

The Internet is part of children's everyday world. They spend many hours surfing it, both in school and at home. That's why parents and children alike must be aware of the risks and know how to mitigate them.

According to data from Save the Children, more than 13 million children in Europe have frequent access to the Net: four million are under 12 years old and nine million are between 12 and 17.



Kids ON THE WEB

MAIN SOURCES OF RISK

Instant messaging has become one of young people's main means of communication and cyber-crooks' weapon of choice to carry out attacks.



INSTANT MESSAGING

1. One of the main dangers is **IDENTITY SPOOFING**: the impersonation of someone else to contact children. This tactic is sometimes used by sex predators. Education is without doubt the best way to protect young people from this particular threat. Advice such as 'don't talk to strangers', is just as sound online as it is in the non-digital world, and children should have sufficient confidence to be able to talk openly to parents or tutors if they have any doubts.



2. **VIRUS OR MALICIOUS CODE ENTRY**. Follow this simple advice: Don't run any file or click any link received though the Internet. At least not without first making sure of the sender's identity.

EMAIL

In this case there are also several threats:

1. **SPAM**. Very often, this kind of junk mail is used to advertise anything from online casinos to pharmaceuticals.



CHILDREN ARE FAR MORE NAIVE THAN ADULTS AND MAY BELIEVE EVERYTHING THEY READ IN EMAILS. They may start gambling or could buy medicines or even drugs.



2. **MALWARE INFECTION**. Some emails use attractive subjects to tempt users into clicking links or download files (which will trigger virus or malicious code infections): movie trailers, erotic photos, game downloads, etc. Many adults are taken in by these techniques, so it's easy to see how children might take the bait.



FILE EXCHANGE NETWORKS

File exchange through programs like emule or Kazaa is one of the most common ways of infecting computers. Many viruses and malicious code take the names of movies, programs, etc. to entice users to download and open them.

CHILDREN SHOULD KNOW WHAT FILES THEY CAN DOWNLOAD AND WHICH FILES THEY SHOULD AVOID.



CELL PHONES, A NEW MEANS OF COMMUNICATION WITH THE SAME RISKS AS THE INTERNET



SOCIAL NETWORKS AND BLOGS

Social networks to share files, know people, etc., and blogs have become one of the most popular resources among young people. A common component of these pages is the need to create a personal profile in order to access them. These profiles usually contain data like names, age, etc. Generally, it is sufficient to enter an email address and a name, which doesn't even need to be a real name, but a nickname. **THEY SHOULD NOT BE GIVING OUT DATA SUCH AS THEIR AGE, ADDRESS, AND IN PARTICULAR, PHOTOGRAPHS OF THEMSELVES.**





TIPS FOR PARENTS

- 1 • SPEAK TO YOUR CHILDREN:** You must know what pages they view, with whom they speak, what they like to see, etc. You wouldn't let them leave the house without knowing where they're going and with whom, so you shouldn't let them access the Internet without knowing what they are doing.
- 2 • LEARN YOURSELF, AND PASS THE KNOWLEDGE ON TO YOUR CHILDREN:** For many parents the Internet is still an unknown world. For this reason it is very important to be aware of the tools that the Net offers children, and to know what the risks are and how to avoid them.
- 3 • SET FIRM RULES FOR USING THE INTERNET:** You should establish clear and firm rules, with timetables, maximum online time and the way they use the Internet. Make sure they abide by the rules, especially with regard to using the Web at night. If you have just one PC for the whole family, it should be in a family room and not in your child's bedroom.
- 4 • FORBID CHILDREN FROM GIVING OUT CONFIDENTIAL:** You must instruct your children not to give out data such as their name, address or photos across the Internet. Advise them to use nicknames in forums.
- 5 • TEACH YOUR CHILDREN TO BE WARY OF APPEARANCES:** On the Web nothing is what it seems. Teach your children to be wary and not to do anything that could jeopardize their security or privacy.
- 6 • INSTALL AN EFFECTIVE SECURITY SOLUTION:** To protect your children from malicious code, the best strategy is to have an up-to-date and effective security solution like PANDA.

PANDA
SECURITY

© Panda Security 2008 0908-MR-PMNR-01

www.defendyourchild.com

KIDS ON THE WEB CHILD'S PLAY?

CAREFUL GUIDANCE
CAN KEEP THEM SAFE
ON THE INTERNET



PANDA
SECURITY | One step ahead.