

curity patches up-to-dated

This is especially true if using Windows OS's.

If your PC and or Network seems to be running too slowly and has done so over several days it is a sure sign that your systems are infected with malware and other intruders.

Clean it up by scanning with good anti intruder ware.

If you want give us a call and we can advise you on what works

or

You might want to subscribe to our anti intruder services. They come over the Internet or by CD and are updated monthly or more often at your convenience.

If you let this go you will pay a lot more for it than you wish.

WE have 20 Years Experience securing everyone from the U.S. Military to you.

Install Robogeek and get a Complete Security cleanup for 1/2 the normal rate.

SOME OF THE SERVICES

THAT WE PROVIDE

- ◆ Help Desk for all your software
- ◆ Data Recovery
- ◆ Data Storage and backup systems
- ◆ Upgrading of Systems
- ◆ We also Buy and sell select new / used equipment and software.
- ◆ Complete repair services for computers Networks and components
- ◆ Full Scale design and maintenance of NETWORKS , Wired and Wireless large and small
- ◆ Remote service and computer support
- ◆ Complete Computer Security – 3 plans available not one program
- ◆ Intruder removal and control
- ◆ Complete Networking
- ◆ Web Hosting and development
- ◆ Repair and maintenance of Computers and other electronic systems and devices
- ◆ A full spectrum of Training
- ◆ System Support for small/ medium size business and homes
- ◆ Consulting/ training on how to use IT to advance and start your business (40+ yrs of experience)
and much more

**INSTALL ROBOGEEK NOW
AND GET A FREE MOUSEPAD
SERVICE AS FAST AS A PHONE
CALL TO 805-988-9540**



A Quick Guide To System Security

Rev 1.31

Since 1987

Cal-Pac Technology

300 Montgomery Ave.

Oxnard, CA. 93036

805-988-9540

nccorthu@calpactech.com

For more Tips join

CPTech@yahoogroups.com. To do so
go to

<http://www.calpactech.com/> choose
CPTech or just email us

13 STEPS TO KEEPING YOUR COMPUTER SECURE

Step 1.

Keep your firewall turned on and running ALWAYS.

Step 2.

Limit access to your machine. Especially in an open business context someone may get you for ????. Reasons.

Step 3.

Use updated anti-virus/ anti-malware software

Use proven Software that works in real time. Don't just scan with something. Do not depend on package software like Norton/Symantec or Mc Affee security suites. Their Anti Virus is good Their anti Malware/Spyware sucks.

Step 4.

Monitor your network usage

Keep your little monitors in the system tray at the bottom right of your desktop and if they keep blinking like crazy when you are doing nothing on the Internet check it out

Step 5.

Use strong passwords .

Don't use words that are found in English or Spanish dictionaries. Crack will get them every time. Preferably have symbols in it e.g. \$%^&* and Numbers. You might use

an easy password for non critical sites and load it for the Bank Account.

AND Protect your passwords.

Step 6

Beware of uncertain web links

Don't download free programs that you have not checked out thoroughly. You may well be getting more than you want..

Step 7

Be cautious in using peer-to-peer file sharing.

Like freeware that is not checked out you may be getting more than you want

Step 8

Turn your computer off when not in use

Along with this be sure that the " Wake on Lan "setting in your CMOS setup is turned OFF.

Step 9

Approach e-mail attachments with care.

Just clicking on them may get your machine infected and your anti virus ware will not help. The reason is that Anti malware will not protect against install that you initiate in many cases.

STEP 10

Be aware of transfers via portable

device

Viruses or spyware can infect your computer just as easily from a flash drive, mp3 player, or PDA as from an e-mail. A safer way to transfer: ask for an e-mailed file instead and scan it for viruses before opening.

Step 11

Guard personal information

Scams by e-mail and phone may try to steal your social security number, passwords, and other personal information. These cons lead you to phony Web sites indistinguishable from legitimate ones. Remember, a legitimate company will solicit for your information.

Sites such as eBay, PayPal, and most online banking sites have systems in place to help you guard against these scams. Find out what is being done to protect your information.

Step 12

Be aware of suspicious IM messages

Viruses transmitted via IM are on the rise. Similar to e-mail, IM viruses can replicate buddy lists and send attachments or disguised links that send you to an infected site. Be careful to avoid IM message links and attachments unless you are sure of their contents.

Step 13

Keep your operating system se-