An internet safety plan for the whole family

McAfee

Introduction

you, your family and the internet

Millions of families worldwide are going online every day and using the internet to learn, research, shop, buy, bank, invest, share photos, 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 numerous benefits, opportunities and conveniences, it is also an increasingly risky one, with many new threats emerging daily.

It is no surprise that cyber criminals are taking advantage of the internet and people who use it. You and your family members need to be on guard whenever you go online. In addition to robust security software that defends 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 the whole family.

As soon as a family member becomes "cyber-active," it is time - no matter the age - for "the talk" about safe surfing and more. You should be aware that even if you do not have a computer at home, pc's are available everywhere, including at schools, libraries, at friends' homes, and even in church basements. It's important that everyone knows the basics about protecting themselves in cyberspace.

Contents

The internet threat landscape

the facts

Using the internet can put your child at potential risk of encountering online predators.

The internet allows predators to remain anonymous and build an online relationship with your child. Under the veil of anonymity, they are more likely to take risks online without fully understanding the possible implications.

Parents can help reduce the risk to your children by becoming aware of the risk in an online environment.

- Your chances of becoming a cyber victim are about 1 in 4.[1]
- Hackers are attacking pc's with internet access every 39 seconds.[2]
- According to McAfee® avert® labs, there are 222,000 known computer viruses out there now and the number of threats is growing daily.
- Virus infections have prompted 1.8 Million households to replace their pc's in the past two years.[3]

71% of 13- to 17-year-olds have received messages online from someone they didn't know.[5]

Chat rooms

Chat rooms are an area online where people with similar interests can chat with other members. It can either be one to one or one to many and messages typed by the user will instantly appear to everybody in that chat room. Web based chat rooms can range in subjects from teen chats, singles chats, sport team chats, video game chats and music chats.

Users can choose to remain anonymous so it's not always possible to know who your are really talking to.

Social networking sites

Social networking is a way for communities of people to share their common interests and activities online.

Social networking sites such as Myspace and Facebook have become an attractive target for cyber criminals looking to mine personal information and trick users.

A user of a site such as Myspace or Facebook can post a personalised profile of themselves containing photos, contact details, interests, hobbies, places of interest as well as chat and post comments online.

1 Consumer reports, State of the Net 2007, September 2007

2 Hackers attack every 39 seconds – A. James Clark School of Engineering at the University of Maryland.

3 Consumer reports, State of the Net 2007, September 2007

5 "Teen safety search," Cox Communications and Teen Research Unlimited, March 2006

The 'compare me' scandal

One of the most popular applications on Facebook is "compare me". Users are asked to say which of their friends are the hottest, the best fun to go shopping with, the most trustworthy, etc. The application writers originally promised that only general results would be made public (e.g. "X is 3rd hottest in your friends circle!"). A few weeks later, however, it turned out that non-anonymous data (e.g. "Your friend x said y was a better friend than you") was being sold for USD $9.

Although the potential 'compare me' damage is trivial, it shows how easy it is for cyber criminals to extract personal information from users on social networking sites. It also shows how little personal restraint users often demonstrate when sharing information and opinions online.

Instant messaging

Instant messaging is a form of real time communication between two or more people and allows for instant text messages to be delivered to your peer.

Instant messaging or IM lets parties know if their peers are available to chat, busy or away from the pc.

Many children use programs such as MSN Messenger, AOL, Yahoo and ICQ to chat to their friends after school and on the weekends. Some of these programs also allow the user to see the person they are talking to by using web cameras.

A 10-step safety plan

that will protect everyone in your family

Step 1. Computer placement

In a home with children, placement of the computer is one of the first and best decisions you can make. We recommend that you put the computer in a high-traffic family area and limit its use. Be sure to have computer security software that has parental controls like those found in McAfee products.

Step 2. Work as a team with your family members to set boundaries

Discuss exactly what is ok and what is not ok regarding:

- The kind of web sites that are appropriate to visit
- The chat rooms and forums that are appropriate to participate in
    - Use only monitored chat rooms
    - Avoid ".Alt" chat rooms – they focus on alternative topics that may be inappropriate for young people
- The kinds of things they can talk about and language that is inappropriate

Step 3. Together agree on a list of family pc rules

We suggest the rule include:

- No user names that reveal true identity or that are provocative
- Never reveal your passwords
- Never reveal phone numbers or addresses
- Never post personally identifying information or inappropriate photos
- Never share any information with strangers met online
- Never meet with strangers met online
- Never open attachments from strangers
- Always turn off the computer when it is not being used

Once you have the rules, make a poster with them and put it next to the computer.

Step 4. Take an active interest in your child's activity online

Do not use the internet as a baby sitter! Learn to surf the web and chat online yourself so you understand what it is that your child is doing. If you don't know how to chat online, ask your child to teach you!

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. This software should be updated frequently, as new threats are emerging daily. Ideally, security that updates automatically like McAfee's set-it-and-forget-it software – is the best choice.

Step 6. Enable your security software'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 learn how they work and use options that filter and block inappropriate material. Of course, these tools have their limitations. Nothing can take the place of an attentive and responsive parent monitoring their children when they are online.

Step 7. Remind your family that the people met online are strangers

Everyone who goes online must understand this: No matter how often you chat with them and how long you've been chatting, and no matter how well you think you know them, people you met online are strangers. It is easy to lie and pretend that you are someone else when you are online. Kids especially need to know a new friend may really be a 40-year-old man instead of a 13-year-old girl.

Social networking web sites like www.myspace.com and www.facebook.com are an ideal way for meeting new people online. Therefore, parents must visit these sites and check out their children's profile to insure that inappropriate conversations and unacceptable photos are taking place or being posted. Monitor you kids' instant messaging conversations to be sure they aren't falling victim to an online predator.

Step 8. Make and use good passwords

To create really good passwords that would be hard to figure out, 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 license plate; for example: "gr8way2b"
- Use several small words with punctuation marks: "betty,boop$car"
- Put punctuation in the middle of a word: "roos%velt"
- Use an unusual way of contracting a word: "ppcrnbll"
- 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. Check to make sure your computer's internal security is enabled

For pc's with Microsoft Windows XP service pack 2 and newer, you can ensure your computer has internal security by clicking on the start menu and going into the control panel's security center.

Here you will want to confirm that all the default settings are active for by clicking on the 3 sections:

1. Internet options – confirm that the security level is at least "medium – high"
2. Windows firewall – confirm this is on as recommended
3. Automatic updates – confirm this is on as recommended

Step 10. Read up online security issues

The more you know, the safer you should be. Check out McAfee's advice center for easy to read and understand computer and internet security educational material at www.mcafee.com/advice.

The GadgetGuy™'s jargon buster

technical terms explained

ADWARE

Software that delivers advertising to your PC, perhaps in the form of popups or sidebars with scrolling adverts.

BOTS, BOTNETS & ZOMBIES

A 'zombie' is a computer with a remote control Trojan installed. It works normally, but the Trojan remains as a silent agent, waiting for its 'master' (often the creator of the Trojan) to take control of the system. A bot is an application running on a zombie, installed by the zombie master to undertake some task – often a denial of service attack (see DDoS opposite) or sending out spam. A botnet is a group of bots infected by the same Trojan, and can be used in conjunction to perform distributed attacks.

DDoS

(Distributed Denial of Service) A DoS or DDoS attack is an attempt to 'choke up' a Net connection or server, typically by flooding it with junk data. Botnets are often used for DDoS attacks – hundreds of computers work to shut down an Internet connection or server.

DUMPSTER DIVING

The practice of sifting through garbage bins (commercial or domestic) for documents that have been thrown away as 'rubbish', but which might be useful to the dumpster diver.

FIREWALL

Software or hardware that blocks network traffic. A firewall tries to distinguish 'good traffic' from 'bad traffic'. Good traffic is allowed to pass, bad traffic is blocked.

MALWARE

A catch-all term for software that does undesirable things to your computer. Viruses, worms and Trojans are all forms of malware.

PHISHING

Using email or a fake website to trick people into giving up private information, such as credit card details. The most common example is the email that purports to be from a bank. The email asks the receiver to go to a specific website and log in using their internet banking username and password. The site looks real enough, but in reality all it is doing is harvesting the user's details. A technique called spear phishing is an evolution of that – it targets specific individuals to make the phishing attempt sound more plausible.

PATCH

A software update designed to fix problems in the shipped versions of products. For example, a security flaw might be found in a piece of software after it has shipped to retailers. So the software developer writes a 'patch' that fixes the flawed parts, and distributes that patch over the Internet.

SPAM

Unwanted email (the equivalent of junk mail), usually advertising, sent out by mass mailers. A spam filter detects and removes spam from email inboxes.

SPY WARE

Spyware is software that sits on your computer and monitors your activity, creating and possibly sending reports to hostile parties.

SCRIPT KIDDIE

A person who uses readily available Internet tools to perform basic attacks on computer systems. For instance, a person who uses a downloadable port scanner to find vulnerabilities (such as file shares and open directories on a Windows system), then perhaps uses a downloaded password hacking program to access those vulnerabilities.

TROJAN

A type of program that installs malicious software (such as viruses) while under the pretence of doing something else. Over time, the term Trojan has become almost synonymous with a type of virus that sits resident on the computer to create a 'backdoor' that hackers can exploit to get into the host system. The Trojan on an infected system will often advertise itself to the creator of the Trojan or other parties, although a good software firewall will prevent that advertisement from getting out (and it will also stop remote hackers from getting in a accessing the backdoor).

VACCINE

A program that injects itself into an executable program to perform a signature check and warns if there have been any changes.

VIRUS

Malicious software that 'infects' a computer system, causing it to do undesirable things (like deleting files, dialling 1800 numbers on the modem or sending private data to remote parties over the Internet). Anti-virus software detects and removes viruses.

WORM

A form of virus that replicates itself over a network. When a worm infects a system, it will use that system to try and infect other systems. The classical example is the email worm; the worm sends out a copy of itself to every user in the host PC's email address book (and the recipients, seeing that the sender is someone they know, might be inclined to trust the email enough to open the file).

The Gadget Guy - Peter Blasina. A well-known face and voice nationally, the Gadget Guy frequently appears in mainstream newspaper dailies, technology magazines, ABC Radio, and TV station Channel Seven. www.gadgetguy.com.au

McAfee

The abc of online security

for young kids (ages 3 – 7)

A. Talking to young children

When you talk to young children about internet safety, do it with the computer turned off, so you have their undivided attention. Start off by explaining 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.

B. Together with the child(ren) to create a list of kids 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
- 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
- Use only special search engines for children like ask for kids™ and Yahoo!® Kids

C. Use browsers for kids and other 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.

The abc of online security

for tweeners (ages 8-12)

A. Talking to your tween-ager

Youngsters between the ages of 8 and 12 are far more sophisticated than children in that age range used to be, hence 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 for their internet usage. In order to communicate clearly what the rules are, you need to first define them. In order 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?
- Where online is it safe for your tween to go?
- 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 the tween, when must they ask for your help and approval?

Once you know the answers to the above questions, you can proceed to the talk: with the computer turned off so you have their undivided attention, you should explain to your tween-ager that a computer is a tool and 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 into it, so you have to buy a new one

B. Ask for parental assistance if something upsetting occurs online

Stress to your tween that they need to tell you if they receive any odd or upsetting messages while chatting, and that you will not be angry with them or ban the internet as a result. Make it clear to the 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 child 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. 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.

C. How to block users and 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 individual, 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.

The abc of online security

for teens (ages 13 – 20)

A. Talking 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 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.

A major difference between hopping in a car and hopping on the internet is that there are no real 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.

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
- 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 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

B. Remind your teen that people met online 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.

C. Check your teen's profile on all the social networking sites

Make sure your teens are not posting too much information on Myspace.com® or Facebook™. Be sure photographs are not provocative. Remind them that they might draw interest from online predators, embarrass friends and family, or disappoint a potential university admissions representative or a future employer.

The abc of online security

for new adult users (especially seniors)

Now, 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 would hope and could fall victim to online scams and cyber attacks. Therefore, they will need a little guidance from you, so your web safety talk should include:

A.

Discussion about 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).

B.

Discussion about identity theft dangers and how phishing works. It may be a good idea to subscribe to a credit monitoring service. Be sure to check your credit card and banking statements frequently.

C.

Discussion about 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! If you're downloading software, you may be getting adware and spyware along with it.

McAfee