Love and ZeroTrust:

Protecting Minors in Online Relationships

By Aaron R. Warner, CEO and Lindy Trout, Creative Technical Writer
ProCircular, Inc.

Love and fear are familiar emotions for any parent, and often they happen at the same time. The modern online world is no exception, and with COVID, these sentiments are amplified. Many of us at ProCircular are parents, and the importance of our work is underlined by emails like this one:

"Tim is 17 and attends a midwestern high school. Last week, we learned that he had been in communication with somebody who had created a fake Instagram account. The individual posed as a female and lured him into some intimate texts and messaging, and eventually, the two of them exchanged some pictures with one another. Tim later learns the Instagram account is fake. Now they are trying to extort him for money or leak his information to all of his social media friends, connections, and colleagues in addition to school and football team."

Earlier this month, Tim's parents reached out to ProCircular for opinions about moving forward in this case. They continued:

"We immediately notified the local PD last and encouraged our son to stop all communication, but he continues to be harassed day and night with non-stop messaging and calls.

We didn't comply with the request for money. Today Tim's Principal received an inbound email message with the explicit photos. They are still demanding money or indicate they will leak to more personal sources."

This case is truly shocking, and our hearts go out to both Tim and his parents. Hearing this story forces us to recall our teenage years and that universal desperation for interpersonal connection. Add two years of confinement during "school from home" and the instant gratification of social media, and it's hard to blame him for getting carried away.

It is important to remember that targets of extortion are victims of criminal behavior. Protecting victims' rights is of top priority in cases that involve the sexual exploitation of a minor, and this is a first-hand example of those cautionary tales we tell our children.

Bring in the Experts

First, ProCirular assured the victim and his family that engaging law enforcement is the right idea, but this case has likely exceeded the scope of local PD, and the FBI should become involved. The images that the two exchanged are forever released to the internet, and there's no way to recall them. Now that the damage is done, the case is in the hands of federal investigators to find and bring to justice the individual or network of individuals responsible.

While we wait for Tim's case to be resolved, we can reverse engineer the situation and offer some preventative measures that might protect other kids in the future. While there is no combatting a teenager's impulses and curiosity regarding the internet, parents can help by starting a transparent, ongoing, and understanding conversation about internet safety and personal security. Everyone's approach to this subject is a little different, so we opened the discussion to our entire bench of ProCircular's compliance and technical security experts and collected that advice into this article.

Lessons Learned

Prevention is the best form of incident management, but in the unfortunate case that you are the victim of an online extortion attempt, these are the tips that you will want to follow:

Don't Pay

Our incident responders have seen more than a few similar cases where victims pay, and the attackers come back for more money. We can't assume that the bad guys are telling the truth. There is no guarantee that you will benefit from complying with their demands. Work with resources that have your best interest in mind, like law enforcement or incident responders, rather than negotiating directly with the criminals. Security professionals have the insight and experience to assess the severity and estimate the validity of the threat actor's claims. They use time-tested strategies to move negotiations forward without giving up information unnecessarily.

Stay Calm

Like in any extortion case, these cybercriminals use time, shame, and secrecy to their advantage. They use psychological tactics to disarm the victim and prevent them from seeking outside help. Fear is the mind-killer, and bad actors will deliberately induce stress to cloud your judgment. Tim did the right thing by reaching out to his parents, and they continued by reaching out to the police and cybersecurity specialists.

Family Cares

The photos are already in the wild; that's virtually guaranteed. As hard as it is to believe, family and friends are more forgiving than people think in these circumstances. Taking a proactive approach to letting people know that they may receive the photos and sharing the story as a cautionary tale will soften the blow and save another kid from being a victim. Ask them to delete rather than open the message.

Child Pornography

The simple possession of these images is an immense personal and professional legal risk, even when they've arrived in your inbox unprompted. Even if you mean well by sharing such content with news media or friends, you can face legal trouble, including second-degree sexual exploitation of a minor. Simply having it on your computer for a brief time, sending it to others to get their opinions, and double-checking to confirm what you thought you may have seen can blur the lines about your intent. There's also a good chance that one of the major internet cloud providers (Google, Apple, Microsoft) may be scanning behind the scenes for images like these. They have a mandatory responsibility to report possession to law enforcement.

Who to Call

The first step should be to contact a trusted legal professional to discuss the next steps. Simply possessing these images will land you in dangerous waters, and you need solid legal assistance to navigate these waters. Your next steps will likely be to speak with both local police and the FBI. There is a good chance that you're not alone, and involving them increases the likelihood that you can protect other kids and their parents. Both take the victim's rights seriously, and neither will judge you or your children for what led to the call.

Education is Key

As digital natives, some of today's children are more tech-savvy than their parents. One of ProCircular's consultants provided an example of a little girl that circumvented screen time limits on her mom's iPhone by starting a "screen recording" before handing the device over to be unlocked. Kids are not stupid. Our young engineers will almost definitely see parental controls as a challenge they need to beat. As one of ProCircular's interns said:

"For a while, my parents would put Spyware (don't know which one) on my desktop and somewhat track me on my phone. I didn't know why they did it at the time, but I, being my young curious self, wanted to know what and why they were spying and blocking my activities at times. When I got more into cybersecurity and the industry, I learned on my own why they did it. I was always trying (sometimes successfully) to get around the Spyware and eventually saw why they wanted to do it."

While monitoring and managing tools have their place, they need to be paired with essential security awareness and hygiene to protect the user effectively. Parents can lock down phones, computers, and the home network, but kids will find a way to stay connected. Second phones, friend's devices, and school computers will eventually become opportunities to get around security controls.

Although parental control software is no silver bullet, most options on the market include valuable features to manage screen time and website access. As a pro tip, we recommend Circle, a parental control subscription service that actually works. (they'll hate it)

Tim's case isn't all that unique; children are targeted by cybercriminals every day. While the FBI works to identify and prosecute the offenders, families can build up their internal defenses. Secure cyber hygiene starts with an open, honest, and ongoing discussion about personal security online. The cyber landscape is everchanging, and new threat vectors emerge every day.

The subject of online security probably doesn't need to take over every discussion around the dinner table. Still, kids and teens should feel comfortable questioning and discussing what they encounter on the internet. For more help getting that conversation started, check out this free resource from the Center for Cyber Safety and Education, or contact ProCircular at 844-957-3287.