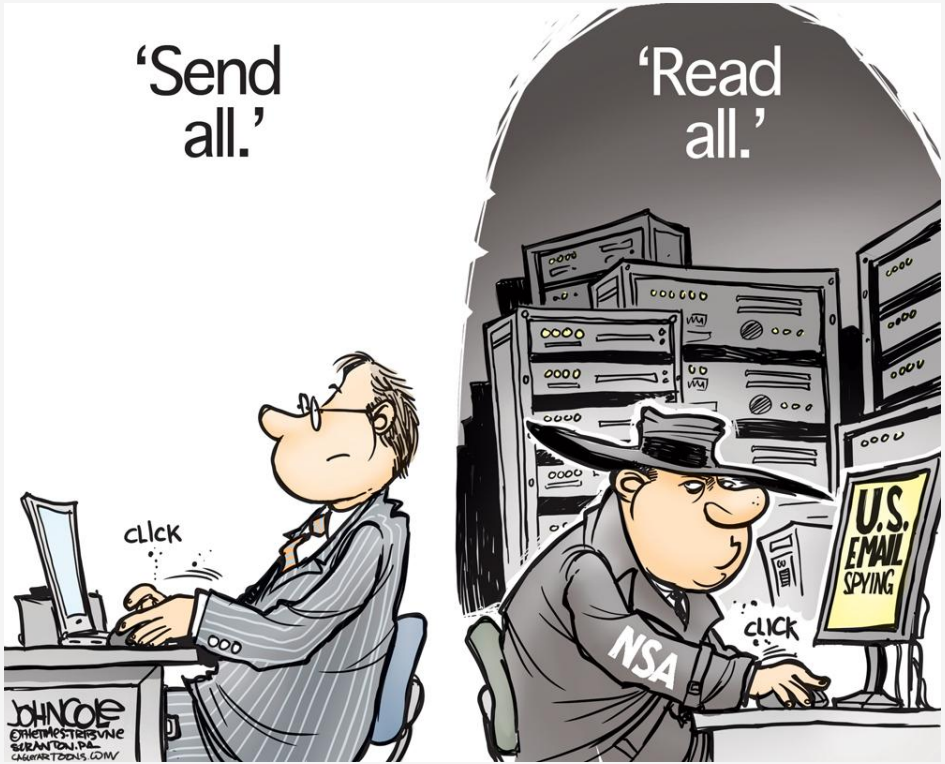
# Action Needed! Helping Users Find and Complete the Authentication Ceremony in Signal

Elham Vaziripour, Justin Wu, Mark O'Neill, Daniel Metro, Josh Cockrell, Timothy Moffett, Jordan Whitehead, Nick Bonner, Kent Seamons, Daniel Zappala

Brigham Young University

Internet Research Lab

# Importance of Secure Messaging



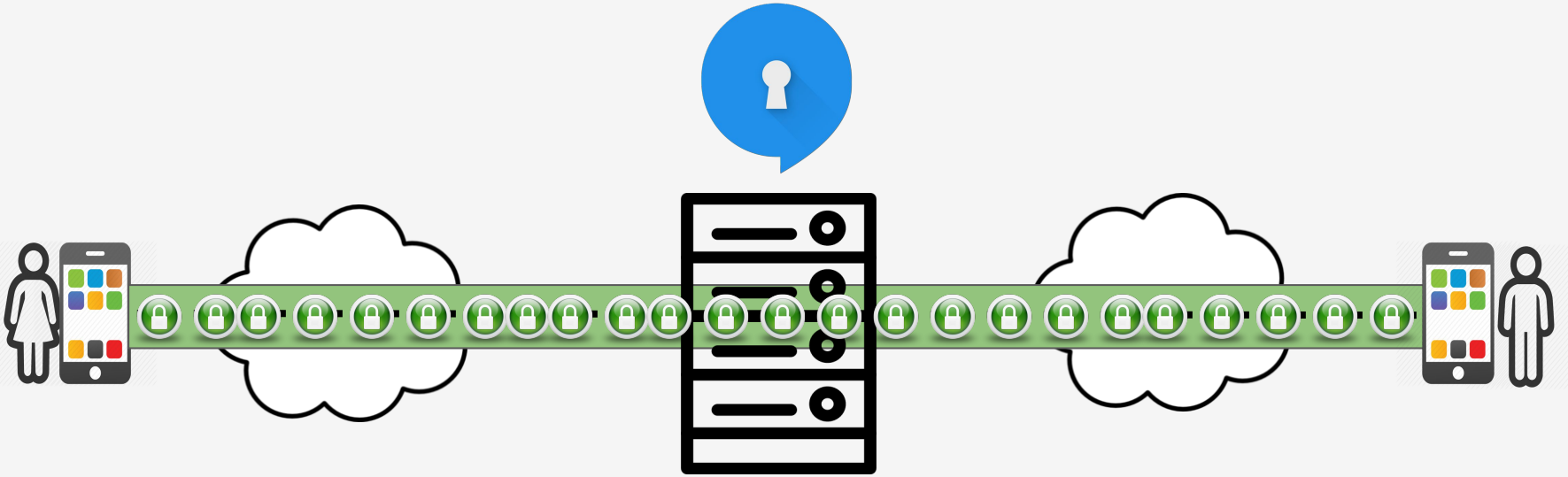

THE HILL

TECHNOLOGY

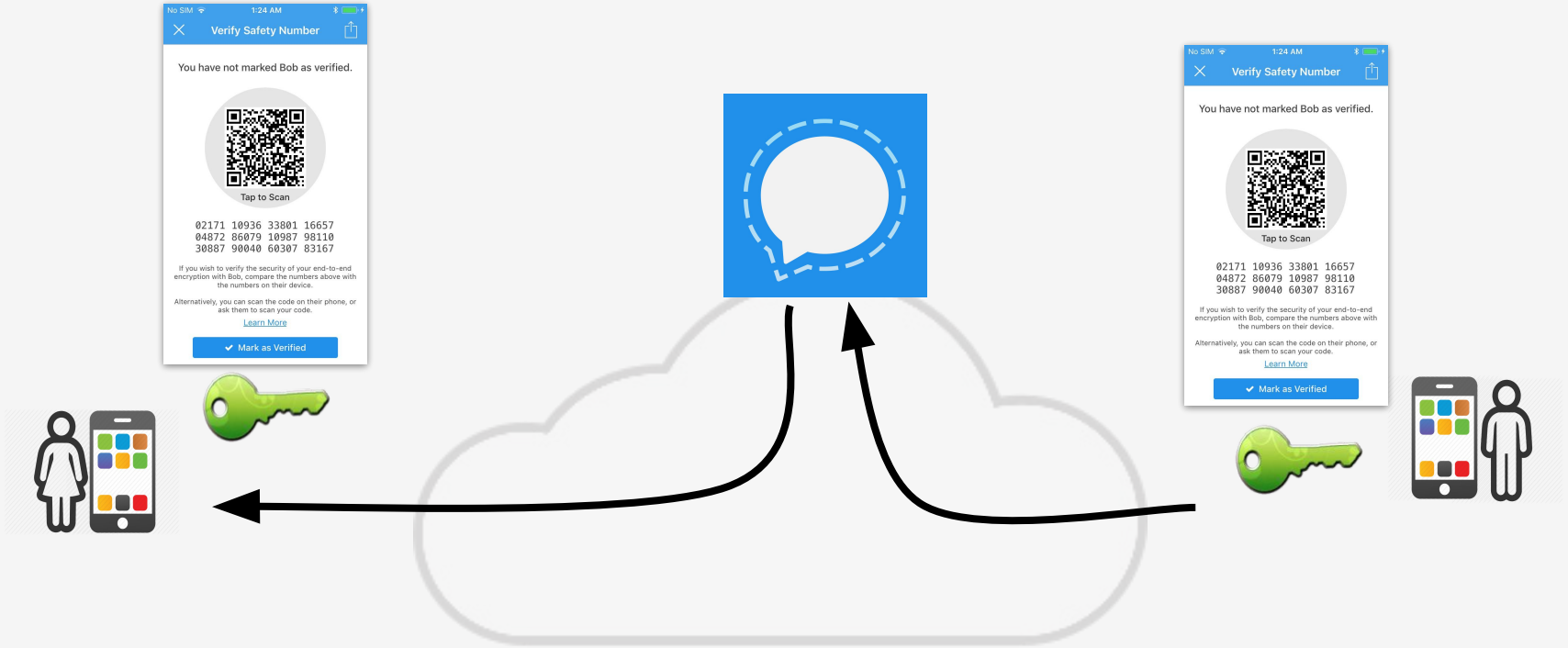
February 14, 2017 - 01:31 PM EST

## Trump staffers using app that deletes their messages: report

# End-to-End Encryption is a Solution

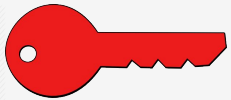


# Verify the Identity Key



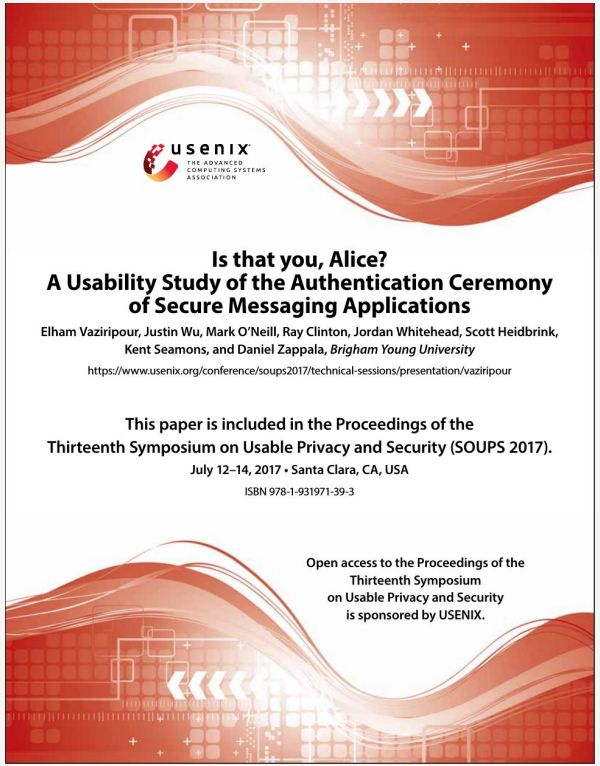
# Verify the Identity Key





# Last year at SOUPS...

- Users have a hard time finding and completing the authentication ceremony without instruction
  - 14% success rate with no instruction
  - 78% success rate with instruction
- It takes too long to complete the ceremony even with instruction
  - 7 minutes, average time to find
  - 11 minutes , average time to complete



# How Can We Help People To Quickly Find and Use the  Authentication Ceremony in Secure Messaging Applications, Without Instruction?

# Our Approach

- Opinionated design: *Make more decisions and leave fewer options* (1)
- Encourage the user to be security minded
    - Nudges (2)
    - Monetary incentive

---


1. A. P. Felt, A. Ainslie, R. W. Reeder, S. Consolvo, S. Thyagaraja, A. Bettes, H. Harris, and J. Grimes. Improving SSL warnings: Comprehension and adherence. In Conference on Human Factors in Computing Systems (CHI), pages 2893–2902. ACM, 2015.
2. A. Acquisti, I. Adjerid, R. Balebako, L. Brandimarte, L. F. Cranor, S. Komanduri, P. G. Leon, N. Sadeh, F. Schaub, M. Sleeper, et al. Nudges for privacy and security: Understanding and assisting users' choices online. ACM Computing Surveys (CSUR), 50(3):44, 2017.

# Our Approach

- Follow design principles from Schroder et al. - EuroUSEC 2016

  (1) Awareness of the security status of conversations

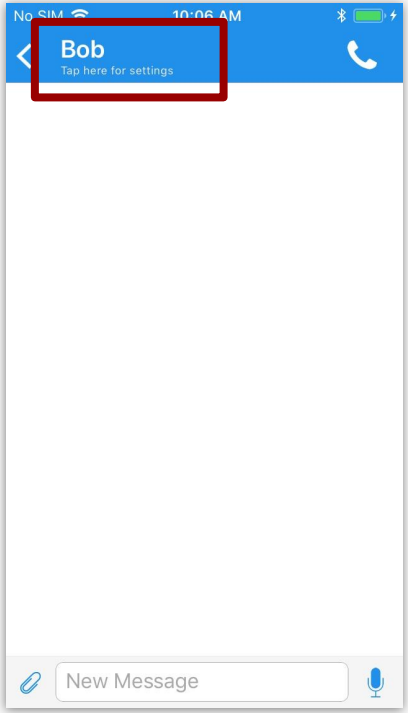
  (2) Comprehensible instructions for recommended actions

  (3) Clear risk communication

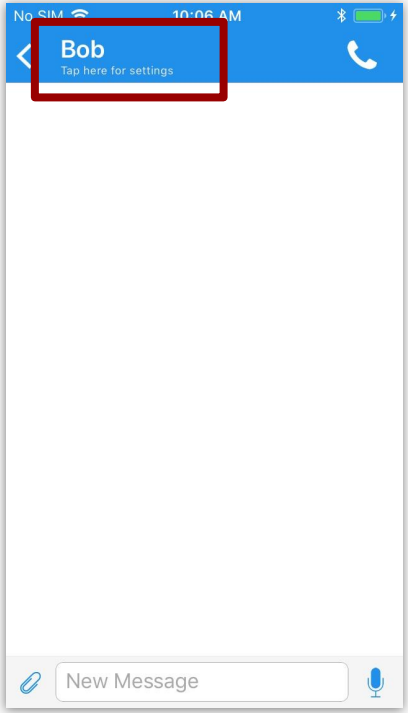
  (4) Easily accessible verification

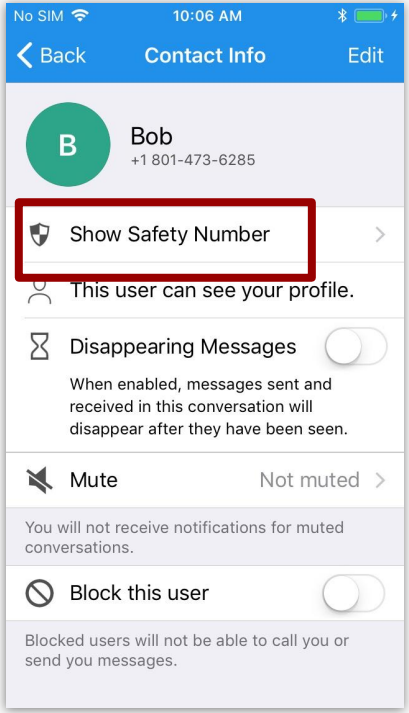
# Original Signal

# Current path to find and use the authentication ceremony in Signal

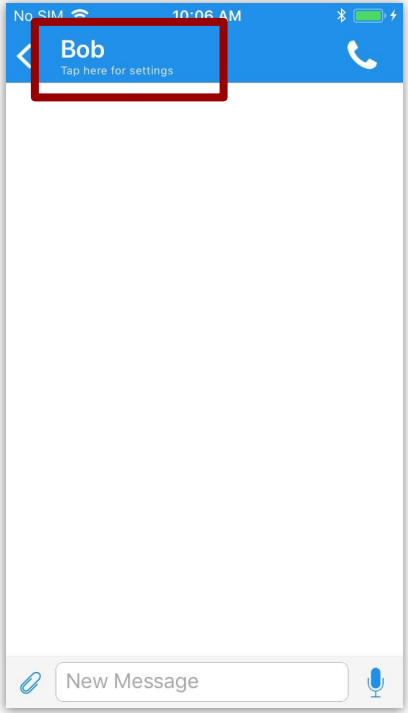


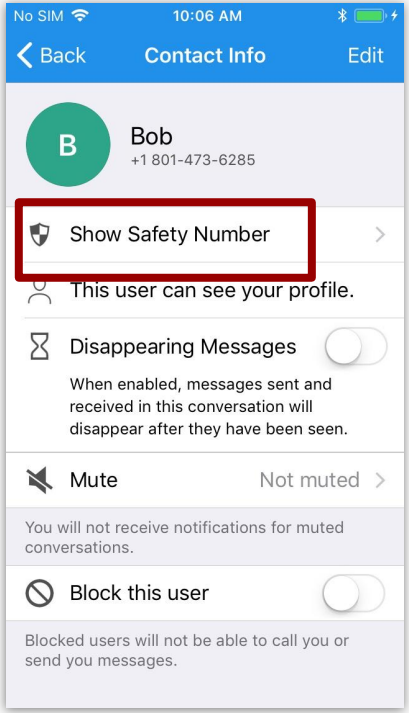
# Current path to find and use the authentication ceremony in Signal



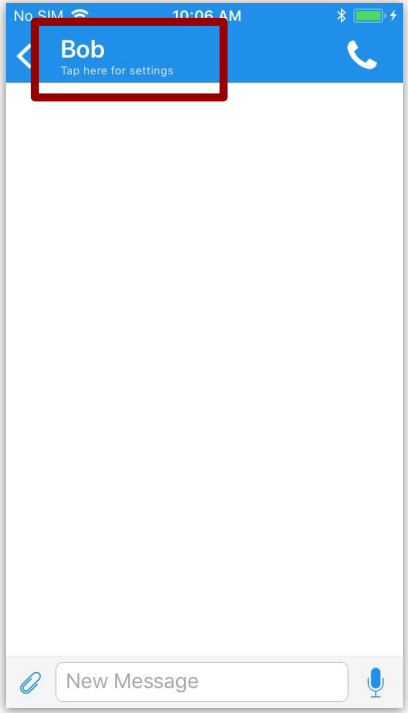



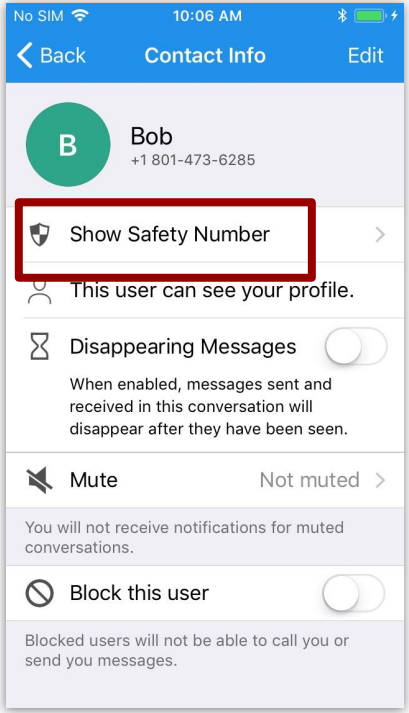
# Current path to find and use the authentication ceremony in Signal



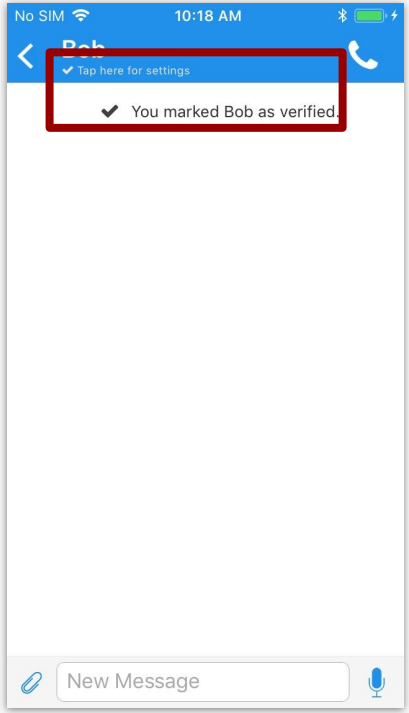




# Current path to find and use the authentication ceremony in Signal



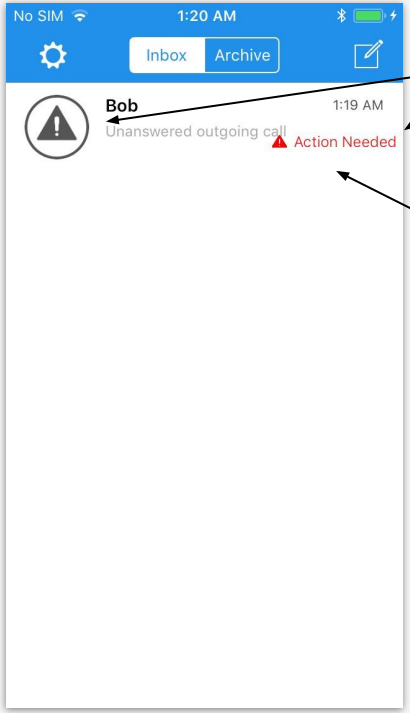







# Modification 1

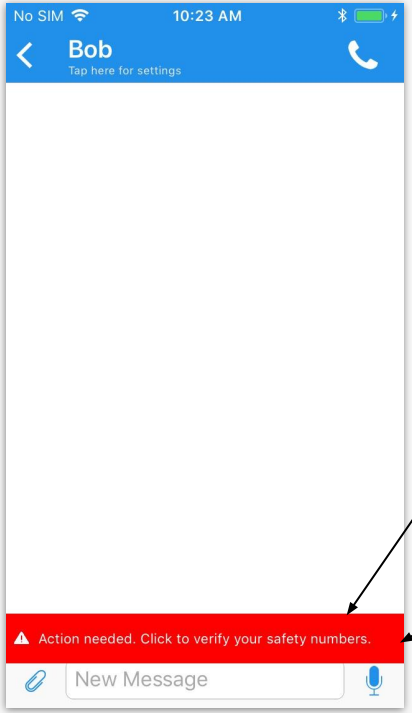
# Modification 1




(1) Awareness of security status

(4) Easily accessible verification

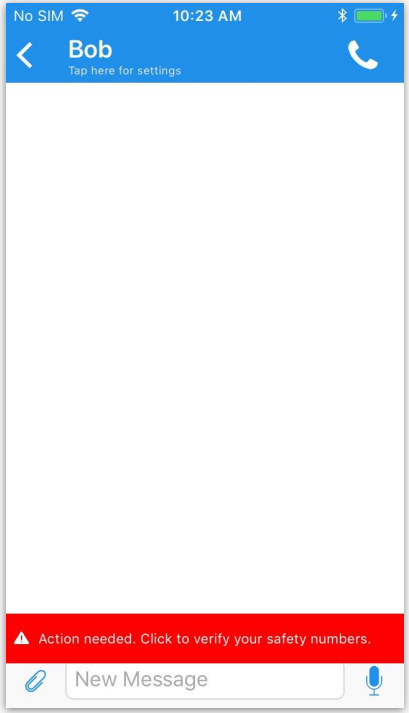
# Modification 1

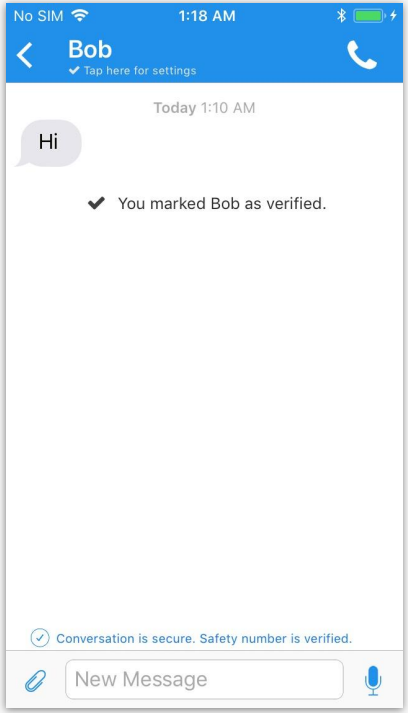

(1) Awareness of security status
(4) Easily accessible verification

(3) Comprehensible instructions

# Modification 1

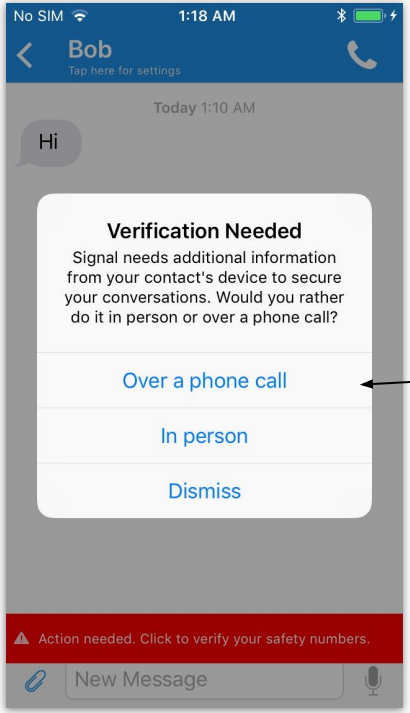







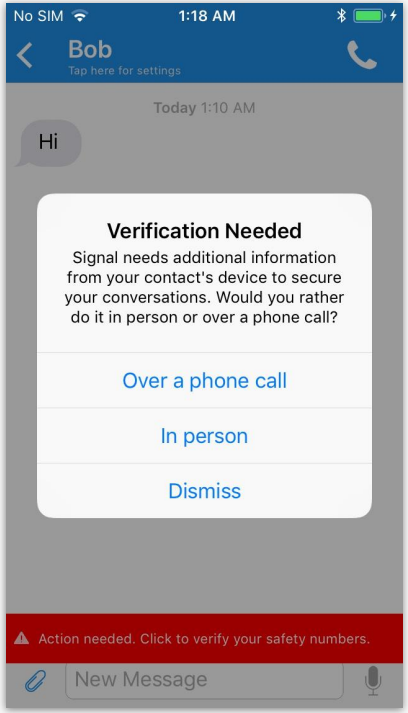
# Modification 2

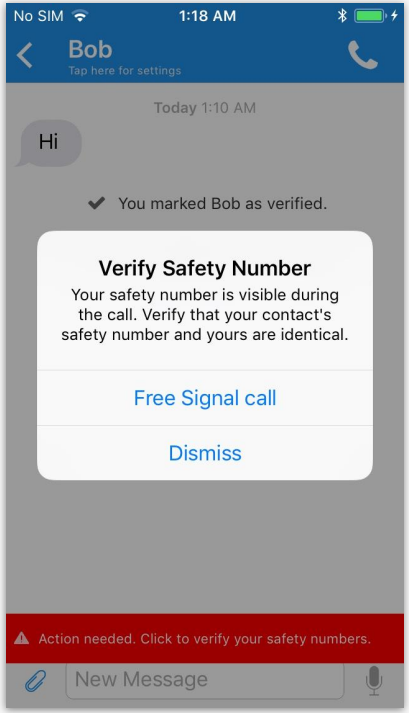
# Modification 2

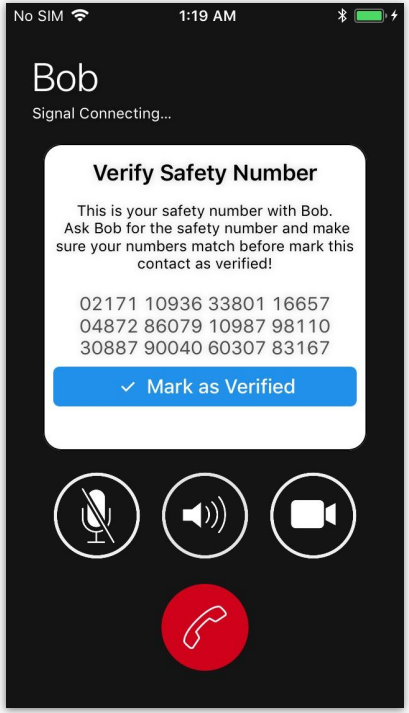


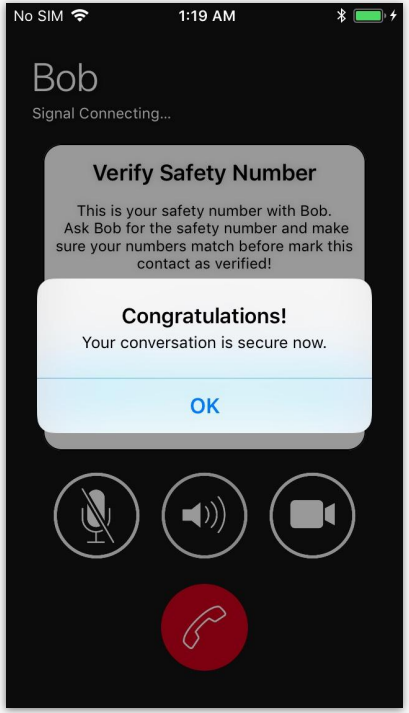

(3) Comprehensible instruction

# Modification 2 (Over a phone call)

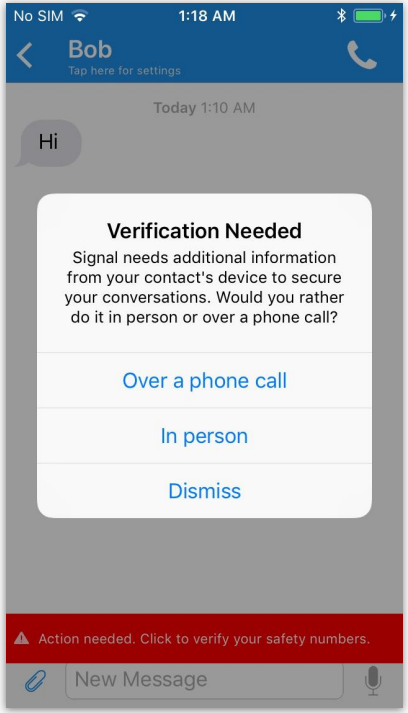


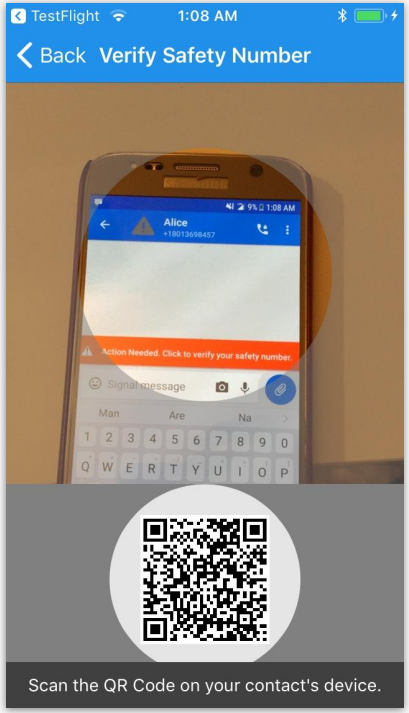



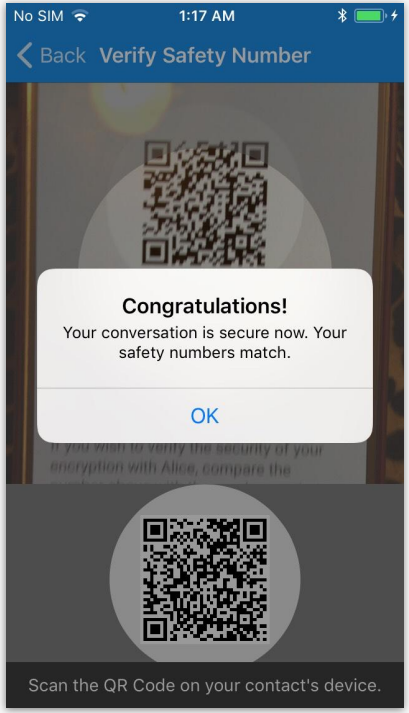



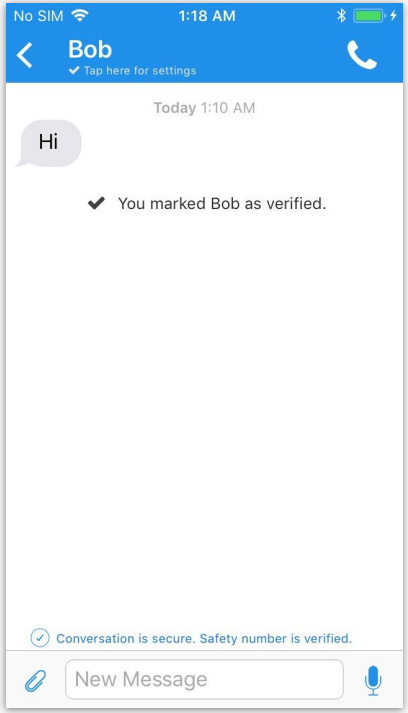



# Modification 2 (In person)



# Lab User Studies to Evaluate the Modifications

# Methodology

- Participants signed up in pairs (30 pairs total)
- Versions cycled through in round robin manner
- 10 pairs for each version
- During the study:
  - One participant was told to send a credit card to the other
  - Participants were given $7 with a $3 bonus to make sure the credit card number is transferred safely
  - Afterward, they filled out a survey and were asked questions about their comprehension

# Results: Find and Complete Ceremony

| | Completion Rate (Self-Reported) | Found (Coordinator-Reported) | Completion Rate (Coordinator-Reported) |
|---|---|---|---|
| Original Signal | 50% | 25% | 0% |
| Modification 1 | 90% | 100% | 30% |
| Modification 2 | 60% | 95% | 90% |

- Half of the participants who used the original Signal, and the majority of participants who used the modified versions, *believed* that they completed the task safely
  - Original: none successfully performed the authentication ceremony
  - Modification 1: majority clicked the toggle before verification

# Confusion Regarding the Original Authentication Ceremony

"I was a little confused at first and I wondered if we needed to **be in the same room** to scan the QR code to make sure our conversation was secure.
At the bottom it **just asked if I could switch the conversation to verified and so I did.**"

"I hit [the button] and then I was like, 'well that did nothing' and so I hit it again and nothing happened...I hit verify and then it says that I just **unhit it immediately afterwards.**..I was just like, 'verify what? **What am I verifying?'** It didn't really tell me...Honestly it meant nothing."

# No Need for Instructions

| | | | |
|---|---|---|---|
| Prior Study | | WhatsApp<br>Facebook Msgr<br>(with instruction) | Viber<br>(with instruction) |
| This Study | Modification 1<br>(without instruction) | | Modification 2<br>(without instruction) |
| Completion Rate | 30% | 70% | 90% |

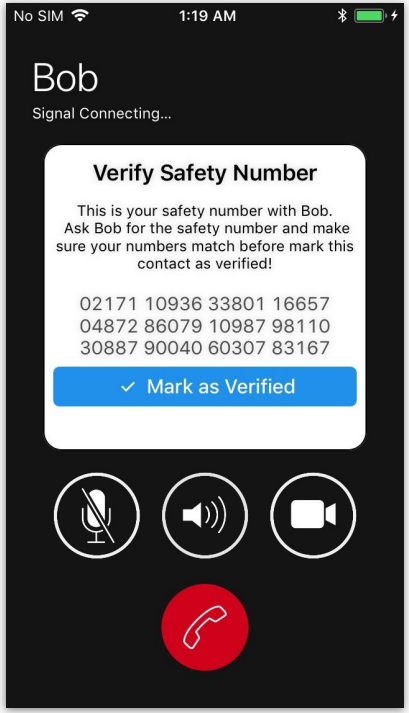
# Result: Timing

- Modification 1: time to locate ceremony drops to under a minute
- Modification 2, time to complete the task drops in half
- Between modification 2 and the previous study, time drops from 11 to 4.5 minutes

| Application | Time to Find the Authentication Ceremony | Completion Time |
|---|---|---|
| Original | 3.5 | N/A |
| Modification 1 | < 1 | 7 |
| Modification 2 | < 1 | 2 |

# Authentication using a Phone Call

"I liked that it came up on the **middle of the phone call screen** rather than being sent through a text message that I would have to pull up during the conversation.
There were **a lot of numbers**, which could be **hard to keep track of if you were reading them over the phone**, but the amount of numbers ensures greater safety."



# Result: Comprehension

- Participants were asked about the purpose of the authentication ceremony
- Even though some expressed understanding of authentication and confidentiality, many of these participants were still unsure of their answers.

| Code | Original | M1 | M2 |
|---|---|---|---|
| *(A) Survey* | | | |
| Authentication | 3 | 4 | 6 |
| Confidentiality | 2 | 2 | 3 |
| Security | 0 | 6 | 7 |
| Trust | 0 | 2 | 1 |
| Didn't know | 0 | 7 | 5 |
| *(B) Interview* | | | |
| Authentication | 7 | 7 | 6 |
| Confidentiality | 3 | 6 | 7 |
| Security | 2 | 1 | 2 |
| Trust | 2 | 0 | 0 |
| Didn't know | 5 | 7 | 5 |

# Result: Adoption

*Are you willing to use the authentication ceremony before you exchange messages with a friend the first time?*

- Yes: 32
- No: 4
- For confidential information: 14
- Certain contacts: 6

"**Am I willing? Yes. Will I? No**. Because here is the thing, I don't really care if my messages get intercepted because most of the time I am not sending my credit card number or social security numbers. Will I use it for things that are really important? For sure."

# Conclusion

- Finding and completing the authentication ceremony improves
  - Using opinionated design
  - Using nudges
  - Apply design principle
  - Encourage to be security minded
- Improvement made with no instructions
- Time to find and complete the ceremony is significantly shorter

# Future Work

- Improve risk communication
- Determine the importance of comprehension
- Encourage people to be security-minded without monetary incentive
- Apply lessons learned to attack scenarios
- Find ways to automate the authentication ceremony