RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: IDY-T07

Studies of 2FA, Why Johnny Can't Use 2FA and How We Can Change That?

Dr. L. Jean Camp

Professor
Indiana University Bloomington
Visiting Scholar
University of California at Berkeley
@ljcamp

Sanchari Das

Doctoral Candidate
Indiana University Bloomington
@sancharidecrypt

Why Not Adopt?

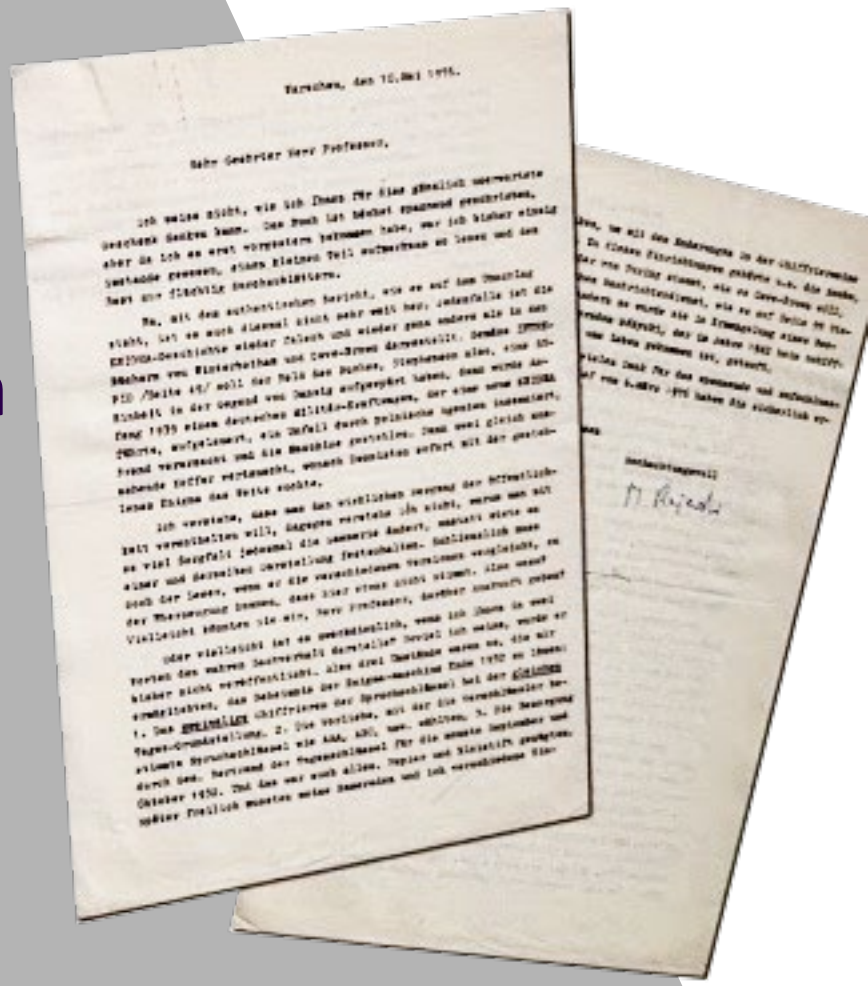
- People do not care about the risk
- People do not know about the risk
- People know and care

Usability Challenges Will Not Disappear

1939: three circumstances that enabled them to solve ENIGMA.

1. Double encoding of the message key
2. The cryptographers' preference for certain specific message keys such as AAA, ABC, etc.
3. General Bertand's acquisition of the daily key for the months of September & October 1932

2015: Most popular Ashley Madison password: AAAA



Courtesy National Cryptologic Museum Letter from Marian Rejewski to David Khan May 10, 1976

People Change Slowly

2015: Most popular Ashley Madison passwords

- 123456

Coming in at 120,000 users (~1%)

- 1234

With 48,425

- 1234567, 12345678, 123456789

Also in top ten

RSAConference2019

Test the Possibilities

Why Not Adopt?

- People do not care about the risk
- Incentives & economics

Why Not Adopt?

- People do not care about the risk
- Incentives & economics

- People do not know about the risk
- Risk communication

Why Not Adopt?

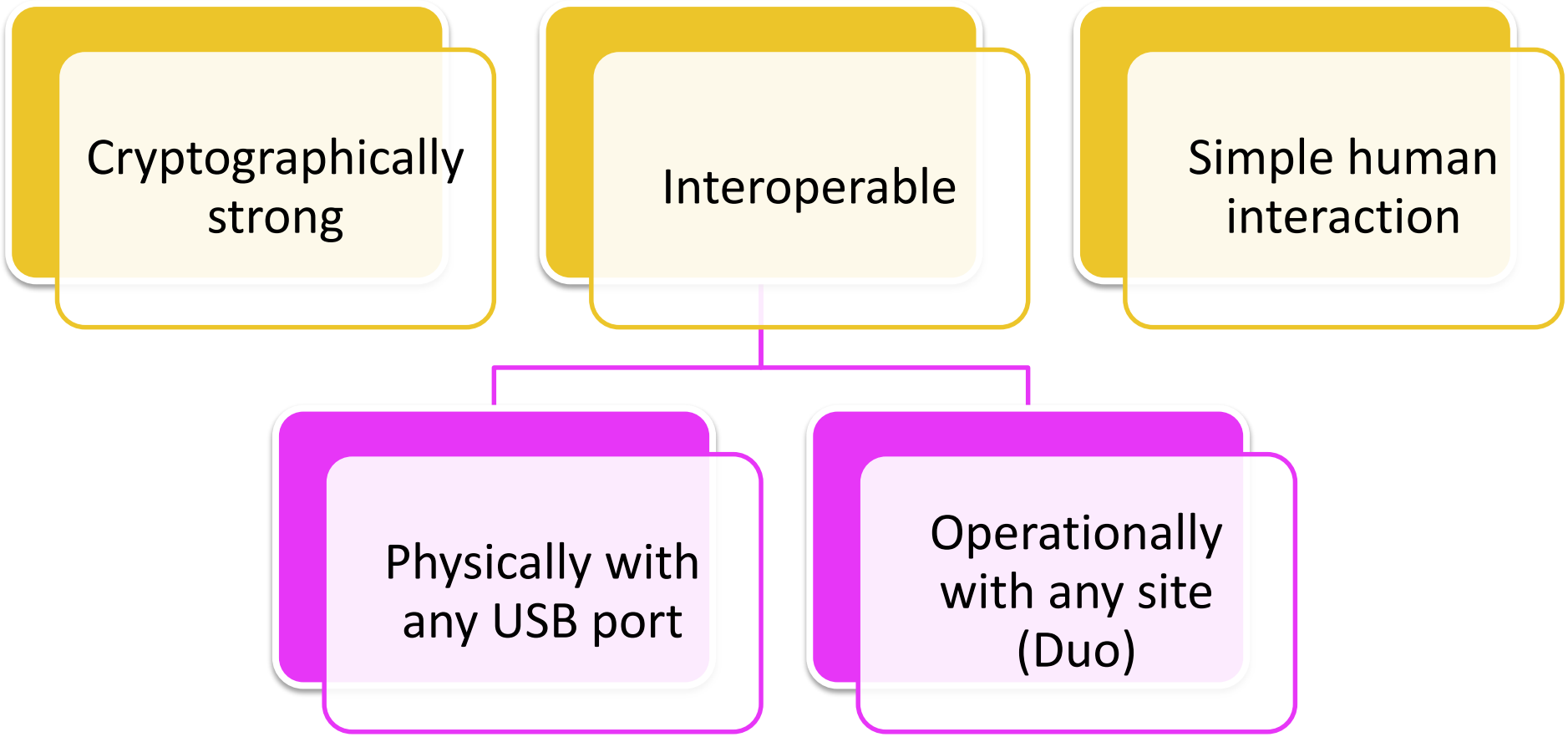
- People do not care about the risk
- Incentives & economics

- People do not know about the risk
- Risk communication

- People know and care
- Usability

Begin with a simple case

Yubico Security Keys



RSAConference2019

Usability and Acceptability

Why Hardware Token?

- High Touch – Low Tech – Srinivas et al.
- Usable – Brett McDowell
- 2FA are not useful – Fegan and Khan

.

- Brett McDowell. Strong Authentication Canine. June 2015. url: https: //www.youtube.com/watch?v=sdJ47NFGlgk.
- Sampath Srinivas et al. “Universal 2nd factor (U2F) overview”. In: FIDO Alliance Proposed Standard (2015), pp. 1–5
- Michael Fagan and Mohammad Maifi Hasan Khan. “Why Do They Do What They Do?: A Study of What Motivates Users to (Not) Follow Computer Security Advice”. In: Twelfth Symposium on Usable Privacy and Security (SOUPS 2016). 2016.

Checklists for 2FA: Stajano

- Stajano proposed five core attributes for the token:
  - Secure, Memoryless, Scalable, Loss resistant, Theft resistant
- Security key does introduce a physical burden, but it is lightweight, and is physically effortless

Frank Stajano. “Pico: No more passwords!” In: International Workshop on Security Protocols. Springer. 2011, pp. 49–81.

Usability Checklist: (Molich & Neilson)

- Simple, natural dialogues
- Speak the user's language
- Minimize the memory load
- Be consistent
- Provide Feedback
- Clearly Mark exits
- Shortcuts
- Good error messages

Usability Checklist for Security (Norcie & Camp)

- Installation procedes operation
- Ensure acurate awareness of trade-offs
- Say why, not how

Lang et al. refer to the use of a security key as

“brainless”

Juan Lang et al. “Security Keys: Practical Cryptographic Second Factors for the Modern Web”. In: Financial Cryptography and Data Security. Financial Cryptography and Data Security. (Accra Beach Hotel & Spa, Barbados, Feb. 22–26, 2016). International Financial Cryptography Association. Feb. 2016. url: http://fc16.ifca.ai/preproceedings/25_ Lang.pdf.
Juan Lang et al. Security Keys: Practical Cryptographic Second Factors for the Modern Web. 2016

Understanding the Challenges

Don’t care? Don’t know?

Security tasks and costs are not acceptable because there is no benefit. Avoidance and risk-taking.

Can’t use?

People understand the benefits but either cannot identify the correct technology or can not use it

RSAConference2019

Methods, From Anecdote to Data

Methods for Usability Evaluations

- Cognitive Walkthrough
- Facilitated Brainstorming
- Focus Group

Method: Cognitive Walkthrough

- The designer pretends to be a user
  - Are the correct options available?
  - What is required of the user?
  - Is action -> consequence clear?
  - Are there stop points?
- Generate success and failure cases

Method: Facilitated Brainstorming

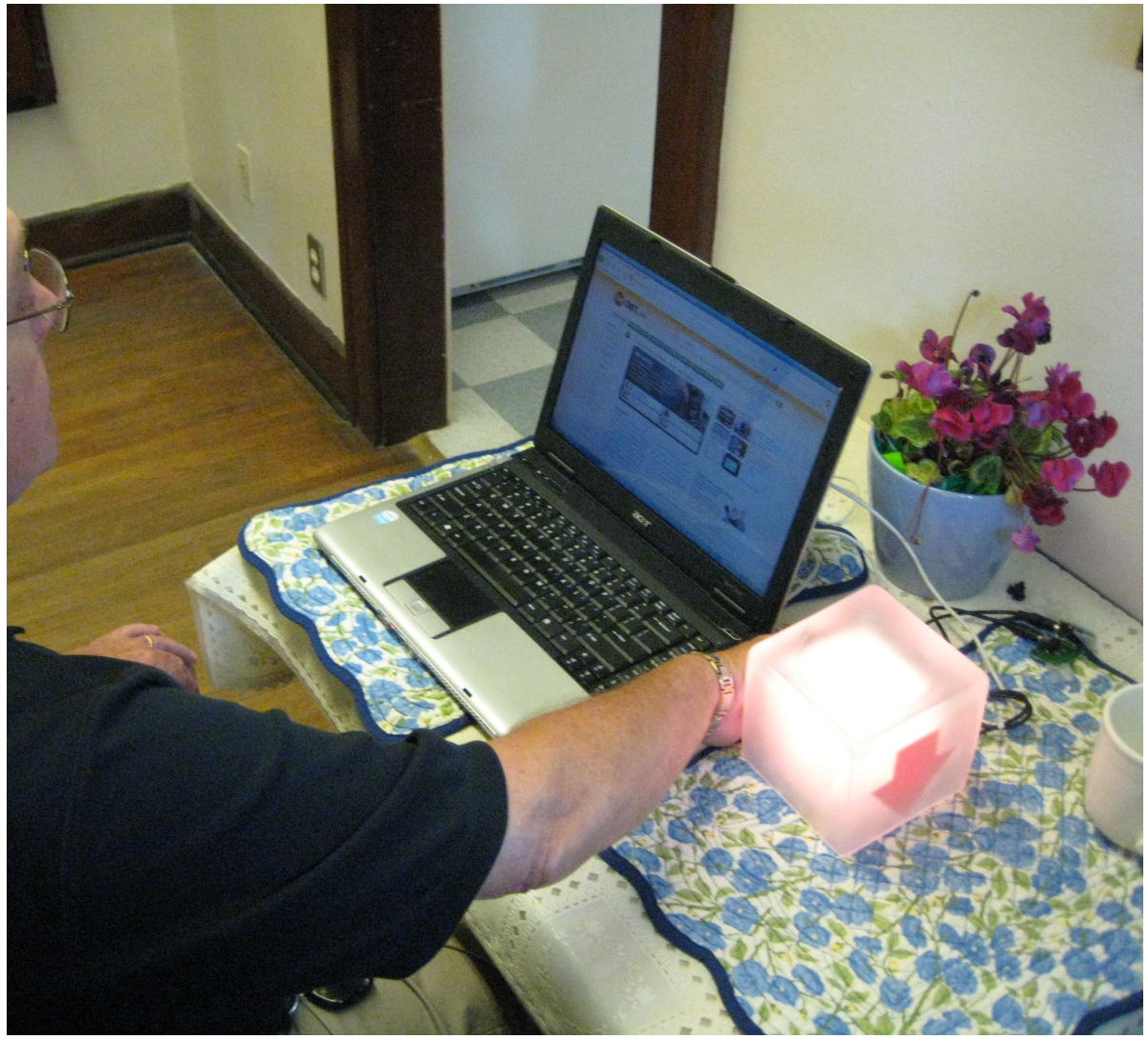
- Can include designers and users
- Have a conversation
- Use and refine
- Both for research protocols and products

Method: Focus Group

- Not the designers!
- Test technology
- Refine experimental protocol
- Source for survey questions

Method: Think Aloud Protocol

- Task analysis
  - Ask what they are doing
  - Identify stop points
  - Mitigate & continue
- Ideally matches your cognitive walk-though
- **Never actually will**



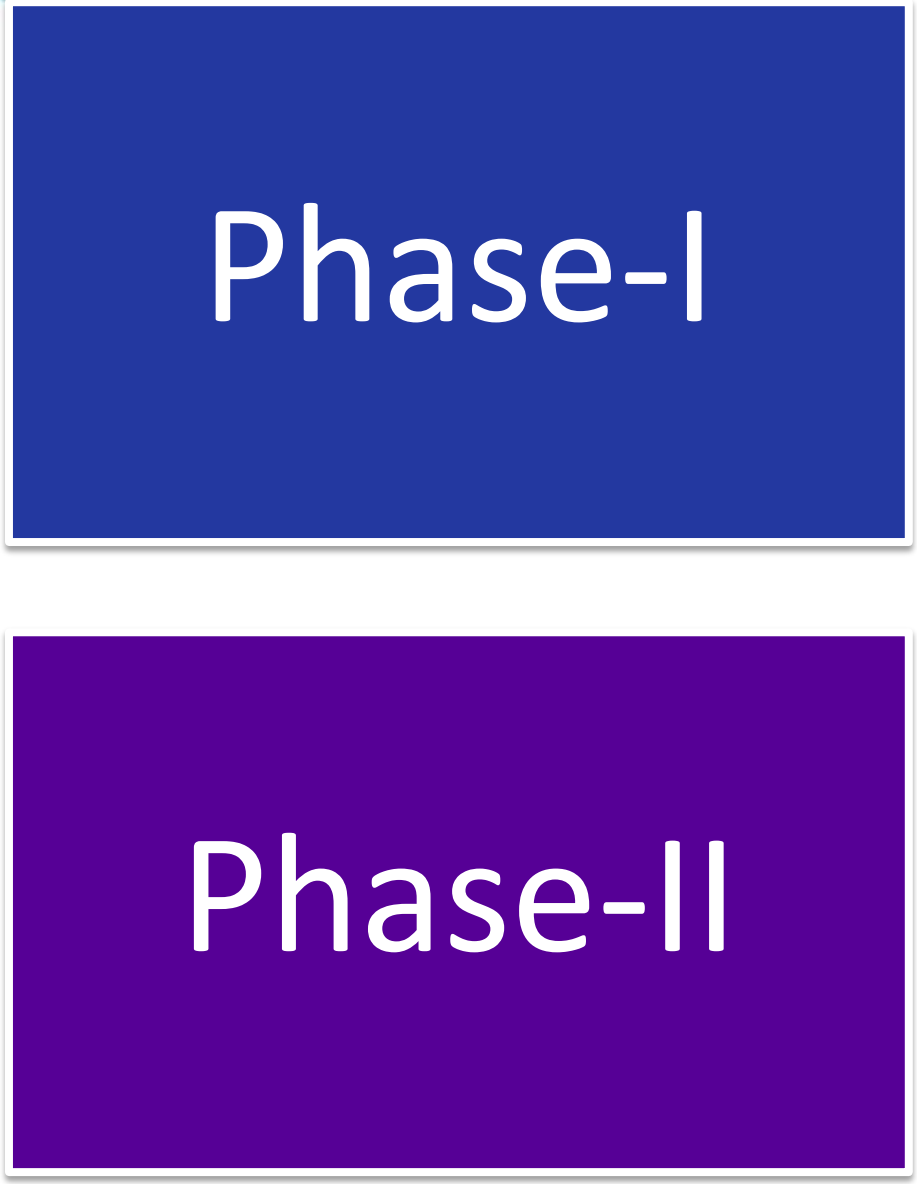
Method: Interviews

- Open discussion
- Question and answer
- Closed
  - pre-determined questions
- Open
  - questions arise during interview

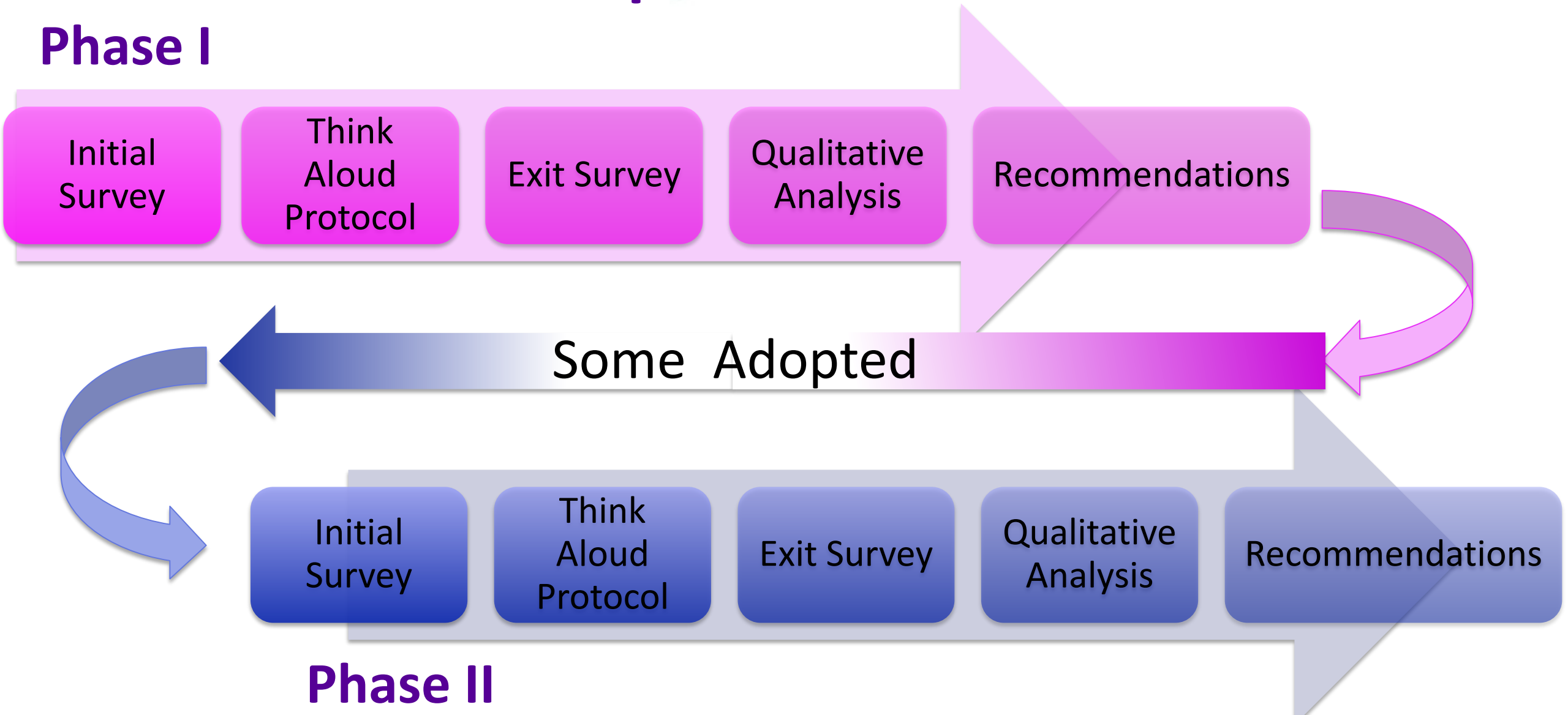
RSAConference2019

Investigating 2FA

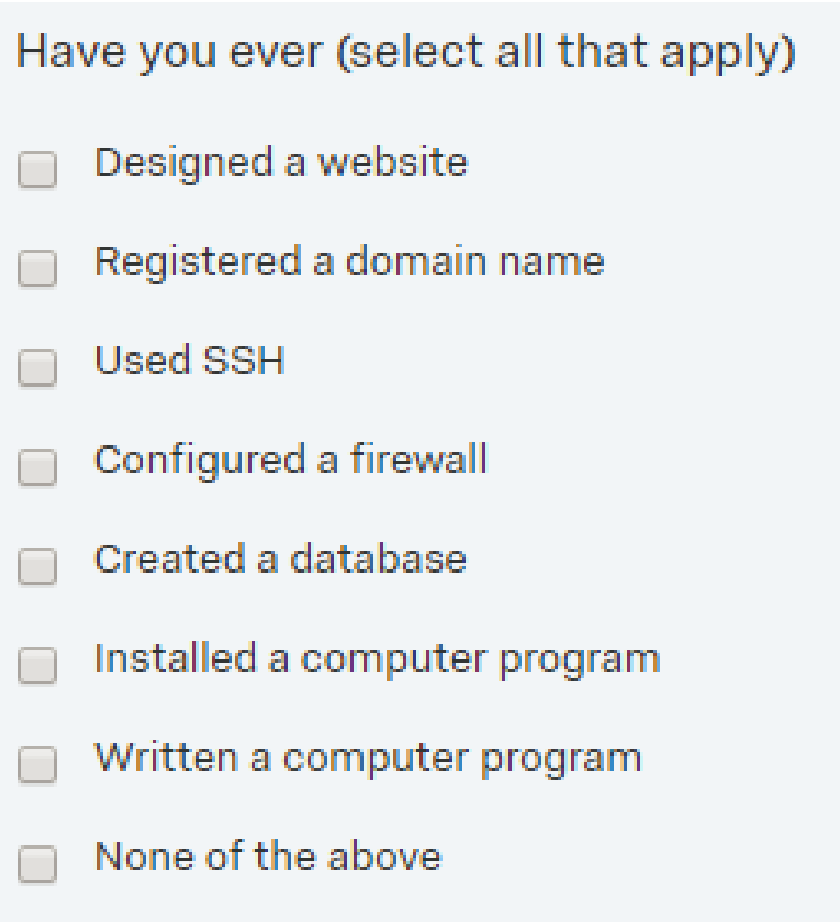
Two Phases



Identical Experimental Protocol



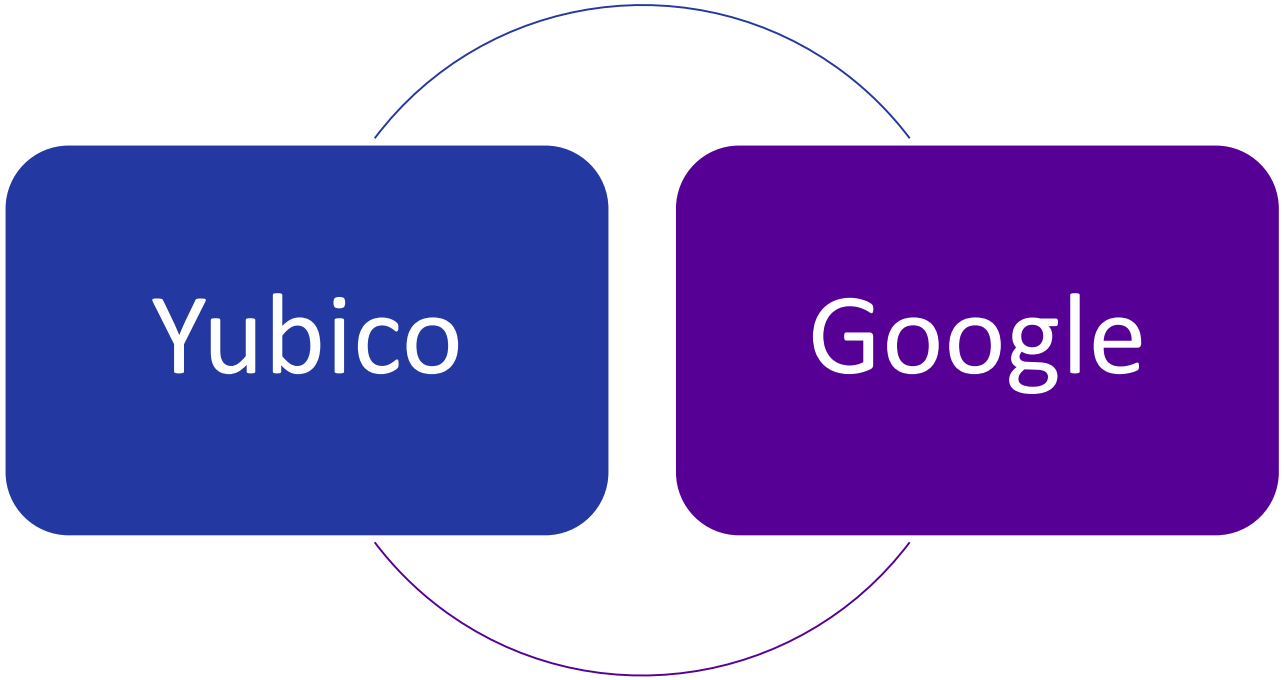
Pre-survey Expertise, Demographics, Experience



- 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 *HAISA* (pp. 199-208).

Instructions



Reasons for Interview

- Participant perceptions of key utility
- Ensure that we would not harm the participants by locking them out of their accounts
- Ensure that they had the contact information of the team and a specific researcher before they left
- Offer them the security keys as a token of appreciation for their participation

Follow-up Survey

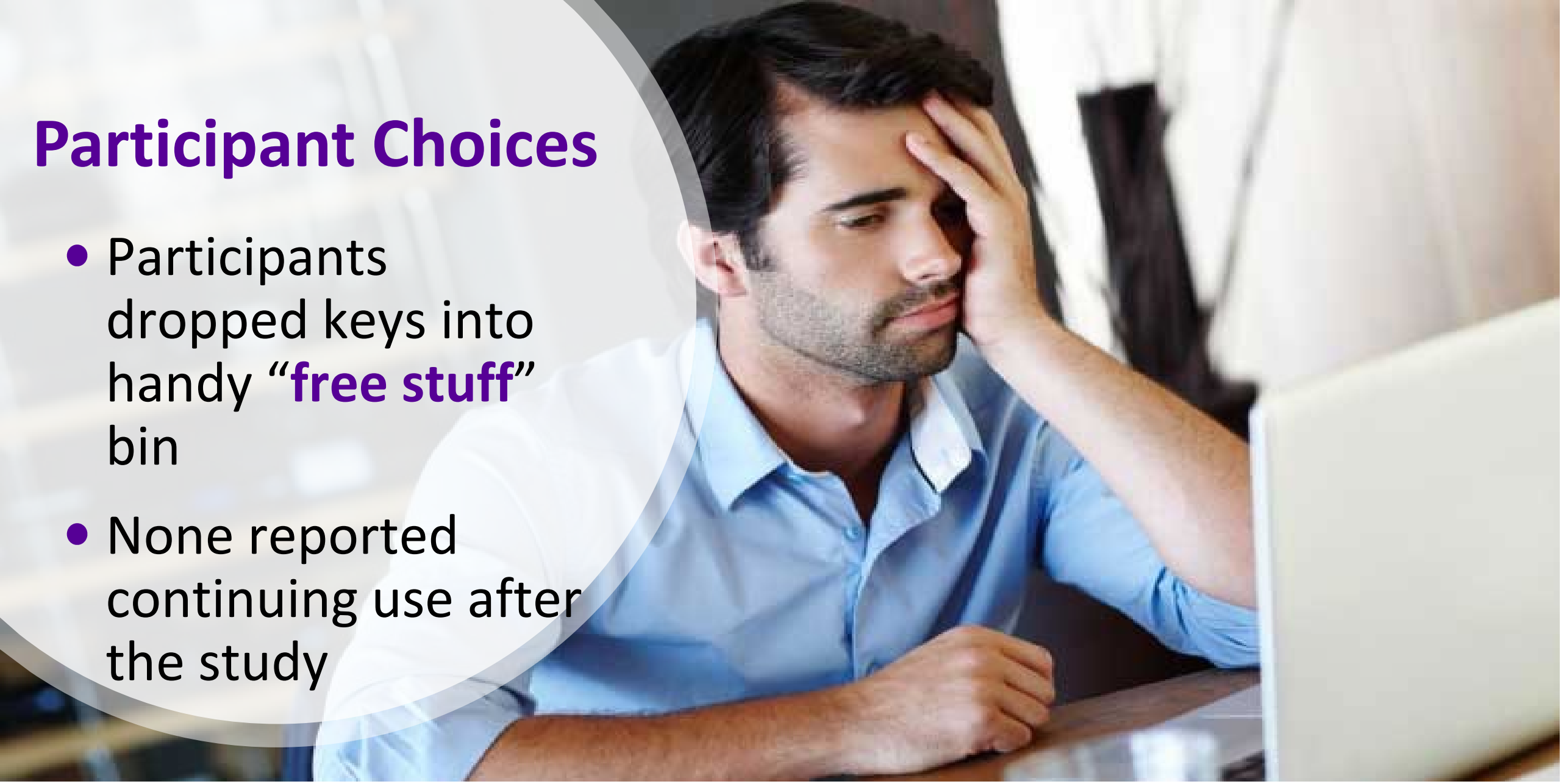
No one responded or showed any sign of using the Yubico security keys

Many discarded the security keys after the survey

They discussed they do not find a benefit in using the keys to secure their accounts

Participant Choices

- Participants dropped keys into handy “**free stuff**” bin
- None reported continuing use after the study



People Don't Know

not at risk
no benefit

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

"Why is it still asking for a password?"

"use it out of curiosity, [as it] might not be practical."

well… I don't really understand the point of the key if I still need to enter my username and 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."

Transcription	Qualitative Coding	Qualitative clustering	Results
Think aloud results Interview questions	Three independent coders Create *code book* from identified themes Set of themes or codes to represent all notable data	Halt Point: can not move forward without help Confusion Point: slowed and asked for help Value perception: benefit, cost, or risk	Analysis: coding allows quantitative as well as qualitative Discussion: return to transcripts for nuance Recommendations

Analysis

RSAConference2019

Test the Recommendations

MORE ABOUT YOUR YUBIKEY

YUBIKEY 4

USB; strong crypto and touch-to-sign, plus One-Time-Password, PIV-compatible smart card, and FIDO U2F. Read more

YUBIKEY NEO

USB and NFC (for Android mobile); One-Time Password, PIV-compatible smart card, and FIDO U2F. Read more

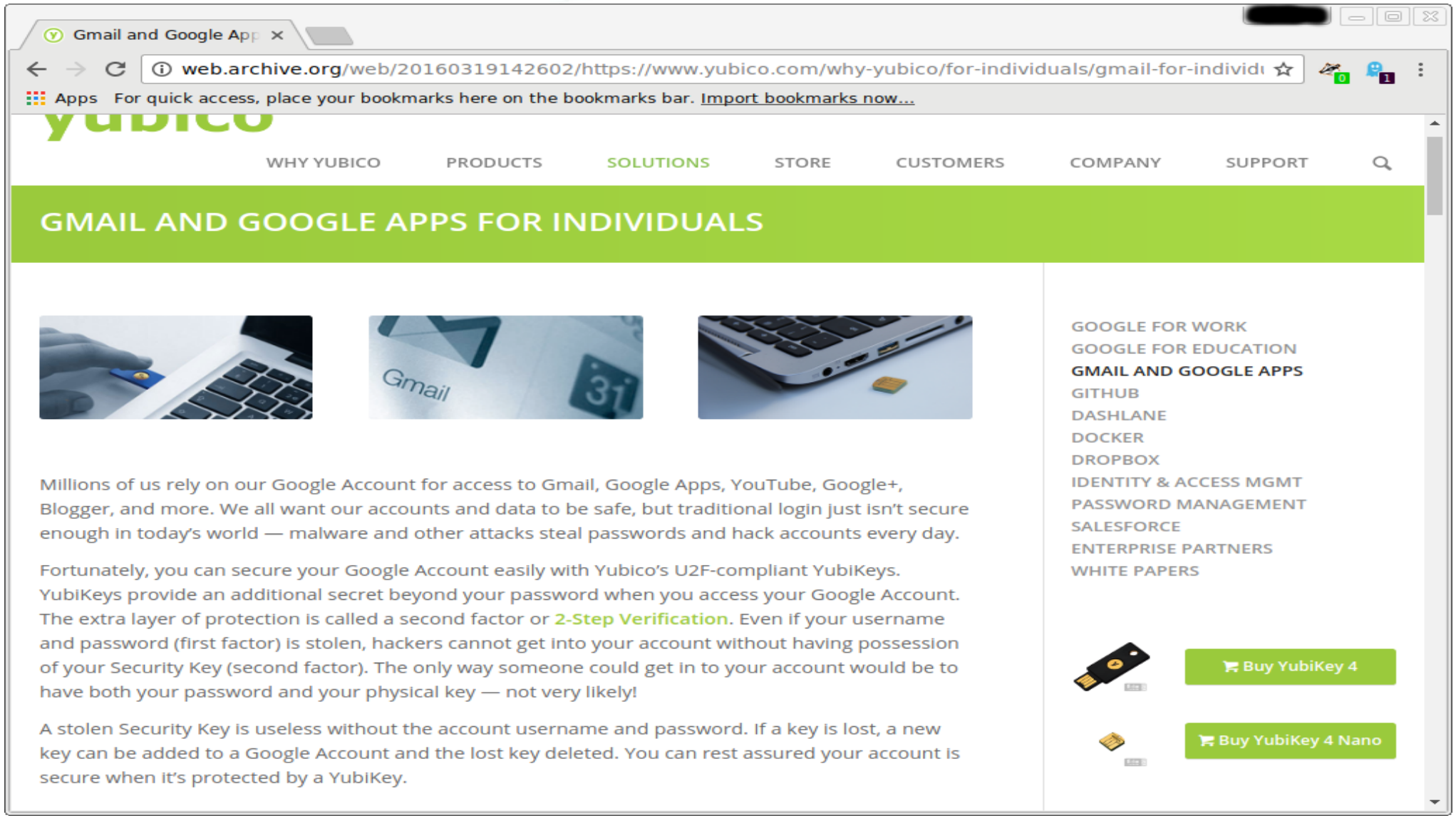
YUBIKEY 4 NANO

Same features as YubiKey 4, its bigger brother, but designed to fit inside the USB

FIDO U2F SECURITY KEY

USB; FIDO U2F. Read more

Phase- I security key comparisons


Gmail and Google App
web.archive.org/web/20160319142602/https://www.yubico.com/why-yubico/for-individuals/gmail-for-individ
Apps For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
WHY YUBICO
PRODUCTS
SOLUTIONS
STORE
CUSTOMERS
COMPANY
SUPPORT
GMAIL AND GOOGLE APPS FOR INDIVIDUALS
Gmail
31
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

Wall of Text

The Yubico security key is a 2FA device designed to be user friendly. We examined the usability of the device by implementing a think-aloud protocol, and documented the halt and confusion points. We provided this analysis to Yubico, who implemented many of the recommended changes. We then repeated the study in the same context; noting significant improvements in usability. However, increase in usability did not affect the acceptability of the device, affecting the prolonged usage of the device. In both phases we interviewed the study participants about the acceptability of the device, finding similar concerns about lack of benefits and the invisibility of risk. A source of opposition to adoption is the concern for loss of access, with participants prioritizing availability over confidentiality. Another concern is that these do not lessen or simplify interaction with services as passwords are still required. We close with open questions for additional research, and further recommendations to encourage online safety through the adoption of 2FA.

We analyzed acceptability and usability of the Yubico security key, a Two Factor Authentication (2FA) hardware token implementing FIDO. This token has notable usability attributes: tactile interaction, convenient form factor, physical resilience, and the design goal of ease of use. Despite the Yubico security key being among best in class for usability, participants in a think-aloud protocol still encountered several difficulties in use. Based on these findings, we proposed design changes, some of which Yubico adopted. We repeated the experiment, showing that these recommendations enhanced ease of use but not necessarily acceptability. With the primary halt points mitigated, we could identify the principal remaining reasons for rejecting 2FA. These reasons were the fear of losing the device and perceptions that there is no individual risk of account takeover. Our results illustrate both the importance and limits of usability on acceptability, adoption, and adherence in two-factor authentication.

The risk of loss of availability was perceived as greater than the risk of loss of control. Participants believed that their passwords were strong enough, and that their accounts were sufficiently secured by their own acumen. We report on both experiments, and detail the progress between them. Our results illustrate both the importance and limits of usability on acceptability, adoption, and adherence in two-factor authentication. Specifically, we implemented a think-aloud protocol to identify stop points, perceived benefits, and perceived costs. We reported the findings along with recommendations to Yubico and documented the consequent changes for a second iteration of the study implementing these modifications. We focused on participants with above average technical literacy by recruiting students from STEM degree programs. Our goal was to identify difficulties that might be barriers to Adoption for technically literate participants, particularly those who were likely to use GitHub, DropBox, or other sharing platforms.

We conducted the entire experiment in two-phases. In both the phases we asked the participants to configure a FIDO U2F security key for their Google account. Significant improvements in usability were noted in Phase-II over Phase-I. However, the overall acceptability did not change. Subsequently, we provided additional recommendations, such as confirmation of successful completion of the login, and the need to communicate the benefits of the device. Our contributions are the specific suggestions for Yubico, the instrument we developed for evaluating

- Finding instructions
- Demo versus reality
- Device identification
- Biometric versus touch
- Confirmation of operation
- Communicate the benefit
- Communicating the risks

Phase I

Phase II Device Identification

YUBIKEY 4	YUBIKEY 4 NANO	YUBIKEY 4C	YUBIKEY 4C NANO	YUBIKEY NEO	FIDO U2F SECURITY KEY
					
Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now
$40 per key	$50 per key	$50 per key	$60 per key	$50 per key	$18 per key
USB authentication key, including strong crypto and touch-to-sign, plus One-Time-Password, smart card, and FIDO U2F; four form factors Learn more about the YubiKey 4 series				Combines USB and NFC for mobile communication, enables One-Time Password, smart card, and FIDO U2F authentication	USB authentication key that works instantly with any service that supports FIDO U2F

Instruction & Touch Sensor

REQUIREMENTS

- Latest version of Google Chrome browser (or at least version 38)
- A U2F Security Key, YubiKey 4, YubiKey 4 Nano, YubiKey NEO, or other Yubico U2F-enabled YubiKey
- One finger (the YubiKey button is a capacitive sensor, not a biometric)
- A Google Account (such as Gmail, Google Apps, YouTube, Google Plus, Blogger, Adwords)

Simple Instructions

1

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

2

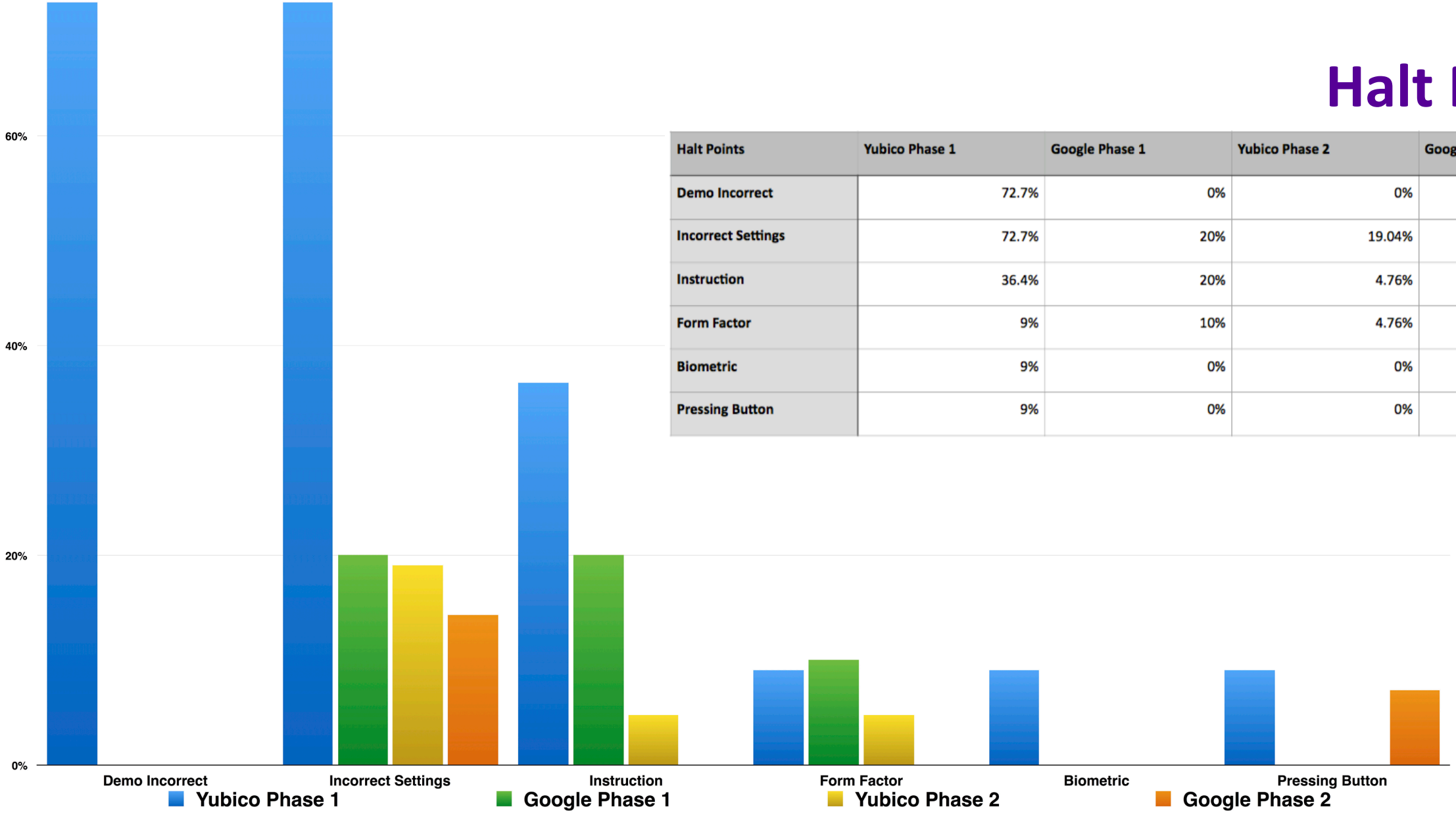
Insert the Security Key in a USB port with the **gold side up**.

3

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

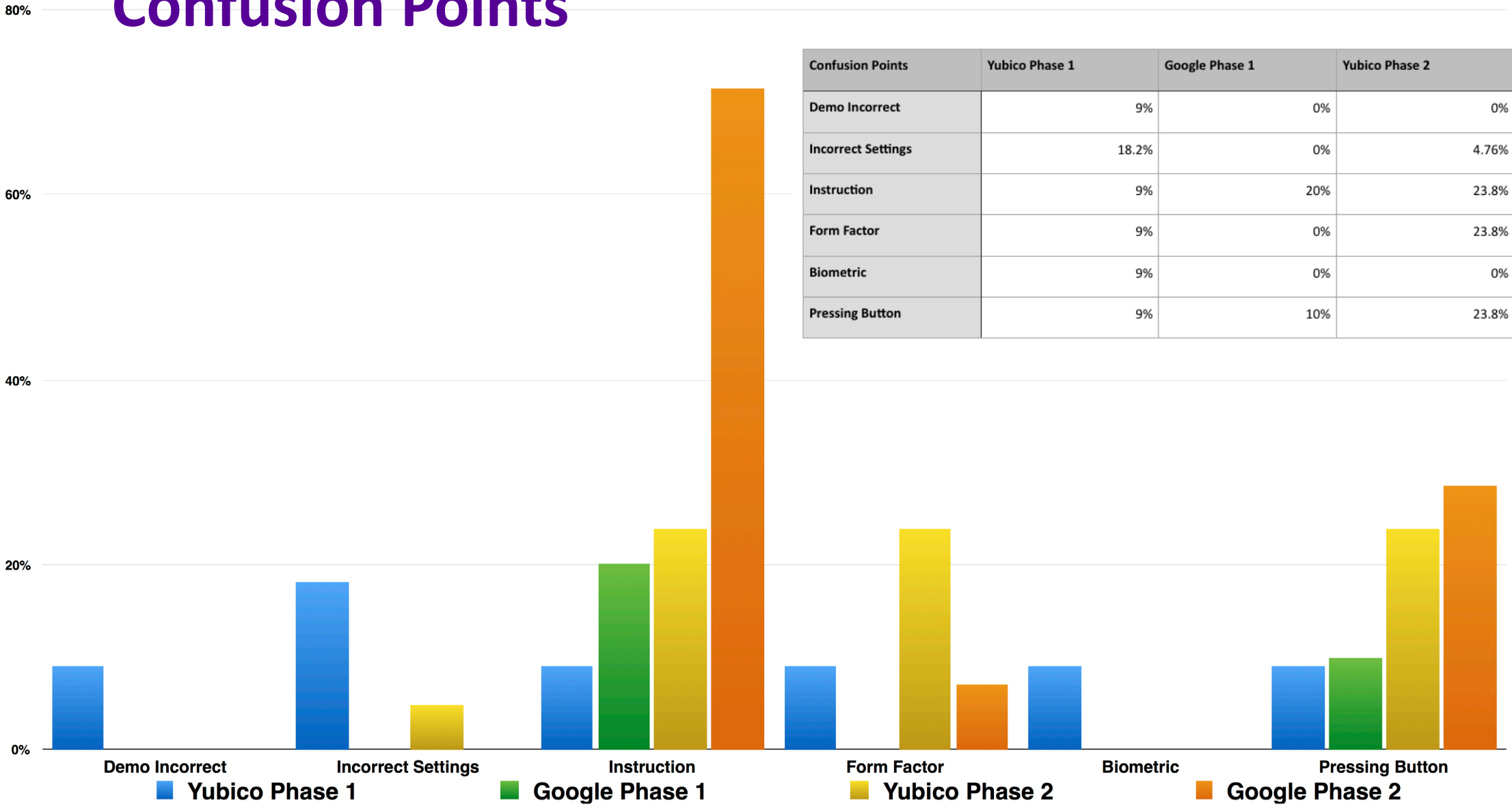
Halt Points

Halt Points	Yubico Phase 1	Google Phase 1	Yubico Phase 2	Google Phase 2
Demo Incorrect	72.7%	0%	0%	0%
Incorrect Settings	72.7%	20%	19.04%	14.29%
Instruction	36.4%	20%	4.76%	0%
Form Factor	9%	10%	4.76%	0%
Biometric	9%	0%	0%	0%
Pressing Button	9%	0%	0%	7.14%



Confusion Points

Confusion Points	Yubico Phase 1	Google Phase 1	Yubico Phase 2	Google Phase 2
Demo Incorrect	9%	0%	0%	0%
Incorrect Settings	18.2%	0%	4.76%	0%
Instruction	9%	20%	23.8%	71.43%
Form Factor	9%	0%	23.8%	7.14%
Biometric	9%	0%	0%	0%
Pressing Button	9%	10%	23.8%	28.57%



RSAConference2019

Risk Communication

Goals

- How do you describe security risks in a way that communicates the risks and benefits?
  - Risk Communication
  - Ambient Risk Communication
  - Action-based Risk Communication
- Mental models

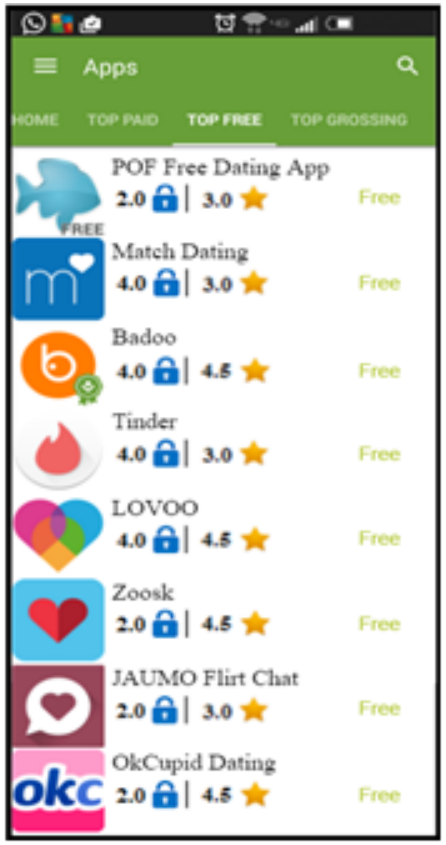
Risk Communication must work for your user population

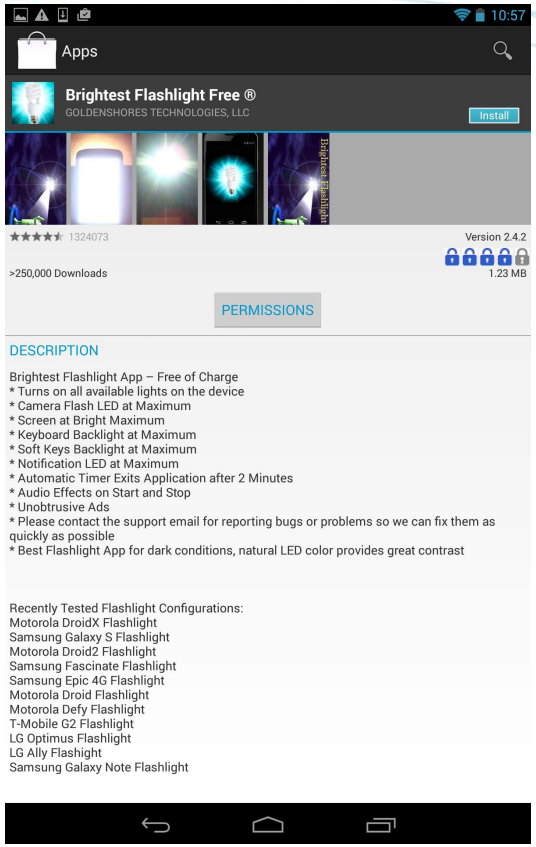
Actual Humans

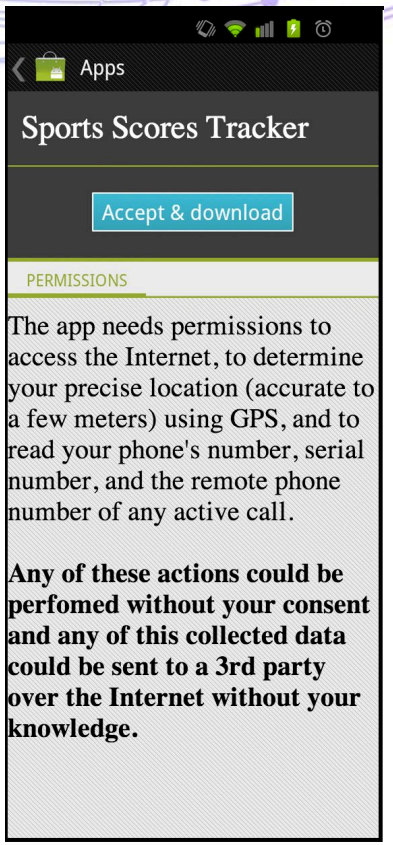
Design for Humans Requires Designing for Humans

Smoking is a factor which contributes to lung cancer. Most cancers that start in lung, known as primary lung cancers, are carcinomas that derive from epithelial cells. Depending on the type of tumor, so-called paraneoplastic phenomena may initially attract attention to the disease. In lung cancer, these phenomena may include Lambert-Eaton myasthenia syndrome (muscle weakness due to auto-antibodies), hyperkalemia, or syndrome of inappropriate antidiuretic hormone (SIADH). Tumors in the top (apex) of the lung, known as Pancoast tumors, may invade the local part of the sympathetic nervous system, leading to changed sweating patterns and eye muscle problems (a combination known as Horner's syndrome) as well as muscle weakness in the hands due to invasion of the brachial plexus.

Warnings for the average user miss half your population







Summarize & Simplify Risks

Security is Risk

- All we have to do is get the **numbers right**
- All we have to do is **tell them the numbers**
- All we have to do is explain what **the numbers mean**

Security is Risk

- All we have to do is show them that they've accepted/ rejected **similar risks in the past**
- All we have to do is show them that **it's a good deal** for them

Security is Risk

- All we have to do is **treat them nice**
- All we have to do is **make them partners**
- All of the above

A Wealth of Research and Results

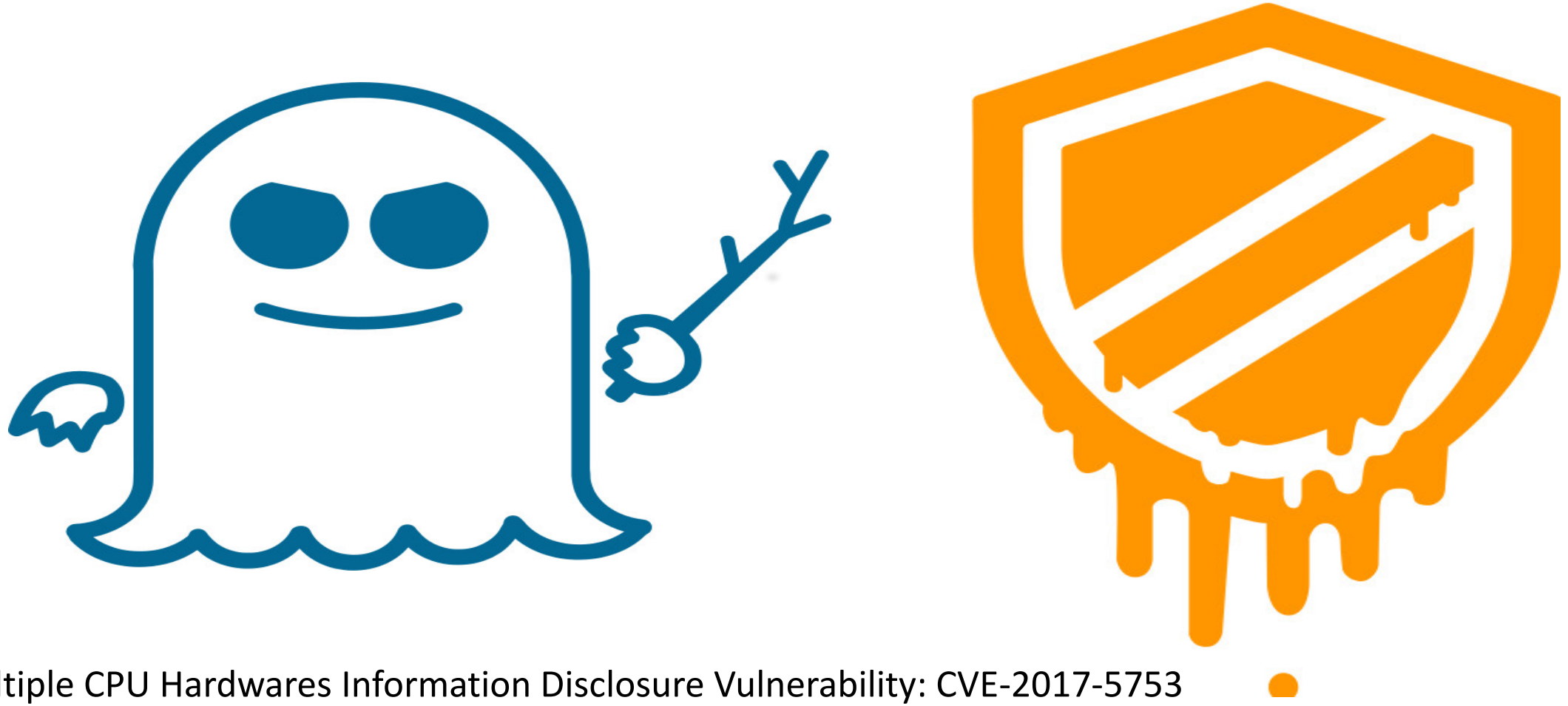
Risk Perception and Communication Unplugged

Twenty Years of Process

1995

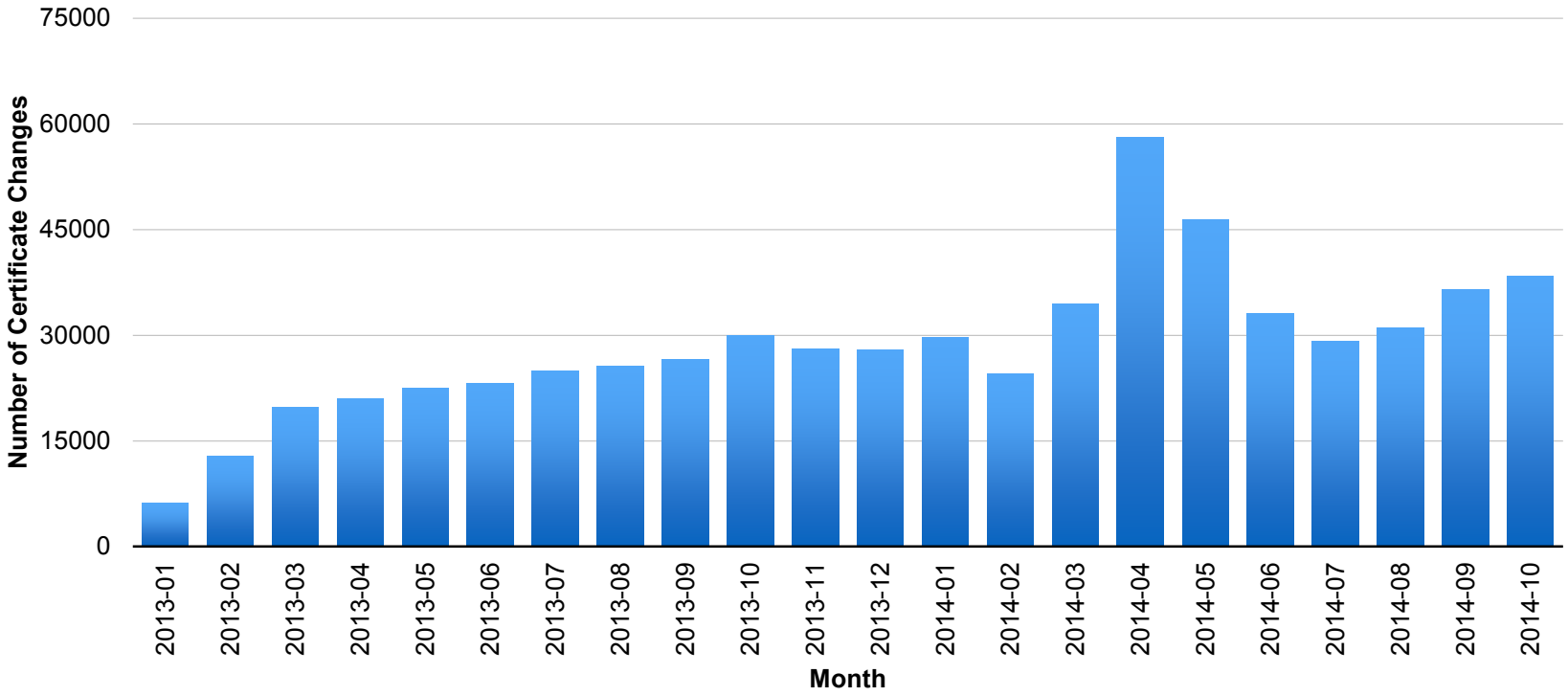
Baruch Fischhoff

Clear, Urgent Communication

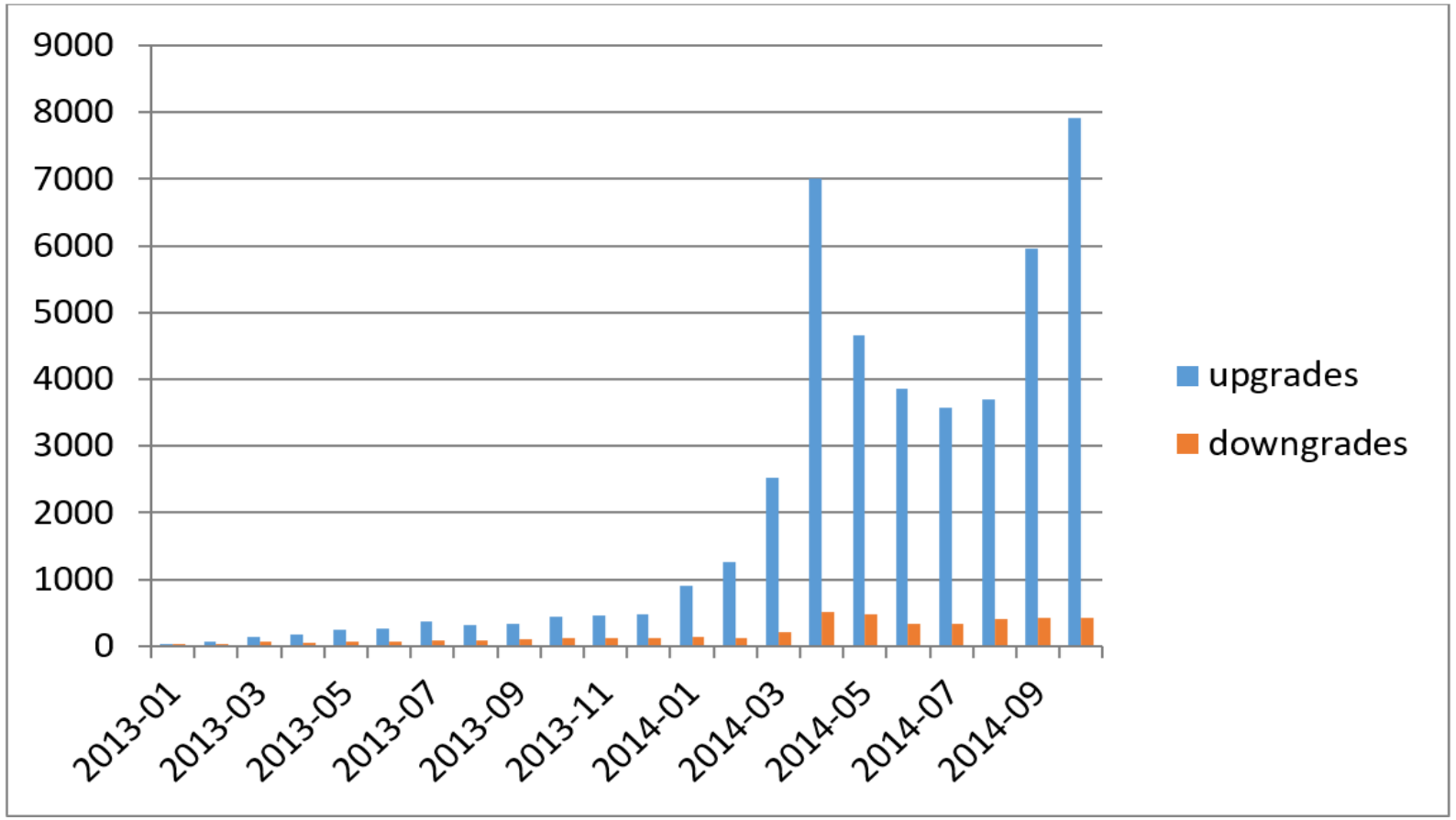


Multiple CPU Hardwares Information Disclosure Vulnerability: CVE-2017-5753

Otherwise, No Response



Or Worse

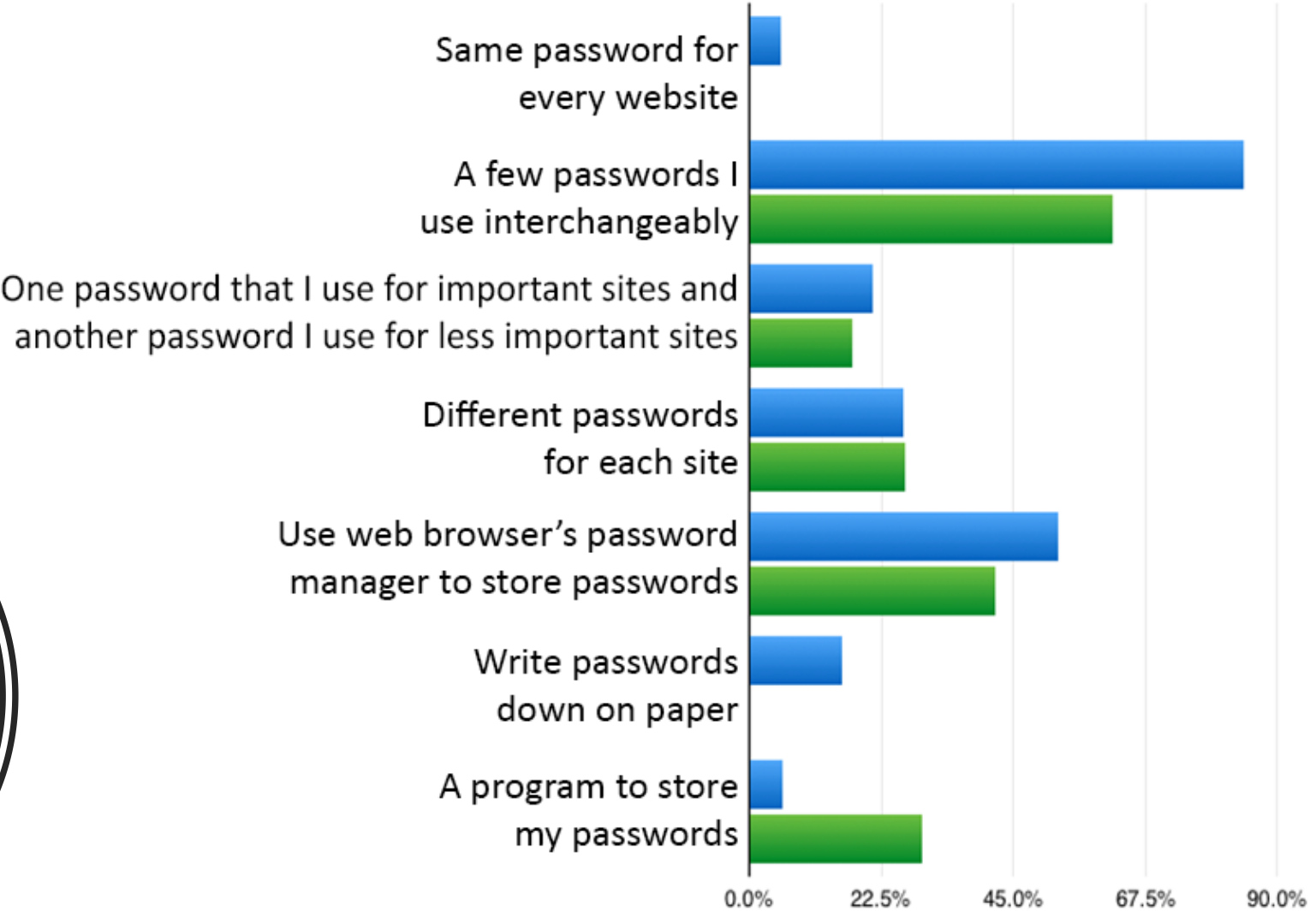

9000
8000
7000
6000
5000
4000
3000
2000
1000
0
2013-01
2013-03
2013-05
2013-07
2013-09
2013-11
2014-01
2014-03
2014-05
2014-07
2014-09
upgrades
downgrades

Risk Communication that Connects

Visceral
Risk
Communication

Consider Password Behaviors

Participants Selected All That Applied



Visceral Risk Communication

Current & Future Research

- Mental model risk communication
- Evaluate avoidance behaviors
- Targeted periodic confirmations

Communication Benefits

- Positive feedback for a positive affect
  - You are enrolled
  - A small celebration
  - Confirmation of benefit
  - Text congratulations

Create Additional Benefits

- Requirements
  - 16 length, control, caps, #'s
  - Reduced reuse risk
  - High account capture risk

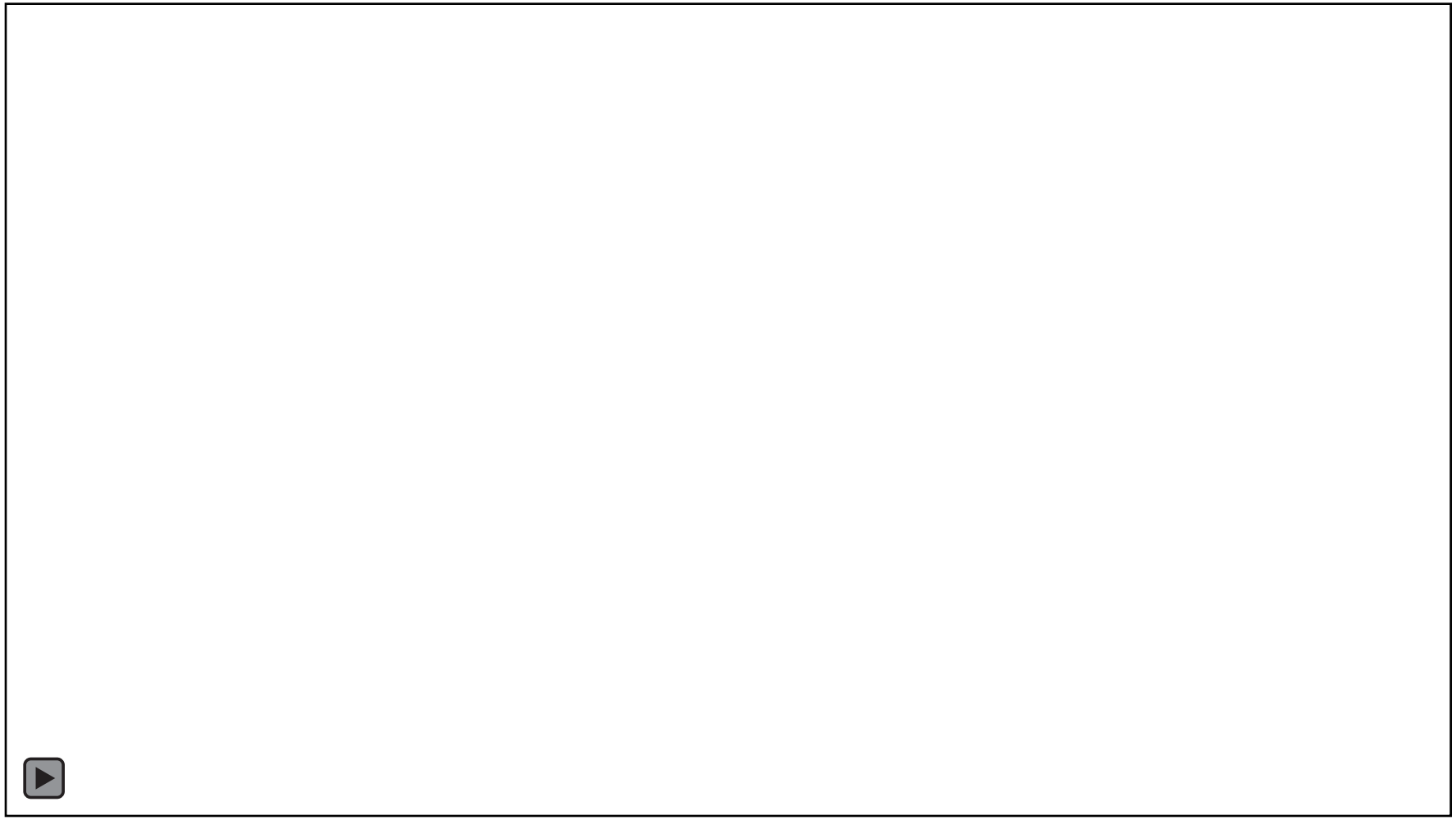
- Requirements
  - Shorter password
  - Increased reuse risk
  - Moderate capture risk

- Requirements
  - PIN
  - High PIN reuse risk
  - Low capture risk

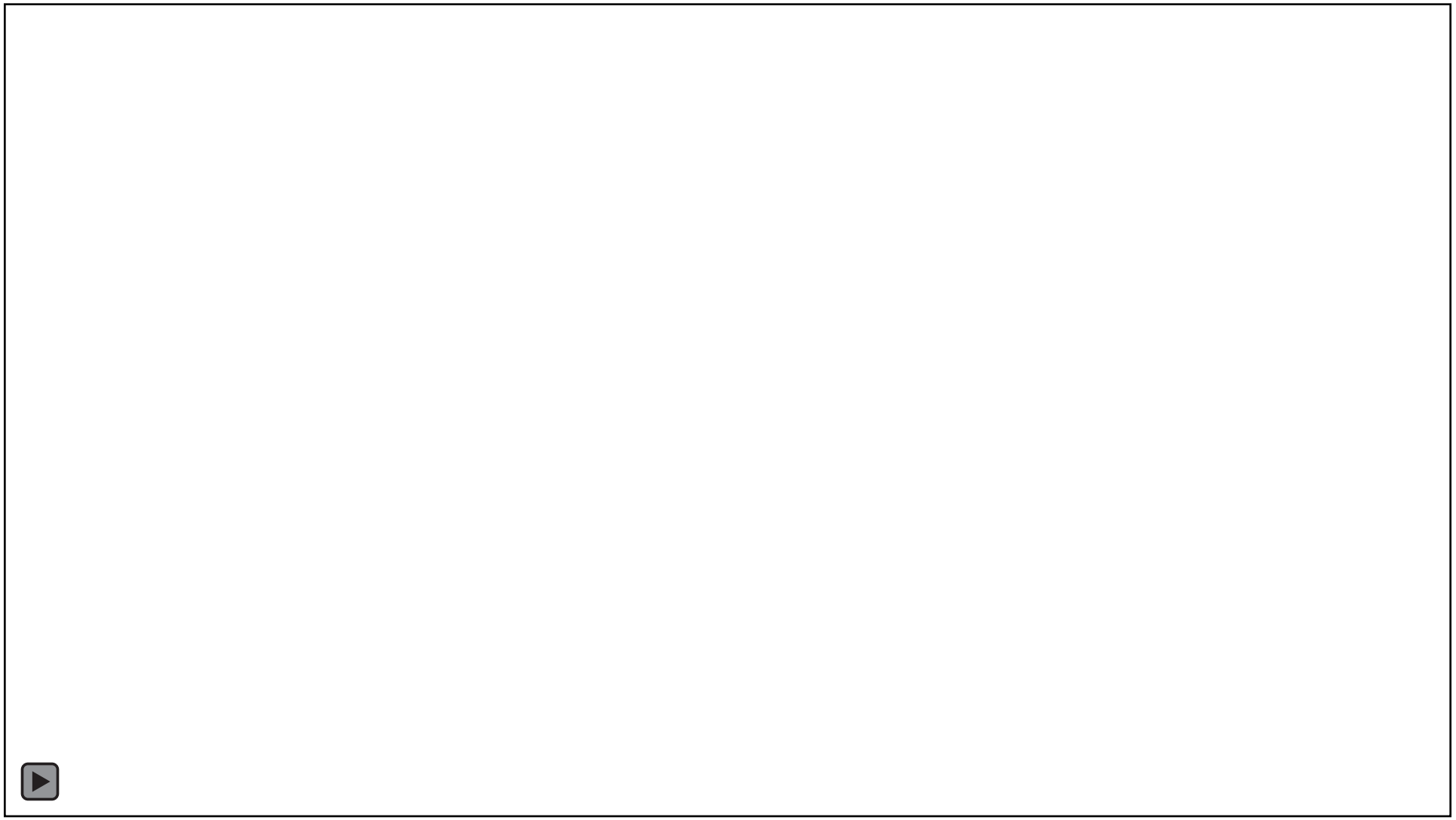
Align with Mental Models

- Communicate risks and benefits
- Social communication
  - 90% of your coworkers always use 2FA
  - Protect your vulnerable coworkers
- Value communication
  - Phishing attacks have gone for 2,000 to 2

Risk Communication using Physical Space



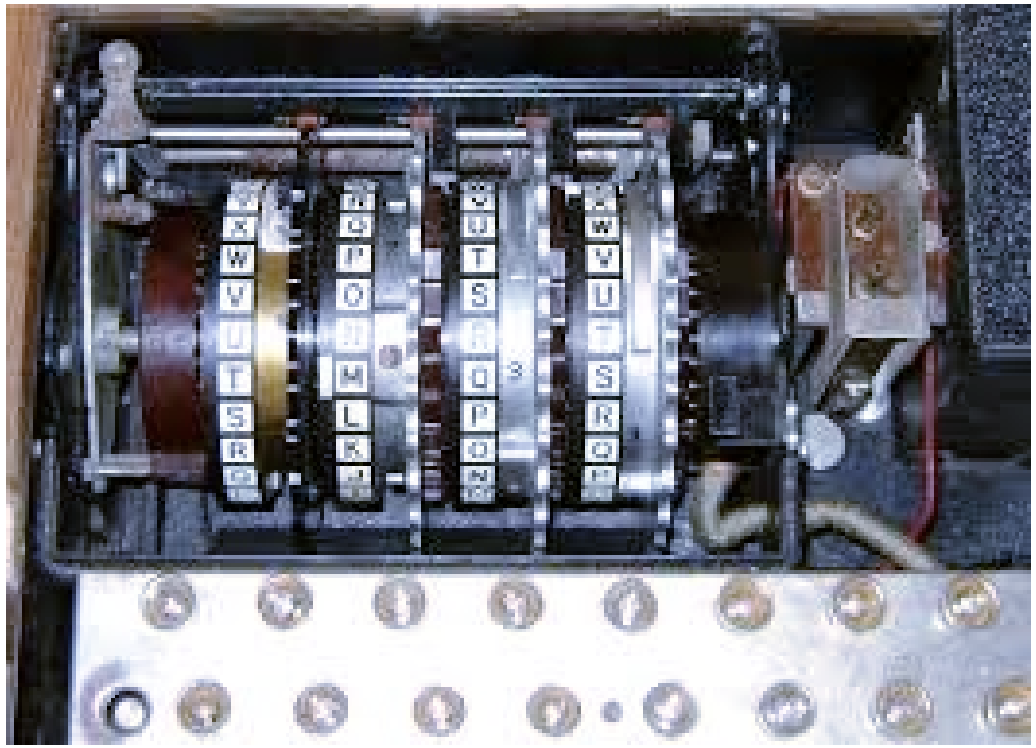
Risk Communication using Bodily Risk

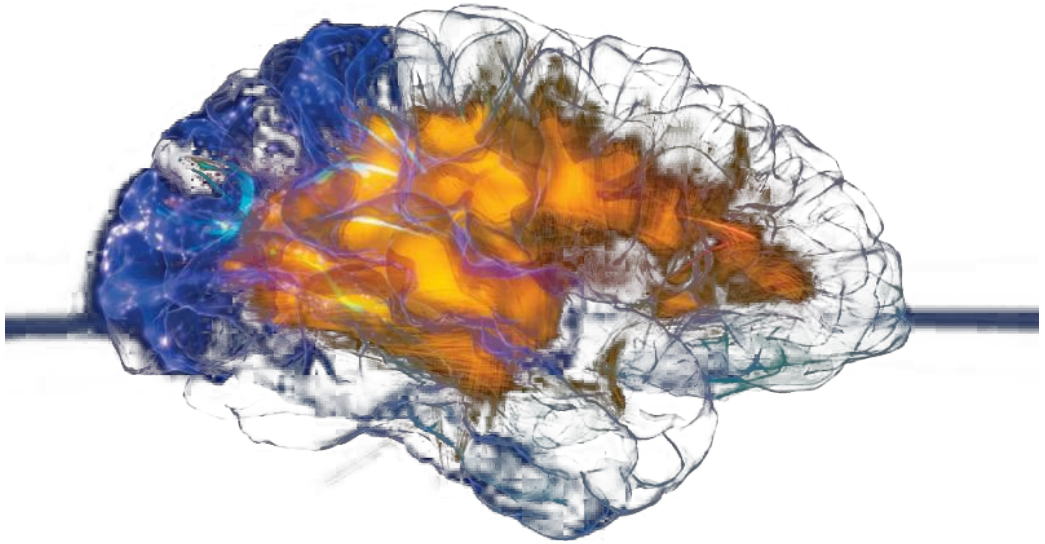


Acceptablity is not just Common Sense

- Different people need different interactions
- Expertise matters
- Authentication will advance
- Behaviors can change
- People change?

The Human Interface Will Remain a Challenge





Apply It

Providing the technology is not enough

Communicate why, then how

You have methods, use them!

- Risk communication and rewards

- Usability rubrics

- Our materials are Creative Commons

Usablesecurity.net

Making security that fits the user & the occasion