



Why a Monthly Program?

#1 – It is your goal and ours to keep your systems running as fast and efficiently as possible. This allows you and your colleagues/employees to be more productive during the workday.

#2 – Regular on-site monitoring of your pcs and server(s) will enable BMB to spot and resolve many potential problems before they turn into major issues. This reduces the chance of system failures, server crashes and other critical network problems.

#3 – BMB can regularly address outstanding issues that have accumulated over the past month.

#4 – BMB can better safeguard your systems against spyware, viruses, spam, and slow-downs by ensuring you've got up-to-date protective programs in place.

#5 – Ultimately, preventative maintenance is a better use of your IT budget verses reactive maintenance as it drives network efficiency and protection, minimizes system and employee downtime, and reduces peripheral costs your company would otherwise incur (such as travel costs).

What is Spyware and why is it so dangerous?

Spyware is software that is installed on a user's computer without his/her knowledge, for the purpose of gathering information on that user and delivering it to a third party. It is a daily nuisance, a financial drain, and a serious security risk for businesses (and individuals).

Spyware has a significant negative effect on network performance. Spyware infesting a network uses valuable bandwidth when transmitting data – your data – back to its maker. It also consumes large amounts of memory – thus drastically degrading computer performance or even causing crashes. Spyware transmits data about users' surfing habits to unauthorized third parties. Users' habits and preferences are analyzed and new content is sent back to the ad bank. The more that Spyware infects your computer or network, the more you pay.

Spyware is created purely for financial gain. It can monitor (and steal) every key stroke a user types, including passwords, account numbers (including bank account information), emails, social security numbers, esoteric company information, customer data, and other vital business activities. It then relays this information back to its creators, who use it for targeted advertising (spam, pop-ups) or, worse; fraud, identity theft or other illegal activities.

Almost 80% of all enterprise computers (i.e. network computers) in the U.S. are infected with Spyware at any given time. The estimated cost of each infected workstation is \$265, based on IT services, computer and employee downtime, and re-imaging.