McAfee®

Protect What You Value

Internet Safety Plans for the Whole Family

DELL

Introduction

Gone are the carefree days when people used the Internet just for gathering information and sending email. Most are venturing online now to create and participate in full cyber lives. Millions of families worldwide are "Web wise" and using the Internet to learn, research, shop, buy, bank, invest, play games, download movies and music, re-connect with old friends, meet new people and do many other activities.

Though cyberspace is an exciting environment with a myriad of benefits, opportunities and conveniences, it is also an increasingly risky one, with numerous new threats emerging almost daily.

It is also imperative that you talk with your children and any other inexperienced family members about Internet safety. You don't have to be a technology expert to initiate this conversation and share what you know about online safety. To guide you in this online safety discussion, below are step-by-step, age-appropriate plans.

The Internet Threat Landscape

Your chances of becoming a cyber victim are about 1 in 4. Hackers are attacking PCs with Internet access every 39 seconds.

Hacker Attacks

- According to McAfee® Avert® Labs, there are 222,000 known computer viruses out there now and the number of threats is growing daily
- 20% of Internet users in the US have had a major, often costly virus problem
- Virus infections have prompted 1.8 million households to replace their PCs in the past two years
- 83% of teens download music; 64% use illegal sites; "digital music" is one of the riskiest search terms

Identity Theft

- In the last 12 months (2006), 8.9 million Americans have become victims of identity fraud
- Average losses per victim in 2006 were more than double the previous year
- The number of unique phishing Web sites rose to 55,643 in April, 2007, a jump of 35,000 from the previous month

Child Predators

- 71% of 13- to 17-year-olds have received messages online from someone they didn't know
- There has been an 79% increase in instant messaging threats (2007 vs. 2006)
- 32% of 13- to 17-year-olds said they usually don't tell anyone about online messages they receive from people they don't know

An Internet Safety Plan for Young Kids

Step 1. Talk to Your Young Child

- With the computer turned off, so you have their undivided attention, explain to your young children that a computer is a tool and how 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 information. Talk about how bad people can take control of your PC and break it, so 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 name and not to talk about where they live or what school they go to.

Step 2. Together with the Child(ren) Create a List of Rules

The list should include:

- No downloading music or program files from Web sites without parental permission
- Use only monitored chat rooms like Disney's Virtual Magic Kingdom where an adult monitors the chat, not just a bad language software filter
- No user names that reveal true identity
- Never tell anyone your passwords
- Never give out your phone numbers or address
- Never send out a picture of yourself without checking with parents
- No bad language
- No viewing adult Web sites
- Share information only with people you know from the real world such as classmates, friends and family members
- No filling out online forms or surveys without a parent's help
- No meeting online friends in-person
- Ignore emails and instant messages from people you don't know
- Turn off the computer when it is not being used
- Use only special search engines for children like Ask for Kids and Yahooligans

Step 3. Monitor Your Child's Use of the Internet

Put the computer in a high-traffic family area and limit its use. Also, consider using online child safety monitoring software like IMSafer™ along with parental controls like those found in McAfee security software. Download software that provides warning protection against dangerous Web sites. For example, McAfee SiteAdvisor™ provides easy to understand red, yellow, and green Web site ratings.

Step 4. Fortify Your Computer with Strong Security Software

Make sure you have robust software that protects against viruses, hackers, and spyware. It should also filter offensive content, pictures, and Web sites. The software needs to be updated frequently, as new threats are emerging daily. Ideally, security that updates automatically – set it and forget it – is the best option.

McAfee®

Step 5. Use Browsers for Kids and Kid-oriented Search Engines

Ensure your children are using browsers that do not display inappropriate words or images. They come pre-loaded with kid-safe Web sites and pre-set word filters. You only need to make sure to review and approve the default Web sites and words.

Step 6. Enable the Computer's Parental Controls

All the major security software providers offer parental controls; be sure to use them. If you are using freeware or software that doesn't have parental controls, consider buying software that does. Take time to read the manual and make use of these options.

Security software parental controls should:

• protect children from dangerous Web sites
• limit the time they may access the Internet
• Filter out keywords
• Block images that may not be appropriate

An Internet Safety Plan for Teens

Step 1. Talk to Your Teen

Just like you have to teach them road safety before they drive a car, you have to teach your teen about Internet safety before you let them surf the Web unmonitored. If you go with the original and now quaint description of the Internet as "the information superhighway" and continue with the driving metaphor, then you will agree that it's a good idea for your teenager to receive some basic defensive driving training before taking the wheel of a hot-rod computer.

Now, before you give the keyboard and mouse to an eager but unsophisticated user, you will want to be sure they understand how things work and what the rules of the road are. A major difference between hopping in a car or hopping on the Internet is that there are no rules on the Internet. This makes it both a very powerful and very dangerous vehicle. So in order 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 avoid online dangers.

By the way, if you have any crazy ideas about trying to deny your teen access to this technology, he or she may suffer social pressures and feel socially ostracized, and then go behind your back and do it anyway.

Talk to your kids about why 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 information
• Discuss how identity theft happens
• 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 you have to buy a new one

Step 2. Work as a team to set boundaries
Discuss with your teen exactly what is OK and what is not OK regarding:

- what kind of Web sites are appropriate for them
- which chat rooms to visit
    - Use only monitored chat rooms
    - Avoid ".alt" chat rooms – they focus on alternative topics that may be inappropriate for teens
- what kinds of things they can talk about there

Step 3. Together with the teens create a list of rules

- No names that reveal true identity - use a chat name that is not provocative and doesn't hint at who you really are
- Never give out your passwords
- Never give out phone numbers or addresses
- Never use bad language
- No viewing adult Web sites
- Never post personally identifying information or inappropriate photos
- Share information only with people you know from the real world such as classmates, friends and family members
- No filling out online forms or surveys without parental approval
- No meeting online friends in-person without parental supervision
- Ignore emails and instant messages from people you don't know
- Never open attachments from strangers
- Need for parental approval to post anything on social networking sites
- Turn off the computer when it is not being used

Step 4. Monitor Your Teen's Use of the Internet
Put the computer in a high-traffic family area and limit its use. Also, consider using online child safety monitoring software like IMSafer™ along with parental controls like those found in McAfee security software. Download software that provides warning protection against dangerous Web sites. For example, McAfee SiteAdvisor™ provides easy to understand red, yellow, and green Web site ratings.

Step 5. Fortify Your Computer with Strong Security Software
Make sure you have robust software that protects against viruses, hackers, and spyware. It should also filter offensive content, pictures, and Web sites. The software needs to be updated frequently, as new threats are emerging daily. Ideally, security that updates automatically – set it and forget it – is the best option.

Step 6. Work as a team to set boundaries
All the major security software providers offer parental controls; be sure to use them. If you are using freeware or software that doesn't have parental controls, consider buying software that does. Take time to read the manual and make use of these options.

Security software parental controls should:

- protect teens from dangerous Web sites
- limit the time they may access the Internet
- filter out keywords
- block images that may not be appropriate

In addition to cybercrime, another thing you need to be aware of is online bullying. When school children leave campus, they don't necessarily leave their classmates and their conflicts behind. By using computers, text pagers and cell phones, students can be in touch with each other at all times and use all this technology to pester, bully and harm others.

While no security software company has a product that can eliminate cyberbullying from your kid's lives, most security software provides parents with tools that can mitigate the online bullying of kids. Software from security leaders like McAfee help with cyberbullying by providing parents these options: (1) limiting the child's time online; (2) blocking access to inappropriate web sites; and (3) filtering bad language.

Of course, these tools have their limitations. Nothing can take the place of an attentive and responsive parent when a child is bullied, either online or offline. Also, be sure that your child is not victimizing other children with bullying.

Step 7. Remind Your Teen that People in Chat Rooms are Always Strangers

No matter how often they chat with them, and no matter how well they think they know them, people met online are strangers. People can lie about who they are, and your new friend may really be a 40-year-old man instead of a 13-year-old girl.

Step 8. Learn how to save chat session logs, how to block users, and how to report problems

You can save sessions by copying and pasting the message text into a word processing program. Most chat programs allow you to block a user by right-clicking on their name in your contact list and choosing the "Block" or "Ignore" feature. If your child has a problem with another chatter, send the copied log to the chat room moderator or administrator. You can find the contact information in the help or reporting section of the program.

Step 9. Check Your Teen's Profile on All the Social Networking Sites

Make sure your teens are not posting too much information on MySpace or Facebook. Be sure photographs are not provocative or might draw interest from online predators, disappoint a potential college admissions representative or a future employer.

An Internet Safety Plan for "Newbies" (Other Loved Ones, Especially Seniors)

Now, your spouse, partner, parents or grandparents may be older, but they are surely interested in using the Internet for all the same reasons you are. However, they may not be as savvy and could fall victim to online scams and cyber attacks. They will need a little guidance and your Web safety chat should follow these steps:

Step 1.
Discuss viruses, spyware, and hackers (if you want good definitions of these terms you can find them easily enough in online searches or the glossary at www.mcafee.com/advice).

Step 2.
Make sure you have robust software that protects against viruses, hackers, and spyware. It should also filter offensive content, pictures, and Web sites. The software needs to be updated frequently, as new threats are emerging daily. Ideally, security that updates automatically – set it and forget it – is the best option.

Step 3.
Discuss identity theft dangers and how phishing works. It may be a good idea to subscribe to a credit monitoring product like Experian's Triple Advantage. Be sure to check your credit card and banking statements frequently.

Step 4.
Discuss "free" downloading with care. Remind your loved ones of the old axiom that everything comes with a price, even if it's FREE! If you're downloading software, you may be getting adware and spyware along with it.

Step 5.
Develop good passwords by using at least 8 characters and combinations of letters, numbers and symbols. Passwords must be changed periodically to reduce the likelihood of a particular password being compromised over time.

Step 6.
Check to make sure your computer's internal security is enabled.

Step 7.
Install robust computer security software that includes anti-virus, anti-spyware, anti-phishing and firewall technology.

Step 8.
Turn off your computer when you are not using it, so the chance of it being hijacked by hackers is greatly reduced.

McAfee® SecurityCenter™

Proactive Online Security for Families

McAfee SecurityCenter is a proactive 8-in-1 always-updating security bundle that protects what users value with multi-user child safety, identity theft prevention, email and IM protection and automated back-up. It gives users the confidence to surf the web, shop, bank, email, chat and download files safely and securely.

More Reasons to buy McAfee at Dell

Pre-Installed - McAfee SecurityCenter is fully installed by Dell Technicians before your computer is delivered. No further set up is required and you benefit from immediate protection.

Always Upgrading, Always Updating Daily – Updating Daily threat protection and updates are delivered you round the clock from McAfee's world-class research centre, McAfee® Avert® Labs. Free software upgrades and enhancements are provided as long as your subscription is active.

Multi-Year Protection – 15, 24 and 36 Months versions of McAfee SecurityCenter are now available at Dell offering long term protection and even better value for Money.

For more information visit www.dell.com