Identity Theft

A Study of Awareness amongst SJSU students

Áine Cahill	Harshada Bhide-Apte	Niveditha Jain
012055524	010764845	010471760

ISE/COMP 219
HCI for Cyber Security
6th April 2017

Overview

- Introduction
- Literature Review
- Hypotheses
- Method: Participants, Tools/Techniques/Data Collection
- Results and Discussion
  - Awareness of Identity Theft
  - Experience of Identity Theft
  - Security-related Online Behavior
  - Cyber-security Knowledge
- Conclusions
- Questions
- Appendix: Survey Questions

Introduction

- E-identities; social, banking, school, work
- Identity Theft
- Stolen identity used in other crimes
- Take precaution at every step
- Survey:
  - Students' awareness
  - Students' behavior
  - Students' knowledge

Literature Review

- The Identity Theft Assumption and Deterrence Act
- 9.3 million adults victims of identity theft in 2004 in U.S.A.
- Three steps of theft
    1. Acquisition
    2. Use
    3. Discovery
- Longer time to discover => greater damage imposed
- Social media related theft = Hard costs + soft costs

Hypotheses

- Principle aims of the study:
  1. Investigate awareness of SJSU students
  2. Investigate online behavior of SJSU students

- Familiarity with:
  1. Concept of identity theft
  2. Safe internet practices to prevent identity theft
  3. Procedures to follow when identity theft occurs

Method

- **Multi-stage process**:
  1. Literature review
  2. Designing a survey
  3. Distributing the survey
  4. Analyzing the results
  5. Interpreting the results
  6. Conclusions
  7. Report

- **Survey**:
  - 22 questions
  - 43 participants
- **Participants**:
  - 43 SJSU students
- **Tools**:
  - Qualtrics
  - Tableau

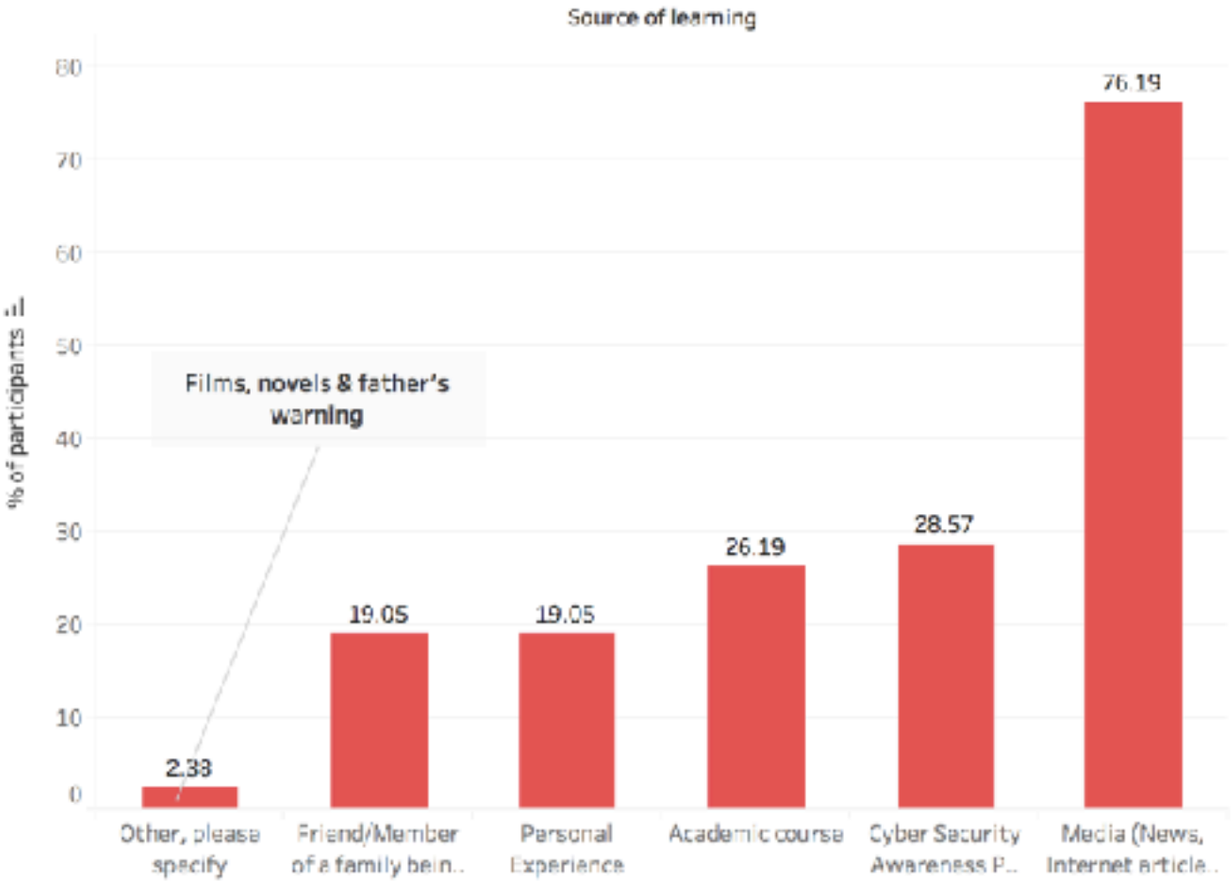
Awareness of Identity Theft (I)

- **97.67%** are aware of identity theft
- Awareness gained from media, academic course, personal experience, films
- Greatest influence from media
- **71%** do not believe information shared on social media is secure
- **95%** think someone may want to steal their identity
- Student believe: Social media = most unsecure, Bank websites = most secure
- **57%** not aware of steps to take following identity theft attack
- **88%** would report attack to concerned organization
- **52%** would report attack to UPD

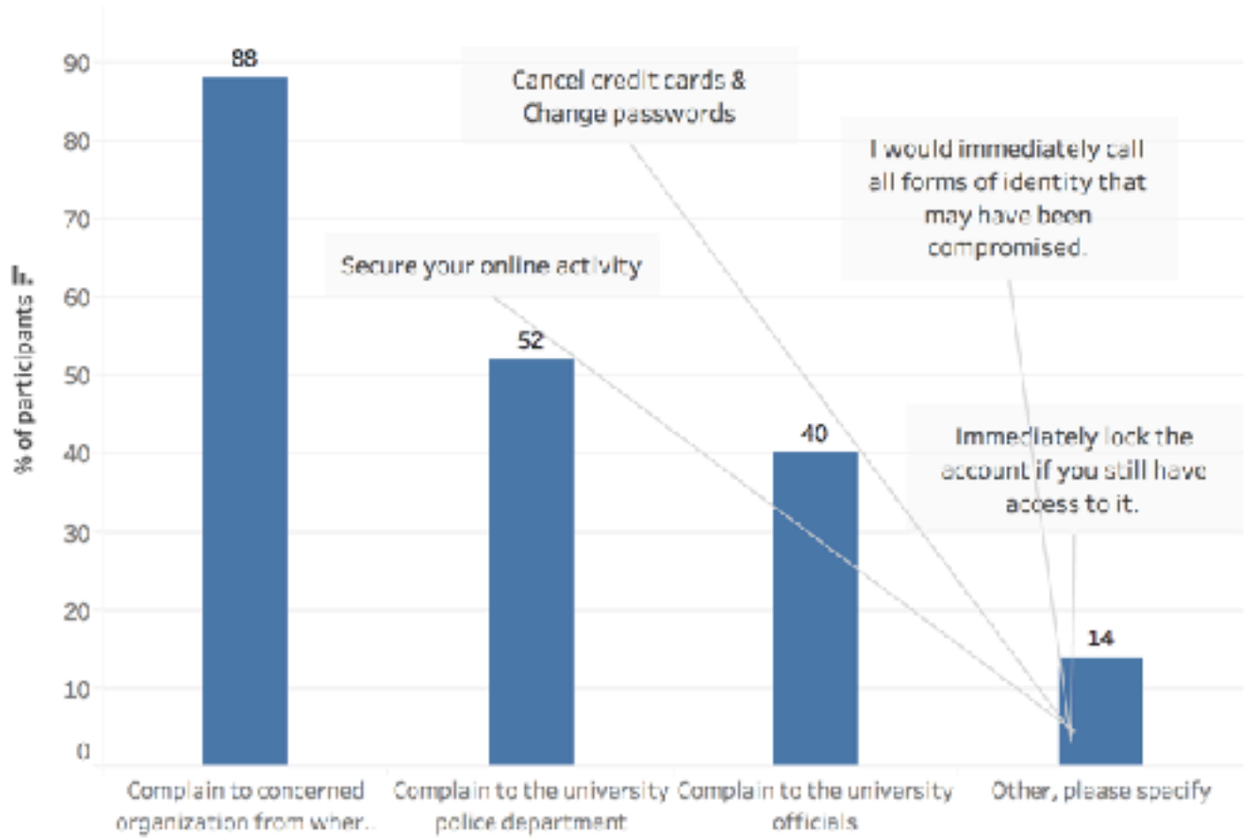
Awareness of Identity Theft (II)

Awareness of Identity Theft

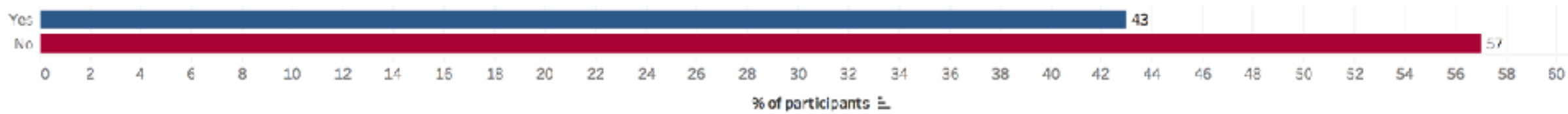
How did you learn about identity theft?



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

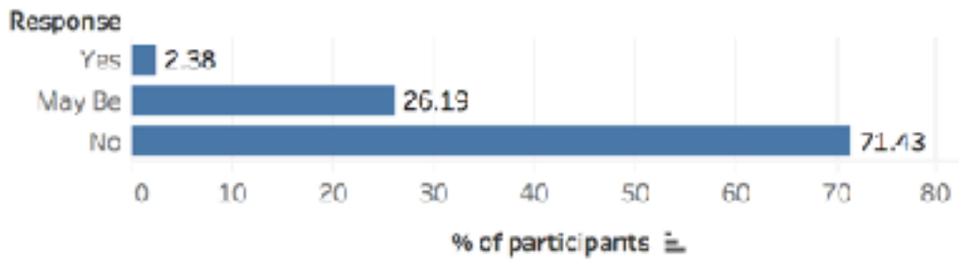


Are you aware of what action needs to be taken if you are a victim of identity theft?

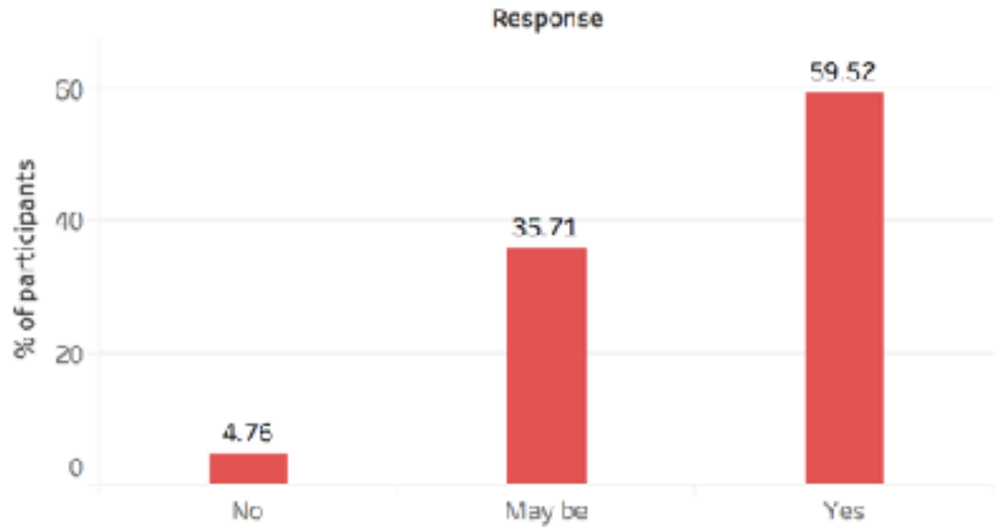


Awareness of Identity Theft (III)

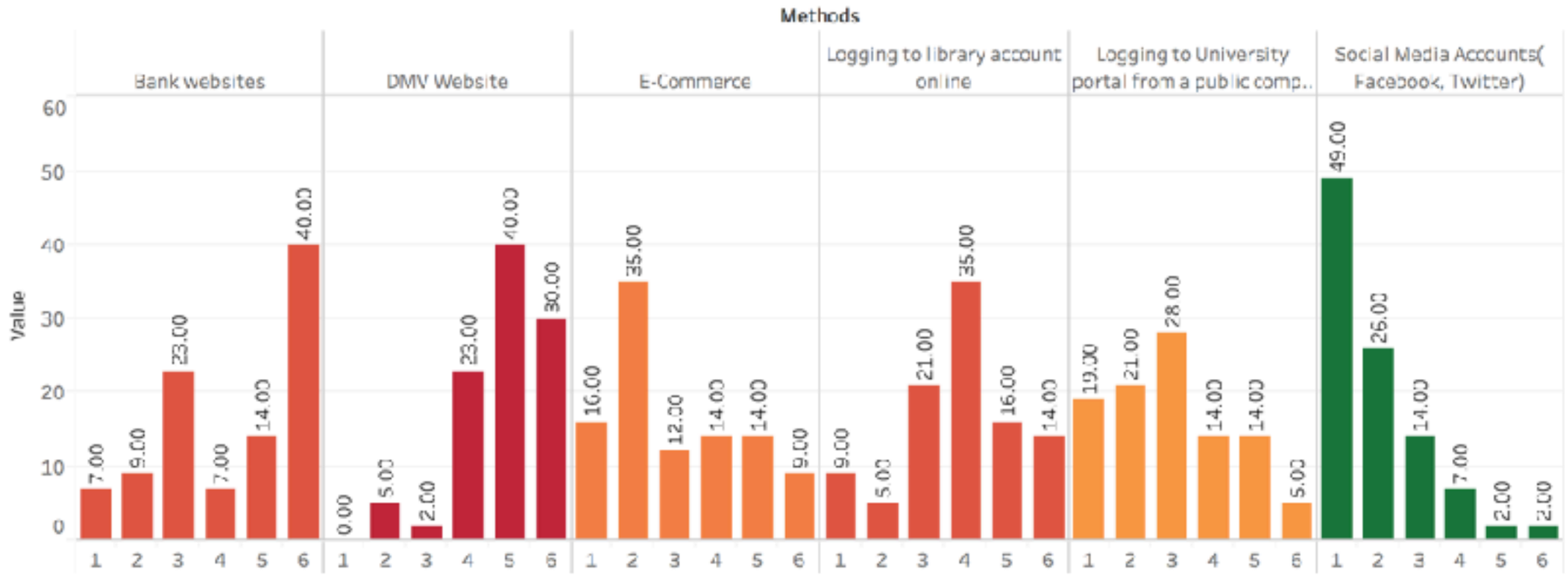
Do you think the information shared on social ook, twitter) is secure?



Do you think anybody would want to steal your identity from social media accounts?



Rank in descending order of likelyhood of your personal information being stolen

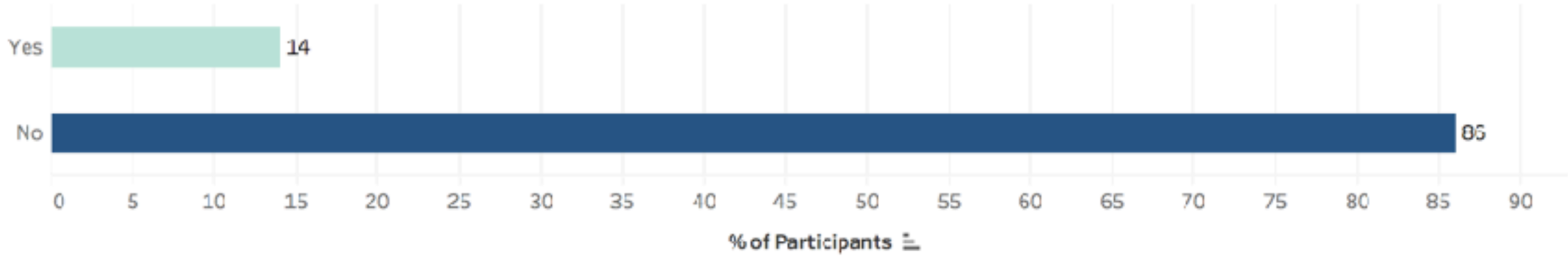


Experience of Identity Theft (I)

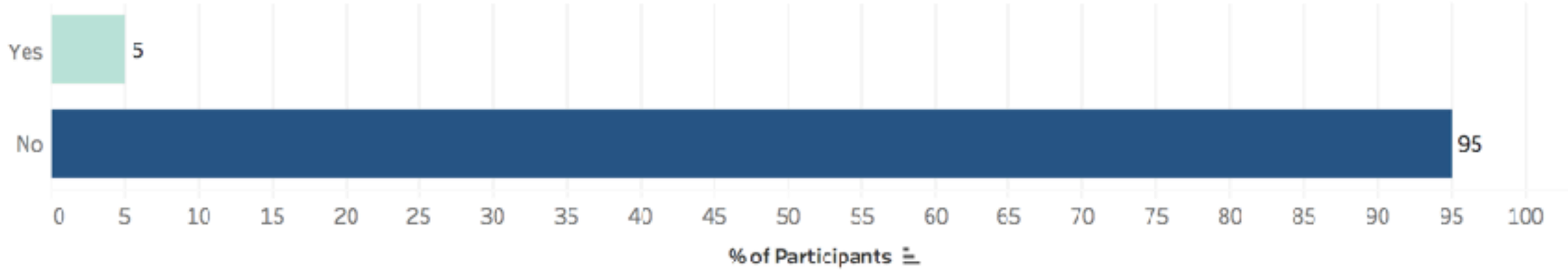
- **5%** experienced identity theft recently
- **14%** shared credentials with trusted 3rd person

Experience of Identity Theft (II)

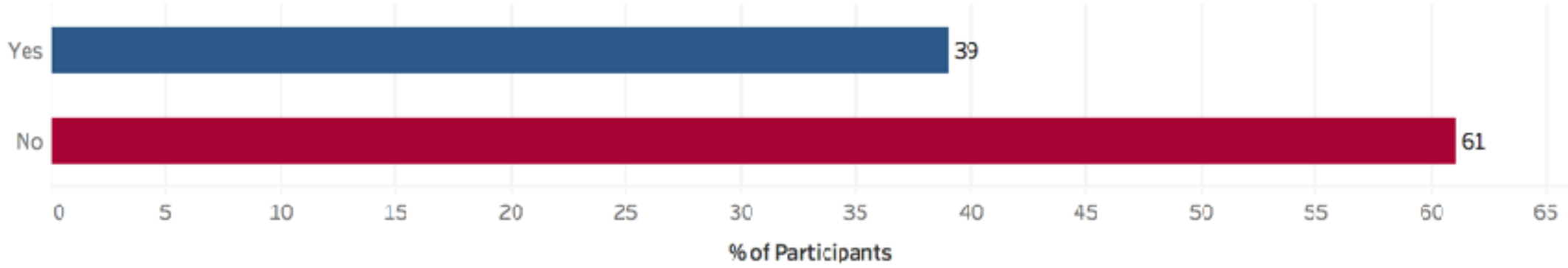
In the past few months, has anybody used your account credentials with your permission on any of the platform?



In the past few months, has anybody used your account credentials without your permission on any of the platform?



Have you changed your password soon after?

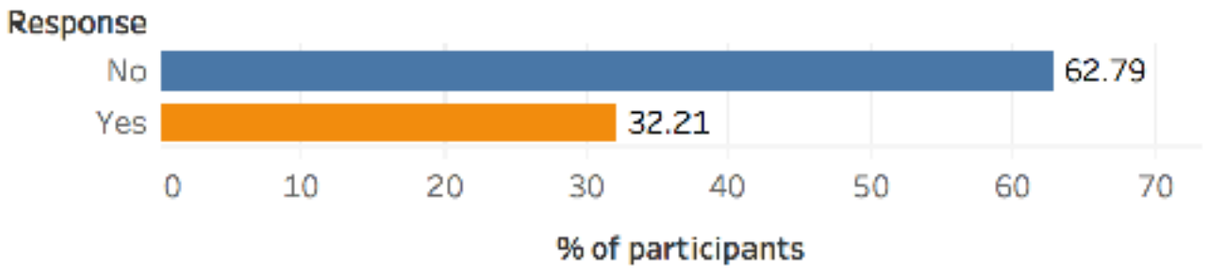


Security-Related Online Behavior (I)

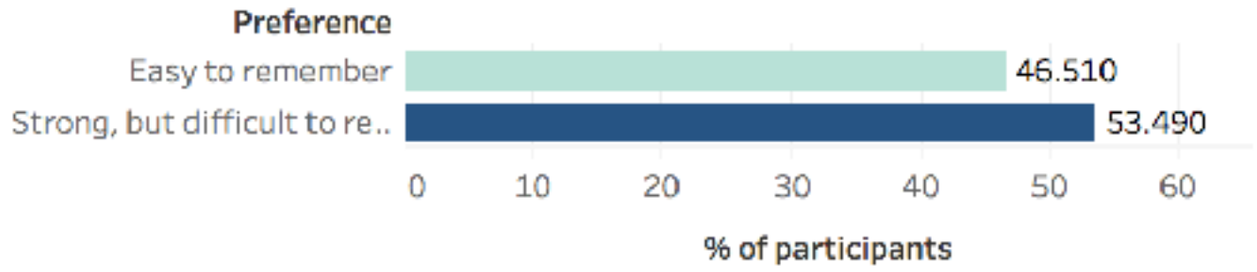
- '**Privacy Paradox**' seen: high awareness but poor behavior for cyber security
- **63%** use different passwords for different accounts
- **46.5%** choose easy-to-remember passwords
- **68%** do not log out of social media websites (considered most insecure platform)
- Only **60%** definitely do log out of all websites maintaining credit card details
- **53%** use two-factor authentication

Security-Related Online Behavior (II)

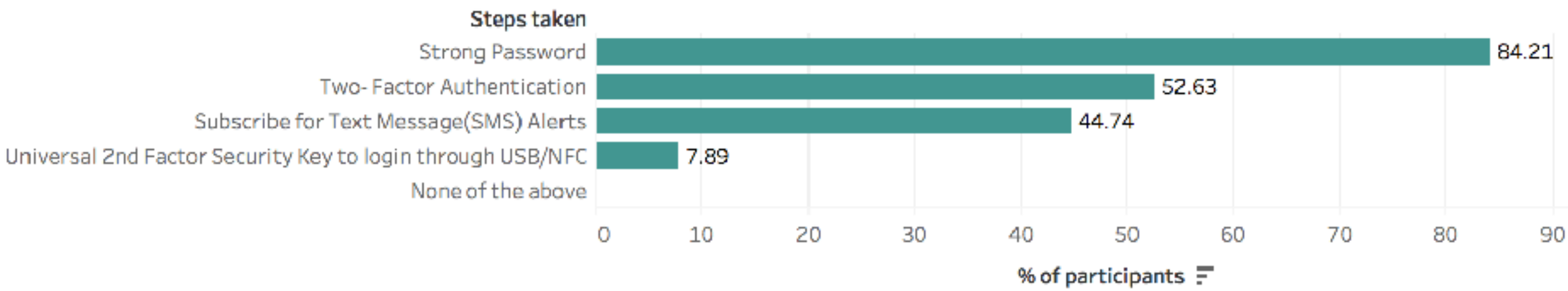
Do you use same password for different type of account?



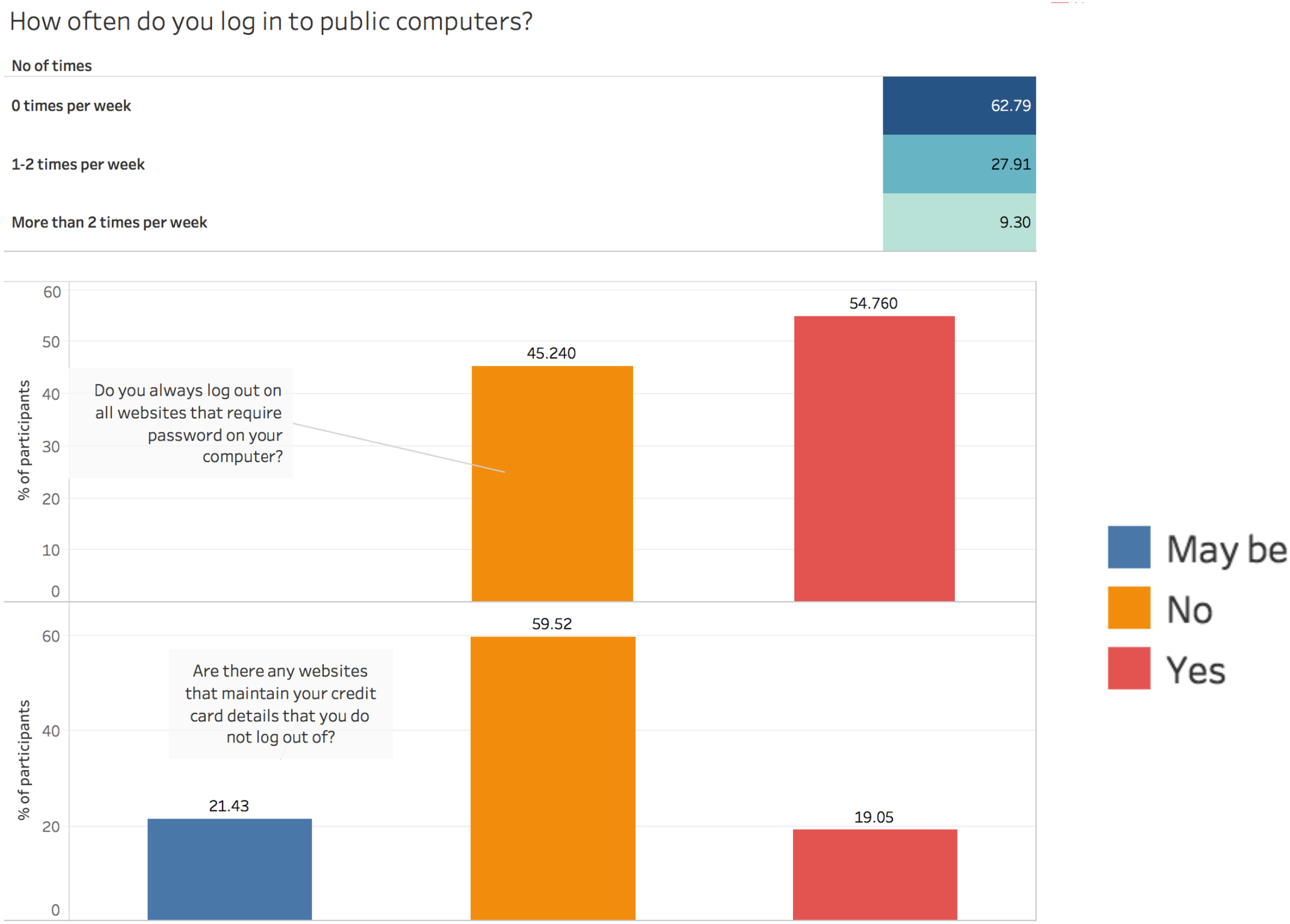
Your preference when you choose a password for an account



What are the actions you have taken to make your social media accounts secure?



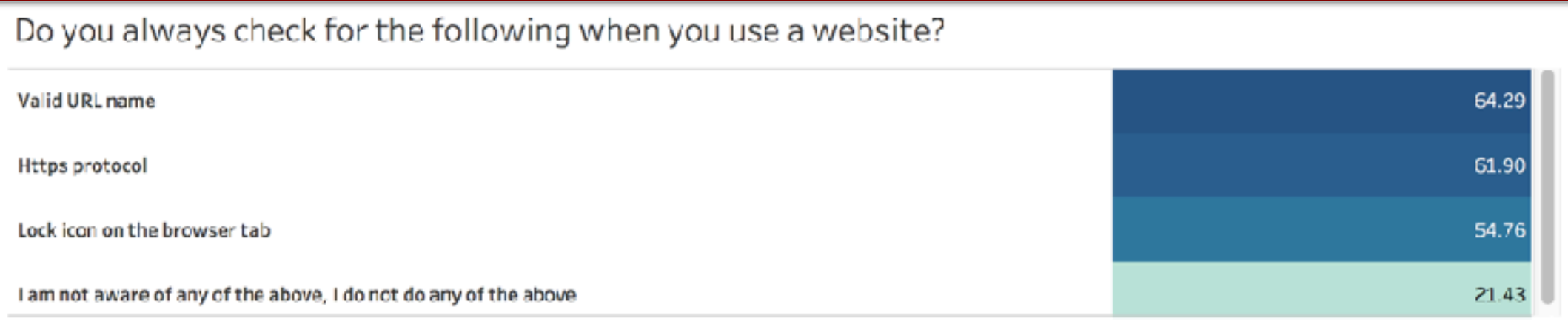
Security-Related Online Behavior (III)

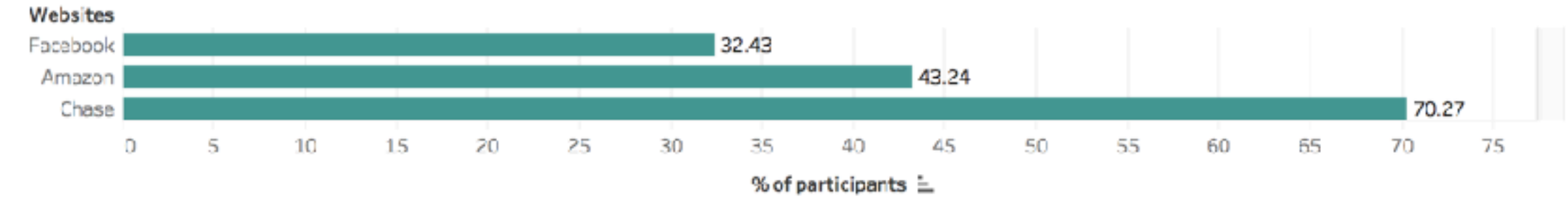


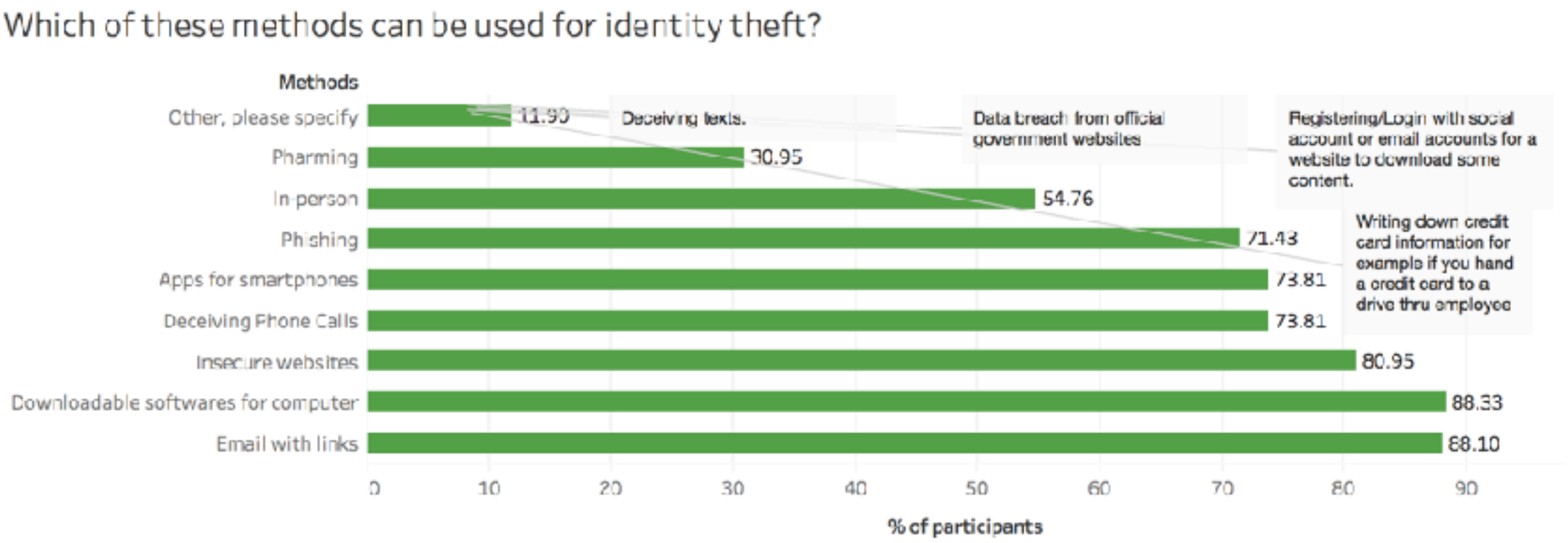
Cyber-Security Knowledge (I)

- **Familiarity** with phishing emails, unsecure websites and downloadable software for identity theft
- **Unfamiliarity** with pharming
- **Poor recognition** of unsecure websites (not using HTTPS, no valid domain name)
- More students **claimed to check** for HTTPS and secure domain name than correctly identified insecure website
- **75%** attended cyber security workshop or seminar

Cyber-Security Knowledge (II)







Conclusions

Awareness of Identity Theft

- High security awareness: 97% aware of concept
- High distrust of social media: 71% believe unsecure

Experience of Identity Theft

- 5% recently experienced identity theft
- 14% shared account credentials

Security-related Online Behavior

- Privacy Paradox demonstrated
- 46.5% choose easy passwords
- 68% log out of social media
- 60% log out of websites storing credit card details

Cyber-security Knowledge

- Poor recognition of unsecure websites (no HTTPS, unsecure domain name)
- High confidence in cyber-security knowledge but poor practical knowledge

Questions

? Identity Theft ?

Appendix: Survey Questions (I)

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

Appendix: Survey Questions (II)

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.