

Parenting and the Internet: The Guide for Raising Your Child to Be Smarter and Safer Online

By Todd Curtis

rev 1 November 2011

Published by Speedbrake Publishing at Smashwords

Copyright 2011 Todd Curtis

Discover other titles by Todd Curtis at Smashwords.com:

[The AirSafe.com Podcasting Production Manual](#)

This ebook is licensed for your personal enjoyment only. This ebook may not be re-sold or given away to other people. If you would like to share this book with another person, please purchase an additional copy for each recipient. If you are reading this book and did not purchase it, or it was not purchased for your use only, then please return to Smashwords.com and purchase your own copy. Thank you for respecting the hard work of this author.

ISBN: 978-1-887674-00-3

~~~~~

## **Table of Contents**

**Foreword**

**Acknowledgments**

**[A Word from the Author](#)**

**Warning—Disclaimer**

**[Chapter 1: Introduction](#)**

[Who Is This Book For?](#)

[What This Book Can Do for You](#)

[How to Use This Book](#)

[Conventions Used in This Book](#)

**[Chapter 2: Parenting and the Internet](#)**

[Basic Philosophy](#)

[Roles and Responsibilities](#)

[Q&A About Being an Online Parent](#)

**[Chapter 3: Your Personal Computer](#)**

[Personal Computer Hardware](#)

[Personal Computer Software](#)

[Internet Service Providers](#)

[Wireless or Wired Connection](#)

[Q&A About Home Computers](#)

[Top 10 Home Computer Accessories](#)

**[Chapter 4: Privacy Online](#)**

[What Does Privacy Mean?](#)

[Key Privacy-related Threats](#)

[Seven Steps to Online Privacy](#)

[Recognizing a Privacy Problem](#)

[Top 10 Privacy Protection Tips](#)

**[Chapter 5: Security Online](#)**

[Key Security-related Threats](#)

[Seven Steps to Online Security](#)

[Recognizing a Security Problem](#)

[Top 10 Security Protection Tips](#)

**[Chapter 6: Internet Legal and Ethical Issues](#)**

[Copyrights and Trademarks](#)

[Q&A About Copyright Issues](#)

[Pornography and Free Speech](#)

[Defamation and Libel Online](#)

[Ten Tips for Avoiding Online Defamation](#)

[Online Piracy](#)

**[Chapter 7: Cyberbullies and Child Predators](#)**

[Online Bullying](#)

[Cyberbullying Warning Signs](#)

[Top 10 Ways to Prevent Cyberbullying](#)

[Child Predators and the Internet](#)

[Law Enforcement Involvement](#)

[Top 10 Tips for Avoiding Online Predators](#)

**[Chapter 8: Email Basics](#)**

[An Overview of Email](#)

[Email Etiquette](#)

[The Gettysburg Criterion](#)

[Top 10 Email Realities](#)

**[Chapter 9: Dealing with Unwanted Email](#)**

[An Overview of Unwanted Email](#)

[Seven Steps to Controlling Email](#)

[Top 10 Ways to Stop Unwanted Email](#)

**[Chapter 10: Web Basics](#)**

[A Quick Overview of a Web Site](#)

[Basic Kinds of Web Sites](#)

[How to Use Search Engines and Directories](#)

[Top 10 Search Engine and Directory Tips](#)

[Finding the Key Sites on a Particular Subject](#)

[Top 10 Tips for Using the Web](#)

**[Chapter 11: Avoiding Inappropriate Content](#)**

[What Is Inappropriate Content?](#)  
[Exposure to Inappropriate Content](#)  
[Filtering Inappropriate Content](#)  
[Seven Steps to Control Inappropriate Content](#)  
[Top 10 Tips About Inappropriate Content](#)

## **[Chapter 12: Online at School and the Library](#)**

[Schools and the Internet](#)  
[Q&A About Being Online at School](#)  
[Top 10 Tips for Being Online at School](#)  
[Libraries and the Internet](#)  
[Q&A About Being Online at the Library](#)  
[Top 10 Tips for Being Online at the Library](#)

## **[Chapter 13: Beyond Email and the Web](#)**

[The Evolving Internet](#)  
[Things You Should Always Do](#)  
[Instant Messaging](#)  
[Chat Rooms](#)  
[Social Networking](#)  
[Online Videos](#)  
[Photo Sharing](#)  
[Webcams](#)

## **[Chapter 14: Managing the Internet](#)**

[Record Keeping](#)  
[Setting the Ground Rules](#)  
[Setting Up Your Home Computer](#)  
[Review of the Online Basics](#)  
[Things You Should Do Regularly](#)  
[Next Steps](#)

## **[Appendix 1: Free Software](#)**

## **[Appendix 2: Online Resources](#)**

## **[Glossary](#)**

## **[About the Author](#)**



## FOREWORD

The Internet is a valuable resource for parents and their children. The key message to parents is: you are in control—no matter whether your kids are more tech savvy than you—and you can feel more comfortable about your kids on the Internet when you know they know the rules. Your kids will feel as though they have a partner in learning when you make the effort to teach yourself about all the wonders of the Internet.

Your child needs to learn a number of technical skills to be able to go online, but he or she will also have to develop a number of social skills in order to use the Internet responsibly. Part of that social development is learning a set of values that will help to guide online behavior and activities in positive directions. With the leadership and values that you as a parent can provide, your child will be better able to avoid the hazards of the Internet and use the technology as a tool that will not only further his or her academic and social development, but also as a tool that will serve your family and community.

Trish Millines Dziko, 2007

Executive Director, Technology Access Foundation

[Back to Table of Contents](#)



## **ACKNOWLEDGMENTS**

There are numerous people from many fields who have helped to shape the advice and information in this book. Many online publishers have supported this effort with their advice and information, especially Mark Hasting and Leo Notenboom.

Educators and library professionals contributed as well, including Andra Addison, Nicole Stark, Sylvia Curtis, and Anna Renault.

Perhaps the most important group of contributors has been the many parents, grandparents, aunts, uncles, and cousins of online children. These adults have provided their questions, wishes, and sometimes cautionary tales during this book's development.

Special thanks go to Arlene Prunkl for editing, Robert Howard for cover design, and publishing consultant Faith Conlon. The most special thanks go to my wife, and especially to my son who regularly demonstrates just how much more I need to learn.

[Back to Table of Contents](#)



## A WORD FROM THE AUTHOR

If you search any large bookstore for books about the Internet, you will find many how-to books on hardware, software, and the latest trends and gadgets, but very little about how to be a parent of an online child. While several books are available about the threats from online predators and some titles focus on parental control software, there are few books that address other concerns.

If you think there is more to being an online parent, this is the book for you. I've done my best to discuss key issues about being the parent of an online child that I do not see discussed in other books, issues that every parent needs to understand even before their child gets on the Internet for the first time. Topics include:

- How to make sure you control how your children use the Internet.
- Where to find all the free software and online resources you and your family will need to protect your computer and make it more useful.
- How to use online resources like search engines to help your child find useful information.
- How to protect your computer and your family from viruses and other malicious software.

No matter how much the technology of the Internet may change, or how your child's interests and needs change, this book will show you how to keep on top of it all and help your child become confident and capable online.

Dr. Todd Curtis, Seattle

[Back to Table of Contents](#)



## **WARNING—DISCLAIMER**

This ebook is for informational purposes only. It is sold with the understanding that the publisher and author are not engaged in rendering legal or other professional services. If such assistance is required, you should seek the services of a competent professional.

It is not the purpose of this work to include all the information that is available, but to complement, amplify, and supplement other resources. You are urged to learn as much as possible about the subject matters covered, and to tailor the information to your individual needs.

Every effort has been made to make this work as accurate as possible. However, there may be mistakes both typographical and in content. Therefore, this text should be used only as a general guide on the subject matters covered. Furthermore, the information contained in this ebook was current only up to the publishing date.

The purpose of this work is to educate and entertain. The author and publisher specifically disclaim any liability that is incurred, or that is alleged to have been caused, directly or indirectly, by the use or application of the contents of this work.

Any term appearing in this work that is known to be a trademark or service mark appears as requested by the owner of that mark. All names of products and services mentioned in this work are used in an editorial fashion only and to the benefit of the trademark or service mark owner, with no intention of infringement of any trademark or service mark. All trademarks and service marks are the property of their respective owners.

The fact that an organization or a web site is mentioned in this work as a source of information does not mean that the author or publisher endorses that organization or the recommendations it may provide. Also, you should be aware that web sites listed in this work may have changed or disappeared since this version of this work was written.

If you do not wish to be bound by the above, please discontinue using this work.

[Back to Table of Contents](#)



## CHAPTER 1: INTRODUCTION

### In This Chapter

- Who Is This Book For?
- What This Book Can Do for You
- How to Use This Book
- Conventions Used in This Book
- Additional Resources

If you have picked up this book, you probably have a child who is on the Internet or will soon be online, and questions about how to manage your child's online experience. Even if you have been online yourself for years, you know that children approach the Internet differently from adults. This book deals with many of the issues that will arise, and will give you advice on how to set rules for online behavior, how to set up your computers, and how give your child the guidance he or she needs to be responsible online.

### Who Is This Book For?

This book is for anyone who is responsible in some way for a child who is on the Internet or about to be on the Internet. It is particularly useful for parents who have children in the home as well as a computer. The following brief sections have examples of the kinds of situations where this book will be helpful.

#### **Parents with Kids Who Are Not Yet Online**

Children often start using computers at a very young age, either at home or at school. For these children, computers are not a mystery, but simply things that are part of their normal lives. By the time your child is in elementary school, she will know about the Internet and will have an opportunity to go online or at least see others online.

#### **Parents Who Want to Understand the Internet**

Figuring out the Internet can be a challenge, but with a little bit of effort you will learn enough to be able to ask the right questions and to make good decisions about your family's online activities. If you understand the basics of what the Internet is about, you will have the tools to be an effective online parent.

#### **Parents Who Want More Control of Their Online Child**

No matter how much more your child knows about the Internet, your child is still a child and you are still a parent. Your rules must be the ones that matter, and you have to have enough control over your children's online activities to be able to protect them from online dangers.

#### **Parents Who Want to Use the Internet for Education**

Whether you homeschool your child or send your child to a traditional school, you can easily use the Internet to supplement your child's education by taking advantage of the resources of major libraries, or perhaps to read the local newspaper as well as newspapers from far away. With the guidance and information offered in this book, you will be able to provide your children with many more tools that will help their formal education.

#### **Parents Who Want More from the Internet**

There are more things to do online than you can imagine. The trick is figuring out which things are most important to you and finding out how to do those things online. There are



many resources in this book that can get you started, and it also shows you how to go out and find what you need on your own.

### **What this Book Can Do for You**

This book aims to be a basic guide for parents who want to get beyond the first hurdles of having their family and especially their children online. To get past those initial hurdles, this book will help you do several things:

**Setting rules:** Every parent needs to have rules for their children regarding the use of the computer. The book has several suggestions for a written agreements that could be used with a young child, as well as agreements for older children.

**Understanding basics:** Whether you have online experience or not, it is important that when your child goes online, she understands how to use a computer and how to use the basic Internet applications like email and search engines. Parents need to know enough about the kinds of online services children use so they can do a better job of making sure their children are acting responsibly online.

**Finding good software:** Not only good software, but good free software. One of the great things about the Internet is that there are communities of computer experts who have created free software for home computers. This book not only shows you where to find a lot of good, useful software, but it also provides resources that will let you find other free software that will work best for you.

**Finding good resources:** The Internet has all kinds of free resources that your family can use right now, from help with homework and online dictionaries to medical information and science education. The book helps you here in two ways: by providing dozens of suggested resources as well as detailed instructions on how to find what you need online.

**Keeping your family safe:** Identity thieves, online bullies, and child predators are just some of the hazards your child and your family face online. This book offers numerous detailed suggestions and guidelines you can use to reduce or eliminate most of these problems from your online lives.

**Avoiding objectionable content:** It is no secret that the Internet has more than a few places your children should not visit. By following the advice given throughout this book, you can keep those uncomfortable and embarrassing moments to a minimum.

### **How to Use this Book**

This book is designed to be used as a resource you can come back to again and again as your needs and the needs of your child change over time. Different parts of the book deal with the different needs you may have as a parent, no matter what kind of relationship you and your child have with the Internet. The following examples show how a general concern may be covered by different parts of the book:

**Role of the parents:** Chapter 2 describes the philosophy behind this book, which is that parents are in charge and should take the lead in making the rules about what their children can do online.

**Setting up your computer:** Whether you already have a computer at home or you plan on getting one soon, chapter 3 tells you what a basic setup looks like and what

kind of software and hardware extras you may need. Appendix 1 also contains descriptions of many kinds of free software you can add at any time.

**Maintaining privacy:** Chapter 4 describes how easy it is for your family's privacy to slip away if you and your children are not careful online. The chapter also has plenty of advice on keeping a low online profile and for creating passwords and user names to protect your privacy.

**Staying secure online:** Chapter 5 gives you a basic review of online safety issues for families, while chapter 7 addresses both online bullying and child predators.

**Using email and the Web:** This is a big subject, but an important one for children learning how to use the Internet. Chapters 8 and 9 discuss how to use email and also how to avoid unwanted email, while chapters 10 and 11 discuss how to find good information and resources online while avoiding objectionable content.

**Rules you should know:** Parents need to know how to keep themselves and their children out of trouble when going online at home, at school, and at the library. Chapter 6 explains some of the basic legal realities of being online, while chapter 12 discusses common online rules at schools and libraries.

**Online activities you should know about:** Kids adapt to change easily, and the enticing new features on the Internet are no exception. Before your kid dives into a new online activity, you need to decide if it is a good idea or one you and your child should pass up. Several popular online activities are covered in chapter 13, including social networking, chat rooms, instant messaging (IM), and photo sharing.

**Managing your child's activities:** Chapter 14 gives you an easy-to-follow plan for setting up your household to make it easy to keep track of all the things your child does online, including all of their online accounts, all of their passwords, and all of their data.

**Handy reference material:** The back of the book includes a glossary of computer and Internet terms in plain English, as well as lists of useful free software and free online resources.

### **Conventions Used in this Book**

#### **Computer Examples**

This book assumes that you will be using either laptop or desktop computers that run some version of an operating system from Microsoft, most of what is in this book also applies to desktop and laptop computers from Apple.

#### **Capitalization**

When a company's specific software programs are mentioned, those names will be capitalized. The word Internet will always be capitalized, as will the phrase World Wide Web or the abbreviation Web. However, phrases referring to something other than the entire World Wide Web will be in lowercase. These would be phrases like web site or web page. The capitalized word Windows refers to the operating system software from the Microsoft Corporation, but the lowercase word window refers to rectangular spaces on a computer display.

#### **Glossary Terms**

At their first occurrence, words and phrases related to computers or the Internet are

usually explained in the text. If an important term is not defined in a chapter, you will find the definition in the glossary in the back of the book.

[Back to Table of Contents](#)



## CHAPTER 2: PARENTING AND THE INTERNET

### In This Chapter

- Basic Philosophy
- Roles and Responsibilities
- Q&A About Being an Online Parent

If you are now a parent, you probably first learned how to use the Internet at school or in the workplace, controlled environments with rules of online behavior enforced by teachers or managers. This is quite different from today, where your child is much more likely to learn about the Internet while at home. If this is the case, you will have to take a very active role in teaching your child how to use the Internet.

### Basic Philosophy

The basic philosophy of this book is simple—parents should be in control and take the lead regarding making the rules about how children use computers and the Internet. There is simply no other way of running a household with children. Allowing the children to make all the decisions about how or when to use a computer makes about as much sense as allowing a child to make all the decisions about how and when to drive a car. Just as is the case with a car, a child may be highly motivated and may even have superior skills when it comes to driving and maintaining a car. However, a child does not have the experience, the judgment, or the level of responsibility that a parent has. Technology has to take a back seat to parenting.

### My Parents and Their Teenage Drivers

The situation that you face as a parent with the Internet in the 21st century is similar to what my parents faced with cars in the 20th century. My parents were teenagers in the early 1940s when it was rare for the average teenager, including both of my parents, to have the use of a car. When I was old enough to drive, there was never any question about whether my parents were justified in telling me when I could drive, where I could drive, and how I could drive. It didn't matter that they never drove cars as teenagers.

My parents' authority over my driving did not depend on their technical skills. I was much more knowledgeable about cars than my mother. I knew how to fill the tank, change a tire, and even hot-wire my 1964 Ford Falcon, which were all things my mother could not do. Did she let the fact that I knew more about cars keep me from following her rules, whether I liked it or not? Not at all.

### Cars, Computers, and Parenting

As was the case with previous generations, it should not matter if you used a particular technology as a child. You are still a parent, and you have to make the kinds of decisions parents make in every generation. When it comes to the Internet, it does not matter whether you are a computer expert who has been online for more than 20 years or if you don't know the first thing about computers. Being online is a very important part of modern life, and one way or another it will be a very important part of your child's life.

Think of computers and the Internet the same way you would treat cars, televisions, cell phones, or any other technology you use. You do not have to understand how any of these technologies work to understand how to make them work for you. If you allow your child to use these technologies, you are also responsible for making sure your child uses

them in a safe, sensible, and responsible manner.

### **Why the Internet is Different**

While the Internet represents a technology, it is different in some important ways from other technologies like cars, phones, television, and even personal computers:

**Community:** By using the Internet, your family becomes part of a much larger community, and learning how to deal with that community is an ongoing process for your entire family.

**Communication:** The tools and services of the Internet allow you and your child to communicate in ways that are very different from what you are used to, and you have to understand how those differences can either help or hurt you or your child.

**Change:** The things that are available online change very quickly, with many new or more sophisticated services being offered every year.

**Culture:** The Internet has become a normal part of everyday life, with most children using it at home, in school, or at the library well before they reach middle school. As a parent, you have little choice but to learn how to deal with it in your child's life.

### **Why the Internet Is Not Different**

The Internet is not magic or mysterious. It is merely one of the many technologies that families deal with every day. As with any other technology, a family has to decide how much or how little a role it plays in the family's life. The Internet can give a family greater options and greater opportunities if the family members, particularly the parents, are willing to make the decisions and take the actions that are sensible and necessary. If you are willing to do those things, the Internet will be a very positive thing in your family's life.

### **Your Technological Generation Gap**

Don't feel left out because you were not online as a child. Chances are, you are too old! The first time computers were ever connected using the technology of the Internet was in 1969, email was first introduced in 1972, and the first browser in 1990.

### **Roles and Responsibilities**

One of the core themes of this book is that parents must take the lead in guiding a child's development on the Internet. Because using the Internet can be at times complicated, with your child able to perform several online activities at the same time, your involvement as a parent will be much different than your involvement with your child using a simpler technology like television.

### **Role of the Parents**

The following are this book's basic assumptions about the role of parents:

**Parents are the leaders:** Within the family, the parents are responsible for providing guidance and boundaries when it comes to a child's use of the Internet, and for making sure that a child's online behavior reflects the family's values. Written agreements such as the examples given elsewhere in the book give both you and your child common reference points when dealing with the Internet.

**Parents make the decisions:** In any significant decision involving a child's online activities, parents must have the final say, such as whether to allow a computer in the

home, what hardware or software should be installed on the computer, or what activities are allowed online.

**Parents make and enforce the rules:** As a parent, you have to set limits on what your children do online. Those include limits on when a child can be online, what he can do online, and who he communicates with online. These parental roles are necessary no matter what technology may be involved.

**Parents guide children toward independence:** Eventually your child will want or need to go online without you at his side. You must anticipate this and work with him, knowing that one of your goals is to make sure he will in time become competent and knowledgeable enough to go online alone.

**Parents provide values as well as skills:** While ensuring that order and discipline govern a child's online activities, parents should also teach and enforce basic values that have meaning beyond the entertainment or education that is offered by the technology of the Internet.

### **Role of the Child**

Your child's role in proper Internet use is very similar to her role in the family. A child will start off needing the close support and supervision of a parent, but eventually she will develop emotionally and intellectually, as well as become more sophisticated in the use of technology. All these things would be very difficult without the close involvement of parents. Some of a child's more important roles include the following:

**Children must play by their parents' rules:** What works in the rest of a child's life also works on the Internet. If your child is not willing to play by your rules, you impose restrictions. Because being online is something that kids generally enjoy, denying access as a consequence of poor behavior often serves as a big incentive for her to change that behavior.

**Children must be responsible for their actions:** Your child must know that when she is online, actions have consequences. You need to make it clear what she can do online, and you should also be prepared to take appropriate actions when she does not live up to her responsibilities.

**Children must share their experience:** It is no secret that kids think and act differently from adults in many areas of life, including their use of the Internet. Even if you have years of online experience, you could likely learn many new things from your child. Encourage your child to share her online experience so you can both learn together.

**Learning about the Internet is a key goal:** No child knows exactly how the Internet will fit into her life. It is important that your child learns as much as she can about the basics of the Internet and how to make it both useful and entertaining.

### **Internet Use Agreements and Your Child**

One of the best things you can do to make the whole process easier is to put things in writing, starting with a written agreement on the use of the Internet. Having a written contract between you and your child may seem to be an extreme measure, but your opinion may change as you go through this book. You will see that being an online parent means keeping track of many different things, including what is acceptable behavior and what is not. Writing things down reduces the confusion and gives both you and your

family a starting place as all of you figure out what kind of relationship your family will have with the Internet.

If you would like to look at some examples of a Internet use agreement, you can download one from Speedbrake Publishing at [forms.speedbrake.com](http://forms.speedbrake.com). After going through some of the other chapters in the book, you may find that you will want to add to or subtract from what you see in these sample agreements.

### **Online Family Values**

The sample agreements in appendix 3 include something that is rarely discussed in books and articles about the Internet: the role of values. The combination of personal computers and the Internet is a powerful tool, and the potential for that tool to expand your child's world is limited only by the imagination. What your child does online will be influenced by values expressed by schools, classmates, and others outside of your family. It is up to you to make sure the values that are important to your family shape what your child does online.

You probably have many different values that you would like your child to take to heart, but your family Internet use agreement should focus on the one or two values you think are the most important. When you sit down with your child to talk about the online agreement, it would also be a good time to talk about what those values are and to put them in writing.

### **Q&A About Being an Online Parent**

#### ***Why should I have a written contract with my child?***

It is important your child understands that being online has many important consequences, and that you have expectations of how she will behave. It also shows her you are serious about issues like her safety online. Most importantly, it will show your child that you plan on being involved in what she does online.

#### ***The Internet seems so complicated. How am I supposed to learn about all that stuff?***

You don't have to understand the entire Internet to be able to use it. It is like anything else involving technology; you learn enough to get started, and you get better at it as you go along.

#### ***My kid knows so much more about the Internet, and I feel like I won't ever be able to catch up.***

That may be true, but you still must act like a parent when it comes to computers and the Internet. Think of the computer and the Internet as tools, or even as a kind of household appliance. Even if your child knows much more than you about how a tool or appliance works, you must use your common sense to figure out whether it is being used properly or not.

#### ***How do I explain to my son why I am making rules about how to use the Internet?***

Explain why you are making the rule, and one of two things will happen: either he will understand your reasoning and follow the rule, or he will not. If he does not understand your reasons, arguing will probably not change that, so save your energy. Saying "because I say so" is a good enough response.

#### ***What is an important value to have in the family Internet agreement?***

That is a question only you can answer. Think of an idea or a goal that sustains your

family in good times and bad, no matter what kinds of distractions, temptations, and roadblocks get in your way. Talk about it with your family, and I'm sure that all of you will come up with several ideas.

[Back to Table of Contents](#)





## CHAPTER 3: YOUR PERSONAL COMPUTER

### In This Chapter

- Personal Computer Hardware
- Personal Computer Software
- Internet Service Providers
- Wireless or Wired Connection
- Q&A About Home Computers
- Top 10 Home Computer Accessories

The one thing your child will need to go online is a computer. If you don't have one in your home and would like to get a new one, you need to know a little about what you'll have to buy. If you already have one, then you should have some idea about whether you need to add any hardware or software, or whether you need to get a new computer.

Computers and the Internet may be complicated technologies, but you don't have to be some kind of technical genius to understand the basics. Let me make another car analogy: think of computers and the Internet the way you think of driving. Cars are complex pieces of machinery and you have to share the road with millions of other drivers, but you can drive a car without knowing how to build a car, and you don't have to know every traffic rule for every situation in order to drive safely.

If you can understand the basic facts in this chapter, you will have enough information to at least ask the right questions about what you may need to get you and your child online.

### Personal Computer Hardware

The two most common types of personal computers used in homes are desktop computers and laptop computers. Both kinds of computers have the same basic components, with the laptop putting all those components into one portable unit and the desktop having those components connected by wires and cables. Some basic components are included in even the cheapest desktop and laptop computers, and there are other components that you will probably want to add to make the computer more useful. Smaller laptop computers, also known netbooks, typically don't include a built-in optical drive.

Other common types of personal computers include tablet computers like the iPad, Internet capable mobile phones like the iPhone, and other Internet capable mobile devices like the iPod Touch. This book will not focus on these types of devices, but rather on desktop and laptop computers. However, many of the issues covered in this book also apply to these smaller devices.

### Basic Personal Computer Components

The following components are usually included with every new desktop or laptop:

**CPU:** Also known as the central processing unit, this is the brain of the computer that uses software and inputs from the user in order to operate. For a desktop computer, this term also refers to the component containing all the basic hardware, including the hard drive.

**Display:** Laptop computers and most new desktop computers come with a flat screen display that uses the same kind of technology as a flat screen television.

**Hard drive:** This is where most of the information on the computer is stored,

including software and data. Information is stored in files, which are organized collections of data that can be saved or retrieved by a computer.

**Keyboard:** This has the same basic keys and layout as a typewriter, with a number of other keys for various computer-related functions.

**Modem:** This is a device that allows the computer to communicate with the Internet through either a telephone line, cable connection, or wireless connection.

**RAM:** Short for random access memory, this is the area of the computer where data is temporarily stored when the computer is operating.

### **Optional But Very Useful Hardware**

The following pieces of hardware are not standard equipment that come with most new computers, but your computer will be much more useful if you have them:

**External hard drive:** This is an independent hard drive that can be connected to a computer. Typically, this kind of drive has much greater capacity than other portable data storage devices.

**Flash drive:** This is another kind of portable data storage device.

**Mouse:** This is a device that can position the cursor and select items on the screen. Most laptops have one built into the keyboard, but for many people an external mouse is easier to use. You could run the computer using only the keyboard, but it is usually easier to use a mouse with the keyboard.

**Printer:** Typically, you can use this to print documents either in black and white or in color.

**Router:** This is a device you need to use if you want to create a home wireless network that allows computers in your home to connect to the Internet without using cables or wires.

**Speakers:** Some online content contains audio. Although you could use headphones or built-in speakers, external speakers usually give a much higher sound quality.

**Surge suppressor:** This electrical accessory is designed to protect sensitive electronic devices from sudden and significant changes in voltage; for example, from a power outage.

**Wireless modem:** This kind of modem allows the computer to connect to the Internet without using wires or cables.

**Optical drive:** This device, typically included as standard equipment in desktop computers and full sized laptop computers, can read and write data, including music and video to a CD-ROM or DVD. Software is sometimes sold and distributed by CD-ROM and you have to have a DVD drive if you want to play movies on your computer.

### **Personal Computer Software**

Most of the software you will need either comes with your computer, or else can be easily obtained. Fortunately, many of the additional programs you and your family are likely to use are often available for free.

### **Basic Personal Computer Software**

The following programs are included with every new desktop or laptop, and you will use them every time you go online:

**Operating system:** This program controls all the other software that operates in the computer and any devices connected to the computer.

**Browser:** This kind of software program allows your computer to interpret, display, or access information from the Internet. While your new computer's operating system typically includes a browser, you can also find high quality free browser programs online.

**Email program:** This kind of program allows you to compose, send, and receive email messages. While new computers typically include an email program, you can also find free email services online.

### **Optional But Very Useful Software**

The following types of software may be included with your computer, or may be provided for free if you pay a company for Internet access services. Free software or free online services that can perform each of the following functions can be found online:

**Antispyware:** This software can detect or remove spyware from a computer, or prevent spyware from being installed.

**Antivirus:** Software designed to detect or remove software viruses from a computer.

**Firewall:** This software controls communications between a personal computer and the Internet and prevents unauthorized access to that computer.

**PDF reader:** This software allows the display of files in the Portable Document Format, a file type widely used to distribute documents online.

**Photo organizer:** This type of software can be used to manage photos and other graphics files.

**Presentation manager:** This software is used to create, display, and print presentations that may use a combination of text, graphics, and audio.

**Spreadsheet:** This kind of software will display data in one or more rectangular grids, and allows the user to perform calculations on that data.

**Word processor:** This software allows a user to create, edit, format, display, and print documents containing both text and graphics.

### **Optional But Entertaining Software**

It is no secret that children enjoy and adults having fun on the computer, especially with music, movies, or video games. Just about every computer comes with basic software that allows you to play music or movies that are online. To make your computer into an even better part-time entertainment center, you could add software allow you and your family to organize and easily play songs and videos that are stored on your computer's hard drive. Perhaps the best free software in this category is Apple's iTunes, which is not only free, but doesn't require you to buy any other Apple product like an iPad or iPhone.

### **Free Software vs. Purchased Software**

When you buy a personal computer, it will likely not have all of the software that you will want or need. New software can be very expensive, with some of the more sophisticated programs costing hundreds of dollars. While you may have to buy some

programs, you have plenty of options for free software that can perform many of the functions that you or your child may want your computer to do

Many of the free software products mentioned in this book were created by for-profit companies. In some cases, the company has more advanced versions of the software that must be purchased, and the less capable free software acts as a marketing tool. Other companies give away the software in order to encourage you to buy other products and services. Some free programs were developed by organizations staffed by volunteers who also provide free support. Whatever the motivation of the creators, your family can benefit by using free programs whenever you have the opportunity.

### **Internet Service Providers**

You must use the services of an Internet Service Provider (ISP) if you want to access the Internet from your home computer. One of your first tasks after getting a new home computer will be to decide what kind of Internet connection you want. Most ISPs will offer you one or more of the following options:

**Dial-up:** This is Internet connection through a telephone line. You cannot connect to the Internet and use your telephone for voice communication at the same time. Typically, this is the cheapest and slowest kind of online connection.

**DSL (Digital Subscriber Line):** This Internet access option allows a higher connection speed than dial-up, and also uses a standard phone line. Unlike a dial-up connection, a user can make and receive voice telephone calls while simultaneously connected to the Internet.

**Cable modem:** This connection to the Internet uses a coaxial cable that may also carry other data such as television programming.

### **Wireless or Wired Connection**

When you choose a higher speed Internet, you typically have the option of having your personal computer directly wired into the connection, or using additional hardware and software to allow wireless connections to the Internet.

Whether you choose a wireless or wired connection depends on your situation. If you only have a single desktop computer, then a wireless connection may not make sense. However, if you have several computers in your home and more than one of them may be in use at the same time, or if you have a laptop computer that you want to use in several places in your home, then it may be practical to have a wireless connection.

### **Wireless Issues**

Two issues have to be addressed if you choose wireless: the issue of wireless security and the issue of managing your child's online activities. The first is easily addressed by using the available security features that are built into a typical wireless system. More details are provided in the section "Seven Steps to Online Privacy" in chapter 4.

The second issue may be more complicated. With a wireless system in a household, a computer can be set up wherever it is convenient. Make sure the computer your child uses is placed in a position where you and other family members can easily see what is happening on or near the computer. If your child is using a laptop, then you may have to include additional rules outlining where the laptop must be located whenever your child

is online.

## **Q&A About Home Computers**

### ***Which is better, a desktop or a laptop computer?***

It depends on your family's needs. If the computer will always be in the same location in your home, then get the desktop. If you need to be able to move it around your home, then the laptop makes more sense.

### ***What do I need to go online?***

Your new computer will come installed with a browser and several options for going online. You need a regular telephone line to access the Internet for most providers. If you want to set up your home for wireless access, you will need additional hardware such as a wireless router.

### ***How much does it cost to go online?***

The cost will depend on the kind of service that you choose, and your choice of service provider. Basic dial-up access plans tend to be the cheapest, and high-speed access using DSL or cable modem usually has both a higher quality service and higher costs. DSL or cable access may also be included in some telephone or cable television service plans. Depending on the quality of your service, Internet access for your home can range anywhere from as low as about \$10 to over \$40 per month. Most areas have several choices for service, so compare offers and pick the one that is best for you.

### ***Can't I get online for free?***

There are many ways to get online for free, but you may not be able to do it from your home. For example, many public libraries allow visitors to access their wireless networks. Some businesses may also offer free wireless access. If you only have a desktop computer in your house, you may live close enough to use the wireless network of a generous neighbor (with your neighbor's permission of course).

### ***What extra equipment should I buy with my computer?***

The one extra that almost everyone needs is a printer. Speakers usually come with a new desktop computer, but laptop speakers tend to be very small and not very loud, so if sound quality is important to you, you may want to buy a pair for your laptop.

### ***Does my hardware have to be from the same company?***

No, it doesn't. You can use printers, speakers, keyboards, and other accessories that come from different companies.

### ***How much is a new computer?***

That depends on what kind of computer you want and what kind of extras you want to have. In late 2011, prices for new desktop and laptop computers from major manufacturers started from below \$300, and there were a wide range of computers costing less than \$500. Lower priced laptop computers usually did not include an optical drive.

### ***Where is the best place to get a new computer?***

You can go to consumer electronics stores, or even large department stores to buy a computer, or you can order one online or by phone. Some companies do not sell their computers through retail outlets and others allow you to buy a computer in traditional stores or online. No matter where you buy a computer, make sure that you buy it from a

company that has a good reputation for customer service.

***What extras do I need to buy to play music and videos?***

Most new computers should come with media software, or you can download a program for free. If anyone in your family plans to store or play a lot of music or video on the computer, then you should pay extra for a larger capacity hard drive, and if your computer does not have an optical drive that can play DVDs, you may want to get an appropriate external optical drive.

***How fancy should my new computer be?***

A basic personal computer will come with an operating system already installed along with enough software and hardware to be able to connect to the Internet. You may not need to buy extra software since all the basic software you'll need to do work for home, for school, or for a small business can be found online for free (see chapter 14 and appendix 1 for details).

***Can I afford a computer on a limited budget?***

Let's put it this way. A new computer and a year's worth of Internet access can cost less than a television with a year's worth of cable access, a video game system with a handful of new games, ten cartons of cigarettes, or a weekend stay at a theme park. That computer will probably do much more for you, for your child, and for your family than any of those other things. If your family budget is limited, cut something else out and get that computer.

***Where is the best place in my home to put a computer?***

If you have only a single computer and if it will stay in one place, keep it in a part of your home where you and other family members can easily drop by and look at what your children are doing online. If you have a wireless connection and laptop computers, insist that your children can only go online if the computer is in an open area where others can see what is going on. No matter what your situation, your child should not be allowed to go online behind closed doors.

**Top 10 Home Computer Accessories**

If you are about to get a new or used computer for your home, make sure you also have the following extra software and hardware accessories. You do not need them to use the computer, but they make using the computer or using the resources of the Internet so much easier. Refer to appendix 1 for details on where to get the free software mentioned in this list.

- 1. Printer:** You can use this to make paper copies of documents from files on your computer or from online resources.
- 2. Mouse:** You can run every program on your computer using the desktop keyboard or your laptop's built-in mouse, but most programs and web sites are much easier to use if you use an external mouse. While most new desktops come with an external mouse, new laptops typically don't.
- 3. Optical drive:** Having this capacity makes it easy to store data or to create music CDs using relatively inexpensive CD-ROMs, or to watch movies on DVDs.
- 4. External speakers:** Most laptops and even some desktops have built-in speakers, but a pair of external speakers, even very cheap ones, will give you a much better-

quality sound.

**5. Flash drives:** You can use these either as a way to back up your files or to transfer files between computers.

**6. Additional browsers:** New desktops and laptops come with at least one browser, but popular alternative browsers like Firefox and Chrome have options that may allow you to have more control over the browsing experience, especially when it comes to blocking advertising.

**7. OpenOffice:** This office application suite has all the software you need for doing word processing, spreadsheets, and presentations for either work or school.

**8. Adobe Reader:** This software can be used to view, print, and search PDF files, which is the preferred file format for many online documents.

**9. Gmail account:** Google has a wide variety of free online services that you may find very useful, and many of them require you to have a Google account. If you sign up to use their Gmail online email account, you will not only have access to a very capable email system that is separate from your computer, you will also be able to sign in and use many of their other free online services.

**10. iTunes media player:** You can use this program to easily manage most of the audio and music files on your computer, and you do not have to buy an iPod, iPad, or iPhone to use the software.

[Back to Table of Contents](#)



## CHAPTER 4: PRIVACY ONLINE

### In This Chapter

- What Does Privacy Mean
- Key Privacy-related Threats
- Seven Steps to Online Privacy
- Recognizing a Privacy Problem
- Top 10 Ways to Protect Your Privacy Online

The Internet is a very social medium. In the United States, more than half of the adult population regularly goes online, and an even larger percentage of teens and preteens make the Internet a regular habit. Part of the habit includes taking steps to protect your privacy. If you don't, you could face all kinds of privacy problems, from junk emails to online predators. Parents have two key roles in protecting their children's privacy, helping them to develop good online habits, and taking steps to make sure that any computer or online service that a child uses is set up to protect that child's private information.

### What Does Privacy Mean?

A simple definition of privacy in this context is the ability to control the type and amount of access others have to your personal information and the amount of control you allow others to have over your online experience.

### Why Online Privacy Is Important

Keeping private and personal information under control is important to anyone who spends time online. If you or your family do not take steps at least some basic steps to protect your online privacy, you may be at increased risk from one or more of the following privacy-related hazards:

- Being sent large amounts of unsolicited email.
- Becoming a victim of identity theft.
- Exposure to large amounts of online advertising
- Unauthorized access to your computer or to an online account.
- Unauthorized bank or credit card activity.

### Examples of Private Information

Private information includes any information about your life or about your child's life that you would like to control. This is information that in the wrong hands could bring unwanted attention or that could put you or your child at emotional, financial, or physical risk. A partial list of that kind of information would include the following:

- Age
- Birth date
- Current or former address
- Current or former employers
- Current or former phone numbers
- Current or former schools



- Email addresses
- Financial information
- Gender
- Information needed to access computers, computer networks, or online services
- Lifestyle information such as travel schedules, group affiliations, clubs, favorite activities, and details about personal relationships
- Medical information
- Mother's maiden name
- Name, nickname, or initials
- Social Security number or other information from government-issued identification

### **Key Privacy-related Threats**

Your family's privacy is at risk when others get too much access to your private information or when others get too much control over the information that gets sent to you. While some of the following types of privacy problems are caused by outsiders, others can be caused by your online habits or by those of your child.

#### **Fraudulent Schemes**

There are several kinds of fraudulent schemes where obtaining privacy-related information is just the first step of a possible crime. Some examples include the following:

**Credit card fraud:** This is any kind of a scheme where the criminal gets someone to volunteer credit card information in order to make bogus or unauthorized charges.

**Identity theft:** The unauthorized use of personal information in order to take on the identity of another person.

**Other scams and cons:** There are a number of other criminal schemes where the goal of the criminal is to gain the confidence of someone over a period of time before the actual crime occurs. These kinds of threats are usually aimed at adults rather than children. Examples include fake lotteries, bogus requests to help transfer funds to a bank account, and stock investing schemes.

**Pharming:** This is a technique used by identity thieves and other criminals in which incoming traffic is redirected from a legitimate web site to a fake site, where the potential victim is then encouraged to provide personal or financial information.

**Phishing:** This is a technique by which a bogus email, web site, or popup message appears to be a legitimate request for private information such as your name, Social Security number, or online account information.

#### **Hardware Issues**

Privacy may be compromised if the personal data stored on a computer is stolen or if the computer is given away or sold to with personal data still on the hard drive. Similar risks exist for lost or stolen data on portable storage media such as a CD-ROM or a flash drive.

#### **Intrusive or Excessive Advertising**

One way advertisers control the type or amount of advertising that you or your child may see on a web site is through the use of cookies. These are small text files that a web site

you are visiting places on your computer. They allow your browser to retain information about your web site visit. When you make a return visit, the web site may show specific advertising based on the data in the cookie.

Another way advertising may intrude on your online experience is through a popup. This is a type of browser window that automatically appears on top of the current browser window during a visit to a particular web page. Poppers do not by themselves cause harm, but they are often associated with aggressive advertising methods.

### **Personal Data in Your Software**

Many of the programs on your personal computer may allow you to add personal information such as your name, address, and telephone number. Each time you send someone a file, that data is also included.

### **Hazards of Home Wireless Networks**

Unless you have taken the time to secure your wireless network, anyone with a wireless-ready computer will be able to use it, including hackers who may use that connection to access the information on your computer. Also, if an unauthorized person uses your network to access the Internet, commit a crime, or perform activities that violate your ISP's terms of service, your ISP may take actions to freeze or cancel your account.

### **Malicious Software Threats**

Malicious software is any software designed to cause harm to a computer or the person using it. There are two general types of malicious software that may cause you to lose control over your personal information or that allow intrusive advertising on your computer:

**Adware:** This type of software allows advertising to appear while you are online and possibly when you are not online.

**Spyware:** This kind of software collects data about your computer and your online activities and sends the information to someone else without your permission or knowledge.

### **Personal Behavior**

Online habits and personal computer habits can directly affect the privacy risks that you and your family may face. Some of the more common risks that are due to personal behavior include the following:

**Not sending sensitive data in a secure way:** The most sensitive kind of personal data is the kind that can lead to identity theft and financial loss.

**Publicly displaying personal information:** Some services encourage users to place personal data onto a web page. Once there, this information is available to anyone who wishes to see it.

**Responding to requests for personal information:** You and your child will likely receive requests for personal information. If there is no way to verify that a request is legitimate, responding in any way may lead to privacy problems.

**Volunteering personal information:** Although you may be asked to provide personal information when using an online service or registering a product, there is usually no requirement to do so. Once you give out this information, it may be used to direct

advertising and unsolicited offers to you or to your child.

### **How Much Privacy Should a Child Have?**

You should take all reasonable steps to allow your child some personal privacy, but you should always be able to get access to any of your child's online accounts and to any data in a computer or in a portable storage device.

### **Key Realities About Privacy**

If you are always at your child's side when he or she is online, privacy will not be an issue since you will have complete control over any online activities. An older child may resist this kind of parental access, but any argument your child may give you has to be considered in light of the following realities:

**No one has total privacy online:** Just about any email, instant message, or other communication has to pass through an ISP, and will also likely pass through several computer systems on the journey between the sender and receiver. Your ISP can also keep records of every site you or your child may visit.

**Parents are responsible for their child's safety:** Every child should have the ability to keep some things private, and parents should respect those needs. However, when it comes to issues involving a child's online behavior or personal safety, parents have a responsibility to intervene.

**Privacy is not the same as secrecy:** Parents and children must learn how to respect each other's privacy. However, the role of a parent will always be different from the role of a child. If a parent needs to go into a child's room, the parent may out of respect for the child knock on the door and ask to enter, but if a child says no, a responsible parent will still go in. Ultimately, children do not have the right to keep information secret from their parents if the parents have a legitimate need to know.

### **Seven Steps to Online Privacy**

Prevention is your best option for establishing control of private information and curbing excessive intrusions into your online experience. Many of the current threats can be addressed with a combination of appropriate technology and sensible online and offline behavior. The technology component of privacy involves both your home computer and the online services you may use. Your family's online behavior contributes to your privacy by steering you away from situations that put privacy at risk. You and your family should heed the following suggestions to enhance your privacy:

1. Develop a family privacy protection plan.
2. Set up your hardware and software to limit or prevent unauthorized activity.
3. Add software designed to protect your privacy.
4. Adopt online habits that protect your personal and private information.
5. Create and use an online alias.
6. Respond appropriately to information requests.
7. Regularly review your family's online activities.

### **Step 1: Have a Family Privacy Protection Plan**

Chapter 2 discussed the role of your child's written Internet use agreement and how it forms the foundation of how you and your child will deal with online issues. Appendix 3

provides an example of a basic agreement for a child who will only be online with a parent and another example of an agreement for a child who can go online alone. The following elements should be included in the agreement if your child will only be online if supervised by you or by another adult:

- I will not go online alone. If I am online, I must be with a parent or another responsible person.
- If my parents say that I can't do something on the computer, I will obey them.
- If your child is allowed to go online alone, the agreement should include the following:
  - I will not give out my name, address, telephone number, or any other personal information about my family or myself to anyone online without my parents' permission.
  - I will not hide anything about what I do online from my parents. If my parents ask, I will let them look at any file I have on any computer, in any online account, or on any data storage device.
  - I will not order or buy anything online without getting my parents' permission.
  - I will not post anything online without my parents' permission.
  - I will not download any file without getting my parents' permission.
  - I will not send a picture or other file to anyone else unless I get my parents' permission.
  - I will tell my parents the user name, password, or any other information they need to get into any online account or online service that I have.

## **Step 2: Set Up Your Hardware and Software**

The typical home computer system has privacy-related features that have to be activated in order to be effective. Activating these features will not prevent all privacy-related problems, but it could make your family's online experience more enjoyable by limiting some kinds of privacy hazards. There are at least three kinds of changes you can make to your system:

- Use the privacy options included in your browser to control how cookies and popups are handled.
- Set up your wireless network by turning on privacy features that will make it more difficult for people outside your family to access your system.
- Ensure that the applications on your computer do not include privacy-related information in files created or edited by those programs.

### ***Protect Your Home Wireless Network***

Performing any of the following steps will help you maintain your privacy when using a wireless network, and performing all of the steps will help even more.

**Change the router's user name and password:** Use something other than the default user name and password in order to make it harder for a hacker to access your system.

**Control access with a user name and password:** Most wireless routers allow you assign a user name and password to limit who can access your network. Change the

default user name to a unique user name. For added protection, set it up to require a password for access.

**Turn off identifier broadcasting:** Hackers near your home can use identifier broadcasting to locate unprotected wireless networks. Disable this mechanism if your wireless router allows it.

**Turn off wireless network when not in use:** If you will not be using your wireless network for an extended period of time, turn it off or disconnect it. Hackers are unable to gain unauthorized wireless access to your computers if the wireless network is not operating.

**Use encryption:** The most effective way to secure your wireless network from intruders is to encrypt, or scramble, communications over the network. Typically, the default setting is to have this system turned off. Follow the directions included with your wireless router, or the product support information on the manufacturer's web site, to turn on encryption. Turning on encryption will allow access only to users with the proper user names and passwords. If your wireless router doesn't have an encryption feature, consider getting one that does. Two main types of encryption are available: Wired Equivalent Privacy (WEP) and the more secure Wi-Fi Protected Access (WPA). Your computer, router, and other equipment must use the same encryption.

**Be careful away from home:** If you are accessing the Internet through a public hot spot, do not use this connection for anything involving sensitive private information.

### ***Remove Privacy Data from Your Programs and Online Services***

Applications on your home computer may or services that are hosted online allow you to add personal information such as a name or address. Each time a file or online record is created, that information becomes part of that file. For every program or online service you use to create files that are then sent to others, make sure the programs or services are set up so no unnecessary personal information is sent out.

### ***Review Email Signature Files***

Most email programs allow you to create a signature file that automatically adds a signature block to the end of any outgoing email. Be sure that you do not have any sensitive information in this signature file. For example, there is usually no need to add your full name, address, and telephone number on all outgoing emails.

### **Step 3: Add Software to Protect Privacy**

The previous section discussed how to set up your operating system, browser, and email program to help protect your family's privacy. This section will describe how additional software can enhance that protection by addressing risks caused by malicious software.

### ***Dealing With Malicious Software***

Malicious software can enter your computer as a result of visiting a web site, from a file attached to an email, from a portable data storage device, or from a variety of other routes. There are three general types of software that can protect your computer by either preventing malicious software from loading on your computer, or by finding and removing malicious software that does make it to your computer:

**Antispyware:** Software designed to detect or remove spyware, or to prevent spyware from being installed.

**Antivirus:** Software designed to either prevent viruses from invading a computer, or to remove viruses already residing on a computer.

**Firewall:** Software that controls communications between a personal computer and the Internet and prevents unauthorized access to that computer.

Malicious software represents a threat that continues to evolve. To keep ahead of this evolution, make sure your operating system, browser, and any additional protective software is updated regularly.

### *Filter External Content in Your Email*

Emails are commonly written in plain text or in HTML, which is a computer language used to control how a browser displays a web page. When you open an email formatted in HTML, it will behave like a web page and load images and other external content. This may be a privacy concern if the external content allows a malicious program to attack your computer. To open formatted emails without loading graphics or other external content, set up your email program so that images and other external content is not automatically loaded when you open an HTML email.

### *Other Options for Protecting Your Computer*

Appendix 1 lists a number of free software packages that can supplement the protection that may already be built into your computer's operating system. That appendix includes listings for programs to block, find, or eliminate viruses, spyware, and other threats to your computer. Appendix 2 has a number of free online privacy resources and privacy-related information. In addition to the resources in this book, you can also check the following resources:

**Software vendors:** You may want to compare other options by reviewing consumer-oriented computer magazines or web sites that rate and compare software. Appendix 2 describes two such sites, Download.com and Sourceforge.net.

**Your computer manufacturer:** If you are buying a new computer, check with the manufacturer to see if protective software is included with your purchase.

**Your Internet service provider:** Check with your Internet service provider to see if antispyware, firewall, antivirus, or other protective software is offered with your service.

### **Step 4: Adopt Habits That Protect Privacy**

The earlier sections of this chapter dealt with developing a family privacy policy, making a home wireless system more secure, and either setting up or adding software to help maintain your family's privacy. These efforts would be wasted if your family does not practice good privacy habits. It is up to you and your child to avoid behavior that allows privacy-related information from escaping your family's control.

Good privacy habits are based on common sense. Parents have the responsibilities of providing guidance with respect to private and personal information, monitoring a child's habits, and making appropriate suggestions or changes. The following three habits should be a central part of any family's efforts to maintain online privacy:

- Creating family privacy rules.
- Managing user names and screen names.
- Creating and managing passwords.

### ***Creating Family Privacy Rules***

In addition to having your child sign an Internet use agreement that has general rules about online behavior, you should also have rules for specific situations. The following suggestions cover several common privacy-related situations, and you may also add your own rules to cover other situations that may affect you or your child:

**Joining mailing lists:** Your child should get your permission before signing up for any mailing list. A mailing list is a managed list of email addresses and other personal information that is used by an individual or organization when sending email. You should review the first few mailings to make sure the content is acceptable to you.

**Responding to suspicious requests:** Teach your child not to respond to suspicious requests and to inform you when this kind of request arrives.

**Sending or publishing personal information:** Your child should always first get your approval before putting any personal information online. You should also minimize the amount of online personal information about your child.

**Sending sensitive information:** An adult should be directly involved in this kind of transaction. Unless you are certain you can send data securely online, use a safe offline method like regular mail.

**Signing up for online services:** Your child should get your permission before signing up for any online service that requires any information beyond a user name or password.

**Using instant messaging (IM) or chat rooms:** The best kind of screen name for your child is one that gives no clues as to identity, location, age, or gender. In addition, your child should avoid including any personal or private information in an IM or chat room conversation.

**Visiting web sites:** Your child must first get your permission before sending any personal information to a web site.

**Volunteering personal information:** Your child should never volunteer any personal information.

**What to do when in doubt or confused:** Instruct your child not to send any message or post anything online if there are any doubts about doing so, or if the situation is confusing to your child.

### ***Managing User Names and Screen Names***

User names and screen names often represent the public face of a user's online activities. For example, for many online email accounts, the user name is the same as the portion of the email that comes before the "@" symbol. For services like IM, your child's screen name should be the only identification others should see, and it should be the only name your child uses if the conversation involves a stranger.

The one basic rule for user names and screen names is that they should contain no

personal information such as name, age, gender, location, or affiliations. If your child's user name or screen name includes any identifying information about her, you or she should create a name that does not contain this type of information.

Your child will probably need user names or screen names for several online activities, and a sensible approach is to create a unique user name for each activity that uses private or sensitive information. Some examples include a Web-based email account, a school account, or a public library account. For an activity that has no sensitive data and that only requires a user name and password, it is safe to use the same user name in multiple places.

### ***Remembering User Names and Screen Names***

Keeping track of all the user names, screen names, and other information about every online service your child may use can be a nightmare. An easy way to manage all of this information together is to write it down and keep it with your family's Internet use agreements. You can use the "List of Online Activities" form that is included in the Family Forms Pack file located at [forms.speedbrake.com](http://forms.speedbrake.com).

### ***Creating and Managing Passwords***

Passwords are an important tool for maintaining online privacy. It should not take a lot of time to create appropriate passwords or to keep track of them once they have been created.

### ***How Strong Should a Password Be?***

If a password is for an account that can be easily replaced and contains no sensitive information, the password can be something easy to remember. Otherwise, a strong password is appropriate.

### ***Creating a Basic Password***

A basic password has one or more of the following characteristics:

- All characters are either upper case or lower case.
- It can be found in a dictionary or reference book.
- It consists of a string of identical characters.
- It is the name of a person, place, or event.
- It is the same as the user name or screen name.

Although you can use the same basic password with several online accounts, you may want to create different basic passwords for each person in your family.

### ***Creating a Strong Password***

A strong password is one that would be very hard to guess, but very easy to create or to remember. One method for making a strong password is to take a word that is easy for you to remember, substitute some of the letters with numbers and special characters, and capitalize at least one letter. For example, take the word parents. With a few changes, it can become p@R&nt\$ or perhaps p&r3N?z.

Another method for creating a password that is even harder to guess is to take a favorite



title, quotation, or line of poetry, write down the first letter of the first few words, and then substitute some of the letters in the resulting string of characters. For example, one of the most famous Shakespeare quotations, “To be, or not to be, that is the question,” has ten words. The first letters from the first six words are tbontb. With a little imagination, you could take those six characters and turn them into something like 2B0#tb or even tbR@2b.

### ***Keeping Track of Passwords***

You can keep track of passwords the same way you keep track of user names and screen names. Keeping them stored electronically may be an option, but it is a good idea to keep a copy of this information on paper as well. You can do this using the “List of Online Activities” in the Family Forms Pack at [forms.speedbrake.com](http://forms.speedbrake.com).

### **Step 5: Create and Use an Online Alias**

One of the great advantages of the Internet is that you can participate in most online activities without revealing your identity. Some of those obvious exceptions would be transactions that require your legal name such as any dealings you may have with a bank, an airline, or your child’s school.

### ***Should You Use an Online Alias?***

If you are legally obligated to provide true information about yourself, it would be wrong and possibly a crime to provide something other than true information. For just about any other online activity, if the service provider has no need to know your true identity, then do not provide it. If the answer to the next two questions is “no,” feel free to use an online alias:

- Are you legally required to provide information about yourself?
- Would anyone suffer any kind of loss if you did not provide true personal information?

### ***What Should Be in an Online Alias?***

An online alias should consist of the kind of personal information that providers of online services typically ask of new users. If you can, leave as many of these fields blank as possible. If you have to enter some information, you may want to consider using some of these suggested alternatives:

**Name:** A single letter or a string of random letters

**Address:** 123 Main Street

**City:** Beverly Hills

**State:** CA (California)

**Zip code:** 90210

**Telephone:** 310-555-1234

**Year of birth:** 1908

**Income:** Pick something in the low range

The example alias given above was not created out of thin air, but rather from my own experience. In all the times I have used some or all of this alias to register for various free online services, it was rejected only one time. The automated registration process of one online service recognized the street as not being one from Beverly Hills and was not

satisfied until I provided an actual Beverly Hills street name.

### **Step 6: Respond Carefully to Requests**

There are two kinds of online requests for personal information, the kind where there is a prior relationship with the requesting organization or individual and the kind where there is no prior relationship. For the first type of request, determine if the request is legitimate. If it is, respond using whatever communication method you typically use for that requester. If it is the second type of request, you should first determine if the request is legitimate. You also have to decide how to communicate private information reliably and securely. Typical options are communicating by regular mail, by phone, or by a secure web page.

It makes sense to be careful when responding, since a fraudulent request can be made to look like it came from a legitimate source. Recognizing the characteristics of a fraudulent request is the first step to protecting your family from a potential loss of privacy.

#### *Characteristics of Fraudulent Requests*

The messages that are more likely to be bogus are those that have one or more of the following characteristics:

- It contains a financial offer that is inappropriate to the recipient, for example a child receiving a credit card or mortgage refinancing offer.
- Something about the request makes you or your child feel uncomfortable.
- The message has several grammatical and spelling errors.
- The request appears to originate from a country where you and your child have no previous business or personal relationships.
- The request claims that personal information is needed to fix a problem.
- The request was contained in a popup.
- The subject line is blank, is in lowercase letters, is in an unfamiliar language, or doesn't make sense.
- There is an offer or promise of a high-value coupon or prize, or a significant amount of money in exchange for providing personal information.
- You are directed to visit a URL (a web site address) in order to provide personal information.
- You are requested to provide a password.
- You or your child are asked to provide sensitive personal information such as your full name, birth date, or Social Security number.

#### *How To Check if a Message Is Legitimate*

Just because a request has fraudulent characteristics does not make it a fraudulent request. If you believe that it is a legitimate request, then your response will depend on the kind of request. The following are a few examples:

**Email requests that ask you to visit a URL:** If an email appears to be from an organization or individual with a prior relationship to you, and asks that you go to a particular URL, do not do so. Instead, contact the source directly to confirm that the

request is legitimate. Do this using the same means you normally use to make contact.

**Request made by a web site:** If you are asked to submit sensitive personal information through a web page, look at the URL. It should look like a legitimate URL. For example, if you think that the URL should end with yourbank.com and instead ends with something else like yourbank.xyz.com or yourbank.ru, then you should not submit any information. The URL should also begin with https:// rather than http://. Data sent from a page that has a URL that begins with https:// is encrypted, so only the intended recipient should be able to read the data.

**Request mentioning a problem with an account:** If the message appears to be from an organization where you have some kind of account, do use any of the addresses provided in the message. Instead, contact that organization in the way you normally do and check on the status of that account.

**Requests to send money to someone in trouble:** If the message asks you to send money to a stranger to deal with some kind of unexpected emergency, ignore the email. If the request is from someone you know don't do anything (especially follow any links in the email) until you confirm that the emergency is real. Because the email account that sent the message may have been improperly used by someone, you should first contact the sender using something other than that email address to confirm the facts of the story.

### ***Requests Directed at Children***

Make it clear to your child that you should be informed any time she receives an online request for information, and should respond only if you have given approval. Your child should also tell you if she receives a request to contact someone by phone or to meet in person.

### **Step 7: Review Your Family's Activities**

No matter how many privacy rules you may have in place, your child may still have too much private and personal information available online. You can reduce your child's risks by regularly reviewing her online activities. You can use the "List of Online Activities" from the Family Forms Pack as a checklist, making note of any changes that should be made. A few examples of the things you may have to correct include the following:

- Having inappropriate people in an email address book or on a list of contacts in an online account.
- Not using a strong password on an account with sensitive information.
- Placing too much personal information about any family member in a web site.
- Placing too much personal information in the user profile section of any online service.
- Using passwords, user names, or screen names that contain personal information such as birth year, name, address, or gender.

### **Recognizing A Privacy Problem**

Even if you implement all of the recommended actions in this chapter, you can still have privacy problems. The following is just a partial list of the kinds of things that could

signal a privacy problem:

- A computer or any storage device with sensitive files is lost, stolen, or damaged.
- Files or programs are mysteriously missing, damaged, or altered.
- New software has been loaded on the computer without your approval.
- Sudden changes appear in your child's behavior or online activity.
- You discover that your child has placed sensitive personal information on a publicly accessible web page or web site.
- You discover that your child is providing personal data or photos to someone without your approval.
- You receive email or other communications from a person you do not know, and the messages indicate that the person knows quite a bit about you or your family.

#### **Top 10 Privacy Protection Tips**

1. Make protecting privacy a regular part of your family's online habits.
2. Use your wireless network's security features.
3. Use your browser to control cookies and popups.
4. Use privacy protection software, including firewall, antivirus, and antispyware programs.
5. Regularly update your operating system and privacy protection software.
6. Keep a written record of every family member's passwords, user names, and other information needed to access any computer or online service.
7. Learn how to create passwords that are hard to guess, but easy to remember.
8. Do not volunteer personal information.
9. Use an online alias whenever it is appropriate.
10. Regularly review your family's online activities and address any potential security problems.

[Back to Table of Contents](#)



## CHAPTER 5: SECURITY ONLINE

### In This Chapter

- What Does Security Mean?
- Key Security-related Threats
- Seven Steps to Online Security
- Recognizing a Security Problem
- Top 10 Security Protection Tips

**B**ecause going online is a normal, everyday activity for people from all walks of life, it should be no surprise that just as in the offline world, there is a small percentage of people online who are up to no good; trying to break into your computer, steal your money, or damage your data. Many online security threats can be avoided using a combination of savvy personal behavior and appropriate technology. As was the case with the privacy issues discussed in the previous chapter, the key to addressing security issues is to encourage behavior in your child that minimizes security risks, and that gets your child into the habit of staying safe online.

### What Does Security Mean?

One useful definition of online security is the ability to identify, manage, or eliminate threats to information, to technology, or to the well-being of a group or individual. For your family, those threats include attempts to steal, damage, or disable your home computer; attempts to steal the information in your computer or data storage device, and attempts to physically or psychologically harm your child.

### Why Online Security Is Important

Identifying, reducing, or eliminating potential online threats to your child is important because of the potential consequences if those threats become real. Just as was the case with online privacy, a child who is new to the Internet and has not yet developed the judgment and skills to avoid dangerous situations is at the greatest risk. Some of the online security hazards your child may face include the following:

- Attempts by strangers to meet with a child.
- Attempts to destroy or steal information.
- Attempts to fraudulently obtain passwords, user names, or other security data.
- Online contacts with potential child predators.
- Unauthorized access to an online account.

### Relationship Of Privacy to Security

Internet security issues are often closely related to Internet privacy issues. Many potential online security problems begin as privacy problems and may later develop into security problems. For example, whenever someone has unauthorized access to a computer, there is a privacy problem because that person has access to all of the information on the computer. It is a potential security issue because any data on that computer can now be copied, changed, or destroyed. Privacy and security are also related because the tools, techniques, and habits that reduce or eliminate privacy threats can also reduce or eliminate many potential security threats.

### Examples of Security-Related Information

The most valuable security-related information is any information that can give a criminal, child predator, or other undesirable person access to your personal data, to your computer, or to your child. Some of the items on the following list are also featured in chapter 4:

- Critical data in your computer, in your data storage devices, or in one of your online accounts.
- Current address or phone number.
- Lifestyle information such as travel schedules, group affiliations, clubs, favorite activities, and details about personal relationships.
- Salary, credit card information, bank account details, and other financial data.
- User names, passwords, or other data needed to access computers, computer networks, or online services.

### **Examples of Security-Related Problems**

Most of security problems, even those that are hardware oriented, start with the actions of your child or of another family member.

**Arranging to meet strangers:** This is a particularly worrisome security problem for families, since there are many predators who use the Internet to arrange meetings with potential victims.

**Being careless with equipment:** Your child should know how to properly operate and care for any computer system in your home, especially basic tasks such as the proper procedures for turning the system on or shutting the system down.

**High-risk online behavior:** There are some online activities; for example, using chat rooms and webcams, that attract the wrong kind of attention, especially if children are involved. According to the FBI, child predators often use these tools to evaluate their potential victims.

**Not backing up data:** Any information that is on a hard drive may be lost or damaged for any number of reasons. Regularly backing up data is a very easy way to prevent this problem.

**Responding to information requests:** This is the same kind of threat that was described in the privacy chapter. Fraudulent requests for passwords and other personal information may lead to a security problem, so you and your child should be aware of how to respond to these kinds of requests.

### **Key Security-related Threats**

As was the case with risks to privacy, security risks can be divided into three broad categories: those that are caused by personal behavior, those that are caused by hardware or software, and those that are due to a combination of the first two categories. The following sections describe a variety security threats from these three categories.

#### **Fraudulent Schemes**

These are the same schemes that were described in the privacy chapter. It is a privacy issue if you lose control of your personal information. It becomes a security issue if that information is used against you or your child. For a detailed description of common fraudulent schemes and specific steps you and your family can take to address this class

of online problems, please review chapter 4.

### **Hardware and Software Security Issues**

Hardware-related security issues include all the privacy-related issues covered in the previous chapter, and they also include the challenges of controlling access to your family's data and making sure the data is not lost, damaged, or destroyed. Software issues are for the most part the same as what were described in chapter 4. There are some additional security concerns where software plays a role, and the following list provides a brief overview of those concerns:

**File sharing software:** This class of software allows users to transfer files from one personal computer to another. If this software is on your computer, it could allow anyone on the Internet to access any file on your computer. You should keep this kind of software off your computer and remove it if already installed.

**Hard drives and portable storage media:** Security may be compromised if personal data that is stored on a personal computer is stolen or if the computer is given away or sold with your family's personal data still on the hard drive. Also, you should take steps to ensure that portable storage media such as CD-ROMs or flash drives are not lost or stolen.

**Lost or stolen computers:** You can keep a lost or stolen computer from becoming a security disaster by making sure you have backup copies of key data and by keeping as little sensitive information on your family's computer as possible.

### **Laptop Security and Airline Travel**

For years, airline travel with a laptop has meant exposing your computer to theft and damage every time you take it out for a security inspection. Your laptop is especially vulnerable if you are taken aside for additional screening and your laptop is out of your sight. Make it a habit to prepare your laptop before you fly. Erase any files with sensitive data. Copy the critical files that need to travel with you and keep them in a flash drive or other data storage device that is packed separately from your laptop's carrying case.

### **Online Habits That Reduce Risk**

Your child's online habits can directly affect the security risks that you and your family may face. Some of the habits that reduce risks include the following:

**Backing up data:** There is an old saying in the computer industry that there are two kinds of users, those who have lost data and those who will. Losing data will happen, but if you and your child make backing up your files a regular habit, most of your data will always be safe.

**Keeping track of software:** Having a process for deciding what software is added to your computer is one way to keep inappropriate or potentially malicious software from being installed.

**Keeping track of data:** It is easy to keep track of data when it is stored on a computer. When you or your child store files in other places such as a flash drive or CD-ROM, you have to make the effort to keep track of the data or you will risk losing it.

**Protecting computers and accessories:** Computers do not respond well to rough treatment. You have to make sure that everyone in the family understands how to take

care of computers, printers, displays, and other devices and what to do to reduce the risks of accidental damage.

**Verifying requests for information:** Your family should have a process for verifying that any request for information is a legitimate one.

### **Seven Steps to Online Security**

Prevention is the best way to deal with security concerns. Many threats can be addressed using a combination of appropriate technology and sensible online behavior. The appropriate technology involves your personal computer hardware and software. Online behavior contributes to security by steering your family away from risky situations. The following general actions should help your family become more secure online:

1. Develop a family plan.
2. Set up your family's computer system to ensure its physical security.
3. Add software designed to protect your computer and computer data from unauthorized access.
4. Develop a process for managing the software on your computer.
5. Develop a process for regularly backing up data.
6. Develop a process for keeping track of data that is outside the computer.
7. Develop a process for regularly reviewing your family's online security efforts.

#### **Step 1: Have A Family Security Protection Plan**

Chapter 2 discusses using a formal Internet use agreement with your child to outline how an agreement forms the foundation of your child's relationship with the Internet. If you allow your child to be online alone, the following should be included in the agreement:

- I will not install any software on any computer without getting my parents' permission.
- I will not open any file sent to me unless I get my parents' permission.
- I will allow my parents to access any account or look at any of my data any time they ask.
- I will not meet or agree to meet in person anyone I have only met online unless I have my parents' permission.
- I will be careful when I use the family's computer equipment.
- I will not let someone else use any of the family's computer equipment, without first getting my parent's permission.

#### **Step 2: Set Up Your Hardware**

Hardware security is mostly basic physical security. The following suggestions will take care of most potential threats to your hardware:

**Electrical issues:** Use a surge suppressor for your computer system. This device protects electronic devices from unexpected changes in voltage. These surges may be caused by appliances in the home being turned on or off, or from problems in the local power grid.

**Food and drink:** Eating or drinking in the area around the computer is never a good



idea.

**Hardware setup:** Make sure the computer, printer, and other components are set up so they are not a trip hazard and will not be bumped or hit during routine household activities.

### *Disposing of Old Computers*

The hard drive on your old computer probably contains thousands of files of every description. While you could erase the files, there is no guarantee that you will get rid of all of the data. There are options for disposing of a computer that will give you more control over your older data:

**Destroy the hard drive:** If the computer can no longer be used, carefully take out the hard drive and damage it to the point that it can no longer be read. Keep in mind that a computer contains hazardous materials, and in most communities you must follow special procedures to dispose of computers and computer components.

**Recycle everything but the hard drive:** In some communities, you may be able to donate computer components to a nonprofit organization that will then recycle any useable parts. If you want to do this, remove the hard drive before you donate your computer. Afterwards, you can either keep the hard drive or destroy it.

**Find other uses for it:** You may be able to find useful tasks for the computer around the house. For example, You can keep the computer offline and use it for various tasks. If your child has developed the maturity and judgment needed to be online alone, let her use the computer to work online. If not, then only allow her to use the computer offline.

**Keep the computer:** If you can find no other use for the computer, and it is still functioning normally, keep it as a backup.

### **Step 3: Adding Software Protection**

The protective software discussed in chapter 4 is also effective for preventing security issues caused by malicious software.

### **Step 4: Manage the Software on The Computer**

Once you have a computer in your home, you or your child will want to add software to enhance the computer's capability and improve your online experience. A useful software management process has to have, at minimum, the following parts:

**Approval process:** Parents should be responsible for deciding if a program should be added to or removed from the computer.

**Evaluation process:** Before allowing new software on the family computer, find out if there have been any serious issues with the software. Web sites that evaluate software are described in the "Computer and Internet Resources" section of appendix 2.

**Record-keeping process:** Review your computer's documentation to find out what programs are installed on your computer. You may also want to have that information written down. When a new program goes on the computer, keep track of it using the "List of Additional Software" form and put that form into the same notebook that has your family's Internet use agreements. You can find and download this by visiting [forms.speedbrake.com](http://forms.speedbrake.com).

### **Step 5: Have A Data Backup Process**

Regularly backing up your data, which involves making a copy of your important files and storing that copy separate from the computer, is probably the single most important thing that you can do to protect your data. You can always replace your hardware and software, but it may be impossible to replace data once it has been lost, stolen, or destroyed. Like exercising, the process is not too complicated, but getting into a regular habit can be an ongoing challenge. The following suggestions should make it easier:

- Choose a family data manager: This person should make sure all data is backed up and stored in a safe place.
- Decide on data storage technology: There are several hardware choices for storing backed-up data, including external hard drives, flash drives, DVD-ROMs, and CD-ROMs.
- Schedule a regular backup time: If you are not sure how often to back up data, do it monthly.

### **Step 6: Use a Data Tracking Process**

Once your family is in the habit of regularly backing up data, everyone must be able to keep track of where all the data resides. The person who is serving as the family data manager should also be responsible for this.

**Keep a written record:** Use the “List of Data Storage Devices” that is part of the Family Forms Pack to keep track of where data is stored outside of your computer’s hard drive.

**Have a plan for securing sensitive data:** Sensitive data, such as medical records or financial records, should have a higher level of security than other files. The family data manager should decide if this data needs to have extra security, such as being kept in a locked file cabinet or even being stored outside of the home.

### **Step 7: Regularly Review Online Activities**

Any review of your family’s online security situation should include the seven-step privacy protection process described in chapter 4, as well as the following two activities:

- Confirm the location of all the items listed in the “List of Data Storage Devices.” Update the list to reflect any additions or changes.
- Using the “List of Additional Software,” make sure all the programs on your computer were approved by you. Remove any program that was not approved by you, or that no longer serves any useful purpose.

### **Recognizing A Security Problem**

Following the recommendations in this chapter is no guarantee that you and your family will be free of any security problems. Early signs of a security problem typically include activity or behavior that seems unusual, unexpected, or inappropriate. If you observe any of the following situations, you should take prompt action:

- Files or programs on your computer are mysteriously missing, damaged, or updated.
- A family member has unexplained or unusual bank or credit card.
- A stranger attempts to arrange a meeting with your child.

- New or unfamiliar software is mysteriously loaded on your computer.
- Your computer has been affected by a virus or other malicious software.
- Your child is installing new software without your knowledge or permission.
- Your computer or any storage device with sensitive files is lost, stolen, or damaged.
- Your computer starts to behave strangely.

### **Top 10 Security Protection Tips**

1. Make online and offline security a key part of your family's online habits.
2. Choose a family data manager who will track where the family's data is stored.
3. Back up data regularly.
4. Keep a written record of where data is stored.
5. Update your operating system software regularly.
6. Use security protection software programs and update them regularly.
7. Use software from reputable and reliable sources.
8. Take action if your computer starts to behave strangely.
9. Regularly review your family's online activities and address any potential security problems.
10. Either keep or destroy old hard drives.

[Back to Table of Contents](#)



## CHAPTER 6: INTERNET LEGAL AND ETHICAL ISSUES

### In This Chapter

- Copyrights and Trademarks
- Q&A About Copyright Issues
- Pornography and Free Speech
- Q&A About Pornography and Free Speech
- Defamation and Libel Online
- Online Piracy

Two things are true about the Internet. The first is that there are tremendous resources available for anyone to use and enjoy, and the second is that there are rules about how you and your child can use those resources. If these rules are not followed, there could be trouble with your child's school, with your ISP, or even with someone's lawyer.

This chapter will review some of the most important legal issues that you and your child may face when using the information and services available online. Knowing some basic things about these issues will help you make decisions that will keep anyone in your family from doing things that can cause problems.

Please note that this chapter, and for that matter the rest of the book, is not designed to provide any legal or professional advice. For further assistance on legal or other issues mentioned herein, please seek the services of a competent professional.

### Copyrights and Trademarks

Copyrights and trademarks are forms of intellectual property protection that allow the owners to control how protected material can be used. The following are the basic facts that you and your child should know:

- Copyrights can apply to written works, sound recordings, and visual works.
- If something is freely available online, your child does not need any permission to read it, view it, or listen to it.
- If your child wants to publish copyrighted or trademarked material in a web page or web site, then she would have to get permission to do so.
- Most of the information published online is also copyrighted.
- The owner of a copyright can control how a work can be used, copied, altered, or distributed.
- Trademarks can apply to the words, symbols, or designs that identify a product. A closely related concept, the service mark, applies to a service rather than a product.

### The Most Important Copyrighted Material

The copyrighted online material that should be of greatest concern to you is content that is protected by copyright and that your child may want to use in a web site, web page, or other online publication. Copyright owners of the following kinds of materials typically have restrictions about how their materials may be used and may take legal action if their content is used without permission:

- Books, newspapers, and magazines
- Music

- Videos

While it would be a violation to transmit or republish copyrighted material without permission, it is acceptable to provide readers with the URL of a copyrighted work.

### **Online Materials That Are Not Protected**

The following categories of material are not restricted and your child is free to use them in any way without getting anyone's permission:

**Facts and ideas:** The words, drawings, or pictures used to express facts and ideas can be copyrighted, but not the underlying ideas or facts.

**Government documents:** In the United States, almost anything published by local, state, or federal governments or their employees, including reports, films, and speeches, can be freely used.

**Material in the public domain:** This is intellectual property that has had its protection expire, could not meet requirements for protection, or was never protected before being released to the public.

**Older works:** In general, if the copyright holder of the work is a person who has been dead for more than 100 years, the work is in the public domain.

**Titles, words, slogans, and phrases:** These items are not protected by copyright, so you are free to use them. However, if a trademark or service mark is associated with a title, word, slogan, or phrase, you may have some limitations.

### **Fair Use and Copyrighted Material**

One of the most important aspects of copyright for your child to understand is the principle of fair use. This is the legal use of copyrighted material without the permission of the copyright holder. The principle of fair use allows your child to do the following with copyrighted material he may find online:

- Print or save a document for personal use.
- Read, view, or listen to material online.
- Use material for educational purposes.

This last example of fair use is the most important one for your child because it allows him to use protected material without charge if it is connected with schoolwork or research.

### **Q&A About Copyright Issues**

#### ***If it is already on the Internet, why can't I use it any way that I want?***

Unless you know the material is in the public domain or has an expired copyright, assume that it is copyright protected. The copyright owner has the freedom to place a work online and to allow the public to view the work. To do almost anything else, you need to get permission.

#### ***Can I use someone's music on my web site to help attract visitors or to help raise money for charity?***

Even if you are not making money from it or using it to raise money for charity, you still have to get permission to use a copyrighted work on your web site.

#### ***How do I know if something is copyrighted?***

The easy way is to look for a copyright notice. A common way to indicate copyright is to use a combination of a copyright symbol (the letter “c” inscribed in a circle), the year the work was first published, and the name of the copyright owner.

***What if I don't see any copyright notice?***

The work may still be protected by copyright since the notice is not required to be visible. If you want to republish part or all of that work, find the group or person who owns or controls the copyright and get permission to use it.

***What if I find that my work is being used on a web site without my permission?***

If you control the copyright to that work, and if it is being used in a way that you think does not meet the standards of fair use, you may want to request that it be removed. If the organization or person who is using your copyrighted work refuses, you can inform the company or ISP hosting that page that the use of the work is a copyright violation and request that the item be removed from the web site.

***Can I put one of Shakespeare's plays on my web site?***

You can place part or all of any of Shakespeare's words on your site because his work, like the work of most writers who have been dead for more than a century, is in the public domain.

***Can I take a song from my music collection and use it on my web page?***

In most cases, you would need to get permission. When you buy music, you have the right to listen to it, but not to republish it online unless the recording is in the public domain (rare for modern recordings) or if you have permission from the copyright holder.

***What if I just sample few seconds of a song on my site?***

It does not matter if it is just a few seconds. You would still need permission to use that copyrighted work.

***Why can't I find newer books on the Web?***

Most books that have been published in the last 100 years are still protected by copyright. For books published in the United States after 1977, the copyright expires 70 years after the death of the last surviving author.

***Do I need to get permission or pay someone to use something from a web site for a school assignment?***

No. The principle of fair use lets you use almost anything you want in a school assignment without first asking the copyright or trademark owner for permission. However, when you use someone else's work in your school project, you should clearly indicate the source of the information; for example, the URL.

***What about using some old NASA videos in a video that I want to put online?***

That would not be a problem. Most everything that is produced by a local, regional, state, or federal government organization in the United States is in the public domain. You can do whatever you want with it, even make money from it, and you do not have to obtain permission or pay anyone. Check with the government organization in question for any exceptions to these public domain rules.

***How can I use selections from this book?***

If you own a copy of my book, you are free to give it away or sell it to someone else. You can also use your own words to express any of the facts or ideas in this book and create a

web site, magazine article, or even a new book. If you want to do something that does not meet the standards for fair use, you will need my permission, as the copyright owner.

***Can I use a photo or video I took of my friend uploaded and put it in my blog?***

You can do it if you have their permission or their parent's permission, but use some common sense. If you took a picture of something that could embarrass your friend later, maybe you shouldn't put it online.

**Pornography and Free Speech**

The Internet was largely a creation of the government of the United States and the laws and traditions of the United States have heavily influenced the extent of information that your child can find online. The Constitution of the United States, specifically the First Amendment, states:

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

The First Amendment forms the basis of laws and traditions in the United States that are related to both online and traditional publishing. The most important tradition for online publishing is freedom of speech, which is the right to express opinions, information, or ideas in public or in private, regardless of content, without interference by a government. This free speech tradition includes allowing adults to view or transmit sexually oriented material on the Internet.

**What Is Pornography?**

Pornography is any material that is sexually explicit and that is intended to cause sexual arousal. Such material does not have to involve descriptions or depictions of nudity or sexual activity. In the United States, most forms of sexually explicit material are protected by the First Amendment, making it legal for adults to create, publish, or consume such material.

**Pornography and Obscenity**

Pornographic material is different from obscene material. Obscene material has been legally determined to be sexually explicit, offensive to conventional standards of decency, and lacking in serious literary, scientific, artistic, or political value. It also does not have First Amendment protection, so it is illegal for anyone in the United States to view, possess, publish, or transmit such material.

**Pornography And Child Pornography**

Like material that is considered to be obscene, material that is considered to be child pornography is illegal for anyone in the United States to view, possess, or publish. Child pornography is any kind of visual depiction of a person under the age of 18 engaged in sexually explicit conduct. The conduct does not have to involve either sexual acts or nudity.

**Accidental Exposure to Pornography**

It is unlikely that your child will ever be accidentally exposed to obscene material or child pornography. Law enforcement organizations and Internet service providers are very aggressive about keeping these kinds of materials off the Internet. Unfortunately,

most sexually explicit material is quite legal, and widely available online. What follows are a few examples of how your child may be accidentally exposed to this kind of content:

**Your child is sent an email containing sexually explicit images:** In the United States, if the sender did not know that the recipient was under the age of 18, then the sender likely did not violate any federal or state laws. Internet service providers may have stricter limitations on what kind of behavior is allowed. You may want to report the incident to your ISP to see what actions can be taken.

**Your child is sent a written message that contains sexually explicit language:** In the United States, sexually explicit writing has fewer restrictions than sexually explicit images. Unless there was some attempt to sexually solicit a child, it is likely that no law was broken. However, it may be worthwhile to at least report the incident to a service provider.

**A child follows a link to an adult web site:** So long as the material has not been declared legally obscene or does not involve child pornography, it is likely that no laws were broken.

Note that a link is a coded part of a web page that when selected takes the user to some other online resource. A link may appear as highlighted, colored, or underlined text, or as part of another element of a web page, such as a picture, logo, or some other graphical element.

### **Free Speech and Children**

As a parent, you are free to allow your child to have as much or as little free expression online as you want. Sensible restrictions include limits on the following:

- The kind of web sites that your child can visit.
- The kinds of videos your child may view.
- The language or vocabulary your child can use while online.
- The music, games, and other online entertainment options your child is allowed to enjoy.

### **Q&A About Pornography and Free Speech**

#### ***Why can't I say anything I want online?***

No country on earth, even countries with a long tradition of free speech, is without rules when it comes to what one can say or write. Beyond the laws that governments may enforce, ISPs and parents will also have rules about what is or what is not allowed online.

#### ***Do children have the same free speech rights as adults?***

No. Children can have many more restrictions on their free speech rights than adults. Parents are allowed to provide as little or as much freedom of speech as they want. In the United States, both schools and libraries that accept federal funding for their online activities are required to restrict what children can do online.

#### ***Can I keep pornographic email from being sent to me?***

Unfortunately, anyone with an email address can be sent unsolicited messages, including those containing adult-oriented material. Chapter 4 on privacy and chapter 9 on unwanted email have many suggestions for keeping such email to a minimum, but there is no way



to completely eliminate the problem.

### **Defamation and Libel Online**

Defamation is a legal term for a false statement that causes harm to someone's reputation, or that causes that person to become a target of public contempt, hatred, ridicule, or condemnation. Libel is defamation that is either written or broadcast.

#### **How This May Become a Problem**

Participating in rumors or gossip about the actions or behaviors of others is a normal occurrence among adults and children. When people talk to one another, the target of the conversation may be spoken of disparagingly, but there is usually nothing left behind to connect a false statement with any particular person. When that kind of statement is sent to others online, however, it can be very easy to connect a message with its sender, which could lead to the following kinds of problems:

- If your ISP gets complaints about messages that were sent from your account, then the ISP may suspend or cancel your service.
- Students who make or pass on false statements about other students or about staff members will likely face disciplinary actions such as loss of Internet privileges or suspension.
- The persons whose reputations are damaged by information sent or posted online may retaliate by bringing legal action.

#### **Ten Tips for Avoiding Online Defamation**

1. Assume that any message you or your child sends or publishes online will always be available.
2. Avoid sending jokes by email, especially if they are about a particular individual.
3. If someone sends or publishes something online about your child that is both untrue and upsetting, encourage your child to talk about it.
4. If you know the source of a message containing false statements about anyone in your family, make the ISP aware of the situation.
5. Avoid composing email while upset.
6. Don't email or publish embarrassing photos of anyone.
7. Avoid arguments and confrontations online.
8. Don't create or spread rumors or gossip online.
9. If your child discovers someone has used the Internet to spread rumors or lies about someone else, encourage your child to tell you about it.
10. If you have the slightest doubt about something you are about to do, then don't do it.

#### **Online Piracy**

Unlike centuries past, where piracy on the high seas was difficult and dangerous, online piracy is very easy. All it takes is the ability to copy or save a file. Quite simply, piracy is a kind of theft. It is the illegal or unauthorized copying, use, installation, or distribution of intellectual property such as software, videos, and music files. Your child does not have

to go online to make an unauthorized copy of a file, but doing so online is more likely to lead to problems because it is more likely that your ISP or the owner of the pirated property will notice.

### **Online Piracy Can Lead to Lawsuits**

The types of piracy most likely to cause problems for your child or for your family are the kinds where there is either a perceived or actual financial loss and the affected organization is willing to take action.

One of the most well-known examples of individual users being sued for acts of online piracy began in 2003 when the Recording Industry Association of America (RIAA), an organization representing the US recording industry, began suing thousands of people for allegedly using file sharing programs to download music illegally. Many settled out of court, sometimes paying thousands of dollars to avoid going to trial.

While this is an extreme case, it shows the potential problems that can happen when you allow someone in the family to download or copy files without permission. As is the case with privacy and security issues, having good online habits will help your family avoid many potential privacy problems.

### **Dealing With a Piracy at Home**

Dealing with piracy in your home is a three-step process:

1. Do not allow your child to download or copy a pirated program or file either at home or away from home.
2. Have a process for adding any files or software to your family's computers.
3. Uninstall any program and erase any file you find that was not legally acquired.

### **Options To Piracy**

Rather than simply saying no to piracy, you can talk with your child in order to find out why she wants a particular program or file. Perhaps you will find a satisfactory compromise, or perhaps you will decide she will not get that file or program. Either way, this kind of discussion leads to a more responsible use of the Internet by your child. Some options to piracy include the following:

- Purchasing the item from a legitimate source.
- Finding a free alternative to the desired item.
- Including the purchase of music or software in the regular family budget.

[Back to Table of Contents](#)



## CHAPTER 7: CYBERBULLIES AND CHILD PREDATORS

### In This Chapter

- Online Bullying
- Cyberbullying Warning Signs
- Top 10 Ways to Prevent Cyberbullying
- Child Predators and the Internet
- Law Enforcement Involvement
- Top 10 Tips for Avoiding Online Predators

There are several ways that your child can be harassed online, but the kinds of harassment that concern most parents are the kinds that could lead to psychological or physical harm. The two most likely sources of this kind of harm are cyberbullies and online child predators. Both kinds of harassers can be dealt with using some of the same approaches discussed in the chapters on privacy and security threats, and you can also fight these threats using the resources of your ISP, of your child's school, or of law enforcement.

### Online Bullying

School bullying existed long before the creation of the Internet. The objective of an online bully is no different than the objectives of a traditional bully; it is generally to make the victim feel intimidated or threatened. Online bullying is psychological rather than physical, and could range from activities such as gossiping and teasing, to more serious actions such as sexual, religious, or racial harassment.

### Definition of a Cyberbully

A person who is a cyberbully engages in repeated or coordinated cruel or harassing actions directed at an individual by means of email, IM, text message, blogs, web sites, or other online resources.

### Why Is Cyberbullying an Important Issue?

Parents should be concerned with this kind of harassment because it could have serious psychological effects on your child, and because threatening online behavior could escalate into more serious offline threats.

Learning to recognize cyberbullying behavior can help to protect your child from being a victim and can help you recognize if your child is becoming a perpetrator.

### Examples of Cyberbullying

Online bullying can take many forms, such as some of the following examples:

- Creating a web site, blog post, or other online publication that makes a person an object of ridicule.
- Damaging, destroying, or altering someone's data, files, programs, or online publications.
- Making threats by using email, a social media page, or some other online communication.
- Posting embarrassing photos of someone.
- Publicizing confidential personal information.

- Retaliating for other acts of bullying.
- Sending messages that are meant to be hurtful.
- Spreading rumors or gossip.

### **Cyberbullying Roles**

As with old-fashioned bullying, there are three ways your child may be involved in cyberbullying:

- As a victim
- As a perpetrator
- As a witness

While each kind of involvement may have different effects on your child, as a parent you have to be willing to take appropriate action whenever you recognize a potential problem.

### **Cyberbullying Warning Signs**

The early signs of cyberbullying are similar to the early signs of other online problems. Before jumping to conclusions, take the time to talk to your child and discover what may be happening. The following are some of the common warning signs:

- Avoiding friends or classmates.
- Significant change in mood.
- Spending much more or much less time online.
- Sudden changes in online or offline behavior.
- You find out that your child is either sending or receiving threatening or harassing messages.
- You find out that your child or someone your child knows is being bullied online.

### **Responding to Cyberbullying**

Unlike with threats to privacy and security, there is little you can do either through technology or personal online behavior to prevent your child from becoming a victim. However, there is plenty you can do to respond to an act of bullying.

**Talk to your child:** If you suspect there may be a problem, or if your child informs you about a cyberbullying situation, find out what you can about the situation, such as how long it has been occurring, and how the bullying took place.

**Gather and save relevant information:** Save copies of emails, web pages, or anything else proving that online bullying had taken place.

**Identify the source of the problem:** If you can, identify the source of the cyberbullying, such as email addresses and web site addresses. Also, ask your child if he knows who is responsible.

**Contact the appropriate organizations:** At the very least, you should contact any organization associated with the source of the cyberbullying, such as the service provider behind an email or a web page, or your child's school if a harassing message was sent from or to an account at the school.

**Take action:** You can do things such as asking an online service provider to remove a web page or block an email account. If appropriate, you may wish to contact your

child's school and request that disciplinary action be taken.

### **Eliminating Bullying Behavior**

Becoming a cyberbully is often not the result of one or two actions, but the result many small actions that may not seem significant at the time. For example, if your child makes fun of a classmate in an email and sends it to a second classmate, it represents a case of bad manners. If that second classmate sends copies of that message to the entire class, your child would be considered a cyberbully.

One of the best things you can do for your child is to encourage responsible online behavior, especially when it comes to talking about other people. A good start in that direction would be making sure your child follows the suggestions in the next section.

### **Top 10 Ways To Prevent Cyberbullying**

1. Don't encourage anyone to use the Internet to bully someone.
2. If you can't say something nice about someone in an email, IM, chat room, or anywhere else on the Internet, then don't say it at all.
3. Don't email or publish online any embarrassing photographs, videos, or audio recordings.
4. If you know that someone is being bullied online, tell someone.
5. Don't send emails or other online messages that threaten a person.
6. Don't send emails or other online messages that use foul or abusive language.
7. Don't send or post angry messages online.
8. Follow family rules about online behavior.
9. Follow school rules about online behavior.
10. If you receive a threatening or harassing message, tell someone, especially a teacher or parent.

### **Child Predators and the Internet**

Adults who harm children have been around long before the Internet was invented. However, the Internet allows a predator to be a threat to the girl next door, or to the boy on the other side of the continent. Predator behavior has not changed, but their methods have changed to adapt to the technology of the Internet.

Child predators are a real and potentially devastating threat, but there are many things you can do to reduce the risk to your family. Ample resources, including those of law enforcement, are also available to help parents deal with the potential threats.

### **Definition of a Child Predator**

A child predator is any adult who actively works to develop a personal relationship with a child in order to cause some future harm. This harm can come either from an inappropriate or illegal online or offline relationship.

While the greatest fear in the hearts of parents is from a predator who wants to physically meet a child in order to cause physical harm, your child may also suffer serious psychological harm from a purely online relationship.

### **Why Is This Issue Important?**

Online child predators are an important issue for you because the threat exists any time your child is online. It is also important because as a parent, you are in the best position to recognize the symptoms of predatory online behavior and to take action to protect your child.

### **Initial Child Predator Behavior**

Most child predators go through a process called grooming where the predator works over a period of time to gain the trust of a potential victim by first building a relationship using online communication tools such as email, chat rooms, and instant messaging. Early contacts with a child may not be at all suspicious, and it may take several contacts by email, IM, or other communication before the predator exhibits inappropriate behavior. The early warning signs may include one or more of the following:

- Arranging to make contact with your child either by phone or in person.
- Asking your child to keep a conversation or an online relationship a secret.
- Providing your child with some kind of online account in order to have private conversations.
- Requesting personal information from your child such as age, address, or school information.
- Requesting that a child send a picture.
- Sending your child letters, photographs, or gifts.

Your child should be discouraged from having these kinds of contacts, accepting gifts from strangers, or giving out private information, even though there is nothing illegal about these actions.

### **Advanced Child Predator Behavior**

If any one of the following situations occurs, it could indicate that a child predator is pursuing your child and that a crime may have already occurred:

**You discover your child engages in sexually explicit online conversations:** You should put a stop to any such conversations, and if you suspect an adult was involved, the appropriate authorities should be contacted.

**You find pornography or other sexually explicit material on a computer your child uses, or on one of your child's portable data storage devices:** Often predators provide pornography to potential victims as a means of starting sexually oriented discussions. If you believe that an adult sent the material to your child, contact the authorities and provide them with copies of any files.

**Your child receives phone calls from someone you don't know or the child is making calls to numbers you don't recognize:** You should put a stop to these kinds of calls, and find out as much as possible about the numbers called, the time and date of calls, and duration of calls. Your monthly billing statement may include these kinds of details.

**Your child calls someone known only through online contacts:** Potential child predators may provide contact numbers to your child, or may even provide a toll-free number or tell your child to call collect.

**Your child arranges to meet someone that he or she knows only from the Internet:** You should always be involved in any first-time meeting with anyone your child has met only online. A huge warning sign would be if the meeting involves any kind of travel. If you find out one day that your child has bus, train, or plane tickets to another city, or that your child expects a visitor from out of town, it is time for a serious talk.

**Your child turns the computer or the display off, changes the screen, or closes an application when you enter the room:** If you see this happening, ask your child for an explanation and then review any recent activity on the computer.

**Your child becomes withdrawn from friends, family, or normal activities:** Online predators sometimes work very hard at driving a wedge between children and their normal relationships. Children may also become withdrawn after sexual victimization or after having been exposed to disturbing information online.

### **Child Predator Preventive Actions**

It is difficult to use technology to block child predators because predators may use several online and offline methods of communication. Predators often seek to gain the trust of potential victims by building a relationship, a relationship that could take weeks or months to develop. Your most effective prevention method is to take the time to be involved with your child's online activities and to be on the lookout for suspicious activity. The following suggestions should help you keep your child from encountering problems from predators:

**Prohibit or closely supervise visits to chat rooms:** The Federal Bureau of Investigation (FBI) has found that most children who fall victim to online sexual predators spend large amounts of time online, particularly in chat rooms. Monitoring chat room activity means being with your child when she is in a chat room, or setting up your computer so all of her conversations can be reviewed later.

**Prohibit or closely supervise a child's use of IM:** Instant messaging shares many of the risks associated with a chat room, and should have similar restrictions.

**Closely supervise online contacts with strangers:** Whenever you find out that your child has any kind of ongoing communication with someone, talk to her and find out what the conversations are about. If the conversations or messages seem at all inappropriate, take steps to keep that person from contacting your child.

**Do not allow your child to arrange a phone call or a meeting with someone known only from online contacts:** An adult should make the first contact with strangers. For added security, phone calls should be made or received at a phone other than your home phone, and any face-to-face meeting should occur in a public place with many potential witnesses.

**Prohibit your child from sending personal photos to anyone without your permission:** This is a privacy issue and a child predator issue. Once a photo is sent out, you lose control over how that image may be used. Exchanging photos is part of the grooming process of many child predators and may escalate from normal photos to those that are highly inappropriate.

**Prohibit or closely supervise a child's use of a webcam:** A common tactic of online predators is to get the child to perform in front of a webcam. If someone only known

to your child from online contacts either encourages your child to use an available webcam or sends one as a gift, this should be considered a huge warning sign.

**Ensure that your child limits the amount of personal information shared online:** If you find that your child is giving personal information to strangers, make sure that she stops that behavior.

**Prohibit or closely supervise late night online activity:** According to the FBI, children are at the greatest risk from online predators during the evening. While offenders are online around the clock, most work during the day and spend their evenings online trying to locate and lure children.

### **Law Enforcement Involvement**

Should one or more of the following situations occur, immediately contact either a local or state law enforcement agency, or the local office of the FBI. The nonprofit National Center for Missing and Exploited Children has an online reporting service at <http://www.missingkids.com/>:

**Your child or anyone in the household has received child pornography:** Child pornography is any kind of visual depiction of a person under the age of 18 engaged in sexually explicit conduct. The conduct does not have to involve either sexual acts or nudity.

**Someone who knows your child is under the age of 18 sexually solicits your child:** This includes any situation where an adult makes a request to engage in sexual activity, has sexually oriented conversations, or makes requests for sexually oriented information.

**Someone who knows your child is under the age of 18 sends your child sexually explicit images:** Sexually explicit images include images that show actual or simulated sexual activity, or images that exhibit the genitals or pubic area in a lewd or provocative way.

**You find out that an adult has traveled or is planning to travel for the purpose of having sex with a minor:** In the United States, the FBI is particularly interested in cases involving traveling sexual predators. It does not matter if this person was planning to meet your child or planning to meet another child.

If any of the above situations occur, log out of any online service you are using and shut the computer down to preserve any evidence for future law enforcement use. Unless directed to do so by a law enforcement agency, do not attempt to copy any of the images or the text found on the computer. If the event involved an online service such as an email account, avoid using that service again until law enforcement has had a chance to review any activity.

### **The FBI Innocent Images Initiative**

The FBI has enlisted the help of dozens of local, state, and national law enforcement organizations to combat online child pornography and child exploitation. Starting in 1995, the Innocent Images Initiative has targeted web sites, individuals, and organizations involved in the criminal exploitation of children.

Since 2004, over a dozen national and international law enforcement agencies from four continents have worked directly with the FBI to deal with child sexual exploitation. This



program has a high profile within the United States, with four Innocent Images Initiative suspects having been placed on the FBI's Ten Most Wanted Fugitives list since 2000.

### **Top 10 Tips for Avoiding Online Predators**

1. Talk with your child about the potential dangers of online child predators.
2. Spend time together when your child is online to become familiar with your child's online habits.
3. Arrange the computers in your home so that the screen is visible to other members of the family.
4. Encourage your child to tell you if he or she is ever made uncomfortable or scared by something experienced online.
5. Make sure you have the user names, passwords, and other information needed to review any of your child's online activities.
6. Occasionally review your child's online activities, including the contents of any online accounts.
7. Occasionally review your child's use of offline communications such as telephones, cell phones, and regular mail.
8. Make sure your child understands your family's rules for being online, and that the rules apply at home and away from home.
9. Closely supervise any risky online activities such as chat rooms, file sharing, and webcams.
10. Immediately report suspected child predators to the appropriate law enforcement organization.

[Back to Table of Contents](#)



## CHAPTER 8: EMAIL BASICS

### In This Chapter

- An Overview of Email
- Email Etiquette
- The Gettysburg Criterion
- Top 10 Email Realities

Of all the applications on the Internet, email is the most popular, and perhaps the most important. If your child can master the basics of email, she will probably have a very easy time working with any other kind of online communication. One reason for email's importance is that it is an application that almost everyone who is online will use regularly. Included in this chapter are the following:

- A description of the basic parts of an email.
- A top ten list of tips for more effective email.
- Advice on when it is appropriate to either send or respond to email.
- An overview of email attachments and suggestions for how to use attachments effectively.
- A review of responsible email behavior.
- Examples of how to send email so the recipient clearly understands the message.

### An Overview of Email

Email is a generic term for messages composed and transmitted on a computer network. It can be accessed through a personal computer program or through one of the many online email services such as Gmail and Yahoo! Mail. No matter what program or service your child uses for email, they all share these common features:

- A field for the body of the message.
- A field for the subject line.
- A "From" field that indicates the email address of the sender of a message.
- Addressing options that allow up to three different kinds of recipients.
- An option to have a customized signature block for every outgoing email.
- The option of attaching one or more files to be sent along with a text message.

### Addressing Options

There are three areas or fields where your child can place a recipient's address: the "To" field, the "Cc" field (carbon copy), or the "Bcc" (blind carbon copy) field. The best option to use depends on the kind of email your child is sending and the number of recipients:

**Use the "To" field:** Use this option for a single recipient or for multiple recipients if everyone already knows one another's email address.

**Use the "To" field and the "Cc" field:** Use this combination for multiple recipients. The people in the "To" field should need to either to take some action or use the information in the message. The people in the "Cc" field need to be aware of the information, but do not need to take any action.

**Use the “Bcc” field:** Use this option if there are multiple recipients, and the recipients do not need to know the addresses of at least some of the other recipients. All the recipients in the “Bcc” field will be able to see the addresses in the “To” or the “Cc” field, and no recipient will be able to see any of the addresses in the “Bcc” field.

### **Subject Line**

One of the most important parts of an email message is the subject line. Upon opening most email programs, the sender’s email address and the subject line are the only parts of the email a recipient sees. Most recipients decide whether to read the email based on what the subject line says. The best kind of subject line is like the headline of a newspaper—it is clear, concise, and encourages the reader to check out the rest of the story. Encourage your child to always use the subject line, and to follow these general rules:

- Clearly describe what the email is about.
- Keep it short, using no more than about ten words (about 50 characters, including spaces).
- Use acronyms, words, or phrases that would be familiar to the recipient.
- Use appropriate language.

### **Bad Ideas for Subject Lines**

A good subject line encourages the recipient to read an email, and a bad one encourages the recipient to delete it. Any email that looks like it is unsolicited, unwanted, or inappropriate will likely not get opened. Make sure your child does not get into any of the following habits:

- Sending email with blank subject lines.
- Using multiple exclamation points!!!, question marks??? or special %&#\$\$@\* characters.
- Using obscene or sexually oriented language.
- Using threatening language.
- Using language that is not appropriate for an educational or professional environment.
- USING ALL CAPITAL LETTERS.
- Using words or phrases associated with fraudulent schemes, chain letters, or other common types of unsolicited email.

### **The Email Body**

The body of an email is either a plain text message or a formatted HTML document with text, graphics, and links to Internet resources. Your child’s email program should be set up to only create and send plain text messages so that the message can be read by any email program.

The typical body of an email is relatively short, from one sentence to about one page of text or other material. Longer messages or ones containing something other than plain text should be sent as an email attachment.

While there are no formal rules on what kind of information should be in the body of an email, the following are common informal rules are followed in plain text emails:

- Double spacing is used to separate paragraphs.
- Paragraphs are not indented.
- The message is written using standard rules of capitalization and grammar.
- Words written in bold type in a regular letter (such as headlines) are written in CAPITAL LETTERS.

### **Attachments**

An attachment is a file that is sent as part of an email message. You should teach your child to take the following precautions when sending attachments:

**Send an attachment only if necessary:** If a plain text message will do, your child should not send an attachment.

**Send only to those who need it:** If your child is not sure whether the recipient needs the file, have your child ask the recipient if he or she wants it.

**Send only to those who are expecting it:** Teach your child to avoid sending attachments when the recipient is not expecting one. Your child should first get permission from the recipient.

**Make sure the recipient can open the attachment:** Only send an attachment if you know the recipient has a program that can open the file.

**Send the smallest file possible:** Many ISPs have a limit on the size of an email attachment. Most should accept files smaller than one megabyte.

### **Organizing Email**

Emails are files that are typically saved in a format that is specific to the email program or online email service that you are using. You usually have to use that particular program or service to find old emails.

Most email programs and online email services use a file structure similar to what is used in the Windows Explorer file management program. Your child should be able to create folders, give the folders descriptive names, and move emails into appropriate folders. In some email programs, your child may not need to create folders to organize email. Gmail for example allows you to search your email collection to find emails.

If your child uses more than one email program or online email account, she will either have to do email management in several places, or make sure that all of her emails are in one convenient place. There are several options for consolidating emails into:

- When using a secondary email account, use the “Bcc” field to send a copy of each outgoing email to the primary account.
- Set up each secondary account to automatically forward a copy of any incoming email to the primary account. A forwarded email is one that is received by one person and then sent out again to one or more other recipients, and with no significant changes to the original content.
- Set up the primary email account so it can access secondary email accounts and download any new incoming emails.

### **Email Access Issues**

Any personal computer that is equipped to access the Internet usually has several options

for email, including an email account supplied by your ISP or free online email accounts. If your child has several email accounts, she may be able to have incoming email from one account forwarded to another, or be able to access one account while using another account.

### **How Many Email Addresses Are Enough?**

Once your child starts using email regularly, it would be a good idea to have four addresses. One primary email address and three kinds of secondary email addresses:

**Primary address:** This is an almost private account that your child should use only with family, a few trusted friends, and for school-related business.

**Administrative address:** This is an address your child should use with important online services such as a social media account or a bank account. If your child is given a special-purpose account—for example, a school email account—it should only be used for that special purpose.

**Throwaway address:** This is an address your child would use for casual online activities like signing up for fan club mailing or from other activities that may only be of passing interest to your child. As the name suggests, this is an email address that your child could simply stop using if she has problems like too much unsolicited email. This is the safest kind of address your child can post online.

**Backup address:** This is an address that will only be used to as a replacement for one of the other three types of addresses if there is a problem with one of them.

By the way, this suggestion to have at least these four kinds of email addresses works for parents and other adults as well.

### **Free Web-based Email**

There are a number of free online email accounts your child can use for either a primary or secondary email address. Refer to the “Online Email Accounts” section of appendix 2 for descriptions of some of these services. These accounts may be convenient, but they usually have a few drawbacks, including little or no customer service and no guarantee that the service will remain free.

### **Abbreviations, Acronyms, and Slang**

Schools, businesses, and organizations routinely use email for written communications, so your child should learn to treat an email the same way that she would treat a regular letter. That means she should follow normal rules for grammar, spelling, and punctuation.

When it comes to writing effective email messages, the same grammar and common-sense rules that apply in other written communication apply to email. Using abbreviations, acronyms, and slang may be an easy way for your child to communicate with friends or classmates, but she should not do this for two reasons. First, the abbreviations, acronyms, and slang that are perfectly understandable today may look confusing or silly next month or next year. The second reason is that email has become an acceptable way to send formal written correspondence, and acronyms and slang are often not appropriate for this kind of communication.

Having a family rule that email should be written in normal English is a good way to get children into writing habits that will benefit them for a lifetime. As a compromise, you may allow a more informal writing style for IM, chat rooms, or email sent to your child’s

friends.

### **Email Etiquette**

When it comes to the socially acceptable ways to send email, no one set of rules will work in every situation, but the following suggestions for email etiquette will probably work most of the time:

- Always check formatting, grammar, and spelling.
- Avoid sending jokes or other kinds of humor. If the recipient is insulted, the email provides written proof that can be used against the sender.
- Don't forward other people's messages without permission.
- Don't send attachments unless you need to.
- Keep emails as short as possible, but as long as necessary.
- Never put anything in an email that would be embarrassing if it were printed on the front page of the newspaper.
- Send an email only if there is something worth saying.
- Use the subject line to give a brief description of the contents of the message.
- When forwarding email, do not forward other people's email addresses.
- When responding to a message, include enough of the previous message so the recipient understands the context of the response.
- When sending a message to multiple recipients, consider using the blind carbon copy address field so the recipients do not see all of the other email addresses.

### **The Gettysburg Criterion**

Emails tend to be short, rather than long. While there is no specific rule about the maximum length of an email, there is one historical example that provides a guide for today.

President Abraham Lincoln's address at the dedication of the cemetery at Gettysburg, PA, on November 19, 1863 was a speech of only 266 words that was both a powerful message on the principles of democratic government and a shining example of how a short message can speak volumes. This speech also provides the inspiration for the Gettysburg Criterion—that the text in the body of an email should be shorter than the Gettysburg Address.

To use the Gettysburg Criterion, email a copy of the Gettysburg Address to your child, and then have your child print the email. Whenever your child is drafting an email that seems a bit long, compare it with the Gettysburg Address email. If the draft is longer than Lincoln's speech, then shorten the text. If making it shorter is not an option, then your child should consider sending the message in an attached file. Here is the text of the Gettysburg Address inscribed in the Lincoln Memorial in Washington, DC (punctuation added for clarity):

Fourscore and seven years ago our fathers brought forth on this continent a new nation, conceived in liberty and dedicated to the proposition that all men are created equal.

Now we are engaged in a great civil war, testing whether that nation or any nation so conceived and so dedicated can long endure. We are met on a great battlefield of that war. We have come to dedicate a portion of that field as a final resting place for those who here gave their lives that that nation might live. It is altogether fitting and proper that we should do this.

But in a larger sense, we can not dedicate, we can not consecrate, we can not hallow, this ground. The brave men, living and dead, who struggled here have consecrated it far above our poor power to add or detract. The world will little note nor long remember what we say here, but it can never forget what they did here. It is for us the living, rather, to be dedicated here to the unfinished work which they who fought here have thus far so nobly advanced. It is rather for us to be here dedicated to the great task remaining before us—that from these honored dead we take increased devotion to that cause for which they gave the last full measure of devotion—that we here highly resolve that these dead shall not have died in vain; that this nation, under God, shall have a new birth of freedom; and that government of the people, by the people, for the people shall not perish from the earth.

The Gettysburg Criterion is only one way to evaluate your child's writing. If she writes an email that is long but effective, don't force her to make it shorter or put it into an attachment. But if using the Gettysburg Criterion encourages you and your child to take the time to talk about writing, it will probably help both of you in ways that go far beyond that particular email.

#### **Top 10 Email Realities**

- 1. Email is an insecure communication:** Treat an email like a postcard and assume that someone other than the recipient will be able to read it.
- 2. Email can't be recalled:** Once an email has been sent, it is out of the sender's control.
- 3. Email is forever:** The sender, the recipient, and any computer system involved with transmitting the email may have copies, and there is no way of knowing how long those copies will stay around.
- 4. Email should be treated seriously:** Many of the laws and traditions associated with written correspondence apply to email.
- 5. The contents of an email may be copyrighted:** This means that the person who wrote the email can control how it can be used. This is true for the United States and for countries with similar copyright laws.
- 6. Not every email you receive deserves a response:** If a response is not expected or not required, don't respond.
- 7. Not every recipient of your email will send a response:** If a response is expected, ask the recipient to send one.
- 8. Free speech has its limits:** The regulations and laws that limit free expression apply to email.
- 9. Pay attention to the rules:** Be aware of the rules that your ISP, school, or organization may have about sending and receiving email.

**10. Email is not going away:** Email will likely remain an important method of communication. Make sure your child becomes comfortable with using email and also knows how to use it responsibly.

[Back to Table of Contents](#)





## **CHAPTER 9: DEALING WITH UNWANTED EMAIL**

### **In This Chapter**

- An Overview of Unwanted Email
- Seven Steps to Controlling Email
- Top 10 Ways to Stop Unwanted Email

Years before there was a World Wide Web, the Internet had email. Sending and receiving email are the most popular activities of Internet users. Unfortunately, much of the email that an average user receives is not useful, not desired, and sometimes downright offensive. This is a problem for anyone who uses email, so one of the earliest online skills your child should learn is how to deal with unwanted email. This chapter will help your child by providing him with practical advice on how to do the following:

- How to recognize unwanted email.
- How to reduce the amount of incoming email.
- How to filter unwanted email.

### **An Overview of Unwanted Email**

Unwanted email includes messages that have malicious software attachments, are part of some kind of fraudulent scheme, or are associated with cyberbullying, online child predators, or other illegal or undesirable activities. Chapter 7 discussed child predator and cyberbullying issues, including the ways predators use email. This chapter focuses on other types of undesirable email:

- Email that makes demands on your time and energy, but provides little or no benefit.
- Email that has potentially harmful attachments.
- Email that encourages visits to web sites associated with malicious software, fraudulent activity, or inappropriate content.
- Unsolicited commercial email.

### **Why Learn About Unwanted Email?**

Every minute your child spends with unwanted email is precious time taken away from more productive uses of the Internet. If you take time to show your child how to deal with this problem, you will make his time online more worthwhile.

### ***The Difference Between Spam and Unwanted Email***

Spam is the popular term for unsolicited commercial email. The term may also be applied to unsolicited email containing chain letters, bogus offers, rumors, and other information that lacks authority, usefulness, or validity. Unwanted email includes spam, but also includes situations where there has been a previous relationship with the sender.

### **How Unwanted Email Ends Up in Your Inbox**

There are a number of sources of unwanted email, some of which can be controlled:

- Any business, organization, or individual who has ever received an email from your child.
- Any business, organization, or individual who has ever sent an email to your child.

- Any business, organization, or online service that has ever obtained your child's email address.
- Any mailing lists that your child has ever joined.
- Any web site or other online resource that displays your child's email address.

### **Categories of Unwanted Email**

It is up to your child to control what email gets opened. You should be very clear about what he is allowed to receive and what he is allowed to open. There are several kinds of email you should not allow your children to accept:

**Adult-oriented:** Emails that contain text or pictures intended for adults; that promote activities, products, services, and intended for adults; or that contain links to adult-oriented online resources.

**Chain letters, jokes, rumors, gossip, and other diversions:** These kinds of emails are not meant to be malicious, but they are usually a distraction.

**Email with unexpected attachments:** It does not matter whether the email appears to be from a familiar source. You should insist that your child avoids opening these kinds of attachments until someone can confirm the attachment is legitimate.

**Money making offers:** Usually associated with fraudulent activity, these emails usually promise either quick profits or large profits for little or no effort.

**Requests for sensitive personal data:** A parent should always respond to this kind of request.

### ***Chain Letters and the Internet***

Chain letters were around long before there was an Internet, and follow a predictable formula, typically promising a very positive result if you forward the message to others. Children are prone to the kind of peer pressure that will lead them to forward a chain letter email sent by a friend or classmate. If you discover your child is creating or forwarding chain letters, take the time to explain that sending chain letters is not appropriate.

### **Seven Steps to Controlling Email**

As long as you have an email address, there will be someone willing to send your child email he does not want to read. However, you can help your child reduce the amount of incoming unwanted email by helping him do the following:

1. Make email less visible online.
2. Make email less visible offline.
3. Divert unimportant email to a secondary address.
4. Use email filters.
5. Review each email before opening.
6. Learn how to respond to unwanted email.
7. Avoid contributing to unwanted email.

### **Step 1: Make Email Less Visible Online**

When an email address is published online in a place such as web page or blog post, it

makes it very easy for that address to be added to mailing lists or otherwise used to send unsolicited or unwanted emails. The best option is to not put the address online at all. If your child has to do so, you can at least make it harder to find or to copy. One way to trick automated email gathering programs is to add a space after and before the “@” sign in the address. A human would have the good sense to remove the blanks, but a program would not. If your child has to publish her email address, have her use one of her secondary addresses and not her main one.

### **Step 2: Make Your Email Less Visible Offline**

Schools, government organizations, and businesses may routinely request your child’s email address. Teach your child to keep the following in mind when someone asks for his email address:

- If an email is needed for administrative or contact purposes, use a secondary email address.
- If it is not required, do not provide it.
- Encourage your child to join only mailing lists that send out useful and worthwhile information. Also, your child should only join mailing lists that have an easy procedure for removing an address.
- Remind your child to remove his email address from any mailing list that sends mailings he no longer wants or needs.
- If someone insists on being provided with an email address, but there is no real need or legal obligation to do so, encourage your child to provide a fake address or an old one he no longer checks.

### **Step 3: Divert Unimportant Email to a Secondary Address**

Some email doesn’t have to be looked at as soon as it arrives, or if it is ignored, there will be few if any consequences. For these kinds of emails, it may be smart to have them sent to a secondary email address, preferably the kind of email account that is free and accessible online. One of the biggest advantages of using this kind of email account is that if your child gets into a situation where your child is receiving a large amount of unwanted email, and can’t get the sender or senders to stop, your child can simply stop using the account and get another one.

### **Step 4: Use Filters in Your Email Program or Online Email Service**

Typically, email program or online email services have the ability to filter emails after they reach your child’s inbox. Email filters are most convenient for doing the following kinds of actions:

- Blocking emails with objectionable words.
- Blocking messages from specific email addresses.
- Blocking emails with very large attachments.
- Directing email from particular addresses into a folder other than the inbox.

Be sure to refer to your email program’s documentation or help files for specific instructions on how to create filters or block senders.

### ***Using Additional Filtering Software***

You can also add software to your home computer that can filter incoming email. Unlike the filtering options in the email program that your computer may have or within a free Web-based email service like Gmail, it may cost money to acquire and maintain the software. Before spending money on additional software or services, you and your child should use the free tools that are already available to you.

### **Step 5: Scan Incoming Email**

No matter how careful your child may be when it comes to avoiding and filtering unwanted email, some will always get through. Your child has to be able to spot suspicious email and delete it because such mail may contain content that may be disturbing to your child and perhaps hazardous to your computer.

#### *Setting Up How Your Inbox Is Displayed*

It is usually easy to spot an unwanted email by simply checking out the sender, the subject line, and perhaps the first few lines of text. If the email program that your child uses is not already set up to display this information, change the settings so that it does.

#### *Spotting an Unwanted Email*

If your child is allowed to check email without adult supervision, make sure that she knows that emails with one or more of the following warning signs should be deleted without first being opened:

- The email, whether sent by a stranger or from a familiar address, has an unexpected attachment.
- The email is from a stranger and the subject line contains random words or characters.
- The sender is unfamiliar and the subject line is blank.
- The subject line indicates that the email probably has inappropriate content.
- The subject line is in an unfamiliar language.
- The subject line says that you have won some kind of contest or lottery.
- The subject line uses threatening language.
- The subject line warns that you are in some kind of trouble or danger.

### **Step 6: How to Respond to Unwanted Email**

How your child should respond to an unwanted email will depend on the relationship your child has with the sender and on the nature of the email:

**The email involves illegal activities such as child pornography or is associated with cyberbullying or other kinds of harassment:** You and your child should follow the advice given in chapter 7 on cyberbullies and child predators.

**The email is from a person who has some kind of continuing offline relationship with your child:** You or your child should ask that person to stop sending that kind of email.

**The email is from an organization, group, or online service that has a relationship with your child:** If your child does not want to receive any more emails, she could request that no further emails be sent. If emails still arrive, take action to block any emails from that source.

**The sender is unknown and the email is only a slight inconvenience:** Most unwanted email falls into this category. Your child should ignore this type of email. Any response will likely generate additional unwanted email.

**The email was sent from your child's school:** Contact the school to deal with this issue. Find out what actions the school plans to take and follow up to make sure the actions are taken.

### *What To Do if the Problem Gets Serious*

When the amount of unwanted email becomes so great that it takes up too much of your child's computer time, or if the type of mail that is coming in is so disturbing or objectionable that you do not want to even look at them, then you should change email addresses. If the problem was with a free online email account, simply use another one. If the problem account is associated with your ISP, contact that ISP to get a new email address. Most ISPs allow you to have multiple email addresses on the same account, so there is no need to stop using an ISP just because of a problem with one of those addresses.

#### **Step 7: Do Not Contribute to The Problem**

Parents should provide guidance for their children regarding how to properly and responsibly use email. Part of that effort includes encouraging your child to create effective emails. You and your child should work together to learn how to follow at least some of the following good habits:

**Keep messages short:** Shorter messages are more likely to be completely read than long messages.

**Have a good reason for sending an email:** If the recipient does not have an immediate use for the information in the email, don't send it.

**Use a clear and descriptive subject line:** Badly written subject lines look too much like spam.

**Use appropriate spelling and grammar:** If your email program has a spell checker, use it. Also, an email written with proper spelling and grammar is more likely to be read and understood.

**Send email only to people who need to see it:** An email with a long list of recipients in the "To" or "Cc" fields may not be seen as urgent as one addressed to an individual or small group.

**Use the blind carbon copy field when sending email to groups of people:** If the recipients have no need to know each other's email addresses, protect everyone's privacy by using the "Bcc" field.

**Think twice before forwarding:** Forward an email only if the recipient really needs to see it. Any forwarded email should include a short note at the beginning that explains why the message was sent.

#### **Top 10 Ways to Stop Unwanted Email**

- 1. Don't volunteer to receive email:** Unless there is a good reason to receive email, just say no.
- 2. Have one or more secondary addresses for less important emails:** If unwanted

email becomes a problem, move to another secondary address.

**3. Use your primary email address only for people and organizations that you trust:** If a sender's habits change for the worse, provide that sender with a secondary address.

**4. Don't put your primary email address online:** Use a secondary address instead.

**5. Use the blind carbon copy field for multiple recipients:** Since each recipient can only see addresses that are in the "To" or "Cc" fields, put your address in the "To" field and all the recipients in the "Bcc" field.

**6. Encourage any group that sends you email to use blind carbon copy:** Contact the person responsible for sending the group's emails and explain how to use the "Bcc" field.

**7. Send unsolicited email only when necessary:** Don't send an email unless the recipient has a good reason to read or respond to the message.

**8. Don't respond to unsolicited commercial email:** Responding to the email or to the commercial offer in any way will likely encourage more unsolicited emails.

**9. Treat the subject line like a newspaper headline:** Summarize the email in less than ten words. An email with a well-written subject line is less likely to be accidentally ignored and deleted.

**10. Teach your child how to recognize and respond to unwanted emails:** Your child should learn to delete unwanted email and to get you involved if the email involves issues that should be addressed by an adult.

[Back to Table of Contents](#)



## CHAPTER 10: WEB BASICS

### In This Chapter

- A Quick Overview of a Web Site
- Basic Kinds of Web Sites
- How to Use Search Engines and Directories
- Top 10 Search Engine and Directory Tips
- Finding the Key Sites on a Particular Subject
- Top 10 Tips for Using the Web

Your child has to understand how to use the World Wide Web if she wants to get the most out of being online. The Web is huge, with hundreds of millions of web sites and billions of web pages. Whether she is online for school or for fun, she has to know how to find the pages and the sites that will give her the information she needs, and she has to know how to do that without wasting a lot of time. This chapter will show her how to do those things by explaining all the steps she needs to find the most important web sites on a particular subject.

### A Quick Overview of a Web Site

A web site is nothing more than a collection of files residing on a computer that is connected to the World Wide Web. Web sites usually contain information in the form of text and graphics, but may also have information in other media like video files. The more recent versions of Firefox and Internet Explorer can access all of the data on most web sites, especially those sites that only contain text and simple graphics.

What makes a web site particularly useful is its ability to take a user from one page to another online resource. These links, also known as hypertext links or hyperlinks, can take a user to another part of the page, another part of the site, or to a completely different web site with one click of the mouse. These links allow a well-designed web site to be a very flexible tool that can connect you to the best available online resources.

### Basic Kinds of Web Sites

While a page within a web site is usually focused on one subject, the entire site may have a broader purpose. Most sites fit into one or more of the following categories:

**Informational:** These sites provide information on a particular subject. The information is often a combination of data within the site and links to related information outside of the site.

**Organizational support:** These sites are designed to support an organization. Sites run by schools or businesses often fall into this category.

**Personal:** These sites are focused on the activities or accomplishments of an individual.

**Promotional:** This kind of site presents mostly positive information about a person, product, concept, or service. Commercial sites selling goods or services fall into this category. Also falling into this category are sites that advocate some kind of political, organizational, or social position.

**Service:** These sites support some online service such as email or search engines.

## **Structure and Organization of a Web Site**

Most sites are organized around a home page that has one or more of the following:

- Links to related resources outside of the site.
- Links to key pages within the site.
- A link to an internal search engine.
- A link to an index or table of contents page.

For example, AirSafe.com is a web site about airline safety. Individual web pages are devoted to specific airlines or aircraft types. The home page acts as a table of contents, with most of the links going directly to a page that deals with one area of the site. There is also an internal search engine link on most pages, including the home page.

### ***Problems with Using Information on the Web***

Just because something is on a web site does not mean it is either true or useful. Before your child uses a web site for something like a school project, she should understand that she has to figure out whether the web site can be trusted. Your child should learn how to keep the following issues in mind when using web sites:

**Authority:** Your child should verify that people who have the appropriate kinds of experience, credentials, or knowledge run the site.

**Detail:** Most web sites only show a small part of the information available on a subject.

**Legal standing:** A web site, even a site managed by a responsible or respected individual or group, should not be considered the official or legally binding version of that information.

**Longevity:** A web site can be changed, moved, or eliminated at any time and without warning.

**Standards:** There are no widely accepted or widely enforced standards for the content, format, quality, or organization of web sites.

**Technical limitations:** Your computer may not be able to properly display all of the contents of a web site.

Of all these problems, the lack of standards for the quality of content on the Web is the most critical one for students. If you want your child to be able to easily find sites and to evaluate if the sites are worth using, then your child should become familiar with the information in the rest of this chapter.

### **How to Use Search Engines and Directories**

Unlike a library, the Web is not organized in any logical way. The number of web sites and web pages is so large that anyone who uses the Web needs to have a tool in order to quickly find information. Fortunately, search engines and directories are two online tools that make it easy to find information. This section of the book provides a general overview of how search engines and directories work, and provides specific advice on using different kinds of search engines for different tasks. A few of the more important definitions include the following:

**Directory:** An online service that organizes links to Internet resources by category or



by some other criteria.

**Keyword:** A word used within a search engine to locate resources online.

**Key phrase:** A group of words, typically enclosed by quotation marks, that are used within a search engine the way that keywords are used.

**Search engine:** An online service that allows a user to find Web-based resources by using one or more keywords or key phrases to describe the desired information.

Unlike a good librarian, a search engine can't use judgment or ask questions to figure out what you need. How well a search engine or a directory works depends on what you tell it to do. In general, the difference between a search engine and directory is that a search engine automatically scans and evaluates a web site. For a directory, human beings evaluate the web sites. Another difference is that a directory arranges information by category. For both a directory and a search engine, a user must start with a goal in mind.

Most search engines have a home page that features an input field for search engine commands that is called a search box. A user types in one or more keywords or key phrases for a basic search and perhaps some logic commands for a more complex search. Most directories have a home page that acts like a table of contents, with links on that home page for each major category. Like a search engine home page, the typical directory home page has a search box allowing a user to search the directory using keywords and key phrases.

### **How to Search Using Google**

The following description provides an explanation of how to use the Google search engine. Google is the most popular search engine on the Web, and the internal search engines of many web sites use its technology. If your child can understand the basics of this search engine, he or she will easily learn how to use other search engines.

#### ***Capitalization Does Not Matter***

Google's search engine ignores capitalization. Also, if a search request has more than one word, the search engine looks for results containing all of the words. For example, the search command [Shakespeare Hamlet] tells that search engine look only for those entries containing both words (the brackets signify the entries in the search box). The results would be the same if the search terms were [Shakespeare hamlet], [shakespeare Hamlet], or even [shakespeare hamlet].

#### ***Order Does Matter***

The order of the words will change the result. The search request [space shuttle] gives different results than the search request [shuttle space]. Search terms should be in the order that makes the most sense. To find results containing a specific phrase, enclose that phrase in quotation marks. For example [space shuttle problem] will get more results than, ["space shuttle problem"] because the results of the first search will include online resources that contain the three words anywhere in the document, and the results of the second search will include only those resources that contain the phrase "space shuttle problem."

#### ***Word Variations Are Included Automatically***

Google and most other search engines will look for the search terms as well as for words

that are similar to the search terms. A search for [africa airline] may turn up resources containing the words “African” and “airlines.”

### ***Common Words Are Ignored***

The Google search engine ignores commonly used words and single digit numbers. There are two ways to keep this from happening: include the common word or the single digit number as part of a key phrase, or place a plus sign in front of the common word or single digit number.

### ***How to Exclude Words or Phrases***

To exclude a word or a phrase from the search results, put a minus sign in front of the word or phrase. For example, a search for [airline safety –Airbus] will give results that include the words “airline” or “safety” but that do not include the name “Airbus.”

### ***Advanced Search Features***

Most search engines have advanced features that allow more specific searches. There is usually a link near the search box or submit button that leads to a detailed explanation of the rules for basic searches and the options for advanced searches. Some of the more useful advanced search options for the Google search engine include the following:

**Either one term or the other:** Inserting the word “OR” in uppercase between two search terms will give results that contain either term or both terms. For example, [airline OR safety] provides resources containing either one or both words.

**Searches within a web site:** Using the operator “site:” in front of a domain name limits search results to that particular web site. For example, [site:airsafe.com midair collision] will return those resources within the site AirSafe.com that contain the words “midair” and “collision.”

**Sites that link to a web page:** Placing the operator “link:” in front of the URL of a web page will generate a list of resources that link to that page.

### **Starting and Refining a Search**

There are two parts to any search: understanding what is needed and then going out and finding it. This often involves doing several searches, refining the search each time to get better results. Depending on the results, your child may have to broaden the search, narrow the search, or take the search in a new direction.

#### **Before the Search**

Your child should take the time to figure out what he wants to find, and think of a few words or phrases that best describe what he wants to find. After that, he can take the following steps:

- Start by using general keywords or key phrases in the initial searches on a particular subject. For example, [airplane airline united] is a more general search than [747 United]. Based on the results of the initial searches, either broaden or narrow subsequent searches.
- To broaden a search, remove at least one keyword from the request, use a minus sign to exclude a word or phrase, or remove the quotation marks from a key phrase. For example, changing a search form [airplane United] to [airplane] or from [“United

Airlines”] to [United Airlines] will return additional entries.

- To narrow a search, include additional keywords or key phrases, or use a more precise keyword or key phrase. For example, the search [United 747] will return fewer results than [United].

- To take the search in a new direction, replace search terms with words or phrases from related concepts or by using synonyms for the search terms. To find synonyms, use a printed thesaurus or an online thesaurus such as the ones described in appendix 2. For example, the search [United airliner] will give results similar to the search [United aircraft].

### **Choosing a Search Engine or Directory**

There are many search engine and directory choices on the Web. Picking a search engine or a directory comes down to finding one that best satisfies the user’s search needs. The best advice is to try several of the search engines or directories to see which ones are consistently useful. Besides Google, the two biggest search engines are Yahoo! and Bing. These three search engines provide the search capabilities for many of the smaller search engines, as well as for the internal search engines of many web sites. Various search engine and directory options are provided in the “Search Engines and Directories” section of appendix 2.

### **How Search Engines Display Results**

The result of most queries to a search engine or directory is a listing of resources that usually includes the name of the resource, its URL, and a short description of the resource’s contents. Each search engine and directory uses different criteria to rank the results, and will return different results for the same set of keywords or key phrases.

### **Search Engine and Directory Limitations**

The key limitation of all search engines and directories is that no single search engine or directory can search the entire contents of the Web. Some web site operators also design their sites so search engines are unable to index some or all of the site.

There are other limitations. For example, when new material is added to a web site, or older material deleted from a site, the database of a search engine or directory may not be immediately updated to reflect that change. As a result, the output of a search engine or directory query may include descriptions of web pages or web sites that may be no longer current, that may be no longer available online, or that may have been moved.

### **Child-friendly Search Engines and Directories**

If you want your child to become familiar with using a search engine or directory, but do not want him to encounter inappropriate or objectionable content, you have a couple of choices. One option is to use any filtering options provided by a search engine or directory. Another option is to have him use a search engine or directory that is designed for younger children.

### **Top 10 Search Engine and Directory Tips**

1. Have your child try out several search engines and directories to find the ones that produce the best results.
2. Make sure your child reviews the help files or online instructions for a search engine or directory to get an idea of how each one works.

3. Make sure your child can use the advanced features of the search engine or directory.
4. Most search engines ignore capitalization.
5. Remember that no search engine or directory can search for all of the information that is online.
6. Become familiar with the techniques for making a search broader.
7. Become familiar with the techniques for making a search narrower.
8. It may take several searches, each one either narrower or broader than the last, in order to find the desired content.
9. Use two or more search engines or directories to get more complete coverage of a subject.
10. Always have a goal in mind when starting a search.

### **Finding The Key Sites On a Particular Subject**

All web sites are not created equal. Although every site has the potential to enlighten, to entertain, or to inspire, the reality is that only a small percentage of the sites that deal with a particular subject are worthy of even a cursory look. Finding the most valuable sites on a particular topic is worth the time and effort; these are the sites that are most likely to satisfy your child's information needs on a particular subject. Finding these web sites takes a combination of prior knowledge of the subject, insights that others may have about the subject, and the ability to properly use a search engine or directory.

#### **What Is a Key Web Site**

A key web site is one that provides a level of information or a level of service that is better than most or all of the available alternatives. The previous section of this chapter discussed how to use a search engine or directory to find useful information on a subject. This section goes further, describing how to find a site that provides information or services that are superior to most or all of the available alternatives. This kind of site should have many of the following characteristics:

- Links from the site go to resources that provide complementary information or services.
- News organizations frequently refer to the site.
- Related key sites also link back to the site.
- The information on the site is kept current.
- The information or service provided on the site is superior to competing sites.
- The site can serve as a reliable reference resource.
- The site does not contain significant factual or grammatical errors.

#### **How to Find Key Sites**

Finding out what sites may be key for a particular subject can be broken down into a four-step process:

1. Take the time to write down what is known about the services or information being sought.

2. Find potential key sites using search engines and directories.
4. Evaluate each potential site to determine which ones deserve further consideration.
4. Carefully review the remaining sites for the quality of their content and the quality of the sites that are linked back to them.

### ***Write Down What Is Wanted***

If you want your child to learn how to consistently find the best web sites about any particular subject, get her into the habit of first writing down what she knows about a subject before going online. If she knows nothing about that subject, she should get some idea about it from a reference book or from a knowledgeable person. The “Encyclopedias and General References” section of appendix 2 lists several online resources she could use. She should identify the most prominent groups, organizations, and individuals that have an ongoing involvement in the subject. She should also be able to describe what she is looking for as precisely as possible.

### ***Start Searching***

The next step is for your child to develop a list of keywords and key phrases that are based on her initial research and to use them to conduct an online search. If initial searches are not satisfactory, she can either broaden or narrow the search using the techniques described earlier in the chapter. She may also want to try a different search engine or directory.

An important part of any search strategy is knowing which leads to follow and which ones to ignore. The following general rules should be helpful to your child:

- If a resource appears to be from a personal site, your child should ignore it unless she was looking for that person’s ideas or opinions.
- If the sponsor of the site is an organization with a significant offline presence, that site is a better candidate for further investigation.
- If the description of the resource contains most or all of the search keywords or key phrases, that site is worth a closer look.
- Your child should focus on recently updated sites unless the information she child wants is either historical data or information that does not change frequently.
- If your child does not find any useful results in the first three to five pages of search results, she should try a different set of search terms, a different search engine, or a different directory.

Once you have a list of candidate sites, the next step is to find out which of these sites contain key information. This kind of site will have one or more of the following characteristics:

- Other key sites will have links back to the site.
- The site has links to other key sites.
- The site provides a superior level of information or a superior level of service.

There are several techniques your child should use to determine whether a site has these characteristics. The following section provides the details on how that should be done.

## **Judging the Quality of A Web Site**

If a site provides a service, you child can judge the quality by using the service. For a site that primarily provides information, your child will have to check to see if it contains the specific information needed to address her particular needs. The steps in this process are as follows:

- Establish the legitimacy of the site.
- Judge the value of the information or the service.
- Evaluate the site's ease of use.
- Evaluate the links from a site.
- Evaluate the links to a site.

### ***Establishing the Legitimacy of the Site***

The first step of establishing its legitimacy is to determine whether the individual or group responsible for the site has the authority or the capacity to discuss the subject matter covered by the site or to provide the services offered by the site. For sites managed by an individual or organization that is widely recognized as an authority on a given subject or the provider of a given service, this step may not be unnecessary. For other sites, your child has to determine if the provider of the information or service is credible. Sites meeting most or all of the following criteria are likely to be a credible source of information:

- The organization or individual that operates the site is easily identifiable.
- The site is authorized to provide the information or service.
- The organization or individual responsible for the information or services provided by the site is qualified by experience, expertise, or credentials.
- The reputation of the person or group responsible for the site would be damaged if the information on the site were not accurate or credible, or if the level of service provided by the site was poor.
- The individual or group that controls the site also has a significant and related offline presence.

### ***Judging the Value of the Information or Service***

A high-value informational site should meet most of the following criteria:

- Any audio, animation, graphics, or other complex elements enhance the information on the site.
- Graphs, charts, and other visual displays of data are clearly labeled and easy to interpret.
- Limitations of the data or of the other information on the site are clearly stated.
- The facts on the site can be verified from at least one independent and reputable source.
- The information on the site is consistent with the purpose of the site.
- The information on the site is current.
- The information on the site is as good as or better than similar information from

other sources.

- The site clearly describes the method or methods used in any analysis discussed within the site.
- The site contains few, if any, factual errors.
- The site has a clear purpose.
- The site identifies the source or sources of any outside information used on the site.
- The site provides definitions of any acronyms or special terminology used on the site.
- The written content consistently follows basic rules of grammar, spelling, and composition.
- There are no apparent conflicts of interest between the sponsor of the site, the advertisers on the site, and the information on the site.
- The value of a service is best judged by using the service. If the service is of high quality, it should also have most of the following characteristics:
  - The service can be tailored to meet a user's needs.
  - The service is available around the clock.
  - The site is not involved in any fraudulent or illegal activity in order to provide the service.
  - Users are required to provide little or no personal information in order to use the service.

### ***Evaluating a Site's Ease of Use***

An easy-to-use web site should have at least several of the following characteristics:

- Every page of the site links to at least one of the following: the home page, the table of contents, the index page, or an internal search engine.
- Most of the useful information on the site is within two links from the home page.
- The design of the site does not detract from the information or service it provides.
- The information or service can be accessed from the home page.
- The site accepts user feedback.
- The site has a table of contents.
- The site has an internal search engine.
- The site has an index.
- The site explains how to use the information or service.
- There are links between related information in different parts of the site.

### ***Evaluating the Links from a Site***

This part of the evaluation can be combined with the evaluation of a site's contents or service. The goal is to see if the site provides links to resources that enhance the information or services it provides. Useful links could be to pages within the same site or to outside sites. A useful link should have most of the following characteristics:

- The destination of the link is a specific relevant piece of information or a relevant service.
- The link is conveniently placed within the page.
- The outside site has links to other related key sites.
- The text or graphics that make up the link indicate what is at the other end of the link.

### *Evaluating the Links to a Site*

On a web page, it is easy to spot the outbound links. However, it takes the help of a search engine to see what outside links point to a particular site. For example, in Google, the command [link:<URL name>] will show what pages point to that URL. If a site is a key site, inbound links have the following characteristics:

- The links are from sites that are also key sites.
- The links come from recently updated pages.
- They are from sites with relevant information or services.

### **Top 10 Tips for Using the Web**

- 1. Have a purpose for every visit to the Web:** Your child should have a clear set of goals each time he or she is online.
- 2. Set time limits on each session:** Make sure your child takes an occasional break during an online session.
- 3. Find a working environment that works for you:** Make sure your child can work comfortably and with few distractions.
- 4. Choose the right equipment and software:** Take the time to find the hardware and software that meets your child's needs.
- 5. Avoid bad web sites:** If a site doesn't meet the legitimacy, quality, and the ease-of-use criteria described earlier, look for a site that does.
- 6. Use your browser more effectively:** Help your browser load pages faster by blocking popups, advertising, or other things that slow it down.
- 7. Use search engines and directories:** Make sure that your child knows how to do a proper search with a search engine or directory.
- 8. Use links in a site to find related information:** Get your child into the habit of checking a site's incoming and outgoing links.
- 9. Find useful sites from offline sources:** Be on the lookout for interesting sites that may be mentioned in other media such as newspapers or television.
- 10. Avoid high-demand times:** The busiest times are weekdays from late morning to early afternoon.

[Back to Table of Contents](#)







## CHAPTER 11: AVOIDING INAPPROPRIATE CONTENT

### In This Chapter

- What Is Inappropriate Content?
- Exposure to Inappropriate Content
- Filtering Inappropriate Content
- Seven Steps to Control Inappropriate Content
- Top 10 Tips About Inappropriate Content

It is no secret that not everything online is appropriate for children. While the nature of the Internet makes it difficult to keep all inappropriate material from your children, there is a lot you and your family can do to keep exposure to this kind of material to a minimum.

### What Is Inappropriate Content?

What is inappropriate is a personal and family decision. Most parents would consider sexually explicit material, material promoting hatred, and material glorifying violence to be inappropriate for their children. The following are only a few examples of this kind of content:

- Adult-oriented stories, discussions, or broadcasts.
- Visual depictions of cruelty to animals.
- Visual depictions of sexual activity.
- Web sites containing graphic violence.
- Web sites promoting the use of illegal drugs.
- Web sites or discussion groups promoting racial, ethnic, or religious intolerance.

### Exposure to Inappropriate Content

There are three ways to become exposed to inappropriate content:

- By accident.
- By looking for it.
- By having it sent to you.

Other parts of this book, specifically chapter 7 on cyberbullying and child predators, and chapter 9 on unwanted email, provide advice on how to address the first kind of exposure to inappropriate material. This chapter will also discuss accidental exposure, but will focus on the other two ways inappropriate material may end up in your home or in front of your child.

### Accidental Exposure To Unwanted Content

Exposure to unwanted web content can happen in three ways:

**Using the wrong URL:** A URL is a very specific address for a resource on the Web. A single incorrect character may lead you to a completely different web site.

**Deceptive web sites:** These are web sites that are designed to lure unsuspecting visitors.

**Careless search techniques:** Sometimes a search engine's output will include many

resources that have nothing to do with the intended topic. You have to make the effort review the search results before following a link.

### **Looking for Inappropriate Content**

Every family has rules about what is allowed and what is not allowed. While accidental exposure to inappropriate material will eventually happen to anyone who is online, such exposures will likely be very rare. However, if your child is regularly visiting places that are off limits, you will likely notice one or more of the following behaviors:

- Being evasive when asked about online activity.
- Going online when no one else is around.
- Hiding flash drives, CD-ROMs or other portable storage devices.
- Quickly closing a window, hiding the screen, or turning off the computer.
- Unusual or inappropriate activity while at the computer.

The following situations may also signal that someone in the family is accessing inappropriate material:

- The browser has bookmarks to inappropriate web sites.
- The browser's history file indicates numerous visits to sites with inappropriate content.
- You find inappropriate material on the computer's hard drive or on portable storage devices.

### **Having it sent to you**

This could happen accidentally or because of a deliberate action. Often unethical companies use purchased email mailing lists to send advertising for inappropriate web sites or services. While many email services such as Gmail do a good job of filtering these emails out automatically, sometimes they do get through.

This could also happen accidentally if your child has signed up to receive legitimate mailings from a company, and the company either starts to send inappropriate material, or that company sells or gives away its mailing list to a company that does.

The other way inappropriate material can be sent to your child is if your child willingly gave his or her email address to a company that offers inappropriate content to its customers or members.

### **Filtering Inappropriate Content**

One way you can limit exposure to inappropriate or objectionable content is through filtering. Filters consist of software or software settings that limit the content that can be displayed or accessed by a computer. Filters can be used to restrict access to one or more of the following:

- Certain categories of web sites.
- Specific types of online activities.
- Web pages with certain kinds of visual content.
- Web pages containing specific words, phrases, or combinations of words and phrases.

- Web sites within a database of banned sites.

### **Where Filters Are Used**

You can find filters in a variety of places, including:

**In a computer network:** These are more elaborate installations that may be used by a corporation, school, or library.

**In a personal computer:** These are made primarily for use in the home.

**Within a program:** Examples include browsers that may be configured to restrict certain types of activity or certain kinds of content.

**Within an online service:** Services such as search engines may allow users to set content restrictions.

### **Filter Limitations**

The following are the most common limitations of filters:

**Lack of updating:** If the database used by the filter to determine what sites to restrict or block has not been updated, new sites will not be blocked.

**Technological limitations:** The filter may not be able to block some types of content, or your child finds ways to work around the filter.

**Overblocking:** A condition where a filter blocks access to sites containing acceptable content.

**Underblocking:** The filter does not block content that you want it to block.

### **Seven Steps to Control Inappropriate Content**

There is no single best way to deal with inappropriate material. The following seven actions will help keep this kind of material away from your family and will help you find out if anyone in your family has been looking at banned material:

1. Enforce family rules on Internet use at home or away from home.
2. Check online accounts.
3. Check portable data storage devices.
4. Use filtering on your online services.
5. Use filtering software on your computer.
6. Check your computer for patterns of unusual or inappropriate activity.
7. Check your computer's hard drive

### **Step 1: Enforcing Family Internet Use Policies**

As mentioned in chapter 2, the two key roles are for the child to play by the parents' rules and for parents to make and enforce those rules. Every situation involving a child being exposed to inappropriate material will be different, but there are two ways you can respond:

**Accidental Exposure:** Encourage your child to talk to you whenever she comes across something she should not be seeing online. It will give you a chance to figure out why it happened, to take steps to prevent it from happening again, and to take the time to deal with any questions or issues she may have as a result of the exposure.

**Deliberate Exposure:** In this situation, the actions you take should be swift, certain, and severe. At the very least, your child's online access should be severely restricted until she understands that such behavior is not acceptable.

Enforcing family rules on inappropriate content will be easier if the following general rules are included in the Internet use agreement of an older child:

- I understand which sites I can visit and which ones are off limits.
- I will follow these same rules when I am at home, in school, at the library, or at a friend's home.
- If I come across something that is off limits or potentially dangerous, I will tell my parents or another responsible adult.

### **Step 2: Check Online Accounts**

Chapter 4 on privacy provides several suggestions for maintaining a family's online privacy. One suggestion was to keep track of every family member's online accounts. Doing so will allow you to easily check to see if your child has accessed inappropriate material. Also, if you find out that your child has an account that is not on the list, access the account and check it for inappropriate material. Keep track of all accounts using the "List of Online Activities" form in the Family Forms Pack located at [forms.speedbrake.com](http://forms.speedbrake.com).

### **Step 3: Check Portable Data Storage Devices**

One of the suggestions from chapter 5 is that the family maintains a record of where everyone keeps their data. If you come across a device that has not been accounted for, check it for anything out of the ordinary and then add it to the "List of Data Storage Devices" form. It is also part of the Family Forms Pack and is available at the above URL.

### **Step 4: Use Filtering on Your Online Services**

You may be able to restrict some kinds of content on some of the online services you and your family use. For example, many of the search engines listed in appendix 2 have filters that will keep some kinds of material from being displayed. Other search engines are either designed for children or do not allow adult-oriented material.

If inappropriate content is a concern, you should only allow your family to use those online resources that allow you to limit objectionable material. One way to keep track of what services your family can access is to use the "List of Online Activities" mentioned in Step 2.

### **Step 5: Use Filtering Software on Your Computer**

If you use filtering software at home, make sure it is designed to deal with the kinds of content that concern you. You still need to monitor your child's computer use since no filter can block all objectionable content.

### **Step 6: Check Your Computer**

Sometimes, your computer may have evidence of inappropriate activity. Two easy ways to find out are to check your browser's history files and the cookies on your hard drive.

#### ***Checking Your Browser's History Files***

The history file shows what sites and what pages the browser has visited. For both

Internet Explorer and Firefox, selecting the history icon on the toolbar will open up a small window that will display the name of each web site visited. In the newly opened window, if you select a web site name, you can see all the pages that were visited on that site. If you see a suspicious site, check to see whether many pages were visited. If you see several pages under that web site, it is likely that it was not an accidental visit.

One warning sign is seeing no data in the history window during periods when you know that someone was spending a lot of time online. This may indicate that someone may have been trying to hide his or her online activities. Also, if you check the history window before you shut the computer down at night, but notice many new sites when you turn it on in the morning, someone has probably been online after hours.

### ***Setting The Number Of Days Of Browser History***

You can set your browser to track a certain number of days of history. Set this value to at least as long as the time between history reviews. For example, if you check once a week, set it to eight days.

### ***Review the Cookies***

A quick review of the cookies collected by your browser can also show if someone has visited a banned site. Keep in mind that a visit to one site may generate a third-party cookie, which is a cookie that is set from another site. Even though you can't tell the difference between regular and third-party cookies, all cookies can provide you with information. If a cookie is from a suspect site, it means either that site or a related site was visited.

Usually, it is easy to tell if a cookie is from a site that may have objectionable content. Often a domain name may have some relationship to the content of the associated web site. If several cookies appear to be from the same category of content, then it may indicate a pattern of behavior rather than just an accidental encounter with suspect material.

### **Step 7: Check Your Computer's Hard Drive**

If you believe inappropriate content has been saved in your computer, you can search the hard drive for any offending files. The Windows Explorer file management program allows you to search for files by file type, file size, file name, and you can even search for particular words and phrases in a file. Perhaps the easiest kinds of files to find are video files, graphics files, and very large files. For graphics or video files, search for file names ending in ".jpg," ".gif," ".bmp," ".avi," ".mov," ".wmv," "m4v," and ".mp4." When it comes to size, start looking for files larger than one megabyte. Increasing the file size will produce fewer files, and decreasing the limit will increase the number of files.

### **Top 10 Tips About Inappropriate Content**

1. Your family should have very clear rules about what is allowed and what is not allowed.
2. Your family rules should apply at home and away from home.
3. Inappropriate content may be sent to a family member or a family member may look for it.

4. Anyone can accidentally encounter inappropriate content online or in an email.
5. Following this book's suggestions for dealing with unwanted email and for doing online searches can help prevent accidental exposure.
6. You can use filters on your home computer to limit the kind of content that can be displayed.
- 7 You may also be able to use a filter in an online service such as a search engine.
8. Inappropriate content can be in an email, on a web site, on a hard drive, or stored offline.
9. Inappropriate content can be in any format, including text, graphics, or video.
10. Evidence of inappropriate activities can be in a browser's history or cookie file, in an online account, on a hard drive, or stored offline.

[Back to Table of Contents](#)



## CHAPTER 12: ONLINE AT SCHOOL AND THE LIBRARY

### In This Chapter

- Schools and the Internet
- Q&A About Being Online at School
- Top 10 Tips for Being Online at School
- Libraries and the Internet
- Q&A About Being Online at the Library
- Top 10 Tips for Being Online at the Library

The average child can go online at home, at the home of a friend or relative, at school, and at the library. Most of this book has been about what you can do to manage your child's Internet use at home, and most of this advice will also work managing Internet use at the home of a friend or a relative. This chapter will give you an idea about what happens at school or at the library. Your child needs your consent to go online in these places, but he will be under the supervision of other people. As a parent, you need to know a little about how the Internet works at school and at the library so you can make decisions that are in the best interests of your child.

### Schools and the Internet

For most public and private schools, the Internet is part of the regular school experience. It could be a major part of a child's experience if your child is issued a laptop and required to use it for most classes, or there may be very limited use of the Internet during class or after school. No matter how much or how little the school uses the Internet, the following will very likely be true:

- A parent has to agree to allow a child to use the Internet at school.
- The school will have rules and codes of conduct that the students must follow.
- There will be very little formal training provided for parents or students on how to use the Internet.

This book addresses the third point, and will likely go well beyond any training the school will provide for you or your child. You should also get to know about the rules at school and be willing to get involved if you feel that the school is not doing right by your child.

### Common School Rules on Internet Use

An Internet acceptable use policy is a set of rules or guidelines for how that resource may be used. Typical acceptable use policies for a school include the following:

- A list of acceptable uses of the Internet.
- A list of possible penalties for violations of the terms of the acceptable use agreement.
- A list of unacceptable uses of the Internet. This list would typically include things like sending or forwarding abusive or threatening messages, or altering information without permission.
- A statement that the school is not responsible for any problems or losses the users may have.



- A statement that users should not expect any privacy when it comes to email and other online communications.
- A statement to be signed by both the student and a parent or guardian indicating that the agreement was read and understood.

### **Q&A About Being Online at School**

***Will my child have to use the Internet at school?***

That will depend on the school. Some classes may require that students use the Internet to complete assignments. The school may also use the Internet to communicate with students about assignments or about administrative matters. Make sure you talk to your child or to a school official to find out about the school's policies.

***Will the school's agreement cover every situation?***

No set of rules can ever anticipate every possible situation. If you are aware of a situation that causes problems for your child or for other students, you may want to discuss it with your child or bring it to the attention of the school.

***How will I know if my child is using the school computer to do things like look at pornography?***

The school may inform parents if a child violates the school's Internet policies. You can also contact the school if you have any questions about your child's activities.

***Will my child be able to use the school's computer to send personal messages?***

Your child may be able to send personal messages, but because there is no guarantee of privacy when a student uses the school's computers, you may want to encourage your child to avoid the school's computer system when sending or receiving a sensitive private message.

***Should my child take a laptop to school to take notes and to do assignments?***

Unless the school requires the use of laptops, do not let your child take one to school. At best, it will be an inconvenience, since your child will have to carry a laptop as well as all required books and materials. Also, unless the school has wireless access, it will be difficult to use the computer to access the Internet.

***What if my child needs to go online, but we don't have a computer at home?***

You may be able to make arrangements with your child's school to get the online access your child needs. That could mean using the school's computer system after hours or using the computers at a public library.

***I have a computer at home that does not connect to the Internet. How can my child use it for school?***

Your computer probably has the basic kinds of word processing, spreadsheet, or presentation programs your child may need to write a paper or complete a project. Your child can do the work on the home computer and use a portable storage device like a flash drive to transfer work between home and school.

### **Top 10 Tips For Being Online At School**

- 1. Become familiar with school policies:** Ideally, these policies should be written and available for students and parents to review.
- 2. Assume that the school can review anything your child does online:** Normally, a

school has the right to review any activity that involves the school's computer system.

- 3. Report any visit to an inappropriate site:** Report any cases of being sent inappropriate material or any accidental visit to an inappropriate site.
- 4. Report any suspicious or unusual activity:** Make sure the school is aware of anything out of the ordinary involving the school's computer system.
- 5. Don't do anything online that is against school rules:** Assume activities that are not allowed in school are also not allowed online at school.
- 6. Stick to schoolwork:** Don't use the school's computers for activities unrelated to schoolwork.
- 7. Make backup copies of key files:** Keep backups somewhere outside the school's computer system.
- 8. Free speech is limited:** Typically, a school has stricter limits on what students can do online compared with rules at the library.
- 9. Make use of all the school's resources:** Internet access is just one educational resource available at school. Become familiar with the school library and other school resources that complement the Internet.
- 10. Use common sense when you are online:** Some situations may not be covered by a school rule or policy. When in doubt, use common sense.

#### **Libraries and the Internet**

The Internet has become a major part of many libraries and is one of the more popular services for children and for adults. In most cases, there is no additional charge to use the library's computers. Even if you know nothing about the Internet, that should not stop you from going online at the library. Most libraries also offer classes or other guidance to help you and your family learn how to use the Internet.

If you or your child do not already have a library card, go out and get one today, and do the same for everyone in your family. A library card at a library with online access gives your child the following benefits:

- Access to the Internet from the library.
- Access to library resources from your home computer.
- Checking out and renewing books online.
- Using online library resources for school projects.

Libraries also offer online services that do not require a library card, such as homework assistance, searching the library catalog, or asking librarians questions by email.

#### **The Role of the Library**

According to data from the American Library Association, an organization of library professionals, there are more than one hundred thousand libraries and four hundred thousand library professionals in the United States. In recent years, the availability of online access has increased dramatically for libraries across the United States, with most large- and medium-sized library systems offering some kind of online access.

Many of the goals of the American Library Association will be reflected in the policies of your local library. Among those goals are supporting First Amendment rights and promoting equal access to information services. What this means in practical terms is that libraries will allow any user of library services to access just about any online information without restrictions.

### **The Internet at the Library**

If you want your child to get the most out of the Internet at the library, you need to understand a few things about the library's role. Many library resources are available online, and a librarian can help you or your child use the Internet to find and use resources from other libraries or from elsewhere online. It is up to you as a parent to make sure your child uses these resources wisely and well.

While libraries may have classes on how to use the Internet, those classes will probably cover only part of what this book covers, most likely the kind of material contained in the chapters on how to use the Web and email. Make sure that your child is aware of the basics before going online at the library. If your child is new to the Internet or uncomfortable around strangers, you should be nearby when he goes online.

### **Library Rules and the Internet**

The rules of conduct in a public library are mostly the same whether you are using the Internet or not. So long as you or your child are not disturbing other users in the library and respecting their rights, you have the freedom to do what you please. There are additional rules for online activity by children. US federal laws, in particular the Child Internet Protection Act, affect library systems that accept federal funding. In these library systems, typically all computers in children's areas of the library are only allowed filtered Internet access.

While computers in designated children's areas of libraries may have restrictions, libraries may allow parents to have restrictions on a child's online access removed for computers in other parts of the library. At least one library system allows minors to remove filtering without parental permission. The King County Library system of the state of Washington requires anyone under 17 to have filtered access to library computers, but allows anyone who is at least 17 the option of requesting unfiltered access. Each library system may have different rules about filtering Internet access, so be sure to ask your librarian for details.

### **The Role of a Librarian**

Librarians can help you find and check out books and help you look up information, but they can do much more. You and your child should understand what a librarian can do for you, as well as what you should be doing to get the most out of the library experience.

#### ***What a Librarian Can Do for You***

Librarians can be of great help in the following areas:

- Finding resources within the library, including reference information such as encyclopedias.
- Finding resources elsewhere in the library system.
- Finding the key resources in a specific area.

- Finding resources for answering specific questions.

### ***What You or Your Child Should be Doing***

To get the most out of a library, you and your child should:

- Find out what you can do online at the library.
- Find out what resources can help with schoolwork.
- Learn how to ask a librarian the right questions.

The first point is easy; just go to the library and either log on one of the computers supplied by the library, or if you have a laptop log on from your own machine. If you have not yet been online at the library, find out how to get access on your next visit. If you use the library's computer, you would also have to have an account with the library. Libraries that allow visitors to use their wireless network sometimes requires an account, and sometimes not. Perhaps most important thing that you and your child can do at the library is learn how to use the expertise of a librarian. The following section should give you or your child the confidence to ask a librarian a question.

### **How to Use a Librarian**

Most library patrons know how to locate or check out books from library or how to use the library's computer system. However, you or your child will need to know more if you want him to use all that the library has to offer. On your next visit, meet with a library professional to discuss what services are available.

For questions that require a quick answer from a reference source, a librarian can help identify the best resource. If the task is more complicated, like doing research for a school project, you or your child needs to do the following before approaching a librarian:

- Take the time to understand what you need.
- Ask for help on a specific question or problem.
- Tell the librarian why you need the information and how it will be used.
- Tell the librarian what you already know.
- Ask the librarian to point out any resources that might help you.

None of the above points have anything to do with the Internet. That's because at the library, the Internet is just one of the tools that you and your child can use to find information.

### **Q&A About Being Online at the Library**

#### ***Will my child's library have Internet filters?***

While US federal laws and regulations may require filtered access for computers in the children's area of the library, different libraries interpret the rules differently for filtering elsewhere in the library. Check with your library to see what the requirements are and what options you and your children may have for filtering.

#### ***Can I ask the librarian to check on what sites my child visited while at the library?***

Probably not. Many libraries delete information about a patron's computer usage after a patron logs out. Even if the data was not deleted, libraries are very protective of every patron's privacy and will likely not agree to this kind of request.

***Can people watch pornography at the library?***

In most libraries, yes. Many libraries in the United States permit anyone who is allowed to have unfiltered Internet access to view anything online that is legal. That includes most sexually explicit material.

***If I see someone watching pornography on one of the library computers, can I tell that person to stop?***

Unless that person is causing a disturbance, such as making noise or bothering other people, the library staff will probably not ask that person to stop. You may ask your librarian if there are other options available, such as moving you to another computer or perhaps putting a privacy screen on the other patron's computer.

***How long can I be online on a library computer?***

That depends on the library. Most libraries limit computer use to about an hour per day. If the library has wireless access, you may be able to have unlimited time online if you have a laptop with wireless capability.

***Can I ask the librarian to watch my child and to prevent him from seeing objectionable things online?***

The librarian is not responsible for what your child does online. It is your responsibility as a parent to oversee what your child does online. If you are unwilling or unable to do this, then your child should not be online at the library.

***Are there computers at the library that block pornography and other inappropriate material?***

Libraries sometimes arrange computers so that those in certain areas are all filtered. Check with your library to see which computers are always filtered and which ones are not.

***Can my child do school work on library computers?***

Library computers may or may not have the basic kinds of software students need to write reports and presentations. Check with your librarian to see what is available.

**Top 10 Tips for Being Online at the Library**

- 1. Get a library card:** You will need a library card to go online at the library. If you use more than one library system, get a card for each of them.
- 2. Supervise your child at the library:** The librarian is not there to look after your child. If your child needs an adult nearby, that person should be you.
- 3. Check the filters on your accounts:** Make sure your child has appropriate filters for his library account.
- 4. Leave other users alone:** Free speech means other library visitors can do whatever they want online, so long they are not breaking the library's rules or bothering others.
- 5. Don't let other people bother you:** If someone interferes with what you are doing online, contact a staff person immediately.
- 6. Make visiting the library a regular habit:** This should be the case even if there is not a single computer in the building.
- 7. Learn how to work with a librarian:** Make sure you and your child are comfortable

with going to a librarian to ask questions.

**8. Learn how to work with a librarian online:** This will allow your child to easily access more library resources.

**9. Make use of all the library's resources:** Make sure you and your child know about all the other resources the library may offer.

**10. Check out other library web sites:** Many library systems have online information and services that are available to the public.

[Back to Table of Contents](#)



## CHAPTER 13: BEYOND EMAIL AND WEB SITES

### In This Chapter

- The Evolving Internet
- Things You Should Always Do
- Instant Messaging
- Chat Rooms
- Social Networking
- Online Videos
- Photo Sharing
- Webcams

The Internet is far more than just email and the Web sites. This book has discussed online privacy, online security, email, and the searching the Web in detail because these four areas are at the heart of your family's online experience. If you make the effort to understand these four areas, understanding how to use other popular online services and technologies will not be a problem for you or your children.

This chapter will review several of the services and technologies that are popular with children and teenagers, and will recommend what you and your children can do to safely participate in these activities.

Keep in mind that many online applications perform several functions. For example, the same online service may allow users to use instant messaging, create a blog, or run a webcam. Make sure you understand the full capabilities of any online service your child uses.

### The Evolving Internet

One of the most important things to understand about the Internet is that it is always evolving and sometimes the evolution happens very quickly. By the time you hear about something new and popular online, it may already be an old fashioned technology for your child. Also something that may be difficult or expensive to do today may be very easy and free to use a few months from now. It is almost impossible to predict what will be available or popular in the future, but based on the past history of the Internet, the following trends are the ones you should expect:

#### **New Technologies**

A few years ago, about the only way to go online was with a desktop computer, and maybe a laptop. Today you desktops and laptops are still popular, but now you have you have smartphones like the iPhone, tablets like the iPad, and special devices like the Kindle. What will be the next big thing? Even the experts who develop technologies can only make a wild guess about what will be popular.

#### **New Combinations**

A few years ago, devices or online services were more specialized. For example, a few years ago, with a Gmail account you could do little more than send or receive email. Today, that same Gmail account lets you combine several things at once. A Gmail account can still be used send and receive email, but it can also be used to send and receive text messages, make phone calls, and create documents.

One of the areas where this is most noticeable is with cell phones. Many phones that are made today also include Internet capability. If you choose to allow your child to have her own cell phone, she will likely insist that it be like her friends' phone and have the capability to do things online.

### **New Internet Access Options**

Internet access is becoming easier for the public with many businesses providing free online access to customers. Also, there are many more options for accessing the Internet with portable devices like smartphones, tablets, and other specialized devices. Even if your child doesn't own or use one of these devices, it is likely that he knows someone who does.

### **Lower Prices and Greater Capability**

Two things that have been consistent with the Internet is that services and technologies either get cheaper, become more capable, or both. For example, Google provides most of their services for free, and the company is constantly either expanding the capability of those services or adding new ones to the public. Prices for the more affordable desktop and laptop computers have been relatively stable since the first edition of this book was published in 2007, but the capabilities of those computers have greatly increased.

### **Ease of Publishing**

The basic online skills that are emphasized in this book such as using email and search engines, don't add much, if any, information online for the public to see. Many of the more popular services such as social networking or photo sharing, make it very easy for your child to publish content that can be easily seen by others. If your child understands the basic privacy issues discussed earlier in this book, then he probably won't have problems using these other online services.

### **Things You Should Always Do**

No matter what your child does online, and no matter how Internet technology changes, you should have the ability to check on what she is doing. Following are things you should do for each online account or service your child uses:

**Write down key information:** Make sure that you have written down any user names, passwords, or other information needed to access the account.

**Become a registered user:** A registered user goes through some kind of registration process in order to use an online service. As a registered user, you can see how the service works, and what parts of it you want your child to avoid. Do this with your child so she can explain how she uses the service.

**Review the rules of the service:** Make sure that your child is observing the rules of the service. If your child does not meet a requirement, for example, being at least as old as the minimum age limit, then she should not use the service.

**Review your child's user profile:** Follow the suggestions in chapter 4 on privacy; that is, leave as much information blank as you can. If you have to submit something, use her online alias.

**Set rules for each service:** As you become familiar with how a service works and how your child uses it, devise sensible rules for her to follow while using that service.



### **Instant Messaging**

Also known as IM, this is an Internet-based application that allows almost instant written communication among two or more individuals. Typically it is a free service that may be included as an option within another service such as Gmail.

Instant messaging can be a much more personal kind of communication than email, and may be the preferred method of some cyberbullies for intimidating your child. Also, child predators may use IM to evaluate potential victims, taking advantage of the instant feedback of IM to get your child to reveal personal information or to arrange a meeting.

Some services, especially Twitter, combine elements of instant messaging with online publishing. Users have the option of sending short messages back and forth to an individual user, or can make that message available to anyone online.

Instant messaging can be a safe and useful application if you do things such as making sure you know who talks to your child using IM or related services like Twitter or reviewing past messages to make sure that the conversations are appropriate.

### **Chat Rooms**

These are online resources that allow two or more users exchange video, audio, or text messages with other active users. The conversation is usually text based, and ongoing conversations are accessible to everyone in the chat room, even those who are not actively engaged in any kind of conversation.

Chat rooms have the privacy issues mentioned for instant messaging. An additional issue is that of lurkers; these are people who visit a chat room to see what others are doing, but who remain anonymous by not posting any of their own messages. A lurker who means harm may join the conversation only after identifying a potential victim.

You shouldn't let your child use a chat room unless that child is under close supervision by you or another responsible person. If you are going to allow chat room visits, you may want to take the following precautions:

- Only allow visits to moderated chat rooms: These managed chat rooms are supposed to be focused on a particular subject, and you should make sure that the moderator is able to keep the room under control.
- Review conversations: If you don't have the ability to review past conversations, you may not want your child to use that chat room.

### **Social Networking**

This term is applied to online services that encourage personal or group interaction by allowing users to easily publish and exchange information about themselves and to build online profiles of themselves in order to attract people with similar interests. The most well-known and popular social networking service is Facebook, though similar services like MySpace are also popular.

Social networking sites allow users to create customized web pages that feature that user. The goal of many users is to invite other users of that same social networking site to become part of their online circle of friends. Facebook allows members to make detailed personal information available, and also allows users to do things like upload videos or

photos to their account.

There are some important limits to these kinds of services, one of the most important of which are minimum age limits. However, these services do not independently check this kind of information, so although only older children are supposed to use such services, there is nothing to stop them.

Most schools restrict visits to these kinds of sites, but the popular social networking sites like Facebook make it easy to use the service on laptops, desktops, tablets, or smartphones.

The biggest issue with social networking sites is privacy. These sites, as well as the friends of people who use these sites, encourage users to post as much personal and private information as they want, and the typical child simply has not had the life experience or judgment to make those decisions. Also, once this information is published to his or her account, it becomes easy for anyone who is allowed to view that account to copy the information and publish it elsewhere.

If your child is going to use a social networking site, there are several precautions you can take:

**Review your child's public profile:** Make sure the profile has no sensitive personal information such as photos, school, or phone number. Instead of his real name, your child should use his online alias. Also, remove anything that you do not want the rest of the world to see.

**Review your child's list of contacts:** Make sure that you know the people your child has invited to be part of his or her network and that they have a relationship with him outside of the Internet.

### **Online Videos**

Watching videos online has become a popular activity, with videos available at a number of sites like YouTube that are dedicated to providing video services. Videos can also be part of the content of other kinds of web sites. Video sharing sites like YouTube may also allow users to upload and share videos with the public. Also, social networking sites like Facebook may also let their users upload and share video.

The most important issue for parents is the content of the videos. YouTube and other video sharing sites have restrictions on content, but others may allow other kinds of videos, including those with explicit sexual content.

If your child is going to view videos online, there are several precautions you can take, including reviewing a web site's policies: If a site allows inappropriate content, you may want to add a family rule that makes that site off-limits. You may also want to use any available filtering on your home computer, in a search engine, or within a web site to limit what can be seen or downloaded.

### **Photo Sharing**

This is an online service that allows users to upload, organize, and distribute photos. The photos may either be available to anyone online, or restricted to invited guests. This function may be included in a site like Flickr which is dedicated to providing photo sharing services, or it may be included within another service such as a social networking

site.

Like the case with social networking sites, the biggest potential problem is privacy, both for your child and for your family. You should not permit any photo to be placed online that will allow anyone to identify or locate your child or your home. Also, you or your child should get permission before placing a photo of someone online if that person can be identified in the photo. If your child wants to start putting photos online, you should approve any photos your child wants to publish and remove any that you think are inappropriate.

Because many portable devices like smartphones and tablets also include cameras and Internet access, it is very easy to take a picture and within seconds upload that picture to a web site or social networking page. If you allow your child to use these kinds of portable devices to upload pictures, you should first make sure that he understands how to so responsibly.

### **Webcams**

A webcam is simply a digital camera that is connected to a computer and that can be used to send live images to a web site, chat room, or some other part of the Internet. The typical webcam on a home computer is set up to take pictures of the person at the keyboard. Many new laptops come with a built-in web cam.

Using webcams can lead to serious privacy and security issues. They are typically set up to broadcast images of whoever is sitting in front of the computer, so anyone looking at the video will know that person's gender and approximate age, two facts that most online predators want to know. If someone, especially a stranger, encourages your child to use a webcam or sends one as a gift, you should not allow it. This kind of request is a common tactic used by online child predators.

To protect your family's privacy and security, you should not allow your child to broadcast live images to the Internet. When the webcam is not in use, you should either turn it off or cover the lens to prevent accidental video broadcasts.

[Back to Table of Contents](#)



## CHAPTER 14: MANAGING THE INTERNET

### In This Chapter

- Record Keeping
- Setting the Ground Rules
- Setting Up Your Home Computer
- Review of the Online Basics
- Things You Should Do Regularly
- The Stuff at the Back of the Book

Managing your family's online activities does not have to take a lot of time or be complicated. A little planning and preparation makes this process a lot easier.

#### Record Keeping

Your first management task is to set up a notebook to keep track of paperwork. A basic three-ring notebook with a few dividers should do just fine. Create a separate section for each family member and one for shared resources. The following forms, as well as a sample Internet use agreement, are all located in the free Family Forms Pack that you can download from [forms.speedbrake.com](http://forms.speedbrake.com):

**Ground Rules for Using the Computer and for Being Online:** You'll find several suggested rules in the next section. Feel free to add, delete, or edit the rules on that list.

**List of Online Activities:** Use this form to describe the activity or service, as well as any information needed to participate in the activity or the service.

**List of Additional Software:** Each of your family's computers should have its own list.

**List of Data Storage Devices:** Use this form to track each family member's data storage devices, as well as for shared storage devices.

#### Setting the Ground Rules

This is an activity that will evolve. As you become more familiar with how you and your child use the computer, you will come up with new rules regarding what your child is allowed to do online. Rules that best fit the philosophy of this book are listed below and are also available in the Family Forms Pack:

1. Parents make the rules when it comes to using the computer and the Internet.
2. Parents should respect a child's privacy, but should also be able to look at any file or get into any account at any time. This means that parents should know every password, user name, or screen name their child uses.
3. Parents must approve of any software before it is added to any computer at home.
4. The rules that apply at home also apply away from home.
5. Using the computer or being online is a privilege, not a right.
6. Protect your personal privacy online, as well as the privacy of others.
7. Do your best to stay safe online.
8. Everyone should help one another learn about computers and the Internet.
9. Don't do anything online that you want to keep a secret or that will embarrass you if

made public.

10. If something unexpected or scary happens while you are online or on the computer, tell someone.

### **Setting Up Your Home Computer**

Chapter 3 discussed the basic hardware and software you will need, and chapters 4 and 5 have details on how to set up your system to keep uninvited software and uninvited people away from your computer. You should also refer to any setup instructions provided by the manufacturer or your ISP.

#### **Wireless Security**

If you are using a wireless network at home, set up your system so you can protect your network from most intruders. If you have any questions about setting up the security, check your documentation or contact your ISP.

#### **Computer Security**

It is important that you have basic security protections in place before you go online or immediately after you go online. If your ISP provides protection, you will likely have to go online first. If you are providing your own security software, then make sure it is set up before you go online. Refer to your documentation to ensure you are setting things up correctly.

#### **Family Privacy Review**

Chapter 4 went into detail about how to protect your family's online privacy in the "Seven Steps to Online Privacy" section. Follow those steps either on a regular schedule or whenever you suspect a privacy problem with your family's online activities.

#### **Family Security Review**

Chapter 5 went into detail about improving your online security in the "Seven Steps to Online Security" section. Follow those steps either on a regular schedule or whenever you suspect a privacy problem with your family's online activities.

Because of the close relationship between online privacy and online security, you should perform privacy reviews the same time you perform security reviews.

### **Review of the Online Basics**

Chapters 6 through 13 covered several key online issues that you and your child should understand. If you have questions or problems in the following areas, review the appropriate chapter:

- Chapter 6: Internet Legal and Ethical Issues.
- Chapter 7: Cyberbullies and Child Predators.
- Chapter 8: Email Basics.
- Chapter 9: Dealing with Unwanted Email.
- Chapter 10: Web Basics.
- Chapter 11: Avoiding Inappropriate Content.
- Chapter 12: Schools, Libraries, and the Internet.
- Chapter 13: Beyond Email and Web Sites.

### **Things You Should Do Regularly**

Once you have set up your computer and you and your child have had time to get some online experience, you should take time regularly to see how things are going. While the following list does not include everything that you can do to keep up with your online child, taking these actions can often stop problems when they are still small:

- Any time you see your child doing something unusual on the computer, make sure it is an activity on the “List of Online Activities.”
- Regularly review your family’s online activities as described in the “Seven Steps” procedures from chapter 4 (privacy), chapter 5 (security), chapter 9 (email), and chapter 11 (inappropriate content).

### **Next Steps**

Now that you are done with this book, you’ve only started your work. The most important thing that you can do is to take action. It could be talking to your child, or taking your child to visit the library, or looking for an unfamiliar word in this book’s glossary. Whatever you do, keep moving forward. The sections at the back of the book are full of information that will be useful to you and your child. You should take the time to go through Appendix 1 or 2 to see if there are some free software options that may work for you, or event a new online resource to try out. If you make the effort, you and your child will be able to tell your own stories about parenting and the Internet.

[Back to Table of Contents](#)



## APPENDIX 1: FREE SOFTWARE

Any time that you add software to your computer, you want to avoid problems either with the software or with your computer, especially from viruses, spyware, and other malicious software. While it is possible that the free software that you download could have problems, you can avoid many potential issues by taking the following precautions:

**Look for reviews of the software:** Two excellent resources for finding reviews of free software are Sourceforge.net at <http://sourceforge.net> and Download.com at <http://www.download.com>. You can also find comparisons with similar software and find out additional information such as how frequently a program has been updated or downloaded.

**Trust your instincts:** If there is anything about a program or the maker of the program that arouse your suspicions, don't download the software.

**Use trusted software makers:** Many free programs available online were created by established software companies or nonprofit organizations. Many of these software makers also provide updates, documentation, and technical support.

### *Web Browsers*

#### **Chrome - [www.google.com/chrome](http://www.google.com/chrome)**

This browser was created by Google, and among other things allows users to access the Google search engine directly form the address bar

#### **Firefox - [www.mozilla.com/firefox/](http://www.mozilla.com/firefox/)**

Designed to aggressively block viruses, spyware, and popup ads. More features that can be added to the browser by using free downloads available on the Firefox site.

#### **Safari - [www.apple.com/safari/](http://www.apple.com/safari/)**

This browser is built into Apple's operating system that comes with Mac related desktops and laptops, and a version is also available for Windows based operating systems.

### *Business and Office Software*

#### **OpenOffice.org - [www.openoffice.org](http://www.openoffice.org)**

This office application suite includes a word processor, database manager, and presentation manager. These programs can read and work with files from a number of similar programs.

#### **Adobe Reader - [www.adobe.com/products/reader.html](http://www.adobe.com/products/reader.html)**

This software can be used to view, print, and search PDF files.

### *Communications Software*

#### **Skype - [www.skype.com](http://www.skype.com)**

This software is primarily designed for voice communication, but it also allows text-based instant messaging as well as a video connection with other Skype users.

### *Security-related Software*

#### **AVG Antivirus Free 2012 - [free.avg.com](http://free.avg.com)**

This antivirus software provides real-time antivirus protection for files and emails on computers running the Windows based operating system.

**Zone Alarm Free Firewall - [www.zonealarm.com](http://www.zonealarm.com)**

This basic firewall identifies and blocks hackers and malicious software from invading your computer. Available for computers running the Windows based operating system.

**Ad-Aware FREE -**

**[www.lavasoft.com/products/ad\\_aware\\_free.php/](http://www.lavasoft.com/products/ad_aware_free.php/)**

This antispysware product provides basic protection against spyware and helps to protect your private data. Available for computers running the Windows based operating system.

*Media Software*

**iTunes - [www.apple.com/itunes/download/](http://www.apple.com/itunes/download/)**

This media player and organizer allows you to play and manage video and audio files from several formats. It can also be used to download podcasts or to create audio CDs from material in your media collection. This application also has parental control options.

**QuickTime Player - [www.apple.com/quicktime/download/](http://www.apple.com/quicktime/download/)**

This digital media player can handle the audio and video formats used for Apple personal computers.

**Real Player - [www.real.com/realplayer/download](http://www.real.com/realplayer/download)**

This digital media player can play audio and graphics files associated with both Apple personal computers and computers that use the Windows operating system. It can act as a CD or DVD player, organize media files, and create CDs from your audio files.

[Back to Table of Contents](#)





## APPENDIX 2: ONLINE RESOURCES

In This Appendix

- Internet Safety and Security
- Online Parenting Resources
- Search Engines and Directories
- Copyright and Intellectual Property
- Online Email Options
- Computer and Internet Resources
- Book and Library Resources
- Information Resources
- World Geography and Politics Resources
- Financial Education
- Homework And Study Resources
- Writing and Literature Resources
- Photo Sharing Resources

### *Internet Safety and Security*

#### **SafeKids.com - [www.safekids.com](http://www.safekids.com)**

A family-oriented guide to making the Internet fun, safe, and productive. Contains links to informational sites and to articles on computer and Internet safety and security.

#### **Komando Kids -**

##### **[www.komando.com/kids/parent-tips.aspx](http://www.komando.com/kids/parent-tips.aspx)**

This part of radio talk show host Kim Komando's web site provides links to many of her Internet-related articles.

#### **US Federal Trade Commission -**

##### **[www.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/idtheft/)**

This is a comprehensive resource for understanding identity theft, including how you can detect and deter such crimes, and specific actions to perform if you are a victim.

#### **GetNetWise - [www.getnetwise.org](http://www.getnetwise.org)**

This site, sponsored by the Internet industry and by various public interest organizations, provides resources and advice for avoiding and minimizing Internet-related risks.

#### **National Center for Missing and Exploited Children -**

##### **[www.missingkids.com](http://www.missingkids.com)**

The mission of this nonprofit organization is to help prevent child abduction and sexual exploitation; help find missing children; and assist victims of child abduction and sexual exploitation.

#### **Net Family News - [netfamilynews.org](http://netfamilynews.org)**

This nonprofit organization provides a forum for technology and media issues that concern children. Includes a weekly newsletter and other resources.

#### **OnGuardOnline.gov - [www.onguardonline.gov](http://www.onguardonline.gov)**

This US Federal Trade Commission site provides advice on how to identify and avoid fraudulent and deceptive practices, and tips on protecting both your personal information and your computer from online threats.

**NetSmartz - [www.netsmartz.org](http://www.netsmartz.org)**

Operated by the National Center for Missing and Exploited Children, this site provides resources for understanding how to stay safer online.

*Online Parenting Resources*

**Childnet International - [www.childnet-int.org](http://www.childnet-int.org)**

This nonprofit organization from the United Kingdom organizes a number of projects that provide useful information for both parents and children on how to use the Internet.

**SuperKids - [www.superkids.com](http://www.superkids.com)**

The site has reviews and ratings of educational software and links to online and offline educational tools.

**Yahoo! Family Resource Center - [family.yahoo.com](http://family.yahoo.com)**

The site has advice for safe browsing and safe communication, as well as links to the Yahoo!igans! online guide for kids.

*Search Engines and Directories*

**Open Directory Project - [www.dmoz.com](http://www.dmoz.com)**

Sites in this directory are screened by a team of volunteers. By selecting the advanced link on the home page, you can limit search results to material appropriate for children, teenagers, and mature teenagers.

**Google - [www.google.com](http://www.google.com)**

The most popular search engine on the Web, the site includes language translation, language specific searching, and search filtering.

**KidsClick! - [www.kidsclick.org](http://www.kidsclick.org)**

This directory is a project of the Ramapo Catskill Library System and is a guide to sites that are considered to be entertaining or enlightening for children.

**Yahoo! Search - [search.yahoo.com](http://search.yahoo.com)**

This search engine allows users to filter search results.

**Yahoo! Directory - [dir.yahoo.com](http://dir.yahoo.com)**

This site has direct links to the major subject areas of the Yahoo! Directory, as well as a search function that allows you to search either the Web or the Yahoo! Directory.

**Yahoo! Kids - [kids.yahoo.com/](http://kids.yahoo.com/)**

This combination of search engine and directory will provide search results that are designed to be appropriate for children.

**Bing! - [www.bing.com](http://www.bing.com)**

This is one of the three biggest search engines and also allows users to filter search results.

*Copyright and Intellectual Property*

**Creative Commons - [www.creativecommons.org](http://www.creativecommons.org)**

Provides extensive resources that explain the concept of a Creative Commons License, how it differs from a traditional copyright, and how material with such a license may be used.

**Public Domain Music List - [www.pdinfo.com/list.htm](http://www.pdinfo.com/list.htm)**

A database of songs and musical works published before 1923 in the United States and that are now in the public domain.

**United States Copyright Office - [www.copyright.gov](http://www.copyright.gov)**

Provides extensive information on copyright and fair use, and information on how to register a copyright.

*Online Email Options*

**Gmail - [www.gmail.com](http://www.gmail.com)**

This full-featured email account can also be used to sign into a wide variety of free Google online services.

**Yahoo! Mail - [mail.yahoo.com](http://mail.yahoo.com)**

Like Gmail, this online email account may also be needed to sign into some online services.

*Computer and Internet Resources*

**Acronym Finder - [www.acronymfinder.com](http://www.acronymfinder.com)**

A searchable database of hundreds of thousands of acronyms and abbreviations related to computers, telecommunications, technology, and the military.

**Ask Bob Rankin - [www.askbobrankin.com](http://www.askbobrankin.com)**

Programmer and computer technology author Bob Rankin provides easy-to-understand technical advice for a number of Internet-related subjects such as online multimedia, security, privacy, and search engines.

**AskLeo! - [ask-leo.com](http://ask-leo.com)**

A resource with links to hundreds of questions and answers about personal computers.

**ComputerHope.com - [www.computerhope.com](http://www.computerhope.com)**

A collection of free services that allows any user to access a database of extensive computer-related information, including hardware and software support for a variety of systems.

**Download.com - [www.download.com](http://www.download.com)**

The site has a wide range of free software for download, including security-related software. The site also has extensive tutorials and other resources that explain how to use software and how to use the Internet.

**Internet101.org - [www.internet101.org](http://www.internet101.org)**

A guide that explains the basics of the Internet in plain English. It provides a short history plus background information on several topics, including email, chat, viruses, searching, online shopping, and newsgroups.

**Learn the Net.com - [www.learnthenet.com](http://www.learnthenet.com)**

The site provides a basic understanding of how to set up and use a personal computer and how use various online services.

**NetLingo - [www.netlingo.com](http://www.netlingo.com)**

Contains definitions to thousands of computer- and Internet-related terms. Also has explanations for many of the acronyms and slang terms that are often used in email,

instant messaging, and other online communications.

**Sourceforge.net - [sourceforge.net](http://sourceforge.net)**

This site has a wide range of free software for download, and is one of the largest online resources for open source projects. These are software projects run by volunteers who work together to develop new software.

**Urban Dictionary - [www.urbandictionary.com](http://www.urbandictionary.com)**

A user-generated dictionary of slang English words and phrases. The site contains million definitions, some of which are not suitable for children.

***Book and Library Resources***

**Answers.com - [www.answers.com](http://www.answers.com)**

This resource draws from reference works from traditional publishers and online reference sources.

**Bartleby.com - [www.bartleby.com](http://www.bartleby.com)**

A multiple reference site that has links to several sources for quotations, encyclopedias, and numerous books from the Harvard Classics series.

**Federal Resources for Education Excellence - [www.free.ed.gov](http://www.free.ed.gov)**

Site has links to more than 1,500 education resources created by numerous US federal agencies.

**Google Book Search - [books.google.com](http://books.google.com)**

This search engine allows a user to find books using the author's name, the book's title, or even by using words and phrases that may be in the book. Some books have their entire contents available online and others may only have limited content available. A user can also find links to local libraries that may have the book in their collections.

**The Internet Public Library - [www.ipl.org](http://www.ipl.org)**

This site from the University of Michigan School of Information provides library services to Internet users. Activities include finding, evaluating, and organizing information resources.

**Library of Congress Online Catalog - [catalog.loc.gov](http://catalog.loc.gov)**

This search engine allows a user to find books by author, title, subject, call number, or keyword. This site also has links to the Library's photographic and audio catalogs.

**Library of Congress Ask a Librarian Service - [www.loc.gov/rr/askalib/](http://www.loc.gov/rr/askalib/)**

This site shows users how to use email, regular mail, phone, or fax to ask questions of Library of Congress reference librarians.

**Library of Congress Virtual Reference Shelf - [www.loc.gov/rr/askalib/virtualref.html](http://www.loc.gov/rr/askalib/virtualref.html)**

A directory with links to dozens of different online reference sources in areas such as abbreviations, almanacs, quotations, statistics, music, and literature.

**The Online Books Page - [onlinebooks.library.upenn.edu](http://onlinebooks.library.upenn.edu)**

This resource from the University of Pennsylvania Library contains a searchable database of thousands of books that can be viewed for free online.

**Project Gutenberg - [www.gutenberg.org](http://www.gutenberg.org)**

This resource contains a searchable database of more than 36,000 books that can be downloaded for free.

*Information Resources*

**The Free Dictionary - [www.thefreedictionary.com](http://www.thefreedictionary.com)**

A multiple reference site that allows searches on specialized dictionaries for finance, computing, medicine, and law, as well as searches in the online Columbia Encyclopedia.

**HowStuffWorks - [www.howstuffworks.com](http://www.howstuffworks.com)**

A source of unbiased, and easy-to-understand explanations of how things work. Areas covered include technology, social behaviors, and consumer products. The site also has consumer opinions and exclusive access to independent expert ratings and reviews.

**Infoplease - [www.infoplease.com](http://www.infoplease.com)**

Searchable almanac, dictionary, atlas, and encyclopedia.

**The Straight Dope - [www.straightdope.com](http://www.straightdope.com)**

A searchable database of the syndicated weekly question and answer column by Cecil Adams. The site has links to most of the columns from the past ten years and to selected columns going back to 1973.

**The Urban Legends Reference Pages - [www.snopes.com](http://www.snopes.com)**

This site is devoted to the study of contemporary lore, with an extensive collection of rumors, urban legends, and other claims that are researched and judged to be either true, false, or something in between.

**Wikipedia - [www.wikipedia.org](http://www.wikipedia.org)**

This online encyclopedia is maintained by volunteers and contains entries on topics found in encyclopedias, as well as on topics typically found in almanacs and news publications. Entries may be added or removed at any time by volunteers, and may contain material that parents could find objectionable or offensive.

*World Geography and Politics Resources*

**Google Maps - [maps.google.com](http://maps.google.com)**

This site provides detailed street maps for the area around a given address, can provide detailed travel directions, and can also show either satellite photos or satellite photos with an overlay of a street map.

**The National Geographic Society - [nationalgeographic.com](http://nationalgeographic.com)**

This site has several geography resources, including an online atlas and printable maps. It also has information about the National Geographic Bee, an academic competition for fourth to eighth grade students.

**Perry-Castañeda Library Map Collection - [www.lib.utexas.edu/maps/](http://www.lib.utexas.edu/maps/)**

A collection of mostly public domain maps from the University of Texas Libraries. Includes historical and contemporary maps covering the entire world.

**The World Factbook -**

**<https://www.cia.gov/cia/publications/factbook/>**

This site is based on the reference book of the same name that is published by the US Central Intelligence Agency. The site has factual information on the political and social situations of the world's nations. Other information includes maps, natural resources, legal systems, political parties, and mortality rates. All information in the book or on the web site, except for the official seal of the CIA, is in the public domain.

**WorldStatesmen.org - [www.worldstatesmen.org](http://www.worldstatesmen.org)**

This site is a frequently updated encyclopedia of all the leaders of nations and territories. International organizations and recent religious leaders are listed separately. This site provides detailed chronologies, flags, national anthems, maps and indexes.

*Financial Education*

**Rich Kid Smart Kid - [richkidsmartkid.com](http://richkidsmartkid.com)**

Created by the Foundation for Financial Literacy, this site is dedicated to increasing the financial literacy of children. There are extensive resources for children, including online financial education games. There are also grade-specific activities that educators can use to understand the basics of finance and entrepreneurship.

*Homework And Study Resources*

**Awesome Library - [www.awesomelibrary.org](http://www.awesomelibrary.org)**

A directory of more than 30,000 educational resources for kindergarten through high school with different sections aimed at children, parents, and teachers.

**How-To-Study.com - [www.how-to-study.com](http://www.how-to-study.com)**

A study skills resource site with free advice on study skills, study strategies, and study tips in areas such as test taking, reading comprehension, and writing techniques.

**Infoplease Homework Center -  
[www.infoplease.com/homework/](http://www.infoplease.com/homework/)**

Drawing on the resources of the Infoplease.com site, this section of that site serves as a directory to resources for the subject areas of writing, geography, history, language arts, mathematics, science, and social studies. It also includes links for research and study skills.

*Writing and Literature Resources*

**Dr. Grammar - [www.drgrammar.org/](http://www.drgrammar.org/)**

This resource from the University of Northern Iowa answers questions about the proper use of words, punctuation, and grammar.

**Encyclopedia Mythica - [www.pantheon.org](http://www.pantheon.org)**

An online encyclopedia of mythology, folklore, and religion that is divided by continent, with further subdivisions to make searching easier. The site also has hundreds of images containing many kinds of deities, heroes, and strange creatures of every description.

**Mr. William Shakespeare and the Internet -  
[shakespeare.palomar.edu](http://shakespeare.palomar.edu)**

This resource from Palomar College is a comprehensive annotated guide to the scholarly Shakespeare resources available on Internet.

**RhymeZone - [www.rhymezone.com](http://www.rhymezone.com)**

A search engine for rhymes where the user enters a word or phrase and the site provides suggested rhyming words, as well as synonyms, definitions, and other information.

**The Poetry Archive - [www.poetryarchive.org](http://www.poetryarchive.org)**

This site contains a collection of recordings of poets reading their own work, with sections of the site for students, teachers, and children.

**Punctuation Made Simple -  
[ilt.ilstu.edu/golson/punctuation/](http://ilt.ilstu.edu/golson/punctuation/)**

This grammar resource from Illinois State University provides visitors with a general idea of how to use colons, semicolons, commas, dashes, and apostrophes.

**Purdue University Online Writing Lab -  
[owl.english.purdue.edu/owl/](http://owl.english.purdue.edu/owl/)**

This writing resource site has tutorials on grammar, sentence structure, English for non-native writers of English, creative writing, technical writing, and citation styles.

**University of Wisconsin Writing Center -  
[www.wisc.edu/writing/Handbook/](http://www.wisc.edu/writing/Handbook/)**

A concise resource on basic writing, including the stages of the writing process, advice on grammar and punctuation, and tips on improving writing style.

*Photo Sharing Resources*

**Flickr - [www.flickr.com](http://www.flickr.com)**

This site allows you to upload photos from the Web, by email, from home computers, or from mobile devices. You must have a Yahoo! account to use the service.

**Picasa Web Albums - [picasaweb.google.com](http://picasaweb.google.com)**

This site allows you to share photos online. You must have a Gmail account to use this resource.

[Back to Table of Contents](#)



## **GLOSSARY**

### **A-B-C-D**

**Acceptable Use** - A set of rules or guidelines that limit how a resource such as Internet access may be used.

**Adware** - Software that allows advertising to appear while the user is online and possibly when the user is offline. Adware may be included as part of another software program. See also Malware, Spyware, Trojan Horse, Virus, and Worm.

**Antispyware Software** - Software designed to detect or remove spyware, or to prevent spyware from being installed. See also Virus, Antivirus Software, Firewall, and Spyware.

**Antivirus Software** - Software designed to detect or remove software viruses from a single computer or from a computer network. See also Antispyware Software, Firewall, Spyware, and Virus.

**Application** - A computer program that is designed to do a particular task, such as browsing or games.

**Attachment** - A file that is sent as part of an email message. See also Bcc, Body, Cc, From, Header, Subject, and To.

**Backup** - A copy of data, software, or other information that is ideally stored in a place physically separate from the original information.

**Bandwidth** - A measure of the capacity of a communication channel, such as the rate that data can flow through an Internet connection, typically measured in bits per second. See also Bit and Binary.

**Bcc** - Blind Carbon Copy. This is one of the three address fields in the header of an email. This field is not visible to the recipient of an email. See also Email, Header, Subject, From, To, Body, Attachment, and Cc.

**Binary** - Information made up entirely of ones or zeros.

**Bit** - Binary Digit. A single-digit number that takes on the value of either one or zero.

**Blind Carbon Copy** - See Bcc.

**Blog** - Short for Web log, this is a journal or diary that is available on the Web. The content could include text, graphics, or other media.

**Body** - The portion of an email that contains the message. See also Header, Subject, From, To, Cc, Attachment, and Bcc.

**Bookmark** - A web browser feature that allows a user to store the location of a web page or other online resource so that it can be quickly accessed later without typing the full address of the resource.

**Broadband** - The term is commonly used to refer to Internet access via cable modems, DSL, and wireless technologies where the bandwidth is usually significantly higher than that of a dial-up connection. See also Bandwidth, DSL, Dial-up, Cable Modem, and Wireless Connection.

**Browse** - To follow links in a page to get from one resource to another on the Web.



**Browser** - A software program such as Internet Explorer or Firefox that allows a computer to interpret, display, or access information from the Internet. The information displayed is typically some combination of text, graphics, and sound. See also Client.

**Buddy List** - A feature of the AOL Instant Messenger instant messaging program that allows a user to view the online status and sometimes the profile of selected users. See also Contact List, Profile, Social Networking, and IM.

**Bulletin Board** - See Newsgroup.

**Burn** - To write data to a compact disc. This term is usually used in the context of copying a music file or some other kind of audio file onto a compact disc. See also Rip.

**Byte** - A unit of measure of computer memory that is equal to eight binary digits or roughly one character of information. See also Kilobyte, Megabyte, and Gigabyte.

**Cable Modem** - A connection to the Internet using a cable connection that is separate from a telephone line. The cable may be dedicated for Internet access or it may carry other data such as television signals. See also Dial-up, Wireless Connection, and DSL.

**Carbon Copy** - See Cc.

**Cc** - Carbon Copy. This is one of the three address fields in the header of an email. Any recipient will be able to see any address listed in this field. See also Email, Header, Subject, From, To, Body, Attachment, and Bcc.

**CD-ROM** - Compact Disc Read-Only Memory. A computer storage medium for digitized information, including data and computer programs. See also DVD.

**Chain Letter** - An email that encourages the recipient to forward the message to several others. See also Spam and Forward.

**Chat** - Any form of interactive online communication that takes place in real time, typically through either a web site or through instant messaging software. Communication can be by text, audio, or video.

**Chat Room** - An online resource that allows two or more users to exchange text, audio, or video content that can be viewed almost instantly by other active users. The conversations are accessible to everyone in the chat room, even those who are not typing messages. See also IM, Lurker, Screen Name, and Real Time.

**Check Box** - A small square target area that a user can select in order to choose from a list of options, typically on a form or dialog box. Once selected, a check mark is placed within the square. See also Radio Button.

**Child Pornography** - Any kind of visual depiction that shows a person under the age of 18 engaged in sexually explicit conduct. The conduct does not have to involve either sexual acts or nudity. In the United States, it is illegal to produce, transmit, buy, sell, trade, or possess such material. See also Pornography and Obscene.

**Child Predator** - Any adult who actively works to develop a personal relationship with a child in order to cause some future harm either from an inappropriate or illegal online or offline relationship. See also Pedophile.

**Client** - A program on a computer or other device that requests services of information

from a server. Servers are typically used to store or generate information that is requested by a client program. See also Server.

Contact List - The group of people who are allowed to have an online relationship with a user, and who can view that user's online status and online profile. See also Buddy List, Social Networking, IM, and Chat Room.

Content - The text, graphics, and other information that is contained in an email, web page, or file.

Cookies - A small text file that a web site's server places on a computer that allows a browser to retain specific information about a web site visit. Such information may include things like a user name, user preferences, or pages visited. When the user makes a return visit, the web site's server collects and uses information stored in that file. See also Third-Party Cookies.

Copyright - A form of intellectual property protection that is provided by the laws of most countries. In general, it applies to most written and visual works. It is usually necessary to get the permission of a copyright holder before using a copyrighted work. See also Fair Use, Intellectual Property, and Piracy.

CPU - Central Processing Unit. This is the integrated circuit chip that performs the data processing and interprets the instructions given by the software and by the user. For a desktop computer, this term also refers to the component containing all the basic hardware, including the hard drive.

Crash - An unexpected shutdown of either a software program or a computer. Often, the system or program may remain active, but ceases to respond to a user's input.

Creative Commons License - A form of intellectual property license that allows works to be created and used under that license that is somewhere between full copyright protection and public domain. See also Public Domain and Copyright.

Cyberbullying - Repeated or coordinated cruel or harassing actions directed at an individual by means of email, instant message, text message, blogs, web sites, or other Internet-related means.

Cyberspace - The nonphysical reality created by a computer or by a network of computers. The term is often used as a metaphor for describing the Internet.

Data - A collection of unorganized facts that have not yet been processed into useful information.

Database - A collection of related information, stored in either physical or electronic form, that is focused on a particular subject or discipline.

Decryption - Decoding or unscrambling data in a way that will recreate the original data prior to being encrypted by the sender. See also Secure Socket Layer and Encryption.

Defamation - A false statement that causes harm to someone's reputation, or that causes that person to become a target of public contempt, hatred, ridicule, or condemnation. If the statement is spoken, it is referred to as slander, and if written or broadcast, as libel. See also Libel and Slander.

Default - The initial or basic settings of a software program or hardware device.

Defragment - The automated process of rearranging files and programs on a hard drive in order to allow a computer to run more efficiently.

Delete - To remove or erase.

Desktop - A personal computer that is composed of several components including a keyboard, display device, and a separate unit that contains the data, software, and the electronics. This also refers to the icons and other graphics visible on a computer's display when no applications are running. See also Laptop.

Dialog Box - A small window that appears within a larger display that either presents information or requests input. See also Toolbar, Menu Bar, and Pull-down Menu.

Dial-up - An Internet connection that requires the exclusive use of a standard phone line. See also DSL, Cable Modem, and Wireless Connection.

Digital - Relating to information that is transmitted or stored as a series of binary digits.

Digital Subscriber Line - See DSL.

Directory - Online, a directory is a service that organizes links to Internet resources by category or by some other criteria. In a personal computer, a directory is an index of the contents of the files in a part of the hard drive, containing information such as the name of a file, the size of a file, and the file's creation date. See also Folder.

Display - A screen or similar device that is used in conjunction with a personal computer.

Domain Name - This is the unique combination of numbers and characters that helps to identify the location of web pages or other Web resources. For example, in the URL <http://www.airsafe.com>, the domain name is [airsafe.com](http://www.airsafe.com). See also URL.

Download - The transfer of data or files from one computer to another. See also Download and Server.

Drop-down Menu - See Pull-down Menu.

DSL - Digital Subscriber Line. A technology for high-speed Internet access using standard phone lines that allows the line to be simultaneously used for Internet access and for making and receiving phone calls. DSL bandwidth is typically higher than the bandwidth of a dial-up connection and lower than that of a cable modem. See also Dial-up, Cable Modem, and Broadband.

DVD - Digital Video Disc. A computer storage medium for digitized information, including computer programs and data. It is similar to a CD-ROM, but stores much more data. See also CD-ROM.

## **E-F-G-H-I-J**

Ebook - A book-length publication that is designed to be read online, on a computer, or in some other kind of dedicated electronic device. See also Kindle.

Email - Electronic Mail. A generic term for messages composed and transmitted on a computer network. See also Header, Subject, From, To, Cc, and Bcc.

E-mail - See Email.

Encryption - The coding or scrambling of information in a way that can only be decoded or unscrambled by the recipient. See also Secure Socket Layer and Decryption.

End User License Agreement - See EULA.

ESSID - Extended Service Set Identifier. See also SSID.

EULA - A software creator's or online service provider's legal terms for using a product or service. See also Privacy Policy.

Executable File - A file that once opened or selected begins to run a software program.

Extension - The group of letters in a file name that occur after the period and that identify the type of file. For example, in the file name "example.txt," the extension "txt" indicates that the file is a plain text file.

External hard drive - This is a hard drive that is not built into a laptop or desktop computer, but that can be connected to a computer. Typically this kind of drive has much greater capacity than other portable data storage devices. See also Hard Drive.

Facebook - A social networking service that allows users to create a personal profile, and allow users to invite others into a private network where they can exchange messages with one another.

FAQ - Frequently Asked Questions. A list of commonly asked questions about a subject.

Fair Use - The legal use of copyrighted material without the permission of the copyright holder. See also Copyright and Piracy.

Favorites - See Bookmark.

File - An organized collection of data that can be saved or retrieved by a computer. Typical file types include, audio files, graphics files, text files, and video files.

File Extension - See Extension.

File Name - The name of a computer file. Usually, such names include a file name extension that is specific to the format of the file. For example, "partylist.mp3" is an audio file, and "partylist.txt" is a plain text file.

File Sharing - Accessing files on one computer from a different computer while using the Internet as the conduit for the data. See also Peer-to-Peer Networking.

Filter - Software or settings that limit the content that can be displayed or accessed by a computer.

Firefox - A browser developed by the Mozilla Foundation. This is open source software that is available as a free download. See also Internet Explorer, Open Source, Download, and Browser.

Firewall - Software that prevents unauthorized access to a computer connected to the Internet. See also Antivirus Software.

First Amendment - An amendment to the Constitution of the United States that among other things guarantees freedom of speech and freedom of the press. See also Free Speech.

Flash Drive - A portable device that is used to store data. Also known as a thumb drive, USB drive, or memory stick. Unlike a hard drive, this device does not contain any moving parts. See also Hard Drive.

Folder - An index of the contents of the files in a part of the hard drive, containing information such as the name of a file, the size of a file, and the file's creation date. See also Directory.

Forward - To redirect or resend an incoming email to one or more recipients. Many email applications will add an abbreviation like "Fw:" or "Fwd:" to the beginning of the subject line to indicate that the email originated with someone other than the previous sender.

Free Software - Software that can be obtained and used without cost, can be used for any purpose, and that can also be copied and distributed without cost. See also Open Source.

Free Speech - The right to express opinions, information, or ideas in public or in private, regardless of content, without interference by a government. See also First Amendment.

Freeware - See Free Software.

Frequently Asked Questions - See FAQ.

From - The field in the header of an email that identifies the sender of an email message. See also To, From, Cc, Body, Attachment, and Bcc.

GIF - Graphics Interchange Format. This is one of the common formats for encoding photographs and other visual information. GIF encoded files have the ".gif" extension.

Gigabyte - A unit of measure, equivalent to 1024 megabytes, that is used to compare data storage capacity. See also Byte, Kilobyte, and Megabyte.

Gmail - A free online email service from Google.

Graphics - Generic term for the visual content in a document or web page.

Graphics Interchange Format - See GIF.

Grooming - A process used by child predators to gain the trust of a potential victim of child sexual abuse by first building an online relationship using communications tools such as email, chat rooms, and instant messaging. See also IM, Chat Room, and Child Predator.

Hacker - Someone who attempts to gain unauthorized access to a computer or computer network.

Harassment - Words or actions that contribute to a hostile social environment and are directed at an individual or group based on characteristics such as gender, race, or age.

Hard Drive - A high-capacity data storage medium that contains the data and programs that are used by a computer. This device can be located within a computer or separate from the computer. See also External Hard Drive.

Header - The portion of an email that identifies the sender and recipients of the message, and sometimes other information such as the date and time the message was sent. See also Email, Subject, From, To, Body, Attachment, and Bcc.

History - A record of the web pages or other online resources that have been visited.

Home Page - The page on a web site that serves as the central focus or starting point for site visitors. Often, the address of the home page is the domain name preceded by "www."

Host - A computer that is connected directly to the Internet rather than indirectly, such as through the computers of an ISP.

Hot Spot - A location that has wireless Internet connections available to the public.

HTML - HyperText Markup Language. A computer language that is used to control how a browser displays a web page and how a web page is linked to other Web resources.

HTTP - HyperText Transfer Protocol. A protocol or set of rules used by servers and browsers for sending information across the Web. The characters "http://" that appear at the beginning of a URL refer to this protocol. See also Server and Browser.

Hyperlink - See Link.

Hypertext - Any document that contains one or more links to other documents. The links may be embedded within a word or phrase in the text, or within some other element such as a picture.

Hypertext Link - See Link.

HyperText Markup Language - See HTML.

HyperText Transfer Protocol - See HTTP.

Icon - A graphical representation of an item that when selected causes some kind of reaction or response such as starting a program or opening a file.

Identity Theft - The unauthorized use of personal information such as name, Social Security number, or date of birth in order to take on the identity of another person, often for the purpose of committing a crime.

IM - Instant Messaging or Instant Message. An online service that allows near instant text-based communication among two or more individuals. Can also refer to the content of a message sent using this technology. See also Chat Room.

Inbox - The default destination for incoming email in most email programs.

Information - Any communication or reception of knowledge such as facts, data, or opinions that can be transmitted, accessed, or stored using some medium.

Information Superhighway - See Cyberspace.

Instant Message or Instant Messaging - See IM.

Intellectual Property - Products of human intellectual effort such as inventions, musical performances, or written works that may be protected or controlled through copyrights, trademarks, or through other means. See also Copyright, Fair Use, and Piracy.

Internet - A worldwide collection of computer networks that uses several protocols whereby computers and other devices can communicate with each other. Email, instant messaging, and the Web are three of the most widely used applications on the Internet. See also Cyberspace.

Internet Explorer - A browser designed to work with the Windows operating system. See also Firefox, Windows, Open Source, Download, and Browser.

Internet Service Provider - See ISP.

Intranet - A computer network inside an organization that uses the same kinds of software and communications protocols as the publicly accessible Internet, but which is not accessible by users outside of the organization. See also Internet.

IP - Internet Protocol. The standard protocol used by computer networks and other systems or devices to communicate within the Internet.

IP Address - The numeric address of a computer, server, or other device that is connected to the Internet.

iPad - A popular tablet computer made by Apple that allows Internet access, multimedia capability, and the ability to use thousands of specialized programs, many of which can also be used on the iPod Touch and iPhone.

iPhone - A popular smartphone made by Apple that combines a telephone, Internet access, multimedia capability, and the ability to use thousands of specialized programs, many of which can also be used on the iPad and iPod Touch.

iPod Touch - A portable media player made by Apple that also has the ability to access the Internet and use thousands of specialized programs, many of which can also be used on the iPad and iPhone.

ISP - Internet Service Provider. An entity, usually a commercial enterprise, that provides access to the Internet, typically for a monthly fee.

JPEG - Joint Pictures Expert Group. This is a common format for encoding photographs and other graphics. JPEG encoded files have the “.jpg” extension.

Junk Email - See Spam.

### **K-L-M-N-O**

Key Phrase - Several words, usually enclosed with quotation marks, that are used in a search engine to locate online resources. See Keyword and Search Engine.

Key Site - A web site that provides a level of information or a level of service that is better than most or all of the available alternatives.

Keyword - A word that is used within a search engine to locate resources online. Search engines can process one or more of these words at a time. See Key Phrase and Search Engine.

Kilobyte - A unit of measure, equal to 1024 bytes, used to compare data storage capacity. See also Byte and Megabyte.

Kindle - A dedicated ebook reader from Amazon.com.

Laptop - A portable personal computer that contains within a single package a keyboard, data storage medium, display screen, and all the other necessary components. See also Desktop, Netbook, and Tablet Computer.

Libel - A false statement, written or broadcast, and that causes harm to someone's

reputation, or that causes that person to become a target of public contempt, hatred, ridicule, or condemnation. See also Defamation and Slander.

Link - These are coded parts of a web page that when selected allow a browser to access some other resource on the Internet. A link may appear as highlighted, colored, or underlined text, or as part of another element of a web page, such as a picture or some other graphical element.

Log Off - To disconnect from the Internet, from some other computer network, from a computer, or from some kind of application or online service.

Log On - To use a combination of a user name and a password to connect to the Internet, to a computer, to an application, or to an online service. See also User Name and Password.

Lurker - A person who may visit a chat room to read what other people type, but who remains anonymous by not posting any messages.

Mailing List - A list of email addresses that is managed by an organization or an individual and that is used to send email to those on the list.

Malicious Software - Any software designed to cause harm to a computer or the person using that computer. Effects may include slowing computer performance, tracking browsing habits, or stealing passwords or other valuable information. See also Virus, Worm, Adware, Trojan Horse, and Spyware.

Malware - See Malicious Software.

Media Player - Software that is able to play one or more types of audio and video files.

Megabyte - A unit of measure, equal to 1024 kilobytes, used to compare data storage capacity. See also Byte, Kilobyte, and Gigabyte.

Menu - A list of items, options, or commands that can be selected by the user. See also Menu Bar, Pull-down Menu, and Toolbar.

Menu Bar - A row of menu titles, usually at or near the top of a window, that when selected commands the program to perform some action or function. See also Pull-down Menu, Menu, and Toolbar.

Minor - A child under the age of 18.

Modem - A device that allows a computer to communicate with other devices or with the Internet.

Monitor - See Display.

Monitoring Software - Personal computer programs that allow a parent or caregiver to monitor a child's online activity without blocking access. See also Filter.

Mouse - This is a device that allows a user to position the cursor or to select icons or objects on the display.

MP3 - Moving Pictures Group Experts Layer 3. This is a format for a type of audio file that is often used for music and podcasts. This kind of file has an ".mp3" file extension.

Multimedia - A file, web page, or other resource that contains more than one type of



information, usually a combination of audio, graphic, or text information.

Net - See Internet.

Network - A group of two or more computers that are able to communicate with one another.

Newsgroup - An online community that is dedicated to the discussion of a particular topic. The discussion usually consists of posts on a topic and responses to those posts. See also Post.

Netbook - Small laptop computers that typically did not include a built-in optical drive, and had keyboards and display screens that were smaller than those of a laptop.

Notebook Computer - Another name for a laptop computer.

Obscene - Material that a judge or jury has determined to be sexually explicit, offensive to conventional standards of decency, and lacking in serious literary, scientific, political, or artistic, value. See also Pornography.

Office Application Suite - A group of programs used to create documents and perform functions appropriate for a business or academic environment. This group of programs typically includes a spreadsheet, word processor, and presentation manager. It may also include a database management program. See also Spreadsheet, Database, Presentation Manager, and Word Processor.

Offline - Used to describe information, resources, or activities that are not associated with accessing a computer network. Also used to describe the state of a system that has the capability to be online but that is not currently online.

Online - Used to describe the activities that involve accessing a computer network such as the Internet.

Online Profiling - The practice of compiling information about a user by tracking actions such as sites visited and items purchased. Personal information volunteered by the user or supplied by a third party may also be included.

Open Source - Software or other intellectual property that is freely distributed and can be modified without restriction by users. See also Intellectual Property.

Operating System - The basic software of a computer that controls all other software in the computer and any devices that are connected to the computer.

Opt-in - A policy where a user explicitly agrees to allow a web site or some other service provider to collect, use, or share personal information.

Opt out - A policy where a user can explicitly request that a web site or some other provider of a service not collect, use, or share personal information.

Optical Disc Drive - A device used to read or write information from a CD-ROM or DVD-ROM.

Outbox - The temporary file that most email programs use for temporary storage of outgoing email before that email is sent to its intended destination.

Outlook Express - An email program that is included with the Internet Explorer browser

of the Microsoft Corporation. See also Browser, Client, Email, and Internet Explorer.

Overblocking - A condition where an Internet filter denies access to content that a user is intended to be able to access. See also Underblocking and Filter.

### **P-Q-R-S-T**

P2P - See Peer-to-Peer Networking.

Parental Controls - Software settings that prevent children from accessing inappropriate Internet content.

Password - A combination of uppercase letters, lowercase letters, numbers, or other characters used to access a program, a computer, or a computer network.

PDF - Portable Document Format. This is a document format that can be viewed using a widely available and free PDF document reader. Documents created in a variety of other formats can be saved in this format.

Pedophile - An adult (male or female) who is either sexually attracted to a child or to children, or who engages in sexual activity with a child or with children. See also Child Predator.

Peer-to-Peer Network - A type of network where computers exchange files or communicate directly with each other, rather than through a central server. Often referred to as peer-to-peer, or P2P. See also File Sharing.

Personal Information - Data that can be used to identify or locate a person. Data includes, but is not limited to, user names, passwords, address, telephone number, job title, school, date of birth, and credit card numbers.

Pharming - A technique used by identity thieves where traffic is redirected from a legitimate web site address to another address, where the potential victim is then encouraged to voluntarily provide personal or financial information. See also Phishing and Privacy.

Phishing - A technique used by identity thieves or other criminals who use an emails, instant messages, popups, or other online communications to misrepresent their identity in order to obtain the personal or financial information of others. See also Pharming and Privacy.

Photo Organizer - A type of software that is used to manage the graphics files on a computer.

Photo Sharing - The process of uploading, organizing, and distributing photos or other graphic information online, usually through web sites dedicated to this function.

Piracy - Illegal or unauthorized copying, use, installation, or distribution of intellectual property such as software or music files. See also Fair Use, Copyright, and Intellectual Property.

Plugin - A small software program that adds features or functions to a larger program.

Podcast - An audio or video file distributed using the Internet. This term also refers to the method of delivery.

**Popunder** - Also written as pop-under. A type of browser window that behaves like a popup, except that it appears beneath the current browser window rather than on top of the current window. See also Popup.

**Popup** - Also written as pop-up. A type of browser window that appears on top of the current browser window while a user is visiting a web page. See also Popunder.

**Pornography** - Any material that is sexually explicit and that is intended to cause sexual arousal. Such material does not have to involve descriptions or depictions of nudity or sexual activity. In the United States, most forms of sexually explicit material are protected by the First Amendment, making it legal for adults to create, publish, or consume such material. See Child Pornography, First Amendment, and Obscene.

**Post** - A message entered into a newsgroup, chat room, web site, or other online resource.

**Presentation Manager** - A type of software used to create, edit, and display presentations by using a combination of text, drawings, graphics, audio and other media. See also Office Application Suite.

**Privacy** - The ability to control the amount of access that others have to your personal information and the amount of control that others have over your online experience.

**Privacy Policy** - A written policy associated with a web site that explains how data from users may be collected and used. Such policies may allow the user to opt-in or opt out from activities of the site. See also EULA.

**Profile** - Personal information that a user provides to an online service. Depending on the online service, this information may be accessible to other users of that service and may consist of items such as name, screen name, address, personal interests, photos, or other personal details. See also Buddy List, IM, and Social Networking.

**Program** - See Software and Application.

**Public Domain** - Intellectual property that is no longer under copyright protection, has failed to meet the requirements for copyright protection, or that was intentionally provided to the public free of copyright restrictions. Works in the public domain may be used freely without the permission of the work's creator or former copyright owner.

**Pull-down Menu** - A list of options that appears when you select an item on a toolbar. See also Toolbar and Dialog Box.

**Radio Button** - A small circular target area that a user can select in order to choose from a list of options, typically on a form or dialog box. Once selected, the interior of the circle usually changes to a dark color. See also Check Box.

**Real Time** - Interaction between two or more users or systems that occurs without any apparent delays.

**Reformat** - The process of erasing all files and programs on a hard drive, and reinstalling the operating system. See also Hard Drive and Operating System.

**Registered User** - A person who has to go through some kind of registration process in order to use a particular online service. See also User.

**Rip** - To copy data from a compact disc to either a personal computer hard drive or to

some other storage media. This term is usually used in the context of copying a music file or other audio file from a compact disc. See also Burn.

Router - A device that connects two or more networks. See also Modem, Wi-Fi, Wireless Connection, and Wireless Network.

Save - A command used to update a file with any editing changes. In most programs, this overwrites the previous version of the file.

Scam - A fraudulent scheme that usually involves one or more voluntary actions on the part of the victim.

Screen Name - An alias or pseudonym someone uses while communicating online. See also Chat Room, IM, and User Name.

Search - The act of looking for online resources through the use of a search engine or directory. See also Search Engine and Directory.

Search Box - An input field for search engine commands.

Search Engine - An online service that allows a user to find online resources by using one or more keywords or key phrases. Most search engines present the results of a search as a list of web pages where the position on that list depends on how well that page's contents match the search terms. See also Directory.

Secure Socket Layer - An Internet industry standard for encrypting and protecting information that is transmitted over the Internet. The URL for this kind of protocol begins with "https://" rather than the "http://" that is normally used.

Security - The ability to identify, manage, or eliminate threats to information, to technology, or to the well-being of a group or an individual.

Select - To choose an option in a program or web page by using either a mouse or keyboard commands.

Server - A computer that responds to requests for services or for information made by other computers in a network.

Service Mark - A combination of one or more words, symbols, or designs that distinguish services provided by one party from those provided by others. See also Copyright, Trademark, and Intellectual Property.

Service Set Identifier - See SSID.

Signature Block - The block of text at the end of the body of an email that typically has the sender's name and contact information. See also Signature File and Email.

Signature File - A short text file containing the signature block information that is placed at the end of an email message. See also Signature Block and Email.

Site - See Web Site.

Slander - A false statement that is spoken and that causes harm to someone's reputation, or that causes that person to become a target of public contempt, hatred, ridicule, or condemnation. See also Defamation and Libel.

Smartphone - A mobile phone that also combines several other functions, typically

including a media player, the ability to access the Internet, and both a still and video camera.

**Social Engineering** - The practice of getting access to sensitive personal information by persuading a potential victim to willingly provide the information or the means to access to the information. See also Identity Theft, Phishing, and Spam.

**Social Networking** - Online services that encourage personal or group interaction by allowing users to easily publish and exchange information about themselves using online tools and applications such as email, instant messaging, chat rooms and blogs.

**Software** - A set of logical instructions that either controls the behavior of computers and other electronic devices, or that provides some specific kind of functionality.

**Spam** - Popular term for unsolicited commercial email, often associated with the promotion of a product or service of questionable value. The term may also be applied to email containing chain letters, fraudulent promotions, and other information that lacks authority, usefulness, or validity.

**Spreadsheet** - A file type formatted so that an appropriate application will display the data in one or more rectangular grids, and that allows the user to perform calculations on data within the grids. This term also refers to software designed to create, edit, save, and print files of this type. See also Office Application Suite.

**Spyware** - A general term for software that collects data about a user's online activities and sends the information to someone else without the user's permission or knowledge. See also Adware, Virus, Worm, Trojan Horse, and Malware.

**SSID** - Service Set Identifier. The name that identifies a wireless network. See also Wireless Network, Wireless Connection, Router, Wi-Fi, and Encryption.

**SSL** - See Secure Socket Layer.

**Subject** - The field in the header of an email that contains a short description of the email's contents. See also To, From, Cc, Body, and Bcc.

**Surf** - To search for information on the Internet without either a goal or a systematic process.

**Surge Suppressor** - Electrical accessory designed to protect sensitive electronic devices from sudden and significant changes in voltage.

**Tab** - A visual element, shaped like the tab on a paper file folder, that is used to navigate in a browser window, dialog box, or other part of a display.

**Tablet Computer** - A small personal computer that typically uses a touch screen rather than a keyboard for user inputs. See also iPad

**Text Editor** - A simple word processing program that allows a user to create, edit, and print files containing only text characters, and that usually has very limited formatting options. See also Word Processor.

**Text Message** - A brief electronic message sent and received through a wireless network to or from a wireless device such as a cell phone or pager.

**To** - The field in the header of an email that identifies the recipients of an email. See also

Subject, From, Cc, Body, Attachment, and Bcc.

Third-Party Cookies - Cookies that are generated from a web site other than the one that the user is visiting.

Thumb Drive - See Flash Drive.

Toolbar - A row of words or icons displayed by an active software application that when selected activates a function or performs some kind of action.

Trademark - A social networking service that allows users to send and read short text messages of up to 140 characters in length.

Trojan Horse - A program that is designed to do something malicious to a computer or to a computer network, but that is disguised as a program designed to do something beneficial. See also Adware, Virus, Worm, Spyware, and Malicious Software.

Twitter - A program that is designed to do something malicious to a computer or to a computer network, but that is disguised as a program designed to do something beneficial. See also Adware, Virus, Worm, Spyware, and Malicious Software.

#### **U-V-W-X-Y-Z**

Underblocking - A condition where an Internet filter permits access to content that a user is not intended to access. See also Overblocking and Filter.

Uninstall - To remove a program from a computer.

Upload - The transfer of data or of one or more files from a user's computer to a server or to some other computer. See also Download and Server.

URL - Uniform Resource Locator. This is an addressing system that uses a combination of characters and numbers to uniquely identify and locate each resource on the Web. For most web pages, the characters "http://" precede the address. Some browsers do not require a user to type the characters "http://" to recognize the address.

USB - Universal Serial Bus. This is common type of computer connection that allows different kinds of hardware to be connected to and communicate with a computer.

User - A person who is accessing an information system or network, either directly or indirectly. See also Registered User.

Username - See User Name.

User Name - The name used to access a particular application, software program, online application, or network.

User Profile - See Profile.

Virus - A computer program designed to make copies of itself without any kind of user action or intervention. This kind of program can spread only after attaching itself to other programs or files, and is often designed to do something malicious to any computer that it infects. See also Adware, Antivirus Software, Worm, and Trojan Horse.

Voice Over Internet Protocol - Also known as VOIP or VoIP, this is a protocol and associated technology that allows users to make and receive telephone calls by using an Internet connection.

VOIP - See Voice Over Internet Protocol.

Web - A portion of the Internet that allows users to access data and services using a browser.

Web Browser - See Browser.

Webcam - A camera that is connected to a computer and that can be used to send live images to a web site, chat room, or some other part of the Internet.

Web Log - See Blog.

Web Page - One page of a document on the Web. It is usually a file that is written in HTML and stored on a server. Typically, each page has links to other online resources. Each page on the Web has an address called a Uniform Resource Locator or URL. See also HTML and Server.

Web Site - A set of related web pages that share a common domain name. See also Domain Name.

WEP - Wired Equivalent Privacy. An encryption protocol used in wireless networking. See also Router, Wireless Networking, WPA, and Encryption.

Wi-Fi - Wireless Fidelity. A communication protocol that allows computers and other devices to exchange data without the use of wires or cables. See also Wireless Connection and Router.

Wiki - A web site that allows users to add, remove, or edit content.

Window - A rectangular space on a computer screen that is created by a browser or other software.

Windows - A class of operating system software created by the Microsoft Corporation. The majority of existing personal computers use some variation of Windows.

Windows Explorer - The file management program included with many versions of the Windows operating system.

Wireless Access Point - See Router.

Wireless Connection - A method for connecting one or more computers to a network or to the Internet without using cables or wiring. See also Wi-Fi and Router.

Wireless Network - One or more computers that can access the Internet or that can communicate with one another without being connected by wires or cables. See also Wi-Fi, Wireless Connection, Router, and Modem.

Word Processor - Software that allows a user to create, edit, format, display, save, and print documents containing both text and graphics. See also Office Application Suite

World Wide Web - See Web

Worm - A virus program that can spread to other computers without attaching itself to other programs and without further action from a user. See also Malicious Software.

WPA - Wi-Fi Protected Access. An encryption protocol used in wireless networking. See also Router, Wireless Networking, WEP, and Encryption.

Write - To create or edit, and then save data to some kind of storage medium, such as the hard drive of a personal computer.

WWW - See Web.

[Back to Table of Contents](#)





## ABOUT THE AUTHOR

Todd Curtis is a parent and a published author who more than a decade ago created the Web's most popular airline safety site, AirSafe.com. He holds a PhD in aviation risk assessment from the Union Institute, as well as engineering degrees from MIT, the University of Texas, and Princeton. His aviation safety work has been featured by numerous news organizations, including the New York Times, and he has appeared on CNN, CBS, Fox News, Discovery Channel, Al Jazeera, the BBC, and National Public Radio. With this book, he combines his insights as a father, engineering risk assessment expert, and online pioneer to create an easy-to-use guide for managing and enhancing a child's online experience. Previously, he has published a number of technical papers in the areas of airline safety and aviation risk assessment and authored the 2000 book *Understanding Aviation Safety Data*.

### *Connect with Me Online*

Twitter: [twitter.com/airsafe](https://twitter.com/airsafe)

Facebook: [facebook.com/pages/Airsafecom/18541639875](https://facebook.com/pages/Airsafecom/18541639875)

LinkedIn: [linkedin.com/pub/dir/Todd/Curtis](https://linkedin.com/pub/dir/Todd/Curtis)

YouTube: [youtube.com/airsafe](https://youtube.com/airsafe)

Smashwords: [smashwords.com/profile/view/speedbrake](https://smashwords.com/profile/view/speedbrake)

Email: [tcurtis@speedbrake.com](mailto:tcurtis@speedbrake.com)

Phone: 202.596.2510