PARENT'S GUIDE TO RAISING SAVVY CYBER KIDS

VOLUME 1

SAVVYCYBERKIDS.ORG

Th3 S@vvy S!x

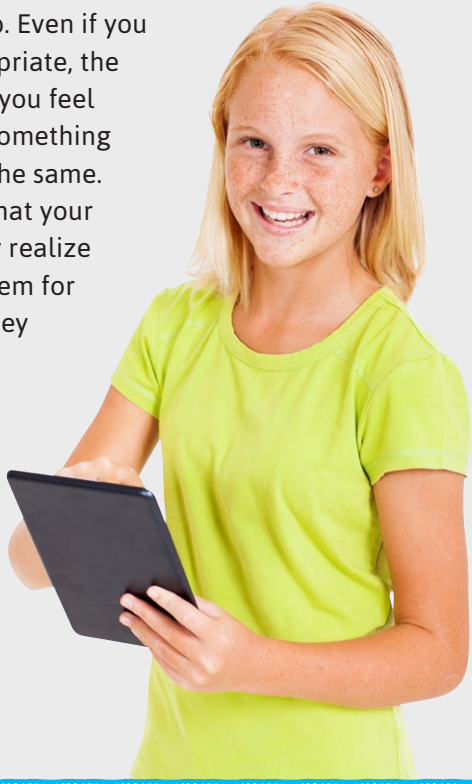
Talking to your child about cyber safety begins with adopting Th3 S@vvy S!x—the things every parent can do to help ensure that their kids are successful with technology. By following these important principles your children can be both empowered by technology as well as understand the implications of technology in their future.

#1 BE INVOLVED.

In order for your children to be successful with technology, you need to be involved in their interactions with it. Do you know your child's favorite game, app, or social media community (and it changes often!)? If not, ask them! Children love talking about what they do with technology.

Now that you know their favorite app, game, or social media community, ask your child who they interact with in those digital spaces. Just as you know your children's friends from the neighborhood or know the parents of the schoolmate that your child goes home with, you should know who your children's friends are online. We will talk about cyber strangers in an upcoming section.

Not everything online is appropriate for children to be exposed to. Even if you use a technology solution to filter content that may be age appropriate, the tools may not always work. In addition, just because you do what you feel is right to protect your children from seeing, reading, or hearing something inappropriate, it does not mean that all their friends' parents do the same. Therefore, you should keep the lines of communication open so that your child will approach you if something upsets them online or if they realize that they made a mistake. If you yell at your children or punish them for bringing something to your attention, that may be the last time they confide in you.



Your children witness your actions, because they admire and look up to you as their daily role model. If you text at meals, they will grow up and text at meals. If you spend all your free time on social media, they will most likely do the same once they get an account. So model the behavior you would like from them. If you don't want your children texting at dinner or spending all of their time updating and posting on social media, you need to be sure they don't observe those behaviors in you.

#2 STOP. THINK. CONNECT.™

As our children mature in a digital world, they will have to make their own decisions about appropriate behavior. Every action they take will follow a decision they make. You need to give your children the critical thinking skills to pause, or stop for a moment—when they are about to update social media or take any action online—then have them think about what they are about to do, before potentially posting or forwarding something mean or suggestive—and answer questions like:

If I forward this picture, will something bad happen to me?
What will people think of me?
What will people think of the other person?
Is this the right thing to do?

Start the dialogue about making these kinds of decisions by asking your child if they have ever seen anything online or in a game that made them feel uncomfortable or strange. Or if anyone has said anything strange to them in an app or game? Ask them if anything online has made them feel funny, hurt their feelings or confused them. Let your children know you are always available to help them understand what they are experiencing.

As a family, discuss the idea of privacy. From the youngest ages, children must understand that they should never share their real name and their physical or email address and phone number. But more than that, our young people need to understand that they shouldn't be sharing the name of the school that they go to—even by wearing a school shirt in a profile picture, where they take after-school activities, family routines or whether Mom and Dad are home or away with anyone that isn't a friend in real life.

A relaxed intimacy can sprout from our online connections. How much contact your children will have with others in the digital realm, in part, will be defined by your family technology rules. But the reality is that once they are exploring the virtual world and certainly as they adopt the social media connections found within most of the apps favored by tweens and teens, your children need to have a very sophisticated understanding of the types of private and public information that can or should be shared and with whom online.

Our Digital Natives—kids and teens of this current generation—have a different opinion about what should be private and what is private. Is a text private? A group chat? Our kids trust their friends but do they know how to tell if a friend is trustworthy and do they understand the ways that a text or a group chat can betray their privacy. Debunk the myth of privacy in the virtual world. It 100% doesn't exist and your kids need to know that.

#3 STRANGERS ARE FOREVER.

To your children, anyone that reaches out to them via an app, game, or social media community seems like a good person just wanting to chat. Kids are trusting, too trusting. Anyone that your child meets online is a stranger, forever.

You can't definitively know who this person is, if they are misrepresenting themselves or if they are safe to engage with. Just as you would not want your child to engage with a stranger in the physical world, you should not allow your children to engage with strangers online.

Children today oftentimes don't distinguish easily between the physical world and the virtual world. They are both real worlds to them. The very concept of a "friend" has been hijacked as any stranger that reaches out to chat and been given new meaning. Until now, because you are involved.

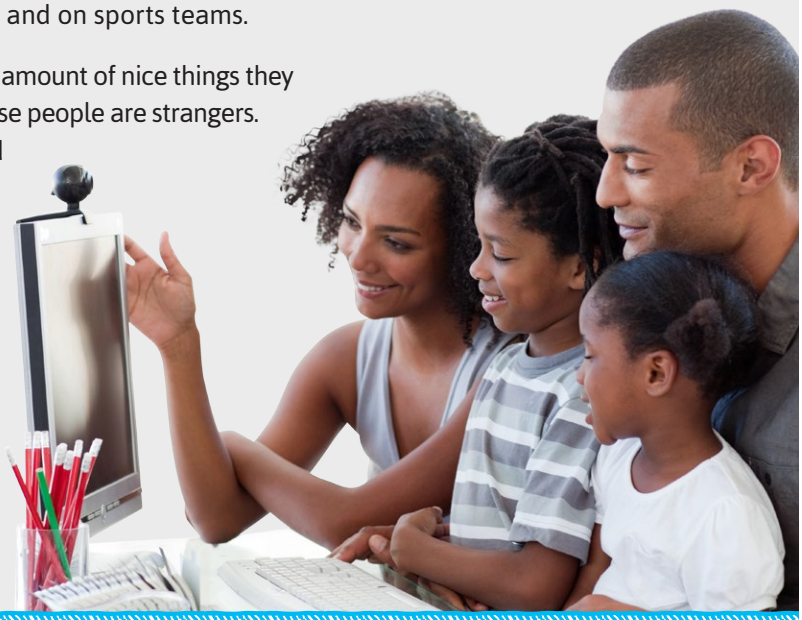
The ways our young people make social connections are different than in generations before. Your children have access to friends of friends—many of whom they may not have met in-person. Your child may explain to you that their friend wants them to become online friends with others because of shared interests. The danger is that your child may not know—and you will not know—if this new "friend" is an IRL (in real life) friend of your child's friend—and if this person is even who they say they are!

Each family needs to define their own rules for "friend-making". Perhaps your family will determine that meeting people in-person before becoming an online friend will be a rule. Yet, as your children gets older, it may not be helpful to simply say 'if you don't know someone in real life you may not connect with them online.' At that point it may be more useful to distinguish the variance in ways that your children can connect with others. But the very act of having this conversation, and continuing to have this conversation as your child gets older, will ensure that you understand your child's online interactions and that your child hears your concerns and is aware of the pitfalls of behaving recklessly in the virtual world.

Ask your children if they have ever received a message from someone in a game or app that they don't know in the physical world. Explain to your kids that the physical world includes your home, friends they play with in your neighborhood, at school and on sports teams.

Teach your child to see strangers as strangers. No amount of nice things they say or gifts they send can change the fact that these people are strangers. Talk to your kids about the concept of privacy and remind them that they should not share personal information—like real names, addresses or phone numbers, if their parents are home, family schedules or what school they attend.

And make sure your kids understand that they should NEVER meet someone they met online, through an app, game, or social media community in the physical world. NOT EVER.



#4 UPDATE EVERYTHING.

It is important for you and your children to update all devices and software on a regular basis and when notified by the manufacturer or creator. Anytime an update (often called a patch) is available, a fix was made to a known problem with that device or software. Perhaps there is a way for someone to remove all the information off of a computer or device. Or maybe there is a way for someone to remotely turn on the video camera on your device and take inappropriate videos.

In addition to keeping up with the latest patches, install (and keep updated) an anti-virus product. Anti-virus products can protect you from certain attacks. And yes, even Mac computers should have anti-virus software too.

#5 UNDERSTAND TECHNOLOGY.

Make no mistake, if your children can access the internet, strangers with malicious intent can access your children. This means that you need to understand how your children are accessing the internet—whether on a handheld device, on a handheld game, on an iPhone, on an Android phone, a tablet, a computer, a gaming console, a video media player, or other connected device. Whatever the mode of access, you need to understand how these technologies provide direct access for strangers—even pedophiles—to your child.

It may not be the most exciting literature, but you should read the privacy policy for each device, app, game, or social media community that your child is using. Reading the policy will let you know exactly what information about your children is being collected by the company providing the service AND what they can do with that information.

Next, look for the available parental controls for each. Some apps, games, and social platforms offer options that can limit who your child can talk to, as well as who can contact your child. If there is an option to create private profiles, consider doing so and talk to your child about not allowing people they do not know in the physical world to connect with them.

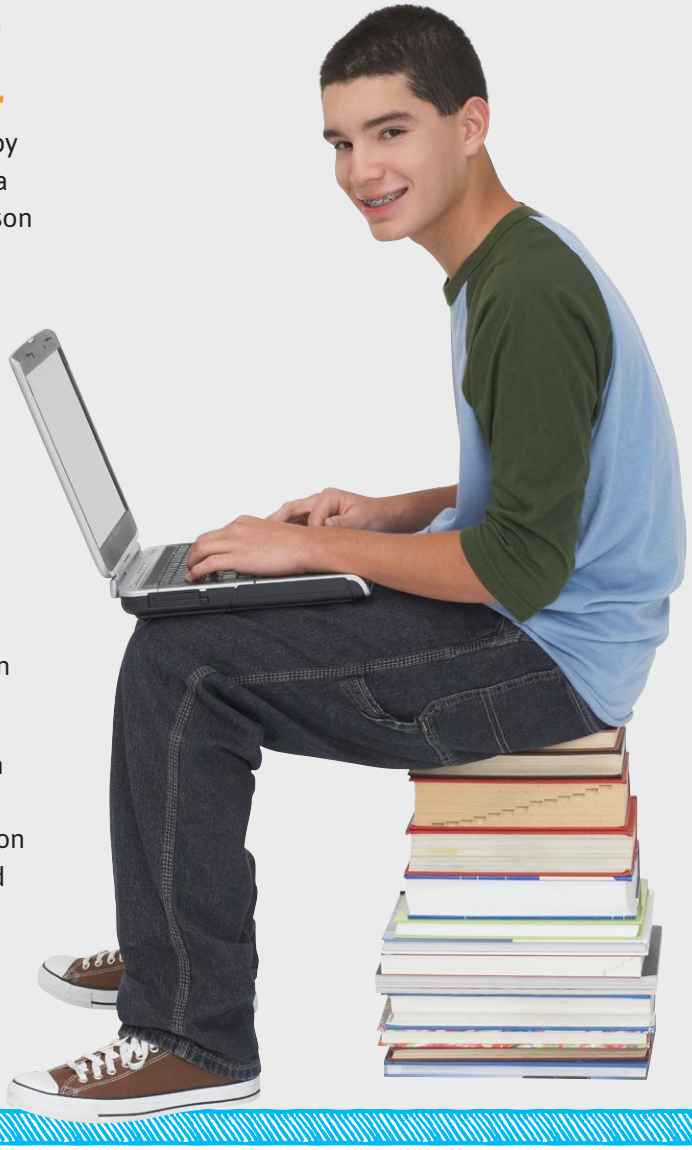
#6 SET SECURITY FREEZES.

The disadvantage of being part of an online community is that all of our personal information is online too (yours and your kids!). If you have ever received a letter from a merchant alerting you to your private information being stolen, you likely were offered free monitoring service for a year or two—as a method to protect you from identity theft. The reality is that monitoring is not enough. Someone can still open an account in your name and ruin your credit history. You would be alerted after the fact and the credit monitoring firm may help you clean up the mess. There is another option, and it is free (or inexpensive, depending on where you live). Contact each of the three credit reporting agencies (TransUnion, Equifax, and Experian) and place a security freeze on your credit file. With a security freeze on your credit file, no one can open a new account (take out a mortgage, a car loan, or other financial commitment on your behalf) unless they have your secret pin.

BONUS #7 ENABLE 2-STEP VERIFICATION.

Every account you and your children use is secured by a user ID, such as a nickname or email address, and a password. This is done to prove that you are the person that is supposed to be accessing the account you are attempting to log in to. Due to the number of security breaches we hear about in the media (and the volume of breach notification letters many of us receive), we all need to take an additional step to secure our accounts. A complex password in today's environment is no longer enough; it is time to enable 2-step verification. 2-step verification typically involves a text message being sent to your phone, a one-time code sent to your email, a call to your phone and/or use of a verification app (sometimes called an authenticator app).

Another aspect of verifying who you are to access an account is the use of security questions. You should teach your children to NOT use any public information as answers. In addition, you and your children should not use answers that can be figured out by someone reviewing your social media accounts, such as a pet name, favorite food, etc.



ABOUT
SAVVY CYBER KIDS

Savvy Cyber Kids (SCK), a 501(c)(3) nonprofit organization whose mission is to enable youth, families, and school communities to be empowered by technology, recognizes that children may be Digital Natives but are also "Digital Naïves", who, without intervention, completely lack understanding of the implications of their digital actions. Founded in 2007 by Internet security expert, noted speaker and author Ben Halpert, Savvy Cyber Kids provides resources for parents and teachers to educate children as they grow up in a world surrounded by technology by teaching numerous cyber ethics concepts such as personal Internet safety, bully response, technology balance, digital reputation, privacy, and more. Savvy Cyber Kids is grateful for the ongoing support of its presenting sponsors, Digital Guardian and Ionic Security and for the support of its education series partner, Earthlink.

SAVVY CYBER KIDS

4780 Ashford Dunwoody Rd
Suite A-312
Atlanta, GA 30338

SavvyCyberKids.org