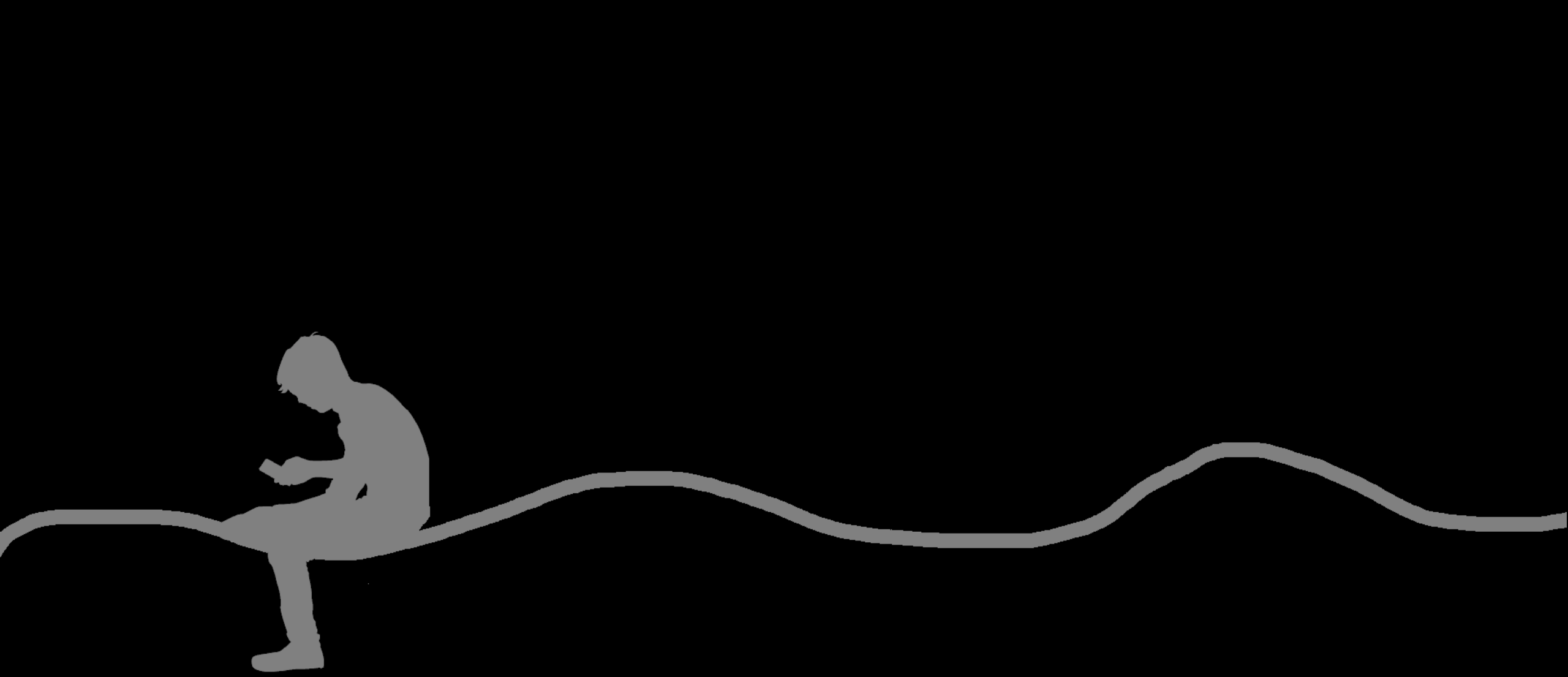
A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web

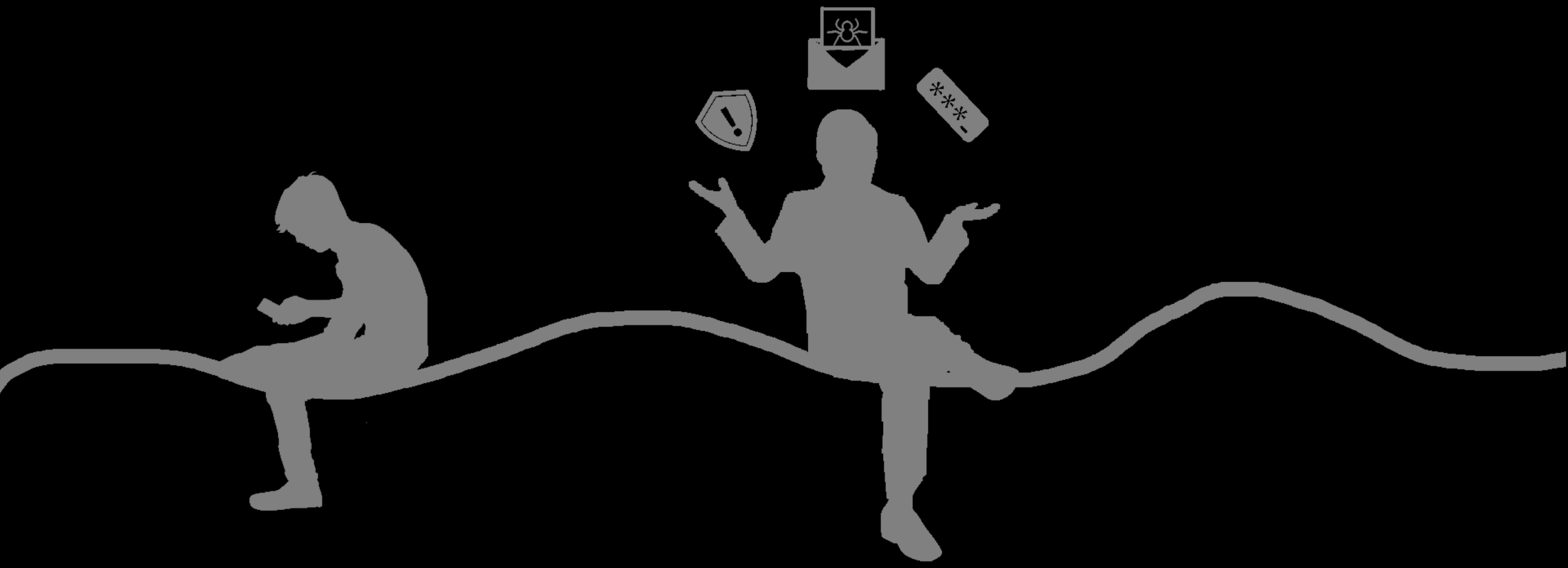
Elissa M. Redmiles, Noel Warford, Amritha Jayanti, and Aravind Koneru,
Sean Kross, Miraida Morales, Rock Stevens and Michelle L. Mazurek

@eredmil1

eredmiles@cs.umd.edu



People must learn a variety of security & privacy behaviors



Despite advances on core security problems, user decisions can still lead to significant security risks

Subscribe

SCIENTIFIC AMERICAN

Cart 0 Sign In | Stay Informed

All people had to do to stay safe from the global WannaCry ransomware attack was update their software. But people often don't, for a number of specific reasons

By Elissa Redmiles, May 16, 2017

COMMUNICATIONS OF THE ACM

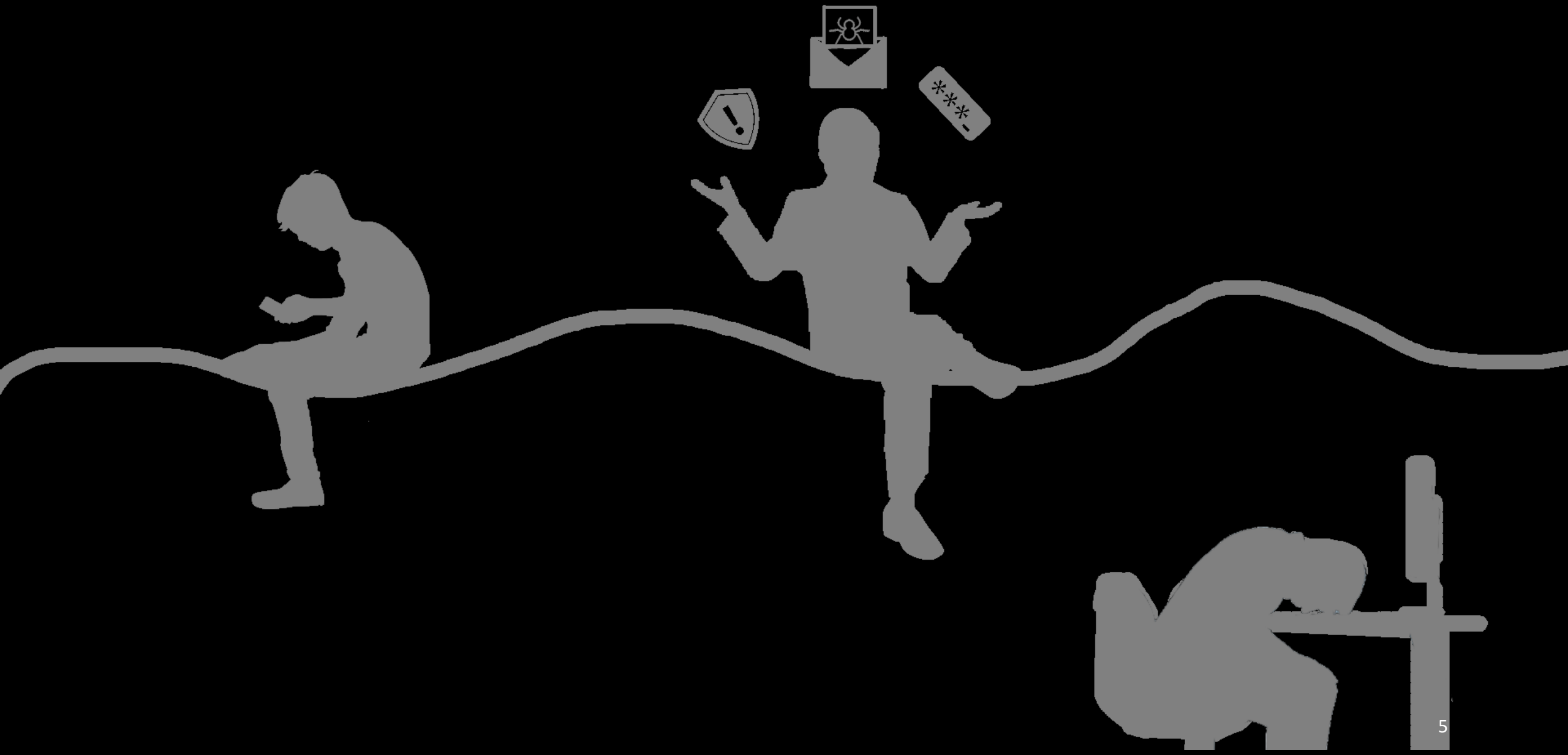
HOME | CURRENT ISSUE | NEWS | BLOGS | OPINION | RESEARCH | PRACTICE | CAREERS | ARCHIVE | VIDEOS

The State of Phishing Attacks

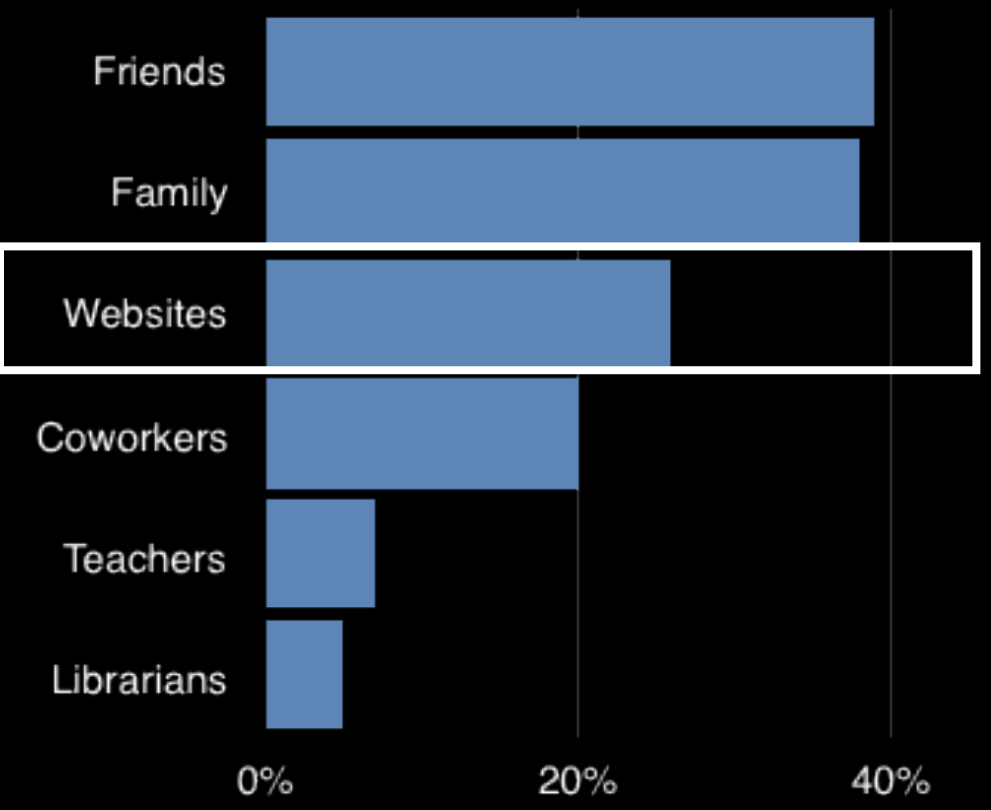
By Jason Hong

Estimates of damage caused by phishing vary widely, ranging from $61 million per year to $3 billion per year of direct losses to victims in the U.S.

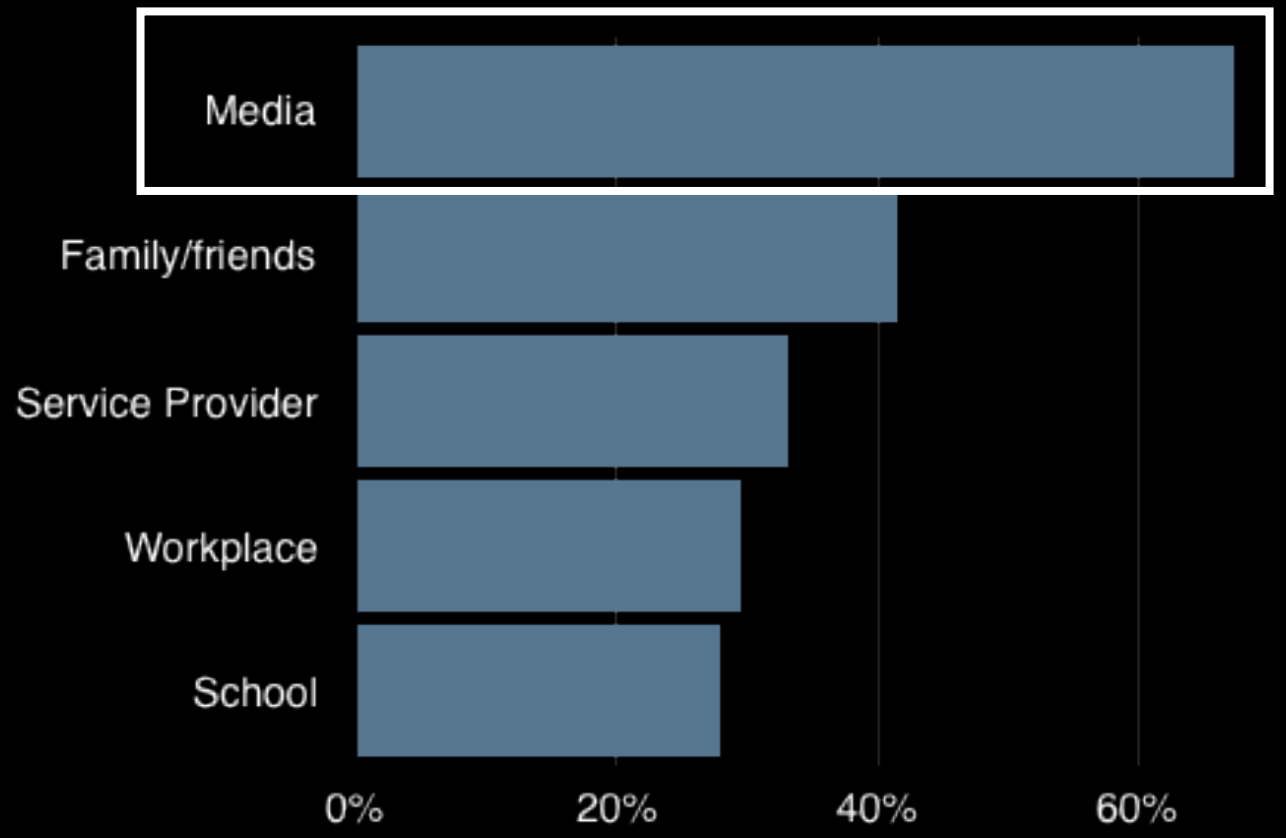
How do they learn security? Is security education working?



Ecosystem-wide quality measurement of one of the most prevalent security education sources: online articles



Where is the Digital Divide? A Survey of Security, Privacy, and Socioeconomics. CHI2017.



How I Learned to be Secure: a Census-Representative Survey of Security Advice Sources and Behavior. CCS2016.

Evaluate quality of corpus along three axes

Comprehensibility: can users understand the document?

Actionability: can users follow the advice?

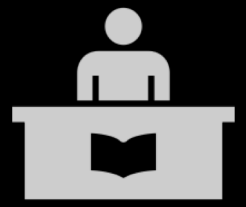
Accuracy: will following the advice make users more secure?

Collected representative corpus of online security advice

Step 1: Collect documents based on user-generated searches & expert recommendations

User Generated Search Queries (989 docs)

- List 5 search queries for each of 3 digital security topics you're interested in learning more about
- Show up to 6 security & privacy news articles
  - First one they indicate interest in: ask for 3 search queries



Expert Recommended Advice (889 docs)

10 security experts & librarians

Step 2: Crowd workers clean corpus "Is this document about online privacy/security?"

1,264 documents left after cleaning

Evaluate quality of corpus along three axes

Comprehensibility: can users understand the document?

Actionability: can users follow the advice?

Accuracy: will following the advice make users more secure?

Evaluate quality of corpus along three axes

Comprehensibility: can users understand the document?

Actionability: can users follow the advice?

Accuracy: will following the advice make users more secure?

What to use when evaluating security documents?

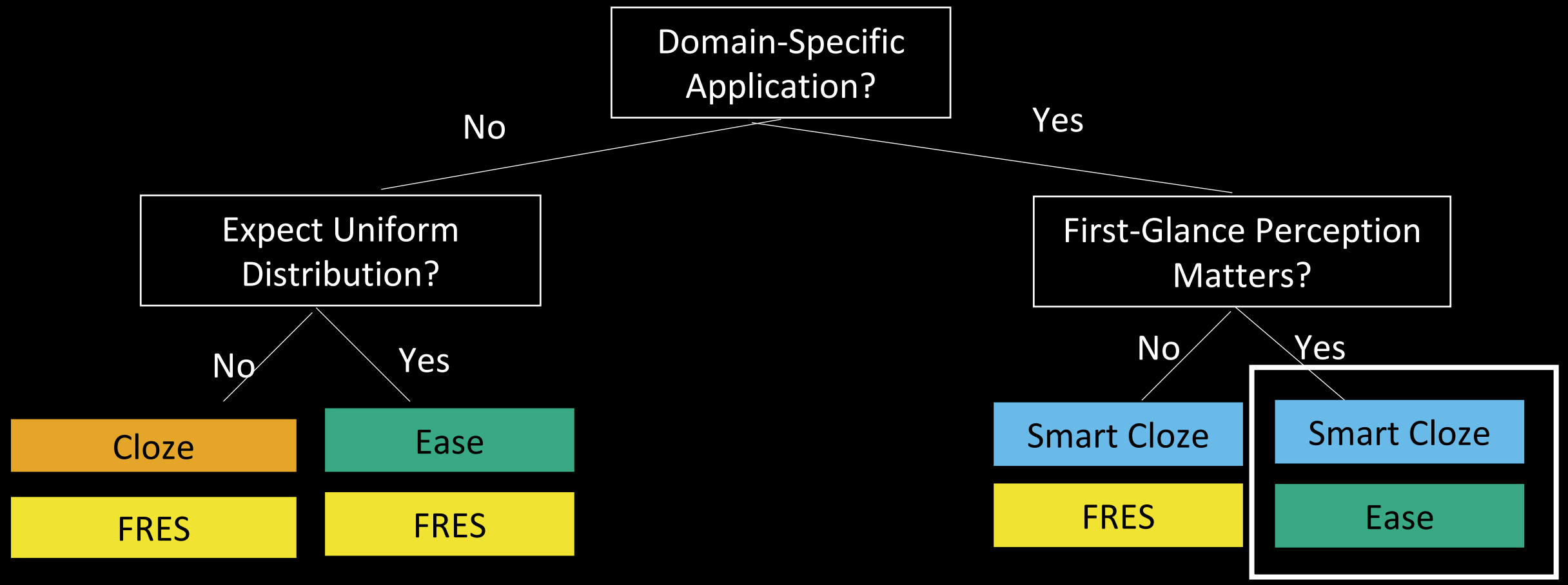


Figure Credit: Comparing and Developing Tools to Measure the Readability of Domain-Specific Texts. EMNLP 2019.

Smart Cloze tool creates domain-relevant distractors

Use NLP techniques to generate four grammatically-probable distractors:

two distractors drawn from a domain-specific dictionary we generate

two from a general dictionary

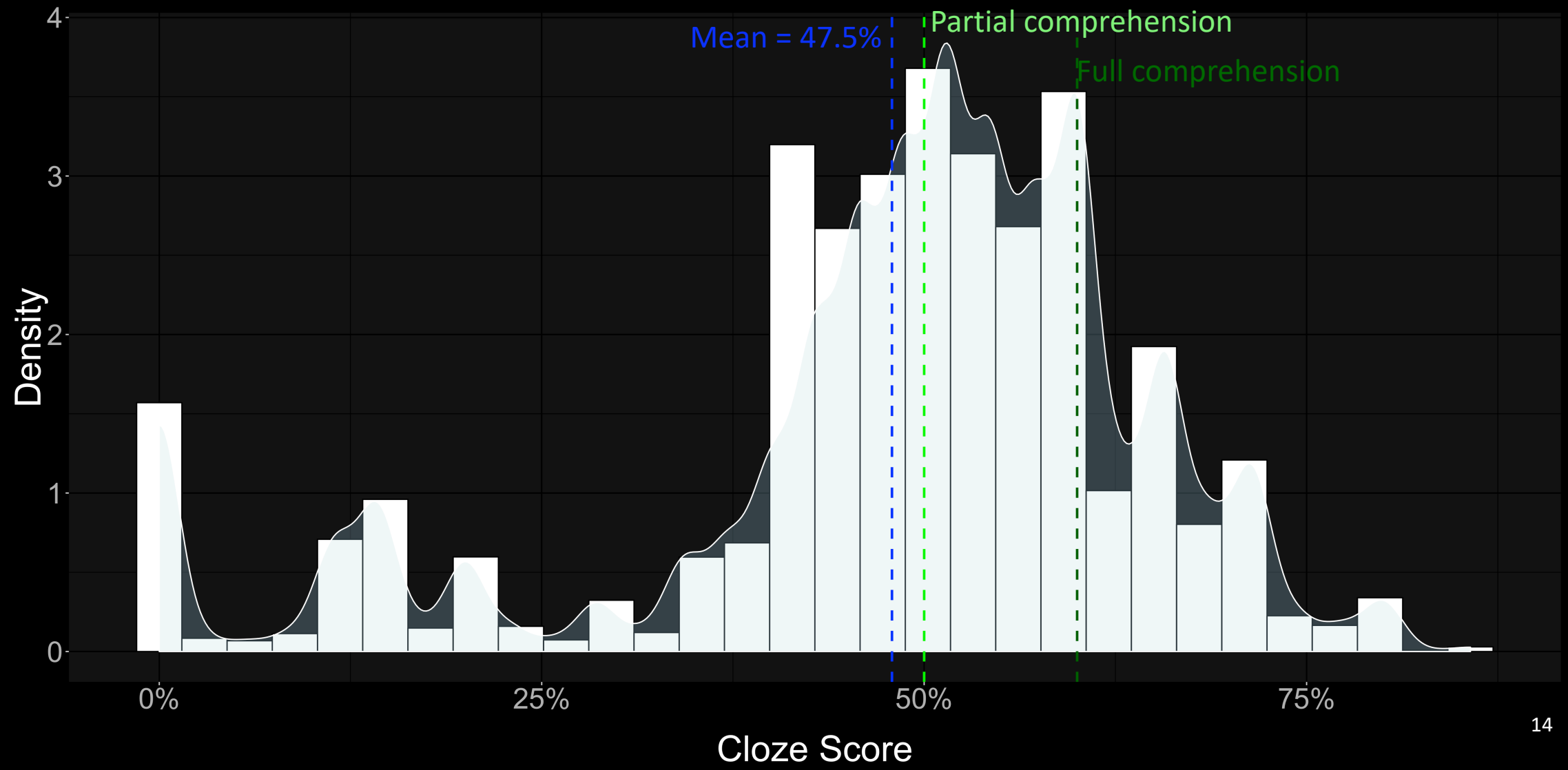
Q.3 Whats a VPN? VPN [ ] for Virtual Private Network. [ ] enables a computer t[✓] and receive data across [ ] or public networks as [ ] it is directly connected [ ] the private networkbenefiting from [ ] , security, and management [ ] of the private network. [ ] can use a VPN [ ] connect to the corporate [ ] ffice while [ ] traveling abroad, while you [ ] at home, or any [ ] time you are out [ ] the office. You can [ ] use a commercial VPN [ ] encrypt your data as [ ] travels over a public [ ] , such as the Wi-Fi [ ] an Internet caf or [ ] hotel. You can use [ ] commercial VPN to circumvent [ ] censorship on a network [ ] blocks certain sites or [ ] . For example, some Chinese [ ] use commercial VPNs to [ ] websites blocked by the [ ] Firewall. You can also [ ] to your home network [ ] running your own VPN [ ] , using open-source software such [ ] OpenVPN. A VPN protects [ ] Internet traffic from surveillance [ ] the public network, but [ ] does not protect your [ ] from people on the [ ] network youre using.

check
trust
webmail
send
see

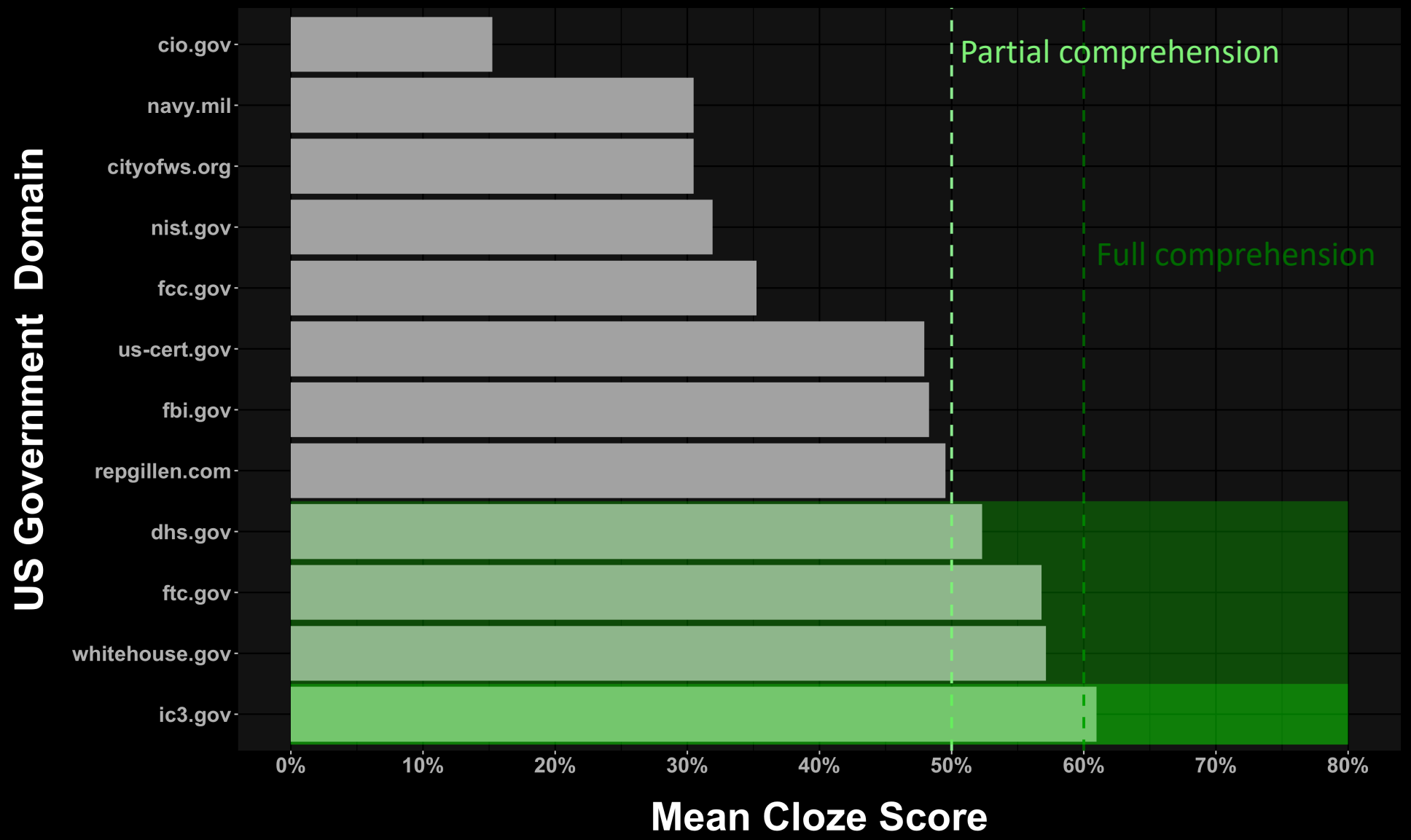
Each document evaluated by three test-takers, who had excellent reliability (ICC>0.90)

Census-representative sample of test takers

55% of documents at least partially comprehensible
Average doc perceived as “somewhat” easy to read



Variance within domain groupings: some government providers far more comprehensible than others



Evaluate quality of corpus along three axes

Comprehensibility: measure with *Smart Cloze* & perceived ease

55% of documents at least partially comprehensible

Actionability: can users follow the advice?

Accuracy: will following the advice make users more secure?

Evaluate quality of corpus along three axes

Comprehensibility: measure with *Smart Cloze* & perceived ease

55% of documents at least partially comprehensible

Actionability: can users follow the advice?

Accuracy: will following the advice make users more secure?

To measure actionability (and accuracy) need to extract advice imperatives from documents

Two research assistants manually annotated 1,264 documents to extract imperatives

..Base passwords on

308 as substitutions for your passwords from now on.

309 Choose events or people that are on your mind

To remember a strong password that will have to change in several months, try selecting an upcoming personal or public event. Use this as an opportunity to remind yourself about something pleasant that is going on in your life, or a person whom you admire or love. You won't be likely to forget the password if it is funny or endearing. Make it unique to you. Be sure to make it a phrase of two or more words, and continue to slip in your symbols. For example: "J0hn$Gr@du@tion".

Started with literature-grounded taxonomy of 194 codes, 206 new codes discovered through annotation

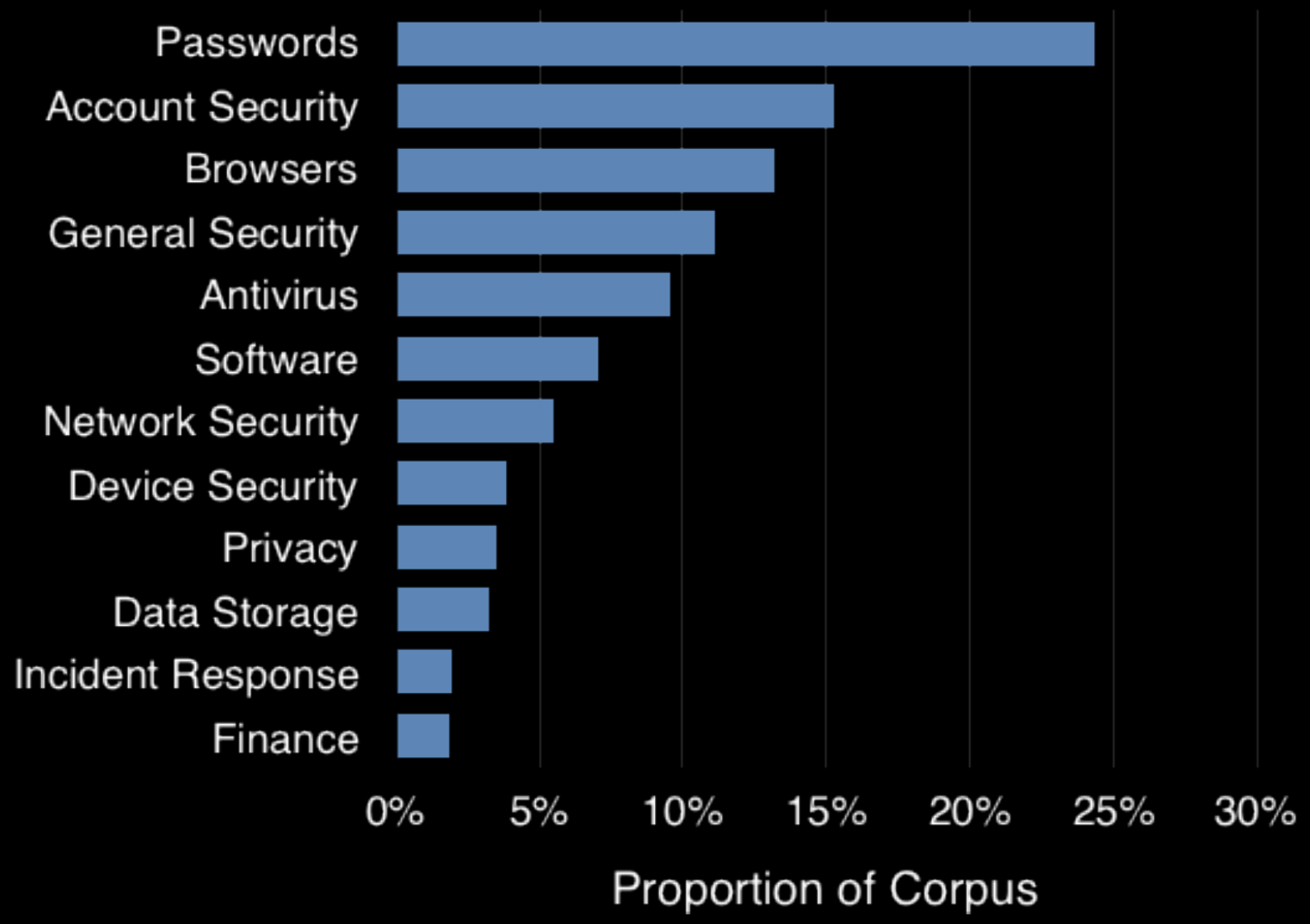
374 unique advice imperatives

2,780 pieces of advice

securityadvice.cs.umd.edu

- Advice Imperative Taxonomy:
  - Account Security
  - Antivirus
  - Browsers
  - Data Storage
  - Device Security
  - Finance
  - General Security
  - Incident Response
  - Network Security
  - Passwords
  - Privacy
  - Software
    - be careful with permissions
    - disable autorun to prevent malicious code from running
    - disable extension-hiding for known file types
    - disable macros
    - install latest os updates
      - Accuracy
      - Actionability
      - Examples
        - First, always make sure you install the latest software updates from your operating system
        - Always make sure your operating system, browsers with plug-ins and e-mail program are up to da safety updates on a regular basis.
        - Maintain current versions of your computer's operating system and Internet browsers.
        - To increase security, make sure youre using up-to-date anti-malware software and that your opera
        - Also, keeping all computer software up to date, especially the operating system software, will hel threats
        - While it is easy to enable automatic updates for your computer, it is also important that you occas make sure your system is staying up-to-date.
      - Literature Source
        - "...no one can hack my mind": Comparing Expert and Non-Expert Security Practices, Ion et al., S
      - Source Documents
        - httpsmyshadow.orgprivacy-and-security-basics.txt
        - httpssecuringtomorrow.mcafee.comconsumerfamily-safetymalware.txt

12 high level topics of security advice



Evaluate quality of corpus along three axes

Comprehensibility: measure with *Smart Cloze* & perceived ease

55% of documents at least partially comprehensible

Actionability: can users follow the advice?

Accuracy: will following the advice make users more secure?

Four theoretically-grounded actionability sub-metrics

Confidence: how confident is the user that they can follow the advice?

PMT (perceived ability) & HiTL (knowledge acquisition)

Time Consumption: how time consuming would it be to follow this advice?

economic frameworks (cost)

Disruption: how disruptive would it be to follow this advice?

economic frameworks (cost)

Difficulty: how difficult would it be to follow this advice?

HiTL (capabilities)

Answered on a Likert Scale: Very to Not at All

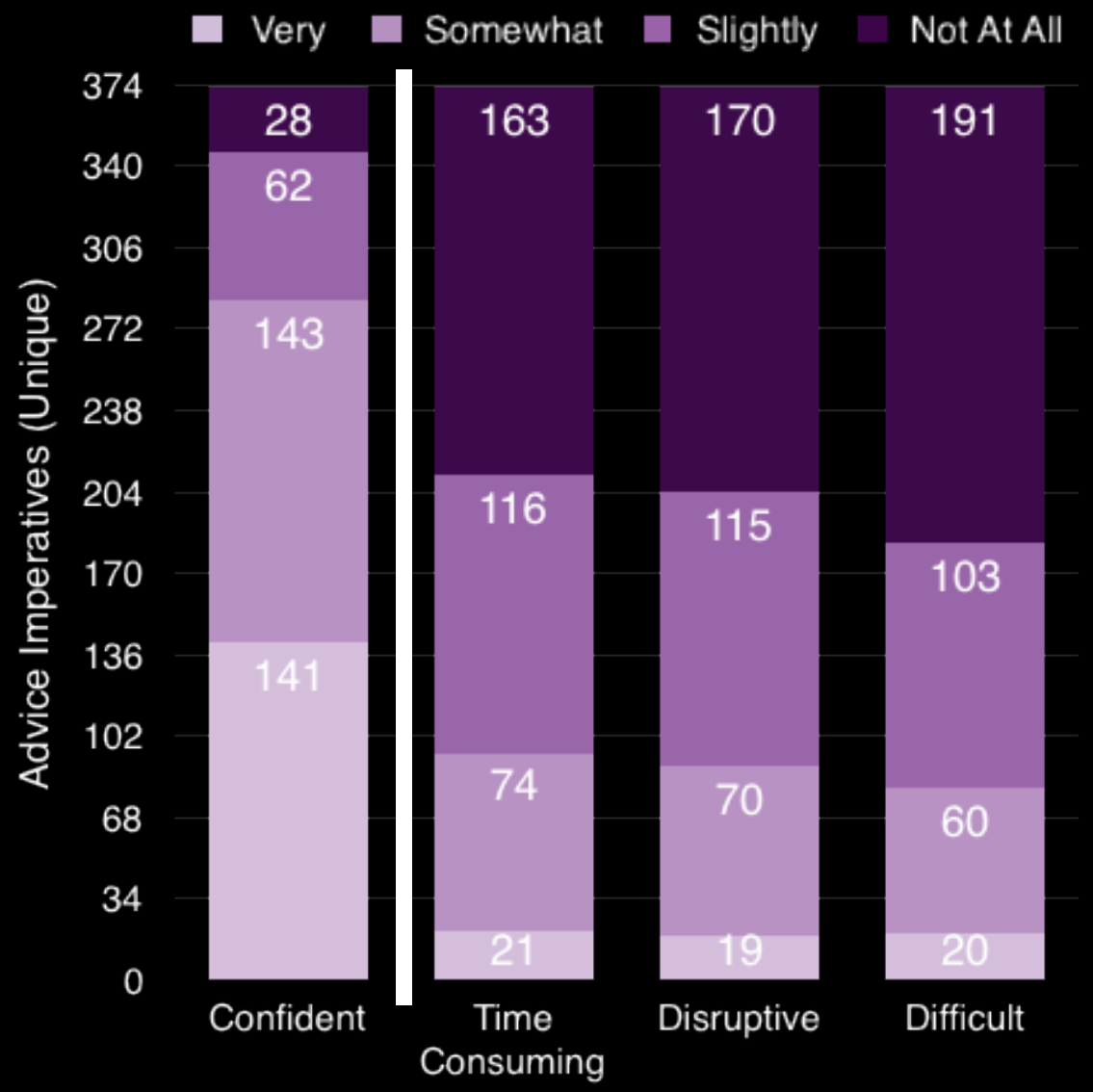
Each piece of advice evaluated by three evaluators, who had good reliability (ICC>0.85)

Census-representative sample of evaluators

Majority of advice rated as actionable

$^{3}/_{4}$ **of advice** "somewhat"+ confident
$^{2}/_{3}$ **of advice at most** "slightly"
time consuming, disruptive, and difficult

20% of documents contain at least one unactionable piece of advice



Evaluate quality of corpus along three axes

Comprehensibility: measure with *Smart Cloze* & perceived ease

55% of documents at least partially comprehensible

Actionability: can users follow the advice?

People are somewhat or very confident about implementing $^{3}/_{4}$ *of advice*
$^{2}/_{3}$ *considered at most slightly time consuming, disruptive, or difficult to implement*

Accuracy: will following the advice make users more secure?

Evaluate quality of corpus along three axes

Comprehensibility: measure with *Smart Cloze* & perceived ease

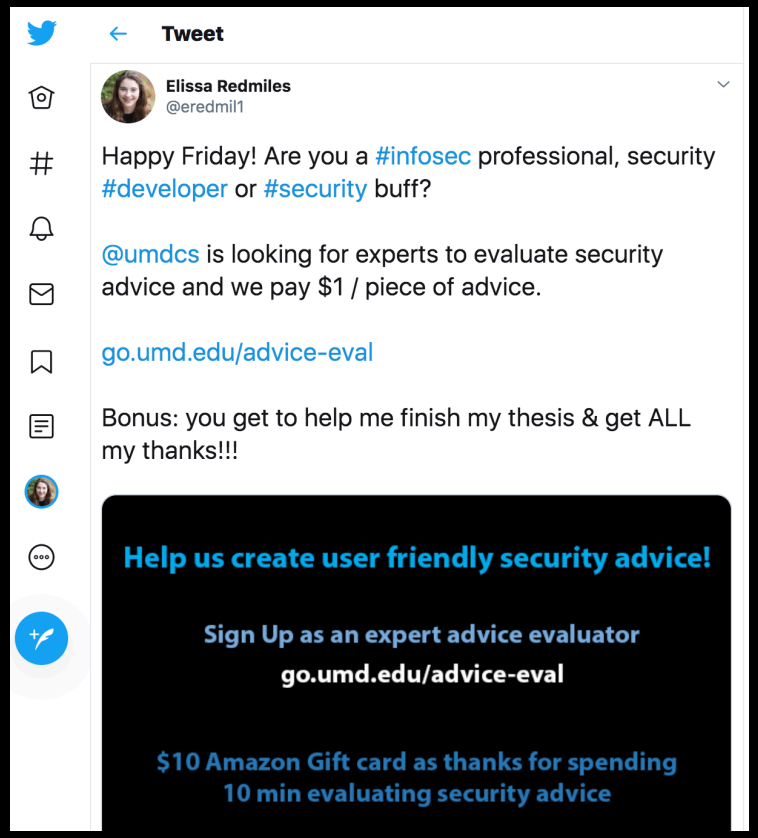
55% of documents at least partially comprehensible

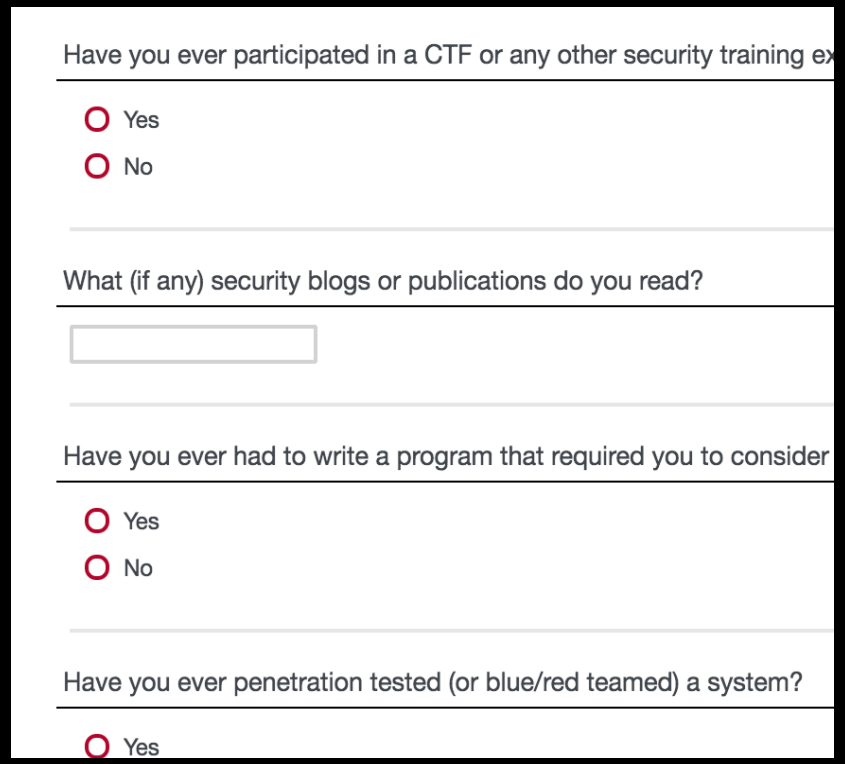
Actionability: can users follow the advice?

People are somewhat or very confident about implementing $^{3}/_{4}$ *of advice*
$^{2}/_{3}$ *considered at most slightly time consuming, disruptive, or difficult to implement*

Accuracy: will following the advice make users more secure?

Recruit security experts to evaluate advice accuracy





41 Experts

Recruitment

Qualification

CTF, pen testing, secure development } 2+

OR those who are certified

Ask experts to evaluate impact on risk & to prioritize

Perceived accuracy: accurate, useless, harmful

Please select the option that best matches your opinion.

- ○ Following this advice would IMPROVE someone's digital security or privacy at least a little bit (e.g., this advice is beneficial)
- ○ Following this advice would HARM someone's digital security or privacy at least a little bit (e.g., this advice is harmful)
- ○ Following this advice would have ABSOLUTELY NO EFFECT on someone's digital security or privacy (e.g., this advice is useless)

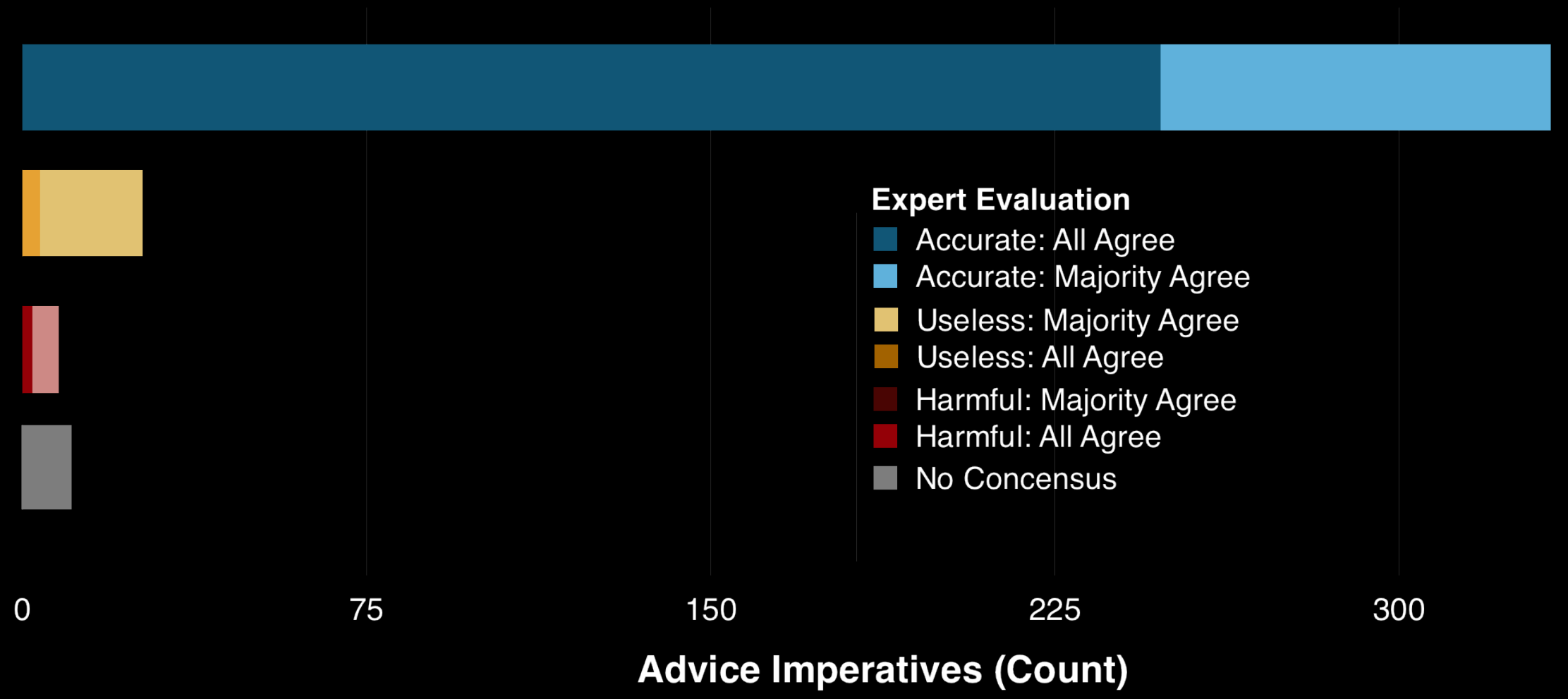
Risk reduction (or increase): 0-50+%

Priority: number 1, top 3, top 5, top 10

Each piece of advice evaluated by three experts, who had good reliability (ICC>0.85)

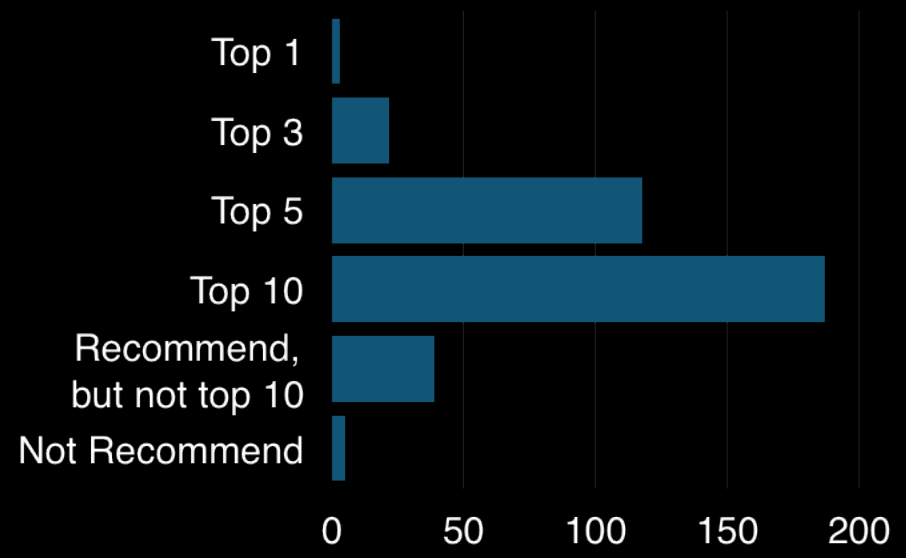
Average of 38 pieces of advice evaluated by each expert

Experts perceive 333 pieces of advice (89%) as accurate



All documents contain at least one piece of accurate advice

Experts are a bit more discerning when prioritizing advice but 118 pieces of advice are rated in the ”top 5”

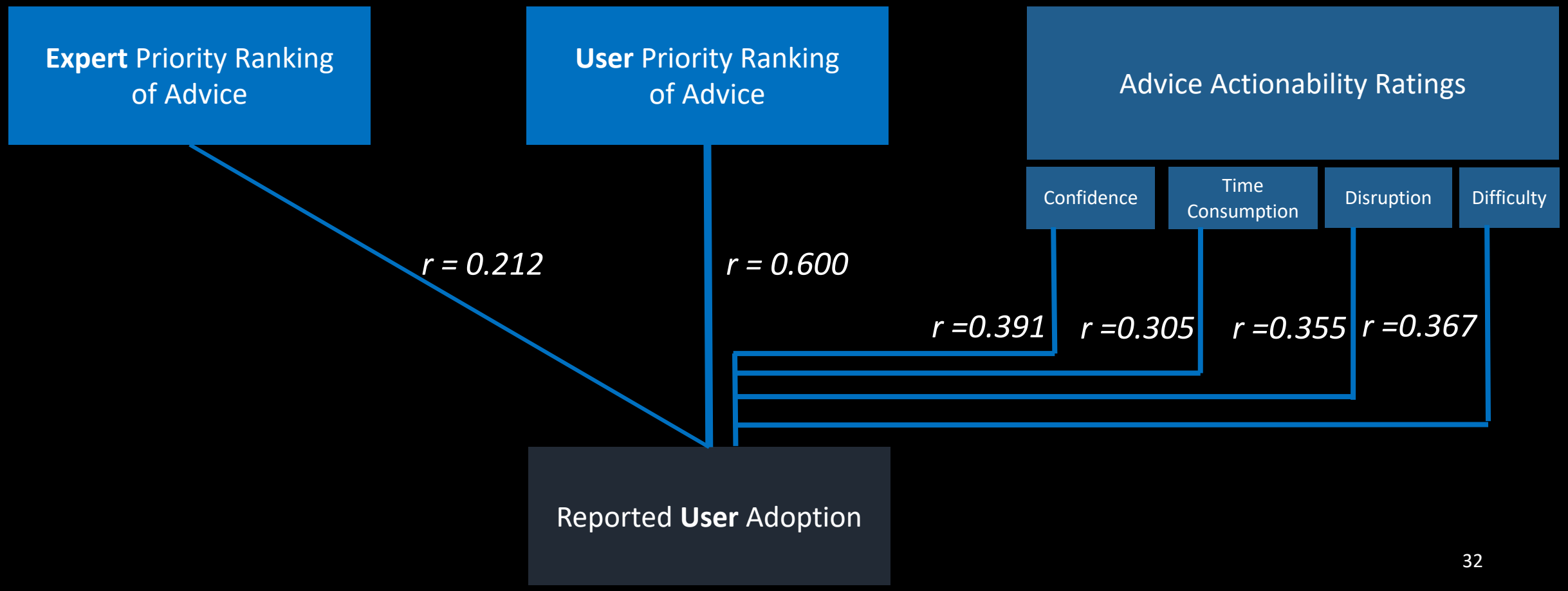


Top Advice

#1 Use unique passwords for different accounts
#2 Update devices
#3 Use anti-malware software
#4 Scan attachments you open for viruses
…

Used matrix factorization to generate full ranked list across all votes

Users' reported adoption of advice correlates with actionability & prioritization



Problem with online security advice: there is too much

Comprehensibility: average document is “partially” comprehensible to the average U.S. user

Leaves behind low-literacy users

Actionability: majority of advice rated as actionable and actionability correlates with prioritization & adoption

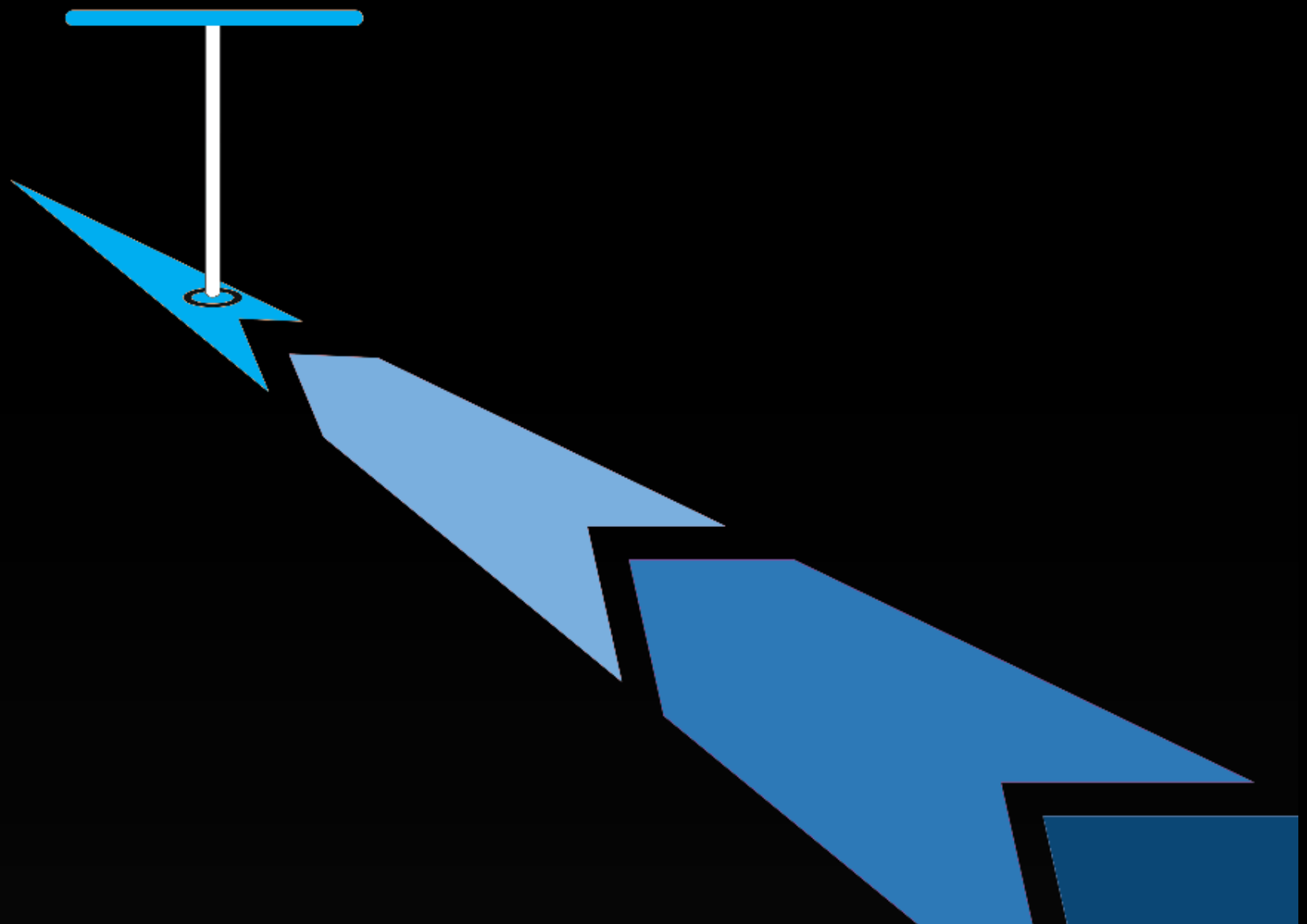
Data storage & network security advice not very actionable
20% of documents contain at least one unactionable piece of advice

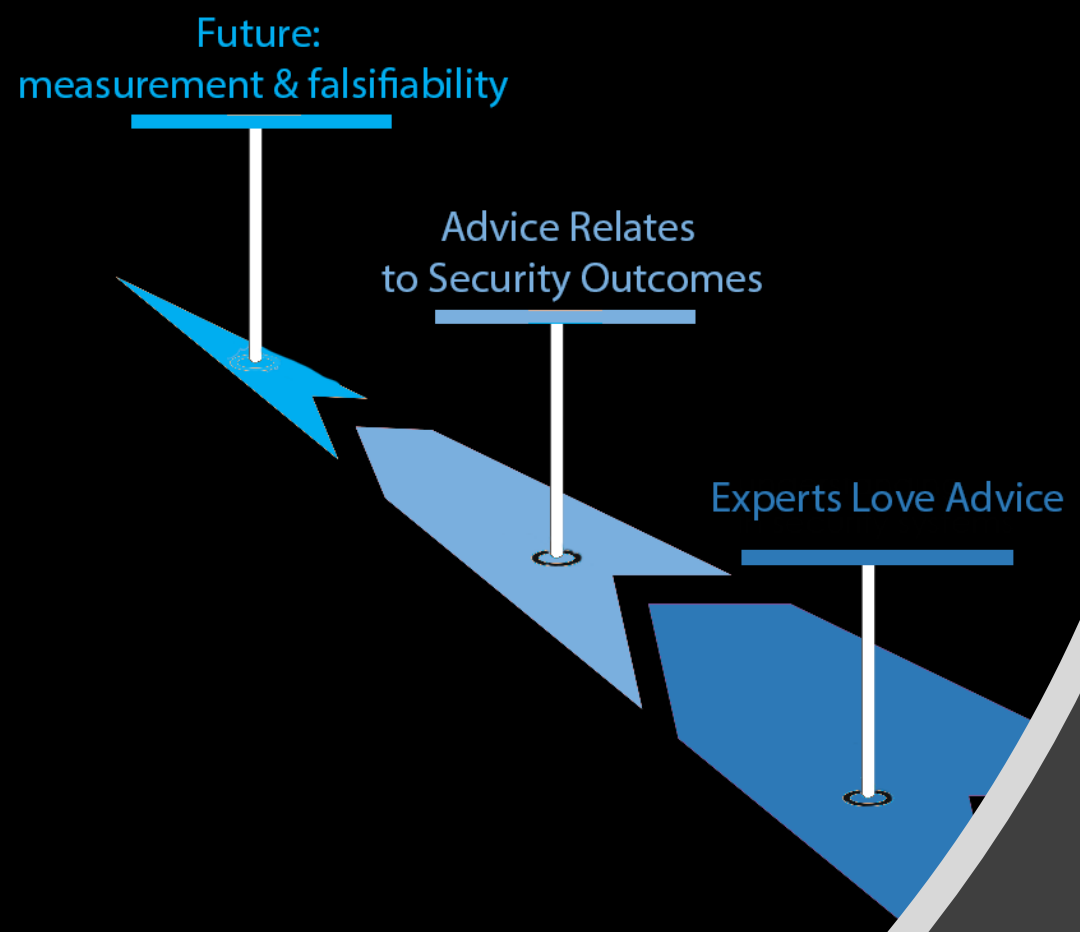
Accuracy: 89% of advice rated accurate

Lack of prioritization & falsifiability:
experts think (almost) all the advice is great

Future of Security Advice

Now What?





Future of security advice requires falsifiability for security claims and empirical studies to narrow down behaviors

A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web

Collected a corpus of 1,264 security advice documents

Through user generated queries and expert recommendations

Evaluated Quality along three axes

Average document is partially comprehensible to the average U.S. user
Majority of advice rated actionable; actionability correlated w/ reported behavior
89% of advice rated accurate by experts

Experts can't narrow down advice; need empirical science

Experts struggle to identify the most impactful advice
We need more concrete measurement & falsifiability

Elissa M. Redmiles, Noel Warford, Amritha Jayanti, and Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens and Michelle L. Mazurek

@eredmil1

eredmiles@cs.umd.edu