SCHOLARS
STRATEGY NETWORK

CYBERCRIME AND THE CHALLENGE OF SECURING VIRTUAL ENVIRONMENTS FOR STUDENTS

By Dr. 'Shawn Smith, Radford University

Transcending demographic, geographic, and behavioral distinctions, virtually every social aspect of who we are and what we do was and continues to be impacted by the COVID-19 pandemic. Perhaps no more keenly has this been observed than in America's school systems, where the effort to limit infections and uphold proper health standards has ushered in an unprecedented era of pedagogical reimagining through digital technology. Internet activity among school-aged children has increased to meet the demands of this new learning landscape, and with it spikes in online targeting and victimization of these younger audiences. In response, school administrators, teachers, and parents must be supported with the knowledge and resources to employ effective safeguards against such cyberthreats.

INCREASED RATES OF CYBERVICTIMIZATION

Some preliminary reports already identify young people being targeted and victimized online at dramatically higher rates since the pandemic sparked worldwide. Reports of *online enticements* – meeting a perpetrator online and being coerced into either transmitting self-produced images online, or producing such images offline after an initial online encounter – increased 48% between January 2020 and June 2020. During the same time period, CyberTipline (a centralized reporting system for the online exploitation of children) received over 12 million reports – an increase of 47% from the same time period in 2019 (O'Donnell, 2020).

Additionally, current Interpol reports reveal several trends supporting cause for heightened concern for the safety of school-aged children online since the pandemic's rise (Interpol, 2020). These include increasing reports among member countries in the following areas:

- Consumption, distribution, and discussion of child sexual exploitation material
- Reports of inadvertent exposure to such material on social media platforms
- The distribution of such material via messaging applications and peer-to-peer networks
- Distribution of child sexual exploitation material via "zoom-bombing" – the phenomenon of uninvited guests invading videoconference sessions (often via the Zoom conferencing application)

The risk and impact of cybervictimization in this climate cannot be understated. With such broad incorporation of virtual learning models both currently and in the foreseeable future, school children will be spending more hours online than ever before. Thus, now more than ever, schools and parents alike must turn their attention to safety education and bolstering technological infrastructure towards addressing the cyberthreats confronting school-aged children.

BEST PRACTICES FOR SCHOOLS AND SCHOOL DISTRICTS

For schools and school districts tasked with facilitating virtual learning, there are a variety of hardware, software, and infrastructure measures critical to minimizing risk of exposure to inappropriate materials and exploitation. Among the more pressing of these:

- Establishing reliable VPN service for students, staff, and faculty (especially for families receiving devices for remote learning),
- Scheduled monitoring of live streams during class sessions,
- Assigning "gatekeepers" from among students, staff, and faculty to help facilitate live stream monitoring (i.e., preventing "zoom-bombing"),
- Installing and running routine maintenance on ad-blocking software,
- Establishing a routine schedule of Internet safety education for students, staff, and faculty,
- Employing restrictions on video and streaming services (e.g., YouTube, Netflix, Hulu) during school hours (filtering out content disassociated with grade-specific curricula),
- Partnering with law enforcement (local, state, and/or federal) for developing and implementing Internet safety training programs and routines for such programming.

Additionally, schools and districts should maintain an active list of approved and unapproved websites, and this list should be made available to all school stakeholders. Notably, websites known for harboring online predators and explicit material like dating websites, social media unrelated to the school curriculum, and gaming communities should at minimum be heavily restricted and avoided altogether if possible.

BEST PRACTICES FOR PARENTS OF SCHOOL-AGED CHILDREN

For the parents and guardians of children engaged in virtual learning, the challenge of securing the virtual experience may be even greater. Parents today often must try to stay on top of the seemingly endless caravan of threats targeting kids online while still juggling vital work and household responsibilities. Playing "Internet-cop" on a 24-7 basis is just not that realistic for many families, and especially those faced with increasing demands on work hours and/or a lack of technological knowledge to keep track of online threats.

Yet, with the known online risks to children more plentiful and potentially damaging than ever before, it is no longer a safe option for parents and other guardians to remain ignorant of the best practices for protecting the online experiences of their children. Thus, parents and guardians of virtual learners should:

- Begin making a habit of talking with both their kids and their kids' friends about making healthy choices online (e.g., monitoring screen time/app access, content age appropriateness, managing notifications, chatroom/e-mail etiquette, detecting/resolving unsafe online behavior),
- Install and become familiar with at least one online monitoring app and/or technique,

Read more in Interpol, "Threats and Trends: Child Sexual Exploitation and Abuse (COVID-19 Impact)," (2020); Brenna O'Donnell, COVID-19 and Missing and Exploited Children, (2020).

- Safeguard webcams so that children only have access to it while using Zoom, Google Classroom, Microsoft Teams, and/or whatever additional videoconferencing applications a school district might have adopted.

In conclusion, as this brief is mainly intended to introduce information and talking points on the subject of cybercrime where school-aged children are concerned, readers are strongly encouraged to use this document towards stimulating further investigation and discourse on the aforementioned issues and suggestions in their respective communities. Schools and parents alike must find a common voice on these matters and work collaboratively towards ensuring a safe and rewarding online experience for students now and moving forward. This way, schools stay in tune with the parents' concerns and parents comprehend more clearly the role schools are taking to best safeguard the educational experience for their kids. At present, such is the root of much disconnect between schools and parents in far too many communities.

Read more in Interpol, "Threats and Trends: Child Sexual Exploitation and Abuse (COVID-19 Impact)," (2020); Brenna O'Donnell, COVID-19 and Missing and Exploited Children, (2020).