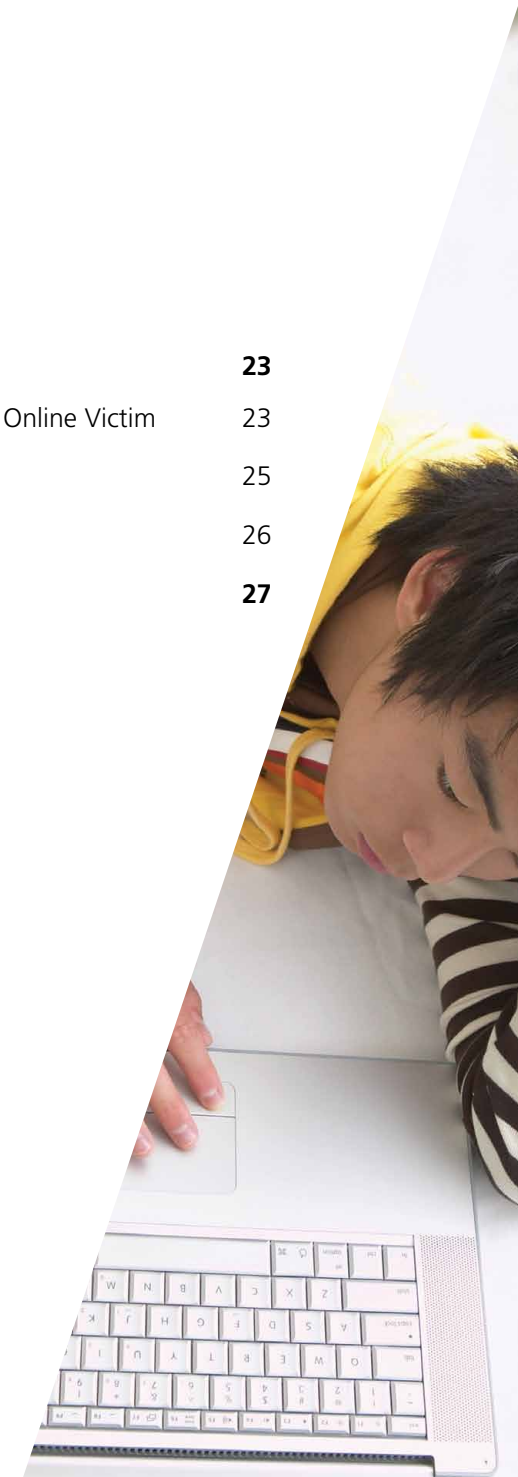
McAfee®

A Parent's Guide to Social Networking Sites

Five Lessons to Keep Your Kids Safe When They Socialize Online

Table of Contents



Introduction

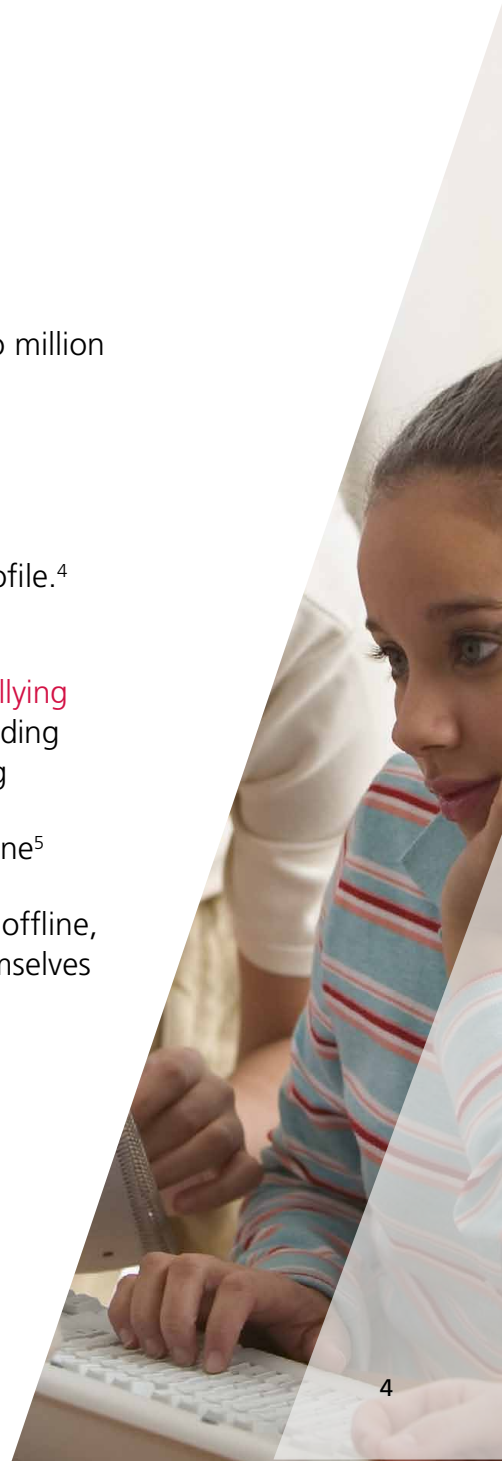
Your children may spend a lot of time on social networking or virtual world sites like MySpace, Facebook, and Club Penguin. These popular sites are a great way for them to interact with friends using computers and mobile devices and have changed the way your children communicate with their friends and family.

Too often though, kids include too much personal information, discuss inappropriate behaviors that could get them into trouble, or otherwise place themselves at risk by what they share online.

The purpose of this e-guide is to provide concerned parents like you with the knowledge to deal with challenges associated with social networking and community websites. Once you understand the basics, you'll be better able to help your kids stay safe when they socialize online.

Facts About Social Networking

- In 2008, nearly 15 million teens in the U.S. were "social network users," and nearly two million children (three to 11 years old) also used social networking websites[1]
- Among teens 12 to 17 years old, 65% have a profile on an online social network[2]
- Facebook is the largest social network, with more than 200 million active members.[3] It's also the most popular among teens. 84% of teens polled said they have a Facebook profile.[4] MySpace has more than 185 million registered users.[4]
- A recent McAfee-sponsored survey[5] revealed that 20% of teens have engaged in cyberbullying behaviors—including posting mean or hurtful information or embarrassing pictures, spreading rumors, publicizing private communications, sending anonymous emails, or cyberpranking
- 28% of teens say they would not know what to do if they were harassed or bullied online[5]
- 52% of teens have given out personal information online to someone they don't know offline, and one in four (25%) have shared personal photos and/or physical descriptions of themselves (twice as many girls as boys)[5]



1 eMarketer, Inc., February, 2009
2 Pew Internet & American Life, "Adults & Social Networking Sites," January 2009
3 Facebook Press Page http://www.facebook.com/press/info.php?statistics
4 Scott Elkin blog, http://scottelkin.com/programming/aspnet-20/myspace-statistics/
5 McAfee & Harris Research Institute, "Mom and Teen Survey," October 2008

Five Lessons for Parents with Social Networking Tweens and Teens

By studying the five lessons in this e-guide, you'll gain an understanding of social networking websites. The more you know, the better you'll be able to educate your children and the safer they'll be.

Lesson 1
What Is Social Networking?

Social networks are websites that provide a virtual community for people interested in a particular subject or to "hang out" together.

These sites are like virtual club houses. Once you become a member and create a profile, you can interact and connect with family and friends via online activities like chat, email, photos, events and status updates.

Examples of social networking sites:

Facebook
MySpace
myYearbook

For younger kids, there are sites that provide stronger parental controls, like:

Club Penguin
Webkinz

Why Are Social Networking Sites So Cool?

Social networking sites are popular because they allow your kids to:

- Communicate with friends and family
- Meet new people
- Reconnect with old buddies
- Share messages, videos, and photos
- Plan their social life
- Participate in a group or cause that interests them
- Play online games with other members

FACT: According to a recent Reuters article, a Nielsen survey revealed that, worldwide, online networking is more popular than email. Learn more.

Exercise
Get Involved

- **Talk to your children about what they do on the Internet**
  WiredSafety.org research shows that teens who discuss social networking websites with their parents behave safer online.
- **Get your own Facebook profile or MySpace page**
  Why not ask your children to help you set up your profile? You never know, they may even ask you to be a "friend" in their network.
- **Be informed**
  Keep yourself up to date on the benefits and challenges of social networking by visiting educational sites like the McAfee Security Advice Center.

Lesson 2
Why Social Networking Can Be Risky

Perhaps the biggest problem with social networking can be summed up with the acronym "TMI" or "too much information."

Your kids need to understand that if they reveal too much about their personal lives, it could lead to problems—like susceptibility to cyberbullies, online predators, invasion of privacy, and identity theft.

These problems are not due to social networking, as they have been around since the advent of email and chat. But with social networking, the volume of content has grown and become much more personal and is easily seen by anyone.

It's not just kids who are at risk. Even adults have been embarrassed by putting too much information on their profile pages for all the world to see.

Example of TMI on social networking websites:

A student was rejected admission at a college after gushing about the school while visiting the campus, then trashing it online.[6]

6 Wall Street Journal, http://online.wsj.com/article/SB122170459104151023.html?mod=googlenews_wsj

Exercise
Talk to Your Kids and Set Limits

Kids have a tendency to want to share information with their friends and connections. A profile on a social networking website is like a window into their lives. They need to understand that they need to protect their privacy and their reputation diligently.

Set some limits and make a few rules for your children with regard to their online behavior, especially on social networking sites.

- Limit the amount of time your kids are allowed to spend on the Internet
- Discuss what is and is not appropriate to share online and remind your child that nothing is secret in cyberspace
- Advise your children to beware of people they don't know who want to join their network—these "friends" may be predators or cyberbullies who want to do them harm

- Teach them the risks and dangers of sharing passwords, phone numbers, addresses, and social security numbers and other personal information—even with their best friends
- Encourage them not to use their full name, city, school, and age in text or images, so this information can not be used to locate them offline
- Have them inform you if they notice anything odd or unusual, such as messages from "friends" that seem out of character or photos that your children never posted
- Teach your children to be wary of messages—especially solicitations or offers with links to websites—that they receive from others in their network, as the messages may be coming from a con artist who has commandeered a friend's profile and is distributing a phishing scam
- Tell your kids that they cannot meet face to face with individuals they've met online
- Tell your kids to trust their gut if they have suspicions—if they ever feel uncomfortable or threatened, encourage them to tell you

Lesson 3
Cyberbullying

Online bullying is an issue your kids face on social networking sites.* Because these sites are all about sharing personal information, and it's easy for the information to be spread, it's easy for your kids to become a victim.

Cyberbullying is defined as the use of the Internet or other technologies to send or post text or images intended to hurt or embarrass another person.

Types of cyberbullying:

- **Flaming:** Online fights sent via email or instant message with angry or vulgar language
- **Harassment:** Repeatedly sending nasty, mean, insulting messages
- **Denigration:** "Dissing" someone online by sending or posting gossip or rumors about a person to damage his or her reputation or friendships

* Cyberbullying can also happen outside of social networking sites using the same or similar technologies such as email and instant messages.

- **Impersonation:** Pretending to be someone else and sending or posting material to damage their reputation
- **Pranking:** Tricking someone into revealing secrets or embarrassing information and then sharing it online

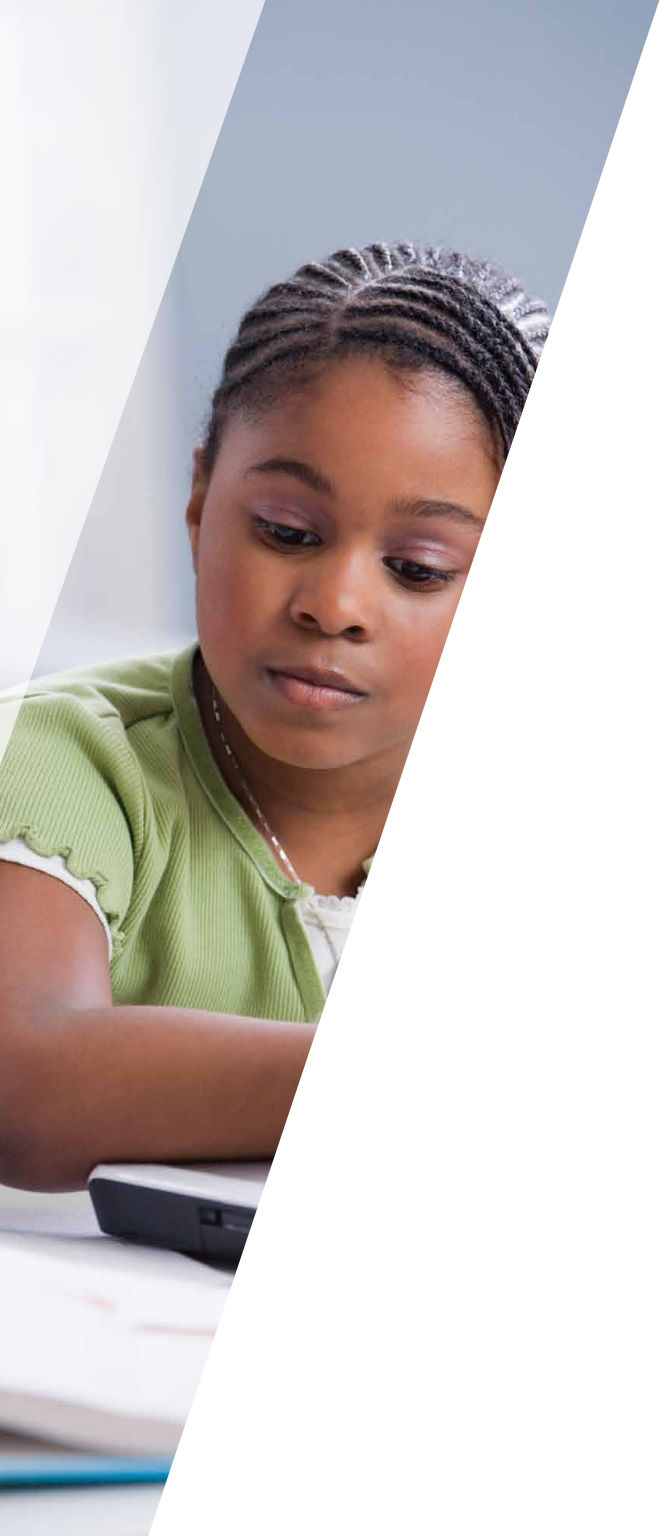
FACT: 43% of teens (4 of 10) report that they have experienced some form of cyberbullying in the last year.[7]

Effects of cyberbullying:

Victims of cyberbullying may experience many of the same effects as those who are bullied in person, such as withdrawal, a drop in grades, lowered self-esteem, a change in interests, or depression. However cyberbullying can seem more extreme to your children because:

- It can happen at home—It can take away the place children feel most safe
- It can be harsher—Kids often say things online that they would not say in person

7 Harris Interactive, "Trends and Tudes," April 2007



- It has more reach—Emails making fun of someone can easily be sent to an entire class or school, or information can be posted on a website for the whole world to see
- It can be anonymous

Example of Cyberbullying:

A tragic case of cyberbullying was orchestrated by a parent—the mother of a 13-year-old girl who set up a MySpace page and pretended to be a 16-year-old "boy." The woman friended a 13-year-old neighbor, who had been chummy with her daughter. After receiving messages from the "boy," who initially was nice, but later became abusive, the neighbor committed suicide. The mother was convicted of misdemeanors by a U.S. federal court.[8]

8 Wired, "Dead Teen's Mother: Misdemeanor Convictions a 'Stepping Stone' in Cyberbullying Case"

Exercise
Check for Warning Signs and Talk to Your Kids

Warning signs[9] that indicate your child might be a victim of cyberbullying:

- Being ill at ease when receiving an email, IM, or text message
- Feeling upset after using the computer
- Refusing to leave the house or go to school
- Withdrawing from friends and family

9 Sameer Hinduja, Ph.D. and Justin W. Patchin, Ph.D.

Warning signs[9] that indicate your child might be a cyberbully:

- Switching screens or closing programs when you walk by
- Using the computer late at night
- Getting upset if he/she cannot use the computer
- Using multiple online accounts or an account that belongs to someone else

If you detect any of these signs, talk to your kids about the issues around cyberbullying as both a victim and a perpetrator. Encourage them to not condone or support others who are cyberbullying. Ask them questions based on the "warning signs" and then sit back and listen.

9 Sameer Hinduja, Ph.D. and Justin W. Patchin, Ph.D.

Lesson 4
Online Predators

It's commonly believed that the Internet is the perfect environment for online predators because it is easy for them to hide their identity, get access to potential victims, and there's a huge pool of kids to target.

An online predator is a criminal who generally targets teens with the goal of manipulating them into meeting for sex. Online predators typically "groom" their victims by building trust with the child through lying, the use of blackmail and guilt, creating different personas, and then attempting to engage the child in more intimate forms of communication, and eventual in-person meetings.

On social networking sites, online predators can use all these techniques to become friends with your children and try to engage with them. Online predators will also use information from your child's profile to try and locate them in person. This is why it is critical for you and your kids to talk about appropriate online behavior and what type of information is okay to post online.

Exercise

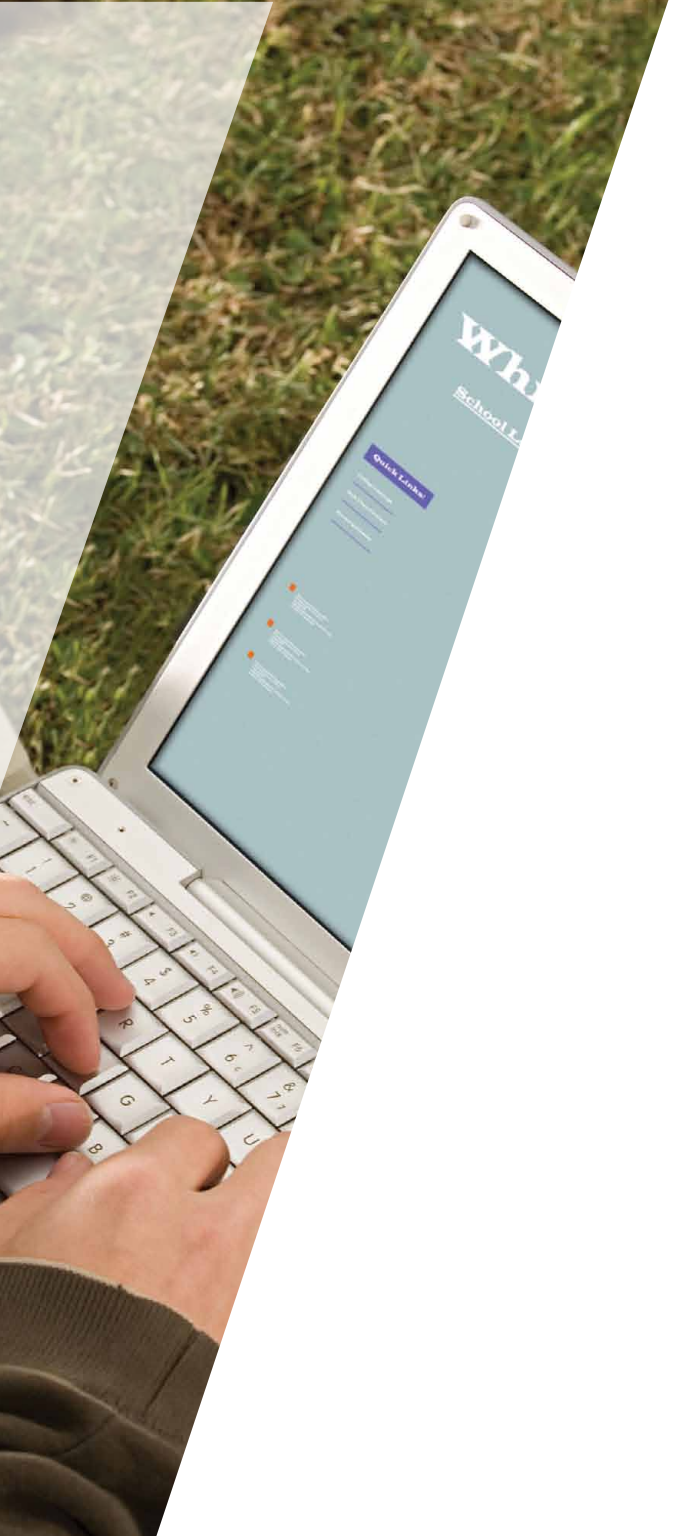
Encourage Kids to Report Inappropriate Behavior

Encourage your kids to come to you for help when they are being cyberbullied or have encountered online predators.

Or if they are uncomfortable speaking with you, tell them to speak with a trusted adult—an aunt, uncle, teacher, or older sibling—to lend an ear.

Be sure your teen knows how to report abuse or inappropriate behavior to social networking sites. With Facebook, for example, they can send an email to abuse@facebook.com.

SUGGESTION: See the resources section at the end of this e-guide for step-by-step information on what to do if your child becomes an online victim.



Lesson 5
Invasion of Privacy, Malicious Impersonation, and Identity Theft

If your children aren't careful on social networking sites, they could become victims of invasion of privacy, malicious impersonation, or identity theft.

Invasion of privacy can happen easily if your children share their passwords, are not selective about who they add as a friend, or are not careful about what information or photos they post online. The level of visibility to friend lists, profiles, or photos varies from site to site, so it is wise to be aware of the privacy options on the sites your children use. The key to preventing invasion of privacy is to make sure your children are careful about what they share, who they share it with, and that they understand that nothing is private when it is posted online, no matter how many controls are in place.

Malicious impersonation occurs when someone pretends to be your child and does malicious things, like posting profanity or inappropriate images. The easiest way for someone to impersonate your child is to get your child's password. Once someone has the password, they can post inappropriate material that looks like it is coming from your child.

Malicious impersonation can also occur when someone pretends to be someone other than who they really are and interacts with your child online. The case of the cyberbullying mother described in Lesson 3 illustrates how malicious impersonation of this type can have unfortunate consequences. Also, online predators often "friend" teens online and misrepresent themselves as peers to lure their victims into a sexual encounter.

Identity theft and phishing scams are becoming more and more commonplace on social networking sites where so much personal information is available to hackers. Phishing scams are attempts to trick you into giving up personal information, including passwords, social security numbers, and credit cards numbers, through phony requests or solicitations that appear to come from legitimate sources. Identity thieves who have gotten their hands on members' passwords not only gain access to their profiles, but also to their network of friends. It's an easy way for identity thieves to use victims' accounts to send phishing messages to large numbers of people in hopes that some of them fall for their scams and turn over confidential information.

Exercise
Commonsense Practices

There's plenty you can do to guard your family against invasion of privacy, malicious impersonation, and identity theft. By teaching your children some commonsense practices, you'll gain peace of mind, and they will have a safer, more enjoyable time socializing online.

Educate your kids

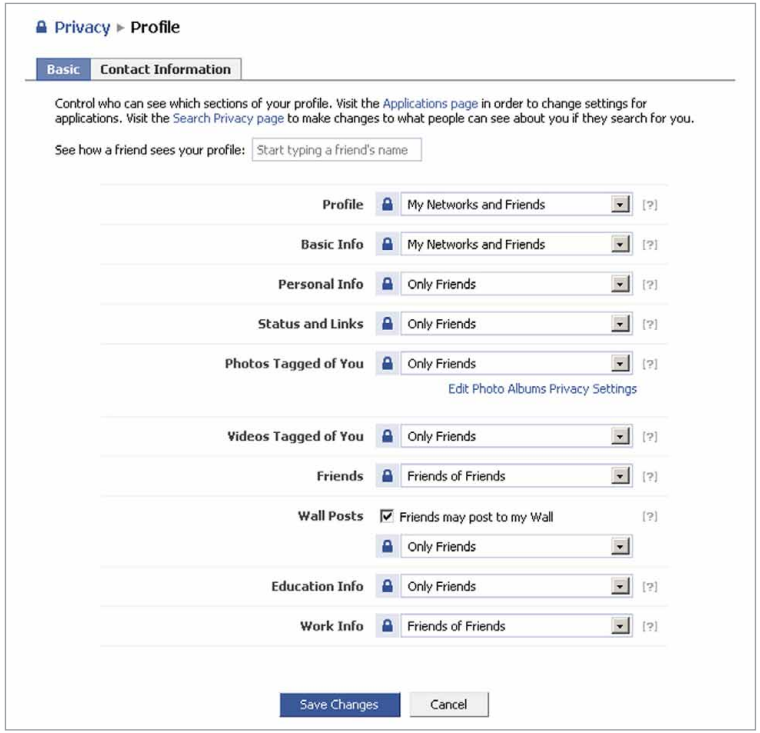
- Refer to the exercise in Lesson 2: "Talk to Your Kids and Set Limits"

Be proactive

- Check to see whether people are impersonating your children. Search your children's names online along with variations and nicknames. It's a good practice to do this often.
- Review your children's friends list—You may want to consider letting them only be friends with people they know offline
- Create your own profile and share the social networking experience with your kids

Use technology

- Use the privacy and safety setting options on social networking sites, such as private profiles, blocking and pre-approving comments to control who your children communicate with
- Have up-to-date computer security software to protect your computer from malware, viruses, spyware, and other threats
- Consider using software that lets you monitor your children's online activities and helps protect them



Facebook's Privacy Settings lets you control who can access your profile and postings

Resources

What to Do if Your Child Becomes an Online Victim

If your child becomes a victim of a cyberstalker or an online predator, here are some steps to follow:

1. Take immediate action

- Ignore contact from the bully or online predator or do not log on to the site where it occurred
- Block the offender's screen name and email address to prevent them from contacting your child
- Change your child's online information or, if necessary, delete the account
- Contact the site where this occurred to have your child's information removed, and report the perpetrator
- Report this to your Internet service provider (ISP) and the offender's ISP

2. Report the incident to the authorities

3. Save the evidence

- Keep a log of all communications from the perpetrator
- Keep track of the offender's screen name, email address, and ISP, if available

4. Learn as much as you can about your children's use of the Internet

- Find out which services they use and what they like to do online
- Find out about the security features on their favorite websites
- Talk to your children about protecting themselves and being safe online

Resources
Additional Safety Tips

Social networking sites are a great way for kids to connect with each other, make new friends, and expand their world in a positive way. Most of these popular websites care about the safety of your children and offer stringent privacy policies and valuable tips for parents who want to make sure their kids' online experience is enjoyable and free of problems.

Facebook

- "Working Together to Keep You Secure" by Jeff Williams
- Reporting abuse
- Privacy

MySpace

- Safety and security
- Reporting abuse
- Privacy settings

myYearbook

- Reporting abuse
- Privacy settings

Club Penguin

- Club Penguin's safety measures

Webkinz

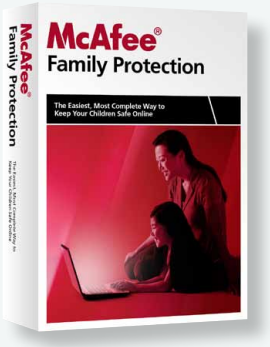
- Parent's area
- General privacy policy

Resources

Security Software Checklist

Another way to safeguard your family against threats that may arise from social networking sites is to install appropriate security software. Here's a checklist of features to look for:

- **Web blocking** prevents your children from viewing inappropriate content
- **Program blocking** blocks games, peer-to-peer file sharing, or any other program you specify
- **Social networking features** record postings of inappropriate or personal information and conversations to help determine if cyberbullying activity is taking place
- **Email blocking** blocks unknown email addresses, so children are not communicating with people they have met online but don't know personally
- **Time limits** help you manage the amount of time your children spend online
- **Instant Message features** monitor and record instant messaging (IM) chats to help you find out if your children are engaging in inappropriate dialog with friends or people they've met online
- **Usage reports** provide you with a complete view of all Internet and IM activity, which you can use as conversation starters to educate your children
- **Instant email or text alerts** notify you when your children attempt to access objectionable material
- **YouTube filtering** enables you to block objectionable videos while allowing your children to enjoy other videos



McAfee® Family Protection software offers all of these features and empowers you to say "yes" to your kids so they can make the most of their digital lives. Learn more.

More Advice on PC and Internet Security

For more information and advice about PC and Internet security, please visit the McAfee Security Advice Center at www.mcafee.com/advice.

About McAfee

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee is committed to relentlessly tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security.

http://www.mcafee.com

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054
1.888.847.8766 www.mcafee.com

5806gde_consumer-social-networking-eguide_0409