Part 2

Note: This is the second part of the report. Part 2 includes the Detailed Findings section of the report with responses to the specific questions, charts and all appendices. Part I includes the abstract, introduction, summary and analysis.

A Look at Consumers' Awareness of Email Security and Practices

or

"Of Course, I Never Reply to Spam – Except Sometimes"

Research conducted for the
Messaging Anti-Abuse Working Group
(MAAWG)

by

Insights Worldwide Research

MAAWG
Messaging Anti-Abuse Working Group
P.O. Box 29920 ■ San Francisco, CA 94129-0920 ■ www.MAAWG.org ■ info@MAAWG.org

A Look at Consumers' Awareness of Email Security and Practices
or
"Of Course, I Never Reply to Spam – Except Sometimes"

Note: The report abstract and introduction are reprinted here. See Part 1 for additional analysis.

Abstract

This survey was commissioned by the Messaging Anti-Abuse Working Group (MAAWG) to gain a better understanding of consumers' awareness of the risks associated with viruses and "bots" spread through email and to determine how the industry can best work with consumers in dealing with important messaging threats. The research covers bot awareness and also asks the frequently voiced question: "Why did you click on that spam link?" It identifies the specific actions consumers take to protect themselves against viruses and junk mail, looks at consumers' attitudes toward virus mitigation, and seeks to quantify and understand consumers' email habits.

One of the most striking results from this research is that while 82% of consumers are aware of "bots" and malware threats, only 20% believe there is a very good chance their computers could get infected. Yet, as reported in the *Financial Times*[1], a majority of junk email today originates from bot-infected computers that are surreptitiously sending spam, which would indicate significantly more consumers' machines are polluted than users would suspect. The data from this survey creates a picture of users familiar with general email-based threats but not necessarily as alert or cautious as they should be to proactively protect themselves against spam, online fraud and other email-related hazards. There also is no general consensus among consumers as to how network operators and industry vendors should interact with customers when addressing these issues.

This is the first consumer survey undertaken by the Messaging Anti-Abuse Working Group, which is the largest global trade association bringing together all elements of the messaging industry – including Internet Service Providers (ISPs), email providers, volume senders and vendors – to cooperate against messaging abuse. MAAWG is the only organization addressing spam and other emerging threats by systematically engaging all aspects of the problem, including technology, industry collaboration and public policy.

The research presented here is based on 800 interviews of general consumers conducted by Insights Worldwide Research with MAAWG participation in developing the questions and analysis of the results. Once the survey was complete, the analyst firm Ferris Research, Inc. was invited to provide additional insights into the findings, which also are included in this report.

[1] *Financial Times*, "Secret war on web crooks revealed," by Maija Palmer. Published: June 15 2009 3:00 http://www.ft.com/cms/s/0457bd68-5945-11de-80b3-00144feabdc0.html

Table of Contents

Explanation of Appendices: In Appendix A, we provide additional cross-tabulated data that may be relevant to specific industry constituents but that does not necessarily reflect general trends or correlations. The cross-tabulated data is provided for selected questions only. The data and charts available in Appendix A also are referenced at the end of each corresponding question in the main "Detailed Findings" section.

Appendix B is a summary of selected data points as they apply to consumers' willingness to allow remote access to their computers for the purpose of removing bots. During the survey, we asked consumers if they would allow ISPs or vendors to access their computers to remove viruses, then cross-tabulated the responses with some of the other questions. This information is provided to help network operators better understand how they can assist customers whose systems are infected.

Appendix C provides the demographic information for the 800 survey respondents, and the survey questionnaire is provided in Appendix D.

I. Introduction

Executive Summary

Most spam originates from computers infected with a "bot,"[2] which is malware covertly downloaded to a computer and used to send spam or carry out other malicious functions without the owner's knowledge. Consequently, that annoying email pushing an erectile dysfunctional drug or the fake bank message asking for personal information very likely could have originated from a computer owned by a upright grandmother who uses email to share family photos or an unsuspecting teenager checking out social networking sites, without either of them being aware their computers were sending the spam.

Considering that 85% to 90% of all email traffic is considered abusive – with a high portion of this volume blocked before it hits users' inbox (see the MAAWG email metrics reports at www.MAAWG.org) – the volume of bot-generated spam is an enormous problem. Bots are often spread when unsuspecting consumers open an infected email, which is frequently sent as spam itself, or when consumers click on links within spam messages that lead to poisoned Web sites.

According to the data from this survey, one in six consumers responded to a message they suspected might have been spam. Although a small percentage of the computing population, these numbers still earn a significant enough return on investment to support a booming spam-driven underground economy.

Most reputable Internet Service Providers and email providers are responding to this threat both by taking action to protect users from malware and by assisting customers with infected machines to remove the bot. The Messaging Abuse Working Group is preparing to release new best practices to help network operators understand how they can best help customers remove malware when found on users' infected computers.

In conjunction with its discussions in developing the new bot mitigation best practices, MAAWG wanted to gauge consumers' awareness of malware, how consumers would prefer to have infections removed, how they managed spam, and their attitudes on other spam-related issues. "A Look at Consumers' Awareness of Email Security and Practices" reports the results of a major North American survey the organization commissioned to better understand consumers' needs and common practices.

Representing almost one billion mailboxes from some of the largest network operators and email providers worldwide, MAAWG is the largest global trade association focused on the challenging work of combating spam, viruses, denial-of-service attacks and other online exploitation. This survey looked at attitudes of consumers in the continental United States and Canada. A comparative 2010 study is planned for Europe and will provide a valuable tool for global organizations looking to better understand the differences and similarities among regional users.

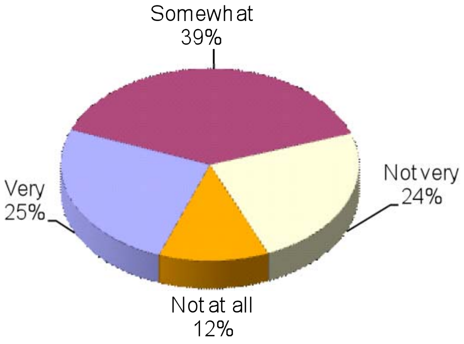
[2] Ars Technica, "Report: spam-wielding botnets are working 9 to 5" by Jacqui Cheng. Published: May 27, 2009 2:33 PM CT (http://arstechnica.com/web/news/2009/05/report-spam-wielding-botnets-apparently-like-us-work-hours.ars)

V. Detailed Findings

A. Internet and Email Usage (Questions 1-5)

Question 1 *(to qualify respondents): On a scale of one to five, with five being expert, how would you describe your experience with security on the Internet including firewalls, spam, junk mail and computer viruses? NOTE: All those who classified themselves as experts were disqualified from this research.*

Self-described Internet Security Experience

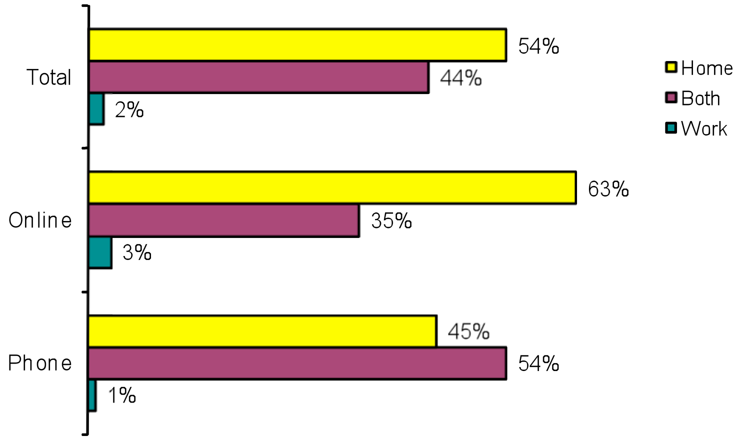


Note – Additional data for this question is available in Appendix A including the graph: Self-described experience with Internet Security – By Age of Respondent

Questions 2-4 *(to qualify respondents): Do you have an email address at work, at home, or both? Are they different or the same email addresses? Regarding your work email address, does your company have an IT service or department that manages and/or maintains the security of your work email?* ***Note:*** *Respondents with only a work email that was managed by an IT department were disqualified from the survey.*

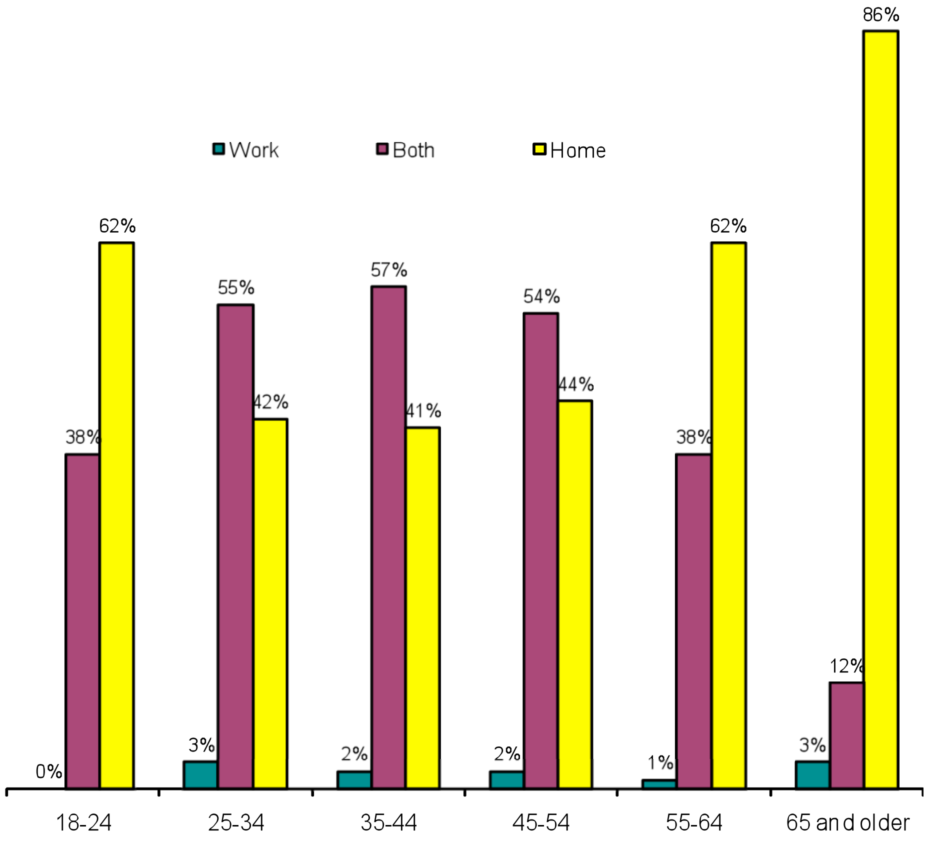
As presented below, very few respondents have an email address at work alone. Most access email at home or both at home and at work.

Location of Email Address



The following graph presents the location of respondents' email addresses based on the age of the respondents. A bell curve emerges. Respondents under the age of 24 and over the age of 55 are more likely to access their email at home only as compared to respondents between the ages of 24 and 54. During the primary years of employment, respondents are more likely to access email both at home and at work.

Location of Email Address – By Age



Note – Additional data is available in Appendix A including the graph:
Self-described experience with Internet Security – By Age of Respondent

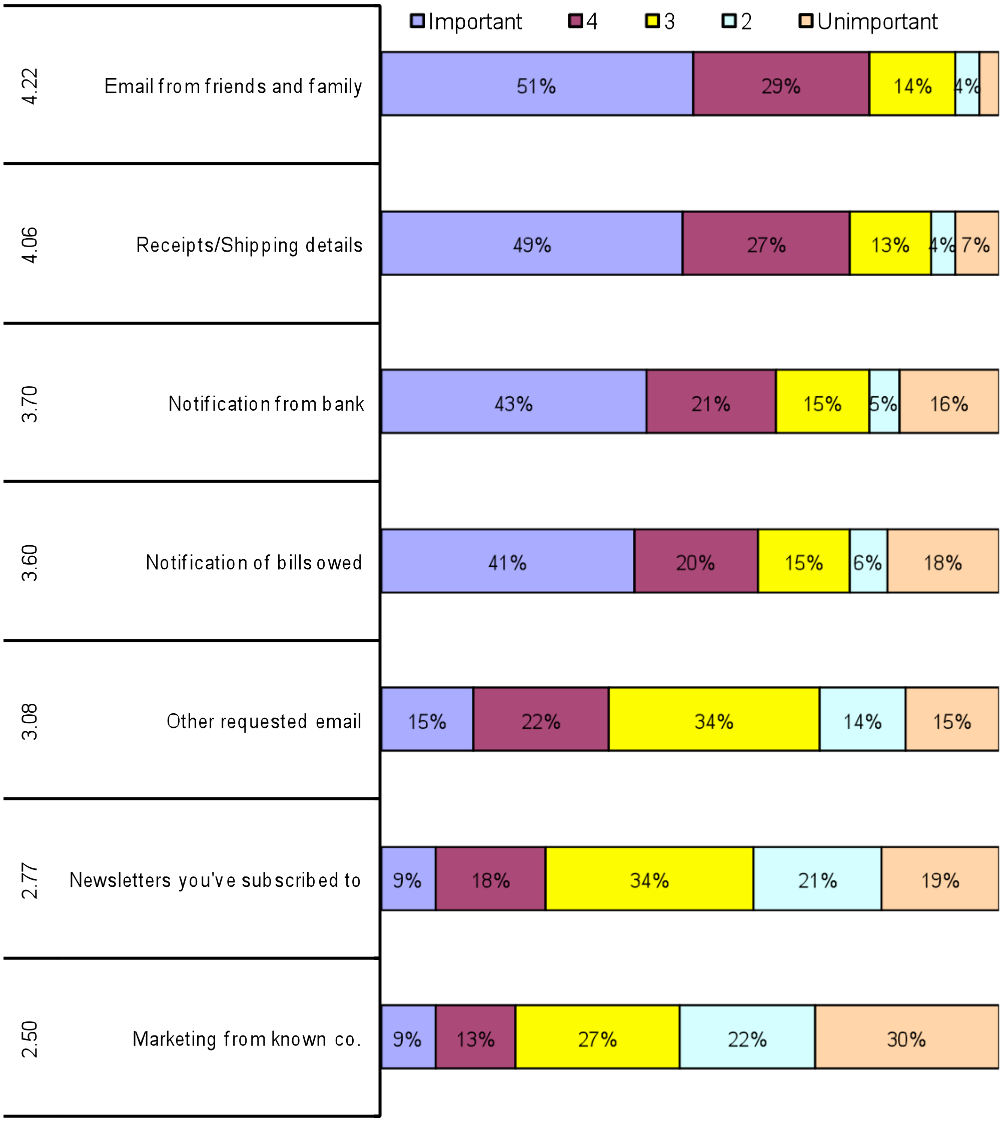
Question 5: *How important are the following when considering sending and receiving personal email? Please use a scale of 1 to 5, where 5 means it is critically important to you and 1 means it is unimportant?*

In order to remove order bias, the order in which each type of email was read or listed to respondents varied. The types of emails revealed to respondents included:

- Email from friends and family
- Newsletters you've subscribed to
- Receipts or shipping details for purchases you've made
- Notifications of bills to be paid
- Notifications from your bank or other financial institution
- Marketing from companies you've purchased from or plan to purchase from
- Other email that you have signed up for

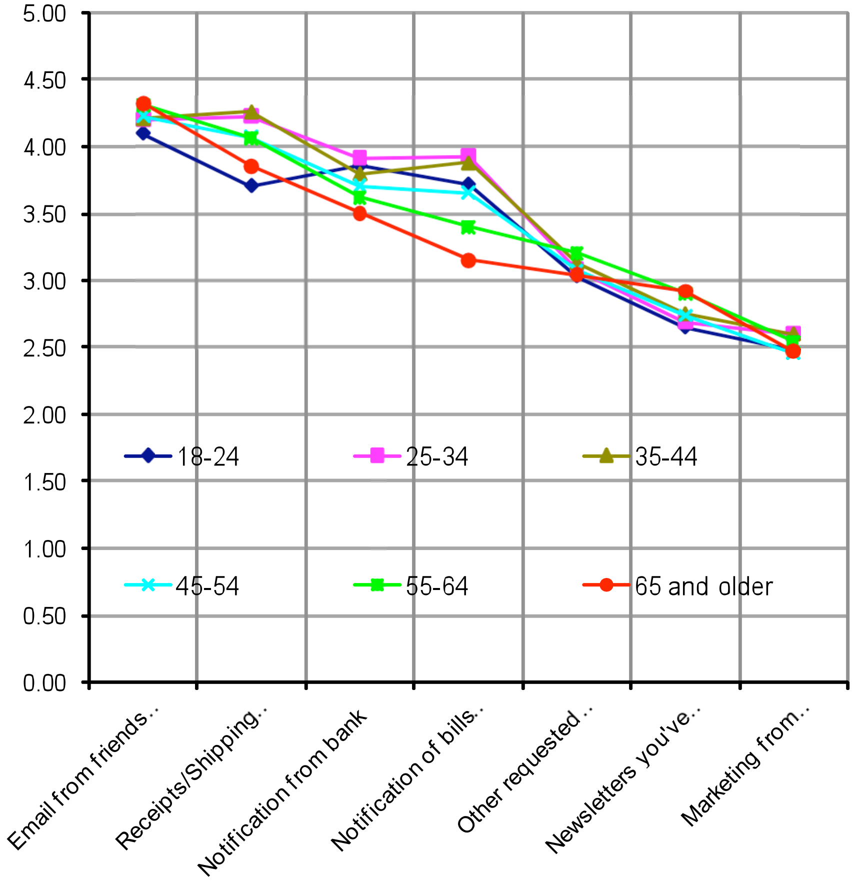
Email from friends and family received the highest rating of importance among all types of emails. This suggests that most respondents use this communications channel to stay in touch with loved ones. The second tier includes commercial interactions, including receipts and notifications. The third and final tier includes informational interactions, including other requested email, newsletters and marketing materials.

Important Personal Email



As with previous questions, differences emerge based on the ages of the respondents when it comes to the importance of different types of personal email.

Important Personal Email – By Age



B. *Virus Infections and Anti-Virus Software Usage (Questions 6-7)*

Question 6: *Which of the following applies to your personal computer?*

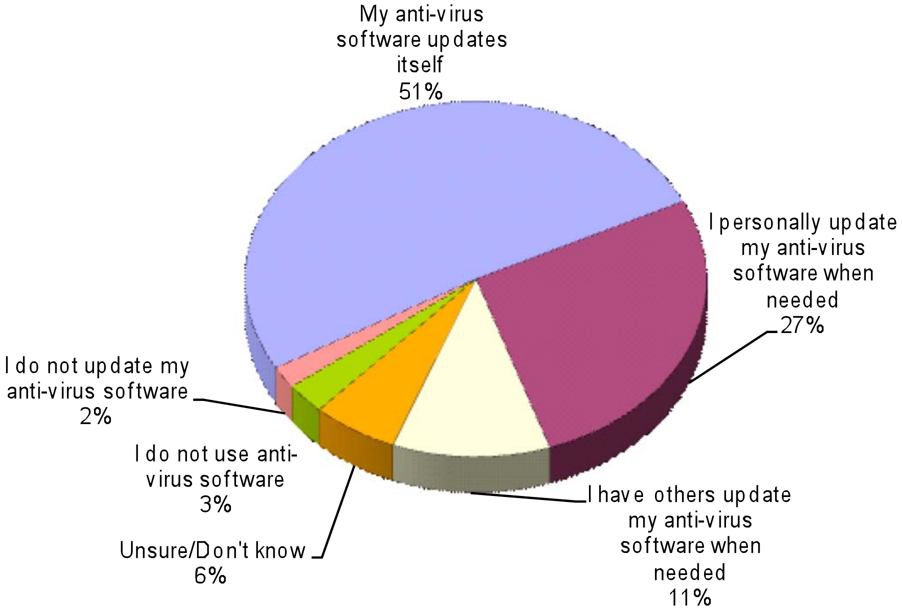
Respondents were read the following scenarios regarding their use of anti-virus software and asked which applies to their personal computer:

- I do not use anti-virus software.
- I personally update my anti-virus software when needed.
- I have others update my anti-virus software when needed.
- I do not update my anti-virus software.
- My anti-virus software updates itself.

As presented below, three-fourths of all respondents indicate that they either personally update their anti-virus software or they believe their anti-virus software automatically updates itself. This may suggest that the majority of respondents perceive the task of updating their anti-virus software as something that is not a complicated process.

It is worth noting that 20% of respondents who say they are not at all experienced with Internet security say they do not know what happens with their anti-virus software.

Usage of Anti-Virus Software



Note – Additional data is available in Appendix A including the graphs:
Usage of Anti-Virus Software – By Age
Usage of Anti-Virus Software – By Willingness to Accept Remote Repair

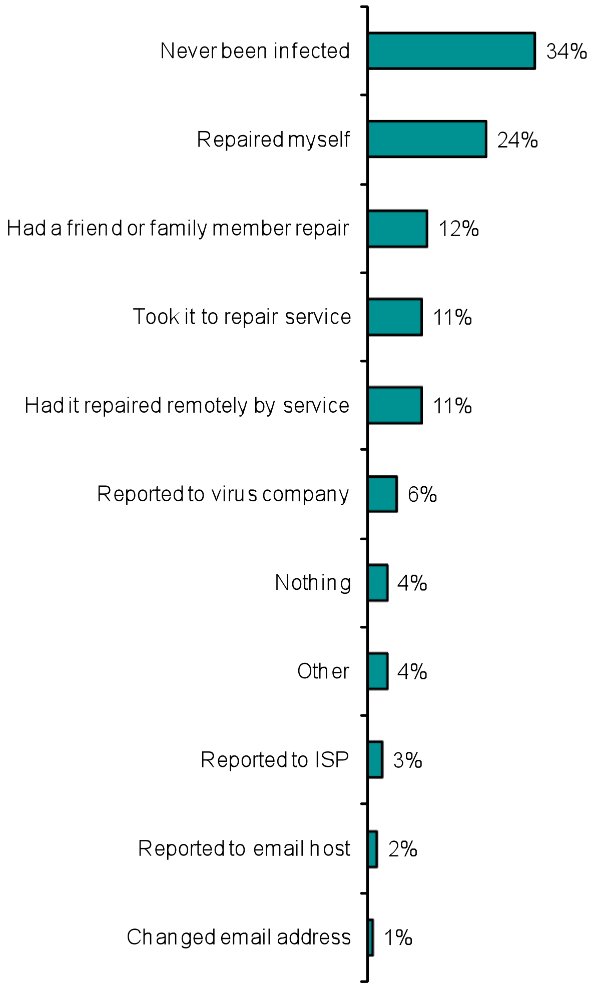
Question 7: *If you have ever been affected by a virus on your computer, what action, if any, did you take?*

Approximately one-third of all respondents said they believe their personal computers have never been infected with a virus. This suggests that two-thirds of all respondents feel their computers have been infected with a virus.

Perhaps not surprising, respondents indicating they are very experienced with computer security were more likely to say they repaired it themselves, while those indicating they are not at all experienced with computer security were more likely to say they called a family or friend to make the repair.

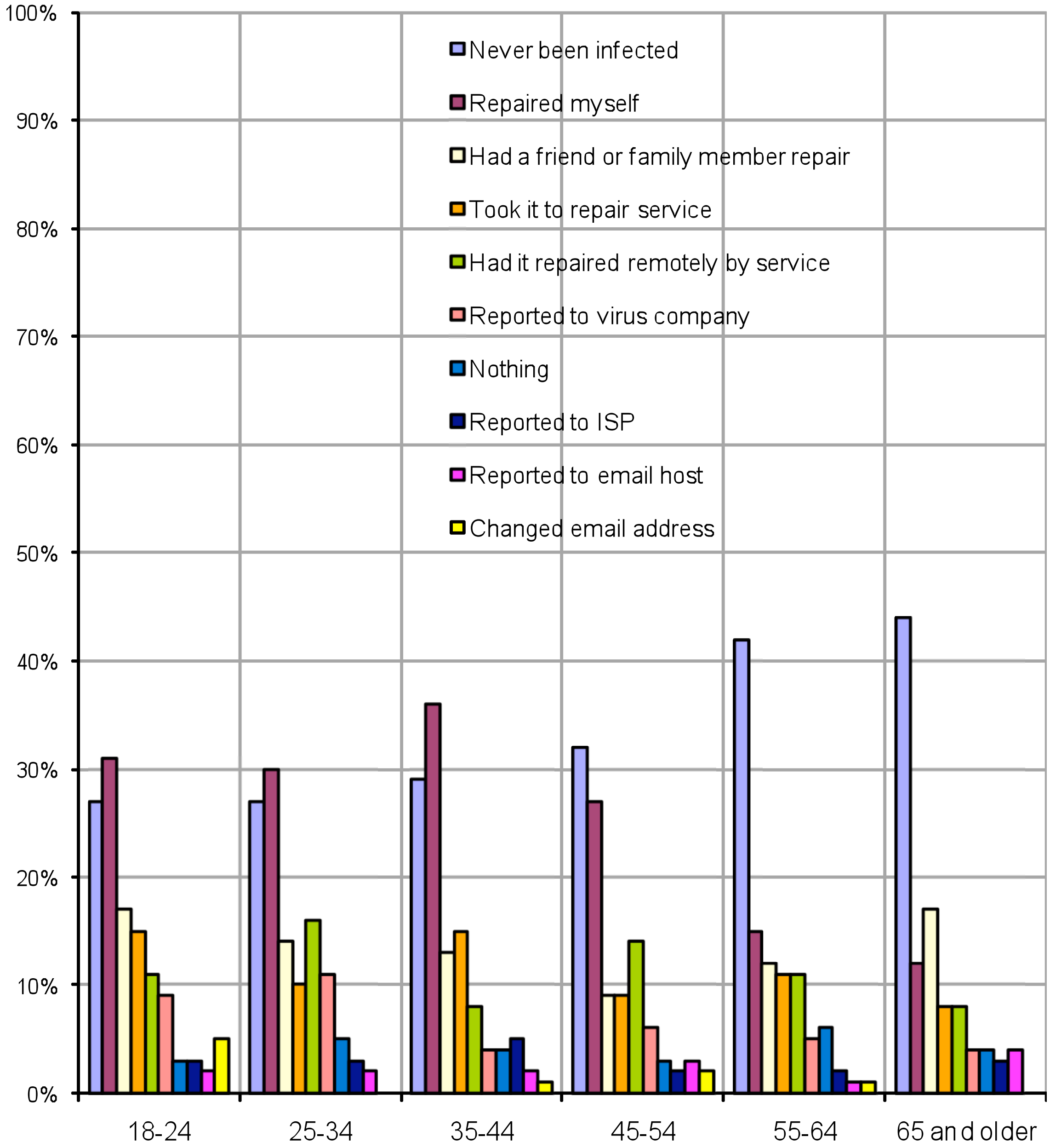
Among only those who indicated their personal computers have been infected by a virus, 38% say they repaired it themselves. Approximately one-third used a professional service, either remotely or by taking the computer in for repair, and 18% reported the incident to a hosting or anti-virus software company. In addition, these same respondents are more likely to say that when they receive email they suspect as fraudulent, they will mark it as spam and delete it. They are also more likely to say they clicked on a link they suspected was spam because they were interested in the product or service offered in the email or wanted to see what would happen.

Action Taken When Affected by A Virus



When segmenting responses based on the age of the respondents, significant differences emerge. Respondents over the age of 45 are more likely to say they have never been infected with a computer virus. Respondents under the age of 44 are more likely to say they repaired it themselves. This probably suggests that younger respondents are more aware of computer viruses.

Action Taken When Affected by A Virus – By Age

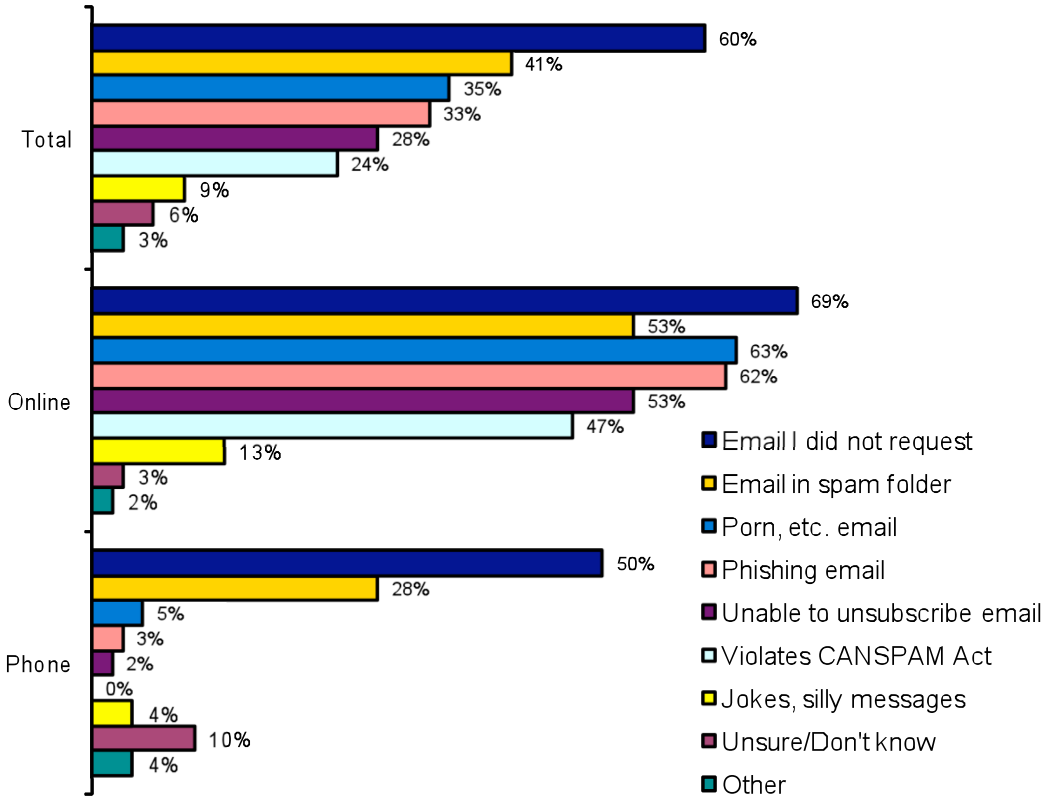


C. *Awareness and Perceptions of Spam (Questions 8-9)*

Question 8*: How do you personally define spam?*

Respondents were asked a series of questions in order to understand their awareness and perceptions of spam. First, respondents were asked to state in their own words how they personally define spam. As presented below, six out of 10 responses indicate that any unrequested email is considered spam. This response is significantly higher among respondents who conducted the interview online.

Definition of Spam

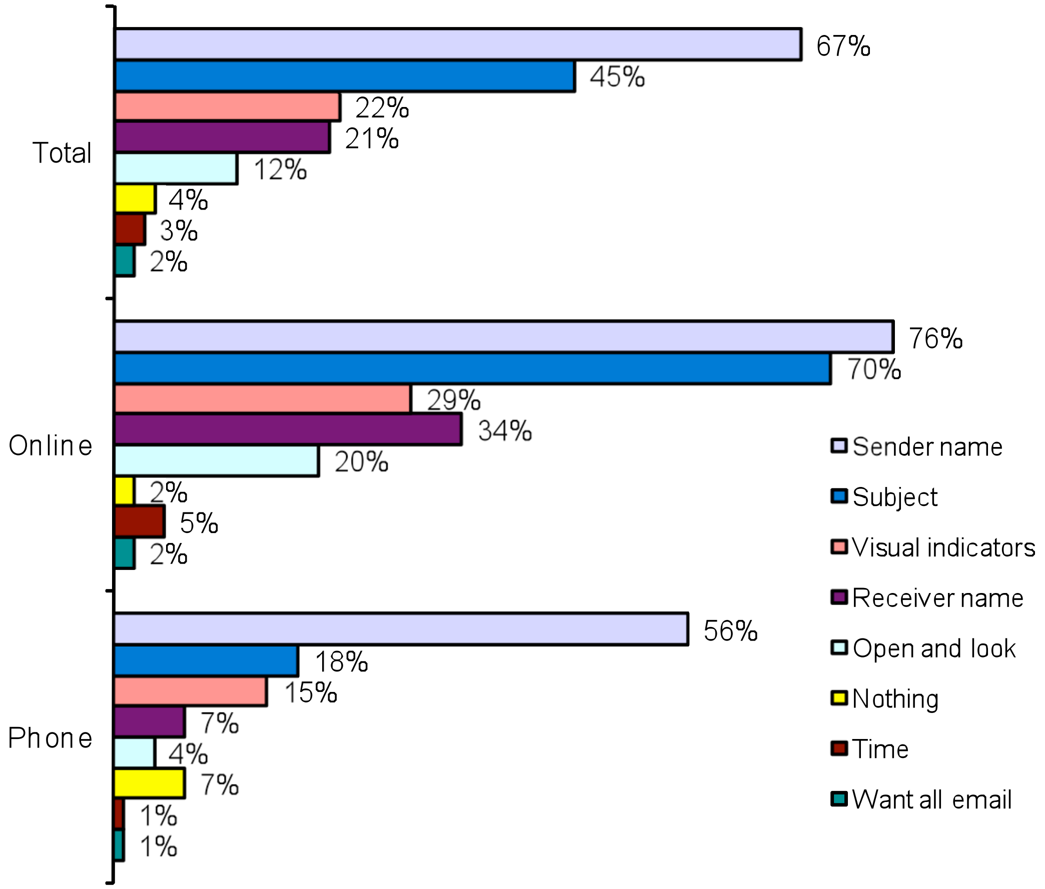


Note – Additional data is available in Appendix A including the graph: Definition of Spam – By Action Taken to Avoid Spam

Question 9: *When going through your email box and deciding which email is spam and which is legitimate, what indicators do you rely on to help you decide?*

Respondents were asked what signals they use to indicate an email is legitimate. Overall, almost 70% said they looked at the sender's name, followed by 45% who said they read the subject line. Other visual indications and the timing of the message were important to about 20% of the respondents.

Personal Alert to Spam Email

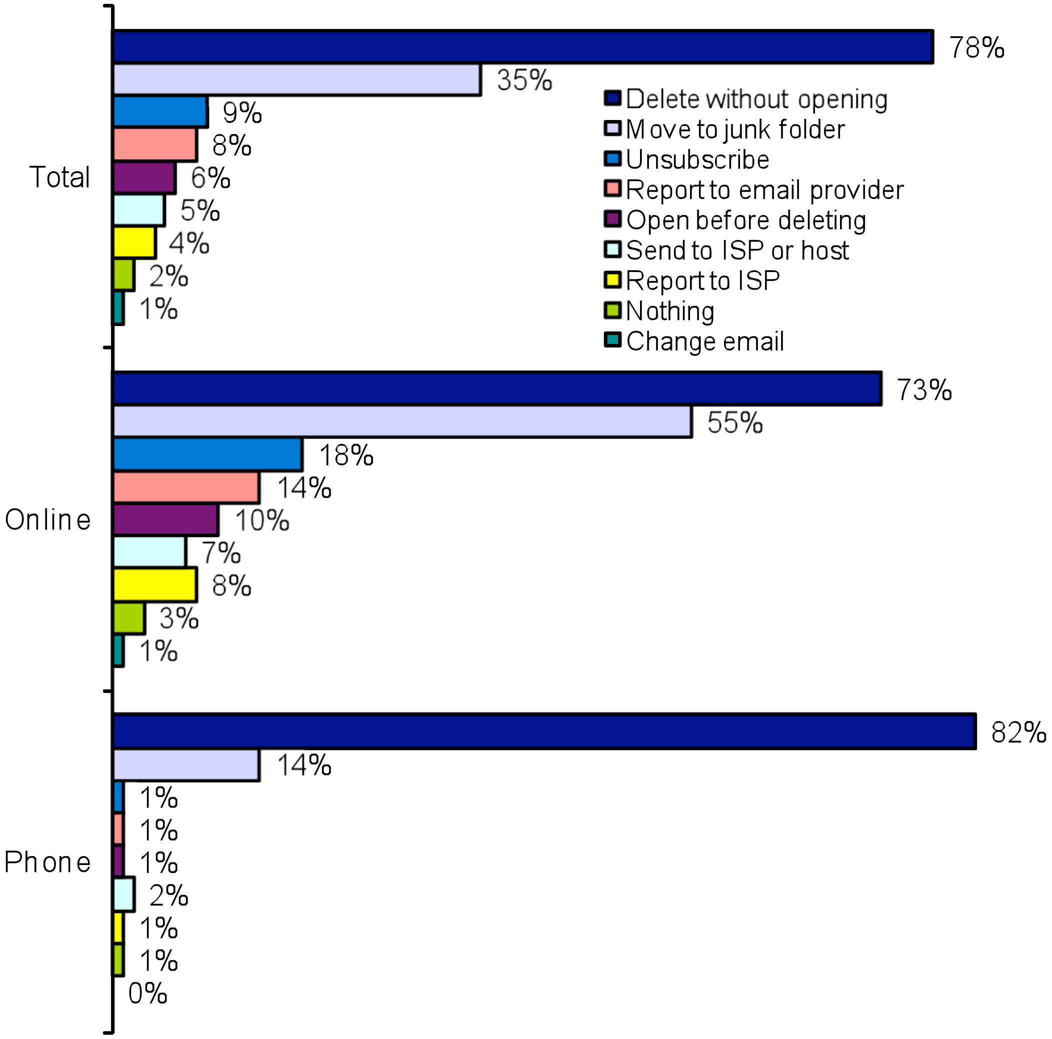


D. *Actions Against Spam (Questions 10-19)*

Question 10: *When you receive email that you think is spam, what do you usually do?*

In questions 10 through 14 respondents were asked a series of questions exploring their actions when confronted with spam. In response to this question, the overwhelming majority, almost 80%, said they deleted the message with 35% saying they moved it to the junk folder. Only 2% ignore the message or do nothing.

Action When Receiving Spam



Interestingly, 12% of those who described themselves as either "very experienced" or "somewhat experienced" with Internet security opened email they suspected as spam before deleting it. This compares to 11% of respondents who also opened suspected spam email but described themselves as either "not very experienced" or having no Internet security experience.

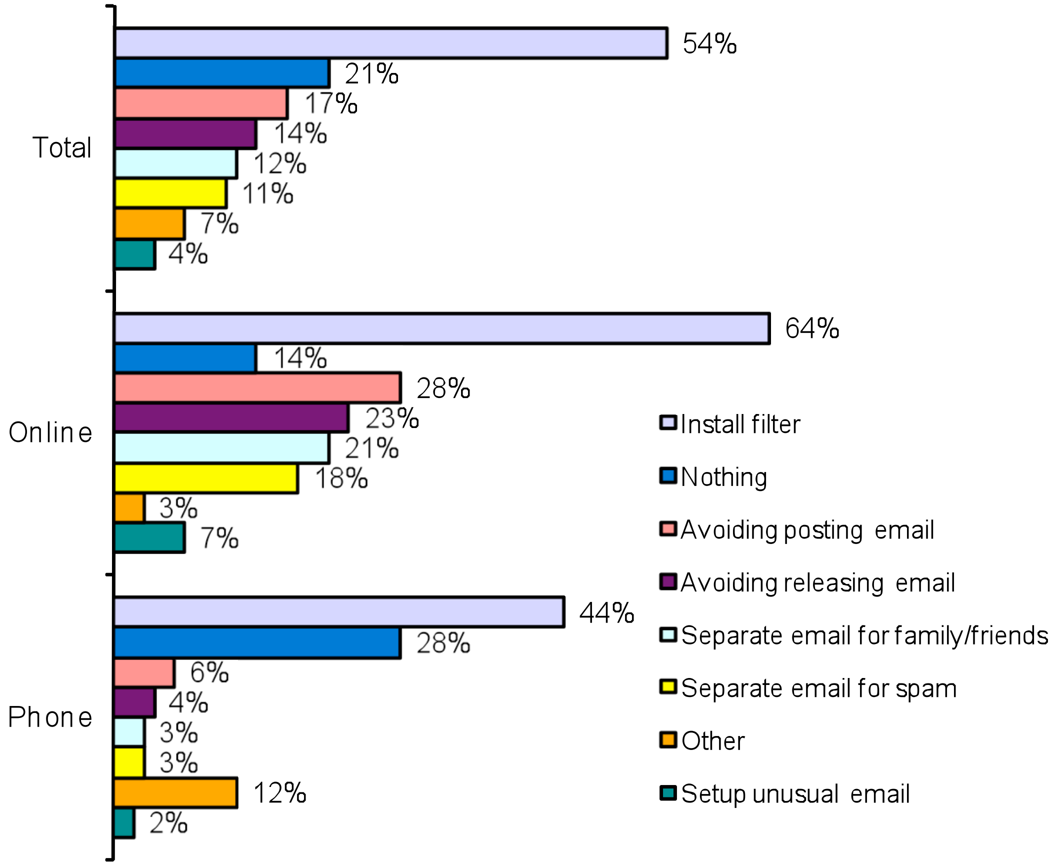
Note – Additional data is available in Appendix A including the graphs:
Action When Receiving Spam – By Action Taken to Avoid Spam
Action When Receiving Spam – By Internet Security
Actions Taken to Avoid Spam – By Age

Question 11: *What actions, if any, have you taken to avoid receiving spam or junk email in your personal email?*

Over half of all respondents say they install a filter to avoid receiving spam. No other option garners the same frequency of response. Nearly one-fourth of all respondents say they do nothing to avoid spam on their personal computers.

It is important to note that this is the question referred to throughout this research as a point of segmentation.

Actions Taken to Avoid Spam

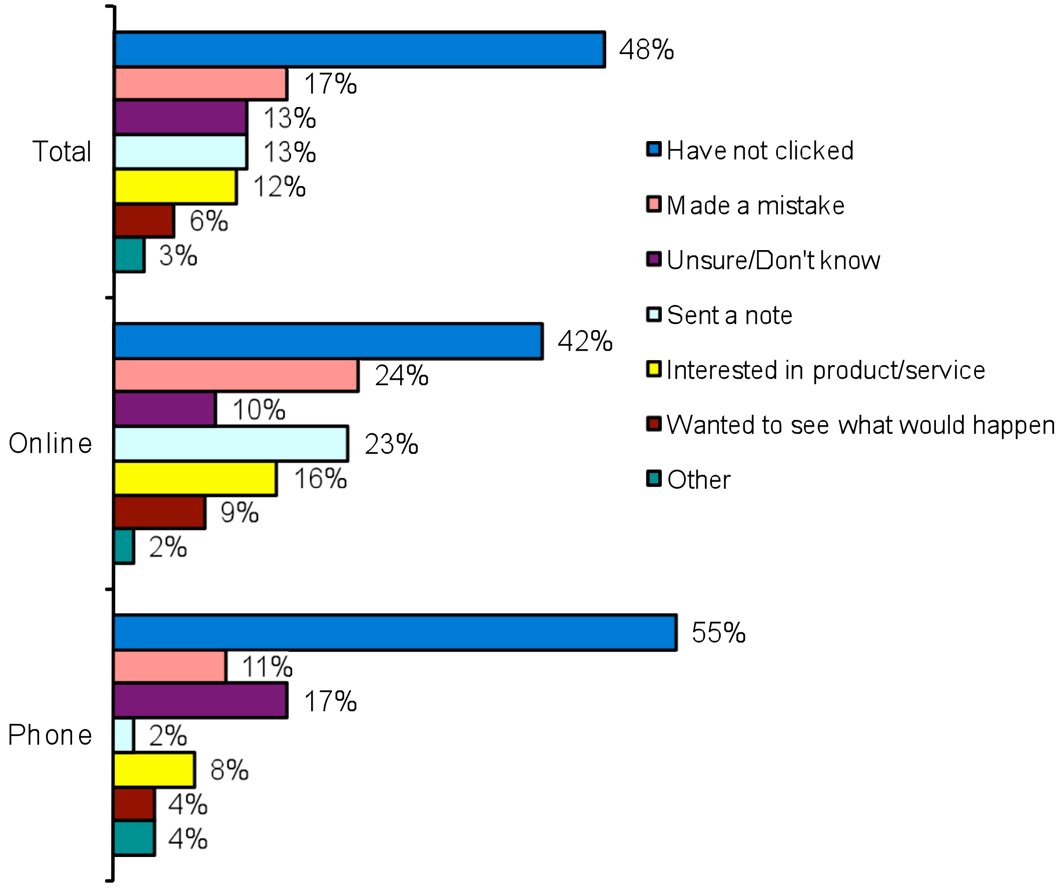


Question 12: *If you have ever clicked on a link or replied to an email that you suspected was spam, why did you take this action?*

Nearly half of respondents say they have never clicked on a link or replied to an email message they suspected was spam. Among all respondents, 17% said they made a mistake when they clicked on spam; however this response occurs more often among online respondents than among telephone respondents.

Respondents stating they use a separate email address or avoid posting or giving out their email addresses to avoid spam are more likely to say they sent a note to remove or complain about spam.

Why Responded To Spam

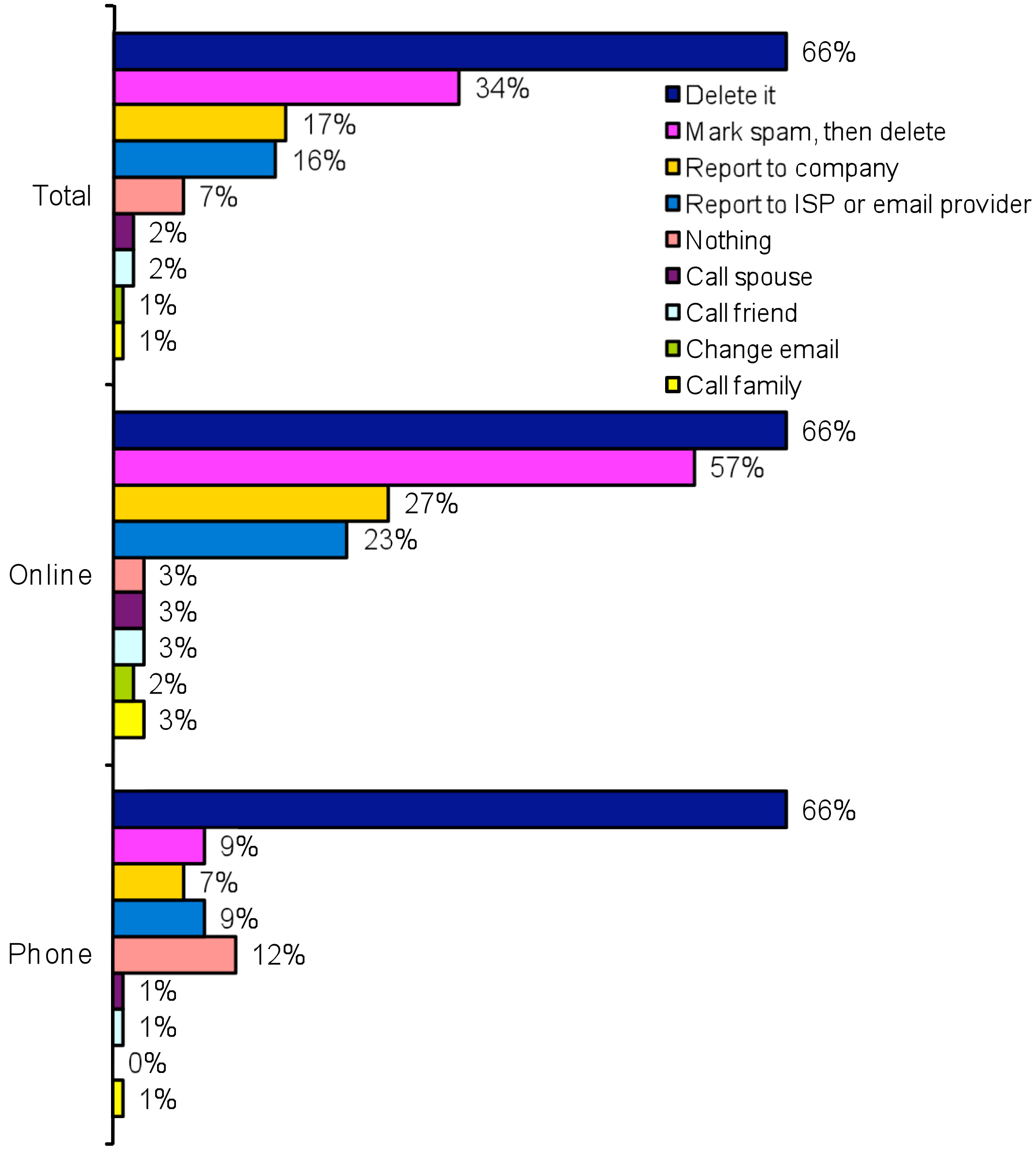


Note – Additional data is available in Appendix A including the graph:
Important Personal Email – By Actions Taken to Avoid Spam

Question 13: *When you receive email that you suspect to be fraudulent, what actions have you taken?*

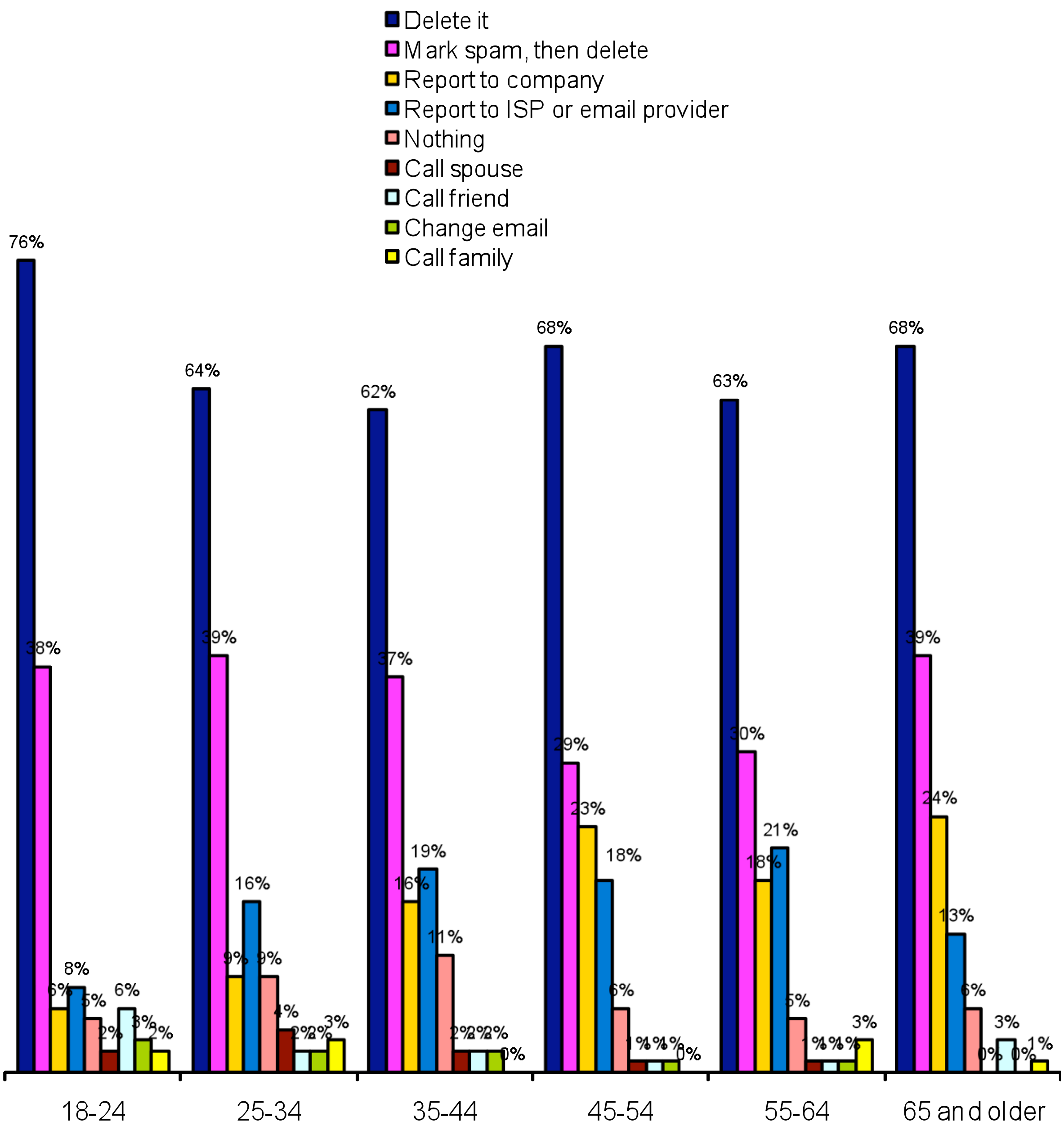
Two-thirds of all respondents say they simply delete fraudulent email. More than half of all online respondents say they also mark it as spam and then delete the fraudulent email.

Reaction to Fraudulent Email



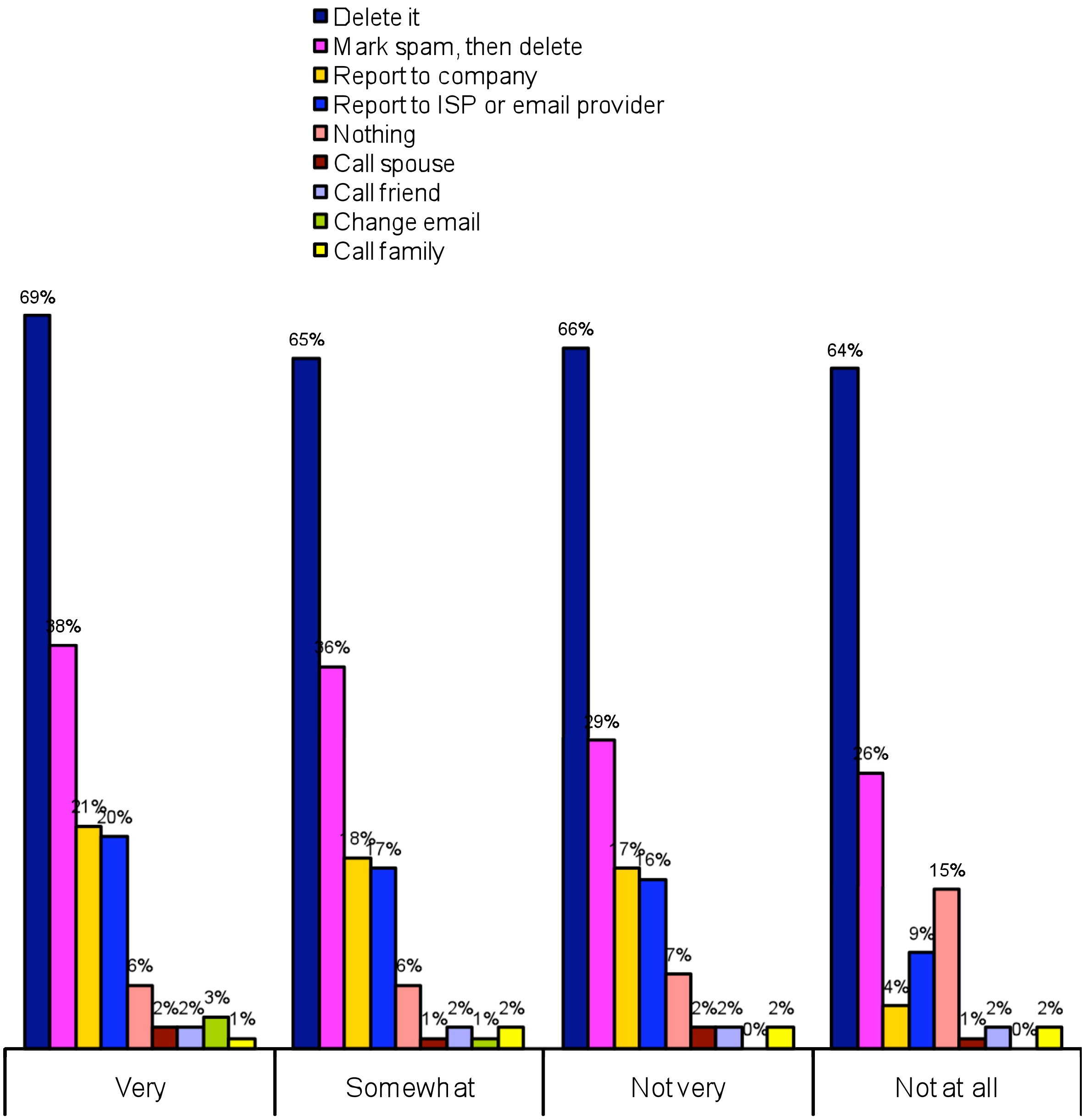
Respondents under the age of 24 are most likely to say they simply delete it, while respondents over the age of 35 are more likely to say they report it to the legitimate company or institution, ISP or email provider.

Reaction to Fraudulent Email – By Age



Respondents stating they have some Internet security experience are more likely to say they reported the fraudulent email to the legitimate company, ISP or email provider.

Reaction to Fraudulent Email – By Internet Security Experience

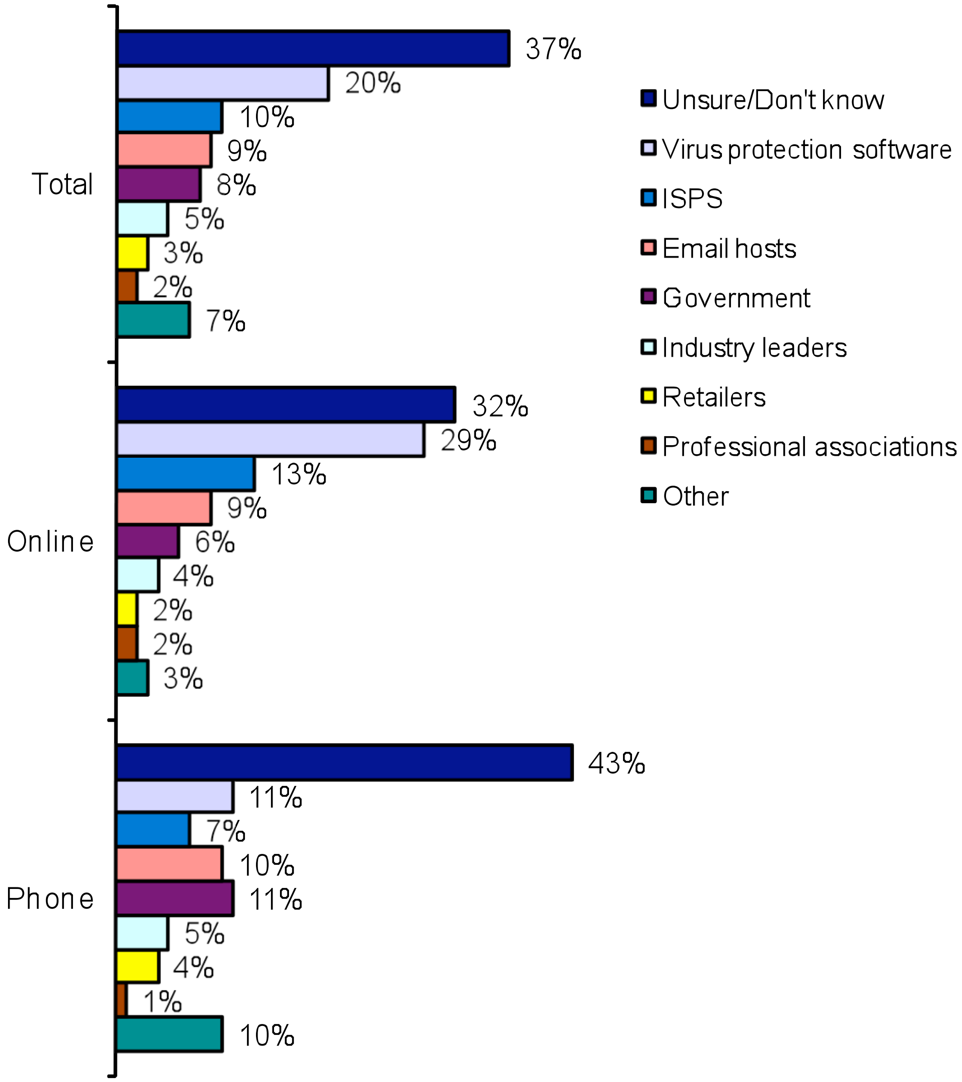


Note – Additional data is available in Appendix A including the graph:
Why Responded to Spam - By Willingness to Accept Remote Repair and Previous Infection of a Computer Virus

Question 14: *Whom do you feel is most responsible for stopping the creation of computer viruses, fraudulent email, spyware, and spam?*

Over one-third of all respondents say they do not know who is responsible for stopping viruses. About 20% look to anti-virus companies to control spam, followed by 10% of respondents who named ISPs.

Responsible for Spam

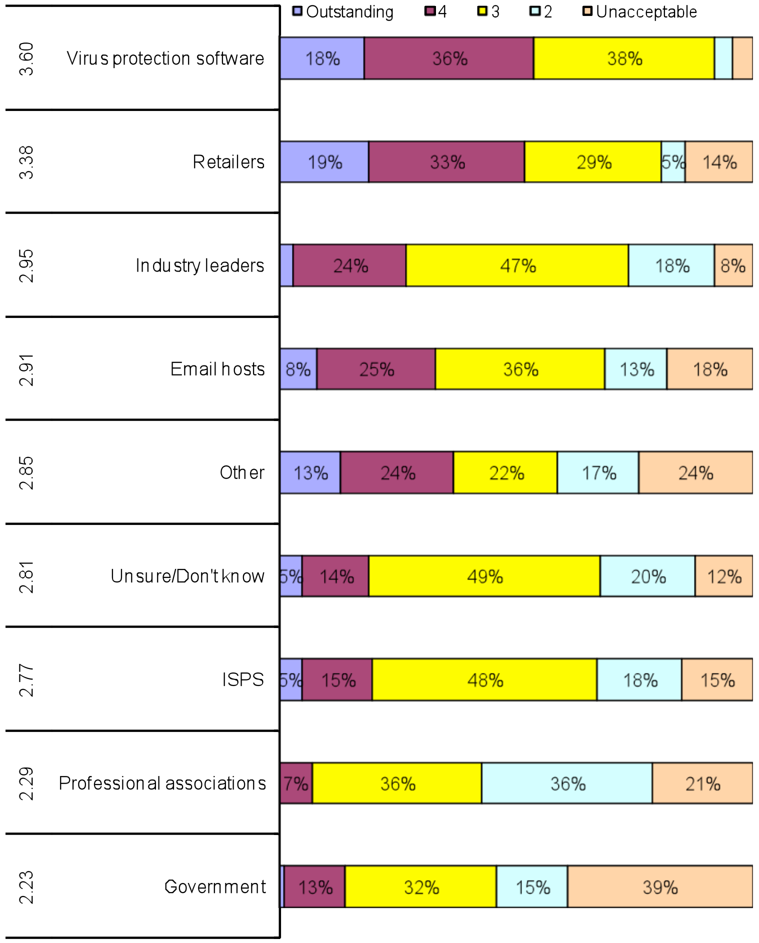


***Question 15:** How would you rate the performance of (**response to question 15**) for stopping these viruses? Please use a scale of 1 to 5, where 5 means performance is outstanding and 1 means performance is unacceptable.*

In this question, respondents rated the performance of the organization they named above as being responsible for stopping viruses. Virus protection software companies, which were most often named as being responsible for stopping viruses in question 14, and retailers received the highest performance ratings; however, it should be noted that no organization receives a performance rating higher than 3.60 on a five-point scale.

Several online survey respondents stated they were unsure or did not know who was responsible for computer viruses, but then provided a performance rating for this unknown entity. This may suggest that some respondents feel that one organization is responsible and have an opinion on their performance but are not sure of the name or brand of this organization.

Performance Rating of Entity Responsible for Spam

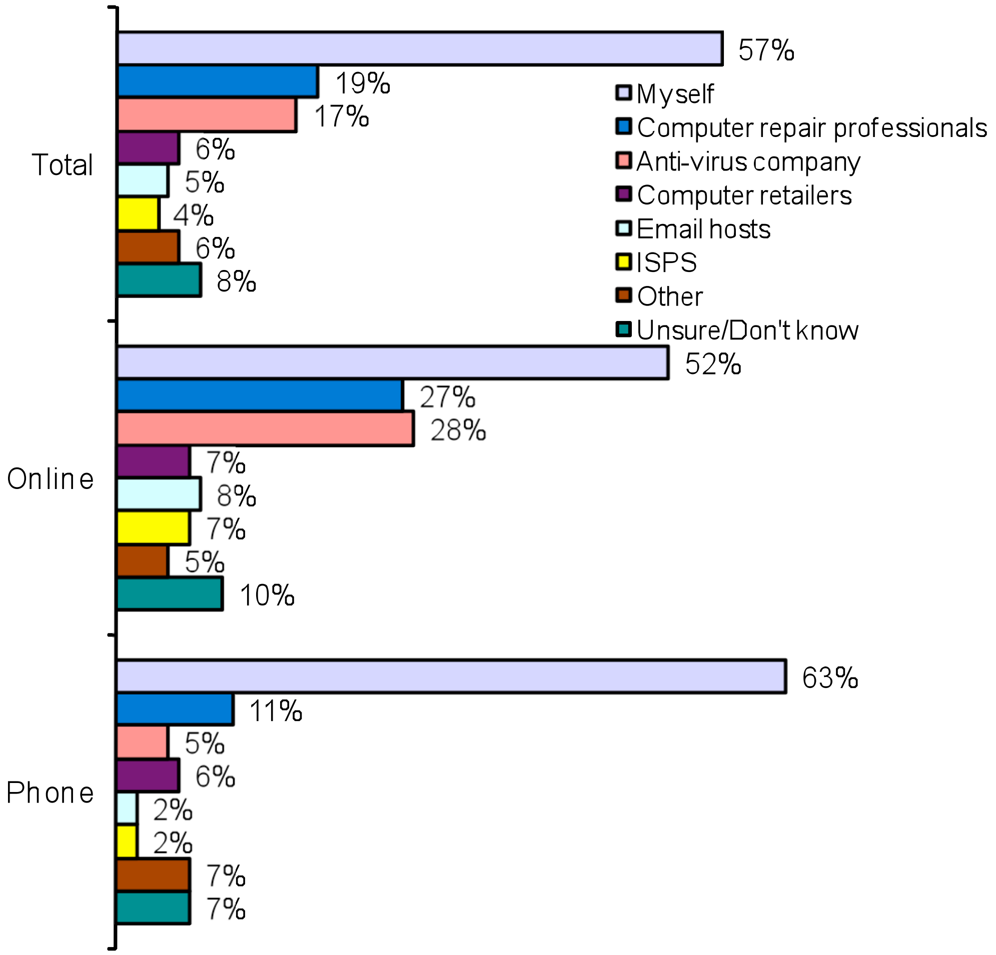


Question 16: *Whom do you feel is responsible for fixing your computer if you find it has been contaminated with a computer virus, fraudulent email, spyware or spam?*

Over half of all respondents say this is a personal responsibility. This response is higher among respondents indicating they have some experience with Internet security than among respondents indicating they have no such experience.

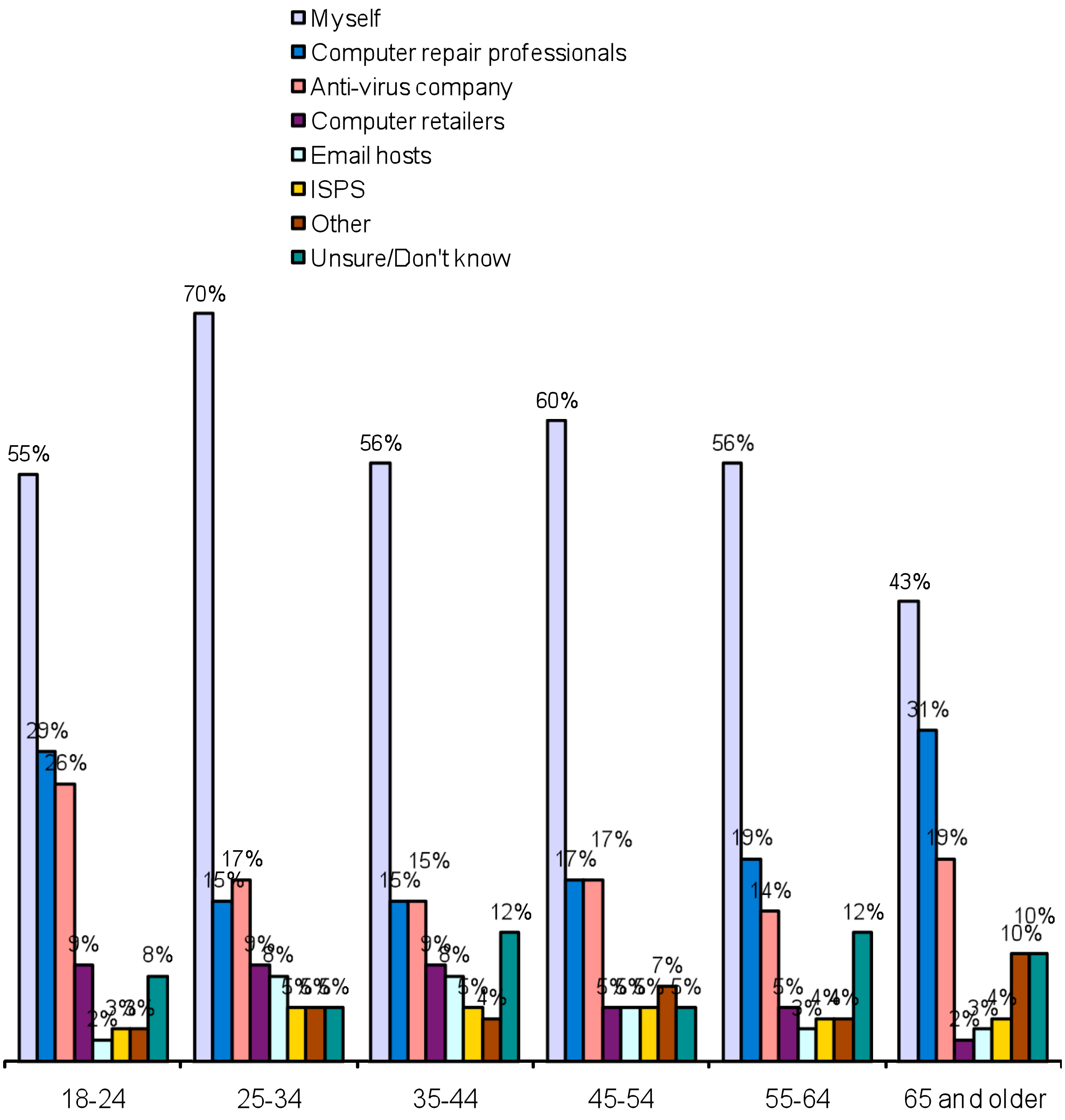
Respondents are more likely to say that anti-virus product or computer repair organizations are more responsible for the repair of an infected computer than are service organizations such as their ISPs.

Repair Responsibility



The following graph presents results of this same question based on the age of the respondents. Respondents over the age of 65 are less likely than younger respondents to say it is their own responsibility to fix their infected computers. As compared to other respondents, respondents under the age of 24 and respondents over the age of 65 are more likely to say that a computer repair professional is responsible for fixing an infected computer than other respondents. Computer retailers are more likely to be mentioned by respondents under the age of 44 than by older respondents.

Repair Responsibility – By Age



Note – Additional data is available in Appendix A including the graph: Action When Receiving Fraudulent Email – By Willingness to Accept Remote Repair and Previous Infection of a Computer

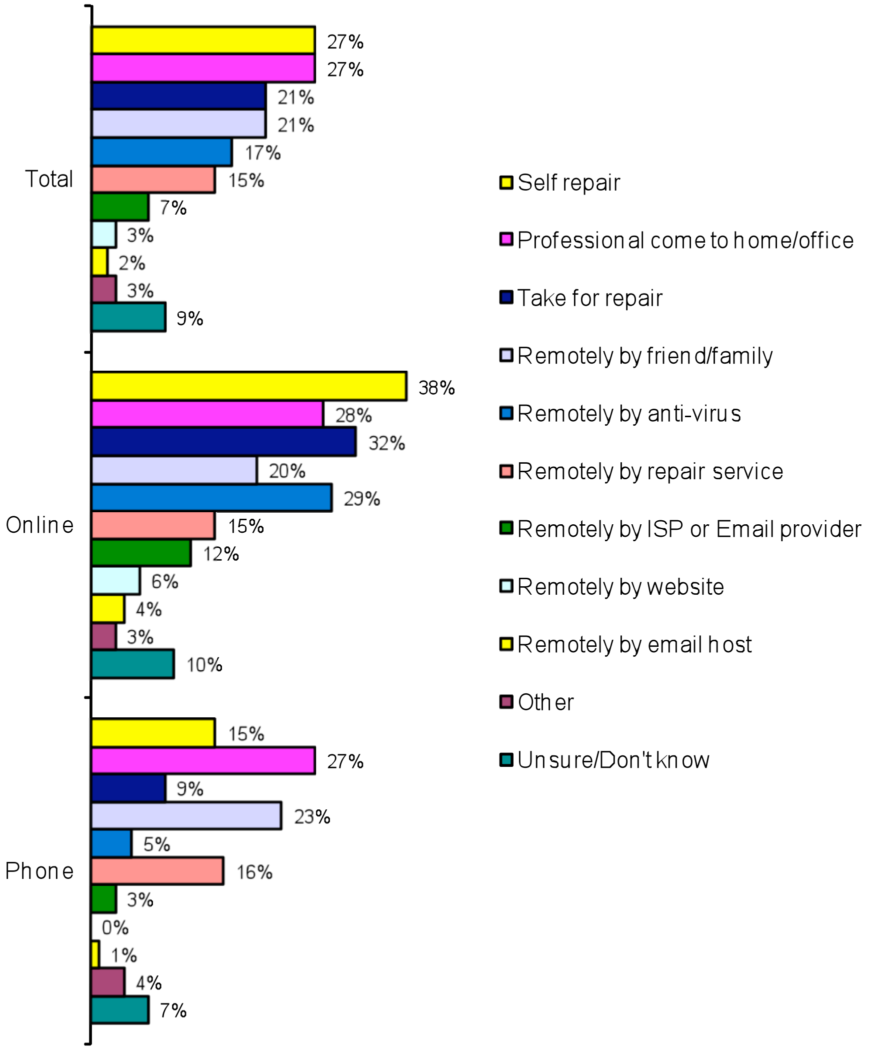
Question 17: *If you found that your computer was infected, who would you allow access to your computer to remove the virus?*

Approximately 63% of all respondents indicate that they would allow remote access for the repair of an infected computer. This response is higher among online respondents (82%) than among telephone respondents (47%).

In addition, respondents indicating they would allow remote repair are more likely to use a separate or unusual email to avoid spam and use the unsubscribe link. These same respondents are also more likely to say that anti-virus companies and computer retailers are responsible for fixing their computer if infected.

Those with at least some experience with Internet security are more likely than those with less experience to say they would repair it themselves. Respondents who stated that their computers have been infected by a computer virus (question 7) are also more likely to say they would repair it themselves. Respondents under the age of 24 are more likely to say they will take it to a computer repair service, while respondents between the ages of 25 and 44 are more likely to say they will repair it themselves.

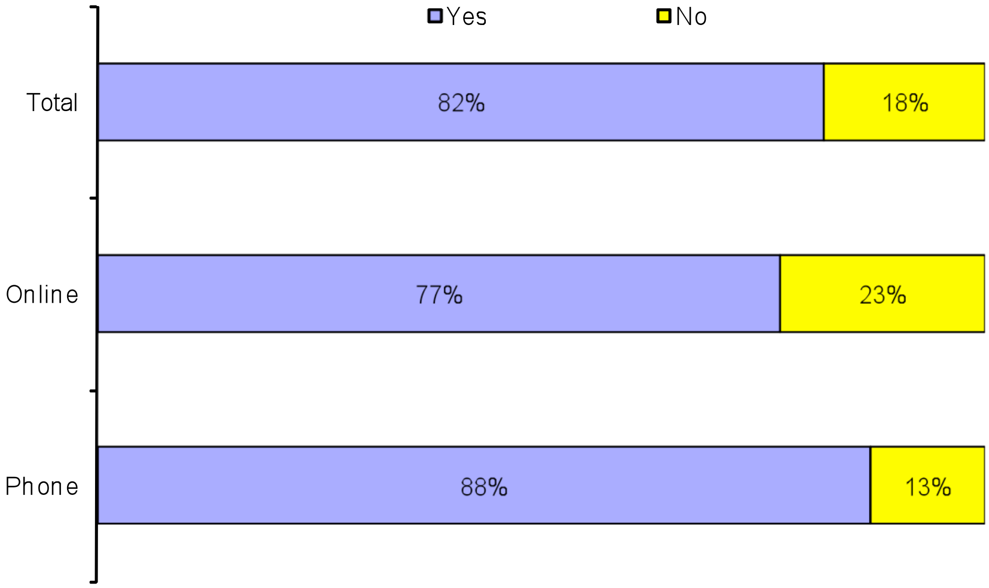
<u>Allowed Access to Remove Virus</u>



Question 18: Are you aware that there are malicious viruses that can control your computer without your knowledge and then use your computer to spread spam?

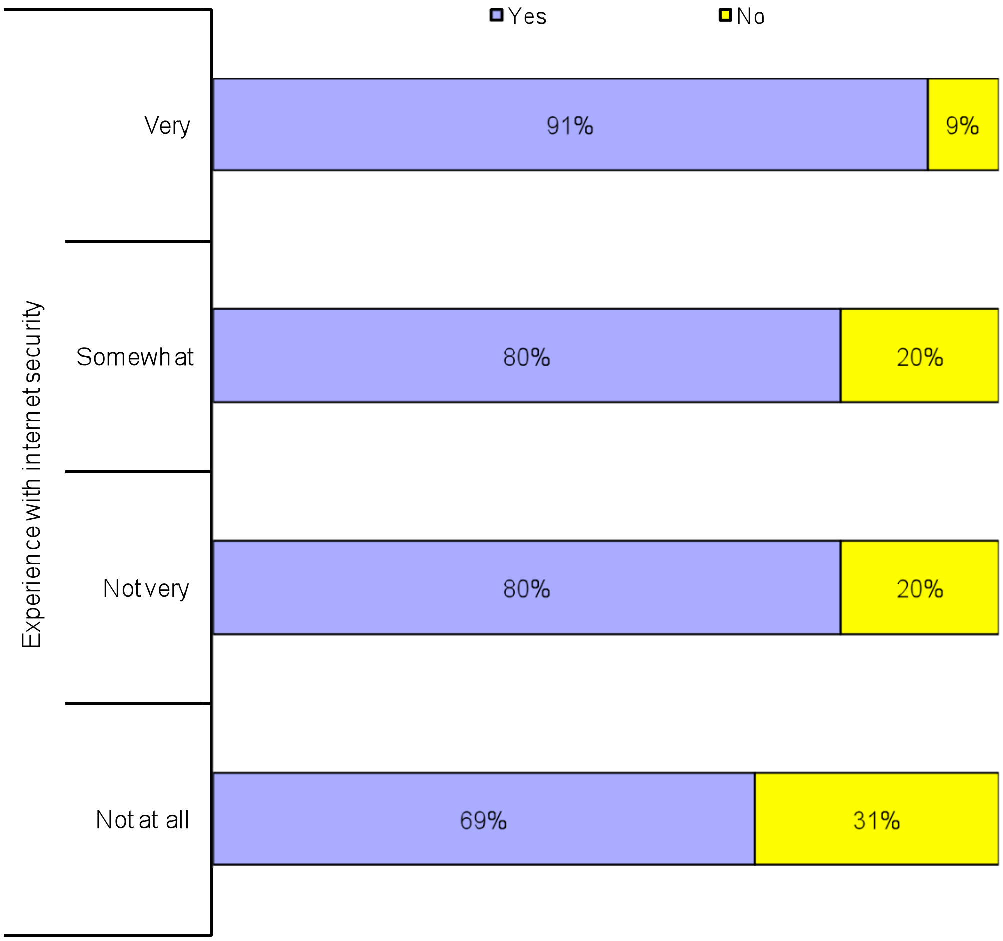
To measure how aware respondents are of bots, they were asked about their awareness of malicious viruses that can control a computer. Respondents were not provided with the words "bot" or "botnet;" instead, they were provided with just the definition and asked for their awareness of this type of computer virus. As presented below, the majority of respondents said they are aware of this type of virus. Respondents indicating they have been infected by a computer virus are more likely to say they are aware of bots. The same is true among respondents who said they would allow their infected computer to be repaired remotely.

Awareness of Botnets



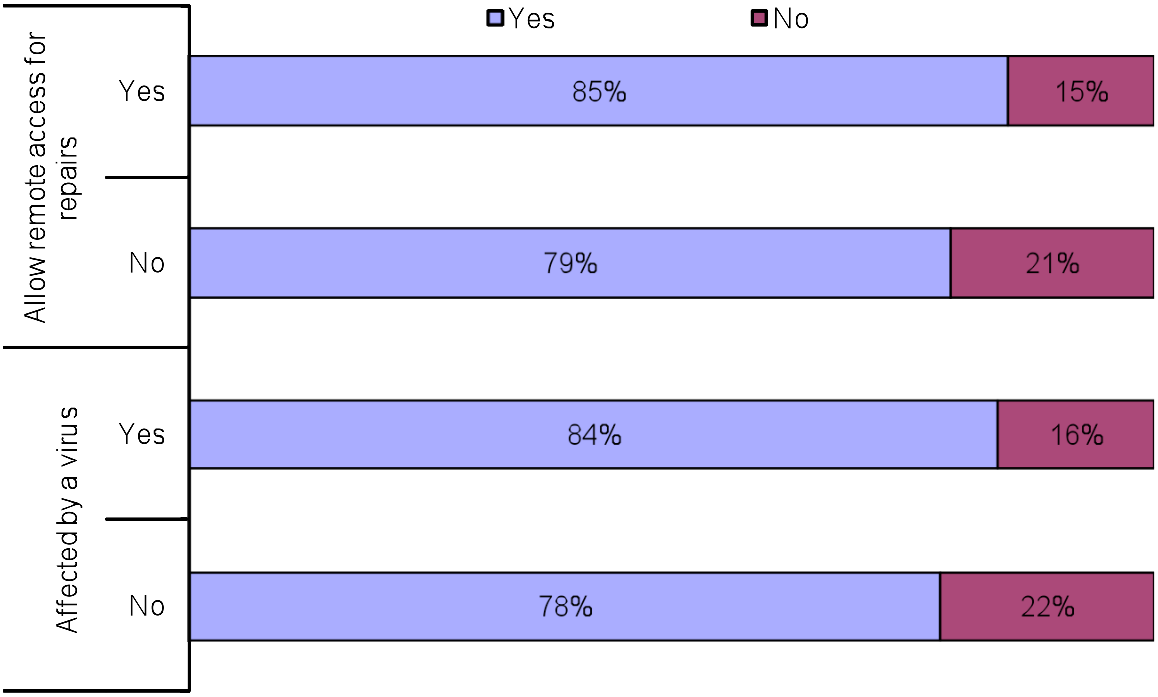
The following graph presents the findings for this awareness question based on self-described experience with Internet security. While nine out of 10 respondents who say they are very experienced with Internet security also say they are aware of botnets, seven out of 10 respondents who say they have no experience with Internet security offer the same positive response.

Awareness of Botnets – By Internet Security Experience



The following graph examines respondents' awareness of botnets based on their willingness to have their computer repaired remotely and on past experience with a computer virus. Results indicate respondents more likely to have their computer repaired remotely are also slightly more likely to be aware of botnets. These results are the same among respondents saying they were previously infected with a computer virus.

Awareness of Botnets
By Willingness to Accept Remote Repair and Previous Infection of a Computer Virus

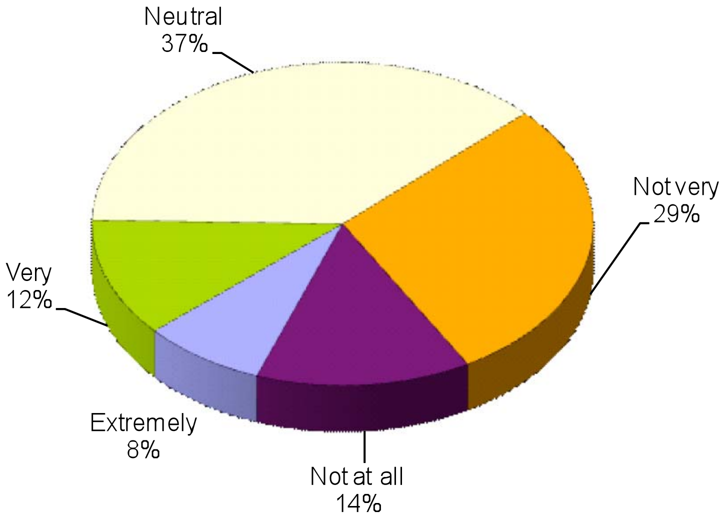


Question 19: Using a scale of 1 to 5, with 5 being extremely likely and 1 being not at all likely, what do you feel are your chances of getting this type of virus on your computer?

Respondents were asked the likelihood of their getting a bot on their personal computers. Just one out of 10 respondents indicate they feel there is a strong likelihood that this type of virus would infect their personal computers. Nearly half indicated there is very little likelihood this would happen to them. This response is consistent among all respondents regardless of age, experience, or action to avoid spam.

Respondents indicating they have been infected by a computer virus are more likely to say they are extremely or very likely to get a malicious virus. The same is true among respondents indicating they would allow their infected computer to be repaired remotely.

Likelihood of Getting a Bot



Note – Additional data is available in Appendix A including the graph:
Likelihood of Getting a Bot By Willingness to Accept Remote Repair and Previous Infection of a Computer Virus

Appendix A: Supplemental Cross Tabulations and Detail

In this appendix, we provide additional cross-tabulated data that may be interesting to specific industry groups but that does not reflect especially notable trends or correlations. While there is not additional data for all the questions, where supplementary analysis is available the numbering is the same as the Detailed Findings section of this report.

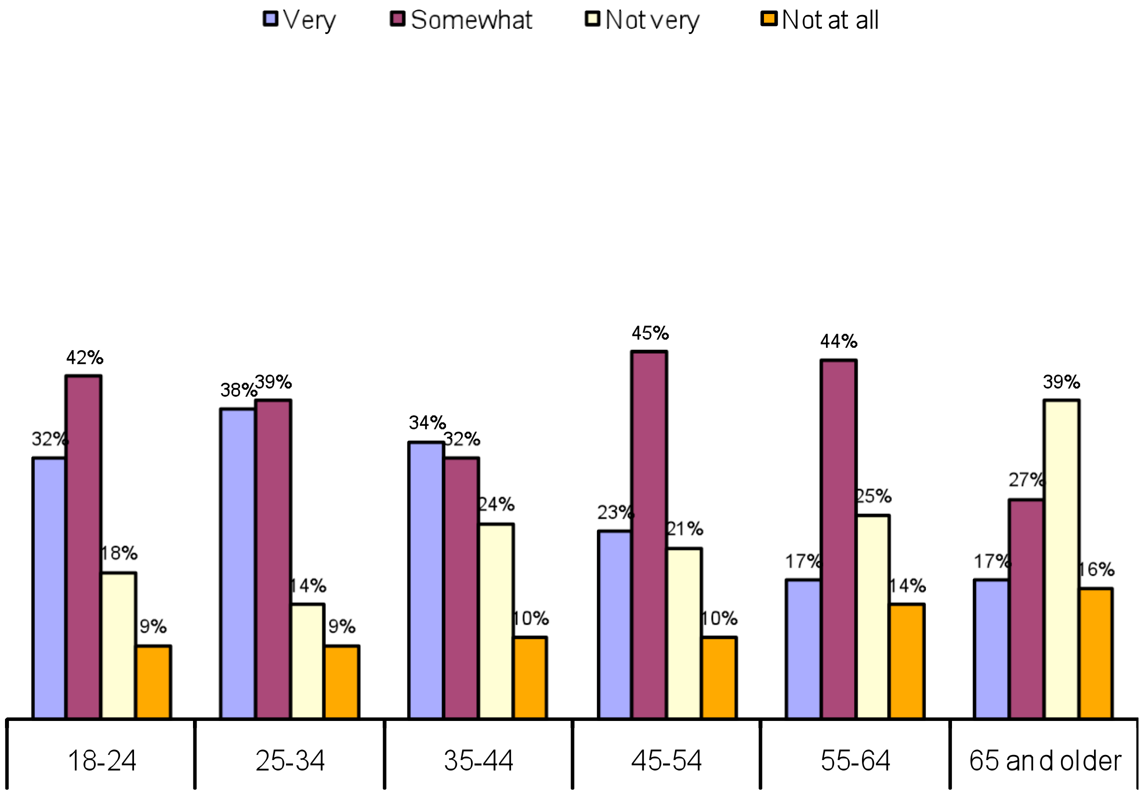
A. Internet and Email Usage (Questions 1-5)

Question 1: *On a scale of one to five, with five being expert, how would you describe your experience with security on the Internet including firewalls, spam, junk mail and computer viruses? NOTE: All those who classified themselves as experts were disqualified from this research.*

The following graph presents the response to self-described experience with Internet security based on the age of the respondent. Overall, respondents under the age of 44 are significantly more likely to say they are very experienced with Internet security than are older respondents.

While not presented below, it is also worth noting that Asian-American respondents are also more likely to say they are very experienced with Internet security than are other respondents.

Self-described experience with Internet Security – By Age of Respondent



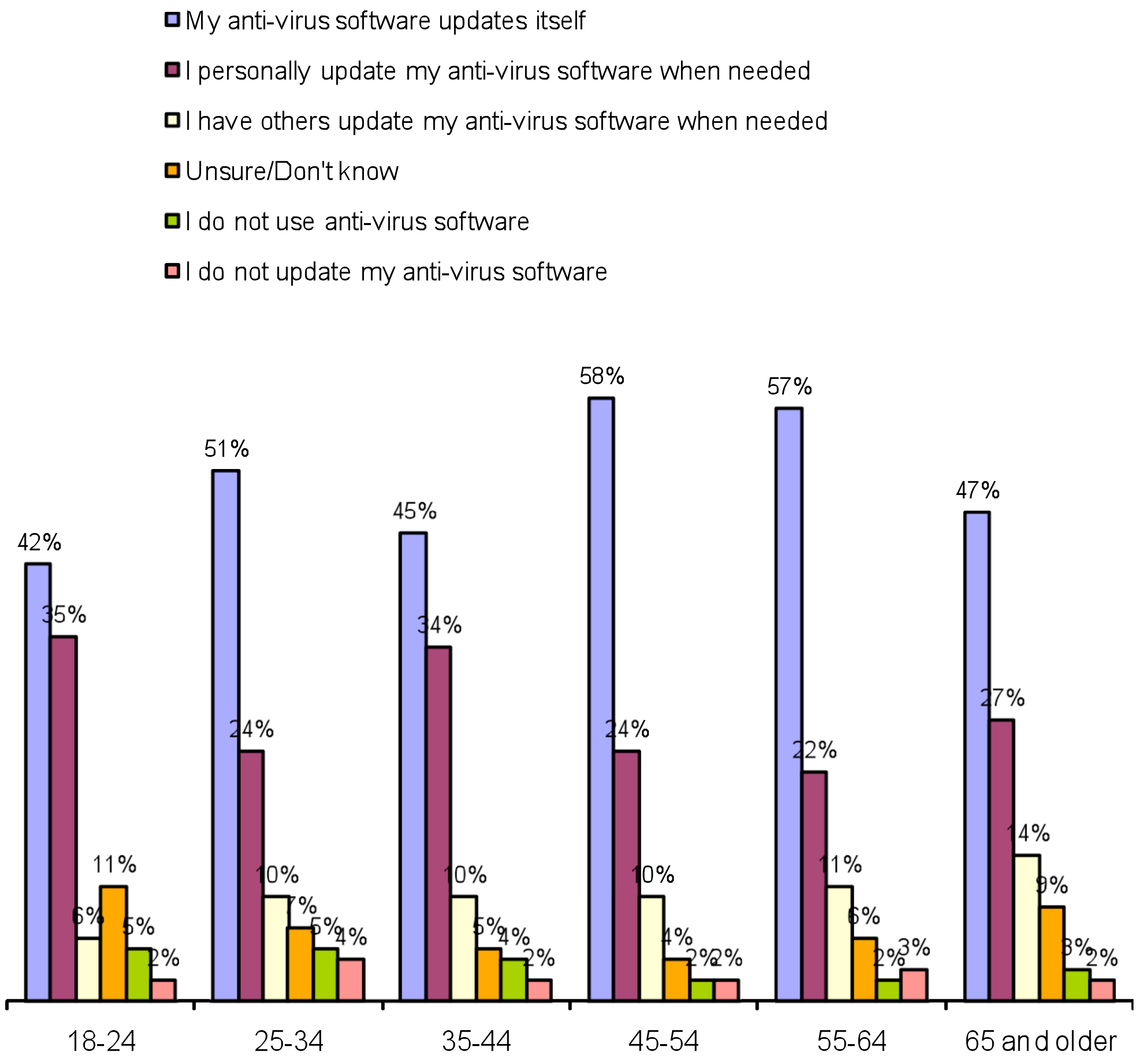
B. *Virus Infections and Anti-Virus Software Usage (Questions 6-7)*

Question 6: *Which of the following applies to your personal computer?*

There were 20 respondents who stated that they do not update their anti-virus software. These respondents were asked why. The most consistent responses indicated the perception that updating of anti-virus software is not needed, it is too expensive or they simply do not know why.

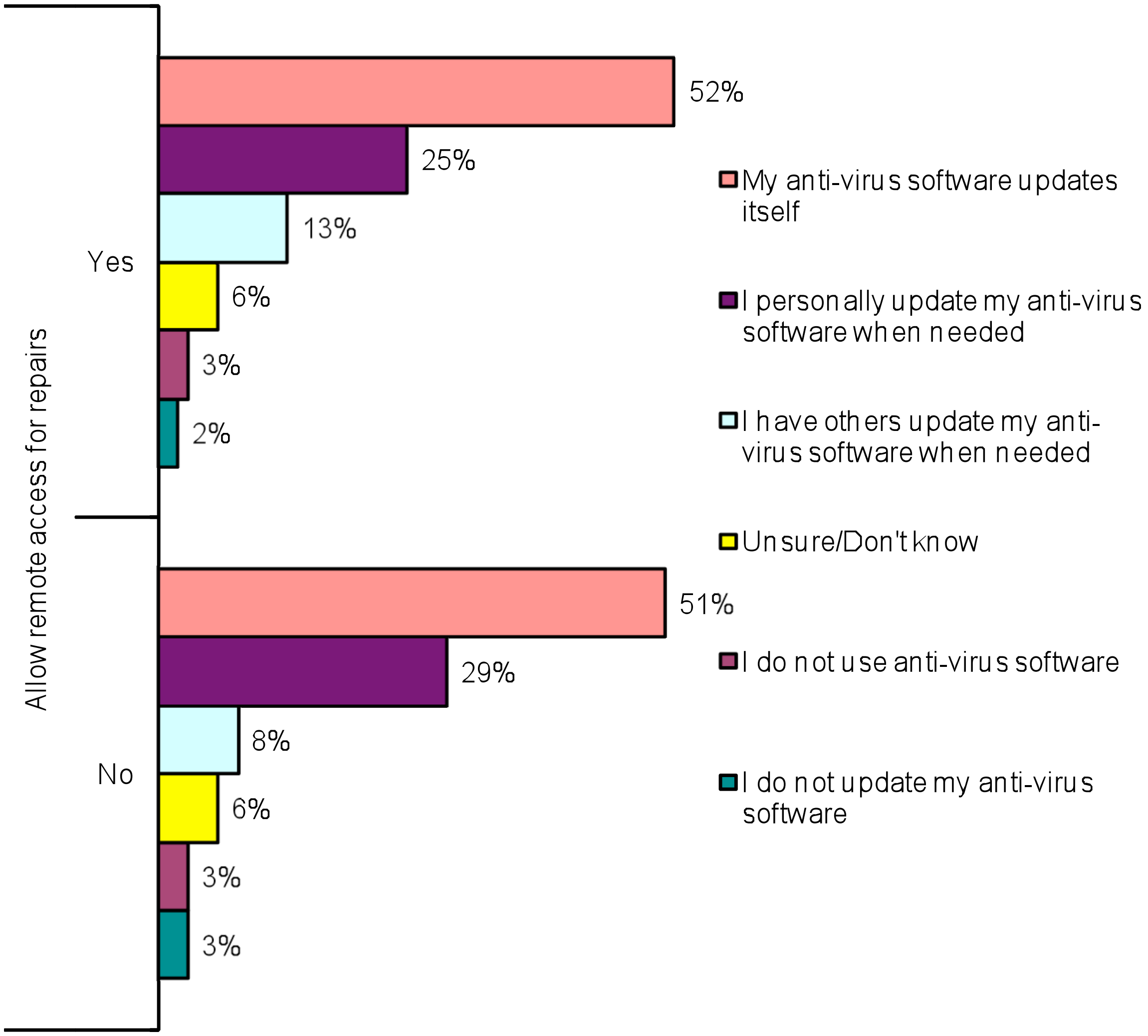
Respondents under the age of 44 are more likely to indicate that they personally update their anti-virus software as needed as compared to older respondents. Respondents over the age of 45 are more likely to say that their anti-virus software updates itself.

Usage of Anti-Virus Software – By Age



Later in the interview respondents were asked if they found their computer was infected, would they allow remote access to their computer to remove the virus. The following graph examines how respondents manage anti-virus software based on their willingness to have their computer repaired remotely. Results indicate respondents more likely to have their computer repaired remotely are also more likely to have others update their anti-virus software when needed, rather than do it themselves.

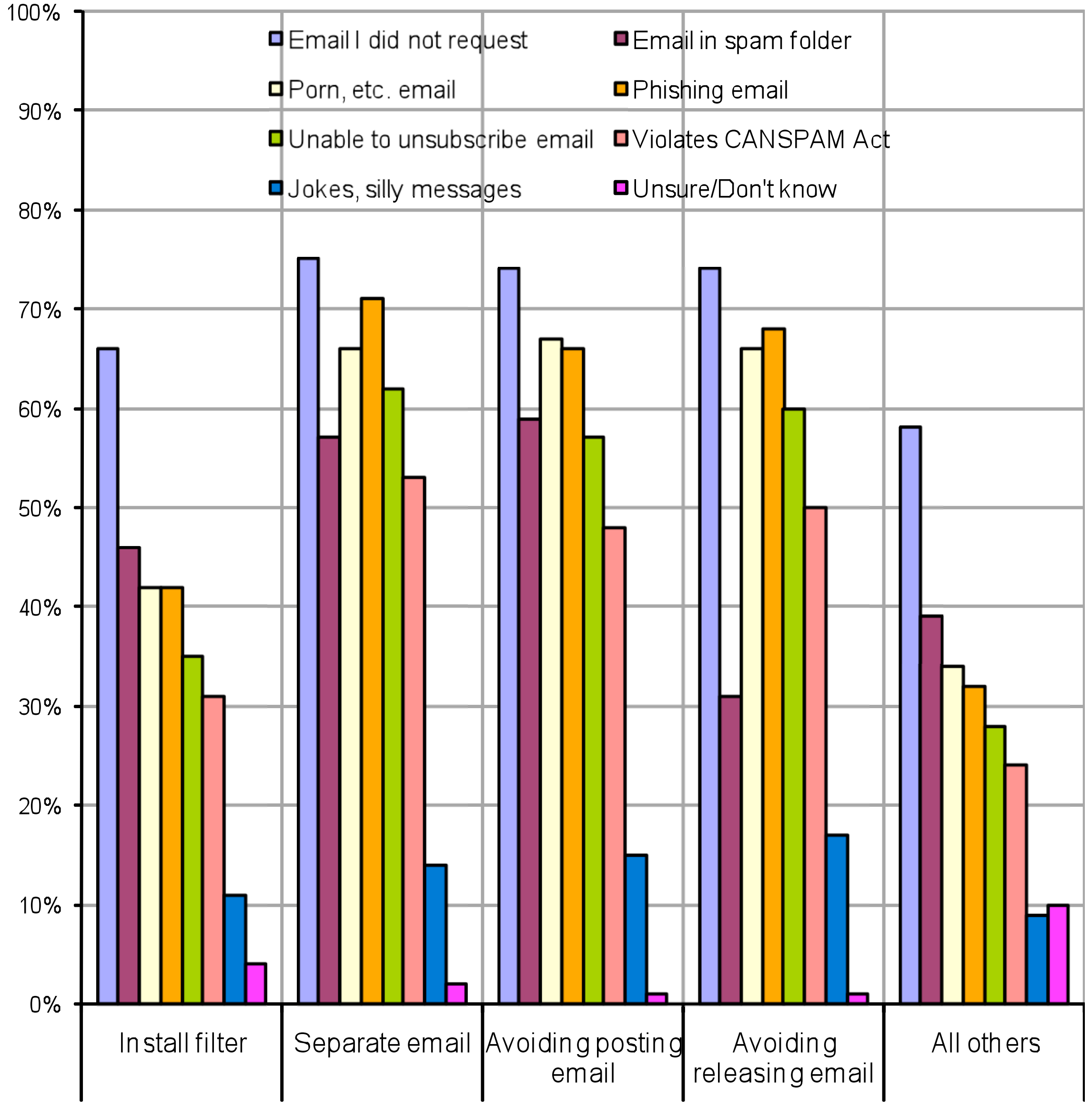
Usage of Anti-Virus Software – By Willingness to Accept Remote Repair



Question 8: How do you personally define spam?

Later in the interview, respondents were asked what actions, if any, they have taken to avoid receiving spam or junk email in their personal email. The graph below illustrates significant differences in how respondents define spam based on the actions they have taken to avoid it. Respondents who are more cautious with their email accounts, either by using a separate email account for possible spam or by avoiding the release or posting of their email address, are more likely to define spam as porn, phishing or email that cannot be unsubscribed from than are respondents who do not take these actions. This may suggest a correlation between definitions of spam and actions taken against spam.

Definition of Spam – By Action Taken to Avoid Spam

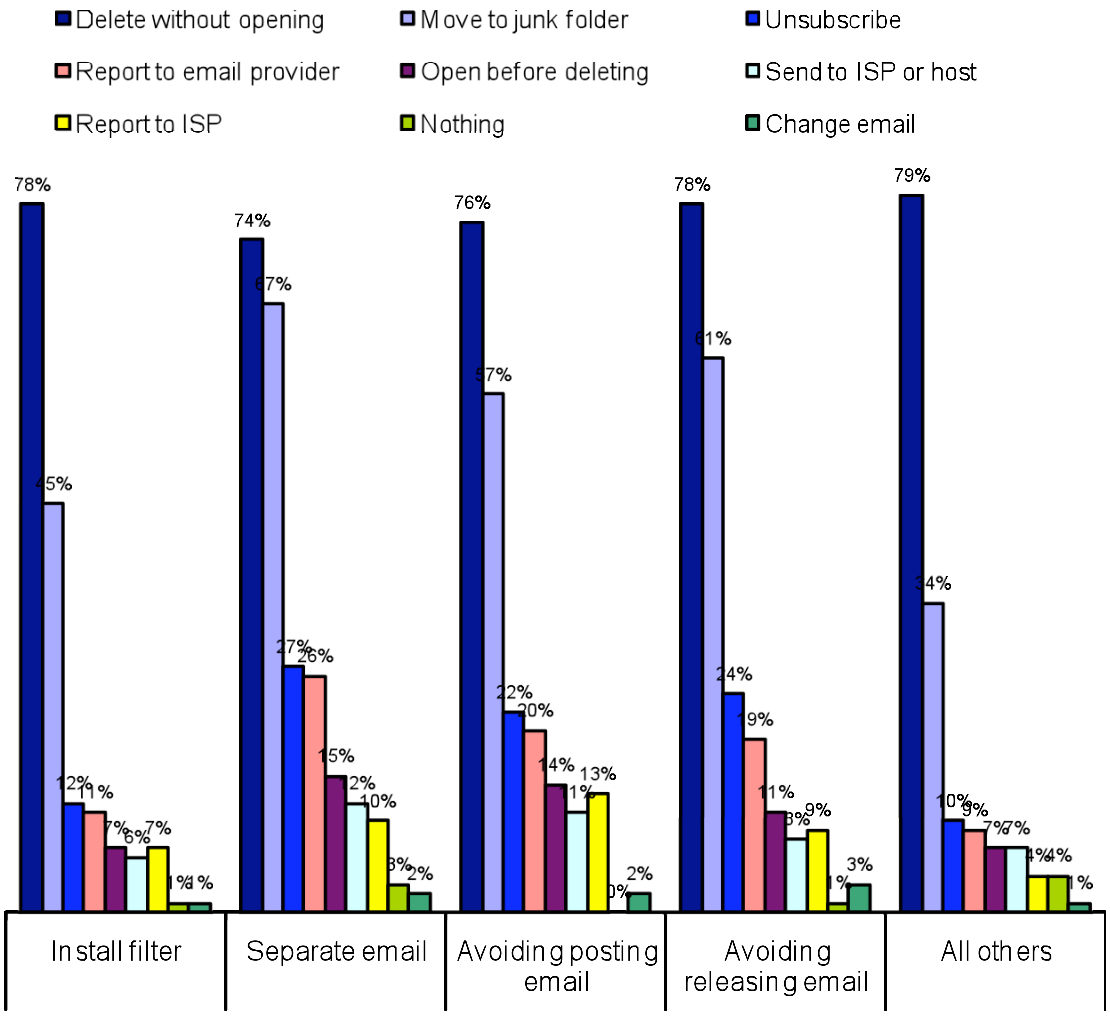


D. Actions Against Spam (Questions 10-19)

Question 10: *When you receive email that you think is spam, what do you usually do?*

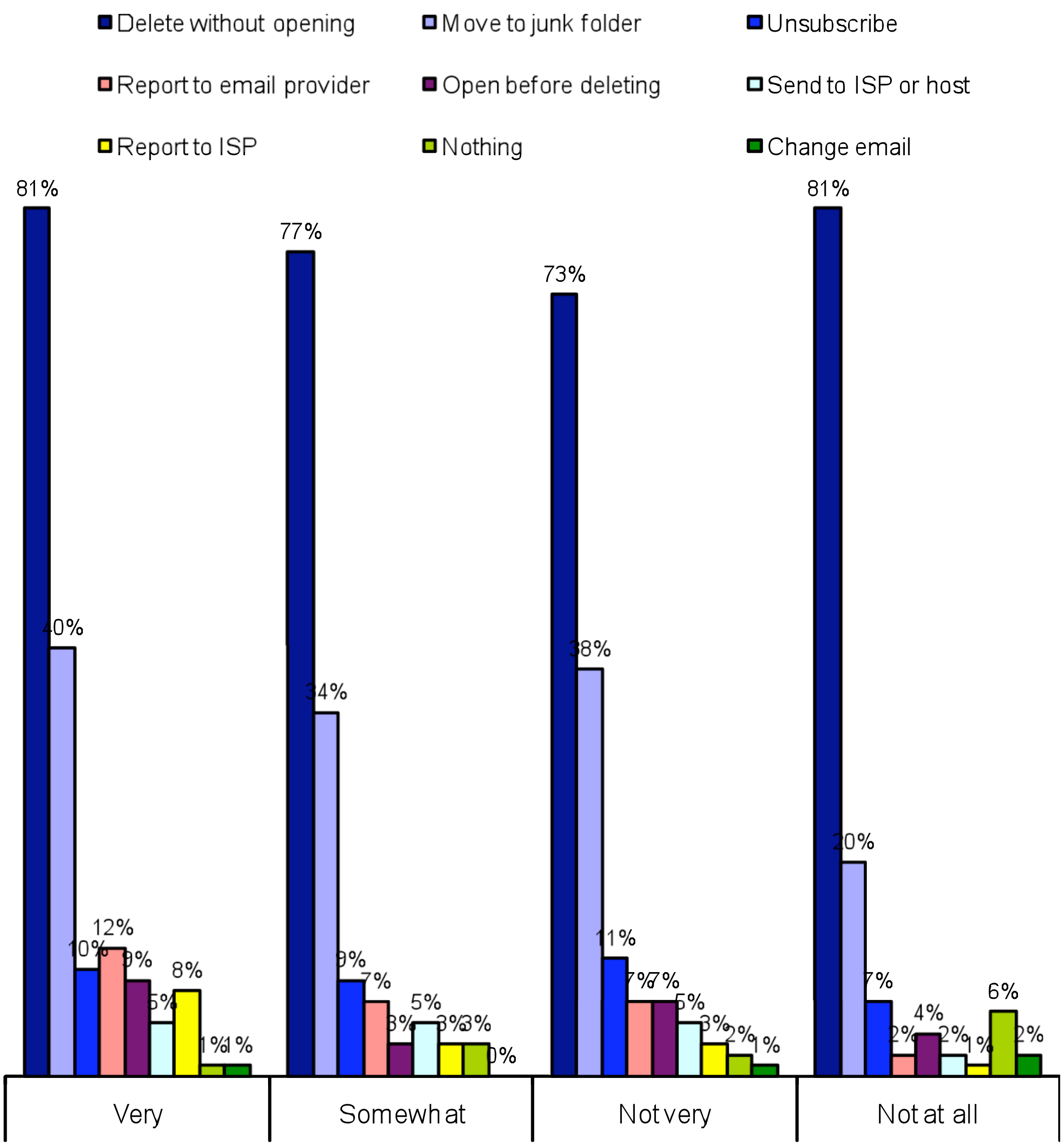
Besides asking what respondents did when they received spam, they were also asked later in the interview, what actions, if any, they have taken to avoid receiving spam. The graph below illustrates significant differences in what action respondents take when they receive spam based on the actions they have taken to avoid spam. Respondents who act more cautiously with their email accounts, either by maintaining a second email account or by avoiding posting of their email address, are more likely to mention moving spam to the junk folder, unsubscribing or reporting to the email provider than are respondents who do not take these actions.

Action When Receiving Spam—By Action Taken to Avoid Spam



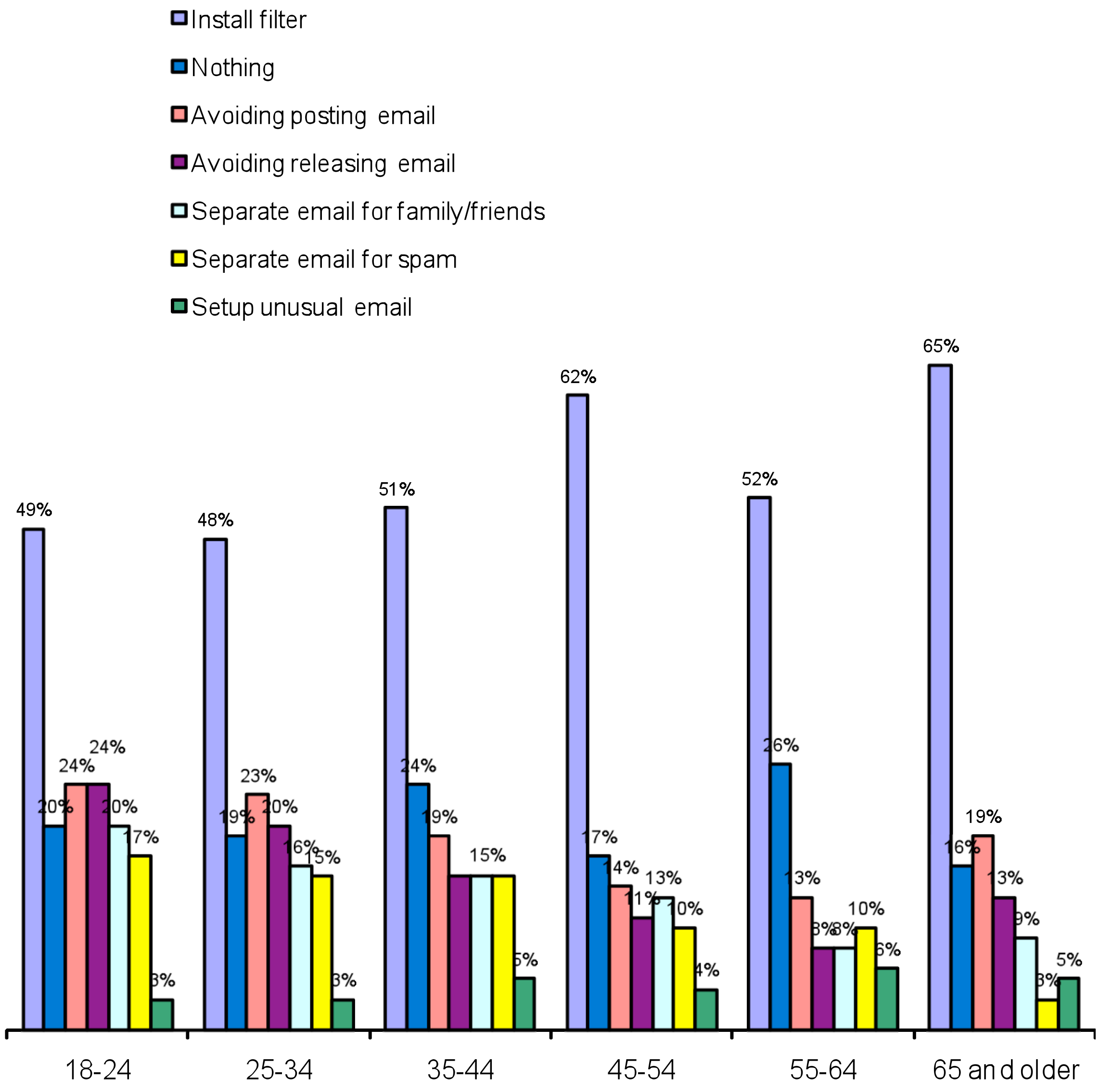
Responses to actions taken when receiving spam also were segmented based on the respondents' self-described Internet security experience. As presented below, respondents stating they have at least some experience with Internet security are more likely to take other actions in addition to deleting suspected spam without opening the email. This may suggest that with Internet security experience comes additional knowledge about options for dealing with spam.

Action When Receiving Spam— By Internet Security Experience



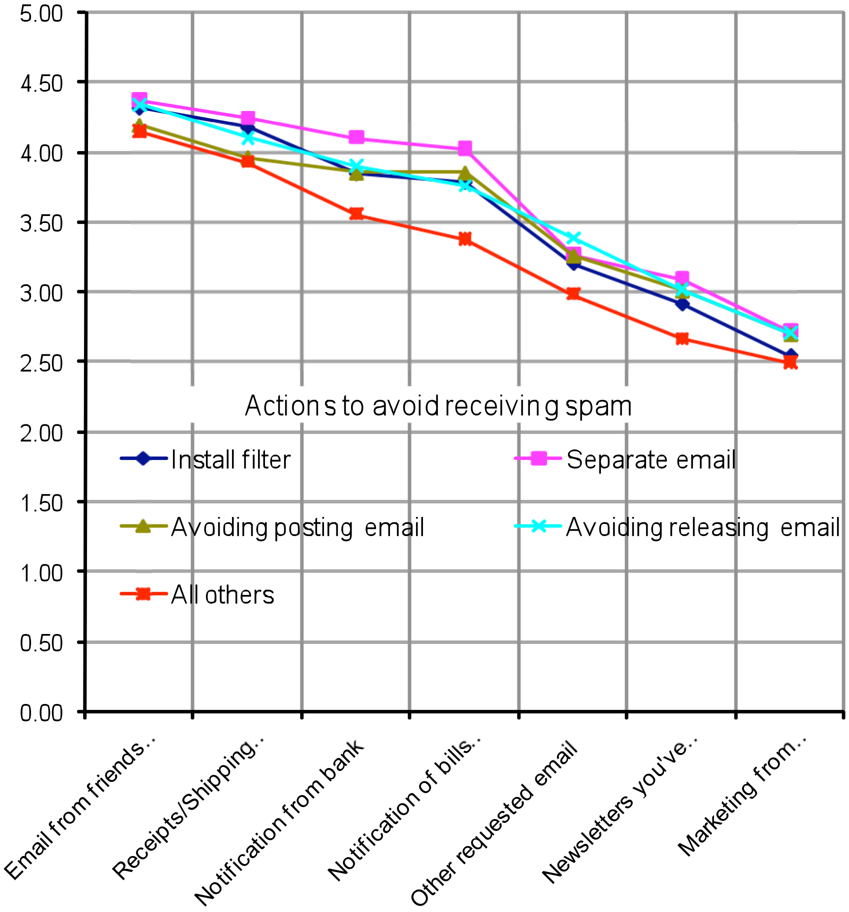
As in previous questions, results were segmented based on the age of the respondent. As presented below, respondents under the age of 35 are more likely to say they avoid posting or releasing their email addresses as a method to avoid spam. These respondents are also more likely to have a separate email account for family and friends. Respondents over the age of 65 are slightly more likely to say they have installed a filter.

Actions Taken to Avoid Spam – By Age



Later in the interview, respondents were asked what actions, if any, they have taken to avoid receiving spam or junk email. The graph below illustrates significant differences in how respondents rate the importance of various types of email based on the actions they have taken to avoid spam. Respondents with more control over their email addresses, either through a separate email account or by avoiding releasing and posting their email addresses, were more likely to rate the different types of email as more important than are other respondents. This may suggest that the use of email for a variety of purposes gains importance as the control of personal email addresses increases.

Important Personal Email – By Actions Taken to Avoid Spam

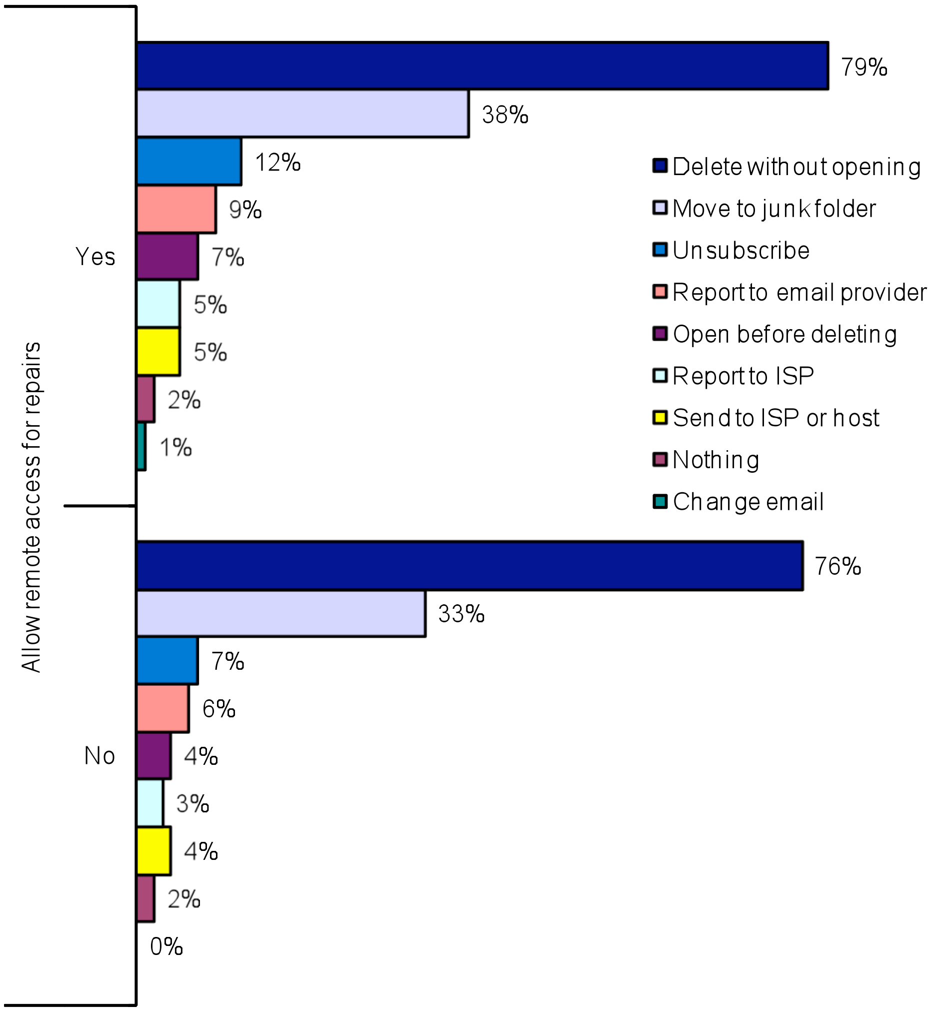


Question 10: *When you receive email that you think is spam, what do you usually do?*

Later in the interview respondents were asked if they found that their computer was infected, would they allow remote access to their computer to remove the virus.

The following graph examines how respondents manage spam based on their willingness to have their computer repaired remotely. Results indicate respondents more likely to have their computer repaired remotely are also more likely to use the unsubscribe link and change their email address when they receive mail that think is spam.

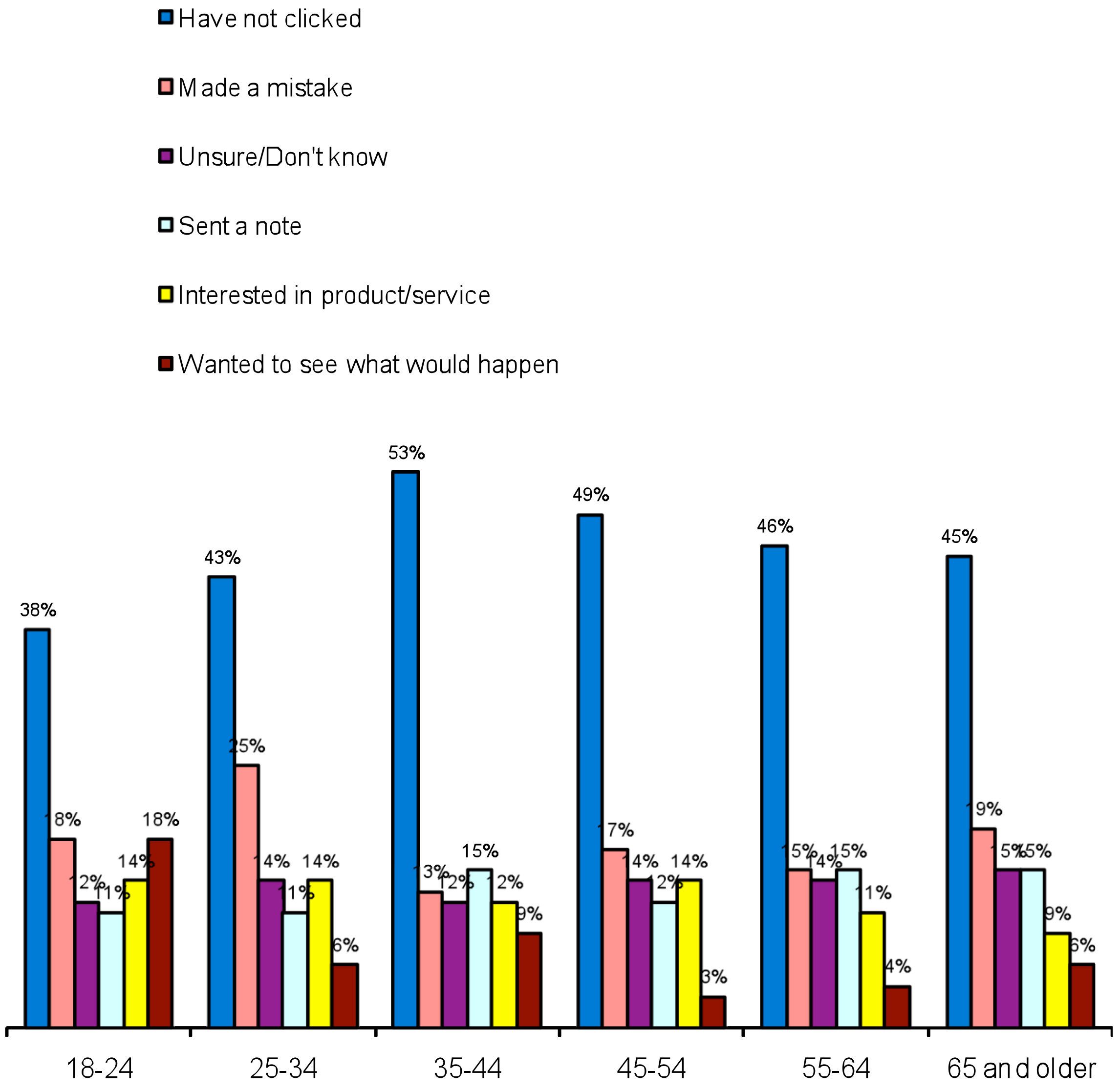
Action When Receiving Spam
By Willingness to Accept Remote Repair



Question 12: *If you have ever clicked on a link or replied to an email that you suspected was spam, why did you take this action?*

Respondents under the age of 24 are more likely than other respondents to say they wanted to see what would happen when they clicked or replied to an email they suspected was spam. Younger respondents are slightly more likely to admit to making a mistake.

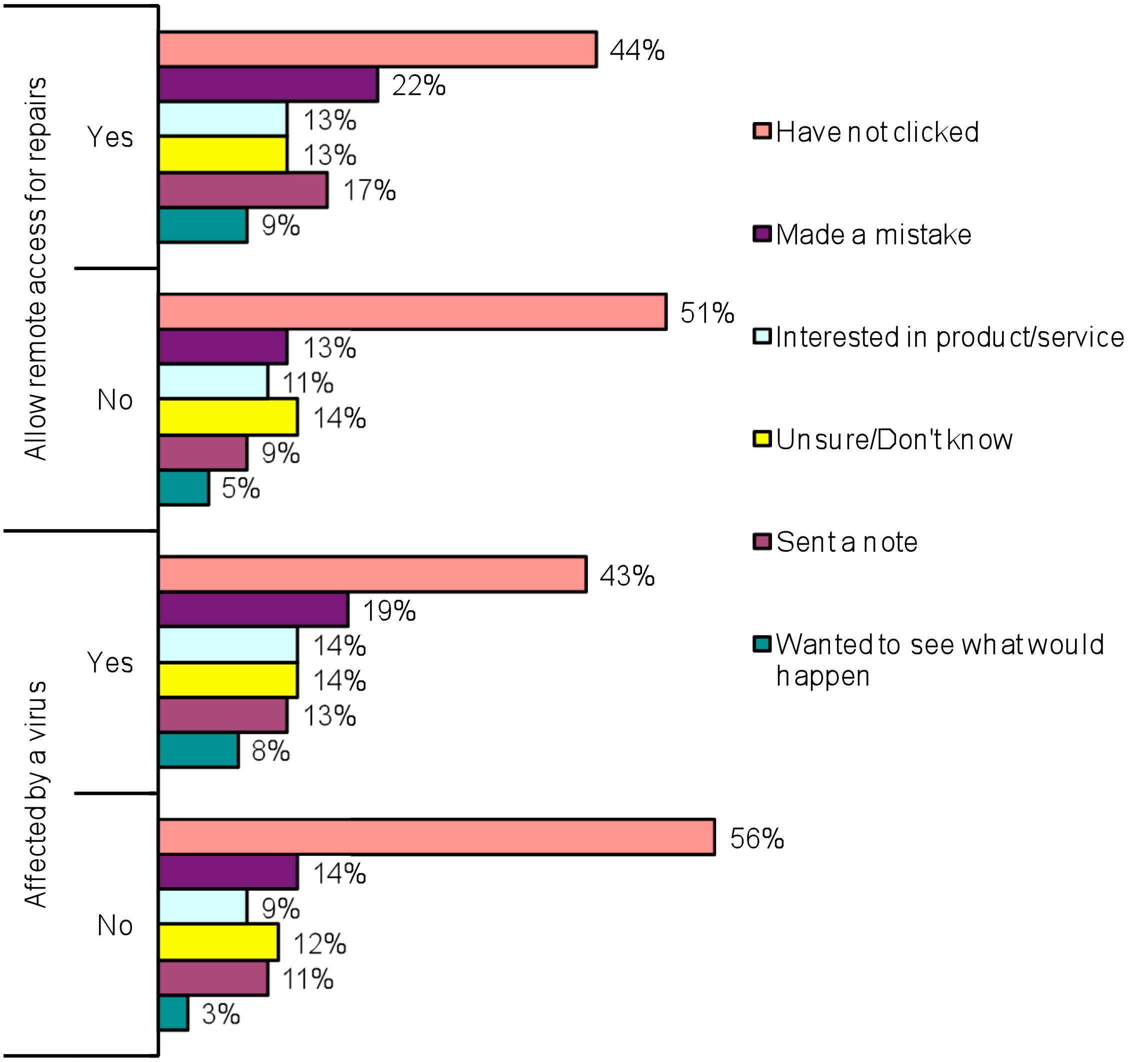
Why Responded To Spam – By Age



Later in the interview respondents were asked if their computer had previously been infected with a virus, and also asked separately if they would allow remote access to their computer to remove a virus if they found their computer had been infected.

The following graph examines why respondents replied to suspected spam based on their response to these other two questions: That is, on the respondents' willingness to have their computers repaired remotely and their past experience with a computer virus. Results indicate respondents willing to have their computer repaired remotely were more likely to say they made a mistake, sent a note of complaint, and wanted to see what would happen. In addition, respondents previously infected with a computer virus were more likely to say they took this action because they were interested in a product or service, or wanted to see what would happen.

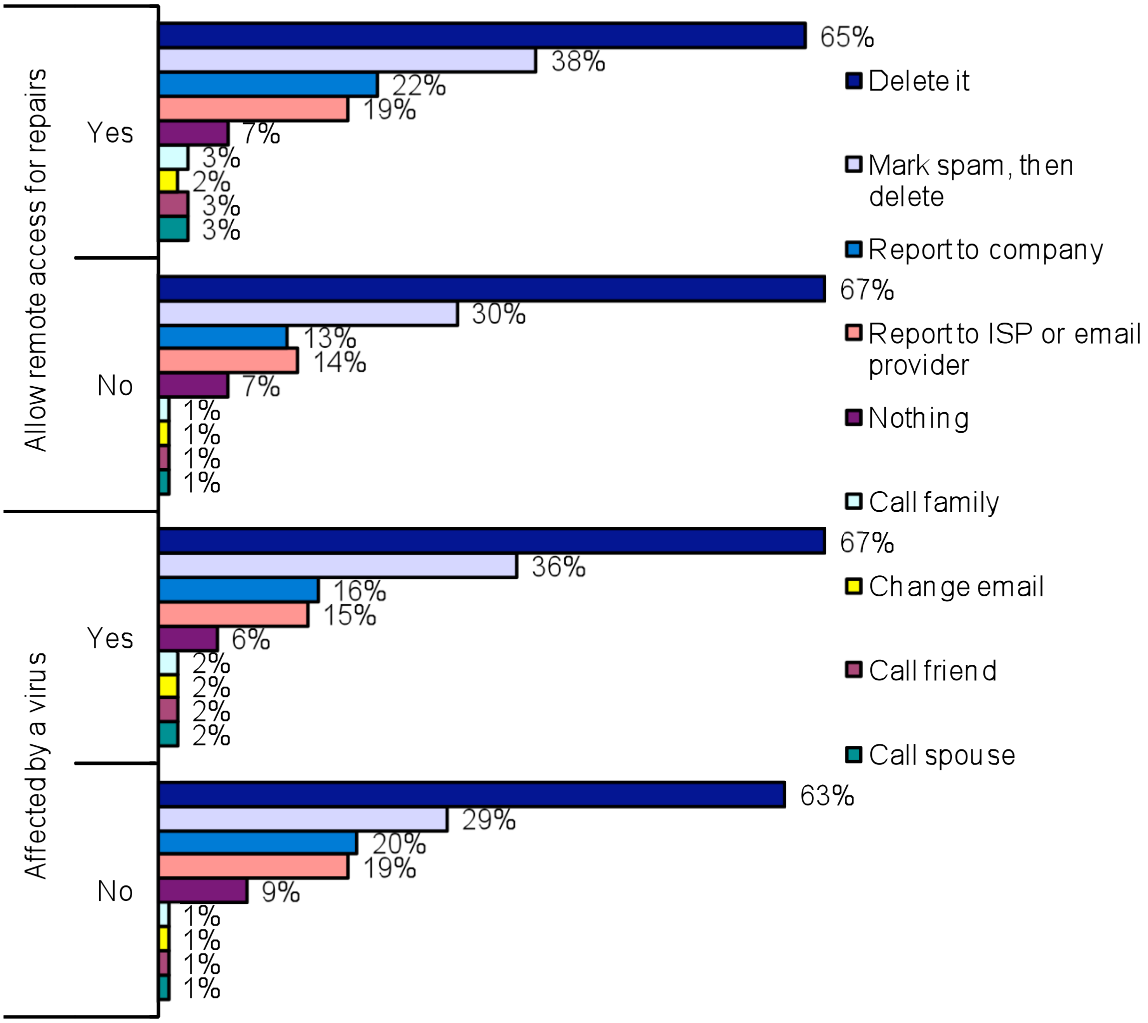
Why Responded to Spam
By Willingness to Accept Remote Repair and Previous Infection of a Computer Virus



Question 13: *When you receive email that you suspect to be fraudulent, what actions have you taken?*

The following graph examines how respondents manage fraudulent email based on 1) their willingness to have their computer repaired remotely and 2) past experience with a computer virus. Results indicate respondents more likely to have their computer repaired remotely are also more likely to mark junk email as spam then simply delete it, and to report it to a legitimate company or institution. In addition, respondents previously infected with a computer virus are also more likely to say that they will mark fraudulent email as spam and then delete it.

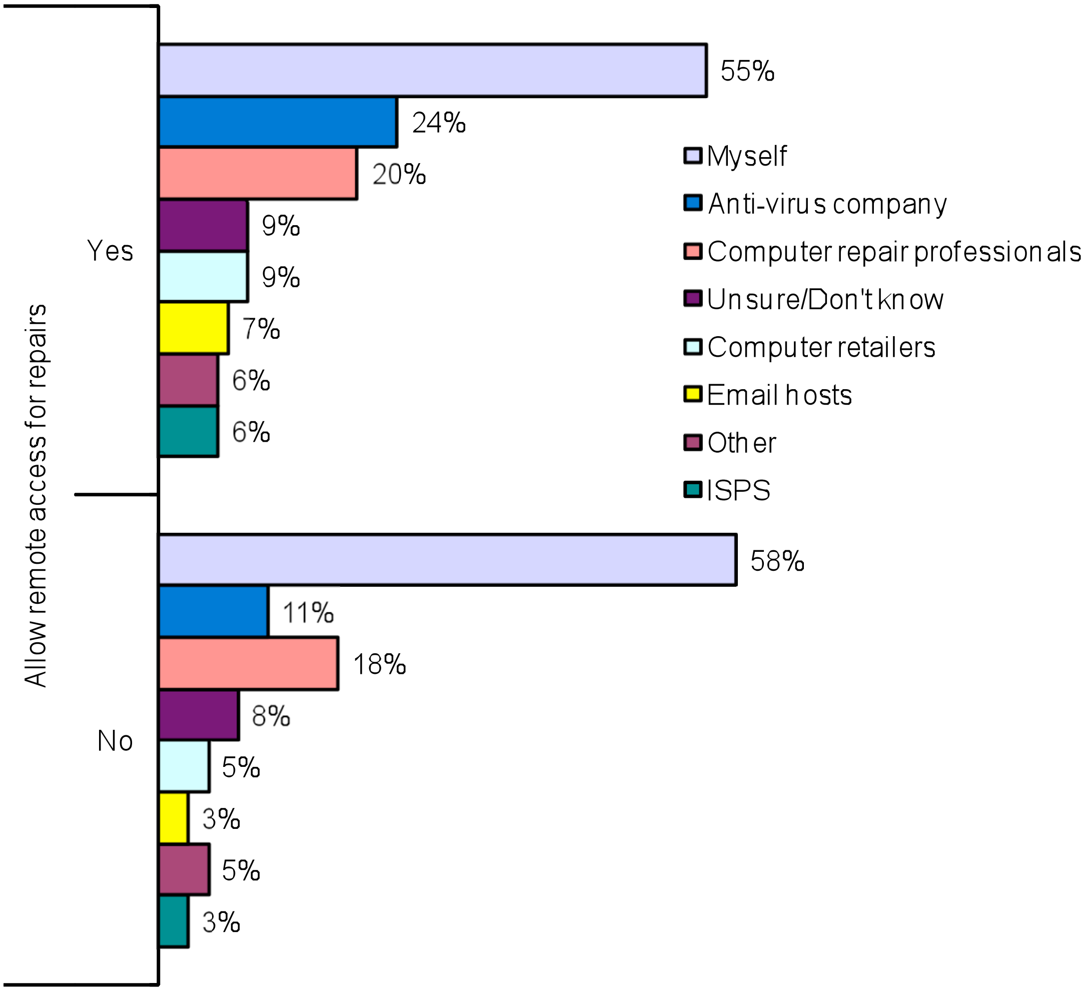
Action When Receiving Fraudulent Email
By Willingness to Accept Remote Repair and Previous Infection of a Computer Virus



Question 16: *Whom do you feel is responsible for fixing your computer if you find it has been contaminated with a computer virus, fraudulent email, spyware or spam?*

The following graph examines who respondents feel is responsible for fixing their contaminated computer based on their willingness to have their computer repaired remotely. Results indicate respondents willing to have their computer repaired remotely are more likely to say that anti-virus companies and computer retailers are responsible for fixing their contaminated computer.

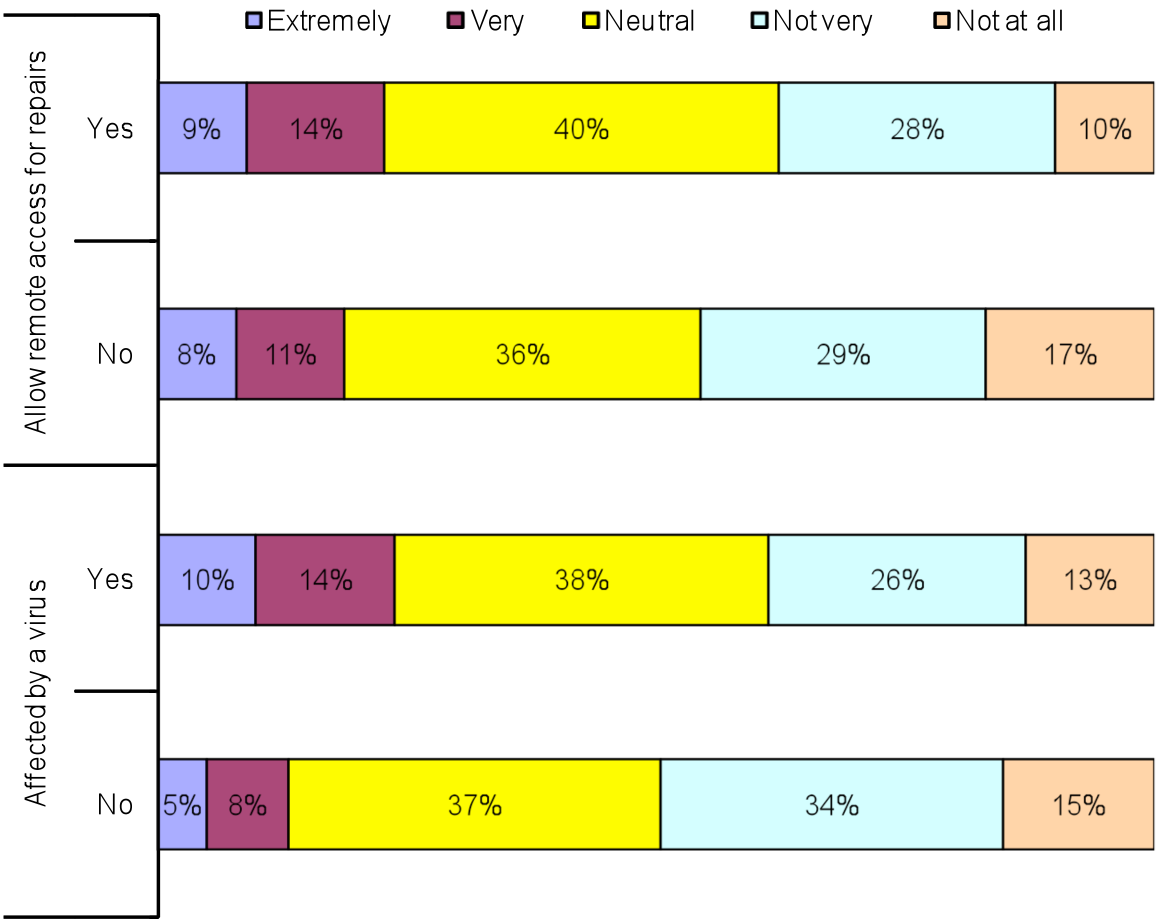
Repair Responsibility — By Willingness to Accept Remote Repair



Question 19: *Using a scale of 1 to 5 with 5 being extremely likely and 1 being not at all likely, what do you feel are your chances of getting this type of virus on your computer?*

The following graph examines respondents' perceived likelihood of getting a bot based on their willingness to have their computer repaired remotely and on past experience with a computer virus. Results indicate respondents more likely to have their computer repaired remotely also are more likely to believe they are likely to get a bot on their computer. These results are the same among respondents saying they were previously infected with a computer virus.

Likelihood of Getting a Bot
By Willingness to Accept Remote Repair and Previous Infection of a Computer Virus



Appendix B: Data By Willingness to Accept Remote Access

A major area of concern for MAAWG is how to block the epidemic of bots and malware that is rapidly spreading across consumers' systems. One aspect of this involves remotely accessing customers' computers to help infected subscribers remove viruses and fix their systems.

Below are a few data points examining how willing consumers are to allow network operators or vendors access to their systems for the purpose of removing detected viruses and bots. This information is summarized from the Detailed Reporting and Appendix A sections of this report.

- Almost half, 63%, of respondents said they would allow remote access to repair their computer.
  - Most, 17%, would look to their anti-virus vendor to repair their computers.
  - The idea of ISPs or email providers offering remote services to remove malware is still new and is not yet expected by consumers. Of those allowing remote access, only 7% said they would look to their ISPs, 3% to a Web site and 2% to their email hosting company for repairs.
- Education regarding bots and messaging abuse could be an important factor in increasing the number of customers that would allow network operators or vendors remote access to remove malware on their systems. The more consumers knew about bots the more open they were to allowing remote access to their systems.
  - Of those allowing access, 25% believe they are either "extremely" or "very likely" to get a bot, compared to 20% of all consumers surveyed.
  - Overall, 85% of those allowing remote access said they were aware of bots compared to 82% of all consumers surveyed.
- Those who would allow access also are more likely to have others update their anti-virus software.
- Consumers who would allow remote access to their systems may be slightly more aware of security issues in their usage of email in general. These consumers are more likely to:
  - Unsubscribe rather than just delete email they considered spam
  - Mark unwanted email as junk and to report it to the company
  - Use separate email addresses for situations they think may generate spam
- These consumers also may be a little more comfortable or experienced with email. They were more likely to admit they clicked on spam because it was a mistake, they wanted to send a note of complaint or they just wanted to see what would happen.
- Age is an important factor in determining how consumers repair their computers.
  - Those under 24 years old are more likely to take their computer to a repair service.
  - Consumers between 24 and 44 are more likely to repair their computers themselves.

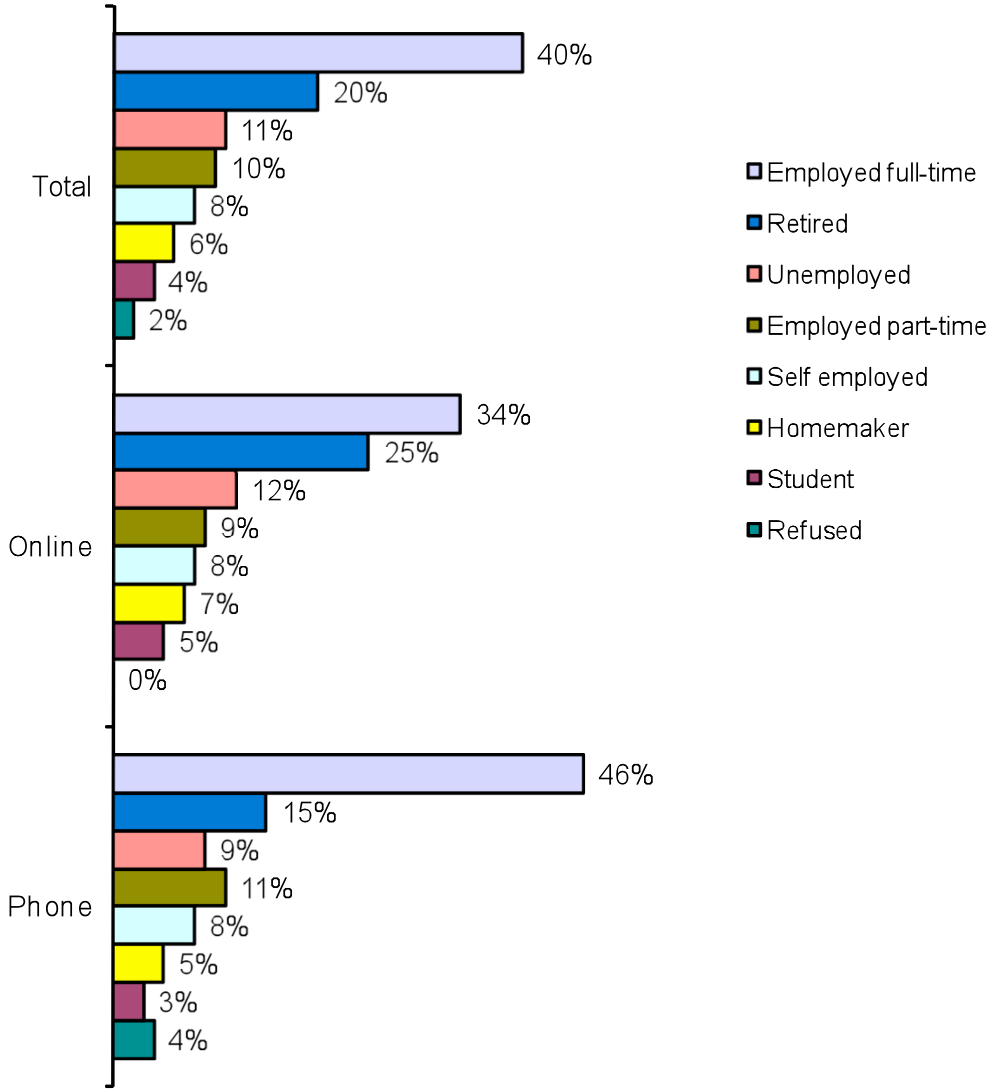
- Starting with those 45 and older, consumers increasingly look to a repair professional to fix their machines. Those over 65 are more likely than others to ask a professional or their ISPs to repair their computers.

Appendix C: Demographics

Question 20: What is your employment status?

Most respondents indicate they are employed (58%). This response is higher among respondents completing the interview over the telephone (65%) than among respondents completing the interview online (51%). Nearly one-fourth of all online respondents are retired, a slightly higher rate than among telephone respondents.

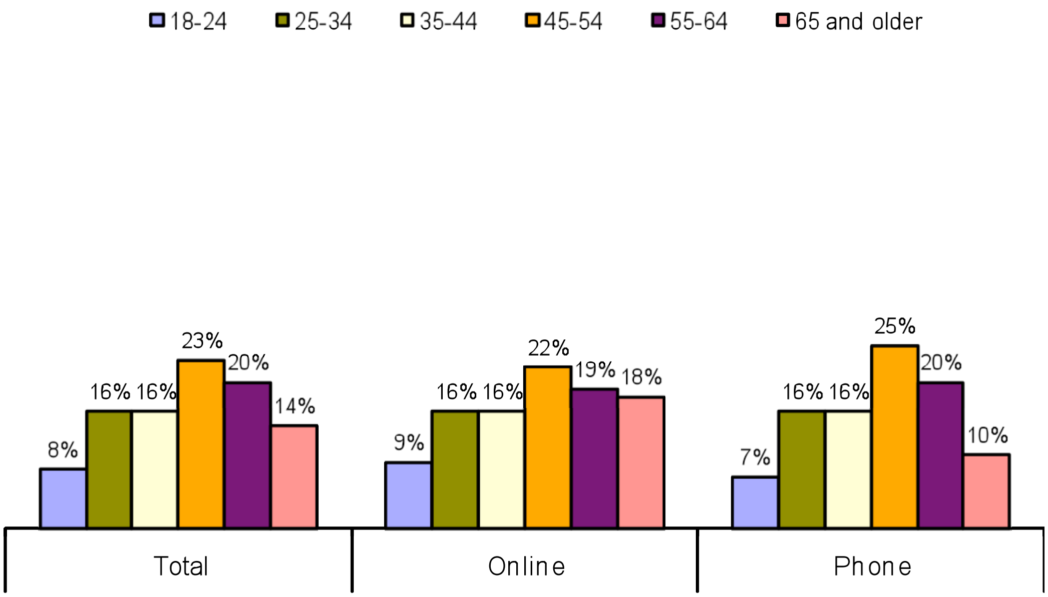
Employment Status



Quesiton 21: May I please have your age?

Respondents represent a variety of age groups. Age quotas were established in selecting participants in order to ensure that all age groups were included in this study.

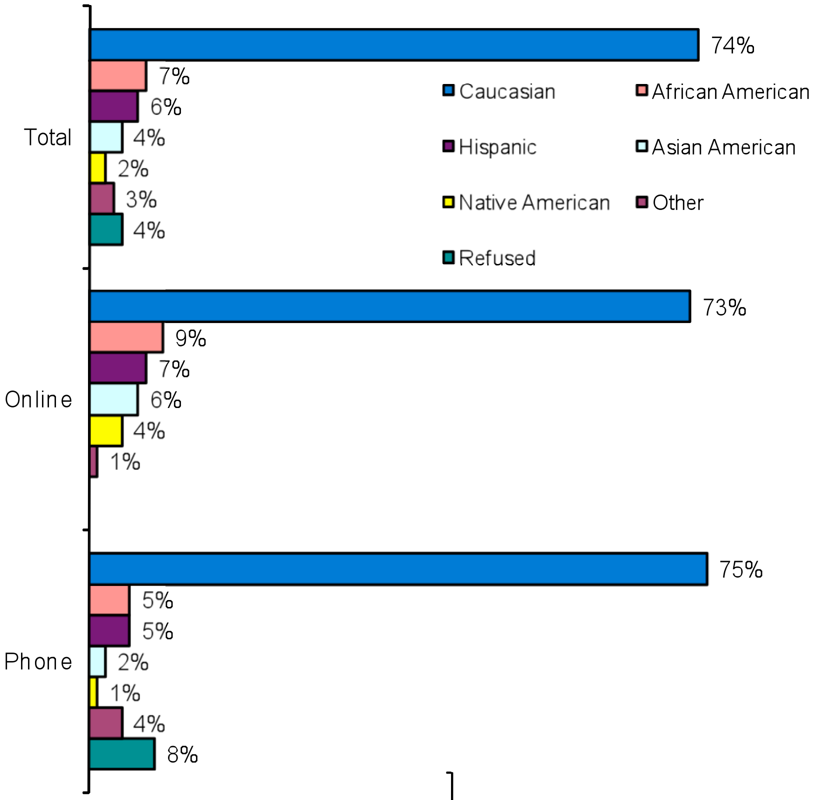
<u>Respondent Age</u>



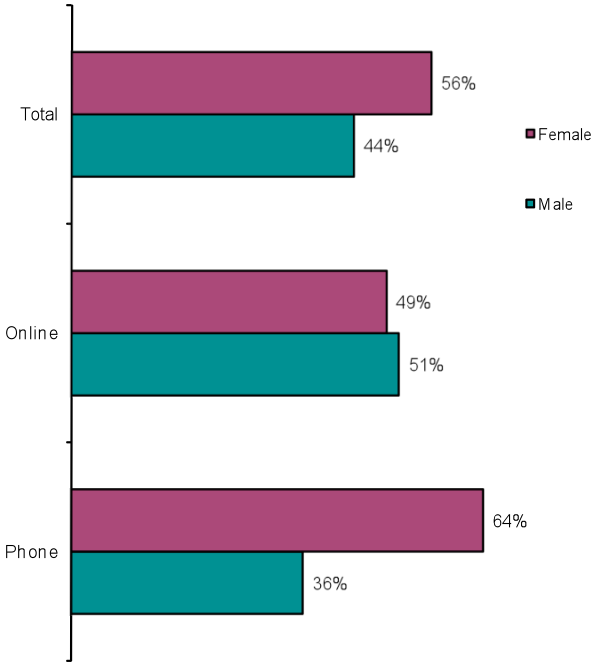
Question 22: *And finally, your ethnicity?*

All ethnicities were represented in this survey. While results suggest that some minorities may be underrepresented based on demographics, respondents were not allowed to participate unless they had an email address not managed by a company IT professional. This selection criterion may have resulted in a higher representation of Caucasian respondents than other ethnicities.

Respondent Ethnicity



Question 23: Respondent Gender



Appendix D: Methodology

Methodology

Insights Worldwide Research conducted 800 interviews—400 by telephone and 400 online. Potential telephone interview respondents were selected using lists provided by Insights Worldwide Research. Lists are designed for research purposes only and include the names and phone numbers of 20,000 potential respondents within the continental U.S. Potential respondents were randomly selected from these lists, contacted by telephone, and asked to participate in this survey. Each interview lasted approximately 10 minutes.

Using the selection criteria established by MAAWG and Insights, potential online survey participants were contacted by Greenfield Online, the leader in online surveys, and asked to participate in an online survey. Those who qualified completed the survey.

Margin of Error

Every sample for a survey is subject to a range of variability. This range of variability refers to the chance variation in results that may occur when a sample, instead of the total population, is surveyed. This variability is known as the *standard error* and reflects the difference between the sample findings and those that would occur from a 100% enumeration of the population using the same questionnaire and research procedures. A statistically estimated sampling error is commonly used as a comparative measure of projectability for a survey sample. The following table presents the sample size and the sampling error:

Market	**Sample Size**	**Standard Error**
Online respondents	400	± 5.0%
Telephone respondents	400	± 5.0%
Total	800	± 3.5%

Questionnaire

With input from the MAAWG Consumer Survey Project team, Insights designed a questionnaire for the interviews. Once approved, minor changes in wording were made to the questionnaire to accommodate both telephone and online interviews. A copy of the questionnaire can be found in Appendix E.

Qualifiers

In order to qualify participants as general consumers for this survey, respondents were asked about their level of security and online expertise. Respondents who classified themselves as experts in Internet security issues, including firewalls, spam, junk mail and computer viruses, were excluded from participating in this survey. In addition, respondents were required to have an email address that is not managed or maintained by a professional IT department within the workplace.

Randomization of Questions

To avoid the problem of systematic position bias—where the order in which a series of questions is asked systematically influences the answer to some of the questions—several of the questions in this survey were randomized such that respondents were not consistently asked the questions in the same order. Details of this occurrence are included in the Detailed Findings section of this report as they relate to a specific question.

Do not Read Questions

For the telephone interviews, the "do not read" questions were asked without providing the respondent with any specific answers from which to choose. For this type of question, respondents were able to mention any issue, topic, or general response relevant to the question without being constrained by a limited number of options. As the interview took place, interviewers recorded the responses that matched those listed in the questionnaire. If a response was not listed, it was recorded separately. Online surveys included a list of responses to choose from, but respondents were given the opportunity to record an alternate response if it was not listed.

Multiple-Response Questions

Some questions within the survey were presented in a multiple-response format. For this type of question, each respondent was given the opportunity to select more than one response. For this reason, the response percentages will typically total more than 100 and represent the frequency of response for a particular response.

Interviewing Dates

Interviewing for the MAAWG Consumer Survey began on December 15th, 2008, and was completed on December 22nd, 2008. Telephone interviews took place between 3 PM and 8 PM PST, Monday through Friday and 11 AM to 5 PM on Saturday and Sunday.

Data Processing

Completed interviews were tabulated using a computer database for analysis. A cross-tabulation program was used to sort responses. The computer tabulation, including the various segments of the sample, is available through Insights Worldwide Research.

Appendix E: Questionnaire

MAAWG ATTITUDE, AWARENESS AND USAGE RESEARCH

TO THE RESPONDENT: Hi, my name is **(FIRST AND LAST NAME)** with Insights Worldwide Research. Today we are interviewing a few select individuals regarding their use of the internet and email for an industry group that works against spam and online abuse. Your opinions are valuable and will help improve internet and email services. We are not selling anything and everything you say will be held in confidence.

1. On a scale of one to five with five being an expert, how would you describe your experience with security on the internet including firewalls, spam, junk mail and computer viruses?

    5 (An expert)........................... 1 **POLITELY DISCONTINUE**
    4 (Very experienced) 2
    3 (Somewhat experienced)...... 3
    2 (Not very experienced) 4
    1 (Not at all experienced) 5

2. Do you have an email address at work, at home, or both?

    Work .... 1 **GO TO Q4**
    Home .... 2 **GO TO Q5**
    Both .... 3 **ASK Q3**

3. Are they different or the same email addresses?

    Different .... **1 GO TO Q5**
    Same .... 2 **ASK Q4**

4. Regarding your work email address, does your company have an IT service or department that manages and/or maintains the security of your work email?

    Yes 1 **POLITELY DISCONTINUE IF WORK IS ONLY EMAIL ADDRESS**
    No 2 **CONTINUE**

5. How important are the following when considering sending and receiving personal email? Please use a scale of one to five where 5 means it is critically important to you and 1 means it is unimportant. **READ AND ROTATE**

Email from friends and family	5	4	3	2	1
Newsletters you've subscribed to	5	4	3	2	1
Receipts or shipping details for purchases you've made	5	4	3	2	1
Notifications of bills to be paid	5	4	3	2	1
Notifications from your bank or other financial institution	5	4	3	2	1
Marketing from companies you've purchased from or plan to purchase from	5	4	3	2	1
Other email that you have signed up for........................	5	4	3	2	1

6. Which of the following applies to your personal computer?

READ AND RECORD ONE RESPONSE
I do not use anti-virus software....................................1 **GO TO Q8**
I personally update my anti-virus software when needed 2 **GO TO Q8**
I have others update my anti-virus software when needed 3 **GO TO Q8**
I do not update my anti-virus software..........................4 **ASK Q7**
My anti-virus software updates itself............................5 **GO TO Q8**
Unsure/Don't know ....6 **GO TO Q8**

7. If you have ever been affected by a virus on your computer, what action, if any, did you take?

DO NOT READ. MULTIPLE RESPONSES ALLOWED
Report to my ISP 1
Report to my email host...2
Report to virus software company 3
Change my email address 4
Had it repaired remotely by a computer repair service .5
Took it to a computer repair service 6
Repaired myself...7
Had a friend or family member repair 8
Other **RECORD** 9
Nothing 10
I've never been infected...11

8. How do you personally define spam?

DO NOT READ. MULTIPLE RESPONSES ALLOWED
Email I did not request...1
Email from porn, pills, body part enlargement, online casinos, etc..2
Email that contains a virus or 'phishing' scheme 3
Email that violates the U.S. CANSPAM Act....................................4
Email in my spam or junk mail folder 5
Email from sources not able to 'unsubscribe' 6
Jokes and silly messages forwarded to me 7
Other **RECORD** 8
Unsure/Don't know 9

9. When going through your email box and deciding what mail is spam and what is legitimate, what indicators do you rely on to help you decide?

DO NOT READ. MULTIPLE RESPONSES ALLOWED

By the sender name.................................1
By the receiver name................................2
By the subject..3
By the time...4
By icons or other visual indicators that appear in my inbox beside the message 5
Open up email and look at the content......6
I want all the email I receive 7
Other **RECORD** 8
Nothing 9

10. When you receive email that you think is spam, what do you usually do?

DO NOT READ. MULTIPLE RESPONSES ALLOWED

Hit the This Is Spam button or move to junk mail folder 1
Delete it immediately without opening it 2
Open and read carefully before deleting................................ 3
Send to my ISP (Internet service provider) or email host 4
Report to my ISP 5
Report to my email provider... 6
Change my email address 7
Use the Unsubscribe link... 8
Other **RECORD** 9
Nothing 10

11. What actions, if any, have you taken to avoid receiving spam or junk email in your personal email?

DO NOT READ. MULTIPLE RESPONSES ALLOWED

Install a spam or junk mail filter 1
Use a separate email address for times when spam might occur ...2
Avoid posting email address on web sites.......................................3
Avoid giving out email address..4
Set up unusual email address that is hard to guess........................5
Using a separate email for friends and family..................................6
Other **RECORD** 7
Nothing 8

12. If you have ever clicked on a link or replied to an email that you suspected was spam, why did you take this action?

DO NOT READ. MULTIPLE RESPONSES ALLOWED
Interested in product or service being offered in email .1
Wanted to see what would happen..............................2
Made a mistake 3
Sent a note to remove me or to complain....................4
Have not clicked on a link or replied to suspected spam 5
Unsure/Don't know 6
Other **RECORD** 7

13. When you receive email that you suspect to be fraudulent, what actions have you taken?

DO NOT READ. MULTIPLE RESPONSES ALLOWED
Delete it..1
Mark as spam then delete it..............................2
Report to my ISP 3
Report to my email provider..............................4
Change my email address 5
Report to the legitimate company or institution..6
Call spouse 7
Call family member other than spouse 8
Call friend that is not a family member 9
Other **RECORD** 10
Nothing 11

14. Who do you feel is most responsible for stopping the creation of computer viruses, fraudulent email, spyware, and spam?

DO NOT READ. ONE RESPONSE ONLY
The government.......................... 1
ISPs 2
Retailers..................................... 3
Professional associations 4
Industry leaders 5
Email hosts 6
Virus protection software 7
Other **RECORD** 8
Unsure/Don't know 9

15. How would you rate the performance of (**PERSON'S RESPONSE TO Q17**) for stopping these viruses? Please use a scale of one to five where 5 means performance is outstanding and 1 means performance is unacceptable.

5 4 3 2 1

16. Who do you feel is responsible for fixing your computer if you find it has been contaminated with a computer virus, fraudulent email, spyware, or spam?

DO NOT READ. MULTIPLE RESPONSES ALLOWED

Myself	1
ISP providers	2
Computer retailers	3
Computer repair professionals	4
Anti-virus company	5
Email hosts	6
Other **RECORD**	7
Unsure/Don't know	8

17. If you found that your computer was infected, who would you allow access to your computer to remove the virus?

READ AND RECORD. MULTIPLE RESPONSES ALLOWED

Remotely by ISP or email provider	1
Remotely by Email host	2
Remotely by a Web site	3
Remotely by computer repair service	4
Remotely by anti-virus software company	5
Remotely by a friend or family	6
Have professional come to my home or office to repair	7
I would repair by myself	8
Take computer to repair service	9
Other **RECORD**	10
Unsure/Don't know	11

18. Are you aware that there are malicious viruses that can control your computer without your knowledge and then use your computer to spread spam?

Yes	1
No	2

19. Using a scale of one to five with 5 being extremely likely and 1 being not at all likely, what do you feel are your chances of getting this type of virus on your computer?

5 4 3 2 1

Just a few more questions for classification purposes.

20. What is your employment status or profession?

DO NOT READ. RECORD

Self employed	1
Employed full-time	2
Employed part-time	3
Retired	4
Homemaker	5
Unemployed	6
Student	7
Other ________________	8
Refused	9

21. May I please have your age?

DO NOT READ. RECORD

18 to 24 years old	1
25 to 34 years old	2
35 to 44 years old	3
45 to 54 years old	4
55 to 64 years old	5
65 or older	6
Refused	7

22. And finally, your ethnicity?

DO NOT READ. RECORD

Caucasian	1	Asian American	4
African American	2	Native American	5
Hispanic	3	Pacific Islander	6
		Other	7
		Refused	8

23. **DO NOT ASK: DO NOT READ RECORD**

Sex:	Male	1
	Female	2

We really value your answers, responses, and patience. Thank you very much for your time.