Institute for Homeland Security Solutions

Applied research • Focused results

Understanding Cyber Security Risk Preferences: A Case Study Analysis Inspired by Public Health Research

November 2012

Authors

Brent Rowe, RTI International

Michael Halpern, RTI International

Tony Lentz, RTI International

Dallas Wood, North Carolina State University

Table of Contents

List of Figures

List of Tables

1. Introduction

Commercial, academic, and government individuals and groups from a variety of disciplines have tried, without full success, to address the problem of cyber security. A significant and growing part of the problem is the relative insecurity of individual Internet users—the threat that some individuals pose to themselves or others through their vulnerability to cyber attack. Addressing the human component of cyber attacks, risk perceptions, and vulnerability will require understanding the incentives and preferences that motivate individuals' behavior. As the number of worldwide Internet users approaches 2 billion, developing an understanding of individuals' risk perceptions of the threat of cyber attacks will be of tremendous value for addressing cyber security and mitigating attacks.

The lack of behavioral data on individual Internet users' cyber security actions presents a challenge to researchers and engineers addressing the human component of cyber security. There is a paucity of research on the factors influencing an individual's cyber security practices or lack thereof; the gap between what is currently understood and what we need to know to address the cyber security weaknesses of individual Internet users is considerable. Two recent efforts addressing cyber security have focused on the risk perceptions of small businesses regarding cyber threats and the cost of preventing cyber attacks (National Cyber Security Alliance, 2010) and the factors affecting home Internet users' demand for security from their Internet Service Providers (ISP) (Rowe et al., 2011). But the National Cyber Security Alliance (NCSA) study did not develop robust risk preference measures for individual Internet users, and the Rowe et al. study was focused on individuals' willingness to pay for security and risk preference related only to ISP-based security solutions. A baseline analysis of individuals' cyber security risk preference does not currently exist.

Leveraging the established body of public health research offers an opportunity to assess cyber security risk perceptions by using the copious amount of research that has investigated individuals' risk perceptions regarding the threat and spread of infectious disease and the factors that may influence an individual's behavior in preventing disease transmission. For example, it has been shown that individuals who perceive a higher vulnerability (i.e., risk perception) of disease infection take significantly more preventive measures than those who feel less vulnerable to infection (de Zwart et al., 2010). This type of finding illustrates that individual perceptions are crucially important to developing targeted communications strategies about diseases and related preventive actions, with the aim to influence individuals' preventive behavior.

The insecurity of individual Internet users has been described by many technology experts as a critically weak component of the Internet that is allowing distributed attacks to occur, much like a population of sick individuals facilitates infectious diseases transmission via

poor public health practices. Insecure computers are often compromised and turned into "bots" that are used to issue large amounts of spam, distributed denial of service (DDoS) attacks, and attacks on other potential bots. Because individuals' insecure computers can be turned into bots that spread attack vulnerabilities, similar to an infectious disease epidemic, developing a baseline of individual risk perceptions using a public health framework will help to improve understanding of individuals' view of risks to themselves and to society from cyber security threats.

This report presents the results of a study conducted to improve understanding of cyber security risk preferences by using the research on public health risk preferences. Our team of researchers with expertise in economics, public health, and cyber security first developed a conceptual framework for identifying the similarities between public health threats and solutions and cyber security threats and solutions (see Rowe at al., 2012). Through this process, vaccines were identified as a public health solution that had many similarities to antimalware software to help prevent cyber threats.

We developed a survey instrument that aimed to leverage both the broad frameworks used in public health to analyze individual perceptions of threats and potential preventative actions and the more specific research technique used to study risk preferences in public health. Vaccine-related studies of risk preferences offered a robust resource and given the similarities between vaccines and antimalware, the development of the survey instrument was guided directly by the types of questions asked in surveys of vaccine risk preferences. We also analyzed the resulting data in a similar way to public health research, focusing on how experience with antimalware, exposure to malware, and general risk aversion might influence what costs and benefits most affect the utility that individuals derive from antimalware software.

Section 2 below describes vaccine-related research and factors that affect antimalware risk preferences and offers an overview of antimalware and factors likely to affect antimalware risk preferences. Section 3 describes how we used past vaccine studies to inform our research on antimalware, and Section 4 delineates the study methodology. Section 5 presents the results and Section 6 provides conclusions.

2. Comparing Vaccines and Antimalware: Key Characteristics and Past Research

There are multiple parallels between cyber security and public health. In Rowe et al (2012), we provide a conceptual review of several public health frameworks and their potential use for cyber security strategic planning and research. In this study, we look at how research on vaccines can be used for research on antimalware software.

Preferences for antimalware software may have similarities to preferences for vaccination. Both vaccines and antimalware are preventive, that is they are designed to prevent a threat from having an adverse effect rather than to treat a problem once it has been diagnosed. An effective vaccine will be invisible – vaccinated individuals will not know if or when they have been exposed to the infectious disease agent against which it offers protection. Effective cyber security may also be invisible, providing protection against threats that computer users do not know are present.

No single vaccine or antimalware software package prevents all disease or cyber threats respectively. Some vaccinations provide protection against multiple related infectious disease threats; for example, influenza vaccines generally protect against multiple strains of influenza virus. Sometimes several vaccines are administered together for greater efficiency, such as the diphtheria, tetanus, and pertussis vaccines (DTP). However, no vaccine or set of vaccines will provide protection against all infectious disease threats. Similarly, no single cyber security application or antimalware program can provide protection against all types of cyber threats.

Even targeted vaccines and antimalware are not 100% effective. That is, vaccines designed to protect against a particular type of infectious disease threat will not provide full protection against that threat in all individuals. For example, individuals who are vaccinated against influenza can get the flu. Cyber security is also not 100% effective; computers running up-to-date antimalware can still have computer virus infections.

Vaccines and antimalware provide protection for a limited time period, such as a year or multiple years. Vaccines may not offer protection for extended periods of time unless they are updated with a “booster.” In the same manner, cyber security applications may offer protection only for a limited time period unless they are updated with patches or other new information.

Both vaccines and cyber security can have negative impacts or “adverse effects.” For vaccines, these can include soreness at the injection site, mild illness symptoms, or rarely serious medical conditions. For cyber security, negative impacts can include slower computer performance.

In a population, vaccination and antimalware can contribute to “herd immunity.” That is, if enough people are vaccinated, the likelihood that someone in this population who is unvaccinated will be exposed to this infectious disease threat is very low. Therefore, the unvaccinated person is protected from this threat since so many others people in his or her environment (i.e., the “herd”) will not get the infection. There are parallels to herd immunity in cyber security. If many computer users are protected against a particular type of computer virus, they will be unlikely to spread the virus to others, giving unprotected computer users immunity by being part of the group. However, because computer users could have contact with (and therefore share computer viruses with) individuals anywhere in the world, herd immunity may be less important for cyber security.

Vaccination is one of several preventive actions to prevent against infectious disease threats. Other action may include washing hands or avoiding areas where the threat is present. Similarly, cyber security protection is one of several actions to avoid cyber threats; other actions include not downloading potentially unsafe files and not going to possibly dangerous websites.

2.1 Understanding Vaccine Risk Preferences

There is a substantial body of published literature on factors influencing preferences for vaccines. Studies on vaccine preference generally involve surveys or interviews to collect information from participants on the factors most likely to influence the choice to purchase or receive a vaccine; choice studies can involve hypothetical or actual vaccines.

Because preference for vaccines can parallel preference for cyber security (based on the similarities between the two, discussed above), we have summarized literature on vaccine preference below. Factors potentially influencing vaccine choice can be broadly categorized into three groups:

- characteristics of the vaccine,
- characteristics of the infectious agents or threat, and
- characteristics of the recipient or user.

Vaccine Characteristics Affecting Preference

The characteristics of a vaccine generally have the strongest impact on preference or choice. The efficacy or effectiveness of the vaccine (i.e., how well it works to prevent infections) is often the most important characteristic (de Bekker-Grob et al., 2010; Flood et al., 2011; Newman et al., 2009; Raley et al., 2004; Zimet et al., 2005). In a survey of parent preferences for pediatric influenza vaccines, 92% of parents chose efficacy as an important vaccine attribute and gave efficacy the highest rating (Flood et al., 2011). In a study of human papillomavirus (HPV) vaccines, Brown et al. (2010) found a five-fold increase in preference for a vaccine that gave full protection against cervical cancer that can be caused by HPV versus a vaccine that provided only 70% protection. This increase in preference corresponded to an increased willingness-to-pay for the fully protective vaccine of $457. In a related study, preference for a hypothetical human immunodeficiency (HIV) vaccine increased by 75% when vaccine efficacy increased from 50% to 99% (Newman et al., 2009).

Safety, or the converse risk of side effects, is also an important characteristic influencing vaccine preference. “Risk of temporary side effects” was selected as an important characteristic of pediatric influenza vaccines by 75% of parents participating in a survey (Flood et al., 2011). In a study of hypothetical HIV vaccines, vaccine preference dropped by almost 25% when the risk of side effects changed from “none” to “minor” (temporary body aches and fever) (Newman et al., 2009). Severity of potential side effects also influenced this choice. In their study HPV vaccines, de Bekker-Grob et al. (2010) found that 25.6% of respondents

indicated that “serious side-effects” was the most important characteristics of a vaccine, but only 2.4% indicated that “mild side-effects” was the most important characteristics.

Not surprisingly, cost is almost always a significant factor influencing vaccine preference. That is, potential vaccine recipients are more likely to purchase or receive a vaccine that has a lower cost (Bishai et al., 2007). In a study of HPV vaccines, Brown et al. (2010) found that eliminating out-of-pocket costs increased vaccine use by 22%. Preference for a free HIV vaccine was almost 50% greater than the preference for an HIV vaccine costing $300 (Liau & Zimet, 2001).

A number of studies have examined the impact of duration of protection (i.e., the time period during which the vaccine protects against the infectious disease) as a factor influencing preference. In studies of preferences for HPV vaccines, respondents preferred a vaccine with lifetime protection (Brown et al., 2010; Oteng et al., 2011). Preference for lifetime HPV protection was more than double the preference for a vaccine with only 5 years of protection (Brown et al., 2010). In a study of adolescent girls, duration was the second most important attribute for HPV vaccines (following effectiveness) (de Bekker-Grob et al., 2010). Preference for an HIV vaccine increased by 14% for protection of 10 years versus 1 year (Newman et al., 2009), and respondents were willing to pay more for a meningococcal vaccine with longer duration (Bishai et al., 2007).

Administration characteristics may also influence preferences for vaccines, although these factors are generally less important than the factors discussed above. In a study of HIV vaccines, Newman et al. (2009) reported that going from oral to injection administration decreased vaccine preference by 6%, while going from a vaccine requiring one dose to a vaccine requiring four doses decreased preference by 8%.

Physician recommendations for a particular vaccine have also been reported to influence vaccine preference, although the impact of physician recommendations is less than that for most other factors (Flood et al., 2011). However, in a study of gynecologists, recommendation of an HPV vaccine by the American College of Obstetricians and Gynecologists (ACOG) was the second most important factor (Raley et al., 2004).

Vaccines may offer protection against a single strain of virus or bacteria, or may provide coverage against multiple strains. Increased breadth of coverage (or antigenic protection) was associated with greater preference for a meningococcal vaccine (Bishai et al., 2007). However, increased breadth of antigenic coverage did not significantly influence preference for an HIV vaccine (Newman et al., 2009).

Infectious Agent/Threat Characteristics Affecting Preference

Characteristics of the infectious agent that is the target of the vaccine, or the sequellae of infections, may also influence vaccine preference. The ability to prevent more serious diseases is generally associated with increased preference. Severity of the disease being prevented (curable vs. chronic vs. fatal) was rated as the most important characteristics for adult vaccines

(Stockwell et al., 2011). Vaccines preventing fatal illness were also more preferred than those preventing curable or chronic illness in a study of parental preference for vaccines for their adolescent children (Zimet et al., 2005); this was the second most important vaccine characteristic, after efficacy. In a Canadian study of an HPV vaccine, participants indicated a willingness to pay (WTP) of $C22 for a 1% reduction in the risk of genital warts, a topical effect of HPV infections. However, respondents were willing to pay more than twice this amount ($C55) for a 1% reduction in the risk of cervical cancer, a serious complication potentially resulting from HPV infections (Oteg et al., 2011).

Infectious diseases may be (very broadly) transmitted sexually (i.e., sexually transmitted infections, or STIs) or nonsexually. In examining attitudes by adult women toward vaccines, vaccines targeting STIs versus other types of infections did not affect preference (Stockwell et al., 2011). STI versus non-STI infections also had no significant impact of preferences by parents for vaccines for their adolescent children (Zimet et al., 2005). Similarly, having a behavioral option to avoid infectious diseases (e.g., not engaging in high-risk behaviors or not going to high-risk locations) was not shown to affect vaccine preference (Stockwell et al., 2011).

User/Recipient Characteristics Affecting Preference

Most studies also examine whether characteristics of potential vaccine recipients (or users, with respect to cyber security) influence preference or willingness to pay for a vaccine. However, results have been inconsistent. In a study of a meningococcal vaccine, income and perceived risk (of meningitis) did not affect vaccine preference (Bishai et al., 2007). However, Brown et al. (2010) found that income and concern about risk influenced choices among mothers for vaccinating their daughters for HPV.

Brown and colleagues (2010) also found that age, race, education, and previous exposure to the infection agent (in this case, HPV) influenced vaccine choices. Liau & Zimet (2001) also found age to significantly influence preferences for an HIV vaccine, with younger participants in the study more likely to give higher ratings to a vaccine. However, Zimet et al. (2005) reported that parental age did not affect preferences for vaccines for their adolescent children; parental education and insurance did affected preference level. In their study of meningococcal vaccine preferences, Bishai et al. (2007) also reported that increased knowledge about the infectious agent (meningococcus) led to less preference for the vaccine, perhaps because this knowledge included information on strains of the bacteria that were not present locally.

Individuals from different countries may have substantial differences in preferences. Bishai et al. (2007) found that German participants were much more price sensitive than were French in a study of meningococcal vaccine preference.

Social saturation, or the proportion of a population already vaccinated, may also affect vaccine preference. As discussed earlier in this section, greater saturation increases the

likelihood of herd immunity, and might therefore be assumed to decrease preference for a vaccine. However, increasing social saturation from 10% to 90% for an HIV vaccine significantly increased vaccine preference (Liau & Zimet, 2001).

2.2 Understanding Antimalware Risk Preferences

Antimalware is software used to prevent, detect, and remove malicious software, referred to as malware. It is an effective means to increasing the security (cyber security) of a computer or network of computers. There are numerous types of antimalware software on the market, ranging from free trial versions for home use to paid versions for large institutions. In all antimalware software, the explicit purpose is to prevent, detect, and remove unwanted and potentially harmful (malicious) software. As the number and sophistication of malware programs grows, so does the need for a preventive solution. Antimalware provides both a systematic and individual-level preventive solution for safeguarding against the increasing threat and burden of malware.

There are number of types of malware programs that threaten the health and performance of a computer (or computer network). Some of the more prevalent malware programs that antimalware is designed to defend against are the following:

- Computer viruses—software (often attached to legitimate programs or e-mail messages) that can cause harm to computers and can replicate themselves and spread from one computer to another.
- Computer worms—programs that infect computers by using “holes” in computer software and can cause harm to a computer.
- Trojan horses—malware that appears to be legitimate files and claims to do one thing (e.g., initiate a game) but instead can cause harm to a computer when it is run.
- Spyware—malware installed on computers used to collect information about computers’ users without their knowledge.

These four malware programs are not an exhaustive list but they do represent the vast majority of malware programs that currently jeopardize cyber security.

Antimalware Characteristics

Antimalware software programs can be differentiated by a number of characteristics including price, performance, and ease of use. However, given that robust security metrics do not currently exist, measuring and comparing features is generally done qualitatively. Consumer Reports (2012) compares antimalware software programs through eight metrics[1] as follows:

[1] A full description of the metrics used for comparison can be found here: http://www.consumerreports.org/cro/security-software.htm.

1. **price**—the cost to download the program and use it on up to 3 computers, for the first year
2. **ease of use**—installation, changing setting, and interacting with the software
3. **resources**—use of memory and tendency to slow computer operation during a scan
4. **net threats**—how well the product protected against list exploits on websites
5. **virus scan**—effectiveness scanning the PC for malware both online and offline
6. **scan speed**—how fast the software can scan a large group of files for threats
7. **updating**—how quickly the product is able to protect against new malware
8. **performance**—how well the software stopped rogue connections to and from the Internet

The first 3 metrics could be classified as "cost" metrics—the monetary and non-monetary costs associated with using antimalware software—whereas the last 5 metrics could be classified as "benefit" metrics—each providing a measure of how well the software will product the host computer from security threats. Combined, these eight metrics can be used to help determine what specific antimalware software may be appropriate for an individual.

In addition to these attributes, several more characteristics may be useful to consider when reviewing antimalware programs.

- time spent each month using antimalware software (cost)
- positive impact of the antimalware on computer performance—i.e., improved speed and potentially reduced risk of a computer slowing down or crashing (benefit)
- reduced risk of computer owner's identity being stolen (benefit)
- reduced risk to other individuals and businesses from malware that has gotten on a user's computer (benefit)

Some of these metrics may be extremely difficult to compare between antimalware software programs, but broadly all of the benefits and costs mentioned above should be considered in order to assess the overall economic value of antimalware software as a group or looking at individual packages.

Antimalware Market and Products

The antimalware software market has steadily grown over the past several years, with software application companies attempting to keep up with the growing number of malware threats jeopardizing cyber security (OPSWAT, 2012). In 2012, an online survey of 358 PC users and 315 Mac users conducted by the technology news website Betanews (Wilcox, 2012) estimated that 90% of PC users have some sort of security software (e.g., antimalware) installed on their computers, whereas an 75% of Mac users do not. Moreover, according to

results from the same survey conducted in 2011, 86% of PC users were estimated to have antimalware installed and 81% of Mac users were estimated not to have antimalware installed, an increase of 4% and 6%, respectively. As threats increase, it seems more and more computer users are turning to antimalware software as a preventive solution.

According to a recent report by OPSWAT, a company based in San Francisco that provides software tools and data to software engineers, in 2012, 10 software application companies made up over 87% of the worldwide market share of antivirus software products, and the top 10 specific products make up 64.94% of the worldwide market share. Many of these products are free to download and install (i.e., users did not have to pay a monetary price for the antimalware product) with the top three worldwide products available for free download. In addition to the software packages available for free download, many antimalware packages charge a price (generally an upfront cost and an annual fee to provide regular updates) for protection. The following are the top 10 products worldwide:

1. Avast! Free Antimalware (11.91%)
2. Microsoft Security Essentials (9.96%)
3. Avira Antivirus Personal – Free Antivirus (9.75%)
4. AVG Antivirus Free Editions (6.83%)
5. ESET NOD32 Antivirus (6.75%)
6. Norton Antivirus (5.00%)
7. Kaspersky Internet Security (4.62%)
8. AVG Antivirus (4.19%)
9. McAfee VirusScan (3.34%)
10. ESET Smart Security (2.59%)

In addition to antimalware that is provided free by the producers of the software, many companies have begun providing antimalware free to their clients. Most Internet service providers (ISPs) and many banks provide free antimalware software to their customers, and Facebook provides free antimalware software to any of its users. However, research by Rowe et al. (2011) indicates that the use of such software is not as high as might be expected given the cost.

Antimalware Preferences

An individual users' decision to use antimalware is influenced by a variety of factors, including whether they think that they might be a target of a cyber attack (are they *afraid*) and whether they *trust* that antimalware software would provide a net benefit to them based on the subset of the costs and benefits delineated above. Beyond these overarching issues, factors such as age, type of computer used, income level, and risk aversion can influence an individual's preference for antimalware software. For example, as noted above, Mac users

have been less likely to purchase antimalware software than PC users in the past (Betanews, 2012).

Although robust cyber security risk preference research is sparse, Ng et al. (2008) surveyed 238 home Internet users and found that individuals stated intent to practice good cyber security behaviors was most influenced by perceptions of the usefulness of the behavior (does the user think the behavior will improve security) and self-efficacy (does the user think he or she can correctly perform the requested behavior), as well as family and peer opinions news and other media information.

Given that many antimalware software products are being offered for free, cost is likely to be less of a factor for many individuals deciding whether to use a certain antimalware software product. However, without objective metrics to easily assess the nonmonetary costs and benefits of antimalware, individuals' *perceptions* of the net effect of the combination of costs and benefits of antimalware are likely used by individuals to make their decision.

---

3. Developing a Research Study of Cyber Security Risk Preferences

To assess how cyber security risk preferences can be better understood by leveraging research on public health risk preferences, we developed an example scenario for comparison purposes. Table 1 provides a summary of certain characteristics that vaccines and antimalware software share. In public health, vaccines are a type of primary intervention aimed at individuals. Vaccines are not 100% effective, although rates of protection must meet a certain threshold before a vaccine is approved for use. Often, multiple vaccinations are required to achieve optimal levels of protection. Vaccines typically require investments of both time and money, the level of which depends on the number of doses needed, the price set by the manufacturer, and any applicable health insurance or public assistance. In some cases vaccines can be free or close to free. Further, vaccines may have or be perceived to have negative consequences (side effects). The duration of protection following receipt of a vaccine is generally multiple years, and some vaccines offer protection against multiple "strains" of an infectious disease.

The likelihood of someone getting vaccinated (or having his or her child vaccinated) depends in part on perceived risk/vulnerability—how likely is it that he or she would get this illness, and if infected, how severe or serious is the disease. This perceived risk may be largely subjective, based on beliefs about potential exposures to the infectious disease agent, previous experience with vaccines and with the specific infections, and general attitude toward risk. A, the source of a recommendation to be vaccinated may influence the likelihood of receiving the vaccine; recommendations from sources such as physicians and well-known

public health organizations likely increase trust and thereby increase the likelihood of vaccination.

Computer antimalware software shares many characteristics with health vaccines. Computer antimalware software is not totally preventive—usually "updates" are needed to boost efficacy against new threats, similar to booster shots for some vaccines. Most vaccines last years, as does antimalware software targeted at specific threat signatures. However, whereas vaccines can sometimes be preventive against threats (e.g., viruses) similar to the targeted virus, antimalware software is more like the syringe in which the vaccine is delivered. Antimalware updates (periodic software downloads) are used to load more threat signatures so that additional threats can be thwarted.

Table 1. Comparing Characteristics of Health Vaccines With Antimalware Software

Characteristic	Vaccines	Antimalware Software
Level of prevention (effectiveness)	Variable (often less than 75%)	Variable
Number of doses/updates needed	Often multiple	Multiple, ongoing
Duration of preventive effect	Years	Years
Ability to simultaneously protect against multiple types of related threats	Seen with certain vaccines such as influenza vaccines ("cross-clade" protection)	Antimalware software is constantly updated, providing the equivalent of a new vaccine or set of vaccines on a weekly or monthly basis.
Cost factors	Price of shot(s), number of doses, insurance coverage, public assistance programs	Price of software, price of annual subscription, availability through an ISP
Negative consequences	Nausea and other potential side effects	Computer performance may decrease slightly
Perceived risk/vulnerability of recipient	Depends on past experience, potential exposures, and attitude toward risk	Depends on past experience, value of data/resources, and attitude toward risk
Source of recommendation for use	Physicians*	ISPs, computer manufacturers, etc.

* Note: More use of vaccines has been seen with recommendations from trusted sources such as physicians.

Antimalware software usually costs money to purchase and a subscription fee to receive updates. However, as with vaccines, antimalware software may be subsidized, for example by ISPs who may offer free or discounted antimalware software to their customers. The primary negative consequences of antimalware software would be the potential for computers' performance to be reduced and desired software downloads or websites to be impeded.

Finally, the perceived risk of recipients of vaccines and antimalware software depends on similar things—past experience (knowledge of threat), perceived exposure risk, knowledge of

potential risk averting behaviors, and general attitude toward risk—and both have trusted parties to which they look for recommendations.

The comparison between vaccines and antimalware software offers an explicit opportunity to assess the relative risk preferences for cyber security solutions. As has been done with past research of vaccines, risk preference research related to antimalware could be used to improve communication/marketing strategies, rates of adoption, and levels of protection against cyber threats, and could possibly affect funding/pricing.

---

4. Study Methodology

The primary goal of this study was to develop a stated-preference survey instrument that quantified how much the various costs and benefits of using antimalware software influenced software choice. However, there are multiple survey approaches that could be pursued to achieve this goal. Therefore, to determine the best survey approach for this study, we reviewed the different approaches that have been used by public health researchers to quantify how vaccine attributes influence individuals' vaccine choices.

Based on this literature review, we identified two possible survey approaches—a *ratings-based approach* and a *choice-based approach*, both stated-preference survey techniques. Under the ratings-based approach, respondents are shown a series of hypothetical vaccines and asked to rate how willing they would be to use each vaccine (typically on a scale from 0, "I will never get this vaccine", to 100, "I will definitely get this vaccine"). In surveys that used this approach, each vaccine differed in terms of their specific attributes—including the potential benefits (e.g. vaccine efficacy) and potential costs (e.g. side effects). Based on how survey respondents rated each vaccine, researchers conducted a statistical analysis to determine which vaccine attributes had the greatest influence on whether the respondent would be willing to take the vaccine. Examples of studies that used this approach include Zimet et al (2005) and Liau and Zimet (2001).

The second stated-preference survey approach that we identified in the literature, the choice-based approach, was very similar to the ratings-based approach. Again, survey respondents were shown hypothetical vaccines that differed based on a series of attributes. However, instead of rating their willingness to take each vaccine, they were asked only whether or not they would take the vaccine. Based on these choices, researchers could apply statistical methods to determine which attributes were most important in determining whether or not a respondent would choose a vaccine. In addition, if the price of the vaccine was included as a vaccine attribute, researchers could estimate how much respondents would be willing to pay (on average) for improvements in each attribute or how much they would be willing to pay for a hypothetical vaccine itself. Examples of studies that used this approach include Bishai et al (2007), de Bekker-Grob et al (2010), and Brown et al (2010).

For the purposes of this study we decided that developing a choice-based stated-preference approach would be the most appropriate for two reasons. First, antimalware software is sold in a competitive market where consumers can choose to either buy or not buy a software product. Therefore, we believed a choice-based appropriate would be more realistic and more intuitive for survey respondents. Second, a choice based approach allows us to estimate how much respondents are willing to pay for improvements in antimalware attributes and hypothetical antimalware products. We believe these sorts of results are more intuitive to understand and also easier for making comparisons of how important an attribute is in a respondent's decision making process and also whether they would prefer one hypothetical vaccine to another.

In order to operationalize the choice-based conjoint approach for this study, we first identified the key costs and benefits that are most important to survey respondents. That is to say, we wanted to identify which software attributes contribute to individual survey respondents' well-being (also known as their utility). Identifying these attributes was crucial because they formed the basis of the hypothetical software products between which we asked survey respondents to choose.

We begin the task of identifying the most important software attributes with the lists of characteristics of antimalware described in Section 2.2. Although all of these attributes could be considered important to an individual's decision to choose one software product over another, it would be impractical to include all of them as software attributes in our choice-based survey design. This is because we eventually used these attributes to create hypothetical software products that respondents had to evaluate, and it seems unreasonable to ask these respondents to weigh more than 6 attributes in making their decision. Therefore, we focused on a set of 3 costs and 3 benefits which we believed were most representative of the factors that would most affect individuals' perceptions of antimalware. These include:

- initial price of the software itself (cost),
- time spent regularly using the antimalware software (cost),
- changes in computer speed after installing software (cost),
- reduced risk of malware crashing a user's computer (benefit),
- reduced risk of identity theft (benefit), and
- reduced risk to others from malware on a user's computer (benefit).

Although little past research exists to confirm our belief that these are the software attributes most important for antimalware consumers, we used several of the same characteristics that Rowe et al (2011) found as having a significant impact on individuals' perceptions of cyber security solutions provided by Internet service providers. Assuming these six characteristics are the primary factors affecting utility associated with antimalware, we can conceptualize the user's utility as a function that takes the form of

$$U = f(P, T, S, C, I, O)$$

where P is the initial price paid for antimalware software, T is time users must spend using antimalware software each month, S is speed of a user's computer after installing the software, C is the risk of malware crashing a user's computer, I is the risk of identity theft, and O is the risk to others from malware on a user's computer.

We hypothesize the following:

- that decreases in the cost of the software will increase personal utility ($\partial U/\partial P < 0$),
- decreases in the time spent each month using the software will increase personal utility ($\partial U/\partial T < 0$),
- decreases in the speed of a user's computer after installing the software will decrease utility ($\partial U/\partial S > 0$),
- decreases in the risk of malware crashing a user's computer will increase utility ($\partial U/\partial C < 0$),
- decreases in the risk of identity theft will increase utility ($\partial U/\partial I < 0$), and
- decreases in the risk others will be harmed from malware on a user's computer will increase utility ($\partial U/\partial O < 0$).

In our study, we operationalize this conceptual model using choice-based conjoint analysis, which is a stated-preference survey method in which survey respondents are asked to choose between hypothetical products.

The survey instrument used for this study was developed by a core research team composed of experts in public health and cyber security and economists experienced in using stated-preference survey methods to study security-related issues.[2] In the following sections, we describe this survey instrument and our study's methods in greater detail. First, we describe the questions we asked respondents regarding their computer usage habits and opinions related to cyber security (Section 4.1). Second, we describe the conjoint portion of the survey (Section 4.2). Lastly, we describe two statistical methods we use to analyze the data we collected from the survey instrument.

4.1 Questions on Respondent Computers, Computer Usage Habits, and Views Related to Cyber Security

We asked survey respondents a variety of questions about the computers they own and how they use them, and their views of the threat of cyber security and possible solutions. All of the questions in these sections fit in to the following categories:

[2] We tested the draft instrument through cognitive interviews with a small group of individuals from the Research Triangle area of North Carolina and the San Francisco area of California. These interviews led to a number of revisions to question wording and presentation to make the instrument easier for respondents to understand.

- Regular activities (online/offline)
- Experience with threat
- Familiarity with prevention mode of interest
- Past / current use of prevention mode of interest
- Experience with impact of successful threat
- Demographic characteristics
- Level of risk aversion

Most of these questions were posed at the beginning of the survey, prior to the state-preference questions described below.

Of note, we developed the above list of categories of interest and the related actual questions included in the survey used to investigate these areas through analyzing similar public health studies of risk preference. Specifically, we used many of the same types of questions found in vaccine stated-preference studies. For instance, we asked questions assessing risk such as, “Do you smoke?” or “Do you wear a seat belt?” to provide baseline comparisons across differing groups of individuals. Both of these questions were pulled directly from the survey conducted by Brown et al. (2010). By developing our survey in this way were able to both build on the extensive past research experience in risk preference analysis and design a survey that would allow for our study’s results to be compared across other bodies of risk preference research, particularly that of vaccinations. Regarding the background questions we asked in our survey, Table 2 provides a comparison between questions we asked and similar questions asked in past surveys focused on vaccine risk preferences.

Table 2. Comparing Questions Asked in Antimalware Risk Preferences Survey with Questions Asked in Similar Vaccine Risk Preferences Surveys

Information of Interest	Types of Questions Asked in Antimalware Software Survey	Types of Questions Asked in Vaccine Survey
Relevant activities	Regular computer usage habits	Habits / regular daily activities
Past exposure to threat	Past exposure to malware	Past exposure to health viruses
Familiarity with / opinions of prevention mode	Familiarity with / opinions of antimalware	Familiarity with / opinions of vaccines
Experience with prevention mode	Experience with antimalware software	Experience with vaccines
Experience with impact of successful threat	Experience with identity theft and computer performance issues	Experience with health impact of viruses
Demographic characteristics	Demographic characteristics	Demographic characteristics
Level of risk aversion	Level of risk aversion	Level of risk aversion

4.2 Stated-Preference Questions

Ten stated-preference questions form the core of the survey (see Figure 1 for an example). These questions can be separated into three groups:

- One Warm-Up Question: answers to this question were not used in our analysis because it was designed exclusively to help respondents become more familiar with answering stated-preference questions.
- Seven Analysis Questions: answers to these questions were used in the statistical analysis described below to estimate a model of consumer preferences.
- Two Internal Validity Test Questions: answers to these questions were exclusively used to test the validity of the model estimated using the seven analysis questions.

Each of the 10 questions described two hypothetical antimalware software products. After respondents selected which of the two hypothetical products they most preferred, they were asked if they would actually buy the product they selected for their personal computer.

Figure 1. Example Choice Task

	Product A	Product B
Costs of Antimalware Software		
Price for one year of antimalware software service.	$10	$40
Time spent each month using antimalware software	0 hours per month	0 hours per month
Speed of computer performance after installing antimalware software	No Change	No Change
Benefits of Antimalware Software		
Risk of your computer slowing down or crashing	Not Reduced	Greatly Reduced
Risk of your identity being stolen	Somewhat Reduced	Somewhat Reduced
Risk to other individuals and businesses from malware on your computer	Somewhat Reduced	Somewhat Reduced
If these were the only options available, which would you choose?	☐	☐
Suppose you were actually offered this antimalware software product in real life. Would you buy it for use on your CURRENT PERSONAL COMPUTER? ☐ Yes ☐ No		

We presented each hypothetical antimalware software product as being composed of the six costs and benefits (known as product "attributes") listed above. These attributes were based on our previous discussion for conceptualizing broadband user utility. Specifically, the following three attributes were used to describe the costs of using a particular antimalware software product:

- Price for one year of antimalware software service
- Time spent each month using antimalware software
- Speed of computer performance after installing antimalware software

Similarly, the following three attributes were used to describe the benefits of using a particular antimalware software product:

- Reduced risk of your computer slowing down or crashing
- Reduced risk of your identity being stolen
- Reduced risk to other individuals and businesses from malware on your computer

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 that the average broadband user would understand.

We attempted to create levels for each of the six attributes so that they would include the range of plausible extremes. For the price attribute, we made this determination by reviewing the prices for actual antimalware software products that range from $0 (such as the free edition of AVG) to as high as $80-$90 (such as Norton 360 or McAfee All Access 2012). Because many of the more expensive software products included features beyond antimalware protection (such as automatic data backup and technical support), we believed that $80 should serve as an adequate upper bound.

To identify a range of levels for the time attribute, we used data collected from our previous study on cyber security (IHSS, 2011). In that previous study, we found that approximately 23% of respondents spent an average of 40 minutes or more each month, but that the vast majority (77%) spent less. Therefore, it seemed plausible that the most time that a typical individual would be willing to spend using antimalware software would be around 40 to 60 minutes each month.

Choosing levels for the speed attribute proved to be particularly difficult given that users may assume that antimalware software would improve the speed of their computer (as we address in one of the benefits metrics), but they may be less familiar with the negative (cost) impact of antimalware software on slowing initiation or running of other programs. We considered using quantitative measures of how much installing antimalware software could reduce computer speed (for example, saying that installing antimalware software would decrease a computer's performance by 20%), but we were concerned that respondents would find this framing difficult to comprehend. Therefore, three qualitative levels were chosen to indicate whether the antimalware product in question greatly slowed down their computer, somewhat slowed down their computer, or did not change the speed of their computer at all.

We faced similar concerns when choosing the levels for the three benefit attributes. Therefore, we made a similar decision to choose three qualitative levels for each attribute to

indicate whether the antimalware product in question greatly reduced malware threats, somewhat reduced threats, or did not reduce threats at all. Similar qualitative levels were used in a past survey that focused on assessing broadband Internet users' demand for ISP-provided security solutions (Rowe et al., 2011). In developing this survey, we reviewed alternative approaches (e.g., quantitative levels) but determined that survey respondents would have a difficult time appropriately weighting the levels when making a decision between hypothetical products. A summary of the attributes and levels used in the final survey instrument are presented in Figure 2.

Figure 2. Attributes and Levels

Strategy	Short Description in Survey
Price	When you purchase antimalware software, the initial price you pay typically covers one year of up-to-date protection against malware. Later in the survey we will ask you to choose between hypothetical antimalware software products that differ based on how much they cost for one year of protection against malware. The prices of these hypothetical antimalware software products will be one of the following: • $0 • $10 • $40 • $80 In actuality, some people pay for their antimalware software while some people use "freeware" antimalware program or get their antimalware software for free through their Internet Service Provider (ISP), Facebook, or bank. In this survey, when we show you hypothetical scenarios, please assume you would pay the full prices shown and select your preferred option accordingly.
Time spent each month using antimalware software	Each month you may spend time maintaining and using your antimalware software. This includes taking time to update your virus definitions and scanning your computer for viruses. Later in the survey, we will ask you to choose between several hypothetical antimalware software products that differ in terms of the amount of time required to maintain and use the antimalware software properly. The amount of time you will be asked to spend per month using these hypothetical antimalware software products will be one of include the following options: • 0 minutes per month • 10 minutes per month • 40 minutes per month • 60 minutes per month

(continued)

Figure 2. Attributes and Levels (continued)

Strategy	Short Description in Survey
Speed of computer performance after installing antimalware software	Using antimalware software can sometimes slow down your computer (i.e., slow how fast programs run on your computer). This is because the software regularly scans files you download to your computer, checks for software updates, and performs other duties that divert resources away from other activities. Later, we will ask you to choose between hypothetical antimalware software products that differ in terms of how much they change the speed of your computer's performance. The change in speed of your computer's performance associated with each hypothetical software product will be one of the following: • No Change—Antimalware software will not change the speed of your computer's performance • Somewhat Slows Down—Antimalware software will somewhat slow down the speed of your computer's performance • Greatly Slows Down—Antimalware software will greatly slow down the speed of your computer's performance
Reduced risk of your computer slowing down or crashing	The purpose of antimalware software is to reduce threats to cyber security. One way to judge the effectiveness of these software packages is whether they reduce the risk of malicious software slowing down or crashing your computer. For example, antimalware software could help to ensure that your computer applications—such as your Internet browser, e-mail, or word processing software—do not run slower as a result of malware. Later in the survey, we will ask you to choose between antimalware software products that differ in terms of how much they reduce the risk of your computer slowing down or crashing due to malware. The following options will be shown: • Not Reduced—the risk of your computer slowing down or crashing will not be reduced (that is, it will be the same as before you installed the antimalware software) • Somewhat Reduced—the risk of your computer slowing down or crashing will be somewhat reduced • Greatly Reduced—the risk of your computer slowing down or crashing will be greatly reduced
Reduced risk of your identity being stolen	Another way to judge the effectiveness of antimalware software is whether it reduces the risk of having your identity stolen (e.g., your credit card, Social Security number, bank account number being used without your permission to commit fraud or other crimes). Later in the survey, we will ask you to choose between antimalware software products that differ in terms of how much the risk of your identity being stolen has been reduced. The amount each hypothetical antimalware software product will reduce the risk of your computer slowing or crashing will range between: • Not Reduced—the risk of your identity being stolen will not be reduced (that is, it will be the same as before you installed the antimalware software) • Somewhat Reduced—the risk of your identity being stolen will be somewhat reduced • Greatly Reduced—the risk of your identity being stolen will be greatly reduced

(continued)

Figure 2. Attributes and Levels (continued)

Strategy	Short Description in Survey
Reduced risk to other individuals and businesses from malware on your computer	The level of security on your computer can also have an impact on other people. For example, if your computer is infected with malware, then it is possible that your computer may be hijacked and used to attack businesses or other home Internet users. This could mean that businesses have data stolen or their computer systems stop working for a period of time because your computer was used to attack them, or that your computer puts other individual computer users at a higher risk of being infected or having their identity stolen. Later in the survey, we will ask you to choose between antimalware software products that differ in terms of how much the risk to other individuals and businesses from malware on your computer has been reduced. The amount each hypothetical antimalware software product will reduce the risk to others from malware on your computer will range between: • Not Reduced—the risk to other individuals and businesses will not be reduced (that is, it will be the same as before you installed the antimalware software) • Somewhat Reduced—the risk to other individuals and businesses will be somewhat reduced • Greatly Reduced—the risk to other individuals and businesses will be greatly reduced

Given the six attributes and levels described above, 1,296 (4 x 4 x 3 x 3 x 3 x 3) possible hypothetical packages 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 attribute being considered is assumed to add linearly to a person's utility. When this assumption is made and a proper subsample of the 1,296 hypothetical package profiles is chosen (this subsample is 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 that possesses several properties (Kanninen, 2002; Zwerina, Huber, & Kuhfield, 1996), such as the following:

- Level balance: The 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.

Unfortunately, it is often impossible 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 (Sawtooth, 2010).

Statistical Analysis

As part of this study we attempt to quantify the preferences of U.S. broadband Internet users for antimalware software. However, the data collected through the survey described above do not allow us to quantify Internet user preferences directly because we only observe the choices they make between hypothetical antimalware software products. Instead, we can only quantify these preferences if we make a series of assumptions regarding the average Internet user's utility function. Specifically, we estimate Internet user preference parameters using a Random Utility Maximization (RUM) model.

The RUM model assumes that utility is defined as a function of the six attributes used to define a hypothetical antimalware software product and some random component. More formally, we define the utility a person receives from antimalware product *j* on choice task t by

$$u_{jt} = v_{jt}(\mathbf{X}_{jt}) + \varepsilon_{jt},\ j = 0, 1, 2,\ t = 1,\ldots,7, \qquad (3.1)$$

where v_j is the deterministic (observable) component of utility that depends on the attribute levels that compose antimalware product *j* in choice task t (represented as the vector $\mathbf{X}_{jt}$) and ε_j is a random error that represents the component of utility that is unobservable to the researcher.

We follow convention and assume that the deterministic portion of the utility function (v_j) follows a linear specification for utility such that preferences for the three alternatives on a given choice occasion are given by

$$\begin{aligned}
&U_{antimalware_package} = (\beta_{\$0} + \beta_{\$10} + \beta_{\$40} + \beta_{\$80})^* \boldsymbol{x}^i_{\mathbf{price}} + \\
&(\beta_{0min} + \beta_{10min} + \beta_{40min} + \beta_{60min})^* \boldsymbol{x}^i_{\mathbf{time}} + \\
&(\beta_{greatly_slowed} + \beta_{somewhat_slowed} + \beta_{no_change})^* \boldsymbol{x}^i_{\mathbf{speed}} + \\
&(\beta_{not_reduced} + \beta_{somewhat_reduced} + \beta_{greatly_reduced})\, \boldsymbol{x}^i_{\mathbf{comp_crash}} + \\
&(\beta_{not_reduced} + \beta_{somewhat_reduced} + \beta_{greatly_reduced})\, \boldsymbol{x}^i_{\mathbf{ident_theft}} + \\
&(\beta_{not_reduced} + \beta_{somewhat_reduced} + \beta_{greatly_reduced})\, \boldsymbol{x}^i_{\mathbf{risk_to_others}} + \\
&\varepsilon_{antimalware_package} \qquad (3.2)\\
&U_{neither_product} = \beta_0 * D_{neither_product}{}^i + \beta^i_{neither_product}
\end{aligned}$$

where $\boldsymbol{x}^j_{\boldsymbol{price}}$ is a vector of four indicator variables for different levels of the "price" attribute, $\boldsymbol{x}^j_{\boldsymbol{time}}$ is a vector of four indicator variables for different levels of the "time" attribute, $\boldsymbol{x}^i_{\mathbf{speed}}$ is a vector of three indicator variables for different levels of the "computer speed" attribute, $\boldsymbol{x}^i_{\mathbf{comp\_crash}}$ is a vector of three indicator variables for different levels of "improved computer performance" attribute, $\boldsymbol{x}^i_{\mathbf{ident\_theft}}$ is a vector of three indicator variables for the "reduced risk of

identity theft" attribute, $\boldsymbol{x}^{i}_{\text{risk\_to\_others}}$ is a vector of three indicator variables for the "reduced risk to other individuals and businesses from your insecurity" attribute, and $D_{\text{neither\_product}}^{i}$ is an indicator variable equal to 1 if alternative *i* is "neither product."

The RUM model presented above was estimated using a conditional-logit model in Stata 11.[3] In this estimation, the indicator variables were entered as effects coded variables[4]. A primary advantage of this approach is that it allows us to interpret the β parameters can be interpreted as relative importance weights (also known as part-worth utilities), where larger values of β indicate greater utility.

In addition to quantifying preferences, we also seek to estimate how much U.S. broadband Internet users are willing to pay for improvements in individual product attributes and how much users are willing to pay for entire hypothetical software products. To do this we estimate another specification that treats price and time as continuous variables. Specifically, we estimate the following:

$$
\begin{aligned}
&U_{\text{antimalware\_product}} = \beta_{\text{price}} * \boldsymbol{price}^{i} + \beta_{\text{time}} * \boldsymbol{time}^{i} + \\
&(\beta_{0\text{min}} + \beta_{10\text{min}} + \beta_{40\text{min}} + \beta_{60\text{min}}) * \boldsymbol{x}^{i}_{\text{time}} + \\
&(\beta_{\text{greatly\_slowed}} + \beta_{\text{somewhat\_slowed}} + \beta_{\text{no\_change}}) * \boldsymbol{x}^{i}_{\text{speed}} + \\
&(\beta_{\text{not\_reduced}} + \beta_{\text{somewhat\_reduced}} + \beta_{\text{greatly\_reduced}})\, \boldsymbol{x}^{i}_{\text{comp\_crash}} + \\
&(\beta_{\text{not\_reduced}} + \beta_{\text{somewhat\_reduced}} + \beta_{\text{greatly\_reduced}})\, \boldsymbol{x}^{i}_{\text{ident\_theft}} + \\
&(\beta_{\text{not\_reduced}} + \beta_{\text{somewhat\_reduced}} + \beta_{\text{greatly\_reduced}})\, \boldsymbol{x}^{i}_{\text{risk\_to\_others}} + \\
&\varepsilon_{\text{antimalware\_product}} \qquad (3.3) \\
&U_{\text{neither\_product}} = \beta_{0} * D_{\text{neither\_product}}^{i} + \beta^{i}_{\text{neither\_product}}
\end{aligned}
$$

where $\boldsymbol{\text{price}}^{i}$ is the price of alternative i, $\boldsymbol{time}^{i}$ is the time associated with complying with ISP security requirements in alternative i, $\boldsymbol{x}^{i}_{\text{speed}}$ is a vector of three indicator variables for different levels of the "computer speed" attribute, $\boldsymbol{x}^{i}_{\text{comp\_crash}}$ is a vector of three indicator variables for different levels of "improved computer performance" attribute, $\boldsymbol{x}^{i}_{\text{ident\_theft}}$ is a vector of three indicator variables for the "reduced risk of identity theft" attribute, $\boldsymbol{x}^{i}_{\text{risk\_to\_others}}$ is a vector of three indicator variables for the "reduced risk to other individuals and businesses from your insecurity" attribute, and $D_{\text{neither\_product}}^{i}$ is an indicator variable equal to 1 if alternative *i* is "neither product."

[3] We use a standard conditional logit model which assumes that the disturbance term follows a Type I extreme-value error structure and uses maximum-likelihood methods to estimate the parameters.

[4] Effects coding is a common way to use categorical variables in estimation models, such as, linear regression. In effects coding a group of data is converted to ones, zeros and minus ones to convey all of the necessary information on group membership and the actual values become the dependent variable.

As before, the RUM model presented above was estimated using a conditional-logit model in Stata 11. However, in this estimation, variables price and time were entered as continuous variables in the regression, while indicator variables for the other four attributes were entered as effects coded variables. A primary advantage of this approach is that it allows us to interpret ($-\beta_{price}$) as the marginal utility of income and ($-\beta$time) as the marginal utility of time (the remaining β parameters can be interpreted as part-worth utilities as before).

Using the β parameters estimated from the second model specification we can measure how much the average broadband user is willing to pay for changes in the levels of a particular attribute (also known as a marginal WTP). A marginal WTP can be estimated by dividing the difference between the part-worth utilities of the two attribute levels in question by the marginal utility of income.

For example, the mean marginal WTP to move from a product that does not reduce the risk of your computer slowing down or crashing to a product that greatly reduced this risk would be calculated taking the difference between the part-worth utilities for these two levels divided by the marginal utility of money: $[(\beta_{not\_reduced} - \beta_{greatly\_reduced})/(-\beta_{price})]$.[5] Standard errors and confidence intervals for these estimated marginal WTP measures were estimated using a Krinsky-Robb bootstrapping procedure with 10,000 iterations (Krinsky and Robb, 1986; Krinsky and Robb, 1990).

In addition to estimating marginal WTPs, we can also estimate the maximum amount the mean Internet user would be willing to pay for a hypothetical antimalware product relative to having no product. For the purposes of this study, we consider the product that would be most preferred by home Internet users. This package would include 0 hours each month using the software, the speed of the user's computer would not change, the risk of the user's computer slowing down is greatly reduced, the risk of identity theft is greatly reduced, and the risk to other individuals from user insecurity is greatly reduced. Although this package would likely be unfeasible from the perspective of actual antimalware software developers, the WTP estimated for this package would represent the most Internet users would ever pay for antimalware software. The maximum amount Internet users would be willing to pay for this product can be calculated by estimating the difference between the total utility this product yields and the total utility a no-product alternative yields, which is done using what is known as the "log-sum" formula (derived in Train, 2003). For example, say we wanted to estimate the maximum WTP (relative to the no-product alternative) for the most preferred antimalware software product.

[5] The intuition behind this calculation is that the difference between the part-worth utilities of the two levels under consideration provides one with the number of "utils" gained from making the package change. These "utils" are converted to monetary units by dividing by the marginal utility of income ($-\beta_{price}$).

This would be estimated as follows:[6]

$$\text{Max Mean WTP} = (-1/\beta_{price}) * [\ln(\exp(\beta_{time}*0 + \beta_{speed\_no\_change} + \beta_{crash\ risk\ greatly\ reduced} + \beta_{id\ theft\ risk\ greatly\ reduced} + \beta_{others\ risk\ greatly\ reduced}) + \exp(\beta_0 - \beta_{price}\$21.68 - \beta_{time}*18.36)) - \ln(\exp(\beta_0 - \beta_{price}*\$21.68 - \beta_{time}*18.36))] \quad (2.3)$$

Here again, standard errors and confidence intervals for these estimated marginal WTP measures were estimated using a bootstrapping procedure with 10,000 iterations.

4.3 Internal Validity Tests

We conduct a number of internal validity tests to be confident in the inferences we make from the analytical results. First, we test whether the choices survey respondents made conform to typical assumptions of rational behavior. Specifically, the following assumptions are typically made about individuals' preferences conjoint studies (e.g., Mansfield et al., 2008):

- **Completeness:** When choosing between two goods, an individual can always choose which good he or she prefers or if they are equally attractive.
- **Monotonicity:** Other things being equal, an individual will prefer more of a good to less.
- **Transitivity:** If an individual reports that "A is preferred to B" and that "B is preferred to C," then he or she must also report that "A is preferred to C."
- **Stability:** In general, if a respondent prefers alternative A to B at one point in the sequence of questions, she should still prefer A to B at any subsequent point.

The experimental design we created allows us to test two of these assumptions: monotonicity and stability. To test monotonicity, we showed 12% of respondents a choice task where the levels of one product were unambiguously better for all attributes than the other product (see Figure 3 for an example). If a person's preferences are monotone, we would expect the person to always choose the product with the unambiguously better levels.

[6] Please note that the \$21.68 and 18.36 minutes are the mean dollars and time shown to respondents in the hypothetical choice tasks. The subtraction of β_{price}*\$21.68 and β_{time}*18.36 from the alternative-specific constant, $\beta_{0,}$ is necessary because we used continuous price and time terms and effects-coding for the other parameters.

Figure 3. Dominated Task

	Product A	Product B
Costs of Antimalware Software		
Price for one year of antimalware software service.	$10	$80
Time spent each month using antimalware software	0 minutes per month	60 minutes per month
Speed of computer performance after installing antimalware software	No Decrease	Significantly Decrease
Benefits of Antimalware Software		
Risk of your computer slowing down or crashing	Greatly Reduced	Somewhat Reduced
Risk of your identity being stolen	Greatly Reduced	Not Reduced
Risk to other individuals and businesses from malware on your computer	Greatly Reduced	Not Reduced
If these were the only options available, which would you choose?	☐	☐

Suppose you were actually offered this antimalware software product in real life. Would you buy it for use on your CURRENT PERSONAL COMPUTER?

☐ Yes
☐ No

To test stability, we used data collected from the two "internal validity test questions" that were described earlier in this section. In reality, this is actually the same question asked twice. Specifically, we ask respondents to answer the question shown in Figure 4 at the beginning of the survey. Then we ask them to answer the same question again at the end of the survey. If a person's preferences are stable, he or she will answer the choice task the same way the second time as he or she did the first time.

In addition to testing these assumptions of rational behavior we also test the internal validity of our results by measuring their predictive power. To do this we again use the "internal validity test questions" to perform what is known as "holdout task analysis". As previously described in this section, only seven of the ten conjoint questions included in the survey were used to estimate the RUM model. Responses to the two "internal validity questions" were excluded or "held out" of the analysis. Therefore, we can test the validity of the RUM model by using it to predict how respondents answered the two internal validity test questions (referred

Figure 4. Preference Stability Question / Hold Out Task

	Product A	Product B
Costs of Antimalware Software		
Price for one year of antimalware software service.	$10	$80
Time spent each month using antimalware software	0 minutes per month	10 minutes
Speed of computer performance after installing antimalware software	Somewhat Decreased	No Decrease
Benefits of Antimalware Software		
Risk of your computer slowing down or crashing	Greatly Reduced	Somewhat Reduced
Risk of your identity being stolen	Somewhat Reduced	Greatly Reduced
Risk to other individuals and businesses from malware on your computer	Greatly Reduced	Not Reduced
If these were the only options available, which would you choose?	☐	☐
Suppose you were actually offered this antimalware software product in real life. Would you buy it for use on your CURRENT PERSONAL COMPUTER? ☐ Yes ☐ No		

to in this context as "hold out tasks"). If the model accurately predicts respondents' choices, this lends additional credibility to the results.[7]

Mathematically, we can predict the percentage of respondents choosing Product A, B, and Neither as follows. The probability that respondents will choose Product A is given by equation 3.4, the probability respondents will choose Product B is given by equation 3.5, and the probability respondents will choose neither product is given by equation 3.6 below

$$P^a = \exp(\sum\beta_i) / [\exp(\sum\beta_i) + \exp(\sum\beta_j) + \exp(\beta_0)] \quad (3.4)$$

$$P^b = \exp(\sum\beta_j) / [\exp(\sum\beta_i) + \exp(\sum\beta_j) + \exp(\beta_0)] \quad (3.5)$$

$$P^0 = \exp(\beta_0) / [\exp(\sum\beta_i) + \exp(\sum\beta_j) + \exp(\beta_0)] \quad (3.6)$$

[7] Note that the levels for the internal validity test questions (aka the hold out tasks) were selected based on recommendations in Orme and Johnson (2010). Specifically, they recommend that levels for a hold out task should be selected so that neither option dominates the other. Examination of Figure 4 should reveal that neither product can be strictly preferred to the other.

where β_i are the coefficient estimates corresponding to the attribute levels associated with Option A and β_j are the coefficient estimates corresponding to the attribute levels associated with Product B and is β_0 the coefficient estimate associated with the no product alternative.

We can compare the predicted proportion of respondents choosing Products A, B, and Neither to the actual proportion using Mean Absolute Error. This is calculated by taking the average of the absolute error between predicted and actual answers for Product A, B, and Neither. For example, suppose the predicted proportion of respondents choosing Products A, B, and Neither are 70%, 20%, and 10%, respectively. By contrast, suppose the actual proportion of respondents choosing Products A, B, and Neither are 60%, 30%, and 10%, respectively. Thus, the absolute error for Product A is 10 percentage points, the absolute error for Product B is 10 percentage points, and the absolute error for Neither Product is 0 percentage points. Therefore, the Mean Absolute Error is approximately 6.67 percentage points (6.67=[(10+10+0)/3]). The closer the Mean Absolute Error is to zero, the better the predictions are said to be.

5. Analysis Results

Data were collected for this study by comScore, Inc. Specifically, the survey instrument described above was fielded in August 2012 to 2,699 members of the comScore panel who were older than 18 years of age and resided inside the United States. The comScore panel is a large opt-in consumer-panel that comScore, Inc. maintains to be representative of the online population and projectable to the total U.S. population. The panelists are recruited across thousands of sites not used by other panel suppliers, and they do not have to be willing to answer surveys to be accepted to the panel. We decided to include only broadband Internet users from the comScore panel in our sample because they are the users who would be most affected by malware. Descriptive statistics of our sample of respondents are shown in Table 3.

Table 3. Sample Characteristics

Sample Size	2,998
Gender	
Male	34.88
Female	65.12
Age	
18-34	22.13
35-54	42.75
55+	35.11
Education	
High school degree or less	22.32
Some college	25.07
College graduate	52.62
Annual Household Income	
less than $50,000	47.43
$50,000-$99,999	33.68
$100,000 or more	13.89
Prefer not to answer	5
Race	
White	85.79
Non-white	14.21

For the remainder of this section we summarize the results obtained from analyzing the data we collected. First, we report qualitative summary statistics regarding individuals' use of antimalware software and the perceived threat of malware. Next, we report quantitative results regarding respondents' preferences for antimalware software attributes, how much respondents are willing to pay for improvements in

these attributes, and how this willingness to pay differs based on respondents' risk perceptions and behaviors.

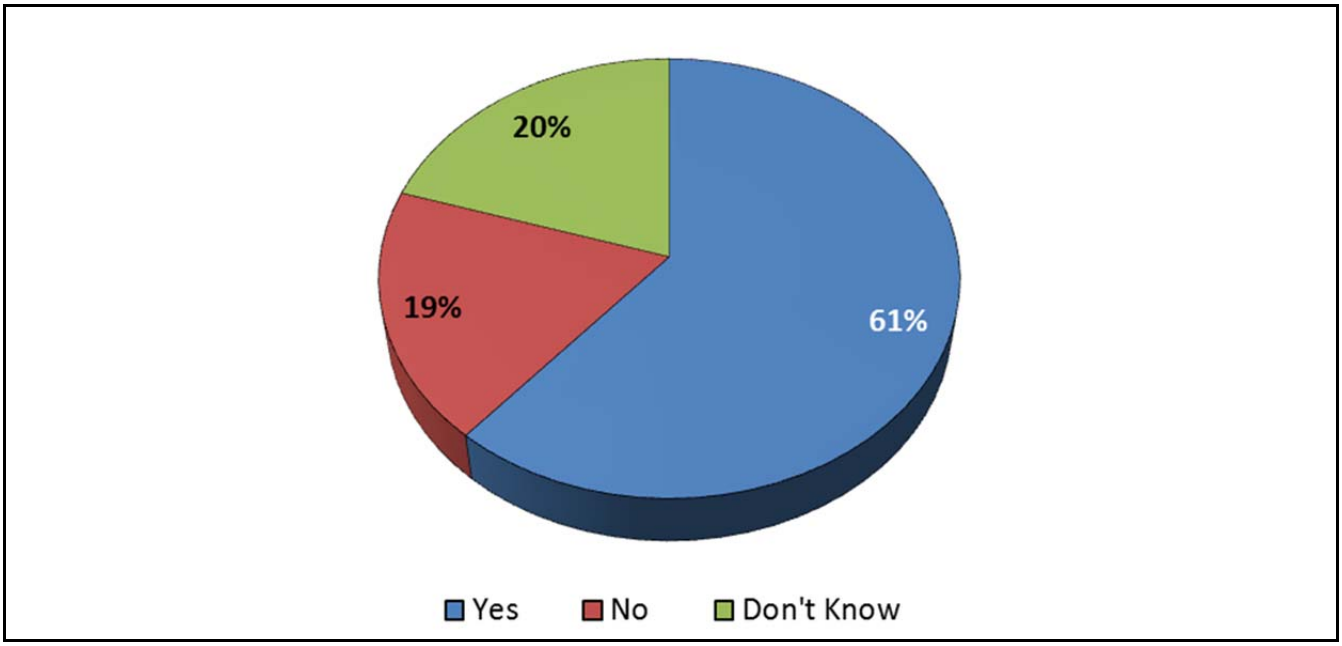
5.1 Summary Statistics

We asked survey respondents a variety of questions about the characteristics of the antimalware software they own and how they use the software, and their views of the threat of malware. The following subsections provide a summary of the results of these questions.

Current Antimalware Ownership, Brand, and Use

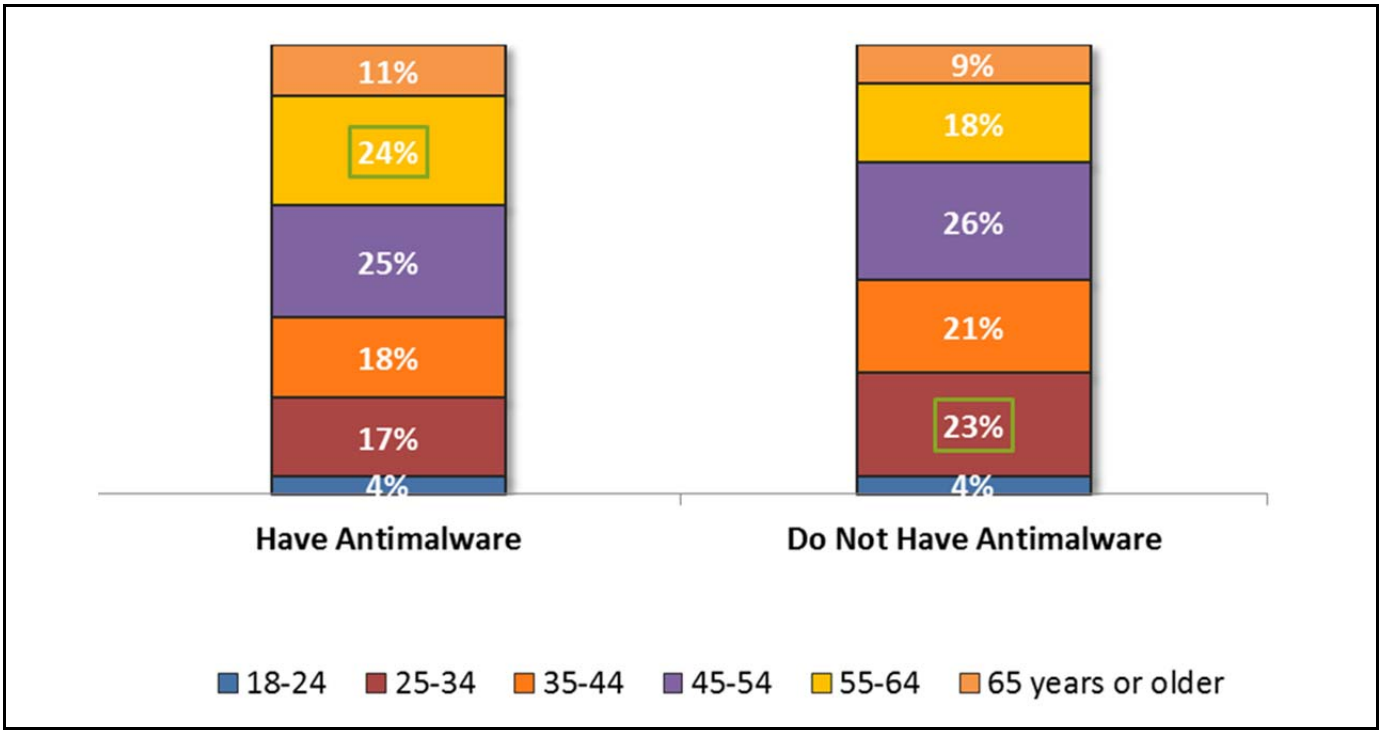
As shown in Figure 5, approximately 61% of the survey respondents indicated that they have some type of antimalware software installed on their current home computers. Some 19% of respondents indicated that they did not have antimalware currently installed, while the remaining 20% of respondents did not know if they had antimalware currently installed.

Figure 5. Do You Have Antimalware Installed on Your Computer



Of those respondents who indicated they currently have antimalware installed, 64% are between 18 and 54 years old. Of those who do not currently have antimalware installed, 74% are between 18 and 54 years old. Respondents with antimalware currently installed tend to be slightly older than those without antimalware installed. Figure 6 provide a graphical representation of these data.

Figure 6. Antimalware Ownership, by Age



The most popular brands of antimalware are Symantec/Norton and McAfee. Of those who have antimalware, 51% have Symantec/Norton or McAfee installed. The remaining three most popular brands in order are: AVG (20%), Microsoft Security Suite (18%), and Avast (11%). Additionally, respondents indicated that the most common method of obtaining antimalware is from an ISP provider (35%), downloaded for free. The second most popular method of obtaining antimalware was buying online (27%). See Figure 7 for a summary of survey respondents' current antimalware usage.

Proper use of antimalware requires periodic scans of the computer and updates to the software. When asked, 71% of respondents with antimalware software indicated that either the antimalware software scans the computer automatically or they have used the antimalware scan at least once in the past week (see Figure 7). Only 3% of antimalware owners indicated that it had been a year or more since the last known scan (see Figure 8). Similarly, 65% of antimalware owners indicated that their antimalware software is either updated automatically or they have updated their software in the past week (see Figure 9).

Figure 7. Most Popular Brands of Antimalware

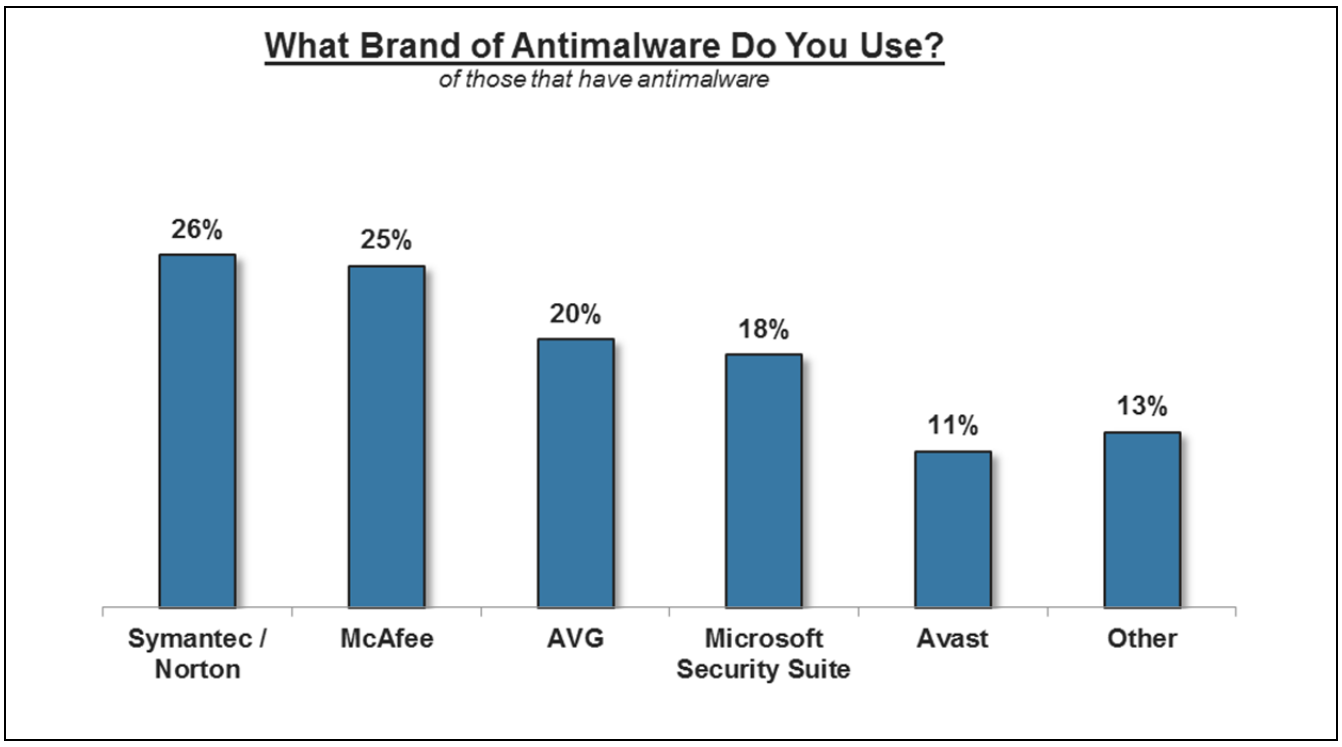


Figure 8. Frequency of Antimalware Scans

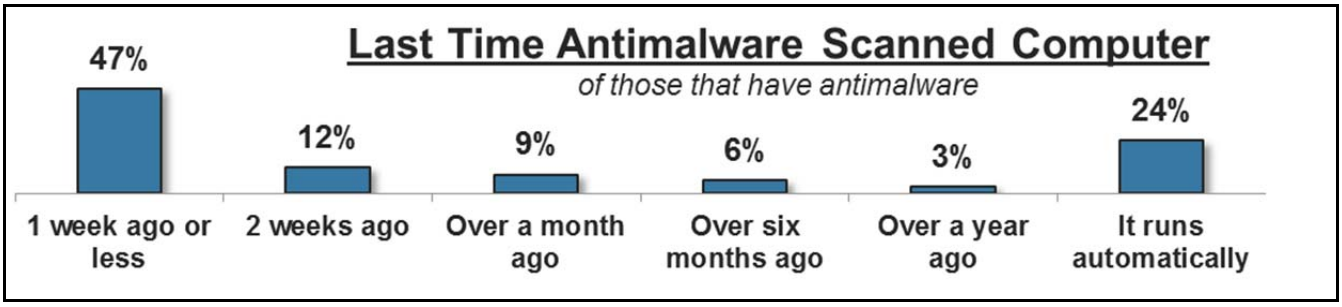
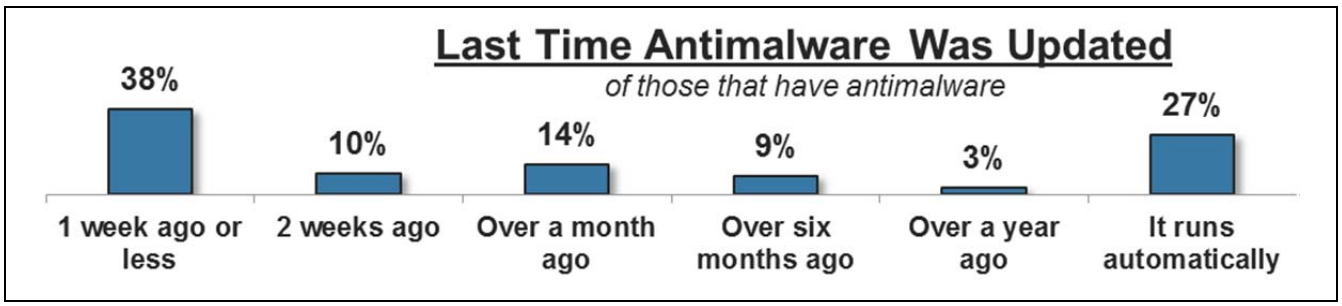


Figure 9. Frequency of Antimalware Updates



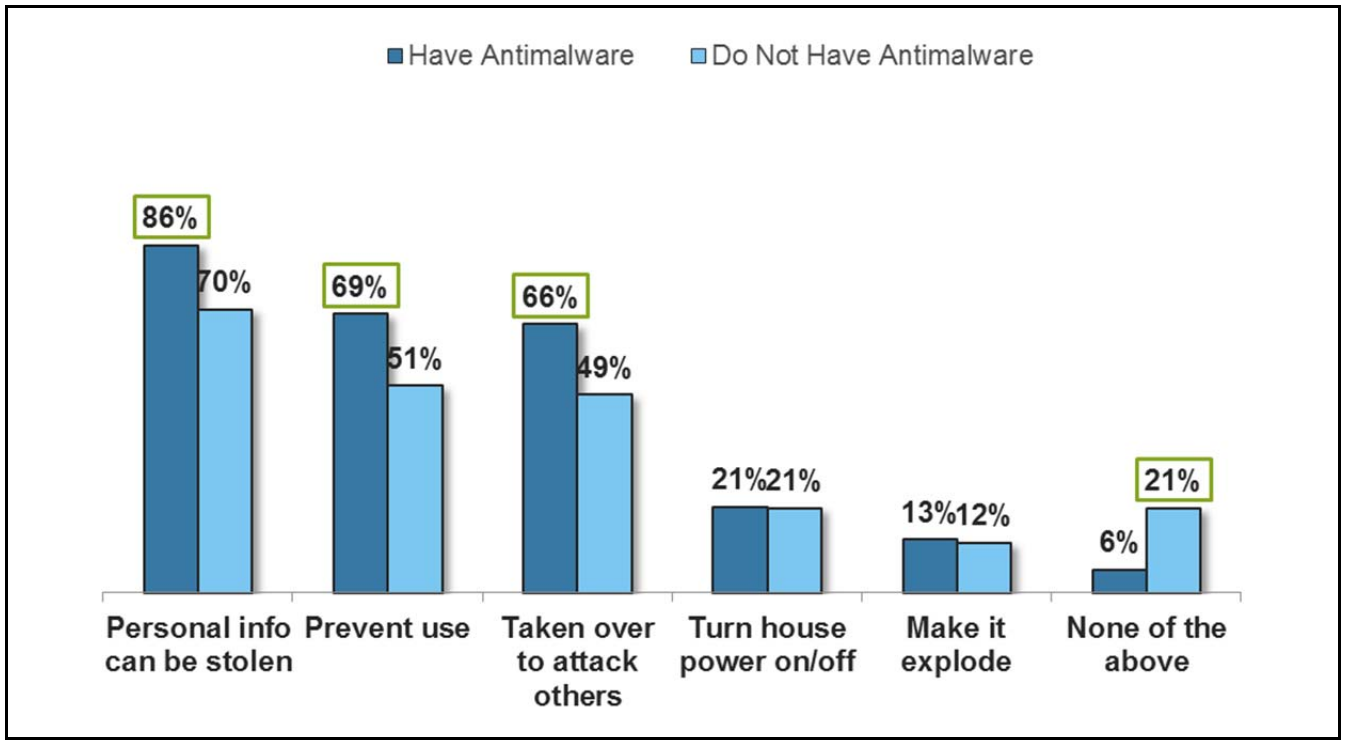
Perceived Risk of Malware

Perceptions of malware are likely influenced by previous experiences with malware. Accordingly, of those who currently have antimalware installed on their computer, 66% indicated that they have had past problems with malware. Those who indicated they did not have antimalware installed reported that they had past problems with malware 34% of the time. Those with antimalware installed reported having past problems with malware at twice the rate of those without antimalware installed. As such, past experience likely has an influence on the perceived risk of malware.

Encountering problems associated with malware costs time and in some cases money. Of those respondents who indicated past problems with malware, 53% report that they spent $0 fixing the problem. However, 63% of those same respondents indicated that they spent at least 2 hours or more attempting to fix the problems caused by malware.

Owners of antimalware also indicated that they believe malware has a great effect on computers. The greatest perceived risk from malware was identity theft (see Figure 10). Antimalware owners and those who do not own antimalware felt similarly about malware's risk of affecting the potential for identity theft. Eighty-two percent of antimalware owners indicated that malware could affect identity theft, while 64% of nonowners indicated the like. However, only 6% of antimalware owners believe that malware has no effect on their computers in contrast to the 24% of nonowners who indicated that malware has no effect on their computers.

Figure 10. Beliefs on How Malware Affects Computers



5.2 U.S. Broadband Internet User Preferences (Conditional Logit Model Results)

As discussed in Section 3, U.S. broadband Internet user preferences were quantified by estimating a RUM model using conditional logit techniques. Specifically, parameter estimates were obtained for two linear specifications of the RUM model. First, we computed parameter estimates for a linear specification where all variables were effects coded (the coefficient estimates for this model are reported in columns two and three of Table 4). Second, we computed parameter estimates for a specification where price and time were treated as continuous variables and all other variables were effects coded (the coefficient estimates for this model are reported in columns two and three of Table 5). These coefficient estimates presented in both Tables 4 and 5 were calculated with a subset (2,182) of the total survey sample; 516 respondents indicated that they would not buy any of the hypothetical antimalware products they were shown during the survey. This can be interpreted as an indication that these respondents were not "in the market" for antimalware software, which makes their responses less relevant for measuring the preferences of individuals that *are* in the market for antimalware software.

As previously discussed, the coefficient estimates reported in Tables 4 and 5 can be interpreted as utilities where large values indicate greater utility. Thus, based on these coefficient estimates we can see that survey respondents typically prefer antimalware software to cost less, take less time to use, and result in less reduction in the speed of their computer.[8] Similarly, respondents prefer antimalware software that yields greater reductions in the risk that their computer might crash, the risk their identity would be stolen, and the risk others may be harmed by malware on their computer. These results are in line with our ex ante expectations of broadband user preferences.

However, note that the coefficient for "neither antimalware product" is positive and statistically significant in both initial regression results. This implies that respondents gain positive utility from not having antimalware software on average, which is contrary to our ex ante expectation of consumer preferences. To better understand if there was a particular subgroup of respondents driving this counterintuitive result, we interacted the "neither antimalware product" indicator with several respondent characteristics—age, sex, income, and how they viewed the threat of malware and the effectiveness of antimalware at addressing that threat.[9] For the interacted terms, positive values are associated with greater utility from not having an antimalware package and negative values are associated with less utility.

[8] Note that the part-worth utility associated with 40 minutes is greater than the part-worth utility associated with 10 minutes. This would seem to imply that respondents prefer spending 40 minutes using their software as opposed to 10 minutes. However, this counterintuitive finding is statistically insignificant.

[9] Note that Brown et al. (2010) study performed a similar adjustment to their multivariate model examining vaccine preference (see Table 2 of the Brown et al. study).

Table 4. Part Worth Utilities Estimated for U.S. Broadband Customers (Fully Effects Coded Model)

	Model Without		Model With	
	Estimated Mean Coefficient	Standard Error of the Mean	Estimated Mean Coefficient	Standard Error of the Mean
Price for one year of antimalware software service				
$0	0.540***	0.021	0.541	0.021
$10	0.300***	0.021	0.300	0.021
$40	-0.090***	0.022	-0.091	0.022
80 (omitted)	-0.750***	0.025	-0.751	0.025
Time spent each month using antimalware software				
0 minutes per month	0.063**	0.022	0.062	0.022
10 minutes per month	-0.010	0.021	-0.010	0.021
40 minutes per month	0.017***	0.022	0.017	0.022
60 minutes per month (omitted)	-0.070***	0.022	-0.070	0.022
Speed of computer performance after installing antimalware software				
No Change	0.391***	0.017	0.392	0.017
Somewhat Slows Down	0.085***	0.017	0.085	0.017
Greatly Slows Down (omitted)	-0.476***	0.018	-0.476	0.018
Reduced risk of your computer slowing down or crashing				
Not Reduced	0.328***	0.017	0.328	0.017
Somewhat Reduced	-0.026***	0.017	-0.025	0.017
Greatly Reduced (omitted)	-0.302***	0.018	-0.303	0.018

(continued)

Table 4. Part Worth Utilities Estimated for U.S. Broadband Customers (Fully Effects Coded Model) (continued)

	Model Without		Model With	
	Estimated Mean Coefficient	Standard Error of the Mean	Estimated Mean Coefficient	Standard Error of the Mean
Reduced risk of your identity being stolen				
Not Reduced	0.374***	0.017	0.374	0.017
Somewhat Reduced	0.054***	0.017	0.054	0.017
Greatly Reduced (omitted)	-0.428***	0.018	-0.428	0.018
Reduced risk to other individuals and businesses from your insecurity				
Not Reduced	0.188***	0.017	0.188	0.017
Somewhat Reduced	0.029***	0.017	0.029	0.017
Greatly Reduced (omitted)	-0.217***	0.017	-0.217	0.017
Neither Antimalware Product (adjusted)	0.281***	0.018	-0.315	0.017
Neither* household income < $50,000	(-)	(-)	0.117	0.037
Neither* age	(-)	(-)	0.008	0.001
Neither* college graduate	(-)	(-)	0.143	0.037
Neither*female	(-)	(-)	0.098	0.037
Neither*not working (retired, laid off, students, etc.)	(-)	(-)	0.066	0.039
Neither*believes contracting malware will not significantly impact computer activities	(-)	(-)	0.107	0.062

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

Table 5. Part Worth Utilities Estimated for U.S. Broadband Customers (Price and Time Coded as Continuous Variables)

	Model Without		Model With	
	Estimated Mean Coefficient	Standard Error of the Mean	Estimated Mean Coefficient	Standard Error of the Mean
Price for one year of antimalware software service	0.016***	0.000	-0.016	0.000
Time spent each month using antimalware software	0.002***	0.001	-0.002	0.001
Speed of computer performance after installing antimalware software				
No Change	0.391***	0.017	0.391	0.017
Somewhat Slows Down	0.084***	0.017	0.084	0.017
Greatly Slows Down (omitted)	0.475***	0.018	-0.475	0.018
Reduced risk of your computer slowing down or crashing				
Not Reduced	0.329***	0.017	0.329	0.017
Somewhat Reduced	0.027***	0.017	-0.027	0.017
Greatly Reduced (omitted)	0.302***	0.018	-0.302	0.018
Reduced risk of your identity being stolen				
Not Reduced	0.374***	0.017	0.374	0.017
Somewhat Reduced	0.052***	0.017	0.052	0.017
Greatly Reduced (omitted)	0.426***	0.018	-0.426	0.018
Reduced risk to other individuals and businesses from your insecurity				
Not Reduced	0.187***	0.017	0.187	0.017
Somewhat Reduced	0.030***	0.017	0.030	0.017
Greatly Reduced (omitted)	0.217***	0.018	-0.217	0.018
Neither Antimalware Product (adjusted)	0.098***	0.026	-0.500	0.078
Neither* household income < $50,000	(-)	(-)	0.117	0.037
Neither* age	(-)	(-)	0.008	0.001
Neither* college graduate	(-)	(-)	0.143	0.037
Neither*female	(-)	(-)	0.097	0.037
Neither*employment status	(-)	(-)	0.066	0.039
Neither*Apple owner	(-)	(-)	0.107	0.062

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

Columns 4 and 5 of Tables 4 and 5 report results for reestimating these models with individual characteristics interacted with the "neither antimalware product" indicator. As we can see, individuals are more likely to not choose a malware product if they are older, female, college graduates, from low-income households (<$50,000), not currently working, and believe contracting malware would not significantly impact their computers. With the exception of the finding for college graduates, these results suggest that the individuals most likely to gain positive utility from not having antimalware software are those less able to afford it or more likely to perceive the dangers of malware as being insignificant.

5.3 Marginal Willingness to Pay Estimates

Coefficient estimates from Table 5 were used to compute marginal willingness to pay estimates: estimates of how much respondents are willing to pay on average for changes in each individual antimalware product attribute level. These marginal WTP estimates are reported in Table 6. Specifically, this table reports estimates for how much the mean respondent is willing to pay to change the level of each attribute from its least favored level to its most favored level. Reporting marginal WTPs in this fashion can help us discern how much respondents are willing to pay to avoid the nonmonetary costs of using antimalware software and how much they are willing to pay to receive the benefits having antimalware software can provide.

As we can see from Table 6, the nonmonetary cost that the respondents are willing to pay the most to *avoid* is a reduction in the speed of their computer's performance. Specifically, respondents are willing to pay approximately $56 per year on average to switch from a product that greatly reduces the speed of their computers performance to one that does not reduce their performance at all (holding all other attributes constant). By contrast, respondents were willing to pay relatively little for reductions in time spent using antimalware software.

Table 6. Mean Marginal Willingness to Pay for Improvements in Individual Product Attributes

	WTP	Std. Dev.
Time Spent Using Antimalware Software: WTP to avoid 1 minute of time using the software each month	$0.10	0.03
Speed of computer performance after installing antimalware software: WTP to move from antimalware software greatly slowing your computer to not slowing it at all	$55.50	2.39
Risk of Computer Slowing Down or Crashing: WTP to move from not reduced to greatly reduced	$40.43	2.18
Risk of Identity Theft: WTP to go from not reduced to greatly reduced	$51.23	2.32
Risk to Other Individuals and Businesses: WTP to go from not reduced to greatly reduced	$25.94	2.02

Specifically, respondents were only willing to pay $.10 to avoid 1 minute of time managing their antimalware software.

In terms of benefits, we find that respondents are willing to pay significantly more for benefits that accrue directly to them as opposed to benefits that accrue mostly to others. In particular, respondents are clearly most concerned about reducing the risk of having their identity stolen. We find that the average respondent is willing to pay over $50 per year to switch from an antimalware product that does not reduce their risk of identity theft to one that greatly reduces this risk. However, respondents were only willing to pay half this much to reduce the risks to others from malware on their computer. Specifically, the average respondent was only willing to pay approximately $26 per year to switch from a product that did not reduce this risk to one that greatly reduces this risk.

It is worth stressing again that these are marginal willingness to pay estimates that only measure how much respondents are willing to pay for improvements in a single attribute while holding all other attributes constant. Therefore, one should not try to estimate how much respondents would be willing to pay for an entire antimalware product by adding these WTPs together. To estimate how much respondents are willing to pay for an entire antimalware product we must consider the utility of having that product as a whole relative to having no product at all (as described in Section 4). To illustrate this, we estimate how much respondents are willing to pay (on average) for their most-preferred antimalware software. The results of this estimation are provided in Section 5.4.

Measuring the Influence of Self-Reported Risk Behaviors and Perceptions on the Marginal Willingness to Pay Estimates

In order to assess what factors are affecting willingness to pay estimates, we conducted additional analysis of the marginal WTP based on the following data from the survey:

- Experience with computer viruses
- Frequency of malware scanning
- Level of risk aversion

Table 7 compares the marginal willingness to pay of each attribute level based on whether a respondent identified him- or herself as someone who previously contracted a virus. Although most of the WTP estimates are the same for both groups of respondents, those who had contracted a virus previously—and most likely experienced some computer performance issues (e.g., slowing down or crashing)—were willing to pay 19% more than those who had not previously contracted a virus for a move from not reduced to greatly reduced risk in their computer slowing down or crashing.

Table 7. Comparison of Marginal Willingness to Pay Based on Previous Stated Experience with Computer Viruses

	Had Virus		Did Not Have Virus	
	WTP	Std. Dev.	WTP	Std. Dev.
Time Spent Using Antimalware Software: WTP to avoid 1 minute of time using the software each month	$0.02	0.09	$0.12	0.04
Speed of computer performance after installing antimalware software: WTP to move from antimalware software greatly slowing your computer to not slowing it at all	$56.68	6.35	$59.70	3.17
Risk of Computer Slowing Down or Crashing: WTP to move from not reduced to greatly reduced	$46.63	5.99	$39.57	2.78
Risk of Identity Theft: WTP to go from not reduced to greatly reduced	$52.77	6.14	$54.21	3.04
Risk to Other Individuals and Businesses: WTP to go from not reduced to greatly reduced	$27.10	5.43	$26.73	2.60

Table 8 compares the marginal willingness to pay of each attribute level based on whether a respondent currently had antimalware installed and the last time it scanned their computer. The results of Table 7 seem to suggest that those who scan less frequently (more than one month since last scan) place more value on the speed of computer performance relative to those who scan for malware more frequently (less than one month since last scan). In addition, those who scan more frequently value reductions in the risk of identity theft and reductions in the risk to other individuals and businesses more relative to those who scan less frequently. In other words, it appears that less risky respondents (who scan more frequently)—again, among those who already have antimalware installed on their current computer—value reductions in risk more than those who appear more risky, and those who appear more risky value computer performance more than those who appear less risky. It appears there is a tradeoff between reducing risk and increasing computer performance (all else equal).

Table 9 identifies the marginal WTP estimates for each attribute level based on respondents' self-assessed risk aversion. These results provide a direct correlation between risk preferences and demand for antimalware software. The research team asked all respondents—owners and nonowners of antimalware software—a series of questions based on how often they pursued behaviors to avoid various types of risk. Specifically, they were asked if they always, sometimes, or never did the following: wear your seatbelt in a moving vehicle, floss your teeth daily, get flu shots every year, or wear sunscreen when you are in the sun. Individuals that said they always pursued at least 3 of these 4 activities were classified as "more risk averse" than the remaining respondents (who were classified as "less risk averse").

Table 8. Comparison of Marginal Willingness to Pay Based on the Stated Frequency of Malware Scanning

	Last Scanned Less than One Month Ago		Last Scanned More than One Month Ago	
	WTP	Std. Dev.	WTP	Std. Dev.
Time Spent Using Antimalware Software: WTP to avoid 1 minute of time using the software each month	$0.05	0.06	$0.25	0.20
Speed of computer performance after installing antimalware software: WTP to move from antimalware software greatly slowing your computer to not slowing it at all	$57.91	4.20	$74.69	15.48
Risk of Computer Slowing Down or Crashing: WTP to move from not reduced to greatly reduced	$46.00	3.87	$43.34	12.58
Risk of Identity Theft: WTP to go from not reduced to greatly reduced	$64.55	4.35	$38.49	12.16
Risk to Other Individuals and Businesses: WTP to go from not reduced to greatly reduced	$30.64	3.54	$21.59	11.29

Table 9. Comparison of Marginal Willingness to Pay Based on Respondents' Level of Risk Aversion

	More Risk Averse		Less Risk Averse	
	WTP	Std. Dev.	WTP	Std. Dev.
Time Spent Using Antimalware Software: WTP to avoid 1 minute of time using the software each month	-$0.04	0.12	-$0.11	0.03
Speed of computer performance after installing antimalware software: WTP to move from antimalware software greatly slowing your computer to not slowing it at all	$71.57	9.73	$52.89	2.37
Risk of Computer Slowing Down or Crashing: WTP to move from not reduced to greatly reduced	$61.75	9.13	$36.88	2.13
Risk of Identity Theft: WTP to go from not reduced to greatly reduced	$76.92	10.11	$47.02	2.26
Risk to Other Individuals and Businesses: WTP to go from not reduced to greatly reduced	$36.38	7.80	$24.24	2.01

The comparison of marginal WTP estimates based on risk aversion is illuminating. At each attribute level, the corresponding marginal WTP estimates are higher for the more risk averse group than the less risk averse group. The more risk averse group is willing to pay more for increased security even at the expense of reduced computer performance.

In addition to examining the marginal WTP estimates for increased security based on self-assessed risk, we examined the marginal WTP estimates for increased security based on perceived risk of identity theft. Table 10 presents the marginal WTP estimates for two groups: those respondents who perceived themselves at high risk of having their identity being stolen and those who perceived themselves at low risk of their identity being stolen. Again, the results are particularly illuminating.

Based on the results from Table 9, the high-risk group is willing to pay more for increased security even at the expense of reduced computer performance, relative to the low risk group. Particularly, the high-risk group is willing to pay 48% more for a reduction in the risk of their computer slowing down or crashing than the low-risk group. Overall, the high risk group is willing to pay more ($68 per year) to go from not reduced to greatly reduced risk in identity theft than any other attribute. The low risk group is willing to pay most ($59 per year) for a move from antimalware software greatly slowing your computer to not slowing it at all.

Table 10. Comparison of Marginal Willingness to Pay Based on Respondents' Perceived Risk of Identity Theft

	High Risk		Low Risk	
	WTP	Std. Dev.	WTP	Std. Dev.
Time Spent Using Antimalware Software: WTP to avoid 1 minute of time using the software each month	$0.04	0.18	$0.11	0.05
Speed of computer performance after installing antimalware software: WTP to move from antimalware software greatly slowing your computer to not slowing it at all	$65.18	13.49	$58.99	3.94
Risk of Computer Slowing Down or Crashing: WTP to move from not reduced to greatly reduced	$62.60	13.35	$43.15	3.49
Risk of Identity Theft: WTP to go from not reduced to greatly reduced	$67.75	13.73	$53.28	3.71
Risk to Other Individuals and Businesses: WTP to go from not reduced to greatly reduced	$40.46	11.65	$25.93	3.22

5.4 Maximum Willingness to Pay for Hypothetical ISP Security Packages

In addition to estimating marginal willingness to pays for improvements in individual attributes, we also estimate the maximum amount the mean Internet user is willing to pay for

an “ideal” or “most-preferred” antimalware product—one that does not require a user to spend any time using it, that does not slow their computer’s performance after it is installed, and that greatly reduces all cyber security risks they face. Table 11 summarizes the results of our analysis.

As we can see, the mean WTP for the most preferred antimalware product was approximately $93 per year. This estimate represents the most an average Internet user would ever pay for an antimalware software product. We estimated a 95% confidence interval for this WTP by using Krinsky-Robb parametric bootstraps and found the lower confidence limit to be $87 per month and the upper confidence limit to be $99 per year. Considering we observe the some cyber security software packages (such as Norton 360 or McAfee All Access 2012) costing $80–$90, and these packages include many features beyond antimalware protection (such as automatic data backup and technical support), we believed that our estimate of $93 is reasonable as an upper-bound estimate for the most respondents are willing to pay on average for antimalware software.

5.5 Internal Validity Tests

In Section 4 we briefly described two types of internal validity tests that we conducted to be confident in the inferences we make from the analytical results. First, we test whether the choices survey respondents made conform to typical assumptions of rational behavior. Specifically, we tested whether respondents’ preferences are monotonic and stable. The experimental design we created allowed us to test preference monotonicity for 268 respondents. Out of the 268 tests conducted, 47 respondents failed (approximately 18%). Similarly, the experimental design we created allowed us to test preference stability for all 2,182 respondents included in our stated-preference analysis. Out of the 2,182 tests conducted, 527 respondents failed (approximately 24%).

Table 11. Willingness to Pay for Hypothetical Antimalware Security Package: Base Case Scenario

Characteristic	Values	Estimated WTP ($/year)	95% Confidence Interval
Time Spent Using Antimalware Software:	0 hours		
Speed of Computer Performance After Installing Antimalware Software	Not reduced	$92.99	[87.28 to 98.69]
Risk of Computer Slowing Down or Crashing:	Greatly reduced		
Risk of Identity Theft:	Greatly reduced		
Risk to Other Individuals and Businesses:	Greatly reduced		

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

The second type of internal validity test we performed was a holdout task analysis to test the "predictive power" of the models we estimated in Table 4 (where all variables are fully effects coded) and Table 5 (where price and time are coded as continuous variables). As previously described, the holdout analysis was conducted as follows. First, in addition to seven regular conjoint questions (which were assigned randomly to each individual), every respondent answered two identical conjoint questions (known as a holdout tasks). Next, we used the respondents' answers to the seven random choice tasks to estimate the conditional logit models in Tables 4 and 5. These models were then used to predict how the average respondent answered each hold task (the percent of respondents who would select Option A, Option B, or Neither). Finally, we compare the predicted distribution of choices with the actual choices respondents made.

The results of the holdout task analysis for the conditional logit models are presented in Tables 12. As we can see, both models do a relatively good job of predicting the actual choices of survey respondents. Specifically, the Mean Absolute Error (MAE) between predicted choices and actual choices never exceeds 5 percentage points for either model.

Table 12. Hold Out Task Analysis

	Conditional Logit Fully Effects Coded (n=2182)		Conditional Logit Price and Time Continuous	
	Question #1	Question #2	Question #1	Question #2
Predicted Percentage Choosing Each Option				
Product A	49	49	45	45
Product B	27	27	24	24
Neither	24	24	30	30
Actual Percentage of Respondents Choosing Each Option				
Product A	47	48	47	48
Product B	23	21	23	21
Neither	30	30	30	30
Measures of Differences				
Absolute Error for Product A	2.26	0.84	1.71	3.13
Absolute Error for Product B	4.10	5.84	1.34	3.08
Absolute Error for Neither	6.37	6.69	0.37	0.05
Mean Absolute Error	4.24	4.46	1.14	2.09

Overall, the results of these tests suggest that the decision of whether to purchase or use antimalware is not straightforward for individuals. Although the vast majority of respondents passed the rationality tests we submitted them to, a relatively large percentage (close to 25%) did fail. To test the robustness of our results, we excluded individuals that failed the preference stability. However, this did not greatly change our results. Part-worth utilities were largely the

same for both models and as a result willingness to pay metrics did not greatly change. Similarly, excluding individuals that failed the preference stability test did not greatly improve the predictive power of our models as measured by the hold out task analysis. As a result, we kept all respondents in our sample.

---

6. Comparing our Results to Past Public Health Studies

Section 2.1 of this report presented summarized results from previously published studies of factors influencing vaccine preferences. Our results indicate a number of interesting differences between vaccine preference and antimalware preference. First, as illustrated in Table 3, cost of antimalware had the strongest impact on antimalware preference. In column 2 of this table, the estimated mean coefficient for free antimalware was six times the coefficient for antimalware costing $40. In contrast, while cost has been reported to have significant impacts on vaccine preference, it is rarely the most important factor. The range of costs used in the present antimalware study (free to $40) was substantially less than that used in many vaccine studies; for example, Liau & Zimet (2001) included vaccine costs ranging from free to $300. However, even this smaller cost range had substantial impacts on preference. This suggests that consumers are much more sensitive to antimalware cost than they are to vaccine cost. This preference could reflect the importance individuals place on vaccination as a way to prevent potentially life-threatening diseases vs. the importance ascribed to antimalware. The greater cost-sensitivity for antimalware may also relate to the availability of free antimalware software from multiple sources, including products distributed by ISPs and limited use version available as shareware. Most individuals are likely accustomed to paying for vaccination, which involves both the vaccine itself and the time of a health care provider to administer the vaccine; there is likely less expectation for paying for antimalware, where the "work" that computer users typical experience (i.e., the installation of the program) is performed by themselves.

Our antimalware preference study assessed antimalware safety (corresponding to the "risk of side effects" for vaccine preference) based on the risk of a computer slowing down or crashing after installation of antimalware. This safety measure was the second most important characteristic influencing antimalware preference. The risk of adverse consequences almost always has a significant effect on vaccine preference, but this factor is generally substantially less important than efficacy or effectiveness. The importance of potential negative consequences associated with antimalware is further emphasized by the positive coefficient for have no antimalware ("neither antimalware product"), in column 2 of Table 3. As stated in Section 5.2, this implies that respondents gain positive utility from (i.e., have an overall preference for) not having antimalware software. When including interactions of the "neither antimalware product" with a number of respondent characteristics, the effect of having no antimalware does become negative (column 4), indicating decreased preference for not having any antimalware. However, these findings suggest a fundamental difference between vaccine

preference and antimalware preference. In general, there is increased preference for being vaccinated. While factors such as cost and safety may limit this preference, individuals will almost always prefer to be vaccinated vs. being non-vaccinated. In contrast, antimalware appears to be viewed as less of a necessity. Negative factors associated with antimalware, such as cost and potential safety issues, may outweigh the potential positive aspects. This finding suggests that increased consumer education regarding the potential consequences of lacking antimalware is needed. Public health information dissemination campaigns may serve as a model for this. In addition, companies producing antimalware need to pay close attention to the potential negative consequences from installing this software and minimize such consequences to the extent possible.

In the majority of vaccine preference studies presented in Section 2.1, vaccine efficacy (or effectiveness) was the most important characteristic affecting vaccine choice. In the present cyber security study, efficacy was measured along two dimensions: "risk of computer slowing down or crashing" and "risk of identity theft". Both of these measures were less important factors for influencing antimalware preference than were cost or safety. As discussed in the previous paragraph, computer users may not regard antimalware as a necessity and may let the potential negative aspects of cost and safety (decreased computer performance) outweigh positive effects, which is different from the results generally seen for vaccine preference. However, the preference results related to efficacy do indicate that survey respondents were able to differentiate between the antimalware efficacy measures presented in this study. "Reduced risk of your identity being stolen" was a stronger attribute than was "Reduced risk of your computer slowing down or crashing". The willingness to pay (WTP) for reducing risk of identity theft was approximately 25% greater that the WTP for reduced risk of slowing down/crashing (Table 5). Identity theft has broad implication, potentially affecting an individual's life in multiple areas and involving substantial time to address. Slowing down or crashing of a computer may be viewed more as an inconvenience, affecting only activities or information directly involving the computer. The difference in responses to these two efficacy measures is similar to the differences observed in vaccine preference studies, where more severe consequences of vaccine-preventable diseases have stronger impact of preference than do minor consequences of these diseases. As discussed above, education campaigns that highlight the potential negative effects of a successful malware event, particularly events that have consequences going beyond impacting computer use (e.g., identify theft), will likely be important for informing the public.

The attribute associated with the risk to other individuals and businesses of malware on a user's computer had the least impact on antimalware preference. Reducing this risk to others may be perceived as even less relevant to an individual, as it does not directly affect him or her; computer users may not even be aware that others have been affected by malware on their computers. To our knowledge, previous studies have not explicitly examined risk to others (i.e., non-vaccinated individuals) as a factor influencing vaccine preference. Liau & Zimet (2001) reported that social saturation, that is, the proportion of individuals already

vaccinated, was significantly associated with vaccine preference. However, contrary to what might be expected, greater levels of social saturation were associated with increased vaccine preference. Rather than assessing an altruistic effect on the benefit of others, this suggests that individuals are more comfortable with a vaccine when they know that others have already experienced it. It would be interesting to assess whether a similar effect is seen with antimalware.

As presented in Table 6, respondents who had previously experienced computer viruses were willing to pay 19% more to greatly reduce the risk of a computer slowing down or crashing (compared with respondents who had not previously experienced a virus). Similarly, respondents who were classified as more risk averse (based on their responses to four questions assessing health behaviors) were willing to pay more to reduce the risk of the antimalware "adverse event" (i.e., reduced computer performance after installing antimalware software) and to increase the efficacy of the antimalware (Table 8). To our knowledge, previous research on vaccine preference has not explicitly examined the impact of level of risk aversion on preference for vaccination. However, other public health studies have noted substantial differences between risk-seeking and risk-averse individuals. For example, individuals who are classified as "risk averse" are less likely to engage in risky health behaviors such as cigarette smoking, heavy drinking, being overweight/obese, or not using seat belts (Anderson & Mellor, 2008). The increase in WTP among respondents with prior computer virus exposure or increased levels of risk aversion corresponds well to the public health frame used for this study.

We observed significant impacts of respondent demographic characteristics on preference for antimalware. Survey respondents who are older, female, college graduates, from lower income households, and not currently working were less likely to choose an antimalware product (Table 3, column 4). Some of these findings are similar to results from vaccine preference studies. For example, Brown et al. (2010) reported that respondents who were college graduates were significantly less likely to choose an HPV vaccine, while higher income respondents were significantly more likely to choose a vaccine. In the Brown et al. study, age had a complicated relationship with vaccine preference; older mothers were significantly more likely to choose an HPV vaccine, but mothers of older daughters were significantly less likely to choose a vaccine. Similar to the finding in our study, Liau & Zimet (2001) found that younger study participants were more likely to give higher ratings to an HIV vaccine. These results indicate that characteristics of computer users are likely to impact preference for antimalware properties, similar to effects of individual's characteristics on preferences for vaccines and other public health interventions.

7. Conclusions and Next Steps

The public health community has been very successful in identifying, monitoring, and reducing the health impacts of many types of threats. Given the many similarities between public health and cyber security, the cyber security community would be wise to leverage relevant public health strategies and analysis techniques. Certainly not all public health strategies will have a comparable approach in the cyber security community. For example, many public health threats are the result of naturally occurring pathogens or biological events; in contrast, in cyber security, the vast majority of threats are manmade.

Although developing a robust community of cyber security stakeholders organized in any way similar to the complexity and scale of public health is daunting, the use of public health research strategies to better understand cyber security risk preferences is a specific area that should be leveraged in the short term. In this study we used past research on public health risk perceptions related to vaccines to stop specific public health threats (e.g., measles) as a model to assess preferences associated with computer antimalware software to more effectively stop certain cyber security threats (e.g., computer viruses).

The results suggest that the utility associated with antimalware software varied significantly. First, approximately 23% of survey respondents preferred no antimalware software over any package they were shown. Several potential explanations exist for this:

- These individuals receive free antimalware so don't think they should ever have to pay for antimalware
- These individuals do not perceive themselves as the potential target of cyber threats
- These individuals do not believe that antimalware will improve their cyber security
- These individuals believe that the costs of antimalware will always outweigh the benefits

In reality individuals who always "opted out" of the all antimalware software packages when such an option was offered likely fall into several of these categories of thinking.

Further, a large group of survey respondents (almost 25%), selected choices that were not rational. This suggests that the costs and benefits are not easily weighed, resulting in responses that were not well thought out. Some individuals may have had difficulty identifying the most rational choice given the complexity of the antimalware characteristics; for example, the fact that two of the characteristics (one cost and one benefit) discuss the impact on computer performance may have been confusing.

However, the majority of survey respondents indicated that they were interested in purchasing some antimalware software. The marginal willingness to pay estimates (indicating the WTP when comparing the best to the worst level within each attribute) for this entire group were as follows:

- $55.50 per year so that computer performance *does not decrease* after installing antimalware software
- $51.23 per year to *greatly reduce* the risk of identity theft
- $40.43 per year to *greatly reduce* the risk of computer crashing or slowing down
- $25.94 per year to *greatly reduce* the risk of malware to others computers
- $0.10 per year to *avoid* 1 minute of time managing antimalware software each month

The highest marginal WTP estimate and the lowest are both costs, so the WTP is more accurately a willingness to avoid the cost. Looking at a variety of risk factors, the following conclusions were drawn about groups within this overall sample:

- Individuals who had contracted a virus previously were willing to pay 19% more than those who had not previously contracted a virus to greatly reduced the risk of their computer slowing down or crashing.
- Individuals who scan their system for malware threats more frequently, among those who have antimalware install on their computers, value risk reductions more than those who scan their systems less frequently.
- Individuals who scan their system for malware threats *less* frequently value computer performance more than those who scan their systems more frequently.
- Individuals who are more risk averse are willing to pay more for all antimalware benefits than individual who are less risk averse, and more risk averse individuals are willing to accept more costs than less risk averse individuals.

The results of this research offer new information to help advance understanding of cyber security risk preferences, which can be used by both the private and public sectors to improve cyber security behaviors. For example, producers of cyber security products and services could use this information to improve the ways in which the market and sell to customers. Further, from a social perspective, these results could be used by government agencies to help design cyber security educational strategies informed by a better understanding of what costs and benefits resonate with individuals and how to target certain subpopulations.

Additional research is needed to assess how public health research can be further utilized to improve cyber security. Research is needed to assess how specifically the public health community uses research on risk perceptions to improve public health outcomes, which may offer insights to the cyber security community. Further, better understanding how communication strategies are developed in public health could help the public and private sectors improve cyber security education and marketing.

References

Anderson LR, Mellor JM. (2008) Predicting health behaviors with an experimental measure of risk preference. *Journal of Health Economics*, 2008 Sep;27(5):1260-74.

Bishai D, Brice R, Girod I, Saleh A, Ehreth J. (2007) Conjoint analysis of French and German parents' willingness to pay for meningococcal vaccine. *Pharmacoeconomics*. 2007; 25(2):143-54.

Brown DS, Johnson FR, Poulos C, Messonnier ML. Mothers' preferences and willingness to pay for vaccinating daughters against human papillomavirus. Vaccine. 2010 Feb 17;28(7):1702-8.

Consumer Reports (2012). *Ratings and Recommended Security Software.* Retrieved from: http://www.consumerreports.org/cro/security-software.htm.

de Bekker-Grob EW, Hofman R, Donkers B, van Ballegooijen M, Helmerhorst TJ, Raat H, Korfage IJ. (2010) Girls' preferences for HPV vaccination: a discrete choice experiment. *Vaccine*. 2010 Sep 24;28(41):6692-7.

Flood EM, Ryan KJ, Rousculp MD, Beusterien KM, Divino VM, Block SL, Hall MC, Mahadevia PJ. (2011) Parent preferences for pediatric influenza vaccine attributes. *Clin Pediatr (Phila)*. 2011 Apr; 50(4):338-47.

Krinsky I, Robb A (1986) On approximating the statistical properties of elasticities. Rev Econ Stat 68:715–719.

Krinsky I, Robb A (1990) On approximating the statistical properties of elasticities: A correction. Rev Econ Stat 72:189-90.

Kuhfeld WF, Tobias RD, Garratt M (1994) Efficient experimental design with marketing research applications. J Mark Res 31:545–557.

Liau A, Zimet GD. (2001) The acceptability of HIV immunization: examining vaccine characteristics as determining factors. *AIDS Care.* 2001 Oct;13(5):643-50.

Mansfield, C., Phaneuf, D., Johnson, F.R., Yang, J., Beach, R. (2008) Preferences for Public Lands Management under Competing Uses: The Case of Yellowstone National Park. *Land Economics*. 84 (2): 282–305

Newman PA, Lee SJ, Duan N, Rudy E, Nakazono TK, Boscardin J, Kakinami L, Shoptaw S, Diamant A, Cunningham WE. (2009) Preventive HIV vaccine acceptability and behavioral risk compensation among a random sample of high-risk adults in Los Angeles (LA VOICES). Health Serv Res. 2009 Dec;44(6):2167-79.

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

Orme, B. and R. Johnson. (2010). Including Holdout Choice Tasks in Conjoint Studies. Retrieved from http://www.sawtoothsoftware.com/download/techpap/inclhold.pdf.

OPSWAT (2012). *Security Industry Market Share Analysis.* March 2012. Retrieved from: http://www.opswat.com/sites/default/files/OPSWAT-market-share-report-march-2012.pdf

Oteng B, Marra F, Lynd LD, Ogilvie G, Patrick D, Marra CA. (2011) Evaluating societal preferences for human papillomavirus vaccine and cervical smear test screening programme. *Sex Transm Infect*. 2011 Feb;87(1):52-7.

Raley JC, Followwill KA, Zimet GD, Ault KA. (2004) Gynecologists' attitudes regarding human papilloma virus vaccination: a survey of Fellows of the American College of Obstetricians and Gynecologists. Infect Dis Obstet Gynecol. 2004 Sep-Dec;12(3-4):127-33.

Rowe, B. R., Halpern, M. T., and Lentz, A. W. (2012). Is a Public Health Framework the Cure for Cyber Security? *CrossTalk: The Journal of Defense Software Engineering*. November/December 2012, 30–38.

Rowe B, Wood D, Reeves D, Braun F. (2011) Economic analysis of ISP provided cyber security solutions. Retrieved from https://www.ihssnc.org/portals/0/Rowe_IHSS_Cyber_Final_ReportFINAL.pdf.

Sawtooth Software, Inc. (2010). *SSI Web v.6.6.12: Choice Based Conjoint* [Computer Software]. Sequim, WA.

Stockwell MS, Rosenthal SL, Sturm LA, Mays RM, Bair RM, Zimet GD. (2011) The effects of vaccine characteristics on adult women's attitudes about vaccination: a conjoint analysis study. Vaccine. 2011 Jun 15;29(27):4507-11.

Train K (2003) Discrete choice methods with simulation. Cambridge University Press, Cambridge.

Wilcox, Joe (2012). *Three-quarters of Mac Owners Don't Use Anti-malware Software.* Betanews, April, 2012. Retrieved from: http://betanews.com/2012/04/06/three-quarters-of-mac-owners-dont-use-anti-malware-software/.

Zimet GD, Mays RM, Sturm LA, Ravert AA, Perkins SM, Juliar BE. (2005) Parentalattitudes about sexually transmitted infection vaccination for their adolescent children. Arch Pediatr Adolesc Med. 2005 Feb;159(2):132-7.

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

Appendix: Survey of Your Views on Cyber Security

Thank you for agreeing to participate in this research study. The goal of this survey is to better understand what you would be willing to do to protect your computer from unauthorized access or attack.

Informational Background

One of the most common threats to your computer's security (**cyber security**) is malicious software (**malware**) that is designed to disrupt your computer's operation, gather sensitive information, and/or use your computer to cause harm to others. Common examples of malware include:
Computer virus – computer software (often attached to legitimate programs or email messages) that can cause harm to your computer.

- Computer worm – a program that infects computers by using "holes" in computer software and can cause harm to your computer.
- Trojan horse – a program that claims to do one thing (e.g., initiate a game) but instead can cause harm to your computer when it is run.
- Spyware – a program installed on your computer to collect information about you without your knowledge.

One way to protect your computer from this threat is to install **antimalware software**, which can identify and remove malware from your computer.

The Survey

In this survey, we will first ask a series of background questions regarding your computer and internet usage habits. Next, we will ask questions about how you view cyber security threats and what steps you take to protect yourself against them. We will then describe the costs and benefits of antimalware software and ask you to choose between different antimalware software products (in a hypothetical scenario).

The survey should take about **25 minutes** to complete and is being conducted by researchers at Research Triangle Institute, a non-profit research organization. If you have any problems or concerns about this survey, please contact Panel Relations at 800-782-7699, and someone will direct your questions to the appropriate researchers at the Research Triangle Institute.

Part I. Questions about Your Current and Previous Personal Computers and Your Home Internet Connection

In this section we are going to ask you questions about your current personal computer(s) and previous personal computer(s). First, we would like to ask you some questions about the computer(s) you currently use and the one you use most often.

1. How many different computers do you typically use in an average week? (including computers owned by the company you work for and computers you own personally)

   _____

   [If "0" to Q1, drop out]
   [If "1" to Q1, ask the following]

   Is this a work-owned computer or computer you own personally?
   __ Work-owned computer
   __ Personally-owned computer
   [If "Work-owned computer", drop out]

If you use more than one computer in a given week, please think about the computer that you personally own that you use most often. From now on, we will refer to this computer as your "CURRENT PERSONAL COMPUTER" throughout this survey.

2. Are you the primary person responsible for making sure your CURRENT PERSONAL COMPUTER is secure?
   __Yes
   __No
   [If "No"] Does your input play an important role in security decisions for this computer?
   __Yes
   __No
   [If No to Q3, drop out of survey]

3. Who manufactured your CURRENT PERSONAL COMPUTER?
   __Apple
   __PC (e.g., Lenovo/IBM, Dell, Toshiba, Acer, etc.)
   __Other (Please specify____)

4. Please tell me if you ever use the internet to do any of the following things. Do you *ever* use the internet to…?
   __Send or read e-mail
   __Get news online
   __Research a product or service online
   __Take part in chat rooms or online discussions with other people
   __Play online games
   __Search online for a map or driving directions
   __PAY to access or download digital content online, such as music, video, or newspaper articles
   __Pay bills online
   __Use a social networking site like Facebook or LinkedIn.com
   __Categorize or tag online content like a photo, news story or blog post

__Post a comment or review online about a product you bought or a service you received
__Use Twitter or another service to share updates about yourself or to see updates about others

5. How many hours do you spend using your CURRENT PERSONAL COMPUTER per day, on average?

   _____ hours per day

   a. Of the total time you spend using your CURRENT PERSONAL COMPUTER per day, what *portion* is devoted to each of the following, on average:
      ___% sending personal emails
      ___% surfing the internet (e.g., looking for news, gossip, etc.)
      ___% playing games
      ___% using online applications (e.g., Facebook, banking, Google Docs, Dropbox, etc.)

6. Do you feel capable of installing software on your CURRENT PERSONAL COMPUTER without any help?
   ☐ Yes
   ☐ No
   ☐ Depends on what software

7. Do you have a smartphone?
   __Yes
   __No

   If Yes, How much time do you spend using the internet on your smartphone each day? _____ minutes

Part II. Questions about Your Cyber Security Habits and Views

In this section, we are going to ask you questions about how you view cyber security threats and what steps you take to protect yourself against them. First, we would like to learn more about your personal experience with cyber security threats.

8. In the past, do you think you have had malware problems with any computer you have owned?
   ☐ Yes
   ☐ No
   ☐ Don't Know

   <Programmer note: If YES, show the following>

   a. How much time did you spend trying to fix each problem on average?
      _____ hours

   b. How much money did you spend trying to fix each problem on average?
      $ _____

9. To your knowledge, has your CURRENT PERSONAL COMPUTER been infected by malware in the last year?
   ☐ Yes
   ☐ No
   ☐ Not sure
   ☐ Don't know what malware is

   <If Yes to Q10, show this>

   What malware do you believe that your CURRENT PERSONAL COMPUTER has been infected with in the last year?
   ☐ Virus(s)
   ☐ Worm(s)
   ☐ Trojan horse
   ☐ Spyware
   ☐ Not sure

The next set of questions are designed to better understand how you think about malware and potential costs involved.

10. Has a computer professional recommended that you should get antimalware, should not get antimalware, or did not give a recommendation either way?
    ☐ Recommended I get antimalware
    ☐ Recommended I not get antimalware
    ☐ Did not give recommendation either way
    ☐ I have not spoken to a computer professional recently
    ☐ Don't know

11. Do you believe the following could happen through the internet? (check all that apply)
    - ☐ Somebody could steal information off of your computer – e.g., files, passwords, etc.
    - ☐ Somebody could "take over" your computer to attack others
    - ☐ Somebody could prevent you from using your computer
    - ☐ Somebody could make your computer explode
    - ☐ Somebody could use your computer to turn on/off power to your home

12. We want to find out how you think you would be affected if your computer was infected by malware. Thinking about your ability to carry out the usual activities for which you use your computer, do you think your usual activities would be very affected, somewhat affected, not very affected, or not affected at all if your computer got malware?
    - ☐ Very affected
    - ☐ Somewhat affected
    - ☐ Not very affected
    - ☐ Not affected at all
    - ☐ Don't know

    The following questions are meant to learn more about what steps you take to protect yourself from malware , how much importance you attach to these measures, and how you view antimalware software packages in general.

13. Do you have antimalware software installed on your CURRENT PERSONAL COMPUTER?
    - ☐ Yes
    - ☐ No
    - ☐ Don't Know

    <Programmer Note: If "YES" to Q14 show the following. Otherwise, skip to Q17>

14. What antivirus software do you have installed on your CURRENT PERSONAL COMPUTER?
    - ☐ Symantec / Norton
    - ☐ AVG
    - ☐ Avast
    - ☐ Microsoft Security Suite
    - ☐ Avira
    - ☐ McAfee
    - ☐ Panda
    - ☐ Kaspersky
    - ☐ ESET
    - ☐ Trend Micro
    - ☐ Other
    - ☐ Don't know

15. How did you purchase / acquire your antimalware software?
    - ☐ Bought online
    - ☐ Bought in a store
    - ☐ Download free version through Facebook
    - ☐ Downloaded free version through my internet service provider (ISP) – e.g., Comcast, Verizon, Time-Warner Cable, or AOL
    - ☐ Downloaded free version through my bank

☐ Other (_____)
☐ Don't know

<Programmer Note: If "NO" to Q14 show the following. Otherwise, skip to Q18>

16. Please indicate whether each of the following is a reason why you have not installed antimalware software on your CURRENT PERSONAL COMPUTER. (Check all that apply).
☐ You've never had any problem with malware.
☐ Installing antimalware takes too much time.
☐ You're not at high risk of getting malware.
☐ You were concerned about the negative effects of antimalware on your computer.
☐ You believe that antimalware does not work very well.
☐ You do not trust what the government says about malware.
☐ Antimalware costs too much.

<Programmer Note: If Q17 is shown, afterwards skip to Q20>

17. Approximately when was the last time your antimalware software scanned your CURRENT PERSONAL COMPUTER for malware?
☐ 1 week ago or less
☐ 2 weeks ago
☐ Over a month ago
☐ Over six months ago
☐ Over a year ago
☐ It runs automatically
☐ I don't know

18. Approximately when was the last time your antimalware software installed on your CURRENT PERSONAL COMPUTER was updated?
☐ 1 week ago or less
☐ 2 weeks ago
☐ Over a month ago
☐ Over six months ago
☐ Over a year go
☐ It runs automatically
☐ I don't know

19. Do you believe that antimalware software could have the following impact(s)? (check all that apply)
☐ Slow down your computer
☐ Speed up your computer (because of fewer viruses)
☐ Protect against identity theft
☐ Protect against other people being affected by malware on your computer

20. How effective do you think antimalware software is at reducing cyber security threats to your computer?
☐ Very Effective
☐ Somewhat effective
☐ Somewhat ineffective
☐ Very Ineffective
☐ I don't know

21. How much do you think you can trust antimalware companies like McAfee, Symantec and AVG to reduce cyber security threats to your computer?
☐ Completely
☐ Somewhat
☐ Not at all
☐ Don't Know

22. How important do you believe the following pieces of security advice are to keep your computer safe?

	Important	Somewhat Important	Not Important	Not Applicable
Use antimalware software				
Keep antimalware updated				
Regularly scan computer with antimalware (if it doesn't scan itself automatically)				
Use firewall (software or hardware that controls information coming to or going from your computer)				
Don't click on attachments in emails from people you don't know				
Be careful downloading from websites				
Be careful which websites you visit				
Use passwords that are hard for others to figure out				
Keep software up to date (e.g. Windows updates)				
Turn off computer when not in use				

23. What are you most concerned about when using the internet? (Check all that apply.)
☐ Someone stealing your personal information (e.g., passwords, social security number, other personal files)
☐ Criminals gaining access to your online banking information (e.g., credit card numbers, bank account numbers)
☐ Your computer crashing or hard drive being erased
☐ The government tracking you
☐ Having sensitive personal information released without your permission
☐ Other (_____)
☐ Not afraid of anything

Part III. Costs of Using Antimalware Software

In this section we will describe **3** different costs associated with using antimalware software:

A. Price for one year of antimalware software service
B. Time spent each month using antimalware software
C. Speed of computer performance after installing antimalware software
D.

The next few pages will provide additional information on these costs and will ask you some questions about each of them.

A. Price for one year of antimalware software service

When you purchase antimalware software, the initial price you pay typically covers one year of up-to-date protection against malware. Later in the survey we will ask you to choose between hypothetical antimalware software products that differ based on how much they cost for one year of protection against malware. The prices of these hypothetical antimalware software products will be one of the following:

- $0
- $10
- $40
- $80

In actuality, some people pay for their antimalware software while some people use "freeware" antivirus program or get their antimalware software for free through their Internet service provider (ISP), Facebook, or bank. In this survey, when we show you hypothetical scenarios, please assume you would pay the full prices shown and select your preferred option accordingly.

In the section immediately below, please answer the questions based on what you are actually paying for your antimalware software.

<Programmer Note: If YES to Q14, show the following>

1. Previously in the survey, you indicated that you have antimalware software installed on your CURRENT PERSONAL COMPUTER. How much did you initially pay for this software?
   $___

2. Do you pay a yearly subscription fee for your antimalware software?
   ___ Yes
   ___ No

   If Yes, approximately how much do you pay? $___ per year

   <Programmer Note: If NO to Q14, show the following>

3. Previously in the survey, you indicated that you do not have antimalware software installed on your CURRENT PERSONAL COMPUTER. If you were considering buying antimalware software, what is the most you think you would pay for this software?
$___

B. Time spent each month using antimalware software

Each month you may spend time maintaining and using your antimalware software. This includes taking time to update your virus definitions and scanning your computer for viruses. Later in the survey, we will ask you to choose between several hypothetical antimalware software products that differ in terms of the amount of time required to maintain and use the antimalware software properly. The amount of time you will be asked to spend per month using these hypothetical antimalware software products will be one of the following options:

- 0 minutes per month
- 10 minutes per month
- 40 minutes per month
- 60 minutes per month

1. Approximately how much time have you spent in the **past year** securing your computer (e.g., updating antimalware software, scanning your computer for harmful software, dealing with a suspected virus/worm/spyware, etc)?
__None
__30 minutes
__1 hour
__2 hours
__3-4 hours
__5-6 hours
__7-8 hours
__8 hours or more

2. Would you be **willing to spend** more time than you currently do securing your computer each month to reduce cyber security threats to your computer?
☐ Yes
☐ No

3. How **effective** do you think that spending at least 30 minutes per month securing your computer would be at reducing cyber security threats to your computer?
☐ Very Effective
☐ Somewhat effective
☐ Somewhat ineffective
☐ Very Ineffective
☐ I don't know

C. Speed of computer performance after installing antimalware software

Using antimalware software can sometimes slow down your computer (i.e., slow how fast programs run on your computer). This is because the software regularly scans files you download to your computer, checks for software updates, and performs other duties that divert resources away from other activities.

Later, we will ask you to choose between hypothetical antimalware software products that differ in terms of how much they change the speed of your computer's performance. The change in the speed of your computer's performance associated with each hypothetical software product will be one of the following:

- No Change – Antimalware software will not change the speed of your computer's performance
- Somewhat Slows Down – Antimalware software will somewhat slow down the speed of your computer's performance
- Greatly Slows Down – Antimalware software will greatly slow down the speed of your computer's performance

1. Would you be **willing to allow** your antimalware program to limit your access to the internet in some way in order to protect you from attacks?
   ☐ Yes
   ☐ No

2. By how much do you think antimalware software is likely to decrease the performance of your computer?
   ☐ Significant decrease in performance
   ☐ Some decrease in performance
   ☐ No decrease in performance
   ☐ I don't know

Part IV. Benefits of Using Antivirus Software

In this section we will describe **3** different cyber security benefits that will result from using antimalware software:

A. Reduced risk of your computer slowing down or crashing
B. Reduced risk of your identity being stolen
C. Reduced risk to other individuals and businesses from malware that has gotten on your computer

The next few pages will provide additional information on these benefits and will ask you some questions about each of them.

A. Reduced Risk of Your Computer Slowing Down or Crashing

The purpose of antimalware software is to reduce threats to cyber security. One way to judge the effectiveness of these software packages is whether they reduce the risk of malicious software slowing down or crashing your computer. For example, antimalware software could help to ensure that your computer applications—such as your internet browser, email, or word processing software—do not run slower as a result of malware.

Later in the survey, we will ask you to choose between antimalware software products that differ in terms of how much they reduce the risk of your computer slowing down or crashing due to malware. The following options will be shown:

- Not Reduced – the risk of your computer slowing down or crashing will not be reduced (that is, it will be the same as before you installed the antimalware software)
- Somewhat Reduced – the risk of your computer slowing down or crashing will be somewhat reduced
- Greatly Reduced – the risk of your computer slowing down or crashing will be greatly reduced

1. Do you think your CURRENT PERSONAL COMPUTER runs slowly?
   ☐ Yes
   ☐ No

   If Yes, do you think this is because of a cyber security issue?
   ☐ Yes
   ☐ No

2. What is the chance of your computer slowing down or crashing from cyber security threats/attacks in the next year?

|_____|_____|_____|_____|_____|_____|_____|_____|_____|_____|

0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

Zero Equal chance (50/50) Definitely

3. How **effective** do you think antimalware software is at reducing the risk of malware causing your computer to slow down or crash?
   - ☐ Very Effective
   - ☐ Somewhat effective
   - ☐ Somewhat ineffective
   - ☐ Very Ineffective
   - ☐ I don't know

B. Reduced Risk of Your Identity Being Stolen

Another way to judge the effectiveness of antimalware software is whether it reduces the risk of having your identity stolen (e.g., your credit card, social security number, bank account number being used without your permission commit fraud or other crimes).

Later in the survey, we will ask you to choose between antimalware software products that differ in terms of how much the risk of your identity being stolen has been reduced. The amount each hypothetical antimalware software product will reduce the risk of your computer slowing or crashing will range between:

- Not Reduced – the risk of your identity being stolen will not be reduced (that is, it will be the same as before you installed the antimalware software)
- Somewhat Reduced – the risk of your identity being stolen will be somewhat reduced
- Greatly Reduced – the risk of your identity being stolen will be greatly reduced

1. Research studies show that in 2011 alone, 11.6 million adults in the United States were the victims of identity theft out of a total adult population of roughly 235 million. If this trend continues, this means that on average, 50 out of 1,000 adults (5%) will have their identities stolen over the next year. What do you think are your own chances of having your identity stolen some time in the next year compared to the average chances of 5% (50 out of 1,000)?
   - ☐ Much higher than the average (about 25% risk of having identity stolen)
   - ☐ Higher than the average (about 10% risk of having identity stolen)
   - ☐ About the same as the average (about 5% risk of having identity stolen)
   - ☐ Lower than the average (about 2.5% risk of having identity stolen)
   - ☐ Much lower than the average (about 1% risk of having identity stolen)

2. Have you ever been the victim of identity theft? For example, has your credit card, social security number, or bank account been stolen and used to commit fraud?
   ☐ Yes
   ☐ No

3. How effective do you think antimalware software is at reducing the risk of malware causing your identity to be stolen?
   ☐ Very Effective
   ☐ Somewhat effective
   ☐ Somewhat ineffective
   ☐ Very Ineffective
   ☐ I don't know

C. Reduced Risk to Other Individuals and Businesses from Malware on Your Computer

The level of security on your computer can also have an impact on other people. For example, if your computer is infected with malware, then it is possible that your computer may be hijacked and used to attack businesses or other home internet users. This could mean that businesses have data stolen or their computer systems stop working for a period of time because your computer was used to attack them, or that your computer puts other individual computer users at a higher risk of being infected or having their identity stolen.

Later in the survey, we will ask you to choose between antimalware software products that differ in terms of how much the risk to other individuals and businesses from malware on your computer has been reduced. The amount each hypothetical antimalware software product will reduce the risk to others from malware on your computer will range between:

- Not Reduced – the risk to other individuals and businesses will not be reduced (that is, it will be the same as before you installed the antimalware software)
- Somewhat Reduced – the risk to other individuals and businesses will be somewhat reduced
- Greatly Reduced – the risk to other individuals and businesses will be greatly reduced

1. In general, how important is it to you personally to help others in need?
   ☐ Essential
   ☐ Very important
   ☐ Somewhat important
   ☐ Not important

2. How effective do you think antimalware software is at reducing the risk of malware on your computer affecting other individuals or businesses?
   ☐ Very Effective
   ☐ Somewhat effective
   ☐ Somewhat ineffective
   ☐ Very Ineffective
   ☐ I don't know

3. How important do you think it is that your antimalware software reduce the risk your computer could pose to other individuals or businesses?
   ☐ Very important

☐ Somewhat important
☐ Somewhat unimportant
☐ Very unimportant
☐ I don't know

Part V. Which Product Would You Buy?

For the next set of questions, assume that you are purchasing a new antimalware software package. As with most purchases, you can choose from a variety of different products. However, each product has its own costs and benefits that you must weigh before making your choice. Specifically, each antimalware software product will be described by the following costs and benefits:

Costs

- Price for one year of antimalware software service
- Time spent each month using antimalware software
- Speed of computer performance after installing antimalware software

Benefits

- ***Reduced risk of your computer slowing down or crashing***
- ***Reduced risk of your identity being stolen***
- ***Reduced risk to other individuals and businesses from malware on your computer***

NOTE: Please examine the products carefully and think about which product you would actually buy in this situation. Some people are more willing to choose expensive products when payment is only imagined than when payment is real. Therefore, we urge you to consider your choice as though you would really be paying the amount stated. Knowing how you would actually choose between these products is very important to the people who have to make decisions about cyber security.

Assume you have two options for the antimalware software products you will buy, Product A or Product B. In this initial choice, the only difference between the two options is the price and whether the risk of your computer crashing has been reduced (the rows shaded in gray). The price of Product A is lower than the price of Product B, but Product A does not reduce the risk of your computer crashing. So ask yourself whether you believe greatly reducing the risk of your computer crashing (offered under Product B) is worth paying $30 more.

Please consider both options carefully and answer the questions under the table.

	Product A	Product B
Costs of Antimalware Software		
Price for one year of antimalware software service.	**$10**	**$40**
Time spent each month using antimalware software	**0 hours per month**	**0 hours per month**
Speed of computer performance after installing antimalware software	No Change	No Change
Benefits of Antimalware Software		
Risk of your computer slowing down or crashing	Not Reduced	Greatly Reduced
Risk of your identity being stolen	Somewhat Reduced	Somewhat Reduced
Risk to Other Individuals and Businesses from Malware on Your Computer	Somewhat Reduced	Somewhat Reduced

If these two were your only options, which product would you choose?
(Please check only 1 box)

A☐ B☐

You chose Product “[insert name of option selected]” as your preferred option. [Show only the option Selected below]

Suppose you were actually offered this antimalware software product in real life. Would you buy it for use on your CURRENT PERSONAL COMPUTER?

☐ Yes
☐ No

Now suppose you were asked to make a choice between two products where all 3 of the costs and all 3 of the benefits may differ between them. Please consider both products carefully. There may be good reasons for you to choose either product. Only you know what is best for you and your household.

	Product A	Product B
Costs of Antimalware Software		
Price for one year of antimalware software service.		
Time spent each month using antimalware software		
Speed of computer performance after installing antimalware software		
Benefits of Antimalware Software		
Risk of your computer slowing down or crashing		
Risk of your identity being stolen		

Risk to Other Individuals and Businesses from Malware on Your Computer		

If these two were your only options, which product would you choose?
(Please check only 1 box)

A☐ B☐

You chose Product "[insert name of option selected]" as your preferred option. [Show only the option Selected below]

Suppose you were actually offered this antimalware software product in real life. Would you buy it for use on your CURRENT PERSONAL COMPUTER?

☐ Yes
☐ No

<**Programmer Note:** The following question would appear randomly after some conjoint question>

Now suppose you were actually given this anti-malware software product, please describe whether and how having this software would influence your computing habits. Specifically, would you increase or decrease the following behaviors?

Using peer-to-peer or file-sharing software (such as uTorrent, Limewire, or Bitorrent).

☐ Definitely increase
☐ Possibly increase
☐ Neither increase or decrease
☐ Possibly decrease
☐ Definitely decrease

Ignoring system (e.g. Windows) updates.

☐ Definitely increase
☐ Possibly increase
☐ Neither increase or decrease
☐ Possibly decrease
☐ Definitely decrease

Keeping personal information such as account numbers, social security numbers, login information and passwords stored in text file on your computer.

- ☐ Definitely increase
- ☐ Possibly increase
- ☐ Neither increase or decrease
- ☐ Possibly decrease
- ☐ Definitely decrease

<<PROGRAMMER NOTE: CONJOINT BRIEFING QUESTIONS (TO BE SHOWN AFTER ALL CONJOINT QUESTIONS ARE ANSWERED**>>**

1. In your opinion, how likely do you think it is that policy makers or antimalware software companies will consider the results from this survey to make decisions about cyber security policy and investments?
   - ☐ Very likely
   - ☐ Somewhat likely
   - ☐ Even chances
   - ☐ Somewhat unlikely
   - ☐ Very unlikely
   - ☐ No opinion

2. Did you find the choices between the antimalware software products easy or difficult to answer?
   - ☐ Easy
   - ☐ Somewhat easy
   - ☐ Somewhat difficult
   - ☐ Difficult

3. What was the most important attribute in your decision making?
   - ☐ Price for one year of antimalware software service
   - ☐ Time spent each month using antimalware software
   - ☐ Speed of computer performance after installing antimalware software
   - ☐ Risk of your computer slowing down or crashing
   - ☐ Risk of your identity being stolen
   - ☐ Risk to other individuals and businesses from malware on your computer

4. Which of the following statements best describes how you chose between the antimalware software products?
   - ☐ I always chose the option with the lowest price
   - ☐ I always chose the option with the least time associated with using antimalware software
   - ☐ I always chose the option with the where the speed of my compute's performance changed the least after installing antimalware software
   - ☐ I always chose the option with the most reduction in risk of computer slowing down or crashing
   - ☐ I always chose the option with the most reduction in risk of identity theft
   - ☐ I always chose the option where the most reduction in risk toward others
   - ☐ I did not base my choice on a single strategy or outcome.

Part VI. Questions About You and Your Family

The survey is nearly complete. We just have a few more questions about you.

1. What is your age (in years)?
   _____

2. What is your race? Please check all that apply.
   ☐ White
   ☐ Black or African American
   ☐ American Indian or Alaska Native
   ☐ Asian
   ☐ Native Hawaiian or Other Pacific Islander
   ☐ Some other race

3. Do you consider yourself Hispanic or Latino?
   ☐ Yes
   ☐ No
   ☐ Don't know or prefer not to say

4. What is your sex?
   __Male
   __Female

5. What is the highest level of schooling you have completed?
   ☐ Some high school, no diploma
   ☐ High school diploma or the equivalent (for example GED)
   ☐ Some college, no degree
   ☐ Associate degree (for example: AA, AS)
   ☐ Bachelor's degree (for example: BA, AB, BS)
   ☐ Master's degree (for example: MA, MS, MEng, MEd, MSW, MBA)
   ☐ Doctorate or Professional degree (for example: PhD, EdD, MD, DDS, JD)

6. What is your current employment status?
   ☐ Working full-time
   ☐ Working part-time
   ☐ Temporarily laid off
   ☐ Unemployed
   ☐ Retired
   ☐ Disabled
   ☐ Homemaker
   ☐ Student

7. The next question is about the <u>total income</u> of YOUR HOUSEHOLD for the PAST 12 MONTHS. Please include your income PLUS the income of all members living in your household (including cohabiting partners and armed forces members living at home). Please count income BEFORE TAXES and from all sources (such as wages, salaries, tips, net income from a business, interest, dividends, child support, alimony, and Social Security, public assistance, pensions, or retirement benefits).

For the PAST 12 MONTHS, how much did all members of your household earn before taxes?
☐ None or less than $9,999
☐ $10,000-$29,999
☐ $30,000 -$49,999
☐ $50,000 -$74,999
☐ $75,000-$99,999
☐ $100,000-$119,999
☐ $120,000 and over

8. Generally speaking, do you usually think of yourself as a REPUBLICAN, a DEMOCRAT, an INDEPENDENT, or something else?
☐ Republican
☐ Democrat
☐ Independent
☐ Other party
☐ No preference

9. Generally speaking, do you believe the **federal government** should have a role in improving cyber security for American citizens?
☐ Yes
☐ No

<Programmer Note: if YES, show the following>

a. What role(s) do you think the federal government should have in improving cyber security? (select all that apply)
☐ Require ISPs to provide more security for their customers
☐ Require software makers to meet a certain level of security

☐ Pay (subsidize) ISPs to provide more security for their customers
☐ Pay (subsidize) software makers to meet a certain level of security

☐ Other (_____)

10. How much of the time do you think you can trust the federal government to do what is right?
☐ Just about always
☐ Most of the time
☐ Only some of the time
☐ Never

11. Do you think overall government spending in the U.S. is:
☐ Too High
☐ About Right
☐ Too Low

12. Do you currently smoke cigarettes?
☐ Yes, daily
☐ Yes, occasionally
☐ No, never

13. How often do you do the following?

	Always	Sometimes	Never
Wear your seatbelt in a moving vehicle			
Floss your teeth daily			
Get flu shots every year			
Wear sunscreen when you are in the sun			