New tools to detect digital domestic abuse

August 14 2019, by Melanie Lefkowitz

Credit: CC0 Public Domain

Carol is locked in a custody battle with her abusive ex-husband. She has an order of protection against him, but he's somehow able to access her private photos and post them on Facebook.

He hacks into her online accounts, where he poses as her to insult her friends and family. He locks her out of her own Gmail account, devastating her sales career.

Carol—a composite invented by researchers who have heard many

similar stories—is vulnerable to digital harassment because her ex-husband bought two of her devices, knows or can guess her passwords and has access to their children's phones.

A new clinical model developed by Cornell Tech researchers aims to respond systematically and effectively to the growing array of digital threats against victims of intimate partner violence. Working with the New York City Mayor's Office to End Domestic and Gender-Based Violence, the researchers created and piloted a questionnaire, a spyware scanning tool and a diagram for assessing clients' digital footprints.

The first-of-its-kind model can help counselors without tech expertise pinpoint online abuse—and protect the safety of abuse victims and their advisers. Using this strategy, researchers found potential spyware, compromised accounts or exploitable misconfigurations for 23 of the 44 clients they advised.

"Prior to this work, people were reporting that the abusers were very sophisticated hackers, and clients were receiving inconsistent advice," said Diana Freed, Cornell Tech doctoral student in the field of information science and co-lead author of "Clinical Computer Security for Victims of Intimate Partner Violence," presented Aug. 14 at the USENIX Security Symposium in Santa Clara, California.

"Some people were saying, "Throw your device out." Other people were saying, "Delete the app." But there wasn't a clear understanding of how this abuse was happening and why it was happening," Freed said. "We felt that a methodical approach through a uniform, data-driven consultation would yield better results so we can help other advocates do this type of work at the level it's needed."

Co-first author of the paper is Sam Havron, Cornell Tech doctoral student in computer science. Senior authors are Nicola Dell, assistant

professor at the Jacobs Technion-Cornell Institute at Cornell Tech, and Thomas Ristenpart, associate professor at Cornell Tech.

The authors are among the researchers from Cornell Tech, Cornell in Ithaca and New York University collaborating to improve technological safety and security for survivors of intimate partner violence. Dell and Ristenpart were recently awarded a $1.2 million grant from the National Science Foundation to continue their research examining the role of tech in intimate partner abuse.

Abusers use a range of digital tools to stalk or harass their victims, from traditional spyware to tracking apps intended for more benign purposes, like finding one's phone. It can be extremely challenging to detect vulnerabilities amid the sheer number of apps, digital devices and online accounts most people use daily—particularly for counselors without tech skills.

"They were making their best efforts, but there was no uniform way to address this," Havron said. "They were using Google to try to help clients with their abuse situations."

At the same time, tech experts don't have the background to advise clients how to fix problems in ways that won't endanger them, such as angering an abuser who just noticed a deleted app or a changed password.

The researchers run a weekly tech clinic in New York City's Family Justice Centers, which provide a full range of services for intimate partner abuse victims. Through this work, the team developed and piloted its Technology Assessment Questionnaire, which includes such questions as, "Does the abuser show up unexpectedly or know things they shouldn't know?" and "Is there a chance the abuser knows (or could guess) the answers to your password reset questions?"

They also created the "technograph," a diagram which helps summarize clients' digital assets; and ISDi (IPV Spyware Discovery), a spyware scanning tool. ISDi scans devices for known spyware apps through a USB cable, rather than a downloadable app, making it impossible for an abuser to detect.

"This sort of tool doesn't exist anywhere else," Havron said. "In earlier work, we did a comprehensive scrape of the Google Play Store and eventually compiled a list of thousands of apps across marketplaces, and that's what the ISDi is based on."

The questionnaire, technograph and ISDi are all freely available on the project team's website.

Though the paper focused on intimate partner abuse, this method could be useful for any victims of online abuse, such as activists, dissidents or journalists, the researchers said.

"It's consistent, it's data-driven and it takes into account at each phase what the abuser will know if the client makes changes," Freed said. "This is giving people a more accurate way to make decisions and providing them with a comprehensive understanding of how things are happening."

More information: Clinical Computer Security for Victims of Intimate Partner Violence. www.nixdell.com/papers/2019-us … al_security_FULL.pdf

Provided by Cornell University