A "STRESS-FREE" PC ©

As you know, there is no such thing as a totally "Stress-Free" PC, but there are many things you can do to reduce the stress and worry of owning one.

As we use our PC's, many of us worry about losing our data files, losing our email, losing our Music, losing our photos, losing our identity, losing our power, losing our ability to boot the PC, losing control of our PC to hackers, Spy-ware, etc. Wow, we worry a lot! It's a wonder we dare use our PC's at all.

To help solve and minimize these worries, here is a collection of ideas to help protect your computing environment. These steps are not really that difficult nor expensive and many of them are free. There's lots of assistance available to help you including; User Groups, Friends, Internet Forums, Internet Googling, PC Magazines, etc. Plus, there is lots of help applying many of these suggestions in the various self-help documents on my website at: www.jimopi.net .

Will it take a lot of thought, time and energy to implement these ideas? Yes at first, but once you have the processes in place, the regular time spent is minimal.

Will I see a payback? You will only see a tangible payback for your time and energy if you experience some kind of catastrophic situation. Just like with house insurance; If nothing bad ever happens, you will never know if it was worth it. I can assure you that having these processes in place will give you a warm fuzzy feeling of being protected, and you will sleep better at night.

There are three main areas of action: 1) Protect your PC from bad things happening, 2) Prepare your environment, so you can recover if bad things do happen, and 3) Practice Behaviors that keep your identity, your data, and your system secure.

1) PROTECT YOUR PC:
  a. HARDWARE ROUTER:
    1. Buy yourself Hardware Router *(Even if you only have one PC)*
    2. Even the cheapest routers act as a hardware firewall to protect you.
    3. Routers simply plug in between your PC and your Modem.
    4. Be sure to change the "Admin" log-in password from the default to something private.
    5. Either disable the Wireless feature and hardwire your connection, or lock-down the Wireless using WPA/WPA2 Encryption and a good password.

  b. WINDOWS 7 8 or 10:
    1. To secure your system do the following:
      i. Create a "Standard" User Account for daily use. *(Never use an Administrator Account for daily use).*
      ii. Secure both the Administrator Account and the Standard Account with a good password.
      iii. Now every time something important is about to happen, you will be asked for the admin password.

    2. All of these operating systems offer added security call UAC (User Account Control) that makes it a little more difficult to get infected while browsing. (This usually happens from a "Fake" Antivirus pop-up that tricks you into installing a trojan). If you accidently click on the fake "You are infected with malware" warning pop-up, UAC gives you a second chance to not get infected. If your Administrator Account is password protected, you have to enter that password before you would get infected. *Note: If you are still using Windows XP, you get no second chance.*

  c. WINDOWS UPDATE:
    1. Understand this: You must keep your Windows Updates current or you will get infected, even if you have the best anti-virus program running and up-to-date. You will get infected simply by browsing the internet and using your PC normally. Hackers know that a vast number of PC users do not do their Windows Updates regularly, and they exploit that fact. There is no substitute for keeping your Windows Updates current.

2. Make sure "Automatic Updates" is turned on, this ensures that all your "HiPriority/Important" Windows Updates get installed. *(Control Panel > Automatic Updates)*
3. XP:
    i. Manually go to Windows Update *(Start > All Programs > Windows Update or Microsoft Update)*, and make sure the "Windows Update Home" screen actually says "Microsoft Update Home". If it says "Windows Update Home", then click "Microsoft Update" on the right-hand side of the Windows Update Main screen. This will ensure that all Microsoft products (like Office) are also up to date and not vulnerable.
    ii. Manually go to Windows Update (or Microsoft Update) and make sure all High Priority Updates are installed.
4. WINDOWS 7 & 8:
    i. Go to Windows Update and make sure your settings are set up to automatically include updates for all Microsoft Products and to include all Recommended Updates with the Important Updates.
    ii. Make sure all "Important", "Recommended" and "Optional" updates are installed.
5. WINDOW 10: There is not option to stop the Updates.

d. WINDOWS FIREWALL: Make sure the Windows Firewall is "ON". *(Control Panel > Windows Firewall). (Note: Some Anti-virus Suites turn it off and use their own Firewall).*

e. ANTI-MALWARE PROGRAMS:
1. GENERAL TIPS:
    a) Make sure your PC is running some kind of Anti-virus Program that includes automatic updates, full-time protection and scheduled scans.
    b) Make you are running the most current version of this program and that its subscription has not expired.
    c) Full-Time Protection, sometimes called "Real-Time" protection, means that it is always running in the background monitoring and protecting you agains intrusions.
    d) Set up your A/V program to scan "Incoming" e-mails, but not "Outgoing" e-mails. If it offers to "Certify" mail, make sure that "Certify" mail is turned "Off".
    e) Setting up a scheduled automatic scan once each week is a good idea.
    f) It is best to only have one anti-malware program running with real-time protection. Not only can they conflict but each program slows down a PC. The more there are running, the slower your PC runs.

2. WINDOWS DEFENDER/MICROSOFT SECURITY ESSENTIALS (MSE): Microsoft has released its free Anti-virus program called "Microsoft Security Essentials". MSE offers automatic updates, full-time protection, ans scheduled scans. Although not a full anti-malware suite, MSE offers good basic protection and is a program that you can install, set-up, and forget about..... as long as you keep your Windows Updates current. You can run MSE along side your preferred anti-malware suite, but I do not suggest it. Running multiple programs all doing the same thing just slows down your PC unnecessarily. .

3. SCAN REMOVABLE DEVICES: Note: If your A/V program offers an option to automatically scan all removable devices each time they are inserted, be sure to activate this feature.

f. MULTIMEDIA SOFTWARE UPDATES:
1. Make sure your multimedia utility programs are all up-to-date. This includes: JAVA, FLASH-for-IE, FLASH-for-Firefox, Adobe Reader, Quicktime, etc.

2. A free utility called Secunia PSI (Personal Software Inspector) is a really cool way to help keep these and other programs up to date against vulnerabilities. Download it, install it, and run it regularly. *Details can be found in my "UTILITY PROGRAMS" sheet.*

A "STRESS-FREE" PC ©

g. UPS: Buy yourself a Battery Backup Power Unit. This protects you if you lose power at a critical time, and allows you to gently close the PC down without crashing. *(A UPS is not as important if you use a Laptop that is plugged in. The charger acts a shield).*

h. AUTOPLAY/AUTORUN:
   1. When you insert a DVD, CD, flash drive, or external hard-drive, your system hops to work to see if it can figure out what you might want to do with the media. This is called Autoplay or Autorun.
   2. This "¿Feature?" of Windows makes your PC vulnerable to trojans and viruses that may be hiding on the media and can infect your PC before you can say "YIKES!".
   3. Autoplay~Autorun can & should be disabled for Removable Drives. For XP, using the TweakUI utility program is the simplest and best way to do this.
   4. See my "XP TIPS" or my "WINDOWS 7 TIPS" sheet at www.jimopi.net for instructions. Window 7 process is the same as Windows 8 / 10.

i. PASSWORDS:
   1. Good passwords are key to securing your PC and your personal information.
   2. Use a different password for each e-mail account and each website log-in. *Remember, if you use the same password for everything, and it gets compromised, you're dead meat.*
   3. Never use a single word password. Instead use a short phrase, including some numbers. For example: "happy2cu4now" or "my5kidsrgr8" or "myh0useisbr0wn".
   4. Officially, it is recommended that you mix upper and lower case characters in a password. Personally, I stick with all lower case for ease of entry and to avoid finger confusion.
   5. It is also recommended that you include at least one special character in every password. Be creative: Something like "C@@LDUDE" works and is easy to remember (and is one case).
   6. Never use all or part of your user ID, your e-mail address, your name, or common personal dates in your passwords.
   7. Use caution when creating passwords that include I, l, 1, 0, o, or O. It is too easy to confuse one's memory and forget the proper password. Using zero's inside a phrase makes it easy to remember. For example: p00persc00per
   8. Use extra long, extra strong passwords for logging in to financial sites like PAYPAL or your bank. For PAYPAL, I also suggest using only a credit card with your account and never link you main bank account to PAYPAL.
   9. STORING "PASSWORDS" IN A FILE:
      a) If you keep a list of passwords in a file on your computer, make sure that file is either hidden or protected by encryption.
      b) At the very least, name your password file something that only has meaning to you. Do not name your file; "passwords.doc" or "passwords.xls". Duhh....
      c) Instead, name your "passwords" file something off-beat, like "Recipes.doc" or "Flowers.doc".
      d) Also, there are "Locker" Programs that are free or cheap that will hide, encrypt, and password protect personal data files.
   10. STORING PASSWORDS IN YOUR BROWSER
      a) If you tell a website to remember you and keep you logged in, you have just allowed the site to store your password in a file called a "Cookie"
      b) Even though Cookie files are located on your PC, unauthorized people can access them under the right circumstances. Therefore, you should not permit websites to remember you. In fact, I automatically clear cookies every time I close my Firefox browser.

    c) It is far safer to let your Browser's Password Manager keep track of your log-in ID's and passwords. (Firefox, IE7, and IE8 can all do this).

    d) The ultra safe method is to log-in to a website manually each time by entering your User ID and password by hand. *That's pretty tiresome but I do it this way with high risk sites like PAYPAL*

j. E-MAIL SET-UP:

    1. E-MAIL PASSWORDS: The best single thing you can do to secure your e-mail is to pick a good password, following the ideas shown in the last section on passwords.

    2. BLOCK IMAGES: Set up your email program to block all images by default. *(Note: Thunderbird can be set up to automatically block all images, except from approved friends and family)*

    3. Setting up your e-mail to use "Plain Text" is safer than using "HTML" e-mail, but not as pretty.

    4. Be aware that even with your anti-virus program set to scan all incoming e-mails, you are not fully protected. You must practice the secure behaviors described later on in the next section.

    5. Note: The Thunderbird program is generally a more secure e-mail client than Outlook, Outlook express, Windows Mail, or any webmail through your browser.

k. SAFER BROWSING:

    1. USE FIREFOX, not INTERNET EXPLORER: The Firefox browser (free) is generally safer than Internet Explorer, and offers several add-on's that enhance security even more. Especially if you use the Firefox add-on called "WOT" (Web Of Trust). For added protection, try the "NoScript" add-on. Also, I always set up Firefox to NOT accept 3rd party cookies. If you insist on browsing with IE, at least install the WOT add-on for IE.

    2. SANDBOXIE: PLEASE install and use the Sandboxie program to make your browsing Safe. To find out what Sandboxie is and how to use it, see the full writeup on my site at: www.jimopi.net

    3. COUPON PRINTING PROGRAMS: Never download and install any Coupon Printing programs. They invade your privacy and can be adware/spyware/malware.

l. PC TEMPERATURE: Install a temperature monitoring utility like "SpeedFan" (free) to ensure that your PC is not overheating and in need of dust removal. NOTE: SpeedFan and similar utilities will not work on most older PC's. A PC must have hardware temperature sensors installed inside for any temperature monitoring program to work.

m. OPENDNS.COM: This site helps secure your browsing. You can activate this site by setting up your Network Connections to use the "opendns.com" DNS servers instead of the servers provided by your ISP. *See: www.opendns.com/start/ for step-by-step instructions.*

2) PREPARE YOUR ENVIRONMENT:

a. RECOVERY DISKS: Make sure you have a full set of "Windows Install" or "System Recovery" DVD's or CD's on hand (or kept safe off-site). Having a "Recovery Partition" on the main hard-drive can restore the system back to a "New" state if you have malware or file corruption, but is of no use if the drive fails. In this case, you will need these disks to put the machine back to a "New" state. If you don't have a set, there may be a utility on your PC to burn a set. Contact the manufacturer for instructions on burning or buying a set. Do it!

b. BACK-UP PLANS: Put multiple back-up processes in place, not just one.

    1. "DATA" BACK-UPS vs "IMAGE" BACK-UPS:

        a) A "Data" backup is an exact copy of just your personal individual data files and folders.

        b) An "Image" backup is an archive of all the files and folders on your entire "C Drive". It is a complete image of your main Hard-drive that can be used to completely restore the PC back it original state at the time the "Image" was taken.

        c) Recovery using an image of the hard-drive saves lots of work and time over putting the PC back to a "New" state using recovery disks, then re-customizing everything.

A "STRESS-FREE" PC [ⓒ]

2. "DATA" BACK-UPS: Plan periodic backups of all your personal data to CD's or DVD's (and then store them off-site in a safe place). Quarterly is good. In addition, you should install a program to do automated weekly data backups to a second hard-drive. *I use a free program called SyncBack. See the tip sheet called "BACKING UP YOUR PERSONAL DATA" at www.jimopi.net for details.*

3. "ON-LINE" DATA BACK-UPS:
   a) Another way to safely back-up your personal data off-site is to use an on-line data backup service like Carbonite, Jungledisk, or Mozy.
   b) This method is fully automated and convenient. Pricing is fairly cheap.
   c) These sites work very well and can even archive several versions of the same document.
   d) Once you set this up, it automatically sends an encrypted copy of every file saved on the hard-drive to their server in the sky.

4. "IMAGE" BACK-UPS: *(See the "BACKING UP AN IMAGE OF YOUR HARD DRIVE" tip sheet at www.jimopi.net for details*).
   a) RESCUE BOOT DISK: After installing an image backup program, the first thing you must do is burn a bootable "Rescue CD". This is the CD you will boot to recover if your System will not boot. Be sure to try out the new CD to make sure it boots OK and recognizes all the hard-drives.

   b) EXTERNAL HARD-DRIVES: It is best to put the back-up image onto an external Hard-drive*.* They are better than internal drives as they are portable, can be used to back-up multiple systems, and be stored off-site. Even more important, external drives can and should be powered off when not in use. When shopping, get a full size drive that has its own power pack and has an ON/OFF switch, so you can turn it off when not doing backups.

   c) TESTING THE WHOLE PROCESS: If at all possible, try out your back-up process to make sure it can restore the system. Trying this on a spare hard-drive is an easy and safe way to do it. *If there is no spare drive, you can do it when you first buy a PC to reduce the risk, because you have your system recovery DVD's (hopefully) to put things back as they were when you bought it.* If you dare not do this, then at least "Validate" the backed up image archive using your Image back-up program.

5. USING FLASH DRIVES FOR BACK-UPS:
   a) **Warning: Never trust Flash Drives as your only means of back-up for data or image archives.**
   b) Flash drives are prone to unexpected catastrophic failure without warning. They could last 10 years or 10 minutes
   c) Using 2 or 3 Flash Drives with duplicate data would possibly be a reasonable alternative to DVD's or CD's for your personal data.
   d) Personally, I never recommend flash drives for storage of back-up data.

3) PRACTICE SECURE BEHAVIORS:
   a. USING YOUR E-MAIL:
      1. ATTACHMENTS:
         a) Never open e-mail attachments from strangers.
         b) Use caution when opening any attachment, even from friends and family. Especially, if it is something that was forwarded from someone else.
         c) To be safer, first detach or save the attachment, then scan it with an anti-virus program before opening it. *Even a Powerpoint show (.pps) or a photo (.jpg) can be infected.*

2. CLICKING LINKS:
   a) Never click a button or a link from inside an e-mail.
   b) Never trust the text of a link to tell you where the link will take you.
   c) If you hover the mouse pointer over a link in an e-mail, a pop-up of some kind usually tells you where the link will go.
   d) If desired, copy & paste the link into your browser, thne look at the link in the URL box and make sure it is going where you think it is going.

3. BCC: Always use BCC when sending or forwarding to a group to protect the privacy of others. Most e-mail providers and clients allow you to change the TO or CC field to BCC by just clicking on it. Each provider is different. You then put everyone's address in the BCC field. If a TO address is required by your provider, put your own address there.

4. FORWARDING E-MAILS:
   a) Do not forward e-mails that include an attachment from someone else. You could be spreading a virus or a trojan even if it did not affect you.
   b) If you must forward an e-mail, be sure to delete all the e-mail addresses, all the way down the body of the e-mail to protect the privacy of those people listed.

b. RUN ANTI-MALWARE SCANS
   1. For each of your Anti-malware Programs, run the on-line updates, and then run a full scan at least once a month.
   2. Anytime you plug in a strange removable device into your system (CD, DVD, Flash drive, or external drive), you should first go to *(My Computer > right-click the drive)* and run an Antivirus scan on it.

c. RUN SECUNIA PSI SCANS: Running this scanner once or twice a month will make sure your most common programs are up-to-date against known software security vulnerabilities; especially JAVA, FLASH, and Adobe Reader.

d. BACKUP, BACKUP, BACKUP
   1. DO "DATA" BACK-UP's REGULARLY: Backup all your personal data files, e-mails, pictures, etc. to CD's, DVD's, or an external hard-drive and save off-site. Monthly or weekly is good

   2. DO "IMAGE" BACK-UP's AT LEAST MONTHLY: Always backup an image of your main Hard Drive to an external or second physical internal Hard drive, never to the same physical drive the system is on. Do an "Image" back-up of the main hard-drive at least once a month. I recommend a full back-up once every 6 months and incremental back-ups each month in between (for a total of 5 incrementals between each full back-up). Incremental back-ups build on the last full back-ups and save on hard-drive space.

   3. KEEP A BACKUP HARD-DRIVE OFF-SITE: Physically take an external hard-drive containing your backed-up image off-site, so you can recover easily in case of fire, flood, theft, etc. (A safe-deposit box or a relative's house is good). *There are now many small cheap external Hard drives that will easily fit in a Safe-Deposit box. Buy two and alternate them off-site every few months.*

   4. DO PERIODIC HARD COPY BACK-UPS:
      a) Periodically, write down or print out all your critical information like: passwords, access info, log-in ID's, etc. and save this in a safe place off-site.
      b) Print out a hard copy of all your e-mail contacts and save off-site.
      c) Do a <Print Screen> of your desktop, paste it into a document, then print it out and save it.
      d) Do <Alt-Print Screen>'s of any confusing or complicated PC setups (like Network Connection settings). Paste those images into documents, print them out, and save them. Off-site if possible.

    e) All this depends on how important your computer is to you, how long you can stand to have it broken, and how much data loss you can tolerate.

e. PUBLIC INTERNET ACCESS: If you use your PC on a public wired or wireless network, you should act as if everyone can see everything you are doing, <u>because they can</u>. It is a bad idea to do on-line banking, purchasing products, or any other private activity while using a public internet access point.

f. SCAN YOUR HARD-DRIVES FOR ERRORS
1. At least twice a year, scan your main hard-drive using the Windows error checker (chkdsk) *(My Computer > right-click drive C > Properties > Tools tab > Error checking, "Check Now" button).* Be sure to check both boxes. Then OK, OK. The scan will run during the next boot.
2. I also recommend running a free utility called "HD TUNE" that indicates any problems with hard-drive health.
3. These scans help protect you against a surprise catastrophic hard drive failure.
4. Personally, I use a great utility called Spin-Rite to scan each of my hard-drives every 6 months or so, but it does cost $90.00.

g. KEEP EXTERNAL HARD-DRIVES POWERED OFF WHEN NOT IN USE: Always keep your external hard-drives powered off when you are not using them. This prevents them from getting infected if your system gets bitten by a malware bug.

BUYING A BATTERY BACKUP POWER UNIT (UPS)
(UPS = Uninterruptible Power Supply):

- When buying a UPS, first add up all the current rating labels (in Amps) on all the PC equipment you plan to connect to the Backup Unit, then multiply that amount by 120 volts to get your VoltAmp requirements. For example, if your total is 4 amps then your VoltAmp requirements are about 480 VA. For an automated calculator for sizing a UPS, see: http://www.csgnetwork.com/upssizecalc.html .

- Now calculate your UPS needs at about 1.5 times the VA's required by your equipment. ie: If your total usage is 480 VoltAmps, then buy a UPS with a rating of at least 700 VA and preferably one rated at least 750 VA. The higher the rating of the UPS, the more minutes of runtime you have after a hard power failure. A runtime of 10-20 minutes will be plenty to gently shut down all your PC's.

- Warning: Do not "under buy" a UPS. One that is rated at exactly your requirements may fault when first powering on all your equipment at once. The first 30 seconds or so is when the highest power usage occurs (As Displays power up and Hard-drives spin up).

- Techie Note: The VA rating vs Watts rating is confusing. With PC equipment the average power factor is roughly 0.6. This means that for PC's 1.0 VA is about 0.6 Watts. If the tag on your PC says 2.0A and 120V, then the 240 VA result would equal about 144 Watts. Most UPS's have both VA and Watts ratings on the box.

- The most reliable brands of UPS's seem to be APC and BELKIN. Triplett is OK.

SOURCES FOR RECOMMENDED SOFTWARE: Note: Details on installing and configuring many of these programs can be found at www.jimopi.net

MOZILLA Products:
- Firefox Browser - Free: www.mozilla.com/en-US/firefox/
  - *The "WOT" Add-on (This is great)*   http://addons.mozilla.org/af/firefox/addon/wot-safe-browsing-tool/
  - *The "NoScript" Add-on (Good but annoying)* http://addons.mozilla.org/en-US/firefox/addon/722
- Thunderbird E-mail Client - Free: www.mozilla.com/en-US/thunderbird/
  - *See Thunderbird Step-By-Step setup at:*   www.jimopi.net/

PRODUCTS TO AVOID MALWARE (Free):
- Microsoft Security Essentials: http://www.microsoft.com/security_essentials/
- Sandboxie (Safely browse the internet - Free w/Nag screen) http://www.sandboxie.com/index.php?DownloadSandboxie
- Secunia PSI (Personal Software Inspector):   http://secunia.com/vulnerability_scanning/personal/
- OPENDNS: (Safer browsing)   http://www.opendns.com/start/

UTILITY PROGRAMS:
- HDTune (Hard-drive health, performance, & Benchmark) http://www.snapfiles.com/get/hdtune.html
- Spin-Rite Program: www.grc.com/sr/spinrite.htm
  - *(NOTE: The SpinRite Data Recovery Utility Program is not free, but is money well spent.)*
- SpeedFan Program (Monitors Temperatures & speeds inside PC) - Free: http://filehippo.com/download_speedfan/
- TweakUI utility: http://www.microsoft.com/windowsxp/downloads/powertoys/xppowertoys.mspx

BACKUP SOFTWARE:
- SyncBack (automated data backups) - Free: http://www.2brightsparks.com/syncback/#download
- Acronis True Image Backup Utility   www.ugr.com/
  - *(This program is available at a discount at the above link and includes a free Tutorial).*

ON-LINE BACKUP:
- Automatic Online Data Backup sites: www.carbonite.com/ , www.jungledisk.com/ & http://mozy.com/
  - *Carbonite is currently $50.00 per year for unlimited storage. Jungledisk is variable priced on usage, but is cheap. ($20.00 startup and $0.10 per GB). Mozy is currently free for 2 GB or less, or about $5.00 per month for over 2 GB of storage.*
- Free OnLine Storage from Microsoft: http://skydrive.live.com/. & http://www.gladinet.com/p/download_starter.htm
  - *Skydrive is best used with a file managing program like Gladinet.*

Always check for the latest version of this article at: www.jimopi.net