

# RSA<sup>®</sup>Conference2019

San Francisco | March 4–8 | Moscone Center



**BETTER.**

SESSION ID: SEM-M01H

## Humanistic Multi-Factor Authentication (MFA) Why We Don't Use MFA

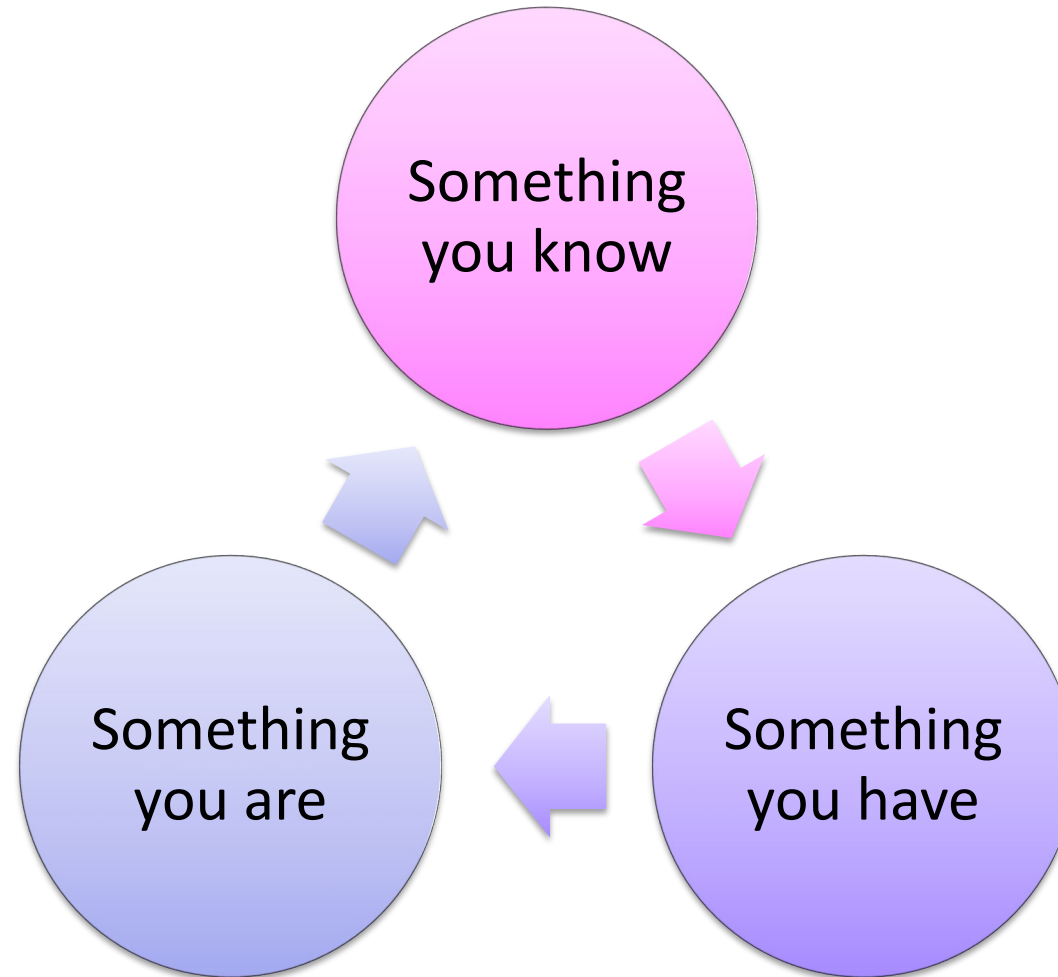
**Sanchari Das**

Doctoral Candidate  
Indiana University Bloomington  
[@sancharidecrypt](#)



#RSAC

# Authentication Technologies



# Are Passwords Secure?

- Reuse Passwords
- Overestimate Password Complexity
- Common Passwords

Rick Wash et al. "Understanding password choices: How frequently entered passwords are re-used across websites". In: Symposium on Usable Privacy and Security (SOUPS). 2016.

Saranga Komanduri et al. "Of passwords and people: measuring the effect of password-composition policies". In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM. 2011, pp. 2595–2604



**RSA**®Conference2019

# Multi-Factor Authentication







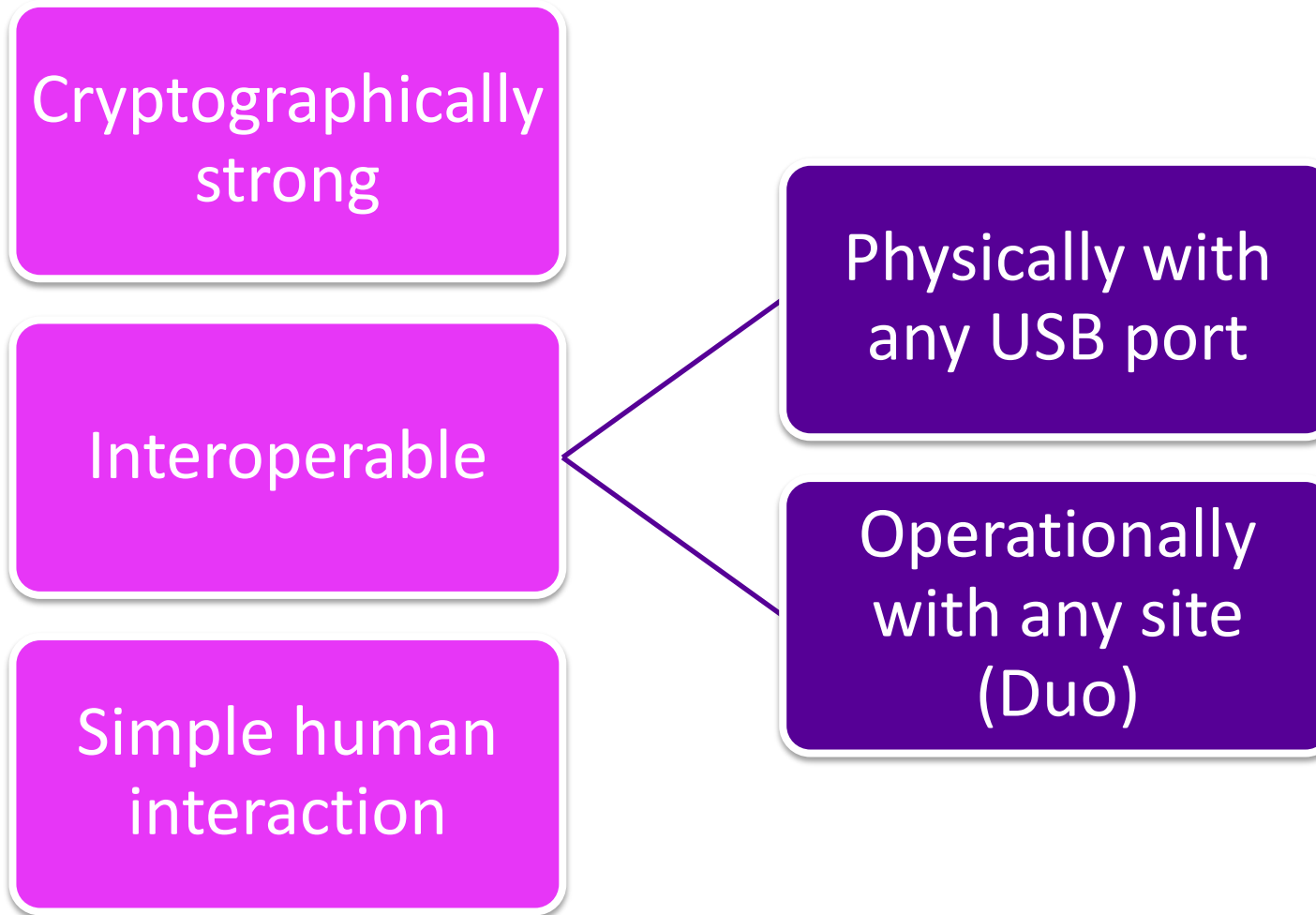
- <https://www.google.com/url?sa=i&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwiumJj--creAhWMulMKHbVvAhQQjRx6BAgBEAU&url=http%3A%2F%2Fwww.technoware.solutions%2Fmulti-factor-authentication&psig=AOvVaw0-GVvXqpJVZ3BFexuUHYsD&ust=1541978038009352>



# A Physical Token to Control Account Access



# Yubico Security Keys



**RSA**®Conference2019

# Brainless





# Identical Experimental Protocol

## Phase I

Initial  
Survey

Think  
Aloud  
Protocol

Exit Survey

Qualitative  
Analysis

Recommendations

Some Adopted

Initial  
Survey

Think  
Aloud  
Protocol

Exit Survey

Qualitative  
Analysis

Recommendations



## Phase II

# Pre-survey Expertise, Demographics, Experience

Have you ever (select all that apply)

- ☐ Designed a website
- ☐ Registered a domain name
- ☐ Used SSH
- ☐ Configured a firewall
- ☐ Created a database
- ☐ Installed a computer program
- ☐ Written a computer program
- ☐ None of the above

- I often ask others for help with the computer.
- Do you know any computer programming languages?
- Have you ever suffered data loss for any reason?  
(ex. Hacking, data corruption, hard drive failure.)



• Rajivan, P., Moriano, P., Kelley, T., & Camp, L. J. (2016). What Can Johnny Do?—Factors in an End-User Expertise Instrument. In *HA/SA* (pp. 199-208).

# Installation Precedes Operation

- Instructions – Yubico & Google
- Task analysis – Think Aloud Protocol
  - Ask what they are doing
  - Identify stop points
  - Mitigate & continue
- Ideally matches your cognitive walkthrough
  - They Never Do





# Interview Questions

- How could you test to confirm that your key is working?
- If your key was lost or stolen, what would you do? (ie. Do you understand the recovery process?)
- Based on your current understanding of the technology, could you use the same key with an account on another web site, or would you need to obtain an additional key?
- Based on your current understanding, could you add a second key to your account?
- Do you see any benefits from using the security key? Please explain.
- Do you expect to continue to use your key after today? Why or why not?
- How would you remove a key from your account if you decided to?
- Do you use alternative emails or file sharing to avoid 2FA?





## Participant Choices – Phase I (Follow Up)

- Participants dropped keys
- None reported continuing use after the study
- They discussed they do not find any value by using the keys to secure their accounts



## Participant Evaluation – Phase I

---

“No, my password is secure enough and alerts are active.”

---

“Why is it still asking for a password?”

---

“Probably not [on] gmail is not important. Would have used for work”.

---

“For my use, No, it is inconvenient to use. The reason is that I don’t have any sensitive information.”



# Analysis



## Transcription

Think aloud results  
Interview questions



## Qualitative coding

Three independent coders  
Create *code book* from  
identified themes  
Set of themes or codes to  
represent all notable data



## Qualitative clustering


Halt Point: participants could  
not move forward without  
help  
Confusion Point: slowed or  
stopped, expressed desire  
for help  
Value perception:  
statements about the  
perceived utility



## Results

Discussion: return to  
transcripts as needed for  
nuance  
Analysis: coding allows  
quantitative as well as  
qualitative  
Recommendations





Gmail and Google Apps x


web.archive.org/web/20160319142602/https://www.yubico.com/why-yubico/for-individuals/gmail-for-indivi

Apps For quick access, place your bookmarks here on the bookmarks bar. [Import bookmarks now...](#)

yubico

WHY YUBICO PRODUCTS SOLUTIONS STORE CUSTOMERS COMPANY SUPPORT

## GMAIL AND GOOGLE APPS FOR INDIVIDUALS




Millions of us rely on our Google Account for access to Gmail, Google Apps, YouTube, Google+, Blogger, and more. We all want our accounts and data to be safe, but traditional login just isn't secure enough in today's world — malware and other attacks steal passwords and hack accounts every day.

Fortunately, you can secure your Google Account easily with Yubico's U2F-compliant YubiKeys. YubiKeys provide an additional secret beyond your password when you access your Google Account. The extra layer of protection is called a second factor or **2-Step Verification**. Even if your username and password (first factor) is stolen, hackers cannot get into your account without having possession of your Security Key (second factor). The only way someone could get in to your account would be to have both your password and your physical key — not very likely!

A stolen Security Key is useless without the account username and password. If a key is lost, a new key can be added to a Google Account and the lost key deleted. You can rest assured your account is secure when it's protected by a YubiKey.

GOOGLE FOR WORK  
GOOGLE FOR EDUCATION  
**GMAIL AND GOOGLE APPS**  
GITHUB  
DASHLANE  
DOCKER  
DROPBOX  
IDENTITY & ACCESS MGMT  
PASSWORD MANAGEMENT  
SALESFORCE  
ENTERPRISE PARTNERS  
WHITE PAPERS



Buy YubiKey 4

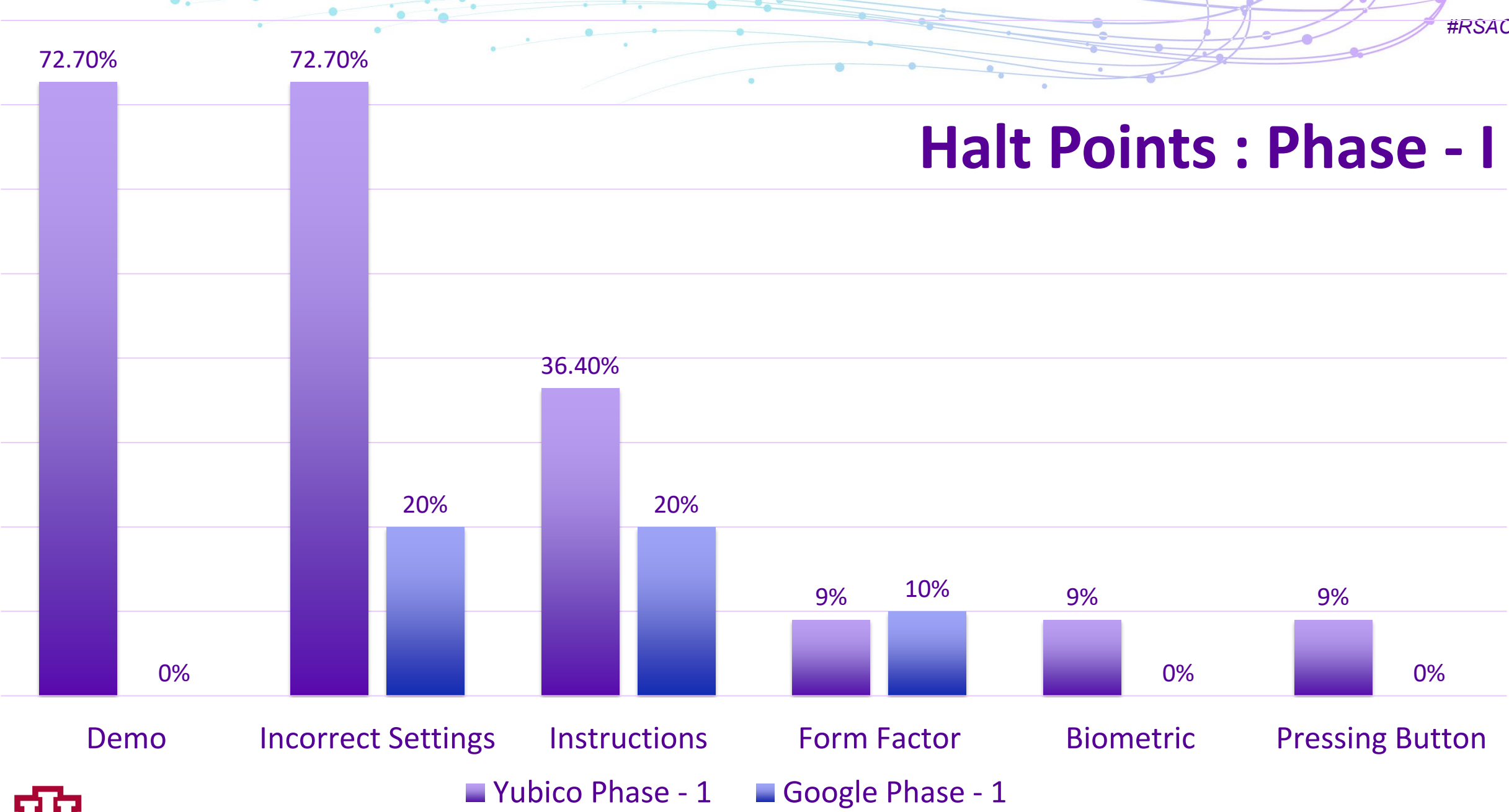
Buy YubiKey 4 Nano

# Phase-I Setup Instructions

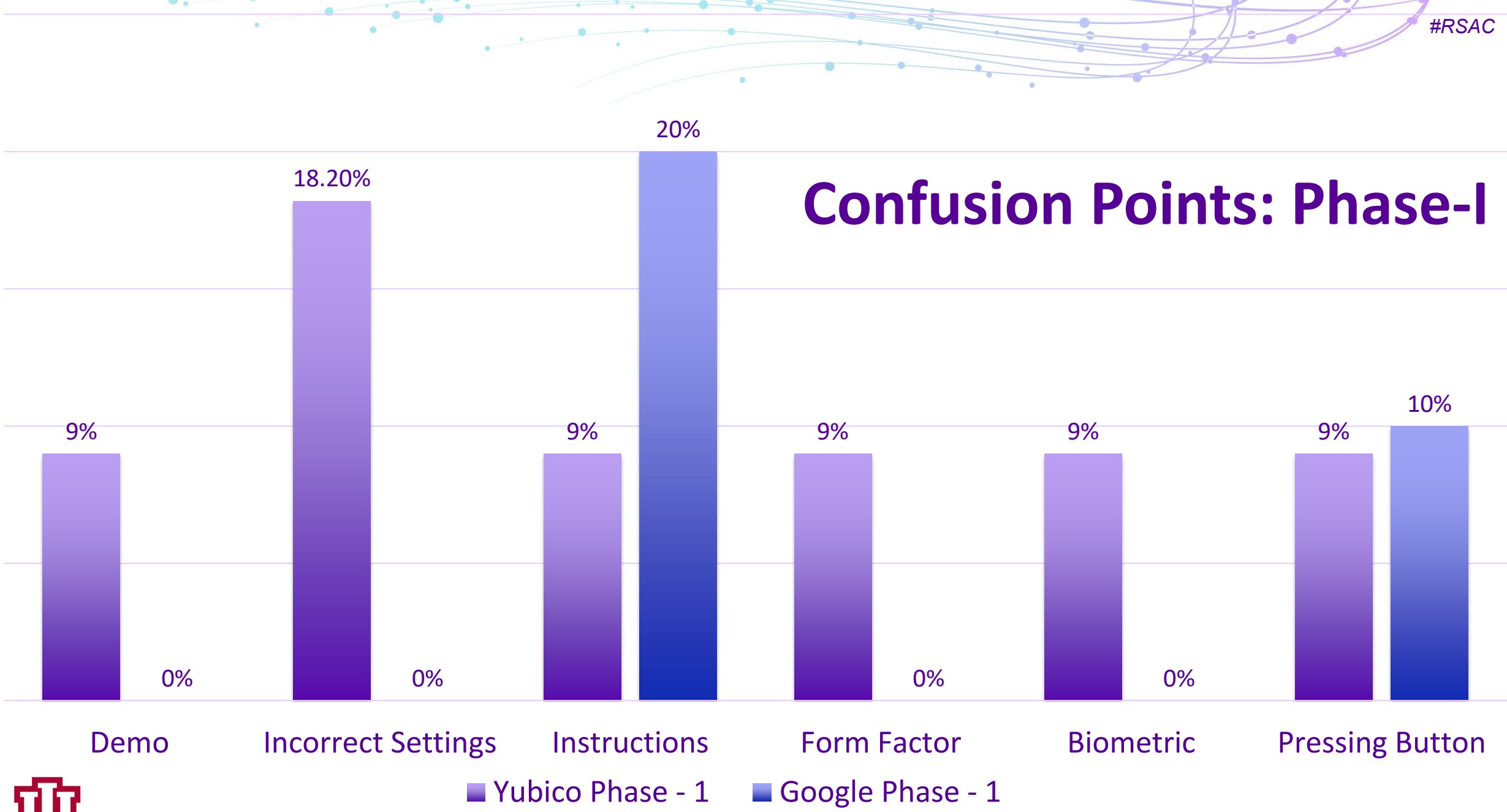




# Halt Points : Phase - I



# Confusion Points: Phase-I



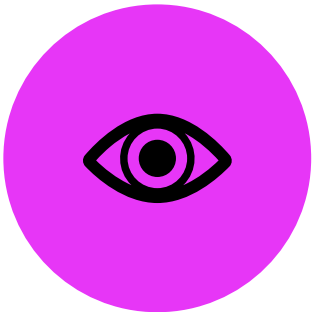
# Adopted Recommendations



**Demo versus reality**



Correctly identifying the device



Biometric versus touch



Finding Instructions



# User Approval and Device Use

1

Enter username and password in the login field of any app that supports FIDO U2F.

2

Insert the Security Key in a USB port with the **gold side up**.

3

Touch the gold button on the Security Key to generate the secure login credentials.





# Phase-II Instructions

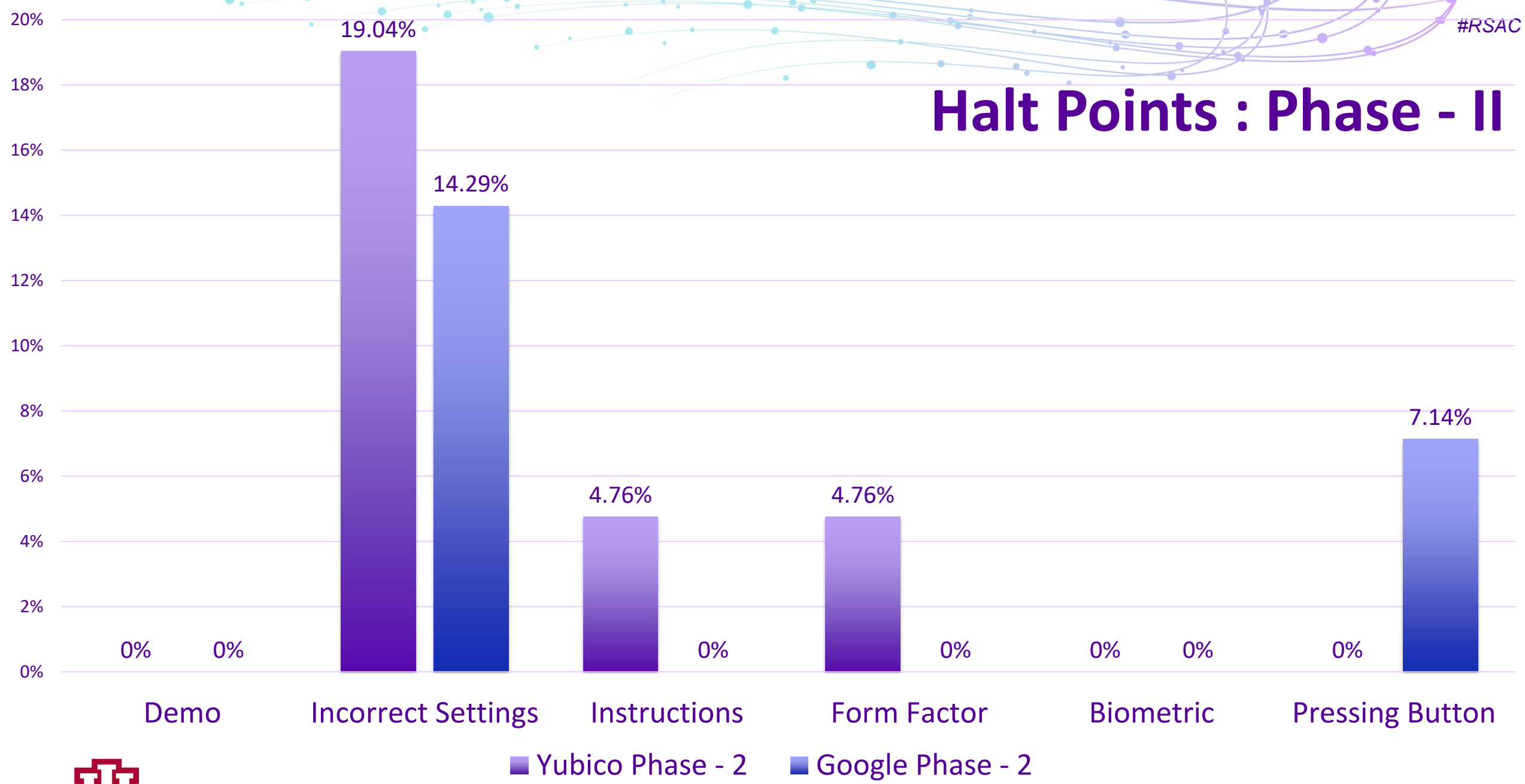


## REQUIREMENTS

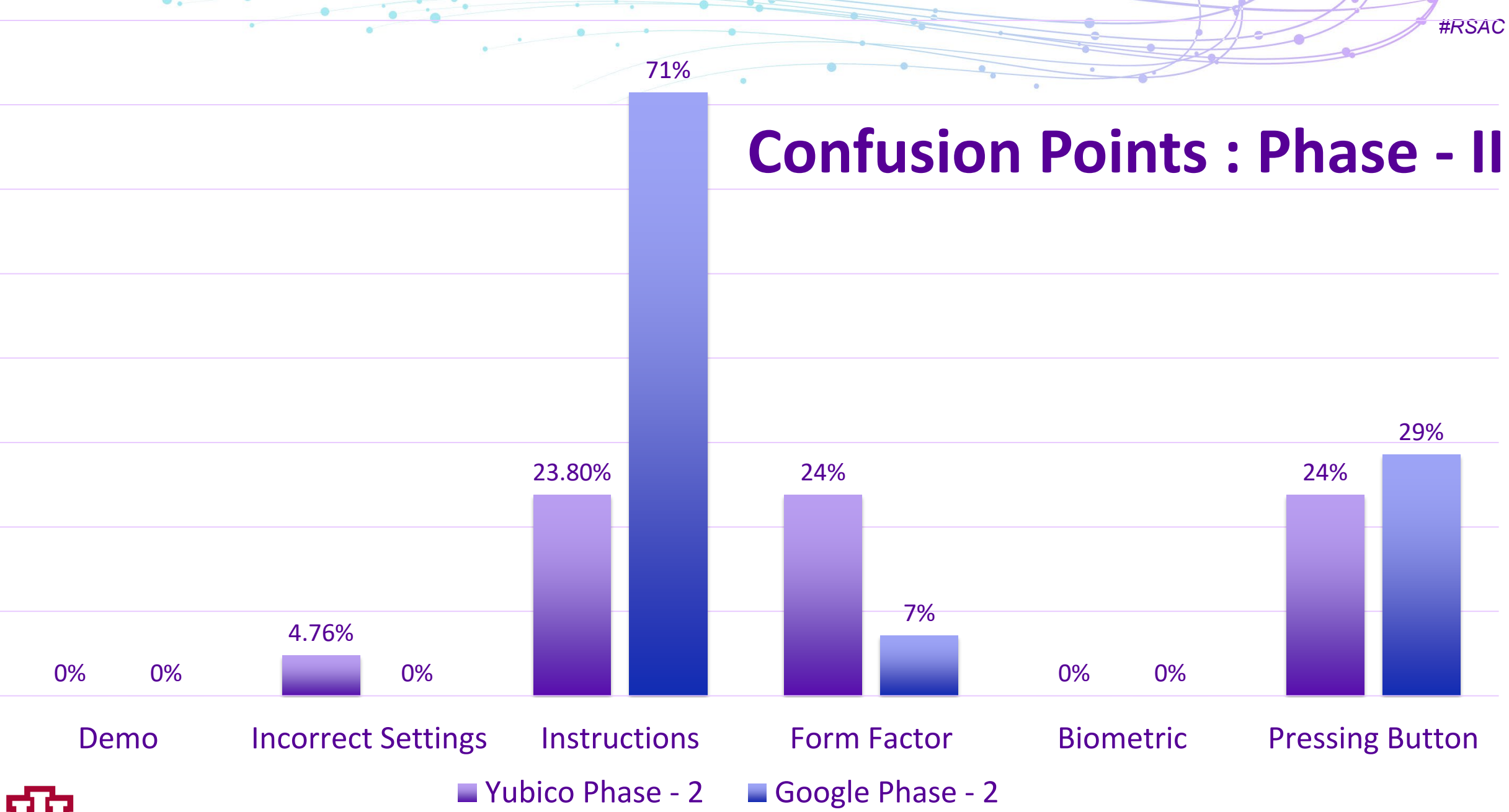
Version of Google Chrome browser (or at least version 38)  
YubiKey, YubiKey 4, YubiKey 4 Nano, YubiKey NEO, or other  
operating system (the YubiKey button is a **capacitive sensor**, not a biometric sensor)  
Google Account (such as Gmail, Google Apps, YouTube, Google Plus,



# Halt Points : Phase - II



# Confusion Points : Phase - II



## Participant Evaluation – Phase II

---

“I find it much easier to use on Duo (2 factor) instead of using my phone. I just keep it in my laptop case.”

---

“It's a convenient way of utilizing two factor authentication without needing to look at my mobile device.”

---

“Improve ease of access for me.”

---

“...I don't use it much because I almost never use a computer that is not my personal computer and the account that I set it up with is not one that I need to access very often anyway.”

---

“Too lazy.”





**RSA**®Conference2019

# Scope of Improvement



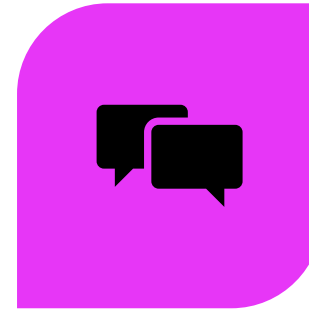
## Recommendations - Phase-II



**INSTRUCTION  
CLARITY**



**CONFIRMATION OF  
INSTALLATION**



**COMMUNICATE THE  
INTRINSIC BENEFIT**



**COMMUNICATING  
THE RISKS**



# RSA<sup>®</sup>Conference2019

**Sanchari Das**, Andrew Dingman, and L. Jean Camp.

"Why Johnny Doesn't Use Two Factor A Two-Phase Usability Study of the FIDO U2F Security Key."

*2018 International Conference on Financial Cryptography and Data Security (FC)*

**Sanchari Das**, Andrew Dingman, Gianpaolo Russo, Jayati Dev, Olivia Kenny,  
L. Jean Camp

"A qualitative study on usability and acceptability of Yubico security key."

*Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust.*

ACM, 2018.

# Why We Don't Use MFA -- Solutions

- Hassle
  - Providing the technology is not enough
- We cannot predict
  - Watch in-action
- Why use? Too Lazy
  - Risk communication for motivation
- Research, Application
  - Qualitative studies and Quantitative Studies





# RSA<sup>®</sup>Conference2019

Thank You!



Questions?

**sancdas@iu.edu**  
**@sancharidecrypt**