How Experts Personalize Privacy & Security Advice for At-Risk Users

Wentao Guo, Alexander Yang, Nathan Malkin,* Michelle Mazurek

University of Maryland
**New Jersey Institute of Technology*

wguo5@umd.edu
@wentaoguo.bsky.social
@wentaochirps

Jo, a journalist, reports on government corruption.

Her devices are targeted by **government actors** using expensive spyware.

Sid is being harassed online by an abusive ex.

Her adversary has high levels of **personal knowledge and access**.

At-risk users face **increased chances** of being digitally attacked and/or suffering **disproportionate harms**.

Warford et al. (2022), “SoK: A framework for unifying at-risk user research”

At-risk users need good privacy and security advice!

Generic advice is often unhelpful.

Tailoring advice requires hazardous judgment calls without obvious answers.

- E.g., deleting spyware can trigger violence

Experts provide tailored advice through clinics.

Providers' processes and perspectives on how to tailor advice are not well understood.

By analyzing providers' processes and perspectives on tailoring advice, we could...

1. Inform efforts to study and improve advice.
2. Address challenges that providers face.
3. Improve self-service advice tools.

Research questions

1. What kinds of choices do providers make to **differentiate** advice, and why?
2. How can research and technology design better **support** providers in tailoring advice?
3. How should **self-service tools** account for risk factors when tailoring advice?

Participant recruitment

We recruited **18 providers** through NGOs, personal networks, and snowball sampling.

Areas of expertise:

- Human rights defenders, journalists (*n* = 16)
- Racial, religious, other minority groups (*n* = 10)
- Tech abuse (*n* = 4)

Key decisions in tailoring advice

Advice providers...

use various methods...

- Ask clients directly
- Search for evidence of compromise
- Observe or research clients
- Infer through educated guesses

icons: flaticon.com

to learn different types of context about clients' situations...

- Threat actors
- Vulnerable/compromised accounts and devices
- Accounts, apps, software, and devices
- Security hygiene
- Home and family situation
- Cultural and geographic context
- Identities

Constraints

- Tech literacy
- Language fluencies
- Resources
- Mental and emotional capabilities

Goals

- Security goals
- Lifestyle and work
- Acceptable trade-offs

State of mind

- Level of stress
- Other physiological state

in order to tailor advice.

- Assess threats and risks
- Rule out advice that violates clients' constraints
- Ensure advice is acceptable to clients
- Avoid unnecessarily upsetting clients
- Uphold their own principles

How do providers learn info about clients?

Ask clients directly

Search for evidence of compromise

Observe or research clients

Infer through educated guesses

Easy but not always reliable

> If you don't have a lot of technical knowledge, it's very easy to feel like your **abuser is capable of anything and everything**.

quotes edited for brevity

How do providers learn info about clients?

Ask clients directly

Search for evidence of compromise

Observe or research clients

Infer through educated guesses

Inconclusive outcomes cause issues

> Whether there is spyware on this device is **not very provable** often. I would rather start by ruling out relatively non-technical issues, because looking for spyware can **really freak out the person that I'm working with**.

How do providers learn info about clients?

Ask clients directly

Search for evidence of compromise

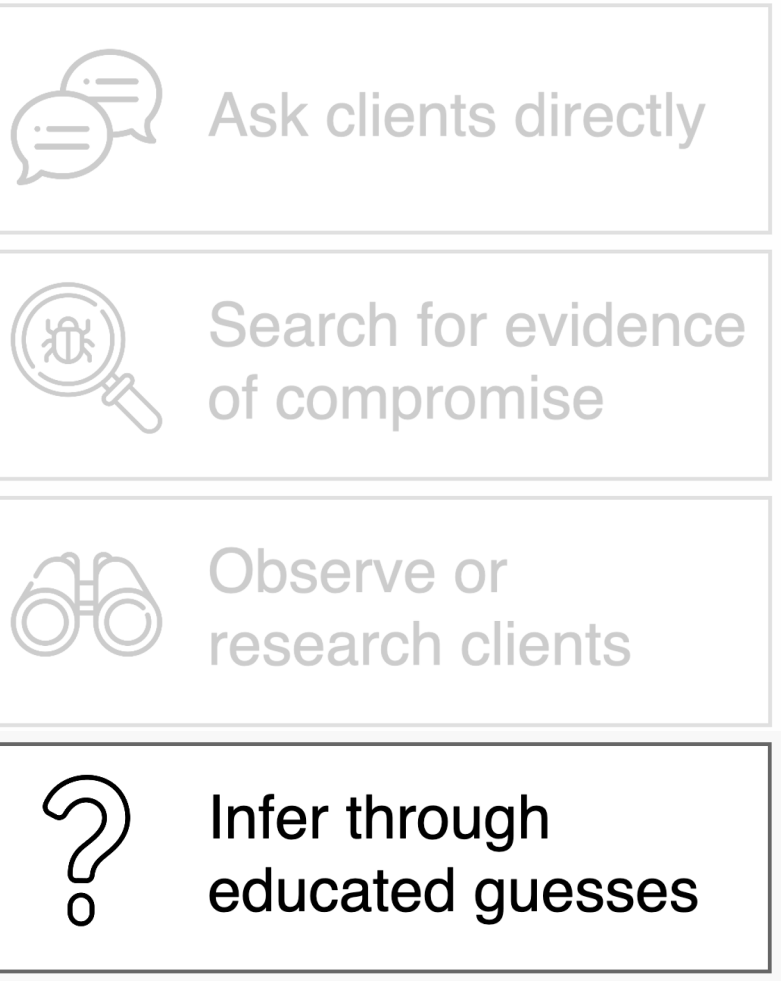
Observe or research clients

Infer through educated guesses

Time-consuming but trustworthy

> I'll show them how to use Veracrypt. If you're a normal person, you're going to totally stumble. But if they get through this, then I'm like, "Okay, **we can give you anything**."

How do providers learn info about clients?



Fills gaps but is error-prone

> Many clients from [redacted area] with similar backgrounds will have some similarities. You can't gauge the technical skills, you can't gauge the exact risk—but **you can get a bit of an approximation**.

Providers constantly grapple with many sources of **uncertainty** when tailoring advice.

What would help?

- More research on evolving threats & technologies
- Better diagnostic tools
- More accessible client-facing tools

How Experts Personalize Privacy & Security Advice for At-Risk Users

Wentao Guo, Alexander Yang, Nathan Malkin, Michelle Mazurek

Come find my poster for more on…

- Objectives and types of information involved in tailoring advice
- Guidelines for designing self-service tools responsibly

I am recruiting grad students in human-centered security and privacy at the University of Georgia, starting Fall 2027!

wguo5@umd.edu
@wentaoguo.bsky.social
@wentaochirps

This work was supported by the following organizations:

DARPA Google NSF