ESET

Proven. Trusted.

TECH BRIEF: EDUCATION
HOW DO WE PROTECT KIDS FROM ONLINE PREDATORS?

BY LYSA MYERS

The Internet is a vast source of information for all of us, and naturally some people use that information for good, and some for ill, like grooming and stalking children. So what things can you as a parent, teacher or other concerned adult do to protect kids against online predators and solicitation?

I recently wrote about privacy and domestic violence survivors and one of the first things that struck me was how much of the advice out there was woefully outdated. For example, at this point I'm not sure how much use it is to tell people how to safely interact with AOL chat rooms. Likewise, a lot of the information about protecting children from online predators is from another Internet era, before we were all carrying the Internet with GPS and hi-definition audio/video capabilities in our pockets.

In searching for statistics, what I found (that wasn't from a bygone era) was that online predators tend to glean a lot of information from social networking sites:

- *In 82% of online sex crimes against minors, the offender used the victim's social networking site to gain information about the victim's likes and dislikes.*

- *65% of online sex offenders used the victim's social networking site to gain home and school information about the victim (InternetSafety101.org)*

But the specific means of gleaning information is less important than the prolific yet largely unwitting sharing of information with strangers. Predators may target children who are participating in attention-seeking behaviors as a way of finding connections with others. Sadly, these kids seeking connection are generally

the ones least apt to have a concerned adult to whom they can turn to report solicitation. These targeted kids may also not wish to report the behavior, as they may simply be glad for the interest and may naturally be naïve about the nature of the attention.

Understanding online solicitation

The following list from Microsoft® describes the actions of online predators:

- *Find kids through social networking, blogs, chat rooms, instant messaging, email, discussion boards and other websites.*

- *Seduce their targets through attention, affection, kindness and even gifts.*

- *Know the latest music and hobbies likely to interest kids.*

- *Listen to and sympathize with kids' problems.*

- *Try to ease young people's inhibitions by gradually introducing sexual content into their conversations or by showing them sexually explicit material.*

- *Might also evaluate the kids they meet online for future face-to-face contact.*

Out of context, this starts out sounding like friendly behavior. But clearly there is a very unhealthy progression. In essence, this behavior is like long-term social engineering, because it is done with harmful intent. Solicitation preys on innocent, trusting people in order to get something that they would not freely give otherwise.

Protecting children on- and off-line

Tips for reducing the risk of children being victimized generally center around monitoring and controlling their access to the Internet in an age-appropriate way. But as this article from the San Diego Police Foundation points out, not all solicitation happens online, so more needs to be done to prepare kids to recognize the signs. It is essential to make sure that kids know from an early age what is appropriate information to share with others, even people who appear to be friends (as this is what predators make themselves out to be).

Establish rules about when it is okay to:

- *Send or post photos*
- *Give contact or identifying information for themselves or family members*

Let kids know it is best to:

- *Socialize online only with kids they know in real life*
- *Avoid personal discussions with strangers online, especially conversations involving sex, violence and illegal activities*

As older kids become eligible for social networking sites, they may wish to meet in person some people whom they have met online. It is important that a parent or guardian accompany the teen to any first meeting, to determine whether the situation is safe and age-appropriate.

The idea of establishing rules is not to make a child fearful of strangers, but to instill in them an ability to scrutinize communications in a way that comes from a healthy sense of self-worth. There is a saying that is popular in the security industry: "Trust, but verify." This means not blindly accepting someone's words at face value, but doing additional research to determine if a communication is trustworthy.

Parental concern versus independence

Good parenting (or mentoring) is about finding that balance between providing children with the tools to become independent adults, and spending enough time with them that they feel loved and protected. When children are younger, you can safely lean towards being overprotective, until they can understand and internalize the reasons for the rules.

Perhaps the most important thing you can do to protect kids from online predators is to establish a good rapport and open lines of communication with them. Social engineering relies on creating a strong feeling either of fear or of trust. If a child feels they can discuss their experiences with a trusted adult, without concern for punishment or judgment, they can verify whether questionable online communications are scams or solicitation. It is important to remember that even if children respond positively to online predators, they are still the victims in the same way that anyone who has fallen for a scam is a victim.

Communication and curiosity

The FBI provides a guide for parents which includes a considerable amount of additional information for parents about how to recognize when a child may be at risk for solicitation, and what to do if you suspect your child has been targeted. They also provide the following list of tips for how to improve communication with children about their online activities:

- *Communicate, and talk to your child about sexual victimization and potential on-line danger.*
- *Spend time with your children on-line. Have them teach you about their favorite online destinations.*
- *Keep the computer in a common room in the house, not in your child's bedroom. It is much more difficult for an online sex offender to communicate with a child when the computer screen is visible to a parent or another member of the household.*

The general idea here is not to come from a place of accusing children, or scaring them about potential dangers. If you approach your child's online activities with a sense of curiosity and interest, you can potentially see a problem before it becomes genuinely dangerous.

Children are naturally curious, and the Internet can be a great way for them to learn and explore, given reasonable boundaries to guide them. With proper adult guidance, they can gain the confidence to protect themselves throughout all their online and offline endeavors.