DO’S AND DON’TS FOR INTERNET USE

NEVER

-visit websites you have never heard of before. if you haven't heard of it, there's probably a good reason.
-click on flashy advertisements, such as those for games or "free" anything.
-type "free" ANYTHING in google searches. 95% of evil sites purport to have something available for FREE. just search for what you are searching for. if it is available for free, it will be one of the first few matches.
-trust those talking ads that Congratulate you for being a "winner". they just want to try to convince you to click on the picture.
-follow a link that a random stranger gives you, especially if you don't recognize the site.
-Follow a link in an email that is from a friend, unless you know where it goes.
-install Flash Player from ANY SITE other than Adobe.com
-install something just because a website tells you it is necessary. unless you REALLY know the site and trust it, and even then, i would ask an "adult" :)
-click on a link that tells you that you need a codec to play a video. Flash Player should be all you need. and maybe CCCP.
-trust a "friend" who wants you to follow a link, but doesn't tell you much info about where it leads. always google it first, and if nothing definitive comes up, avoid it.
-click on that sexy girl (or guy). only bad things await you, not more sexy people...
-use easy-to-guess Answers for your Security Questions. if it is easy for YOU, it will be even easier for someone who knows you.
-assume that a website is secure just because lots of people use it. Facebook and MySpace are perfect examples of this. anyone can put whatever they want on their websites, including malicious software and trojans.

ALWAYS

-close Internet Explorer if a site keeps redirecting you over and over repeatedly.
-close Internet Explorer if a site pops up with a "virus" or trojan warning, and it does NOT mention YOUR AntiVirus software by name.
-know the name of your AntiVirus program, and what it's icon looks like.
-keep your AntiVirus up-to-date. it should have an icon down by the time. check it regularly for any problems.
-log out of online banking sites (including PayPal) when done using them.
-keep your passwords different from your password for your banking institution.
-keep your passwords safe somewhere in case you forget them ;)
-keep hard copies of any "vital" documents.
-check for "https" in the address bar before entering ANY information that you don't want EVERYONE to have. hackers lurk on unsecured web pages, just waiting for you to enter your credit card info...
-use a HOSTS file to help eliminate ads (especially the malicious ones):
http://winhelp2002.mvps.org/hosts.htm
-use pseudonyms whenever possible (as long as it is not for official business). the more people know about you, the more they can do to you if they are malicious-minded. there's no reason for people to get your personal info unless you are shopping and having a package sent to you.
-Go to Adobe’s or Java’s websites if you need the latest Flash Player or Java Runtime:
adobe.com
java.com