I Think They're Trying to Tell Me Something

Advice Sources and Selection for Digital Security

Elissa M. Redmiles, Amelia R. Malone, and Michelle L. Mazurek

@eredmil1

HCIL

MARYLAND CYBERSECURITY CENTER

Security Advice

U.S. CERT
~30,000 words
60+ topics

McAfee
~40,000 words
49 topics

NCPC
~12,000 words
30 topics

Research Questions

1. Where do users get advice?
2. How do they evaluate this advice?
3. Do users with different backgrounds make different choices?

Research Design

Research Questions

Where do users get advice?

Why do they take it?

How can we improve it?

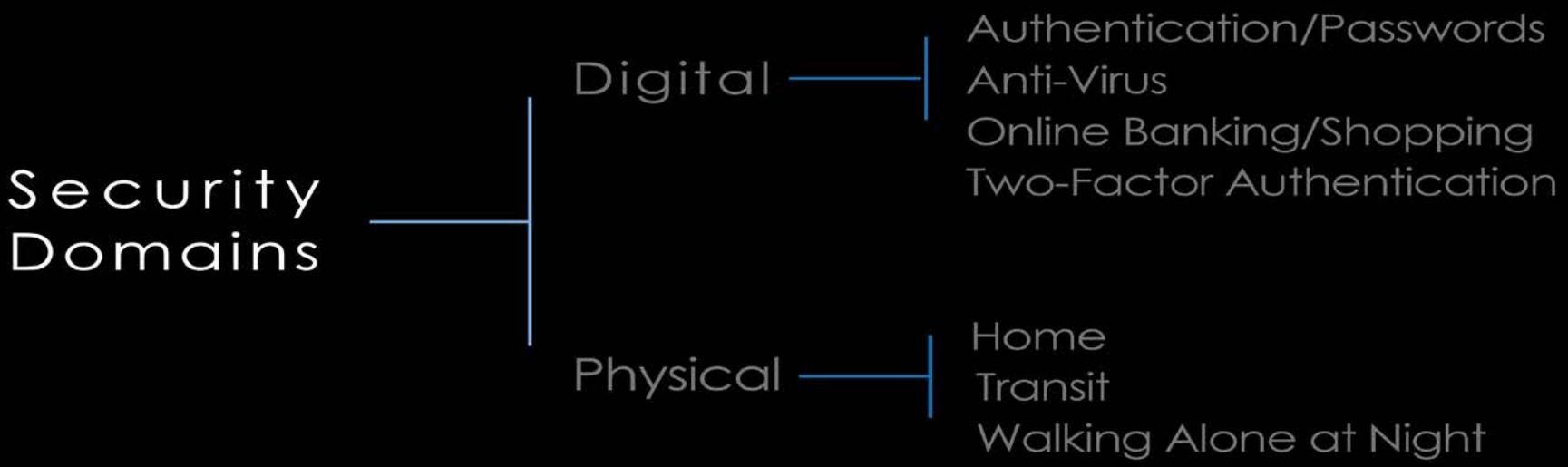
Methods

Semi-structured 60 minute interview w/ 25 participants

Questions about digital and physical security:

- Device securement, updating, 2FA
- Dwelling and transit security, walking alone @ night

Interview Details



Questions

Information Source | Decision Making | Strategies Not Used | Negative Experiences | General Advice Seeking & Eval.

Selected Results

Advice Evaluation

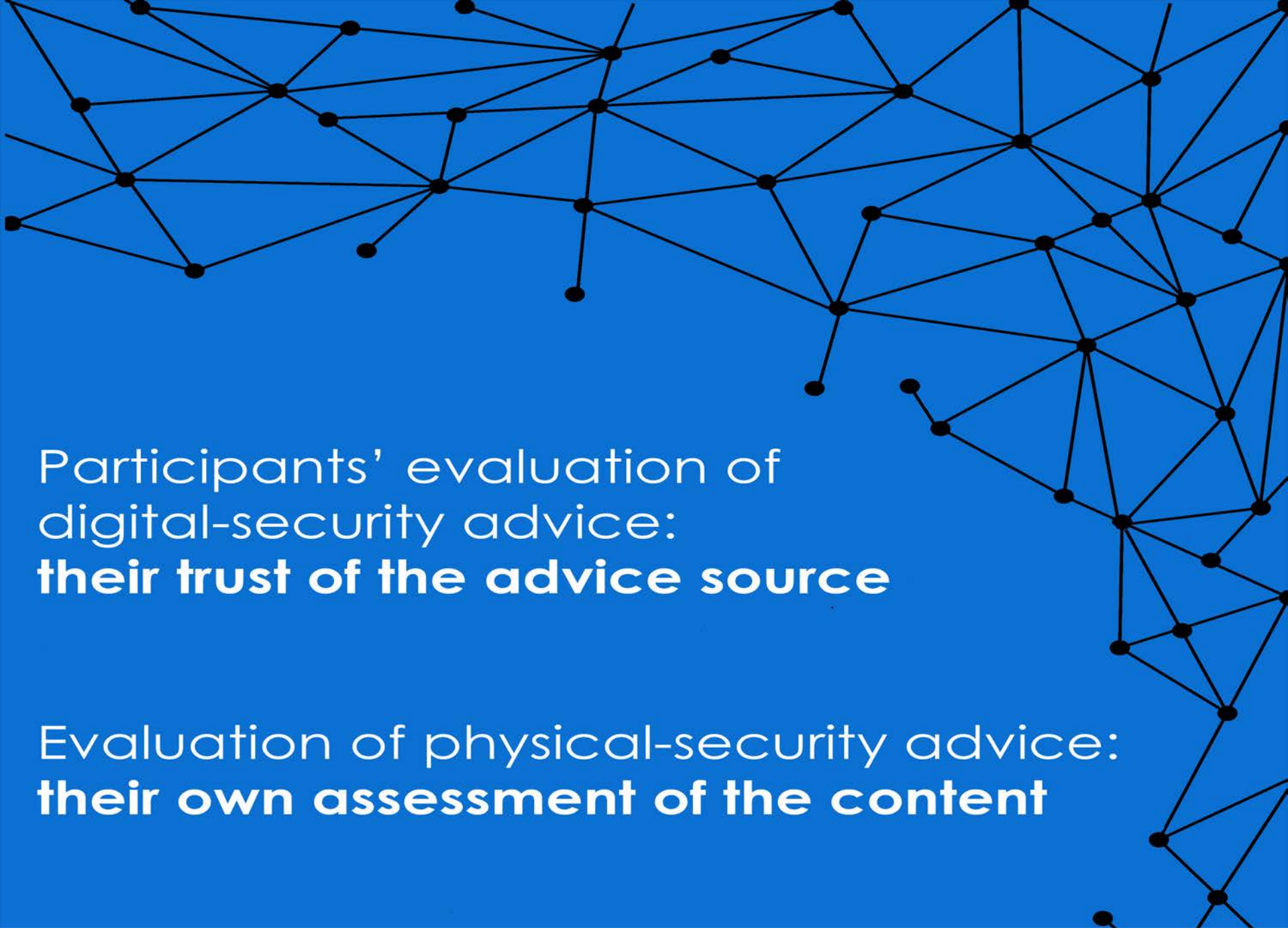
Why did you choose to use or not use this security strategy?

Security Sensitivity

Do you hold a security clearance or work with HIPAA or FERPA data?

Negative Security Experience

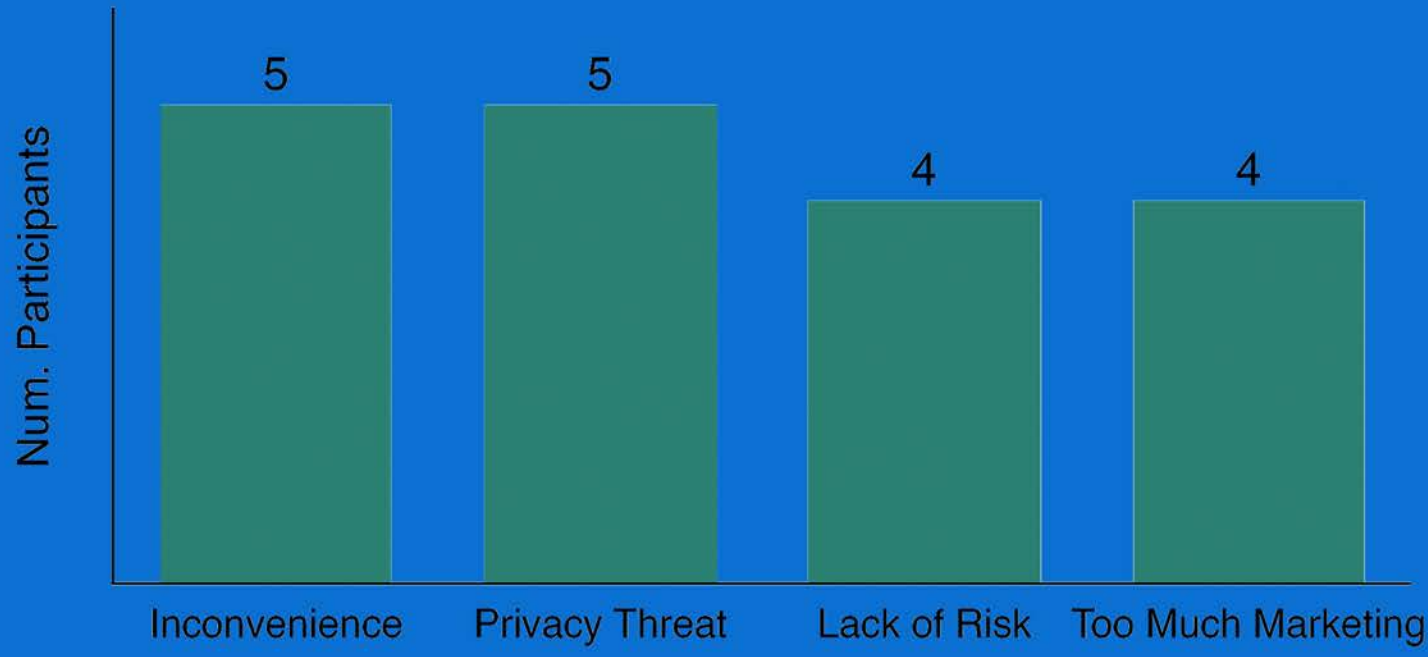
Have you ever had a negative experience with this activity?


Participants' evaluation of digital-security advice:
their trust of the advice source
Evaluation of physical-security advice:
their own assessment of the content

"With computer security, I'm securing myself from threats that I don't even know anything about...

I know when somebody walks up with a gun that I should be worried."

Participants rejected advice for containing **too much marketing** or **threatening their privacy**



Selected Results

Advice Evaluation

Why did you choose to use or not use this security strategy?

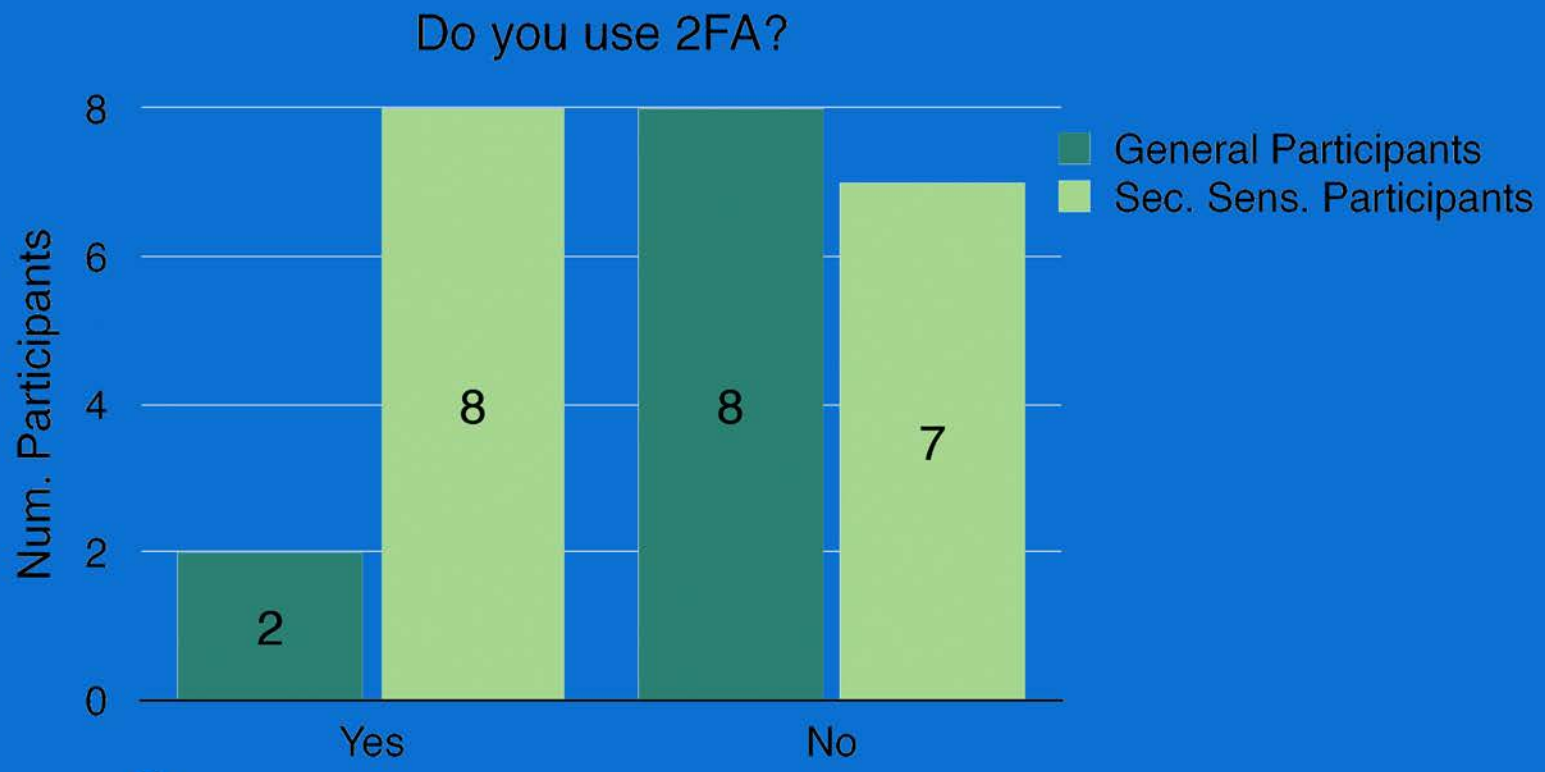
Security Sensitivity

Do you hold a security clearance or work with HIPAA or FERPA data?

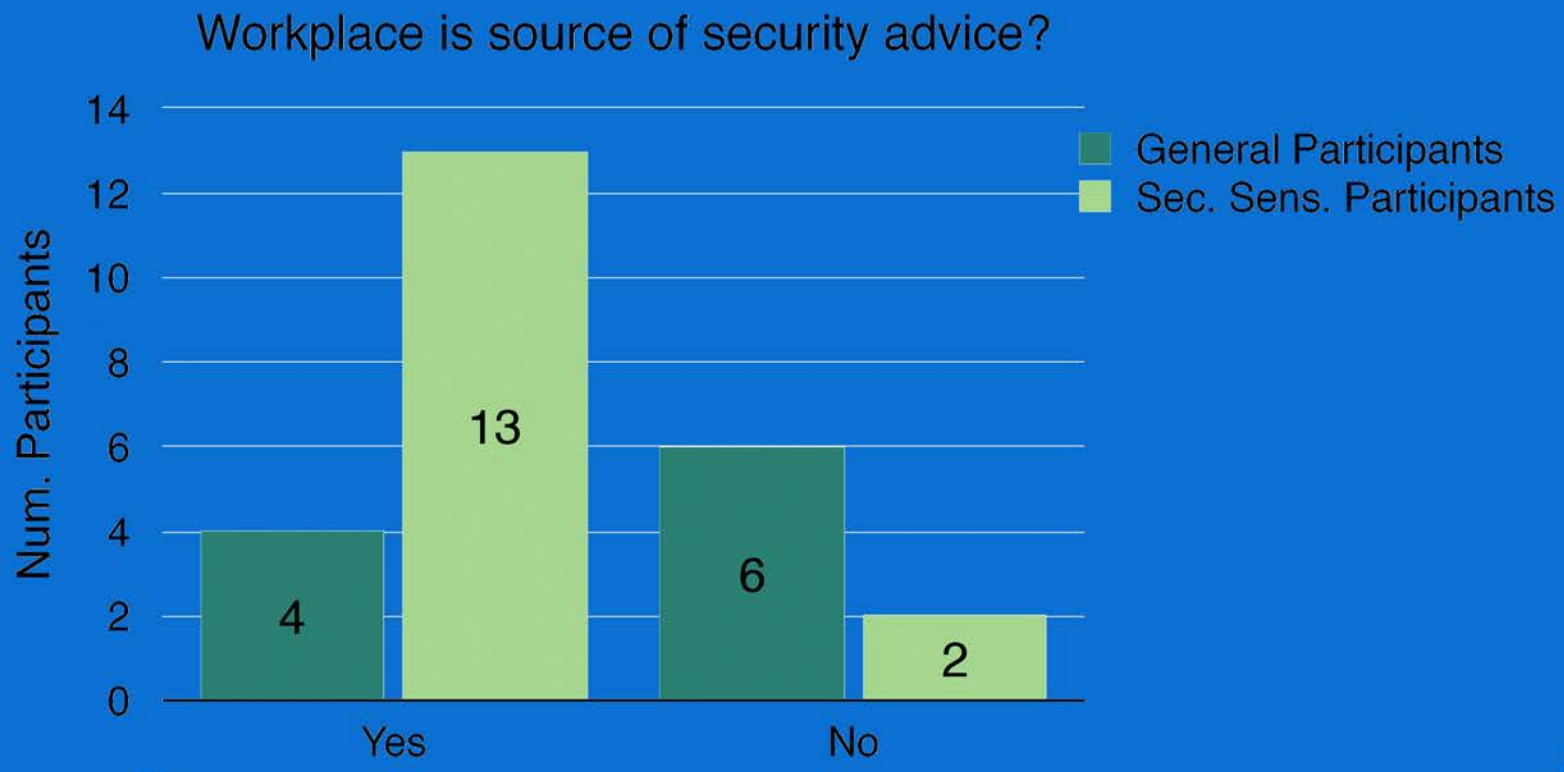
Negative Security Experience

Have you ever had a negative experience with this activity?

Security sensitive participants differ from general participants in **behavior, source & beliefs**



Security sensitive participants differ from general participants in **behavior, source & beliefs**



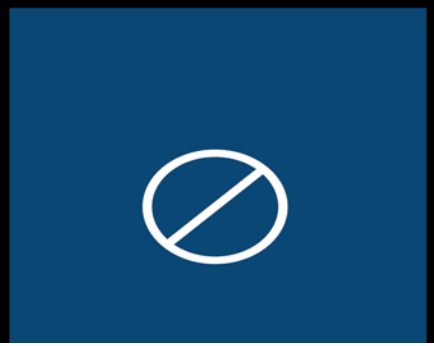
Selected Results

Advice Evaluation

Why did you choose to use or not use this security strategy?

Security Sensitivity

Do you hold a security clearance or work with HIPAA or FERPA data?



Negative Security Experience

Have you ever had a negative experience with this activity?

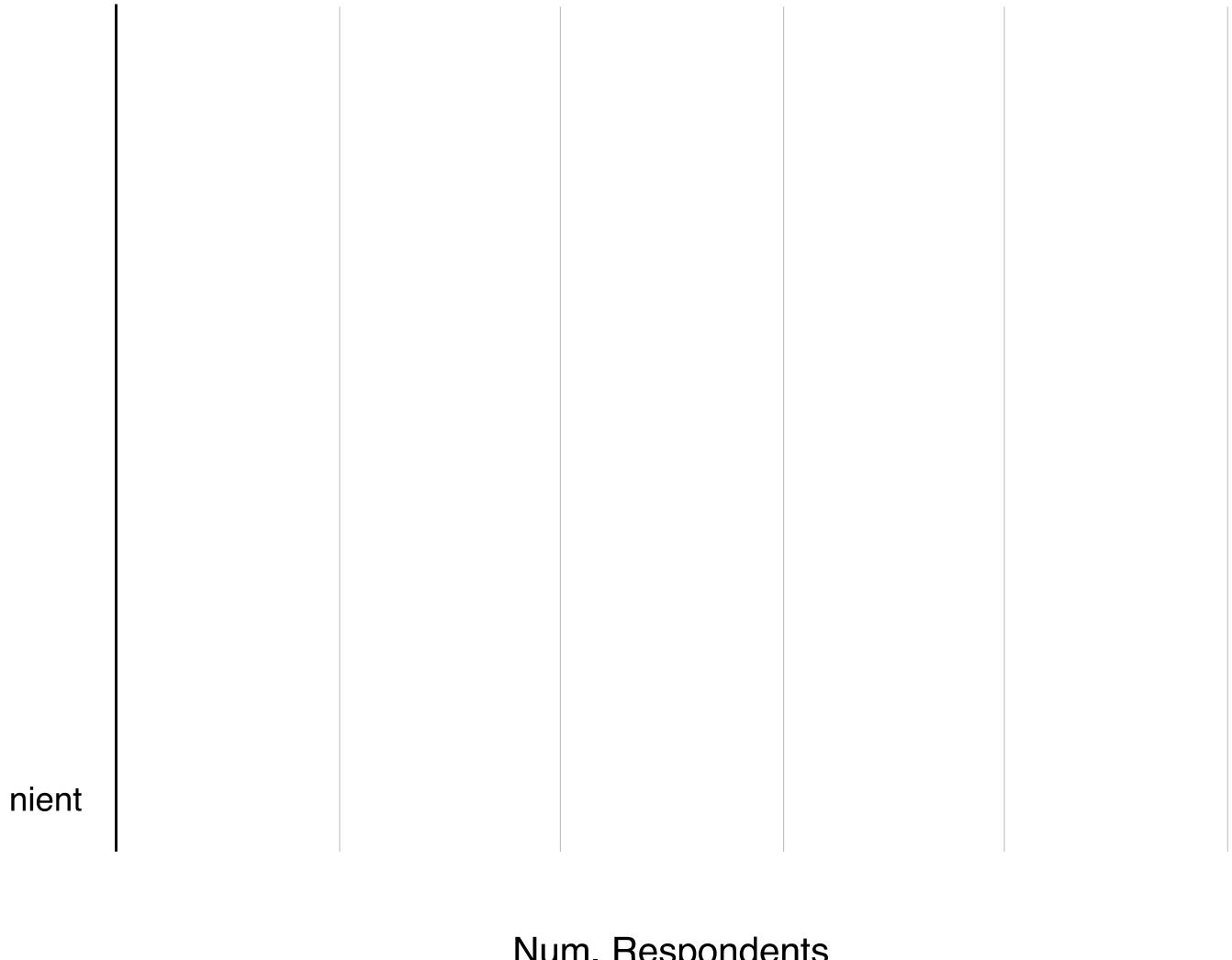

Participants noted the
impact of negative-security events
including events portrayed in
fictional narratives like T.V. shows
on altering their security behavior

“I put a password on my WiFi network after watching a TV show.

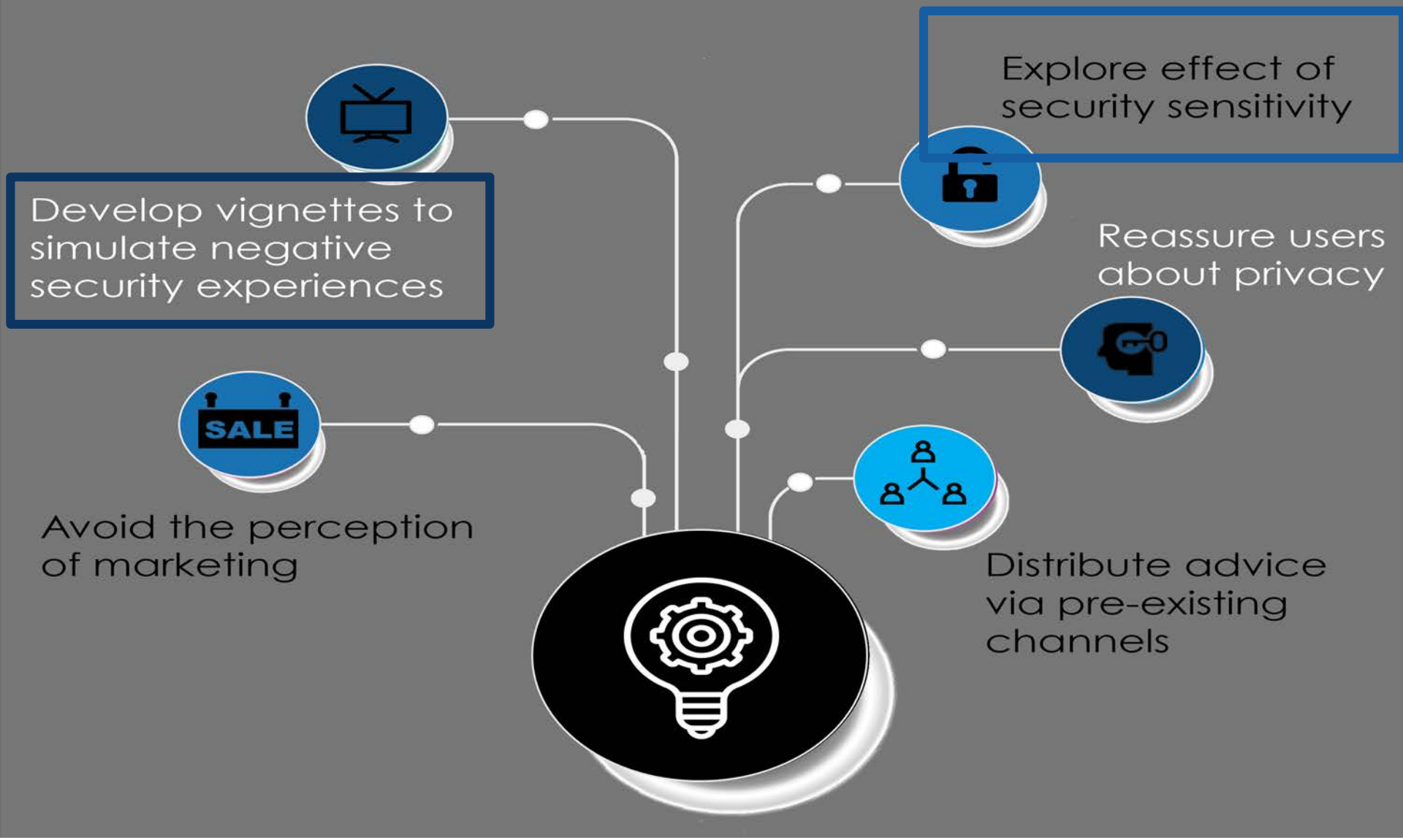
It showed people going by houses and WiFi snooping

. . . shows like that, they make you think.”

Advice Rejection



Research & Design Recommendations



Summary

Research Questions

Where do users get advice?

Why do they take it?

How can we improve it?

Methods

Semi-structured interview w/ 25 participants

Selected Results

Trust of source key metric for digital security

Advice rejection: marketing & privacy concern

Security-sensitive participants differ

Fictional narratives can alter security behavior

Questions?
Contact: eredmiles@cs.umd.edu

Measuring and Improving Management of Today's PKI

PI(s): Dave Levin

Researcher(s): Frank Cangialosi

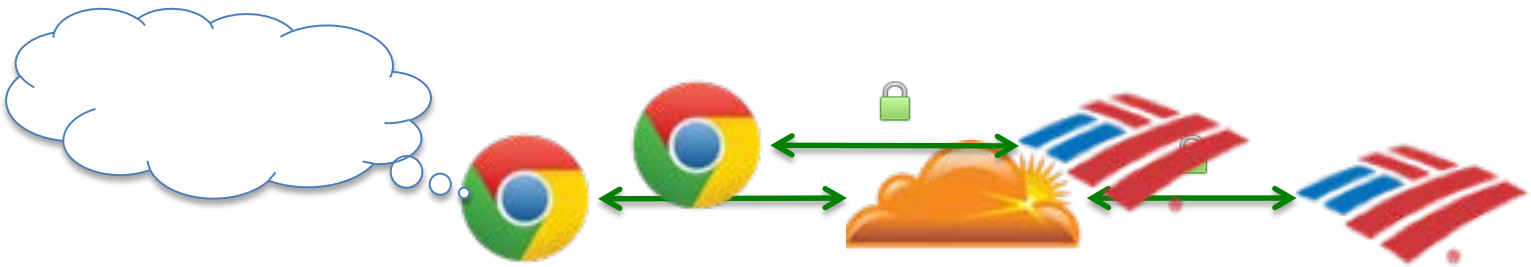
For more details, see Frank's poster

Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?

Fundamental assumption:

The only one who knows Alice's key is Alice



Reality:

Many (and most popular) websites are hosted on CDNs and web hosting providers

To support HTTPS, they *share their private keys* with these providers

Studying Key Sharing in the Web's PKI

Wide-scale, IPv4-wide measurement study
From Rapid7 scans

- Mar 2013-Oct 2015
- 5.1M valid certs
- 2.6M unique domains

How often do organizations share their private keys?

How many keys have third party providers aggregated?

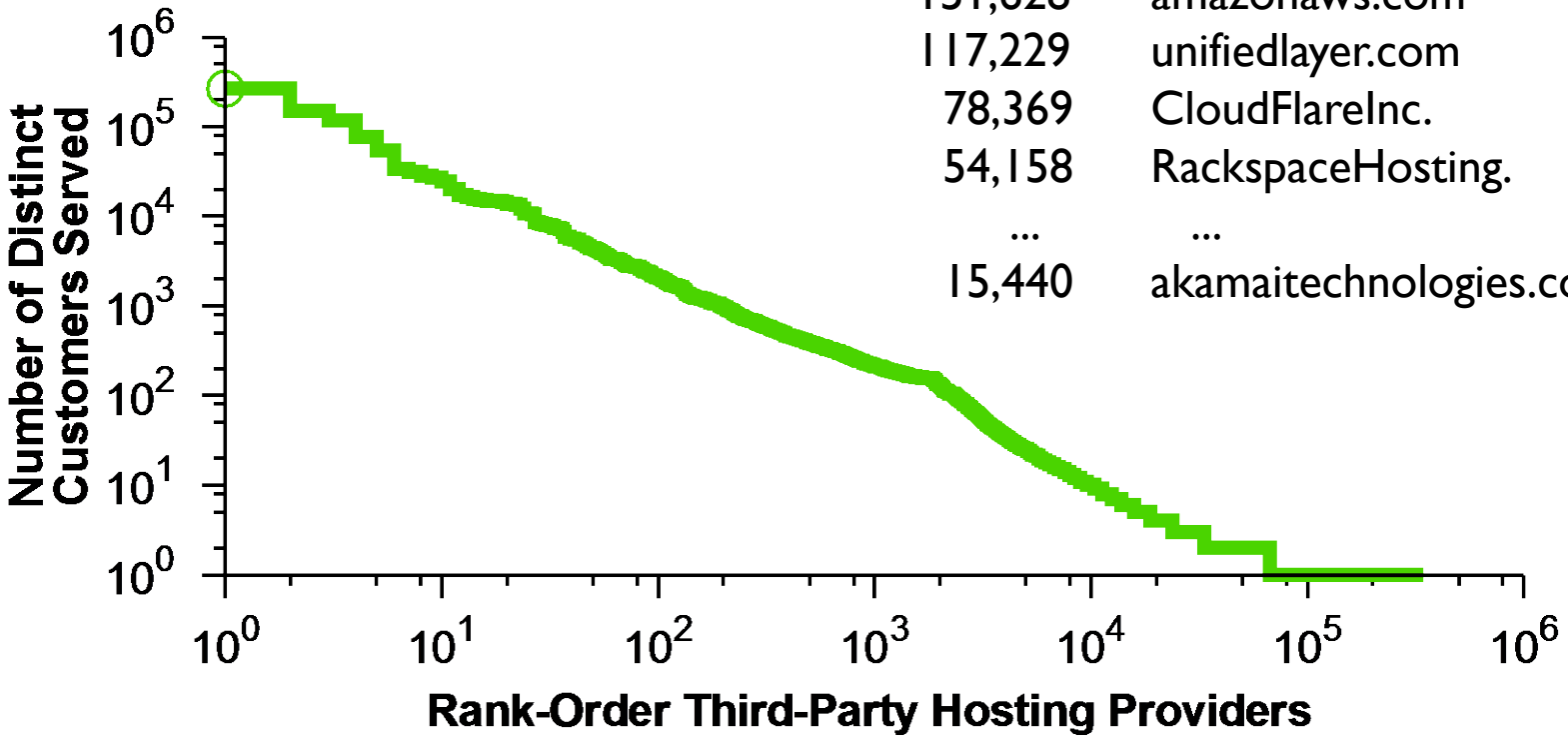
How does key sharing impact certificate management?

The mapping between certs and orgs is not one-to-one

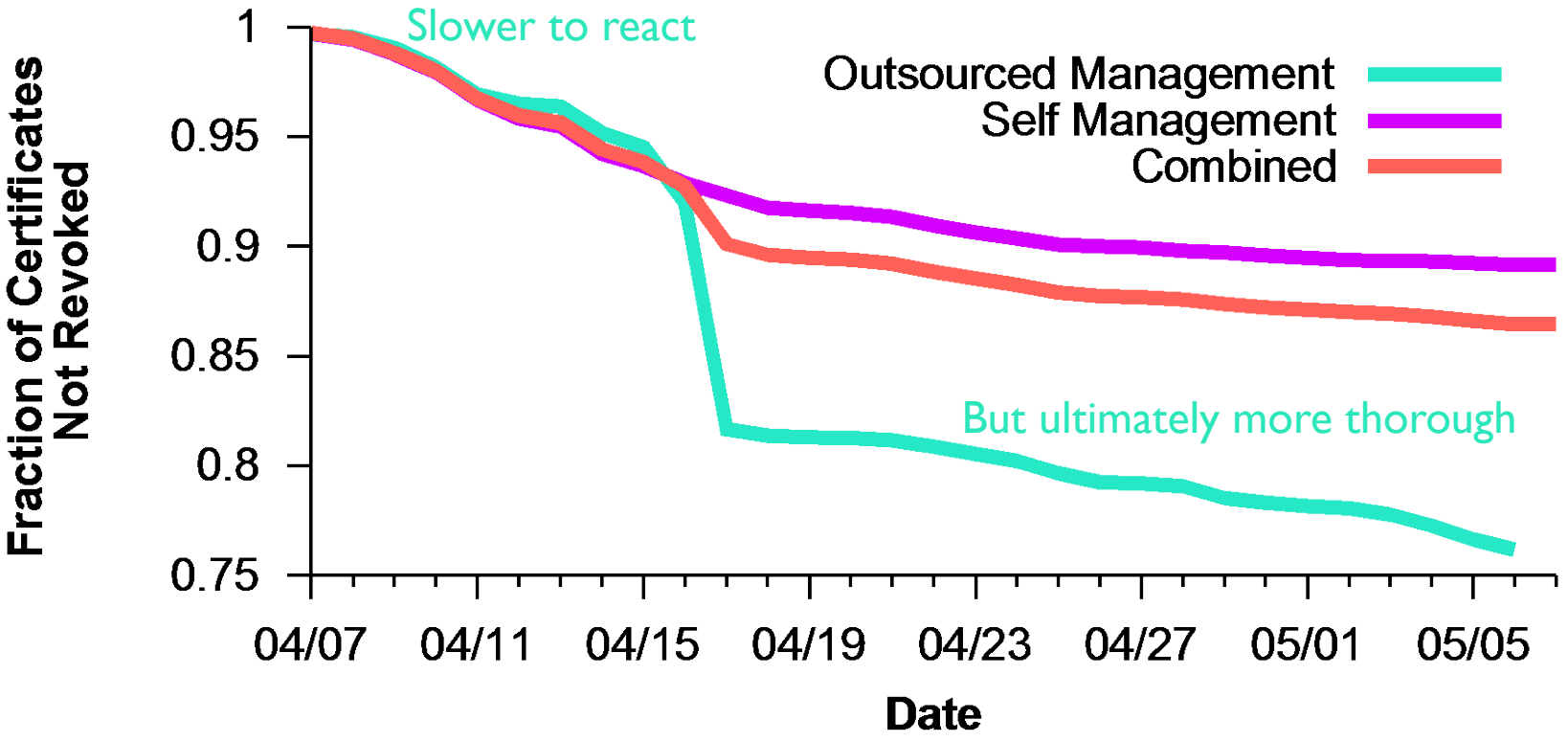
Who manages them?

Key sharing is rampant

# Orgs' keys	Hosting provider
266,110	secureserver.net
151,628	amazonaws.com
117,229	unifiedlayer.com
78,369	CloudFlareInc.
54,158	RackspaceHosting.
...	...
15,440	akamaitechnologies.com



Third-party management



Studying Key Sharing in the Web's PKI

How often do organizations share their private keys?

It's the norm for both popular & unpopular sites

How many keys have third party providers aggregated?

The majority of the Alexa top-1,000

How does key sharing impact certificate management?

May actually be an improvement

Future: New protocols to keep hosting providers from needing access to everything