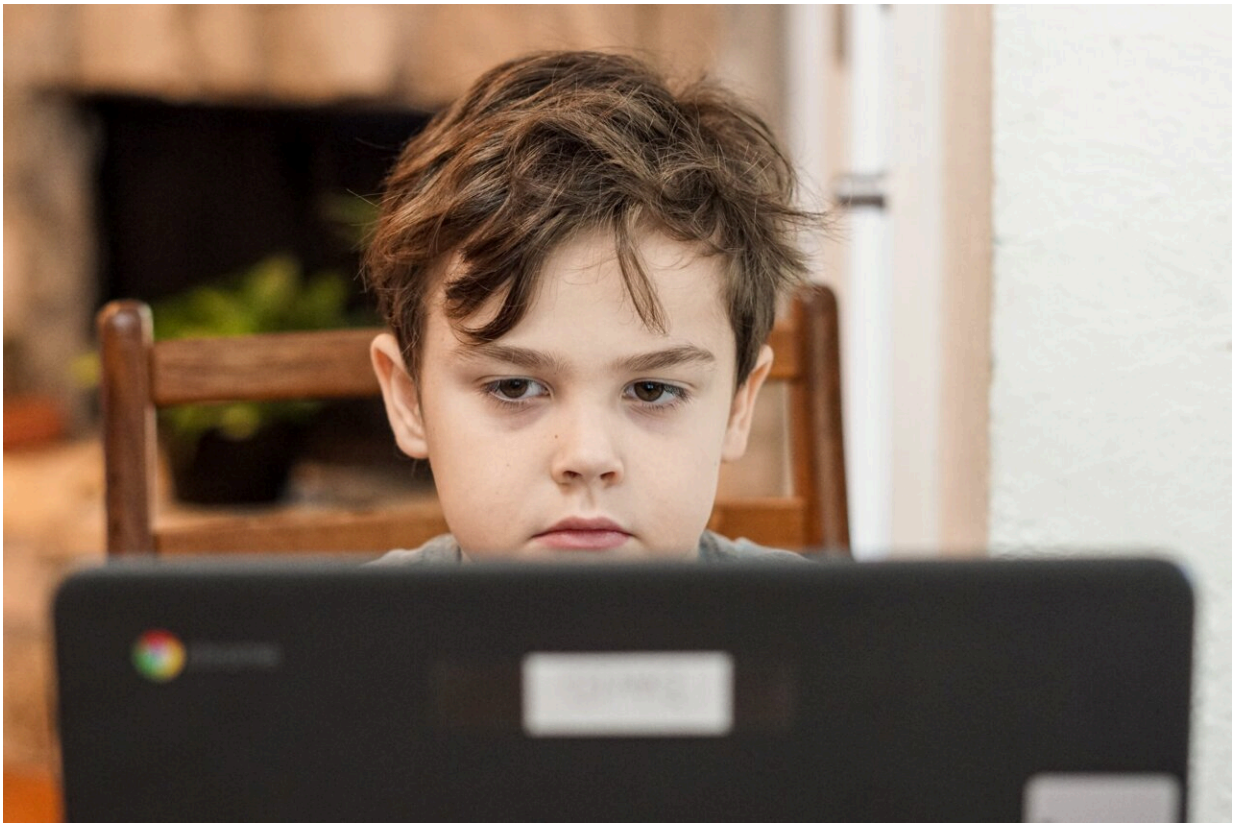
Online predators target children's webcams, study finds

May 3 2023, by Eden Kamar and Christian Jordan Howell



Credit: Unsplash/CC0 Public Domain

There has been a tenfold increase in sexual abuse imagery created with webcams and other recording devices worldwide since 2019, according to the the Internet Watch Foundation.

Social media sites and chatrooms are the most common methods used to facilitate contact with kids, and abuse occurs both online and offline. Increasingly, predators are using advances in technology to engage in technology-facilitated sexual abuse.

Once having gained access to a child's webcam, a predator can use it to record, produce and distribute child pornography.

We are criminologists who study cybercrime and cybersecurity. Our current research examines the methods online predators use to compromise children's webcams. To do this, we posed online as children to observe active online predators in action. The results of our latest research are published in the journal *Computers in Human Behavior*.

Chatbots

We began by creating several automated chatbots disguised as 13-year-old girls. We deployed these chatbots as bait for online predators in various chatrooms frequently used by children to socialize. The bots never initiated conversations and were programmed to respond only to users who identified as over 18 years of age.

We programmed the bots to begin each conversation by stating their age, sex and location. This is common practice in chatroom culture and ensured the conversations logged were with adults over the age of 18 who were knowingly and willingly chatting with a minor. Though it's possible some subjects were underage and posing as adults, previous research shows online predators usually represent themselves as younger than they actually are, not older.

Predator	hi
Predator	how r you
Predator	what r u up to
Chatbot	Hi 14 girl, asl?
Predator	19 m uk
Predator	what r u up to now?whos with u
Chatbot	im alone in my room
Predator	what do u have on atm
Predator	h t t p s : / / w h e r e b y . c o m / [redacted]
Chatbot	pj
Predator	cute. same
Predator	let meknow when u there

A section of dialogue between a self-identified adult and the researchers' chatbot posing as a 13-year-old. Credit: Eden Kamar, CC BY-ND

Most prior studies of child sexual abuse rely on historical data from police reports, which provides an outdated depiction of the tactics currently used to abuse children. In contrast, the automated chatbots we used gathered data about active offenders and the current methods they use to facilitate sexual abuse.

Methods of attack

In total, our chatbots logged 953 conversations with self-identified adults who were told they were talking with a 13-year-old girl. Nearly all the conversations were sexual in nature with an emphasis on webcams. Some predators were explicit in their desires and immediately offered payment for videos of the child performing sexual acts. Others attempted to solicit videos with promises of love and future relationships. In addition to these commonly used tactics, we found that 39% of conversations included an unsolicited link.

We conducted a forensics investigation of the links and found that 19% (71 links) were embedded with malware, 5% (18 links) led to phishing websites, and 41% (154 links) were associated with Whereby, a video conferencing platform operated by a company in Norway.

(Editor's note: The Conversation reviewed the author's unpublished data and confirmed that 41% of the links in the chatbot dialogs were to Whereby video meetings, and that a sample of the dialogs with the Whereby links showed subjects attempting to entice what they were told were 13-year-old girls to engage in inappropriate behavior.)

It was immediately obvious to us how some of these links could help a predator victimize a child. Online predators use malware to compromise a child's computer system and gain remote access to their webcam. Phishing sites are used to harvest personal information, which can aid the predator in victimizing their target. For example, phishing attacks can give a predator access to the password to a child's computer, which could be used to access and remotely control the child's camera.

Whereby video meetings

At first, it was unclear why Whereby was favored among online predators or whether the platform was being used to facilitate online sexual abuse.

After further investigation, we found that online predators could exploit known functions in the Whereby platform to watch and record children without their active or informed consent.

This method of attack can simplify online sexual abuse. The offender does not need to be technically savvy or socially manipulative to gain access to a child's webcam. Instead, someone who can persuade a victim to visit a seemingly innocuous site could gain control of the child's camera.

Having gained access to the camera, a predator can violate the child by watching and recording them without actual—as opposed to technical—consent. This level of access and disregard for privacy facilitates online sexual abuse.

Based on our analysis, it is possible that predators could use Whereby to control a child's webcam by embedding a livestream of the video on a website of their choosing. We had a software developer run a test with an embedded Whereby account, which showed that the account host can embed code that allows him to turn on the visitor's camera. The test confirmed that it is possible to turn on a visitor's camera without their knowledge.

We have found no evidence suggesting that other major videoconferencing platforms, such as Zoom, BlueJeans, WebEx, GoogleMeet, GoTo Meeting and Microsoft Teams, can be exploited in this manner.

Control of the visitor's camera and mic is limited to within the Whereby platform, and there are icons that indicate when the camera and mic are on. However, children might not be aware of the camera and mic indicators and would be at risk if they switched browser tabs without exiting the Whereby platform or closing that tab. In this scenario, a child

would be unaware that the host was controlling their camera and mic.

(Editor's note: The Conversation reached out to Whereby, and a spokesperson there disputed that the feature could be exploited. "Whereby and our users cannot access a user's camera or microphone without receiving clear permission from the user to do so via their browser permissions," wrote Victor Alexandru Truică, Information Security Lead for Whereby. He also said that users can see when the camera is on and can "close, revoke, or 'turn off' that permission at any time." A lawyer for the company also wrote that Whereby disputes the researchers' claims. "Whereby takes the privacy and safety of its customers seriously. This commitment is core to how we do business, and it is central to our products and services.")

Revoking access to the webcam following initial permission requires knowledge of browser caches. A recent study reported that although children are considered fluent new media users, they lack digital literacy in the area of safety and privacy. Since caches are a more advanced safety and privacy feature, children should not be expected to know to clear browser caches or how to do so.

Keeping your kids safe online

Awareness is the first step toward a safe and trustworthy cyberspace. We are reporting these attack methods so parents and policymakers can protect and educate an otherwise vulnerable population. Now that videoconferencing companies are aware of these exploits, they can reconfigure their platforms to avoid such exploitation. Moving forward, an increased prioritization of privacy could prevent designs that can be exploited for nefarious intent.

Here are some recommendations to help keep your kid safe while online. For starters, always cover your child's webcam. While this does not

prevent sexual abuse, it does prevent predators from spying via a webcam.

You should also monitor your child's internet activity. The anonymity provided by social media sites and chatrooms facilitates the initial contact that can lead to online sexual abuse. Online strangers are still strangers, so teach your child about stranger danger. More information about online safety is available on our labs' websites: Evidence-Based Cybersecurity Research Group and Sarasota Cybersecurity.

More information: Eden Kamar et al, Parental guardianship and online sexual grooming of teenagers: A honeypot experiment, *Computers in Human Behavior* (2022). DOI: 10.1016/j.chb.2022.107386

Provided by The Conversation