PFA Tips

Help Prevent Cyber Crimes Committed By Or Against Your Child

Face it – EVERYONE is online from what seems to be starting at age two (if not younger). While most of us are using the internet for good – shopping, research, watching cat videos, trolling friends' social media accounts – not everyone's experiences have positive outcomes. Navigating the online world can be tricky, especially for our loved ones with autism that may have difficulty understanding the social aspects. This can lead to them becoming victims of cybercriminals, or unintentionally be committing cyber crimes themselves. What rules can we put in place to reduce the risks?

First, what YOU need to know and do

What happens on the internet stays on the internet…. forever

Emphasize to your child that deleted items on the internet and social media apps are never really gone for good. If they regret something they put out there (nudes/partial nudes, selfies, images/video doing stupid tricks that could land them in trouble, etc.), they can't really take it back.

A stranger is a stranger. Period.

Think about it – depending on the age of your child, you wouldn't let them talk to a stranger even under your supervision. Talking to a stranger is talking to a stranger regardless of the medium. Just because the interaction may not be in person in no way makes it less dangerous.

Keep open lines of communication

This may be one of the most important strategies for you to put in place so that if something does go wrong, or someone comes on to your child inappropriately, they won't be afraid to talk with you about the situation.

It's really MY phone…. I just let you use it

That's right parents. Are you paying for the phone? Is your child on your phone plan? Let your child know it's YOUR phone and you are simply allowing them usage. It's best to set these rules in place before actually giving (loaning) them the phone in the first place, because once the phone is in their hands, it will be difficult to create new rules. Two basic rules to implement from the beginning are:

- Charge your child's phone in your room at night. Just like on the streets, nothing good happens online after 11pm.
- Make them share their passwords with you. I guarantee you will hear arguments such as, "I have a right to privacy!!!" However…..

What expectation of privacy??

Check your child's phone and browser history – OFTEN. Despite your child's pleadings, there is no expectation of privacy for a child under the age of 18. Now for adults age 18 and older, there can be limited expectation based on the person's maturity and cognitive level.

Your child didn't "accidentally" click on that porn site

You walk in and your child slams the laptop cover to hide the porn site he's watching while screaming to you that someone hacked his computer and planted links to porn sites. Here's the flaw with that statement: hackers STEAL (your identity, personal information, etc.), they don't LEAVE things. Think of this analogy: car thieves don't break into your car and leave $100. They break in and TAKE things. Along the same lines, ads for porn sites, dating sites, Victoria's Secret, etc. on the guidebar are based on clicked-on links. So someone

has used that computer to look up porn sites, lingerie sites, adult toy sites, etc. Now, all of that being said, it should be noted that depending on the age of the person, it is normal age-appropriate behavior. You may want to use this experience as a teaching moment for privacy and to make sure it is conducted in a healthy way.

Your child's skill set could be a hot commodity

Coding and hacking are sought-after skills by organized cybercriminals. For some people it's not the intent to commit online crimes, but sometimes they get caught up in the challenge of hacking just to see if they can break a code. For them it becomes a game. For others, they may be driven by a strong desire for friendship and an eagerness to please, and hacking can award them with glorification in that online community.

Implement rules to reduce the risk of online harassment

3 x 3 rule

Sometimes our loved ones don't understand

continued on page 2

their online behavior can be misinterpreted as stalking or harassment. So here's an easy-to-understand rule. After 3 attempts to contact a person in one day by text/calling/email/messaging, if the person has not responded, do not send another message. You may try again the following day but you may only do this for 3 days. Then you may not attempt to contact the person again. However, this rule is null and void immediately if the other person has stated they do not want to be contacted. At that point if your child attempts to make contact he can be charged with harassment. This law can apply to all ages.

How Harassment Law works

Depending on your jurisdiction, harassment could be a crime. If Person A believes she is being harassed online, she must first tell Person B to stop calling/texting/emailing/messaging. If Person B continues to pursue contact, Person A may file a charge of harassment. This law also applies to third-party contact. In other words, if Person B is told not to contact Person A, then Person C cannot contact Person A on Person B's behalf. If your loved one is the person being harassed, make sure she saves proof that she told the person not to contact her.

General online safety guide

To friend or not to friend

It can be difficult for anyone, but maybe especially individuals with autism, to understand the many nuances that go into a decision for who it is safe to friend online. So an easy rule is if your child has never physically met a person (walked up to the person and shaken their hand), they may not friend that person on social media.

Think twice or a hundred times before agreeing to meet an online friend in person

You don't want your children to grow up believing that only bad people are online. But you also don't want them lured into a tragic situation by ill-intentioned individuals. Use your discretion to set rules – whether it be all face-to-face interactions must be at a public location during certain hours, that research must be done to learn as much as possible about the person, etc. It is strongly encouraged that all initial interactions should be in the presence of a third-party.

Keep personal information personal

It's no secret that individuals with autism can be eager to please and possess a strong desire for friendship. That's a combination thieves will prey on. You may find you need to print a list that stays next to the computer of the items/topics your child may not share on social media such as phone number, home address, banking or credit card information, etc. Do not give any information that could identify you such as your school, sports team, church, sibling names, place of employment, etc.

Check privacy settings for apps and each browser and social media

Make sure your child isn't inadvertently sharing information only meant for actual friends.

Stop, think – don't just click

Warn your loved one that scammers and hackers are always looking for ways to lure people with links that look like tempting ads, apps, and games. Emphasize to never click on an unsolicited link.

Only make purchases from secure sites

Depending on the age of your child, you may have a no purchase rule. However, at some point they may make purchases themselves and will need to understand that if the link doesn't begin with https: it's not secure.

Choose strong passwords

It's understandable your child wants something easy to remember. Help them understand that passwords that are obvious are also easy for hackers to figure out.

**This article is not meant to serve in place of legal advice.*

Additional Resources

Internet Safety resources
http://pathfindersforautism.org/resources/safety/internet-safety/

Written by Shelly McLaughlin, Director of Safety Programs, Pathfinders for Autism. A special thank you for their contributions to this article: Detective Joseph Dugan and Deputy First Class Janelle Myers, Harford County Sheriff's Office