



PROTECTING CHILDREN ON-LINE GUIDE

HOW TO SECURE AND DEFEND THE DIGITAL EXPERIENCE
OF YOUR KIDS

LOREDANA BOTEZATU, RAZVAN LIVINTZ
E-THREATS ANALYSIS AND COMMUNICATION SPECIALISTS

FAMILY, PARENTS AND TEACHERS



Table of Contents

Table of Contents2

Children and the World Wide Web3

Risks and dangers directly targeting kids.....4

 On-line addiction 4

 Cyber-bullying 4

 Exposure to inappropriate content..... 5

 Encouragement of unethical conduct 5

 Illegal actions 5

E-threats targeting systems and data.....6

 Malware..... 6

 Phishing and ID Theft..... 6

 Spam..... 7

Safety tips while on the World Wide Web7

Tips for children and teens8

Tips for parents8

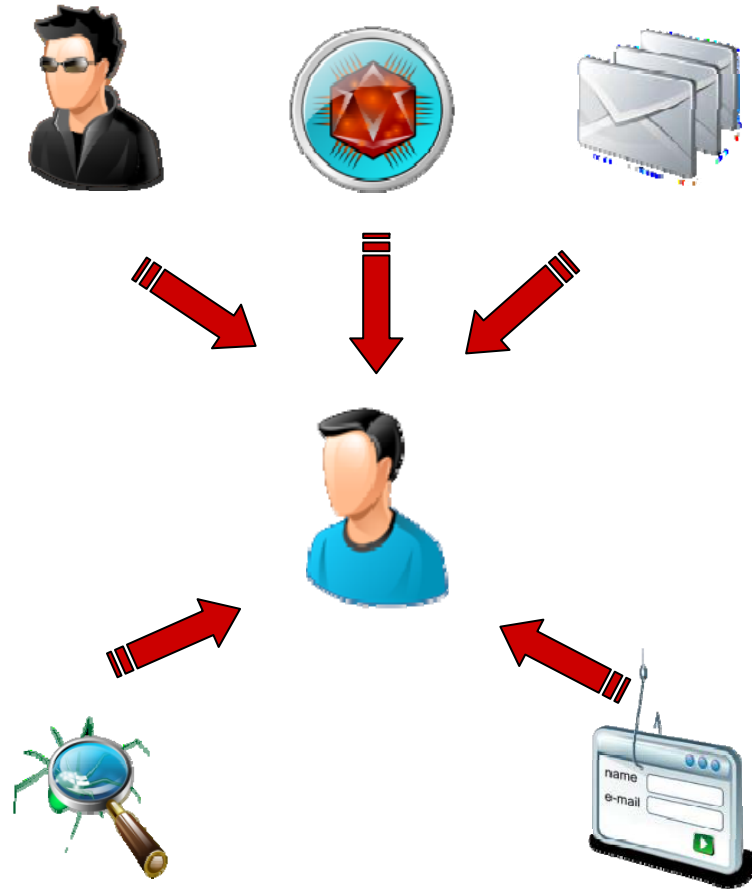
Tips for teachers 10

BitDefender helps you protect your children 11

BitMoms: Sharing your experience with a dedicated parents' on-line community 12



Children and the World Wide Web



Kids are significantly more likely to fall into e-traps than the average adult user.

The mass production and accessibility of computers have turned them into regular family or household commodities, while high-speed Internet connections have become a standard for both home and business users. A significant change has occurred in our day-to-day routine as it now cannot be conceived of without the regular use of e-mail, instant messaging, social networking, blogging, on-line shopping etc.

Considering that the average user spends up to five hours (sometimes even more) in front of a computer, both at work and at home, chances are for children to get familiar with PCs from a very fresh age. Grandparents on the other side of the country can now wish their favorite three year old grandchild a "Merry Christmas" through on-line video chat, for instance.

Kids are fascinated by the Internet and most of them turn out to be extremely skilled when it comes to using a computer. There is no funnier or easier instrument for them to make friends, play games or exchange data both for school and entertainment purposes. A conversation started after classes could easily continue on-line, via IM, or on the "battleground" of the latest on-line role-playing game.

Despite its obvious communication-related benefits, the Internet could also be a hazardous place. It can be used to spread a wide variety of e-threats, such as viruses, worms, Trojans, password stealers, key loggers, adware, phishing schemes or e-mail spam. It can enable the dissemination of inappropriate content, such as pornography or discriminatory material, and it can sometimes set very loose (if any) barriers against unethical conduct, such as plagiarism or cheating.

Because of their age and natural curiosity to try out new things, kids can very easily get into tight spots on the net. That is why it is important for them to get good guidance from the start and to learn about all the good and the bad the Internet has in store.

“On-line predators should not be regarded as someone else’s problem. They are your problem, too,” warns Catalin Cosoi, Senior Researcher at BitDefender® “if you don’t obey some simple safety guidelines meant to protect your children and your family as a whole” adds Cosoi.

Risks and dangers directly targeting kids

On-line addiction

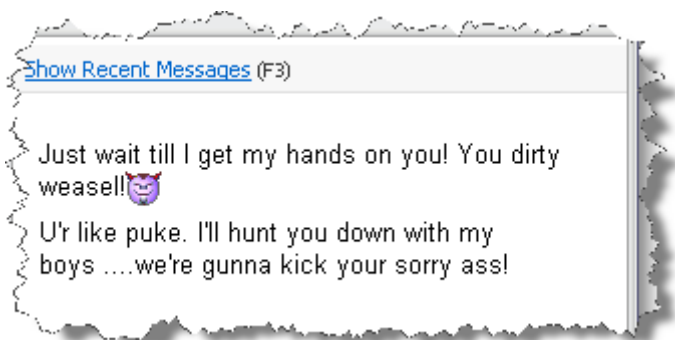
On-line addiction manifests itself as compulsive instant messaging, social networking or gaming and it can alter children’s social behavior and development as well as their physical condition.

If parents don’t constantly monitor Internet activities and the amount of time spent in front of the computer, chances are that children and teenagers withdraw into a virtual universe and isolate themselves from the real world, unable or unwilling to socially interact with others in non-virtual ways.

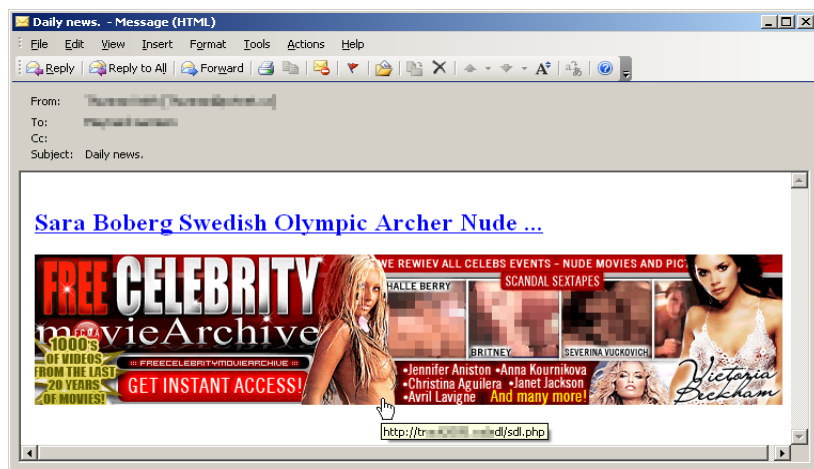
Cyber-bullying

This is described as a situation when a child or a teen is repeatedly tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child or teen using text messaging, e-mail, instant messaging or any other type of digital technology.

This type of behavior is usually recurrent and it involves a credible threat. The reasons behind it can be anger, revenge or frustration, but sometimes kids do it for entertainment or because they are bored.



Cyber-bullying should not be disregarded when it comes to the on-line safety of your kids.



E-mail spam could expose kids to inappropriate content.

Exposure to inappropriate content

Pornographic or discriminatory materials are another risk parents should seriously consider. Without direct supervision or a security solution that blocks unwanted or inappropriate content, curiosity might bring children to look for violent and sexually explicit movies and images.

Similarly, in the absence of appropriate filtering, they might stumble upon materials that infringe social, religious, cultural or other norms and standards, as well as upon content that instructs them on illegal activities. Kids can also accidentally find out about these things via unwanted advertisements displayed by various Web sites.

Encouragement of unethical conduct

Without guidance, children and teenagers could be tempted to plagiarize or cheat when they have to complete their projects or home assignments.

Illegal actions

If kids' on-line interactions are poorly supervised, one of their most frequent mistakes that might have legal implications is the sharing of copyright-protected content.

Since most such content is stored on pirate Web sites or on file-sharing platforms, chances are that computers and data will be compromised in the process. As illustrated in [BitDefender's E-Threat Landscape Report](#), these underground sources are also responsible for a large number of infections, as they also spread malware bundled with the pirated content.



An apparently innocent Web site for children activities is used to spread malware.

E-threats targeting systems and data

Malware

Malware designates any kind of computer program created with a malicious intent and aiming to tamper with the operation of your computer, render your stored information unusable, steal your personal data for financial gain, etc.

In the example here to the left, a Trojan is exploiting the searches one conducts on Twitter for interesting ways to keep kids entertained. Instead of reaching a Web site with games and activities for children, when parents click the displayed shortened URLs, they are redirected towards pages serving different types of malware, including spyware. Without the appropriate security solution any system is at risk.

Phishing and ID Theft

These terms refer to a mechanism that cybercriminals put together in order to trick people into giving them personal data (e.g. credit card numbers, PIN numbers included). To get this information, they create lookalikes of trusted Web pages (banks, social media applications, state authorities, etc.). Mistakenly believing that they are dealing with the real thing, users will type their data and expose themselves to the risk of financial loss.

Additionally, the data posted on social networking pages, blogs and community pages is always at risk. An e-mail address or a photo are enough to make a dishonest buck on somebody else's back. Two known cases stand proof of this: a hijacked family Christmas card appeared in a grocery commercial and a stolen picture of a baby was used in a fraudulent scheme for an alleged adoption.



Safety tips while on the World Wide Web



Spam

Spam indicates the unsolicited e-mails sent to large groups of people, generally to advertise various products. These e-mails are also used as baits in more complicated malicious activities, such as phishing, but they can also expose kids to unsuitable content, such as pornography.

At least half of our daily interaction with computers revolves around the World Wide Web. This is probably due to the fact that it is perceived as a friendly environment for the exchange of different types of content and social interactions. From this point of view, the Internet represents, probably, one of the most valuable educational tools of the 21st century, seen both as the largest human knowledge repository, as well as one of the most complex and effective communication tools.

As previously detailed, while using this valuable communication medium, kids can inadvertently be exposed to inappropriate content or they can become targets for individuals who aim at using them for pornographic, financial or other illegal purposes. Fortunately, these undesirable situations can and should be easily avoided by children, parents and teachers once they decide to openly discuss various aspects concerning on-line safety and to take the steps that will keep them safe. As for the perfect timing to initiate this type of conversation, it depends on how early PCs become part of children's life. The important thing is that before they actually get to use the computer, kids should be aware of the threats Internet interaction poses.



Always talk to your kids, explain to them your concerns about their safety while on the WWW and listen to what they say.

Tips for children and teens

Do not allow the computer to take over your life, affect your school performance, or to replace quality time with your friends and family.

When you create an account to become a member of an on-line community, please ask for your parents' help to make up a list of persons you trust and who will be allowed to contact you.

You can always stop the on-line conversations that you find uncomfortable; if someone or something on the Web makes you feel scared, confused, trapped, offended or threatened, talk to your parents about it and ask for their advice.

Do not share information about you and your family with people you do not know and trust. Do not accept to meet unknown people who have contacted you on-line and make sure you tell your parents about any such person's attempt to see you face-to-face.

Be very careful what photos and videos you choose to upload as – once they are published on the Internet – you will not be able to fully control what happens to them.

When you want to buy something online, and you need to use a credit card, ask your parents for permission and assistance.

Pay attention when you download free games and applications – they might contain malware or inappropriate content.

Tips for parents

Here are some ideas for parents who want to take an active part in their children's on- and off-line life.



Try to spend some time together with your children on-line and help them with their searches, projects or interests. These are valuable moments when you could also give them some guidance along the way.

Try to find out as much as possible about the Internet and computer-related needs of your children and try to solve together the mysteries of the cyber world. Take the time to discuss about the threats that the Internet poses to them as well as to the family as a whole.

If possible, place the family computer in a place where you could keep an eye on the monitor when the circumstances ask for it.

Together with your kids, search for their name on the Internet and see what comes out. You might find interesting things such as blogs they may have, communities they are active in, information about them and about the entire family. This could give your children a sense of responsibility and make them realize that their actions will also have repercussions on all the members of the family.

When children create an account for a social on-line community, help them use the privacy protection features. Create a list of trustworthy persons who contact can contact them. Encourage them to restrict the amount of exposed information to a certain number of people that you know and trust; and make sure you know your child's on-line friends just as you would do in real life.

Together with your children, set some rules regarding computer/Web use, underlining the safety reasons you are concerned about – you might want to make your child an ally in our fight for safety.

Use an antivirus with a “Parental Control” component that provides comprehensive settings for Web and application control as well as the ability to filter Web, mail and instant messaging traffic for certain keywords.

Advise your children not to respond to e-mails that contain spam, obscene and aggressive messages and, furthermore, to avoid sending this kind of e-mails themselves. Teach them about the responsibility they have towards the others in the on-line community, as well as the essential rules of netiquette.

It might also be interesting, if not even useful, to get familiarized with kids and teens' computer lingo: *P911* - "my parents are coming", *PA* - "parent alert", *PAL* - "parents are listening", *PANB* - "parents are nearby", *TAW* - "teachers are watching", etc.

Tips for teachers

Along with the parents, you as teachers, need to be aware of your pupils/students' on-line interests so as to identify and encourage the strong and unique features of each generation.

Make sure you know what filters are installed in your school and discuss with your students/pupils why these safety measures are so important for the school and for them as persons.

Involve your students in on-line activities, using the computer as a didactic tool for diverse teaching purposes. Encourage them to use the computer and the Internet for research, while pointing out the importance of original and creative work. Advise them to use legitimate applications and tell them about the importance of copyright.

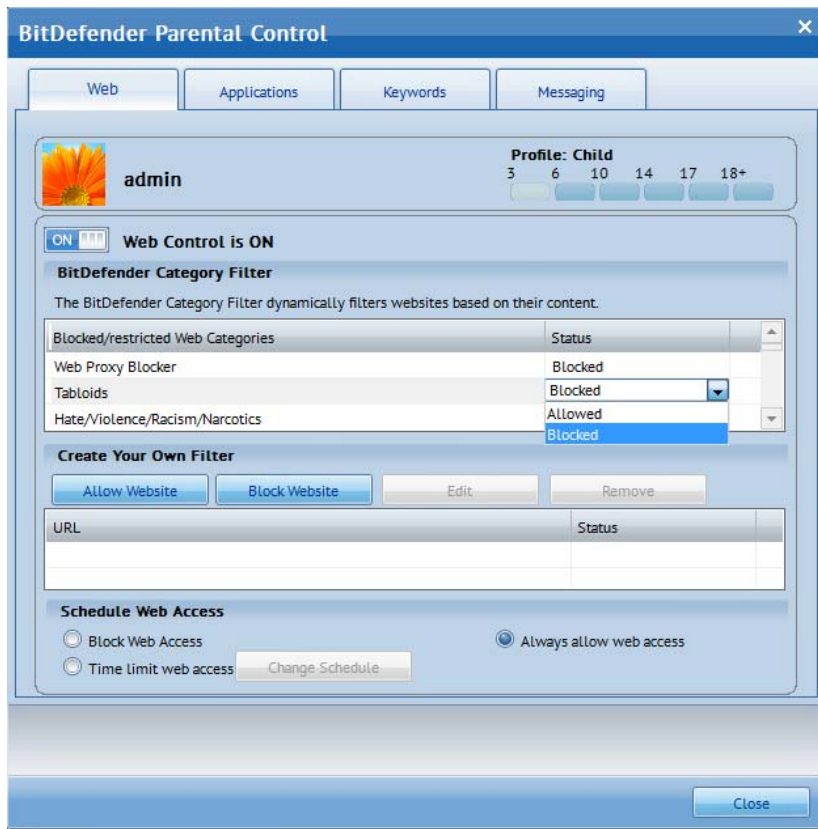
Make sure your students understand that apparently innocent actions on the Internet might hide dangerous intentions and that malevolent individuals could use a great variety of methods to mislead credulous PC users for lucrative purposes.

Explain to your students and pupils why they should not accept to meet people they do not know and why it is so important to always discuss with their parents about this kind of proposals that they receive while on-line.

Involve parents in students' school activities and put them in contact with the authorities directly involved in protecting children from illegal activities - on-line pornography, drugs or data theft.



BitDefender helps you protect your children



BitDefender's Parental Control module offers an easy way to protect your children on-line.

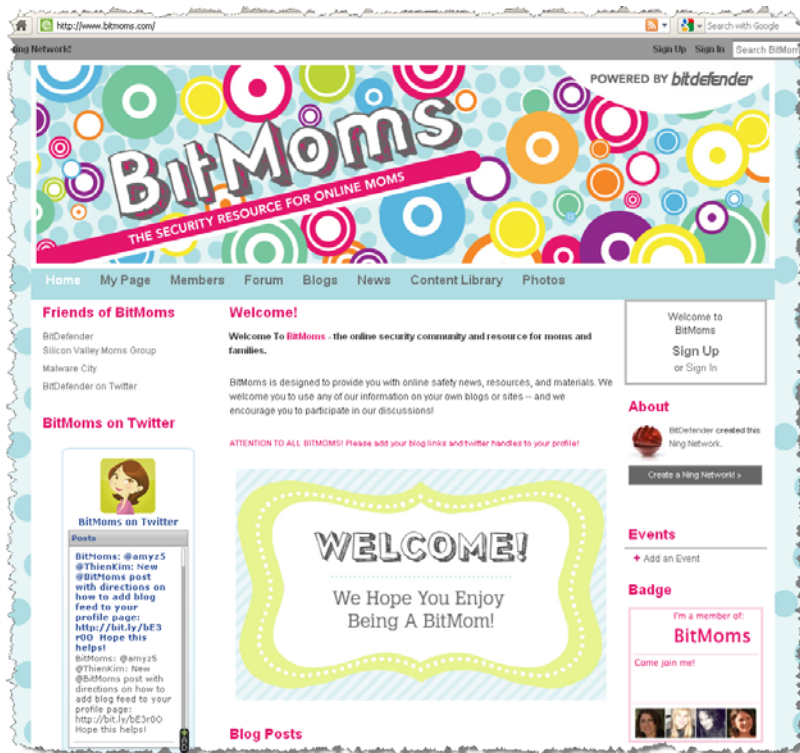
The BitDefender Parental Control module offers monitoring and control options both for Web activities and for various applications that your children use daily. It provides three customizable restriction levels – *Child*, *Teenager* and *Adult*, based on the user's age.

The **Web Control** component enables you – as parent or teacher – to filter Web, mail and instant messaging traffic for certain keywords. That is, you are the one to decide which site the child can or cannot visit based on the type of the content it displays or who is the contact he or she can chat on messaging systems.

The additional **Web Time Limiter** section allows or blocks access to the Internet within predetermined time frames. The intuitive interface looks like a calendar table. When clicked, each box restricts access to the Internet for a certain user; if the same box is clicked twice, the restriction is eliminated.

The **Application Control** component allows you to define a strict schedule based on which (such as games or your own programs, if we refer to a family computer) the child has access to specific applications. You can either set up an hourly or daily cycle, or completely block access to that particular piece of software.

Instant Messenger Control enables you to block or allow messenger IDs, while **Keywords Control** helps you restrict access to Web, e-mail and instant messenger content based on specific words.



BitDefender's on-line community for parents helps you share your experience in protecting kids on-line.

Another important feature of the Parental Control module is that parents can receive a notification e-mail every time the solution blocks an activity the child attempted to perform or they can consult a log with the history of the websites the child has accessed. Only the system administrator, therefore the parent, can make changes in the Parental Control section and these settings can be protected with a password.

BitDefender and its Parental Control module are available for download for a 30 day free trial at : <http://www.bitdefender.com/solutions>.

BitMoms: Sharing your experience with a dedicated parents' on-line community

BitDefender has created and supports several initiatives dedicated to the on-line security of children and families in general.

BitMoms is a community that focuses on kids' on-line safety, its main goal being to provide a common platform for parents' interaction and valuable content sharing, via the BitMoms blog network.

To find out more about or to join the on-line community, please visit <http://www.bitmoms.com>.

MalwareCity is another BitDefender project dedicated to the software security community and a free resource for those interested in defending their systems and data. BitDefender's analysts write about their experiences and discoveries every day, sharing their knowledge with users worldwide. The aim of this Web site is to provide useful information for all those interested in malware and antimalware as well as to help them clarify subjects related to computer security.

To read the latest news about malware or subscribe to the newsletter, please visit <http://www.malwarecity.com>.

The information and data asserted in this document represent the current opinion of BitDefender® on the topics addressed as of the date of publication. This document and the information contained herein should not be interpreted in any way as a BitDefender's commitment or agreement of any kind.

Although every precaution has been taken in the preparation of this document, the publisher, authors and contributors assume no responsibility for errors and/or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein. In addition, the information in this document is subject to change without prior notice. BitDefender, the publisher, authors and contributors cannot guarantee further related document issuance or any possible postrelease information.

This document and the data contained herein are for information purposes only. BitDefender, the publisher, authors and contributors make no warranties, express, implied, or statutory, as to the information stated in this document.

The document content may not be suitable for every situation. If professional assistance is required, the services of a competent professional person should be sought. Neither BitDefender, the document publishers, authors nor the contributors shall be liable for damages arising here from.

The fact that an individual or organization, an individual or collective work, including printed materials, electronic documents, websites, etc., are referred in this document as a citation and/or source of current or further information does not imply that BitDefender, the document publisher, authors or contributors endorses the information or recommendations the individual, organization, independent or collective work, including printed materials, electronic documents, websites, etc. may provide. Readers should also be aware that BitDefender, the document publisher, authors or contributors cannot guarantee the accuracy of any information presented herein after the date of publication, including, but not limited to World Wide Web addresses and Internet links listed in this document which may have changed or disappeared between the time this work was written and released and the moment it is read.

The readers are entirely responsible to comply with all applicable international copyright laws arising from this document. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of BitDefender.

BitDefender may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from BitDefender, this document does not provide any license to these patents, trademarks, copyrights, or other intellectual property.

Copyright © 2010 BitDefender. All rights reserved.

All other product and company names mentioned herein are for identification purposes only and are the property of, and may be trademarks of, their respective owners.