

TEN SOLUTIONS

Safe Computer Habits

PRESENTED BY E.F.CUSSINS OF TEN SOLUTIONS

© 2005 TEN Solutions
445 S. Maple Grove • Suite 12
Boise, ID 83709
Phone 208.323.2570

I want to thank my lovely wife for putting up with me through out this project.
I want to thank Donna Houck for helping me with the editing process.
I must thank everyone who gave input, to make these pages a quality working help for the computer users.

Table of Contents

Introduction		Web Surfing Habits	11
CHAPTER 1		Downloading Habits	12
<u>Threats and Symptoms</u>		Web Blog Habits	15
Virus	1		
Trojans	1	CHAPTER 4	
Phishing	2	<u>Physical Computer Habits</u>	
Spyware	2	Workstation Habits	15
Symptoms of Possible Infection	2	Backup Habits	16
		Maintenance Habits	17
		Habits Concerning Selling a Computer	17
CHAPTER 2			
<u>Basic Protection Habits</u>		CHAPTER 5	
Operating System Updates	3	<u>E-commerce Habits</u>	
Anti Virus Program	4	Online Shopping Habits	19
Anti-spyware	4	Online Banking Habits	20
Firewalls	5		
Intrusion Detection	5	CHAPTER 6	
Layered Protection	6	<u>Family Computing Habits</u>	
		Communication Habits	22
CHAPTER 3		Activity Habits	23
<u>Good Computing Habits</u>		Resources	24
Password Habits	9		
Email Habits	10		
Instant Message Habits	10		

Introduction



Proper Planning Prevents Poor Performance

Why is it that some people go virtually untouched by viruses and other malicious software while others are constantly fighting it? I have seen both ends of the extreme. You could put two computer users side by side. Give them the same internet connection, same operating system, same software, and one will fall victim to attacks more than the other computer users.

I will not kid you computer security is not cheap. It requires time and money, and a conscience effort. The payoff is when everyone else around you is losing personal information because of some cyber attack. All of your hard work pays for itself when your computer crashes and it takes less than a day to recover all your data. Where someone else is still struggling weeks later to get their system back up and running. Good protection and fast recovery are the two big pay offs to having good computer habits.

These habits include not just having a good antivirus program, but keeping it up to date. Just as important is the practices of each employer, employee or family member that sits behind a computer.

Packed in these few short pages are volumes of tested and proven habits that will not only protect, but also enhance a safe and secure experience between you and your personal computer.

What I have put in the following pages, will not keep bad things from happening to your computer and/or your network. It will prevent problems and help you recover them much quicker.

Disclaimer:

Like in all good self-help and instructional books there must be a legal disclaimer. This is mine.

What you find written in these pages are a product of research and practical experience. I have found these habits to enhance my family and my computer experience. If you disagree with what I have written, let me know at Everett@tensolutions.biz I am always open to new insights and learning.

I have put the resource page on the web at www.tensolutions.biz and click on Habits. I did this so I could keep you updated on what professionals are saying about the best habits to use. I hope you find this an advantage in having extra up to date information and resources at your fingers.

Take what you read here and investigate it for yourself, and then use what is most helpful for you.

Threats and Symptoms

“You can’t really know what you are protecting yourself from if you do not know what is the threats and how to spot them.” -

- Everett Cussins



To start off with, everyone needs a good clear understanding of what kind of threats that are able to invade a computer. In the past year, people who have had their computers invaded by malicious types of programs have found that they were attacked by a combination of attacks. They sneak past basic elementary forms of protection. Here are several examples of the different types of attacks. We will begin with the different classification of the basic forms of attacks.

Virus The first computer virus was in the early 1970's. Along with growth and use of personal computers came the increase and variety of viruses. There are four basic types of computer viruses. A virus typically cannot execute itself. A virus needs to be activated by some type of action, such as clicking a link or file. Each virus is known by the way that it infects a computer.

- **Macro:** These viruses are spread by sharing document files from Microsoft Word or Excel. Macro viruses are an affect PCs and Apple computers.
- **Boot Sector:** These types of virus are spread by sharing files between different computers. Any file can spread a boot sector virus, even if the computer is not booted when installing the file.
- **Program:** A program virus is spread through the sharing of programs. Most computer users download wallpaper or screensavers from the internet. Because of all the websites that offer free download of programs, this type of program is easy to spread.

- **Polymorphic:** Has the ability to change form each time it is executed. It was developed by hackers to get around antivirus software and other forms of detection.

Trojan In Greek history, the Trojan horse was used by the Greeks to trick the residents of the city of Troy to open their gates and let them inside. Today, the Trojan gets into a computer wrapped inside a screensaver, or some other program. These types of threats first showed up with Windows 95 and 98. They open a computer to the internet via a backdoor thus; they are given the name **Backdoor Trojan**. A common use of late for a Trojan Horse is for the installation of zombie software. **Zombies** are used for remote control attacks from the infected computer. When they are running, it takes full access of the computer to the Internet to perform some predetermined tasks.

Phishing Before mid-2003, most Phishing arrived in text-heavy e-mails. Today, they contain logos and fake domain names. Phishing is email that poses as someone from a bank or business that you are likely to have some kind of business dealings. In this email, you are asked to reply with your logon, password, credit number, or personal financial information.

Spyware During dot-com crashes of the late 1990's, advertisers started looking to collect your data and send it to a central database computer over the internet. Today spyware is used to gathering Marketing Data, Hacking, and for Monitoring. The legal form of spyware is to monitor your child's activity on the web. Employers use spyware to monitor their employee's computer activity.

The spyware is typically bundled with downloadable freeware or packaged with **ActiveX controls** (code that defines how online content and desktop applications will interact with each other) that install themselves on your PC when you visit certain Web sites.

The unwanted result of spyware that has gotten attention in the past few years is called spam. Spam is known for flooding your inbox with hundreds or even thousands of unsolicited e-mails. Spammers get email address in three basic ways.

1. Buy list of emails.
2. Scan posting of email address on message boards.
3. There software known as robots they go out and search website for email addresses, or any text with @ in it.

Root Kits

Just when you think there could not be another way for a hacker to invade your computer, it shows up. Root Kits have been around for quite some time. It has not been until 2005 that there has been wide use on the Windows operating systems. Up until now, root kits have largely been used on UNIX or Linux systems.

A root kit will sneak in through an email or download and install itself on a computer. It can set there, monitor activity of the computer, and periodically send the results back

to a hacker. The best defenses are good computing habits and scan for the root kits by specialized software, and someone trained in its use.

Affects of Infection

The most common types of computers that are open prey for attacks are computers that children use, computers that are used just for the internet, and computers that haven't had their patches and antivirus software updated.

The best antivirus programs and anti-spyware programs still have new or mutated versions slip by them. However, there are some signs that should raise a red flag as to a computer has been infected with a form of malicious software.

Types of Infection

- **Hackers** do check for weakness in any network computer's protection.
- **Spyware** monitors your computer habits.
- **Trojans** try to get remote control over your computer.
- **Denial-of-Service** Attacks try to crash your system.
- **Keyloggers** records everything you type on your keyboard

Symptoms

- Pop-up ads happen more frequently.
- The computer starts slower than normal.
- The computer runs slower than normal.
- Windows open and close quickly.
- The web browser homepage changes, on its own.
- You are blocked from accessing the Microsoft website.
- You start getting more spam than normal.
- You get emails saying that people have received spam from you.

Sever Results

- Hard drive crashes.
- Personal privacy is breached.
- Stolen username, passwords or credit card numbers.
- Sluggish computer and Internet access.

Chapter
2

“How well we protect ourselves depends on the type of tools we use.”-EFCussins

Basic Protection Habits

I get the question, “How do I know if my computer is infected?” The simplest way to find out if you are infected is to run a scan on the hard drive. If you are sloppy about personal information, and what you download from the web, there is a good chance that you will be infected with a virus or some other form of malicious program.



There are some simple things that everybody can do to protect themselves when they sit behind a computer. The first step is to make sure that there are certain programs running on the computer that are for protection. These programs along with good computing habits will keep data on your computer safe and it running at peak efficiency.

Every computer should have updated operating system, antivirus, anti-spyware, firewall, along with an intrusion detection/prevention program, at the very least.

Operating System Updates

Humans wrote computer programs. Humans are not perfect. As time passes, the programs are rewritten, with new bells and whistles to improve its functionality and ease of use.

The biggest program that you will have on your computer will be its operating system. Whether you are running, Windows XP, Mac OS, or Linux, they all will come out with new updates, periodically. Keeping up with operating system updates will insure that you have the best possible operating system available.

These updates can be classified into two categories.

1. Increase the ease of functionality, and run smoother.
2. Decrease the risk of someone gaining unwanted access to important data.

Antivirus Programs

If nothing else, every computer should have an up to date antivirus program running on their computer. I have seen computers without an updated antivirus program or with no antivirus program at all! These computers are telling the bad guys, “Come and take control. I am an open door to you.”

There are three ways an antivirus program protects a computer.

1. It scans and blocks incoming e-mail or files that have the potential of being dangerous. The weakness here is that most antivirus programs cannot scan compressed (zipped) or encrypted files. All antivirus programs will scan a computer’s hard drive for infected files. The determination of an infected file is done during the scan and identified by a list that the program keeps of attributes of infections.
2. Removal or quarantine of a virus is the secondary job that an antivirus program does. Removal is completed when the virus has been identified and infected files are deleted without causing any loss of data to the operating system. Quarantine of a virus is used when its deletion of the infected files could cause damage to other files.
3. There is a new breed of antivirus programs. They don’t go off a database. They take known behaviors of viruses and compare that information to what is happening within a computer. In some ways this is a better method. There raises a question on how reliable this method is going to be in the end.

The most important thing to remember with any good antivirus software is to keep it updated. If you are scanning your computer looking for viruses, with a six-month-old set of virus definition, this could lead to problems. The newer viruses are not so likely to be detected and the antivirus program is just taking up space and CPU cycles.

Know that you are getting a good working antivirus program. Check out; av-test.org, www.icsalabs.com, and www.virusbtn.com. These are three top independent testing labs. All they do is test antivirus programs and rate them according to how fast they can spot and remove different viruses

Anti-Spyware Programs

Anti-Spyware programs are a dime a dozen, there are good ones and bad ones. Most all anti-spyware programs compare known spyware files to what is on the hard drive of the installed computer.

I have seen anti-spyware programs that would run spyware in the background of its own program. The Security and Exchange Commission has stepped in and ordered one maker of an anti-spyware program to take it off the market. It was scanning the hard drive, saying there was spyware on the computer, and wanted \$49.95 to clean up

SAFE COMPUTER HABITS

the spyware on the hard drive. During this whole process, they would install spyware on that computer.

SypwareWarrior.com and Lavasoft.com are two good sources for choosing a good anti-spyware program. Spyware Warrior tests spyware programs and report on their reliability.

Firewalls

Firewalls have two major functions. That is to keep the bad guys out, and not letting what is inside out unless you give it permission.

When you go on the internet, you will do different things, like email or online transactions. These functions will go through specific doors or frequencies, which are called ports. Email is usually sent and received on ports 110 and 25, respectfully. Web surfing is done on port 80.

Most firewall set-ups allow or deny certain programs to access the internet. This will allow your web browser and Windows Media Player, the two basic ones, online access. Some programs need to access the internet in order to run. A good example is the Help and Support function of Windows XP. This saves disk space on the hard drive and gives the computer user up to date help.

The rule of thumb that I use is, if I click on a program I trust, and it wants to go out to the World Wide Web, to retrieve some information, then I will allow it. While I am just reading a web page and then I get a pop up from my firewall about going to another web site for no apparent reason, then I will tell my firewall to block it.

Zone Alarm.com is considered an award winning firewall company. They have branched out in the past few years in other types of protection.

Intrusion Detection

An intrusion detection program works differently than the way a firewall works. Intrusion detection stops and informs you that something is trying to make a change to your computer. Unlike antivirus programs, which scan a computer's hard drive periodically, an intrusion detection program monitors the behaviors of the computer. Intrusion programs are becoming more popular with the increased use of broadband connections, where the computer stays on all the time. This gives an extra layer of protection.

Below are the commons behaviors that are monitored, by an intrusion detection program.

- Changes to the programs when Windows starts.
- The launching of new programs.
- The alteration of existing programs including DLLs.

SAFE COMPUTER HABITS

- Changes to key areas of the Window Registry.
- The launching of new processes or modification of existing processes.
- Installation of new hardware/software drivers.
- Termination of key programs, processes and services.
- Browser home page changes.

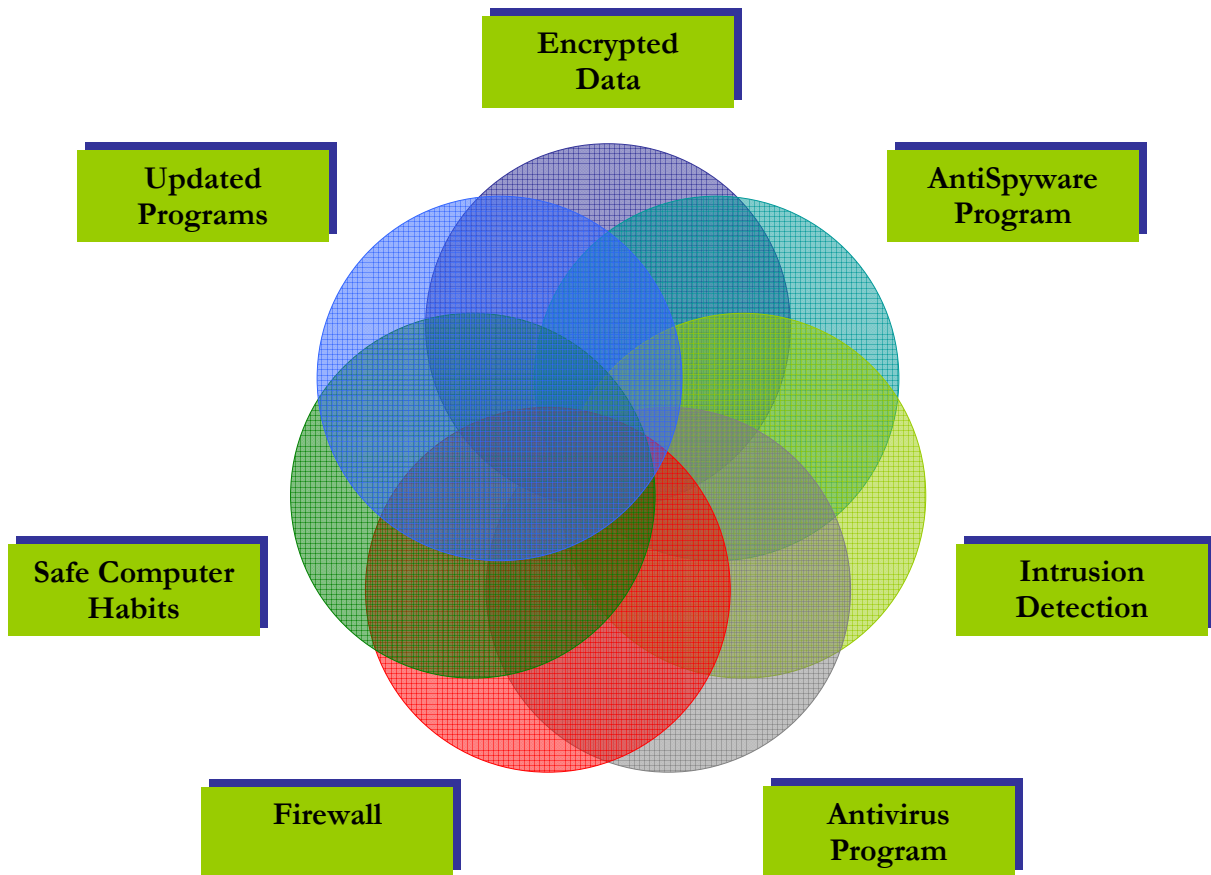
Layered Protection

I am not a big fan of putting all my eggs in one basket. This especially holds true when it comes to the security of my computer and its connecting network. I have seen attackers use different types of attacks to gain entrance into a network. Entrance was gained by gaps or holes in the protection.

I have found that programs that overlap in their protection give extra protection from an intruder slipping through those gaps. I use antivirus program for my antivirus protection. A firewall program, from a different vendor, as my firewall protection. Another vendor supplies my spyware removal program. Finally, I use intrusion detection program that constantly monitors my computer for any unusual activity. These combinations of two are proactive (the firewall and intrusion detection), and another combination is reactive to attacks (antivirus and anti-spyware programs) give me a healthy protected system.

The best way to illustrate this is by picturing seven layers covering your data. First, update programs and operating system. Second, a firewall, limits what can go into and out of your computer. Third, there is an antivirus program that inspects for malicious computer code. Fourth, is an intrusion detection program that looks for any changes to the computer's file system and alerts the user. Five, is a spyware program scanning the hard drive. Six, for protection of important information there is encryption, of sensitive data and stored passwords. Finally, number seven, safe computing habits that make the first five work together as a unit. You can see this illustrated on the next page.

SAFE COMPUTER HABITS



Chapter
3

“Bad habits produce little and poor quality, and poor results. The level of good habits produces the same level of quality and good results.”-EFCussins

Good Computing Habits

Computer security experts agree that when it comes to infected computers it is the 80/20 rule. 80% of computer infections come through the person sitting behind the computer. This is by way of either, an on purpose retaliation or through lack of good computer habits. The other 20% of infections come from an outside source invading a network.



Protection from most all attacks can be hindered through some simple habits that can be done when in front of the computer. These habits should be taught, practiced, and encouraged for everyone who sets in front of a computer. This goes for family members at home, to employers and everyone in the work place.

Password Habits

Today, most operating systems, or enterprise level programs require a logon and password to access data or the World Wide Web. This is the first level of defense in protecting data on one's computer. The type and complexity of a logon and password can make accessing personal information extremely difficult if not near impossible.

One of the first major computer hackers, Kevin Mitnick used what was termed “Social Engineering”. He would get people to tell him their logons and passwords. In turn, he would use them to evade Federal government agents for years. There have been surveys, for years telling us, all of them denoting how easy it is to get logons and passwords from individuals. Stories arise, periodically how employees would give them up for a cup of coffee.

What is a good password?

The more complex the password the harder it is to crack. The more critical the data, the need for that password not only to be complex, but it needs to be changed 30 to 60 days. Unless there is question of a password being lost or stolen, then it may need to be changed sooner.

Password cracking software uses one of three approaches: **Intelligent guessing**, **Dictionary attacks**, and **Automation**. These password-cracking programs try every possible combination of letters, numbers, and characters to get a password. Given enough time, the automated method can crack any password. However, it still can take months to crack a strong password.

A good password should be 8 letters, numbers, or characters. The letters should be a combination of more character. These character need to have upper and lower case alphabet with one or more numbers thrown in for good measure. Ectkr5j8 is a good example of a password. Usually the best way to remember it without writing it down is have the letters and numbers part of a sentence or phrase that is easy to remember. (An example is "President Lincoln read from 2 books when growing up." This translates into a password, pLrf2Bwgu.

If you have trouble remembering multiple passwords, like me, there are several good secure password-managing programs on the market. Put it on a jump drive, and keep it in a safe place. Never write your login and password on a piece of paper, and stick it in your wallet or purse. That is asking to have your secure information compromised.

How Often Should a Password be Changed?

In the middle of 2005, About.com did a survey of 200 computer users. They were asked, "How often do you change your password?" A surprising 60% said they never change their password. 10% said they changed theirs weekly. 11% changed theirs yearly. 8% change their password every month.

Depending upon how secure and sensitive the access demands are, dictates the complexity, how often the passwords need to be changed. Access to financial information, like credit card accounts and other banking accounts, need to be changed every 30 to 60 days. Non-sensitive email accounts can go a year or more. On a personal home computer the passwords needs to be changed annually if not sooner, depending upon how many people use it.

E-mail Habits

The single most important source of attacks to a computer system is through opening e-mail. Think about it, you are inviting in digital code into your computer, when you open a piece of email. A group of ones and zeros in the right combination can send out all sorts of personal information from your computer

SAFE COMPUTER HABITS

to any place on the internet. The content of revealed information can range from Social Security numbers, credit card numbers, and addresses of friends and/or business associates whom you email.

When a computer user clicks to open their e-mail there are three basic expectations. When any of these three expectations are violated, the email system loses its value.

1. **Authentication** – The email comes from who it says that is comes from.
2. **Integrity** – The message of the email is what the sender sent.
3. **Privacy** – The only ones who know the message of the email is the sender and the intended receiver.

Phishing (pronounced fishing) has become the term for email that you receive. It appears to be from a well know business, but in reality, it is a fake. The purpose behind these emails is to get your credit card number, logon, and password. The result is capturing them to use in your name. They will drain your bank account or max out your credit.

This type of email can be spotted in four ways.

1. No real business will send you an email asking you for your credit card number or other personal information.
2. You must respond at once. They do not want you to think, or check out the email by calling the company's customer service dept.
3. These types of emails usually will not contain your first or last name, because they are sent out to thousands of email addresses at once.
4. Click within the email to verify your account. This is dangerous. If you move your cursor over the link, a box will show up at the bottom of the cursor. If the email link and what is in that box at the bottom of the cursor do not relate, this means your web browser is going to a look-a-like web site.



If you have a question about it being real, you can always call that company and verify that they sent you an email asking for personal information. If the company did send you the email, I personally, would stop doing business with a company that is careless with my personal financial information.

The best habit to check on an account from the bank or online store is not to follow a link in an email. Instead, log in through your usual method, by following a bookmark or going directly to the site's home page and logging in manually.

SAFE COMPUTER HABITS

Email attachments are another area in which email can infect your computer through email. Number one rule is do not open any email attachments. There is an exception to this rule. You will always find friends and relatives sending you family pictures via email. My recommendation, then is that you verify with the known sender that they sent it and if is free of any malicious software.

At the end of all computer files is a dot and three letters. These three letters tell you what kind of file it is. There are some files that are abused by bad people, such as **.EXE, .COM, .BAT, .SCR, .PIF, and .VBS**. Below are what these files extensions mean and why they can be so dangerous.

These file types are most often abused by bad guys, such as **.EXE, .COM, .BAT, .SCR, .PIF, and .VBS**.

.SCR Screen saver program, which includes binary executable code. Other codes can be attached to it. Trojans can sneak in by downloading a screensaver.

.BAT Batch processing file, used to execute a series of contained commands in sequential order. Viruses, spyware, and Trojans can all use this type of file.

.COM Command file, containing scripts or even executables for DOS and Windows systems. A file containing “.com” as a suffix can run a virus on the Windows 95 and 98 operating systems.

.EXE Windows executable program can unleash a virus by just clicking on it.

.PIF Program Information File, tells Windows how to run a non-Windows Application. Root Kits that are based on UNIX can use this file to run its program.

.VBS Visual Basic Script, a scripting language built into many Windows programs, like Word, and Excel. These scripts can be modified to perform some malicious purpose.

Encrypted email, as a rule, is sent over the internet in a plain text format. It is like sending a post card through the US Postal Service. To have any type of privacy or expectation of real privacy, emails must be sent with some sort scrambling of the message; this is known as encryption.

| Encryption is nothing more than mixing up and/or replacing the letter, numbers, and symbols of your email message. Over the years, the way the encryption scrambles things, has gotten quite complex. PGP and Transport Layer Security with encryption are industry standards.

I am not going to go in depth about email encryption. I am just going to say, if you are going to encrypt some of your email, you may want to encrypt all your email. That way if someone is watching your email traffic, they will think nothing when you send something important, because everything you send is encrypted.

Web Surfing Habits

Tim Berners-Lee and scientists at CERN (Geneva) designed the World Wide Web concept in 1989. These men were interested in making it easier to retrieve research documentation.

The World Wide Web has become loaded with information for research and bargains to the online shopper. The Web has grown far beyond what anybody would of have expected. Along with these great new tools has come its dark side.

My recommendation when it comes to surfing the web is, know where you are going, and know the risks you will be taking. I like to download and test free programs. However, there are websites with malicious programs hidden inside, music, picture, and computer optimizing programs. Go to www.tensolutions.biz and click on Habits for a list of some of the sites I use.

Before registering on a website for a free newsletter or computer software, read their privacy statement. There are several good website you can download free software.

The Privacy Statement: The Privacy Statement of a website can protect you from getting into something that will cost you needless money and time. Most people just click, "Yes, I have read and accept these terms". Most people consider this a nuisance and click on "yes" without having read a word.

I know of only one or two people who read the Privacy Policies of websites they visit. Like most of us, we think it is a waste of time. It is a lot of legal jargon that is confusing.

Did you know that if you are installing a program or putting your email address on a website with the purpose of putting your email address on a mailing list for spam? They can do this legally because it would say so in that Privacy Policy.

I am going to give you three examples of why you should read the Privacy Policy.

1. I went to NASCAR.com and found in their privacy statement. "You may also be able to submit information about other people. For example, you might submit a **person's name and e-mail address** to send an electronic greeting card and, if you order a gift online and want it sent directly to the

recipient, you might submit the recipient's name and address. The types of personally identifiable information that may be collected about other people at these pages include: recipient's name, address, e-mail address, and telephone number."

Guess whom they give out this to? "We may also **disclose personally identifiable information to companies whose practices are not covered by this privacy notice** (e.g., other marketers, magazine publishers, retailers, participatory databases, and non-profit organizations) that want to market products or services to you." This has me questioning who is getting my personal information.

2. ZoneAlarm.com, a popular firewall vendor, has a more ethically safe Privacy Policy. "Except as described below, Zone Labs will **only disclose your personally identifiable information to third parties if acting under a good faith belief that such action is necessary** (1) Conform to legal requirements; (2) Protect and defend the rights or property of Zone Labs; (3) Enforce the Zone Labs Terms of Service; or (4) In the event of a merger, acquisition or sale of all or substantially all Zone Labs' assets relating to the business in connection with which the information was collected."
3. Ebay.com states in the first line, "Your privacy is very important to us. We do **not sell or rent** your personal information to third parties for their marketing purposes without your explicit consent." After reading through it, I felt secure doing business on eBay.

I have listed just three websites and their Privacy Policy. The point I am trying to make here is to take a little extra time and read the Privacy Policy before you give out any information. You may be surprised about the kind of people whose website you are visiting.

Downloading Habits

Programs with malicious programs inside often come from questionable websites. Some of the most prolific spreading of these malicious programs spread is through downloading file-sharing programs. The one that has gained the biggest attention in the past few years has been the download of music. To counteract the spread of infected music several businesses have started pay to download music. Real Player, Wal Mart, and several others e-stores sell music to download.

Before registering on a website for a free newsletter or computer software, read their privacy statement. There are several good websites you can download free software. Lists of those sites are at the end of this book or you can go to www.TENSolutions.biz and click on Habits.

SAFE COMPUTER HABITS

The best advice is to use caution. Know the site, read the Privacy Policy and End User License Agreements. Investigate the site before you invite into your home and computer any of their downloads.

The best advice is to use caution. Know the site, read the Privacy Policy and End User License Agreements. Investigate the site before you invite their download into your home and computer.

Read the EULA (End User License Agreement): It may seem like a lot of boring reading that some lawyer wrote. Yes, a lawyer probably wrote it. The best practice is to read the EULA on software, you buy. The EULA is a legal agreement you are making with the software vendor. Without reading it, you may be unwittingly agreeing to install spyware or a variety of other questionable actions that may not be worth it to you. If in doubt about something, you may just be better off answering, "No, I do not accept." at the bottom of the agreement. There is plenty of good software out there, without having to allowing spyware on your computer, just to use some free program.

Sometimes when you visit a web site a text box might pop up. Like the EULA, many users simply consider these a nuisance and will just click away to make the box disappear. Users will click "yes" or "ok" without stopping to see that the box said, "Would you like to install our spyware program?" Ok, admittedly, they do not generally come out and say it that directly, but that is even more reason you should stop to read those messages before you click "ok".

Instant Messages Habits

Security professionals all agree that the hardest area of computer communications to secure is the instant message. The best mindsets to have when using instant messaging is consider your self on an old telephone party line.

50 to 100 years ago, three or more neighbors would have their telephone lines connected. If you picked up your telephone to call someone, you might hear your neighbor talking to her aunt in another state. You would have to wait until she quit her telephone conversation before you could make your call. When you were on one of these party lines, you would have to be careful, about what you said, because someone might be listening. The same holds true when you use an IM.

When using Instant Messaging always protect yourself by:

- Only communicate with people on your know. Like e-mail address, do not post your screen name online. You can get spam through instant message.
- Never agree to meet a stranger in person whom you have met on IM.
- Never accept files or downloads from someone that you do not know.

SAFE COMPUTER HABITS

- Never accept files from people you know, unless they tell you first that they are sending it.
- Never use a screen name that includes your personal information. Never use Unhappyme13; this gives the impression of an unhappy 13-year-old. A better choice would be something like CareerWoman. No reference is given to emotional state or age. This will help keep online predator away.
- Sending personal instant messages at work is not a good idea. Your boss may have a right to view those messages.
- Be careful how much personal information you reveal when you're online or not.
- Children should be supervised when online or using IM. Make sure you know exactly whom they are chatting with online. What I have found to be a good way to accomplish this is to have the family computer in the dining room or living room, where the computer monitor is visible to everyone.

Chat Room Habits

Chat Rooms are a great way to communicate with people from around the world who have like interests. I have had conversations with an engineer in India, and a writer in England. Like with any use of the World Wide Web, there must be some precautions to be safe. I will refer you back to the section I have written on Instant Messaging. The reason being, Chat Rooms are a form of instant messaging and should be treated as such.

Web Blog Habits

In recent years, web blogs have been springing up all over the internet. You ask what a web blog is; well it is like a diary that is put on the internet. There have been several lawsuits concerning the content of what was written or displayed on these web blogs. Some families use them to keep in touch and find out what other members of the family are doing.

Like everything else, I know there are some basic practical habits to have when keeping a web blog. Note what I have listed below are from a safe and secure perspective. There is plenty of content ideas and guidance out there. Links to these resources are located at www.tensolutions.biz and clicking on Habits.

- **Identify Yourself:** You do not have to give your name, rank, and serial number. Give your readers some background about yourself. Such as interests, education, and age.
- **Give Readers a Way to Contact You.** Blogs are a way for fostering communication. When writing a blog or leaving a comment, leave an email address or another blog's URL for people to contact you. It is just good etiquette to give other readers a way to respond to your posting.

SAFE COMPUTER HABITS

- **Write in Good Format.** Web articles are usually short, about 150 words, simple, and to the point. Pick a good and easy font to read. Do not use more than a couple of font types and sizes. Look at the blog and see if it is easy on your eyes.
- **Remember Copyright Laws.** A quick way to get in trouble, when writing a blog, is to violate copyright laws. Don't post pictures and/or text that are not yours, unless you've been given written permission from the owner.
- **Credit Your Sources.** If you are quoting another blog or article, give him or her credit for what they have written. Always try to provide a link to the source of the quote that is used. When you use a certain part of an article or blog entry, it is important to attribute it to the author accordingly. It is also a good practice to mention your source, if you found a useful piece or link from someone else.
- **Validate Your Information.** If you are going to write about some event or news item, check your source. It could be embarrassing for you down the road if you find your information was not correct. A good rule of thumb is to link your information to at least two different sources. Don't forget to let the readers know what is fact and what is assumption.
- **If You Make a Mistake Post a Correction.** It is only natural that mistakes or wrong assumptions will be made. Be quick to admit to the mistake and make the correction. Your readers will love you for it.
- **Post Disclosures,—and Conflict of Interests.** When promoting a personal venture, on a blog, be up front about any conflict of interest. Your readers deserve to know that your bias will affect your writing.
- **Post a Disclaimer.** A disclaimer is there for protection when it comes to offering advice about anything. You will find disclaimers on everything from self-help books to many websites. It is good legal practice, especially if someone finds your advice to be faulty and they want to take legal action against you.
- **Use the Golden Rule.** Do not put secrets in a blog on the World Wide Web. It is a good way to make enemies and have a lawsuit brought against you. People have posted nude pictures and lost their jobs. While others have revealed company secrets. There have been a few blogs that have published their discontent with their employer. None of these folks has had good results.

I know there are free speech and First Amendment rights. However, keep in mind, would you want to read on someone's blog, the kind of content you are thinking about writing.

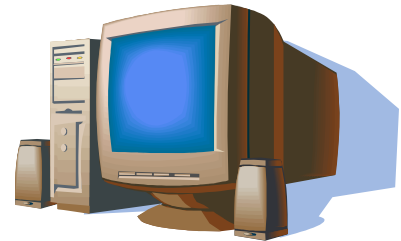
Chapter 4

“One must take care of the physical and spiritual to have a well-balanced life.” -EFCussins

Physical Computer Habits

Workstation Habits

In the next chapter, we will cover doing financial transactions online, because there is a whole lot of risk, and special precautions that need to be taken. First, let us discuss the physical part of Safe Computer habits.



There are some hard questions that you need to ask yourself as you look at where your computer sits in your home or office.

1. **Where do you keep your computer?** Placement of a computer, keyboard, and monitor need serious thought. The ability to stay alert and not take short cuts or make mistakes is influenced by the way the workstation is setup.
2. **Who can look over your shoulder when you are online?** I have done business with doctors, accountants, and wholesale companies. In some cases it is all too easy to look over the secretary's shoulder and get someone's personal data. The computer monitor and desk should be setup so if anyone comes into the room; they would not be able to see the face of the computer monitor. This goes for home computers. You do not want your children seeing your financial information and telling the neighbors.
3. **Can a visitor use your computer?** What I like about Windows XP is if someone has come to visit, and they want to check their email, I can set up a Guest account for them. They can check email, surf the web, and still not have access to any of my personal data. This includes not having the ability to installing any program, on my computer without my permission.

Backup Habits

Now that you are secure, back up those files and data, just in case a physical failure happens to the software or hardware aspects of the computer. We live in an imperfect world. Things do break unexpectedly. If one is not prepared for a disaster, then it could be costly and devastating. If we are prepared, a computer hardware or software failure can be recoverable with a minimal amount of downtime and money.

I could tell you story upon stories of individuals and small businesses that lost customer lists, orders, and money from not having their computer system backed up. With each back up there must come a set of practices to ensure the backups are good.

1. **Back up of data must be done regularly.** Usually a weekly full system backup and daily data backup is recommended.
2. **Verify that each back up is good.** The best way to do this is take a (non-essential) file in that back up and damage the original, and then restore it. Nothing is worse than restoring lost files and finding that the back up disc has damaged files, and cannot be used to recover the data.
3. **Keep the back up discs or tapes offsite** from where the computer is located. Suppose a fire happens. Not only would the computer and its data would be lost, but the back ups will be gone. Then it is the same as wasting time doing the back up.

A bank's safety deposit box, or some secure location is a good place to rotate the back ups, as often you do back ups.

What to Backup? The big question that I am asked is "What should I back up, the whole hard drive or just certain files?" If you have an external hard drive, large enough, back up all the drives on the computer. However, if you do not want to back up the complete hard drive, then there are certain files and difficult to replace information, that should be backed up. Below is a list to start with when backing up selected files and information.

- Document, MS Word files, spreadsheets, and resumes.
- Quicken or MS Money back up files.
- All logon and passwords to websites or web accounts.
- Photos, movies, and any edited artwork.
- MP3's and other music files.
- Web browser bookmarks and /or favorites.
- Activation codes for programs that you have registered.
- Internet Service Provider and Email Settings.
- Any other information that would be hard or next to impossible to replace.

Maintenance Habits

A computer will not do you any good if the mechanical part doesn't function properly. As I do regular maintenance on my car, so I have to do regular maintenance on each one of my computers. Below is a list of month maintenance routines.

1. **Verify all Windows Updates** are current. There are settings to have computers check for updates and fix problems automatically, but it never hurts to check that the updates and fixes are being done. If you have, Windows XP connect the computer to the internet. Click on the **Start** button, go the **Control Panel > Security Center**. On the left side click check on Windows Updates
2. **Verify the antivirus program is up to date and full scan** was run in the past 24 hours. This is done by opening the antivirus programs' control panel from the **Start > All Programs**. Then navigate to where it records the last update and the last time a full scan was done.
3. **Verify the spyware program is up to date and has run a full scan** in the past 24 hours. Most spyware programs are structurally similar to antivirus programs. So checking on when the last time it was updated and scanned is completed.
4. **Delete all junk and temporary files; make sure these files** have been cleaned off the hard drive. This maintenance functions can be done several ways. The easiest is to click on the **Start** button **>All Programs >Accessories >System Tools >Disk Cleanup**.
5. **Defragmenting the hard drive** so the data can be arranged on the hard drive in an efficient manner. This makes it quicker to access files. To defrag the hard drive click on the **Start** button **>All Programs >Accessories >System Tools >Disk Defragmenter**. This operation can take from a few minutes to several hours. It all depends on the speed of the processor, the size of the hard drive, and how fragmented the hard drive has become.
6. **Back up important information** that you do not want to lose. Windows has built in a backup program in most of its operating systems. Some programs, especially financial programs, have a built in back up function. Copying files from the hard drive to some form of removal media is the simplest and often the easiest.
7. **Check for dust and dirt build up** around the power supply fans, and any other fans. For people who are not comfortable opening the computer case, it is best to have a professional clean it out at least in the Spring before the weather start to get to hot.

Habits Concerning Selling a Computer

Do not just sell or get rid of your old computer without first getting any personal information off your hard drive. The easiest and best way to accomplish this is to reformat the hard drive and re-install the operating system. Reformatting a disk cleans the hard drive and gets it ready to accept a new operating system. It also wipes out everything on the hard drive.

If you are not sure how to do this, there are inexpensive programs that can reformat or erase the hard drive. My preference is to erase the hard drive by writing zero and then ones on the hard drive. The better programs will do this three to seven times. You can find such a program for around \$20.00. In addition, there are some free ones online.

If you are going to sell the computer, and don't have the original operating system disk, you might consider donating it to some organizations that refurbishes them and gives them to schools or students who can use an older computer. Depending upon the state, you can get a healthy tax write off.

Chapter
5

“I work hard for my money. I don’t need to waste my money by shopping foolishly.” -EFCussins

E—commerce Habits

I have devoted this whole chapter to financial transaction done over the internet. If you stop to think about it, exchanging money for goods and services over the internet is an easy way to be ripped off.



I love the convenience of punching in a couple of number and all my bills are paid. What I do not like is losing hundreds or thousands of dollars, because someone intercepted important account information.

The bulk of the responsibility for your online financial transactions being secure falls to the company that wants your business. However, there are some basic things you can do to protect yourself. That can be summed up in one-word “**VERIFY**”. Verify every online store, means of transfer and transaction.

Online Shopping Habits

Take a little time to know some things that will make you a wise shopper online. These tips will help keep you from someone trying to take advantage of you next time you shop online.

- **Read Product Reviews.** Read product reviews from more than two sources. Everybody has his or her own bias. To get a good well-rounded review about a product, read several reviews from different sources. For a list of resource of product reviews go to www.tensolutions.biz and click on habits
- **Shop for the Best Deal.** Shopping online has no real advantage if you will end up paying more than, if you went to the local mall.

SAFE COMPUTER HABITS

Compare prices and make sure that the price includes shipping, and any other extras you might want.

- **Read Everything:** Read the terms of purchase, privacy statement, and warranties. Then ask yourself if this is a place, you want to spend your money. If you do not feel comfortable, there are plenty of other websites that have an online store.
- **Know Your Rights:** There are laws that protect you wherever you shop. There are website listed in the appendix where you can go to find out about your shopping rights. Do not let some e-store rip you off, because you do not know your rights.
- **Pay By Credit or Charge Card:** This is one more way you can protect yourself from someone taking advantage. All credit card transactions are protected by the [Fair Credit Billing Act](#), which covers disputes over non-delivered or misrepresented merchandise.
- **Maintain Your Privacy:** When making a purchase; make sure you are on a secure connection. Check in the address bar. Make sure there is an s after the http. In the lower right hand corner of your web browser will also be a little lock that is closed.
- **Keep Records:** A printed copy of order confirmation along with a digital copy is the best defense if something goes wrong. The order confirmation usually will have a shipper tracking number, so you can track your order.
- **When Something Goes Wrong:** An unsatisfactory shopping experience, starts when you realize the goods you order is something less than you had purchased. Stay calm contact customer service of the e-store. Make sure you have all your documentation ready. Most online retailers want to maintain a good relationship with their customers.

Online Banking Habits

In a society when time is so critical, the opportunities to do all your banking from the family computer can be a time saver. One can be spoiled by getting a paycheck through direct deposit, and then pay all the bills online.

Today, it is a rarity for a bank not to offer online bill pay. Larger companies want their employee to have direct deposit. Banks find that in providing such a great convenience for its customers, it also inadvertently has opened the doors for hackers. Through a computer terminal thousands of miles away, a bank could be robbed. Getting your banking information a thief could take your money, before you could become aware that has happened.

Know who has access to your computer. Someone using your computer could access entering a PIN number or a password on an e-commerce website. Separate logons with individual access permission is a good start. Encrypted important logon and passwords are the safest way to protect yourself from other people, who have access to the same computer you use, possibly getting this information.

Shred documents before they get in the garbage: Thieves will dumpster-dive for old credit card bills and other important documents. Even a scrap of paper with a password is an open door to opening up your bank account to the world.

Erase digital data. You cannot shred your hard drive like paper. However, there are ways to delete a file, and to erase it. Deleting a file just removes the pointer to where it resides on the hard drive.

Erasing a file runs a bunch zeros over the file and then a bunch of ones. This is done various numbers of times. One such standard runs zero and then ones over a file seven times. This removes all possibility of recovering any of information in the file.

Check your online statements regularly. My personal favorite part of doing online banking is that I can check my balance any time I want. By checking my bank account or credit card balance every other day, I can catch any identity theft or unauthorized transfer of money.

Pay your bills with a secure connection. Data is transmitted over the internet in an easy way to be intercepted. When it comes to paying bills, and being

SAFE COMPUTER HABITS

connected to your financial institution, check your web browser's address bar. If the first five letters are https, then you can continue knowing that you are on a secure connection. If that last little "s" does not appear, Log off and contact your financial institution's tech support. That little "s" means you are on a secure connection.

Limit the information that you give out. Having your social security number or driver's license number on your personal check is giving out too much personal information about yourself. A single young woman should have her check printed with C. Smith not Cindy Smith. I am even opposed to having one's telephone number on personal checks. It just gives too much information for anybody to read.

Check your credit report annually. Since recent laws have been enacted, one can check their credit report free once a year. The big three credit reporting agencies (Equifax, Experian and TransUnion) joined forces to provide free credit reports to consumers.

Check the accuracy of all the information. If there is anything you disagree with, get it taken care of as soon as possible. You do not want to apply for some big loan and find out that you don't qualify because someone else has been using your credit or identity.

If you question something, contact your bank. Any irregularity could be a sign of someone sneaking money out of your and other people's accounts. Do not stop until you get a satisfactory answer. Some bank employees do not like making waves, so they try to quiet a questioning customer with some canned answer.

If you do not feel secure with how your bank handles your online transaction, then it is time to switch to one that can give confidence in how they handle your money.

Chapter 6

“If I cannot protect my family then I am worst that a heathen or infidel.” -EFCussins

Family Computing Habits

This chapter is not long, but it is one, I feel is the most important. All of the previous chapters are mere words unless they are used to protect the reader, and their family.



Communication Habits

Family communication can build a strong wall of protection for every member of the family. The best way, I know, is to instill **Safe Family Computing Habits** is by making everyone accountable to other members of the family about their time on the computer. It does not take rocket science, but it does take time and energy to make it work.

1. Encourage and share websites that are a benefit to family members.
2. Share pictures and music with other family members.
3. Discuss precautions about going to chat rooms.
4. Discuss chatroom, email correspondence of family and friends.
5. Have the family computer monitor easily seen by parents.

Activity Habits

The whole family, school, or special interest groups can enjoy many activities. With the right habits, there are many ways a family can have fun with their computer. Children use computers so much in school and in life today, it is beneficial to any parent to work with their children on family projects.

Organizing family photos Take old family photos and scan them on to the hard drive, then organize them by branches of the family or by date. I cannot think of any

SAFE COMPUTER HABITS

better way to teach children about family history and give them some computer skills at the same time.

Play games You don't need an X Box or Play Station. There are many interactive games for all ages. My wife and daughter play Sims together. See the Appendix for more choices.

Desktop publishing There are hundreds of things you create and print. It could be from coloring book pages, customize tee shirts, greeting cards, poster, or award certificates.

Keep in contact with family members A \$50 web cam and speaker in both households can allow family members to communicate anywhere in the world. We have seen this same setup used by soldiers with their family in Iraq.

Plan vacations A good fun filled family time could be gathered around the computer, planning a family vacation. It may sound like the last few minutes of a tied basketball game, but it will be fun.

Research a project It does not have to be for school. Maybe you want to get some background before taking a trip up to Hell's Canyon. If a child or anyone in the family has a question, research it in the internet. You may be surprised at the information, and the way it is presented.

If you lack the knowledge and/or skill to do a project that you want to carry out, you can find many resources where you can learn about how to do them, on the internet. It doesn't have to be a college course. A lot of Adult Education programs, Public Libraries, and Local PC Users Groups, all provide help for the novice users.

Resources

Go to www.TENSolutions.biz and click on Habits for a complete list of website you can visit about the topics discussed above. I have decided to post the resources online, so I can keep them up to date. As things change and new material comes out. The web page will be update.