Institute for Homeland Security Solutions
Applied research • Focused results

Economic Analysis of ISP Provided Cyber Security Solutions

June 2011

Authors

Brent Rowe, RTI International

Dallas Wood, RTI International

Doug Reeves, North Carolina State University

Fern Braun, RTI International

Table of Contents

List of Figures

List of Tables

1. Introduction

Cyber attacks resulting from the current insufficient state of Internet security have led to large financial losses for businesses, governments, and individuals. Home users, who often are not well informed on the consequences of cyber threats and therefore are poorly prepared to prevent an attack, are a large factor in this problem. Internet Service Providers (ISPs) such as Comcast and AT&T have the potential to play an important role in improving security among home users, and some ISPs are starting to take action. Not only do ISPs have the ability to monitor and control a user's Internet access—including identifying threats originating from or aimed at a particular use or set of users—they have the opportunity to provide the user with security software and educate him or her on the importance of cyber security.

Most medium and large businesses employ teams of information technology (IT) personnel charged with ensuring that up-to-date cyber security infrastructure is in place, staying apprised of current security threats, and repairing infected machines. In stark contrast, home Internet users are often highly vulnerable to cyber attacks, but rarely have any security provided to them by default (without having to purchase a specific security product or service). As such, estimates suggest that between 10 and 35 percent of home users (Wilson, 2011) may already be part of a botnet—a network of compromised computers used to distribute spam, attack corporate networks or websites and spread viruses; home Internet users therefore represent a weak link in national cyber security.

This research project examined the potential roles of ISPs in providing cyber security from an economics perspective. The research consists of three main parts—an assessment of the potential role of ISPs from a technical, logistical, and legal perspective; an analysis of the supply of ISP-provided security services and the associated costs and prices; and finally, an estimate of the demand for ISP-provided security services by home Internet users. We conducted a variety of interviews with experts and industry members to understand the technical, legal, and cost factors and conducted a review of the literature and available pricing information on the Internet to discern the current supply and pricing structures. For the demand assessment, we conducted a survey of 3,635 home Internet users which focused on a set of stated preference choice experiments to help us estimate how much home Internet users were willing to pay for security and the relative importance of both potential benefits of additional security (e.g., decreased threat of identity theft) and the nonmonetary costs that may be incurred (e.g., ISPs might limit a user's Internet access if they appear to be infected).

Our findings support the notion that consumers are willing to pay an additional premium to an ISP for various security services and that they are willing to accept ISP-required security training and suspensions of their Internet service when malware is detected on their computer in exchange for reductions in the risk of their computer slowing down or crashing, the risk that their identity being stolen, or the risk that others will be impacted by their in-security. For example, on average, consumers indicated that they would pay approximately $3 per month to protect against botnets and other viruses that could be used to attack other individuals and business and about $6.50 per month to protect themselves from identify theft.

2. The Role of ISPs in Cyber Security: A Review of Business Considerations and Legal Issues

ISPs are key participants in an ongoing public debate over securing Internet activities, particularly in the case of home users. Many experts think that ISPs are in the position to help secure Internet transactions in a very cost-effective way. The proper role of ISPs, however, depends on a variety of factors including how security would fit into ISPs' business model (i.e., what are the costs and legal issued involved in providing security to customers, how much are customers willing to pay, and are there any benefits to ISPs) and how ISPs' involvement in security would affect home Internet users, business Internet users, and other companies providing security products and services. Text box 1 provides a summary of the primary characteristics of ISPs' current business model. The remainder of this section focuses on ISPs' role in providing security.

Because ISPs control a user's Internet access, they possess the ability to identify users who appear to be experiencing or causing security threats and inform them of the problem, limit their access (by either slowing their access speed or restricting their activities, often referred to as "quarantining"), or remove them from the network. Because many ISPs already monitor Internet traffic, such actions would not be significantly beyond their current technical capabilities.

However, more than threat analysis is needed. Upon identifying suspicious activity on a customer's computer, an ISP can take several actions (often in combination):

- notify the customer (by e-mail, phone, postal mail, instant message, text message, or by web browser notification);
- direct the user to helpful online information;
- reduce the user's Internet upload speeds;
- restrict the user's access to certain types of Internet activities; or
- require the user to demonstrate compliance with requirements, including potentially removing the infected software.

Text Box 1. A Brief Industry Profile of ISPs

ISPs' primary source of income is the provisioning of access to the Internet, which carries data and in recent years, a significant amount of voice traffic. The top five U.S. ISPs currently provide more than 50 percent of broadband Internet service in the United States, broken out as follows: AT&T (15.4%), Comcast (15.3%), Road Runner (9.0%), Verizon (8.8%), and America Online (7.7%). Although none of these ISPs has a dominant position nationally, in specific regions, the story is mixed. ISPs charge different prices based primarily on the connection speed that the customer receives. Text Box Table 1 shows mean and median prices for Internet access services.[1]

In addition to providing users with Internet access, many ISPs also offer services such as web hosting, web page design, consulting services, and remote data storage. However, these other services typically comprise a small share of the total revenue of ISP firms.

Text Box Table 1. 2009 Mean and Median Prices for Broadband and Dial-up Services

	Mean ($/month)	Median ($/month)
All Internet Users	$37.60	$35
Broadband	$39.00	$38
Dial-up	$26.60	$20
By connection type		
DSL	$33.70	$30
Cable	$43.20	$40
Other high-speed	$37.50	$35

Source: Pew Research Center, 2009.

According to the U.S. Census Bureau, which collects economic data for various industries as part of its economic census every 5 years, in 2007 firms identified as being in the Wired Telecommunications Carriers industry (classified under NAICS 717110, which included ISPs) obtained approximately 10.9 percent of their revenue (approximately $31.8 billion) from the sale of Internet access services. The remaining 90 percent of revenue (approximately $259.1 billion) is obtained from multichannel programming distribution (22.2%), local telephone services (19.8%), and other services (U.S. Census Bureau, 2010).

ISPs can also play a preventive role in cyber security. Many ISPs provide antivirus, firewall, or antimalware software to customers either free (i.e., included in the purchase of their Internet plan) or for an additional fee, which is often a lower price than individuals purchasing directly from companies such as McAfee or Norton. In this way, ISPs are helping to incentivize more home Internet users to use security software—they are presenting this option to customers who may not have thought to buy security software on their own and offering them a lower price than they could fine otherwise. Further, ISPs are validating the quality of these programs. Some home Internet users may not know which security products to trust, and by

[1] Note that these estimates are based on self-reported data that were collected by the Pew Research Center during its 2009 Home Broadband Adoption study. These data were intended to exclude any other services that may have been bundled with a person's monthly bill, such as cable or telephone service.

offering specific security packages, ISPs are implicitly approving certain products and services.[2]

In addition, because home users must initially interact with their ISP to gain access to the Internet, the ISP is in a position to educate the user on cyber security threats by, for example, directing users to an in-house or external website with material explaining different types of security threats and ways to prevent attacks. Most ISPs provide educational information on their websites, describing security advice (e.g., "you should install antivirus software") and cautionary information (e.g., "do not click on attachments or links in e-mails from people you do not know") for home Internet users. However, ISPs are resistant to *force* education on their customers for fear they will switch providers.

At the most extreme, some ISPs offer a remote remediation service, particularly for customers subscribing to more expensive plans or paying a monthly support fee. ISPs may provide services such as:

- Backing up files
- Downloading patches and updates
- Configuring the computer, and applications software, to auto-update
- Information about contacting law enforcement

Although ISPs could play all of these roles, wide disagreement exists on the proper role of ISPs among and within groups of researchers, policy makers, and companies of various types. The Federal Communications Commission (FCC) and the legal system have recently begun to play a large role in the debate over what ISPs can and should be able to do in terms of treating customers differently and managing their network, including security-related activities. In 2008, Comcast began slowing user access to a file-sharing site. The FCC attempted to enforce net neutrality—generally defined to mean not discriminating against Internet traffic based on the content—by ordering that Comcast cease such activities. Comcast appealed the sanction, and in 2010 the U.S. Court of Appeals ruled unanimously in favor of Comcast, stating that the FCC does not have the power to halt this practice (NY Times, 2010).

The Comcast case demonstrated that the legal restrictions on ISPs are not currently well defined. It is unclear how the FCC will be able to regulate the Internet in the future. Broadband may become a highly regulated utility like the telephone service industry or, if the current state of policy stands, the FCC may be unable to enforce its net neutrality policy. Text box 2

[2] If consumers are unhappy with their security product, they may blame their ISP, since their ISP suggested the product. Further, if ISPs suggest the security software that makes their users' computer the most secure (as compared to other software), the ISPs benefit by having a "cleaner" network. Thus, for both reasons, it should be in ISPs' best interest to approve a high-quality product. However, if one security company provides a better deal to the ISP (a kickback) or if it is too difficult for the ISP to tell which security product is better or worse, then the approval may not be as useful or beneficial to home Internet users.

provides additional discussion of the legal issues surrounding the role of ISPs in providing security.

In terms of ISPs' role in providing security to home Internet users, the FCC has so far only provided guidance to ISPs. A working group in FCC's Communications Security, Reliability and Interoperability Council released a network protection best practices document for ISPs in December 2010 (CSRIC 2010). The paper includes 24 best practices, divided into the categories of prevention, detection, notification, mitigation, and privacy considerations, and emphasizes the importance of timely detection and notification, security software provision, and improved end-user education. The group recommends that ISPs quarantine infected customers only after multiple contact attempts, except in extreme cases.

The U.S. policy community has also tried to address the proper role of ISPs. In 2009, the National Information Technology Research and Development (NITRD) Program held a National Cyber Leap Year Summit, which convened a large group of cyber security experts for a multiday brainstorming event in Washington, DC. The event resulted in two reports describing the results of the discussions. The "National Cyber Leap Year Summit Co-Chairs' Report" (2009) offered the following suggestion:

> [P]olicies [should be considered that] empower ISPs… to take action to stop cyber-criminal activities – while also considering their accountability for failures to address clearly abusive behaviors. A pilot government program could be enacted to reward ISPs who discover, repair, and clean computers infected with crimeware – in order to realign the incentives of ISPs to keep their networks from harboring crimeware. The results of the pilot could be used to evaluate whether such interventions might be helpful on a large scale" (p. 29).

Text Box 2. Legal Restrictions on ISPs

ISPs operate within the scope of regulations and laws at both the state and federal levels. In addition, ISPs cooperatively develop standards and share information through industry associations and other organizations such as the Internet Security Alliance and the Federation of ISPs in America. An individual ISP may be restricted from conducting certain activities, required to do others, and have agreed to do others.

In the United States, federal law speaks to the role of ISPs in a variety of ways:

- The Federal Wiretap Act of 1968 prevents ISPs from intercepting the contents (such as payload and application data) of communications except for purposes of protecting the network (Title III of the Omnibus Crime Control and Safe Streets Act).
- The Stored Communications Act of 1986 (Title II of the Electronic Communications Privacy Act [ECPA]) prevents ISPs from disclosing information about communications outside their organization.
- The Pen Register Act of 1986 (Title III of the ECPA) restricts what information ISPs can collect about "calls" and how such information can be used.
- The USA PATRIOT Act of 2001 (Title II: Enhanced Surveillance Procedures) required that ISPs give law enforcement agents access to their networks without a warrant for the purpose of tracking hackers. (Prior to the Act, ISPs were specifically forbidden from granting access without customer permission or a warrant.)

The legal requirements of and restrictions on ISPs regarding their ability to monitor users, to alter service provisioning, and to store and share data are both complex and not well established.

In the European Union, a report commissioned by the European Network and Information Security Agency (ENISA) (Anderson et al., 2008), recommended that the European Union "introduce a statutory scale of damages against ISPs that do not respond promptly to requests for the removal of compromised machines, coupled with a right for users to have disconnected machines reconnected if they assume full liability" (p. 4). The authors also suggested that ENISA collect and publish data on "bad traffic" coming out of European ISPs, as a way to motivate ISPs into action.

Finally, the Internet Engineering Task Force (IETF), a nonregulatory group that develops voluntary consensus Internet standards and recommendations for Internet management policies and procedures, published an Internet Draft[3] titled "Recommendations for the Remediation of Bots in ISP Networks," authored by employees of Comcast (Livingston et al., 2009). This document describes why and how ISPs can mitigate the effects of bots, including suggestions for how ISPs can identify and remediate computers that are infected with bot software. Detection methods that are mentioned include the following:

- Analysis of application traffic flows using, for instance, netflow statistics
- Scanning for unpatched PCs
- Monitoring of DNS query patterns
- Operation, monitoring, and analysis of honeynets
- Complaints or warnings of suspicious behavior by other ISPs and by security alert organizations (e.g., US-CERT)
- Feedback from users

Existing ISP Policies Related to Security

All ISPs create a variety of policies and procedures which structure how and when ISPs can monitor their customers' Internet activities and how and when they can react to such. The impact of these policies and procedures on Internet users are detailed in ISPs' Acceptable Use Policies (AUPs). A list of standard provisions included in U.S. ISPs' AUPs are shown in Text Box 3.

Text Box 3. ISP Acceptable Use Policies: Standard ISP "Rights"

U.S. ISPs all post acceptable use policies, or service agreements, for subscribers. These typically enumerate prohibited activities, the rights of the ISP, and procedures for resolving grievances. The rights of the ISP that are generally enumerated include:

- ISP may monitor transmissions
- ISP may preserve or disclose content
- ISP may deny or cease service to subscriber
- ISP may require customer to cease excessive use or employ corrective actions
- ISP has right to submit to dispute resolution/ binding arbitration
- ISP may refer abuses for prosecution
- Standard disclaimers and limitations of liability

Some ISPs report using these rights to secure their customers and decrease "bad traffic" on their networks. For example, Comcast has

[3] IETF Internet Drafts are "works in progress" and are not standards; however, often IETF documents are adopted as pseudo-standards.

stated that they may remove customers with security problems from the network regardless of knowledge or intent (Comcast, 2011). However, most ISPs note in AUPs that they “reserve the right” to remove customers from the network in the event that activity from their computer is disrupting the network. It is unclear how many ISPs regularly take advantage of this ability. However, the rights listed above clearly demonstrate that ISPs are positioned to play a critical role in improving cyber security.

ISPs also regularly list **prohibited user activities** in their AUPs. The following is a list of common prohibited activities:

- Illegal activities
- Harm to minors, including child pornography
- Theft of intellectual property
- Theft, abuse, or exceeding limits of service
- Unauthorized access to other computers or networks
- Transmitting threats
- Giving offense
- Spamming
- Disruption of service
- Failure to exercise diligence, including failure to adopt adequate security measures to prevent unauthorized use of the account

ISPs’ AUPs also suggest that violation of these policies could result in **punitive action by the ISP**. Sample sanctions mentioned in one or more AUPs include the following:

- Suspension or termination of account
- Making website unavailable
- De-prioritization of traffic
- Warnings
- Blocking of access to websites or web pages
- Billing for administrative/operations costs of prohibited activities
- Legal action
- Blocking/altering of prohibited outgoing e-mail, spam, or messages
- Blocking/altering incoming spam
- Blocking/altering transmission of viruses or harmful content
- Requiring customer to upgrade to higher service level
- A fee of $500 plus $1 per message and $50 per complaint for spamming

It is difficult to ascertain how many ISPs regularly take disciplinary action against customers. ISPs may clarify these rights—e.g., seeking action against customers with clear intent to conduct a malicious or illegal activity such as spamming—rather than a user whose computer was used to distribute spam by an attacker because of insufficient security measures; however, many such ISP polices are vague and actual ISP actions are not widely known or publicized.

3. Supply Assessment of ISP-based Cyber Security Solutions

As described above, there are many ways that ISPs can help secure home Internet users; however, in reality, ISPs often play very limited roles. To analyze the roles that ISPs are currently playing in providing security services to customers, we examined Internet and security packages offered by the leading 23 ISPs in the United States as determined by market share (ISP Planet, 2008). Appendix A provides a list of these ISPs and a summary of the data used to calculate the costs in this analysis.

Many ISPs provide educational resources to their customers. Training or educating users about security generally and, more specifically, how to defend their computers are relatively low-cost investments but have potentially large benefits to home users and ISPs, if effective. An examination of ISP websites revealed that many ISPs link to third-party information, such as Microsoft pages about Windows security or government websites. Some, such as Earthlink,[4] Verizon,[5] and Comcast[6] provide their own security information or white papers.

Figure 1 displays the percentage of ISPs examined which report on their websites or in their AUPs that they take various security measures. Eight-seven percent of large ISPs do offer some security services or security software to their home Internet customers. Sometimes these security software or services are bundled with packages, in particular those that include higher connection speeds, and other times various security services are available for purchase for additional cost. Fifty-two percent of ISPs offer some type of technical support which could be used to fix security problems, ranging from services which simply direct customers to online help guides to remote virus removal, equipment repair, and home visit services. Several ISPs charge an additional monthly fee (ranging from $2 to $15) for improved technical support, while others include these services at no additional charge with more expensive (higher download speed) plans. We found explicit statements by 13 percent of ISPs stating that they cut off customers with security issues until the issues are resolved. ISPs seem to stop short of controlling or managing the individual computer, but most are very aware of the traffic being transmitted across their network by their users and some act on this knowledge.[7] Because ISPs are not required to report whether, for example, they restrict or cut off customers with security issues, the actual percentage may be higher. Unfortunately, this level of specificity was not possible.

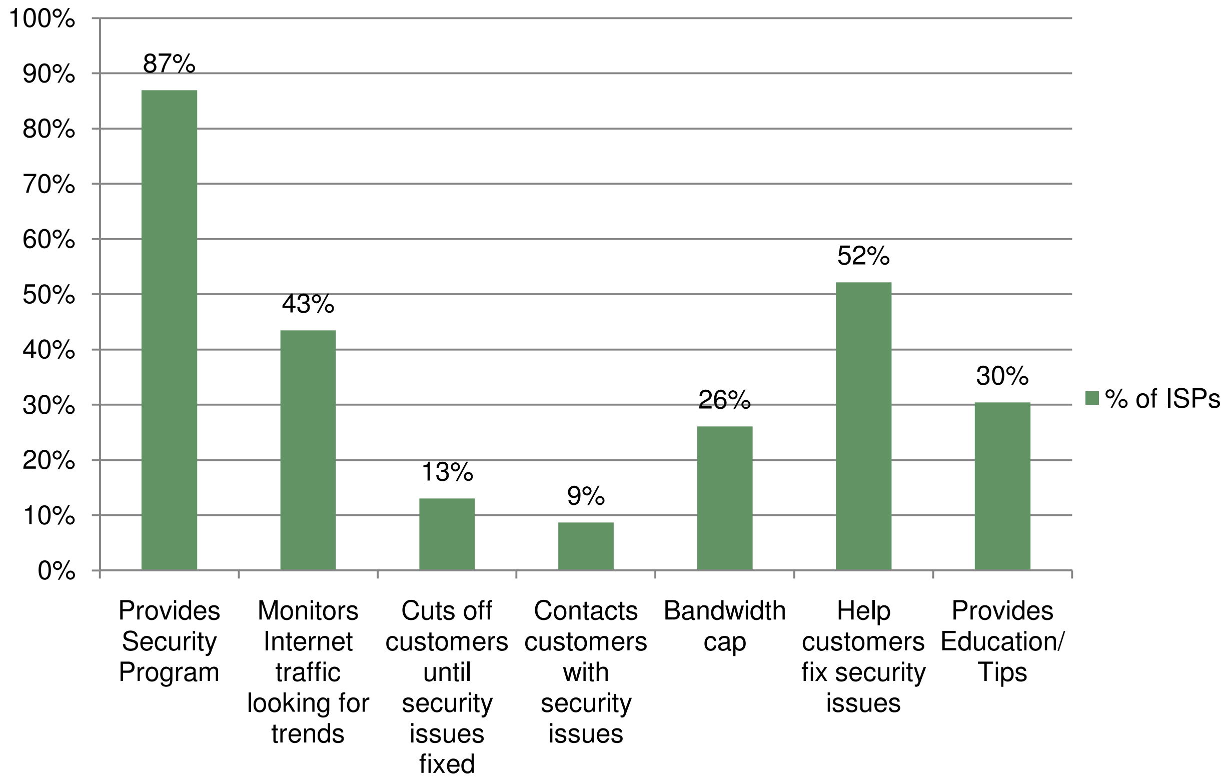
[4] http://www.earthlinksecurity.com/home.html

[5] http://surround.verizon.com/shop/utilities/internetsecuritysuite.aspx

[6] http://security.comcast.net/

[7] In our interviews, most ISPs indicated that they monitor traffic, at least for the purpose of protecting the network. However, all expressed reluctance to examining the contents of packets, primarily based on the technical difficulties of deep packet inspection and unwillingness to antagonize subscribers. No ISPs mentioned legal issues as the source of their reluctance.

Figure 1. Percent of ISPs Reporting to Take Security Measures



We sought to determine the amount that ISPs are currently charging customers for security, to develop an upper-bound estimate of the per month cost to ISPs of providing cyber security to a large number of customers. If the price of each individual security feature, such as antispam or antivirus, could be separated out, then the cost of providing specific features could be weighed against their respective benefits.

To analyze the cost to ISPs of providing security services to customers, we examined Internet and security packages offered by the leading 23 ISPs in the United States. Of the 87 packages examined, 68 were DSL or cable broadband services. We excluded dial-up Internet service in our analysis as they are much less of a target for hackers based on the fact that they are not online as often (broadband users are often online 24 hours a day 7 days a week) and their upload and download speeds are often significantly slower. One additional ISP and its three plans were also excluded from the analysis because they are only offered to a small, remote user base at a price well above that charged in a typical market. Figures 2 and 3 show how the sample was developed, based on the number of ISPs we looked at (23) and the specific number of packages examined (65).

Figure 2. Cost Analysis Sample Characteristics (ISPs)

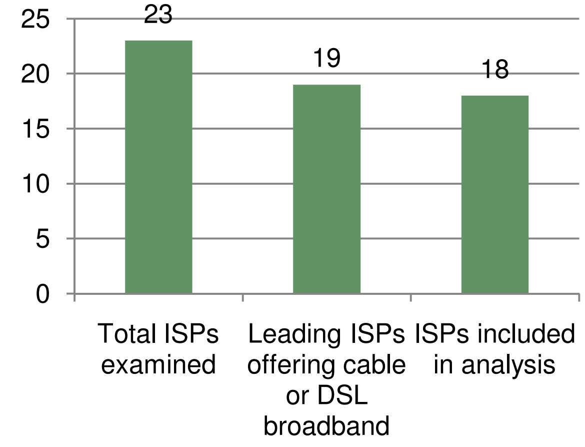
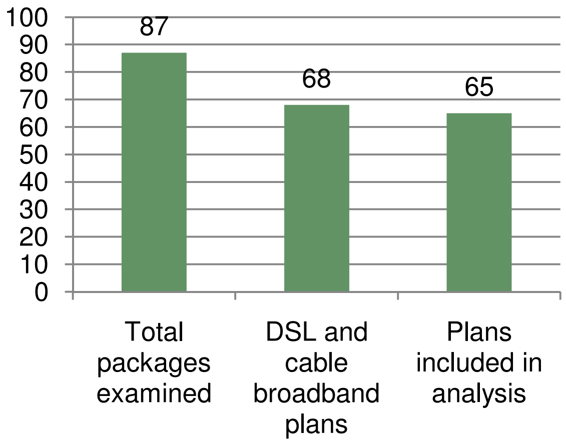


Figure 3. Cost Analysis Sample Characteristics (Plans)



The average monthly plan price was $50 or $18 per Mbps, not including additional optional security costs. Table 1 summarizes the price data.

Table 1. Internet Plan Prices and Speed: Summary Statistics

	Monthly Cost	Cost/Mbps*
Mean	$50.12	$17.59
Median	$42.00	$13.33
Max	$202.00	$69.00
Min	$20.00	$2.00

* The summary statistics in the Cost/Mbps column is not related to the Monthly Cost column. Mean, median, max, and min values were calculated for both separately.

Ninety-seven percent of these broadband plans offer some type of security service. Of these plans, 49 percent charge a separate monthly fee for security. Monthly fees range from $2 to $7 with a mean cost of $4.34. Several of the companies examined offer multiple security options for each download speed, giving customers the option of using a free or low-cost antivirus service or paying extra for a more comprehensive security suite (often included in higher download speed plans). Some plans offer security services through a well-known provider such as McAfee or Norton; others, such as Verizon, seem to develop their own security suite that they offer to customers.

Among plans with security included in the monthly rate, the average cost was $52.54, as compared to $47.47 for optional security packages (not including the optional security fee). Thus, ISPs appear to be charging customers an average of $5.07 for included security features and $4.34 (the mean monthly fee) for optional security programs, placing the average cost to consumers of security provided through their ISP at around $5 per month. Table 2 displays the price differences between these plans.

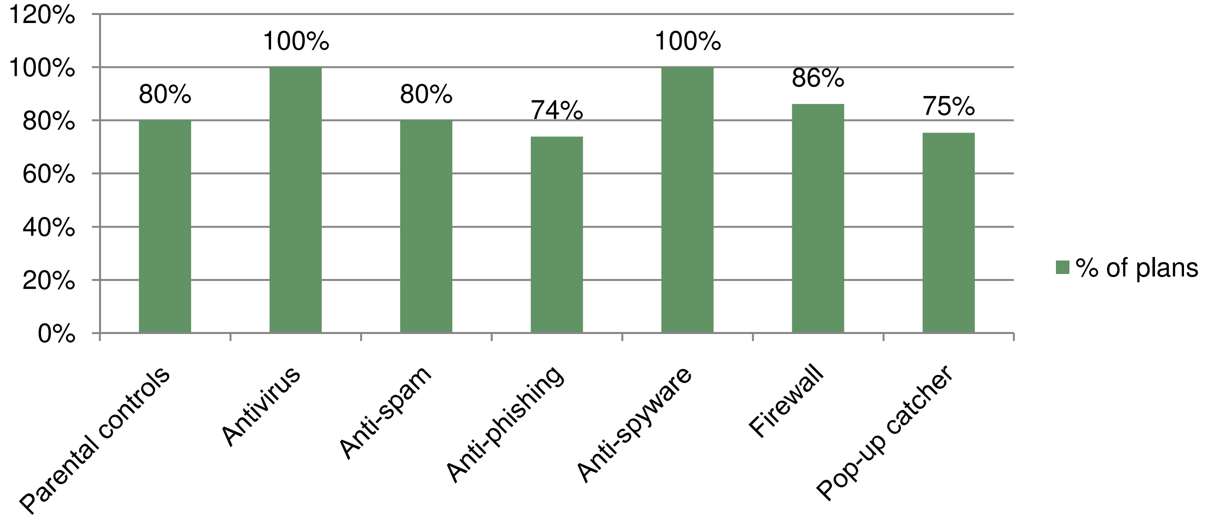
Table 2. Internet Plan Prices: Summary Statistics by Security Package Type

	Monthly Price—Security Included	Monthly Price—Security Optional (Fees Excluded)	Monthly Price—Security Optional (Fees Included)
Mean	$52.54	$47.47	$52.24
Median	$44.00	$40.00	$46.00
Max	$202.00	$105.00	$109.00
Min	$20.00	$20.00	$23.00

Figure 4 shows the breakdown of the portion of the ISPs that we looked at that offered various security software to their subscribers (either included or for a fee). We attempted to regress the data to estimate the price charged for each individual security feature. However, because of the limited number of plans offered and the large variety of features, there were not enough observations to produce significant and reportable results.

It should also be noted that some ISPs offer different rates at different locations. Because not all ISPs are available in all cities, location could not be held constant across all plans.

Figure 4. Percent of Internet Plans Studied that Offered (as Included or Optional) Specific Security Options



3.1 Cost Analysis of ISP-Based Security Options

As was expected, ISPs we spoke with were somewhat guarded about their operational and product and service cost structures. Looking at the prices they charge for various security-related products and services as was described above provides one picture of the likely costs they are incurring for related activities. In some cases, we were told that ISPs are losing money on their security-related products and services. Offering educational tips or antivirus software can result in a slight increase in profits or customer retention, or even reduce costs related to managing a network clogged with excessive spam. However, when ISPs take on larger roles—such as Internet monitoring or filtering or, most costly, engaging more directly with home Internet users (e.g., by offering telephone or in-person technical support)—their costs can increase dramatically. We have heard that in some cases, ISPs are losing money to increase customer retention or reduce government pressure for them to take on a larger role in securing their home Internet customers.

The data we collected on ISP prices suggest that certain security activities are likely more expensive for ISPs than others. Because most ISPs charge an additional fee for technical support that goes beyond minimal online or phone assistance, it is clear that this service is time-consuming and therefore expensive for ISPs to provide. Because antivirus and antispyware were included in all security packages, including many of those offered for free with low download speed plans costing only $20 per month, it can be assumed that these services come at a low cost to the ISP. Further, in an interview, one ISP we spoke with suggested that they it $1.00 per month for each of its customers who downloads a Norton security package through the ISP's website.

We also developed proxy cost estimates by talking with several organizations which were willing to share information about their security spending. In one case, we developed a total assessment of the spending per employee on IT security by a medium-sized firm, as a way to estimate the high-end costs that may be incurred by an ISP to secure its customers. In another case, we looked at how much a school system spends per student/staff on IT security. Relevant caveats are discussed below.

3.1.1 A Proxy Estimate of ISP-Security Costs: A Medium Business Cost Analysis

To develop an estimate of the cost of providing cyber security services to a large group of users (as ISPs might), we examined the costs incurred by the security team of a medium-sized business. This analysis provides a high-end proxy estimate of the costs which an ISP could incur to provide comprehensive security services to its customers.

The business studied has approximately 3,000 employees. The company incurs a variety of costs including labor, capital, and services aimed at both proactively preventing successful cyber security attacks and reducing the likely damages caused by such attacks and reactively addressing attacks that occur and minimizing the impact in real time. Table 3 provides an overview of the number of full-time employees (FTEs) and costs used for various purposes. As shown in the table, the company's IT department serves many of the same purposes that an ISP can. Some features, however, such as cutting off customers with security problems, were not applicable to the company. Costs were unknown for smaller items such as providing education and tips to employees.

Table 3. Security Costs for a Medium Business

	Labor		Capital		
ISP Security Activity Proxy	Number of FTEs	Total Annual Labor Costs ($)	Annualized Purchase Cost ($)	Annual Cost ($)	Total ($)
Provides security program*	11.75	$1,967,484	$41,733	$67,759	$2,076,976
Monitors Internet traffic looking for trends	1	$135,196	$0	$33,700	$168,896
Cuts off customers until security issues fixed	NA	NA	NA	NA	$0
Contacts customers with security issues	0**	$0	$0	$0	$0
Bandwidth cap	NA	NA	NA	NA	$0
Helps customers fix security issues	0.5	$49,101	$0	$0	$49,101
Provides education/ tips	0**	$0	$0	$0	$0
Other	0	$0	$13,333	$17,000	$30,333
Total IT Security FTEs	**17**	—	—	—	
Total IT Security FTEs / Per Staff	**0.006**	—	—	—	
Total Annual IT Security Costs	—	**$2,151,781**	**$55,067**	**$118,459**	**$2,325,306**
Total Annual IT Security Costs / Per Staff	—	**$717**	**$18**	**$39**	**$775**

* "Provides security program" is a catchall that was used to capture all security-related activities that did not cleanly fit into a category that an ISP security program might include.

** FTEs could not be separated out between security staff spending time on Helps customers fix security issues, Contacts customers with security issues, and Provides education/tips. All such FTEs were put in Helps customers fix security issues as the majority of staff time is assumed to be spent there.

The company studied employs approximately 17 IT professionals/FTEs for security purposes (although some staff are not working on IT security full time, so this number includes some aggregated partial FTEs). Labor costs were calculated using salary information and estimated time spent on security-specific tasks. The total cost of labor and capital was estimated at $2,325,306 per year. This yields an average cost of $775 per employee per year. As a monthly cost, this equals $64.58.

These figures are similar to those estimated by Gartner in a 2009 survey. Gartner found that firms categorized as “Professional Services” were spending an average of $836 per employee per year on security (Wheatman, 2010), or $69.67 per month.

However, no ISP is likely to provide security to its customers as robust as that provided by a business to its employees. If we remove the security costs most likely not to be incurred by an ISP for its customers—by removing the catchall category “Provides security program” which we assumed would be beyond services provided by an ISP—the costs decrease to $248,330 per year for all 3,000 employees or $82.78 per employee per year. As such, spending per month on ISP-like activities equals $6.90, which is very close to the costs estimated above based on ISP pricing estimates. However, this business also spent approximately $58 per month per employee on additional security features (e.g., firewalls and network level security analysis). As such, the potential for threats to individual employees was greatly reduced by these “network-level” security activities and policies.

3.1.2 A Proxy Estimate of ISP-Security Costs: A Nonprofit Educational Network

Additional security cost numbers were developed using data on the cost of web filtering services to K–12 schools. Price estimates were collected from five different companies offering security services to a state school system. Among the seven packages offered by the five companies, total prices per subscriber per year ranged from $4.08 to $13.80 with a median of $7.67 and a mean of $7.93.

These plans place the cost per customer per month much lower than the fees being charged by ISPs (about $.65 per month as compared to around $5 per month for ISPs). It should be noted, however, that the school system is mostly concerned with web filtering and the prices listed are therefore for plans with only basic malware protection (e.g., antivirus, antispyware). Thus, the specific features included may be different from those generally provided by ISPs. Further, these costs do not include any customer contact or remediation costs that may be needed once the web filtering software identifies a potential problem.

4. Demand Assessment

ISPs largely contend that home Internet users are not willing to pay for improvements in cyber security, and in fact, are often very reluctant to accept the costs associated with improving cyber security. As described above, to achieve increased cyber security, home Internet users may need to spend money and time on cyber security and may also be subject to having their Internet access restricted if their computer is perceived to be sending malicious traffic that may harm others.

This study sought to analyze this issue quantitatively. Specifically, we answered three research questions related to these issues:

1. How willing are broadband Internet users to accept the costs associated with obtaining additional cyber security from their Internet service provider? And what specific benefit attributes (associated with increased security) do they value most?
2. What is the most broadband Internet users would be willing to pay for hypothetical ISP security packages?
3. Can the amount Internet users are willing to pay for these hypothetical packages be influenced by information treatments designed to either make them (a) more concerned about cyber security threats (such as identity theft) or (b) more trusting of their ISP's ability to improve their (and other's) security?

This section summarizes the methods used to explore each of these questions and the results of our analysis.

4.2 Economic Framework and Methods for Quantitative Demand Assessment

The three research questions this study seeks to explore all regard how willing broadband Internet users are to accept the costs associated with ISP security packages and whether that willingness can be changes. To answer this question, we must investigate how the various costs and benefits of these ISP strategies contribute to an individual broadband user's utility. Based on a review of the cyber security literature, we can identify at least three primary costs to home users:

- Increases in the Cost of Internet Access
- Time Spent Complying with ISP Security Requirements
- Limits Placed on their Internet Access

and three types of benefits they would receive in exchange for accepting these costs:

- Improved Computer Performance
- Reduced Risk of Identity Theft
- Reduced Risk to Other Individuals and Business from your Insecurity

Although other costs and benefits could be considered in relation to ISP security strategies, we believe that these are the ones that would most concern broadband Internet users. Therefore, we can conceptualize the broadband user utility as a function that takes the form of:

$$U = f(F, T, A, P, S, O)$$

Where F is the additional fee ISPs charge broadband users for pursuing the security strategy, T is time users must spend complying with ISP security strategies, A is a measure of the user's ability to access the Internet (which can be impeded by some ISP security strategies), P is a measure of the performance of the user's computer (which can be reduced by the presence of malware on their machine), I is a measure of the risk of identity theft (which can be reduced by ISP security strategies), and O is a measure of the losses incurred by others due to an individual broadband user's lack of security. We hypothesize that increases in the cost of Internet access decrease personal utility ($\partial U/\partial F < 0$), increases in the time it takes to comply with ISP security requirements decrease personal utility ($\partial U/\partial T < 0$),improvements in a user's access to the Internet increase utility ($\partial U/\partial A > 0$), improvements in the performance of a user's computer increase utility ($\partial U/\partial P > 0$), improvements in computer performance increase utility ($\partial U/\partial S > 0$), increases in losses incurred by others reduce an individual user's utility ($\partial U/\partial O < 0$).

To operationalize this conceptual model, we used choice-based conjoint analysis to quantify the impact that policy attributes would have on an individual's utility. Choice-based conjoint analysis is a stated-preference survey method where survey respondents are asked to choose between hypothetical products or policies. Conjoint analysis has been extensively used by market researchers over the past 30 years to evaluate the market potential of new products and in creating pricing strategies (Orme, 2010). In recent years, conjoint analysis has also been increasingly used to value the net benefits of government health and environmental policies (Hensher, Rose, and Greene, 2005) and types of security policies (Smith & Mansfield, 2006). In the following sections, we describe how the survey used to conduct conjoint analysis in this study was developed and how it was administered. Evidence supporting the reliability of conjoint analysis for making credible estimates of purchasing decisions has also been obtained through field experiments (see List et al., 2006).

For the purposes of this study, we created conjoint choice task that required survey respondents to choose between ISP security packages that were differentiated by the costs they would impose on the respondent and the security benefits they would provide. In the following sections, we describe how the survey was developed and administered

4.2.1 Survey Development

Data for this study were collected through a survey instrument, the primary component of which was a set of seven forced-choice questions that included a no-choice alternative (an opton) follow-up question (see Figure 5 for an example). Each question described two hypothetical security packages that an ISP might offer broadband customers. After respondents selected which of the two hypothetical packages they most preferred, they were then asked if they would actually support their own ISP pursuing the package they selected. For the purposes of this study, we consider this choice task as thus being composed of three alternatives—Option A (if a person selected Option A and indicated he or she would support the ISP pursuing that option), Option B (if a person selected Option B and indicated he or she would support the ISP pursuing that option), and a third No Choice Alternative (if a person selected either Option A or B and indicated he or she would not support the ISP pursuing that option).

Figure 5. Example Choice Question

	Option A	Option B
ISP Strategies to Improve Security		
Adding a fee to your bill to provide security services to Internet subscribers	$4 per month	$7 per month
Requiring you and other Internet subscribers to comply with security requirements and training	0 hours per month	0 hours per month
Limiting Internet access for you or other subscribers who show signs of malicious or illegal activity	ISP can never limit your access to the Internet	ISP can never limit your access to the Internet
Cyber Security Outcomes		
Reduced risk of your computer slowing down or crashing	Greatly Reduced	Greatly Reduced
Reduced risk of your identity being stolen	Not Reduced	Not Reduced
Reduced risk to other individuals and business from your insecurity	Not Reduced	Greatly Reduced
If these were the only options available, which would you choose?	□	□

Suppose your ISP was going to pursue the strategies for improving security that are included in your preferred option and that these strategies resulted in the outcomes described in the table above. Would you support your ISP pursuing these strategies?

□ Yes, I would support my ISP pursuing these strategies

□ No, I would not support my ISP pursuing these strategies

Each hypothetical ISP security package was presented as being composed of the six costs and benefits (known as package "attributes") we used to conceptualize broadband user utility. However, in order to make the description of these attributes tractable in an experimental setting, we had to establish a set of finite descriptors known as "levels" to describe each attribute in a way the average broadband user would understand. We attempted to create levels for each of the six attributes so that they would include the set of plausible extremes. For example, the levels chosen for the attribute for limiting access to the Internet range from the ISP never having the ability to limit one of its customers' access to the ISP being able to totally disconnect them from the Internet if their computer appears to be infected by malware.

However, choosing the levels for the cyber security outcomes (benefits) attributes proved to be more difficult. We considered using quantitative measures of the how much various threats could be reduced (for example saying the risk of identity theft would be reduced by 50%) but were concerned that (1) respondents would find these questions difficult to comprehend and (2) respondents would be answering questions from different baselines as to what the current risks were. Therefore, three qualitative levels were chosen for each attribute to indicate whether the package in question "greatly reduced" a given threat, "somewhat reduced it," or did not reduce it at all. A summary of the attributes and levels used in the final survey instrument are presented in Table 4.

Choosing the levels for the cyber security outcomes (benefits) attributes proved to be particularly difficult. We considered using quantitative measures of the how much various threats could be reduced (for example saying the risk of identity theft would be reduced by 50%) but were concerned that (1) respondents would find these questions difficult to comprehend and (2) respondents would be answering questions from different baselines as to what the current risks were. Therefore, three qualitative levels were chosen for each attribute to indicate whether the package in question "greatly reduced" a given threat, "somewhat reduced it," or did not reduce it at all.

Given the attributes and levels described above, there are 729 (3 x 3 x 3 x 3 x 3 x 3) possible hypothetical packages that could be created. However, one of the primary benefits of conjoint analysis is that only a small fraction of these potential packages have to be evaluated by actual respondents if each the attributes being considered are assumed to add linearly to a person's utility. When this assumption is made, and a proper subsample of the 729 hypothetical policy profiles is chosen (this subsample being referred to as the "experimental design"), then statistical analysis can be used to predict how respondents would answer the remaining hypothetical choice tasks (Orme, 2010). A "proper subsample" or statistically efficient experimental design is one which posses several properties (Kanninen, 2002; Zwerina et al. 1996;), such as:

- *Level Balance*: levels of an attribute occur with equal frequency.
- *Orthogonality*: the occurrences of any two levels of different attributes are uncorrelated.

- *Minimal Overlap*: cases where attribute levels do not vary within a choice set should be minimized.
- *Utility Imbalance*: the probabilities of choosing alternatives within a choice set should be as efficient as possible. For example, for two alternatives the probabilities should be approximately 0.75 and 0.25 (Kanninen, 2002).

Table 4. Attributes and Levels for Choice Experiment Design

Attributes	Levels
Fee	• $4 per month • $7 per month • $12 per month
Require Internet users to follow certain security policies and be trained regularly	• 0.5 hours per month • 1 hour per month • 3 hours per month
Limit Internet access of customers whose computers show signs of being hacked	• ISP can never limit your access to the Internet • ISP can restrict your usage to certain functions or Web sites if they suspect you have been hacked • ISP can cut off your connection to the Internet entirely if they suspect you have been hacked
Reduced risk of your computer slowing down or crashing	• Not reduced • Somewhat reduced • Greatly reduced
Reduced risk of your identity being stolen	• Not reduced • Somewhat reduced • Greatly reduced
Reduced risk to other individuals and businesses from your insecurity	• Not reduced • Somewhat reduced • Greatly reduced

Unfortunately, it is often not possible to achieve both level balance and orthogonality in small designs. However, Kuhfeld, Tobias, and Garratt (1994) show that it is possible to produce relatively efficient designs that are neither balanced nor orthogonal. Such efficient designs can be produced using an iterative computer algorithm. The experimental design for our stated preference questions was created using Sawtooth Choice-Based Conjoint Software.

4.2.2 Survey Administration and Sample Size

After the survey instrument was completed, it was programmed for web administration by comScore, Inc., which maintains a large opt-in consumer panel that it maintains to be representative of the online population and projectable to the total U.S. population. These panelists are recruited across thousands of sites not used by other panel suppliers and panelists do not have to be willing to answer surveys to be accepted to the panel. Once the survey was programmed, it was administered from November 2010 to December 2010 to members of the comScore panel that had broadband Internet access, exceeded 18 years of age, and resided inside the United States. We decided to include only broadband users in our sample because they are the users that would be most impacted by ISP security packages.

To determine the proper sample size for this survey, we used the technique recommended by Orme as a starting point. This method relies on the number of total questions per respondent (t), the maximum number of attribute levels (c), the number of alternatives in the tradeoffs (a), and the number of respondents (n). In this study, c=3 (all attributes possess only 3 levels), a=2 (alternatives of A or B), and t=7 main questions. Specifically, Orme recommends that (nta/c ≥ 500), for a minimum sample size of at least n=107 for each version of our survey. To improve the statistical power and reliability of our analyses we sampled a significantly greater number n=3,635.

4.3 Results

4.3.1 Sample Descriptive Statistics

Descriptive statistics of the sample we collected are provided in Table 5. The sample was approximately evenly split between males and females. Approximately half of the sample was less than 40 years of age. The vast majority of survey respondents (~70%) were college educated. The majority of respondents (57%) had household incomes exceeding $50,000. The vast majority of the sample were white (81%). The majority of respondents pay more than $40 per month for broadband access (54%). Specifically, the mean monthly broadband bill was estimated to be $46. Based on the average broadband prices described in Section 3, this suggests that survey respondents are likely not paying a high enough price to receive security (included or optional) from their ISP.

In addition to collecting information about sample demographics, we asked survey respondents a variety of questions about the computers they own, how they use them, and how they view the threat of cyber security and possible solutions. The following sections provide a summary of the results of these questions.

4.3.1.1 Computer Usage and Internet Service

Approximately 50 percent of respondents only use more than one computer each week, which suggests that differing security environments are likely present. When asked to think about the primary personal computer they use, 90 percent of respondents indicated that they were the person in charge of security for this computer. The majority of respondents (59%) have had their computer for less than 2 years and 60 percent spent less than $1,000 on this computer (average cost was $794). Most people (73%) had a computer before their current computer, and they kept that computer for an average of just under 5 years.

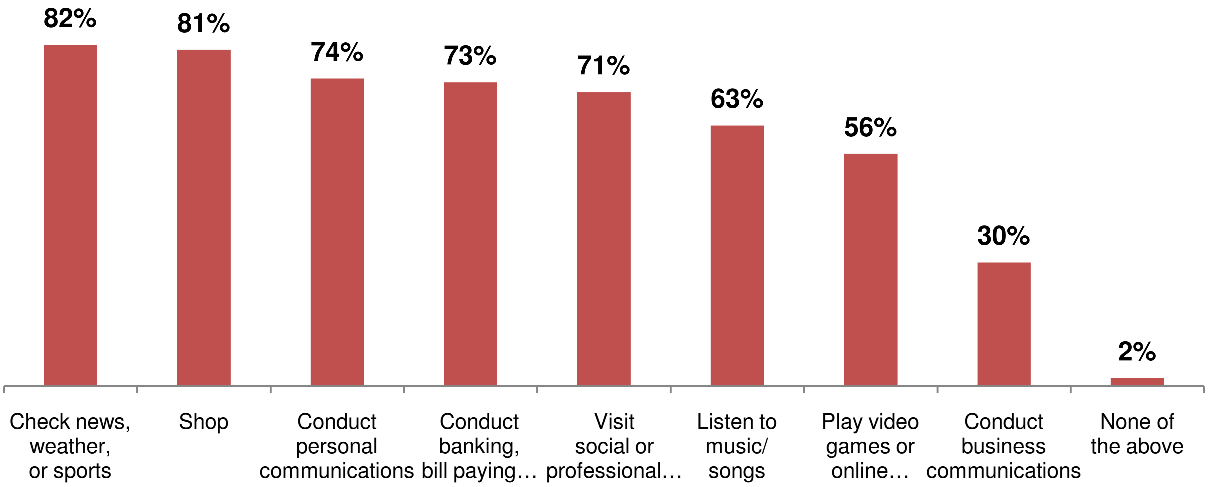
Table 5. Characteristics of Survey Respondents (n = 3,635)

	Percent of Respondents		Percent of Respondents
Gender		**Annual Household Income**	
Male	49	<$50,000	44
Female	51	$50,000-$99,000	36
		$100,000+	21
Age		**Race**	
18-24 years	11	White	81
25-34 years	31	Non-white	19
35-44 years	15	**Monthly Broadband Bill**	
45-54 years	26	<$20	8
55-64 years	12	$20-$39	38
65 years & above	5	$40+	54
Education			
High school diploma or less	21		
Some college	30		
College graduate	49		

The average amount of time spent online was 1.9 hours per day, with approximately 45 percent spending 5 hours or more online each day. Respondents indicated that they use their main computer for a variety of activities, as shown in Figure 6. Note that 81 percent shop online (likely using credit cards) and 73 percent conduct banking transactions online. In terms of people's comfort with their computer, 73 percent feel comfortable installing new software, but if they need help with their computer, 51 percent would ask either a family member (34%) or a friend or coworker (17%).

Most people selected their current ISP based on a variety of reasons with speed, price, and bundling (with cable and our telephone) being the top reasons. Seventy-five percent of respondents indicated that their Internet was bundled with their cable service, telephone service, or both. Security was only an important factor to 4 percent of respondents when deciding on their ISP. In contrast with figures presented in Section 3, only 40 percent of respondents thought that their ISP provided security solutions that they could get for free or at a price (18% were unsure).

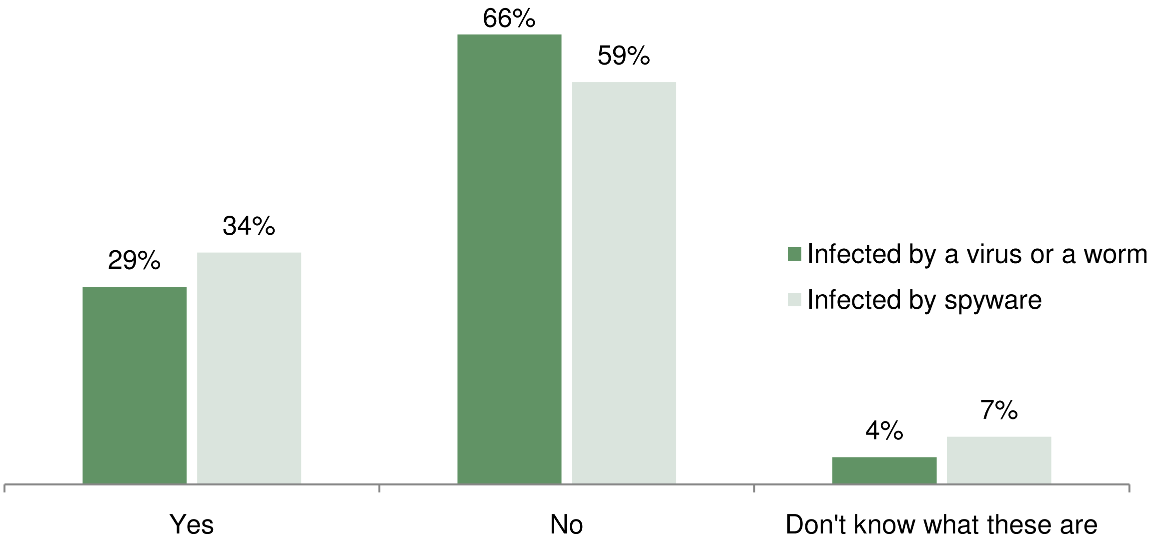
Figure 6. Computer Activities, Indicated by Survey Respondents



4.3..1.2 Cyber Security Habits and Views

As shown in Figure 7, most consumers are not aware of their computer having been infected by a virus, worm, or spyware. For those who have had a security problem in the past year (approximately 40% of respondents), most were able to fix these issues in under 6 hours (59% of respondents) and by spending $56 or less (56% of respondents).

Figure 7. Individuals Perception of Whether Their Computer Has Been Infected by a Virus, Worm, or Spyware in the Last Year



Consumers claim to be spending more time educating themselves about cyber security threats—approximately 6 hours per year—versus spending time securing their computer each year—about 2 hours per year on average.

The vast majority (89%) of consumers believe they have antivirus software installed on their current home computer and 82 percent believe that they can avoid getting a virus if the right precautions are taken. Sixty-nine percent would also be either very or somewhat more likely to take steps to improve their computer security if their best friend was doing so.

The most important pieces of security advice are felt to be using antivirus software, keeping this software updated and regularly scanning your computer, using security software and good passwords, being careful which websites you visit, and using caution when downloading from websites.

The number one concern that people have when using the Internet is that someone will steal their personal information. Sixty-nine percent of respondents indicated that this was a concern, followed by fear of criminals accessing individuals' bank records (61%), fear of individuals' hard drive crashing (58%), and fear of having sensitive personal information released without permission (54%).

Most (83%) are aware that someone can break into their computer without their knowledge and although they believe that it is somewhat or very unlikely that someone has done this in the past, they are at least somewhat concerned about this occurring in the future.

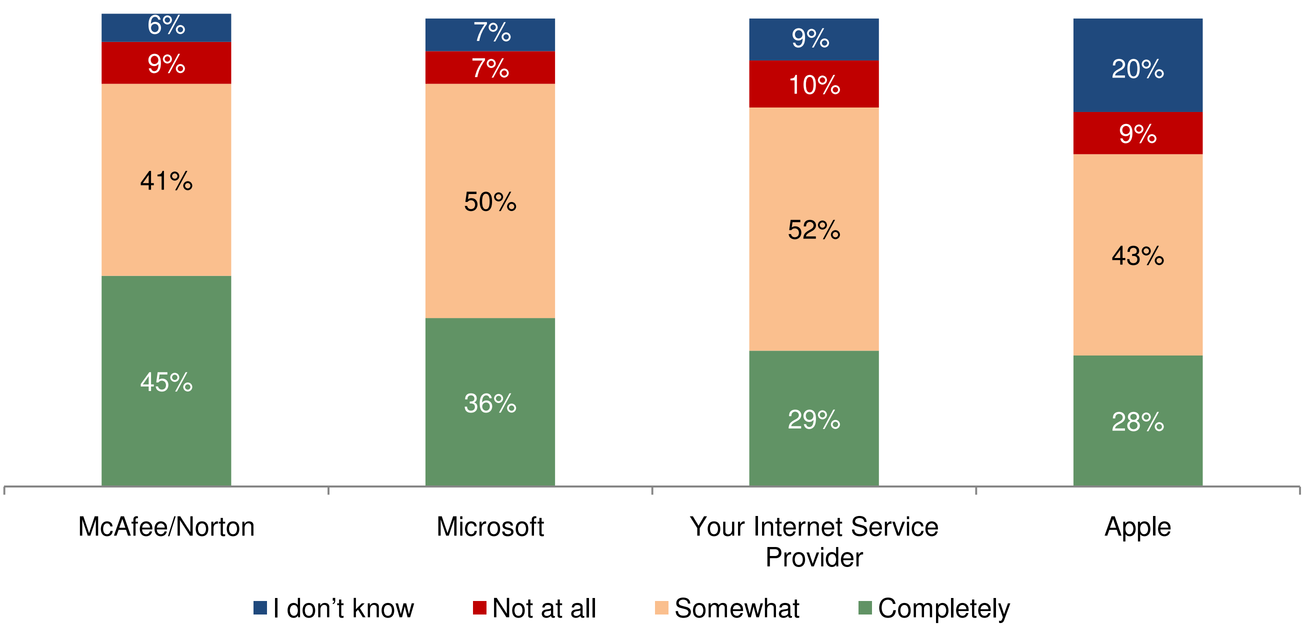
As shown in Figure 8, when it comes to trusting that companies are doing what they can to help reduce cyber security threats, McAfee/Norton and Microsoft are seen as more trustworthy than ISPs and Apple. This is very important knowledge for both companies and policy makers to begin to educate the public and to design solutions that will work, based on their current frame of reference (referred to in psychology as the framing effect).

Most consumers (88%) feel that everyone could be a target of malware, and approximately 50 percent believe that their computer likely has been used to send spam or attack others. Sixty-five percent of respondents believe this is likely to happen in the future. Still, 82 percent of respondents believe that you can avoid being a victim of malware.

4.3.1.3 Opinions on Strategies to Improve Cyber Security

Among the various monetary and nonmonetary costs associated with increased security that we included in our survey, more people indicated that they would be willing to spend time securing their computer against cyber security threats or receiving security training (76%) than they would be willing to pay a fee to their ISP to do so (48%). They also believe that this time spent would be more effective than paying a fee and are not very concerned that they would be asked to spend too much time doing so. Most are concerned that they would be overcharged by their ISP for their efforts if that route was taken to reduce cyber security threats.

Figure 8. Individuals' Willingness to Trust Companies to Do What They Can to Reduce Cyber Security Threats to Your Computer



Consumers would prefer to have their Internet access limited only if their computer appeared to have been hacked or hijacked instead of having their ISP proactively monitoring their Internet activity. Most are at least somewhat concerned that their ISP would abuse both situations and do not feel that either would be more effective over the other in reducing cyber security threats. Consumers' willingness to allow their ISP to limit their Internet access is similar regardless of whether it appeared that the threat would be to just their computer or that their computer could be a threat to other computers.

When asked their number one concern regarding what an ISP might do with the Internet activity data that they collect, 48 percent of respondents thought the ISP might sell the data to a third party for marketing purposes.

4.3.1.4 Opinions on Cyber Security Outcomes

Most respondents (64%) felt that their current home computer runs slowly, and most would be willing to pay a monthly fee of up to $5 or a one-time fee of up to $10 for a 50 percent increase in their computer's speed.

Perception is often greater than reality when it comes to estimating the amount of time and money that it takes to resolve an identity theft situation. Victims of identity theft usually spent under 7 hours and $50 or less to resolve their situation, yet those who have not been victims expect to spend more than 12 hours and more than $50.

Many believe that efforts by their ISP to improve cyber security could reduce the risk that their computer would slow down or crash and would help to reduce the risk of identity theft. However, 4 in 10 survey participants think there is still a 50 percent or greater chance that these situations would occur even with ISP security efforts in place.

Approximately 59 percent of respondents believe that the federal government should have a role in improving cyber security. Respondents indicated a desire for the government to mandate ISPs and software makers to meet specific security standards, but respondents were not supportive of the government subsidizing compliance with these new standards..

4.3.2 U.S. Broadband User Preferences

To address the three primary research questions of this paper, we first had to quantify the preferences of U.S. broadband users for each of the attributes and levels used to construct the hypothetical ISP security policies presented in the conjoint portion of the survey. Table 6 (column 2) shows the statistical model of preferences for U.S. broadband users, which were estimated using maximum likelihood techniques in Stata 11. Fee and time spent complying with ISP security requirements were included in the model as continuous variables. Therefore, their coefficients can be interpreted directly as inverse marginal utilities. Specifically, the coefficient on the fee attribute indicates that every $1 increase in the cost of Internet access decreases utility by 0.14 (or equivalently that the utility of an additional dollar, the marginal utility of money, is 0.14). Similarly, the coefficient on the time attribute indicates that every hour less spent complying with ISP security standards increases utility by 0.10.

All other attributes are effects coded. As a result, their coefficients represent part-worth utilities. Unlike marginal utilities these do not represent rates of change, they are additive scores that indicate the relative preference of a particular level within an attribute. Larger part-worth utilities indicate attribute levels that more preferred to attribute levels with smaller utilities (Orme, 2010). For example, inside the attribute for limiting Internet access, the part-worth utility associated with the “Never Allowed” level (0.31) is greater than the part-worth utility associated with the “Entirely cut off access” level (–0.30). This implies, as one would expect, that on average the “Never Allowed” level was preferred for this attribute to the “Entirely cut off access” level.

Based on the size and sign of model coefficients, we can see that user preferences coincide well with the hypotheses stated in constructing our conceptual model. Specifically, increases in the cost of Internet access decrease personal utility, increases in the time it takes to comply with ISP security requirements decrease personal utility, improvements in a user’s access to the Internet increase utility, improvements in the performance of a user’s computer increase utility, improvements in computer performance increase utility, and increases in losses incurred by others reduce an individual user’s utility.

Table 6. Preference Parameter Estimates (coefficients from mixed logit model)

	Estimated Mean Coefficient	Standard Error of the Mean	Estimated Standard Deviation	Standard Error of the Standard Deviation
Add a fee to provide security services to Internet subscribers	–0.14**	0.00	NA	NA
Require Internet users to follow certain security policies and be trained regularly	–0.10**	0.01	NA	NA
Limit Internet access for customers whose computers show signs of being "hacked"				
Never limit access	0.31**	0.02	0.51	0.03
Only restrict access	–0.01**	0.02	0.00	0.05
Entirely cut off access	–0.30**	0.02	NA	NA
Reduced risk of your computer slowing down or crashing				
Not reduced	–0.30**	0.02	0.26	0.05
Somewhat reduced	–0.02**	0.02	–0.09	0.08
Greatly reduced	0.32**	0.02	NA	NA
Reduced risk of your identity being stolen				
Not reduced	–0.49**	0.02	–25.23	0.00
Somewhat reduced	0.06**	0.02	0.92	0.36
Greatly reduced	0.43**	0.02	NA	NA
Reduced risk to other individuals and businesses from your insecurity				
Not reduced	–0.21**	0.02	–0.10	0.08
Somewhat reduced	0.00**	0.02	–0.01	0.04
Greatly reduced	0.21**	0.02	NA	NA
No choice alternative (adjusted)	–0.46**	0.07	1.17	0.42

Note: (1) Effects coded variables used for all attributes except fee and time spent complying with security requirements. (2) Standard errors on omitted coefficients were estimated by Krinsky-Robb parametric bootstraps. (3) *** denotes p <0.01, **p <0.05, *p <0.10.

In addition, we can also see that the cyber security outcome (or benefit) that matters most to broadband users is reduction in the risk of identity theft. This is demonstrated by the fact that the part-worth utility associated with great reductions in the risk of identity theft (0.43) is larger than the part-worth utility associated with great reductions in the risk of computer slowing down or crashing (0.32) or risk to others (0.21).

4.3.3 Willingness to Pay for Improvements in ISP Security Package Features

The first research question we explored in the demand assessment was how much individuals would pay to achieve improvements in ISP security policy attributes (or alternatively, how much they would have to be compensated to accept unfavorable changes in ISP policies). We estimate how much respondents would be willing to pay (on average) for improvements in attribute levels by dividing the difference between the part-worth utilities associated with each level by the marginal utility of income.[8] For example, the mean willingness to pay to move from allowing an ISP to entirely cut off one's Internet access to never allowing an ISP to restrict one's access is estimated to be $4.32 per month. Alternatively, this can be considered as the amount respondents would have to be paid on average to switch their preference from an ISP security policy in which the ISP is never able to restrict Internet access to an ISP security policy in which the ISP is able to entirely cut off access (all else being held constant).

We used the formula described above to convert the preferences parameter estimates in Table 6 into willingness to pay estimates. Table 7 shows the mean willingness to pay (WTP) for changes in each ISP security strategy from their least to their most favored level along with 95 percent confidence intervals. In terms of nonmonetary costs associated with ISP security policies, respondents were only willing to pay $0.73 per month to avoid 1 hour time spent complying with ISP security requirements. Or, alternatively, respondents would have to be paid $0.73 per month to accept such requirements (all else being held constant). This would represent less than a 2 percent decrease in the mean monthly broadband bill.

Table 7. Mean Willingness to Pay for Improvements in ISP Security Package Features

	Estimated WTP ($/month)	95% Confidence Interval
Time Spent Complying with ISP Security Requirements: WTP to avoid 1 hour of time complying with security requirements	0.73	[0.57 to 0.92]
Limiting Internet Access: WTP to move from ISP being able to entirely restrict access to not restrict access at all	4.32	[3.72 to 4.92]
Risk of Computer Shutting Down or Crashing: WTP to move from not reduced to greatly reduced	4.40	[3.83 to 4.97]
Risk of Identity Theft: WTP to go from not reduced to greatly reduced	6.51	[5.86 to 7.16]
Risk to Other Individuals and Businesses: WTP to go from not reduced to greatly reduced	2.94	[2.44 to 3.45]

Note: 95% confidence interval was estimated using Krinsky-Robb parametric bootstrapping technique.

[8] The intuition behind this calculation is that the difference between the part-worth utilities of the two levels under consideration provides you with the number of "utils" gained from making the plan change. These "utils" are converted to monetary units by dividing by the marginal utility of income.

By contrast, with regard to limitations on Internet access, respondents would be willing to pay $4.32 per month to shift from allowing ISPs to entirely cut off one's Internet access to never being allowed to restrict one's access. Or, conversely, respondents have to be paid $4.32 per month to accept a shift in the other direction (all else being held constant). This would represent a 9 percent reduction in the mean monthly broadband bill.

In terms of how much respondents were willing to pay to achieve improvements in cyber security outcomes, we see that (in contrast to the expectations of ISPs) all WTP estimates are greater than zero and statistically significant at the 0.05 significance level. Specifically, respondents were willing to pay $6.51 per month to greatly reduce the risk of identity theft (other things being equal). If ISPs could achieve and charge for such an improvement, this would represent a 14 percent increase in ISP revenue over the current mean monthly broadband bill. In terms of improvements in other cyber security outcomes, respondents were willing to pay $4.40 per month to greatly reduce the risk of their computer crashing and $2.94 per month to greatly reduce the risks of cyber security threats to others that may result from their personal insecurity.

4.3.4 Willingness to Pay for Hypothetical ISP Security Packages

The second research question we explored in the demand assessment was how much would the mean broadband user be willing to pay for hypothetical security packages offered by ISPs relative to having no security package. For the purposes of this study, we consider two hypothetical security packages. First, we consider the package that would be most preferred by home broadband users. This package would include 0 hours each month complying with ISP security requirements, ISP can never limit user Internet access, risk of computer slowing down is greatly reduced, risk of identity theft is greatly reduced, risk to other individuals from user insecurity is greatly reduced. Although this package would likely be unfeasible from the perspective of the ISP, the WTP estimated for this package would represent the most broadband users would ever pay for ISP-based security solutions.

The second hypothetical security package we consider in this study is one that is similar to the type of ISP-based security solutions discussed above. Specifically, this package would "quarantine" users that were identified as having malware on their machines and require them to spend time removing this malware from their machine. This package would certainly benefit individuals besides the user herself as such a package would go toward preventing the spread of botnets and other cyber security threats. However, it is not readily apparent how much benefit the broadband user herself would receive from this package. Therefore, to achieve the most conservative willingness to pay estimate, we assume she receives no direct benefit. In terms of the attribute levels used in the choice experiments, this package would be described as including 3 hours of time each month complying with ISP security requirements, ISP can entirely cut off user Internet access if they suspect you have been hacked, risk of computer slowing down is not reduced, risk of identity theft is not reduced, risk to other individuals from user insecurity is greatly reduced.

This maximum WTP for both packages can be calculated using the “log-sum” formula (Train, 2003). Specifically, the maximum WTP for the most preferred ISP security package relative to having security package is estimated from the log-sum formula as[9]:

$$WTP = (-1/\beta_{fee}) * [\ln(\exp((\beta_{time}*0)+ \beta_{isp\ never\ limit\ access} + \beta_{crash\ risk\ greatly\ reduced} + \beta_{id\ theft\ risk\ greatly\ reduced} + \beta_{risk\ to\ others\ greatly\ reduced}) + \exp(\beta_0 - \beta_{fee}*\$7.15 - \beta_{time}*1.40)) = \$7.24.$$

In other words, the maximum amount the average respondent would be willing to pay for additional security is $7.24 per month (in addition to his or her current Internet access bill) if no time is required and his or her Internet cannot be limited in any way.

This procedure can be used to answer questions important to both ISPs interested in implementing similar security policies of their own or U.S. government agencies. For example, we can use this procedure to estimate how much U.S. broadband users would be willing to pay for an ISP security package with the following features: ISPs could entirely cut off Internet access to their subscribers and the risk of cyber security threats to other individuals and businesses would be reduced, but the risk of subscribers’ Internet crashing/slowing would not be reduced and the risk of identity theft would not be reduced, (i.e., the respondent receives no benefit). Such a policy would be of particular interest to policy makers or ISPs concerned with reducing the threat of botnets:

$$WTP = (-1/\beta_{fee}) * [\ln(\exp((\beta_{time}*0)+ \beta_{isp\ can\ cut\ off\ subscriber\ Internet\ access} + \beta_{crash\ risk\ not\ reduced} + \beta_{id\ theft\ risk\ not\ reduced} + \beta_{risk\ to\ others\ greatly\ reduced}) + \exp(\beta_0 - \beta_{fee}*\$7.15 - \beta_{time}*1.40)) = \$1.34$$

Based on the results of our model, we can see that the average respondent would be willing to pay approximately $1.34 for this package.

[9] Please note that the $7.15 and 1.40 hours are the mean dollars and time shown to respondents in the hypothetical choice tasks. The subtraction of β_{fee}*$7.15 and β_{time}*1.40 from the alternative-specific constant, $\beta_{0,}$ is necessary because we used continuous fee and time terms and effects-coding for the other parameters.

Looking at both of these example estimates of willingness to pay (shown in Text Box 4), it is clear that home Internet users value both the potential benefits of security (particularly a reduction in the threat of identity theft) and their ability to use the Internet without the threat of being cut off. As such, ISPs interested in designing packages that consumers would pay for should try to reduce the chance of cutting consumers off and sell their products by touting the benefits that consumers care about most. However, to increase overall security, this may mean contacting consumers directly (versus cutting them off too quickly) which would increase ISPs' costs.

Text Box 4. Example Willingness to Pay Estimates

Package #1: Benefits to you and others, no nonmonetary costs

Features:

- Your Internet *cannot be cut off* if you look like a bot (malicious traffic coming from you)
- Greatly reduced risk of identity theft
- Greatly reduced risk of your computer slowing down or crashing
- Greatly reduced risk to others (individuals and businesses) from your computer

Willingness to Pay: **$7.24 per month**

Package #2: Benefits primarily to others

Features:

- Your Internet *can be cut off* if you look like a bot (malicious traffic coming from you)
- Greatly reduced risk to others (individuals and businesses) from your computer

Willingness to Pay: **$1.34 per month**

4.3.5 The Impact of Information Treatments on Security Preferences

The third research question that we explored in our assessment of consumers' demand for ISP-based security is the impact that information treatments (e.g., marketing messages by ISPs or educational messages put out by the government) may have on security preferences. To answer this question we presented different information treatments to survey respondents near the beginning of the survey. Specifically, the research team created seven information treatments designed to influence (1) broadband user perceptions of cyber security threats and (2) the amount broadband users are willing to pay for ISP security packages. The ultimate goal of these information treatments was to either make respondents more concerned about cyber security threats (by emphasizing the harmful consequences of insecurity), to elevate their level of trust in their ISP (by emphasizing the positive role ISPs can play in an individual's security), or both. A summary of the information treatments is provided in Table 8 and the full-text of the treatments themselves is provided in Appendix B.

Table 8. Information Treatments Shown to Some Survey Respondents

Information Treatment	Description of Information Treatment
1	A "**fear**" message directed at describing the consequences a respondent's insecurity has on *themselves*
2	A "**fear**" message directed at describing the consequences a respondent's insecurity has on *others*
3	A "**trust**" message directed at encouraging the respondent to trust their ISP in assisting with *securing their personal computer*
4	A "**trust**" message directed at encouraging the respondent to trust the ISP to monitor their Internet traffic in order *to thwart potential threats to others like botnets*
5	A combination of treatments 1 and 3
6	A combination of treatments 1 and 4
7	A combination of treatments 2 and 4

Note: The survey sample was split in to eight groups. One group saw no information treatment. The other seven groups were shown one of the information treatments described in this table.

To quantify the impact that information treatments have on how willing broadband users are to pay for ISP security policies, we divided each information treatment subgroup into its own sample and then re-estimated the regressions described 4.3.2 and estimated how much individuals in each subgroup would be willing to pay for the two hypothetical ISP security packages considered in section 4.3.4: (1) the most preferred ISP security package[10] and (2) the security policy that claims to greatly reduce the risk of cyber threats to others (i.e., a policy designed to combat botnets) but not to provide any benefit to the ISP subscriber directly.[11]

Figure 9 provides a visual representation of the results of this analysis for the first policy described above (complete results provided in Appendix C). As this figure indicates, the "baseline" subgroup (which received no information treatment) was willing to pay $7.73 per month for the best possible ISP security policy relative to the no-choice alternative with a 95 percent confidence interval ranging from $5.05 to $10.240 per month. Mean WTP does appear to slightly differ from baseline across the seven information treatment subgroups. For example, mean WTP appears to be higher for respondents receiving treatments 1, 2, and 7. By contrast, respondents receiving treatments 3, 4, 5, and 6 appear to have a lower WTP compared to baseline. However, t-tests reveal that there is no statistically significant difference between these means even at the 15% significance level.

[10] This most preferred security package was defined as that policy that contained the most preferred level for each attribute. Specifically, fee = $0, time = 0 hours, limit on Internet access = never, and all security risks are "greatly reduced."

[11] This ISP security policy was defined as fee = $0, time = 0 hours, limit on Internet access = can entirely cut off Internet access, and all security risks are "greatly reduced."

Figure 9. Willingness to Pay by Message Treatment: Most Preferred ISP Security Policy

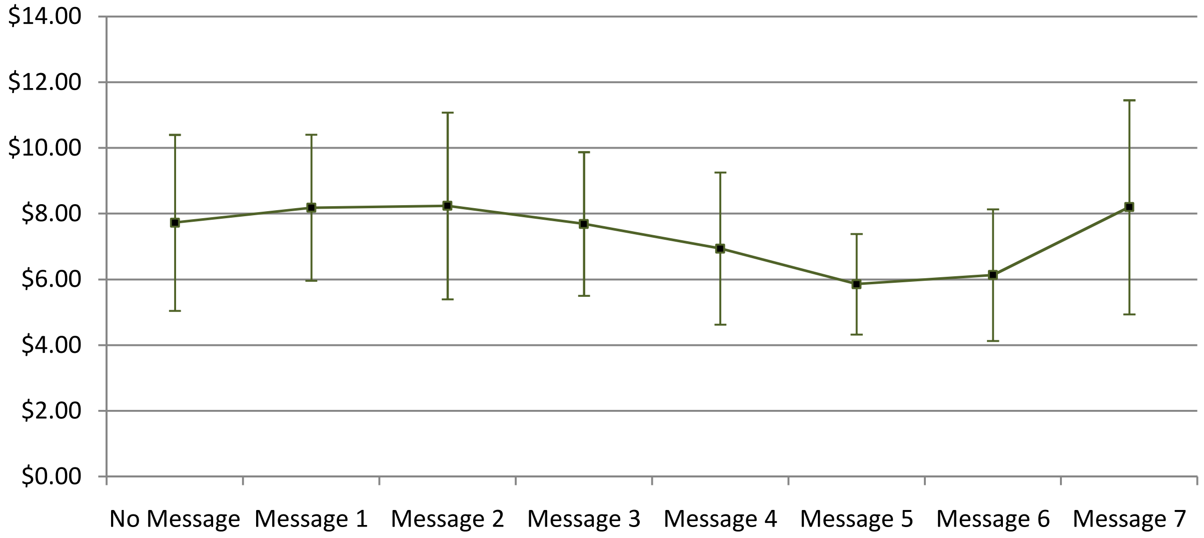
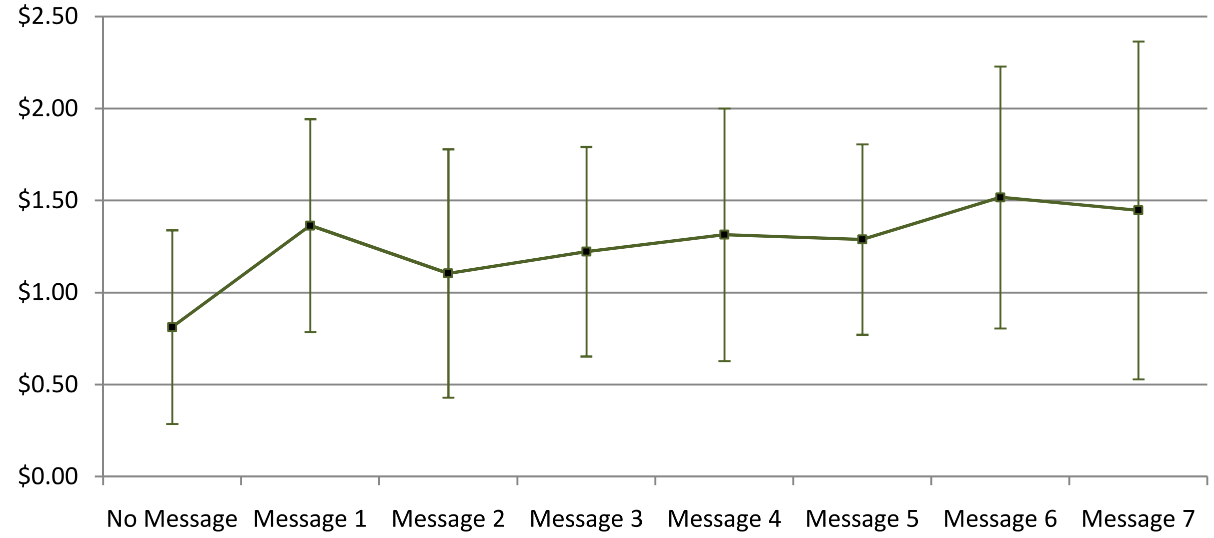


Figure 10 provides a similar representation of the results of this same analysis for the second policy described above (complete results are again provided in Appendix C). As this figure indicates, the "baseline" subgroup was willing to pay on average $0.81 per month for this policy relative to the no-choice alternative with a 95 percent confidence interval ranging from $0.29 to $1.34. Mean WTP appears to increase over the subgroups to a peak of $1.52 per month for respondents receiving information treatment 6.

Because this policy does not benefit the individual respondent at all, we would expect that subgroups receiving information treatments that were designed to make respondents more concerned about cyber security faced by others (treatments 2, 4, 6, and 7) would have higher mean WTPs than observed in the baseline subgroup. For the most part this is exactly what we observe. Mean WTP for subgroups 4, 6, and 7 are all higher than mean WTP for the baseline subgroup (in fact, mean WTP in subgroup 6 is nearly two times larger than the mean WTP observed for the baseline subgroup). T-tests reveals that this difference is statistically significant at the 5.5% level for subgroup 6 and at the 12% level for subgroups 4 and 7. The only one of these 3 subgroups whose mean WTP is not statistically different from the baseline at even the 15% significance level is the subgroup receiving information treatment 2. This information treatment relied only on fear appeals to persuade respondents to be more concerned for the threats directed at other individuals and businesses. Therefore, the fact that it appears to have had no impact on individual preferences would be consistent with some public health research that finds that exclusive fear appeals can be ineffective or at least less effective than trust appeals or fear/trust appeal combinations (Job, 1988; Davis et al., 2011).

Figure 10. Willingness to Pay by Message Treatment: ISP Security Policy Designed to Reduce Threat to Others



Given that the information treatments had no statistically significant impact on the mean WTP for the most preferred ISP package, but do appear to have made respondents more willing to pay for the package that would only benefit others, this suggests that information treatments could potentially be used to influence broadband user preferences, but that their impact is not linear across all ISP package attributes. In the future, we intend to continue research on this topic to better understand how information treatments can be used to influence public opinion.

5. Conclusions

The purpose of this study was to explore two questions. First we sought to determine how much it would cost ISPs to provide security solutions to home Internet users and what security solutions are currently being provided. Second, we sought to estimate how much home Internet users would be willing to pay to their ISP for additional security and what factors would influence the amount they would be willing to pay.

First, our assessment of the cost of ISP-based security found that ISPs are charging an average price of $5.07 for security features which are included in a monthly package (bundled with Internet service) and $4.34 when security programs must be explicitly purchased separately. We found that most ISPs are offering some security solutions, but the number that are conducting threat analysis and taking actions on such (e.g., cutting off customers until their computers are cleaned or providing IT support) was very difficult to determine. Our analysis suggests that these are activities are the most costly to ISPs but are also likely to have the greatest impact on security. We also looked at two proxy estimates of cyber security costs—for example, one medium-sized business that we talked with spends approximately $6.90 per employee per month on security support similar to what an ISP might provide; however, it also spent approximately $58 per month per employee on additional security features (e.g., firewalls and network-level security analysis).

Second, our analysis suggests that U.S. broadband users are indeed willing to pay positive and statistically significant sums to ISPs to achieve improvements in their own security and in others. Specifically, we found that home Internet users were willing to pay up to $6.51 per month to greatly reduce the risk of identity theft and $4.40 per month to greatly reduce the risk of their computer crashing. We also found that home Internet users were will to pay $2.94 per month to reduce the risks other individuals and businesses might face as a result of their personal insecurity. This conflicts with past views on this topic (e.g., Anderson, 2001; Varian, 2000) which doubted whether Internet users would be willing to pay to improve the security of others.

In addition, we find that broadband users are also willing to accept nonmonetary costs associated with ISPs for only modest reductions in the monthly cost of Internet access. For example, respondents would only have to be paid $0.73 per month to accept an ISP security policy that required them to spend 1 hour complying with ISP-determined security standards. Given that the mean monthly broadband bill for the sample was $46 per month, this compensation would correspond to less than a 2 percent decrease in monthly ISP per person revenue. Similarly, for home Internet users to accept a move from ISPs never being able to interrupt an individual's Internet access to allowing ISPs to entirely cut off one's Internet access if they are determined to be suffering from a security problem that may harm others, they would have to receive at least $4.32 per month in compensation. This would correspond to a 9 percent reduction in the mean monthly broadband bill.

In combination, our research suggests that ISPs need to provide specific assurances of benefits to their customers (in particular a reduction in the threat of identity theft) for them to be willing to pay both monetary and nonmonetary costs of additional security solutions. If ISPs can develop security solutions that minimize nonmonetary costs (time and the threat of having one's Internet cut off) to home Internet users and maximize perceived benefits (reduced threat of identity theft, system crashing, and impacts on others), our research suggests that home Internet users would be willing to pay as much as $7.24 per month.

As a secondary research effort, we also explore whether Internet users could be motivated to pay more for ISP security packages using information treatments (e.g., marketing or educational messages) that (1) articulated the dangers of insecurity and/or (2) described how ISPs could act positively to improve an individual's security. The results of our analysis indicated that information treatments can have impact, but that this impact is not the same across all ISP security packages. In future research, we will attempt to better understand how information treatments influence willingness to pay.

6. References

Anderson, R. (2001). Why Information security is hard - an economic perspective. *Proceedings of the 17th Annual Computer Security Applications Conference.*

Anderson, R., Bohme, R., Clayton, R., & Moore, T. (2008). *Security economics and the internal market.* Commissioned by the European Network and Information Security Agency (ENISA).

Comcast. (2011). *Comcast acceptable use policy for high-speed Internet*. Available at http://www.comcast.com/Corporate/Customers/Policies/HighSpeedInternetAUP.html.

The Communications Security, Reliability and Interoperability Council (CSRIC). (2010). *Internet Service Provider (ISP) network protection*. Available at http://www.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf.

Davis, K. C., Nonnemaker, J. M., Farrelly, M. C., & Niederdeppe, J. (2011). Exploring differences in smokers' perceptions of the effectiveness of cessation media messages. *Tobacco Control*, *20*(1), 26–33.

Hensher, D. A., Rose, J. M., & Green, W. H. (2005). *Applied choice analysis: A primer*. Cambridge, UK: Cambridge University Press.

ISP Planet. (2008). *Top 23 U.S. ISPs by subscriber: Q3 2008*. Available at http://www.isp-planet.com/research/rankings/usa.html.

Job, R. F. S. (1988). Effective and ineffective use of fear in health promotion campaigns. *American Journal of Public Health, 78*(2), 163–167.

Kanninen, B. (2002). Optimal design for multinomial choice experiments. *Journal of Marketing Research, 39*(2), 214–227.

Krinksky, I., & Robb, A. (1986). On approximating the statistical properties of elasticities. *Review of Economics and Statistics,* 68, 715–719.

Kuhfeld, W. F., Tobias, R. D., & Garratt, M. (1994). Efficient experimental design with marketing research applications. *Journal of Marketing Research,* 31, 545–557.

List, J., Sinha, P., & Taylor, M. (2006). Using Choice Experiments to Value Non-Market Goods and Services: Evidence from Field Experiments. *Advances in Economic Analysis & Policy, 6*(2), 1-37.

Livingston, J., Mody, N., & O'Reirdan, M. (2009). *Recommendations for the remediation of bots in ISP networks*. Available at http://tools.ietf.org/html/draft-oreirdan-mody-bot-remediation-03.

NY Times. (2010). *U.S. court curbs F.C.C. authority on web traffic*. Available at http://www.nytimes.com/2010/04/07/technology/07net.html.

Orme, B. (2010). *Getting started with conjoint analysis*. Research Publishers, LLC.

Pew Research Center. (2009). *2009 home adoption of broadband*. Available at http://www.pewinternet.org/Reports/2009/10-Home-Broadband-Adoption-2009.aspx.

Smith, V., & Mansfield, C. A. (2006, June). *Valuing airline security: An analysis of the MANPADS Program*. Paper presented at the Workshop on Benefit Methodologies for Homeland Security Analysis, Washington, DC.

Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. §§ 2510-22. 1968. Available at <http://www.it.ojp.gov/default.aspx?area=privacy&page=1284#contentTop>.

Title II of the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2510-22.1986. Available at <http://www.it.ojp.gov/default.aspx?area=privacy&page=1285#contentTop>.

Title III of the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2510-22.1986. Available at <http://www.it.ojp.gov/default.aspx?area=privacy&page=1285#contentTop>.

Train K. *Discrete choice methods with simulatio*n. 2003. Cambridge: Cambridge University Press.

Varian, H. (2000, June 1). Managing online security risks. Economic Science Column, *The New York Times*. Available at http: //www.nytimes.com/library/financial/columns/ 060100econ-scene.html.

U.S. Bureau of the Census. (2010). *2007 Economic Census*. Wired Telecommunications Carrier Industry Series. Available at http://www.census.gov/econ/census07/.

Wheatman, V. (2010). *2010 update: What organizations are spending on IT security*. Gartner Report.

Wilson, T. (2011). *Report: Botnet victim population grew more than 600 percent in 2010*. Available at http://www.darkreading.com/vulnerability-management/167901026/security/attacks-breaches/229219325/report-botnet-victim-population-grew-more-than-600-percent-in-2010.html.

Zwerina, K., Huber, J., & Kuhfeld, W. F. (1996). *A general method for constructing efficient choice designs*. SAS Working Paper. Available at http://support.sas.com/techsup/technote/mr2010e.pdf.

Appendix A

Table A-1 gives the list of ISPs examined for this analysis. Embarq and CenturyTel have since merged to form CenturyLink. Some plans can be attributed to multiple ISPs; for example, Road Runner provides service through Time Warner and other cable companies. The AOL ISP includes both dial-up offered under AOL and cable broadband under Time Warner.

Table A-2 displays the database of DSL and cable broadband plans used in this analysis. These data were collected directly from ISP websites.

Table A-1. US ISPs by Market Share

ISP	U.S. Market Share in 2008 (%)
AT&T	15.4
Comcast	15.3
Road Runner (Time Warner)	9.0
Verizon	8.8
America Online (all U.S. brand accounts)	7.7
Earthlink	3.1
Charter	3.0
Qwest	2.9
Cablevision	2.5
United Online—NetZero/Juno	1.5
Embarq	1.4
Windstream	1.0
Mediacom	0.8
CenturyTel	0.7
Citizens	0.6
Hughes Network Systems	0.4
Insight Broadband	0.4
Clearwire	0.4
LocalNet	0.3
Cincinnati Bell	0.2
SureWest	0.1
GCI	0.1
ACS	0.1

Table A-2. Broadband Plans and Prices

Company	Download Mbps	Security Program	Monthly Service Cost	Monthly Security Cost
AT&T	6	McAfee Internet Security Suite	$45	$0
AT&T	3	McAfee Internet Security Suite	$40	$0
AT&T	1.5	McAfee Internet Security Suite	$35	$5
Comcast	50	Norton Internet Security	$115	$0
Comcast	30	Norton Internet Security	$78	$0
Comcast	20	Norton Internet Security	$68	$0
Comcast	15	Norton Internet Security	$58	$0
Comcast	1	Norton Internet Security	$40	$0
Verizon	7.1	Verizon Internet Security Suite powered by McAfee	$50	$6
Verizon	3	Verizon Internet Security Suite powered by McAfee	$40	$6
Verizon	1	Verizon Internet Security Suite powered by McAfee	$30	$6
Earthlink	6	Protection Control Center	$42	$0
Earthlink	3	Protection Control Center	$40	$0
Earthlink	1.5	Protection Control Center	$40	$0
Earthlink	6	Norton Antivirus	$42	$4
Earthlink	3	Norton Antivirus	$40	$4
Earthlink	1.5	Norton Antivirus	$40	$4
Earthlink	6	Norton 360	$42	$7
Earthlink	3	Norton 360	$40	$7
Earthlink	1.5	Norton 360	$40	$7
Charter	25	F Secure—Charter Security Suite	$50	$0
Charter	16	F Secure—Charter Security Suite	$40	$0
Charter	8	F Secure—Charter Security Suite	$30	$0
Charter	1	F Secure—Charter Security Suite	$20	$0
Qwest	20	Norton Antivirus	$45	$0
Qwest	12	Norton Antivirus	$35	$0
Qwest	7	Norton Antivirus	$25	$0
Qwest	1	Norton Antivirus	$20	$0
Cablevision	30	CA Internet Security Suite	$55	$0
Cablevision	15	CA Internet Security Suite	$30	$0
CenturyLink	10	PC Security Suite	$50	$4
CenturyLink	1.5	PC Security Suite	$40	$4
CenturyLink	0.768	PC Security Suite	$30	$4
NetZero	1.5	Norton Antivirus	$30	$0
NetZero	0.768	Norton Antivirus	$20	$0
NetZero	1.5	Norton Internet Security	$30	$3

(continued)

Table A-2. Broadband Plans and Prices (continued)

Company	Download Mbps	Security Program	Monthly Service Cost	Monthly Security Cost
NetZero	0.768	Norton Internet Security	$20	$3
Windstream	12	McAfee Internet Security Suite	$40	$3
Windstream	6	McAfee Internet Security Suite	$35	$3
Windstream	3	McAfee Internet Security Suite	$30	$3
Mediacom	12	CA Internet Security Suite	$50	$0
Citizens	6	F Secure PC Protection	$90	$4
Citizens	3	F Secure PC Protection	$70	$4
Citizens	1.5	F Secure PC Protection	$50	$4
Citizens	1	F Secure PC Protection	$40	$4
Citizens	6	F Secure PC Protection Plus	$90	$5
Citizens	3	F Secure PC Protection Plus	$70	$5
Citizens	1.5	F Secure PC Protection Plus	$50	$5
Citizens	1	F Secure PC Protection Plus	$40	$5
Insight Broadband	20	CA Internet Security Suite	$45	$0
Insight Broadband	10	CA Internet Security Suite	$55	$0
Cincinnati Bell	5	F Secure—Zoomtown Internet Security	$40	$2
Cincinnati Bell	0.768	F Secure—Zoomtown Internet Security	$25	$2
SureWest	50	Kapersky Internet Security	$202	$0
SureWest	20	Kapersky Internet Security	$80	$0
SureWest	10	Kapersky Internet Security	$64	$0
SureWest	8	Kapersky Internet Security	$57	$0
SureWest	5	Kapersky Internet Security	$44	$0
SureWest	1	Kapersky Internet Security	$38	$0
GCI	4	GCI Security Guard	$105	$4
GCI	3	GCI Security Guard	$75	$4
GCI	2	GCI Security Guard	$55	$4
GCI	1	GCI Security Guard	$45	$4
ACS	3	None	$89	NA
ACS	1	None	$69	NA
Time Warner	10	CA Internet Security Suite	$45	$0
Time Warner	7	CA Internet Security Suite	$35	$0

Appendix B
Full Text of Information Treatments

Information Treatment 1, a "fear" message directed at describing the consequences a respondent's insecurity has on him- or herself:

To keep your body healthy, you must follow good habits like washing your hands to protect yourself from germs that make you sick. In the same way, you must follow good habits to keep your computer from getting infected by viruses and other types of harmful software. Not following these habits could lead to very serious consequences. For example, if you do not properly protect your computer, hackers anywhere in the world could install software on your machine without your knowledge that would allow them to **STEAL YOUR PERSONAL INFORMATION OR YOUR IDENTITY.**

- In 2006, 8.9 million people were the victims of identity theft in the United States.
- Identity theft costs $6,383 per person, on average.
- Identity theft victims spent 40 hours, on average, attempting to resolve their cases.

The questions in this section will help us better understand how you currently protect your computer and how you view cybersecurity issues in general.

Information Treatment 2, a "fear" message directed at describing the consequences a respondent's insecurity has on others:

To keep your body healthy, you must follow good habits like washing your hands to protect yourself from germs that make you sick. In the same way, you must follow good habits to keep your computer from getting infected by viruses and other types of harmful software. Not following these habits could lead to very serious consequences. For example, if you do not properly protect your computer, hackers anywhere in the world could install software on your machine without your knowledge that would allow them to **STEAL YOUR PERSONAL INFORMATION OR YOUR IDENTITY.**

- In 2006, 8.9 million people were the victims of identity theft in the United States.
- Identity theft costs $6,383 per person, on average.
- Identity theft victims spent 40 hours, on average, attempting to resolve their cases.

In addition, your infected computer could be used to attack millions of other home Internet users and businesses. For example, your infected computer could be used to **SEND THOUSANDS OF DANGEROUS SPAM E-MAIL MESSAGES.**

- Spam e-mails are not just a nuisance—spam can be used to install harmful software on someone's computer without his or her knowledge.
- This software could be used to steal personal information or someone's identity.
- Your lack of security could result in a business or individual's data being stolen.

The questions in this section will help us better understand how you currently protect your computer and how you view cybersecurity issues in general.

Information Treatment 3, a "trust" message directed at encouraging the respondent to trust his or her ISP in assisting with securing his or her personal computer:

To keep your body healthy, you must follow good habits like washing your hands to protect yourself from germs that make you sick. In the same way, you must follow good habits to keep your computer from getting infected by viruses and other types of harmful software. Not following these habits could lead to very serious consequences. For example, if you do not properly protect your computer, hackers anywhere in the world could install software on your machine without your knowledge that would allow them to **STEAL YOUR PERSONAL INFORMATION OR YOUR IDENTITY.**

YOUR INTERNET SERVICE PROVIDER (ISP) CAN HELP! It has technical experts who could serve as "PC Doctors" to help make sure your computer is healthy. Specifically, your ISP could provide:

- Technical assistance for home users needing "hands on" help.
- Tutorials for how to keep your computer more secure.
- Free security software for you to use on your computer.

Many ISPs already offer these types of Internet security options to their subscribers!

The questions in this section will help us better understand how you currently protect your computer and how you view cybersecurity issues in general.

Information Treatment 4, a “trust” message directed at encouraging the respondent to trust the ISP to monitor their Internet traffic to thwart potential threats to others like botnets:

To keep your body healthy, you must follow good habits like washing your hands to protect yourself from germs that make you sick. In the same way, you must follow good habits to keep your computer from getting infected by viruses and other types of harmful software. Not following these habits could lead to very serious consequences. For example, if you do not properly protect your computer, hackers could install software on your machine without your knowledge that would allow the hackers to **ATTACK OTHER PEOPLE’S COMPUTERS THROUGH YOUR COMPUTER** (perhaps by sending out spam e-mails that contain harmful software).

YOUR INTERNET SERVICE PROVIDER (ISP) CAN HELP! Doctors fight the spread of a deadly illness by identifying infected individuals and separating them from the healthy population. In the same way, ISPs can use information they already collect on the *amount* and *type* of Internet activities of their subscribers (but *not* the content of those activities) to identify computers that are being used to attack others.

If it turns out that your computer was infected, then the ISP could:

- **First,** disconnect your computer from the Internet to protect other people.[12]
- **Second,** help you remove the software that is allowing a hacker to control your computer.
- **Third,** get you back online!

Many ISPs already offer these types of Internet security options to their subscribers!

The questions in this section will help us better understand how you currently protect your computer and how you view cybersecurity issues in general.

[12] Remember, your ISP employs a staff of technical experts and has a financial stake in the quality of your Internet experience. So it has every incentive to ensure that your time off-line is as short as possible and that you are protected from future interruptions.

Information Treatment 5, a combination of treatments 1 and 3:

To keep your body healthy, you must follow good habits like washing your hands to protect yourself from germs that make you sick. In the same way, you must follow good habits to keep your computer from getting infected by viruses and other types of harmful software. Not following these habits could lead to very serious consequences. For example, if you do not properly protect your computer, hackers anywhere in the world could install software on your machine without your knowledge that would allow them to **STEAL YOUR PERSONAL INFORMATION OR YOUR IDENTITY.**

- In 2006, **8.9 million people** were the victims of identity theft in the United States
- Identity theft **costs $6,383 per person**, on average.
- Identity theft **victims spent 40 hours**, on average, attempting to resolve their cases.

YOUR INTERNET SERVICE PROVIDER (ISP) CAN HELP! It has technical experts who could serve as “PC Doctors” to help make sure you computer is healthy. Specifically, your ISP could provide:

- Technical assistance for home users needing “hands on” help.
- Tutorials for how to keep your computer more secure.
- Free security software for you to use on your computer.

Many ISPs already offer these types of Internet security options to their subscribers!

The questions in this section will help us better understand how you currently protect your computer and how you view cybersecurity issues in general.

Information Treatment 6, a combination of treatments 1 and 4:

To keep your body healthy, you must follow good habits like washing your hands to protect yourself from germs that make you sick. In the same way, you must follow good habits to keep your computer from getting infected by viruses and other types of harmful software. Not following these habits could lead to very serious consequences. For example, if you do not properly protect your computer, hackers anywhere in the world could install software on your machine without your knowledge that would allow them to **STEAL YOUR PERSONAL INFORMATION OR YOUR IDENTITY.**

- In 2006, **8.9 million people** were the victims of identity theft in the United States.
- Identity theft **costs $6,383 per person**, on average.
- Identity theft **victims spent 40 hours**, on average, attempting to resolve their cases.

In addition, your infected computer could be used to attack millions of other home Internet users and businesses. For example, your infected computer could be used to **SEND THOUSANDS OF DANGEROUS SPAM E-MAIL MESSAGES.**

- Spam e-mails are not just a nuisance—spam can be used to install harmful software on someone's computer without his or her knowledge.
- This software could be used to steal personal information or someone's identity.
- Your lack of security could result in a business or individual's data being stolen.

YOUR INTERNET SERVICE PROVIDER (ISP) CAN HELP! It has technical experts who could serve as "PC Doctors" to help make sure you computer is healthy. Specifically, your ISP could provide:

- Technical assistance for home users needing "hands on" help.
- Tutorials for how to keep your computer more secure.
- Free security software for you to use on your computer.

Many ISPs already offer these types of Internet security options to their subscribers!

The questions in this section will help us better understand how you currently protect your computer and how you view cybersecurity issues in general.

Information Treatment 7, a combination of treatments 2 and 4:

To keep your body healthy, you must follow good habits like washing your hands to protect yourself from germs that make you sick. In the same way, you must follow good habits to keep your computer from getting infected by viruses and other types of harmful software. Not following these habits could lead to very serious consequences. For example, if you do not properly protect your computer, hackers anywhere in the world could install software on your machine without your knowledge that would allow them to **STEAL YOUR PERSONAL INFORMATION OR YOUR IDENTITY.**

- In 2006, **8.9 million people** were the victims of identity theft in the United States
- Identity theft **costs $6,383 per person**, on average.
- Identity theft **victims spent 40 hours**, on average, attempting to resolve their cases.

In addition, your infected computer could be used to attack millions of other home Internet users and businesses. For example, your infected computer could be used to **SEND THOUSANDS OF DANGEROUS SPAM E-MAIL MESSAGES.**

- Spam e-mails are not just a nuisance—spam can be used to install harmful software on someone's computer without his or her knowledge.
- This software could be used to steal personal information or someone's identity.
- Your lack of security could result in a business or individual's data being stolen.

YOUR INTERNET SERVICE PROVIDER (ISP) CAN HELP! Doctors fight the spread of a deadly illness by identifying infected individuals and separating them from the healthy population. In the same way, ISPs can use information they already collect on the *amount* and *type* of Internet activities of their subscribers (but *not* the content of those activities) to identify computers that are being used to attack others.

If it turns out that your computer was infected, then the ISP could:

- **First,** disconnect your computer from the Internet to protect other people.[13]
- **Second,** help you remove the software that is allowing a hacker to control your computer.
- **Third,** get you back online!

Many ISPs already offer these types of Internet security options to their subscribers!

The questions in this section will help us better understand how you currently protect your computer and how you view cybersecurity issues in general.

[13] Remember, your ISP employs a staff of technical experts and has a financial stake in the quality of your Internet experience. So it has every incentive to ensure that your time off-line is as short as possible and that you are protected from future interruptions.

Appendix C
Statistical Comparison of WTP Estimates Across Information Treatment Subgroups

We used a standard z-test to evaluate whether maximum WTP for each information treatment subgroup was statistically different from the WTP estimated for the baseline subgroup. Specifically, we tested the null hypothesis that the difference between the two mean WTPs (the mean estimated for the baseline subgroup and the mean estimated for a given information treatment subgroup) is zero against the one-sided alternative hypothesis that the mean for the information treatment subgroup is greater than the mean for the baseline subgroup.

The test statistic is given by:

$$z = \frac{\overline{X}_1 - \overline{X}_2}{s_{\overline{X}_1 - \overline{X}_2}}$$

where 1 = the information treatment subgroup in question and 2= the baseline subgroup and where

$$s_{\overline{X}_1 - \overline{X}_2} = \sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}}$$

where (s_1^2/n$_1$) and (s_2^2/n$_2$) are the squared standard errors for the two subgroups (which were estimated by Krinsky-Robb parametric bootstraps).

Table C-1 provides information on the mean WTP estimated for the two hypothetical ISP security packages described in the main body of the report: (1) the most preferred ISP security package[14] and (2) the security policy that claims to greatly reduce the risk of cyber threats to others (i.e., a policy designed to combat botnets) but not to provide any benefit to the ISP subscriber directly.[15] Table C-2 provides z-statistics estimated using the data in Table 1 and their respective p-values.

Table C-1. Estimated Willingness to Pays and Standard Errors for Hypothetical ISP Security Packages by Information Treatment Subgroup

	Most Preferred ISP Security Package		ISP Security Package that Primarily Benefits Others	
Information Treatment Subgroup	Mean Maximum Willingness to Pay ($/month)	Standard Error	Mean Maximum Willingness to Pay ($/month)	Standard Error
No treatment	0.81	0.26	7.73	1.34
1	1.36	0.29	8.18	1.11
2	1.10	0.34	8.24	1.42
3	1.22	0.28	7.69	1.09
4	1.31	0.34	6.94	1.16
5	1.29	0.26	5.86	0.76
6	1.52	0.36	6.13	1.00
7	1.45	0.46	8.20	1.63

[14] This most preferred security package was defined as that policy that contained the most preferred level for each attribute. Specifically, fee = $0, time = 0 hours, limit on Internet access = never, and all security risks are "greatly reduced."

[15] This ISP security policy was defined as fee = $0, time = 0 hours, limit on Internet access = can entirely cut off Internet access, and all security risks are "greatly reduced."

Table C-2. Test Statistics and P-Values for Statistical Comparison of Mean Willingness to Pays for Each Information Treatment Subgroup Against No Information Treatment Baseline Subgroup

Information Treatment Subgroup	Most Preferred ISP Security Package		Security Package that Primarily Benefits Others	
	Mean Maximum Willingness to Pay ($/month)	Standard Error	Mean Maximum Willingness to Pay ($/month)	Standard Error
1	0.263	0.40	1.412	0.08
2	0.263	0.40	0.682	0.25
3	–0.021	0.51	1.057	0.15
4	–0.444	0.67	1.160	0.12
5	–1.213	0.89	1.291	0.10
6	–0.952	0.83	1.593	0.06
7	0.224	0.41	1.199	0.12