Users Really Do Answer Telephone Scams

Huahong Tu (Raymond), *UMD*
Adam Doupé, *ASU*
Ziming Zhao, *RIT*
Gail-Joon Ahn, *ASU & Samsung*

What inspired our research?

CNN politics • LIVE TV

FCC: Nearly half the calls you receive this year will be spam

5, 2019

Users Really Do Plug in USB Drives They Find

Matthew Tischer† Zakir Durumeric‡† Sam Foster† Sunny Duan†
Alec Mori† Elie Bursztein◇ Michael Bailey†

Champaign ‡University of Michigan ◇Google, Inc.
, syduan2, ajmori2, mdbailey}@illinois.edu
@umich.edu elieb@google.com

t end users median time to connection of 6.9 hours and the first connection
completing occurring within six minutes from when the drive was dropped.
drives on Contrary to popular belief, the appearance of a drive does not
is effective increase the likelihood that someone will connect it to their
litious with computer. Instead, users connect all types of drives unless
We analyze there are other means of locating the owner—suggesting that
se users to

Research Question

What causes the users to **answer** and **fall victim** to telephone scams?

Collect and listen to scam samples

Collected over 150 telephone scam samples from the IRS, YouTube, Sound Cloud, News sites, etc.

Listened to each them identify different attributes.

What are the telephone scam attributes we've identified?

Area Code: e.g. Washington (202), Local (480), Toll Free (800)

Caller Name: a known name displayed with the caller ID

Voice Production: e.g. human or synthesized voice

Gender: e.g. male or female voice

Accent: e.g. American or Indian accent

Entity: who to impersonate, e.g. IRS or the university's HR dept

Scenario: provide motivation to divulge SSN, e.g. tax or payroll

How did we design our experiments?

Design a minimum set of experiments that allow **comparison** of **different properties** of **an attribute** with a set of **standard background conditions**.

List of all our experiments and their attribute properties

	Caller ID	Area Code Location	Caller Name	Voice Production	Gender	Accent	Entity	Scenario
E1	202-869-XXX5	Washington, DC	N/A	Synthesizer	Male	American	IRS	Tax Lawsuit
E2	800-614-XXX9	Toll-free	N/A	Synthesizer	Male	American	IRS	Tax Lawsuit
E3	480-939-XXX6	University Location	N/A	Synthesizer	Male	American	IRS	Tax Lawsuit
E4	202-869-XXX0	Washington, DC	N/A	Synthesizer	Female	American	IRS	Tax Lawsuit
E5	202-869-XXX2	Washington, DC	N/A	Synthesizer	Male	American	IRS	Unclaimed Tax Return
E6	202-849-XXX7	Washington, DC	N/A	Human	Male	American	IRS	Tax Lawsuit
E7	202-869-XXX4	Washington, DC	N/A	Human	Male	Indian	IRS	Tax Lawsuit
E8	480-462-XXX3	University Location	N/A	Synthesizer	Male	American	ASU	Payroll Withheld
E9	480-462-XXX5	University Location	W-2 Administration	Synthesizer	Male	American	ASU	Payroll Withheld
E10	480-462-XXX7	University Location	N/A	Synthesizer	Male	American	ASU	Bonus Issued

How we gathered our phone number recipients?

Downloaded our university's public phone directory associated with our staffs and faculties.

Removed telephone numbers of people already aware of the study.

Randomly selected 3,000 telephone numbers and assigned 300 to each experiment.

Steps we took to mitigate the risks to our recipients

Worked with IRB on our experimental process.

In all experiments, no SSN was actually collected.

Upon entering any SSN digit, the user was immediately informed that the call was just an experiment, and no SSN was actually collected, IRB contact was given at the end.

Each recipient only received one phone call.

Prior to dissemination, we communicated and coordinated with the HR dept and tech support office.

Dissemination

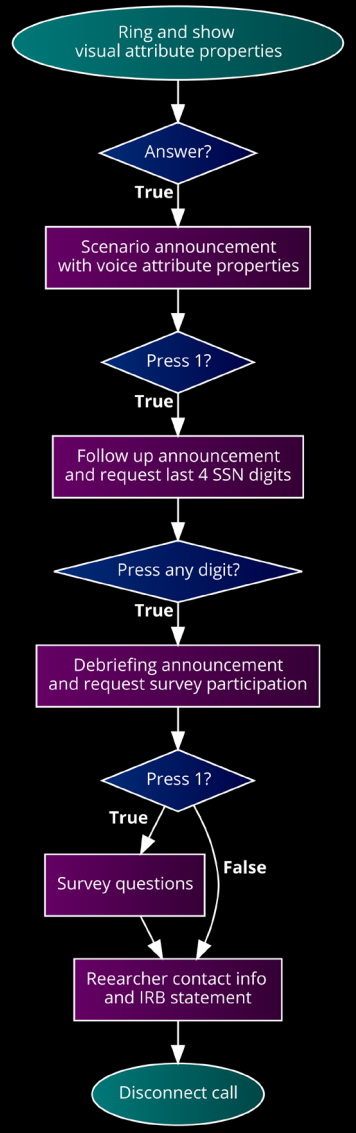
Set up our experiments using an online robocalling platform.

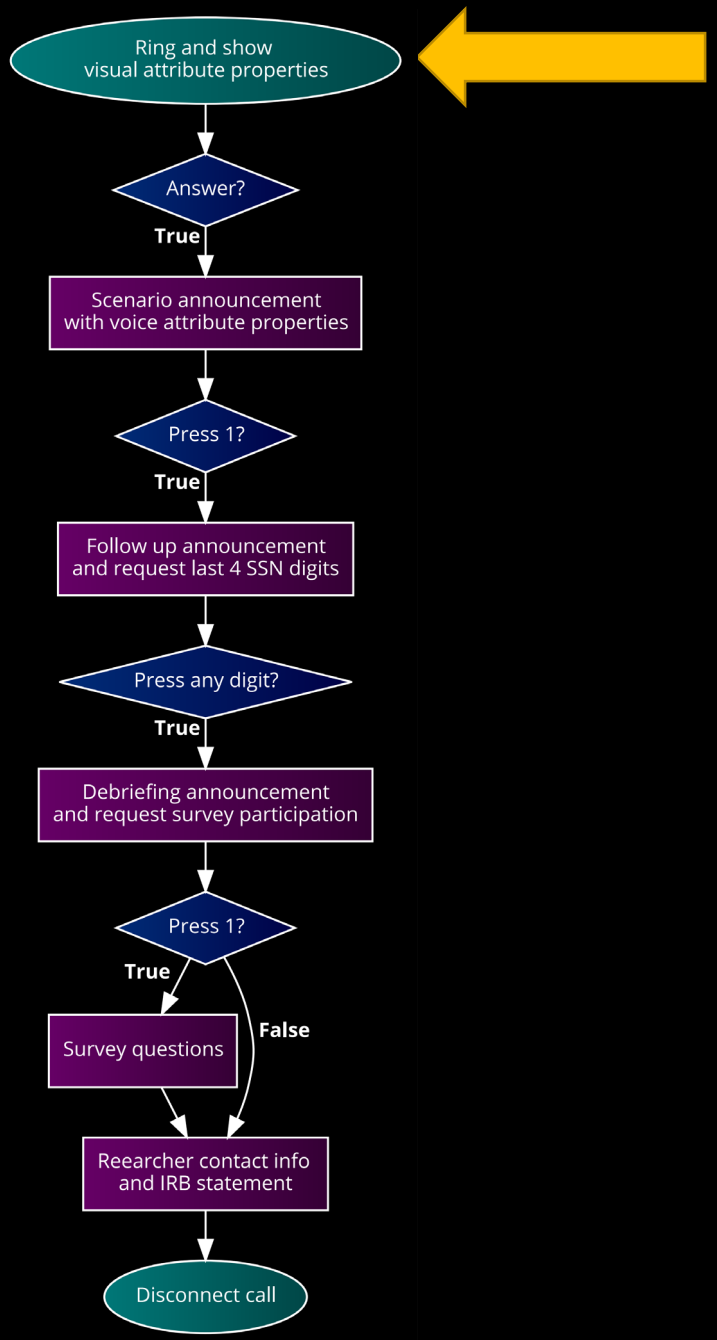
10 experiments can run simultaneously.

Limited all experiments to a single work week, duringthe work hours of 10am – 5pm.

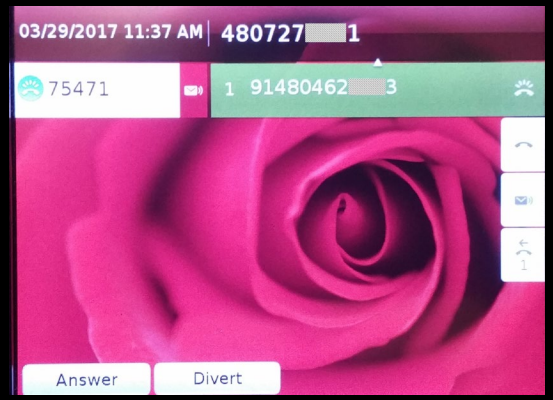
Outbound and return calls were directed to start of each experiment’s standard procedure.

The standard procedure of each experiment

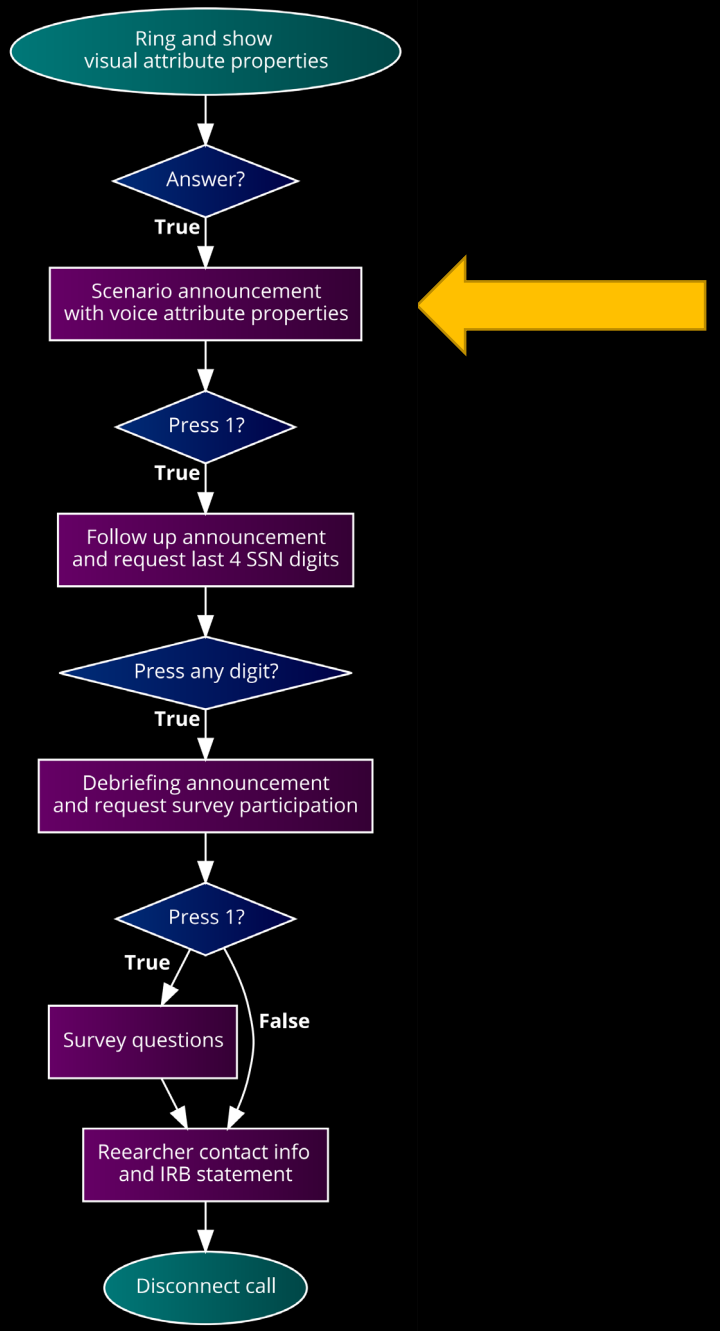




Ring and show visual attribute properties

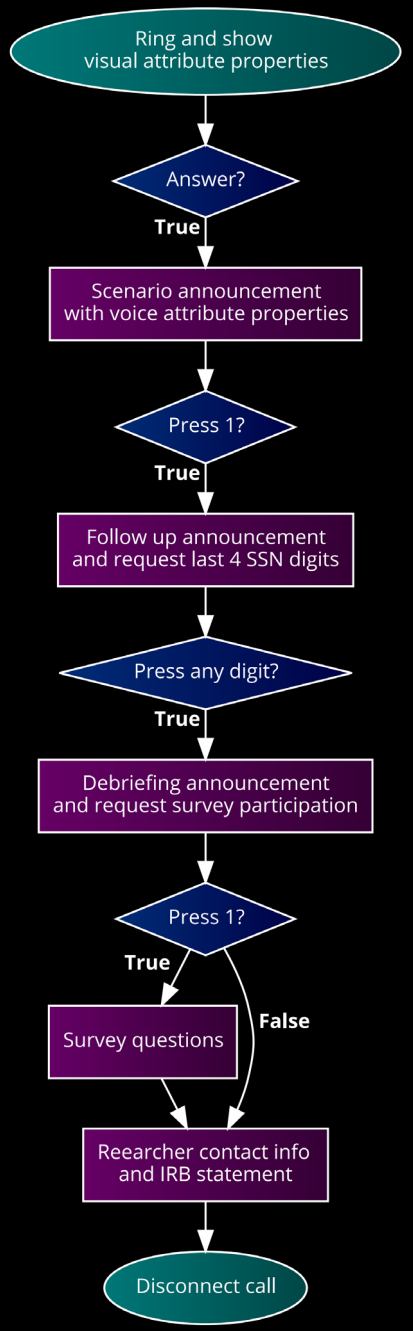


e.g.



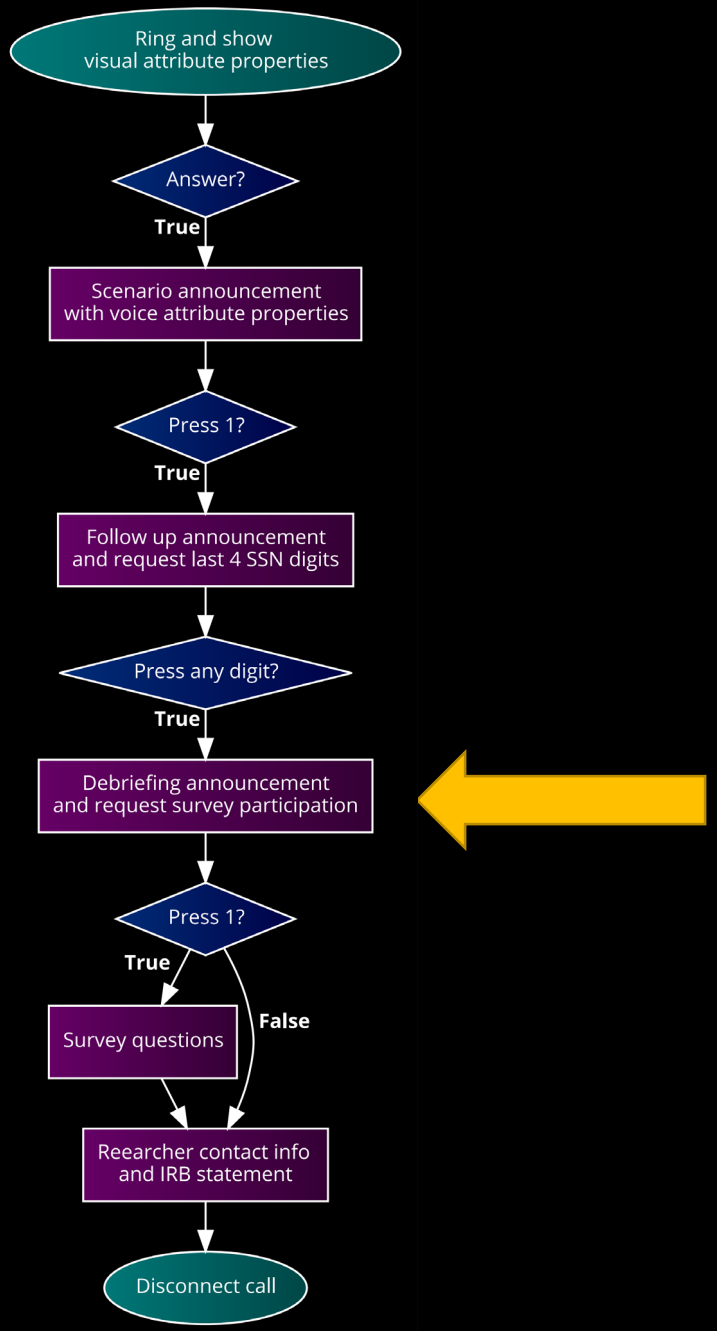
Scenario announcement
with voice attribute properties

e.g.



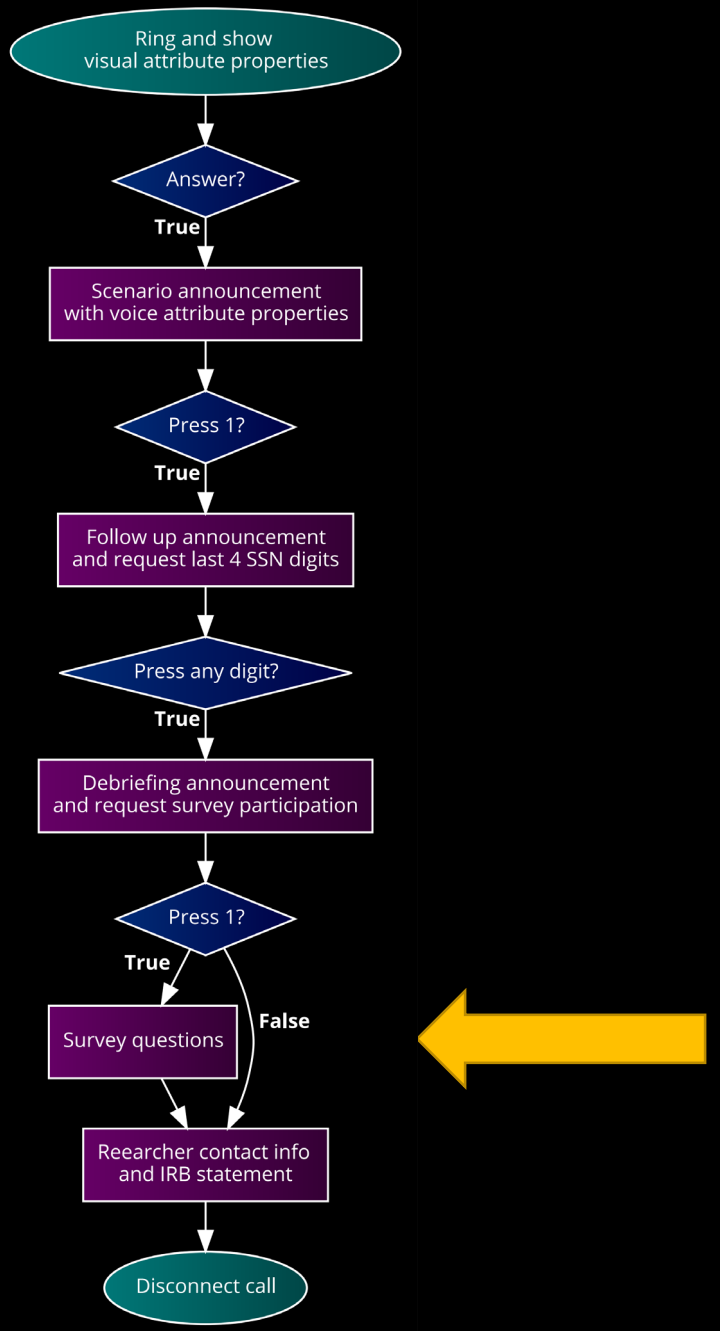
Follow up announcement and request last 4 SSN digits

e.g.



Debriefing announcement and request survey participation

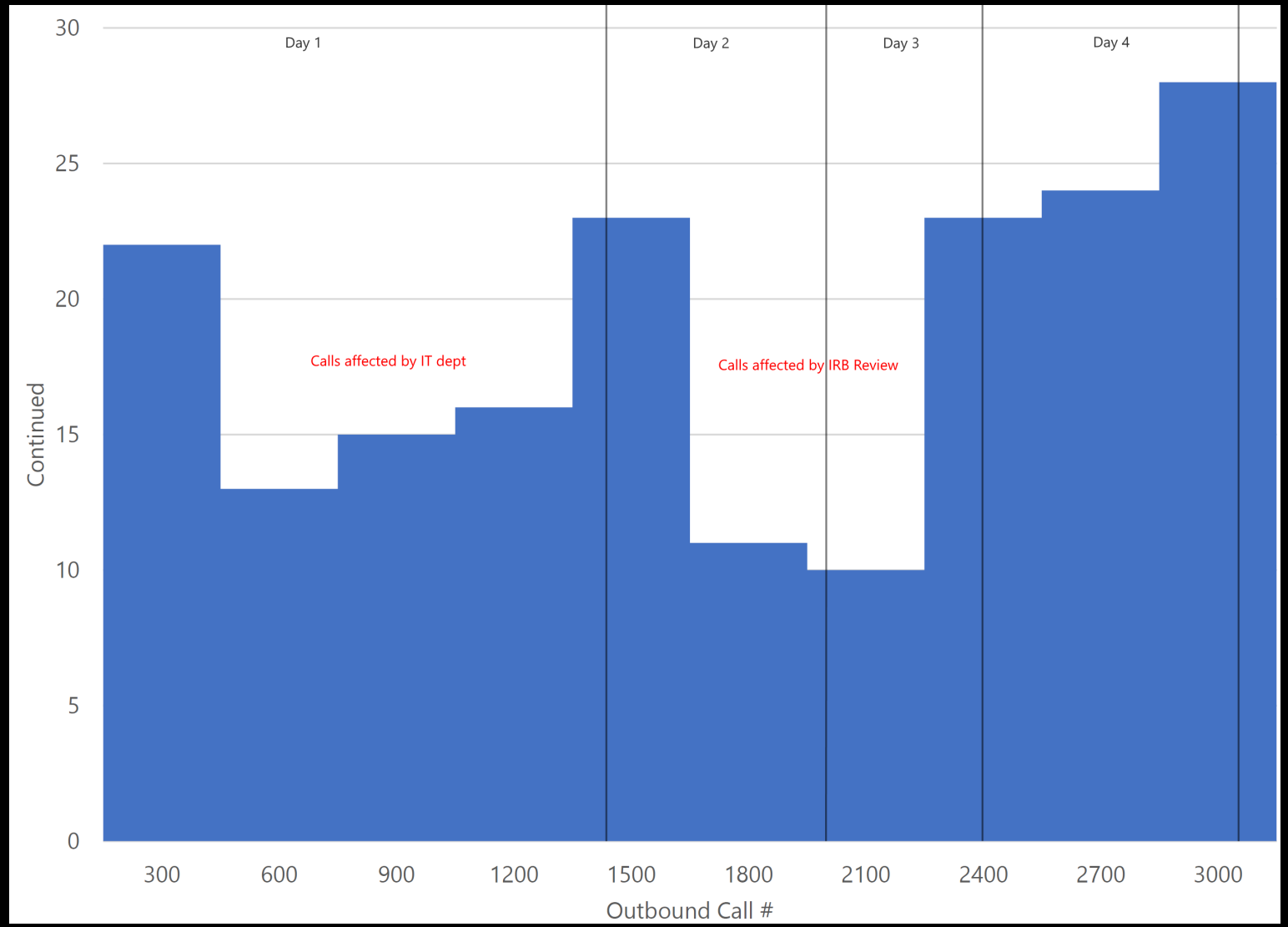
e.g.



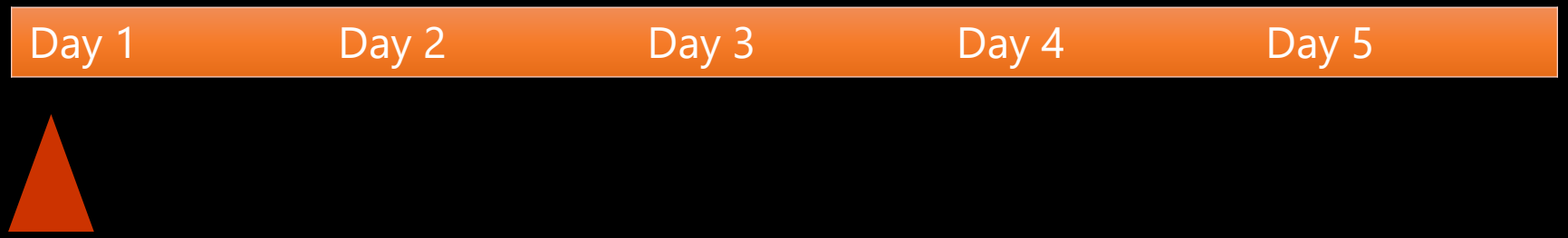
Survey questions

e.g.

Call log of recipients that pressed 1 to continue



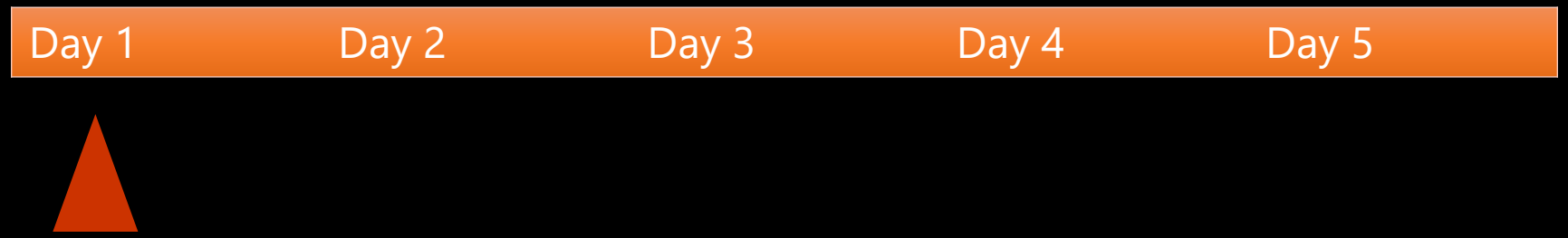
Incidents during call dissemination



2 hours and 45 minutes since launch:

The school of journalism and mass communication identified our scam calls…

They did not consult with the IT department and sent out mass emails in their dept to warn about the scam calls.

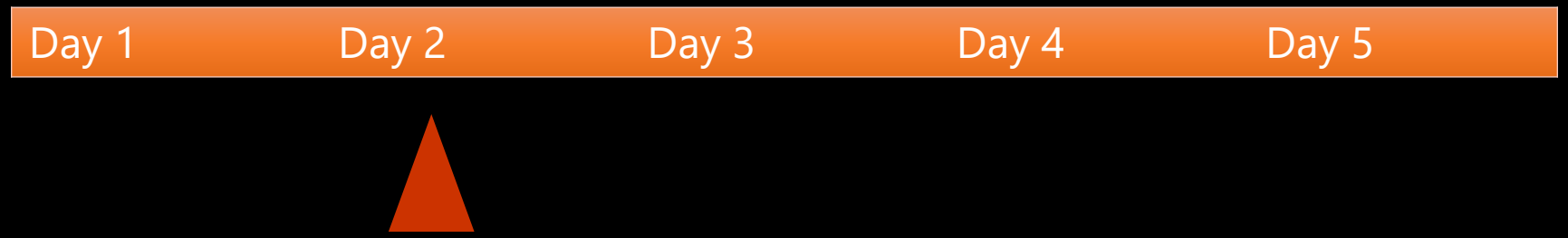


4 hours and 22 minutes since launch:

The university's telephone service office started blocking our phone calls…

Our calls were triggering IT system alerts as they were exhausting the university's telephone trunk routes.

So we had to reduce the rate of outgoing calls.

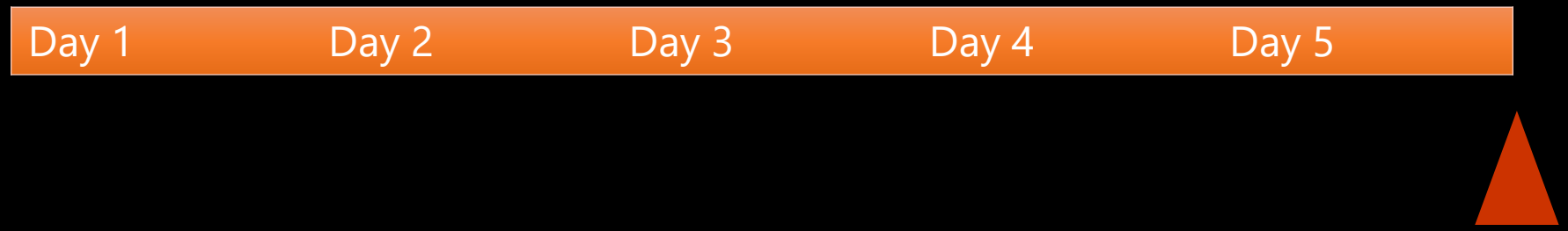


Day 2 since launch:

The IRB received many complaints…

So they asked us to pause our experiments so that they could review the study was proceeding as described.

12 hours later, after review, they found everything was in order, and suggested we proceed.


Day 1
Day 2
Day 3
Day 4
Day 5

Collected Results

	Continued		Entered SSN		Convinced		Recordings		Unconvinced		Recordings	
E1	12	4.00%	6	2.00%	0	0.00%	0	0.00%	4	1.33%	2	0.67%
E2	19	6.33%	15	5.00%	3	1.00%	0	0.00%	3	1.00%	3	1.00%
E3	13	4.33%	8	2.67%	1	0.33%	1	0.33%	2	0.67%	1	0.33%
E4	23	7.67%	13	4.33%	2	0.67%	0	0.00%	3	1.00%	2	0.67%
E5	9	3.00%	2	0.67%	1	0.33%	0	0.00%	1	0.33%	1	0.33%
E6	9	3.00%	8	2.67%	2	0.67%	2	0.67%	2	0.67%	1	0.33%
E7	13	4.33%	9	3.00%	3	1.00%	1	0.33%	5	1.67%	4	1.33%
E8	53	17.67%	30	10.00%	8	2.67%	3	1.00%	9	3.00%	8	2.67%
E9	60	20.00%	35	11.67%	7	2.33%	3	1.00%	4	1.33%	3	1.00%
E10	45	15.00%	22	7.33%	8	2.67%	7	2.33%	4	1.33%	2	0.67%
Total	256	8.53%	148	4.93%	35	1.17%	17	0.57%	37	1.23%	27	0.90%

Finding an Analysis Metric

Entered SSN: # of users entered a digit when asked for last 4 SSN digits

- Issue: **Too lax** as a measure since users could have enter fake SSNs

Convinced: # of users enter 1 indicating that they were convinced by the scam

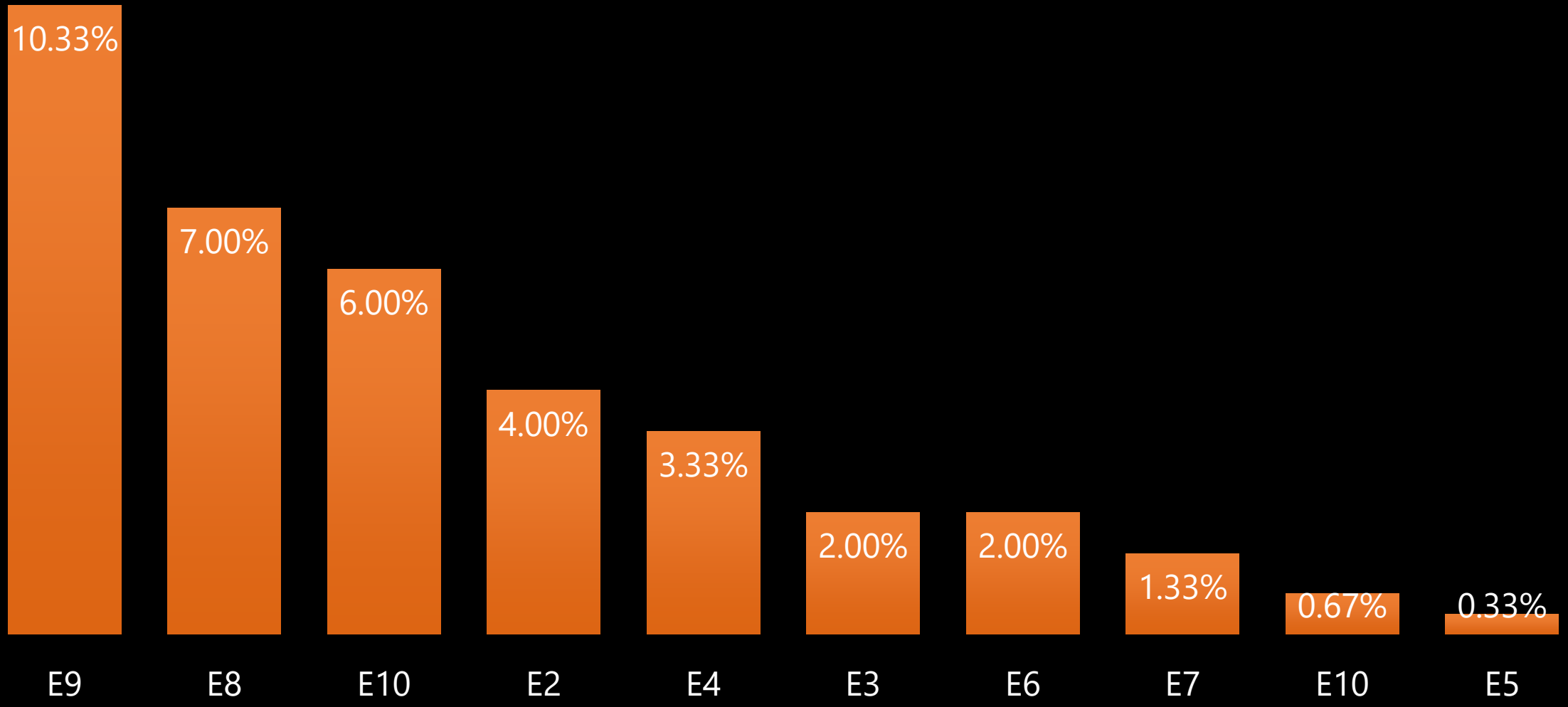
- Issue: **Too sparse** as users rarely indicated that they were convinced by the scam

Our Chosen Metric

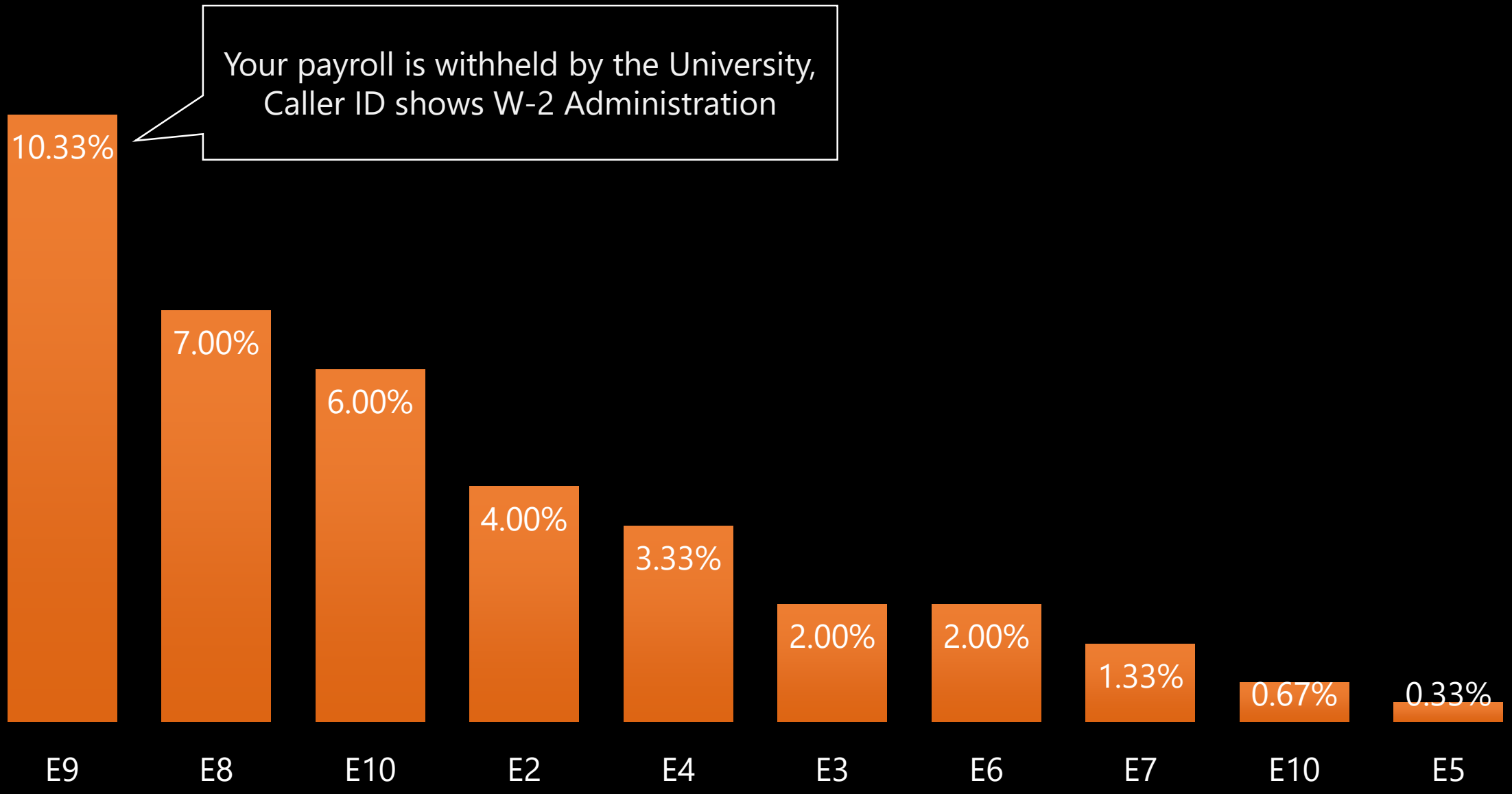
Possibly Tricked: # of users Entered SSN - Unconvinced

A more reasonable estimate of the actual number of recipients that fell for the scam that is not too lax and not too sparse.

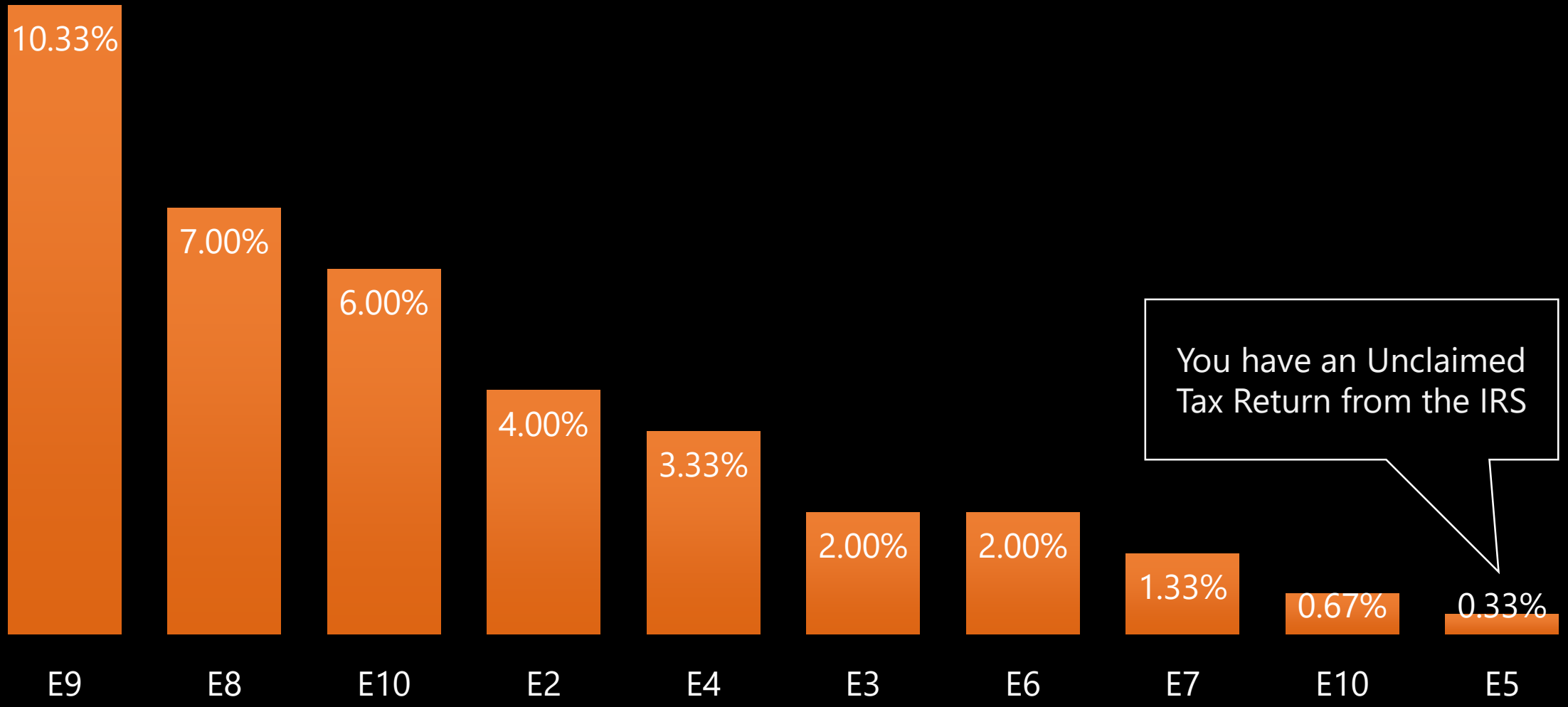
Results of Possibly Tricked



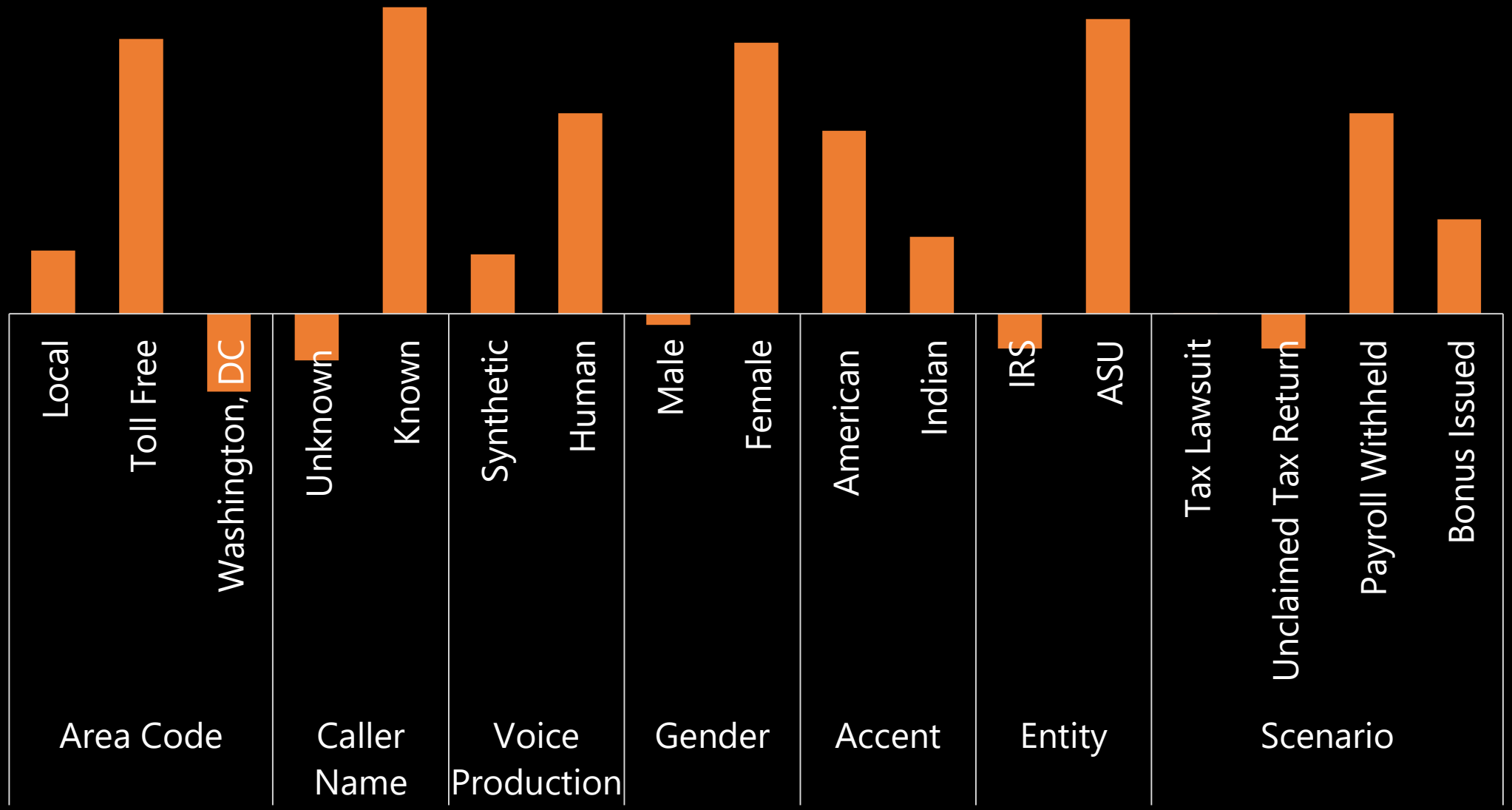
Results of Possibly Tricked



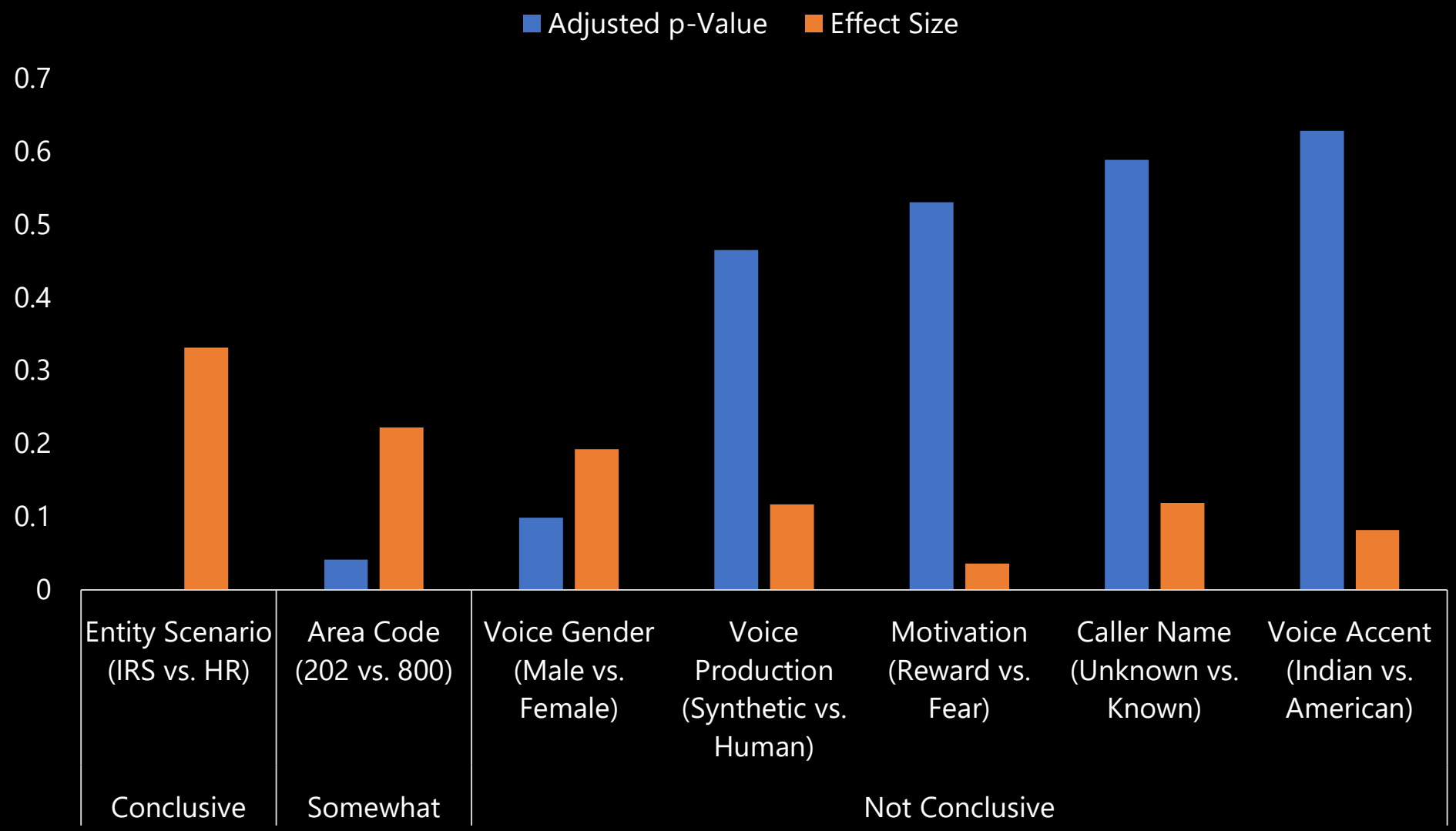
Results of Possibly Tricked



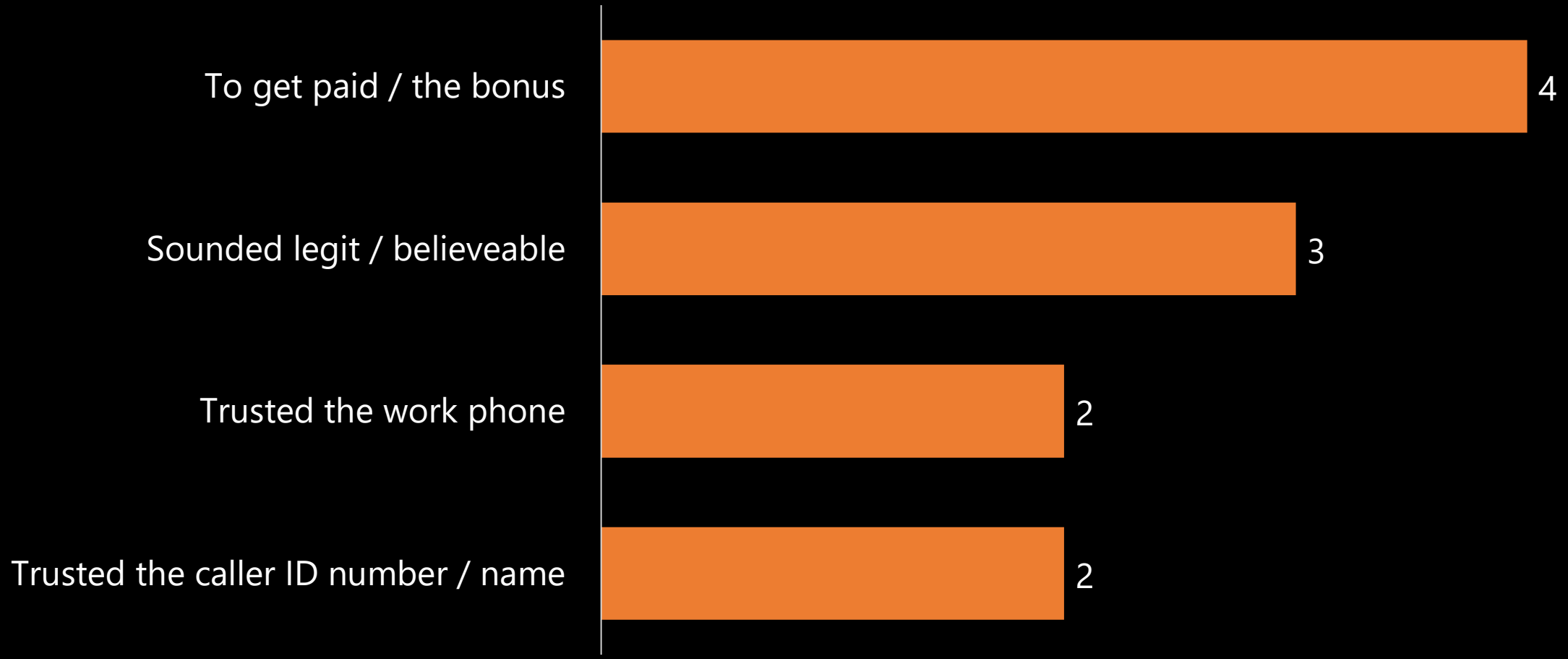
Linear regression coefficients of all attribute properties



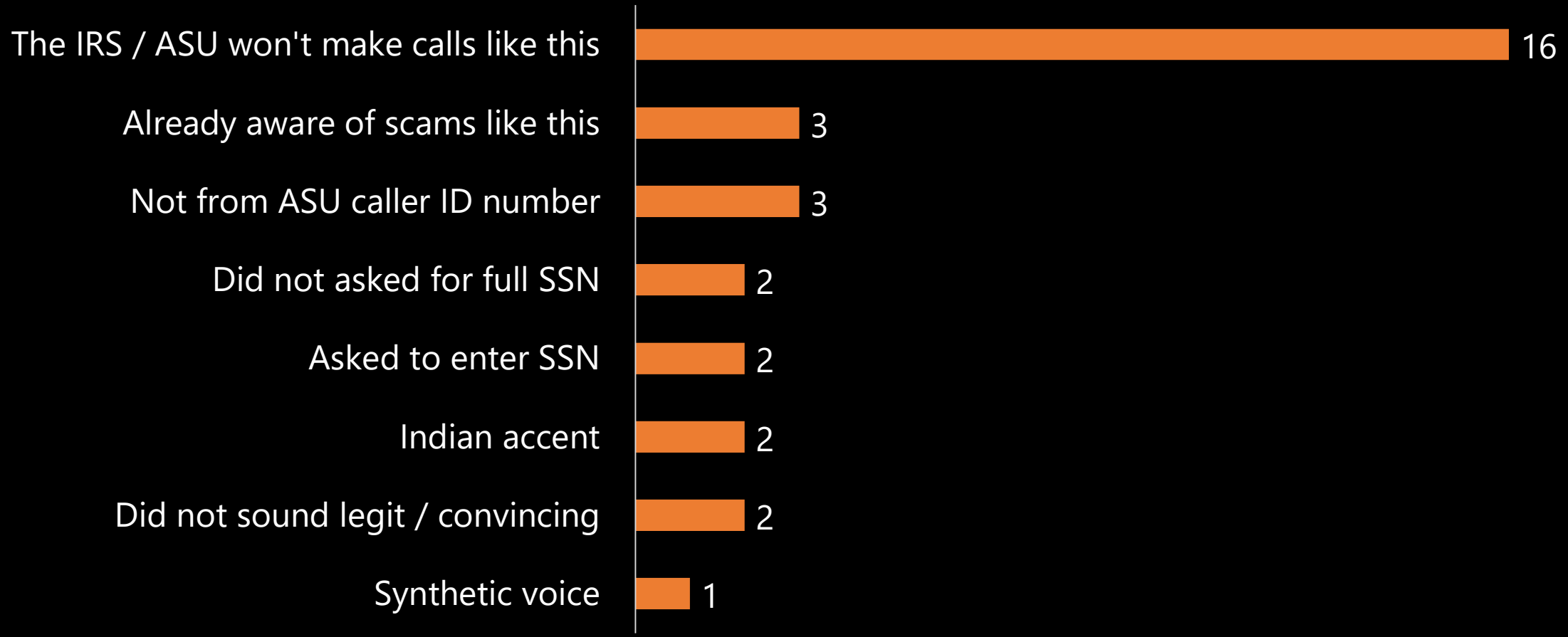
Statistical significance & effect size of comparable attribute properties



Reasons Convinced



Reasons Unconvinced



Spearphishing is effective

Telephone scammers may spoof a **known caller ID name** and **voice a plausible scenario** to make the scam exceptionally convincing.

Ways to protect the users

Make the users be aware of telephone scams.

- E.g. The HR won’t make calls like this

Adopt caller ID authentication technology.

- Provide safeguards against caller ID spoofing
- Fight malicious calls with a caller ID reputation system

More research into the understanding of scammers.

Thank you for your attention!

Post your questions to @h2raymond