black hat USA 2018

AUGUST 4-9, 2018
MANDALAY BAY / LAS VEGAS

Two-Factor Authentication, Usable or Not?

Sanchari Das, Andrew C. Dingman, Gianpaolo Russo, and L. Jean Camp

Indiana University Bloomington

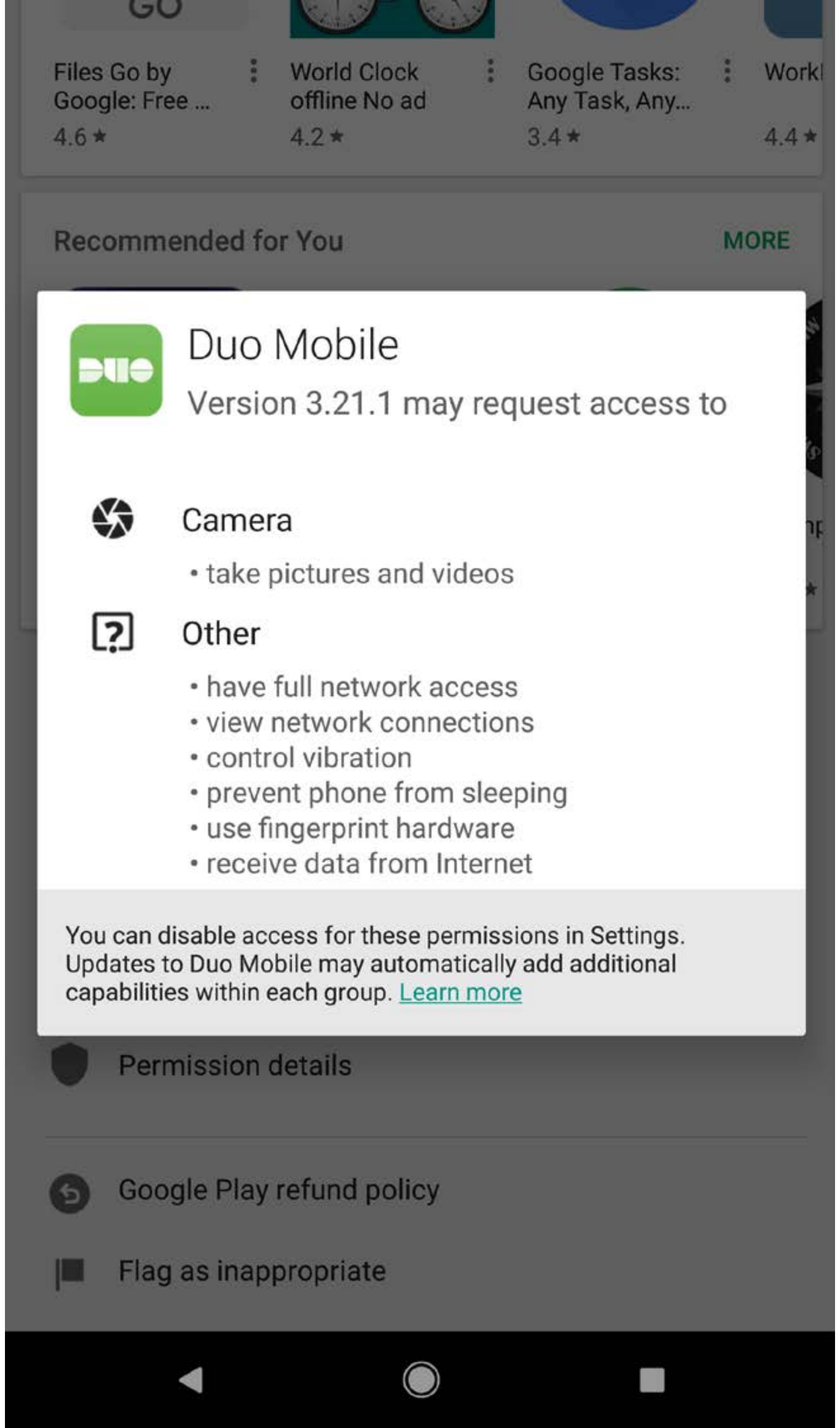
Two-Factor Options

- SMS
- OTP apps
- Tokens

OTP & SMS Apps Interrupt Login

OTP Apps Data Sharing

- Data for your Boss


Files Go by Google: Free ...
4.6 ★
World Clock offline No ad
4.2 ★
Google Tasks: Any Task, Any...
3.4 ★
Work
4.4 ★
Recommended for You
MORE
Permission details
Google Play refund policy
Flag as inappropriate

Duo Mobile

Version 3.21.1 may request access to

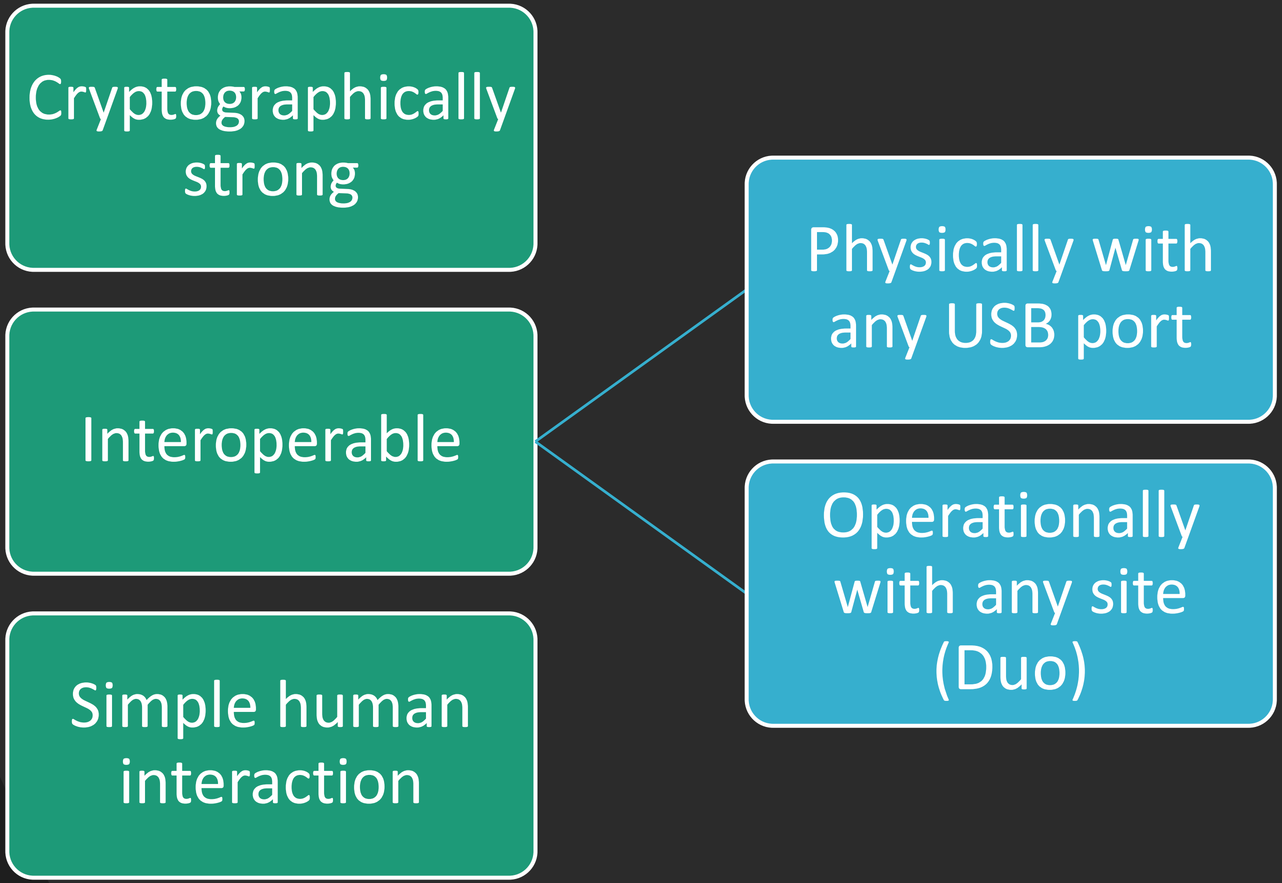
Camera
- take pictures and videos

Other
- have full network access
- view network connections
- control vibration
- prevent phone from sleeping
- use fingerprint hardware
- receive data from Internet

You can disable access for these permissions in Settings. Updates to Duo Mobile may automatically add additional capabilities within each group. Learn more

A Physical Token to Control Account Access

Yubico Security Keys



Cryptographically strong

Interoperable

Simple human interaction

Physically with any USB port

Operationally with any site (Duo)

Usability and Acceptability

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
- Speaks the user’s language
- Minimizes the memory load
- Be consistent
- Provide Feedback
- Clearly Mark exits
- Provide shortcuts
- Good error messages

R. Molich and J. Nielsen. Improving a human-computer dialogue. Communications of the ACM, 33(3):338–348, 1990.

Lang et al. refer to the use of a security key as “**brainless**”, which seems to indicate a belief that there are no halt points in security key adoption

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

From Stories to Science

Methods for Usability Evaluations

- Cognitive Walkthrough
- Facilitated Brainstorming
- Focus Group

Method: Cognitive Walkthrough

- The designer pretends to be a user
  - Are the correct options visible and available?
  - What is required of the user to find the options?
  - How are the options associated with the goal?
  - Are the correct actions clear?
  - Do the correct actions illustrate progress towards the goal?
  - Are there stop points?
- Generate success and failure cases

Method: Facilitated Brainstorming

- Can include designers and users
- Pretend to be user
- Use and refine

Method: Focus Group

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

Lost and Confused

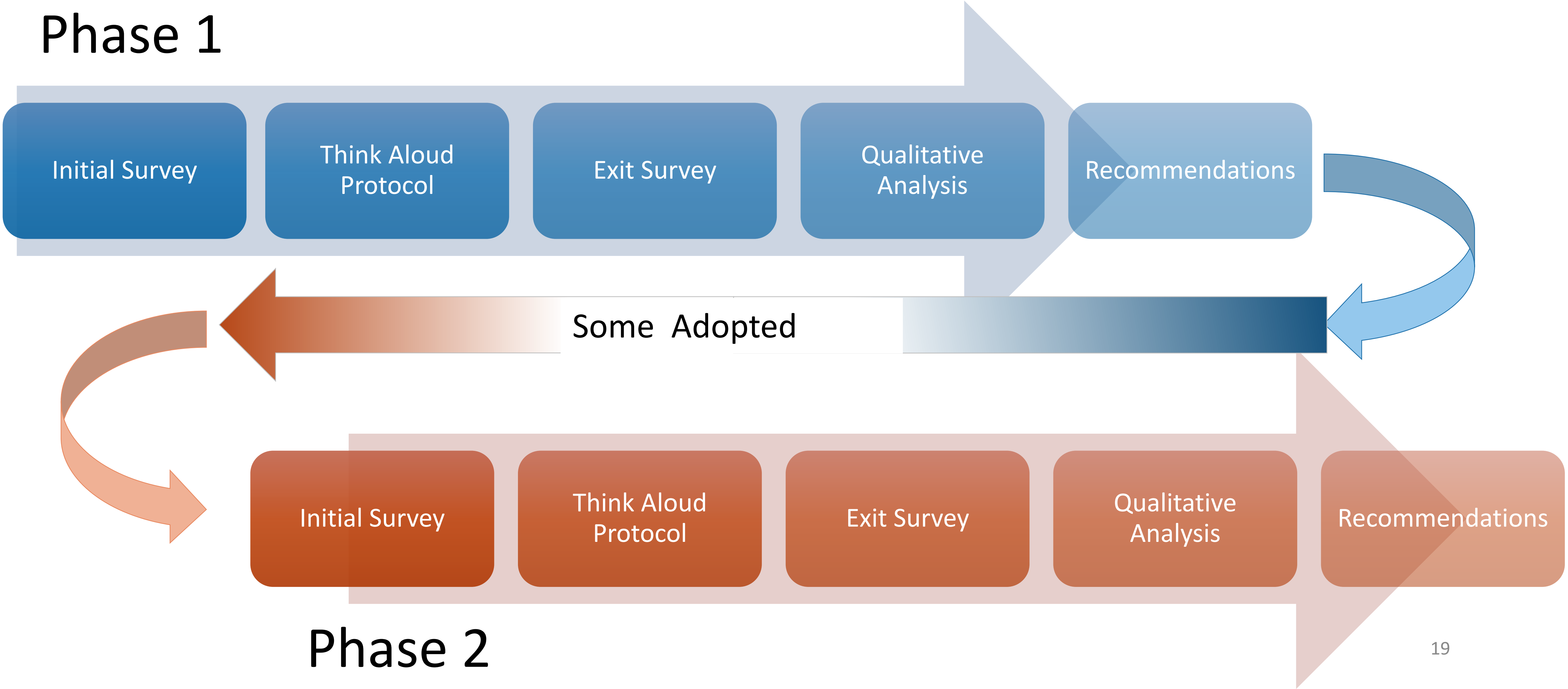
▶

Two Phases

Phase-I

Phase-II

Identical Experimental Protocol



Phase 1

Initial Survey

Think Aloud Protocol

Exit Survey

Qualitative Analysis

Recommendations

Some Adopted

Initial Survey

Think Aloud Protocol

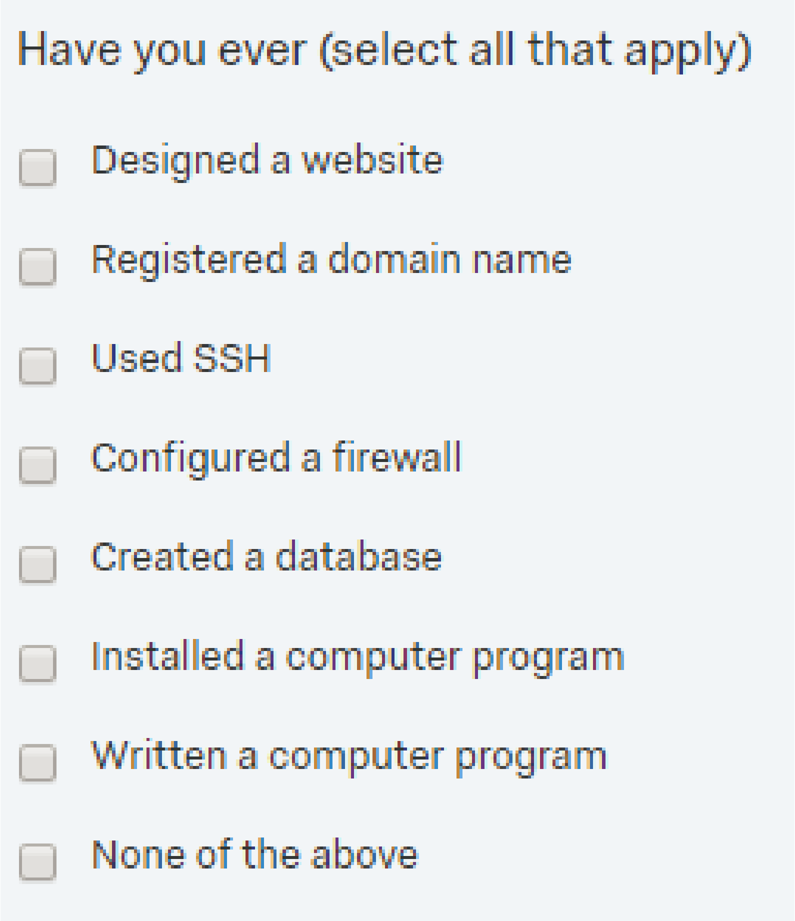
Exit Survey

Qualitative Analysis

Recommendations

Phase 2

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

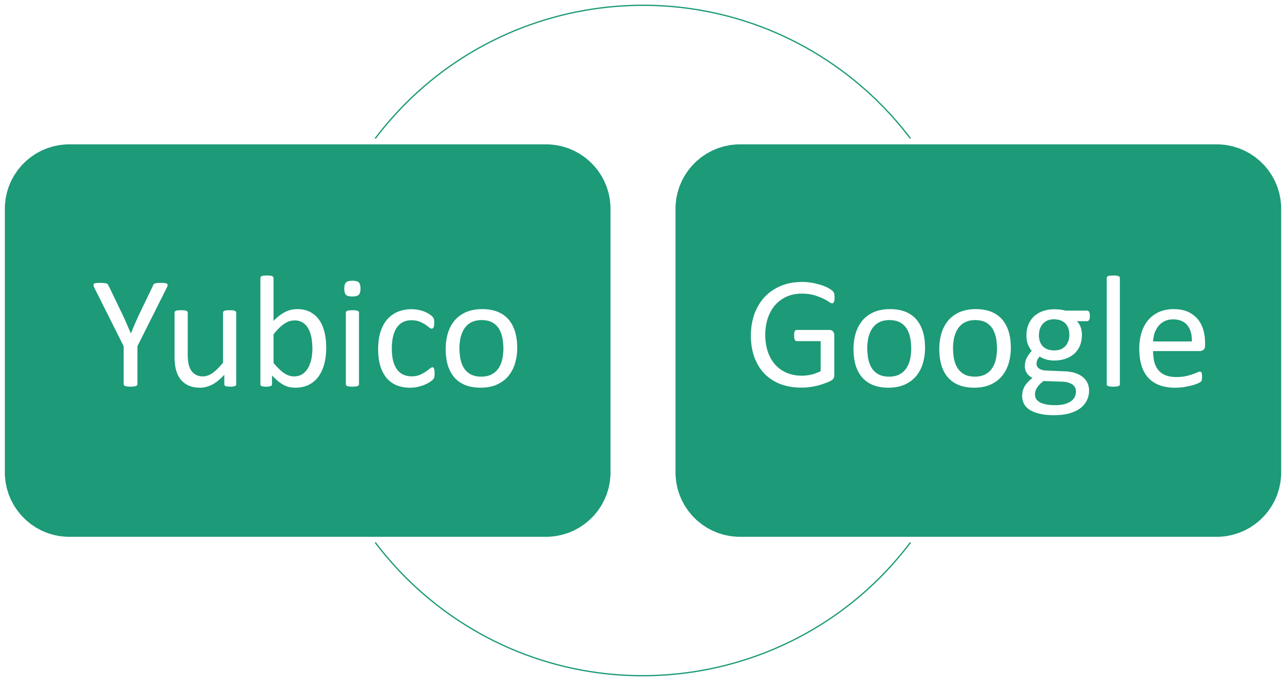
□ Written a computer program

□ 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 *HAISA* (pp. 199-208).

Instructions



Yubico

Google

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

Reasons for the 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 any value by using the keys to secure their accounts

Participant Choices

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

Participant Evaluation

“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.”

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

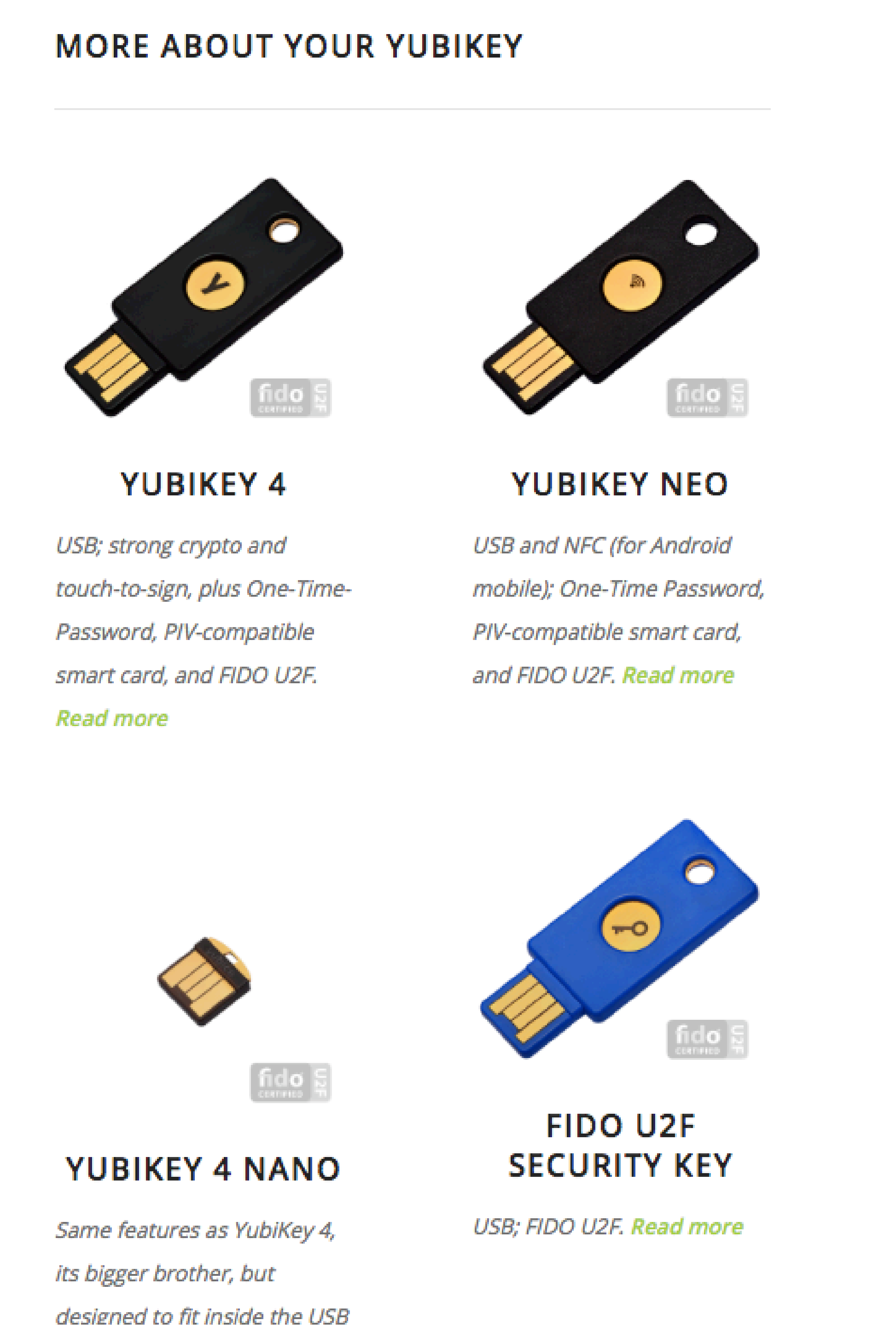
Discussion: return to transcripts as needed for nuance

Analysis: coding allows quantitative as well as qualitative

Recommendations

Recommendations

Phase- I security key comparisons



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**

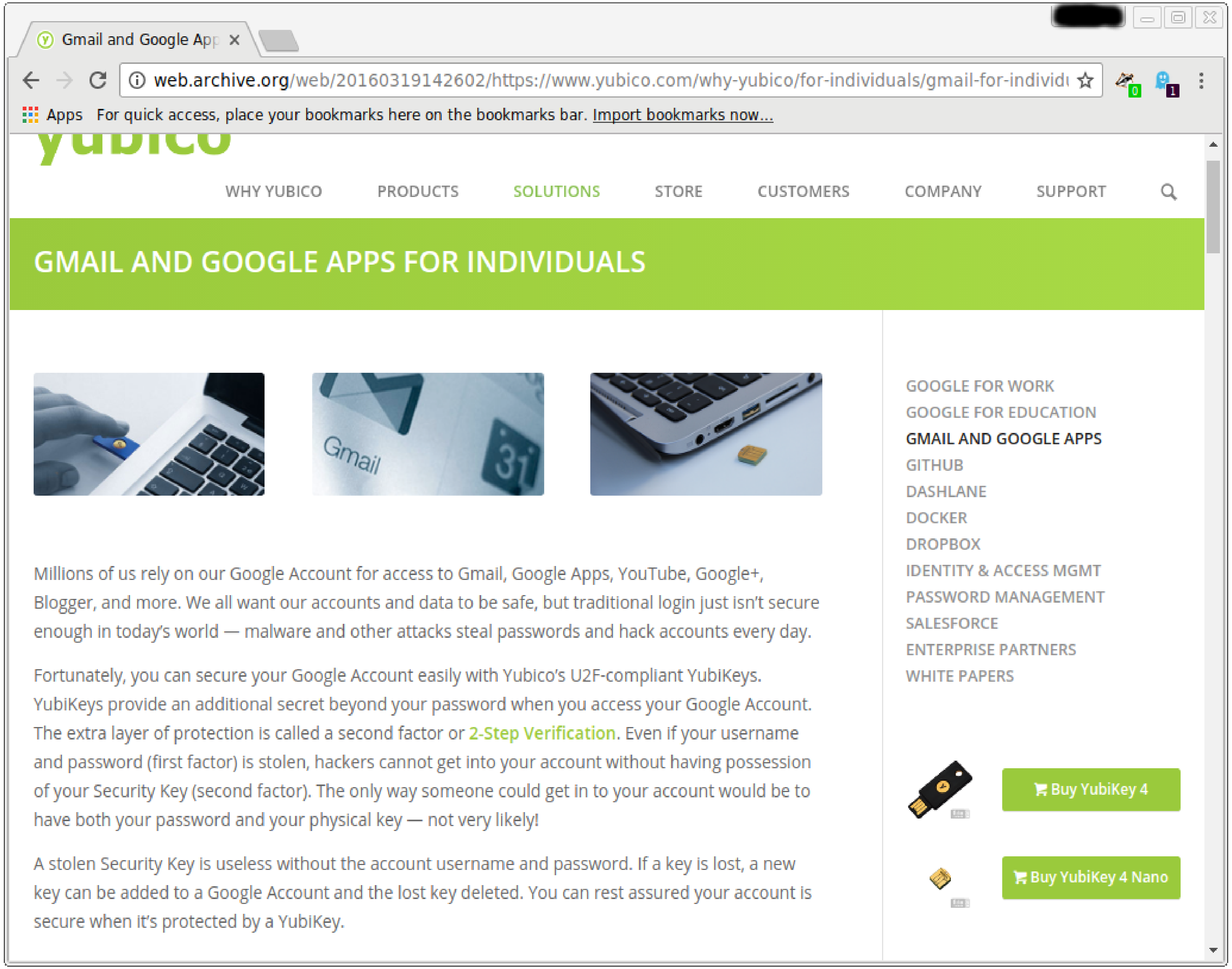
YUBIKEY 4 NANO

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 Setup Instructions



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.

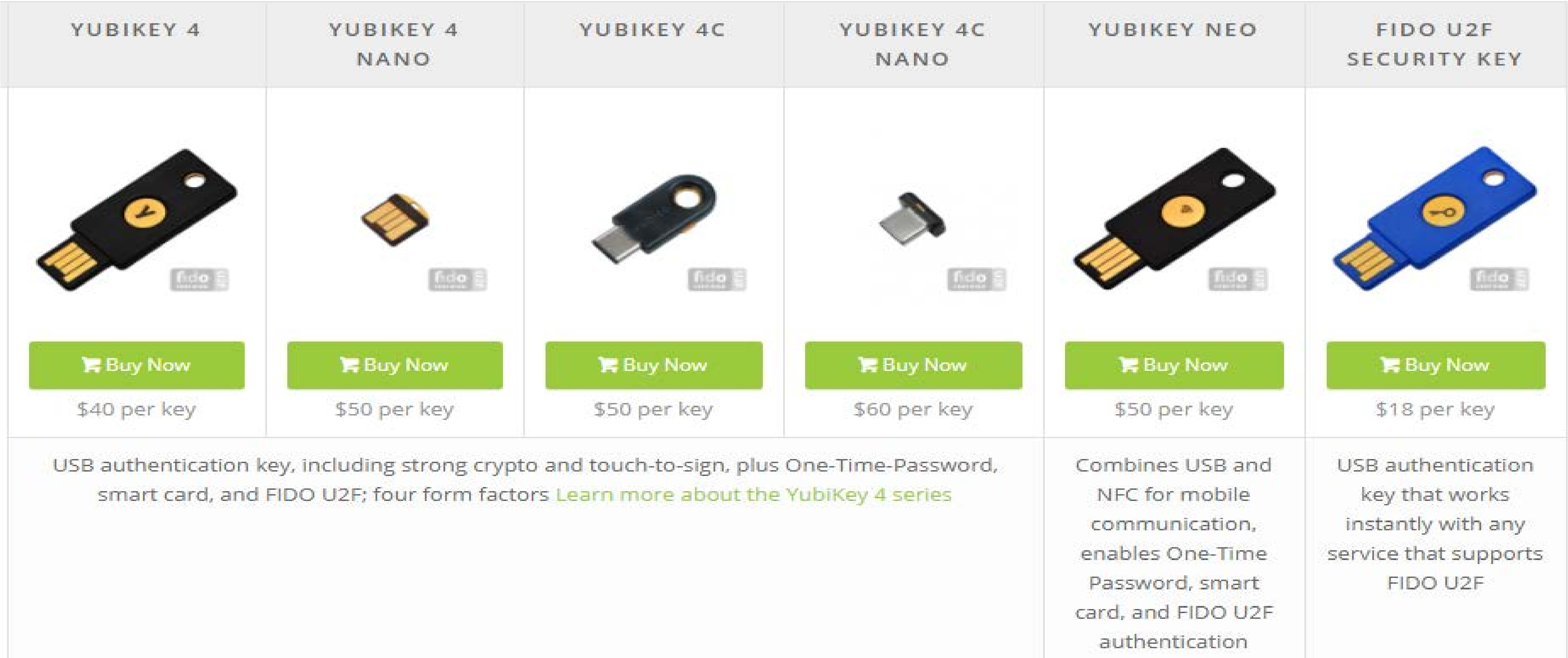
Fortunately, you can secure your Google Account easily with Yubico's U2F-compliant YubiKeys. YubiKeys provide an additional secret beyond your password when you access your Google Account. The extra layer of protection is called a second factor or 2-Step Verification. Even if your username and password (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.

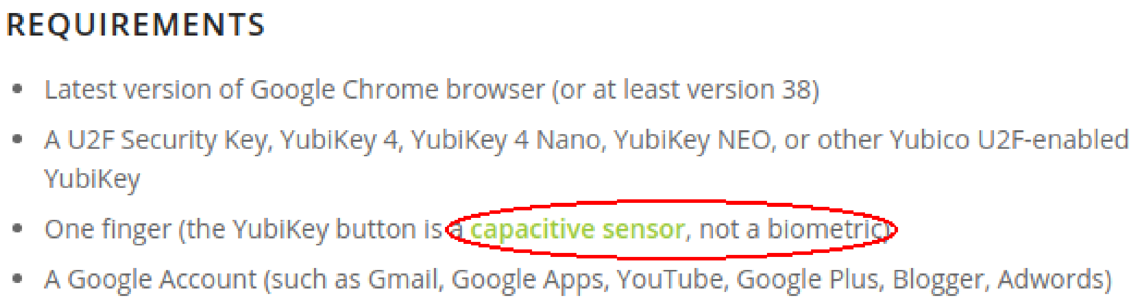
Phase-I Recommendations

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

Phase- II security key comparisons



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



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)

Phase-II 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

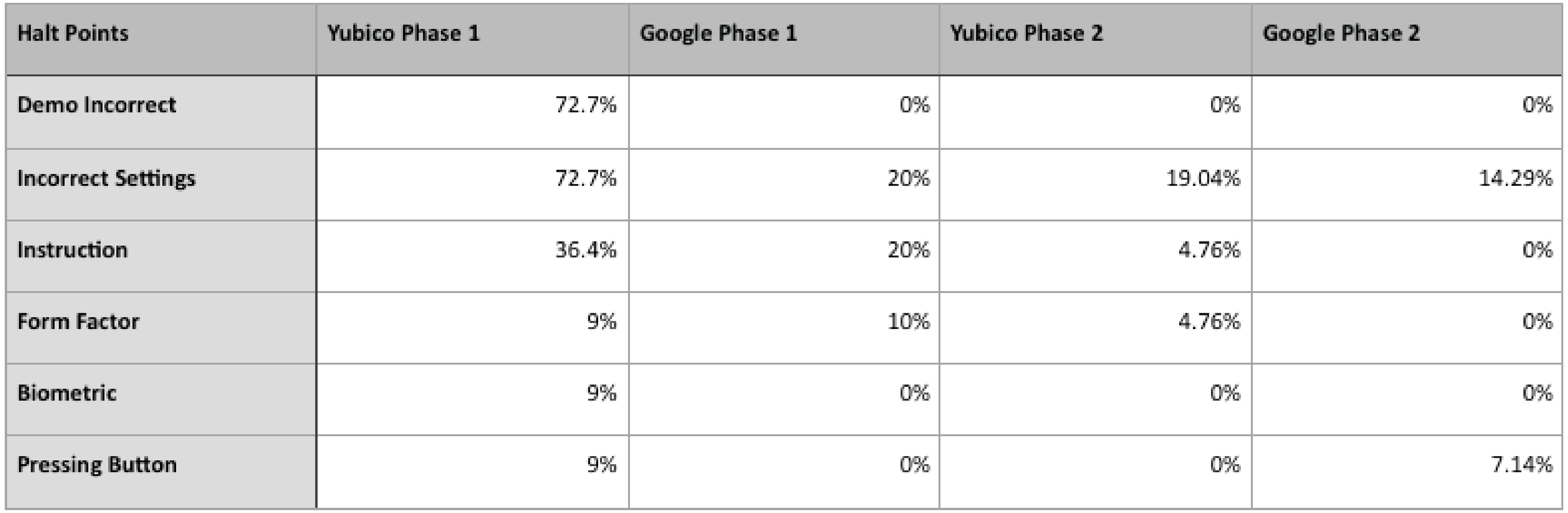
Touch the gold button on the Security Key to generate the secure login credentials.

User Approval and Device Use

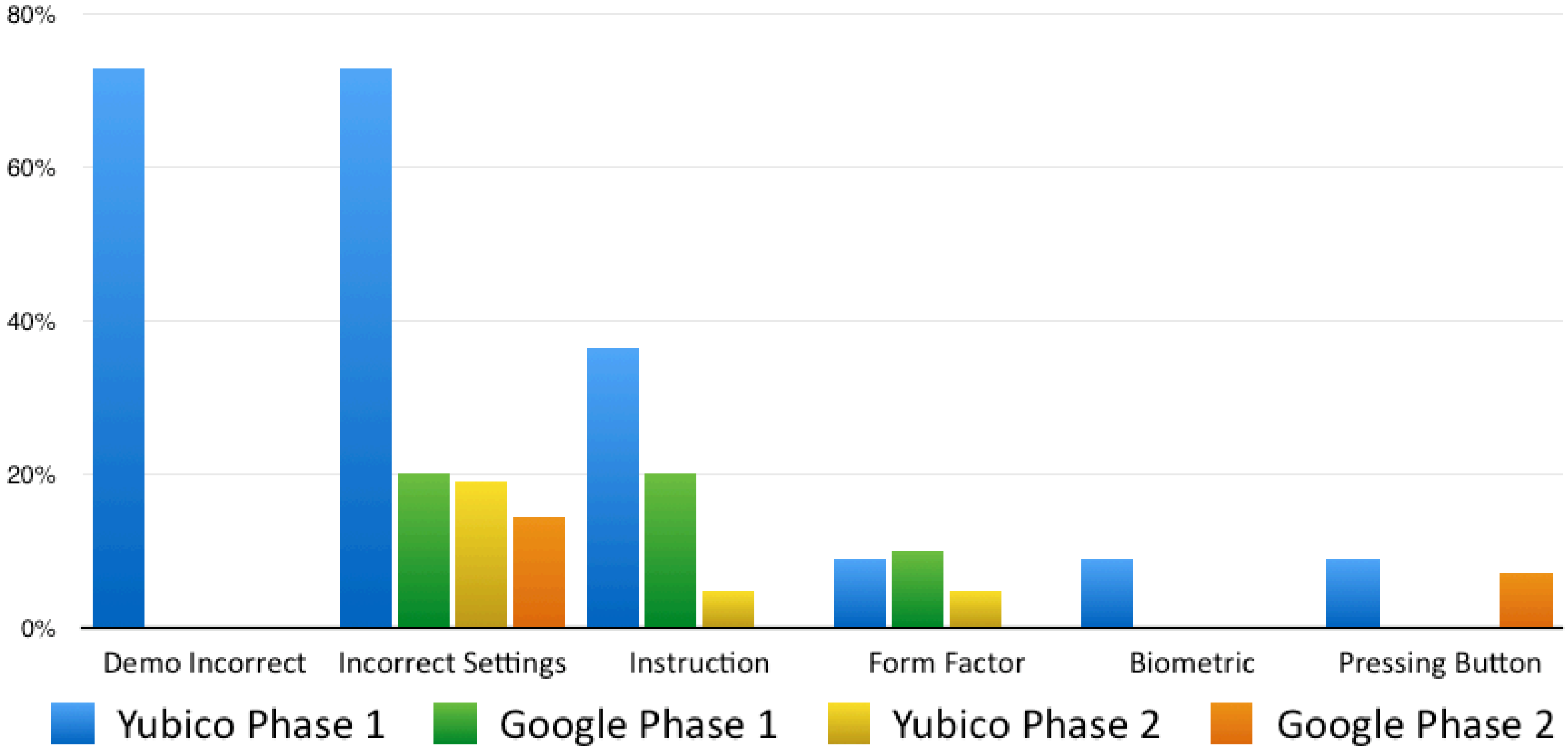
Results

Halt Points

Halt Points



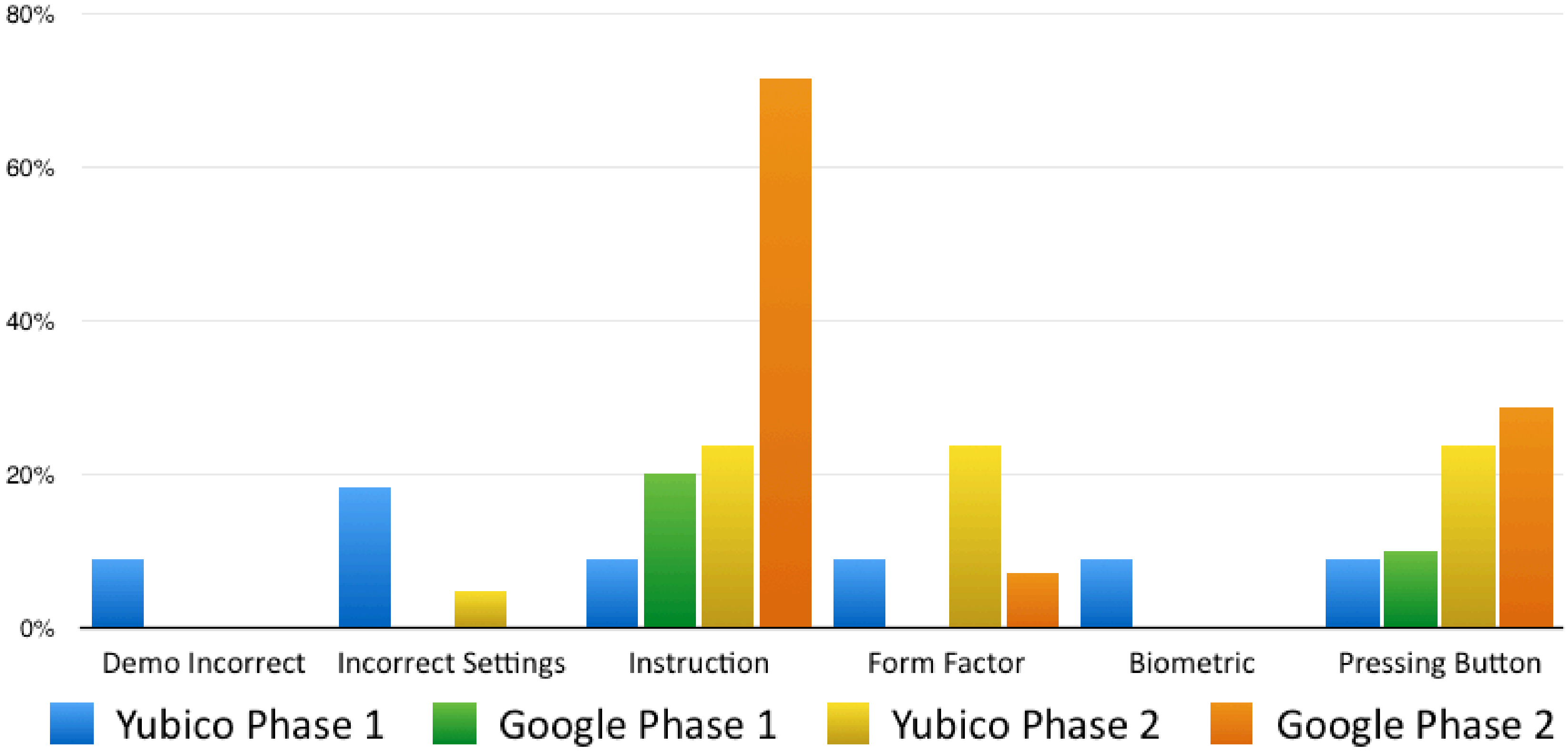
Halt Points	Yubico Phase 1	Google Phase 1	Yubico Phase 2	Google Phase 2
Demo Incorrect	72.7%	0%	0%	0%
Incorrect Settings	72.7%	20%	19.04%	14.29%
Instruction	36.4%	20%	4.76%	0%
Form Factor	9%	10%	4.76%	0%
Biometric	9%	0%	0%	0%
Pressing Button	9%	0%	0%	7.14%



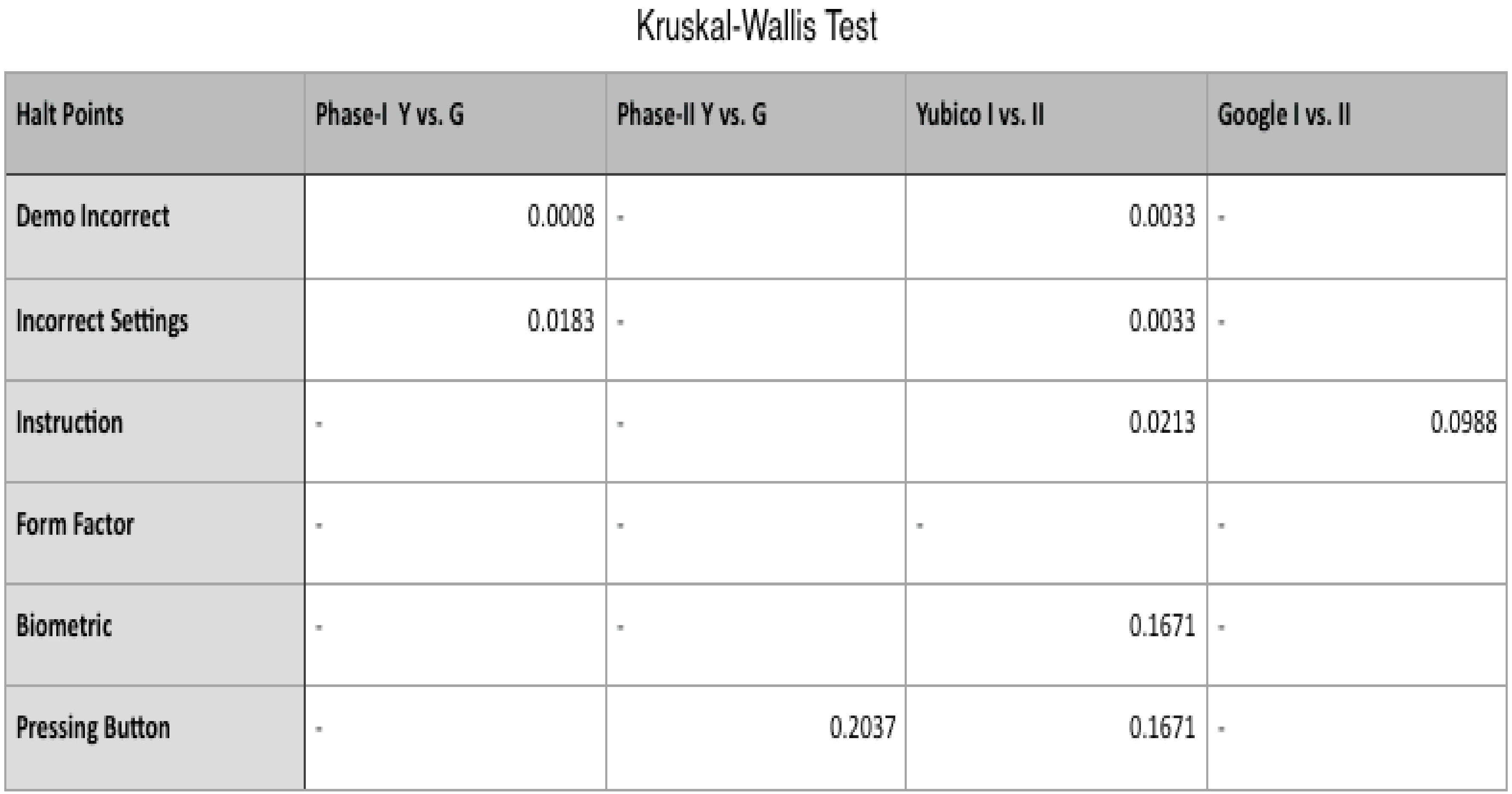
Confusion Points

Confusion Points

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%



Kruskal-Wallis Test



Kruskal-Wallis Test

Halt Points	Phase-I Y vs. G	Phase-II Y vs. G	Yubico I vs. II	Google I vs. II
Demo Incorrect	0.0008	-	0.0033	-
Incorrect Settings	0.0183	-	0.0033	-
Instruction	-	-	0.0213	0.0988
Form Factor	-	-	-	-
Biometric	-	-	0.1671	-
Pressing Button	-	0.2037	0.1671	-

Finding instructions

Demo versus reality

Correctly identifying the device

Biometric versus touch

Confirmation of operation

Communicate the Intrinsic Benefit

Communicating the risk

Recommendations- Phase-II

Recommendations- Phase-II

Finding instructions

Demo versus reality

Correctly identifying the device

Biometric versus touch

Confirmation of installation

Communicate the intrinsic benefit

Communicating the risks

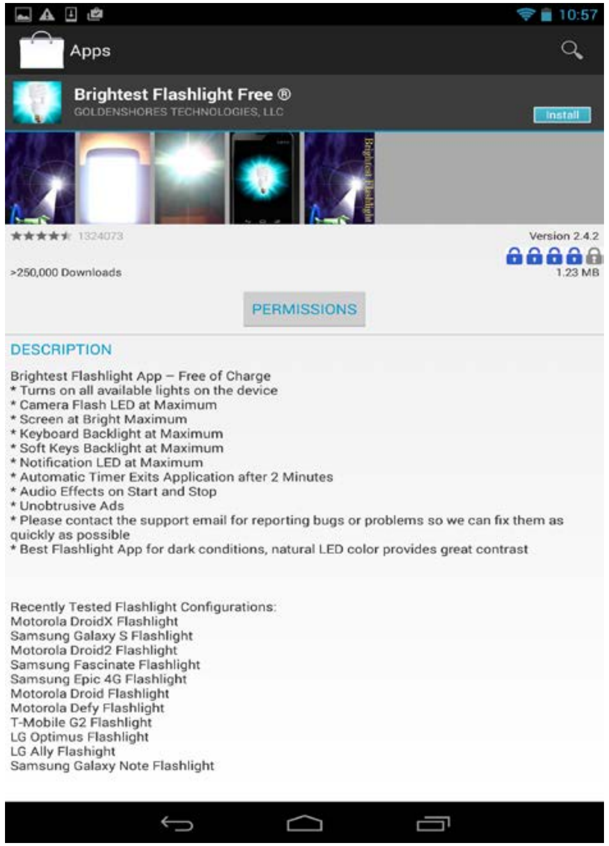
Risk Communication

Future Research & Call To Action

Risk Communication for 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 myasthenic syndrome (muscle weakness due to auto-antibodies), hypercalcemia, 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.



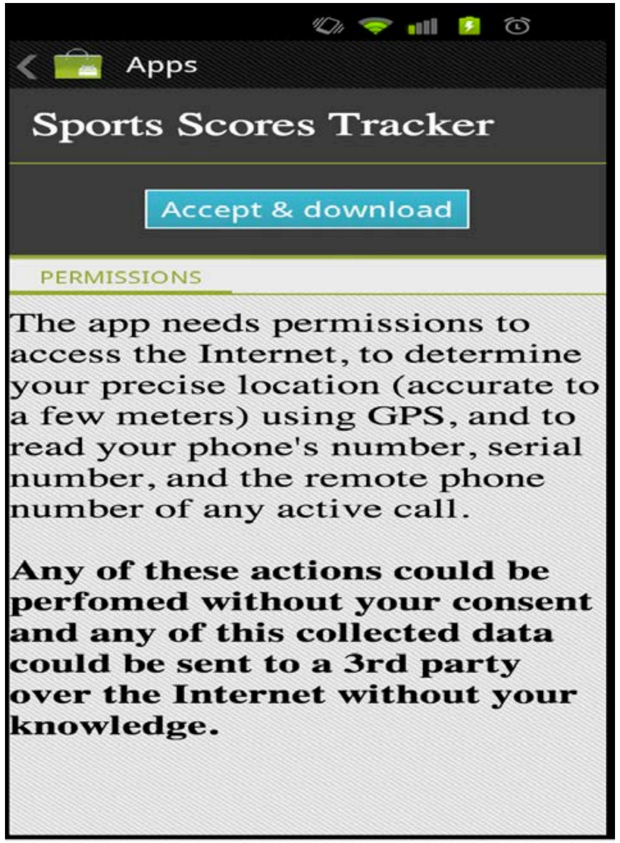
Brightest Flashlight Free ®
GOLDENSHORES TECHNOLOGIES, LLC

★★★★½ 1324073
Version 2.4.2
>250,000 Downloads
1.23 MB

DESCRIPTION

Brightest Flashlight App – Free of Charge
* Turns on all available lights on the device
* Camera Flash LED at Maximum
* Screen at Bright Maximum
* Keyboard Backlight at Maximum
* Soft Keys Backlight at Maximum
* Notification LED at Maximum
* Automatic Timer Exits Application after 2 Minutes
* Audio Effects on Start and Stop
* Unobtrusive Ads
* Please contact the support email for reporting bugs or problems so we can fix them as quickly as possible
* Best Flashlight App for dark conditions, natural LED color provides great contrast

Recently Tested Flashlight Configurations:
Motorola DroidX Flashlight
Samsung Galaxy S Flashlight
Motorola Droid2 Flashlight
Samsung Fascinate Flashlight
Samsung Epic 4G Flashlight
Motorola Droid Flashlight
Motorola Defy Flashlight
T-Mobile G2 Flashlight
LG Optimus Flashlight
LG Ally Flashlight
Samsung Galaxy Note Flashlight

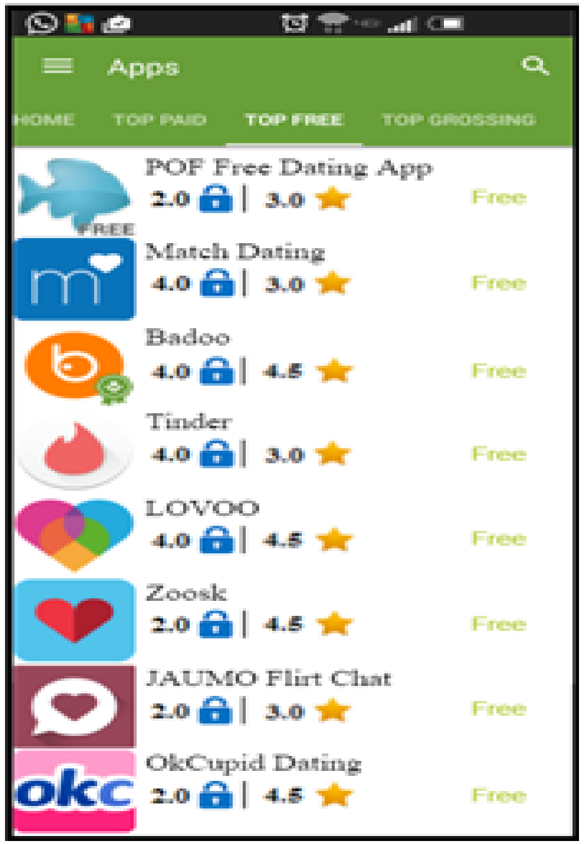


Sports Scores Tracker

PERMISSIONS

The app needs permissions to access the Internet, to determine your precise location (accurate to a few meters) using GPS, and to read your phone's number, serial number, and the remote phone number of any active call.

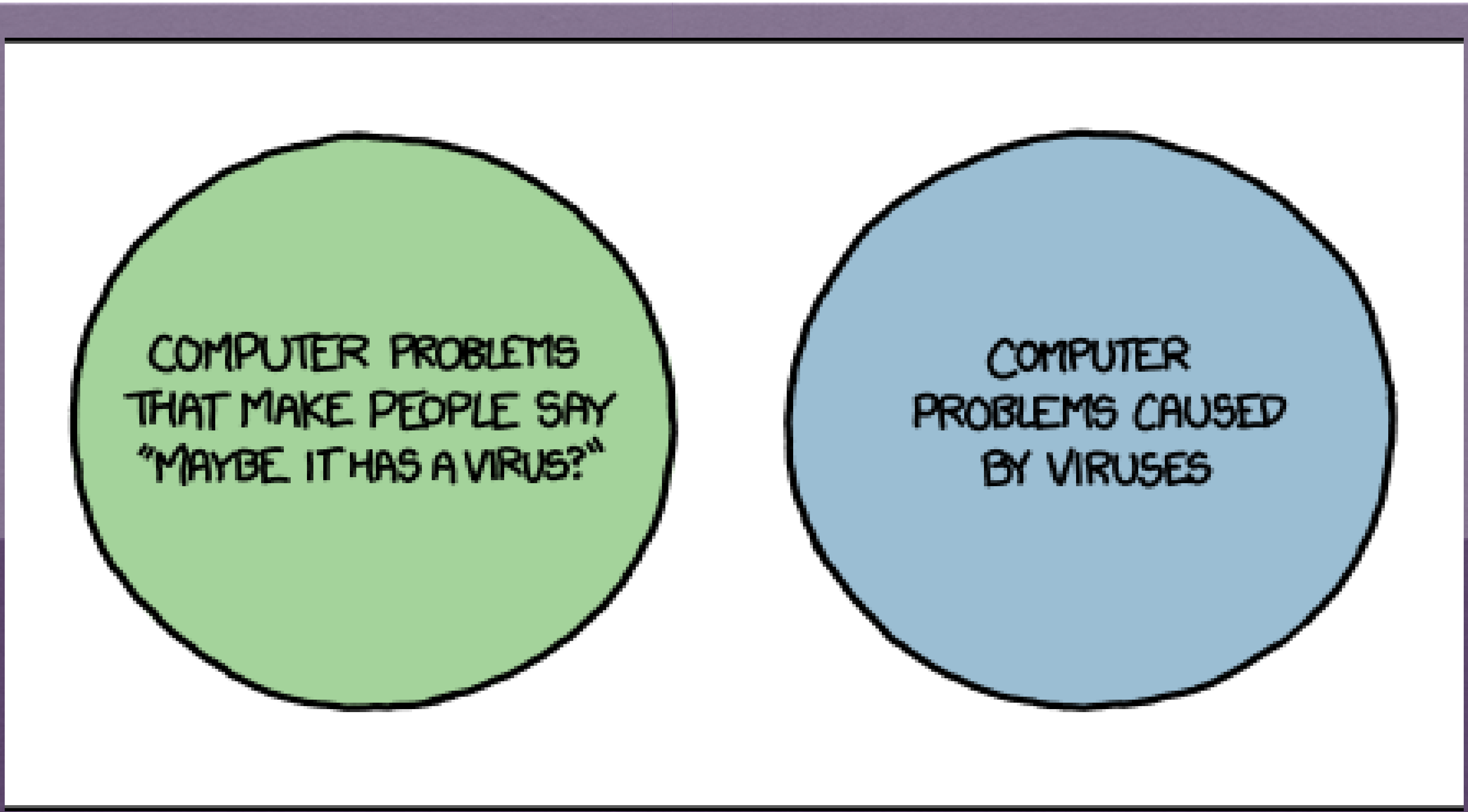
Any of these actions could be perfomed without your consent and any of this collected data could be sent to a 3rd party over the Internet without your knowledge.



POF Free Dating App	2.0 🔒	3.0 ★	Free
Match Dating	4.0 🔒	3.0 ★	Free
Badoo	4.0 🔒	4.5 ★	Free
Tinder	4.0 🔒	3.0 ★	Free
LOVOO	4.0 🔒	4.5 ★	Free
Zoosk	2.0 🔒	4.5 ★	Free
JAUMO Flirt Chat	2.0 🔒	3.0 ★	Free
OkCupid Dating	2.0 🔒	4.5 ★	Free

Summarize, Simplify Risks

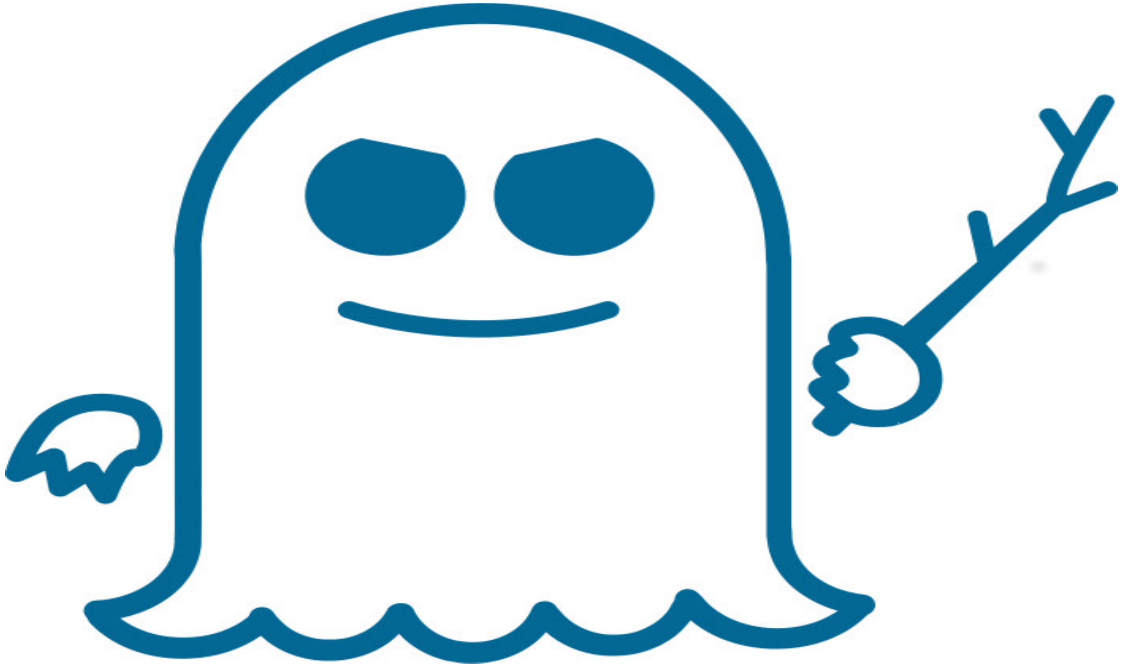
Use Mental Models


COMPUTER PROBLEMS THAT MAKE PEOPLE SAY "MAYBE IT HAS A VIRUS?"
COMPUTER PROBLEMS CAUSED BY VIRUSES

https://www.youtube.com/watch?v=zicpivBH8p8

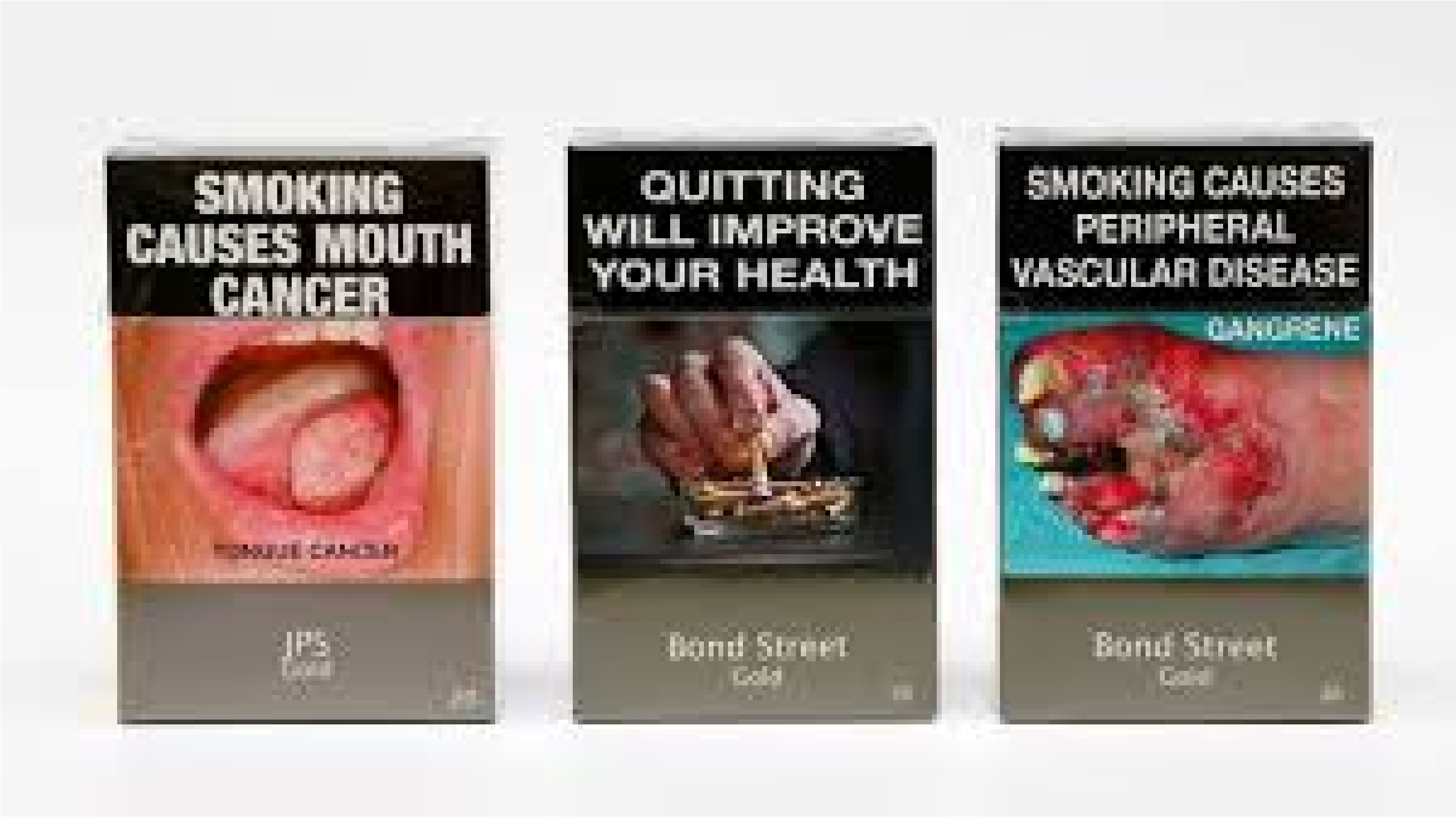
https://www.youtube.com/watch?v=gIYINvH62ZY

Clear, Urgent Communication

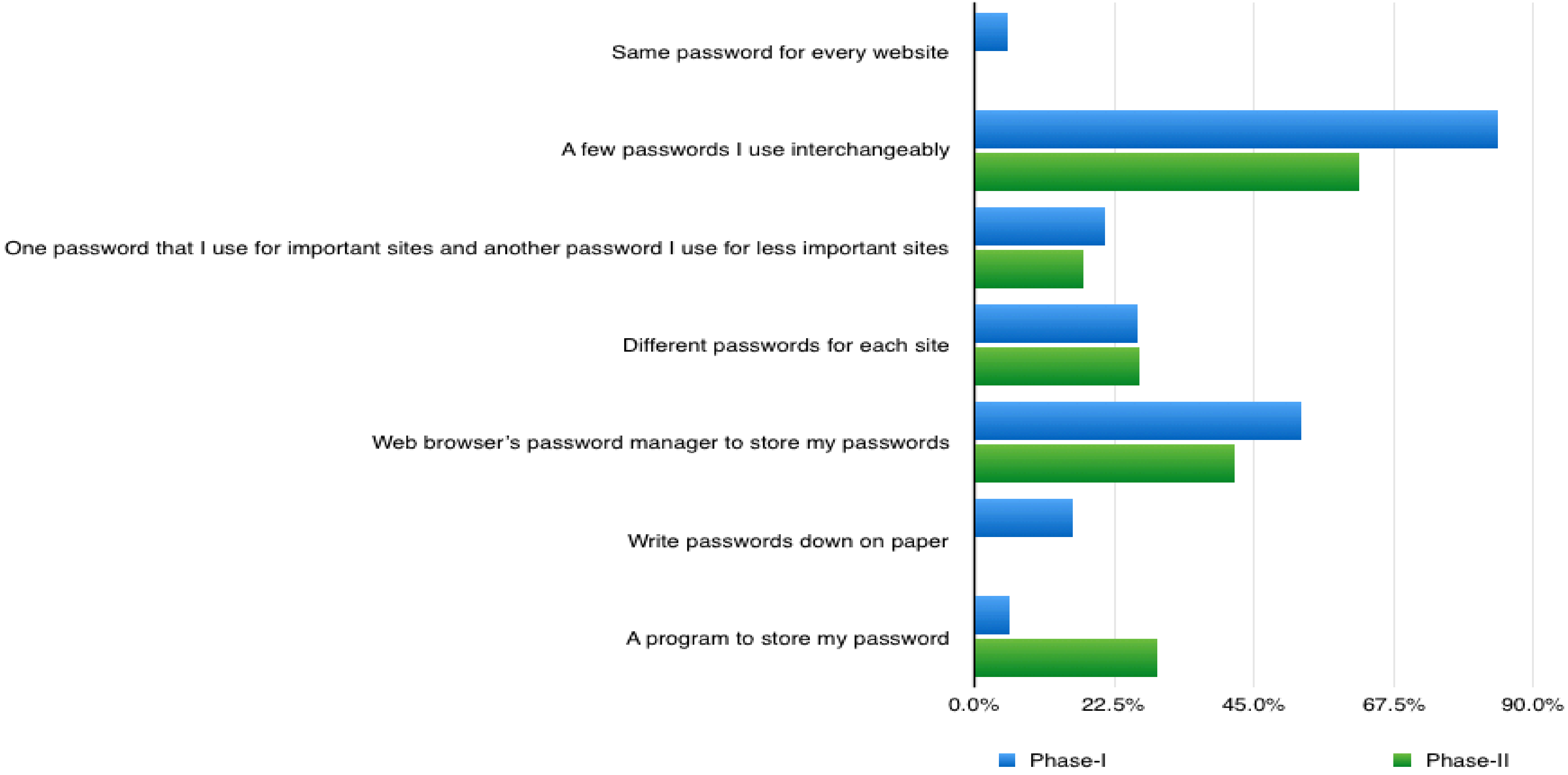


Multiple CPU Hardwares Information Disclosure Vulnerability: CVE-2017-5753

Visceral Risk Communication


SMOKING CAUSES MOUTH CANCER
TONGUE CANCER
JPS
Gold
QUITTING WILL IMPROVE YOUR HEALTH
Bond Street
Gold
SMOKING CAUSES PERIPHERAL VASCULAR DISEASE
GANGRENE
Bond Street
Gold

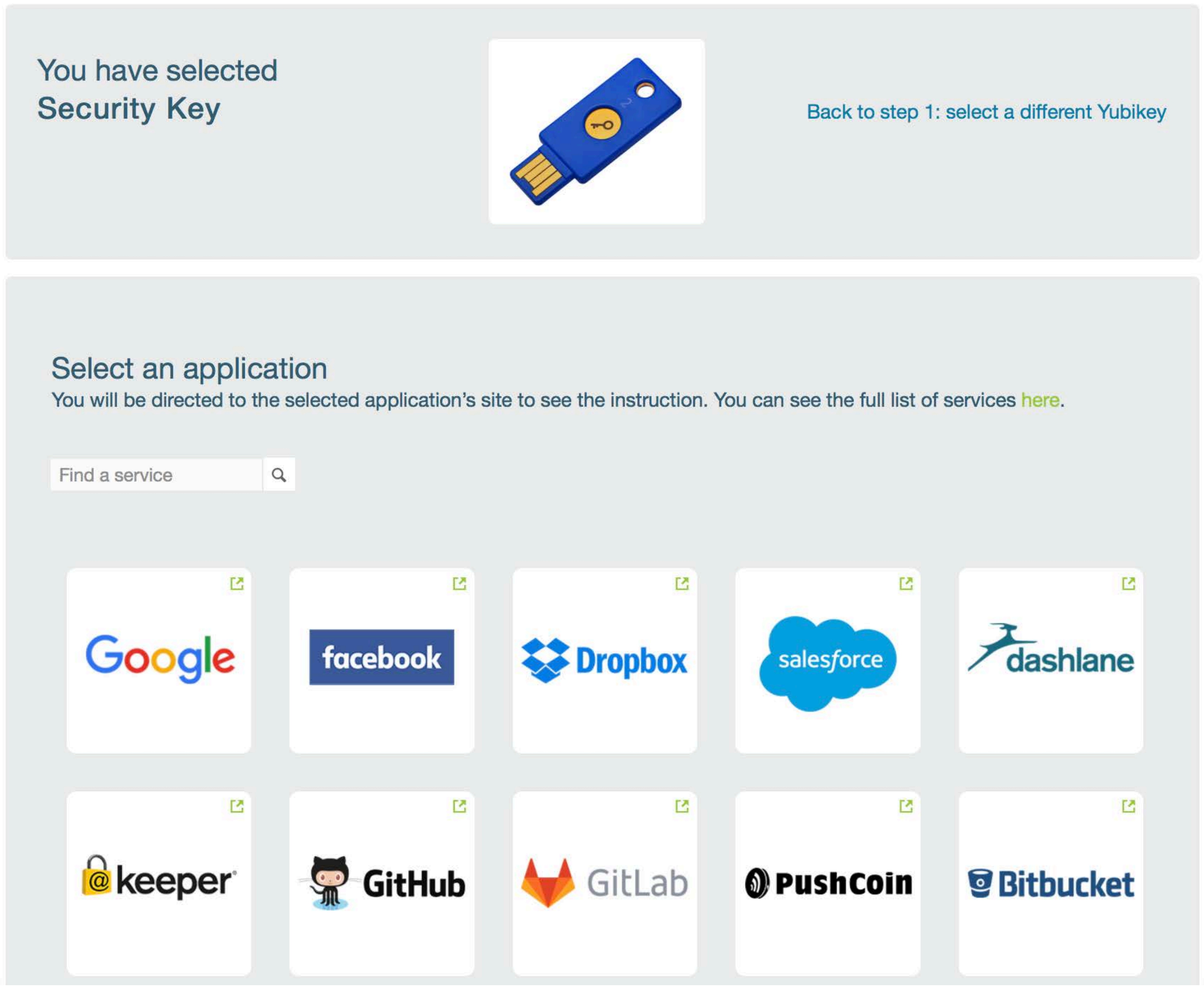
Password Behavior



Visceral Risk Communication

Takeaways

- Providing the technology is not enough
- We cannot predict; Watch in-action
- Communicate why
- Risk communication for motivation
- Periodic positive feedback
- Qualitative studies can be quantified



You have selected
Security Key

Back to step 1: select a different Yubikey

Select an application

You will be directed to the selected application’s site to see the instruction. You can see the full list of services here.

Find a service

Sanchari Das
@SanchariDecrypt

Gianpaolo Russo
russog@indiana.edu

Andrew Dingman
@ACDingman

Dr. L. Jean Camp
www.ljean.com
@ljean