these methods could be used to steal one's identity, in your opinion?
   Phishing; E-mails with links; Downloadable software for your computer; Apps for smartphones; In-person; Pharming; Insecure Websites; Deceptive Phone calls; Other, please specify.

4. Please rank, in descending order of likelihood, the context in which your personal information might be stolen.
   Logging in to library account online; Logging in to University portal from a public computer; Social Media accounts (e.g. Facebook, Twitter); Bank websites; DMV website; E-commerce websites (e.g. Amazon, eBay).

5. How many types of accounts do you have?
   (social media, bank, school, work, email, other; please specify)

6. If you have more than one account, do you use the same password for more than one account?

7. If you answered YES to the above question, please specify the domains in which you share the same password (Drag the options into groups)?

8. What is your preference when you choose a password for any account?
   Easy to remember; Strong, but difficult to remember.

9. How often do you login to public computers?
   1-2 times per week; More than 2 times per week; 0 times per week.

10. Do you always log out of all websites that require passwords on your computer?
    Yes/No

11. If no, please specify the websites you do not log out of.
    (Textbox)

12. Are there any websites that maintain your credit card details that you do not log out of?
    Yes/Maybe/No

13. Do you think the information shared on social media platforms (e.g. Facebook, Twitter) is secure?
    Yes/Maybe/No

14. Do you think anybody would want to steal your identity from social media accounts?
    Yes/Maybe/No

15. What are the actions you have taken to make your social media accounts secure?
    Strong password; Two-Factor Authentication; Subscribe for Text Message alerts;
    Universal 2nd factor security key to login through USB/NFC; None of the above.

16. Which of these websites do you think are secure?
    (Screenshots of insecure Amazon, Facebook and Chase websites)

17. Which of the following do you check for when you use a website, to ensure it is secure?
    Https protocol; Lock icon on the browser tab; Valid URL name; I am not aware of
    any
    of the above/ I do not do any of the above.

18. In the past few months, has anybody used your account credentials without your permission in any of your online accounts?
    Yes/No

19. If answered YES to Q18, did you change your password soon afterwards?
    Yes/No

20. Have you ever attended a workshop or security seminar on identity theft?
    Yes/No

21. Are you aware of what action needs to be taken if you are a victim of identity theft?
    Yes/No

22. What are the actions one should take if they were ever a victim of identity theft, in your opinion?

Complain to the university police department; Complain to the university officials; complain to the concerned organisation from which your information has (you think it has) been stolen (e.g. Amazon, DMV); Other, please specify.