Who comes up with this stuff? Interviews with security advice authors

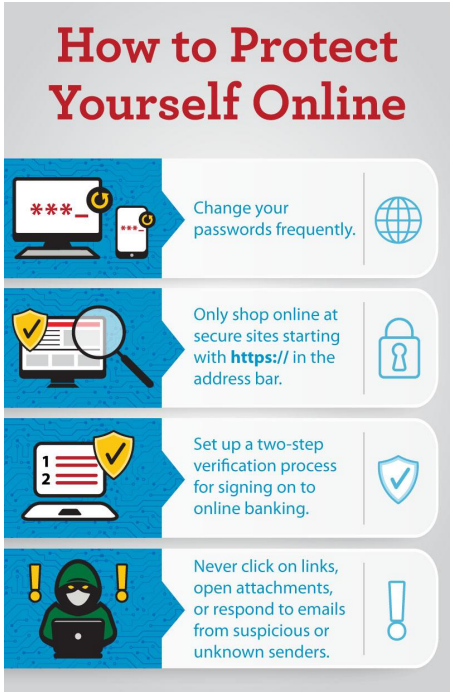
Lorenzo Neil[1], Harshini Sri Ramulu[2], Yasemin Acar[2], Bradley Reaves[1]

North Carolina State University[1]
The George Washington University[2]

19th Symposium on Usable Privacy and Security (SOUPS 2023)
Anaheim, CA

Security advice is plentiful, but hard to prioritize

- Users do not know which advice they should adopt.
- In a previous user study, 41 security experts mentioned 118 different pieces of security advice as the top 5 most important advice for users (Redmiles 2020).



Motivation

- Security advice is also…
  - Variable in coverage of important concepts (Acar 2017, Neil 2021).
  - Hard to adopt (Herley 2009, Christin 2011).

- Research Goal:
  - **To investigate root causes for why security advice varies in quality and prioritization.**

How is Security Advice Created?

- **Methodology:**
  - Conduct semi-structured interviews with 21 authors of security advice to learn:
    - Motivations for writing, revising, and publishing security advice.
    - Key decision making impacting the advice content.
    - Challenges in writing security advice.

Participant Recruitment

Various Recruitment Channels:

- Personal/professional contacts
- Social media
- Upwork
- Email Universities

Screening Survey:

- Describes research
- Qualifier to confirm professional experience

Perform Interviews:

- Scheduled after screening
- Performed remotely via Zoom

Interview Coding Analysis

- We use qualitative coding to accurately capture themes for advice creation from participants.
  - Coders meet weekly to resolve disagreements (Krippendorff's Alpha > 0.75).

- We use our codebook data to express our key findings and themes.

Advice Writing Processes

Formal four step writing process with common structure among advice writers.

Security Advice is Responsive

- Advice authors focus on novel security threats or events, prompting ad hoc additions to security advice.
- Such areas experience variable amounts of attention over time, indicating advice may undergo cycles of prioritization or fluctuate.

“So sometimes if they give advice, it’s based on something that’s going on. Yes. For example, a ransomware attack, they say, okay, universities are confronted with this type of attack, we should be careful with this”

A wide coverage of novel topics

- Advice writers cover a wide variety of less- common topics:
  - Participants mentioned **14 different topics** when asked what is the most common advice they cover.
  - Only online fraud and password advice were prioritized by at least 5 participants, respectively.

"I've seen a lot of advice that we've been putting out regarding job scams or email scams. Phishing is a big one that we've put out a lot of general guidance on. Those are the only big ones that really come to mind is the job scams and the phishing."

Advice writers rarely deprioritize advice

- Participants lacked s significant response when asked what advice isn't prioritized.
  - **A reluctance to actively curate or deprioritize content partially explains the advice prioritization crisis, as documented by prior work.**

Advice content is influenced by multiple distinct sources

- **20 different external sources mentioned, only 4 mentioned by at least 7 participants.**

- Sample Advice Influences:
  - Legal Regulations (e.g., GDPR, HIPAA).
  - Technical Standards (e.g., ISO, NIST).
  - External Entities (e.g., public websites, security awareness orgs).

“Normally, most of the companies we experienced are starting, and for certain companies, we normally recommend starting with NIST and ISO; they are well known, and their resources are well known, and they are well used”

Authors struggle with defining advice for wide audiences

- Defining the scope of their advice for broad audiences who lack fundamental security knowledge.
- Decisions about scope have major consequences on every other aspect of advice creation.

“I would say that just the process of deciding what advice to write like, what are the questions you're getting, putting some research into where the real problems are, and where are the gaps?”

Recommendations

- Develop the domain of general security advising.
  - e.g., Human-centered engagement in earlier writing stages.
- Proactive advice updates and curation.
- Establish a set of agreed upon standards for advice curation.
  - Collaborative effort between writers, industries, and researchers.

Conclusion

Advice writers struggle to gather and prioritize the information necessary to write advice, thus having a trickling effect into the processes and key decisions made in advice writing.

Thank You!

Lorenzo Neil: **lcneil@ncsu.edu**
Personal Website: lcneil23.github.io