Guided understanding, not rules, could help children stay safer online

March 4 2022, by Jessica Hallman

Credit: Unsplash/CC0 Public Domain

As an increasing number of children use digital technologies to play, communicate, create, socialize and learn, the number of opportunities for their privacy to be exploited continues to grow. With many parents unaware of looming threats, and few formal school-based curricula on the topic, how can young users learn how to stay safe online?

The answer isn't asking children to memorize privacy rules, but rather helping them to learn from real-world experience, according to Priya Kumar, assistant professor in the College of Information Sciences and Technology. Kumar proposes a new practice-based approach that could lead to critical educational interventions designed to guide children in making informed decisions on how their private information is shared or stored online.

"Privacy literacy isn't about teaching kids facts about privacy, but more about helping them understand what it means to enact privacy in our everyday lives," she said. "By grounding privacy education in theories of learning, we can focus on how adults can help strengthen children's privacy literacy."

It starts with changing adults' attitudes, she said. Rather than thinking of things children do—such as sharing personally identifiable information—as naïve or flawed, adults should think about the world from a child's perspective to try to understand why actions that seem risky to adults might seem appropriate to children.

"Part of what I want to do through my research is to help us adults put ourselves in the minds of children and think about in what ways something like disclosing information might make sense to them, given their life experience," said Kumar. "This shifts the lesson from 'you did something wrong; that was bad' to 'let's think about the fact that social media is a place where strangers can contact you." We should be adding different layers to children's understanding of the digital world."

Kumar devised her proposed approach by blending two theoretical frameworks—contextual integrity, which views privacy from the perspective of how information flows; and the situative/pragmatist-sociohistorical perspective of learning, which posits that learning best happens in a community-based experience. To demonstrate what her approach offers to privacy education, she selected a single experience from a separate study she led on understanding how school-age children interpret and handle privacy online and further analyzed it through each of these frameworks.

In that case, an 11-year-old boy told Kumar about how he used Instagram to keep in touch with his friends who lived abroad. One day, people posing as children sent him messages asking for his video game system password in exchange for virtual rewards. When he asked his mom for the password, his mother—who knew to approach unsolicited requests with skepticism—used the organic opportunity to talk with her son about navigating risky online activities.

"He would have given (the password) in a heartbeat had he known it,'" the boy's mother told Kumar during the interview.

Kumar first analyzed the incident through the privacy framework of contextual integrity, which provides a way of understanding how flows of data and information may or may not raise privacy issues. In this explanation, she aimed to provide a sense of why the child interpreted the specific flow of information from the Instagram messengers in one way and his parent viewed it in another.

"He is in a headspace of Instagram being a place where friends connect and exchange information about games that he's really excited about. So, when someone he thinks is a peer is going to give him stuff that will help him out in the game in exchange for a password, to him, that information flow can seem like a good thing, like something appropriate," said Kumar. "Whereas his mom recognized that social media is a place where strangers can contact you, and that most of the time when somebody is asking you for a password, they usually don't have your best intentions in mind."

She added, "So for her the flow or the pieces didn't add up, and she was able to signal to her son that it wasn't a good idea to share the password."

Next, Kumar examined the incident through the situative/pragmatist-sociohistorical perspective of learning, which approaches learning as a shared practice of building identity in a community with others over time, to illustrate why children might be motivated to engage in seemingly risky actions. Kumar identified how the boy's posting on social media unwittingly opened himself up to interactions with people beyond his friends. When other users began to follow his account and engage with him based on content he'd posted, he assumed that they were other children enjoying the same game as him and his friends. And he interpreted their messages as coming from peers who shared his gaming interests rather than from actors with questionable motives.

According to Kumar, the Instagram messengers' effort to tap into the boy's identity as a gamer could explain why the requests to share his password resonated with him.

"I want for us to move away from more behaviorist orientations to learning, such as the idea that you should just tell people facts and make sure they memorize them," she said. "Instead, we must recognize the context that children are already engaging in, consider how their practices are shaping their identity, and then figure out how privacy fits into those practices and identities."

Through the practice-based approach to privacy literacy, children can begin to understand how everyday experiences shape their privacy and reflect on how they can make decisions that embody what privacy means to them. This shouldn't be a process of adults instructing children what to do, but of adults helping children hone their skills in managing information.

"Today's children are growing up in a world that is digital by default—they're using technologies, interacting with people, and making decisions," she said. "Privacy literacy is actually something that children already have, by virtue of the fact they are living in a digital environment. Our job as adults is to try and understand the world from their perspective and to offer guidance to help them make sense of data flows in different ways."

Kumar hopes that her approach will lead to future efforts to design educational experiences that help children understand and navigate privacy questions, specifically through communities of practice that children engage in and the identities they shape through them.

Kumar presented her paper, "Toward a Practice-Based Approach to Privacy Literacy," this week at iConference 2022, where it was one of five finalists for the conference's Best Short Research Paper award. Kumar also was a runner up for the iSchools Doctoral Dissertation Award, announced earlier this week, which recognizes the year's most outstanding dissertations from across iSchools' global membership.

More information: Toward a Practice-Based Approach to Privacy Literacy. www.springerprofessional.de/en … cy-literacy/20158314

Provided by Pennsylvania State University

Citation: Guided understanding, not rules, could help children stay safer online (2022, March 4) retrieved 4 May 2024 from https://techxplore.com/news/2022-03-children-safer-online.html