



Privacy, Security & Virus Information

Continue Chatting the Day Away

Teens and children love to use chatrooms. They are great online locations where kids from places across the globe can meet other kids from around the world. However, it is important to note that chatrooms can also be dangerous places for those who are not protected.

It is important that your children are made aware that people in chatrooms are strangers, and that their true identities may not be revealed online. Children can become victims of bullying and become victims of hate speech within these chatrooms. Children are innocent, and as a result, can reveal private information about family and friends that could lead to fraud and other crimes unintentionally.

What are the Risks?

It can be hazardous for kids to use the Internet unsupervised, considering the anonymity that the internet creates. A lonely child, looking for friendship, can be easily seduced by a dangerous stranger who is willing to listen to their troubles with a sympathetic ear. By pretending to be another child who shares the same interests, a stranger can easily bring a child into conversation. There is no question that this stranger could easily be a paedophile, interested in luring the child into a meeting that can lead to a sexual assault.

There could be potentially devastating results, if a child shares even small, seemingly harmless bits of personal information. It is very simple for a predator to locate the child, for example, base simple on his/her name, gender, and school sports team. The results could be tremendously damaging.

Online games allow voice as well as text chatting, in-between game sessions. As a result, kids should use extra caution when using these online chatting abilities. Children should also be made aware of those online gaming 'friends' who are overly eager and who pressure them for their contact information, their phone number, or for a face-to-face meeting.

Children can protect their privacy and their family's security by cutting off chats with people who are online, asking and bothering the child for personal information. For those fishing for information, it is especially important that the child immediately stops communication. There are responsible safeguards that you can implement to help ensure that your children will have safe, educational, and fun online experiences.

How To Keep Your Children Safe in Cyberspace: 10 Easy Steps

These tips will help you and your children make the right choices while online:

1. Ensure that the position of the computer is in your main, open living area in your home. Make sure that the monitor faces outward into the room, to prevent secrecy. If your child changes the screen when you pass by, suspect that they are doing something that may put them in danger. If your child is using hard disks containing files, check with the child to see what they are downloading.

McAfee Security



2. Work together as a family to establish rules and guidelines. Discuss with your child which websites and downloads are appropriate, and which downloads are inappropriate. Also, discuss which chatrooms to visit and what kinds of things they are allowed to discuss in those chatrooms. Only let your child use chatrooms where the conversations are monitored. Explain to your children that “.alt” chatrooms – chatrooms which focus on alternative topics that may be inappropriate to children – that these chatrooms are off-limits. Take the time to get to know your child’s online friends. Become familiar with surfing the web and chatting online, as you can therefore grasp the difficulties and problems associated with online experiences. By doing this, you will be able to understand what your child is doing online.

3. It is important to explain to your child that you will not punish them or prevent them from using the Internet, if they receive an odd or threatening e-mails or messages while online. Explain to your child that you understand that they cannot control what other people say to them. Stress to your child that they are not to blame if this happens.

4. Be sure to set time limits for Internet use – and remember to enforce them. There is software readily available that can easily enforce these limits. Ban use of the Internet at late-night. A child is most vulnerable when they have been online for a long period of time – do not permit them to be alone in cyberspace for extended periods.

5. Always make it clear to your child that the people involved in chatrooms are considered strangers. Explain that no matter how often they chat with them or how well they think they know them, online chatrooms are still full of strangers and should be treated that way. Children should understand that people can lie about who they are - and that their new friend could be a 40-year-old man instead of a 13-year-old friend.

6. Ensure that your child understands that they should never reveal personal information. Personal information may include the child’s real name, gender, age, school, phone number, or where they live. Make sure your child uses a pseudonym that is non-provocative and doesn’t reveal their true identity. It is also important that the child guard’s other people’s personal information, including their friend’s names and telephone numbers.

7. Never let your child open an attachment of file from their e-mail address if you don’t have a proper scanner for content on your computer. Explain to them that attachments can contain viruses. Predators can send pornography or other questionable material that could be revealed in the file.

8. Install security software on your computer that is up-to-date. The McAfee Internet Security Suite offers trusted 8-in-1 protection from identity thieves, spammers, and predators, ensuring a worry-free experience for you and your kids. The McAfee Internet Security Suite filters offensive content and pictures that a predator may send, and blocks inappropriate Web sites. The privacy features on this software also protect your personal information by restricting sending personal documents without your knowledge.

McAfee Security



9. Explain to your child that it is extremely important that they do not meet friends from online places without your knowledge. Always determine the person's identity before allowing any meeting to take place. If you do go ahead with the meeting, make sure the location is a public place and always accompany your child.

10. Teach yourself how to block users, save chat session logs, and how to report problems. You can save sessions by copying and pasting the message text into a word processing program. Many chatrooms allow you to block the user from communication by right-clicking on their name and choosing the "block" or "delete" feature on most messaging or chat programs. If there is a problem with a chatroom person, report them to the system administration or discussion moderator. You can find this information in the help sections of the chatroom program.