

What If... Your ISP Could Offer a *SECURE* Internet Connection?

How much would you pay for it?

By Brent Rowe, *NC State '99*



The total cost of cyber security breaches and associated losses is estimated to be over \$1 trillion every year. This includes a variety of attacks and breaches, including ID theft, theft of company information, and attacks aimed at slowing or shutting down a company's public web site or internal network. Over \$100 billion is spent every year on cyber security products and services, with consumers spending approximately \$8 billion for home security software, hardware, and subscriptions. And still, the total cost of security prevention and losses continues to increase each year as the Internet becomes more entrenched in our daily lives.

You yourself may have been the victim of identity theft. Or your computer may currently be used to wage attacks on other computers. Remember that web site you went to that looked a little strange? It could have been a phishing site which automatically downloaded software on your computer so that a cyber criminal can now send e-mail or other Internet traffic from your computer, thus helping to hide their location and identify. Even if the hacker doesn't steal any of your information, your computer performance could be much slower, and one day an FBI agent might come knocking on your door asking why you've been sending out so much spam (side note: an FBI agent was knocking on my door recently, but for more benign purposes.). Either way, you're losing time or money.

What if your Internet Service Provider (ISP) was able to offer you more security? The technology exists for ISPs, both cable and DSL-based services, to conduct a variety of scans on the networks they manage and detect malicious activity. They could also provide antivirus software at a lower cost than you probably pay currently. And if they detect that you may have been "compromised," they could let you know and help you clean up your computer. More generally, ISPs are in a place to provide better security to home Internet users for a much lower per customer cost than is currently being spent on software fees, security subscription fees, losses from fraud, etc. ISPs, however, are hesitant.

Legal concerns top their list. Although ISPs can scan traffic across their networks and look for general patterns without "looking inside" your traffic, identifying malicious home Internet users' traffic would likely cause some consumers to raise privacy concerns. Further, ISPs fear that once they state "we are now working to secure your connection", even if they say that they cannot provide perfect protection, they will be sued any time one of their customers is successfully attacked.

Possibly more importantly, ISPs are not convinced that they could make money by offering new services, which would be very costly to implement. They worry that businesses and consumers, like you, would not be willing to pay enough to justify their investment. Past research has shown that home users are often completely unaware that their computers have been breached, and as such, they are often not willing to pay much to secure their computers. The result is that there are literally tens of millions of hijacked U.S. computers, called "bots," that are used by hackers to send spam and attack other home users or companies. So, not only might a hacker be stealing your information and slowing down your computer, they might also be attacking others from your computer.

So, now that you know that *you're* probably insecure and that *your* computer is probably being used to attack other folks like me, how much would you be willing to pay your ISP to essentially guarantee your security? Would you pay \$10 per month? Maybe even \$15?

The Institute of Homeland Security Solutions recently provided me with funding to study this issue. I'm trying to estimate out how much home Internet users would be willing to pay ISPs to increase their security, and what types of security solutions and marketing strategies most interest customers. I'm also studying how much it will cost ISPs to provide various types of security. Are certain solutions more cost effective than others?

As part of this study, we're conducting interviews with ISPs, and developing a survey to help consumers estimate the value they would put on additional security, as well as what educational and marketing campaigns might provide consumers with the necessary information to make the most cost effective decision.

And then comes the tricky part. If consumers and businesses are not willing to pay enough to cover the costs that ISPs would have to incur, should the government step in to force them to do so? Or should the government help subsidize ISPs' investments and security activities so that all Internet users are more secure? These questions remain unanswered.

Brent Rowe is an Economist at RTI International. He recently co-authored a book entitled Cyber Security: Economic Strategies and Public Policy Alternatives that is being used in a variety of university technology policy courses.