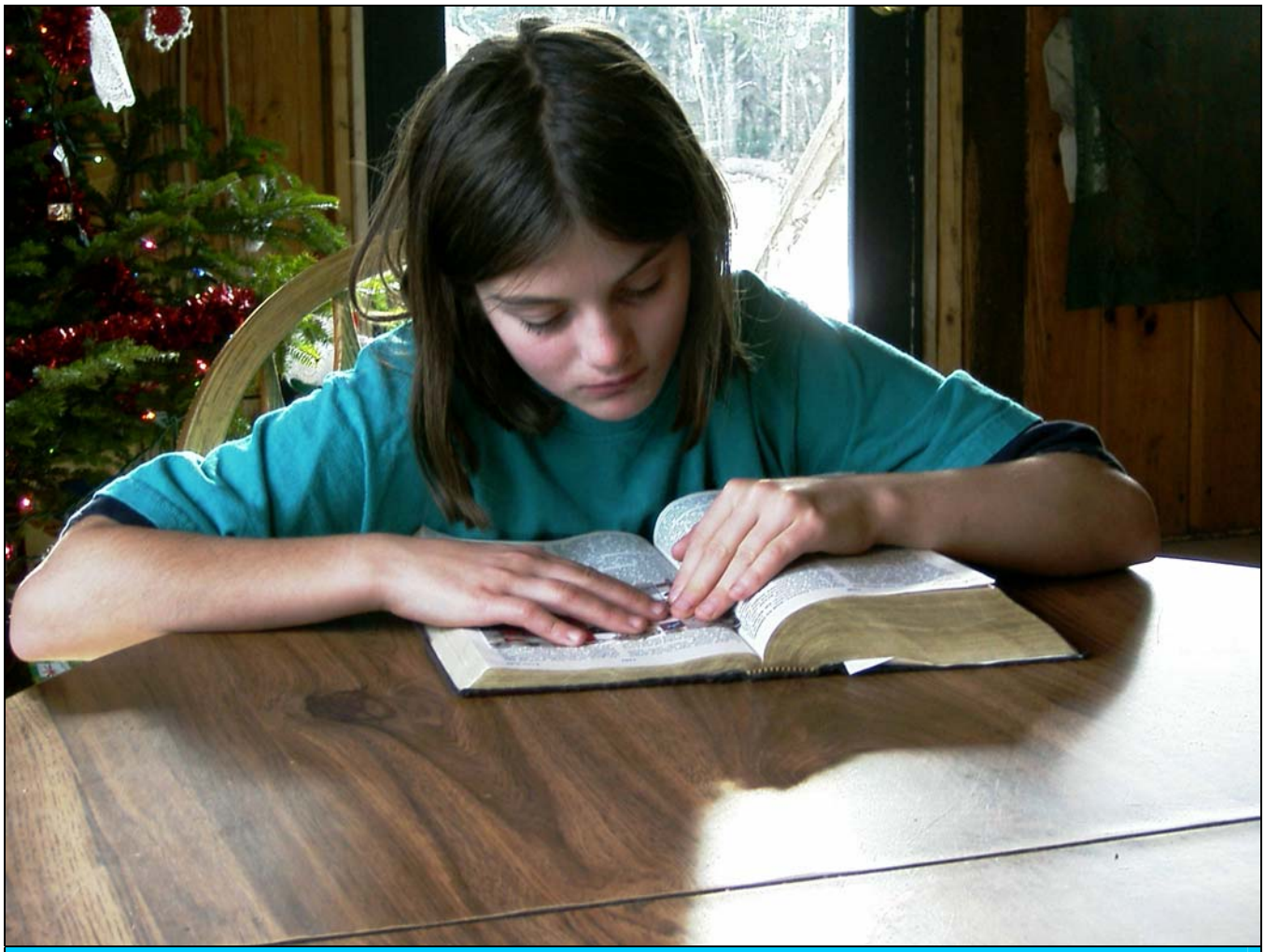


WHAT EVERY CHRISTIAN SHOULD KNOW ABOUT

INTERNET SAFETY

A guide to protecting your children, your self, and your computer from the threats on the Internet

© 2007 Ronald Meldrum. All rights reserved. The material in this booklet is based upon the author's own personal and professional experience. It will not be appropriate for all situations. Make your own informed decisions as to how to protect yourself and your family.

If you have purchased this publication, then we grant you the right to copy and distribute it for educational or personal purposes, such as in church bulletins and via e-mail to friends. However, it may not be posted on a web site for free access nor may it be used in part or in whole for any commercial purpose without the express written permission of the author. If you are unsure as to whether or not your use is permissible, or if you would have a commercial purpose in mind, please contact the author by e-mail at ron@ronmeldrum.com.

Should Christians Connect to the Internet?

The Internet seems to have much to offer to make life easier. On-line shopping, plane reservations, banking, and other services promise to save us time and money. On-line classes and a variety of news outlets promise to make learning easier and more convenient. The Internet has even given birth to a new class of recreation and leisure opportunities.

Although it has so much to offer, the Internet has a dark side. It is a seething pool of cult and occult propaganda and recruitment activity. Dozens of new pornographic web sites launch every day. Con artists prey tirelessly on anyone who seems a good target. Stalkers, rapists, and pedophiles use it to find victims. Misinformation and disinformation is much more common than real, valuable information. The lure and mystique of the virtual world and virtual relationships has broken up thousands of marriages.

With such a wicked facet to it, should Christians connect to the Internet at all?

Whether or not a Christian should connect to the Internet -- or whether or not they allow their children to connect -- is an individual decision. It is possible to navigate, explore, and make practical use of the Internet if one has sufficient safeguards in place.

However, Internet access may not be for everyone.

A person who has a problem with alcohol should not go into a place where alcoholic beverages are served. They shouldn't even walk by a bar unless they have someone responsible with them, to help them if they are weak.

A person who lacks self-control or self-discipline should not have a credit card, unless a disciplined, responsible person controls their access to the card.

A person who is trying to stop smoking should not hang around with others in the "smoke room" at work, and they should not keep a pack of cigarettes in the cupboard "just in case." They should not even allow guests to smoke in their house or car.

Likewise, people who have addictions, problems with self-control, lack of discipline, or other weaknesses or challenges, should not have un-tethered access to the Internet. If they access the

Internet at all, they need to have good safeguards in place.

In fact, everyone should have some safeguards in place. The extent and complexity of safeguards will depend on the individual, their weaknesses, and their maturity.

Basic Safeguards

Some common and effective measures that one can employ are:

Purchasing Anti-virus, Anti-Spyware, and Anti-Adware software. Viruses are malicious programs that try to do harm to your computer or to take control of it. Businesses lose millions of dollars a year due to damage caused by viruses. Also, hundreds of thousands of personal computers have been turned into "Zombie Machines" without the owner even knowing it. These Zombies are used to send unwanted e-mail and to conduct attacks against other computers on the Internet. An up-to-date anti-virus program is vital to protect your computer from these threats.

Spyware are programs than install themselves on your computer (usually without your knowledge) for the purpose of gathering personal information about you, such as credit card numbers, names of web sites you visit, etc.

Adware are programs that install themselves on your computer for the purpose of pushing ads to you – often via pop-up windows.

One researcher connected an unprotected computer to the Internet and found that it was penetrated within 45 seconds. Software to protect from these intrusions should be considered a part of the cost of having a computer on the Internet, and once they are purchased they should always be kept up-to-date. Never go on-line with a computer that is not protected.

Subscribing to a filtered Internet access service. These services make many of the worst web sites on the Internet inaccessible. They aren't foolproof, but they do filter out the bulk of the dangerous material. *Avoidance* is our first line of defense.

> Enter not into the path of the wicked, and go not in the way of evil men. Avoid it, pass not by it, turn from it, and pass away. [Proverbs 4:14-15]

Creating Accountability. *Accountability* can be a very effective tool for safeguarding the on-line experience. Making it possible for other people to see what a person is doing on the computer helps create accountability. Accountability systems can be as extreme as always having someone else around when a person is on the computer or as simple as putting the computer in a well-traveled area of the home or facing the computer screen out into the room so that anyone in the room can see what is being done. Often, when one person might succumb to temptation when alone, when there is no accountability, the presence of another person will strengthen them.

> Two are better than one; because they have a good reward for their labour. For if they fall, the one will lift up his fellow: but woe to him that is alone when he falleth; for he hath not another to help him up. Again, if two lie together, then they have heat: but how can one be warm alone? And if one prevail against him, two shall withstand him; and a threefold cord is not quickly broken. [Ecclesiastes 4:9-12]

Flee. When you are tempted to do something immoral or impure on the Internet, turn the computer off immediately and pray or read the Bible for a while. The biblical model, exemplified by Joseph when he fled Potiphar's wife at the expense of his own career and comfort, is to flee from temptation. Flirting with temptation is a dangerous game -- a game that we usually lose.

> Flee also youthful lusts: but follow righteousness, faith, charity, peace, with them that call on the Lord out of a pure heart. [II Tim 2:22]

> But thou, O man of God, flee these things; and follow after righteousness, godliness, faith, love, patience, meekness. [I Timothy 6:11]

> Flee fornication. Every sin that a man doeth is without the body; but he that committeth fornication sinneth against his own body.
> [I Corinthians 6:18]

Protect Your Personal Information. Never give out personal information about yourself, such as your real name, where you live, where you work, your phone number, passwords, etc. unless you are absolutely certain of the identity of the person with whom you are chatting or to whom you are sending e-mail.

Don't Open Unknown E-mail Attachments. When you receive e-mail with a picture or other file attached to it, don't open the attached file unless you know exactly what it is and who sent it to you. The most common way that computer viruses spread today is through e-mail attachments. Some viruses, once they infect a computer, actually "hijack" the person's e-mail account and send hundreds or thousands of messages with the virus attached to it. For this reason, even if you receive an e-mail

from someone you know, don't open the attached file unless you know what the file is. Once your computer is infected with a virus, it can be very difficult and time-consuming to "disinfect" it. If you don't know that you have a virus, it could be spreading itself to your friends through e-mail messages with infected files attached.

A computer virus may do a number of nasty things to your computer. Some exist only to spread themselves to other computers and don't do any harm other than using up some extra memory and slowing your computer down a little. Others do more damaging things, such as erasing your hard drive, corrupting your files, e-mailing your private information across the Internet, etc. For this reason, it is very smart to make the small investment (usually under $40) in an anti-virus program for your computer. Most anti-virus programs will even scan your incoming e-mail for viruses. Once you have purchased your anti-virus software, be sure to update it regularly so that you'll be protected against new viruses, which come out daily. Most anti-virus software vendors offer free updates for one year after your purchase.

Adults usually require less stringent safeguards than children. Children are more naive, have less life-experience, and are more susceptible to many of the dangers lurking on the Internet. However, adults should never take a casual attitude toward their on-line activity. Thousands of adults have been lured into unhealthy relationships, occultism, divorces, cults, con artists' schemes, unhealthy lifestyles, and more through the Internet.

Protecting the Children

Parents are often very concerned about how to protect their children from the perils of the Internet while still enjoying its benefits. With pornography sites just a click away . . . with cults aggressively seeking and recruiting on-line. . . with sexual-predators actively looking for **your** child in chat rooms and e-mail forums . . . wise Christians will take common-sense steps to protect their children.

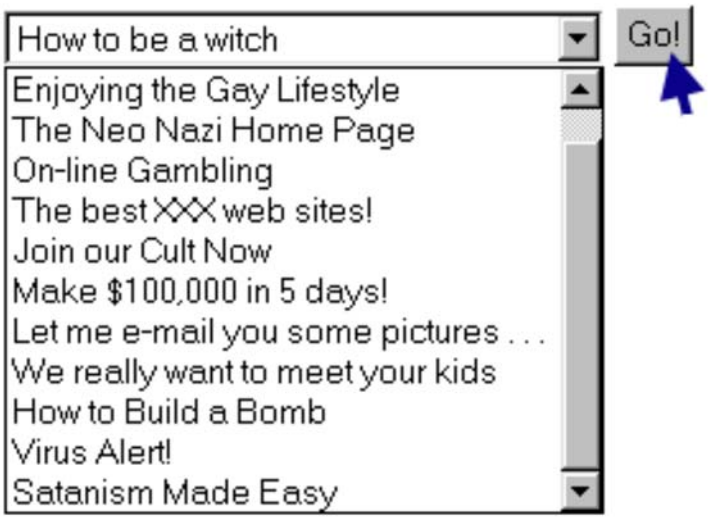
Do your children even need Internet access? Do they need to be on the Internet in the first place? Many (maybe most) don't even need to be on the Internet. Particularly with younger children, consider not letting them use a computer that is connected to the Internet, except in closely-supervised sessions.

Don't let your kids have a computer connected to the Internet in their bedroom. That's just asking for trouble. You wouldn't let a stranger in your child's bedroom would you? Then why let them in via the Internet?

Put the computer in a public, well-traveled area of the home with the screen facing OUT into the room. "What about my child's privacy? What about *trust*?" some parents will cry. Forty years from now, after a life-long struggle with a life-destroying pornography addiction, your child will wish you had been less concerned about their "privacy" and more concerned about their **safety and well-being**.

ALWAYS have an adult present when children -- including (especially!) teens -- are on the Internet. Kids and even teenagers are not aware of the potential dangers of idle curiosity. Five minutes of curiosity at the wrong web site could destroy a life.

Educate your children about the dangers on the Internet. The naive child is easier prey, and an educated child will better understand the steps you take to protect them. Tell them why (in an age-appropriate manner) you are setting up safeguards for them, and explain why they should not reveal personal information about themselves (not even their names) when they are on-line.



Review your children's e-mail. One parent at a church right here in Maine opened his 9-year-old daughter's e-mail because he wanted to know who was writing to her, and he found in it a photograph of the worst kind. You might feel self-conscious monitoring your children's e-mail, and they might protest with cries of "what about my privacy" and "don't you trust me?" but you may find yourself very glad that you had the guts to love your child enough to protect them in that way. When they have their own house, buy their own computer, and pay for their own Internet access, then they can have their "privacy." Until then, God holds you accountable for their actions and their protection.

Subscribe to a filtered Internet service. There are Internet service providers that filter out and prohibit access to most pornographic and other inappropriate web sites. This does not mean we can ignore all of the other suggestions given here, but it is a big step in the right direction

Avoid "chat rooms" and "Instant Messaging" if possible. Again, your children will protest, but they simply do not know and understand the dangers that exist. You know better than they do. Yes, you even know better than your teenager. If you permit your child to enter a "chat room," be sure you are right there sitting next to them -- unless you are accustomed to letting your child hang out and chat with homosexuals, cult members, and child pornographers. Every week there is another story in the news about a pervert preying on children in a "chat room." Once *your* child is in the news, it's too late . . .

Did your parents always used to say "Never talk to strangers"? It applies even more to the Internet. There is no way to know who those other people in the "chat room" really are, or why they are there.

Don't forget that the head of internet operations for a very prominent, child-oriented company was arrested by the FBI for impersonating a 16-year-old in internet chat rooms in order to find kids to satisfy his sexually-perverted lifestyle. He was arrested on his way to meet one of the children he had met in such a "chat room." The FBI confiscated his computer and found it stuffed with child-porn images. Don't trust anyone in a "chat room," *ever*, and have your child avoid them altogether unless you are present with them. *Most predators are not caught until it is too late for their victims.*

Some of these suggestions may sound drastic in relation to the permissiveness and apathy of today's America, but they are by no means as drastic as one might at first glance think. A smart parent will limit their children's Internet activities even more, and will even take steps to protect themselves and their spouse. Remember, marriages are broken *literally* every day by relationships struck up in Internet "chat rooms" and "bulletin boards" -- and by the porn addictions spawned by a few moments at the wrong web site.

Your child's life, prosperity, and well-being are at stake, and if you love your child they are important enough to warrant drastic measures. The Internet is as dangerous and deadly as a loaded gun to your child. Loving parents will take whatever steps are necessary to protect their children from inappropriate or naive activities on the Internet. Their tomorrow is worth today's inconvenience.

Conclusion

Yes, it is possible to enjoy the benefits of the Internet while minimizing its risks. For most adults, some very simple safeguards are sufficient. For adults with special challenges or addictions, more stringent safeguards are necessary.

For children, more extreme and obtrusive protections must be in place. We can't afford to take chances with our children, so we must be particularly careful what they do, where they go, and with whom they talk.

The key to a successful and safe on-line experience is to never be casual about it. Always ask yourself if what you are doing is glorifying to God. How would you feel if Jesus were with you in that chat room, or looking over your shoulder at that web site?

> All things are lawful for me, but all things are not expedient: all things are lawful for me, but all things edify not. [I Corinthians 10:23]