Getting Rid of Crap

Ready

- What OS?
- Is there a recent backup?
- Is there a system restore point?
- Is ANYTHING working?
    - Can I plug in a USB stick?
    - Can I use a CD/DVD?
    - Can I connect to the Internet?
- Am I actually capable of fixing this?

Set

- Make some notes or look at your check sheet or both…
- Keep doing that, so you know where you are!
- Advise client of what you're doing and how long you think it might take. Be as non-technical as you can. ("I am going to scan so that we can find all the malware and try to remove it. You have a fast/slow system with lots/not much RAM, so this will take at least……")

GO!

- Retrieve the data!
- If you can clean out the temp files before you scan, go for it. But don't delete the System Restore point yet!
- Run antispyware tools if you can, and save the logs!
- Keep running things till you're sure you're clean
- Reboot as many times as necessary to satisfy yourself and your client that you can
- Flush System Restore
- Set a Restore point

Follow up

- Check the startup to see if anything looks wrong and disable what seems sensible
- Can you connect to the Internet?
- Is the email working?
- Clean the temp files
- Check processes and services looking for anything abnormal
- Check the hosts file
- Check for BHOs, bad toolbars, ActiveX and kill as necessary

- Check to see if your right-click (context menu/shellex) is working, because sometimes cleaning out crap kills you. Use ShellExView from Nirsoft to get yourself out of trouble
- Make sure the Antivirus is up-to-date and working
- Use secunia.com online inspector to check update status on windows, flash, java, etc
- Do something with that data
    - Virus/malware scan + restore?
    - Erase from your drive?

And if time permits…

- Look for ways to prevent this problem in the future
    - Can I uninstall this stupid Incredimail?
    - Install Firefox
    - Install the WOT add-on for IE and Firefox
    - Teach them what warning signs are (or refer them to my column!)

Finally…

- Is there anything else I can do for you today?
- Get the customer's email address
- Secure future business
    - Set up a backup routine?
    - Periodic updates and maintenance?
    - Help uninstall/cleanup/speed up?
    - Whatever…
- Collect the money!
- Give them two business cards, and "the pitch"