Recovering from an Attack

"Hope for the best but prepare for the worst."

Despite the precautions, you may be faced with putting out a fire.

This tutorial will give you a check list of things to do if you get infected by a virus.

DISCONNECT

Immediately disconnect your computer from the network or Internet.

By disconnecting from your network you prevent the virus from spreading to other computers in your network. By disconnecting from the Internet, you stop the attacker from accessing your computer or the files on your computer.

IDENTIFY

Identify the virus.

Tell your anti-virus (AV) software to scan your entire hard drive plus all removable devices that may have infected your computer. If your virus scanner can do a boot scan, have your AV software scan the computer before it boots to the operating system - this helps discover really bad root kits that hide in the operating system.

If your AV software does not detect the virus, then you may have to reconnect to the Internet and access an online service that will scan your computer.

Click on the image or link below to check out the service that Symantec provides.

http://security.symantec.com

DISINFECT

Disinfect your computer - kill the virus!

If you get this far you are doing good. All you need to do is kill the virus. This may not be easy. Have your AV software either remove the virus or quarantine the virus. If your AV software could not detect the virus, then use an online scanner/removal tool such as the Microsoft Windows Malicious Software Removal Tool.

Click on the image or link below to access the Malicious Software Removal Tool.

http://www.microsoft.com/security/malwareremove/default.mspx

RECHECK

Once the virus is removed, scan the computer again for any more signs of the virus. Since your original AV software betrayed you, you may want to use another brand of AV software (after removing the first) or use an online service as mentioned before.

REINSTALL

If all else fails, you may have to rebuild your operating system, reinstall your applications and restore your data from backup. You may possibly get by with simply restoring your entire computer from backup, but you risk restoring the virus as well.

ANALYZE

So that you do not lose anymore downtime, which is sometimes the most expensive part of being infected with a virus, you need to brainstorm on how you can prevent this from happening again.

1. Check the validity and age of your virus signature files. Are you scanning everything?
2. Make sure your operating system is up-to-date (with patches and service packs).
3. Check your email trash or emails that were opened for suspicious emails - but do so on a sacrificial computer.
4. Review your security policies and procedures.