

The McAfee 10-Step Internet Safety Plan for Your Family

How to talk to kids, tweens,
teens, and novices of any age
about online security

10

Table of Contents

- 3 Introduction
- 4 Today's Internet:
Proceed with Caution
- 5 A 10-Step Safety Plan to Help
Protect Everyone in Your Family
- 17 The ABCs of Online Security:
 - 17 For Kids (3 to 7 years old)
 - 21 For Tweens (8 to 12 years old)
 - 26 For Teens (13 to 19 years old)
 - 30 For Novices of Any Age
- 33 About McAfee

10





Introduction

Millions of families worldwide use the Internet every day to learn, research, shop, buy, bank, invest, share photos, play games, download movies and music, connect with friends, meet new people, and engage in a host of other activities. Though cyberspace offers numerous benefits, opportunities, and conveniences, it is also increasingly risky, with **many new threats emerging daily**.

It is no surprise that cybercriminals are taking advantage of the Internet and the people who use it. You and your family members need to be on guard whenever you go online. In addition to installing robust security software from a trusted company to defend your family against hackers, identity thieves, email con artists, and predators, you need to **follow some basic Internet safety rules** and use good old-fashioned, real-world common sense. You need an Internet safety plan for your family.

As soon as family members become active online—and no matter what their age—it's time to educate them about cyber safety. **You should be aware** that even if you do not have a computer at home, PCs are available almost everywhere—at schools, libraries, friends' homes, and even in church basements. It's important for everyone to know the basics about protecting themselves in cyberspace.



Today's Internet: Proceed With Caution

- 50% of online teens have given out personal information¹
- Hackers are attacking PCs with Internet access every 39 seconds²
- According to McAfee® Avert Labs®, there are 222,000 known computer viruses out there now, and the number of threats is growing daily
- 30% of teens experienced cyberbullying one or more times during the school term³
- Internet crime is up 33% in 2008 from 2007⁴
- 31% of children have been exposed to harmful content¹
- 3.2 million people worldwide are defrauded by mass marketing scams annually⁵

1 EU Kids Online, Comparing children's online opportunities and risks across Europe (2006–2009)

2 Hackers Attack Every 39 Seconds – James Clark School of Engineering at the University of Maryland

3 theage.com.au

4 2008 Internet Crime Report, IC3

5 National Fraud Strategic Authority



A 10-Step Safety Plan to Help Protect Everyone in Your Family



Step 1

Consider Where You Place the Computer

In a home with children, where you place the family computer is one of the most important decisions you can make. We recommend that you set up the computer in a **high-traffic family area** and limit the number of hours your children spend on it. Be sure you have computer **security software** with parental controls like those found in McAfee products or use specific software designed to protect children online, like McAfee Family Protection.

Step 1



Step 2

Step 2 Work As a Team to Set Boundaries

Decide exactly what is okay and what is not okay with regard to:

- The kinds of websites that are appropriate to visit
- The chat rooms and forums that are appropriate to participate in:
 - Use only monitored chat rooms
 - Make sure your children avoid “.alt” chat rooms, which focus on alternative topics that may be inappropriate for young people
- The kinds of things your children can discuss online and language that is considered inappropriate



Step 3

Together, Agree Upon Family PC Rules

We recommend the following:

- Never log in with user names that reveal true identity or that are provocative
- Never reveal your passwords
- Never reveal phone numbers or addresses
- Never post information that reveals your identity
- Never post inappropriate photos or ones that may reveal your identity (for example: city or school names on shirts)
- Never share any information with strangers met online
- Never meet face-to-face with strangers met online
- Never open attachments from strangers

Once you have established the rules, post them next to the computer.

Step 3



Step 4

Sign an Agreement for Appropriate Online Behaviour

Write up an agreement or **use the one on the following page**, so that there is a clear understanding among all family members on appropriate computer use and **online behaviour**.

Step 4



Online Safety Pledge

Because using the computer and the Internet is a privilege I do not want to lose,

- I will surf, search, work, play, and chat safely whenever I go online
- I will follow all of the rules that we have agreed on
- I will not reveal my real name, my phone number, my address, or my passwords with online “friends”
- I will never meet in person with people I met online
- If I find myself in an online situation where I am unsafe or uncomfortable, I promise to let you (my parent/guardian/teacher) know so that you can assist me
- I commit to this pledge and recognise that there are consequences to every decision I make

Child’s Signature _____

- As your parent/guardian/teacher, I promise to make myself available to you when you ask for assistance and will help you resolve any problems that may arise in any way that I can.

Parent/Guardian/Teacher Signature _____



Step 5

Install Security Software

Make sure you have robust security software that protects your computer against viruses, hackers, and spyware. It should also filter offensive content, pictures, and websites. This software **should be updated frequently**, as new threats are emerging daily. Ideally, security that updates automatically—like McAfee **set-it-and-forget-it software**—is the best choice.

Step 5



Step 6

Use Parental Controls

All the major security software providers offer parental controls. Be sure to enable them. If you are using freeware or software that doesn't have parental controls, consider purchasing software that does. Take time to learn how these controls work, and use options that filter and block inappropriate material.

To completely protect your children online, use McAfee Family Protection software in addition to the parental controls in your security software. McAfee Family Protection software keeps children of all ages safe from exposure to inappropriate content, social networking risks, strangers, and other online threats.

Of course, these tools have their limitations. Nothing can take the place of attentive and responsive parents who monitor their children when they are online.

Step 6



Step 7

Step 7

Remind Family Members That People Met Online Are Strangers

Everyone who goes online must understand this:

No matter how often you chat with online “friends,” no matter how long you’ve been chatting, and no matter how well you think you know them, people you meet online are strangers. **It is easy to lie and pretend you are someone else when you are online.** Kids especially need to know that a new “friend” may really be a 40-year-old man rather than someone their own age.

Social networking websites like Bebo, Orkut and Facebook are an ideal way to meet new people online. Therefore, you must visit these sites and **check out your children’s profile** to ensure that inappropriate conversations are not taking place and that unacceptable photos are not being posted. You should also monitor your children’s instant messaging conversations to make sure they aren’t being pursued by an online predator.



Step 8

Step 8 Create Strong Passwords

To create passwords that are difficult to crack, start by using at least 8 characters and then use a combination of letters, numbers, and symbols. **Passwords should be changed periodically** to reduce the likelihood of a particular password being compromised over time.

Techniques for strong passwords:

- Use a vanity licence plate: "GR8way2B"
- Use several small words with punctuation marks: "Bindi#the^jungle@girl"
- Put punctuation in the middle of a word: "Beck%ham"
- Use an unusual way of contracting a word: "ftblplyr"
- Use the first letter of each word in a phrase, with a random number: "hard to crack this password" = "htc5tp"
- Don't share your passwords!



Step 9

Step 9

Check Your Computer's Security Software

Open whatever security software you are using and verify that your computer is protected by the following **three core protections: anti-virus, anti-spyware, and a firewall.**

These core protections should be augmented by anti-spam and safe search software like McAfee SiteAdvisor® that features anti-phishing protection and safety ratings. It is also a very good idea for families to have a suite of protections on home PCs that includes parental controls, like McAfee Family Protection software and identity theft prevention tools.



Step 10

Stay Informed

The more you know, the safer you will be. Check out McAfee's Security Advice Center for easy-to-read educational material on computer and Internet security: www.mcafee.com/advice.

Step 10



The ABCs of Online Security

For Kids 3–7 Years Old



A

Talking to young kids

When you talk to young children about Internet safety, do it with the computer turned off, so that you have their undivided attention. Start off by explaining that a computer is a tool and that the Internet is like a giant electronic library full of information.

Explain why it's important to be safe online because the computer can be an open door to your important personal information. Talk to them about how bad people can take control of your PC and break it, so that you have to buy a new one.

Explain to them why it's important not to share personal information with people online. Tell them not to use their real names and not to talk about where they live or what school they go to.



B

Create a special list of rules for computer use by young kids

The list should include:

- Do not download music or program files from websites without parental permission
- Use only monitored chat rooms where an adult actually monitors the chat
- Never send out a picture of yourself without talking to your parents first
- Do not use bad language
- Do not visit adult websites
- Share information only with people you know from the real world, such as classmates, friends, and family members
- Do not fill out online forms or surveys without a parent's help
- Use only special search engines for children like Ask for Kids and Yahoo! Kids



C

Use browsers and search engines especially designed for children

Make sure that your children are using browsers and search engines that do not display inappropriate words or images. Check that they come preloaded with safe websites and preset word filters. All you need to do is review and approve the default websites and words.

If your children use a standard search engine, make sure you turn on the parental controls in the search engine to block inappropriate images and content from appearing in search results.



The ABCs of Online Security

For Tweens 8–12 Years Old



A

Talking to your tween-ager

Youngsters between the ages of eight and twelve are far more sophisticated than children in that age range used to be. The term “tween” was coined to accurately reflect this population of kids who are no longer considered “young” but are not yet teenagers. Understand that tweens are quite comfortable using a computer, having grown up with one at home and/or at school.

Before you speak to tweens, you need to make some decisions so that you can create boundaries surrounding their Internet use. In order to clearly communicate what the rules are, you need to first define them. To help keep your tween safe, you need to know the answers to the following questions:

- Is the computer in a public area of the home?
- What websites are safe for your tween to visit?
- How long should their online sessions be?
- What can they do while they are online?
- Who are they allowed to interact with?
- If you are not going to monitor your tweens, when should they seek your help and approval?



Once you know the answers to those questions, you can proceed with the talk. With the computer turned off, so that you have their undivided attention, you should explain to your tween-ager that a computer is a tool and that it's important to be safe online.

Be sure to cover the following points:

- Discuss viruses, spyware, and hackers
- Discuss how child predators like to lure kids into talking about themselves
- Explain why it's important to be safe online because the computer can be an open door to your important personal information
- Discuss how identity theft occurs
- Discuss the fact that you or a computer expert (if you're not one) can track every single thing that is done on your computer
- Talk about how criminals can take control of your PC and break it, so that you have to buy a new one



B

Remind your child to ask for assistance if something upsetting occurs online

Stress to your tweens that they need to tell you if they receive any odd or upsetting messages while chatting online and that you will not be angry with them or ban them from using the Internet as a result. Make it clear to your child that you understand that they cannot control what other people say to them and that they are not to blame if this happens.

Also, be sure that your tween is not being bullied or bullying other children online. When school children leave campus, they don't necessarily leave their classmates and their conflicts behind. Using computers, text pagers, and cell phones, students can be in touch with each other at all times and they may abuse this technology to pester, bully, and harm others.



C

How to block users and how to report problems

If your child has an online incident while chatting, you can report the problem and block the user. First, copy the chat messages and paste the text into a word processing program. Next, send the copied log to the chat room moderator or administrator. You can find contact information for the moderator or administrator in the help or reporting section of the program. Most chat programs also allow you to block a user by right clicking on the name in the contact list and choosing the "Block" or "Ignore" feature.



The ABCs of Online Security

For Teens 13–19 Years Old



A

Talking to your teens

Just like you have to teach teenagers road safety before they drive a car, you also have to teach them about Internet safety before you let them surf the web unmonitored.

A major difference between hopping in a car and hopping on the Internet is that there are no real “rules of the road” on the Internet. This makes it both a very powerful and a very dangerous vehicle. So, to avoid computer crashes or worse, you need to make the rules and enforce them. The goal here is to teach teens common sense to steer clear of online dangers.



Talk to your teenager about why it's important to be safe online.

Be sure to cover the following points:

- Discuss viruses, spyware, and hackers and how they operate
- Discuss how predators like to lure vulnerable young people into talking about themselves
- Explain why it's important to be safe online because the computer can be an open door to all of your important personal information
- Discuss how identity theft occurs
- Discuss the fact that you or a computer expert (if you're not one) can track every single thing that is done on your computer
- Talk about how criminals can take control of your PC and break it, so that you have to buy a new one



B

Remind your teen that the people they meet online are strangers

No matter how often they chat with them and no matter how well they think they know them, people your teens meet online are strangers. People can lie about who they are, and your teenager's new "friend" may really be a 40-year-old man instead of someone their own age.

C

Check your teen's profile on social networking sites

Make sure your teens are not posting too much information about themselves on Bebo, Orkut or Facebook. Be sure that the photographs they post are not provocative. Remind them that they might draw interest from online predators, embarrass friends and family, disappoint a potential college admissions representative, or negatively influence a future employer.



The ABCs of Online Security

For Novices of Any Age



Your spouse, your partner, your parents, your in-laws, or your grandparents may be new to using a computer and the Internet. They may not be as savvy as you think and could fall victim to online scams and cyber attacks. Therefore, they will need a little guidance from you. Your web safety discussion should include the following:

A

Viruses, spyware, and hackers

If you want definitions of these terms you can find them easily through online searches or the glossary at www.mcafee.com/advice.



B

Identity theft dangers and phishing

Phishing occurs when criminals spoof a website and email of a legitimate company, trying to steal passwords and credit card numbers. Be sure to check your credit card and banking statements frequently.

C

The importance of using caution when downloading “free” items

Remind your loved ones of the old axiom that everything comes with a price, even if it’s free! Also, warn them that if they download software, they may get adware and spyware along with the application.

More Advice on PC and Internet Security

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

About McAfee

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

<http://www.mcafee.com>

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

McAfee and/or other noted McAfee related products contained herein are registered trademarks or trademarks of McAfee, Inc., and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. Any other non-McAfee related products, registered and/or unregistered trademarks contained herein is only by reference and are the sole property of their respective owners.
© 2009 McAfee, Inc. All rights reserved.